T.C.
KONYA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

WİNDOWS VE GNU/LİNUX İŞLETİM SİSTEMLERİNDE GÜVENLİK SIKILAŞTIRMALARININ ANALİZİ VE İYİLEŞTİRME MODELİ

Serhat YAPICI

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Ocak-2025
KONYA

TEZ KABUL VE ONAYI

Serhat YAPICI tarafından hazırlanan "WİNDOWS VE GNU/LİNUX İŞLETİM SİSTEMLERİNDE GÜVENLİK SIKILAŞTIRMALARININ ANALİZİ VE İYİLEŞTİRME MODELİ" adlı tez çalışması 15/01/2025 tarihinde aşağıdaki jüri tarafından oy birliği / oy çokluğu ile Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Başkan Prof. Dr. Halife KODAZ (Konya Teknik Üniversitesi)	……..
Danışman Dr. Öğr. Üyesi Hazim İŞCAN (Konya Teknik Üniversitesi)	……..
Üye Dr. Öğr. Üyesi Onur İNAN (Selçuk Üniversitesi)	……..

Yukarıdaki sonucu onaylarım.

Prof. Dr. Mevlüt UYAN
Enstitü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Serhat YAPICI

Tarih: 15.01.2025

ÖZET

YÜKSEK LİSANS TEZİ

WİNDOWS VE GNU/LİNUX İŞLETİM SİSTEMLERİNDE GÜVENLİK SIKILAŞTIRMALARININ ANALİZİ VE İYİLEŞTİRME MODELİ

Serhat YAPICI

Konya Teknik Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Hazim İŞCAN

2025, 230 Sayfa

Jüri
Dr. Öğr. Üyesi Hazim İŞCAN
Prof. Dr. Halife KODAZ
Dr. Öğr. Üyesi Onur İNAN

Günümüzde bilişim dünyasındaki hızlı gelişmeler, siber saldırıların çeşitlenmesine ve artmasına yol açmıştır. Güvenlik açıklarının çoğalması ve savunmasız sistemlerin hedef haline gelmesiyle birlikte dijital ortamda karşılaşılan riskler artış göstermiştir. Bu sebep ile bilişim sistemlerinin temel yapı taşı olan işletim sistemlerinin güvenliği önemli derecede değer kazanmıştır. Bu tez, Windows ve GNU/Linux işletim sistemlerinin güvenlik risklerini derinlemesine inceleyerek, bu sistemlerin güvenliğini artırmaya yönelik yenilikçi ve sistematik stratejiler geliştirmeyi amaçlamaktadır. Özellikle güvenlik seviyelerinin yükseltilmesi için otomatize çözümler üreterek, kullanıcı yetkilendirme, gereksiz servislerin kapatılması, ağ güvenliği ve yazılım güncellemeleri gibi temel güvenlik önlemleri kapsamında iyileştirmeler yapılmıştır. Çalışmada, Türkiye Cumhuriyeti Dijital Dönüşüm Ofisi'nin Bilgi ve İletişim Güvenliği Rehberi (BİGR) ile birlikte uluslararası güvenlik standartları (CIS Benchmarks, ISO 27001, NIST SP 800-53 gibi) esas alınarak uyumlu bir yaklaşım benimsenmiştir. Hem teorik hem de uygulamalı bir şekilde güvenlik yönetim sistemlerinin etkinliğini artırmayı hedefleyen bu çalışma, işletim sistemlerinin güvenliğini güçlendirerek modern siber tehditlere karşı sağlam bir savunma mekanizması oluşturmayı amaçlamaktadır. Geliştirilen iyileştirme modeli, Bilgi ve İletişim Güvenliği Rehberi (BİGR) içerisindeki kritiklik seviyelerine göre 3 gruba ayrılmıştır. Önerilen iyileştirme modelinin, siber güvenlik alanında daha dayanıklı sistemler geliştirilmesine katkı sağlayarak, güvenlik risklerini minimize ettiği ve denetim sırasında tespit edilen bulguları kapattığı görülmüştür.

Anahtar Kelimeler: Bilgi Güvenliği, GNU/Linux Sıkılaştırma, Güvenlik Analizi, İşletim Sistemleri Güvenliği, Sıkılaştırma Stratejileri, Siber Güvenlik, Windows Sıkılaştırma,

ABSTRACT

MS THESIS

ANALYSIS AND IMPROVEMENT MODEL OF SECURITY HARDENING IN WINDOWS AND GNU/LINUX OPERATING SYSTEMS

Serhat YAPICI

Konya Technical University
Institute of Graduate Studies
Department of Computer Engineering

Advisor: Asst.Prof.Dr. Hazim İŞCAN

2025, 230 Pages

Jury
Asst. Prof. Dr. Hazim İŞCAN
Prof. Dr. Halife KODAZ
Asst. Prof. Dr. Onur İNAN

The rapid advancements in the field of information technology have led to the diversification and proliferation of cyberattacks. As the number of security vulnerabilities increases and vulnerable systems become primary targets, the risks encountered in digital environments have grown significantly. Consequently, the security of operating systems, which constitute the backbone of information systems, has gained substantial importance. This thesis aims to conduct an in-depth analysis of the security risks associated with Windows and GNU/Linux operating systems and to develop innovative and systematic strategies to enhance their security. Automated solutions have been devised to improve security levels, focusing on fundamental security measures such as user authorization, disabling unnecessary services, network security, and software updates. The study adopts a harmonized approach based on the Information and Communication Security Guide - Bilgi ve İletişim Güvenliği Rehberi (BİGR) issued by the Republic of Turkey Digital Transformation Office, as well as international security standards, including CIS Benchmarks, ISO 27001, and NIST SP 800-53. By aiming to enhance the effectiveness of security management systems both theoretically and practically, this research seeks to strengthen the security of operating systems and establish a robust defense mechanism against contemporary cyber threats. The proposed improvement model categorizes recommendations into three groups based on the criticality levels outlined in the Information and Communication Security Guide - Bilgi ve İletişim Güvenliği Rehberi (BİGR). The findings indicate that the suggested model contributes to the development of more resilient systems in the field of cybersecurity by minimizing security risks and addressing findings identified during audits.

Keywords: Cybersecurity, Hardening Strategies, Information Security, Linux Hardening, Operating System Security, Security Analysis, Windows Hardening,

ÖNSÖZ

Son yıllarda bilişim sistemlerine yönelik artan siber tehditler, işletim sistemlerinin güvenliğini daha da kritik hale getirmiştir. Windows ve GNU/Linux işletim sistemlerinin güvenlik açıkları, dijital ortamda karşılaşılan risklerin artmasına yol açmaktadır. Bu çalışmada, söz konusu işletim sistemlerinin güvenlik riskleri derinlemesine incelenmiş ve güvenlik seviyelerinin yükseltilmesi amacıyla yenilikçi çözümler geliştirilmiştir. Bilgi ve İletişim Güvenliği Rehberi (BİGR) ile CIS Benchmark esas alınarak, otomatik sıkılaştırma sağlayan bir iyileştirme modeli geliştirilmiştir. Bu modelin, siber güvenlik alanında daha dayanıklı ve güvenli sistemler inşa edilmesine katkı sağlaması hedeflenmiştir.

Çalışmam süresince bilgi ve desteğini benden hiçbir zaman esirgemeyen danışmanım Sayın Dr. Öğr. Üyesi Hazim İŞCAN'a içten teşekkürlerimi sunarım.

Ayrıca, her aşamada desteklerini ve motivasyonlarını eksik etmeyen sevgili aileme sonsuz teşekkürlerimi iletmek isterim. Tez çalışmasının tamamlanmasında katkı sağlayan tüm sevdiklerime minnettarım.

Serhat YAPICI
KONYA-2025

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

Kısaltmalar

ABD : Amerika Birleşik Devletleri
ACK : Acknowledgment (Onay)
AI : Artificial Intelligence (Yapay Zekâ)
AIDE : Advanced Intrusion Detection Environment (Gelişmiş İhlal Tespiti Ortamı)
ALT : Alternate (Alternatif)
API : Application Programming Interface (Uygulama Programlama Arayüzü)
ARP : Address Resolution Protocol (Adres Çözümleme Protokolü)
ASP.NET : Active Server Pages .NET (Aktif Sunucu Sayfaları .NET)
BGD : Bilgi Güvenliği Derneği
BGYS : Bilgi Güvenliği Yönetim Sistemi
BİGR : Bilgi ve İletişim Güvenliği Rehberi
BK : Bakınız
BSD : Berkeley Software Distribution (Berkeley Yazılım Dağıtımı)
BT : Bilgi Teknolojileri
CAGR : Compound Annual Growth Rate (Bileşik Yıllık Büyüme Oranı)
CBDDO : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
CD : Compact Disc (Dijital Optik Disk)
CIFS : Common Internet File System (Ortak İnternet Dosya Sistemi)
CIS : Center for Internet Security (İnternet Güvenliği Merkezi)
CMMC : Cybersecurity Maturity Model Certification (Siber Güvenlik Olgunluk Modeli Sertifikası)
COM : Component Object Model Plus (Bileşen Nesne Modeli)
CRAMFS : Compressed ROM File System (Sıkıştırılmış ROM Dosya Sistemi)
CSAT : Customer Satisfaction Score (Müşteri Memnuniyeti Skoru)
CSRF : Cross-Site Request Forgery (Web Sitesi Arası İstek Sahteciliği)
CTRL : Control (Kontrol)
CVE : Common Vulnerabilities and Exposures (Yaygın Zafiyetler ve Maruziyetler)
DAC : Discretionary Access Control (Takdirî Erişim Kontrolü)
DC : Domain Component (Alan Bileşeni)
DDO : Dijital Dönüşüm Ofisi
DDoS : Distributed Denial of Service (Dağıtık Hizmet Reddi Saldırısı)
DEL : Delete (Sil)
DISA : Defense Information Systems Agency (Savunma Bilgi Sistemleri Ajansı)
DLL : Dynamic Link Library (Dinamik Bağlantı Kütüphanesi)
DNS : Domain Name System (Alan Adı Sistemi)
DoD : Department of Defense (Savunma Bakanlığı)
DoS : Denial of Service (Hizmet Reddi Saldırısı)
DSS : Data Security Standard (Veri Güvenliği Standartları)
DVD : Digital Versatile Disc (Dijital Çok Yönlü Disk)
EBYS : Elektronik Belge Yönetim Sistemi
ECMA : European Computer Manufacturers Association (Avrupa Bilgisayar Üreticileri Birliği)

e-Devlet : Elektronik Devlet
GNU : Gnu's Not Unix (Gnu, Unix değildir)
GPL : General Public License (Genel Kamu Lisansı)
GRUB : Grand Unified Bootloader (Büyük Birleşik Önyükleyici)
GUI : Graphical User Interface (Grafiksel Kullanıcı Arayüzü)
HDD : Hard Disk Drive (Sabit Disk Sürücüsü)
HFS : Hierarchical File System (Hiyerarşik Dosya Sistemi)
HFSPLUS : Hierarchical File System Plus (Hiyerarşik Dosya Sistemi Gelişmiş)
HIPAA : Health Insurance Portability and Accountability Act (Sağlık Sigortası Taşınabilirliği ve Hesap Verebilirlik Yasası)
HP-UX : Hewlett-Packard Unix (Hewlett-Packard Unix İşletim Sistemi)
HTML : HyperText Markup Language (Hiper Metin İşaretleme Dili)
HTTP : HyperText Transfer Protocol (Hiper Metin Transfer Protokolü)
HTTPS : HyperText Transfer Protocol Secure (Güvenli Hiper Metin Transfer Protokolü)
ID : Identification (Kimlik)
IEC : International Electrotechnical Commission (Uluslararası Elektrik ve Elektronik Mühendisliği Komitesi)
IIS : Internet Information Services (İnternet Bilgi Hizmetleri)
IoT : Internet of Things (Nesnelerin İnterneti)
IP : Internet Protocol (İnternet Protokolü)
ISACA : Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Derneği)
ISO : International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
ITIL : Information Technology Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)
IWAM : Internet Information Services (IIS) Web Anonymous User (İnternet Bilgi Hizmetleri Web Anonim Kullanıcısı)
İAU : İstanbul Aydın Üniversitesi
JCB : Japan Credit Bureau (Japon Kredi Bürosu)
JFFS : Journaling Flash File System 2 (Günlükleyen Flash Dosya Sistemi)
KVM : Kernel-based Virtual Machine (Çekirdek Tabanlı Sanal Makine)
LDAP : Lightweight Directory Access Protocol (Hafif Dizin Erişim Protokolü)
LDAPs : Lightweight Directory Access Protocol Secure (Güvenli Hafif Dizin Erişim Protokolü)
LILO : Linux Loader (Linux Önyükleyicisi)
LMHOSTS : LAN Manager Hosts (LAN Yöneticisi Ana Bilgisayarlar)
LXC : Linux Containers (Linux Konteynerleri)
MAC : Media Access Control (Ağ Erişim Kontrolü)
MBSA : Microsoft Baseline Security Analyzer (Microsoft Temel Güvenlik Analizörü)
MitM : Man-in-the-Middle (Ortadaki Adam Saldırısı)
MSM : Microsoft System Management (Microsoft Sistem Yönetimi)
NetBIOS : Network Basic Input/Output System (Ağ Temel Giriş/Çıkış Sistemi)
NetBT : Network Basic Input/Output System over TCP/IP (TCP/IP Üzerinde Ağ Temel Giriş/Çıkış Sistemi)
NSA : National Security Agency (Ulusal Güvenlik Ajansı)
NTP : Network Time Protocol (Ağ Zaman Protokolü)
OS : Operating System (İşletim Sistemi)

OSI : Open Systems Interconnection (Açık Sistem Bağlantı Modeli)
OWASP : Open Web Application Security Project (Açık Web Uygulama Güvenliği Projesi)
PAM : Privileged Access Management (Ayrıcalıklı Erişim Yönetimi)
PCI DSS : Payment Card Industry Data Security Standard (Ödeme Kartı Endüstrisi Veri Güvenliği Standartları)
PCI : Payment Card Industry (Ödeme Kartı Endüstrisi)
PCMCIA : Personal Computer Memory Card International Association (Kişisel Bilgisayar Bellek Kartları Uluslararası Derneği)
PRO : Professional (Profesyonel)
PUKÖ : Planla-Uygula-Kontrol Et-Önlem al
QEMU : Quick Emulator (Hızlı Emülatör)
RBAC : Role-Based Access Control (Rol Tabanlı Erişim Kontrolü)
ROP : Return-Oriented Programming (Dönüş Yönlendirilmiş Programlama)
SCAP : Security Content Automation Protocol (Güvenlik İçeriği Otomasyon Protokolü)
SGID : Set Group ID (Grup Kimliği Ayarları)
SMB : Server Message Block (Sunucu Mesaj Bloğu)
SMTP : Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü)
SOAR : Security Orchestration, Automation and Response (Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı)
SP : Special Publications (Özel Yayınlar Dizisi)
SQL : Structured Query Language (Yapılandırılmış Sorgu Dili)
SSD : Solid State Drive (Katı Hal Sürücüsü)
SSL : Secure Sockets Layer (Güvenli Yuva Katmanı)
STIGs : Security Technical Implementation Guides (Güvenlik Teknik Uygulama Kılavuzları)
SUID : Set User ID (Kullanıcı Kimliği Ayarları)
SYN : Synchronize (Senkronize Etme)
SYN-ACK : Synchronize-Acknowledge (Senkronize-Onay)
T.C. : Türkiye Cumhuriyeti
TBD : Türkiye Bilişim Derneği
TCP : Transport Layer Security (Taşıma Katmanı Güvenliği)
TDK : Türk Dil Kurumu
TLS : Transport Layer Security (Taşıma Katmanı Güvenliği)
TOCTOU : Time-of-check to Time-of-use (Kontrol Zamanı ile Kullanım Zamanı Arasındaki Fark)
TS : Türk Standarları
TSE : Türk Standardları Enstitüsü
UDF : Universal Disk Format (Evrensel Disk Format)
UDP : User Datagram Protocol (Kullanıcı Veri Paketi Protokolü)
UID : User Identifier (Kullanıcı Kimliği)
USB : Universal Serial Bus (Evrensel Seri Veri Yolu)
VM : Virtual Machine (Sanal Makine)
VT : Virtualization Technology (Sanallaştırma Teknolojisi)
WINS : Windows Internet Name Service (Windows İnternet Adı Servisi)
WSUS : Windows Server Update Services (Windows Sunucu Güncelleme Hizmetleri)
XSS : XCross-Site Scripting (Web Sitesi Arası Scripting Saldırısı)
ZFS : Zettabyte File System (Zettabayt Dosya Sistemi)

ÇİZELGELER LİSTESİ

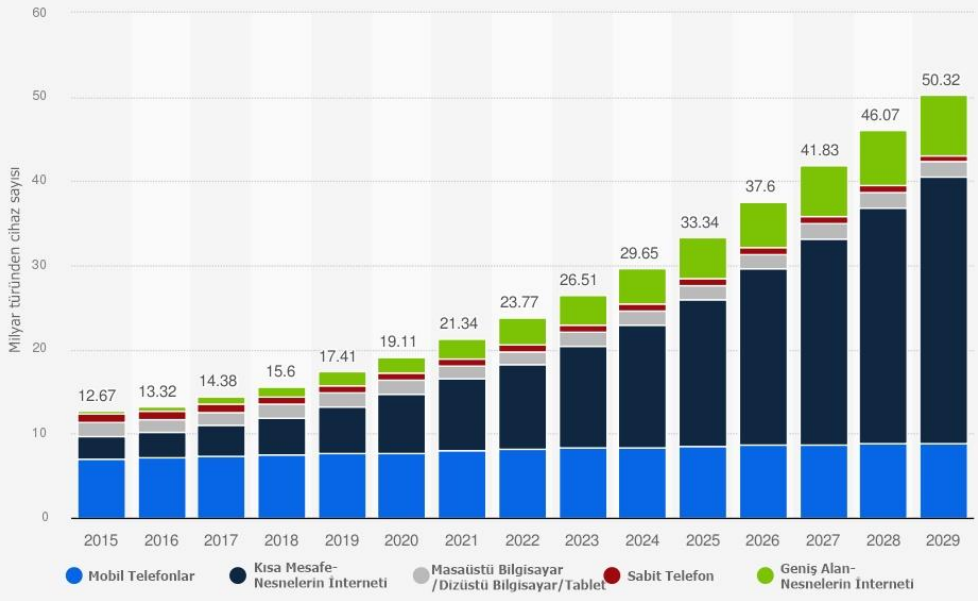
ŞEKİLLER LİSTESİ

1. GİRİŞ

Bilgi ve iletişim teknolojilerinin gelişimi, yaşamın her alanına yayılan dijitalleşme ile birlikte siber güvenliğin önemini büyük ölçüde artırmıştır. Günümüzde teknolojinin hızla yayılması, bilgisayar sistemlerinin yaygınlaşmasının sonucunda siber saldırıların sayısında ve çeşitliliğinde artış göstermektedir. Siber saldırı terimi Alkan'ın tanımına göre, "hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" şeklinde ifade edilmektedir (Alkan, 2012).

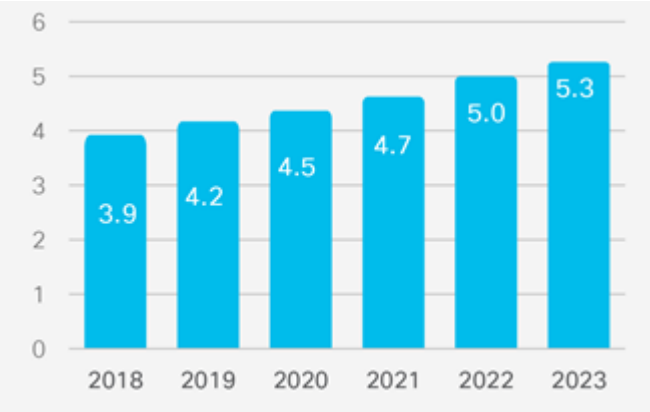
Siber saldırılar, kişilere ve kurumlara maddi, manevi ve çeşitli zararlar vermektedir. Güvenlik açıklarının artması ve savunmasız sistemlerin hedef haline gelmesiyle birlikte, dijital ortamda karşılaşılan risklerin karmaşıklığını artırmaktadır. Siber saldırılar ve siber güvenliğin önemi, bilişim sistemlerinin insan hayatındaki yeri arttıkça yani IP (internet protokolü) adresi alan cihazların sayısı arttıkça, her geçen gün artmaktadır (Özbay, 2015).

Şekil 1.1. 2015 ve 2029'da dünya çapında bağlı cihazların sayısı, cihaza göre (milyar olarak) (Ericsson, 2024), Ericsson Telekomünikasyon Şirketinin 1 Haziran 2024 yayımladığı çalışmada, dünya çapında 2015 ve 2029 yılları arasındaki farklı cihaz türleri açısından küresel ölçekteki büyümeyi ele alınmıştır. 2029 yılına kadar küresel bağlantılı cihaz sayısının önemli bir artış göstermesini öngörmektedir. Ericsson, bu verilerle birlikte dijitalleşmenin hızla arttığı ve bağlantılı cihazların hayatımızda her geçen gün daha fazla yer aldığına dikkat çekmektedir (Ericsson, 2024).



Şekil 1.1. 2015 ve 2029'da dünya çapında bağlı cihazların sayısı, cihaza göre (milyar olarak)

İnternetin günümüzde geniş bir kullanıcı kitlesine hitap etmesi ve hayatın her alanında kritik bir rol oynaması, küresel çapta teknolojik gelişmelerin hızlanmasına yol açmıştır. Şekil 1.2'de küresel internet kullanıcı artışı (milyar olarak) (Cisco, 2024), 2018-2023 yılları arası Cisco teknoloji şirketinin yıllık internet raporu teknik incelemesine göre, CAGR (Compound Annual Growth Rate) olarak bilinen bileşik yıllık büyüme oranı %6 olarak hesaplanmıştır. Teknolojinin yaygınlaşması bireyler, kurumlar ve devletler için fırsatlar sunduğu kadar çeşitli tehditleri de beraberinde getirmiştir. Özellikle internet üzerinden gerçekleştirilen siber saldırılar dijital dünyanın karanlık yüzünü ortaya koymaktadır.



Şekil 1.2. Küresel internet kullanıcı artışı (milyar olarak)

Siber saldırıların artmasının temel sebeplerinden biri, teknolojinin günlük yaşamdaki rolünün artması ve internet kullanıcı sayısının hızla yükselmesidir. Her geçen gün daha fazla kişi ve kurum, dijital araçları kullanarak verilerini saklamakta, işlemlerini gerçekleştirmekte ve iletişim kurmaktadır. Bilgisayar korsanlarının motivasyonları arasında ekonomik kazanç elde etme, fikri mülkiyet hırsızlığı, politik veya ideolojik amaçlarla zarar verme, rekabet avantajı sağlama ve devlet destekli operasyonlar gerçekleştirme gibi çeşitli nedenler bulunmaktadır.

Siber saldırılar, bireysel düzeyden uluslararası ilişkilere kadar geniş bir yelpazede etkili olmaktadır. Bireylerin kimlik bilgilerinin çalınmasından, ulusal altyapıların hedef alınmasına kadar uzanmaktadır. Teknolojik cihazların birbiriyle bağlantılı olduğu günümüzde, bir saldırının etkisi sadece hedefi değil dolaylı olarak diğer sistemleri de etkileyebilmektedir.

Siber saldırılardan özellikle verilen hizmetin kesintiye uğratılması saldırısı firmalar için büyük bir sorun teşkil ederek maddi kayıplara sebep olmaktadır. 2000'li yıllardan başlayan bu saldırı türü yıllar boyu devam etmiş ve etkisini göstermiştir (Atasever ve ark., 2019). 2024 yılı sonuna kadar siber saldırılardan kaynaklanacak küresel mali kaybın 9,5 trilyon dolar düzeyine ulaşacağı öngörülmektedir (Sausalito, 2024). Bu öngörüye göre siber güvenlik önlemlerinin ne kadar kritik olduğu ortaya konulmaktadır. Siber saldırılar, yalnızca bireysel ve kurumsal veri ihlalleriyle sınırlı kalmamakta, aynı zamanda altyapı sistemlerinin çökmesine, hizmet kesintilerine, itibar kayıplarına ve büyük finansal kayıplara neden olabilmektedir.

Siber saldırıların artması sonucu, siber güvenliğin sağlanması ve alınması gereken önlemlerin gerekliliği son yıllarda ciddi bir şekilde artmıştır (Savaş ve Karataş, 2022). Siber güvenliğin öneminin artmasıyla birlikte bu alanda geliştirilen teknolojiler ve uygulamalar da hızla yaygınlaşmaktadır. Güvenlik duvarları, şifreleme teknikleri ve yapay zekâ tabanlı tehdit algılama sistemleri gibi yenilikçi çözümler siber saldırılara karşı önemli bir savunma hattı oluşturmuştur.

Bilgisayar korsanlarının sistemleri ele geçirmek ve zarar vermek için kullanmış olduğu çeşitli teknikler ve metodolojiler sürekli bir değişim göstermektedir. Bu durumdaki söz konusu saldırılara karşı geliştirilen savunma mekanizmalarının da daha

kapsamlı ve yenilikçi stratejilerle tasarlanmasını zorunlu kılmaktadır. Yapılan bu çalışmalar için siber tehditlere karşı ulusal ve uluslararası düzeyde uygulanması gereken güvenlik standartları belirlenmiş ve bu standartlara yönelik denetim yöntemleri geliştirilmiştir.

Siber güvenlik alanında etkin çözümler üretmek ve uygulamak, bilgi ve iletişim sistemlerini korumak için hayati önem taşımaktadır. Siber güvenlik saldırılarına karşı güvenlik savunma mekanizmalarının geliştirilmesi hem bireylerin hem de kurumların dijital varlıklarını korumak adına acil bir ihtiyaçtır. Bilgi teknolojilerindeki bu hızlı ilerleme sonucunda savunma mekanizmalarının sürekli olarak güncellenmesini gerektirir. Siber güvenlik adına atılacak olan bu adımlar, dijital ortamda karşılaşılan risklere ve siber saldırılara karşı daha güçlü bir savunma ve bilgi güvenliği önlemleri sağlamaktadır.

Bilgi güvenliği önemleri için bilgi sistemleri güvenlik yönetimi, politikalar, standartlar, yönergeler, rehber dokümanlar ve prosedürler yardımıyla bir bilgi sistemi içinde gizlilik, bütünlük ve sürekliliğin sağlanmasını hedefler (Akın ve Tanç, 2022). Bu varlıklara olan tehditler ortaya konularak, bu tehditlerin oluşturduğu riskler belirlenir ve bu riskleri en aza indirecek önlemler alınır (Kara, 2018).

Riskleri azaltmak amacıyla iyileştirme önceliği verilen işletim sistemleri, bilgisayar üzerinde geliştirilen yazılımlar ve sistemlerin düzgün çalışabilmesi için gerekli olup, donanım ile yazılımlar arasında köprü işlevi görerek kritik bir öneme sahiptir. Windows ve GNU/Linux işletim sistemleri, dünya genelinde yaygın olarak kullanılan ve farklı güvenlik mimarileri sunan iki temel platformdur. Windows, merkezi bir güvenlik modeli ile kullanıcı yönetimi ve erişim kontrolleri sağlar. GNU/Linux işletim sistemleri ise dağıtık bir kullanıcı yönetim sistemiyle esneklik sunarken, özellikle açık kaynak doğası sayesinde geniş bir güvenlik özelleştirme imkânı sunar.

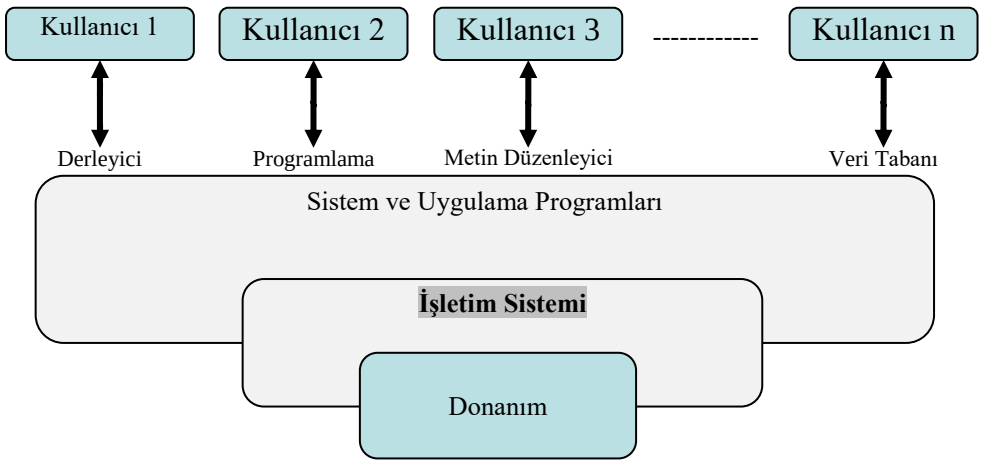
Bu çalışmada, Windows ve GNU/Linux işletim sistemlerinin güvenlik sorunları ile bu sorunları gidermeye yönelik ulusal ve uluslararası standartlara dayalı sıkılaştırma stratejileri detaylı bir şekilde incelenmiştir. Siber güvenliği artırmak için işletim sistemlerinin sıkılaştırılmasını sağlayacak bu çalışma, yalnızca mevcut güvenlik önlemlerini incelemekle kalmayacak, aynı zamanda bir iyileştirme modeli sunarak,

işletim sistemlerinin daha güvenli bir hale getirilmesine katkı sağlamayı amaçlamaktadır. İşletim sistemlerinin mimari yapıları, güvenlik politikaları, kullanıcı yetkilendirme, parola yönetimi, gereksiz servislerin devre dışı bırakılması, ağ güvenliği ve yazılım güncellemeleri gibi kritik önlemler analiz edilerek değerlendirilmiştir.

Bu çalışmada, işletim sistemlerinin güvenlik seviyelerinin artırılmasına yönelik hem teorik hem de uygulamalı yaklaşımlar ortaya konulmuştur. Uluslararası güvenlik standartları (ISO 27001, CIS, NIST SP 800-53 gibi) ve Türkiye Cumhuriyeti Dijital Dönüşüm Ofisi'nin yayımladığı Bilgi ve İletişim Güvenliği Rehberi (BİGR) çerçevesinde, yerel güvenlik politikalarına uygun olarak işletim sistemlerinin sıkılaştırılması için geliştirilen stratejiler kapsamlı bir şekilde değerlendirilmiştir. Elde edilen bulgular, işletim sistemi güvenliği konusundaki akademik literatüre önemli katkılar sunmakta olup, özellikle sistem yöneticileri, güvenlik uzmanları, denetçiler ve araştırmacılar için pratik analizler ve uygulanabilir iyileştirme modeli sunmaktadır.

1.1. Tezin Amacı

Bilişim sistemlerinin temel yapı taşı olan işletim sistemleri, bilgisayar donanımı ile kullanıcılar arasında bir köprü görevi görerek, donanım kaynaklarının verimli ve güvenli bir şekilde kullanılmasını sağlar. İşletim sisteminin konumu Şekil 1.3 de gösterilmektedir. Bu sistemler, kullanıcıların bilgisayar ile etkileşimde bulunmasını kolaylaştırırken, aynı zamanda uygulama yazılımlarının çalışması için gerekli ortamı sunar (Geeksforgeeks, 2024).



Şekil 1.3. İşletim sistemi yapısı ve konumu

İşletim sistemi güvenliği, olası bir güvenlik ihlali durumunda saldırganların sistemi ele geçirerek kötü niyetli eylemler gerçekleştirebilme riskini en aza indirmek için büyük bir önem taşır. İşletim sistemleri, sistem üzerindeki tüm kontrollerin merkezi noktasıdır ve güvenlik zafiyetleri durumunda tüm altyapı saldırılara açık hale gelebilir. Bu nedenle işletim sistemlerinin güvenliği bilişim sistemlerinin geneli için hayati bir önceliktir.

İşletim sistemlerinin en popüler öncülerinden biri olan Microsoft, 1975 yılında Amerika Birleşik Devletinde Paul Allen ve Bill Gates tarafından kurulmuş olan bir şirkettir. GNU/Linux işletim sistemi ise 1991 yılında Linus Torvalds tarafından Windows'a alternatif olarak geliştirilen bir işletim sistemidir (Karakoç ve Varol, 2016). Linux çekirdeği ve GNU araçlarının bir araya getirilmesi sonucunda, işlevsel bir işletim sistemi oluşturulmuş ve bu yapı GNU/Linux dağıtımı olarak adlandırılmıştır. Ancak, günlük konuşma dilinde ve kullanımda genellikle yalnızca Linux terimiyle ifade edilmektedir (GNU, 2021). Günümüzde en çok kullanılan bu iki işletim sistemi kritik noktalarda istemci ve sunucu bazlı modelleri ile kullanılmaktadır.

Günümüzde geniş bir kullanıcı kitlesi tarafından benimsenen Windows ve GNU/Linux işletim sistemleri, periyodik olarak versiyon ve güvenlik güncellenmeleri yayınlamakta ve güvenlik açıklarıyla mücadele etmek adına sürekli açıklık kapatma önerilerini duyurmaktadırlar. Yapılan duyurular arasında, güvenlik standartlarını artırmak amacıyla belirli dönemlerde artık eski sürüm olarak nitelendirdikleri versiyonların destek süreçlerini sonlandırmaktadırlar.

İşletim sistemlerinin destek süreçlerinin sona ermesi, eski versiyonlardaki güvenlik açıklarının güncellenmediği ve çıkan açıklıklara karşı çözüm alınmadığı için kritiklik arz etmektedirler. Bu durumda üreticiler, kullanıcıları ve sistem yöneticilerini güvenliklerini sürdürmek amacıyla en güncel ve desteklenen sürümlere geçmeye yönlendirmektedir. Ancak kurumsal çevrelerde geçiş süreçlerinin göz ardı edilmesi, başarılamaması veya güncelleme eksiklikleri sorun yaratmaktadır. Bahsi geçen güvenlik güncellemelerine geçilse bile yeni sürümlerde de ortaya çıkan güvenlik açıklarının sürekli bir izleme gerekliliğini, güvenlik sıkılaştırmalarının yapılması gerektiğini ortaya koymaktadır.

Sıfırıncı gün açıklıkları (Zero-Day) yazılım veya donanım üreticilerinin henüz fark etmediği veya çözüm üretmediği güvenlik açıklarıdır. Bu tür açıklıklar saldırganlara sisteme erişim kazanma veya zararlı faaliyetlerde bulunma fırsatı tanır. Sıfırıncı gün açıklıkları (Zero-Day), genellikle hedef sistemdeki savunma önlemlerini atlatmak için kullanılan önemli bir saldırı vektörüdür. Antivirüs yazılımlarının veya saldırı tespit ve önleme sistemlerinin imza tabanlı tarama ile bu saldırıları fark etmeleri mümkün değildir (Bilge ve Dumitras, 2012).

Günümüz bilişim teknolojisi bağlamında kritik bir öneme sahip olan Windows ve GNU/Linux işletim sistemlerinin güvenlik analizi ve sıkılaştırma stratejilerini detaylı bir şekilde ele almak gerekmektedir. Tüm bu problemler ve sebeplerden kaynaklı olarak güvenlik analizi yapmak her iki işletim sistemi için de kritik bir öneme sahiptir. İşletim sistemlerinin güvenliğini değerlendirmek ve sıkılaştırma stratejileri geliştirmek, siber saldırılara karşı daha etkili bir savunma sağlamak için hayati önem taşır.

Bu çalışmada güvenlik analizi ve sıkılaştırma stratejileri bağlamında, Windows ve GNU/Linux işletim sistemlerinin derinlemesine incelenmesi gerçekleştirilmektedir. Bu inceleme, her iki platformun güvenlik risklerini belirleme, saldırılara karşı dirençli hale getirme ve en iyi uygulamaları belirleme amacını taşımaktadır.

Sıkılaştırma stratejileri ve tedbirleri hakkında, Tripware şirketinin 2018 yılında oluşturduğu Siber Hijyen Durumu Raporuna (State of Cyber Hygiene Report) göre her 3 kuruluştan 2'si CIS ya da DISA STIGs gibi sıkılaştırma standartlarını kurumlarında uygulamamaktadır (Tripwire, 2018). Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberi (BİGR) içerisinde, İşletim Sistemi Sıkılaştırma Tedbirleri başlığı altında sunulan güvenlik önlemleri de bu çalışmanın önemli bir bileşenini oluşturmaktadır (DDO, 2020). Bu tedbirlerin bu çalışma bağlamında kullanılması bilişim güvenliği alanına önemli bir katkı sağlayacaktır.

Tüm bu politika dokümanları incelenerek, işletim sistemleri üzerinde gerçekleştirilen analiz sonuçlarına dayanarak, her iki işletim sistemi için güvenlik sıkılaştırmalarına dair öneri ve iyileştirmeler tespit edilmektedir. Bu öneri ve iyileştirmeler, güvenlik politikalarının güncellenmesini, izin düzeylerinin gözden

geçirilmesini, güvenlik açığı oluşabilecek noktaların sıkılaştırılmasını ve güvenlik açıklarının kapatılmasını içermektedir. Bu sürecin ana hatları, işletim sistemlerinin güvenlik değerlendirmesi için kullanılan metodolojinin uygulanmasını sağlar. Uyumluluk politikalarının dikkate alındığı her iki işletim sisteminin güvenlik seviyelerini değerlendirmek ve güçlendirmek adına etkili bir çerçeve sunar.

Tezin genel amacı, Windows ve GNU/Linux işletim sistemlerinin güvenlik mekanizmalarını inceleyerek, bu sistemlerin potansiyel tehditlere karşı daha dirençli hale gelmesini sağlamak için kapsamlı bir anlayış geliştirmektir. Bu amaç doğrultusunda belirlenen bazı özel hedefler bulunmaktadır. İlk olarak, Windows işletim sistemi üzerindeki güvenlik zayıflıkları ve potansiyel riskler sistematik bir şekilde analiz edilmiştir. Bu analiz sayesinde, işletim sisteminin içsel güvenlik mekanizmalarının etkinliği değerlendirilmiştir. Elde edilen bulgulara dayanarak, Windows işletim sistemi için önerilen sıkılaştırma stratejileri belirlenmiş ve bu stratejilerin uygulanabilirliği incelenmiştir.

Benzer şekilde GNU/Linux işletim sistemi için de güvenlik analizleri yapılmış ve sıkılaştırma stratejileri geliştirilmiştir. GNU/Linux'un açık kaynak doğası göz önüne alındığında, güvenlik açıkları üzerinde yapılan bu analiz kullanıcılar için önemli bir sistemi oluşturacaktır. GNU/Linux işletim sistemi üzerindeki güvenlik açıklarını kapatma ve güvenlik önlemlerini güçlendirme konusunda rehber niteliğinde bilgiler sunarak, sistematik bir şekilde güvenlik sıkılaştırmasını yapmak için iyileştirme modeli sunulmuştur.

Son olarak, tez kapsamında elde edilen bulgular ve geliştirilen stratejiler, genel olarak siber güvenlik alanına katkıda bulunacaktır. Aynı zamanda bu alandaki araştırmacılara, güvenlik uzmanlarına ve sistem yöneticilerine bir rehber niteliği taşıyacak analiz ve iyileştirme modeli geliştirmiştir. Tezin ana amacı işletim sistemlerinin güvenliğini artırmak ve modern siber tehditlere karşı daha etkili bir savunmayı sağlamak için alınabilecek pratik önlemler konusunda daha derinlemesine bir anlayışa sahip olunması ve güvenlik risklerini daha düşük hale getirmek için kurum ve kuruluşların sistematik bir iyileştirme modelini kullanması hedeflenmektedir.

1.2. Tezin Önemi

Aloul'un yapmış olduğu inceleme ve araştırmalara göre, gelişmiş güvenlik teknolojisi kullanımlarının artması sonucu, olası teknik siber saldırıların gerçekleşmesine ilişkin risk azalabilmektedir (Aloul, 2012). Ancak, gelişmiş güvenlik teknolojilerinin varlığına rağmen işletim sistemlerinin güvenlik iyileştirmeleri yapılmadığı takdirde, siber saldırılara karşı savunmasız kalınmaktadır.

Bu çalışma, Windows ve GNU/Linux işletim sistemlerinin güvenlik mekanizmalarını detaylı bir şekilde inceleyerek, siber güvenlikte kritik öneme sahip açıkları kapatma ve sıkılaştırma stratejilerini belirleme amacını taşımaktadır. Metodolojik olarak işletim sistemleri güvenlik analizi ve sıkılaştırma stratejileri konularında bir çerçeve sunmayı hedeflemektedir.

Bilimsel kalite perspektifinden değerlendirildiğinde, Windows ve GNU/Linux işletim sistemlerinin güvenlik mimarileri, içsel güvenlik mekanizmaları ve güvenlik politikaları üzerine detaylı bir inceleme yapılarak güçlü bir bilimsel temel oluşturmayı amaçlamaktadır. İyileştirme modeli olarak otomatik bir sistem haline getirilmesi ve bu sistemin işletim sistemlerine uygulanması sonucunda sıkılaştırılmanın gerçekleştirilmesiyle farklı bir perspektif bakış açısı kazandırarak, saldırganlara karşı daha etkili bir savunmayı oluşturması beklenmektedir. İyileştirme modelinde gerçekleştirilen yazılım, yapılacak olan denetimler için denetçiler adına kontrol aracı olarak kullanılmasına da fayda sağlayacaktır.

Yapılan çalışma farklılık ve yenilik açısından değerlendirildiğinde, her iki işletim sistemi için özel olarak tasarlanmış güvenlik analizi ve sıkılaştırma stratejileri sunarak, işletim sistemleri güvenliği konusunda mevcut literatürde bulunmayan bir perspektif ortaya koymayı amaçlamıştır.

Siber güvenlik risklerinin azaltılması ihtiyacı, ülkelerin uluslararası standartlar ve iyi uygulamalardan faydalanarak bilgi güvenliği alanında uygun yasal mevzuat hazırlanmasını ve uygulanması gereken tedbirlerin belirlenmesini tetiklemiştir (Sağıroğlu ve Şenol, 2018).

Ülkemizde kurumsal ve kişisel bilgi varlıklarının güvenliği, siber saldırıların önlenmesi, bilgi güvenliği risklerinin azaltılması ve etkisiz hale getirilmesi, özellikle gizlilik, bütünlük ve erişilebilirlik unsurlarının ihlal edilmesi durumunda milli güvenliği tehdit edebilecek veya kamu düzenini bozabilecek kritik veri türlerinin güvenliği ve gizliliğinin sağlanması amacıyla, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) tarafından 27 Temmuz 2020 tarihinde yayımlanan Bilgi ve İletişim Güvenliği Rehberi (BİGR) üzerinde İşletim Sistemi Sıkılaştırma Tedbirleri kapsamlarının da dahil edilerek, özellikle işletim sistemlerinin güvenlik açıklarını otomatize olarak kapatma ve saldırılara karşı güçlü bir savunma mekanizması oluşturma noktasında özgün çözümler getirmeyi içermektedir (DDO, 2020).

İlgili bilim ve teknoloji alanlarına metodolojik olarak kavramsal ve kuramsal katkı sağlama amacıyla, Windows ve GNU/Linux işletim sistemlerinin güvenlik analizi ve sıkılaştırma stratejilerine dair sistematik bir çerçeve sunacaktır. İşletim sistemleri güvenliği konusundaki eksiklikleri ele alarak, Windows ve GNU/Linux işletim sistemlerinin güvenlik seviyelerini artırmak amacıyla özgün, sistemik ve detaylı bir yaklaşım sunmayı hedeflemektedir. Bu çerçeve, işletim sistemleri güvenliğini değerlendirmek ve işletim sistemlerini sıkılaştırmak isteyen güvenlik uzmanları veya sistem yöneticileri için kapsamlı bir iyileştirme modeli olarak kullanılabilecektir.

Tez çalışmasında, kurum ve kuruluşların risk değerlerine göre iyileştirme modelinde risk derecelerini seçmeli, ardından gerekli güvenlik sıkılaştırmalarını yaparak işletim sistemlerini daha güvenli hale getirmeleri ve bu şekilde standartlara uygun olarak risklerini azaltmaları sağlanacaktır.

1.3. Tezin Organizasyonu

İlk bölüm, tez çalışmasının genel çerçevesini ve araştırma problemini ortaya koymaktadır. Bu bölümde, çalışmanın amacı, önemi ve kapsamı belirlenerek konunun literatüre ve pratik uygulamalara sağlayacağı katkılar açıklanmıştır. Ayrıca yapılan araştırma ve tez kapsamında ele alınacak temel kavramlar sunulmuştur.

İkinci bölümde, ilgili literatürün kapsamlı bir şekilde incelendiği ve tez konusuna temel oluşturan çalışmaların derlendiği bölümdür. Bu bölümde, kaynak

araştırmaları yapılmış olup, kapsamlı bir şekilde sorunlar değerlendirilmiştir. Genel olarak temel kavramlara ek olarak açıklamalar bu bölümde verilmiştir.

Üçüncü bölümde, çalışmada kullanılan yöntem ve materyalleri açıklamaktadır. Windows ve GNU/Linux işletim sistemlerinin güvenlik mimarisi, sıkılaştırma stratejileri, ulusal ve uluslararası güvenlik standartları gibi konular ele alınmıştır. Sanallaştırma ortamında oluşturulan test sistemleri, kullanılan araç, veri toplama yöntemleri ve güvenlik sıkılaştırma süreçleri açıklanmıştır. Ayrıca, işletim sistemlerinin karşı karşıya olduğu yaygın siber tehditler ve bu tehditlere karşı geliştirilen önlemler hakkında mevcut literatürdeki yaklaşımlar detaylandırılmıştır.

Dördüncü bölüm, güvenlik sıkılaştırma tedbirlerinin detaylı bir şekilde ele alındığı ve bu tedbirlerin sıkılaştırma kurallarına göre iyileştirme kodlarının sunulduğu bölümdür. Bu bölümde, Windows ve GNU/Linux işletim sistemlerinde güvenlik sıkılaştırması için yazılmış olan iyileştirme modelinin BİGR (Bilgi ve İletişim Güvenliği Rehberi) ile CIS (Center for Internet Security) denetimleri arasındaki tedbirler tablo olarak eşleştirilmiş olup kaynak kodları açıklanmıştır. İyileştirme modelinde BİGR (Bilgi ve İletişim Güvenliği Rehberi) kritiklik seviyeleri 1, 2 ve 3 şeklinde yapılandırılmıştır.

Beşinci bölümde, araştırma sonuçlarının analiz öncesi ve sonrasında yapılan değerleri açıklanmaktadır. Tez kapsamında gerçekleştirilen analizlerin ve uygulamaların adımları bu bölümde detaylandırılmıştır. Windows ve GNU/Linux işletim sistemlerinde yapılan güvenlik sıkılaştırma uygulamalarının metodolojisi ve karşılaştırmalı analiz süreçleri bu bölümde sunulmuştur.

Son bölüm olan altıncı bölüm, tezin genel sonuçlarını özetlemekte ve gelecekte yapılabilecek çalışmalara dair öneriler sunmaktadır. Güvenlik sıkılaştırma alanında geliştirilebilecek yeni modeller, metodolojik iyileştirmeler ve bu çalışmanın temelini oluşturan konulara yönelik genişletilmiş araştırma alanları bu bölümde ele alınmıştır.

Bu yapıyla birlikte, tez çalışması hem bilimsel bir perspektif hem de pratik bir rehber sunarak, işletim sistemleri güvenliği konusunda kapsamlı bir inceleme sağlamayı amaçlamaktadır.

2. KAYNAK ARAŞTIRMASI

Siber güvenlik alanında etkili çözümler üretme ve uygulama yapmak için, bilgi ve iletişim sistemlerini koruma konularında yaşanan sorunlara odaklanmak gerekmektedir. Literatür taraması, mevcut bilgi ve iletişim sistemlerinin güvenlik durumunu, karşılaşılan sorunları, eksiklikleri ve çözülmesi gereken konuları ayrıntılı bir şekilde analiz ederek ortaya koymaktadır.

Bilişim güvenliği, dijital ortamda depolanan bilgilerin yetkisiz üçüncü taraflarca ele geçirilmesini önleme, bilgi transferi esnasında bilginin bütünlüğünün ve yapısının bozulmadan aktarılmasını sağlama, sistemlere yetkisiz erişimi engelleme ve sistemin sürekli olarak erişilebilir olmasını temin etme amacıyla gerçekleştirilen çabaların genel adıdır (Resmî Gazete, 2013). Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ın 20 Haziran 2013 tarihinde 28683 sayılı Resmî Gazete'de yayımlanması ve yürürlüğe girmesiyle birlikte, bilişim güvenliği bu karar doğrultusunda tanımlanmıştır.

Siber güvenlik alanında yürütülen akademik çalışmalar genellikle teorik ağırlıklı olup, uygulama açısından eksik kalmaktadır. Vural ve Sağıroğlu'nun çalışmasında, kurumsal bilgi güvenliğinin yüksek düzeyde sağlanmasıyla ilgili literatürde yeterince kapsamlı ve güncel bir çalışmanın eksikliğine vurgu yapılarak, mevcut çalışmaların çoğunlukla ticari içeriğe sahip veya güvenilir olmayan web sitelerinde bulunan yetersiz çalışmalar olduğu belirtilmiştir (Vural ve Sağıroğlu, 2008).

Hackleme faaliyeti (Hacking) bilgisayar ve ağ sistemlerine kişinin izni olmadan giriş yapmak ve aynı zamanda farklı verilere erişerek bu bilgilere zarar verme gibi işlemler yapmaya denir. Diğer bir ifadeyle hacker sistemdeki engelleri aşarak yapılan sızma faaliyetleridir (Harris, 2006). Türkiye Bilişim Derneği tarafından hazırlanan bilişim sözlüğünde, hacker tabiri "bilgisayar korsanı" olarak adlandırılmaktadır (TBD, 2023). Bilgisayar korsanlarının amacı sistemdeki açıkları bulup, bu açıklardan yararlanarak özel uygulamaların şifresini kırmak, sistemlerine izinsiz ulaşmak ve ulaştıkları ortamdan bilgi çalmaktır (Mitnick ve ark., 2005). TDK'ya (2023) göre bilgisayar korsanları, bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli

verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kişilerdir. Bilgisayar korsanları üç farklı gruba ayrılır.

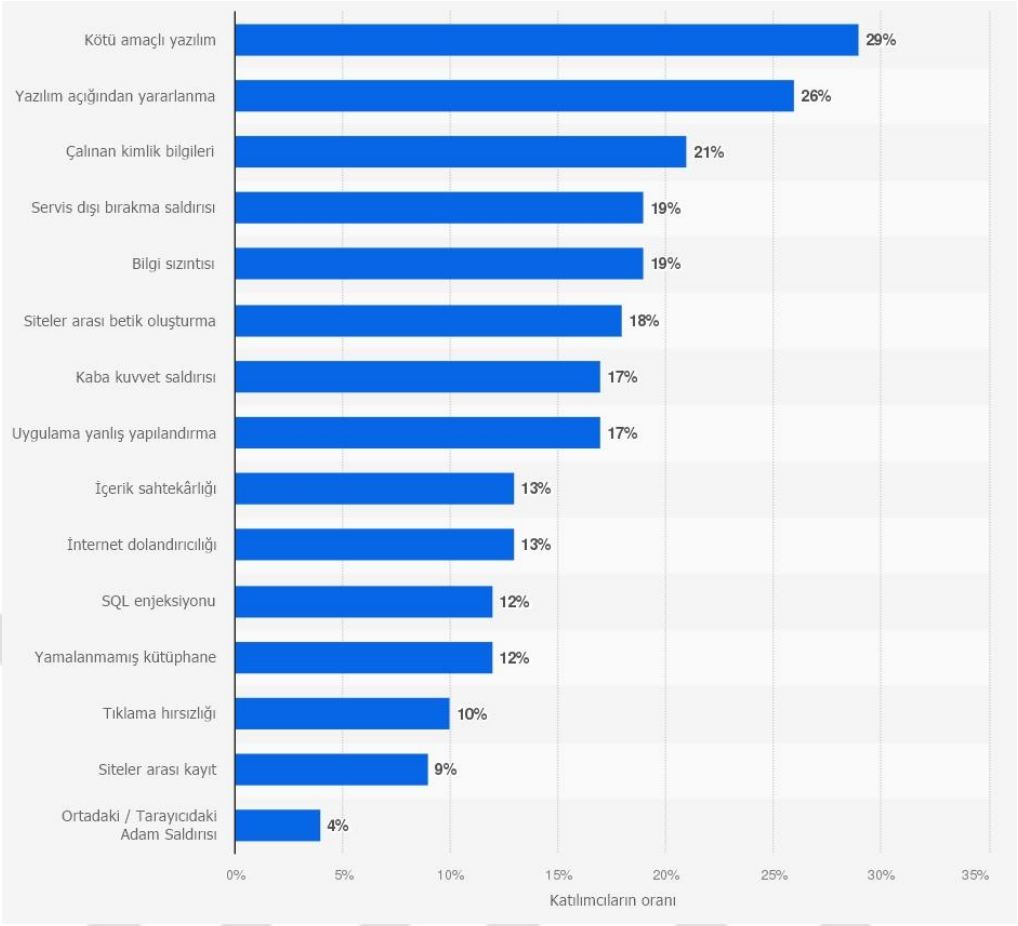
Bu gruplar onların amaçları ve faal oldukları alana göre kategorileştirilmiştir; Siyah, Beyaz ve Gri şapkalı (Elbahadır, 2011).

1. **Siyah Şapkalı Bilgisayar Korsanları:** Siyah şapkalı bilgisayar korsanları, zarar verme potansiyeli en yüksek olan gruptur. Her tür sistem açığını tespit ederek bu sistemlere izinsiz giriş yapabilirler. Sisteme girdiklerinde, genellikle sistemin tamamına zarar vererek ciddi güvenlik ihlallerine yol açarlar.

2. **Beyaz Şapkalı Bilgisayar Korsanları:** Beyaz şapkalı bilgisayar korsanları, siyah şapkalı bilgisayar korsanlarının aksine, sistemlere zarar vermek yerine faydalı işler yaparlar. Bir sisteme giriş yaptıklarında, güvenlik açıklarını tespit eder ve bu açıkların farkına varılmasını sağlayarak zayıf noktaları bildirir. Böylece, sistemin güvenliğini artırmak için gerekli önlemler alınır. Bireysel şirketler, özel sektör kuruluşları ve kamu kurumları, beyaz şapkalı bilgisayar korsanlarından faydalanmaktadır.

3. **Gri Şapkalı Bilgisayar Korsanları:** Gri şapkalı bilgisayar korsanları ise özel durumlara göre hem beyaz hem de siyah şapkalı bilgisayar korsanları gibi davranabilirler. Onlar sistem açığını tespit eder ve sistemlere izinsiz erişim sağladıkları için beyaz şapkalı sayılamazlar, fakat girdikleri sisteme de zarar vermezler ve dolayısıyla tam olarak siyah da sayılamazlar. Bu nedenle gri şapkalı bilgisayar korsanları olarak bilinmektedirler.

Bilgisayar korsanlarının, günümüzde çeşitli saldırılar düzenleyerek, özellikle kötü amaçlı yazılımlar ve yazılım açıklarından yararlanarak, hedef aldıkları organizasyonlara zarar verdikleri görülmektedir. 2024 yılında yapılan bir ankette, siber saldırıların gerçekleştiği kuruluşlar, bu tür saldırıların, organizasyonlar arasında en yaygın karşılaşılan siber tehdit türleri olduğunu belirtmektedir (Cybersecurity Insiders, 2024). Bu anketin sonuçları Şekil 2.1'de gösterilmektedir.



Şekil 2.1. 2024 yılında siber güvenlik anketine göre uygulamalara yönelik güvenlik saldırı türleri (Cybersecurity Insiders, 2024)

Bu saldırılara karşı etkili bir savunma stratejisi, yalnızca ağ güvenliği önlemleriyle sınırlı kalmayıp aynı zamanda işletim sistemi güvenliğini de kapsamaktadır. İşletim sistemi, bir bilgisayarın tüm yazılımsal altyapısını kontrol ettiği için siber saldırılara karşı en savunmasız noktalardan biri olabilir.

İşletim sistemi güvenliği üzerine yapılan literatür taramalarında, Siik, işletim sistemi sıkılaştırması tanımını "sistem saldırı yüzeyini azaltmak ve böylece güvenliği artırmak için sistem özelliklerini, programları veya bağlantı noktalarını kaldırmak veya devre dışı bırakmak" olarak tanımlamıştır (Siik, 2017).

Andress, işletim sistemi sıkılaştırmasını "İşletim sistemi sıkılaştırmasının ana amaçlarından biri işletim sisteminin saldırıya uğrayabileceği uygun alanları azaltmak" olarak tanımlamıştır (Andress, 2014). Siber olaylar genellikle, işletmenin işletim sistemi

gibi iç çevre ve ağ katmanları vasıtasıyla ortaya çıkmaktadır (Center for Audit Quality, 2019).

İşletim sistemleri güvenliği, günümüz bilişim teknolojisinin merkezinde yer almaktadır. Ancak, en çok kullanılan ve kritiklik seviyesi yüksek olan Windows ve GNU/Linux işletim sistemleri üzerindeki güvenlik mekanizmalarının detaylı bir şekilde incelenmediği ve güncellenme süreçlerinin yeterince ele alınmadığı gözlemlenmektedir. Özellikle, işletim sistemlerinin destek süreçlerinin sona ermesi, sıfırıncı gün açıklıkları (Zero-Day) ve güvenlik açıklarının etkin bir şekilde kapatılması gibi kritik konular, mevcut literatürde yeterince ele alınmamıştır.

Kök Kullanıcı Takımı (Rootkit), genel itibari ile işletim sisteminde çekirdek seviyesinde (kernel level) bulunduklarından dolayı, bu tür virüsleri takip etmek ve ortaya çıkarmak zorluk derecesindedir (Güntay, 2014).

Windows ve GNU/Linux sistemlerine yönelik yapılan araştırmaların detaylı incelemeleri sonucunda, Çizelge 2.1'de belirtilen, 2024 yılı Common Vulnerabilities and Exposures (CVE) indeksine göre en fazla güvenlik açığına maruz kalan ilk 10 işletim sistemi arasında Windows ailesinden 7 adet, GNU/Linux ailesinden ise 1 adet çekirdek (Kernel), Google Android ailesinden 1 adet ve Apple Macos ailesinden de 1 adet yer almaktadır (CVE, 2024).

Çizelge 2.1. 2024'teki toplam "farklı" güvenlik açığı sayısına göre en çok 10 işletim sistemi

Sıra No	Ürün Adı	Üretici	Ürün Tipi	Açıklık Sayısı
1	Linux Kernel	Linux	OS	2877
2	Windows Server 2019	Microsoft	OS	586
3	Windows Server 2022	Microsoft	OS	583
4	Windows 11 22h2	Microsoft	OS	500
5	Windows 11 23h2	Microsoft	OS	499
6	Macos	Apple	OS	498
7	Windows Server 2016	Microsoft	OS	495
8	Android	Google	OS	489
9	Windows 10 22h2	Microsoft	OS	476
10	Windows 10 21h2	Microsoft	OS	467

Yapılan bir araştırmaya göre, CIS (Center for Internet Security) sıkılaştırma standartlarının ilk beş kontrolünün kuruluşlar tarafından etkin bir şekilde uygulanması durumunda, siber saldırıların %85'i engellenebilmektedir. Aynı araştırmaya göre, bu

kontrol standartlarının tamamının uygulanması halinde ise saldırıların %97'si önlenebilmektedir (Lapena, 2018).

Yapılan çalışmalar bütününde güvenlik uyumluluğu için literatürde farklı tanımlar bulunmaktadır. Lustig'in yapmış olduğu tanıma göre, "Düzenleyici uyumluluk, organizasyonların endüstri için gereken kanun, kural, standart, tanımlama ve düzenlemelere bağlı olmasıdır" (Lustig, 2015).

Julisch, güvenlik uyumluluğu tanımını "Bilgi teknolojisi sistemlerinde dışarıdan dayatılan fonksiyonel güvenlik gereksinimlerine uygunluk durumu" olarak ifade etmiştir (Julisch, 2009).

ISACA tarafından 2017 yılında yayınlanan "Auditing Cyber Security: Evaluating Risk and Auditing Controls" başlıklı çalışma da, siber güvenlik alanında risk değerlendirmesine ve denetim kontrollerinin değerlendirilmesine odaklanmaktadır. Bu kapsamlı kaynak, siber güvenlik politikaları, standartları ve prosedürlerin etkinliği üzerinde durarak, organizasyonların karşılaştığı riskleri güvenilir bir şekilde tanımlamayı, değerlendirmeyi ve düzeltmeyi amaçlamaktadır (ISACA, 2017). ISACA tarafından hazırlanan bu kılavuz siber güvenlik alanındaki denetim süreçlerinin etkin bir şekilde uygulanması için rehberlik sağlamaktadır.

Ausgewählte Kapitel der IT-Security'de gerçekleştirilen araştırmada, John Ostrowski'nin 2020 yılında bir seminerde sunduğu "OS Hardening (İşletim Sistemi Sıkılaştırması)" başlıklı çalışmada, teorik olarak sıkılaştırma tedbirleri anlatılmış olup herhangi bir iyileştirme modeli veya sıkılaştırma kodları geliştirilmemiştir (Ostrowski, 2020).

Gazi Üniversitesi Fen Bilimleri Enstitüsü'nde gerçekleştirilen araştırmada, Hasan YALPI'nın 2020 yılında tamamladığı yüksek lisans tezi olan "Güvenlik Uyumluluğu İçin Windows İşletim Sistemi Sıkılaştırma Kurallarının Uygulanması ve Denetimi" başlıklı çalışmada, yalnızca Windows işletim sistemi üzerinde odaklandığı gözlemlenmiştir (Yalpı, 2020).

Jamk University of Applied Sciences üniversitesinde gerçekleştirilen araştırmada, Ronald Clark'ın 2020 yılında tamamladığı yüksek lisans tezi olan "Security Automation for Windows Hosts: Hardening of Windows 10 Password Policy (Windows Bilgisayarları için Güvenlik Otomasyonu: Windows 10 Parola Politikasının Sıkılaştırılması)" başlıklı çalışmada, yalnızca Windows işletim sisteminin parola politikalarının sıkılaştırmaları ele alınmıştır (Clark, 2020).

Literatür taramalarında, işletim sisteminin güvenlik sıkılaştırması konusunda iki işletim sistemi için de analiz ve iyileştirme modeli üzerinde çalışılmadığı görülmüştür. Bu çalışmada mevcut literatürdeki bu boşluk doldurulmak istenmiştir.

2.1. Windows İşletim Sistemleri

Microsoft tarafından geliştirilen ve ticari bir işletim sistemi ailesi olan Windows, dünya genelinde geniş bir kullanıcı kitlesine sahiptir. İlk olarak 1985 yılında piyasaya sürülen Windows, grafiksel kullanıcı arayüzü (GUI) sunan ilk işletim sistemlerinden biri olarak öne çıkmıştır (Microsoft, 2009). Günümüzde bireysel kullanıcılar, kurumsal altyapılar ve sunucu sistemleri için farklı sürümleri ile hem istemci hem de sunucu düzeyinde kapsamlı çözümler sunmaktadır.

Windows işletim sistemi, güvenlik mimarisinde merkezi bir yaklaşım benimsemektedir. Active Directory, Windows Defender ve BitLocker gibi entegre araçlar, sistem güvenliği ve kullanıcı yönetimini optimize etmeyi amaçlamaktadır. Windows işletim sistemlerinin yaygın kullanımı, siber saldırganların hedefi haline gelmesine yol açmış ve özellikle sıfırıncı gün açıkları (Zero-Day), Fidye yazılımları (Ransomware) saldırıları ve kötü amaçlı yazılımların (Malware) yayılması gibi tehditler açısından güvenlik sıkılaştırmasının önemini artırmıştır.

Windows'un kapalı kaynak yapısı, güvenlik açıklarının tespitinde üreticinin insiyatifini ön plana çıkarmaktadır. Her ne kadar düzenli güncellemeler ve güvenlik yamaları yayınlansa da eski sürümler için desteğin sona erdirilmesi, bu sistemleri kullanan bireyler ve kuruluşlar açısından bu sürümleri kullanan sistemlerin güncel tehditlere karşı savunmasız hale gelmesine neden olmuştur.

Windows işletim sisteminin güvenlik politikaları ve kullanıcı izinlerinin merkezi olarak yönetilmesi açısından güçlü araçlar sunmasına rağmen karmaşık yapısı ve üçüncü taraf yazılımlara olan bağımlılığı sıkılaştırma stratejilerinin dikkatle ele alınmasını gerektirmektedir.

2.2. GNU/Linux İşletim Sistemleri

GNU/Linux, özgür ve açık kaynaklı bir işletim sistemi ailesi olup hem bireysel hem de kurumsal kullanıcılar tarafından tercih edilmektedir. 1991 yılında Linus Torvalds tarafından geliştirilmeye başlanan Linux çekirdeği, GNU araçlarıyla birleştirilerek farklı dağıtımlar ile kullanıcıya sunulmaktadır (GNU, 2021). Debian, Ubuntu, Fedora ve Red Hat gibi popüler Linux dağıtımları, farklı ihtiyaçlara yönelik çözümler sağlamaktadır.

GNU/Linux'un açık kaynak doğası, kullanıcıların kod tabanına erişmesine ve sistem üzerinde tam kontrol sağlamasına olanak tanımaktadır. Bu özellik yalnızca kullanıcıların sistemlerini özelleştirmesine değil aynı zamanda güvenlik açıklarını tespit edip hızla gidermesine de katkıda bulunmaktadır. SELinux, AppArmor ve FirewallD gibi yerleşik güvenlik araçları GNU/Linux'un esnek ve güçlü bir güvenlik altyapısı sunmasını sağlamaktadır.

GNU/Linux'un güvenlik modeli, kullanıcı tabanlı yetkilendirme ve erişim kontrolüne dayanmaktadır. Dosya izinleri ve kullanıcı grupları gibi temel güvenlik mekanizmaları, sistemin saldırılara karşı dayanıklılığını artırmaktadır. GNU/Linux üzerinde sık kullanılan paket yönetim sistemleri (ör. apt, yum) ve güncellemelerin açık kaynak topluluğu tarafından denetlenebilmesi güvenlik açıklarının hızlı bir şekilde giderilmesine olanak tanımaktadır.

İşletim sistemleri kullanımı ve yönetimi konusunda GNU/Linux sistemlerinin dağıtık yapısı güvenlik sıkılaştırması açısından belirli zorlukları da beraberinde getirmektedir. Özellikle farklı dağıtımların çeşitli güvenlik standartlarına uyumlu hale getirilmesi sistem yöneticilerinin detaylı bilgi ve beceriye sahip olmasını gerektirmektedir.

GNU/Linux işletim sistemleri, bulut bilişimden gömülü sistemlere kadar geniş bir yelpazede kullanılan güvenilir bir platform olarak öne çıkarken güvenlik sıkılaştırma tedbirleri ile bu esnek yapının daha etkin korunması sağlanabilmektedir. Ancak, açık kaynak yapısı ve dağıtımlar arasındaki farklılıklar, güvenlik önlemlerinin etkili bir şekilde uygulanabilmesi için dikkatle yönetilmesi gereken önemli faktörlerdir.

3. MATERYAL VE YÖNTEM

Bu bölümde tez çalışmasında kullanılan ulusal bilgi ve iletişim güvenliği rehberi, uluslararası bilgi güvenliği standartları ve düzenlemeler, yaygın tehditler, bilgi ve iletişim güvenliği rehberi sıkılaştırma tedbirleri, sanallaştırma ortamı ve sıkılaştırma kurallarının denetimi hakkında bilgi verilmiştir.

3.1. Ulusal Bilgi ve İletişim Güvenliği Rehberi

Bilgi ve İletişim Güvenliği Rehberi (BİGR), dijitalleşmenin hızla arttığı günümüzde ulusal güvenlik ve kurumların bilgi altyapısının korunmasında kritik bir öneme sahiptir. Türkiye'de bu alandaki standartların belirlenmesi ve uygulanması amacıyla Bilgi ve İletişim Güvenliği Rehberi (BİGR) hazırlanmıştır. Bu rehber, ilk kez 6 Temmuz 2019 tarihli ve 30823 sayılı Resmî Gazete'de 2019/12 sayılı yayımlanan Cumhurbaşkanlığı Genelgesi ile duyurulmuş ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yapılan çalışmalar 24 Temmuz 2020 tarihinde tamamlanarak onaylanmıştır (DDO, 2020).

Kamu kurumları ve kritik altyapılarda bilgi güvenliği yönetim sistemlerini standartlaştırmak ve güvenlik açıklarını en aza indirmek için gerekli adımları belirlemek üzere hayata geçirilmiştir. Bu çalışmada, Bilgi ve İletişim Güvenliği Rehberi (BİGR) işletim sistemi sıkılaştırma tedbirleri detaylandırılmış, tedbirlerin türleri, kullanım alanları, uluslararası standartlara göre eşleştirilmesi ve analizleri yapılarak iyileştirme modeli geliştirilmiştir.

3.1.1. Bilgi ve İletişim Güvenliği Rehberi Yapısı

Bilgi ve İletişim Güvenliği Rehberi (BİGR) toplamda 237 sayfa ve 661 güvenlik tedbirinden oluşmaktadır. Rehber, bilgi güvenliği yönetim süreçlerini detaylı bir şekilde açıklayan dört ana temel bölümden oluşmaktadır.

Rehberin birinci bölümü, bilgi ve iletişim güvenliği rehberinin uygulama sürecini ele almakta ve mevcut bilgi güvenliği yönetim sistemlerini tamamlayıcı bir

yaklaşım sunmaktadır. Bu süreçte rehberde tanımlanan tedbirlerin uygulanabilirliğini artırmayı hedeflemekte ve teknik anlamda mevcut sistemlere destek sağlamaktadır.

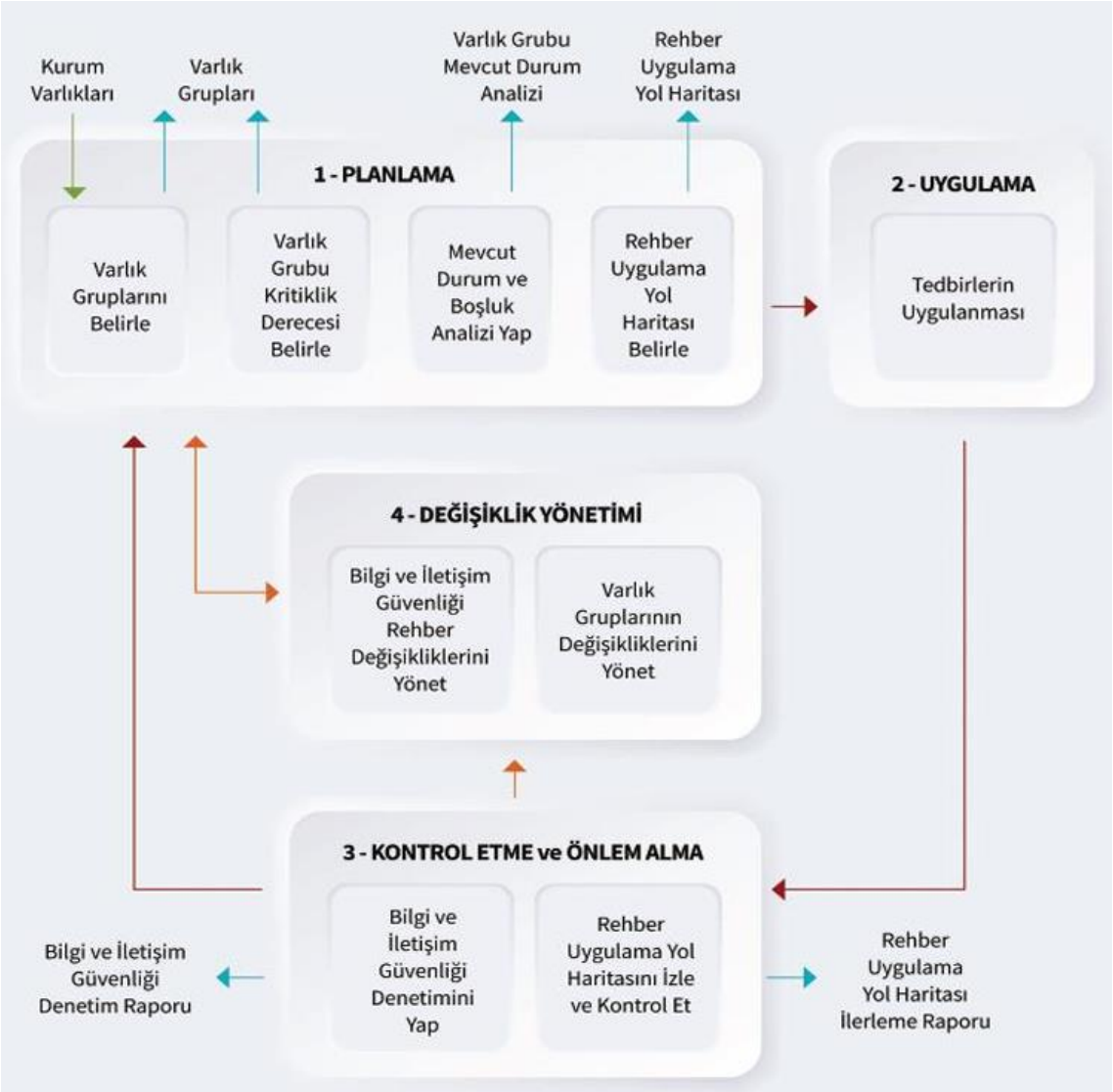
Rehberin ikinci ana bölümü olan varlık gruplarına yönelik güvenlik tedbirleri, her bir varlık grubuna ilişkin asgari güvenlik tedbirlerini detaylı bir şekilde tanımlamakta ve bu tedbirlerin varlıkların dâhil olduğu ana başlıklarla ilişkilendirilerek uygulanmasını öngörmektedir.

Üçüncü ana bölüm ise uygulama ve teknoloji alanlarına özgü güvenlik tedbirlerini kapsamaktadır. Her bir varlık grubunun ilgili uygulama ve teknoloji alanları ile eşleştirilmesi ve gerekli ek güvenlik önlemlerinin hayata geçirilmesi gerektiği vurgulanmaktadır.

Rehberin dördüncü ve son bölümü ise işletim sistemi, veri tabanı ve sunucular gibi temel bileşenlerin güvenliğini artırmaya yönelik sıkılaştırma tedbirlerini içermektedir. Bu tedbirler sistemlerin güvenlik açıklarını minimize etmeyi hedeflemektedir. Kurumların, rehber kapsamında tanımlanan faaliyet ve tedbirleri, kendi mevcut bilgi güvenliği yönetim süreçlerine entegre ederek ve ihtiyaçlarına uygun bir şekilde uyarlayarak uygulamaları beklenmektedir. Bu yaklaşımla beraber rehberin teknik derinliğini ve bütüncül güvenlik anlayışını ön plana çıkaran bir yapı sunmaktadır.

3.1.1.1. Uygulama Süreci

Uluslararası geçerliliği bulunan bilgi güvenliği sistemi için gerekliliklerin belirlendiği ISO/IEC 27001 standardına benzer şekilde, Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ) döngüsüne dayalı bilgi güvenliği yönetim süreçlerini ele almaktadır. Rehberin bu yapısı, bilgi güvenliği yönetim sistemi (BGYS) kullanan kurumların rehberi kolaylıkla entegre etmesine olanak tanır (ISO, 2013). Şekil 3.1’de Bilgi ve İletişim Güvenliği Rehberi (BİGR) uygulama süreci şekillendirilmiştir (DDO, 2020).



Şekil 3.1. Bilgi ve İletişim Güvenliği Rehberi (BİGR) uygulama süreci (DDO, 2020).

3.1.1.2. Varlık Gruplarına Yönelik Güvenlik Tedbirleri

Günümüzün dijitalleşen dünyasında, varlık gruplarına yönelik güvenlik tedbirleri bilgi sistemlerinin bütünlüğünü, erişilebilirliğini ve gizliliğini korumak için kritik bir öneme sahiptir. Güvenlik önlemleri başlıca ağ ve sistem güvenliğinden veri sızıntısı önlemeye, kimlik doğrulamadan fiziksel mekân güvenliğine kadar geniş bir yelpazede uygulanmaktadır.

Toplamda 416 tedbiri kapsayan bu yaklaşım, farklı varlık gruplarının karşı karşıya kalabileceği tehditlere yönelik kapsamlı bir koruma sağlamayı hedeflemektedir.

Bu kapsamda Çizelge 3.1'de belirtildiği üzere, ağ ve sistem güvenliği, uygulama ve veri güvenliği, taşınabilir cihaz ve ortam güvenliği, nesnelerin interneti (IoT) cihazlarının güvenliği, personel güvenliği ve fiziksel mekânların güvenliği olmak üzere altı alt başlığa ayrılmaktadır.

Çizelge 3.1. Varlık gruplarına yönelik güvenlik tedbirleri alt başlıkları

Ağ ve Sistem Güvenliği
Donanım Varlıklarının Envanter Yönetimi
Yazılım Varlıklarının Envanter Yönetimi
Tehdit ve Zafiyet Yönetimi
E-Posta Sunucusu ve İstemcisi Güvenliği
Zararlı Yazılımlardan Korunma
Ağ Güvenliği
Veri Sızıntısı Önleme
İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi
Sanallaştırma Güvenliği
Siber Güvenlik Olay Yönetimi
Sızma Testleri ve Güvenlik Denetimleri
Kimlik Doğrulama ve Erişim Yönetimi
Felaket Kurtarma ve İş Sürekliliği Yönetimi
Uzaktan Çalışma
Uygulama ve Veri Güvenliği
Kimlik Doğrulama
Oturum Yönetimi
Yetkilendirme
Dosyaların ve Kaynakların Güvenliği
Güvenli Kurulum ve Yapılandırma
Güvenli Yazılım Geliştirme
Veri Tabanı ve Kayıt Yönetimi
Hata Ele Alma ve Kayıt Yönetimi
İletişim Güvenliği
Kötücül İşlemleri Engelleme
Dış Sistem Entegrasyonlarının Güvenliği
Taşınabilir Cihaz ve Ortam Güvenliği
Akıllı Telefon ve Tablet Güvenliği
Taşınabilir Bilgisayar Güvenliği
Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
Ağ Servisleri ve İletişimi
Dâhili Veri Depolama
Kimlik Doğrulama ve Yetkilendirme
API ve Bağlantı Güvenliği
Diğer Güvenlik Tedbirler
Personel Güvenliği
Genel Güvenlik Tedbirleri
Eğitim ve Farkındalık Faaliyetleri
Tedarikçi İlişkileri Güvenliği
Fiziksel Mekânların Güvenliği
Genel Güvenlik Tedbirleri Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)

Güvenlik tedbirlerinin detaylı bir şekilde incelenmesi hem kurumsal hem de bireysel varlıkların korunması açısından kritik bir referans niteliği taşımaktadır. Bu tedbirler, yalnızca teknik gereksinimleri karşılamakla kalmayıp aynı zamanda güvenlik kültürünü kurumsal yapılara entegre etmeyi amaçlayan bir çerçeve sunmaktadır.

3.1.1.3. Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri

Veri güvenliği, kripto uygulamaları ve bulut bilişim güvenliği gibi konulara odaklanan toplam 146 güvenlik tedbiri, teknoloji altyapılarının karşı karşıya olduğu riskleri etkin bir şekilde yönetmek amacıyla tasarlanmıştır.

Çizelge 3.2'de belirtildiği üzere, kişisel verilerin güvenliği, anlık mesajlaşma güvenliği, bulut bilişim güvenliği, kripto uygulamaları güvenliği, kritik altyapılar güvenliği ve yeni geliştirmeler ve tedarik genel güvenlik tedbirleri olmak üzere altı alt başlığa ayrılmaktadır.

Çizelge 3.2. Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri alt başlıkları

Kişisel Verilerin Güvenliği
Kayıt Yönetimi
Erişim Kayıtları Yönetimi
Yetkilendirme
Şifreleme
Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme
Aydınlatma Yönetimi
Açık Rıza Yönetimi
Kişisel Veri Yönetim Sürecinin İşletilmesi
Anlık Mesajlaşma Güvenliği
Genel Güvenlik Tedbirleri
Bulut Bilişim Güvenliği
Genel Güvenlik Tedbirleri
Kripto Uygulamaları Güvenliği
Kriptografik Algoritmalar ve Kullanımı
Şifreleme ve Anahtar Yönetimi
Kriptografik Uygulamalar
Kritik Altyapılar Güvenliği
Genel Güvenlik Tedbirleri
Enerji Sektörü Özelinde Güvenlik Tedbirleri
Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri
Yeni Geliştirmeler ve Tedarik Genel Güvenlik Tedbirleri
Genel Güvenlik Tedbirleri

Bu tedbirler yalnızca mevcut güvenlik gereksinimlerini karşılamakla kalmayıp aynı zamanda sürekli gelişen teknolojik tehditlere karşı proaktif bir savunma

mekanizması oluşturmayı hedefler. Özellikle kripto uygulamaları güvenliği ve bulut bilişim güvenliği gibi alanlarda güvenlik kültürünün organizasyonel yapılara entegrasyonu büyük bir önem taşımaktadır.

Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirlerinin detaylı analizi hem bireysel hem de kurumsal düzeyde güvenlik ihtiyaçlarını karşılarken, aynı zamanda teknolojik sistemlerin sürekliliğini ve güvenilirliğini sağlamada önemli bir referans oluşturmaktadır. Güvenlik önlemlerinin yalnızca teknik değil aynı zamanda etik ve operasyonel boyutlarını da kapsamaktadır.

3.1.1.4. Sıkılaştırma Tedbirleri

Sıkılaştırma tedbirleri bölümü, işletim sistemleri, veri tabanları ve sunucular gibi kritik altyapı bileşenlerinin güvenliğini artırmak için uygulanan yöntem ve standartlardan oluşmaktadır. Bilgi ve İletişim Güvenliği Rehberi (BİGR)'nin dördüncü son ana bölümünü içermektedir.

Toplamda 99 farklı tedbiri kapsayan sıkılaştırma uygulamaları, modern bilgi teknolojisi altyapılarının en zayıf noktalarını hedef alarak sistemleri daha güvenilir ve dayanıklı hale getirmeyi amaçlamaktadır.

Tez çalışması konusunda derinlemesine incelenen kısım olarak Çizelge 3.3'te yer alan alt başlıklar çerçevesinde, işletim sistemi sıkılaştırma tedbirleri, veri tabanı sıkılaştırma tedbirleri ve sunucu sıkılaştırma tedbirleri yer almaktadır.

Sıkılaştırma tedbirlerinin detaylı olarak analiz edilmesi ve uygulanabilirliğinin değerlendirilmesi hedeflenmektedir. Sıkılaştırma süreçlerinin tehdit modellerine karşı etkinliğini incelemekle birlikte, sistemin verimliliğine olan etkileri de değerlendirilmektedir. Özellikle işletim sistemleri ve sunucular üzerinde gerçekleştirilen güvenlik yapılandırmaları, sistemin işlevselliğini koruyarak aynı zamanda saldırılara karşı dirençli bir yapı inşa edilmesini sağlamaktadır.

Sıkılaştırma tedbirlerinin önemi vurgulanacak ve kritik altyapıların korunmasında sunduğu katkılar detaylandırılacaktır. Sıkılaştırma yöntemlerinin,

güvenlik standartlarına uyumu, uygulanabilirliği ve verimliliği üzerine yapılacak değerlendirmeler, bilgi teknolojileri altyapılarının güvenliğini artırmaya yönelik değerli bir kaynak oluşturmayı amaçlamaktadır.

Çizelge 3.3. Sıkılaştırma tedbirlerine yönelik alt başlıklar

İşletim Sistemi Sıkılaştırma Tedbileri
Genel Sıkılaştırma Tedbirleri
Linux İşletim Sistemi Sıkılaştırma Tedbirleri
Windows İşletim Sistemi Sıkılaştırma Tedbileri
Veri Tabanı Sıkılaştırma Tedbirleri
Genel Güvenlik Tedbirleri
Sunucu Sıkılaştırma Tedbirleri
Web Sunucusu Sıkılaştırma Tedbirleri
Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

3.1.2. Bilgi ve İletişim Güvenliği Rehberi Varlık Gruplarının Belirlenmesi

Bilgi güvenliği yönetimi süreçlerinde etkili bir korunma mekanizmasının oluşturulabilmesi için kurumsal varlıkların kategorize edilmesi ve bu kategorilere uygun güvenlik tedbirlerinin uygulanması kritik öneme sahiptir. Bilgi ve İletişim Güvenliği Rehberi (BİGR) kapsamında yürütülen çalışmalarda, varlıkların belirlenen ana başlıklar altında gruplandırılması ve bu gruplara özgü tedbirlerin geliştirilmesi önerilmektedir.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), bilgi ya da verinin elektronik ortamda depolanması, işlenmesi ve iletilmesi süreçlerinde kullanılan bilgi işleme olanaklarını, bu olanakları kullanan personeli ve fiziksel ortamları kapsayacak şekilde geniş bir perspektifle hazırlanmıştır. Varlık grupları altı ana başlık olarak aşağıdaki gibi ayrılmıştır.

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihazlar ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel

Kurumların bilgi güvenliği yönetim süreçleriyle uyumlu bir şekilde varlık gruplarının belirlenmesi, bilgi güvenliği politikalarının etkin uygulanabilirliği açısından kritik bir rol oynamaktadır. Bu kapsamda gerçekleştirilen kurumsal varlıkların uygun başlıklar altında sınıflandırılması, varlık yönetiminde standartlaşmayı sağlayarak güvenlik tedbirlerinin doğru şekilde uygulanmasına imkân tanımaktadır.

Varlıkların sınıflandırılmasında, bir varlığın mümkün olduğunca yalnızca bir varlık grubunda yer alması sağlanmalı, bunun mümkün olmadığı durumlarda ise en kritik grubun temel alınarak değerlendirme yapılması gerekmektedir.

Varlık gruplarının tanımlanması sürecinde özellikle kurumların organizasyon yapısı, hizmet alanları ve kullanılan teknolojik altyapılar gibi unsurlar dikkate alınmalıdır. Güvenlik izolasyonunun sağlanabilmesi için aynı güvenlik seviyesine sahip varlıkların aynı grup altında toplanması, farklı güvenlik seviyelerine sahip varlıkların ise ayrı gruplarda değerlendirilmesi gerekmektedir. Böylelikle güvenlik politikalarının etkinliği artırılarak olası güvenlik açıklarının önüne geçilmesi hedeflenmektedir.

Varlık gruplarının yönetilebilir bir sayıda tutulması ve kayıtlı olması kurumsal süreçlerin etkin yürütülmesine katkı sunacaktır. Bu nedenle benzer güvenlik seviyesine ve ihtiyaçlarına sahip varlıkların birleştirilmesi güvenlik önlemlerinin daha verimli bir şekilde uygulanmasına zemin hazırlayabilir. Kurumların ihtiyaçları doğrultusunda tanımlanan varlık gruplarının her biri için uygulanacak güvenlik tedbirleri ilgili grubun önem derecesi göz önünde bulundurularak belirlenmelidir. Tüm bu süreçler kurumsal gerekliliklere uyum sağlayan esnek bir çerçevede ele alınmalı ve sürdürülebilir bir bilgi güvenliği yönetim sistemi oluşturulmasına katkı sunmalıdır.

3.1.3. Bilgi ve İletişim Güvenliği Rehberi Kritiklik Derecesinin Belirlenmesi

Varlık gruplarının kritiklik derecelerinin belirlenmesi, bilgi güvenliği yönetim sistemi süreçlerinin etkinliğini artırmak ve güvenlik tedbirlerini doğru bir şekilde önceliklendirmek için temel bir adımdır. Varlık gruplarının tanımlanmasının ardından, her bir grubun kritiklik derecesinin belirlenmesi gerekmektedir. Bu süreçte varlık gruplarının işlediği verilerin gizlilik, bütünlük ve erişilebilirlik gibi unsurları ile güvenlik ihlallerinin oluşturabileceği etkiler dikkate alınmalıdır. Kritiklik derecesi

belirleme süreci, verinin güvenlik unsurları ile etki alanını kapsayan çok boyutlu bir değerlendirme gerektirir.

Değerlendirme kapsamında kullanılan boyutlar, işlenen veri ile ilgili unsurlar ve etki alanına ilişkin faktörlerdir. Veriyle ilgili unsurlar arasında, gizlilik, bilginin yetkisiz kişilerin erişimine karşı korunması, bütünlük, bilginin tam ve doğru olma durumunun sürdürülmesi ve erişilebilirlik ise bilginin yetkili kişiler tarafından ulaşılabilir ve kullanılabilir olması gibi kriterler yer alır.

Etki alanı faktörleri ise varlık grubuna bağımlı diğer varlıklar üzerindeki etkiler, ihlal durumunda etkilenen kişi sayısı, kurumsal sonuçlar, sektörel etkiler ve toplumsal sonuçları kapsamaktadır.

3.1.3.1. Varlık Gruplarının Tanımlanması

Rehber kapsamında kurumların bilgi güvenliği yönetim sistemlerinde yer alan tüm varlıklar, altı ana başlık altında gruplanmalıdır. Bu varlık gruplarının doğru bir şekilde tanımlanması, hem organizasyonel düzeyde hem de teknik açıdan güvenlik açıklarının önlenmesi için önemlidir. Aşağıda belirtilen altı ana başlık, kurumların bilgi güvenliği yönetim sistemlerinde yer alan varlıkları kapsayan genel kategoriler olup, her bir başlık altında örnek varlık türlerine de yer verilmiştir. Bu kategoriler, kurumların tüm varlıklarını eksiksiz bir şekilde değerlendirmesine olanak tanır.

1. **Ağ ve Sistemler**: Yönlendiriciler, modemler, güvenlik duvarları, SCADA sistemleri gibi kritik altyapı elemanları.
2. **Uygulamalar**: Kurum içi yazılımlar, e-Devlet uygulamaları, elektronik belge yönetim sistemleri (EBYS).
3. **Taşınabilir Cihaz ve Ortamlar**: Akıllı telefonlar, USB bellekler, taşınabilir sabit diskler.
4. **Nesnelerin İnterneti (IoT) Cihazları**: Kamera sistemleri, ortam sensörleri (nem, gaz, sıcaklık gibi).
5. **Personel**: Yönetici, sistem yöneticisi, yazılım geliştirici ve son kullanıcılar.
6. **Fiziksel Mekânlar**: Veri merkezleri, felaket kurtarma merkezleri, personel odaları, yönetici odaları.

Her varlık grubu, içerisinde yer alan varlıkların detaylı bir envanteri ile birlikte ele alınmalıdır. Tüm varlıkların en az bir gruba dâhil edilmesi sağlanmalı ve böylece herhangi bir varlığın güvenlik önlemleri dışında kalması önlenmelidir.

3.1.3.2. Anketin Hazırlanması ve Uygulanması

Anket, her varlık grubunun kritiklik derecesini belirlemek üzere tasarlanmış sorular içermektedir. Anketin, ilgili paydaşlar ve kurumun bilgi güvenliği konusunda en yetkin personeli tarafından doldurulması gereklidir. Delfi metodu önerilen bir yöntemdir.

Delfi metodu, bu tür anketlerde kullanılan ve uzmanların görüş birliğine varmalarını sağlamak amacıyla kullanılan iteratif bir yaklaşımdır. Uzmanlar belirli bir konuya dair fikirlerini anonim olarak paylaşır ve her aşamada geri bildirimler doğrultusunda görüşlerini gözden geçirirler. Bu süreç daha güvenilir ve geçerli sonuçlar elde edilmesini sağlar (Bañuls ve Turoff, 2011). Delfi metodunun en büyük özelliği yüz yüze etkileşim olmadan farklı coğrafi konumlarda olan katılımcıların görüşlerinin toplanabilmesine imkân tanımasıdır (Landeta ve Barrutia, 2011).

Delfi metodunun anonimlik, yazılı geri bildirim ve katılımcılar arasında coğrafi uzaklık gibi avantajlara sahip olduğu vurgulanmaktadır (Shen ve diğerleri 2010). Bu özellikler, özellikle bilgi güvenliği gibi kritik konularda farklı uzmanların katkılarının toplanmasında önemli bir rol oynamaktadır (Şahin, 2001).

Delfi metodolojisi uzmanların görüş birliği sağlamasına yönelik iteratif bir yaklaşımdır ve uygulama süreci aşağıdaki maddelerde belirtilmiştir.

1. **Uzmanların Belirlenmesi**: Anketi dolduracak katılımcılar, sistem yöneticileri, varlık sahipleri ve bilgi güvenliği uzmanları arasından seçilir.
2. **Anketin Uygulanması**: Her bir soru için yalnızca bir şık işaretlenir ve en kritik varlık dikkate alınır.
3. **Sonuçların Değerlendirilmesi**: İlk turda alınan sonuçlar analiz edilir ve uzmanlar arasında bir fikir birliği oluşana kadar süreç tekrarlanır.

4. **Uzlaşının Sağlanması**: Nihai kararlar tüm katılımcıların uzlaşısı doğrultusunda belirlenir.

3.1.3.3. Kritiklik Derecesi Belirleme Boyutları

Varlık grupları iki ana boyut üzerinden değerlendirilmektedir. İşlenen veri boyutları bilgi güvenliğinin üç temel unsurunu içermektedir. Etki alanı boyutları beş temel başlıkta değerlendirilmektedir.

3.1.3.3.1. İşlenen Veri Boyutları

1. **Gizlilik**: Bilginin yalnızca yetkilendirilmiş kişiler tarafından erişilebilir olmasını sağlar. Gizliliğin korunması için şifreleme, erişim kontrolü ve kimlik doğrulama gibi yöntemler kullanılır.
2. **Bütünlük**: Bilginin doğru ve değiştirilmeden korunmasını ifade eder. Veri bütünlüğü, dijital imzalar ve karma işlevi (hash) fonksiyonları gibi araçlarla sağlanır ve yetkisiz değişikliklerden korunur.
3. **Erişilebilirlik**: Bilginin ihtiyaç duyulduğunda yetkili kişiler tarafından erişilebilir olmasını sağlar. Yedekleme, felaket kurtarma ve ağ dayanıklılığı gibi yöntemlerle bilgi sürekli erişilebilir kılınır.

3.1.3.3.2. Etki Alanı Boyutları

1. **Etkilenen Kişi Sayısı**: Güvenlik ihlalinden doğrudan etkilenebilecek kişi sayısını belirtir.
2. **Toplumsal Sonuçlar**: İhlalin toplum üzerindeki etkisi ve oluşturabileceği riskleri belirtmektedir. Toplumsal güvenin sarsılması, kamu güvenliği riskleri veya genel huzursuzluk gibi durumları içerir.
3. **Kurumsal Sonuçlar**: İhlalin kurumun organizasyon yapısı ve itibarı üzerindeki etkisini belirtir. Mali kayıplar, çalışan motivasyonunda azalma ve marka güveninin zedelenmesi gibi sonuçları kapsar.
4. **Sektörel Etki**: İhlalin hizmet verilen sektöre doğrudan etkisini gösterir.

5. **Bağımlı Varlıklar**: Varlık grubunun diğer varlıklar üzerindeki kritik bağımlılıklarını açıklar. Bu, bir sistemin veya hizmetin, diğer altyapılara ve varlıklara olan bağlantılarından kaynaklanan güvenlik risklerini gösterir.

3.1.3.4. Puanlama ve Kritiklik Derecelerinin Belirlenmesi

Bilgi ve İletişim Güvenliği Rehberi (BİGR) Anket cevapları, her soru için önceden tanımlanmış puanlama sistemi kullanılarak değerlendirilir. Puanlama, varlık grubunun sahip olduğu riski ve etki seviyesini yansıtacak şekilde tasarlanmıştır.

Toplanan puanlar doğrultusunda, varlık grubunun kritiklik derecesi, rehberdeki BİGR Tablo 3'e göre belirlenir. Çizelge 3.4'te göre anket puan aralıkları ve kritiklik seviyeleri belirlenmiştir.

Çizelge 3.4. BİGR Anket puan aralığı ve kritiklik seviyeleri

Derece	Anket Puan Aralığı	Kritiklik Seviyesi
Derece 1	18'den düşük	Düşük kritiklik seviyesi
Derece 2	18 ile 28 arasında	Orta düzeyde kritiklik seviyesi
Derece 3	28 ve üzeri	Yüksek kritiklik seviyesi

3.1.3.5 Anket Sonuçlarının Yönetimi

Anket sonuçları ilgili varlık grubu için güvenlik tedbirlerinin planlanmasında temel teşkil eder. Sonuçlar rehberin BİGR EK-C.2 formunda kayıt altına alınarak aşağıdaki maddede bulunan bilgileri içermektedir.

- Varlık grubunun adı ve numarası.
- Anket puanı ve buna karşılık gelen kritiklik derecesi.
- Anketin tamamlanma tarihi ve çalışmayı koordine eden kişi.
- Anket sonuçlarını onaylayan yetkililer ve onay tarihleri.

Varlık gruplarının güvenlik gereksinimleri dinamik olduğundan, anket sonuçlarının periyodik olarak gözden geçirilmesi gereklidir. Gerektiğinde varlık gruplarının kapsamı yeniden değerlendirilmeli ve anket çalışmaları tekrarlanmalıdır.

3.2. Uluslararası Bilgi Güvenliği Standartları ve Düzenlemeler

Bilgi güvenliği, günümüz dijital dünyasında işletmeler ve kurumlar için vazgeçilmez bir gereklilik haline gelmiştir. Uluslararası bilgi güvenliği standartları, özellikle sistemlerin korunması, veri bütünlüğünün sağlanması ve güvenlik ihlallerinin önlenmesi amacıyla oluşturulmuştur. Standartlar, ürün ya da hizmetlerin güvenlik, kalite, güvenilirlik, verimlilik gibi istenilen özelliklere sahip olmasını sağlar (Tofan, 2001). En yaygın kullanılan uluslararası bilgi güvenliği standartları detaylı bir şekilde incelenecek bu standartların kritiklik türleri, benzerlikleri, kullanım durumları ve işletim sistemi sıkılaştırma kurallarının detayları ele alınacaktır.

3.2.1. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS)

ISO/IEC 27001 standardı, ISO/IEC 17799'un yerine geçerek bilgi güvenliği yönetimi için daha etkin bir yapı sunmayı hedefleyen uluslararası bir standarttır. Resmi adı "Information Technology - Security Techniques - Information Security Management Systems - Requirements" olan bu standart, Türk Standartları Enstitüsü (TSE) tarafından "Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler" başlığıyla Türkçeye çevrilmiştir. Teknik bir standart olmaktan ziyade, ISO/IEC 27001, kurum ve kuruluşların bilgi güvenliği gereksinimlerini tanımlamakta, ancak bu gereksinimlerin nasıl karşılanacağını kuruluşların inisiyatifine bırakılmaktadır (Koç ve ark. 2019).

ISO/IEC 27001 hem kurumsal hem de dış kaynaklı tehditlere karşı bilgiyi koruma altına almak amacıyla asgari beklentileri ortaya koymaktadır. TSE tarafından yayımlanan TS ISO/IEC 27001 kitapçığında standardın temel amacı, Bilgi Güvenliği Yönetim Sistemi (BGYS) için bir model oluşturarak bu sistemin kurulmasını, uygulanmasını, işletilmesini, izlenmesini, gözden geçirilmesini, sürdürülebilirliğini ve iyileştirilmesini sağlamak olarak açıklanmaktadır (Yılmaz, 2014). Bu bağlamda

ISO/IEC 27001, kuruluşların bilgi güvenliği yönetimi süreçlerini daha sistematik ve yapılandırılmış bir şekilde ele almasına olanak tanımaktadır.

Bu standardın amacı, kuruluşların bilgi güvenliği yönetim sistemlerini kurarak güvenlik risklerini yönetmeleridir. Diğer güvenlik standartlarına kıyasla daha çok bir yönetimsel çerçeve sunar, teknik gereksinimlere girmemektedir. Kullanım durumu, bilgi güvenliği yönetimi için uluslararası düzeyde en yaygın kabul görmüş sistemlerden birisidir ve büyük işletmeler ile kamu kuruluşları tarafından yaygın olarak kullanılır. ISO/IEC 27001, özellikle güvenlik politikalarının ve süreçlerinin belirlenmesi ve yönetilmesine yönelik sıkılaştırma kurallarını önerir. Bu kurallar, organizasyonların güvenlik yönetim sistemlerini sürekli olarak izlemeleri ve iyileştirmeleri gerektiğini belirtir.

3.2.2. CIS (Center for Internet Security)

CIS (Center for Internet Security), bilgi sistemlerinin güvenliğini artırmak ve siber tehditlere karşı daha dayanıklı hale getirmek amacıyla 2000 yılında Amerika Birleşik Devletleri tarafında kurulan bir organizasyondur (CIS, 2024). CIS, dünya genelinde tanınan bir otorite olarak işletim sistemleri ve uygulamalar için güvenlik standartları ve en iyi uygulama kılavuzları sağlar. Üzerinde çalışılmış olan rehberler özellikle sistem yöneticileri ve güvenlik uzmanları tarafından işletim sistemlerinin sıkılaştırılması ve güvenlik açıklarının azaltılması için yaygın olarak kullanılmaktadır.

CIS'in sağladığı en önemli düzenlemeler arasında CIS Kontrol (CIS Controls) ve CIS Ölçütleri (CIS Benchmarks) bulunmaktadır. Bu düzenlemeler işletim sistemleri için optimize edilmiş güvenlik yapılandırmaları ve kontrol listeleri sunarak siber saldırıların önlenmesinde kritik bir rol oynar.

3.2.2.1. CIS Kontrol (CIS Controls)

Bilgi ve İletişim Güvenliği Rehberi (BİGR)'de yer alan ve tedbir seviyesi 1, 2 ve 3 olarak tanımlanan yaklaşım, CIS Kontrolleri çerçevesinde uygulanan üç aşamalı güvenlik tedbirleriyle CIS L1 ve L2 tedbir seviyeleri ile paralellik göstermektedir. Rehberde belirtilen "Ağ ve Sistem Güvenliği", "Taşınabilir Cihaz ve Ortam Güvenliği",

“Personel Güvenliği”, “Kripto Uygulamaları Güvenliği”, “Kritik Altyapılar Güvenliği” ve “Yeni Geliştirmeler ve Tedarik” gibi başlıklar, CIS Kontrolleri’nde yer alan güvenlik önlemlerinden faydalanılarak geliştirilmiştir (Tulgar ve ark., 2022).

3.2.2.2. CIS Ölçütleri (CIS Benchmark)

CIS Ölçütleri sistemlerin güvenli bir şekilde yapılandırılmasına dair en iyi uygulamaları sunan rehberlerdir. CIS organizasyonu, 25 farklı satıcı ürün ailesinden 100’ün üzerinde CIS Ölçütleri yani CIS Benchmark’ı geliştirmiştir. Bu dokümanlar, dünya çapında pek çok siber güvenlik uzmanının katkılarıyla şekillenmiştir (Tulgar ve ark., 2022). CIS Ölçütleri, kamu ve özel sektörün yanı sıra akademik dünyada da kabul gören, güvenli yapılandırma kılavuzlarını içermektedir.

CIS ölçütleri (CIS Benchmark) dokümanlarında işletim sistemleri, veri tabanları, sanallaştırma yazılımları ve ağ cihazları gibi birçok farklı sistem için kapsamlı ve teknik detaylar içeren sıkılaştırma önerileri bulunmaktadır. CIS ölçütleri (CIS Benchmark) DDO BİGR “İşletim Sistemi Sıkılaştırma”, “Veri Tabanı Sıkılaştırma” ve “Sunucu Sıkılaştırma” gibi tedbirlerin oluşturulmasında önemli bir rol oynamaktadır.

3.2.2.3. CIS Kontrol Kategorileri ve Uyarlanabilirliği

CIS Kontrolleri, işletim sistemleri için temel ve ileri düzey güvenlik konfigürasyonlarını kapsar. CIS sıkılaştırma kuralları, kritik varlıkların korunmasında etkili bir yöntem olarak kabul edilir. ISO/IEC 27001 gibi diğer yönetimsel güvenlik çerçeveleriyle uyumlu olup, daha teknik bir düzeyde işletim sistemleri için yapılandırma standartları sağlar. CIS, sistem yöneticilerine yönelik olan ve açıkları minimize etmek için yapılandırma kılavuzları içeren rehberler sunar. Özellikle Windows, GNU/Linux gibi yaygın işletim sistemleri üzerinde sıkılaştırma uygulamalarına odaklanır ve ağ yapılandırma, veri güvenliği, erişim kontrolü gibi alanlarda önemli düzenlemeler önerir.

CIS standartları özellikle sistem güncellemelerinin hızlı uygulanması durumunda siber saldırıların %95’inin önlenebileceğini göstermiştir (Lapena, 2018). CIS, bilgi güvenliği en iyi uygulamalarını belirleyen, işletim sistemlerinin sıkılaştırılmasında rehberlik sağlayan bir organizasyondur.

3.2.3. CMMC (Cybersecurity Maturity Model Certification)

Amerika Birleşik Devletleri Savunma Bakanlığı US Department of Defense (DoD), savunma sanayi faaliyetlerinde asgari bilgi güvenliği şartlarını belirlemek amacıyla "Cybersecurity Maturity Model Certification" (CMMC) adını verdiği bir model oluşturmuştur (Federal Register, 2024).

CMMC, Amerika Birleşik Devletleri Savunma Bakanlığının yürüttüğü savunma sanayi projelerinde, tedarikçilerden bilgi güvenliği alt yapısını güçlendirmeleri için uygulamalarını beklediği gereksinimlerden oluşan bir bilgi güvenliği yönetimi modelidir. Modelin gereksinimleri, uygulamanın kapsamına bağlı olarak farklı olgunluk seviyeleri ile ifade edilmektedir (Selinger, 2022).

CMMC programı, ilk kez 2019 yılında duyurulmuş olup, birçok bilgi güvenliği standardından faydalanılarak savunma sanayi sektörü için özel olarak hazırlanmıştır. Bu yönüyle, güncel ve yeni olması ve savunma sanayinde bilgi güvenliği yönetimi uygulamaları için önemli rehber ve standartları derlemesi nedeniyle önemli bir referans niteliği taşımaktadır.

CMMC, ISO/IEC 27001 gibi uluslararası standartlarla benzer bir yönetimsel yaklaşım sergilese de daha çok savunma sektörü odaklıdır. Bu model, işletim sistemleri için kritik güvenlik önlemleri içeren sıkılaştırma kurallarını belirler. Özellikle izinsiz erişimlerin tespiti ve tehdit algılama sistemlerinin kurulması gibi ileri düzey koruma önlemleri önerir. Bu kurallar, savunma sanayindeki tedarikçilere yönelik bilgi güvenliği uygulamalarını güçlendirmek için zorunlu hale gelir.

3.2.3.1. Olgunluk Seviyeleri ve İşletim Sistemleri

CMMC, işletim sistemleri sıkılaştırmasında şu olgunluk seviyelerine odaklanır. İşletim sistemlerinde CMMC'nin ileri seviye gereklilikleri arasında yetkisiz erişimlerin izlenmesi ve kötü amaçlı etkinliklerin tespiti yer alır.

1. **Temel Koruma (Level 1):** Temel güvenlik önlemleri.
2. **Orta Düzey Koruma (Level 2):** Risk yönetimi uygulamaları.
3. **Gelişmiş Koruma (Level 3):** Tehdit algılama ve yanıt sistemleri.

3.2.4. Microsoft Security Baselines

Microsoft Security Baselines, Microsoft tarafından sağlanan ve Windows işletim sistemleri ile diğer Microsoft ürünleri için güvenlik yapılandırma önerileri sunan bir dizi rehberdir. Bu rehber, işletim sistemlerinin varsayılan ayarlarını sıkılaştırmak, siber tehditlere karşı koruma sağlamak ve güvenlik açıklarını minimize etmek için geliştirilmiştir. Microsoft'un bu rehberleri özellikle işletmelerde güvenlik yönetimini kolaylaştıran, uyum süreçlerini hızlandıran ve işletim sistemlerini optimize eden yapılandırma politikaları sunar (Microsoft, 2024).

Microsoft Security Baselines hem küçük ölçekli hem de büyük ölçekli organizasyonlar için uygulanabilir çözümler sunar. Bu rehberler, varsayılan sistem ayarlarının sıkılaştırılması ve güvenlik risklerinin yönetilmesinde önemli bir rehber olarak kabul edilir. Özellikle Microsoft ürünlerini kullanan organizasyonlar için kritik bir öneme sahiptir. Benzerlik olarak, CIS ve ISO/IEC 27001 gibi diğer rehberlerle uyumludur. Microsoft Security Baselines, Windows işletim sistemlerinin varsayılan ayarlarını sıkılaştırmak için adımlar sunar ve sistem güvenliğini artırmak için yapılandırma politikaları önerir. Özellikle yazılım güncellemeleri, erişim yönetimi ve güvenlik duvarı yapılandırmaları gibi önemli alanlarda sıkılaştırma kuralları içerir.

3.2.5. NSA (US National Security Agency)

NSA (US National Security Agency), ABD'nin ulusal güvenliğinden sorumlu bir kurum olarak, bilgi güvenliği ve siber tehditlere karşı önlemler geliştiren bir otoritedir. NSA, özellikle hassas ve kritik altyapıların korunması için güvenlik politikaları ve teknik çözümler sunar. İşletim sistemleri bağlamında, NSA'nın rehberlik ettiği güvenlik kılavuzları ve standartlar, sistem sıkılaştırması için önemli bir referans niteliğindedir (NSA, 2024).

NSA’nın sağladığı kılavuzlar, işletim sistemlerinin güvenlik açıklarını minimize etmeyi, veri bütünlüğünü sağlamayı ve yetkisiz erişimleri engellemeyi hedefler. Kamu ve özel sektörde kullanılan sistemler için pratik çözümler sunar. Ulusal güvenlik ve askeri sistemler için yüksek önemdeki verilerin korunmasıyla ilişkilidir.

NSA’nın hazırlamış olduğu kılavuzlar, CIS ve diğer kurallarla benzerlik gösterir ancak daha derinlemesine teknik detaylar içerir. NSA güvenlik kılavuzları, özellikle sistemlerin sıkılaştırılmasında uygulanacak detaylı güvenlik önlemleri sunar. İşletim sistemleri için bu kurallar, ağ güvenliği, erişim kontrolü, şifreleme ve tehdit öncesi savunma gibi unsurları kapsamaktadır.

3.2.6. DISA STIGs (Security Technical Implementation Guides)

The Security Technical Implementation Guides (Güvenlik Teknik Uygulama Kılavuzları), US Defense Information Systems Agency, DISA (Amerika Birleşik Devletleri Savunma Bilgi Sistemleri Ajansı) tarafından oluşturulan bir dizi güvenlik rehberi ve standarttır. Bu kılavuzlar, bilgi sistemlerinin güvenlik seviyelerini artırmak, siber tehditlere karşı koruma sağlamak ve güvenlik açıklarını minimize etmek için tasarlanmıştır. Özellikle ABD Savunma Bakanlığı ve kamu sektöründe kullanılan sistemlerde zorunlu olan bu standartlar, özel sektör tarafından da sıkça benimsenmektedir.

DISA STIGs, işletim sistemleri de dahil olmak üzere yazılım, donanım, ağ ve veri tabanı sistemleri için sıkılaştırma politikaları sunar. İşletim sistemleri üzerindeki etkileri, özellikle güvenlik açıklarını önlemek ve güvenlik politikalarına uyumu sağlamak açısından oldukça kritiktir. CIS Ölçütleri (CIS Benchmark) ve Microsoft Security Baselines ile uyumludur. Sıkılaştırma kuralları, güvenlik açıklarını minimize etmek ve sistemlerin dayanıklılığını artırmak amacıyla çok detaylıdır. DISA STIGs, kurumların sistemlerinin dış tehditlere karşı korunmasını sağlamak için çok sıkı güvenlik politikaları belirler.

3.2.7. NIST/US Department of Defense – (SP 800-53)

National Institute of Standards and Technology (NIST) SP 800-53, ABD Ulusal Standartlar ve Teknoloji Enstitüsü tarafından yayınlanan ve bilgi sistemleri ile organizasyonlar için güvenlik ve gizlilik kontrollerini kapsayan bir çerçevedir. Bu standart, federal bilgi sistemleri ve kritik altyapılar için zorunlu bir rehber niteliğindedir, ancak özel sektör ve uluslararası kuruluşlar tarafından da geniş çapta benimsenmiştir. SP 800-53, bilgi güvenliği risklerinin yönetilmesi, tehditlere karşı direnç oluşturulması ve hassas verilerin korunması için kapsamlı bir yol haritası sunar.

ISO/IEC 27001 ve CIS ile benzer yönetimsel ve teknik çerçeveleri sunar. NIST, özellikle bilgi sistemlerinin güvenliğini sağlamak için geniş çaplı kontrol listeleri ve yapılandırma önerileri sunar. Bu kontroller, işletim sistemlerinin güvenliğini artırmaya yönelik sıkılaştırma kuralları sunar ve genellikle tehditleri öngörme, önleme ve tespit etme stratejileri içerir.

3.2.8. ITIL (Information Technology Infrastructure Library)

Birleşik Krallık, Bilgi Teknolojileri (IT) birimlerinin ve iş süreçlerinin daha etkin bir şekilde yönetilmesi gerektiğini fark ettiğinde, Bilgi teknoloji birimlerinin organizasyonel bir çerçevede ele alınması gerektiği fikri ortaya çıkmıştır. Bu eksiklikleri gidermek amacıyla iş süreçlerinin ve hizmetlerinin daha verimli bir şekilde yürütülmesi için net yönergelerin oluşturulması gerektiği anlayışı, ITIL (Information Technology Infrastructure Library) metodolojisinin temellerini atmıştır (Demir, 2014).

ITIL, özellikle 1980'li yıllarda İngiltere'deki Bilgi Teknolojileri şirketlerinde hizmet kalitesini artırmayı amaçlayan bir sistem olarak geliştirilmiştir. İlk versiyonu 1985 yılında yayımlanmış, ardından sırasıyla 2001, 2007 ve 2019 yıllarında yeni sürümleri yayımlanmıştır (Kökoğlu, 2020). ITIL, yalnızca teknolojik altyapıya odaklanmakla kalmayıp bir bütün olarak hizmet yönetimini ele alan bir yaklaşım benimsemiştir. Bu metodoloji ile bilgi teknolojileri servislerinin etkin ve verimli bir şekilde yönetilmesi için farklı takımları ve hedefleri bir araya getirmiştir.

ITIL'ın her versiyonunda yapılan yeniliklerle birlikte, servis yönetimine dair bazı temel değerler de evrilmiştir. 2000'lerin başında, ITIL daha çok süreç odaklı bir yaklaşım benimserken, 2019'daki versiyonuyla daha esnek ve sürekli gelişen bir yapı ortaya çıkmıştır. ITIL, servislerin kalitesini ve güvenilirliğini artırmayı amaçlarken, sadece belirli işlevlerin yerine getirilmesini değil, tüm süreçlerin etkili bir şekilde çalışmasını sağlamayı hedefler (Elibol, 2020).

Bu bütünsel yaklaşım, organizasyonların ve hizmet sağlayıcılarının daha verimli bir şekilde çalışmasını, daha iyi müşteri deneyimleri sunmasını ve nihayetinde iş değerini artırmasını sağlar. ITIL, yalnızca teorik bir çerçeve olmakla kalmayıp, aynı zamanda pratikte uygulamaya konulabilecek metodolojiler de sunmaktadır. Bunun yanı sıra, ITIL ile birlikte kullanılabilecek başka yönetimsel yaklaşımlar ve metodolojiler de mevcuttur. Bu tür metodolojiler, şirketlerin hizmet kalitesini artırma çabalarına katkı sağlayan önemli araçlardır (Tımartaş, 2022).

ITIL metodolojisi, bilgi teknolojileri servislerinin etkin ve verimli bir şekilde yönetilmesi için küresel çapta kabul görmüş bir yaklaşım olup, işletmelerin iş süreçlerine değer katmaktadır. Teknolojinin ve iş dünyasının hızla değişen ihtiyaçlarına uyum sağlamak, şirketlerin yalnızca altyapılarını değil, tüm iş süreçlerini de optimize etmelerini gerektirmektedir. ITIL, servis yönetimini daha sürdürülebilir ve müşteri odaklı hale getiren önemli bir rehberdir.

3.2.9. PCI DSS (Payment Card Industry Data Security Standard)

Payment Card Industry Data Security Standard (PCI DSS), yani Ödeme Kartı Endüstrisi Veri Güvenliği Standardı, ödeme kartı işlemleri sırasında hassas müşteri bilgilerinin korunmasını sağlamak için oluşturulmuş bir güvenlik standartıdır. İlk kez 2004 yılında önde gelen kredi kartı şirketleri (Visa, MasterCard, American Express, Discover ve JCB) tarafından geliştirilmiş ve tüm dünyada ödeme kartı sistemlerini kullanan kuruluşlar için uygulanması zorunlu hale getirilmiştir (Mariano, 2024).

Bu standart, finansal verilerin gizliliğini, bütünlüğünü ve güvenliğini sağlamak için teknik ve organizasyonel kontrolleri tanımlayan kapsamlı bir çerçeve sunar. PCI

DSS hem fiziksel hem de sanal sistemlerin korunması için spesifik gereklilikler içerir ve özellikle işletim sistemlerinin sıkılaştırılmasında önemli bir rehber niteliğindedir.

Diğer güvenlik standartlarıyla benzer şekilde, CIS ve ISO/IEC 27001 gibi rehberlerle uyumlu olup, özellikle ödeme kartı endüstrisine yönelik sıkılaştırma kuralları içerir. PCI DSS'in sıkılaştırma kuralları, veri şifreleme, erişim yönetimi ve sistem güvenliği konularında ayrıntılı yönergeler sunmaktadır.

3.2.10. HIPAA (The Health Insurance Portability and Accountability Act)

The Health Insurance Portability and Accountability Act (HIPAA), yani Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası, 1996 yılında Amerika Birleşik Devletleri'nde kabul edilmiş, sağlık hizmetleriyle ilişkili verilerin gizliliğini ve güvenliğini koruma amacı taşıyan bir yasadır.

Bu yasanın temel amacı, sağlık hizmeti sunan kuruluşların, bireylerin sağlık bilgilerini koruma ve doğru bir şekilde yönetme konusundaki yükümlülüklerini belirlemektir. HIPAA hem bilgi güvenliği hem de hasta mahremiyeti bağlamında geniş bir çerçeve sunar ve özellikle sağlık sektöründeki işletim sistemlerinin sıkılaştırılmasında kritik bir rol oynar.

ISO/IEC 27001 ve NIST ile uyumlu olmakla birlikte, sağlık sektörü özelinde düzenlemelere sahiptir. HIPAA, sağlık hizmetleri sunan organizasyonların, kişisel sağlık bilgilerinin güvenliğini sağlamalarına yönelik sıkılaştırma kuralları sunar. Özellikle veri erişimi, şifreleme ve hasta gizliliği yönetimi gibi konularda teknik önlemler içerir.

3.3. Yaygın Tehditler

Yaygın tehditler özellikle bilgisayar sistemleri, işletim sistemleri ve ağları üzerindeki güvenlik açıklarından faydalanarak sistemlere zarar vermeyi amaçlayan çeşitli saldırı türlerini kapsamaktadır. Bu tehditler, her geçen gün daha sofistike hale gelirken, savunma önlemlerinin yetersiz olduğu durumlarda büyük güvenlik riskleri

oluşturur. Zararlı yazılımlar, yetkisiz erişimler, hizmet kesintisi saldırıları ve ağ tabanlı tehditler gibi başlıca kategoriler, organizasyonları ve bireyleri ciddi şekilde etkileyebilir.

3.3.1. Zararlı Yazılımlar (Malware)

Zararlı yazılımlar, işletim sistemlerine zarar vermek, sistemdeki verileri çalmak veya sistemin kontrolünü ele geçirmek amacıyla tasarlanmış kötü amaçlı yazılımlardır. Zararlı yazılımlar arasında virüsler, solucanlar (worms), truva atları (trojan), fidye yazılımları (ransomware) ve kök kullanıcı takımı (rootkit) yer alır.

3.3.1.1. Virüsler

Bilgisayar virüsleri, biyolojik virüslerden esinlenerek adlandırılmış ve kendilerini çoğaltarak yayılabilen kötü amaçlı yazılımlardır. Biyolojik virüsler, bir organizmanın hücrelerine girerek onları kendi çoğalmaları için kullanırken; bilgisayar virüsleri, yazılımlar veya dosyalar aracılığıyla bilgisayar sistemlerine zarar verir ve kendilerini çoğaltarak diğer sistemlere yayılırlar (Marion ve Twede, 2020).

3.3.1.2. Solucanlar (Worms)

Solucanlar, bilgisayar virüslerinden farklı olarak, yayılmak için kullanıcı etkileşimine ihtiyaç duymayan zararlı yazılımlar (malware) grubuna dahil edilir. Solucanlar, bir bilgisayara bulaştıktan sonra ağlar üzerinden kendilerini başka sistemlere bulaştırabilir ve böylece hızlıca yayılabilir (Marion ve Twede, 2020). Bu tür zararlı yazılımlar, genellikle ağdaki güvenlik açıklarını kullanarak savunmasız bilgisayarları hedef alır ve kopyalarını bu sistemlere ileterek kendi yayılmalarını sağlar.

Solucanlar, özellikle internet ve yerel ağlar üzerinde etkili olabilir çünkü ağları kullanarak başka bilgisayarlara bulaşabilirler. Bulaştıkları bilgisayarlar, solucanın kendilerini kopyalayıp diğer sistemlere yayılmasına olanak tanıyan bir başlangıç noktası olur (Ahmad, 2021). Bir solucan virüsü, bir ana bilgisayara ilk olarak bulaştığında bu bilgisayar üzerinden güvenlik açığı bulunan diğer bilgisayarları tarar ve bu bilgisayarlara da bulaşarak yayılarak ağın geniş alanlarına ulaşabilir.

3.3.1.3. Truva Atları (Trojan)

Truva Atı, adını Yunan mitolojisindeki Truva Savaşı'nda kullanılan Truva Atı'ndan alır. Bir Truva Atı, genellikle kendisini zararsız bir program veya dosya olarak gizler, ancak çalıştırıldığında kötü amaçlı bir yazılım olarak ortaya çıkar. Diğer zararlı yazılımlardan farklı olarak, Truva Atları, kendi başlarına çoğalmaz veya yayılmazlar; bunun yerine, kullanıcının veya saldırganın başka bir zararlı yazılım yüklemesine veya bir sistemin savunma önlemlerini geçmesine olanak tanır (Bowles ve ark, 2015).

Truva Atları, genellikle hedef sistemin kontrolünü ele geçirmek amacıyla kullanılabilir. Ayrıca, bazı Truva Atları, kullanıcıdan fark edilmeden sistem kaynaklarını kullanarak robot ağı (botnet) ağlarına dahil olabilir ya da fidye yazılımlarının (ransomware) çalışmasına yol açabilir.

3.3.1.4. Fidye yazılımları (Ransomware)

Fidye yazılımları, son yıllarda siber güvenlik alanında en büyük tehditlerden biri haline gelmiş olan zararlı yazılım türlerindendir. Bu yazılımlar, genellikle kullanıcıların bilgisayarlarını veya belirli dosyalarını şifreleyerek erişimlerini engeller ve ardından fidye talep eder.

Fidye yazılımlarının etkisi, kullanıcıların kritik verilere erişimlerini kaybetmeleri ve ödeme yapmayı kabul etmemeleri durumunda bu verilerin silinmesi, bozulması ya da ifşa edilmesi tehdidiyle ciddi hale gelir (Kharraz, 2018). Bu tür yazılımlar, işletim sistemlerinde göz ardı edilen zayıflıklardan yararlanarak dosyaların şifrelenmesine ve erişilemez hale gelmesine yol açmaktadır.

3.3.1.5. Kök kullanıcı takımı (Rootkit)

Kök kullanıcı takımı, bir işletim sistemi üzerinde çalışan süreçler, dosyalar veya sistem bilgilerini gizleyerek varlığını fark ettirmeden sürdüren zararlı yazılım veya yazılım grubudur. Temel amacı sistemdeki varlığını gizleyerek fark edilmeden çalışmasını sürdürmektir ve bu nedenle yayılma veya bulaşma gibi bir hedefi bulunmamaktadır. Başlangıçta çok kullanıcılı sistemlerde sıradan kullanıcıların yönetici

programlarına veya kritik sistem bilgilerine erişimini engellemek amacıyla geliştirilmişken, zamanla kötü niyetli saldırılar için de kullanılmaya başlanmıştır (McAfee, 2006).

Genellikle güvenilir olduğu düşünülen bir program aracılığıyla üst düzey yetkilerle (örneğin root kullanıcısı) çalıştırıldığında sisteme bulaşır. Benzer şekilde, çok kullanıcılı bir ortamda işletim sistemi çekirdeğindeki (kernel) güvenlik açıklarından yararlanarak yönetici (root) yetkisi elde edilmesi ve ardından kök kullanıcı takımı (rootkit) kurulması yaygın bir bulaşma yöntemidir.

3.3.2. Yetkisiz Erişimler

Yetkisiz erişim, bir kullanıcının veya saldırganın, güvenlik önlemleri yetersiz olduğunda, sisteme veya sisteme ait verilere erişim sağlamasıdır. Yetkisiz erişim tehditlerinde en popüler saldırı türleri, parola saldırısı, gökkuşağı tablosu saldırısı ve yetki yükseltme işlemleridir.

3.3.2.1. Parola Saldırıları (Brute Force Attack)

Kaba Kuvvet Saldırısı (Brute Force Attack) bir parola saldırısı türüdür. Hedef sistemdeki parolayı deneme yoluyla kırmayı amaçlayan bir saldırı yöntemidir. Bu amaçla, harfler ve özel karakterler içeren bir liste (wordlist) hazırlanır (Kara, 2019). Hazırlanan liste (wordlist) üzerinden deneme yanılma yoluyla parola saldırısı gerçekleştirilir.

Kaba Kuvvet saldırısının başarı süresi, hedef sistemdeki parolanın karmaşıklığına ve saldırıda kullanılan sistemin donanım gücüne bağlı olarak değişiklik göstermektedir.

3.3.2.2. Gökkuşağı Tablosu Saldırıları (Rainbow Table Attack)

Gökkuşağı Tablosu Saldırısı (Rainbow Table Attack) yöntemi, hedef sistemdeki parolaları kırmak için belirli bir ölçüte göre seçilen, düz metin ve karma işlevi (hash) fonksiyonları içeren şifre tablolarını kullanarak çalışmaktadır (Bhanot ve Hans, 2015).

Bu saldırı türü, kaba kuvvet saldırılarından (brute-force attack) farklı olarak, parolaların tek tek denenmesinin yerine, önceden hesaplanmış karma işlevi (hash) değerlerini içeren bir tabloyu kullanmayı amaçlar.

Kaba kuvvet saldırılarında (brute-force attack) her bir parola tek tek denenirken, gökkuşağı tablosu saldırısında karma işlevi (hash) edilmiş parolaların düz karşılıkları, belirli bir düzene göre seçilerek bilgisayar sisteminde sürekli olarak test edilir (Beşkirli vd. 2019).

3.3.2.3. Yetki Yükseltme (Privilege Escalation)

Saldırganlar, sistemde düşük yetkili bir kullanıcı olarak başladığında, yazılım hatalarını veya zafiyetlerini kullanarak daha yüksek ayrıcalıklar elde etmeye çalışabilirler. Bir sistemde yönetici hakları elde etmeyi hedefleyen bir saldırıdır. Dikey ve yatay ayrıcalık yükseltme olarak ikiye ayrılmaktadır (Proofpoint, 2024).

- **Dikey Ayrıcalık Yükseltme (Vertical Privilege Escalation)**: Düşük yetkilerle sisteme giren bir kullanıcı (user), yönetici hakları (root/administrator) alır.
- **Yatay Ayrıcalık Yükseltme (Horizontal Privilege Escalation)**: Bir kullanıcının başka bir kullanıcının verilerine veya kaynaklarına yetkisiz erişim sağlaması.

3.3.3. Hizmet Kesintisi Saldırıları

Hizmet aksattırma saldırıları ingilizce olarak, Denial of Service (DoS) ve dağıtık hizmet reddi Distributed Denial of Service (DDoS) saldırısı olarak iki ana başlık altında toplanır. Hedeflenen işletim sistemlerini veya ağları aşırı yükleyerek, kullanıcıların sisteme erişmesini engeller. Bu saldırılar hedef sistemin hizmetlerini kesintiye uğratır.

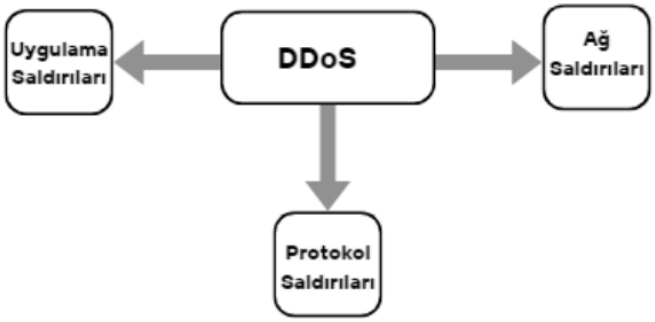
3.3.3.1. Hizmet Aksattırma (DoS) Saldırıları

Denial of Service (Dos) hizmet aksattırma saldırısıdır. Tek bir kaynaktan yapılan ve sistemin kaynaklarını tüketecek şekilde trafik göndererek sistemleri aksattıran saldırı türüdür. Uslu, bu saldırıları, “Hizmet aksattırma saldırıları olarak da bilinen DoS

saldırıları sistemin hizmetlerini engellemek amacıyla yapılırlar. Bunu yapmak için sisteme cevap verebileceğinden çok daha fazla istek gönderilerek verilen hizmet aksattırılır.” olarak tanımlamıştır (Uslu, 2009).

3.3.3.2. Dağıtık Hizmet Reddi (DDoS) Saldırıları

Birden fazla kaynaktan yapılan saldırılarla, hedef sistemi aşırı yükleyerek hizmet dışı bırakma işlemine denir. Sisteme aşırı yük bindirerek veya kaynakların tükenmesini sağlayarak, hizmetin erişilemez hale gelmesini hedefleyen saldırılardır. Distributed Denial of Service (DDoS) saldırıları daha fazla tehlikeli olabilir çünkü birden fazla kaynaktan saldırı yapılır. Saldırganlar genel olarak Şekil 3.2’de gösterildiği gibi üç tip DDoS saldırı yöntemini (Ağ, Protokol ve Uygulama) kullanmaktadır (İnce, 2024).



Şekil 3.2. DDoS saldırı yöntemleri (İnce, 2024).

Ağ saldırıları, özellikle hedef sistemin bant genişliğini tüketmeye yönelik gerçekleştirilen saldırılarla tanınır. Bu tür saldırılar arasında TCP/UDP Flood, DNS, NTP ve Memcached amplifikasyon saldırıları öne çıkmaktadır.

Protokol saldırıları, sahte port tabanlı isteklerin gönderildiği çok sayıda kullanıcıya hizmet veren sistemlere yönelik gerçekleştirilen saldırılardır. Bu saldırılar, OSI modelinin ağ ve taşıma katmanı protokollerini hedef alır ve bunlara SYN, SYN-ACK, ACK Flood saldırıları örnek verilebilir.

Uygulama saldırıları, OSI modelinin uygulama katmanındaki web hizmetlerini hedef alır ve HTTP, HTTPS, SMTP gibi protokoller üzerinden yapılan saldırılarla kendini gösterir. Layer 7 seviye saldırı türü olarak geçer.

3.3.4. Sıfırıncı Gün Güvenlik Açıkları (Zero-Day)

Sıfırıncı gün açıkları literatür üzerinde Zero-day olarak karışımıza çıkmaktadır. Bir yazılımın veya işletim sisteminin güvenlik açığının, yazılım geliştiricileri veya güvenlik uzmanları tarafından henüz fark edilmeden kötüye kullanılmasıdır. Bu tür açıklar genellikle saldırganlar tarafından hızla keşfedilip kullanılarak büyük güvenlik tehditleri yaratabilir. Zero-day saldırıları genellikle işletim sisteminde bulunan yamanmamış açıkları hedef alır ve bu nedenle ciddi riskler taşır.

3.3.5. Kernel Hataları ve Sömürüler (Exploit)

İşletim sistemi çekirdeği (kernel), en temel sistem işlevlerini yöneten yazılımdır. Çekirdek seviyesinde bulunan hatalar ve güvenlik açıkları, saldırganların sistem üzerinde tam kontrol elde etmelerine olanak tanıyabilir.

Bu hatalar, kötü niyetli kişiler tarafından sömürülerek (exploit) sistemdeki güvenlik zafiyetlerinden yararlanılabilir. Sömürme işlemi, bir saldırganın sistemin çekirdek seviyesindeki açıkları kullanarak, normalde erişilemeyecek verilere veya sistem kaynaklarına izinsiz erişim sağlamasına olanak tanır. Bu tür bir saldırı, kullanıcının verilerini çalmak, kötü amaçlı yazılım yüklemek veya sistem üzerinde tam kontrol sağlamak gibi çeşitli kötü niyetli amaçlarla yapılabilir.

Kernel hatalarının sömürülmesi, özellikle sistemin çekirdek seviyesinde güvenlik önlemleri yetersizse büyük bir tehdit oluşturur ve işletim sistemi güvenliği için ciddi bir risk kaynağıdır.

3.3.6. Tampon Taşması (Buffer Overflow)

Tampon Taşması saldırıları, yazılımda bir bellek tamponunun kapasitesinin aşılması durumunda meydana gelir. Yazılımda bir bellek tamponunun (buffer)

kapasitesinin aşılması ve bunun sonucunda komşu belleklere veri yazılması durumudur. Bir tampon, bilgisayar programlarının geçici veri depolamak için kullandığı bellek alanıdır. Genellikle bir dizinin (array) veya karakter dizisinin (string) verilerini saklamak için kullanılır. Her tamponun belirli bir boyutu vardır ve programlar bu tampona yalnızca belirli bir miktarda veri yazmayı hedefler. Ancak, tampon taşması durumunda, tamponun belirlenen sınırları aşılır ve bu durum, programın beklenmeyen bir şekilde davranmasına veya güvenlik açıkları oluşturmasına yol açabilir.

- **Arabellek Taşması (Stack Overflow):** Fonksiyon çağrılarının geri dönüş adreslerini değiştirmek amacıyla yapılır. Bu şekilde kötü amaçlı kod çalıştırılabilir.
- **Arabellek Taşması (Heap Overflow):** Dinamik bellek üzerinde veri taşması sonucu bellek bölgelerinin manipüle edilme işlemidir.
- **Geri Dönüş Odaklı Programlama - Return-Oriented Programming (ROP):** Saldırganın yazılımın mevcut kod parçalarını kullanarak zararlı komutlar çalıştırmasıdır.

3.3.7. Yarış Durumu (Race Condition)

Yarış Durumu, iki veya daha fazla işlem birbirine bağlı olduğunda ve bu işlemler sırasıyla yürütülmesi gereken bir kaynağa erişmeye çalıştığında hatalar oluşur. Bu durum, özellikle çoklu işlem veya çoklu iş parçacığı (multi-threading) kullanılan ortamlarda meydana gelir ve genellikle eş zamanlı (concurrent) erişim yönetimi eksikliklerinden kaynaklanır. Yarış durumu, işlemler arasındaki zamanlama sırasının doğru bir şekilde yönetilememesi sonucunda beklenmedik ve hatalı sonuçların ortaya çıkmasına neden olabilir.

Yarış durumunun temel özelliği, sistemin doğru bir şekilde çalışması için kritik olan işlemlerin sırasının ve zamanlamasının doğru yönetilememesidir. Bu durum, aynı kaynağa (örneğin, bir dosya, veritabanı kaydı veya bellek alanı) aynı anda veya sırasız bir şekilde erişilmeye çalışıldığında meydana gelir. Bu hatalar, genellikle veri bütünlüğünü bozabilir ve sistemin güvenliğini tehlikeye atabilir. Bu tür saldırılar, dosya yarışı (file race), hafıza yarışı (memory race) ve zamanlamalı saldırılar (TOCTOU) durumlarında görülebilir.

- **Dosya Yarışı (File Race):** Bir uygulama bir dosyaya erişmeye çalışırken, başka bir işlem dosyayı değiştiriyorsa, kötü niyetli kullanıcı bu durumu manipüle edebilir.
- **Hafıza Yarışı (Memory Race):** Aynı bellek alanına birden fazla işlem aynı anda erişmeye çalıştığında, bu tür hatalar ortaya çıkabilir.
- **Zamanlamalı Saldırılar (Time-of-Check to Time-of-Use, TOCTOU):** Uygulama bir kaynağı kontrol ederken, aynı kaynağa müdahale eden başka bir işlem nedeniyle güvenlik açığı oluşabilir.

3.3.8. DLL Enjeksiyonu (Dynamic Link Library Injection)

Saldırganlar kötü amaçlı bir DLL dosyasını uygulamanın hafızasına enjekte ederek çalıştırılmasını sağlayabilir. Bu tür saldırılar Windows işletim sistemlerinde gerçekleşmektedir.

DLL enjeksiyonunun etkileri geniş çaplı olabilir. Saldırganlar, bu yöntemi kullanarak sistem üzerinde tam kontrol sağlayabilir, kötü amaçlı yazılım (malware) yükleyebilir, veri hırsızlığı yapabilir veya yasal uygulamanın işleyişini bozabilirler. Örneğin, bir virüs veya truva atı (trojan), DLL enjeksiyonu yoluyla sisteme yerleşebilir ve kullanıcıya fark etmeden zararlı aktiviteler gerçekleştirebilir.

3.3.9. Yan Kanal Saldırısı (Side-channel Attacks)

Doğrudan veriyi ele geçirmeden bir sistemin dışsal yan etkilerinden (örneğin, işlemci sıcaklığı, elektriksel tüketim vb.) bilgi toplama saldırılarıdır. Bu tür saldırılar genellikle kriptografik anahtarları hedef alır.

Bu tür saldırılar, geleneksel şifreleme sistemlerini aşmanın alternatif bir yolu olarak karşımıza çıkar. Örneğin, bir saldırgan, şifreli verilerin işlendiği sırada işlemcinin güç tüketimini izleyerek, belirli algoritmaların hangi adımda çalıştığı hakkında ipuçları elde edebilir. Bu ipuçları, anahtarın belirli kısımlarını ortaya çıkarmak için kullanılabilir. Benzer şekilde, zamanlama saldırılarında, bir işlemcinin farklı kriptografik işlemleri farklı sürelerde tamamlaması, saldırgana hangi işlemlerin yapıldığını ve hangi verilerin işlendiğini gösterebilir.

Yan kanal saldırıları, genellikle yüksek güvenlikli sistemlerde (örneğin, bankacılık, dijital ödeme sistemleri veya askeri iletişimde) büyük bir tehdit oluşturur. Çünkü şifreleme algoritmaları, veri güvenliğini sağlamak için kritik öneme sahiptir ve bu tür sistemlerin başarısız olması hem finansal kayıplara hem de kişisel veri ihlallerine yol açabilir. Bu saldırı türünün etkili olabilmesi için genellikle hedef sisteme fiziksel erişimin sağlanması veya işlemci düzeyinde ince ayarlamalar yapılması gereklidir. Ancak, saldırganın sistemi uzaktan analiz edebilmesi, yan kanal saldırılarının daha tehlikeli ve yaygın hale gelmesine olanak tanımaktadır.

3.3.10. Uygulama Açıkları

Uygulama açıkları, yazılım sistemlerinin yanlış ya da eksik yapılandırılması, kod hataları veya bilinen güvenlik zafiyetleri sonucu ortaya çıkabilen tehditlerdir. Bu tür açıklar, saldırganların kötü niyetli faaliyetlerde bulunarak sistemlere zarar vermelerine yol açabilir. Uygulama güvenliği, yazılım geliştirme sürecinin temel bir parçası olmalıdır çünkü bu açıklar saldırılara zemin hazırlayan en yaygın güvenlik risklerinden biridir.

Yaygın uygulama açıkları, SQL Enjeksiyonu (SQL Injection), Siteler Arası Betik Yazma (XSS), Komut Enjeksiyonu (Command Injection), Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery) ve Deserileştirme Saldırıları (Deserialization Attacks) olarak öne çıkmaktadır.

3.3.10.1. SQL Enjeksiyonu (SQL Injection)

SQL enjeksiyonu, veri tabanı sorgularını manipüle ederek kötü amaçlı komutların çalıştırılmasına neden olan bir saldırı türüdür. Saldırganlar, uygulama üzerinden veri tabanına gönderilen kullanıcı girdilerini manipüle ederek, veri tabanına yetkisiz erişim sağlayabilir ve hassas bilgilere ulaşabilirler. Bu tür saldırılar, genellikle uygulama yazılımlarında giriş doğrulaması yapılmaması veya yetersiz güvenlik önlemleri ile mümkün hale gelir (OWASP, 2021).

3.3.10.2. Siteler Arası Betik Yazma (XSS)

XSS saldırıları, web uygulamalarındaki kullanıcı girişlerinin yeterince doğrulanmaması sonucu meydana gelir. Saldırgan, zararlı JavaScript kodlarını kullanıcıya sunar ve bu kodlar, kullanıcının tarayıcısında çalıştırılarak veri hırsızlığına yol açabilir. XSS saldırıları, genellikle web uygulamaları aracılığıyla, kullanıcıların kimlik bilgilerini, çerezlerini veya oturum verilerini çalmayı amaçlar. XSS, doğru güvenlik önlemleri alınmadığında büyük bir tehdit oluşturabilir.

3.3.10.3. Komut Enjeksiyonu (Command Injection)

Komut enjeksiyonu, dış komutların sistem üzerinde kötüye kullanılmasını sağlayan bir saldırı türüdür. Saldırganlar, uygulamanın çalıştırdığı sistem komutlarına müdahale ederek, işletim sistemi üzerinde kontrol sağlamak için komutlar gönderebilir. Bu tür saldırılar, özellikle sunucu tarafı uygulamalarında ve dış kaynaklarla entegrasyon sağlayan yazılımlarda yaygın olarak görülmektedir. Uygulamalar, dış komutları çalıştırırken doğru güvenlik önlemleri almazsa, saldırganlar sisteme zarar verebilir veya yetkisiz veri erişimi sağlayabilir.

3.3.10.4. Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery)

Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery - CSRF), bir web uygulamasında, bir kullanıcının oturum bilgileri kullanılarak, kullanıcının bilgisi ve onayı olmadan başka bir işlem yapılmasına yol açan bir saldırı türüdür. Bu saldırılar, genellikle bir kullanıcının oturum açmış olduğu web sitesindeki güvenlik açıklarından yararlanır. CSRF saldırısı, saldırganın, hedef kullanıcının tarayıcısına zararlı istekler göndererek, kullanıcının isteği dışında işlem gerçekleştirmesini sağlar. İşletim sistemlerine, web uygulamaları üzerinden yapılan yetki yükseltme işlemleri, ciddi güvenlik tehlikeleri barındırmaktadır.

3.3.10.5. Deserileştirme Saldırıları (Deserialization Attacks)

Deserileştirme saldırıları, kötü niyetli verilerin uygulama verisi olarak yeniden oluşturulması ile gerçekleştirilen bir saldırı türüdür. Deserialization, bir veri yapısının

bayt (byte) dizisine dönüştürülüp, ardından bu dizinin geri dönüştürülerek veri yapısına dönüştürülmesidir. Eğer veri doğrulaması yapılmazsa, saldırganlar zararlı veriler göndererek uygulamanın kontrolünü ele geçirebilirler. Bu saldırılar, genellikle uygulamanın güvenli olmayan veri yönetimi veya hatalı yapılandırılması nedeniyle etkili olabilir.

3.3.11. Ağ Tabanlı Saldırılar

İşletim sistemi, ağ üzerinden gelen verileri alır ve işler, bu da onu ağ tabanlı saldırılara karşı savunmasız hale getirebilir. Yaygın ağ tabanlı tehditler, Veri Dinleme (Sniffing), Sahtecilik (Spoofing), Çift Yönlü Yönlendirme (Man-in-the-Middle Attack) olarak görülmektedir.

3.3.11.1. Veri Dinleme (Sniffing)

Ağ üzerindeki veri trafiğini izleyerek, kullanıcı şifreleri ve hassas bilgilerini çalma işlemidir. Saldırganlar, genellikle ağ trafiğini izleyerek, hedef sistemlere ait şifreler, kullanıcı adı bilgileri, kredi kartı numaraları ve diğer hassas verileri elde etmeye çalışırlar. Bu saldırı, genellikle şifrelenmemiş ağ bağlantıları üzerinde gerçekleşir.

3.3.11.2. Sahtecilik (Spoofing)

Sahte kimlik bilgileri kullanarak, hedef bilgisayarları yanıltma ve yetkisiz erişim sağlama saldırısıdır. Spoofing, ağda kimlik sahteciliği yapmak, hedefleri yanıltmak ve yetkisiz erişim sağlamak için kullanılan geniş bir saldırı kategorisidir. Bu tür saldırılar, genellikle ağ güvenliği zafiyetlerinden faydalanarak, hedefin güvenlik önlemlerini aşmayı amaçlar.

Bu saldırılar çoğunlukla, IP Sahteciliği (IP Spoofing), E-posta Sahteciliği (E-mail Spoofing), DNS Sahteciliği (DNS Spoofing), ARP Sahteciliği (ARP Spoofing) şeklinde olmaktadır.

- **IP Sahteciliği (IP Spoofing):** Saldırgan, sahte bir IP adresi kullanarak, hedef bilgisayarları yanıltmak ve onlara erişim sağlamak amacıyla bu yöntemi

kullanır. IP spoofing ile, saldırgan, hedef bilgisayarın gerçek IP adresi gibi görünerek güvenlik önlemlerini aşmaya çalışır.

- **E-posta Sahteciliği (E-mail Spoofing):** Sahte bir e-posta adresi kullanarak, saldırganlar genellikle phishing (oltalama) saldırıları gerçekleştirir. Hedef kullanıcılara güvenilir bir kaynaktan geldiği izlenimi veren zararlı e-postalar gönderilir.
- **DNS Sahteciliği (DNS Spoofing):** Saldırgan, DNS sorgularını yönlendirerek, kullanıcının güvenli olmayan bir web sitesine yönlendirilmesini sağlar. Bu tür saldırılarla, kullanıcılar sahte bir siteye yönlendirilerek, kimlik bilgileri gibi hassas verilerini çalmaya yönelik işlemler yapılır.
- **ARP Sahteciliği (ARP Spoofing):** ARP Spoofing, Address Resolution Protocol (ARP) protokolünün kötüye kullanılmasıdır. Bu saldırıda, saldırgan ağdaki cihazlara yanlış ARP mesajları gönderir ve hedef cihazların, yanlış bir MAC adresine yönlendirilmesi sağlanır. ARP Spoofing, saldırganın ağdaki iletişimi dinlemesine veya yönlendirmesine olanak tanır. Bu saldırı genellikle yerel ağlarda (LAN) yapılır ve iletişimin izlenmesi veya değiştirilmesi amacıyla kullanılır.

3.3.11.3. Çift Yönlü Yönlendirme (Man-in-the-Middle Attack)

Man-in-the-Middle (MitM) saldırıları, bir saldırganın iki taraf arasında gerçekleşen iletişimi gizlice dinlemesi veya manipüle etmesidir. İşletim sistemi, ağ bağlantılarını yönetirken bu tür saldırılara maruz kalabilir. Özellikle şifreli olmayan ağ bağlantılarında, saldırgan iletişimi kesebilir veya değiştirebilir.

MitM saldırıları, kullanıcıların kimlik bilgilerini ele geçirmek veya verileri değiştirmek amacıyla kullanılır. SSL/TLS protokollerinin zayıf kullanımı veya eksik yapılandırmalar, bu tür saldırıların etkili olmasına neden olabilir.

3.4. Bilgi ve İletişim Güvenliği Rehberi Sıkılaştırma Tedbirleri

Bilgi ve İletişim Güvenliği Rehberi (BİGR) sıkılaştırma tedbirlerinde, GNU/Linux ve Windows işletim sistemlerine yönelik sıkılaştırma tedbirleri ayrı ayrı ele alınmış ve her bir işletim sistemi için tedbirler, tedbir seviyelerine göre tablolar halinde

tanımlanmıştır. Bu tablolarda, her bir tedbirin açıklamaları ve uygulanması gereken seviyeler ayrıntılı bir şekilde açıklanmıştır.

3.4.1. Linux İşletim Sistemi Sıkılaştırma Tedbirleri

BİGR 5.1. İşletim Sistemi Sıkılaştırma Tedbirlerine göre Linux işletim sistemleri için 1.seviye 2 adet tedbir, 2.seviye 5 adet, 3.seviye 1 adet olmak üzere toplamda 8 adet tedbir maddesi bulunmaktadır. Bu tedbirler Çizelge 3.5'de gösterilmiştir.

Çizelge 3.5. Linux İşletim Sistemi Sıkılaştırma Tedbirleri

Tedbir No	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.2.1	1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) pasif hale getirilmelidir.
5.1.2.2	1	Yetkili Kullanıcı Hesap Yönetimi	Sisteme erişecek her kişi için ayrı bir kullanıcı hesabı oluşturulmalıdır. Oluşturulan kullanıcılar için yetkiler belirlenmelidir. Kullanılmayan hesaplar kaldırılmalıdır. Sistem kullanıcılarının kabuğu /sbin/nologin olmalıdır. Root login mümkünse engellenmelidir. Tüm makinelerde UID değeri 0 olan tek kullanıcı root olmalıdır. Ayrıca aynı isme veya UID değerine sahip kullanıcı veya grup bulunmamalıdır. Servis ve sistem kullanıcıları hariç parolasız kullanıcılar bulunmamalıdır. Sudoers kullanıcıları değişikliklere karşı takip edilmelidir.
5.1.2.3	2	Dosya Sistemi Güvenli Erişim Düzenlemeleri	İçeriği değiştiğinde, silindiğinde veya taşındığında sistemin çalışmasını olumsuz yönde etkileyebilecek çalışma dosyalarının, kütüphanelerin ve yapılandırma dosyalarının (SUID ve SGID dosyaları, kayıt dosyaları, cron dosyaları, başlangıç betikleri, /etc/passwd, /etc/shadow vb.) yetkilendirmeleri amacına uygun şekilde düzenlenmeli ve kurum politikaları doğrultusunda denetlenmelidir. Varsayılan kullanıcı umask değeri en az yetki prensibine göre ayarlanmalıdır.
5.1.2.4	2	Güvenli Disk Bölümlendirme	İşletim sistemi dosyaları ile kullanıcı dosyaları, /home, /root, /boot, /tmp vb. birimler ayrı disk bölümlerinde tutulmalıdır.
5.1.2.5	2	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	CD/DVD ve USB gibi harici medyanın otomatik olarak mount edilmesini önlemek adına otomatik mount özelliği pasif hale getirilmelidir. Ayrıca /tmp dizini gibi mount noktalarında noexec, nodev, nosuid parametreleriyle çalıştırılabilir dosyalar pasif hale getirilmelidir.
5.1.2.6	2	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	Önemli görülen dosyaların bütünlüğü düzenli olarak kontrol edilmelidir.
5.1.2.7	2	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	Kullanılan makinelerde önyükleyici (bootloader) parolası belirlenmeli ve zorunlu tutulmalıdır. Ayrıca tek kullanıcı modu için kimlik doğrulaması yapılmalıdır. Boot edilebilir cihazlar listesi kısıtlanmalıdır. Kullanılmıyorsa USB, Firewire, Thunderbolt, PCMCIA vb. cihazlar iptal edilmelidir.
5.1.2.8	3	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	İşletim sistemi üzerinde erişim kontrolü, ilgili servisler (SELinux, AppArmor vb.) kullanılarak zorunlu erişim kontrolü (MAC) modeline göre yapılmalıdır.

3.4.2. Windows İşletim Sistemi Sıkılaştırma Tedbirleri

BİGR 5.1. İşletim Sistemi Sıkılaştırma Tedbirlerine göre Windows işletim sistemleri için 1.seviye 6 adet tedbir, 2.seviye 7 adet olmak üzere toplamda 13 adet tedbir maddesi bulunmaktadır. Bu tedbirler Çizelge 3.6'da gösterilmiştir.

Çizelge 3.6. Windows İşletim Sistemi Sıkılaştırma Tedbirleri

Tedbir No	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.3.1	1	Kullanıcı Haklarının Kısıtlanması	Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.
5.1.3.2	1	Otomatik Güncellemenin Aktif Olması	Tüm kullanıcı makinelerinde otomatik güncelleme özelliği aktif hale getirilmelidir.
5.1.3.3	1	SMB Protokolü Güvenliği	Windows işletim sistemlerinde SMB versiyon 1 protokolü yerine daha güvenli ve güncel SMB protokol versiyonları kullanılmalıdır.
5.1.3.4	1	Yerel Yönetici Hesapları Yönetimi	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmalıdır. Gerekli kullanıcılar için varsayılan olarak aynı tanımlanan yerel yönetici hesaplarının parolaları değiştirilmelidir.
5.1.3.5	1	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Etki alanı yöneticisi (Domain Admin) ve diğer yetkili hesapların (Enterprise Admin, Backup Admin ve Schema Admin) sayısı sınırlandırılmalıdır.
5.1.3.6	1	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Yetkili hesapların parola özetlerinin çalınmasının engellenmesi için: Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında gerekli olmadıkça işlem yapılmamalı, işlem yapıldığı durumlarda kullanıcı bilgisayarlarının yeniden başlatılması sağlanmalıdır. Yerel bilgisayarlarda parola özetleri tutulma sayısı 0 yapılmalıdır. Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) grubuna alınmalıdır.
5.1.3.7	2	Kullanılmayan Hesapların Devre Dışı Bırakılması	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmalıdır. Bk. Tedbir No: 3.1.12.10
5.1.3.8	2	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Sistemlerde yer alan varsayılan yönetici ve misafir hesapları pasif hale getirilmelidir.
5.1.3.9	2	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Standart kullanıcıların betik çalıştırma motorlarına (Windows Script Host, Powershell, Command Prompt ve Microsoft HTML Application Host vb.) erişimi engellenmeli veya kısıtlanmalıdır.
5.1.3.10	2	Aktif Dizin Sorguları Güvenliği	Aktif dizin sorguları LDAP protokolü yerine güvenli LDAPs protokolü ile yapılacak şekilde konfigüre edilmelidir. Bk. Tedbir No: 3.2.9.1
5.1.3.11	2	Yönetici Hesaplarının İzlenmesi	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmelidir. Bk. Tedbir No: 3.1.12.11
5.1.3.12	2	Güvenli Yönetici İş İstasyonu Kullanımı	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu konumlandırılmalı, ek yazılım veya rol yüklenmemeli, eposta, internet vb. erişimleri için kullanılmamalıdır.
5.1.3.13	2	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmelidir.

3.5. Sanallaştırma Ortamı

Bu bölümde sanallaştırma ürünleri, ürünlerin karşılaştırılması ve sanallaştırma yöntemi hakkında bilgi verilmektedir.

3.5.1. Sanallaştırma Ürünleri

Sanallaştırma teknolojileri, bilgi teknolojileri altyapısının verimliliğini artırmak, kaynak kullanımını optimize etmek ve maliyetleri düşürmek amacıyla yaygın bir şekilde kullanılmaktadır. Bu teknolojiler, donanım kaynaklarını daha verimli bir şekilde dağıtarak, birden fazla sanal sistemin aynı fiziksel altyapı üzerinde çalışmasını sağlar. Bu bölümde, önde gelen sanallaştırma ürünleri detaylı bir şekilde incelenmiştir. Tez kapsamında kullanılan sanallaştırma yöntemi, belirli gerekliliklere ve hedeflere göre dikkatlice seçilmiş olup, bu seçimde performans, güvenlik ve ölçeklenebilirlik gibi faktörler göz önünde bulundurulmuştur.

3.5.1.1. Oracle VM Virtual Box

Oracle VM VirtualBox, Oracle Corporation tarafından geliştirilen açık kaynaklı bir sanallaştırma platformudur. Çok platformlu yapısı sayesinde Windows, macOS, GNU/Linux ve Solaris işletim sistemlerinde çalışabilmektedir. VirtualBox, kullanıcıların tek bir fiziksel makine üzerinde birden fazla işletim sistemini eşzamanlı olarak çalıştırmasına olanak tanır.

VirtualBox'ın en önemli özelliklerinden biri geniş donanım desteğidir. USB cihazları, çoklu ekranlar ve paylaşımlı klasörler gibi özelliklerle kullanıcı deneyimini zenginleştirir. Ayrıca, anlık görüntü alma (snapshot) ve geri yükleme gibi gelişmiş özellikler sayesinde sistem durumunu kaydetmek ve gerektiğinde geri dönmek mümkündür.

3.5.1.2. Broadcom VMware

VMware, sanallaştırma alanında öncü firmalardan biri olarak kabul edilir ve yakın zamanda Broadcom tarafından satın alınmıştır. VMware'in ürün portföyü,

masaüstü ve sunucu sanallaştırmasından bulut bilişime kadar geniş bir yelpazeyi kapsar. VMware Workstation ve VMware vSphere gibi ürünleri kurumsal seviyede sanallaştırma ihtiyaçlarına karşılamak üzere çıkartılmıştır.

VMware'in en belirgin avantajlarından biri yüksek performans ve güvenilirlik sunmasıdır. vMotion ve High Availability gibi özellikler sayesinde kesintisiz hizmet ve iş sürekliliği sağlanır. Ayrıca, VMware'in geniş ekosistemi ve üçüncü taraf entegrasyonları, işletmelerin özelleştirilmiş çözümler geliştirmesine olanak tanır.

VMware Fusion ve VMware Workstation, 11 Kasım 2024 tarihinden itibaren tüm kullanıcılar için ücretsiz sunulmaya başlanmıştır. Bu değişiklik hem ticari hem eğitimsel hem de bireysel kullanıcıların bu güçlü masaüstü sanallaştırma araçlarına erişimini daha da kolaylaştırmayı hedeflemektedir. Ücretli abonelik modelinden geçişle birlikte, VMware Fusion ve VMware Workstation ürünlerinin Pro sürümleri artık satışa sunulmamaktadır (Chuang,2024).

3.5.1.3. Microsoft Hyper-V

Microsoft Hyper-V, Windows tabanlı sistemler için geliştirilmiş bir hipervizör çözümüdür. Windows Server işletim sistemi ile birlikte ek olarak gelen Hyper-V, özellikle Microsoft teknolojileri ile yoğun çalışan kurumlar için idealdir. Hyper-V, sanal makinelerin oluşturulması, yönetimi ve izlenmesi için kapsamlı araçlar sunar.

Hyper-V'nin öne çıkan özellikleri arasında canlı geçiş (live migration), dinamik bellek yönetimi ve ağ sanallaştırması bulunur. Ayrıca, Hyper-V Replica ile felaket kurtarma senaryoları için sanal makinelerin asenkron replikasyonu mümkündür. Hyper-V, System Center ile entegrasyonu sayesinde merkezi yönetim ve otomasyon imkânları sunmaktadır.

3.5.1.4. Xen Project

Xen Project, açık kaynaklı ve topluluk odaklı bir hipervizördür. İlk olarak Cambridge Üniversitesi'nde geliştirilen Xen, günümüzde Linux Foundation tarafından

desteklenmektedir (Xenserver, 2024). Xen, bulut servis sağlayıcıları ve büyük ölçekli veri merkezleri tarafından tercih edilmektedir.

Xen'in mimarisi, güvenlik ve izolasyon konularına odaklanır. Sanal makinelerin ayrıcalıklı ve ayrıcalıksız modlarda çalışabilmesi, kaynakların daha güvenli bir şekilde yönetilmesini sağlar. Xen, farklı işletim sistemlerini ve çekirdekleri destekleyerek esneklik sunar.

3.5.1.5. KVM

KVM, Intel VT veya AMD-V gibi donanım sanallaştırma teknolojilerini destekleyen sistemler üzerinde çalışabilen, GNU/Linux işletim sistemi için geliştirilmiş, çekirdek düzeyinde bir sanallaştırma çözümüdür. Bu çözüm, 32-bit (x86) işlemci mimarisine sahip olup açık kaynaklı bir hipervizör olarak işlev görmektedir (Işık, 2021).

KVM, donanım tabanlı sanallaştırma özelliklerini kullanarak yüksek performanslı sanal makineler oluşturur. Açık kaynaklı yapısı ve geniş topluluk desteği sayesinde sürekli gelişmektedir.

KVM'nin avantajları, düşük işlemci yükü, yüksek derecede ölçeklenebilirlik ve güçlü güvenlik önlemleri ile dikkat çekmektedir. Libvirt ve QEMU gibi araçlarla birlikte kullanıldığında, sanal makinelerin yönetimi ve otomasyonu kolaylaşır. KVM, bulut bilişim platformları, özellikle OpenStack tarafından yoğun bir şekilde kullanılmaktadır.

3.5.1.6. Proxmox

Proxmox Virtual Environment, açık kaynaklı bir sanallaştırma yönetim platformudur. KVM ve Linux Containers (LXC) teknolojilerini bir araya getirerek hem tam sanallaştırma hem de konteyner tabanlı sanallaştırma imkânı sunmaktadır. Web tabanlı arayüzü sayesinde kullanıcı dostu bir yönetim deneyimi sağlar.

Proxmox'un özellikleri arasında yüksek erişilebilirlik kümeleri, depolama replikasyonu ve yedekleme çözümleri bulunur. Ayrıca, ZFS entegrasyonu sayesinde

gelişmiş depolama yönetimi ve veri güvenliği sağlar. Proxmox, özellikle küçük ve orta ölçekli işletmeler için maliyet etkin bir çözüm olarak öne çıkar.

3.5.2. Sanallaştırma Ürünlerinin Karşılaştırması

Sanallaştırma ürünleri, farklı ihtiyaç ve ölçeklere göre çeşitli özellikler sunar. Oracle VM VirtualBox, daha çok kişisel kullanım ve test ortamlarında tercih edilirken, VMware ve Hyper-V, kurumsal düzeyde gelişmiş özellikler ve teknik destek sağlamaktadır. Xen Project ve KVM, açık kaynaklı ve esnek yapıları ile büyük ölçekli ve özelleştirilmiş sanallaştırma çözümleri için uygun seçenekler sunmaktadır. Proxmox ise entegre yapısı ve kullanım kolaylığıyla öne çıkmaktadır.

Performans açısından, KVM ve VMware genellikle yüksek performans gerektiren uygulamalar için tercih edilirken, yönetim ve kullanım kolaylığı açısından Hyper-V ve Proxmox daha avantajlıdır. Maliyet değerlendirmesinde ise, açık kaynaklı ürünler olan KVM, Xen ve Proxmox, lisans maliyetlerini minimize etmek isteyen kurumlar için daha uygun bir seçenek oluşturmaktadır.

Güvenlik ve destekleme politikaları, sanallaştırma çözümü seçiminde kritik bir rol oynamaktadır. VMware ve Microsoft, kapsamlı teknik destek ve güvenlik güncellemeleri sunarken, açık kaynaklı ürünler topluluk desteğine dayanır. Sonuç olarak, sanallaştırma çözümünün seçimi, kurumun özel ihtiyaçları, mevcut altyapısı ve gelecekteki büyüme hedefleri göz önünde bulundurularak yapılmalıdır.

3.5.3. Sanallaştırma Yöntemi

Yöntem kapsamında ilk adım, Windows ve GNU/Linux ailesine ait işletim sistemlerinden en yaygın kullanılan istemci modellerinin belirlenmesi olup, bu modeller sanal makineler olarak çalıştırılacaktır. İşletim sistemleri belirlenirken, sıkılaştırma kurallarının denetim aracının da desteklediği işletim sistemlerinden seçilmiştir. Sanallaştırma sürecinde, bilinen popüler sanallaştırma yazılımları olan Oracle VM VirtualBox ve Broadcom VMware Workstation kullanılmıştır. Bu çalışma kapsamında, profesyonel bir çözüm olarak GNU Genel Kamu Lisansı (GPL) ile serbestçe ve ücretsiz kullanılabilen Oracle VM VirtualBox bu yüzden tercih edilmiştir. Ayrıca, 2024 yılında

Broadcom tarafından kullanıcılara ücretsiz olarak sunulmaya başlanan VMware, yedeklilik ve çeşitlilik sağlamak amacıyla dahil edilmiş ve her iki yazılım birlikte kullanılmıştır.

Sanal makinelerden aynı işletim sisteminden iki adet kopya imaj oluşturulmuştur. Birinci imaj, analiz süreçlerinin gerçekleştirilmesi amacıyla konfigürasyon ayarlarını orijinal haliyle koruyarak hazırlanmıştır. İkinci imaj ise iyileştirme modeli uygulanarak düzenlenmiş ve bu sayede karşılaştırmalı analizler yapılmıştır. Bu yöntemle, her iki imaj arasındaki farklar belirlenip açığa çıkarılmasıyla sonlandırılmıştır.

3.6. Sıkılaştırma Kurallarının Denetimi

Sıkılaştırma kurallarının denetlenmesinde üçüncü taraf araçlar önemli bir rol üstlenmektedir. Microsoft Baseline Security Analyzer (MBSA), güvenlik güncellemelerinin ve yaygın yapılandırma hatalarının tespit edilmesi amacıyla kullanılan ücretsiz bir araçtır (Microsoft, 2012). Ancak, bu araç yalnızca Windows işletim sistemlerine yönelik denetim yapmaktadır.

GNU/Linux analiz süreçlerinde de üçüncü taraf araçlar önemlidir. Lynis, kapsamlı bir güvenlik taraması gerçekleştirerek zafiyetleri keşfetmeye ve konfigürasyon iyileştirmeleri önermeye yardımcı olan yaygın bir açık kaynak güvenlik denetim aracıdır (Wikipedia, 2023). Sadece GNU/Linux işletim sistemlerine yönelik denetim yapmaktadır.

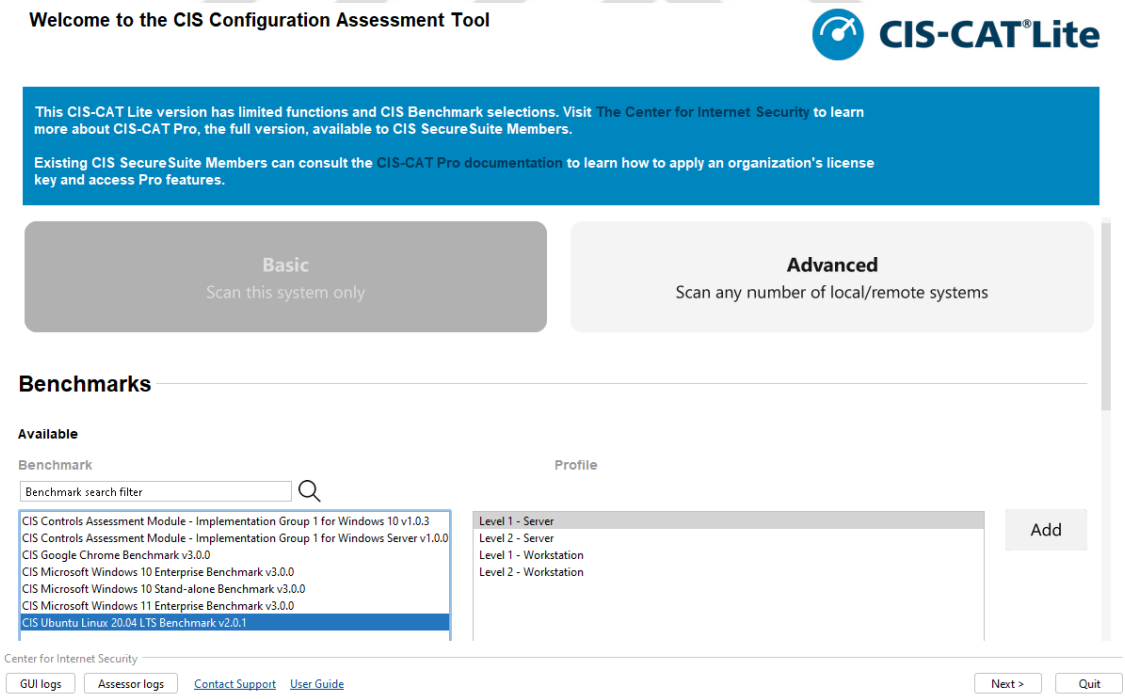
Center for Internet Security (CIS) tarafından yayımlanan güvenlik kılavuzlarına dayalı olarak geliştirilen CIS Benchmark Tools, birçok işletim sistemi ve yazılımın denetimi için kullanılmaktadır. Bu araç, sistem yapılandırmalarını kontrol eder ve CIS'in önerdiği güvenlik standartlarına uyumluluğu değerlendirir (CIS, 2023).

Bu tez kapsamında, hem GNU/Linux hem de Windows işletim sistemlerinde kullanılabilen ve ücretsiz olarak sunulan CIS-CAT-Lite aracı, her iki sistem için de kapsamlı güvenlik testi yapma olanağı sağladığı için tercih edilmiştir.

3.6.1. CIS-CAT Denetim Aracı

CIS-CAT (Center for Internet Security Configuration Assessment Tool), CIS Ölçütleri (Benchmark) doğrultusunda sistem yapılandırmalarını değerlendirmek ve denetlemek için kullanılan bir araçtır. CIS-CAT'in Lite ve Pro olmak üzere iki farklı sürümü bulunmaktadır. CIS-CAT, her iki sürümüyle de kullanıcıların güvenlik yapılandırmalarını gözden geçirmelerine ve potansiyel zafiyetleri belirlemelerine olanak sağlar.

CIS-CAT Lite sürümü, belirli işletim sistemleri üzerinde ücretsiz denemeler ve testler yapma imkânı sunmaktadır. Şekil 3.3'te görülen CIS-CAT Lite denetim aracı arayüzünde, Windows 10 Enterprise ve Ubuntu 20.04 LTS sürümleri test edilebilmektedir. Bu nedenle, çalışmamızda her iki işletim sistemi sürümü baz alınarak testler gerçekleştirilmiştir. CIS-CAT'in profesyonel (Pro) sürümü daha fazla işletim sistemi desteği sunmakta olup, ücretli bir versiyondur.



Şekil 3.3. CIS-CAT Lite denetim aracı arayüzü

CIS-CAT'i çalıştırmak için, bazı Java bağımlılıkları gerekebilir, bu nedenle öncelikle Java yüklü olmalıdır. GNU/Linux işletim sistemlerinde Java'nın

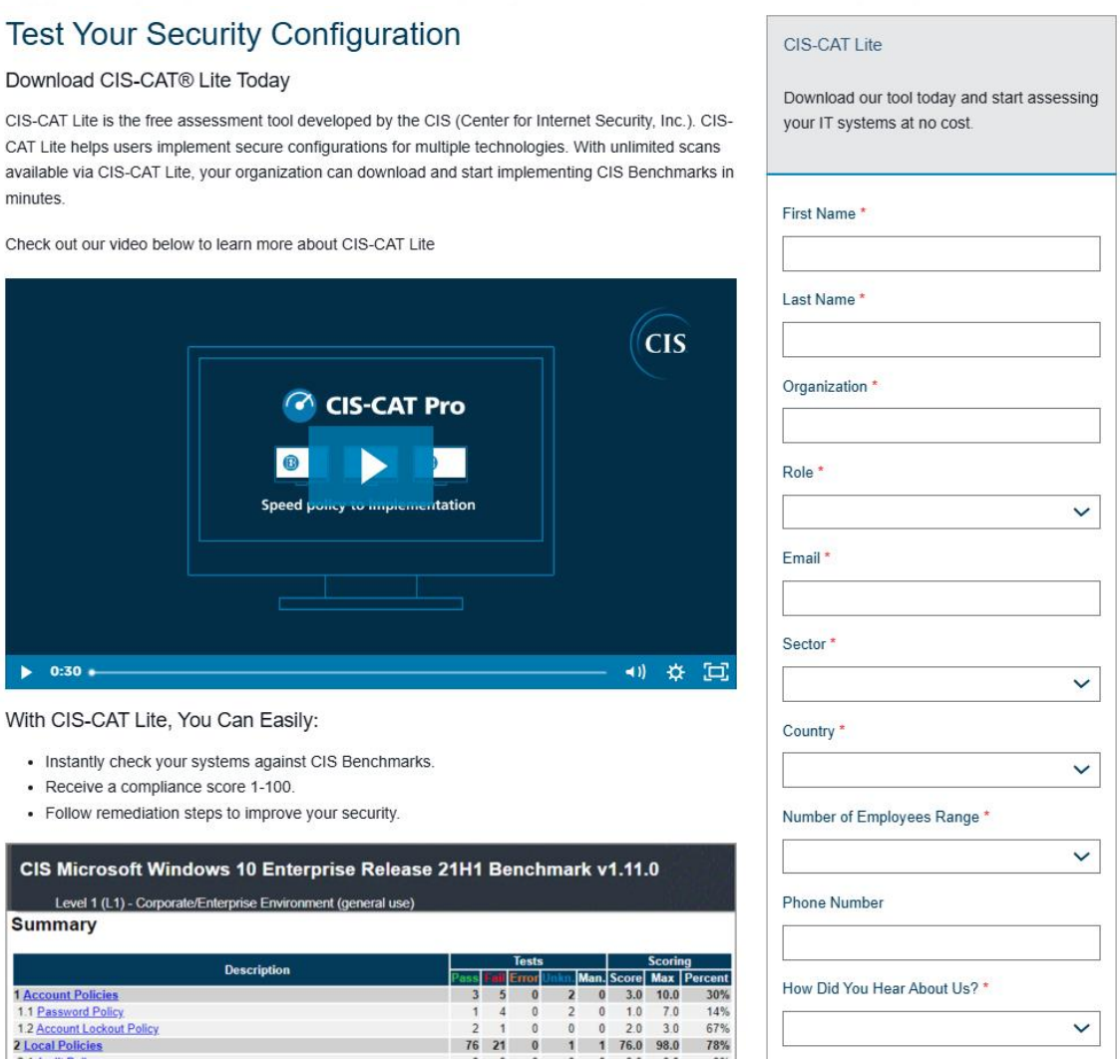
yüklenebilmesi “sudo apt install openjdk-11-jre” komutu kullanılabilir. Windows işletim sistemlerinde Java kurulumu için Java’nın resmi internet sitesi kullanılabilir.

CIS-CAT'in sunduğu detaylı raporlama özellikleri, sistem yöneticilerinin güvenlik açıklarını tespit etmelerini ve bu açıkları gidermelerine yönelik öneriler alabilmelerini sağlar. CIS-CAT, yalnızca sistem güvenliği için değil, aynı zamanda düzenleyici uyum ve iç denetimler için de önemli bir araçtır.

4. İYİLEŞTİRME MODELİ

BİGR (Bilgi ve İletişim Güvenliği Rehberi) ile CIS (Center for Internet Security) denetimleri arasındaki karşılaştırmalar, kurumların güvenlik uyumluluğunu sağlamak ve potansiyel güvenlik açıklarını belirlemek için önemli bir yöntemdir. BİGR, CIS denetimlerinin uygulanabilirliğini değerlendirirken, her bir denetimin "pass" ya da "fail" olarak test edilmesini sağlar ve buna bağlı olarak iyileştirme adımları önerir.

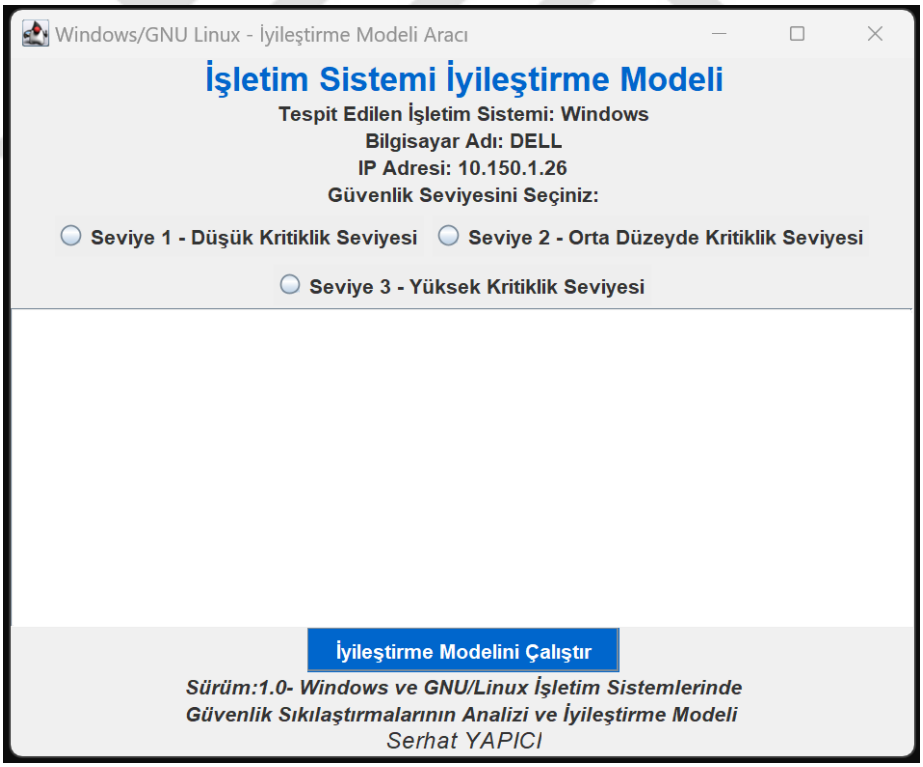
Bu adımlara başlarken Şekil 4.1'e göre Cisesecurity resmi internet adresi üzerinden CIS-CAT Lite indirmek için gerekli bilgileri doldurulmalıdır.



Şekil 4.1. CIS-CAT Lite resmi internet sitesi indirme sayfası

Bilgiler doldurulduktan sonra, CIS'ın resmi e-posta adresi üzerinden Java denetim aracı gönderilmektedir. Java denetim aracı "Assessor" çalıştırılarak daha önce ifade edilen, Şekil 3.3. CIS-CAT Lite denetim aracı arayüzü karşılayacaktır ve buradan işletim sistemi modeli seçilerek analiz edilmektedir. Analiz sonuçları Hiper Metin İşaretleme Dili, HyperText Markup Language (HTML) olarak kayıt edilmektedir.

Java dili kullanılarak gerçekleştirilen bu iyileştirme modeli aracı, Windows işletim sistemleri için Powershell Script (.ps1) uzantısı, GNU/Linux işletim sistemleri için (.sh) uzantısı ile modellenmiştir. Şekil 4.2'de, bu çalışmada gerçekleştirilen iyileştirme yazılımının giriş arayüzü gösterilmektedir. İyileştirme modeli olarak sunulan 'ProgramGUI.java' çalıştırıldığında, program sistem bilgilerinden işletim sistemi, bilgisayar adı ve IP adresini otomatik olarak çekmektedir. Kurum veya kuruluş, BİGR'e göre kritiklik seviyesini seçtikten sonra iyileştirme modeli çalıştırılarak sıkılaştırma işlemi yapılmaktadır.



Şekil 4.2. İşletim sistemi iyileştirme modeli görüntüsü

Bu süreçte, BİGR ve CIS denetimleri arasında yapılan karşılaştırma tablosunda, her bir tedbirin uygulanıp uygulanmadığına göre otomatik kod geliştirme işlemleri gerçekleştirilmiştir. Eğer bir tedbir CIS uyumlu olarak başarıyla uygulanmışsa, bu

tedbirin yeni bir kod geliştirme işlemine ihtiyaç duymadığı kabul edilmiştir. Yani, sistem zaten güvenlik gereksinimlerini karşılıyorsa, ek bir yazılım veya yapılandırma değişikliği yapılmamıştır. Bu işlemler ilk imaj kurulumundan sonra yapılması, sonradan yapılacak olan değişiklikleri etkilememesi için önerilmektedir.

Harici olarak kodlar istenildiği gibi Windows tarafında Powershell ile yüklenebilirken GNU/Linux tarafında Ansible ile yüklenebilir.

Ansible playbook, birbirine bağlı birçok işin rutin olarak yapıldığı bir ortamda, bu işleri belirli bir sıraya, işlerin çıktılarına göre kararlara bağlayan ve silsile yoluyla çalışmasını sağlayan üst seviye bir iş akışıdır (Pazoğlu, 2020). Tüm temel güvenlik yapılandırmalarını kapsayan kapsamlı güvenlik standartlarını tanımlamanıza olanak tanır. Bu playbook'lar, sıkılaştırılmış bir başlangıç durumu oluşturmak için sistemlere hızlı bir şekilde uygulanabilir.

Ansible aynı zamanda sistemleri sürekli olarak izleyebilen ve uyumluluk raporları oluşturabilen bir araçtır. Bu, sistemlerin belirlenen güvenlik standartlarına ne kadar uygun olduğunu izlemeyi ve değerlendirmeyi sağlar. Bu raporlar, herhangi bir uyumsuzluk veya potansiyel sorunun belirlenmesi için kullanılabilir ve Ansible, bu sorunların gözden geçirilmesi ve düzeltilmesi için bir mekanizma sağlar.

4.1. Windows İşletim Sistemi

4.1.1. Kullanıcı Haklarının Kısıtlanması

Windows sistemlerinde güvenlik, kullanıcı haklarının en az yetki prensibine dayalı olarak yönetilmesini gerektirir. Bu prensibe göre, her kullanıcı yalnızca görevini yerine getirebilmesi için gerekli olan izinlere sahip olmalıdır. Gereksiz yetkilerin kısıtlanmasıyla sistemin güvenliğini artırarak potansiyel saldırılara karşı savunmayı güçlendirir.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), kurumların güvenlik durumu değerlendirmelerini CIS (Center for Internet Security) denetimlerinden yararlanarak yapmaktadır. Bu denetimler sistemin güvenlik politikaları ve uygulamaları ile uyumunu

değerlendirir. “Kullanıcı Haklarının Kısıtlanması” tedbiri, CIS denetimlerinin bir parçası olarak, kullanıcıların sadece işlerini gerçekleştirebilmek için gerekli olan haklara sahip olmalarını ve fazladan yetkilerin verilmemesini önerir. Çizelge 4.1’de, BİGR 5.1.3.1 maddesi, Kullanıcı Haklarının Kısıtlanması tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.1. Windows işletim sistemi kullanıcı haklarının kısıtlanması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.1	Kullanıcı Haklarının Kısıtlanması	Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' 2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users' 2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One' 2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' 2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users' 2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' 2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators' 2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' 2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users' 2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators' 2.2.11 (L1) Ensure 'Create a token object' is set to 'No One' 2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' 2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One' 2.2.14 (L1) Configure 'Create symbolic links' 2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators' 2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' 2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests' 2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests' 2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests' 2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' 2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' 2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' 2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' 2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' 2.2.26 (L1) Ensure 'Load and unload device drivers' is

			set to 'Administrators' 2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One' 2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' 2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One' 2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators' 2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' 2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators' 2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' 2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' 2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators' 2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users' 2.2.39 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'

4.1.1.1. Kimlik Bilgisi Yöneticisinin Güvenilir Bir Şekilde Yapılandırılması

Credential Manager (Kimlik Bilgisi Yöneticisi), özellikle yedekleme ve geri yükleme işlemlerinde kullanılan bir güvenlik ayarıdır. Güvenlik ayarı kullanıcıların kimlik bilgilerini saklama ve yönetme işlevine sahiptir. Ancak bu güvenlik ayarı herhangi bir hesaba verilmemelidir çünkü bu hak yalnızca işletim sistemi Winlogon (Windows Oturum Açma) servisine atanmalıdır. Aksi takdirde başka bir hesap bu hakka sahip olduğunda kötü niyetli yazılımlar veya uygulamalar bu hesapla kimlik bilgilerine erişebilir ve ciddi güvenlik açıkları oluşturulabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.1 maddesi tedbirine göre yapılan testlerde, halihazırda mevcut sistemde, “Access Credential Manager as a trusted caller” ayarının “Hiç Kimse (No One)” olarak yapılandırıldığı tespit edilmiştir ve bu durumda sistemin güvenliğinde herhangi bir ihlal bulunmamaktadır. Bu nedenle ayar zaten doğru bir şekilde yapılandırıldığı için iyileştirme modelinde ek bir sıkılaştırma uygulanmamıştır.

4.1.1.2. Ağ Üzerinden Erişim Politikası Gruplarının Ayarlanması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.2 maddesinde bulunan Windows güvenlik yapılandırmalarında SeNetworkLogonRight adlı kullanıcı politikalarını kontrol eder ve yalnızca belirli gruplara, yani Yöneticiler (Administrators) ve Uzak Masaüstü Kullanıcıları (Remote Desktop Users) gruplarına ağ üzerinden bilgisayara erişim izni verir. Bu güvenlik önlemi sadece yetkili kullanıcıların ağ üzerinden sisteme bağlanmasına olanak tanır ve diğer kullanıcıların bu tür erişim taleplerini engeller.

İyileştirme modeli olarak, SecEdit aracını kullanarak mevcut kullanıcı haklarını dışa aktardıktan sonra tavsiye edilen grupların doğru şekilde atanıp atanmadığını kontrol eder. Eğer mevcut yapılandırma gerekli grupları içermiyorsa, bu gruplar eklenir veya güncellenir. Bu işlem sistemde gereksiz kullanıcı erişimlerinin engellenmesine ve güvenlik risklerinin azaltılmasına yardımcı olur. Kullanıcıların ağ üzerinden bilgisayara bağlanmalarına izin verir ve Server Message Block (SMB) tabanlı protokoller, NetBIOS, Common Internet File System (CIFS) ve Component Object Model Plus (COM+) gibi çeşitli ağ protokollerinin çalışabilmesi için gereklidir.

Bu ayarın önerilen durumu, Yöneticiler (Administrators) ve Uzak Masaüstü Kullanıcıları gruplarının bu hakka dahil edilmesidir. Bu ayar kullanıcıların paylaşılmış yazıcılara ve dosyalara erişebilmesi için gereklidir.

Bu yapılandırmayı uygularken dikkat edilmesi gereken önemli noktalar şunlardır:

- Domain Controller (etki alanı denetleyici) üzerinde bu kullanıcı hakkı tüm kullanıcılardan kaldırılırsa, kimse etki alanına giriş yapamayacak ya da ağ kaynaklarını kullanamayacaktır.
- Member Server (üye sunucu) üzerinde bu hak kaldırılırsa, kullanıcılar bu sunuculara ağ üzerinden bağlanamayacaktır.
- IPsec bağlantılarının başarılı bir şekilde yapılabilmesi için bu kullanıcı hakkı, başlatan makinelerde bulunmalıdır.

- ASP.NET veya Internet Information Services (IIS) gibi ek bileşenler kuruluysa bu bileşenler için gereken ek hesaplar da bu hakka sahip olmalıdır.

Bu ayarın doğru yapılandırılmasıyla yalnızca yetkilendirilmiş kullanıcıların ağ üzerinden bilgisayara erişmesini sağlar ve sistemin güvenliğini artırır.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, Windows işletim sisteminde "SeNetworkLogonRight" kullanıcı politikasını kontrol etmek ve gerekirse güncellemek için kullanılır. Bu politika, ağ üzerinden bilgisayara bağlanma hakkını belirler ve yalnızca yetkili kullanıcı gruplarına (Yöneticiler ve Uzak Masaüstü Kullanıcıları) bu hakkı verir. Script, "secedit.exe" aracı ile mevcut güvenlik yapılandırmasını dışa aktarır, ardından "SeNetworkLogonRight" politikasının mevcut değerini kontrol eder. Eğer politika zaten mevcutsa, bu değer önerilen SID'ler (Yöneticiler ve Uzak Masaüstü Kullanıcıları) ile güncellenir eğer politika yoksa, yeni bir satır eklenir. Yapılandırma dosyasındaki değişiklikler ardından "secedit" komutu ile uygulanır ve son olarak geçici dosya silinir. Bu işlem, ağ erişim politikalarının doğru şekilde yapılandırılmasını ve yalnızca yetkili kullanıcıların sisteme erişimini sağlar.

```
$MetodArgumani = 'SeNetworkLogonRight'
$onerilenDegerler = @(
    '*S-1-5-32-544',  # Yöneticiler SID'i
    '*S-1-5-32-555'   # Uzak Masaüstü Kullanıcıları SID'i
)
$sidler = @()
$onerilenDeger = ''
$SecEditPath = 'C:\Windows\System32\secedit.exe'

# Çalıştırılan script'in bulunduğu dizin
$scriptDirectory = (Get-Location).Path
$benzersiz = (Get-Date).ToString("yyyyMMddHHmmssfff")
# Dosya yolunu düzgün bir şekilde oluştur
$secedit = "$scriptDirectory\secedit$benzersiz.cfg"

Write-Host "Geçici dosya yolu: $secedit"

# Secedit komutuyla USER_RIGHTS alanını dışa aktar
& $SecEditPath /export /areas USER_RIGHTS /cfg $secedit /quiet

if (-Not (Test-Path $secedit)) {
    Write-Host "Geçici dosya bulunamadı: $secedit"
    exit
}

$konfigurasyon = Get-Content -Path $secedit

# Tavsiye edilen SID'leri birleştir
for ($i = 0; $i -lt $onerilenDegerler.Count; $i++) {
    if ($i -eq $onerilenDegerler.Count - 1) {
        $onerilenDeger += $onerilenDegerler[$i]
    }
```

```
33.     else {
34.         $onerilenDeger += $onerilenDegerler[$i] + ','
35.     }
36. }
37.
38. # 'SeNetworkLogonRight' politikasını kontrol et
39. if (Get-Content $secedit | Select-String -Pattern $MetodArgumani) {
40.     # Politika varsa, mevcut değeri tavsiye edilen değerle değiştir
41.     $konfigurasyon = $konfigurasyon -replace "$MetodArgumani\s*=\s*.*$",
"$MetodArgumani = $onerilenDeger"
42.     $konfigurasyon | Set-Content -Path $secedit
43. } else {
44.     # Politika yoksa, yeni satır ekle
45.     $yeniKonfigurasyon = @()
46.     $indeks = $konfigurasyon.IndexOf("[Privilege Rights]") + 1
47.     $eklenecekSatin = "$MetodArgumani=$onerilenDeger"
48.     foreach ($satir in $konfigurasyon) {
49.         $yeniKonfigurasyon += $satir
50.         if ($konfigurasyon.IndexOf($satir) -eq $indeks) {
51.             $yeniKonfigurasyon += $eklenecekSatin
52.         }
53.     }
54.     $yeniKonfigurasyon | Set-Content -Path $secedit
55. }
56.
57. # Secedit komutunu çalıştırarak yapılandırmayı uygula
58. & $SecEditPath /configure /db secedit.sdb /cfg $secedit
59.
60. # Geçici dosyayı sil
61. Remove-Item -Path $secedit -Force
```

4.1.1.3. İşletim Sistemi Servisi Yetkisinde Çalışan Kullanıcıların Sıkılaştırılması

İşletim sistemi servisi gibi çalışan kullanıcı hesaplarının güvenlik ayarları bir işlem tarafından herhangi bir kullanıcı kimliğinin üstlenilmesine ve dolayısıyla kullanıcının erişim haklarına sahip olan kaynaklara ulaşılmasına olanak tanır. Bu kullanıcı hakkı son derece güçlüdür ve bu haktan yararlanan bir kullanıcı, bilgisayar üzerinde tam kontrol sağlayabilir ve faaliyetlerinin izlerini silebilir. Bu güvenlik ayarının önerilen durumu “Hiç Kimse (No One)” olarak yapılandırılmalıdır.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.3 maddesi tedbirine göre yapılan testlerde, halihazırda mevcut sistemde “Act as part of the operating system” ayarının “Hiç Kimse (No One)” olarak yapılandırıldığı tespit edilmiştir. Bu nedenle güvenlik ayarı doğru şekilde yapılandırıldığı için iyileştirme modelinde ek bir sıkılaştırma uygulanmamıştır.

4.1.1.4. İşlemler İçin Bellek Kotalarını Ayarları

Bu güvenlik ayarı bir kullanıcının bir işleme tahsis edilebilecek bellek miktarını ayarlamasına olanak tanır. Bellek kotalarını ayarlamak, sistem performansını

iyileştirmek için faydalı olabilir ancak saldırganlar tarafından kötüye kullanılabilir. Bu yetki bir DoS (Hizmet Reddi) saldırısı başlatmak için kullanılabilir. Bu güvenlik ayarının önerilen durumu, "Yöneticiler (Administrators), LOCAL SERVICE, NETWORK SERVICE" olarak yapılandırılmasıdır.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.4 maddesi tedbirine göre yapılan testlerde, halihazırda mevcut sistemde "Adjust memory quotas for a process" ayarının doğru bir şekilde yapılandırıldığı tespit edilmiştir. Bu nedenle, bu ayar zaten doğru şekilde yapılandırıldığı için iyileştirme modelinde ek bir sıkılaştırma uygulanmamıştır.

4.1.1.5. Yerel Oturum Açma İzni Kuralları

"Allow log on locally" politikası, Windows işletim sistemlerinde kullanıcılara yerel oturum açma izni veren bir güvenlik ayarıdır. CIS Benchmark v3.0.0-2.2.5 yönergelerine göre, bu izin yalnızca sistemin yönetimi için gerekli olan gruplara ve kullanıcılara verilmelidir. En az ayrıcalık ilkesine göre, Yöneticiler (Administrators) ve Kullanıcılar (Users) gibi temel grupların bu hakka sahip olması gerekir. Böylece yalnızca yetkili kullanıcılar ve gruplar yerel olarak sisteme giriş yapabilir.

BİGR 5.1.3.1 maddesi, kullanıcı haklarının sadece gerekli kişilerle sınırlı tutulması gerektiğini vurgular. CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.5 maddesi tedbirine göre, sadece gerekli olan yetkilere sahip kullanıcıların sisteme erişim sağlamak için yerel oturum açma iznine sahip olmalarını sağlar. Bu yapılandırma sistem güvenliğini artırır, yetkisiz erişimleri ve potansiyel tehditleri azaltır.

"Yerel Olarak Giriş Yapmaya İzin Ver" Ayarını 'Yöneticiler (Administrators)' "Kullanıcılar (Users) Olarak Yapılandırma" olarak geçen güvenlik ayarı, kullanıcıların bilgisayarınıza yerel olarak nasıl giriş yapabileceğini belirler. CTRL+ALT+DEL tuşlarına basarak başlatılan oturumlar bu kullanıcı hakkını gerektirir. Ayrıca, Terminal Hizmetleri / Uzaktan Masaüstü Hizmetleri veya IIS üzerinden giriş yapmaya çalışan kullanıcılar da bu hakka ihtiyaç duyarlar.

Bu ayarın önerilen durumu, Yöneticiler (Administrators) ve Kullanıcılar (Users) gruplarının dahil edilmesidir. Varsayılan olarak, Konuk hesabı da bu kullanıcı hakkına sahip olmasına rağmen bu hesap varsayılan olarak devre dışıdır. Bu kullanıcı hakkı genellikle Yöneticiler (Administrators) ve Kullanıcılar (Users) gruplarıyla sınırlı olmalıdır.

Herhangi bir kullanıcı, yerel olarak giriş yapmaya izin ver hakkına sahip olduğunda, bilgisayarın konsoluna giriş yapabilir. Bu hak ile kötü niyetli yazılımların çalıştırılmasına ve yetkisiz kullanıcıların bilgisayarın kontrolünü ele geçirmesine yol açabilir.

Bu ayarı yapılandırırken, Yöneticiler (Administrators) ve Kullanıcılar (Users) gruplarını dışarıda bırakmak, bu gruplara atanan yönetici rollerinin yeteneklerini sınırlayabilir. Bu yüzden yapılan değişikliklerin yetkilendirilmiş kullanıcıların görevlerini yerine getirebilmesini engellemeyecek şekilde yapılması önemlidir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, Windows işletim sisteminde “SeInteractiveLogonRight” kullanıcı politikasını kontrol etmek ve gerekirse güncellemek için kullanılır. Bu politika, yerel olarak sisteme giriş yapma iznini belirler ve yalnızca gerekli gruplara (Yöneticiler ve Kullanıcılar) verilmesi gereken bir güvenlik ayarıdır. Script, “secedit.exe” aracını kullanarak mevcut güvenlik yapılandırmasını dışa aktarır, ardından “SeInteractiveLogonRight” politikasının mevcut değerini kontrol eder. Eğer politika zaten mevcutsa, bu değer önerilen SID’ler (Yöneticiler ve Kullanıcılar) ile güncellenir eğer politika yoksa, yeni bir satır eklenir. Yapılandırma dosyasındaki değişiklikler ardından “secedit” komutu ile uygulanır ve son olarak geçici dosya silinir. Bu işlem, yalnızca yetkili kullanıcıların yerel oturum açma iznine sahip olmasını ve sistemin güvenliğini artırmayı sağlar.

```
1. $MetodArgumani = 'SeInteractiveLogonRight'
2. $onerilenDegerler = @(
3.     '*S-1-5-32-544'  # Yöneticiler SID'i
4.     '*S-1-5-32-545'  # Kullanıcılar SID'i
5. )
6. $sidler = @()
7. $onerilenDeger = ''
8. $SecEditPath = 'C:\Windows\System32\secedit.exe'
9. $benzersiz = (Get-Date).ToString("yyyyMMddHHmmssfff")
10. # Geçici dosya yolunu oluştur
11. $secedit = $Env:Temp + '\secedit' + $benzersiz + '.cfg'
```

```
12.
13. # Secedit komutuyla USER_RIGHTS alanını dışa aktar
14. &$SecEditPath /export /areas USER_RIGHTS /cfg $secedit /quiet
15. $config = Get-Content -Path $secedit
16.
17. # Tavsiye edilen SID'leri birleştir
18. for ($i = 0; $i -lt $onerilenDegerler.Count; $i++) {
19.     if ($i -eq $onerilenDegerler.Count - 1) {
20.         $onerilenDeger += $onerilenDegerler[$i]
21.     }
22.     else {
23.         $onerilenDeger += $onerilenDegerler[$i] + ','
24.     }
25. }
26.
27. # 'SeInteractiveLogonRight' politikasını kontrol et
28. if (Get-Content $secedit | Select-String -Pattern $MetodArgumani) {
29.     # Politika varsa, mevcut değeri tavsiye edilen değerle değiştir
30.     $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
31.     $config | Set-Content -Path $secedit
32. } else {
33.     # Politika yoksa, yeni satır ekle
34.     $yeniKonfigurasyon = @()
35.     $indeks = $config.IndexOf("[Privilege Rights]") + 1
36.     $eklenecekSatir = "$MetodArgumani=$onerilenDeger"
37.     foreach ($satir in $config) {
38.         $yeniKonfigurasyon += $satir
39.         if ($config.IndexOf($satir) -eq $indeks) {
40.             $yeniKonfigurasyon += $eklenecekSatir
41.         }
42.     }
43.     $yeniKonfigurasyon | Set-Content -Path $secedit
44. }
45.
46. # Secedit komutunu çalıştırarak yapılandırmayı uygula
47. &$SecEditPath /configure /db secedit.sdb /cfg $secedit
48.
49. # Geçici dosyayı sil
50. Remove-Item -Path $secedit -Force
```

4.1.1.6. Uzak Masaüstü Hizmetleriyle Giriş İzinleri Ayarları

Tedbirde belirtilen bu güvenlik ayarı, hangi kullanıcıların veya grupların Remote Desktop Services (RDS) istemcisi olarak oturum açma hakkına sahip olduğunu belirler. Organizasyonunuzda yardım masası stratejisi olarak Remote Assistance (Uzak Yardım) kullanılıyorsa, bir grup oluşturulmalı ve bu kullanıcı hakkı Group Policy (Grup Politikası) aracılığıyla atanmalıdır. Eğer organizasyonunuzda Remote Assistance kullanılmıyorsa, bu kullanıcı hakkı yalnızca Yöneticiler (Administrators) grubuna atanmalı ya da Restricted Groups (Sınırlı Gruplar) özelliği kullanılarak, Remote Desktop Users (Uzak Masaüstü Kullanıcıları) grubunda hiçbir kullanıcı hesabının bulunmaması sağlanmalıdır.

Bu kullanıcı hakkı, yalnızca Yöneticiler (Administrators) grubuna ve gerekirse Uzak Masaüstü Kullanıcıları (Remote Desktop Users) grubuna atanarak, istenmeyen kullanıcıların ağdaki bilgisayarlara Remote Assistance (Uzak Yardım) özelliğiyle erişmesi engellemiş olunur. Bu güvenlik ayarının önerilen durumu: Yöneticiler (Administrators), Uzak Masaüstü Kullanıcıları (RDU) olarak yapılandırılmalıdır.

Yapılan testlerde CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.6 maddesi tedbirine göre, halihazırda mevcut sistemde "Allow log on through Remote Desktop Services" ayarının doğru bir şekilde yapılandırıldığı tespit edilmiştir. Bu nedenle, güvenlik ayarları doğru şekilde yapılandırıldığı için iyileştirme modelinde de ek bir sıkılaştırma uygulanmamıştır.

4.1.1.7. Dosya ve Dizileri Yedekleme Yetkisinin Ayarları

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.7 tedbirine göre, "Backup files and directories" (Dosya ve dizinleri yedekleme) politikası, yalnızca güvenilir ve yetkilendirilmiş kişilere, yani yöneticiler grubuna atanmalıdır. Bu politika, sistemdeki kritik dosya ve dizinlerin yedeklenmesini yönetme yetkisini yalnızca güvenli bir şekilde denetlenen kullanıcılarla sınırlayarak, kötüye kullanım ve yanlış erişim risklerini azaltır. Yedekleme işlemleri, verilerin geri alınabilirliğini sağlamak için hayati öneme sahiptir ve bu yüzden yalnızca yüksek düzeyde erişim iznine sahip kullanıcılar tarafından yapılmalıdır. Bu ayarın doğru yapılandırılması veri kaybını önlemeye ve sistemin güvenliğini sağlamaya yardımcı olur.

Bu güvenlik ayarı, kullanıcıların dosya ve dizinlerin yedeğini alırken, dosya ve dizin izinlerini geçersiz kılmalarına olanak tanır. Yedekleme işlemi, genellikle NTBACKUP gibi bir uygulama aracılığıyla yapılır ve yalnızca bu tür uygulamalar NTFS dosya sistemi yedekleme API'si aracılığıyla erişim sağladığında bu hak etkinleşir. Aksi takdirde dosya ve dizin izinleri uygulanır. Bu güvenlik politikası, Yöneticiler (Administrators) grubunu içererek yedekleme işlemlerini yalnızca yönetici seviyesindeki kullanıcıların gerçekleştirmesini sağlar. Bu ayarın önerilen durumu Yöneticiler (Administrators) grubunu belirtmektir.

Yedekleme işlemleri sırasında bu hakka sahip kullanıcılar, yedekleme medyasını başka bir bilgisayara alabilir ve buradan yedekleri geri yükleyerek veriler üzerinde değişiklik yapabilir veya şifrelenmemiş verileri görüntüleyebilir. Bu durumda verilerin gizliliği ve bütünlüğü için potansiyel bir güvenlik riski oluşabilir. Yedekleme yetkisi, aynı zamanda dosya ve dizinler üzerinde uygulanan diğer güvenlik önlemlerini aşabilen bir hakka sahip kullanıcılar tarafından kötüye kullanılabilir.

Yedekleme işlemlerini yalnızca yetkilendirilmiş yönetici kullanıcılarının gerçekleştirmesi gerektiği için bu ayarın doğru yapılandırılması önemlidir. Yedekleme yetkisinin, yanlış kişilerin eline geçmemesi için sadece Yöneticiler (Administrators) grubuyla sınırlaması, organizasyonel güvenliği artıracaktır. Bu ayarın uygulanması, yedekleme yöneticilerinin gerekli izinlere sahip olduğundan emin olunarak yapılmalıdır. Aksi takdirde yedekleme işlemleri gerçekleştirilmediği için veri kaybı yaşanabilir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, Windows işletim sisteminde “SeBackupPrivilege” (Dosya ve dizinleri yedekleme) kullanıcısı için gerekli güvenlik yapılandırmasını kontrol eder ve günceller. Bu politika, yalnızca yetkilendirilmiş kullanıcıların kritik dosya ve dizinlerin yedeklemesini yapabilmesi için gereklidir ve genellikle yalnızca Yöneticiler (Administrators) grubuna atanmalıdır. Script, önce mevcut kullanıcı haklarını dışa aktarır ve ardından “SeBackupPrivilege” politikasının mevcut değerini kontrol eder. Eğer bu politika zaten mevcutsa, önerilen değer (Yöneticiler SID’i) ile güncellenir eğer yoksa, yapılandırmaya yeni bir satır eklenir. Yapılandırmadaki değişiklikler, “secedit” komutuyla uygulanır ve son olarak geçici dosyalar silinir. Bu işlem, yalnızca güvenli ve yetkilendirilmiş kullanıcıların dosya ve dizinlerin yedeğini almasını ve veri kaybını engellemek için kritik güvenlik önlemleri uygulanmasını sağlar.

```
1. $MetodArgumani = 'SeBackupPrivilege'  # Yedekleme yetkisi
2. $onerilenDegerler = @(
3.     '*S-1-5-32-544'  # Yöneticiler SID'i
4. )
5. $SecEditYolu = 'C:\Windows\System32\secedit.exe'  # Güvenlik yapılandırma aracı
6.
7. # Benzersiz dosya adı oluştur
8. $benzersiz = (Get-Date).ToString("yyyyMMddHHmmssfff")  # Benzersiz tarih ve saat
formatında dosya adı
9. $secedit = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Geçici yapılandırma dosyasının
yolu
10.
11. # Kullanıcı haklarını dışa aktar
```

```
&$SecEditYolu /export /areas USER_RIGHTS /cfg $secedit /quiet

# Yapılandırma dosyasını al
$config = Get-Content -Path $secedit

# Tavsiye edilen SID'leri birleştir
$onerilenDeger = ""
for ($i = 0 ; $i -lt $onerilenDegerler.Count; $i++) {
    if ($i -eq $onerilenDegerler.Count - 1) {
        $onerilenDeger += $onerilenDegerler[$i]
    }
    else {
        $onerilenDeger += $onerilenDegerler[$i] + ','  # SID'leri virgülle ayır
    }
}

# Eğer parametre zaten mevcutsa, değerleri güncelle
if (get-content $secedit | Select-String -Pattern $MetodArgumani) {
    $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
    $config | Set-Content -Path $secedit
}
else {
    # Eğer parametre yoksa, [Privilege Rights] bölümüne ekle
    $yeniConfig = @()
    $indeks = $config.IndexOf("[Privilege Rights]") + 1
    $satirEkle = "$MetodArgumani=$onerilenDeger"
    foreach ($satir in $config) {
        $yeniConfig += $satir
        if ($config.IndexOf($satir) -eq $indeks) {
            $yeniConfig += $satirEkle  # Yeni satırı ekle
        }
    }
    $yeniConfig | Set-Content -Path $secedit
}

# Yapılandırmayı uygula
&$SecEditYolu /configure /db secedit.sdb /cfg $secedit

# Geçici dosyayı sil
Remove-Item -Path $secedit -Force

# Konfigürasyonun doğru yapıldığını kontrol et
$sonConfig = & $SecEditYolu /export /areas USER_RIGHTS /cfg
$Env:Temp\final_secedit.cfg /quiet
$sonConfigIcerik = Get-Content -Path $Env:Temp\final_secedit.cfg

# Tavsiye edilen değeri içerip içermediğini kontrol et
if ($sonConfigIcerik -match $MetodArgumani) {
    $mevcutDeger = ((Select-String -Pattern $MetodArgumani -Path
$Env:Temp\final_secedit.cfg) -Split '=')[1].Trim()
    if ($mevcutDeger -eq $onerilenDeger) {
        Write-Output "Script sonucu: [GECTI]"  # Yapılandırma başarılı
    }
    else {
        Write-Output "Script sonucu: [BASARISIZ] - Mevcut değer tavsiye edilen değerle
eşleşmiyor"  # Değer eşleşmiyor
    }
} else {
    Write-Output "Script sonucu: [BASARISIZ] - $MetodArgumani yapılandırmada
bulunamadı"  # Parametre bulunamadı
}

# Geçici dosyayı temizle
Remove-Item -Path $Env:Temp\final_secedit.cfg -Force
```

4.1.1.8. Sistem Saatini Değiştirme Yapılandırılması

Sistem saatinin değiştirilmesi, güvenlik açısından önemlidir çünkü kötü niyetli kullanıcılar saat ayarlarını değiştirerek etkinliklerin zaman damgasını değiştirebilir. Bu durum özellikle Kerberos kimlik doğrulama protokolünü olumsuz etkileyebilir. Bu yetkinin yalnızca Yöneticiler (Administrators) ve LOCAL SERVICE gibi gruplara verilmesi önerilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.8 maddesi tedbirine göre yapılan testlerde uygun olarak, sistem saatini değiştirme yetkisi yalnızca Yöneticiler (Administrators) ve LOCAL SERVICE gruplarına verildiğinden herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle sistemde zaten uygun yapılandırma sağlandığından, iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.9. Zaman Dilimini Değiştirme Yapılandırılması

Zaman diliminin değiştirilmesi, genellikle güvenlik açısından kritik bir tehdit oluşturmaz. Ancak sistemdeki zaman dilimi ayarlarının yanlış olması, kullanıcının doğru zaman diliminde çalışmamasına yol açabilir. Yöneticiler (Administrators), LOCALSERVICE ve Kullanıcılar (Users) gibi gruplara bu yetkinin verilmesi uygundur.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.9 maddesi tedbiri yapılanmasında, zaman dilimi değiştirme yetkisinin Yöneticiler (Administrators), LOCAL SERVICE ve Kullanıcılar (Users) gruplarına verildiği için sistemde herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle zaman dilimini değiştirme yetkisi doğru şekilde yapılandırıldığından, iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.10. Sayfa Dosyası Oluşturma Yapılandırılması

Sayfa dosyası oluşturma yetkisi, yalnızca Yöneticiler (Administrators) grubuna verilmelidir. Bu yetki, kötüye kullanıldığında sistemin performansını olumsuz etkileyebilir. Bu nedenle yalnızca güvenilir kullanıcıların ve grupların bu yetkiye sahip olması önerilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.10 maddesi tedbirinde yapılan testlerde, sayfa dosyasını oluşturma yetkisi yalnızca Yöneticiler (Administrators) grubuna verildiğinden, sistemde herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle sayfa dosyasının oluşturulmasına yönelik yapılandırma doğru şekilde yapılmış olduğundan tedbir için iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.11. Bir Erişim Tokeni Oluşturma Sıkılaştırması

Erişim tokeni oluşturma yetkisi, yalnızca Hiç Kimse (No One) grubuna verilmelidir. Bu yetki kötüye kullanıldığında ciddi güvenlik tehditlerine yol açabilir. Bu sebep ile bu yetkinin devre dışı bırakılması önemlidir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.11 maddesi tedbirinde yapılan testlerde, bu yetkinin Hiç Kimse (No One) grubuna verildiği sistemlerde herhangi bir güvenlik ihlali gözlemlenmemiştir. Erişim tokeni oluşturma yetkisi doğru şekilde yapılandırıldığı için iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.12. Küresel Nesneler Oluşturma Yapılandırılması

Küresel nesneler oluşturma yetkisi, yalnızca Yöneticiler (Administrators), LOCAL SERVICE, NETWORK SERVICE ve SERVICE gruplarına verilmelidir. Bu yetki, kötüye kullanıldığında sistemde sorunlara yol açabilir ve veri bozulmasına neden olabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.12 maddesi tedbirinde yapılan testlerde, küresel nesneler oluşturma yetkisinin yalnızca Yöneticiler (Administrators), LOCAL SERVICE, NETWORK SERVICE ve SERVICE gruplarına verildiği görülmüş olup sistemlerde güvenlik ihlali tespit edilmemiştir. Bu tedbirde küresel nesneler oluşturma yetkisi için iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.13. Kalıcı Paylaşılan Nesneler Oluşturma Kuralları

Kalıcı paylaşılan nesneler oluşturma yetkisi, Hiç Kimse (No One) grubuna verilmelidir. Bu yetki kötüye kullanıldığında sistemde önemli güvenlik açıklarına yol açabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.13 maddesi tedbirinde yapılan testlerde, bu yetkinin Hiç Kimse (No One) grubuna verildiği görülmüş ve sistemlerde herhangi bir güvenlik ihlali gözlemlenmemiştir.

Bu nedenle, kalıcı paylaşılan nesneler oluşturma yetkisi doğru şekilde yapılandırıldığından, iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.14. Sembolik Bağlantılar Oluşturma Yapılandırılması

Sembolik bağlantılar oluşturma yetkisi, yalnızca Yöneticiler (Administrators) ve NT VIRTUAL MACHINE\Virtual Machines gruplarına verilmelidir. Bu yetkide kötüye kullanıldığında ciddi güvenlik risklerine yol açabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.14 maddesi tedbirinde yapılan testlerde, sembolik bağlantılar oluşturma yetkisinin yalnızca Yöneticiler (Administrators) ve NT VIRTUAL MACHINE\Virtual Machines gruplarına verildiği için sistemlerde herhangi bir güvenlik ihlali tespit edilmemiştir. Sembolik bağlantılar oluşturma yetkisi doğru şekilde yapılandırıldığından iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.15. Hata Ayıklama Yapılandırılması

Programların hata ayıklama yetkisi yalnızca Yöneticiler (Administrators) grubuna verilmelidir. Bu yetki kötüye kullanıldığında sistemin kritik bileşenlerine erişim sağlanarak ve bunlardan bilgi edinerek ciddi güvenlik açıklarına yol açabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.15 maddesi tedbirinde yapılan testlerde, hata ayıklama yetkisinin yalnızca Yöneticiler (Administrators) grubuna verildiğinden sistemlerde herhangi bir güvenlik ihlali tespit

edilmemiştir. Bu nedenle, hata ayıklama yetkisi doğru şekilde yapılandırıldığından iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.16. Ağdan Bilgisayara Erişimi Reddetme Yapılandırılması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.16 maddesi tedbirindeki bu güvenlik ayarı, kullanıcıların ağ üzerinden bilgisayara bağlanmalarını engeller. Ağ üzerinden bağlanma izni verilen kullanıcılar, sistem kaynaklarına erişip verileri değiştirme veya okuma gibi işlemler yapabilir. Yüksek güvenlikli ortamlarda, uzaktaki kullanıcıların bilgisayarlara bağlanarak veri erişimini sağlamaları genellikle gereksizdir. Bunun yerine dosya paylaşımı ağ sunucuları üzerinden yapılmalıdır. Ağ üzerinden bu bilgisayara erişim hakkını, ağ üzerinden bu bilgisayara erişimi reddet hakkını geçersiz kılar.

Bu ayarın önerilen durumu, Misafirler ve Yerel Hesap gruplarını dahil etmek olacaktır. Bu yapılandırma yalnızca yerel bilgisayar üzerinde oturum açma yetkisi olan kişilerin ağ üzerinden erişim sağlamasına izin verir ve dışarıdan gelen bağlantılar engellenir. Bu ayarın, bağımsız (domain'e bağlı olmayan) bir iş istasyonu üzerinde uygulanması, uzaktan yönetim işlemlerinin yapılamaması gibi sorunlara yol açabilir.

Ağ üzerinden bağlanma iznine sahip hesaplar, kullanıcı adı, grup adı ve paylaşılan kaynakların listesini sorgulayabilirler. Ağ üzerinden paylaşılan dosyalar veya klasörler erişilebilir hale gelir ve bu kullanıcılar verileri görüntüleyebilir veya değiştirebilirler.

Bu ayarın uygulanmasıyla ağ üzerinden erişimi engelleyerek, yalnızca yerel kullanıcılara erişim izni verir ve böylece kötü niyetli kullanıcıların sistem kaynaklarına erişmesini zorlaştırır. Ağ üzerinden bu bilgisayara erişimi reddet hakkı, diğer hesaplara uygulanırsa, yönetimsel haklara sahip kullanıcıların görevlerini yerine getirememesi gibi olumsuz etkilerle karşılanır. Bu yüzden sıkılaştırma ayarının uygulanacağı kullanıcı hesaplarının belirlenmesi önemlidir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, ağ üzerinden bilgisayara erişimi reddetmek için "SeDenyServiceLogonRight" güvenlik ayarını

yapılandırır. CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.16 tedbirine göre, ağ üzerinden bilgisayara bağlanma izninin yalnızca yerel kullanıcılarla sınırlı olması gerektiği belirtilir. Bu script, yalnızca Misafirler ve Yerel Hesap gruplarının ağ üzerinden erişim izni almasını sağlar ve dışarıdan gelen bağlantıları engeller.

Script, önce mevcut yapılandırmayı dışa aktarır, sonra bu parametrenin mevcut olup olmadığını kontrol eder. Eğer "SeDenyServiceLogonRight" parametresi zaten mevcutsa, script mevcut değeri tavsiye edilen değerle değiştirir. Eğer parametre yoksa, "Privilege Rights" bölümüne yeni bir satır ekler. Yapılandırma güncellemesi tamamlandıktan sonra, değişiklikler "secedit" komutu ile uygulanır ve geçici dosya silinir. Bu yapılandırma, yalnızca yerel kullanıcıların ağ üzerinden bilgisayara erişmesini sağlayarak kötü niyetli kullanıcıların sisteme erişmesini engeller.

```
1. $MetodArgumani = 'SeDenyServiceLogonRight'  # Hizmet girişi engelleme hakkı
2. $onerilenDegerler = @(
3.     '*S-1-5-32-546'  # Kullanıcı grubu SID (Hizmet Girişi engelleme hakkı)
4. )
5. $sids = @()  # SID'leri tutacak dizi
6. $onerilenDeger = ''  # SID'lerin birleştirileceği değişken
7. $SecEditYolu = 'C:\Windows\System32\secedit.exe'  # Güvenlik yapılandırması aracı
8. $benzersiz = (Get-Date).ToString("yyyyMMddHHmmssffff")  # Benzersiz dosya adı oluşturma
9. $secedit = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Geçici yapılandırma dosyası
10.
11. # Kullanıcı haklarını dışa aktar
12. &$SecEditYolu /export /areas USER_RIGHTS /cfg $secedit /quiet
13.
14. # Yapılandırma dosyasını oku
15. $config = Get-Content -Path $secedit
16.
17. # Tavsiye edilen SID'leri birleştir
18. for ($i = 0 ; $i -lt $onerilenDegerler.Count; $i++) {
19.     if ($i -eq $onerilenDegerler.count - 1) {
20.         $onerilenDeger += $onerilenDegerler[$i]  # Son değeri ekle
21.     }
22.     else {
23.         $onerilenDeger += $onerilenDegerler[$i] + ','  # SID'leri virgülle ayırarak
ekle
24.     }
25. }
26.
27. # Eğer parametre zaten mevcutsa, değerleri güncelle
28. if (get-content $secedit | Select-String -Pattern $MetodArgumani) {
29.     # Mevcut değeri tavsiye edilen değerle değiştir
30.     $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
31.     $config | Set-Content -Path $secedit  # Değişiklikleri dosyaya yaz
32. } else {
33.     # Parametre mevcut değilse, [Privilege Rights] bölümüne ekle
34.     $yeniConfig = @()  # Yeni konfigürasyon dizisi
35.     $indeks = $config.IndexOf("[Privilege Rights]") + 1  # [Privilege Rights]
satırının bir altındaki satırın indexi
36.     $satirEkle = "$MetodArgumani=$onerilenDeger"  # Eklemek için yeni satır
37.
38.     foreach ($satir in $config) {
39.         $yeniConfig += $satir  # Mevcut satırları yeni diziye ekle
```

```
40.         if ($config.IndexOf($satir) -eq $indeks) {
41.             $yeniConfig += $satirEkle  # Parametreyi ekle
42.         }
43.     }
44.     $yeniConfig | Set-Content -Path $secedit  # Yeni düzenlemeleri dosyaya yaz
45. }
46.
47. # Yapılandırmayı uygula
48. &$SecEditYolu /configure /db secedit.sdb /cfg $secedit
49.
50. # Geçici dosyayı sil
51. Remove-Item -Path $secedit -Force
```

4.1.1.17. Toplu İşlem Olarak Giriş Yapmayı Reddet Ayarının Yapılandırılması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.17 maddesi tedbirindeki bu güvenlik ayarı, hangi hesapların bilgisayara toplu işlem olarak giriş yapmalarını engelleyeceğini belirler. Burada toplu işlem, bir batch (.bat) dosyası değil, toplu işlem kuyruğu anlamına gelir. Görev zamanlayıcısı kullanarak işler planlayan hesaplar, bu kullanıcı hakkına sahip olmalıdır.

Bu ayarın önerilen durumu, Misafirler grubunu içerecek şekilde yapılandırılmalıdır. Bu şekilde yalnızca yetkilendirilmiş kullanıcıların toplu işlem olarak giriş yapmalarına izin verilir ve izinsiz kullanıcıların bu işlemleri gerçekleştirmesi engellenir. Toplu işlem olarak giriş yapma hakkına sahip bir hesap, bilgisayar kaynaklarını aşırı derecede tüketebilecek ve DoS (Denial of Service) durumuna neden olabilecektir.

Bu ayar misafirler grubunun dışındaki belirli hesaplar için de geçerli olabilir. Ancak bu ayarın yanlış yapılandırılması, yönetici rolleriyle ilişkili kullanıcıların görevlerini yerine getirmelerini engelleyebilir. Örneğin, IWAM_(BilgisayarAdı) hesabına toplu işlem olarak giriş yapmayı reddet hakkı verilirse, MSM Yönetim Noktası çalışmayı durdurabilir. Bu nedenle hangi hesapların hangi gruplara ait olduğunu ve toplu işlem olarak giriş yapmayı reddet hakkının hangi hesaplara atanacağını dikkatle belirlemek önemlidir.

Eğer bu kullanıcı hakkı, bazı ilgisiz hesaplara atanırsa, bu hesapların planladığı görevler çalışamayabilir ve bu da sistemin işleyişini etkileyebilir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, Windows bilgisayarlarında “Toplu İşlem Olarak Giriş Yapmayı Reddet” güvenlik ayarını yapılandırmak için kullanılır. Bu ayar, hangi kullanıcıların toplu işlem (batch logon) olarak sisteme giriş yapamayacağını belirler. Script, öncelikle bilgisayarın mevcut güvenlik yapılandırmasını dışa aktarır, ardından Misafirler grubunun SID’ini (S-1-5-32-546) bu ayara dahil eder ve eğer gerekli yapılandırma zaten mevcutsa, mevcut değeri günceller eğer mevcut değilse, yeni bir satır ekler. Sonrasında, yapılan değişiklikleri uygulamak için güvenlik yapılandırma aracını (secedit.exe) kullanarak yapılandırmayı uygular. Bu süreç, toplu işlem olarak giriş yapmak isteyen yalnızca yetkilendirilmiş kullanıcıların sisteme erişebilmesini sağlarken, izinsiz erişimlerin engellenmesine yardımcı olur.

```
$MetodArgumani = 'SeDenyBatchLogonRight'  # Toplu giriş engelleme hakkı
$onerilenDegerler = @(
    '*S-1-5-32-546'  # Kullanıcı grubu SID (Batch Logon engelleme hakkı)
)
$sidler = @()
$onerilenDeger = ''
$SecEditYolu = 'C:\Windows\System32\secedit.exe'  # Güvenlik yapılandırması aracı
$benzersiz = (Get-Date).ToString("yyyyMMddHHmmssfff")  # Benzersiz dosya adı oluşturma
$secedit = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Geçici yapılandırma dosyası

# Kullanıcı haklarını dışa aktar
&$SecEditYolu /export /areas USER_RIGHTS /cfg $secedit /quiet

# Yapılandırma dosyasını oku
$config = Get-Content -Path $secedit

# Tavsiye edilen SID'leri birleştir
for ($i = 0 ; $i -lt $onerilenDegerler.Count; $i++) {
    if ($i -eq $onerilenDegerler.Count - 1) {
        $onerilenDeger += $onerilenDegerler[$i]
    }
    else {
        $onerilenDeger += $onerilenDegerler[$i] + ','  # SID'leri virgülle ayır
    }
}

# Eğer parametre zaten mevcutsa, değerleri güncelle
if (get-content $secedit | Select-String -Pattern $MetodArgumani) {
    # Mevcut değeri tavsiye edilen değerle değiştir
    $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
    $config | Set-Content -Path $secedit
} else {
    # Parametre mevcut değilse, [Privilege Rights] bölümüne ekle
    $yeniConfig = @()
    $indeks = $config.IndexOf("[Privilege Rights]") + 1
    $satirEkle = "$MetodArgumani=$onerilenDeger"
    foreach ($satir in $config) {
        $yeniConfig += $satir
        if ($config.IndexOf($satir) -eq $indeks) {
            $yeniConfig += $satirEkle  # Yeni satırı ekle
        }
    }
    $yeniConfig | Set-Content -Path $secedit
```

```
44. }
45.
46. # Yapılandırmayı uygula
47. &$SecEditYolu /configure /db secedit.sdb /cfg $secedit
48.
49. # Geçici dosyayı sil
50. Remove-Item -Path $secedit -Force
```

4.1.1.18. Hizmet Olarak Giriş Yapmayı Reddet Ayarının Yapılandırılması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.18 maddesi tedbirindeki güvenlik ayarı, hizmet hesaplarının bir işlem kaydederek hizmet olarak başlatılmalarını engeller. Eğer bir hesap her iki politikaya da tabiyse, hizmet olarak giriş yapmaya izin ver politikasının yerine hizmet olarak giriş yapmayı reddet politikası geçer. Bu ayarın amacı, sistemin güvenliğini artırmak ve kötü amaçlı yazılımların sistemde hizmet olarak çalışmasını engellemektir. Misafir hesaplarının hizmet olarak giriş yapmalarını engellemek, kötü amaçlı yazılımların bu yöntemle başlatılmasını zorlaştırır.

Bu ayar için önerilen durum, Misafirler grubunu içerecek şekilde yapılandırılmasıdır. Yalnızca yetkili kullanıcıların hizmet olarak giriş yapabilmesi sağlanmalı ve izinsiz kişilerin bu tür işlemleri yapması engellenmelidir.

Bu güvenlik ayarı Sistem, Yerel Hizmet ve Ağ Hizmeti hesapları için geçerli değildir. Bu nedenle belirtilen hesaplar her durumda hizmet olarak giriş yapmaya devam edebilir. Hizmet olarak giriş yapma hakkına sahip bir hesap, kötü niyetli bir yazılımın veya kötü amaçlı bir kullanıcının, hizmet olarak başlatılmasını sağlayabileceği yeni hizmetler oluşturmasına olanak tanıyabilir. Bu sebeple yalnızca yönetici ayrıcalıklarına sahip kullanıcılar yeni hizmetleri yapılandırabilir ve başlatabilir.

Eğer hizmet olarak giriş yapmayı reddet hakkı belirli hesaplara atanırsa, bazı hizmetlerin başlatılamaması riski vardır. Bu durumda bazı hizmetlerin düzgün çalışmamasına ve bu da servis kesintilerine yol açarak DoS (Denial of Service) durumuna neden olabilir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, “Hizmet Olarak Giriş Yapmayı Reddet” güvenlik ayarını yapılandırmak için kullanılmaktadır. Bu ayar,

sistemde yalnızca yetkilendirilmiş kullanıcıların hizmet olarak giriş yapmasına izin verir ve izinsiz girişleri engeller. Script, önce mevcut güvenlik yapılandırmalarını dışa aktarır, ardından önerilen 'Users' SID değerini ekler. Eğer parametre zaten mevcutsa, mevcut değer güncellenir. Parametre mevcut değilse, "Privilege Rights" bölümüne yeni bir satır olarak eklenir. Yapılandırma dosyasındaki değişiklikler uygulandıktan sonra, geçici dosya silinir. Bu ayar, hizmet olarak giriş yapma hakkına sahip kötü niyetli yazılımların sistemde çalışmasını engelleyerek, güvenliği artırmaya yardımcı olur.

```
1. $MetodArgumani = 'SeDenyInteractiveLogonRight'  # Etkileşimli oturum açma engelleme
hakkı
2. $onerilenDegerler = @(
3.     '*S-1-5-32-546'  # Tavsiye edilen değer: 'Users' SID
4. )
5. $sids = @()  # SID'ler için liste (boş)
6. $onerilenDeger = ''  # Tavsiye edilen değer
7. $SecEditYolu = 'C:\Windows\System32\secedit.exe'  # Güvenlik yapılandırma aracı
8. $benzersiz = (Get-Date).ToString("yyyyMMddHHmmssfff")  # Benzersiz dosya adı oluşturma
9. $secedit = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Geçici yapılandırma dosyası
10.
11. # Kullanıcı haklarını dışa aktar
12. &$SecEditYolu /export /areas USER_RIGHTS /cfg $secedit /quiet
13.
14. # Yapılandırma dosyasını oku
15. $config = Get-Content -Path $secedit
16.
17. # Tavsiye edilen SID'leri birleştir
18. for ($i = 0 ; $i -lt $onerilenDegerler.Count; $i++) {
19.     if ($i -eq $onerilenDegerler.count - 1) {
20.         $onerilenDeger += $onerilenDegerler[$i]  # Son değeri ekle
21.     }
22.     else {
23.         $onerilenDeger += $onerilenDegerler[$i] + ','  # SID'leri virgülle ayırarak
ekle
24.     }
25. }
26.
27. # Eğer parametre zaten mevcutsa, değerleri güncelle
28. if (get-content $secedit | Select-String -Pattern $MetodArgumani) {
29.     # Mevcut değeri tavsiye edilen değerle değiştir
30.     $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
31.     $config | Set-Content -Path $secedit  # Değişiklikleri dosyaya yaz
32. } else {
33.     # Parametre mevcut değilse, [Privilege Rights] bölümüne ekle
34.     $yeniConfig = @()  # Yeni konfigürasyon dizisi
35.     $indeks = $config.IndexOf("[Privilege Rights]") + 1  # [Privilege Rights]
satırının bir altındaki satırın indexi
36.     $satirEkle = "$MetodArgumani=$onerilenDeger"  # Eklemek için yeni satır
37.
38.     foreach ($satir in $config) {
39.         $yeniConfig += $satir  # Mevcut satırları yeni diziye ekle
40.         if ($config.IndexOf($satir) -eq $indeks) {
41.             $yeniConfig += $satirEkle  # Parametreyi ekle
42.         }
43.     }
44.     $yeniConfig | Set-Content -Path $secedit  # Yeni düzenlemeleri dosyaya yaz
45. }
46.
47. # Yapılandırmayı uygula
48. &$SecEditYolu /configure /db secedit.sdb /cfg $secedit
49.
```

```
# Geçici dosyayı sil
Remove-Item -Path $secedit –Force
```

4.1.1.19. Yerel Olarak Giriş Yapmayı Reddet Ayarının Yapılandırılması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.19 maddesi tedbirindeki güvenlik ayarı, hangi kullanıcıların bilgisayara yerel olarak giriş yapamayacağını belirler. Bu politika ayarı bir hesap her iki politikaya da tabiyse, Yerel olarak giriş yapmaya izin ver politikası ayarını geçersiz kılar.

Önerilen durum, Misafirler grubunun bu hakka dahil edilmesidir. Misafir hesaplarının yerel olarak sisteme giriş yapmalarını engelleyerek, yetkisiz erişimi kısıtlar. Bu güvenlik ayarının Herkes grubuna uygulanması, yerel giriş yapacak kimsenin kalmamasına yol açar. Yerel olarak giriş yapma yetkisi olan her hesap, bilgisayara doğrudan konsoldan giriş yaparak kötü amaçlı yazılım yükleyebilir veya sistemdeki ayrıcalıkları yükseltebilir. Bu nedenle yerel girişin yalnızca yetkili kullanıcılarla sınırlı olması önemlidir.

Bu ayarın yapılandırılması sırasında, misafir hesapları yerel erişimden dışlanmalıdır. Ayrıca servislerden IIS 6.0 çalışan bilgisayarlarda, ASPNET hesabına bu hakkın verilmediğinden emin olunmalıdır.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, “Yerel Olarak Giriş Yapmayı Reddet” güvenlik ayarını yapılandırmak amacıyla kullanılır. Script, bilgisayara yerel giriş yapması gereken kullanıcıları belirler ve yetkisiz girişleri engeller. İlk olarak, mevcut güvenlik yapılandırmalarını dışa aktarır ve ardından, Misafir grubunu ve diğer belirli kullanıcıları (örneğin, ‘Users’ SID) bu politika kapsamında tanımlar. Eğer belirtilen parametreler mevcutsa, mevcut değer güncellenir. Aksi takdirde, yeni bir satır eklenir. Yapılandırma başarıyla uygulandıktan sonra, geçici dosya silinir. Bu güvenlik ayarının amacı, sistemin yerel erişimini yalnızca yetkilendirilmiş kullanıcılarla sınırlandırarak, kötü amaçlı yazılımların yerel giriş yapmasını engellemektir.

```
$MetodArgumani = 'SeDenyInteractiveLogonRight'  # Etkileşimli oturum açma engelleme hakkı
$onerilenDegerler = @(
```

```
3.      '*S-1-5-32-546'  # Tavsiye edilen değer: 'Users' SID
4. )
5. $sids = @()  # SID'ler için liste (boş)
6. $onerilenDeger = ''  # Tavsiye edilen değer
7. $SecEditYolu = 'C:\Windows\System32\secedit.exe'  # Güvenlik yapılandırma aracı
8. $benzersiz = (Get-Date).ToString("yyyyMMddHHmmssffff")  # Benzersiz dosya adı oluşturma
9. $secedit = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Geçici yapılandırma dosyası
10.
11. # Kullanıcı haklarını dışa aktar
12. &$SecEditYolu /export /areas USER_RIGHTS /cfg $secedit /quiet
13.
14. # Yapılandırma dosyasını oku
15. $config = Get-Content -Path $secedit
16.
17. # Tavsiye edilen SID'leri birleştir
18. for ($i = 0 ; $i -lt $onerilenDegerler.Count; $i++) {
19.     if ($i -eq $onerilenDegerler.count - 1) {
20.         $onerilenDeger += $onerilenDegerler[$i]  # Son değeri ekle
21.     }
22.     else {
23.         $onerilenDeger += $onerilenDegerler[$i] + ','  # SID'leri virgülle ayırarak
ekle
24.     }
25. }
26.
27. # Eğer parametre zaten mevcutsa, değerleri güncelle
28. if (get-content $secedit | Select-String -Pattern $MetodArgumani) {
29.     # Mevcut değeri tavsiye edilen değerle değiştir
30.     $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
31.     $config | Set-Content -Path $secedit  # Değişiklikleri dosyaya yaz
32. } else {
33.     # Parametre mevcut değilse, [Privilege Rights] bölümüne ekle
34.     $yeniConfig = @()  # Yeni konfigürasyon dizisi
35.     $indeks = $config.IndexOf("[Privilege Rights]") + 1  # [Privilege Rights]
satırının bir altındaki satırın indexi
36.     $satirEkle = "$MetodArgumani=$onerilenDeger"  # Eklemek için yeni satır
37.
38.     foreach ($satir in $config) {
39.         $yeniConfig += $satir  # Mevcut satırları yeni diziye ekle
40.         if ($config.IndexOf($satir) -eq $indeks) {
41.             $yeniConfig += $satirEkle  # Parametreyi ekle
42.         }
43.     }
44.     $yeniConfig | Set-Content -Path $secedit  # Yeni düzenlemeleri dosyaya yaz
45. }
46.
47. # Yapılandırmayı uygula
48. &$SecEditYolu /configure /db secedit.sdb /cfg $secedit
49.
50. # Geçici dosyayı sil
51. Remove-Item -Path $secedit -Force
```

4.1.1.20. Uzaktan Masaüstü Servisleri Üzerinden Giriş Yapmayı Reddet Ayarının Yapılandırılması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.20 maddesi tedbirindeki politika ayarı, kullanıcıların Uzaktan Masaüstü Servisleri (Remote Desktop Services) üzerinden oturum açmalarına izin verilip verilmediğini belirler. Bir bilgisayar, bir etki alanına katıldıktan sonra, yerel hesaplarla ağ üzerinden çalıştırılmasına gerek

yoktur. Yönetim ve son kullanıcı işlemleri için etki alanı hesapları kullanılabilir. Bu kullanıcı hakkı, bir hesap her iki politikaya da tabiyse, Uzaktan Masaüstü Servisleri üzerinden giriş yapmaya izin veren kullanıcı hakkını geçersiz kılar.

Eğer bir kullanıcı, Uzaktan Masaüstü Servisleri üzerinden giriş yapma yetkisine sahipse, bu hak ile bilgisayarın uzaktan konsoluna erişim sağlamak için kullanılabilir. Eğer bu kullanıcı hakkı, yalnızca uzaktan konsola erişmeye ihtiyaç duyan yetkili kullanıcılarla sınırlanmazsa, yetkisiz kullanıcılar kötü amaçlı yazılım indirip çalıştırarak yetkilerini artırabilir. Bu ayarın doğru şekilde yapılandırılması için Misafirler ve Yerel Hesaplar gruplarına bu hakkı reddetme yetkisi verilmelidir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "Uzaktan Masaüstü Servisleri Üzerinden Giriş Yapmayı Reddet" güvenlik ayarını yapılandırmak için kullanılır. Script, bilgisayarların uzaktan masaüstü üzerinden yetkisiz kullanıcıların erişimini engellemeyi amaçlar. Başlangıçta, mevcut güvenlik yapılandırması dışa aktarılır ve ardından, Misafirler ve Yerel Hesaplar gibi gruplar için uzaktan giriş hakkı reddedilir. Eğer parametre mevcutsa değerler güncellenir. Parametre yoksa, yeni parametreler eklenir. Bu yapılandırma, sadece yetkili kullanıcıların uzaktan masaüstü erişimi sağladığı, yetkisiz girişlerin engellendiği bir ortam oluşturur. Son olarak, geçici dosya silinir ve yapılan değişiklikler etkinleştirilir. Bu güvenlik önlemi, kötü amaçlı yazılımların uzaktan sistem erişimi sağlama çabalarını engeller.

```
1. $MetodArgumani = 'SeDenyRemoteInteractiveLogonRight'  # Uzaktan etkileşimli oturum açma
engelleme hakkı
2. $onerilenDegerler = @(
3.     '*S-1-5-32-546',  # Tavsiye edilen değer: 'Users' SID
4.     '*S-1-5-113'  # Tavsiye edilen değer: 'Enterprise Domain Controllers' SID
5. )
6. $sids = @()  # SID'ler için liste (boş)
7. $onerilenDeger = ''  # Tavsiye edilen değer
8. $SecEditYolu = 'C:\Windows\System32\secedit.exe'  # Güvenlik yapılandırma aracı
9. $benzersiz = (Get-Date).ToString("yyyyMMddHHmmssffff")  # Benzersiz dosya adı oluşturma
10. $secedit = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Geçici yapılandırma dosyası
11.
12. # Kullanıcı haklarını dışa aktar
13. &$SecEditYolu /export /areas USER_RIGHTS /cfg $secedit /quiet
14.
15. # Yapılandırma dosyasını oku
16. $config = Get-Content -Path $secedit
17.
18. # Tavsiye edilen SID'leri birleştir
19. for ($i = 0 ; $i -lt $onerilenDegerler.Count; $i++) {
20.     if ($i -eq $onerilenDegerler.count - 1) {
21.         $onerilenDeger += $onerilenDegerler[$i]
22.     }
23.     else {
24.         $onerilenDeger += $onerilenDegerler[$i] + ','  # SID'leri virgülle ayır
```

```
25.     }
26. }
27.
28. # Eğer parametre zaten mevcutsa, değerleri güncelle
29. if (get-content $secedit | Select-String -Pattern $MetodArgumani) {
30.     # Mevcut değeri tavsiye edilen değerle değiştir
31.     $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
32.     $config | Set-Content -Path $secedit
33. } else {
34.     # Parametre mevcut değilse, [Privilege Rights] bölümüne ekle
35.     $yeniConfig = @()
36.     $indeks = $config.IndexOf("[Privilege Rights]") + 1
37.     $satirEkle = "$MetodArgumani=$onerilenDeger"
38.     foreach ($satir in $config) {
39.         $yeniConfig += $satir
40.         if ($config.IndexOf($satir) -eq $indeks) {
41.             $yeniConfig += $satirEkle  # Yeni satırı ekle
42.         }
43.     }
44.     $yeniConfig | Set-Content -Path $secedit
45. }
46.
47. # Yapılandırmayı uygula
48. &$SecEditYolu /configure /db secedit.sdb /cfg $secedit
49.
50. # Geçici dosyayı sil
51. Remove-Item -Path $secedit -Force
```

4.1.1.21. Uzaktan Sistemi Kapatmaya Zorla Yapılandırılması

Bu politika, kullanıcıların Windows Vista ve sonraki sürümlerdeki bilgisayarları ağ üzerinden uzaktan kapatabilmelerini sağlar. Bu yetkiyi alan kişiler bilgisayarın hizmet veremez hale gelmesine ve DoS saldırısına yol açabilir. Bu nedenle yalnızca yüksek güvenilirliğe sahip yönetici hesaplarının bu kullanıcı hakkına sahip olması önerilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.22 maddesi tedbirindeki yapılan testlerde, Yöneticiler (Administrators) grubuna bu kullanıcı hakkı verildiği için sistemin güvenliğinde herhangi bir ihlal tespit edilmemiştir. Bu nedenle uygulanan bu yetkiyi yalnızca yönetici hesaplarında olduğundan iyileştirme modelinde uygulanan sıkılaştırma kodu yazılmamıştır.

4.1.1.22. Güvenlik Denetim Kayıtları Oluşturma Yapılandırılması

Bu politika, hangi kullanıcıların veya süreçlerin güvenlik günlüklerinde denetim kaydı oluşturabileceğini belirler. Bu kullanıcı hakkı ile işletim sistemi üzerinde kötüye kullanımda sistem yöneticisinin, kötüye kullanım etkinliklerinin bulmasını zorlaştıracak şekilde çok sayıda denetim kaydının oluşturulmasına yol açabilir. Ayrıca olay günlüğü

gerekli olduğunda olayları üzerine yazmak üzere yapılandırıldıysa, yetkisiz etkinliklere dair kanıtlar silinebilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.23 maddesi tedbirindeki yapılan testlerde, LOCAL SERVICE, NETWORK SERVICE gruplarına bu kullanıcı hakkı verildiğinden güvenlik ihlali tespit edilmemiştir. İşletim sistemi üzerinde doğru yapılandırma sağlandığı için iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.23. Kimlik Doğrulama Sonrası Kullanıcı Ayarları Yapılandırılması

Bu kullanıcı hakkı, bir kullanıcının veya belirli bir hesabın adına işlem yapabilmesini sağlar. Eğer bir kötü niyetli kullanıcı bu kullanıcı hakkına sahip olursa, bir hizmet oluşturup istemciyi bu hizmete bağlamaya kandırarak istemcinin yetkilerini taklit edebilir ve saldırganın izinlerini artırabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.24 maddesi tedbirindeki yapılan testlerde, Yöneticiler (Administrators), LOCAL SERVICE, NETWORK SERVICE, SERVICE gruplarına bu kullanıcı hakkı verildiği görülmüş olup güvenlik ihlali tespit edilmemiştir. Söz konusu yapılandırma doğru olduğundan iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.24. Zamanlama Önceliğini Artırma Yapılandırılması

Bu yapılandırma kullanıcılara bir sürecin temel öncelik sınıfını artırma yetkisi verir. Bu yetkiyi alan bir kullanıcı, bir sürecin önceliğini çok yüksek yaparak diğer süreçlerin işlemci zamanı almasını engelleyebilir ve sistemde DoS durumu yaratabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.25 maddesi tedbirindeki yapılan testlerde, Yöneticiler (Administrators) ve Window Manager\Window Manager Group gruplarına bu kullanıcı hakkı verildiğinden herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle, zaten uygun yapılandırma sağlandığı için iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.25. Cihaz Sürücülerini Yükleme ve Kaldırma Ayarları

Bir kullanıcının hesabı aracılığıyla dinamik olarak yeni bir cihaz sürücüsü yüklemesi sağlanabilir. Ancak bu yetkiye sahip kötü niyetli bir kullanıcı, cihaz sürücüsü gibi görünen kötü amaçlı yazılımları sisteme yükleyebilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.26 maddesi tedbirindeki yapılan testlerde, Yöneticiler (Administrators) grubuna bu kullanıcı hakkı verildiği ve doğru yapılandırma sağlandığından güvenlik ihlali tespit edilmemiş olup iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.26. Bellekte Verileri Kilitle Ayarları

Bu politika, bir işlemin verilerini fiziksel bellekte tutmasına izin verir ve verilerin sanal belleğe yazılmasını engeller. Bu yetkiyi alan bir kullanıcı, bellek üzerindeki diğer süreçler için yeterli RAM bırakmadan, bellek üzerinde çok sayıda işlem çalıştırarak DoS durumuna yol açabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.27 maddesi tedbirindeki yapılan testlerde, Hiç Kimse (No One) olarak yapılandırıldığından herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle güvenlik yapılandırması zaten doğru olduğundan, iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.27. Denetim ve Güvenlik Günlüklerini Yönetme Ayarları

Denetim ve güvenlik günlüklerini yönetme, hangi kullanıcıların dosya ve dizinlerin denetim seçeneklerini değiştirebileceğini ve güvenlik günlüklerini temizleyebileceğini belirler. Bu ayrıcalık ile önemli güvenlik günlüklerinin silinmesini engellemek amacıyla yalnızca yönetici hesaplarıyla sınırlanmalıdır. Aksi takdirde kötü niyetli bir kullanıcı bu yetkiyi kötüye kullanarak kritik güvenlik bilgilerini silebilir.

Yapılan testlerde, CIS Benchmark v3.0.0-2.2.30 maddesi doğrultusunda, “Denetim ve güvenlik günlüklerini yönetme” yetkisi yalnızca Yöneticiler (Administrators) olarak ayarlandığında, herhangi bir güvenlik açığı tespit edilmemiştir. Bu nedenle ayarın önerilen yapılandırması Yöneticiler (Administrators) olarak

bırakılmalıdır. Testlerde çıkan sonuçlara göre güvenlik yapılandırması zaten doğru olduğundan, iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.28. Yazılım Ortamı Değiştirme Yapılandırılması

Bir nesnenin etiketini değiştirme yapılandırması kullanıcıların başkalarına ait dosya ve süreçlerin bütünlük etiketini değiştirmelerini engeller. Bu yetki yalnızca belirli yönetici hesaplarına verilmelidir. Aksi takdirde kötü niyetli bir kullanıcı başka birinin etiketini değiştirerek, daha yüksek ayrıcalıklara sahip işlemleri çalıştırabilir ve güvenlik risklerini artırabilir. Firmware ortamı değerlerini değiştirme kullanıcı hakkı verilen herhangi bir kişi, bir donanım bileşeninin ayarlarını yapılandırarak arızalanmasına neden olabilir ve bu durumda veri bozulmasına veya Hizmet Reddi (DoS) durumuna yol açabilir.

Yapılan testlerde, CIS Benchmark v3.0.0-2.2.31 maddesi doğrultusunda, bu yetkiyi Hiç Kimse (No One) olarak yapılandırmak, herhangi bir güvenlik açığı oluşturmaz. Testlerin incelemesinde güvenlik yapılandırması zaten doğru olduğundan, iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.29. Donanım Yazılımı Ortam Değerlerini Değiştirme Ayarları

Donanım yazılımı ortam değerlerini değiştirme, kullanıcıların donanım yapılandırmalarını değiştirmelerini sağlar. Bu yetkiyi kötüye kullanan bir kullanıcı, sistemin donanım bileşenlerini bozarak hizmet kesintilerine neden olabilir.

Yapılan testlerde, CIS Benchmark v3.0.0-2.2.32 maddesi doğrultusunda, bu ayrıcalığın yalnızca Yöneticiler (Administrators) tarafından kullanılması gerektiğinden güvenlik yapılandırması doğru uygulandığı görüldüğünden iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.30. Bakım Görevlerini Yerine Getirme Ayarları

Bakım görevlerini yerine getirme, bir kullanıcının sistemdeki disk yapılandırmasını yönetmesini sağlar. Bu yetki disk hacimlerinin silinmesi gibi işlemleri yaparak veri kaybına veya hizmet kesintilerine neden olabilir.

Yapılan testlerde, CIS Benchmark v3.0.0-2.2.33 maddesi doğrultusunda, bu ayarın Yöneticiler (Administrators) olarak yapılandırılmasının doğru uygulandığı görüldüğünden iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.31. Tek Süreç Profili Yapılandırılması

Tek Süreç Profili (Profile Single Process) politikası, bir kullanıcının yalnızca belirli bir sistem sürecini izlemesine olanak tanır. Ancak bu tür izlemeler, saldırganların sistemdeki zayıf noktaları tespit etmesine yardımcı olabilir. Bu nedenle, bu tür yetkiler yalnızca güvenilir kullanıcılar ve yöneticilerle sınırlı olmalıdır.

Yapılan testlerde, CIS Benchmark v3.0.0-2.2.34 maddesi doğrultusunda, "Profile Single Process" yetkisinin yalnızca Yöneticiler (Administrators) grubuna verilmesinin herhangi bir güvenlik açığına yol açmadığı ve bu ayarın güvenli olduğu gözlemlenmiştir. Bu nedenle Yöneticiler (Administrators) grubunun bu yetkiye sahip olması önerilmektedir. Bu sebep ile iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.32. Sistem Performansı Profil Oluşturma Yapılandırılması

Sistem performansını profil oluşturma, kullanıcıların sistemin farklı süreçlerinin performansını izlemelerine olanak tanır. Bu yetki kötü niyetli kullanıcıların aktif süreçleri analiz etmelerini sağlayarak, güvenlik zafiyetlerine ve güvenlik risklerine yol açabilir.

Yapılan testlerde, CIS Benchmark v3.0.0-2.2.35 maddesi doğrultusunda, bu ayarın Yöneticiler (Administrators), NT SERVICE\WdiServiceHost olarak yapılandırılığı görüldüğünden güvenlik açısından herhangi bir olumsuz etki

oluşturmadığı tespit edilmiştir. Bu sebep ile iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.33. İşlem Düzeyinde Jeton (Token) Değiştirme Ayarlarının Yapılandırılması

Bir işlem düzeyi jeton(token)'ları değiştirme, bir işlemin başka bir güvenlik belirteciyle çalıştırılmasına olanak tanır. Yapılan bu işlemi kötüye kullanan bir saldırganın ayrıcalıklarını yükseltmesi ve kötü niyetli işlemler gerçekleştirmesi sağlanabilir.

Yapılan testlerde, CIS Benchmark v3.0.0-2.2.36 maddesi doğrultusunda, bu ayarın LOCAL SERVICE, NETWORK SERVICE olarak yapılandırılmasının doğru olduğu ve bu yapılandırmanın herhangi bir güvenlik açığına yol açmadığı tespit edildiğinden iyileştirme modelinde sıkılaştırma kodları yazılmamıştır.

4.1.1.33. Dosya ve Dizinleri Geri Yükle Yetki Yapılandırılması

Bu güvenlik politikası, Windows Vista veya Windows'un daha üst çıkan sürümlerini kullanan bilgisayarlarda, yedeklenen dosya ve dizinlerin geri yüklenmesi sırasında hangi kullanıcıların dosya, dizin, kayıt defteri ve diğer kalıcı nesne izinlerini geçebileceğini belirler. Bu kullanıcı hakkı, geçerli güvenlik ilkelerini nesne sahipleri olarak atayabilen kullanıcıları da belirler.

SeRestorePrivilege hakkına sahip bir saldırgan, bilgisayara hassas verileri geri yükleyebilir ve daha yeni verilerin üzerine yazabilir. Bu da önemli veri kaybına veri bozulmasına veya hizmet reddine yol açabilir. Saldırganlar, geçerli yöneticiler veya sistem hizmetleri tarafından kullanılan çalıştırılabilir dosyaların üzerine, kötü amaçlı yazılım içeren versiyonlar yükleyerek kendilerine yükseltilmiş ayrıcalıklar elde edebilir, verileri tehlikeye atabilir veya bilgisayara arka kapılar kurarak sürekli erişim sağlayabilir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.37 tedbirine göre, bu güvenlik açığının önlenmesi için "Restore files and directories" (Dosya ve dizinleri geri yükleme) hakkı yalnızca Yöneticiler (Administrators) grubuna atanmalıdır. Bu sayede yalnızca yönetici haklarına sahip kullanıcıların bu işlemi yapabilmesi sağlanır.

Bu tedbir ile ilgili iyileştirme modeli geliştirilmiş olup, tedbiri olumlu sonuçlandıracak sıkılaştırma kodları aşağıdaki gibi uygulanmıştır.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "Dosya ve Dizinleri Geri Yükle Yetkisi" güvenlik ayarını yapılandırmak için kullanılır. Bu politika, yedeklenen dosya ve dizinlerin geri yüklenmesi sırasında, hangi kullanıcıların sistemdeki önemli nesnelere (dosyalar, dizinler, kayıt defteri vb.) yetki ile müdahale edebileceğini belirler. Bu script, SeRestorePrivilege (Dosya ve Dizinleri Geri Yükleme) hakkının yalnızca Yöneticiler (Administrators) grubuna verilmesini sağlamak için tasarlanmıştır. Script, geçerli yapılandırmayı dışa aktarır, önerilen değerle karşılaştırarak gerektiğinde Administrators grubuna ait SID'yi ekler veya günceller. Bu, sadece yöneticilerin sistem dosyalarını geri yükleyebilmesini sağlar ve saldırganların kötü amaçlı yazılımlar yükleyerek yetki kazanmalarını engeller.

```
1. # Hedef kullanici hakkı (Restore files and directories)
2. $HakkinAdi = 'SeRestorePrivilege'
3.
4. # "Administrators" grubunun SID degeri
5. $OnerilenDegerler = @(
6.     '*S-1-5-32-544'  # Administrators grubunun SID'i (Security Identifier)
7. );
8.
9. # Gecici dosya adlarini olustur
10. $sidler = @()
11. $onerilenDeger = ''
12. $SeceditAraci = 'C:\Windows\System32\secedit.exe'  # Secedit aracinin yolu
13. $benzersiz = (Get-Date).ToString("yyyyMMddHHmmssfff")  # Benzersiz dosya adi
olusturmak icin tarih
14. $seceditYolu = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Gecici yapilandirma
dosyasinin yolu
15.
16. # Mevcut yapilandirmayi disa aktar
17. &$SeceditAraci /export /areas USER_RIGHTS /cfg $seceditYolu /quiet;
18.
19. # Yapilandirma dosyasini oku
20. $config = Get-Content -Path $seceditYolu
21.
22. # "SeRestorePrivilege" hakkı icin onerilen degeri birlestir
23. for ($i = 0; $i -lt $OnerilenDegerler.Count; $i++) {
24.     if ($i -eq $OnerilenDegerler.Count - 1) {
25.         $onerilenDeger += $OnerilenDegerler[$i]
26.     }
27.     else {
28.         $onerilenDeger += $OnerilenDegerler[$i] + ','
29.     }
30. }
31.
32. # "SeRestorePrivilege" hakkı zaten atanmis mi diye kontrol et
33. if (get-content $seceditYolu | Select-String -Pattern $HakkinAdi) {
34.     # Eger atanmis ise, mevcut degeri onerilen degerle degistir
35.     $config = $config -replace "$HakkinAdi\s*=\s*.*$", "$HakkinAdi = $onerilenDeger"
36.     $config | Set-Content -Path $seceditYolu
37. }
38. else {
39.     # Eger atanmis degilse, yeni bir satir ekleyerek onerilen degeri ata
```

```
    $configYeni = @()
    $indeks = $config.IndexOf("[Privilege Rights]") + 1  # [Privilege Rights] kısmının hemen sonrasına ekle
    $satirEklenecek = "$HakkinAdi=$onerilenDeger"
    foreach ($satir in $config) {
        $configYeni += $satir
        if ($config.IndexOf($satir) -eq $indeks) {
            $configYeni += $satirEklenecek
        }
    }
    $configYeni | Set-Content -Path $seceditYolu
}

# Yapilandirma dosyasini uygula
&$SeceditAraci /configure /db secedit.sdb /cfg $seceditYolu

# Gecici dosyayi sil
Remove-Item -Path $seceditYolu -Force
```

4.1.1.34. Sistemi Kapat Ayarının Yetki Yapılandırılması

Bu politika ayarı, bilgisayarlarınızdaki hangi kullanıcıların yerel olarak "Sistemi Kapat" komutunu kullanarak işletim sistemini kapatabileceğini belirler. Sistemi kapatma yetkisi, genellikle yalnızca yöneticiler ve yetkilendirilmiş kullanıcılar için sağlanmalıdır. Misafir veya yetkisiz kullanıcıların bu yetkiye sahip olması, potansiyel olarak hizmet aksaklıklarına (Denial of Service - DoS) yol açabilir. Bu nedenle, bu yetkinin sadece belirli kullanıcılara verilmesi, sistemin güvenliğini sağlamak için kritik önem taşır.

Önerilen yapılandırma, "Sistemi Kapat" komutunu sadece Yöneticiler (Administrators) ve Kullanıcılar (Users) gruplarındaki kullanıcılara vermek olup, diğer grupların bu yetkiye sahip olmaması gerektiğidir. Böylece, kötüye kullanım riski azaltılır ve yalnızca güvenilir kullanıcıların sistemi kapatmasına izin verilmiş olur.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.38 ayarın uygulanması, yetkisiz kişilerin sistemi kapatma yetkisini kullanmalarını engelleyecektir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "Sistemi Kapat" komutunun yalnızca belirli kullanıcı gruplarına, yani Yöneticiler (Administrators) ve Kullanıcılar (Users) gruplarına verilmesini sağlamak için kullanılır. "SeShutdownPrivilege" adı verilen bu yetki, yalnızca güvenilir kullanıcıların bilgisayar sistemini kapatma yetkisini kullanabilmesini sağlar, bu da hizmet aksaklıklarının ve

kötüye kullanım risklerinin önlenmesine yardımcı olur. Script, geçerli güvenlik yapılandırmasını dışa aktarır, tavsiye edilen yönetici (Administrators) ve kullanıcı (Users) gruplarının SID'lerini birleştirir, mevcut yapılandırmayı kontrol eder ve gerekiyorsa günceller. Son olarak, yeni yapılandırmayı uygular ve geçici dosyayı siler. Bu sayede, sadece yetkili kullanıcıların sistemi kapatmasını sağlar, böylece kötüye kullanım ve Denial of Service (DoS) gibi güvenlik tehditlerini engeller.

```
$MetodArgumani = 'SeShutdownPrivilege'  # Kapatma ayrıcalığı
$onerilenDegerler = @(
    '*S-1-5-32-544',  # Administrators (Yönetici grubu)
    '*S-1-5-32-545'   # Users (Kullanıcı grubu)
)
$sids = @()  # SID'ler için liste (boş)
$onerilenDeger = ''  # Tavsiye edilen değer
$SecEditYolu = 'C:\Windows\System32\secedit.exe'  # Güvenlik yapılandırma aracı
$benzersiz = (Get-Date).ToString("yyyyMMddHHmmssfff")  # Benzersiz dosya adı oluşturma
$secedit = $Env:Temp + '\secedit'+$benzersiz+'.cfg'  # Geçici yapılandırma dosyası

# Kullanıcı haklarını dışa aktar
&$SecEditYolu /export /areas USER_RIGHTS /cfg $secedit /quiet

# Yapılandırma dosyasını oku
$config = Get-Content -Path $secedit

# Tavsiye edilen SID'leri birleştir
for ($i = 0 ; $i -lt $onerilenDegerler.Count; $i++) {
    if ($i -eq $onerilenDegerler.count - 1) {
        $onerilenDeger += $onerilenDegerler[$i]
    }
    else {
        $onerilenDeger += $onerilenDegerler[$i] + ','  # SID'leri virgülle ayır
    }
}

# Eğer parametre zaten mevcutsa, değerleri güncelle
if (get-content $secedit | Select-String -Pattern $MetodArgumani) {
    # Mevcut değeri tavsiye edilen değerle değiştir
    $config = $config -replace "$MetodArgumani\s*=\s*.*$", "$MetodArgumani =
$onerilenDeger"
    $config | Set-Content -Path $secedit
} else {
    # Parametre mevcut değilse, [Privilege Rights] bölümüne ekle
    $yeniConfig = @()
    $indeks = $config.IndexOf("[Privilege Rights]") + 1
    $satirEkle = "$MetodArgumani=$onerilenDeger"
    foreach ($satir in $config) {
        $yeniConfig += $satir
        if ($config.IndexOf($satir) -eq $indeks) {
            $yeniConfig += $satirEkle  # Yeni satırı ekle
        }
    }
    $yeniConfig | Set-Content -Path $secedit
}

# Yapılandırmayı uygula
&$SecEditYolu /configure /db secedit.sdb /cfg $secedit

# Geçici dosyayı sil
Remove-Item -Path $secedit -Force
```

4.1.1.35. Dosyaların veya Diğer Nesnelerin Sahiplik Yetkisi Ayarları

Dosya, klasör, kayıt defteri anahtarları, işlemler veya iş parçacıkları gibi nesnelerin sahipliğini almak için verilen bu yetki, kullanıcıların mevcut izinleri geçersiz kılarak bu nesnelerin sahipliğini değiştirmesine olanak tanır.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-2.2.39 maddesi tedbirindeki yapılan testlerde, Windows 10 işletim sistemi üzerinde "Dosyaların veya Diğer Nesnelerin Mülkiyetini Alma" yetkisi yalnızca "Yöneticiler" grubuna verildiğinde, sistem güvenliğinde herhangi bir ihlal tespit edilmemiştir. Bu nedenle, mevcut sistemde bu yetki zaten yalnızca Yöneticiler (Administrators) grubuna verilmiş olup, herhangi bir sıkılaştırma kodu uygulanmamıştır.

4.1.2. Otomatik Güncellemenin Aktif Olması

Windows sistemlerinde güvenliğin sağlanabilmesi için otomatik güncelleme özelliğinin her kullanıcı makinesinde aktif hale getirilmesi gerekmektedir. Otomatik güncellemeler, işletim sisteminin ve yazılımlarının en son güvenlik yamaları ile güncel tutulmasını sağlar. Bu sayede, sistemler bilinen güvenlik açıklarına karşı korunur ve potansiyel saldırıların önüne geçilir.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerini dikkate alarak kurumların güvenlik uygulamalarını değerlendirir. "Otomatik Güncellemenin Aktif Olması" tedbiri, CIS denetimlerinin bir parçası olarak, tüm kullanıcı makinelerinde otomatik güncellemelerin etkinleştirilmesini önerir. Bu, sistemin her zaman güncel ve güvenli kalmasını sağlayarak, siber tehditlere karşı güçlü bir savunma mekanizması oluşturur. Çizelge 4.2'de, BİGR 5.1.3.2 maddesi, Otomatik Güncellemenin Aktif Olması tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.2. Windows işletim sistemi otomatik güncellemelerin aktif olması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.2	Otomatik Güncellemenin Aktif Olması	Tüm kullanıcı makinelerinde otomatik güncelleme özelliği aktif hale getirilmelidir.	18.10.92.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' 18.10.92.2.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 – Every day'

4.1.2.1. Otomatik Güncellemeleri Yapılandırma

"Otomatik Güncellemeleri Yapılandırma" politikası, bilgisayarların Windows Update veya Windows Server Update Services (WSUS) aracılığıyla güvenlik güncellemelerini alıp almayacağını belirleyen bir ayardır. Bu ayar etkinleştirildiğinde, işletim sistemi, ağ bağlantısı mevcut olduğunda Windows Update veya belirlenen intranet sitesini kontrol ederek ilgili güncellemeleri indirir ve uygular. Bu politika özellikle organizasyonların tüm bilgisayarlarının güvenlik açıklarına karşı korunmasını sağlamak için önemlidir çünkü her güncelleme, bilinen güvenlik açıklarını kapatır ve sistemin istikrarlı çalışmasını sağlar. Bu ayarın önerilen durumu "Enabled" olarak belirlenmiştir. Bu durumda bilgisayarlar güncellemeleri alacak ve otomatik olarak güncelleme yapacaktır.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-18.10.92.2.1 tedbirine göre bu ayar, özellikle ağdaki tüm cihazların güncel kalmasını sağlayarak, potansiyel güvenlik açıklarına karşı koruma sağlar. Güvenlik açığının hızlı bir şekilde kapatılmasını ve güncel olmayan sistemlerin kötü amaçlı yazılımlar tarafından hedef alınmasını engeller.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "Otomatik Güncellemeleri Yapılandırma" politikasını etkinleştirmek için kullanılır. İlk olarak, Windows Update ayarlarını içeren kayıt defteri anahtarının (HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU) var olup olmadığı kontrol edilir. Eğer anahtar mevcut değilse, bu anahtar oluşturulur. Ardından, "NoAutoUpdate" adında bir kayıt defteri değeri sıfır (0) olarak ayarlanır. Bu işlem, bilgisayarların otomatik güncellemeleri almasını sağlamak için gereklidir, çünkü

NoAutoUpdate değerinin 0 olması, otomatik güncellemelerin etkinleştirilmesi anlamına gelir. Böylece bilgisayarlar, güvenlik güncellemelerini otomatik olarak alacak ve uygulayacaktır. Bu ayar, sistemin güncel ve güvenli kalmasını sağlamaya yardımcı olur.

```
1. $sonuc1 = (Test-Path -Path
'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU')
2. # 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' yolundaki kayıt defteri
anahtarının var olup olmadığını kontrol et
3.
4. If ($sonuc1 -ne $true){
5.      # Eğer anahtar mevcut değilse, yeni bir anahtar oluştur
6.      New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' -Force
7. }
8.
9. # 'NoAutoUpdate' özelliğini 0 olarak ayarla
10. Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' -
Name 'NoAutoUpdate' -Value 0 -Force -PassThru
```

4.1.2.2. Otomatik Güncellemelerin Zamanlanmış Yükleme Gününü Yapılandırma

"Otomatik Güncellemeler: Zamanlanmış Yükleme Günü" politikası, bilgisayarların güvenlik güncellemelerini Windows Update veya Windows Server Update Services (WSUS) aracılığıyla hangi günlerde alacağını belirler. Bu ayar, sistemlerin her gün güncellenmesini sağlayarak, güvenlik açıklarının hızlı bir şekilde kapatılmasını ve güncel olmayan yazılımların sistemden uzak tutulmasını amaçlar.

Bu ayarın önerilen durumu "0 - Her gün" olarak belirlenmiştir. Bu durumda, Windows güncellemeleri her gün, genellikle sabah 3:00'te otomatik olarak indirilecek ve kurulacaktır. Bu, özellikle organizasyonlarda güncellemelerin tutarlı ve zamanında uygulanması için kritik bir adımdır. Günlük güncellemeler, potansiyel güvenlik açıklarına karşı hızlı bir yanıt verilmesini ve sistemin her zaman en son güvenlik yamalarına sahip olmasını sağlar.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-18.10.92.2.2 tedbirine göre bu ayarın etkinleştirilmesi, bilgisayarların kritik işletim sistemi güncellemeleri ve servis paketlerini her gün almasını sağlar. Bu, ağdaki cihazların güvenliğini artırır ve organizasyonların yazılım yönetim sürecini iyileştirir. Ayrıca, zamanında uygulanan güncellemelerle cihazların kötü amaçlı yazılımlar ve diğer siber tehditlere karşı savunması güçlendirilir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, “Otomatik Güncellemelerin Zamanlanmış Yükleme Gününü Yapılandırma” politikasını etkinleştirmek için kullanılır. İlk olarak, belirtilen kayıt defteri yolunun (HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU) var olup olmadığı kontrol edilir. Eğer yol mevcut değilse, bu kayıt defteri yolu oluşturulur. Sonrasında, “ScheduledInstallDay” adlı kayıt defteri değeri sıfır (0) olarak ayarlanır. Bu değer, güncellemelerin her gün yapılacağını belirtir. Yani, ScheduledInstallDay değeri 0 olarak ayarlandığında, Windows Update her gün güncellemeleri otomatik olarak indirip yükler. Bu ayar, bilgisayarların sürekli olarak güncel kalmasını sağlar, güvenlik açıklarının hızla kapanmasına ve kötü amaçlı yazılımların engellenmesine yardımcı olur.

```
1. # İlk olarak, belirli bir kayıt defteri yolunun var olup olmadığını kontrol ederiz.
2. $sonuc2 = (Test-Path -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU)
3.
4. # Eğer bu yol mevcut değilse, yeni bir yol oluşturulur.
5. If ($sonuc2 -ne $true){
6.       # Kayıt defteri yolunu oluşturur
7.       New-Item -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU -Force
8. }
9.
10. # Bu noktada ScheduledInstallDay adındaki özelliğin değerini 0 olarak ayarlarız.
11. # Bu, güncelleme için otomatik olarak belirli bir gün seçilmeden işlem yapılacağı
anlamına gelir.
12. Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' -
Name 'ScheduledInstallDay' -Value 0 -Force -PassThru
```

4.1.3. SMB Protokolü Güvenliği

Windows işletim sistemlerinde, daha güvenli ve güncel SMB (Server Message Block) protokol versiyonlarının kullanılması gerekmektedir. SMB versiyon 1, eski ve güvenlik açıklarına sahip bir protokoldür, bu nedenle daha yeni versiyonlarla değiştirilmesi, sistemin güvenliğini önemli ölçüde artırır. SMB versiyon 2 ve 3, gelişmiş şifreleme ve güvenlik özellikleri sunarak veri iletimini güvenli hale getirir.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayalı olarak, SMB protokolünün güvenli kullanımını vurgular. “SMB Protokolü Güvenliği” tedbiri, SMB versiyon 1’in devre dışı bırakılmasını ve daha güvenli olan versiyonların kullanılmasını önerir. Bu uygulama ağ içi iletişimin güvenliğini artırır ve olası siber saldırılara karşı savunmayı güçlendirir. Çizelge 4.3’te,

BİGR 5.1.3.3 maddesi, SMB Protokolü Güvenliği tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.3. Windows işletim sistemi SMB protokolü güvenliği

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.3	SMB Protokolü Güvenliği	Windows işletim sistemlerinde SMB versiyon 1 protokolü yerine daha güvenli ve güncel SMB protokol versiyonları kullanılmalıdır.	18.4.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' 18.4.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'

4.1.3.1. SMB v1 İstemci Sürücüsünü Yapılandırma

"SMB v1 İstemci Sürücüsü Yapılandırması" politikası, Server Message Block (SMB) protokolünün birinci sürümünün istemci tarafındaki sürücü hizmetinin başlangıç türünü ayarlamaktadır. SMB v1, 30 yılı aşkın bir geçmişe sahip, ağ dosya paylaşımı ve yazıcı hizmetleri için kullanılan eski bir protokoldür. Ancak modern ağlarda güvenlik açıkları nedeniyle kullanımı önerilmemektedir. Microsoft, Eylül 2016'dan itibaren SMB v1'in devre dışı bırakılmasını önermektedir. Çünkü SMB v1, daha yeni ve güvenli protokoller olan SMB v2 ve SMB v3'e kıyasla çok daha savunmasızdır. Özellikle, WannaCry gibi fidye yazılımlarının, SMB v1 protokolündeki açıkları kullanarak büyük çapta zarar vermesi, bu protokolün güvenlik risklerini gözler önüne sermektedir.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-18.4.3 tedbirine göre, bu ayarın önerilen durumu "Enabled: Disable driver (recommended)" olarak belirlenmiştir. Bu konfigürasyon, SMB v1 istemci sürücüsünü devre dışı bırakır, böylece bu eski ve güvensiz protokolün istemci tarafındaki kullanımı engellenmiş olur. Bu ayarın etkinleştirilmesi, ağdaki güvenlik açığını azaltarak kötü niyetli saldırılara karşı önemli bir koruma sağlar.

Ancak, bu ayar asla "Disabled" olarak yapılandırılmamalıdır, çünkü bu durumda kayıt defterindeki ilgili giriş silinir, bu da ciddi sistem sorunlarına yol açabilir. SMBv1'i

devre dışı bırakmak bazı eski işletim sistemleri ve uygulamalarla uyumsuzluklara yol açabilir. Örneğin, Windows XP, Windows Server 2003 gibi eski işletim sistemleri ve bazı eski cihazlar, SMB v1'e bağımlıdır. Bu nedenle bu ayarın etkinleştirilmeden önce dikkatli bir şekilde test edilmesi ve uyumsuzlukların giderilmesi gerekmektedir. Microsoft, SMB v1 uyumsuzlukları için kapsamlı bir liste tutmakta ve bu liste, kullanıcıların potansiyel uyumsuzlukları önceden tespit etmelerini kolaylaştırmaktadır.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "SMB v1 İstemci Sürücüsünü Yapılandırma" politikasını uygulamak için kullanılır. İlk olarak, belirtilen kayıt defteri anahtarının (HKLM:\SYSTEM\CurrentControlSet\Services\mrxsmb10) var olup olmadığı kontrol edilir. Eğer bu anahtar mevcut değilse, script yeni bir anahtar oluşturur. Sonrasında, Start değeri 4 olarak ayarlanır. Bu değer, SMB v1 istemci sürücüsünün devre dışı bırakılmasını sağlar. SMB v1'in devre dışı bırakılması, eski ve güvenli olmayan protokolün ağda kullanılmasını engelleyerek, ağ güvenliğini artırır. Bu ayar, özellikle eski protokolün güvenlik açıklarından korunmak amacıyla tavsiye edilen bir konfigürasyondur ve saldırılara karşı koruma sağlar.

```
1. # mrxsmb10 anahtarının var olup olmadığını kontrol et
2. $sonuc3 = (Test-Path -Path HKLM:\SYSTEM\CurrentControlSet\Services\mrxsmb10)
3.
4. # Eğer anahtar yoksa, yeni bir anahtar oluştur
5. If ($sonuc3 -ne $true){
6.      New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\mrxsmb10 -Force
7. }
8.
9. # Anahtarın Start değerini 4 olarak ayarla
10. Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\mrxsmb10' -Name
'Start' -Value 4 -Force -PassThru
```

4.1.3.2. SMB v1 Sunucusunu Yapılandırma

"SMB v1 Sunucusu Yapılandırması" politikası, sunucu tarafında Server Message Block (SMB) protokolünün birinci sürümünün (SMB v1) işleme biçimini belirler. SMB v1, 1980'lerin sonlarına doğru geliştirilen ve uzun yıllar boyunca ağ dosya paylaşımı ve yazıcı hizmetleri için yaygın olarak kullanılan bir protokoldür. Ancak, SMB v1'in eski ve güvenlik açıkları barındıran bir protokol olması nedeniyle modern ağlarda kullanımı şiddetle tavsiye edilmemektedir. Microsoft, Eylül 2016'dan itibaren SMB v1'in devre dışı bırakılmasını ve kullanılmamasını önermektedir. Çünkü SMB v1, daha yeni protokoller olan SMB v2 ve SMB v3'e kıyasla çok daha

savunmasızdır ve bu protokoller çok daha güvenli, performanslı ve verimli çözümlemeler sunmaktadır.

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-18.4.4 tedbirine göre, SMB v1'in devre dışı bırakılması, ağların güvenliğini artırarak saldırılara karşı koruma sağlar. SMB v1, birçok güvenlik açığını ve potansiyel kötü niyetli saldırıları barındıran bir protokol olduğundan, ağda kullanılan cihazların ve uygulamaların bu protokole olan bağımlılığı ortadan kaldırılmalıdır.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "SMB v1 Sunucusu Yapılandırma" politikasını uygulamak için kullanılır. İlk olarak, HKLM:\SYSTEM\CurrentControlSet\Services\ LanmanServer\Parameters kayıt defteri anahtarının var olup olmadığı kontrol edilir. Eğer anahtar mevcut değilse, script yeni bir anahtar oluşturur. Sonrasında, anahtara ait SMB 1 değeri 0 olarak ayarlanır. Bu, SMB v1 protokolünün sunucu tarafında devre dışı bırakılmasını sağlar. SMB v1'in devre dışı bırakılması, ağdaki güvenlik açıklarını azaltarak, daha güvenli ve verimli olan SMB v2 ve SMB v3 protokollerinin kullanılmasını teşvik eder. Bu ayar, ağ güvenliğini artırır ve kötü niyetli saldırılara karşı koruma sağlar.

```
# LanmanServer\Parameters anahtarının var olup olmadığını kontrol et
$sonuc4 = (Test-Path -Path
'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters')

# Eğer anahtar yoksa, yeni bir anahtar oluştur
If ($sonuc4 -ne $true){
      New-Item -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -
Force
}

# Anahtarın 'SMB1' değerini 0 olarak ayarla
Set-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' -Name 'SMB1' -Value 0 -
Force -PassThru
```

4.1.4. Yerel Yönetici Hesapları Yönetimi

Windows sistemlerinde yerel yönetici hesaplarının yalnızca gerekli kullanıcılar için aktif tutulması ve diğer tüm kullanıcıların bu hesaplardan çıkarılması gerekmektedir. Etki alanı üzerinde yapılacak çalışmada, gereksiz erişim yetkileri engellenerek sistemin güvenliği artırılır. Ayrıca gerekli kullanıcılar için varsayılan yerel

yönetici hesaplarının parolaları düzenli aralıklarla değiştirilmelidir. Bu tedbir, potansiyel saldırganların bu hesaplara erişim sağlamasını zorlaştırır.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerini temel alarak, yerel yönetici hesaplarının doğru şekilde yönetilmesini sağlar. "Yerel Yönetici Hesapları Yönetimi" tedbiri, gereksiz yönetici hesaplarının devre dışı bırakılmasını ve mevcut yönetici hesaplarının parolalarının düzenli olarak güncellenmesini önerir. Bu önlemler sistemin yetkisiz erişimlere karşı korunmasına yardımcı olur. Window işletim sisteminde etki alanına bağlı istemciler için düzenlenmiş olan bu tedbir CIS Benchmark v3.0.0-18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)" maddesinde bulunmaktadır. Bu çalışmada Microsoft Windows 10 Enterprise işletim sistemi için BİGR maddesi ile CIS maddesinin karşılık tedbiri bulunmamaktadır. Bu durumdan kaynaklı olarak Çizelge 4.4'te eşleştirmesi yapılamamıştır.

Çizelge 4.4. Windows işletim sistemi yerel yönetici hesapları yönetimi

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.4	Yerel Yönetici Hesapları Yönetimi	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmalıdır. Gerekli kullanıcılar için varsayılan olarak aynı tanımlanan yerel yönetici hesaplarının parolaları değiştirilmelidir.	Bulunmamaktadır.

4.1.5. Ayrıcalıklı Hesap Sayılarının Sınırlandırılması

Windows ortamlarında, etki alanı yöneticisi (Domain Admin) ve diğer yüksek yetkili hesapların (Enterprise Admin, Backup Admin, Schema Admin) sayısının sınırlanması gerekmektedir. Bu hesaplar, sistem üzerinde geniş yetkilere sahip olduğu için sayılarının azaltılması potansiyel güvenlik risklerini minimize eder. Ayrıcalıklı

hesapların yalnızca gerçekten ihtiyaç duyulan kişilerde bulunması, kötü niyetli erişimlerin ve iç tehditlerin önüne geçilmesine yardımcı olur.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayanarak, ayrıcalıklı hesapların yönetimini düzenler. "Ayrıcalıklı Hesap Sayılarının Sınırlandırılması" tedbiri, etki alanı yöneticisi ve diğer yüksek yetkili hesapların sayısının minimumda tutulmasını önerir. Bu, sistemin güvenliğini artırarak, yalnızca gerekli kullanıcıların kritik hesaplara erişimini sağlar ve yönetimsel hataları ya da kötüye kullanımları engeller. Windows işletim sistemi de etki alanına bağlı istemciler ve sunucular için düzenlenmiş olan Etki Alanı Sıkılaştırma Güvenliği kapsamında değerlendirilmesi gerekmektedir. Bu çalışmada, bu tedbir başlığı için Microsoft Windows 10 Enterprise işletim sistemi üzerinde BİGR maddesi ile CIS maddesinin karşılık tedbiri bulunmamaktadır. Bu durumdan kaynaklı olarak Çizelge 4.5'te eşleştirmesi yapılamamıştır.

Çizelge 4.5. Windows işletim sistemi ayrıcalıklı hesap sayılarının sınırlandırılması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.5	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Etki alanı yöneticisi (Domain Admin) ve diğer yetkili hesapların (Enterprise Admin, Backup Admin ve Schema Admin) sayısı sınırlandırılmalıdır.	Bulunmamaktadır.

4.1.6. Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi

Yetkili hesapların parola özetlerinin çalınmasının önlenmesi için, etki alanı yöneticisi (Domain Admin) hesabıyla kullanıcı bilgisayarlarında yalnızca gerekli işlemler yapılmalıdır. Gereksiz işlem yapılması durumunda, kullanıcı bilgisayarlarının yeniden başlatılması sağlanarak potansiyel riskler en aza indirilir. Ayrıca, yerel bilgisayarlarda parola özetlerinin tutulma sayısı sıfırlanmalı ve bu özetlerin depolanması engellenmelidir. Ayrıcalıklı kullanıcı hesapları ise Korunan Kullanıcılar (Protected

Users) grubuna dahil edilmelidir. Bu önlemler parola özetlerinin çalınarak kötüye kullanılmasını engellemeye yardımcı olur.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerini referans alarak, yetkili hesapların güvenliğinin sağlanması için belirli tedbirleri önerir. "Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi" tedbiri, etki alanı yöneticisi ve diğer ayrıcalıklı hesapların parola özetlerinin çalınmasını önlemek amacıyla bu hesaplarla yapılan işlemleri sınırlamayı ve güvenlik önlemleri almayı önerir. Sistemin güvenliğini artırarak yetkisiz erişimlerin ve veri hırsızlıklarının önüne geçilmesini sağlar. Çizelge 4.6'da, BİGR 5.1.3.6 maddesi, Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.6. Windows işletim sistemi yetkili hesapların parola özetlerinin çalınmasının engellenmesi

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.6	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Yetkili hesapların parola özetlerinin çalınmasının engellenmesi için: Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında gerekli olmadıkça işlem yapılmamalı, işlem yapıldığı durumlarda kullanıcı bilgisayarlarının yeniden başlatılması sağlanmalıdır. Yerel bilgisayarlarda parola özetleri tutulma sayısı 0 yapılmalıdır. Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) grubuna alınmalıdır.	2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'

4.1.6.1. LAN Manager Karma İşlevi (Hash) Değerini Saklama Yapılandırması

LAN Manager (LM) karma işlevi (hash) değeri, eski ve zayıf bir şifreleme metodudur. Eğer bu değer saklanırsa şifre veritabanı ele geçirildiğinde, saldırganlar şifreyi kolayca çözebilir. Bu nedenle, parola değiştirildikten sonra LM karma işlevi (hash) değerinin saklanmaması, güvenlik açısından önemli bir önlemdir.

Yapılan testlerde, CIS Benchmark v3.0.0-2.3.11.5 maddesine uygun olarak "Ağ güvenliği: LAN Manager karma işlevi (hash) değerini bir sonraki şifre değişikliğinde saklama" politikası etkinleştirildiğinden, sistemde herhangi bir güvenlik ihlali tespit edilmemiştir. Bu ayarın etkin olduğu görüldüğünden, iyileştirme modelinde ek bir sıkılaştırma kodu gerekmemektedir.

4.1.7. Kullanılmayan Hesapların Devre Dışı Bırakılması

Windows sistemlerinde, aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarının tespit edilmesi için bir prosedür oluşturulmalıdır. Bu hesaplar, güvenlik riskleri oluşturabileceğinden, belirli bir süre boyunca kullanılmayan hesaplar düzenli olarak devre dışı bırakılmalıdır. Bu işlemde potansiyel sızma girişimlerine karşı önlem alınmasına yardımcı olur ve sistemin güvenliğini artırır.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayanarak, kullanılmayan hesapların yönetimini ve devre dışı bırakılmasını önerir. "Kullanılmayan Hesapların Devre Dışı Bırakılması" tedbiri, aktif dizinde uzun süre kullanılmayan hesapları tespit etmek için bir prosedürün oluşturulmasını ve bu hesapların devre dışı bırakılmasını önerir. Bu önlem yalnızca aktif ve yetkili kullanıcıların sisteme erişmesini sağlayarak, olası güvenlik açıklarını kapatır.

Windows işletim sisteminde, etki alanına bağlı sunucular için düzenlenmiş olan Etki Alanı Sıkılaştırma Güvenliği kapsamında değerlendirilmesi gerekmektedir. CIS 17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) maddesine karşılık gelmektedir ve sadece Etki Alanı Yönetim Sunucusu-Domain Controller (DC) tarafında uygulanmaktadır. Bu çalışmada, bu tedbir başlığı için Microsoft Windows 10 Enterprise işletim sistemi üzerinde BİGR maddesi ile CIS

maddesinin karşılık tedbiri bulunmamaktadır. Bu durumdan kaynaklı olarak Çizelge 4.7'te eşleştirmesi yapılamamıştır.

Çizelge 4.7. Windows işletim sistemi kullanılmayan hesapların devre dışı bırakılması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.7	Kullanılmayan Hesapların Devre Dışı Bırakılması	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmalıdır. Bk. Tedbir No: 3.1.12.10	Bulunmamaktadır.

4.1.8. Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması

Windows sistemlerinde varsayılan yönetici (Administrator) ve misafir (Guest) hesaplarının pasif hale getirilmesi gerekmektedir. Bu hesaplar genellikle güvenlik açıklarına sahip olabileceğinden, aktif olmamaları sistemin güvenliğini artırır. Varsayılan hesaplar saldırganlar tarafından hedef alınabilir ve bu nedenle yalnızca gerektiğinde etkinleştirilmeli veya tamamen devre dışı bırakılmalıdır.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerini referans alarak, varsayılan yönetici ve misafir hesaplarının devre dışı bırakılmasını ve yalnızca güvenli bir şekilde yapılandırılmasını önerir. "Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması" tedbiri, sistemlerde yer alan bu hesapların pasif hale getirilmesi gerektiğini vurgular. Bu tedbir sistemin siber tehditlere karşı savunmasını güçlendirir ve yetkisiz erişimlerin önüne geçilmesini sağlar. CIS Benchmark v3.0.0-2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (MS only) olarak yapılandırılması, etki alanında bulunan istemci tarafında uygulanmaktadır. Çizelge 4.8'de, BİGR 5.1.3.8 maddesi, Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.8. Windows işletim sistemi varsayılan yönetici ve misafir hesaplarının yapılandırılması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.8	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Sistemlerde yer alan varsayılan yönetici ve misafir hesapları pasif hale getirilmelidir.	2.3.1.1 (L1) Ensure ‘Accounts: Administrator account status’ is set to ‘Disabled’ (MS only) 2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'

4.1.9. Standart Kullanıcıların Betik Çalıştırma Erişiminin Kısıtlanması

Windows sistemlerinde, standart kullanıcıların betik çalıştırma motorlarına (Windows Script Host, PowerShell, Command Prompt, Microsoft HTML Application Host vb.) erişimi kısıtlanmalı veya tamamen engellenmelidir. Bu motorlar, kötü niyetli yazılımlar tarafından kötüye kullanılabilir ve sistem güvenliği için ciddi tehditler oluşturabilir. Kullanıcıların yalnızca gerekli işlemler için bu araçlara erişmesi sağlanmalı ve gereksiz erişimler engellenmelidir.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerini temel alarak, standart kullanıcıların betik çalıştırma motorlarına erişiminin kontrol edilmesini önerir. “Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması” tedbiri, bu motorların yetkisiz kullanıcılar tarafından kullanılmasını engellemeyi amaçlar. CIS Benchmark v3.0.0-18.10.80.3 (L2) Ensure “Prevent Internet Explorer security prompt for Windows Installer scripts” is set to ‘Disabled’ maddesi Internet Explorer yazılımı için tedbir alınmış fakat Microsoft tarafından 2023 yılında Internet Explorer desteği sonlandırıldığı ve kullanılmadığı için iyileştirme modeli uygulanmamıştır (Microsoft, 2023). Bu önlem sistemdeki güvenlik açıklarının azaltılmasına ve olası zararlı yazılımların yayılmasının önlenmesine yardımcı olur. Çizelge 4.9’da, BİGR 5.1.3.9 maddesi, Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.9. Windows işletim sistemi standart kullanıcıların betik çalıştırma motorlarına erişiminin kısıtlanması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.9	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Standart kullanıcıların betik çalıştırma motorlarına (Windows Script Host, Powershell, Command Prompt ve Microsoft HTML Application Host vb.) erişimi engellenmeli veya kısıtlanmalıdır.	18.10.86.1 (L2) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' 18.10.86.2 (L2) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled'

4.1.9.1. PowerShell Script Komut Günlüğü Yapılandırılması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-18.10.86.1 tedbirine göre, PowerShell komutlarının tüm girişlerini kaydederek izlenmesini sağlamak adına bu güvenlik tedbiri maddesi uygulanması gerekmektedir. Powershell, Applications and Services Logs\Microsoft\Windows\PowerShell\Operational Event Log kanalına kaydedilir ve bu kanal, PowerShell komutlarının ne zaman çalıştırıldığını ve hangi komutların kullanıldığını görmek için önemli bilgiler sağlar. Bu özelliğin etkinleştirilmesi (Enabled), güvenlik denetimleri ve olay incelemeleri için oldukça faydalıdır çünkü kötü niyetli aktiviteleri tespit etmek ve saldırıların izini sürmek adına script girişlerinin kaydını tutmak kritik öneme sahiptir.

Bu özelliği etkinleştirdiğinizde, PowerShell tarafından tetiklenen komut bloklarının başlatılma ve sonlandırılma zamanlarını kaydetmek de mümkün olur. Ancak bu özelliği etkinleştirmeniz durumunda yüksek miktarda günlük kaydı üretilir. CIS, bu seçeneğin etkinleştirilmesini tavsiye etmemektedir çünkü büyük bir günlük kaydı hacmi oluşturabilir.

Günlükler, PowerShell saldırıları ile ilgili adli araştırmalar yaparken çok değerli olabilir, çünkü ne tür komutların çalıştırıldığını ve hangi parametrelerin kullanıldığını gösterir. Bu güvenlik özelliği etkinleştirildiğinde, kimlik bilgileri ve hassas bilgiler de günlüklerde yer alabileceği için güvenlik riski oluşturabilir. Microsoft, bu günlüklerin

daha güvenli bir şekilde saklanabilmesi için Korunan Olay Günlüğü (Protected Event Logging) gibi bir özellik sunmaktadır.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "PowerShell Script Komut Günlüğü" özelliğini etkinleştirmek amacıyla kullanılmaktadır. İlk olarak, belirtilen kayıt defteri yolunun (HKLM:\SOFTWARE\Policies\Microsoft\Windows \PowerShell\ScriptBlockLogging) mevcut olup olmadığı kontrol edilir. Eğer yol mevcut değilse, script bu kayıt defteri anahtarını oluşturur. Daha sonra, "EnableScriptBlockLogging" değerini 1 olarak ayarlar, yani PowerShell komut bloklarının günlüklerini kaydetmek için bu özelliği etkinleştirir. Bu, PowerShell ile çalıştırılan komutların kaydının tutulmasını sağlar ve güvenlik izlemesi için oldukça faydalıdır.

```
1. # İlk olarak, belirtilen kayıt defteri yolunun mevcut olup olmadığını kontrol ediyoruz.
2. $sonuc1 = (Test-Path -Path
HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging)
3.
4. # Eğer belirtilen yol mevcut değilse, yeni bir kayıt defteri anahtarı oluşturuyoruz.
5. If ($sonuc1 -ne $true){
6.       New-Item -Path
HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging -Force
7. }
8.
9. # Kayıt defteri yolunda 'EnableScriptBlockLogging' değerini 1 olarak ayarlıyoruz
(Script Block Logging'i etkinleştiriyoruz).
10. Set-ItemProperty -Path
'HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging' -Name
'EnableScriptBlockLogging' -Value 1 -Force -PassThru
```

4.1.9.2. PowerShell Komut Günlüğü Yapılandırılması

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-18.10.86.2 tedbirine göre, bu güvenlik politikası, Windows PowerShell komutlarının giriş ve çıkışlarını metin tabanlı transkriptler olarak kaydetmeyi sağlar. Bu özellik etkinleştirildiğinde, PowerShell komutlarının her biri, çalıştırılmadan önce ve sonrasında kaydedilen bir metin dosyasına yazılır. Bu özellik PowerShell ile yapılmış saldırıları veya şüpheli aktiviteleri izlemek ve adli araştırmalar yapmak için son derece değerli olabilir.

Bu özelliğin etkinleştirilmesi, her kullanıcının Belgelerim (My Documents) klasöründe, her gün için ayrı bir alt klasör içerisinde PowerShell_transcript adıyla günlüklerin kaydedilmesini sağlar. İsterseniz farklı bir klasör yolu belirleyebilir ve tüm

transkriptlerin o dizine kaydedilmesini sağlayabilirsiniz. Ancak PowerShell transkript günlükleri, kullanıcının dosyalarına kaydedildiği için başka kullanıcıların bu dosyaları okuma yetkisi olması durumunda şifreler ve diğer hassas bilgiler ifşa oluşturabileceği için önemli bir güvenlik riski oluşturur.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "PowerShell Komut Günlüğü" özelliğini etkinleştirir ve komutların giriş ve çıkışlarını metin tabanlı transkriptler olarak kaydetmek amacıyla kullanılır. İlk olarak, belirtilen kayıt defteri yolu (HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription) kontrol edilir. Eğer bu yol mevcut değilse, script bu kayıt defteri anahtarını oluşturur. Ardından, "EnableTranscripting" değerini 1 olarak ayarlayarak PowerShell komutlarının transkriptlerini etkinleştirir. Bu, her PowerShell komutunun giriş ve çıkışlarının metin dosyasına kaydedilmesini sağlar. Ancak, bu günlükler kullanıcıların dosyalarına kaydedildiği için güvenlik riskleri oluşturabilir, özellikle şifreler ve hassas bilgilerin ifşa edilmesi durumunda. Bu nedenle, dosyaların güvenli bir şekilde saklanması ve izlenmesi önemlidir.

```
1. # İlk olarak, belirtilen kayıt defteri yolunun mevcut olup olmadığını kontrol ediyoruz.
2. $sonuc2 = (Test-Path -Path
HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription)
3.
4. # Eğer belirtilen yol mevcut değilse, yeni bir kayıt defteri anahtarı oluşturuyoruz.
5. If ($sonuc2 -ne $true){
6.       New-Item -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription
-Force
7. }
8.
9. # Kayıt defteri yolunda 'EnableTranscripting' değerini 1 olarak ayarlıyoruz (PowerShell
Transcription'ı etkinleştiriyoruz).
10. Set-ItemProperty -Path
'HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription' -Name
'EnableTranscripting' -Value 1 -Force -PassThru
```

4.1.10. Aktif Dizin Sorguları Güvenliği

Windows sistemlerinde, aktif dizin sorguları LDAP (Lightweight Directory Access Protocol) protokolü yerine güvenli LDAPs (LDAP over SSL) protokolü ile yapılacak şekilde yapılandırılmalıdır. LDAPs protokolü, verilerin şifreli bir şekilde iletilmesini sağlayarak, aktif dizin sorgularının güvenliğini artırır ve potansiyel siber saldırılara karşı koruma sağlar. Bu konfigürasyon hassas bilgilerin korunmasına yardımcı olur ve iletişimdeki gizliliği sağlar.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayanarak, LDAP protokolünün güvenli bir versiyonu olan LDAPs ile değiştirilmesini önerir. “Aktif Dizin Sorguları Güvenliği” tedbiri, LDAPs protokolünün kullanımını teşvik eder ve aktif dizin sorgularının güvenli bir şekilde gerçekleştirilmesini sağlar. Bu önlem ağ içindeki veri iletimini güvenli hale getirerek potansiyel tehditlere karşı ek bir savunma katmanı oluşturur.

CIS Benchmark v3.0.0-2.3.5.3 (L1) Ensure ‘Domain controller: LDAP server channel binding token requirements’ is set to ‘Always’ (DC Only) maddesine karşılık gelmektedir ve sadece Etki Alanı Yönetim Sunucusu-Domain Controller (DC) tarafında uygulanmaktadır. Bu çalışmada, bu tedbir başlığı için Microsoft Windows 10 Enterprise işletim sistemi üzerinde etki alanına dahil olmadan BİGR maddesi ile CIS maddesinin karşılık gelen 1 tedbir maddesi bulunmaktadır. Çizelge 4.10’da, BİGR 5.1.3.10 maddesi, Aktif Dizin Sorguları Güvenliği tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.10. Windows işletim sistemi aktif dizin sorguları güvenliği

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.10	Aktif Dizin Sorguları Güvenliği	Aktif dizin sorguları LDAP protokolü yerine güvenli LDAPs protokolü ile yapılacak şekilde konfigüre edilmelidir. Bk. Tedbir No: 3.2.9.1	18.4.8 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'

4.1.10.1. NetBT NodeType Yapılandırması

“NetBT NodeType Configuration” politikası, NetBIOS over TCP/IP (NetBT) kullanılarak ad çözümleme ve ad kaydının hangi yöntemle yapılacağını belirler. NetBIOS, ağ üzerinde cihazların birbirini tanıması ve iletişim kurabilmesi için kullanılan bir protokoldür. NetBT, TCP/IP üzerinde NetBIOS adlarını çözmek ve bu adları kaydetmek için çeşitli yöntemler sunar.

Eğer sistemde NetBIOS adresinin adını çözümleme için WINS sunucusu yapılandırılmamışsa veya sunucuya ulaşılamıyorsa ve çözülmek istenen ana bilgisayar adı yerel önbellekte, LMHOSTS veya HOSTS dosyalarında tanımlı değilse, NetBIOS ad çözümlemesi başarısız olur. Ancak WINS sunucusu sağlandığında, P-node yöntemiyle ad çözümlemesi güvenli bir şekilde yapılabilir. Bu iyileştirme modeli kapsamında, CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-18.4.8 tedbiri için uygulanmaktadır.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, NetBT NodeType yapılandırmasını düzenler. İlk olarak, belirtilen kayıt defteri yolu (HKLM:\System\CurrentControlSet\Services\ Netbt\Parameters) kontrol edilir. Eğer bu kayıt defteri anahtarı mevcut değilse, script yeni bir anahtar oluşturur. Ardından, bu anahtarda NodeType değerini 2 olarak ayarlar. Bu, NetBIOS ad çözümleme yöntemini belirler. NodeType değerinin 2 olarak ayarlanması, P-node (Point-to-Point) yöntemiyle ad çözümlemesi yapılmasını sağlar. Bu yöntem, ağdaki cihazların birbirlerini tanıyabilmesi için güvenli bir çözümleme şeklidir ve genellikle WINS sunucusunun sağlandığı ağlarda kullanılır.

```
1. $sonuc8 = (Test-Path -Path 'HKLM:\System\CurrentControlSet\Services\Netbt\Parameters')
2. # Netbt\Parameters yolunda belirtilen kayıt defteri anahtarının var olup olmadığını
kontrol et
3.
4. If ($sonuc8 -ne $true){
5.      # Eğer anahtar mevcut değilse, yeni bir anahtar oluştur
6.      New-Item -Path 'HKLM:\System\CurrentControlSet\Services\Netbt\Parameters' -Force
7. }
8.
9. # Netbt\Parameters anahtarındaki NodeType değerini 2 olarak ayarla
10. Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\Netbt\Parameters' -
Name 'NodeType' -Value 2 -Force -PassThru
```

4.1.11. Yönetici Hesaplarının İzlenmesi

Windows sistemlerinde, ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ile oturum açma ve kapama işlemleri düzenli olarak izlenmelidir. Bu tür işlemler, yüksek yetkili hesapların kötüye kullanımını veya izinsiz erişim girişimlerini tespit etmek için kritik öneme sahiptir. Yönetici hesaplarının etkinliklerinin izlenmesi, sistemin güvenliğini artırır ve potansiyel tehditlere karşı erken uyarı sağlar.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayalı olarak, yönetici hesaplarının etkinliklerini izlemeyi önerir. "Yönetici Hesaplarının İzlenmesi" tedbiri, ayrıcalıklı etki alanı gruplarına yapılan kullanıcı ekleme ve çıkarma işlemleri ile oturum açma ve kapama işlemlerinin izlenmesini ve kaydının tutulmasını öngörür. Bu, güvenlik olaylarının doğru bir şekilde tespit edilmesine ve şüpheli etkinliklerin hızlıca analiz edilmesine olanak tanır. Çizelge 4.11'de, BİGR 5.1.3.11 maddesi, Yönetici Hesaplarının İzlenmesi tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.11. Windows işletim sistemi yönetici hesaplarının izlenmesi

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.11	Yönetici Hesaplarının İzlenmesi	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmelidir. Bk. Tedbir No: 3.1.12.11	17.2.1 (L1)' Ensure 'Audit Application Group Management' is set to 'Success and Failure' 17.2.2 (L1) Ensure 'Audit Security Group Management' is set to include 'Success' 17.2.3 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'

4.1.11.1. Uygulama Grup Yönetimi Denetimi Politikası

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-17.2.1. maddesi olarak "Audit Application Group Management" politikası, Windows işletim sistemi üzerinde uygulama gruplarına yapılan değişikliklerin denetlenmesine olanak tanır. Bu politika, uygulama gruplarının oluşturulması, değiştirilmesi, silinmesi, üyelerin eklenmesi veya çıkarılması gibi önemli olayları izler. Uygulama grupları, Microsoft tarafından geliştirilen Windows Authorization Manager tarafından kullanılan bir bileşendir ve bu bileşen, uygulamalara rol tabanlı erişim kontrolü (RBAC) entegrasyonu sağlar. Bu politika ayarının "Success and Failure" olarak yapılandırılması, başarıyla gerçekleştirilen ve başarısız olan tüm denetim olaylarının kaydedilmesini sağlar. Bu tür denetimlerin yapılması özellikle güvenlik olaylarının araştırılması sırasında kritik öneme sahip olabilir.

Windows Authorization Manager, uygulamalara kullanıcı ve grup yönetimini ve uygulama erişimini düzenleyen bir çerçeve sunar. Uygulama gruplarındaki değişiklikler, potansiyel güvenlik açıklarını veya yetkisiz erişim girişimlerini tespit etmek için önemli bir veri kaynağı olabilir. Bu ayarın doğru bir şekilde yapılandırılmaması, organizasyonel güvenlik olaylarının tespit edilememesine veya yetersiz delillerle analizlerinin yapılmasına yol açabilir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "Audit Application Group Management" denetimini yapılandırmak için kullanılır. Komut, uygulama gruplarındaki değişikliklerin başarıyla gerçekleştirilen ve başarısız olan tüm olaylarını kaydetmek üzere Windows güvenlik denetim politikasını ayarlar. AuditPol komutu, "Application Group Management" alt kategorisinde hem başarılı (success:enable) hem de başarısız (failure:enable) olayların kaydedilmesini etkinleştirir. Bu, uygulama grubu yönetimiyle ilgili her türlü değişikliği takip etme ve kaydetme imkânı tanır, böylece güvenlik olayları ve potansiyel yetkisiz erişim girişimleri denetlenebilir. Bu ayarın yapılandırılması, organizasyonun güvenliğini artırarak, kritik güvenlik açıklarını ve güvenlik tehditlerini tespit etmede önemli bir rol oynar.

```
1. # Audit Application Group Management Success ve Failure olarak ayarlama
2. AuditPol /set /subcategory:"Application Group Management" /success:enable
/failure:enable
```

4.1.11.2. Güvenlik Grubu Yönetimi Denetiminin Yapılandırılması

Güvenlik grubu oluşturma, değiştirme, silme veya bir üyenin gruba eklenmesi ya da çıkarılması gibi işlemler, bu denetim aracılığıyla takip edilebilir. Bu denetim politikası etkinleştirildiğinde yöneticiler, güvenlik grubu hesaplarının yetkisiz, kazara veya kötü niyetli bir şekilde oluşturulup oluşturulmadığını tespit edebilirler.

Denetim ayarlarının doğru yapılandırılması, özellikle güvenlik olaylarının izlenebilirliğini sağlar ve olası kötüye kullanımları erkenden tespit etmeye yardımcı olur. Ancak denetim ayarlarının yetersiz yapılandırılması güvenlik olaylarının zamanında tespit edilememesine veya olay sonrası adli analiz için yeterli kanıt sağlanamamasına yol açabilir.

Özellikle düzenlemelere tabi sektörlerde faaliyet gösteren işletmelerin, belirli olayların veya aktivitelerin kaydını tutma yasal zorunluluğu olabilir. Bu nedenle, güvenlik grubu yönetimi ile ilgili denetim ayarlarının doğru bir şekilde yapılandırılması hem güvenlik ihlallerinin önlenmesi hem de yasal gerekliliklerin yerine getirilmesi açısından kritik öneme sahiptir. Bu ayar, yapılan incelemelerde etkinleştirildiği için iyileştirme modelinde uygulanan sıkılaştırma kodu yazılmasına ihtiyaç duyulmamıştır.

4.1.11.3. Kullanıcı Hesabı Yönetimi Denetimi Politikası

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0-17.2.3. maddesi olarak "Audit User Account Management" politikası, kullanıcı hesaplarının yönetimiyle ilgili her olayı denetler. Bu olaylar arasında bir kullanıcı hesabının oluşturulması, değiştirilmesi, silinmesi, adının değiştirilmesi, devre dışı bırakılması veya etkinleştirilmesi, şifrelerin ayarlanması veya değiştirilmesi yer alır. Bu denetim politikası etkinleştirildiğinde, yöneticiler, kötü niyetli bilgisayar korsanlarını, kazara yapılan işlemleri veya yetkisiz kullanıcı hesapları oluşturma girişimlerini tespit etmek için bu olayları takip edebilir.

Aşağıda bulunan iyileştirme modelindeki PowerShell scripti, "Audit User Account Management" denetimini yapılandırmak için kullanılır. Komut, kullanıcı hesaplarıyla ilgili yönetim işlemlerinin başarıyla gerçekleşen ve başarısız olan tüm olaylarını kaydetmek üzere Windows güvenlik denetim politikasını ayarlar. AuditPol komutu, User Account Management alt kategorisinde hem başarılı (success:enable) hem de başarısız (failure:enable) işlemlerin denetlenmesini etkinleştirir. Bu denetim, kullanıcı hesaplarının oluşturulması, değiştirilmesi, silinmesi, adlarının değiştirilmesi, etkinleştirilmesi veya devre dışı bırakılması gibi işlemleri kapsar.

```
1. # Audit User Account Management Success ve Failure olarak ayarlama
2. AuditPol /set /subcategory:"User Account Management" /success:enable /failure:enable
```

4.1.12. Güvenli Yönetici İş İstasyonu Kullanımı

Windows sistemlerinde, etki alanı yönetimini (Domain Controller) gerçekleştirmek için yalnızca güvenli bir yönetici iş istasyonu kullanılmalıdır. Bu iş

istasyonu, yalnızca yönetimsel görevler için kullanılmalı ve ek yazılım veya rol yüklenmemelidir.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayalı olarak, güvenli yönetici iş istasyonlarının kullanımını önerir. Yönetici iş istasyonunun yalnızca gerekli güvenlik işlevlerini yerine getirmesini sağlar ve potansiyel saldırı yüzeylerini minimize eder. "Güvenli Yönetici İş İstasyonu Kullanımı" tedbiri, yalnızca etki alanı yönetimi için kullanılan bu istasyonların, ek uygulamalar ve internet gibi potansiyel tehditlerden izole edilmesini vurgular. Bu önlem, yönetici iş istasyonlarının daha güvenli bir şekilde kullanılmasını sağlayarak sistemin siber tehditlere karşı korunmasına yardımcı olur.

CIS Benchmark v3.0.0-2.3.5.1 (L1) "Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only)" maddesi, etki alanı denetleyicisi (Domain Controller - DC) üzerinde sunucu operatörlerinin zamanlanmış görevler oluşturmasına izin verilmemesi gerektiğini belirtmektedir. Bu ayar kötü niyetli kullanıcıların veya yetkisiz kişilerin zamanlanmış görevler oluşturmasını engellemek amacıyla "Disabled" olarak yapılandırılmalıdır. Bu yapılandırma, yalnızca Etki Alanı Yönetim Sunucusu (DC) üzerinde uygulanmalıdır.

CIS Benchmark v3.0.0-2.3.5.2 (L1) "Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only)" maddesi, Netlogon üzerinden yapılan güvenli kanal bağlantılarının zayıf güvenlik protokollerine izin verilmesini engellemek için "Not Configured" olarak bırakılmasını tavsiye etmektedir. Bu yapılandırma, yalnızca Etki Alanı Yönetim Sunucusu (DC) üzerinde uygulanmalıdır.

CIS Benchmark v3.0.0-2.3.5.3 (L1) "Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only)" maddesi, LDAP sunucusu üzerinden yapılan bağlantıların güvenliğini artırmak amacıyla kanal bağlama token'larının her zaman kullanılmasını zorunlu kılmaktadır. Bu ayarın etkinleştirilmesi, man-in-the-middle (MITM) saldırılarına karşı koruma sağlarken, yalnızca DC üzerinde geçerlidir.

Benzer şekilde, CIS Benchmark v3.0.0-2.3.5.4 (L1) “Ensure ‘Domain controller: LDAP server signing requirements’ is set to ‘Require signing’ (DC only)” maddesi, LDAP sunucusundan yapılan tüm iletişimlerin dijital imza ile güvence altına alınmasını zorunlu kılarak, veri bütünlüğü ve güvenliği sağlar. Bu yapılandırma da yalnızca DC tarafında uygulanmalıdır.

CIS Benchmark v3.0.0-2.3.5.5 (L1) “Ensure ‘Domain controller: Refuse machine account password changes’ is set to ‘Disabled’ (DC only)” maddesi, etki alanı denetleyicisinin makine hesaplarının şifre değişikliklerine izin vermesini sağlamak amacıyla bu ayarın “Disabled” olarak yapılandırılması gerektiğini belirtmektedir. Bu, şifre değişimlerinin doğru şekilde yapılabilmesi için gereklidir ve yalnızca DC üzerinde uygulanır.

İyileştirme modeli için CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 tedbirleri üzerinde herhangi bir eşleşen kural bulunmamaktadır. Bu durumdan kaynaklı olarak Çizelge 4.12’te eşleştirmesi yapılamamıştır.

Çizelge 4.12. Windows işletim sistemi güvenli yönetici iş istasyonu kullanımı

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.12	Güvenli Yönetici İş İstasyonu Kullanımı	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu konumlandırılmalı, ek yazılım veya rol yüklenmemeli, eposta, internet vb. erişimleri için kullanılmamalıdır.	Bulunmamaktadır.

4.1.13. Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi

Aktif dizinde devre dışı bırakılan kullanıcı hesaplarının e-posta erişimi devre dışı bırakılmalıdır. Özellikle devre dışı bırakılan hesaplar için ActiveSync e-posta

erişimi, kullanıcı hesabı geçerli olmadığı anda hemen engellenmelidir. Bu tedbir devre dışı bırakılan hesapların kötüye kullanımını önler ve güvenlik risklerini minimize eder.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayanarak, devre dışı bırakılan hesapların mail erişiminin kesilmesi gerektiğini belirtir. "Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi" tedbiri, devre dışı bırakılan hesapların e-posta erişiminin hemen durdurulmasını önerir. Bu önlem olası siber tehditlere karşı sistemin güvenliğini artırır ve yetkisiz erişimlerin önüne geçilmesini sağlar. Windows işletim sisteminde, etki alanına bağlı sunucular için düzenlenmiş olan Etki Alanı Sıkılaştırma Güvenliği kapsamında değerlendirilmesi gerekmektedir. Bu çalışmada, bu tedbir başlığı için Microsoft Windows 10 Enterprise işletim sistemi üzerinde BİGR maddesi ile CIS maddesinin karşılık tedbiri bulunmamaktadır. Bu durumdan kaynaklı olarak Çizelge 4.13'te eşleştirmesi yapılamamıştır.

Çizelge 4.13. Windows işletim sistemi devre dışı bırakılan hesabın mail erişiminin engellenmesi

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 – (L1&L2)**
5.1.3.13	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmelidir.	Bulunmamaktadır.

4.2. GNU/Linux İşletim Sistemi

4.2.1. Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi

En iyi güvenlik uygulamalarına dayanan bir sistem yönetimi yaklaşımı, gereksiz dosya sistemlerinin aktif olmasını engellemeyi içerir. Bu tedbir sistemin potansiyel saldırılara karşı daha dayanıklı olmasını sağlar.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), bir kurumun mevcut güvenlik durumunu değerlendirirken, CIS (Center for Internet Security) denetimlerini temel alır

ve bu denetimler sistemin en iyi güvenlik uygulamalarına ne kadar uyduğunu ölçer. "Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi" tedbiri, CIS denetimlerinin bir parçası olarak, gereksiz dosya sistemlerinin aktif olmasının engellenmesini önermektedir. Çizelge 4.14'te, BİGR 5.1.2.1 maddesi, Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.14. GNU/Linux işletim sistemi kullanılmayan dosya sistemlerinin pasif hale getirilmesi

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1**
5.1.2.1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) pasif hale getirilmelidir.	1.1.1.1 Ensure mounting of cramfs filesystems is disabled 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled 1.1.1.3 Ensure mounting of jffs2 filesystems is disabled 1.1.1.4 Ensure mounting of hfs filesystems is disabled 1.1.1.5 Ensure mounting of hfsplus filesystems is disabled 1.1.1.6 Ensure mounting of squashfs filesystems is disabled 1.1.1.7 Ensure mounting of udf filesystems is disabled

4.2.1.1. Cramfs Modülü Sıkılaştırma

CIS Benchmark v2.0.1-1.1.1.1 "Ensure mounting of cramfs filesystems is disabled" maddesi, Linux tabanlı sistemlerde kullanılan cramfs (Compressed ROM File System) dosya sisteminin devre dışı bırakılmasını önermektedir. Cramfs, sıkıştırılmış, salt okunur bir dosya sistemi olup, genellikle düşük kaynak tüketimi gerektiren gömülü sistemler ve küçük aygıtlar gibi ortamlarda kullanılır. Bu dosya sistemi, verilerin sıkıştırılarak depolanmasına olanak tanır ve sistemin depolama alanını daha verimli kullanmasını sağlar. Cramfs dosya sistemi, birçok modern Linux dağıtımında yer almaz ve kullanım alanı giderek azalmaktadır.

Cramfs dosya sistemi, genellikle dosya sistemine erişim sağlayan araçlar veya yazılımlar tarafından yüklenir. Eğer sistemde cramfs desteği aktifse, kötü niyetli kullanıcılar bu dosya sistemini kullanarak çeşitli saldırılar gerçekleştirebilir. Örneğin, bir saldırgan cramfs dosya sistemini sistemin bir parçası olarak yükleyebilir ve burada zararlı yazılımlar barındırabilir. Ayrıca cramfs sistemi üzerinden erişilen veriler,

sıkıştırılmış halde olsa da potansiyel olarak açılabilir ve manipüle edilebilir. Bu da güvenlik açıklarına yol açabilir.

Bu sebeple, sistemde cramfs dosya sistemine gerek yoksa, bu özelliğin devre dışı bırakılması önerilir. Böylece bu dosya sistemine dair potansiyel güvenlik açıkları engellenmiş olur. Sistemde cramfs desteğini devre dışı bırakmak, özellikle sadece gerekli dosya sistemlerinin kullanımda olmasını sağlamak açısından önemlidir. Sistemde gereksiz modüllerin yüklenmesini engelleyerek, kötü niyetli yazılımların veya güvenlik açıklarının hedef alacağı daha küçük bir yüzey bırakır.

Sistem yöneticileri, cramfs modülünü devre dışı bırakmak için belirli yapılandırmalar yapabilir. Bunlar arasında cramfs modülünün yüklenmesini engellemek için /etc/modprobe.d/ dizininde ilgili yapılandırma dosyaları oluşturmak, bu modülün blacklist (yasaklı liste) içine alınması ve sistemde aktifse, modülün kernel'den kaldırılması yer alır. Alınacak önlemler sistemin güvenliğini artırarak, istenmeyen dosya sistemlerinin kullanımını engeller ve yalnızca gereken dosya sistemlerinin aktif olmasını sağlar.

İyileştirme yöntemi olarak bu güvenlik önlemi, gereksiz dosya sistemleri ve modüllerle ilgili riskleri ortadan kaldırarak Linux tabanlı sistemlerin güvenliğini artırmaya yardımcı olur ve sistemin saldırılara karşı daha dirençli olmasını sağlar.

Aşağıda bulunan iyileştirme modelindeki bash komutu, GNU/Linux sistemlerinde cramfs dosya sisteminin yüklenmesini engellemeyi amaçlar. Komut, cramfs modülünün sistemdeki tüm dizinlerde mevcut olup olmadığını kontrol eder ve eğer varsa, bu modülün yüklenmesini engellemek için gerekli adımları atar. İlk olarak, /etc/modprobe.d/ dizininde cramfs modülünü yasaklamak için bir konfigürasyon dosyası oluşturur ve modülün yüklenmesini engellemek amacıyla install cramfs /bin/false satırını ekler. Ardından, eğer cramfs modülü yüklenmişse, modprobe -r cramfs komutunu kullanarak modül sistemden kaldırılır. Ayrıca, modül blacklist'e eklenmemişse, blacklist cramfs komutuyla blacklist'e eklenir. Bu işlem, sistemde sadece gerekli modüllerin aktif olmasını sağlayarak güvenlik risklerini azaltır. Bu sayede, gereksiz modüller devre dışı bırakılır ve sistemin güvenliği artırılır.

```
#!/usr/bin/env bash

{
  l_ad="cramfs"  # Modul adi
  l_tur="fs"      # Modul turu (dosya sistemi)
  l_yol="/lib/modules/**/kernel/$l_tur"  # Modul dizin yolları
  l_padi="$(tr '-' '_' <<< "$l_ad")"     # Modul adini daha uygun hale getir
  l_dizinadi="$(tr '-' '/' <<< "$l_ad")"      # Dizin adi olustur

   # Modul yuklenmesini engelleyen fonksiyon
   modul_yuklenebilir_fix() {
     l_yuklenebilir="$(modprobe -n -v "$l_ad")"
     [ "$(wc -l <<< "$l_yuklenebilir")" -gt "1" ] && l_yuklenebilir="$(grep -P --
"(^\h*install|\b$l_ad)\b" <<< "$l_yuklenebilir")"

     if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_yuklenebilir"; then
       echo -e "\n - \"$l_ad\" modulunun yuklenmesini engelliyorum"
       echo -e "install $l_ad /bin/false" >> /etc/modprobe.d/"$l_padi".conf
     fi
   }

   # Modul yuklenmisse, yuklemeyi kaldirma fonksiyonu
   modul_yuklendi_fix() {
     if lsmod | grep "$l_ad" > /dev/null 2>&1; then
       echo -e "\n - \"$l_ad\" modulunu yukluden kaldiriyorum"
       modprobe -r "$l_ad"
     fi
   }

   # Modul blacklist'e eklenmemisse, blacklist'e ekleme fonksiyonu
   modul_engelle_fix() {
     if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_padi\b"; then
       echo -e "\n - \"$l_ad\" modulunu blacklist'e ekliyorum"
       echo -e "blacklist $l_ad" >> /etc/modprobe.d/"$l_padi".conf
     fi
   }

   # Modul sistemde mevcut mu kontrol etme ve engellemeyi saglama
   for l_dizin in $l_yol; do
     if [ -d "$l_dizin/$l_dizinadi" ] && [ -n "$(ls -A $l_dizin/$l_dizinadi)" ]; then
       echo -e "\n - \"$l_ad\" modulu \"$l_dizin\" dizininde mevcut\n - Engellenip
engellenmedigini kontrol ediyorum..."
       modul_engelle_fix

       if [ "$l_dizin" = "/lib/modules/$(uname -r)/kernel/$l_tur" ]; then
         modul_yuklenebilir_fix
         modul_yuklendi_fix
       fi
     else
       echo -e "\n - \"$l_ad\" modulu \"$l_dizin\" dizininde mevcut degil\n"
     fi
   done

   echo -e "\n - \"$l_ad\" modulunun engellenmesi tamamlandi\n"
}
```

4.2.1.2. Freevxfs Modülü Sıkılaştırma

Freevxfs dosya sistemi CIS Benchmark v2.0.1-1.1.1.2 maddesi altında bulunmaktadır. Freevxfs özellikle HP-UX işletim sistemlerinde kullanılan bir dosya sistemidir ve Linux sistemlerinde yaygın olarak kullanılmaz. Freevxfs, Veritas tarafından geliştirilmiş olan ve yalnızca bazı özel Linux dağıtımlarında mevcut olan bir

dosya sistemidir. Ancak modern Linux sistemlerinde çoğunlukla gereksizdir ve desteklenmesi sistemde gereksiz bir saldırı yüzeyi oluşturur. Yani gereksiz dosya sistemlerinin etkin olması kötü niyetli kişilerin sisteme zarar vermek için kullanabileceği potansiyel açıkları ortaya çıkarabilir.

Bu dosya sistemi genellikle büyük sistemler veya HP-UX tabanlı özel ortamlar için kullanıldığından, çoğu GNU/Linux dağıtımında kullanılmaz. Sistemde mevcut olmayan veya kullanılmayan modüllerin desteklenmesi sadece güvenlik risklerini artırır ve sistemde yer kaplayan gereksiz modüllerle ilgili yönetimsel zorluklara yol açabilir. Freevxfs dosya sistemine desteğin kaldırılması sistemde potansiyel tehditleri engellemenin etkili bir yoludur.

Eğer Freevxfs dosya sistemi modülü sistemde yüklüyse bu modülün devre dışı bırakılması gereklidir. Bunu yapmak için modül yüklenmesinin engellenmesi gerekir. Ayrıca sistemde yüklü olan çekirdek (kernel) üzerinde bu modül kaldırılmalıdır. Bunun için "/etc/modprobe.d/" dizininde ilgili modülün yüklenmesini engelleyen konfigürasyon dosyaları oluşturulabilir. Bu dosyalar modülün yüklenmesini engelleyerek sistemi yalnızca gerekli ve güvenli modüllerle çalışacak şekilde yapılandırılmasını sağlar.

İyileştirme yöntemi olarak bu güvenlik önlemi için Freevxfs dosya sisteminin sistemde etkin olmaması sağlanarak, Linux sistemleri gereksiz güvenlik risklerinden arındırılabilir. Saldırı yüzeyini küçültür ve sadece gerekli dosya sistemlerinin aktif olduğu daha güvenli bir çalışma ortamı oluşturur. Sistemde yalnızca kullanılan ve güvenli dosya sistemlerinin bulundurulması güvenlik tehditlerine karşı önemli bir koruma sağlar.

Aşağıda bulunan iyileştirme modelindeki bash komutu, Freevxfs dosya sistemi modülünün sistemde yüklenmesini engellemek amacıyla kullanılır. Komut, Freevxfs modülünün mevcut olup olmadığını kontrol eder, yüklü ise modülü sistemden kaldırır ve modülün yüklenmesini engellemek için /etc/modprobe.d/ dizininde bir konfigürasyon dosyası oluşturur. Bu dosya, modülün yüklenmesini install freevxfs /bin/false komutuyla engeller. Ayrıca, modül sistemde blacklist'e eklenmemişse, bu modül blacklist'e eklenir. Bu sayede, Freevxfs dosya sistemi modülünün yüklenmesi tamamen

engellenmiş olur ve sistemde yalnızca gerekli modüllerin aktif olmasına olanak tanır. Bu güvenlik önlemi, sistemde gereksiz modüllerin etkin olmasının önüne geçerek, saldırı yüzeyini küçültür ve sistemin güvenliğini artırır.

```
1. #!/usr/bin/env bash
2.
3. {
4.   l_mad="freevxfs"  # Modul adi
5.   l_mtur="fs"        # Modul turu (dosya sistemi)
6.   l_myol="/lib/modules/**/kernel/$l_mtur"  # Modul dizin yollari
7.   l_madp="$(tr '-' '_' <<< "$l_mad")"     # Modul adini uygun hale getirme
8.   l_mndir="$(tr '-' '/' <<< "$l_mad")"      # Modul dizini istenen formatta olusturma
9.
10.   # Modulun yuklenmesini engelleme fonksiyonu
11.   modul_yuklenebilir_fix() {
12.     l_yuklenebilir="$(modprobe -n -v "$l_mad")"
13.     [ "$(wc -l <<< "$l_yuklenebilir")" -gt "1" ] && l_yuklenebilir="$(grep -P --
"(^\h*install|\b$l_mad)\b" <<< "$l_yuklenebilir")"
14.
15.     if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_yuklenebilir"; then
16.       echo -e "\n - \"$l_mad\" modulunun yuklenmesini engelliyorum"
17.       echo -e "install $l_mad /bin/false" >> /etc/modprobe.d/"$l_madp".conf
18.     fi
19.   }
20.
21.   # Modul yuklendi ise, yuklemeyi kaldirma fonksiyonu
22.   modul_yuklendi_fix() {
23.     if lsmod | grep "$l_mad" > /dev/null 2>&1; then
24.       echo -e "\n - \"$l_mad\" modulunu yukluden kaldiriyorum"
25.       modprobe -r "$l_mad"
26.     fi
27.   }
28.
29.   # Modul blacklist'e eklenmemisse, blacklist'e ekleme fonksiyonu
30.   modul_engelle_fix() {
31.     if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_madp\b"; then
32.       echo -e "\n - \"$l_mad\" modulunu blacklist'e ekliyorum"
33.       echo -e "blacklist $l_mad" >> /etc/modprobe.d/"$l_madp".conf
34.     fi
35.   }
36.
37.   # Modulun sistemde olup olmadigini kontrol etme ve engellemeyi saglama
38.   for l_mdir in $l_myol; do
39.     if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
40.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut\n - Engellenip
engellenmedigini kontrol ediyorum..."
41.       modul_engelle_fix
42.
43.       if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtur" ]; then
44.         modul_yuklenebilir_fix
45.         modul_yuklendi_fix
46.       fi
47.     else
48.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut degil\n"
49.     fi
50.   done
51.
52.   echo -e "\n - \"$l_mad\" modulunun engellenmesi tamamlandi\n"
53. }
```

4.2.1.3. Jffs2 Modülü Sıkılaştırma

JFFS2 (Journaling Flash File System 2) özellikle USB bellek gibi sık yazma/okuma işlemleri gerektiren ortamlar için tasarlanmış bir dosya sistemi türüdür. Bu dosya sistemi verilerin kaybolmaması için jurnal (kayıt) tutma özelliğine sahip olup, özellikle taşınabilir cihazlar ve gömülü sistemler için kullanılır. JFFS2 dosya sistemi, log-structured (günlük yapılı dosya sistemi) bir yapı kullanarak veri yazma işlemlerini verimli hale getirmeyi amaçlar. Ancak çoğu modern Linux sunucu sistemlerinde ve masaüstü ortamlarında kullanılmaz ve bu sistemler genellikle HDD veya SSD gibi daha güçlü ve büyük depolama ortamlarıyla çalışmaktadır.

Bu tür dosya sistemlerinin desteği sistemde gereksiz bir güvenlik riskine yol açabilir. Herhangi bir dosya sistemi tipi işlevsel değilse ve gereksizse dışarıdan yapılabilecek kötü niyetli saldırılar için bir saldırı yüzeyi oluşturur. Bu nedenle JFFS2 gibi kullanılmayan dosya sistemlerinin devre dışı bırakılması önerilmektedir. Böylece sistemin saldırılara karşı daha güvenli hale gelmesi sağlanır.

JFFS2 dosya sistemi, yalnızca bazı özel durumlarda kullanılır dolayısıyla çoğu Linux sisteminde bu dosya sistemine destek verilmemelidir. Eğer bu dosya sistemi sistemde bulunuyorsa özellikle kernel seviyesinde bu modülün devre dışı bırakılması gereklidir. Bunun için "/etc/modprobe.d/" dizinine uygun konfigürasyon dosyaları eklenebilir. Bu dosyalar modülün yüklenmesini engeller ve mevcutsa modülün sistemden kaldırılmasını sağlar.

CIS Benchmark v2.0.1-1.1.1.3 maddesi gereği, JFFS2 dosya sisteminin gereksiz olduğu sistemlerde devre dışı bırakılması, sistemin güvenliğini artırmak için kritik bir adımdır. Bu gereksiz modüllerin yüklenmesinin önüne geçer ve potansiyel saldırı yüzeyini azaltır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, JFFS2 (Journaling Flash File System 2) dosya sistemi modülünün sistemde etkin olmasını engellemek için kullanılır. Komut, JFFS2 modülünün mevcut olup olmadığını kontrol eder ve eğer modül yüklü ise bu modülün sistemden kaldırılmasını sağlar. Ayrıca, JFFS2 modülünün yüklenmesini engellemek için /etc/modprobe.d/ dizininde bir konfigürasyon dosyası

oluşturulur. Bu dosya, modülün yüklenmesini install jffs2 /bin/false komutuyla engeller. Modül sistemde blacklist'e eklenmemişse, modül blacklist'e de eklenir. Bu adımlar, sistemde gereksiz ve kullanılmayan dosya sistemlerinin etkin olmasını engelleyerek güvenlik risklerini azaltır ve saldırı yüzeyini küçültür. Bu güvenlik önlemi, yalnızca gerekli ve güvenli modüllerin sistemde bulundurulmasını sağlar, böylece sistemin güvenliği artırılır.

```
1. #!/usr/bin/env bash
2.
3. {
4.   l_mad="jffs2"  # Modul adi
5.   l_mtur="fs"     # Modul turu (dosya sistemi)
6.   l_myol="/lib/modules/**/kernel/$l_mtur"  # Modul dizin yollari
7.   l_madp="$(tr '-' '_' <<< "$l_mad")"     # Modul adini uygun hale getirme
8.   l_mndir="$(tr '-' '/' <<< "$l_mad")"      # Modul dizini istenen formatta olusturma
9.
10.   # Modulun yuklenmesini engelleme fonksiyonu
11.   modul_yuklenebilir_fix() {
12.     l_yuklenebilir="$(modprobe -n -v "$l_mad")"
13.     [ "$(wc -l <<< "$l_yuklenebilir")" -gt "1" ] && l_yuklenebilir="$(grep -P --
"(^\h*install|\b$l_mad)\b" <<< "$l_yuklenebilir")"
14.
15.     if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_yuklenebilir"; then
16.       echo -e "\n - \"$l_mad\" modulunun yuklenmesini engelliyorum"
17.       echo -e "install $l_mad /bin/false" >> /etc/modprobe.d/"$l_madp".conf
18.     fi
19.   }
20.
21.   # Modul yuklendi ise, yuklemeyi kaldirma fonksiyonu
22.   modul_yuklendi_fix() {
23.     if lsmod | grep "$l_mad" > /dev/null 2>&1; then
24.       echo -e "\n - \"$l_mad\" modulunu yukluden kaldiriyorum"
25.       modprobe -r "$l_mad"
26.     fi
27.   }
28.
29.   # Modul blacklist'e eklenmemisse, blacklist'e ekleme fonksiyonu
30.   modul_engelle_fix() {
31.     if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_madp\b"; then
32.       echo -e "\n - \"$l_mad\" modulunu blacklist'e ekliyorum"
33.       echo -e "blacklist $l_mad" >> /etc/modprobe.d/"$l_madp".conf
34.     fi
35.   }
36.
37.   # Modulun sistemde olup olmadigini kontrol etme ve engellemeyi saglama
38.   for l_mdir in $l_myol; do
39.     if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
40.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut\n - Engellenip
engellenmedigini kontrol ediyorum..."
41.       modul_engelle_fix
42.
43.       if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtur" ]; then
44.         modul_yuklenebilir_fix
45.         modul_yuklendi_fix
46.       fi
47.     else
48.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut degil\n"
49.     fi
50.   done
51.
52.   echo -e "\n - \"$l_mad\" modulunun engellenmesi tamamlandi\n"
53. }
```

4.2.1.4. Hfs Modülü Sıkılaştırma

HFS (Hierarchical File System) özellikle Mac OS işletim sistemlerinde kullanılan bir dosya sistemidir. Bu dosya sistemi, dosyaların ve dizinlerin hiyerarşik bir yapıda düzenlenmesini sağlar ve genellikle macOS işletim sistemlerine özgüdür. HFS, Linux ve diğer Unix tabanlı sistemlerde doğrudan kullanılmaz ancak bu dosya sistemine destek sağlayan modüller bazı durumlarda Mac OS dosya sistemlerine GNU/Linux ortamında okuma ve yazma yeteneği sunar. Ancak çoğu Linux sunucu ve masaüstü kullanıcısı için HFS desteği gereksizdir.

Eğer GNU/Linux sisteminde HFS dosya sistemine gerek yoksa bu tür modüllerin yüklenmesini engellemek güvenliği artırabilir. Gereksiz dosya sistemi türlerinin desteği sistemdeki potansiyel güvenlik açıklarını artırabilir. HFS gibi desteklerin devre dışı bırakılması, sisteme yönelik olası kötü niyetli saldırıları engellemeye yardımcı olabilir. Eğer HFS dosya sistemi sistemde yüklü ise bu modülün devre dışı bırakılması ve yüklenmesinin engellenmesi gerekir.

Bu işlem için, “modprobe” komutu kullanılarak HFS modülü yüklenmeden önce “/etc/modprobe.d/” dizinine gerekli yapılandırma dosyaları eklenebilir. Bu dosyalar modülün yüklenmesini engeller ve mevcutsa modülün sistemden kaldırılmasını sağlar. HFS dosya sistemine dair herhangi bir işlevsellik bulunmadığı sürece bu modülün devre dışı bırakılması sistemin güvenliğini artırır.

CIS Benchmark v2.0.1-1.1.1.4 maddesi gereği, HFS dosya sistemi türünün gereksiz olduğu durumlarda, sistemdeki yükleme engellemeleri ve modül kaldırma işlemleri gerçekleştirilerek sistemdeki gereksiz riskler ortadan kaldırılır. Bu adım sistemin sadece gerekli olan dosya sistemlerini çalıştırmasını sağlar ve güvenlik risklerini minimize eder.

Aşağıda bulunan iyileştirme modelindeki bash komutu, HFS (Hierarchical File System) dosya sistemi modülünün Linux sistemlerinde etkin olmasını engellemek için kullanılır. Komut, HFS modülünün mevcut olup olmadığını kontrol eder ve modül yüklü ise, modülün sistemden kaldırılmasını sağlar. Ayrıca, modülün gelecekte yüklenmesini engellemek için /etc/modprobe.d/ dizinine bir yapılandırma dosyası ekler

ve modülün yüklenmesini install hfs /bin/false komutuyla engeller. Eğer HFS modülü daha önce blacklist'e eklenmemişse, modül blacklist'e de eklenir. Bu adımlar, HFS dosya sistemi desteğinin gereksiz olduğu durumlarda, sistemdeki potansiyel güvenlik açıklarını ve saldırı yüzeylerini azaltarak sistemin güvenliğini artırır.

```
#!/usr/bin/env bash

{
  l_mad="hfs"  # Modul adi
  l_mtur="fs"   # Modul turu (dosya sistemi)
  l_myol="/lib/modules/**/kernel/$l_mtur"  # Modul dizin yollari
  l_madp="$(tr '-' '_' <<< "$l_mad")"     # Modul adini uygun hale getirme
  l_mndir="$(tr '-' '/' <<< "$l_mad")"      # Modul dizini istenen formatta olusturma

   # Modulun yuklenmesini engelleme fonksiyonu
   modul_yuklenebilir_fix() {
     l_yuklenebilir="$(modprobe -n -v "$l_mad")"
     [ "$(wc -l <<< "$l_yuklenebilir")" -gt "1" ] && l_yuklenebilir="$(grep -P --
"(^\h*install|\b$l_mad)\b" <<< "$l_yuklenebilir")"

     if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_yuklenebilir"; then
       echo -e "\n - \"$l_mad\" modulunun yuklenmesini engelliyorum"
       echo -e "install $l_mad /bin/false" >> /etc/modprobe.d/"$l_madp".conf
     fi
   }

   # Modul yuklendi ise, yuklemeyi kaldirma fonksiyonu
   modul_yuklendi_fix() {
     if lsmod | grep "$l_mad" > /dev/null 2>&1; then
       echo -e "\n - \"$l_mad\" modulunu yukluden kaldiriyorum"
       modprobe -r "$l_mad"
     fi
   }

   # Modul blacklist'e eklenmemisse, blacklist'e ekleme fonksiyonu
   modul_engelle_fix() {
     if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_madp\b"; then
       echo -e "\n - \"$l_mad\" modulunu blacklist'e ekliyorum"
       echo -e "blacklist $l_mad" >> /etc/modprobe.d/"$l_madp".conf
     fi
   }

   # Modulun sistemde olup olmadigini kontrol etme ve engellemeyi saglama
   for l_mdir in $l_myol; do
     if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut\n - Engellenip
engellenmedigini kontrol ediyorum..."
       modul_engelle_fix

       if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtur" ]; then
         modul_yuklenebilir_fix
         modul_yuklendi_fix
       fi
     else
       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut degil\n"
     fi
   done

   echo -e "\n - \"$l_mad\" modulunun engellenmesi tamamlandi\n"
}
```

4.2.1.5. Hfsplus Modülü Sıkılaştırma

HFSPLUS (Hierarchical File System Plus) dosya sistemi, Mac OS X işletim sistemlerinde kullanılan bir dosya sistemi türüdür. HFS'nin gelişmiş bir versiyonudur ve daha büyük diskler ile gelişmiş özellikler sunar. HFSPLUS, özellikle Mac OS dosya sistemlerini Linux sistemlerinde çalıştırmak için kullanılır. Ancak Linux sistemlerinde genellikle HFSPLUS desteğine ihtiyaç yoktur. Eğer GNU/Linux ortamında Mac OS dosya sistemlerine dair bir işlem yapılmıyorsa HFSPLUS modülünün aktif olması gereksizdir.

Gereksiz dosya sistemi türlerinin yüklenmesi, sistemin güvenliğini riske atabilir. HFSPLUS modülünün etkin olduğu durumlarda, saldırganlar bu modül üzerinden potansiyel güvenlik açıkları arayabilir. Bu nedenle, bu tür modüllerin yüklenmesini engellemek önemlidir. Eğer HFSPLUS dosya sistemi kullanılmıyorsa, bu modülün sistemde etkin olması gereksiz bir risk oluşturur ve devre dışı bırakılmalıdır.

HFSPLUS modülünü devre dışı bırakmak için, modprobe aracı kullanılarak ilgili modülün yüklenmesinin engellenmesi sağlanabilir. /etc/modprobe.d/ dizinine uygun yapılandırma dosyaları eklenerek, bu dosya sisteminin yüklenmesi engellenebilir ve varsa modül sistemden kaldırılabilir. Bu işlem modülün sadece gerekli olan zamanlarda yüklenmesini sağlamak ve diğer zamanlarda sistemde devre dışı bırakılmasını temin etmek amacıyla yapılır.

CIS Benchmark v2.0.1-1.1.1.5 maddesi gereği, HFSPLUS dosya sistemine dair desteğin gereksiz olduğu durumlarda, bu modülün yüklenmesinin engellenmesi sistemin güvenliğini artırır. Gereksiz modüllerin devre dışı bırakılması, sistemin yalnızca gerekli olan işlevleri çalıştırmasını sağlar ve böylece güvenlik açıkları üzerine saldırılara karşı daha sağlam bir savunma oluşturulur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, HFSPLUS (Hierarchical File System Plus) dosya sistemi modülünün GNU/Linux sistemlerinde gereksiz olduğunda devre dışı bırakılmasını sağlamak için kullanılır. Komut, HFSPLUS modülünün sistemdeki mevcut durumunu kontrol eder. Eğer modül sistemde yüklü ise, modprobe -r komutuyla modül kaldırılır. Ayrıca, modülün yüklenmesini engellemek

için /etc/modprobe.d/ dizinine bir yapılandırma dosyası eklenir ve modülün yüklenmesi install hfsplus /bin/false komutuyla engellenir. Modül daha önce blacklist'e eklenmemişse, bu işlem de yapılır. Böylece, HFSPLUS dosya sistemi desteği gereksiz olduğunda bu modülün sistemdeki potansiyel güvenlik açıklarını önlemek amacıyla devre dışı bırakılması sağlanır.

```
1. #!/usr/bin/env bash
2.
3. {
4.   l_mad="hfsplus"  # Modul adi
5.   l_mtur="fs"       # Modul turu (dosya sistemi)
6.   l_myol="/lib/modules/**/kernel/$l_mtur"  # Modul dizin yollari
7.   l_madp="$(tr '-' '_' <<< "$l_mad")"     # Modul adini uygun hale getirme
8.   l_mndir="$(tr '-' '/' <<< "$l_mad")"      # Modul dizini istenen formatta olusturma
9.
10.   # Modulun yuklenmesini engelleme fonksiyonu
11.   modul_yuklenebilir_fix() {
12.     l_yuklenebilir="$(modprobe -n -v "$l_mad")"
13.     [ "$(wc -l <<< "$l_yuklenebilir")" -gt "1" ] && l_yuklenebilir="$(grep -P --
"(^\h*install|\b$l_mad)\b" <<< "$l_yuklenebilir")"
14.
15.     if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_yuklenebilir"; then
16.       echo -e "\n - \"$l_mad\" modulunun yuklenmesini engelliyorum"
17.       echo -e "install $l_mad /bin/false" >> /etc/modprobe.d/"$l_madp".conf
18.     fi
19.   }
20.
21.   # Modul yuklendi ise, yuklemeyi kaldirma fonksiyonu
22.   modul_yuklendi_fix() {
23.     if lsmod | grep "$l_mad" > /dev/null 2>&1; then
24.       echo -e "\n - \"$l_mad\" modulunu yukluden kaldiriyorum"
25.       modprobe -r "$l_mad"
26.     fi
27.   }
28.
29.   # Modul blacklist'e eklenmemisse, blacklist'e ekleme fonksiyonu
30.   modul_engelle_fix() {
31.     if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_madp\b"; then
32.       echo -e "\n - \"$l_mad\" modulunu blacklist'e ekliyorum"
33.       echo -e "blacklist $l_mad" >> /etc/modprobe.d/"$l_madp".conf
34.     fi
35.   }
36.
37.   # Modulun sistemde olup olmadigini kontrol etme ve engellemeyi saglama
38.   for l_mdir in $l_myol; do
39.     if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
40.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut\n - Engellenip
engellenmedigini kontrol ediyorum..."
41.       modul_engelle_fix
42.
43.       if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtur" ]; then
44.         modul_yuklenebilir_fix
45.         modul_yuklendi_fix
46.       fi
47.     else
48.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut degil\n"
49.     fi
50.   done
51.
52.   echo -e "\n - \"$l_mad\" modulunun engellenmesi tamamlandi\n"
53. }
```

4.2.1.6. Squashfs Modülü Sıkılaştırma

SquashFS, genellikle küçük cihazlarda kullanılan sıkıştırılmış, salt okunur bir dosya sistemidir. Eğer sisteminizde bu dosya sistemi kullanılmıyorsa, güvenlik açısından devre dışı bırakılması önerilir. Çünkü gereksiz dosya sistemlerinin aktif olması, saldırganlar için potansiyel bir güvenlik açığı oluşturabilir.

Yapılan testlerde halihazırda bulunan Ubuntu 20.04 makinesi için CIS Benchmark v2.0.1-1.1.1.6 maddesi gereği, SquashFS desteği devre dışı bırakıldığı sistemin güvenliğinde herhangi bir ihlal tespit edilmemiştir. Bu nedenle SquashFS dosya sistemi desteği zaten devre dışı bırakıldığı için iyileştirme modelinde uygulanan sıkılaştırma kodu yazılmamıştır.

4.2.1.7. Udf Modülü Sıkılaştırma

UDF (Universal Disk Format), ISO/IEC 13346 ve ECMA-167 standartlarını uygulamak için kullanılan, geniş bir medya yelpazesinde veri depolama için tasarlanmış açık kaynaklı bir dosya sistemi türüdür. Genellikle DVD yazma ve yeni optik disk formatlarıyla uyumlu olmak amacıyla kullanılır. Linux sistemlerinde, optik disklerdeki verilere erişim sağlamak için UDF modülüne gerek duyulabilir. Eğer sistemde optik diskler ya da DVD yazma gibi işlemler yapılmıyorsa bu modülün etkin olması gereksizdir.

Gereksiz dosya sistemi türlerinin etkin olması, saldırganların potansiyel güvenlik açıklarından yararlanmasına olanak tanıyabilir. Bu nedenle UDF dosya sistemine ihtiyacınız yoksa modülün yüklenmesi engellenmelidir. UDF modülünün yüklenmesinin engellenmesi sadece gerekli olduğunda aktif olması gerektiğinden sistemin güvenliğini artıracaktır.

UDF modülünü devre dışı bırakmak için modprobe komutunu kullanarak bu modülün yüklenmesini engelleyen yapılandırma dosyaları oluşturulabilir. Bunun için /etc/modprobe.d/ dizinine gerekli konfigürasyon dosyaları eklenir ve mevcutsa modül sistemden kaldırılır. Bu işlem UDF modülünün sisteme gereksiz yere yüklenmesinin önüne geçer.

CIS Benchmark v2.0.1-1.1.1.7 maddesi bulgusunu kapatmak için, sistemde UDF dosya sistemine dair desteğin gereksiz olduğu durumlarda bu modülün yüklenmesinin engellenmesi, güvenliği artıran önemli bir adımdır. Bu tür gereksiz modüllerin devre dışı bırakılması sistemin yalnızca gerçekten ihtiyaç duyulan işlevleri çalıştırmasını sağlar ve potansiyel güvenlik açıklarını azaltır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, UDF (Universal Disk Format) dosya sistemi modülünün GNU/Linux sistemlerinde gereksiz olduğunda devre dışı bırakılmasını sağlamak için kullanılır. İlk olarak, UDF modülünün sistemdeki mevcut durumu kontrol edilir. Eğer modül yüklü ise, modprobe -r komutuyla modül kaldırılır. Ardından, /etc/modprobe.d/ dizinine modülün yüklenmesini engelleyecek bir yapılandırma dosyası eklenir; bu dosya, install udf /bin/false komutunu içerecek şekilde oluşturulur. Eğer modül daha önce blacklist'e eklenmemişse, bu işlem de gerçekleştirilir. Böylece, UDF modülünün yalnızca gerekli olduğunda aktif olmasını sağlamak için bu modül sistemde gereksiz yere yüklendiğinde engellenir, bu da güvenliği artırır.

```
1. #!/usr/bin/env bash
2.
3. {
4.   l_mad="udf"  # Modul adi
5.   l_mtur="fs"   # Modul turu (dosya sistemi)
6.   l_myol="/lib/modules/**/kernel/$l_mtur"  # Modul dizin yollari
7.   l_madp="$(tr '-' '_' <<< "$l_mad")"     # Modul adini uygun hale getirilmis
8.   l_mndir="$(tr '-' '/' <<< "$l_mad")"      # Modul dizini istenen formatta
olusturulmus
9.
10.   # Modulun yuklenmesini engelleme fonksiyonu
11.   modul_yuklenebilir_fix() {
12.     l_yuklenebilir="$(modprobe -n -v "$l_mad")"
13.     [ "$(wc -l <<< "$l_yuklenebilir")" -gt "1" ] && l_yuklenebilir="$(grep -P --
"(^\h*install|\b$l_mad)\b" <<< "$l_yuklenebilir")"
14.
15.     if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_yuklenebilir"; then
16.       echo -e "\n - \"$l_mad\" modulunun yuklenmesini engelliyorum"
17.       echo -e "install $l_mad /bin/false" >> /etc/modprobe.d/"$l_madp".conf
18.     fi
19.   }
20.
21.   # Modul yukluyse, yuklemeyi kaldirma fonksiyonu
22.   modul_yuklendi_fix() {
23.     if lsmod | grep "$l_mad" > /dev/null 2>&1; then
24.       echo -e "\n - \"$l_mad\" modulunu yukluden kaldiriyorum"
25.       modprobe -r "$l_mad"
26.     fi
27.   }
28.
29.   # Modul blacklist'e eklenmemisse, blacklist'e ekleme fonksiyonu
30.   modul_engelle_fix() {
```

```
31.     if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_madp\b"; then
32.       echo -e "\n - \"$l_mad\" modulunu blacklist'e ekliyorum"
33.       echo -e "blacklist $l_mad" >> /etc/modprobe.d/"$l_madp".conf
34.     fi
35.   }
36.
37.   # Modulun sistemde olup olmadigini kontrol etme ve engellemeyi saglama
38.   for l_mdir in $l_myol; do
39.     if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
40.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut\n - Engellenip
engellenmedigini kontrol ediyorum..."
41.       modul_engelle_fix
42.
43.       if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtur" ]; then
44.         modul_yuklenebilir_fix
45.         modul_yuklendi_fix
46.       fi
47.     else
48.       echo -e "\n - \"$l_mad\" modulu \"$l_mdir\" dizininde mevcut degil\n"
49.     fi
50.   done
51.
52.   echo -e "\n - \"$l_mad\" modulunun engellenmesi tamamlandi\n"
53. }
```

4.2.2. Yetkili Kullanıcı Hesap Yönetimi

Güvenlik açısından en iyi uygulamalardan biri, sadece yetkilendirilmiş kullanıcıların sisteme erişmesine izin vermek ve her bir kullanıcıya yalnızca gerekli olan yetkileri tanımaktır. Bu tedbir sistemdeki kullanıcı hesaplarının etkin yönetilmesini sağlayarak yalnızca yetkilendirilmiş kişilerin erişimine izin verir ve böylece kötü niyetli kişilerin sisteme girişini zorlaştırır.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), bir kurumun güvenlik durumunu değerlendirirken, CIS (Center for Internet Security) denetimlerini referans alır ve bu denetimler sistemin en iyi güvenlik uygulamalarına ne kadar uyduğunu ölçer. “Yetkili Kullanıcı Hesap Yönetimi” tedbiri de CIS denetimlerinin bir parçası olarak, her kullanıcıya özgü hesaplar oluşturulmasını ve yalnızca gerekli izinlerin verilmesini önermektedir.

Bu tedbirler kapsamında, kullanıcıların yalnızca ihtiyaçları doğrultusunda hesaplar oluşturulmalı, kullanılmayan hesaplar kaldırılmalı ve sistem üzerinde yüksek yetkiler gerektiren işlemler yalnızca belirli kullanıcılara verilmelidir. Tüm kullanıcı hesapları için güvenli şifreleme, doğru yetkilendirme ve izleme sistemleri kullanılarak, sadece yetkilendirilmiş kullanıcıların yönetici yetkilerine sahip olmaları sağlanmalıdır.

Çizelge 4.15'te, BİGR 5.1.2.2 maddesi, Yetkili Kullanıcı Hesap Yönetimi tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.15. GNU/Linux işletim sistemi yetkili kullanıcı hesap yönetimi

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1**
5.1.2.2	Yetkili Kullanıcı Hesap Yönetimi	Sisteme erişecek her kişi için ayrı bir kullanıcı hesabı oluşturulmalıdır. Oluşturulan kullanıcılar için yetkiler belirlenmelidir. Kullanılmayan hesaplar kaldırılmalıdır. Sistem kullanıcılarının kabuğu /sbin/nologin olmalıdır. Root login mümkünse engellenmelidir. Tüm makinelerde UID değeri 0 olan tek kullanıcı root olmalıdır. Ayrıca aynı isme veya UID değerine sahip kullanıcı veya grup bulunmamalıdır. Servis ve sistem kullanıcıları hariç parolasız kullanıcılar bulunmamalıdır. Sudoers kullanıcıları değişikliklere karşı takip edilmelidir.	4.2.7 Ensure SSH root login is disabled 4.2.9 Ensure SSH PermitEmptyPasswords is disabled 4.4.1 Ensure password creation requirements are configured 4.4.2 Ensure lockout for failed password attempts is configured 4.4.3 Ensure password reuse is limited 4.4.4 Ensure strong password hashing algorithm is configured 4.5.1.1 Ensure minimum days between password changes is configured 4.5.1.2 Ensure password expiration is 365 days or less 4.5.1.3 Ensure password expiration warning days is 7 or more 4.5.2 Ensure system accounts are secured 4.5.3 Ensure default group for the root account is GID 0 5.2.3.1 Ensure changes to system administration scope (sudoers) is collected 5.2.3.3 Ensure events that modify the sudo log file are collected 5.2.3.12 Ensure login and logout events are collected 6.2.10 Ensure root is the only UID 0 account

4.2.2.1. SSH Yönetici (Root) Girişi Devre Dışı Bırakma Yapılandırması

SSH üzerinden yönetici (root) kullanıcısının girişine izin verilmesi, sistem yöneticilerinin daha sonra bu erişimlerin denetimini sağlamasını zorlaştırır. Yönetici (root) girişinin engellenmesi, güvenlik açısından kritik bir önlemdir. Bu tedbir sistem yöneticilerinin kendi kullanıcı hesaplarıyla oturum açmasını ve ardından yönetici (root) yetkilerine yükseltilmesi gerektiğini belirtir. Bu uygulama işlemler üzerinde daha iyi bir denetim sağlar ve güvenlik olayları durumunda denetim izlerini korur.

Yapılan testlerde, Ubuntu 20.04 sisteminde CIS Benchmark v2.0.1-4.2.7 maddesi doğrultusunda SSH yönetici (root) login devre dışı bırakıldığı görülmüştür. Sistemde SSH yönetici (root) girişinin engellenmiş olduğunu doğrulayan herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle yönetici (root) login devre dışı bırakıldığı için iyileştirme modelinde ek bir sıkılaştırma kodu uygulanmamıştır.

4.2.2.2. SSH PermitEmptyPasswords Özelliği Devre Dışı Bırakma Yapılandırması

SSH sunucusunun PermitEmptyPasswords parametresi, boş şifreli hesaplara uzaktan giriş izni verilip verilmeyeceğini belirler. Boş şifreli hesaplara uzaktan erişimin engellenmesi, yetkisiz erişim olasılığını azaltır ve sistemin güvenliğini artırır. Bu tedbir, boş şifrelere sahip hesapların sisteme erişimini engelleyerek, yalnızca güçlü ve doğrulanmış kimlik bilgileri ile erişim sağlanmasına olanak tanır.

Yapılan testlerde, Ubuntu 20.04 sisteminde CIS Benchmark v2.0.1-4.2.9 maddesi doğrultusunda PermitEmptyPasswords parametresi devre dışı bırakılmıştır. Sistemde boş şifreli hesaplara erişim engellenmiş olup, güvenlik açısından herhangi bir ihlal tespit edilmemiştir. Bu nedenle, boş şifreli hesaplara erişim zaten engellendiği için iyileştirme modelinde ek bir sıkılaştırma kodu uygulanmamıştır.

4.2.2.3. Parola Oluşturma Gereksinimleri Yapılandırması

Parola oluşturma gereksinimlerinin yapılandırılması, sistem güvenliği için kritik bir adımdır. Güçlü parolalar, kullanıcı hesaplarının kötü niyetli saldırılara karşı korunmasına yardımcı olur, özellikle kaba kuvvet saldırıları (brute-force attacks) ve parola tahmin etme gibi yöntemlerle yapılan saldırılar için etkili bir engel oluşturur. Bu gereksinimlerin parolaların belirli bir uzunlukta olması, karmaşık karakterler içermesi ve belirli kurallara uyması gerektiği belirtilir.

Bu tedbir için pam_pwquality.so modülü, parolaların güçlülüğünü kontrol eder ve birkaç gereksinimi yerine getirip getirmediğini test eder. Bu gereksinimler parolanın uzunluğunu, içeriğindeki karakter çeşitliliğini ve karakterlerin karmaşıklığını içerir. Modülün yapılandırılması hem parola uzunluğunu hem de karmaşıklık gereksinimlerini

belirlemek için işletim sistemi üzerindeki /etc/security/pwquality.conf dosyasına yapılacak değişiklikleri gerektirir.

Sistem üzerinde PAM yoksa ilk olarak pam_pwquality.so modülünü kurmak gerekir. Bu sistemi güçlü parolalar kullanmaya zorlamak için gerekli olan bir yazılımdır. Bu modül parolaların en az 14 karakter uzunluğunda olmasını sağlayabilir. Ayrıca, parola karmaşıklığı için 4 farklı karakter sınıfının (büyük harf, küçük harf, rakam ve özel karakter) kullanılması zorunlu kılınır. Alternatif olarak, belirli kredi seçenekleri de kullanılabilir.

Parolaların oluşturulması sırasında bu gereksinimlere uyulması gerektiğini belirten parametreler /etc/pam.d/common-password dosyasına eklenir. Bu dosya, kullanıcıların parolalarını değiştirdiklerinde veya oluşturduklarında uygulanan politika ayarlarını kontrol eder. Kullanıcılar parolalarını belirlenen kurallara uymaması durumunda kullanıcıya üç deneme hakkı verir.

CIS Benchmark v2.0.1-4.4.1 tedbiri için yapılan iyileştirme modelindeki yapılandırma, kullanıcıların daha güçlü parolalar belirlemelerini zorunlu kılarak, sisteme yönelik saldırıları engellemeye yardımcı olur. Parola uzunluğu ve karmaşıklık gereksinimlerini belirlerken organizasyonun güvenlik politikasına uygun değerleri seçmek önemlidir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, güçlü parola gereksinimlerini sağlamak amacıyla GNU/Linux sisteminde pam_pwquality.so modülünü yükler ve yapılandırır. İlk olarak, pam_pwquality modülü yüklenir. Ardından, /etc/security/pwquality.conf dosyasına parola uzunluğu ve karmaşıklığı ile ilgili gereksinimler eklenir; burada parolaların en az 14 karakter uzunluğunda olması gerektiği belirtilir ve parolaların en az 4 farklı karakter sınıfını içermesi zorunlu hale getirilir (örneğin, büyük harf, küçük harf, rakam ve özel karakter). Ayrıca, alternatif olarak kredi seçenekleri de yapılandırılabilir. Son olarak, /etc/pam.d/common-password dosyasına pam_pwquality.so modülünün eklenmesiyle, kullanıcıların parola oluştururken veya değiştirirken bu güvenlik politikalarına uymaları sağlanır. Bu işlem, güçlü parolaların kullanılmasını zorunlu kılarak sistemin güvenliğini artırır.

```
#!/usr/bin/env bash

# pam_pwquality modülünün yüklenmesi
echo -e " - pam_pwquality modülü yükleniyor..."
sudo apt install -y libpam-pwquality

# /etc/security/pwquality.conf dosyasının yapılandırılması
echo -e " - /etc/security/pwquality.conf dosyasına şifre uzunluğu ve karmaşıklık gereksinimleri ekleniyor..."

# Parola uzunluğunu 14 karakter olarak ayarlama
sudo sh -c 'echo "minlen = 14" >> /etc/security/pwquality.conf'

# Parola karmaşıklığı gereksinimlerini ayarlama (minimum 4 sınıf, ya da kredi seçeneklerinden biri)
# Burada minclass ve dcredit, ucredit, ocredit, lcredit gibi seçeneklerden birini kullanabiliriz.

# Seçenek 1: minclass = 4 (Minimum 4 karakter sınıfı)
sudo sh -c 'echo "minclass = 4" >> /etc/security/pwquality.conf'

# Alternatif olarak, kredi seçeneklerini kullanmak için aşağıdaki satırlar eklenebilir.
# sudo sh -c 'echo "dcredit = -1" >> /etc/security/pwquality.conf'
# sudo sh -c 'echo "ucredit = -1" >> /etc/security/pwquality.conf'
# sudo sh -c 'echo "ocredit = -1" >> /etc/security/pwquality.conf'
# sudo sh -c 'echo "lcredit = -1" >> /etc/security/pwquality.conf'

# /etc/pam.d/common-password dosyasına pam_pwquality.so eklenmesi
echo -e " - /etc/pam.d/common-password dosyasına pam_pwquality.so ekleniyor..."

sudo sed -i '/common-password/ s/$/ password requisite pam_pwquality.so retry=3/' /etc/pam.d/common-password

echo -e "\n - Şifre güvenliği gereksinimleri başarıyla yapılandırıldı."
```

4.2.2.4. Başarısız Parola Denemeleri için Hesap Kilidi Yapılandırması

Başarısız giriş denemeleri sonrası kullanıcıların kilitlenmesi, sistem güvenliği için kritik bir önlemdir. Bu yapılandırma özellikle kaba kuvvet (brute-force) saldırılarının önlenmesinde etkilidir. Saldırganlar, doğru parolayı tahmin edene kadar sürekli olarak parola denemeye devam edebilirler. Başarısız giriş denemeleri sayısı sınırlanarak bu tür saldırılara karşı korunmuş olunur.

Sistemde, PAM (Pluggable Authentication Module) yapılandırma dosyalarında değişiklik yaparak bu güvenlik önlemi uygulanabilir. /etc/pam.d/common-auth dosyasına pam_tally2.so modülü eklenir. Bu modül kullanıcıların belirli sayıda başarısız giriş denemesi yaptıktan sonra hesaplarını kilitler. Yapılandırmada deny=5 parametresi ile 5 başarısız giriş denemesi sonrası hesabın kilitlenmesi ve unlock_time=900 parametresi ile kullanıcı hesabının 15 dakika sonra (900 saniye) tekrar aktif hale gelmesi sağlanır.

Sistem üzerinde /etc/pam.d/common-account dosyasına da pam_tally2.so modülünün eklenmesi gerekir. Bu işlem kullanıcı hesabının durumu üzerinde kontrol sağlar ve başarısız girişlerin izlenmesini mümkün kılar. Ayrıca pam_deny.so modülü de bu dosyaya eklenerek geçersiz giriş denemeleri sonucunda kullanıcıların sisteme erişimi engellenmiş olur.

CIS Benchmark v2.0.1-4.4.2 tedbiri için alınan bu güvenlik önlemi, sistem üzerine yapılan potansiyel saldırıları engellemeye yardımcı olur ve yalnızca geçerli parolalarla giriş yapmayı mümkün kılmaktadır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemde başarısız giriş denemeleri sonrası kullanıcı hesaplarının kilitlenmesini sağlayan bir yapılandırma işlemi gerçekleştirir. İlk olarak, /etc/pam.d/common-auth dosyasına pam_tally2.so modülü eklenir ve bu modül, kullanıcıların 5 başarısız giriş denemesinden sonra hesaplarının kilitlenmesini sağlar (deny=5 parametresiyle). Ayrıca, unlock_time=900 parametresiyle, hesapların 15 dakika (900 saniye) sonra otomatik olarak tekrar aktif hale gelmesi sağlanır. Ardından, /etc/pam.d/common-account dosyasına da pam_tally2.so modülü eklenir, böylece başarısız girişler izlenebilir ve geçersiz giriş denemeleri sonrasında pam_deny.so modülü ile kullanıcıların sisteme erişimi engellenir. Bu yapılandırma, sistemin kötü niyetli kaba kuvvet (brute-force) saldırılarına karşı daha güvenli hale gelmesini sağlar.

```
1. #!/usr/bin/env bash
2.
3. # Başarısız giriş denemeleri sonrası kullanıcıyı kilitleme yapılandırması
başlatılıyor...
4. echo -e " - Başarısız giriş denemeleri sonrası kullanıcıları kilitleme yapılandırması
başlatılıyor..."
5.
6. # /etc/pam.d/common-auth dosyasına pam_tally2.so yapılandırmasını ekle
7. echo -e " - /etc/pam.d/common-auth dosyasına pam_tally2.so ekleniyor..."
8. sudo sed -i '/^auth\srequired\s/pam_tally2.so\s*/a auth required pam_tally2.so
onerr=fail audit silent deny=5 unlock_time=900' /etc/pam.d/common-auth
9.
10. # /etc/pam.d/common-account dosyasına pam_tally2.so yapılandırmasını ekle
11. echo -e " - /etc/pam.d/common-account dosyasına pam_tally2.so ekleniyor..."
12. sudo sed -i '/^account\srequired\s/pam_deny.so\s*/a account required pam_tally2.so'
/etc/pam.d/common-account
13. sudo sed -i '/^account\srequired\s/pam_tally2.so\s*/a account requisite pam_deny.so'
/etc/pam.d/common-account
14.
15. echo -e "\n - Başarısız giriş denemeleri sonrası kullanıcı hesapları kilitleme
yapılandırması başarıyla tamamlandı."
```

4.2.2.5. Parola Yeniden Kullanımı Sınırlanma Yapılandırması

Parola tekrarını sınırlama, kullanıcıların geçmişteki parolalarını yeniden kullanmalarını engelleyerek güvenlik seviyesini artıran önemli bir önlemdir. Bu işlem sistemin güvenliğini sağlamak amacıyla kullanıcıların son birkaç parolasını tekrar kullanmalarına izin verilmemesini sağlar. Yapılan iyileştirme modeli kapsamında, saldırganların kullanıcıların eski parolalarını tahmin etme olasılığı azalır ve böylece sistemin korunması sağlanır.

Bu güvenlik önlemini uygulamak için /etc/security/opasswd dosyasında kullanıcıların eski parolaların saklandığı bilgiyi kullanarak, her kullanıcı için parola geçmişi kontrol edilir. Kullanıcıların son 5 parolasını kullanmalarını önlemek amacıyla yapılandırılır.

Bu adımlar sistemdeki /etc/pam.d/common-password dosyasını düzenleyerek yapılır. Öncelikle bu dosyaya pam_pwhistory.so modülü eklenir ve kullanıcıların geçmiş parolalarını 5 defa hatırlamalarını sağlayacak şekilde yapılandırılır. pam_unix.so modülündeki use_authtok parametresi de eklenerek, parola değişikliği işlemi sırasında eski parolaların doğru bir şekilde kontrol edilmesi sağlanır.

CIS Benchmark v2.0.1-4.4.3 tedbiri için yapılan bu işlemle birlikte, sistem kullanıcılarının güvenliği artırılır ve parolaların sıklıkla tekrar edilmesinin önüne geçilmektedir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, kullanıcıların eski parolalarını yeniden kullanmalarını engelleyen bir yapılandırma işlemi gerçekleştirir. İlk olarak, /etc/pam.d/common-password dosyasına pam_pwhistory.so modülü eklenir ve bu modül, kullanıcıların son 5 parolasını hatırlamamalarını sağlayacak şekilde yapılandırılır (remember=5 parametresiyle). Ardından, pam_unix.so modülündeki use_authtok parametresi eklenerek, parola değişikliği sırasında eski parolaların doğruluğu düzgün bir şekilde kontrol edilir.

```
1. #!/usr/bin/env bash
2.
3. # Parola tekrarını sınırlama yapılandırması başlatılıyor...
```

```
4. echo -e " - Şifre tekrarını sınırlama yapılandırması başlatılıyor..."
5.
6. # /etc/pam.d/common-password dosyasına pam_pwhistory.so ekle
7. echo -e " - /etc/pam.d/common-password dosyasına pam_pwhistory.so ekleniyor..."
8. sudo sed -i '/^password\srequired\s*pam_unix.so/ i password required pam_pwhistory.so
remember=5' /etc/pam.d/common-password
9.
10. # /etc/pam.d/common-password dosyasındaki pam_unix.so satırını 'use_authtok' ile
güncelle
11. echo -e " - /etc/pam.d/common-password dosyasındaki pam_unix.so satırı
güncelleniyor..."
12. sudo sed -i 's/password \[success=1 default=ignore\] pam_unix.so/\0 use_authtok/'
/etc/pam.d/common-password
13.
14. echo -e "\n - Şifre tekrarını sınırlama yapılandırması başarıyla tamamlandı."
```

4.2.2.6. Parola Değişiklikleri Arasında Minimum Gün Sayısı Belirleme

Parola değiştirme sıklığını sınırlamak, güvenlik açısından önemli bir adımdır çünkü kullanıcıların parolalarını sıkça değiştirmeleri güvenlik önlemlerini zayıflatabilir. Örneğin, bir kullanıcı parola politikasına uymamak amacıyla eski bir parolayı tekrar kullanmak için parola değişikliklerini sıklıkla yapabilir. Bu tür davranışları engellemek için parolaların belirli bir süre zarfında değiştirilmesini yasaklamak ve her parola değişikliği arasında minimum bir gün sayısı belirlemek gerekmektedir.

Bu işlem için /etc/login.defs dosyasındaki PASS_MIN_DAYS parametresi kullanılır. Bu parametre kullanıcıların parolalarını değiştirmeleri için gerekli minimum günü belirler. Önerilen değer genellikle 1 gündür. Yani bir kullanıcı parolasını değiştirdikten sonra 1 gün boyunca tekrar değiştiremez. Bu kullanıcıların parolalarını sürekli olarak değiştirmelerini engelleyerek güvenlik ihlallerini önler.

CIS Benchmark v2.0.1-4.5.1.1 maddesi için uygulanan iyileştirme modeli ile parola değiştirme sıklığının sınırlanması, kötü niyetli kullanıcıların parola değiştirme prosedürlerini manipüle etmelerini engeller. Bu tür güvenlik önlemleri sistemin güvenliğini sağlamak adına oldukça önemlidir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, kullanıcıların parolalarını değiştirme sıklığını sınırlamak için yapılandırmalar yapmaktadır. İlk olarak, /etc/login.defs dosyasındaki “PASS_MIN_DAYS” parametresi güncellenerek, kullanıcıların parolalarını en az 1 gün arayla değiştirmeleri sağlanır. Ardından, tüm kullanıcılar için bu parametreyi 1 gün olarak ayarlayan bir döngü çalıştırılır ve her bir

kullanıcı için chage komutu ile minimum değişiklik günü 1 olarak belirlenir. Bu yapılandırma, CIS Benchmark v2.0.1-4.5.1.1 maddesi ile uyumlu olup, kötü niyetli kullanıcıların parolalarını sıkça değiştirerek güvenlik önlemlerini aşmalarını engeller ve sistem güvenliğini artırır.

```
1. #!/usr/bin/env bash
2.
3. # Parola değiştirme sıklığını sınırlama yapılandırması başlatılıyor...
4. echo -e " - Şifre değiştirme sıklığını sınırlama yapılandırması başlatılıyor..."
5.
6. # /etc/login.defs dosyasındaki PASS_MIN_DAYS parametresini güncelle
7. echo -e " - /etc/login.defs dosyasındaki PASS_MIN_DAYS parametresi güncelleniyor..."
8. sudo sed -i 's/^PASS_MIN_DAYS\s.*/PASS_MIN_DAYS   1/' /etc/login.defs
9.
10. # Tüm kullanıcılar için minimum gün parametresini 1 olarak ayarlama
11. echo -e " - Tüm kullanıcılar için şifre değiştirme minimum gün sayısı 1 olarak
ayarlanıyor..."
12. for user in $(awk -F: '{ print $1 }' /etc/passwd); do
13.   sudo chage --mindays 1 "$user"
14. done
15.
16. echo -e "\n - Şifre değiştirme sıklığını sınırlama yapılandırması başarıyla
tamamlandı."
```

4.2.2.7. Parola Süresi Belirleme

Parola süresi yapılandırması, güvenliğin artırılması açısından önemli bir adımdır. Parolaların belirli bir süre sonra sona ermesini sağlamak bir saldırganın çalınan veya kırılan parolaları kötüye kullanma süresini sınırlayarak sistemin güvenliğini sağlar. Ayrıca bu uygulama, kullanıcıların parolalarını güncel tutmalarını teşvik eder ve eski parolaların güvenlik açıkları oluşturmasını engeller.

PASS_MAX_DAYS parametresi, her kullanıcının parola geçerliliğini belirli bir süreyle sınırlamak için kullanılır. Bu parametre, kullanıcı parolalarının geçerliliğini 365 günle sınırlandırmak için yapılandırılmalıdır. Bu sayede parolalar, her yıl otomatik olarak sona erecek ve kullanıcılar yeni bir parola belirlemek zorunda kalacaklardır. Bu parolanın uzun süre kullanılmasına bağlı güvenlik açıklarını azaltır.

Bu tür bir parola süresi yönetimi, kullanıcıların parolalarını belirli aralıklarla yenilemelerini sağlar ve potansiyel bir güvenlik açığını daha erken tespit etmeyi, önlem almayı mümkün kılar. Eğer bir kullanıcı parolasını değiştirmezse, sistem yöneticisi tarafından belirlenen bu sürenin sonunda kullanıcıya uyarı gönderilebilir veya parolası otomatik olarak geçersiz hale gelebilir.

CIS Benchmark v2.0.1-4.5.1.2 tedbirinin sonucu olarak, parola süresinin sınırlandırılması sistemin güvenliğini artırmak için kritik bir uygulamadır. Bu uygulama ile özellikle hesaplar üzerindeki denetimi güçlendirir ve potansiyel saldırganlara karşı koruma sağlamaktadır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemdeki kullanıcıların parolalarının geçerlilik süresini sınırlandırmak amacıyla yapılandırmalar yapmaktadır. İlk olarak, /etc/login.defs dosyasındaki "PASS_MAX_DAYS" parametresi güncellenerek, parolaların 365 gün sonra sona ermesi sağlanır. Ardından, sistemdeki tüm kullanıcılar için bu parametreyi 365 gün olarak ayarlayan bir döngü çalıştırılır ve her bir kullanıcı için chage komutu ile maksimum parola süresi 365 gün olarak belirlenir. Bu yapılandırma, kullanıcıların parolalarını her yıl güncellemelerini zorunlu kılarak, eski parolaların güvenlik açıklarına yol açmasını engeller ve sistemin genel güvenliğini artırır.

```
1. #!/usr/bin/env bash
2.
3. # Şifre süresi yapılandırması başlatılıyor...
4. echo -e " - Şifre süresi yapılandırması başlatılıyor..."
5.
6. # /etc/login.defs dosyasındaki PASS_MAX_DAYS parametresini güncelle
7. echo -e " - /etc/login.defs dosyasındaki PASS_MAX_DAYS parametresi güncelleniyor..."
8. sudo sed -i 's/^PASS_MAX_DAYS\s.*/PASS_MAX_DAYS   365/' /etc/login.defs
9.
10. # Tüm kullanıcılar için maksimum şifre süresini 365 gün olarak ayarlama
11. echo -e " - Tüm kullanıcılar için şifre süresi 365 gün olarak ayarlanıyor..."
12. for user in $(awk -F: '{ print $1 }' /etc/passwd); do
13.   sudo chage --maxdays 365 "$user"
14. done
15.
16. echo -e "\n - Şifre süresi yapılandırması başarıyla tamamlandı."
```

4.2.2.8. Sistem Yönetimi Değişikliklerinin Toplanması

Sistem yöneticilerinin yetki kapsamındaki değişikliklerin izlenmesi, özellikle /etc/sudoers dosyasında veya /etc/sudoers.d/ dizinindeki değişikliklerin izlenmesiyle sağlanabilir. Bu dosyalar sistem yöneticilerinin hangi komutları çalıştırabileceğini ve hangi yetkilerle işlem yapabileceğini tanımlar. Bu dosyadaki herhangi bir değişiklik sistemdeki yetki yönetimini değiştirebilecek kritik bir işlem olabilir.

Öncelikle, auditd servisi sistemde yüklü olmalı ve çalışır durumda olmalıdır. Eğer auditd yüklü değilse bu paket yüklenmeli ve servis başlatılmalıdır. auditd servisi

yapılan değişiklikleri kaydeden güvenlik denetimleri için önemli bir araçtır. Daha sonra /etc/audit/rules.d/ dizininde bir audit kural dosyası oluşturulmalıdır. Bu dosya /etc/sudoers dosyasındaki ve /etc/sudoers.d/ dizinindeki dosyalarda yapılan yazma işlemlerini izlemek için kuralları içerir. Böylece bu dosyalarda herhangi bir değişiklik yapıldığında, audit sistemi bu olayları kaydedecektir. Bu değişiklikler genellikle bir sistem yöneticisinin yetki kapsamını değiştiren izinsiz bir müdahale olabileceğinden izlenmesi çok önemlidir.

Kurallar eklendikten sonra, bu kurallar audit sistemine yüklenmeli ve izleme başlatılmalıdır. Ayrıca sistemin bu yeni kurallarla doğru çalışıp çalışmadığını kontrol etmek amacıyla bir yeniden başlatma gerekliliği olup olmadığı kontrol edilmelidir. Eğer yeniden başlatma gerekliyse sistemin yeniden başlatılması sağlanmalıdır.

CIS Benchmark v2.0.1-5.2.3.1 maddesindeki tedbir gerçekleştirilen iyileştirme modeli sayesinde, sudoers dosyasında yapılacak izinsiz değişiklikler kolaylıkla tespit edilebilir ve gerekli güvenlik önlemleri alınabilir hale gelecektir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistem yöneticilerinin /etc/sudoers dosyası ve /etc/sudoers.d/ dizinindeki değişikliklerini izlemeyi amaçlamaktadır. İlk adımda, auditd paketi yüklenir ve servis başlatılır. Ardından, /etc/sudoers dosyasındaki ve /etc/sudoers.d/ dizinindeki dosyalarda yapılan yazma işlemlerini izlemek için bir izleme kuralı eklenir. Bu kurallar, herhangi bir izinsiz değişiklik durumunda auditd tarafından kaydedilecektir. Son olarak, eklenen audit kuralları sisteme yüklenir ve sistemin yeniden başlatılması gerekip gerekmediği kontrol edilir. Bu işlem, sudoers dosyasındaki yetki değişikliklerini izlemek ve güvenliği sağlamak için önemlidir.

```
1. #!/bin/bash
2.
3. # 1. auditd paketini yükle
4. echo "Auditd paketini yüklüyor..."
5. sudo apt update
6. sudo apt install -y auditd
7.
8. # 2. auditd servisini başlat ve otomatik başlatma için etkinleştir
9. echo "Auditd servisini başlatıyor..."
10. sudo systemctl start auditd
11. sudo systemctl enable auditd
12.
```

```
13. echo "Sistem yönetimi kapsamındaki (sudoers) değişikliklerin izlenmesi yapılandırması
başlatılıyor..."
14.
15. # 1. Sudoers dosyaları için izleme kuralları ekleniyor
16. echo "Izleme kuralları ekleniyor..."
17. echo -e "
18. -w /etc/sudoers -p wa -k scope
19. -w /etc/sudoers.d -p wa -k scope
20. " | sudo tee /etc/audit/rules.d/50-scope.rules
21.
22. # 2. Audit kurallarını yükle
23. echo "Audit kuralları yükleniyor..."
24. sudo augenrules --load
25.
26. # 3. Yeniden başlatma gerekip gerekmediğini kontrol et
27. echo "Sistemin yeniden başlatılmasına gerek olup olmadığı kontrol ediliyor..."
28. if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then
29.     echo "Yeniden başlatma gereklidir."
30. else
31.     echo "Yeniden başlatma gerekmez."
32. fi
33.
34. echo "Sistem yönetimi kapsamındaki (sudoers) değişikliklerin izlenmesi başarıyla
tamamlandı."
```

4.2.2.9. Sudo Log Dosyasını Değiştiren Olayların Toplanması

Sudo log dosyasındaki değişikliklerin izlenmesi, özellikle sudo komutlarıyla yönetici hakları kullanılarak yapılan işlemleri takip etmek için kritik bir güvenlik önlemidir. Sistem yöneticileri, sudo komutlarıyla yapılan işlemleri /var/log/sudo.log dosyasına kaydeder. Bu log dosyasındaki herhangi bir değişiklik ya bir yönetici komutunun çalıştırıldığını ya da log dosyasının manipüle edildiğini gösterir. Bu tür değişikliklerin izlenmesi sistemin güvenliğini sağlamak için önemlidir.

Sudo log dosyasındaki değişikliklerin izlenebilmesi için auditd (denetim aracı) kullanılarak sudo log dosyasındaki her okuma ve yazma işlemine dair denetim kuralları eklenmelidir. Bu kurallar, log dosyasındaki her türlü değişikliği kaydedecek ve bu değişikliklerin güvenlik analizi için kullanılmasını sağlayacaktır. Ayrıca sudo log dosyasındaki değişikliklerin kim tarafından ve ne zaman yapıldığını, işlemlerinde hangi komutların çalıştırıldığını da belirleyebilmek mümkün olacaktır.

Denetim kuralları /etc/audit/rules.d/ dizinine eklenir ve aktif hale getirilir. Bu sayede log dosyasına yazılan her yeni bilgi ya da yapılan her değişiklik kaydedilir. Ancak bu kuralların uygulanabilmesi için auditd servisi doğru şekilde yapılandırılmalı ve kurallar sisteme yüklenmelidir. Sudo log dosyasına yönelik denetim kuralları başarıyla yüklenirse tüm değişiklikler izlenebilir. Auditctl aracı ile denetim kurallarının

etkin olup olmadığı kontrol edilebilir. Eğer denetim kuralları etkin ise sistem yöneticisi bu kuralların doğru çalışıp çalışmadığını ve gerektiğinde sistemin yeniden başlatılmasının gerekip gerekmediğini belirleyebilir.

CIS Benchmark v2.0.1-5.2.3.3 tedbirinin güvenlik önlemi, yönetici haklarıyla gerçekleştirilen komutların izlenmesini sağlayarak, kötü niyetli aktivitelerin erkenden fark edilmesini ve gerekli güvenlik önlemlerinin alınmasını mümkün kılar. Bu sayede yetkisiz erişimler ve sistem manipülasyonları engellenebilir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sudo komutlarıyla yapılan işlemleri ve sudo log dosyasındaki değişiklikleri izlemeyi amaçlar. İlk olarak, auditd paketi yüklenir. Ardından, /var/log/sudo.log dosyasına yapılan yazma ve ekleme işlemleri için bir denetim kuralı eklenir. Bu kurallar, sudo log dosyasındaki değişiklikleri kaydeder ve bu değişiklikler üzerinden analiz yapılmasını sağlar. Daha sonra, auditd servisi yeniden başlatılır, böylece eklenen kurallar aktif hale gelir. Son olarak, /etc/sudoers dosyasına, sudo log dosyasının kaydını tutacak bir satır eklenir. Bu işlemle, sudo log dosyasındaki değişikliklerin kaydı tutulur ve güvenlik açısından önemli olan her türlü değişiklik izlenebilir hale gelir.

```
1. #!/bin/bash
2.
3. # auditd paketini yükle
4. sudo apt install auditd -y;
5.
6. # /var/log/sudo.log dosyasına yapılan yazma ve ekleme işlemlerini denetlemek için audit
kuralı ekle
7. echo "-w /var/log/sudo.log -p wa -k sudo_log_modification" | sudo tee -a
/etc/audit/rules.d/audit.rules;
8.
9. # auditd hizmetini yeniden başlat
10. sudo systemctl restart auditd;
11.
12. # sudoers dosyasına sudo.log dosyasının kaydını tutacak satırı ekle
13. echo "Defaults logfile=\"/var/log/sudo.log\"" | sudo tee -a /etc/sudoers;
```

4.2.2.10. Login ve Logout Olaylarının İzlenmesi ve Güvenlik Önlemleri

Login ve logout olaylarını izlemek için auditd servisi kullanılarak sistemdeki bu tür aktivitelerin takip edilmesi sağlanabilir. İlk adım olarak auditd paketini yüklemek gerekmektedir. Yükleme işlemi sonrasında auditd servisi başlatılmalı ve otomatik olarak başlaması için etkinleştirilmelidir.

Login ve logout olaylarını izlemek için gerekli kurallar /etc/audit/rules.d/ dizininde, .rules uzantılı bir dosya içinde tanımlanmalıdır. Bu kurallar, kullanıcı girişlerinin ve çıkışlarının kaydının tutulduğu dosyalar olan /var/log/lastlog ve /var/run/faillock dosyalarını izleyecek şekilde yapılandırılmalıdır. Kuralların başarıyla eklenmesinin ardından audit kuralları yüklenmeli ve sistemdeki izleme süreci başlatılmalıdır.

CIS Benchmark v2.0.1-5.2.3.12 maddesinin olumlu sonuçlanması için, sistemin yeniden başlatılması gerekip gerekmediği kontrol edilmeli, eğer yeniden başlatma gerekiyorsa gerekli işlem yapılmalıdır. Bu işlem sistemdeki login ve logout olaylarının izlenmesini sağlayarak olası güvenlik tehditlerine karşı önceden önlem alınmasına yardımcı olur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemdeki login ve logout olaylarını izlemek için auditd servisini yapılandırmayı amaçlar. İlk olarak, auditd paketi yüklenir ve ardından auditd servisi başlatılır ve otomatik olarak başlaması sağlanır. Daha sonra, kullanıcıların giriş ve çıkış işlemlerini izlemek için gerekli olan denetim kuralları /etc/audit/rules.d/50-login.rules dosyasına eklenir. Bu kurallar, /var/log/lastlog ve /var/run/faillock dosyalarındaki yazma ve ekleme işlemlerini izler. Kurallar başarıyla eklendikten sonra, auditd servisi yeniden başlatılır ve yeni kurallar sisteme yüklenir. Son olarak, sistemin yeniden başlatılması gerekip gerekmediği kontrol edilir. Eğer yeniden başlatma gerekli ise, ilgili işlem yapılır. Bu yapılandırma, login ve logout olaylarının izlenmesini sağlayarak olası güvenlik tehditlerini önceden tespit etmeye yardımcı olur.

```
#!/bin/bash

# 1. auditd paketini yükle
echo "Auditd paketini yüklüyor..."
sudo apt update
sudo apt install -y auditd

# 2. auditd servisini başlat ve otomatik başlatma için etkinleştir
echo "Auditd servisini başlatıyor..."
sudo systemctl start auditd
sudo systemctl enable auditd

echo "Login ve logout olaylarının izlenmesi yapılandırması başlatılıyor..."

# 1. Login ve logout izleme kuralları ekleniyor
```

```
echo "Izleme kuralları ekleniyor..."
echo -e "
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
" | sudo tee /etc/audit/rules.d/50-login.rules

# 2. Audit kurallarını yükle
echo "Audit kuralları yükleniyor..."
sudo augenrules --load

# 3. Yeniden başlatma gerekip gerekmediğini kontrol et
echo "Sistemin yeniden başlatılmasına gerek olup olmadığı kontrol ediliyor..."
if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then
    echo "Yeniden başlatma gereklidir."
else
    echo "Yeniden başlatma gerekmez."
fi

echo "Login ve logout olaylarının izleme yapılandırması başarıyla tamamlandı."
```

4.2.3. Dosya Sistemi Güvenli Erişim Düzenlemeleri

Güvenlik açısından en iyi uygulamalar, sistemin önemli dosyalarına ve çalışma dosyalarına yetkisiz erişimi engellemeyi amaçlar. Özellikle çalışma dosyalarının, kütüphanelerin ve yapılandırma dosyalarının (örneğin, SUID ve SGID dosyaları, kayıt dosyaları, cron dosyaları, başlangıç betikleri, /etc/passwd, /etc/shadow gibi kritik dosyalar) güvenli bir şekilde düzenlenmesi sistemin güvenliğini artırır. Bu dosyaların içeriği değiştirildiğinde, silindiğinde veya taşındığında, sistemin düzgün çalışmaması ve güvenlik açıklarının ortaya çıkması riski bulunur.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerini kullanarak, bir kurumun mevcut güvenlik durumunu değerlendirir. Bu denetimler, kurumların sistemlerini en iyi güvenlik uygulamalarına göre yapılandırmalarını sağlamak için rehberlik eder. “Dosya Sistemi Güvenli Erişim Düzenlemeleri” tedbiri, özellikle kritik dosyaların ve dizinlerin yetkilendirmelerinin amacına uygun olarak düzenlenmesini ve kurum politikaları doğrultusunda denetlenmesini önerir.

Bu tedbirler sistemdeki önemli dosyaların güvenliğini sağlamak ve en az yetki ilkesine uygun bir erişim düzeni oluşturmak için kritik bir adımdır. Çizelge 4.16’da, BİGR 5.1.2.3 maddesi, Dosya Sistemi Güvenli Erişim Düzenlemeleri tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.16. GNU/Linux işletim sistemi dosya sistemi güvenli erişim düzenlemeleri

Tedbir No.	Tedbir Adı	Tedbir Tanımı	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1
5.1.2.3	Dosya Sistemi Güvenli Erişim Düzenlemeleri	İçeriği değiştiğinde, silindiğinde veya taşındığında sistemin çalışmasını olumsuz yönde etkileyebilecek çalışma dosyalarının, kütüphanelerin ve yapılandırma dosyalarının (SUID ve SGID dosyaları, kayıt dosyaları, cron dosyaları, başlangıç betikleri, /etc/passwd, /etc/shadow vb.) yetkilendirmeleri amacına uygun şekilde düzenlenmeli ve kurum politikaları doğrultusunda denetlenmelidir. Varsayılan kullanıcı umask değeri en az yetki prensibine göre ayarlanmalıdır.	4.1.1 Ensure cron daemon is enabled 4.1.2 Ensure permissions on /etc/crontab are configured 4.1.3 Ensure permissions on /etc/cron.hourly are configured 4.1.4 Ensure permissions on /etc/cron.daily are configured 4.1.5 Ensure permissions on /etc/cron.weekly are configured 4.1.6 Ensure permissions on /etc/cron.monthly are configured 4.1.7 Ensure permissions on /etc/cron.d are configured 4.1.8 Ensure at/cron is restricted to authorized users 5.2.3.5 Ensure events that modify the system's network environment are collected 5.2.3.8 Ensure events that modify user/group information are collected 5.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected 6.1.1 Ensure permissions on /etc/passwd are configured 6.1.2 Ensure permissions on /etc/passwd- are configured 6.1.3 Ensure permissions on /etc/group are configured 6.1.4 Ensure permissions on /etc/group- are configured 6.1.5 Ensure permissions on /etc/shadow are configured 6.1.6 Ensure permissions on /etc/shadow- are configured 6.1.7 Ensure permissions on /etc/gshadow are configured 6.1.8 Ensure permissions on /etc/gshadow- are configured 6.1.11 Ensure world writable files and directories are secured

4.2.3.1. Cron Daemon'un Etkinleştirilmesi ve Aktif Etme Yapılandırması

Cron daemon, sistem üzerinde periyodik işlemleri otomatik olarak çalıştırmak için kullanılan önemli bir bileşendir. Çoğu GNU/Linux sisteminde bakım işlemleri, güvenlik izleme ve sistem güncellemeleri gibi rutin görevler cron aracılığıyla yapılır. Eğer sistemde belirli bir kullanıcı işi yoksa bile, sistemin bakımına dair görevlerin yerine getirilmesi için cron aktif olmalıdır.

Eğer cron kullanımı yerine başka bir zamanlama yöntemi (örneğin systemd zamanlayıcıları) tercih ediliyorsa, cron'un devre dışı bırakılması ve alternatif zamanlayıcı yöntemlerinin güvenli bir şekilde yapılandırılması gerekmektedir.

Yapılan testlerde, halihazırda bulunan Ubuntu 20.04 makinesinde CIS Benchmark v2.0.1-4.1.1 maddesi kapsamında, cron daemon'un etkin olduğu ve sistemde güvenlik işlemlerinin sorunsuz şekilde devam ettiği gözlemlenmiştir. Bu nedenle cron daemon zaten aktif olduğu için iyileştirme modelinde uygulanan sıkılaştırma kodu yazılmamıştır.

4.2.3.2. /etc/crontab Dosyasının İzinlerinin Yapılandırılması

Sistemdeki /etc/crontab dosyası, sistemdeki cron görevlerinin yönetildiği bir dosyadır. Bu dosya, zamanlanmış görevlerin hangi kullanıcının ve hangi komutların çalıştırılacağını belirtir. Dolayısıyla, bu dosyaya izinsiz erişim, sisteme zarar verebilecek değişikliklerin yapılmasına ya da bilgi sızdırılmasına yol açabilir. Özellikle dosyaya yazma izni olan kişiler, sistemdeki görevleri değiştirebilir ve yetkisiz erişim sağlayabilirler.

Bu güvenlik açığını engellemek için, /etc/crontab dosyasının sahipliği ve izinlerinin doğru bir şekilde yapılandırılması gerekmektedir. Öncelikle, dosyanın sahibi ve grubu yönetici (root) olmalıdır. Aksi takdirde, izinsiz kullanıcıların bu dosyaya erişmesi veya değişiklik yapması mümkün olabilir. Bunun için chown root:root /etc/crontab komutu ile dosyanın sahibi ve grubu yönetici (root) olarak değiştirilir.

Dosyanın yalnızca sahibi (root) tarafından okunup yazılabilir olması gerekir. Diğer kullanıcılar (grup ve diğerleri) bu dosyaya erişim sağlayamamalıdır. Sadece yönetici (root) kullanıcısı bu dosyayı okuyabilir ve yazabilir, diğer kullanıcıların herhangi bir erişimi engellenir. Bu işlem için chmod og-rwx /etc/crontab komutu kullanılır.

CIS Benchmark v2.0.1-4.1.2 tedbirleri, sistemdeki kritik cron görevlerinin güvenliğini sağlar ve izinsiz erişim riskini azaltır. Bu tür dosyalara doğru izinler verilerek, sistemin güvenliği artırılabilir ve potansiyel tehditler önlenebilir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemdeki /etc/crontab dosyasının sahipliğini ve izinlerini güvenli bir şekilde yapılandırmayı amaçlar. İlk olarak, crontab_izinlerini_ayarla fonksiyonu tanımlanır ve bu fonksiyonun içerisinde

/etc/crontab dosyasının sahipliği ve izinleri kontrol edilir. Eğer dosyanın sahibi veya grubu "root" değilse, chown root:root /etc/crontab komutu ile dosyanın sahipliği "root:root" olarak değiştirilir. Ardından, dosyanın izinleri kontrol edilir. Eğer izinler doğru şekilde ayarlanmamışsa (yalnızca root'un okuma ve yazma izni olmalı), chmod og-rwx /etc/crontab komutu ile diğer kullanıcıların erişimi engellenir. Eğer sahiplik veya izinler zaten doğruysa, betik uygun mesajları verir. Bu işlem, sistemdeki cron görevlerinin güvenliğini artırarak izinsiz erişimlere karşı koruma sağlar.

```
1. #!/usr/bin/env bash
2.
3. # /etc/crontab dosyasının sahipliğini ve izinlerini yapılandırma
4.
5. crontab_izinlerini_ayarla() {
6.   echo -e "\n - /etc/crontab dosyasının sahipliğini ve izinlerini yapılandırıyorum..."
7.
8.   # /etc/crontab dosyasının sahipliğini root:root olarak ayarlama
9.   if [ "$(stat -c %U /etc/crontab)" != "root" ] || [ "$(stat -c %G /etc/crontab)" !=
"root" ]; then
10.     chown root:root /etc/crontab
11.     echo -e " - /etc/crontab dosyasının sahipliğini root:root olarak değiştirdim"
12.   else
13.     echo -e " - /etc/crontab dosyasının sahipliği zaten root:root"
14.   fi
15.
16.   # /etc/crontab dosyasının izinlerini og-rwx olarak ayarlama
17.   if [ "$(stat -c %a /etc/crontab)" != "600" ]; then
18.     chmod og-rwx /etc/crontab
19.     echo -e " - /etc/crontab dosyasının izinlerini og-rwx olarak değiştirdim"
20.   else
21.     echo -e " - /etc/crontab dosyasının izinleri zaten doğru"
22.   fi
23. }
24.
25. # Ana işlem
26. crontab_izinlerini_ayarla
27.
28. echo -e "\n - /etc/crontab dosyasının izin yapılandırması tamamlandı\n"
```

4.2.3.3. /etc/cron.hourly Dosyasının İzinlerinin Yapılandırılması

/etc/cron.hourly dizini, sistemde her saat başı çalıştırılması gereken cron görevlerini barındıran bir dizindir. Bu dizindeki dosyalar, düzenli aralıklarla belirli sistem görevlerini yerine getiren betikler veya komutlar içerir. Dizine yazma izni vermek yetkisiz kullanıcıların sisteme zarar vermesine veya sistem yönetim görevlerini değiştirmesine neden olabilir. Bu neden ile dizinin sahiplik ve izinlerinin doğru bir şekilde yapılandırılması kritik öneme sahiptir.

Dizinin sahibi ve grubu yönetici (root) olarak ayarlanmalıdır. Aksi takdirde, yetkisiz kullanıcılar bu dosyalara erişebilir ve değişiklik yapabilirler. Bunu sağlamak

için, chown root:root /etc/cron.hourly komutu ile dizinin sahipliği ve grubu yönetici (root) olarak ayarlanır.

İkinci adımda, yalnızca yönetici (root) kullanıcısının bu dizini okuyup yazabilmesi gerekir. Diğer kullanıcıların, grupların ve herkesin bu dizine erişim hakkı olmamalıdır. Yalnızca yönetici (root) kullanıcısının dizini okuyup yazabileceği anlamına gelir, diğer tüm kullanıcılar bu dizine erişemez. Bu işlem için chmod 700 /etc/cron.hourly komutu kullanılır.

CIS Benchmark v2.0.1-4.1.3 düzenlemesi, yalnızca yetkilendirilmiş kullanıcıların bu kritik görev dosyalarına erişmesini ve değiştirmesini sağlar ve böylece sistemdeki görevlerin güvenliği korunmuş olur. Bu tür dizinlere yalnızca yönetici (root) erişimi vererek, potansiyel tehditlerin önüne geçilmiş olur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemdeki /etc/cron.hourly dizininin sahipliğini ve izinlerini güvenli bir şekilde yapılandırmayı amaçlar. İlk olarak, cron_hourly_izinlerini_ayarla fonksiyonu tanımlanır ve bu fonksiyonun içerisinde dizinin sahipliği ve izinleri kontrol edilir. Eğer dizinin sahibi veya grubu "root" değilse, chown root:root /etc/cron.hourly komutu ile dizinin sahipliği "root:root" olarak değiştirilir. Ardından, dizinin izinleri kontrol edilir. Eğer izinler doğru şekilde ayarlanmamışsa (yalnızca root'un okuma, yazma ve dizine erişim izni olmalı), chmod 700 /etc/cron.hourly komutu ile diğer kullanıcıların erişimi engellenir. Eğer sahiplik veya izinler zaten doğruysa, betik uygun mesajları verir.

```
#!/usr/bin/env bash

# /etc/cron.hourly dizini için sahiplik ve izinleri yapılandırma

cron_hourly_izinlerini_ayarla() {
   echo -e "\n - /etc/cron.hourly dizini için sahiplik ve izinleri yapılandırıyorum..."

   # /etc/cron.hourly dizininin sahipliğini root:root olarak ayarlama
   if [ "$(stat -c %U /etc/cron.hourly)" != "root" ] || [ "$(stat -c %G
/etc/cron.hourly)" != "root" ]; then
     chown root:root /etc/cron.hourly
     echo -e " - /etc/cron.hourly dizininin sahipliğini root:root olarak ayarladım"
   else
     echo -e " - /etc/cron.hourly dizininin sahipliği zaten root:root"
   fi

   # /etc/cron.hourly dizininin izinlerini 700 olarak ayarlama
   if [ "$(stat -c %a /etc/cron.hourly)" != "700" ]; then
     chmod 700 /etc/cron.hourly
     echo -e " - /etc/cron.hourly dizininin izinlerini 700 olarak ayarladım"
```

```
20.   else
21.     echo -e " - /etc/cron.hourly dizininin izinleri zaten 700"
22.   fi
23. }
24.
25. # Ana işlem
26. cron_hourly_izinlerini_ayarla
27.
28. echo -e "\n - /etc/cron.hourly dizini için sahiplik ve izinler başarıyla
yapılandırıldı\n"
```

4.2.3.4. /etc/cron.daily Dosyasının İzinlerinin Yapılandırılması

/etc/cron.daily dizini, sistemin her gün çalıştırması gereken cron görevlerini barındıran bir dizindir. Bu dizindeki dosyalar, cron tarafından belirli zamanlarda otomatik olarak çalıştırılmak üzere düzenlenir ve genellikle sistem yöneticileri tarafından yönetilir. Sistemdeki önemli cron görevlerini içeren bu dizine yetkisiz erişim, güvenlik açığına neden olabilir. Yazma izni verilmesi, kötü niyetli kullanıcıların bu dosyaları değiştirmesine olanak tanır ve potansiyel olarak kötü amaçlı yazılımların sistemde çalıştırılmasına yol açabilir. Okuma izni ise, bu dosyaların içeriğini öğrenerek, sistemdeki diğer güvenlik açıklarını hedeflemeye yönelik bilgi edinilmesini sağlayabilir.

Bu neden ile /etc/cron.daily dizini üzerinde uygun sahiplik ve izinlerin yapılandırılması önemlidir. Bu dizinin yalnızca yönetici (root) kullanıcısı tarafından erişilebilir olması sağlanmalıdır. Dizin sahipliği root:root olarak ayarlanmalı ve dosya izinleri yalnızca yönetici (root) kullanıcısının okuma, yazma ve çalıştırma yetkisine sahip olacak şekilde 700 olarak yapılandırılmalıdır. Bu yapılandırma ile diğer kullanıcıların ve grupların bu dizine erişimini engellenir ve sistemin güvenliği artırılır.

CIS Benchmark v2.0.1-4.1.4 işlemi, sistemdeki otomatik görevlerin düzgün çalışmasını sağlarken, yalnızca yetkili kullanıcıların bu görevleri değiştirme ve etkileme yeteneğine sahip olmasını garantiler. Bu tür güvenlik önlemleri, sistemin izinsiz erişime karşı korunmasına yardımcı olur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemdeki /etc/cron.daily dizininin sahiplik ve izinlerini güvenli bir şekilde yapılandırmayı amaçlar. Betik, ilk olarak cron_daily_izinlerini_ayarla adlı bir fonksiyon tanımlar. Bu fonksiyon, dizinin sahipliğini ve izinlerini kontrol eder ve gerektiğinde düzeltir. Eğer dizinin sahibi ya da grubu “root” değilse, chown root:root /etc/cron.daily komutu ile

dizinin sahipliği ve grubu “root” olarak ayarlanır. Ardından, dizinin izinleri kontrol edilir; eğer izinler doğru ayarlanmamışsa (yalnızca root kullanıcısının erişimi olması gerektiği gibi), chmod 700 /etc/cron.daily komutu ile yalnızca root kullanıcısının dizini okuma, yazma ve çalıştırma yetkisine sahip olması sağlanır. Diğer kullanıcıların ve grupların bu dizine erişimi engellenir. Bu yapılandırmalar, sistemin güvenliğini artırarak yalnızca yetkili kullanıcıların cron görevlerini değiştirmesini sağlar.

```
#!/usr/bin/env bash

# /etc/cron.daily dizini için sahiplik ve izinleri yapılandırma

cron_daily_izinlerini_ayarla() {
  echo -e "\n - /etc/cron.daily dizini için sahiplik ve izinleri yapılandırıyorum..."

  # /etc/cron.daily dizininin sahipliğini root:root olarak ayarlama
  if [ "$(stat -c %U /etc/cron.daily)" != "root" ] || [ "$(stat -c %G /etc/cron.daily)"
!= "root" ]; then
    chown root:root /etc/cron.daily
    echo -e " - /etc/cron.daily dizininin sahipliğini root:root olarak ayarladım"
  else
    echo -e " - /etc/cron.daily dizininin sahipliği zaten root:root"
  fi

  # /etc/cron.daily dizininin izinlerini 700 olarak ayarlama
  if [ "$(stat -c %a /etc/cron.daily)" != "700" ]; then
    chmod 700 /etc/cron.daily
    echo -e " - /etc/cron.daily dizininin izinlerini 700 olarak ayarladım"
  else
    echo -e " - /etc/cron.daily dizininin izinleri zaten 700"
  fi
}

# Ana işlem
cron_daily_izinlerini_ayarla

echo -e "\n - /etc/cron.daily dizini için sahiplik ve izinler başarıyla
yapılandırıldı\n"
```

4.2.3.5. /etc/cron.weekly Dosyasının İzinlerinin Yapılandırılması

/etc/cron.weekly dizini, sistemin haftalık olarak çalıştırması gereken cron görevlerini içerir. Bu dizindeki dosyalar, genellikle sistem yöneticileri tarafından metin editörleri ile düzenlenir, çünkü crontab komutlarıyla doğrudan manipüle edilemezler. Dizin üzerinde uygun erişim izinleri yapılandırılmadığı takdirde, bu dosyalar kötü niyetli kullanıcılar tarafından manipüle edilebilir ve bu da ciddi güvenlik açıklarına yol açabilir.

Dizin üzerinde yazma izninin, yalnızca sistem yöneticisi olan root kullanıcısına verilmesi gerekir. Bunun dışındaki kullanıcıların yazma erişimi olmamalıdır. Aynı

şekilde, okuma izninin de yalnızca yönetici (root) kullanıcısına verilmesi gerekmektedir. Bu şekilde yalnızca yetkili kullanıcıların bu dosyalar üzerinde değişiklik yapması sağlanır. Alınacak bu önlem yetkisiz kullanıcıların sistemdeki görevler hakkında bilgi edinmelerini engeller ve kötüye kullanım olasılıklarını ortadan kaldırır.

CIS Benchmark v2.0.1-4.1.5 maddesinde sistemde başka yöntemler kullanılıyorsa (örneğin, systemd zamanlayıcıları gibi), cron kaldırılmalı ve alternatif yöntem güvenlik politikalarına uygun şekilde yapılandırılmalıdır. Bu tür güvenlik önlemleri, sistemin iç işleyişine dair hassas bilgilerin kötüye kullanılmasını engelleyerek, sistemin bütünlüğünü korur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, /etc/cron.weekly dizininin sahiplik ve izinlerini güvenli bir şekilde yapılandırmayı amaçlar. Betik, cron_haftalik_izinlerini_ayarla adında bir fonksiyon tanımlar. Bu fonksiyon, dizinin sahipliğini ve izinlerini kontrol eder ve gerektiğinde düzeltir. İlk olarak, dizinin sahipliğinin "root:root" olup olmadığı kontrol edilir. Eğer dizinin sahibi veya grubu root değilse, chown root:root /etc/cron.weekly komutu ile sahiplik ayarlanır. Ardından, dizinin izinleri kontrol edilir; eğer izinler doğru ayarlanmamışsa (yani yalnızca root kullanıcısının okuma, yazma ve çalıştırma yetkisine sahip olması gerektiği gibi), chmod 700 /etc/cron.weekly komutu ile bu izinler düzenlenir. Bu yapılandırma, yalnızca root kullanıcısının dizine erişim sağlayabilmesini ve dizindeki dosyaların güvenli bir şekilde korunmasını sağlar. Diğer tüm kullanıcıların bu dizine erişimi engellenir.

```
1. #!/usr/bin/env bash
2.
3. # /etc/cron.weekly dizini için sahiplik ve izinleri yapılandırma
4.
5. cron_haftalik_izinlerini_ayarla() {
6.   echo -e "\n - /etc/cron.weekly dizini için sahiplik ve izinleri yapılandırıyorum..."
7.
8.   # /etc/cron.weekly dizininin sahipliğini root:root olarak ayarlama
9.   if [ "$(stat -c %U /etc/cron.weekly)" != "root" ] || [ "$(stat -c %G
/etc/cron.weekly)" != "root" ]; then
10.     chown root:root /etc/cron.weekly
11.     echo -e " - /etc/cron.weekly dizininin sahipliğini root:root olarak ayarladım"
12.   else
13.     echo -e " - /etc/cron.weekly dizininin sahipliği zaten root:root"
14.   fi
15.
16.   # /etc/cron.weekly dizininin izinlerini 700 olarak ayarlama
17.   if [ "$(stat -c %a /etc/cron.weekly)" != "700" ]; then
18.     chmod 700 /etc/cron.weekly
19.     echo -e " - /etc/cron.weekly dizininin izinlerini 700 olarak ayarladım"
20.   else
```

```
21.     echo -e " - /etc/cron.weekly dizininin izinleri zaten 700"
22.   fi
23. }
24.
25. # Ana işlem
26. cron_haftalik_izinlerini_ayarla
27.
28. echo -e "\n - /etc/cron.weekly dizini için sahiplik ve izinler başarıyla
yapılandırıldı\n"
```

4.2.3.6. /etc/cron.monthly Dosyasının İzinlerinin Yapılandırılması

/etc/cron.monthly dizini, sistemdeki aylık olarak çalıştırılması gereken cron görevlerini içerir. Bu dosyalar genellikle crontab komutlarıyla değil, sistem yöneticileri tarafından metin editörleri ile düzenlenir. Bu dizin ve içeriğindeki dosyalar, yalnızca yetkili kullanıcılar tarafından erişilebilir ve düzenlenebilir olmalıdır.

Dizin üzerinde yazma ve okuma izinlerinin yalnızca yönetici (root) kullanıcısına verilmesi gerekir. Diğer kullanıcıların bu dizine erişim izinlerinin olmaması sistemdeki kritik görevlerin kötüye kullanılmasını engeller. Aynı zamanda yazma erişiminin sadece yönetici kullanıcılarına verilmesi, kötü niyetli kullanıcıların izinsiz değişiklikler yapmasını engeller.

CIS Benchmark v2.0.1-4.1.6 tedbirine göre eğer sistemde başka zamanlayıcılar (örneğin, systemd zamanlayıcıları) kullanılıyorsa, cron kaldırılmalı ve alternatif yöntemler güvenlik politikalarına uygun şekilde yapılandırılmalıdır. Bu güvenlik önlemi, yalnızca yetkili kullanıcıların dizin ve dosyalar üzerinde değişiklik yapabilmesini sağlayarak, sistemin bütünlüğünü ve güvenliğini korur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, /etc/cron.monthly dizininin sahiplik ve izinlerini doğru bir şekilde yapılandırmayı amaçlar. Betik, cron_aylik_izinlerini_ayarla adında bir fonksiyon tanımlar. Bu fonksiyon, dizinin sahipliğini ve izinlerini kontrol eder ve gerektiğinde düzeltir. İlk olarak, dizinin sahipliğinin "root:root" olup olmadığı kontrol edilir. Eğer dizinin sahibi veya grubu root değilse, chown root:root /etc/cron.monthly komutu ile sahiplik ayarlanır. Ardından, dizinin izinleri kontrol edilir; eğer izinler doğru ayarlanmamışsa (yani yalnızca root kullanıcısının okuma, yazma ve çalıştırma yetkisine sahip olması gerektiği gibi), chmod 700 /etc/cron.monthly komutu ile bu izinler düzenlenir. Bu yapılandırma, yalnızca root

kullanıcısının dizine erişim sağlayabilmesini ve dizindeki dosyaların güvenli bir şekilde korunmasını sağlar.

```
#!/usr/bin/env bash

# /etc/cron.monthly dizini için sahiplik ve izinleri yapılandırma

cron_aylik_izinlerini_ayarla() {
   echo -e "\n - /etc/cron.monthly dizini için sahiplik ve izinleri yapılandırıyorum..."

   # /etc/cron.monthly dizininin sahipliğini root:root olarak ayarlama
   if [ "$(stat -c %U /etc/cron.monthly)" != "root" ] || [ "$(stat -c %G
/etc/cron.monthly)" != "root" ]; then
      chown root:root /etc/cron.monthly
      echo -e " - /etc/cron.monthly dizininin sahipliğini root:root olarak ayarladım"
   else
      echo -e " - /etc/cron.monthly dizininin sahipliği zaten root:root"
   fi

   # /etc/cron.monthly dizininin izinlerini 700 olarak ayarlama
   if [ "$(stat -c %a /etc/cron.monthly)" != "700" ]; then
      chmod 700 /etc/cron.monthly
      echo -e " - /etc/cron.monthly dizininin izinlerini 700 olarak ayarladım"
   else
      echo -e " - /etc/cron.monthly dizininin izinleri zaten 700"
   fi
}

# Ana işlem
cron_aylik_izinlerini_ayarla

echo -e "\n - /etc/cron.monthly dizini için sahiplik ve izinler başarıyla
yapılandırıldı\n"
```

4.2.3.7. /etc/cron.d Dosyasının İzinlerinin Yapılandırılması

/etc/cron.d dizini, /etc/crontab gibi sistemdeki cron işlerinin daha ayrıntılı bir şekilde zamanlanmasını sağlayan görev dosyalarını içerir. Bu dizindeki dosyalar, crontab komutu ile değil, sistem yöneticileri tarafından metin editörleri ile düzenlenir. Bu dosyaların yalnızca yönetici (root) kullanıcısı tarafından okunabilir ve yazılabilir olması gerektiğinden, diğer kullanıcıların bu dosyalara erişimi sınırlanmalıdır.

Eğer cron yerine başka zamanlayıcılar (örneğin, systemd zamanlayıcıları) kullanılıyorsa, cron kaldırılmalı ve alternatif yöntemler güvenlik politikalarına uygun şekilde yapılandırılmalıdır. Bu dizindeki dosyaların yazma erişimi sadece yetkili kullanıcılar tarafından yapılabilmelidir, aksi takdirde yetkisiz kullanıcılar sisteme zarar verebilir ya da kötüye kullanabilir.

CIS Benchmark v2.0.1-4.1.7 maddesinde bu dizindeki dosyaların yalnızca yönetici (root) kullanıcıları tarafından erişilmesi sağlanarak, sistemin güvenliği artırılır ve izinsiz erişimlerin önüne geçilir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, /etc/cron.d dizininin sahiplik ve izinlerini doğru şekilde yapılandırmayı amaçlar. Betik, cron_d_izinlerini_ayarla adında bir fonksiyon tanımlar. Fonksiyon, dizinin sahipliğini ve izinlerini kontrol eder, ve gerektiğinde düzeltir. İlk olarak, dizinin sahipliğinin "root:root" olup olmadığını kontrol eder. Eğer dizinin sahibi veya grubu root değilse, chown root:root /etc/cron.d komutu ile sahiplik root:root olarak ayarlanır. Ardından, dizinin izinleri kontrol edilir; eğer dizinin izinleri 700 olarak ayarlanmamışsa, yani yalnızca root kullanıcısının okuma, yazma ve çalıştırma yetkisine sahip olduğu belirtilen izinler yoksa, chmod 700 /etc/cron.d komutu ile izinler doğru şekilde ayarlanır. Bu ayar, yalnızca root kullanıcısının bu dizine erişebilmesini ve dizindeki dosyaların güvenli bir şekilde korunmasını sağlar. Diğer kullanıcıların bu dizine erişimi engellenmiş olur, böylece sistemin güvenliği artar ve izinsiz erişimler önlenir.

```
1. #!/usr/bin/env bash
2.
3. # /etc/cron.d dizini için sahiplik ve izinleri yapılandırma
4.
5. cron_d_izinlerini_ayarla() {
6.   echo -e "\n - /etc/cron.d dizini için sahiplik ve izinleri yapılandırıyorum..."
7.
8.   # /etc/cron.d dizininin sahipliğini root:root olarak ayarlama
9.   if [ "$(stat -c %U /etc/cron.d)" != "root" ] || [ "$(stat -c %G /etc/cron.d)" !=
"root" ]; then
10.     chown root:root /etc/cron.d
11.     echo -e " - /etc/cron.d dizininin sahipliğini root:root olarak ayarladım"
12.   else
13.     echo -e " - /etc/cron.d dizininin sahipliği zaten root:root"
14.   fi
15.
16.   # /etc/cron.d dizininin izinlerini 700 olarak ayarlama
17.   if [ "$(stat -c %a /etc/cron.d)" != "700" ]; then
18.     chmod 700 /etc/cron.d
19.     echo -e " - /etc/cron.d dizininin izinlerini 700 olarak ayarladım"
20.   else
21.     echo -e " - /etc/cron.d dizininin izinleri zaten 700"
22.   fi
23. }
24.
25. # Ana işlem
26. cron_d_izinlerini_ayarla
27.
28. echo -e "\n - /etc/cron.d dizini için sahiplik ve izinler başarıyla yapılandırıldı\n"
```

4.2.3.8. Cron Yetkili Kullanıcılara Sınırlanma Yapılandırması

Cron servisini yalnızca belirli kullanıcıların kullanmasına izin vermek için /etc/cron.allow dosyasını yapılandırmak gerekir. Eğer bu dosya mevcut değilse, /etc/cron.deny dosyası kontrol edilir. Ancak bu dosyada yer almayan herhangi bir kullanıcı cron hizmetini kullanabilir. Bu durumda yalnızca /etc/cron.allow dosyasında belirtilen kullanıcılar cron hizmetini kullanabilir.

- Eğer bir kullanıcı, /etc/cron.allow dosyasına eklenmemişse, bu kullanıcı yine de cron işleri çalıştırabilir. Ancak /etc/cron.allow dosyası yalnızca cron işlerini planlamak ve düzenlemek için kimlerin izinli olduğunu kontrol eder.
- Birçok sistemde yalnızca sistem yöneticisinin cron işleri planlamaya yetkisi vardır. /etc/cron.allow dosyasını kullanarak yalnızca yetkili kullanıcıların cron servisinden yararlanmasını sağlamak bu politikayı güçlendirir. Bir "allow" listesi, "deny" listesine göre daha yönetilebilir bir yaklaşımdır çünkü "deny" listesinde kullanıcı eklemek unutulabilir.

CIS Benchmark v2.0.1-4.1.8 tedbirinde, cron hizmetinin sadece belirli yetkili kullanıcılar tarafından kullanılmasına izin verilir ve sistemin güvenliği sağlanmış olur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, cron hizmetini yalnızca yetkili kullanıcılara sınırlamak amacıyla yapılandırma yapar. Betik, cron_izinlerini_kisitla fonksiyonunu kullanarak /etc/cron.deny dosyasını kaldırır (varsa) ve /etc/cron.allow dosyasını oluşturur (yoksa). Bu işlem, yalnızca cron işlerini kullanmaya yetkili olan kullanıcıların belirli bir dosyada listelenmesini sağlar. Eğer /etc/cron.allow dosyası mevcut değilse, betik bu dosyayı oluşturur ve ardından dosyanın izinlerini chmod 600 komutu ile kısıtlar; yani yalnızca root kullanıcısı tarafından okunabilir ve yazılabilir hale gelir. Ayrıca, dosyanın sahipliğini root:root olarak ayarlayıp, grubunu crontab olarak değiştirir. Böylece, yalnızca yetkili kullanıcılar cron işlerini planlayabilir ve çalıştırabilir. Bu yapılandırma, sistemin güvenliğini artırır ve izinsiz cron kullanımlarını engeller, yalnızca belirlenen kullanıcıların cron hizmetine erişmesini sağlar.

```
#!/usr/bin/env bash

# Cron icin yetkili kullanicilari kisitlama islemi

cron_izinlerini_kisitla() {
   echo -e " - Cron icin yetkili kullanicilari kisitlama islemi baslatiliyor..."

   # /etc/cron.deny dosyasini kaldirma (eger varsa)
   if [ -e /etc/cron.deny ]; then
      echo -e " - /etc/cron.deny dosyasi bulunuyor, kaldiriliyor..."
      rm -f /etc/cron.deny
   fi

   # /etc/cron.allow dosyasini olusturma (eger yoksa)
   if [ ! -e /etc/cron.allow ]; then
     echo -e " - /etc/cron.allow dosyasi bulunmuyor, olusturuluyor..."
     touch /etc/cron.allow
   fi

   # Dosya izinlerini kisitlama
   chmod 600 /etc/cron.allow
   chown root:root /etc/cron.allow
   chgrp crontab /etc/cron.allow

   echo -e " - Cron kullanici kisitlamasi islemi tamamlandi."
}

# Ana islem
cron_izinlerini_kisitla

echo -e "\n - Cron icin yetkili kullanici kisitlama islemi tamamlandi.\n"
```

4.2.3.9. Sistemin Ağ Ortamı Değişikliklerinin Kayıt Edilmesi

Bu işlem sistemin ağ çevresi ile ilgili değişikliklerin izlenmesini sağlar. Sistem yöneticileri, ağ ayarlarını ve yapılandırmalarını değiştirebilirler ancak bu tür değişiklikler bazen kötü niyetli kişiler tarafından güvenlik açıkları yaratmak amacıyla yapılabilir. Bu nedenle ağla ilgili kritik dosyaların ve sistem çağrılarının izlenmesi önemlidir.

- /etc/issue ve /etc/issue.net: Kullanıcı girişinden önce görünen mesajlar. Bu dosyalar, saldırganlar tarafından kullanıcıları aldatmak amacıyla değiştirilebilir.
- /etc/hosts: IP adresleri ile ana bilgisayar adlarının eşleştiği dosya. Bu dosya değiştirilirse yanlış IP adreslerine yönlendirme yapılabilir ve sistem güvenliği tehlikeye girebilir.
- /etc/networks: Ağ adlarını barındırır. Değişiklikler ağ yapılandırmasında istenmeyen sonuçlara yol açabilir.

- /etc/network/: Ağ arayüzleriyle ilgili yapılandırma dosyalarını içerir. Buradaki değişiklikler sistemin ağ bağlantısının bozulmasına veya başka sistemlere sızılmasına neden olabilir.

Bu kurallar, ağ çevresiyle ilgili yapılan değişiklikleri izlemeyi sağlar ve şüpheli aktivitelerin tespit edilmesine yardımcı olur. CIS Benchmark v2.0.1-5.2.3.5 maddesi tedbirini karşılamaktadır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemdeki ağ çevresiyle ilgili yapılan değişikliklerin izlenmesini sağlamak amacıyla auditd paketini yükler, gerekli izleme kurallarını ekler ve ardından bu kuralları uygulamaya alır. İlk olarak, auditd servisi yüklenir, başlatılır ve otomatik başlatma için etkinleştirilir. Daha sonra, sistemin 64-bit ya da 32-bit olup olmadığı kontrol edilerek, her iki platform için uygun izleme kuralları /etc/audit/rules.d/50-system_locale.rules dosyasına eklenir. Bu kurallar, ağ yapılandırma dosyalarında (örneğin, /etc/issue, /etc/hosts, /etc/network/) yapılan değişiklikleri izlemeyi amaçlar. Eklenen kurallar, bu dosyaların üzerinde yazma (w) ve erişim (r) işlemlerini izleyerek, ağ yapılandırmalarındaki herhangi bir değişikliği kaydeder. Son olarak, augenrules komutu ile kurallar yüklenir ve sistemin yeniden başlatılması gerek olup olmadığı kontrol edilir.

```
#!/bin/bash

# 1. auditd paketini yükle
echo "Auditd paketini yüklüyor..."
sudo apt update
sudo apt install -y auditd

# 2. auditd servisini başlat ve otomatik başlatma için etkinleştir
echo "Auditd servisini başlatıyor..."
sudo systemctl start auditd
sudo systemctl enable auditd

echo "Sistemin ağ çevresine dair değişikliklerin izlenmesi yapılandırması başlatılıyor..."

# 64-bit ve 32-bit sistemlere uygun izleme kuralları ekleniyor
echo "Izleme kuralları ekleniyor..."
if [ "$(getconf LONG_BIT)" = "64" ]; then
    echo -e "
    -a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
    -a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
    -w /etc/issue -p wa -k system-locale
    -w /etc/issue.net -p wa -k system-locale
    -w /etc/hosts -p wa -k system-locale
    -w /etc/networks -p wa -k system-locale
    -w /etc/network/ -p wa -k system-locale
    " | sudo tee /etc/audit/rules.d/50-system_locale.rules
else
```

```
    echo -e "
    -a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
    -w /etc/issue -p wa -k system-locale
    -w /etc/issue.net -p wa -k system-locale
    -w /etc/hosts -p wa -k system-locale
    -w /etc/networks -p wa -k system-locale
    -w /etc/network/ -p wa -k system-locale
    " | sudo tee /etc/audit/rules.d/50-system_locale.rules
fi

# 2. Audit kurallarını yükle
echo "Audit kuralları yükleniyor..."
sudo augenrules --load

# 3. Yeniden başlatma gerekip gerekmediğini kontrol et
echo "Sistemin yeniden başlatılmasına gerek olup olmadığı kontrol ediliyor..."
if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then
    echo "Yeniden başlatma gereklidir."
else
    echo "Yeniden başlatma gerekmez."
fi

echo "Sistemin ağ çevresi izleme yapılandırması başarıyla tamamlandı."
```

4.2.3.10. Kullanıcı/Grup Bilgisi Değişikliklerinin Kayıt Edilmesi

Kullanıcı ve grup bilgilerini, şifreleri ve eski şifreleri içeren dosyalardaki değişiklikleri izlemek kritik öneme sahiptir. Bu tür değişiklikler, özellikle bir sistemin güvenliği söz konusu olduğunda olası yetkisiz erişimlerin veya kötü niyetli eylemlerin tespiti için önemlidir. Aşağıda kullanıcı ve grup bilgisi içeren dosyalar sunulmuştur.

- /etc/group - sistem grupları
- /etc/passwd - sistem kullanıcıları
- /etc/gshadow - her grup için şifrelerin şifrelenmiş halleri
- /etc/shadow - sistem kullanıcılarının şifreleri
- /etc/security/opasswd - eski şifrelerin saklanması (gerektiği takdirde PAM modülü kullanılır)

Bu dosyalardaki beklenmedik değişiklikler, sistemin ele geçirilmiş olabileceğine dair bir belirti olabilir. Bu nedenle bu dosyalar üzerinde yapılan yazma işlemleri ve dosya izinlerinde yapılan değişiklikler audit loglarına kaydedilmelidir.

CIS Benchmark v2.0.1-5.2.3.8 maddesine göre bu işlemde, kullanıcı ve grup bilgilerini içeren dosyaların değiştirilmesiyle ilgili olayların izlenmesi sağlanacaktır. İlk olarak, auditd paketi sisteme yüklenecek ve bu servis başlatılmalıdır. Daha sonra,

/etc/audit/rules.d/50-identity.rules dosyasına, /etc/group, /etc/passwd, /etc/gshadow, /etc/shadow, ve /etc/security/opasswd dosyalarına yönelik izleme kuralları eklenmelidir. Bu kurallar, dosyalar üzerinde yapılan yazma ve erişim değişikliklerini izleyecek şekilde yapılandırılmalı ve her bir değişiklik "identity" anahtar kelimesiyle işaretlenmelidir. Bu adımlar, sistemdeki kullanıcı ve grup bilgilerini içeren dosyalarda meydana gelen değişikliklerin kaydedilmesini ve denetlenmesini sağlayacaktır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, kullanıcı ve grup bilgileri içeren kritik dosyalardaki değişikliklerin izlenmesini sağlamak amacıyla yapılandırılır. İlk olarak, auditd paketi yüklenir ve servis başlatılır, böylece sistemdeki güvenlik olayları izlenebilir hale gelir. Daha sonra, ağ yapılandırmaları ve kimlik bilgileriyle ilgili dosyalara (örneğin, /etc/group, /etc/passwd, /etc/gshadow, /etc/shadow, /etc/security/opasswd) yönelik izleme kuralları eklenir. Bu kurallar, dosyalar üzerindeki yazma (w) ve erişim (a) işlemlerini izleyerek, herhangi bir değişikliği kaydeder ve bu değişiklikler "identity" anahtar kelimesiyle işaretlenir. Kurallar /etc/audit/rules.d/50-identity.rules dosyasına eklenir, ardından augenrules komutu ile yüklenir. Son olarak, sistemin yeniden başlatılmasına gerek olup olmadığı kontrol edilir.

```
1. #!/bin/bash
2.
3. # 1. auditd paketini yükle
4. echo "Auditd paketini yüklüyor..."
5. sudo apt update
6. sudo apt install -y auditd
7.
8. # 2. auditd servisini başlat ve otomatik başlatma için etkinleştir
9. echo "Auditd servisini başlatıyor..."
10. sudo systemctl start auditd
11. sudo systemctl enable auditd
12.
13. echo "User ve grup bilgisi izleme yapılandırması başlatılıyor..."
14.
15. # 1. İlgili izleme kurallarını /etc/audit/rules.d/50-identity.rules dosyasına ekleyin
16. echo "Izleme kuralları ekleniyor..."
17. echo -e "
18. -w /etc/group -p wa -k identity
19. -w /etc/passwd -p wa -k identity
20. -w /etc/gshadow -p wa -k identity
21. -w /etc/shadow -p wa -k identity
22. -w /etc/security/opasswd -p wa -k identity
23. " | sudo tee /etc/audit/rules.d/50-identity.rules
24.
25. # 2. Audit kurallarını yükle
26. echo "Audit kuralları yükleniyor..."
27. sudo augenrules --load
28.
29. # 3. Yeniden başlatma gerekip gerekmediğini kontrol et
30. echo "Sistemin yeniden başlatılmasına gerek olup olmadığı kontrol ediliyor..."
31. if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then
32.     echo "Yeniden başlatma gereklidir."
```

```
33. else
34.     echo "Yeniden başlatma gerekmez."
35. fi
36.
37. echo "User ve grup bilgisi izleme yapılandırması başarıyla tamamlandı."
```

4.2.3.11. Zorunlu Erişim Kontrolü Değişikliklerinin Toplanması

Sistem üzerinde zorunlu erişim denetimlerini (Mandatory Access Control) izlemek ve özellikle AppArmor'ı izlemek için, AppArmor yapılandırma dosyalarının bulunduğu dizinlere yönelik denetim kuralları oluşturulmalıdır. İzlenmesi gereken dizinler, /etc/apparmor/ ve /etc/apparmor.d/'dir. Bu dizinlerdeki herhangi bir değişiklik dosya değiştirme veya özellik değişikliği izlenmelidir.

Auditd servisi sistemde yüklü ve çalışır durumda olmalıdır. Eğer yüklü değilse auditd paketini sisteme eklemek gereklidir. Paket yüklendikten sonra auditd servisi başlatılmalı ve otomatik olarak sistem açılışında başlaması sağlanmalıdır. Audit kuralları /etc/audit/rules.d/ dizininde oluşturulmalıdır. Kurallar eklendikten sonra, bu kurallar audit sistemine yüklenmeli ve izlemeye başlanmalıdır. Yapılan değişikliklerin etkin olabilmesi için sistemin yeniden başlatılması gerekip gerekmediği kontrol edilmelidir. CIS Benchmark v2.0.1-5.2.3.14 tedbiri AppArmor yapılandırma dosyalarındaki izinsiz değişikliklerin kaydedilmesini sağlayarak sistem güvenliğini korumaya yardımcı olur.

Aşağıda bulunan iyileştirme modelindeki bash komutu, zorunlu erişim denetimlerini (MAC - Mandatory Access Control) izlemek amacıyla AppArmor yapılandırma dosyalarındaki değişiklikleri takip etmek için bir dizi adımı otomatikleştirir. İlk olarak, sistemde auditd paketinin yüklenmesi sağlanır ve ardından auditd servisi başlatılır ve otomatik olarak açılışta başlatılması için yapılandırılır. Audit kuralları için gerekli dizin, /etc/audit/rules.d/, oluşturulur (eğer mevcut değilse). Sonra, AppArmor yapılandırma dosyalarının bulunduğu /etc/apparmor/ ve /etc/apparmor.d/ dizinlerinde yapılan değişikliklerin izlenmesi amacıyla MAC politikalarını belirleyen kurallar yazılır. Bu kurallar, dosyaların üzerinde yazma (w) ve erişim (r) işlemlerini izlemeyi sağlayacak şekilde yapılandırılır ve 50-MAC-policy.rules dosyasına eklenir. Ardından, kurallar augenrules komutu ile yüklenir. Son olarak, sistemin yeniden başlatılıp başlatılmaması gerektiği kontrol edilir. Bu işlem, AppArmor

yapılandırmalarındaki olası izinsiz değişikliklerin kaydedilmesini ve güvenliğin artırılmasını sağlar.

```
#!/bin/bash

# 1. auditd paketini yükle
echo "Auditd paketini yüklüyor..."
sudo apt update
sudo apt install -y auditd

# 2. auditd servisini başlat ve otomatik başlatma için etkinleştir
echo "Auditd servisini başlatıyor..."
sudo systemctl start auditd
sudo systemctl enable auditd

# 3. /etc/audit/rules.d/ dizini mevcut değilse oluştur
echo "Audit kural dosyası dizinini oluşturuyor..."
sudo mkdir -p /etc/audit/rules.d/

# 4. Kuralları /etc/audit/rules.d/50-MAC-policy.rules dosyasına ekle
echo "MAC izleme kurallarını ekliyor..."
echo -e "
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
" | sudo tee /etc/audit/rules.d/50-MAC-policy.rules

# 5. Kuralları yükle
echo "Audit kurallarını yüklüyor..."
sudo augenrules --load

# 6. Yeniden başlatma gereksinimini kontrol et
echo "Yeniden başlatma gereksinimi kontrol ediliyor..."
if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then
    echo "Reboot required to load rules"
else
    echo "Audit kuralları başarıyla yüklendi."
fi

echo "MAC izleme yapılandırması başarıyla tamamlandı."
```

4.2.3.12. /etc/passwd İzinleri Yapılandırılması

/etc/passwd dosyası, sistemdeki kullanıcı hesaplarına dair bilgileri içeren ve birçok sistem aracı tarafından kullanılan kritik bir dosyadır. Bu dosyanın doğru şekilde yapılandırılması, sistem güvenliği açısından büyük önem taşır. Eğer bu dosyanın izinleri yanlış yapılandırılırsa, yetkisiz kullanıcılar bu dosyayı değiştirebilir ve sistemin güvenliği tehlikeye girebilir. Yapılan testlerde, mevcut bir GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/passwd dosyasının sahiplik ve izinleri doğru bir şekilde yapılandırıldığından, sistemde herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle, /etc/passwd dosyasının güvenliği sağlandığı için iyileştirme kodu yazılmamıştır.

4.2.3.13. /etc/passwd~ İzinleri Yapılandırılması

/etc/passwd~ dosyası, /etc/passwd dosyasının yedeğini tutar. Bu dosyanın da güvenliği tıpkı ana dosya gibi korunmalıdır. Yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/passwd- dosyasının korunması sağlandığından herhangi bir güvenlik ihlali meydana gelmemiştir. Bu nedenle, bu dosyanın yedeği zaten korunmuş olduğundan, ek bir sıkılaştırma işlemi uygulanmamıştır.

4.2.3.14. /etc/group İzinleri Yapılandırılması

/etc/group dosyası, sistemdeki grupların listesini içerir. Bu dosyanın sadece root kullanıcısı tarafından yazılabilir olması ve tüm kullanıcılar tarafından okunabilir olması gerekmektedir. Yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/group dosyasının doğru şekilde yapılandırıldığı ve sadece gerekli izinlerin verildiği tespit edilmiştir. Bu nedenle, sistemde herhangi bir güvenlik ihlali bulunmadığı için iyileştirme kodu eklenmemiştir.

4.2.3.15. /etc/group~ İzinleri Yapılandırılması

/etc/group- dosyası, /etc/group dosyasının yedeğini tutar. Bu dosya da tıpkı ana dosya gibi korunmalıdır. Yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/group- dosyasının yedeği güvenli bir şekilde saklandığı için, güvenlik açığına rastlanmamıştır. Bu nedenle, yedek dosyanın güvenliği zaten sağlandığı için ek bir sıkılaştırma işlemi yapılmamıştır.

4.2.3.16. /etc/shadow İzinleri Yapılandırılması

/etc/shadow dosyası, kullanıcı hesaplarının şifre bilgilerini ve diğer güvenlik bilgilerini saklar. Bu dosyaya yetkisiz erişim, şifrelerin kırılmasına ve diğer güvenlik bilgilerine ulaşılmasına yol açabilir. Yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/shadow dosyasının doğru izinlerle yapılandırılması sonucu herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle, dosyanın güvenliği zaten sağlandığından iyileştirme kodu eklenmemiştir.

4.2.3.17. /etc/shadow~ İzinleri Yapılandırılması

/etc/shadow- dosyası, /etc/shadow dosyasının yedeğini tutar. Bu dosyanın güvenliği, ana dosya kadar önemli olup, yanlışlıkla ya da kötü niyetli müdahalelerle değiştirilebilir. Yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/shadow- dosyasının yedeği güvenli bir şekilde yapılandırıldığından, herhangi bir güvenlik ihlali meydana gelmemiştir. Bu nedenle, yedek dosyanın güvenliği sağlandığı için ek bir sıkılaştırma kodu yazılmamıştır.

4.2.3.18. /etc/gshadow İzinleri Yapılandırılması

/etc/gshadow dosyası, grup bilgilerini ve şifre bilgilerini saklar. Bu dosyaya yetkisiz erişim, grup şifrelerinin çözülmesine ve grup güvenliğinin tehlikeye girmesine yol açabilir. Yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/gshadow dosyası doğru izinlerle yapılandırıldığından, herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle, dosyanın güvenliği zaten sağlandığı için iyileştirme kodu eklenmemiştir.

4.2.3.19. /etc/gshadow~ İzinleri Yapılandırılması

/etc/gshadow- dosyası, /etc/gshadow dosyasının yedeğini tutar. Yedek dosyanın da güvenli bir şekilde korunması gerekmektedir. Yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde, /etc/gshadow- dosyasının güvenliği sağlandığından herhangi bir güvenlik ihlali bulunmamıştır. Bu nedenle, yedek dosyanın güvenliği sağlandığı için ek bir sıkılaştırma kodu yazılmamıştır.

4.2.3.20. Dosya ve Dizinlerin Yazma Yapılandırılması

CIS Benchmark v2.0.1-6.1.11 “Ensure world writable files and directories are secured” maddesi, bilgisayar üzerindeki yazılabilir dosya ve dizinlerin güvenliğinin sağlanmasını önermektedir. Yazılabilir dosyalar, sistemdeki herhangi bir kullanıcı tarafından değiştirilebilen dosyalardır. Bu durum dosyalardaki verilerin kötü niyetli kişiler tarafından değiştirilmesine ve sisteme zarar verilmesine yol açabilir. Ayrıca yazılabilir dosyalar hatalı yazılmış bir script ya da programın belirtisi olabilir ve bu da

daha büyük bir güvenlik ihlaline yol açabilecek potansiyel bir tehdit oluşturur. Yazılabilir dosyaların ve dizinlerin güvenliğini sağlamak, sistemin bütünlüğünü korumak açısından kritik öneme sahiptir.

Yazılabilir dizinler, genellikle sistemin geçici dosyalarını barındıran dizinlerdir. Bu dizinlerdeki dosyalar, sistemin doğru çalışabilmesi için önemli olabilir ancak kötü niyetli kullanıcılar bu dosyaları değiştirebilir, silebilir veya manipüle edebilir. Bu durum da özellikle sistemin güvenliği açısından ciddi riskler oluşturur.

Bu güvenlik açığının önüne geçmek için, yazılabilir dosya ve dizinlerin düzenli olarak kontrol edilmesi ve sadece gerekli durumlarda yazılabilir izinlerin verilmesi gerekmektedir. Özellikle yazılabilir dizinlere sticky bit (yapışkan bit) ayarının uygulanması, o dizindeki dosyaların yalnızca sahipleri tarafından silinmesini veya adlarının değiştirilmesini sağlar. Sticky bit, sistemdeki geçici dosya dizinlerinde (örneğin, /tmp gibi dizinlerde) güvenliği artırmak için yaygın olarak kullanılır. Bu önlem, başka kullanıcıların sahip olduğu dosyalar üzerinde işlem yapmasını engeller, böylece kötü niyetli eylemleri önler.

Sistem yöneticileri, yazılabilir dosya ve dizinler üzerinde kontrolü sağlamak için uygun izinler ve güvenlik önlemleri almalıdır. Bunun yanı sıra yazılabilir dizinlerde gereksiz dosyaların ve dizinlerin bulunmaması, yalnızca gerekli dosya ve dizinlere yazma izinlerinin verilmesi önemlidir. Böylelikle sistemdeki potansiyel güvenlik açıkları minimize edilir ve sistemin bütünlüğü korunmuş olur.

İyileştirme yöntemi olarak bu güvenlik önlemi, yazılabilir dosya ve dizinlerin güvenliğini sağlamak, kötü niyetli kullanıcıların sistem üzerinde gerçekleştirebileceği saldırıları engellemek ve genel sistem güvenliğini artırmak için etkili bir yaklaşımdır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, dünyadaki yazılabilir dosya ve dizinlerin güvenliğini sağlamak amacıyla yazılabilir dosya ve dizinlere yönelik denetim ve düzenleme işlemlerini otomatikleştirir. İlk olarak, sistemdeki yazılabilir dosya ve dizinler tespit edilir. find komutu kullanılarak, tüm dosya ve dizinler incelenir ve yazılabilir olanlar liste halinde görüntülenir. Sonrasında, bu dosya ve dizinlerdeki (others) yazma izinleri kaldırılır. chmod o-w komutu ile, tüm yazılabilir dosya ve

dizinlerden başkalarının yazma izni alınır. Ancak, bazı özel dizinler (örneğin, /tmp) hariç tutulur. Bu dizinlerde yazma izinlerinin kaldırılması istenmez. Son olarak, yazılabilir dosya ve dizinler üzerinde yapılan değişiklikler kontrol edilerek, işlem tamamlanır. Bu betik, CIS Benchmark v2.0.1-6.1.11 maddesindeki "world writable files and directories" güvenlik açığını kapatmaya yönelik bir önlem olarak çalışır ve sistemin bütünlüğünü koruyarak güvenliğini artırır.

```
#!/bin/bash

#dosya ve dizinleri bulma
find / -xdev -type f -perm -0002 -exec ls -l {} \;
find / -xdev -type d -perm -0002 -exec ls -ld {} \;

#dosya ve dizinlerden yetkileri kaldırma
find / -xdev -type f -perm -0002 -exec chmod o-w {} \;
find / -xdev -type d -perm -0002 -exec chmod o-w {} \;

#özel dizinleri hariç tutma
find / -xdev -type d -perm -0002 ! -path "/tmp/*" -exec chmod o-w {} \;

#kontrol
find / -xdev -type f -perm -0002
find / -xdev -type d -perm -0002
```

4.2.4. Güvenli Disk Bölümlendirme

Bu çalışmada, güvenli disk bölümlendirme tedbirlerinin otomatik kodlarla iyileştirilmesi mümkün değildir. Çünkü bu işlem, sistemin ilk kurulum aşamasında gerçekleştirilmesi gereken bir uygulamadır. Özellikle, Linux sistemlerinde işletim sistemi dosyaları ile kullanıcı dosyalarının güvenliğini sağlamak amacıyla, kritik dizinler (örneğin /home, /root, /boot, /tmp gibi) farklı disk bölümlerinde saklanmalıdır. Bu tür bir bölümlendirme, sistem güvenliğini önemli ölçüde artırarak bir bölüme yapılacak saldırıların diğer bölümlere zarar vermesini engeller. Ayrıca kritik sistem dosyalarının izole edilmesi, olası veri kaybı veya erişim ihlallerine karşı ek koruma sağlar.

Bilgi ve İletişim Güvenliği Rehberi (BİGR) ve CIS (Center for Internet Security) denetimlerine dayalı olarak, güvenli disk bölümlendirme uygulamaları önerilmektedir. Bu tedbir maddesinde işletim sistemi dosyalarının ve kullanıcı verilerinin ayrı bölümlerde saklanmasını ve her bir bölümün bağımsız olarak güvence altına alınmasını öngörür. Bu yöntem, sistem performansını etkilemeden güvenliği artırır ve potansiyel tehditlere karşı savunmayı güçlendirir. Ancak bu güvenlik önlemi iyileştirme modeli

içerisinde otomatik olarak sıkılaştırması olamayacağından sadece sistemin ilk kurulum aşamasında gerçekleştirilerek etkinleştirilebilir. Çizelge 4.17'de, BİGR 5.1.2.4 maddesi, Güvenli Disk Bölümlendirme tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.17. GNU/Linux işletim sistemi güvenli disk bölümlendirme

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1**
5.1.2.4	Güvenli Disk Bölümlendirme	İşletim sistemi dosyaları ile kullanıcı dosyaları, /home, /root, /boot, /tmp vb. birimler ayrı disk bölümlerinde tutulmalıdır.	1.1.3.1 Ensure separate partition exists for /var 1.1.4.1 Ensure separate partition exists for /var/tmp 1.1.5.1 Ensure separate partition exists for /var/log 1.1.6.1 Ensure separate partition exists for /var/log/audit 1.1.7.1 Ensure separate partition exists for /home

4.2.5. Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi

Linux sistemlerinde, CD/DVD ve USB gibi harici medyanın otomatik olarak mount edilmesini önlemek amacıyla otomatik mount özelliği devre dışı bırakılmalıdır. Ayrıca, /tmp gibi kritik dizinlerde mount işlemleri noexec, nodev ve nosuid parametreleriyle yapılandırılmalı, böylece bu dizinlerde çalıştırılabilir dosyaların çalıştırılması engellenmelidir. Bu önlem, kötü niyetli yazılımların veya zararlı dosyaların sisteme sızmasını önlemeye yardımcı olur.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayalı olarak, otomatik mount işlemlerinin devre dışı bırakılmasını ve kritik dizinlerde güvenlik önlemlerinin alınmasını önerir. "Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi" tedbiri, harici medyaların güvenli bir şekilde kontrol edilmesini sağlar ve potansiyel saldırı vektörlerini minimize eder. Bu, sisteme zarar verebilecek kötü amaçlı yazılımların etkisini azaltır ve sistem güvenliğini artırır. Çizelge 4.18'de, BİGR 5.1.2.5 maddesi, Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.18. GNU/Linux işletim sistemi otomatik başlatma (mount) özelliğinin pasif hale getirilmesi

Tedbir No.	Tedbir Adı	Tedbir Tanımı	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1
5.1.2.5	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	CD/DVD ve USB gibi harici medyanın otomatik olarak mount edilmesini önlemek adına otomatik mount özelliği pasif hale getirilmelidir. Ayrıca /tmp dizini gibi mount noktalarında noexec, nodev, nosuid parametreleriyle çalıştırılabilir dosyalar pasif hale getirilmelidir.	1.1.1.1 Ensure mounting of cramfs filesystems is disabled 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled 1.1.1.3 Ensure mounting of jffs2 filesystems is disabled 1.1.1.4 Ensure mounting of hfs filesystems is disabled 1.1.1.5 Ensure mounting of hfsplus filesystems is disabled 1.1.1.6 Ensure mounting of squashfs filesystems is disabled 1.1.1.7 Ensure mounting of udf filesystems is disabled 1.1.2.2 Ensure nodev option set on /tmp partition 1.1.2.3 Ensure noexec option set on /tmp partition 1.1.2.4 Ensure nosuid option set on /tmp partition 1.1.9 Disable Automounting 1.1.10 Disable USB Storage

4.2.5.1. /tmp Bölümünde nodev Seçeneği Ayarının Yapılandırılması

Nodev montaj seçeneği, dosya sisteminin özel cihazları içermemesini sağlar. /tmp dosya sistemi, cihazları desteklemek amacıyla kullanılmaz, yalnızca geçici dosyaların depolandığı bir alan olarak işlev görür. Bu nedenle /tmp bölümünde nodev seçeneğinin etkinleştirilmesi, kullanıcıların blok veya karakter özel cihazları oluşturamamalarını sağlamak amacıyla gereklidir.

CIS Benchmark v2.0.1-1.1.2.2 tedbirinde yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde /tmp bölümüne nodev seçeneği eklenmiş ve bu ayar uygulandığında güvenlik ihlali tespit edilmemiştir. Bu nedenle, iyileştirme modeli gereği, /tmp bölümünde nodev seçeneği zaten etkinleştirildiği için ek bir sıkılaştırma kodu yazılmamıştır.

4.2.5.2. /tmp Bölümünde noexec Seçeneği Ayarının Yapılandırılması

Noexec montaj seçeneği, dosya sisteminin çalıştırılabilir dosyalar içermemesi gerektiğini belirtir. /tmp dosya sistemi yalnızca geçici dosya depolama amacıyla kullanıldığından, bu dosya sisteminden çalıştırılabilir dosyaların çalıştırılmasını engellemek önemlidir.

CIS Benchmark v2.0.1-1.1.2.3 tedbirinde yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde /tmp bölümüne noexec seçeneği eklenerek, bu bölümde çalıştırılabilir dosyaların çalıştırılmasına engel olunmuş ve güvenlik ihlali tespit edilmemiştir. Bu nedenle, iyileştirme modelinde noexec seçeneği zaten etkin olduğu için ek bir sıkılaştırma kodu yazılmamıştır.

4.2.5.3. /tmp Bölümünde nosuid Seçeneği Ayarının Yapılandırılması

Nosuid montaj seçeneği, dosya sisteminin setuid dosyalarını içermemesi gerektiğini belirtir. /tmp dosya sistemi yalnızca geçici dosya depolama için kullanıldığından, bu dosya sisteminde setuid dosyalarının oluşturulmasının engellenmesi gereklidir.

CIS Benchmark v2.0.1-1.1.2.4 tedbirinde yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 sisteminde /tmp bölümüne nosuid seçeneği eklenmiş ve bu ayar uygulandığında herhangi bir güvenlik ihlali tespit edilmemiştir. Bu nedenle, iyileştirme modelinde nosuid seçeneği zaten etkinleştirildiği için ek bir sıkılaştırma kodu yazılmamıştır.

4.2.5.4. Otomatik Montajı Devre Dışı Bırakma

Autofs, genellikle CD/DVD ve USB sürücülerini otomatik olarak bağlamayı sağlayan bir özelliktir. Bu özellik etkinleştirildiğinde, fiziksel erişimi olan herhangi bir kullanıcı, kendilerine bağlama izni verilmemiş olsa bile, bir USB sürücüsü veya disk bağlayabilir ve içeriğine erişebilir.

Taşınabilir sabit disklerin kullanımı, özellikle masaüstü kullanıcıları arasında yaygındır. Eğer organizasyonunuz, masaüstü bilgisayarlar üzerinde taşınabilir depolama veya medya kullanımına izin veriyorsa ve fiziksel erişim kontrolleri yeterliyse, otomatik montajı devre dışı bırakmak ek bir güvenlik faydası sağlamayabilir. Bu durumlarda, otomatik montajın devre dışı bırakılması, sistem yönetimini daha karmaşık hale getirebilir ve kullanıcı deneyimini olumsuz etkileyebilir.

CIS Benchmark v2.0.1-1.1.9 tedbirinde yapılan testlerde, GNU/Linux İşletim sistemi Ubuntu 20.04 üzerinde autofs paketinin kaldırılmasının veya servisin maskelenmesinin herhangi bir güvenlik ihlali oluşturmadığı gözlemlenmiştir. Bu nedenle, otomatik montajın devre dışı bırakılması işlemi başarılı bir şekilde uygulanmış olup, iyileştirme modeline ek bir kod yazılmamıştır.

4.2.5.5 USB Bellek Devre Dışı Bırakma

USB depolama cihazları, dosya transferi ve depolama için yaygın olarak kullanılır. Ancak bu cihazlar, ağ bağlantısı olmadan bile dosyaların kalıcı olarak depolanmasına olanak tanır. Bu özellikleri, aynı zamanda USB tabanlı kötü amaçlı yazılımların yayılmasını kolaylaştırabilir. Birçok kötü amaçlı yazılım, USB aygıtlarını kullanarak ağlara sızar ve sistemlere kalıcı tehditler yerleştirir. Bu nedenle, USB depolama cihazlarının kullanımını kısıtlamak, fiziksel saldırı yüzeyini azaltır ve kötü amaçlı yazılımın yayılmasını engelleyebilir.

Sistem üzerinde USB depolama modülünü devre dışı bırakmak için, usb-storage modülünü engellemek gereklidir. Bu işlem için, sistemin modül yükleme yapılandırmasını değiştiren birkaç adım takip edilebilir. İlk olarak, /etc/modprobe.d dizinine, usb-storage modülünün yüklenmesini engelleyen bir konfigürasyon dosyası eklenir. Bu dosya, install usb-storage /bin/false komutunu içerir ve böylece sistem, bu modülü yüklemeye çalıştığında herhangi bir işlem yapılmaz.

Eğer usb-storage modülü sistemde zaten yüklüyse, modül kaldırılmalıdır. Bunun için modprobe -r usb-storage komutu kullanılır. Ayrıca modülün tekrar yüklenmesini engellemek için, modülün yasaklı listeye (blacklist) eklenmesi sağlanır. Bu, sistemin tekrar usb-storage modülünü yüklememesi için gereklidir. Eğer modül, yasaklı liste (blacklist)'de yer almıyorsa, yasaklı liste (blacklist) usb-storage komutu ile bunu eklemek mümkündür.

Sonuç olarak, CIS Benchmark v2.0.1-1.1.10 Disable USB Storage tedbiri bu adımlarla USB depolama cihazlarının kullanımını engelleyerek, kötü amaçlı yazılımların sisteme girişini zorlaştırır ve güvenliği artırır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, USB depolama cihazlarının kullanımını devre dışı bırakmak amacıyla, sistemdeki usb-storage modülünü engellemeye yönelik adımları otomatikleştirir. İlk olarak, modül adı ve yolu belirlenir. Ardından, modülün yüklenebilir durumunu kontrol eden bir fonksiyon tanımlanır. Eğer modül yüklenebilir durumdaysa, /etc/modprobe.d/ dizinine, usb-storage modülünün yüklenmesini engelleyen “install usb-storage /bin/false” komutunu ekler. Modül zaten yüklüyse, modprobe -r usb-storage komutu kullanılarak modül sistemden kaldırılır. Ayrıca, usb-storage modülü blacklist’e eklenir, yani sistemin tekrar bu modülü yüklememesi sağlanır. Betik, her adımda yapılan işlemleri kullanıcıya bildirir ve işlemlerin doğru şekilde tamamlandığını gösterir.

```
#!/bin/bash

# Modül adını ve tipini tanımla
l_modul_adi="usb-storage"
l_modul_turu="drivers"
l_modul_yolu="/lib/modules/**/kernel/$l_modul_turu"
l_modul_adi_p="$(tr '-' '_' <<< "$l_modul_adi")"
l_modul_dizin_yolu="$(tr '-' '/' <<< "$l_modul_adi")"

# Eğer modül yüklenebilir durumdaysa, "/etc/modprobe.d" dizinine "install usb-storage /bin/false" ekler
modul_yuklenebilir_durumu() {
    l_yuklenebilir="$(modprobe -n -v "$l_modul_adi")"
    [ "$(wc -l <<< "$l_yuklenebilir")" -gt "1" ] && l_yuklenebilir="$(grep -P -- "(^\h*install|\b$l_modul_adi)\b" <<< "$l_yuklenebilir")"

    if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_yuklenebilir"; then
        echo -e "\n - Modül: \"$l_modul_adi\" yüklenemez hale getiriliyor"
        echo -e "install $l_modul_adi /bin/false" | sudo tee -a /etc/modprobe.d/"$l_modul_adi_p".conf > /dev/null
    fi
}

# Eğer modül yüklüyse, onu sistemden kaldırır
modul_yuklendi_durumu() {
    if lsmod | grep "$l_modul_adi" > /dev/null 2>&1; then
        echo -e "\n - Modül \"$l_modul_adi\" sistemden kaldırılıyor"
        sudo modprobe -r "$l_modul_adi"
    fi
}

# Eğer modül blacklist'e alınmamışsa, blacklist dosyasına ekler
modul_engelleme() {
    if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_modul_adi_p\b"; then
        echo -e "\n - Modül \"$l_modul_adi\" blacklist'e ekleniyor"
        echo -e "blacklist $l_modul_adi" | sudo tee -a /etc/modprobe.d/"$l_modul_adi_p".conf > /dev/null
    fi
}

# Modülün sistemde mevcut olup olmadığını kontrol et
for l_modul_dizin in $l_modul_yolu; do
    if [ -d "$l_modul_dizin/$l_modul_dizin_yolu" ] && [ -n "$(ls -A $l_modul_dizin/$l_modul_dizin_yolu)" ]; then
        echo -e "\n - Modül: \"$l_modul_adi\" \"$l_modul_dizin\" dizininde mevcut\n - Engellenip engellenmediği kontrol ediliyor..."
        modul_engelleme
```

```
42.         if [ "$l_modul_dizin" = "/lib/modules/$(uname -r)/kernel/$l_modul_turu" ];
then
43.             modul_yuklenebilir_durumu
44.             modul_yuklendi_durumu
45.         fi
46.     else
47.         echo -e "\n - Modül: \"$l_modul_adi\" \"$l_modul_dizin\" dizininde mevcut
değil\n"
48.     fi
49. done
50.
51. echo -e "\n - \"$l_modul_adi\" modülünün engellenmesi tamamlandı"
```

4.2.6. Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması

GNU/Linux sistemlerinde, önemli dosyaların bütünlüğü düzenli olarak kontrol edilmelidir. Bu işlem, dosya sisteminde meydana gelebilecek değişikliklerin izlenmesi ve potansiyel yetkisiz müdahalelerin tespit edilmesi için kritik öneme sahiptir. Dosya bütünlüğü kontrolleri, güvenlik açıklarını ve zararlı yazılımların etkisini erken aşamada tespit etmeye yardımcı olur.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayanarak, dosya bütünlüğü kontrollerinin düzenli aralıklarla yapılmasını önerir. “Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması” tedbiri, sistemdeki kritik dosyaların, yapıların ve uygulamaların bütünlüğünün izlenmesini ve her türlü değişikliğin kaydedilmesini sağlar. Bu önlem, sistemin güvenliğini artırarak, yetkisiz erişim ve veri değişikliklerini engeller. Çizelge 4.19’da, BİGR 5.1.2.6 maddesi, Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.19. GNU/Linux işletim sistemi dosya sistemi bütünlük kontrollerinin düzenli olarak yapılması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1**
5.1.2.6	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	Önemli görülen dosyaların bütünlüğü düzenli olarak kontrol edilmelidir.	1.2.1 Ensure AIDE is installed 1.2.2 Ensure filesystem integrity is regularly checked 6.2.9 Ensure root PATH Integrity

4.2.6.1. AIDE Güvenlik Aracı Kontrolü

AIDE (Advanced Intrusion Detection Environment), dosya sistemindeki değişiklikleri izleyen ve bu değişiklikleri tespit etmeye yarayan bir güvenlik aracıdır. AIDE, dosya sisteminin anlık görüntüsünü alır; bu görüntüde dosyaların izinleri, karma işlevi (hash) değerleri ve değiştirilme zamanları gibi bilgiler yer alır. Bu anlık görüntü, sistemin ilerleyen zamanlarında karşılaştırılarak, dosya sisteminde izinsiz değişikliklerin veya potansiyel güvenlik ihlallerinin tespit edilmesini sağlar.

AIDE'nin kurulumu ve yapılandırılması için önce AIDE paketinin yüklü olup olmadığı kontrol edilir. Eğer AIDE yüklü değilse, sistemdeki paket yöneticisi kullanılarak yüklenir. Kurulumdan sonra, AIDE'in veritabanı başlatılır. Bu veritabanı, dosya sisteminin ilk durumunu kaydeder. Veritabanı oluşturulduktan sonra, AIDE'in veritabanı eski bir veritabanı ile değiştirilir ve bu yeni veritabanı, sistemdeki dosya değişikliklerini takip etmek için kullanılır.

AIDE ile yapılan bu izleme, sisteme yapılan izinsiz müdahaleleri erken aşamada tespit etmeyi sağlar. Örneğin, kötü niyetli bir kullanıcı veya yazılım tarafından yapılan dosya değişiklikleri AIDE sayesinde kolayca fark edilebilir. Bu sayede sisteme yönelik kötü amaçlı aktiviteler engellenebilir veya sınırlanabilir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, AIDE (Advanced Intrusion Detection Environment) güvenlik aracının kurulumu ve yapılandırmasını otomatikleştirir. İlk olarak, AIDE paketinin sistemde yüklü olup olmadığı kontrol edilir. Eğer AIDE yüklü değilse, apt paket yöneticisi kullanılarak AIDE ve gerekli bileşenleri yüklenir. Kurulum tamamlandığında, AIDE'in veritabanı başlatılır. Bu veritabanı, sistemin ilk durumunun kaydını tutar ve dosya sistemi değişikliklerini izlemek için kullanılır. Ardından, başlatılan yeni veritabanı eski veritabanı ile değiştirilir ve AIDE'in dosya izleme ve değişiklik tespiti için kullanıma hazır hale gelir. Betik sonunda, AIDE'in kurulumu ve yapılandırması tamamlandığını bildirir.

```
1. #!/usr/bin/env bash
2.
3. # AIDE kurulumu ve yapılandırması
4.
5. aide_kurulum() {
```

```
6.    echo -e " - AIDE kurulumu başlatılıyor..."
7.
8.    # AIDE paketlerini kurma
9.    if dpkg-query -W aide > /dev/null 2>&1; then
10.      echo -e " - AIDE zaten yüklü."
11.   else
12.      echo -e " - AIDE kurulumu başlatılıyor..."
13.      apt update && apt install -y aide aide-common
14.      echo -e " - AIDE kurulumu tamamlandı."
15.   fi
16. }
17.
18. aide_baslatma() {
19.   # AIDE'i başlatma ve veritabanını başlatma
20.   echo -e " - AIDE veritabanı başlatılıyor..."
21.   aideinit
22.
23.   # Yeni veritabanını eski veritabanı ile değiştirme
24.   mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db
25.   echo -e " - AIDE veritabanı başarıyla başlatıldı."
26. }
27.
28. # Ana işlem
29. aide_kurulum
30. aide_baslatma
31.
32. echo -e "\n - AIDE kurulumu ve yapılandırması tamamlandı.\n"
```

4.2.6.2. Dosya Sistemi Bütünlüğünün Kontrolünün Sağlanması

Dosya sistemi bütünlüğünü düzenli olarak kontrol etmek, sistemin güvenliği açısından önemli bir adımdır. Bu işlem, özellikle sistem yöneticilerinin kritik dosyaların izinsiz bir şekilde değiştirilip değiştirilmediğini tespit etmelerini sağlar. AIDE (Advanced Intrusion Detection Environment) gibi araçlar, dosya sisteminde yapılan değişiklikleri izlemek için kullanılabilir. Ancak bu araçların yalnızca bir kez çalıştırılması yeterli değildir; düzenli aralıklarla çalıştırılması, sürekli izleme sağlayarak değişikliklerin zamanında fark edilmesine yardımcı olur.

Bu işlem için iki farklı yöntem kullanılabilir: cron ve systemd. Cron, zamanlanmış görevlerin yönetildiği klasik bir Linux zamanlayıcıdır ve belirli aralıklarla belirli komutları çalıştırmak için kullanılır. Cron ile AIDE'in her gün belirli bir saatte çalışması sağlanabilir. Bu durumda yönetici (root) kullanıcısının cron tablosuna AIDE kontrolünü her gün saat 05:00'te çalıştıracak bir görev eklenir.

Diğer bir yöntem ise systemd kullanmaktır. Systemd, modern Linux sistemlerinde yaygın olarak kullanılan bir sistem ve hizmet yöneticisidir. AIDE kontrolünü her gün belirli bir saatte çalıştırmak için systemd timer ve service dosyaları

oluşturulabilir. Bu method, sistemin yönetilmesinde daha esnek ve güçlü bir çözüm sunar. Servis (service) dosyası AIDE'in çalıştırılmasını sağlar ve zamanlayıcı (timer) dosyası ise bu çalıştırma zamanını belirler.

Her iki yöntemde sistem yöneticisinin dosya sistemi bütünlüğünü düzenli olarak kontrol etmesini sağlar. Bu sayede sisteme yapılan izinsiz müdahaleler veya değişiklikler tespit edilebilir ve gerekli önlemler alınabilir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, dosya sistemi bütünlüğünü düzenli olarak kontrol etmek için iki farklı yöntemle (cron ve systemd) AIDE güvenlik aracının yapılandırılmasını otomatikleştirir. İlk olarak, cron kullanarak AIDE'in her gün saat 05:00'te çalışacak şekilde yapılandırılmasını sağlar. Bunun için root kullanıcısının cron tablosuna uygun bir cron job eklenir. İkinci yöntem olarak, systemd kullanılarak AIDE kontrolünün her gün belirli bir saatte yapılması için gerekli servis (aidecheck.service) ve zamanlayıcı (aidecheck.timer) dosyaları oluşturulur. Bu dosyalar, systemd'ye AIDE'in düzenli olarak çalıştırılması talimatını verir. Betik sonunda, seçilen yönteme bağlı olarak dosya sistemi bütünlüğü kontrolünün başarıyla yapılandırıldığı bildirilir.

```
#!/usr/bin/env bash

# Dosya sistemi bütünlüğünü düzenli olarak kontrol etme kurulumu

aidecheck_cron_kurulum() {
   echo -e " - AIDE dosya sistemi kontrolü için cron yapılandırması başlatılıyor..."

   # Root kullanıcısının cron tablosunu düzenleyin
   crontab -u root -e <<EOF
0 5 * * * /usr/bin/aide.wrapper --config /etc/aide/aide.conf --check
EOF
   echo -e " - Cron job başarıyla eklendi: AIDE kontrolü her gün 05:00'te çalışacak."
}

aidecheck_systemd_kurulum() {
   echo -e " - AIDE dosya sistemi kontrolü için systemd timer yapılandırması
başlatılıyor..."

   # aidecheck.service dosyasını oluşturma
   cat <<EOF > /etc/systemd/system/aidecheck.service
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/bin/aide.wrapper --config /etc/aide/aide.conf --check

[Install]
WantedBy=multi-user.target
EOF
```

```
30.
31.   # aidecheck.timer dosyasını oluşturma
32.   cat <<EOF > /etc/systemd/system/aidecheck.timer
33. [Unit]
34. Description=Aide her gün 05:00'te kontrol eder
35.
36. [Timer]
37. OnCalendar=*-*-* 05:00:00
38. Unit=aidecheck.service
39.
40. [Install]
41. WantedBy=multi-user.target
42. EOF
43.
44.   # Dosya izinlerini ayarlama
45.   chown root:root /etc/systemd/system/aidecheck.*
46.   chmod 0644 /etc/systemd/system/aidecheck.*
47.
48.   # Systemd daemon'ı yeniden yükleme
49.   systemctl daemon-reload
50.
51.   # Systemd servislerini ve zamanlayıcıyı etkinleştirme
52.   systemctl enable aidecheck.service
53.   systemctl --now enable aidecheck.timer
54.
55.   echo -e " - AIDE dosya sistemi kontrolü için systemd timer başarıyla
yapılandırıldı."
56. }
57.
58. # Seçilen yönteme göre işlem başlatma (Cron veya systemd)
59. aidecheck_cron_kurulum
60. # aidecheck_systemd_kurulum  # Eğer systemd kullanılacaksa bu satırı aktif
edebilirsiniz
61.
62. echo -e "\n - Dosya sistemi bütünlüğü kontrolü başarıyla yapılandırıldı.\n"
```

4.2.6.3. Yönetici (Root PATH) Bütünlüğünün Sağlama Yapılandırması

Yönetici (root) kullanıcısı, sistemdeki herhangi bir komutu çalıştırabilme yeteneğine sahip olup, PATH değişkeni doğru şekilde yapılandırılmadığı takdirde yanlışlıkla zararlı programları çalıştırabilir. Eğer yönetici (root) kullanıcısının yürütme yolu (PATH) içerisine geçerli çalışma dizini (.) veya diğer yazılabilir dizinler eklenmişse, bir saldırganın bu dizinlerde bulunan kötü amaçlı yazılımları çalıştırmasını sağlamak kolaylaşır. Bu durum da yönetici (root) kullanıcısının bir trojan programını çalıştırmasına neden olabilir ve saldırganın sisteme süper kullanıcı erişimi kazanmasına yol açabilir.

Yapılacak denetimlerde, yönetici (root) kullanıcısının PATH ortam değişkeninde yalnızca güvenilir dizinlerin bulunması gerektiği tespit edilmelidir. Eğer PATH değişkeni hatalı veya tehlikeli bir şekilde yapılandırılmışsa, bu konfigürasyonlar düzeltilmeli veya gerekçe sunulmalıdır.

CIS Benchmark v2.0.1-6.2.9 tedbirinde yapılan testlerde, yönetici (root) kullanıcısının PATH'inin doğruluğu kontrol edilerek, herhangi bir yanlış yapılandırma veya güvenlik açığına yol açacak durum tespit edilmemiştir. Bu nedenle PATH bütünlüğü sağlanmış ve iyileştirme modeline herhangi bir yeni kod eklenmemiştir.

4.2.7. Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması

GNU/Linux sistemlerinde, kullanılan makinelerde önyükleyici (bootloader) parolası belirlenmeli ve bu parolanın kullanımı zorunlu kılınmalıdır. Ayrıca tek kullanıcı modu için de kimlik doğrulaması yapılması gereklidir. Bu önlemler sistemin kötü niyetli kullanıcılar tarafından önyükleme sırasında değiştirilmesini engellemeye yardımcı olur. Ek olarak sadece güvenli ve onaylı boot edilebilir cihazların listesine izin verilmeli, kullanılmayan cihazlar (USB, Firewire, Thunderbolt, PCMCIA vb.) iptal edilmelidir.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayalı olarak, önyükleme ayarlarının güvenli şekilde yapılandırılmasını önerir. "Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması" tedbiri, önyükleyici parolasının kullanılması, tek kullanıcı moduna kimlik doğrulama eklenmesi ve gereksiz cihazların devre dışı bırakılmasını öngörür. Bu, sistemin güvenliğini artırarak önyükleme aşamasında yetkisiz değişikliklerin yapılmasını engeller. Çizelge 4.20'de, BİGR 5.1.2.7 maddesi, Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.20. GNU/Linux işletim sistemi önyükleme (boot) ayarlarının güvenli şekilde yapılandırılması

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Debian 10 CIS_Debian_Linux_10_Benchmark_v1.0.0**
5.1.2.7	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	Kullanılan makinelerde önyükleyici (bootloader) parolası belirlenmeli ve zorunlu tutulmalıdır. Ayrıca tek kullanıcı modu için kimlik doğrulaması yapılmalıdır. Boot edilebilir cihazlar listesi kısıtlanmalıdır. Kullanılmıyorsa USB, Firewire, Thunderbolt, PCMCIA vb. cihazlar iptal edilmelidir.	1.4.1 Ensure bootloader password is set 1.4.2 Ensure permissions on bootloader config are configured 1.4.3 Ensure authentication required for single user mode

4.2.7.1. Önyükleme (Bootloader) Parola Koruması Yapılandırılması

Bootloader şifreleme, bir sistemin açılışında güvenliği artırmak için kritik bir adımdır. Bu güvenlik önlemi bir saldırganın veya yetkisiz bir kullanıcının sistemin bootloader ayarlarına erişmesini veya boot parametrelerini değiştirmesini engeller. Özellikle kullanıcıların güvenlik özelliklerini (örneğin, AppArmor gibi) açılışta devre dışı bırakmalarını önler.

Bootloader parolası etkinleştirildiğinde, sistemin güvenliği önemli ölçüde artmaktadır. Dikkat edilmesi gereken husus ise bootloader parolasının güvenli bir şekilde saklanması ve unutulmaması kritik önem taşımaktadır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemin GRUB bootloader'ı için parola koruması yapılandırılmasını otomatikleştirir. İlk olarak, belirlenen bir kullanıcı adı (örneğin, "admin") ve parola kullanılarak GRUB parolası için hash değeri oluşturulur. Ardından, GRUB yapılandırma dosyasının (40_custom) yedeği alınır. Yedeğin alınmasının ardından, yapılandırma dosyasına kullanıcı adı ve oluşturulan parola hash değeri eklenir. Son olarak, GRUB yapılandırması güncellenir.

Bu işlem, sistemin bootloader'ına erişimi sınırlayarak, yetkisiz kişilerin açılış parametrelerini değiştirmesini veya güvenlik özelliklerini devre dışı bırakmasını engellemeyi amaçlar.

```
#!/bin/bash

# GRUB yapılandırma dosyasının yolu
grub_dosyasi="/etc/grub.d/40_custom"
# GRUB için belirlenen kullanıcı adı
kullanici_adi="admin"  # GRUB kullanıcı adı
# GRUB için belirlenen parola
parola="12345"  # Parolayı buraya istediğiniz gibi değiştirin

# GRUB parolası hash değeri oluşturuluyor
echo "GRUB parola hash değeri oluşturuluyor..."
parola_hash=$(echo -e "$parola\n$parola" | grub-mkpasswd-pbkdf2 | awk '/PBKDF2/ {print $NF}')

# GRUB yapılandırma dosyasının yedeği alınıyor
echo "$grub_dosyasi dosyasının yedeği alınıyor..."
cp $grub_dosyasi $grub_dosyasi.bak

# GRUB yapılandırma dosyasına kullanıcı adı ve parola ekleniyor
echo "GRUB dosyası yapılandırılıyor..."
echo "set superusers=\"$kullanici_adi\"" | sudo tee -a $grub_dosyasi
echo "password_pbkdf2 $kullanici_adi $parola_hash" | sudo tee -a $grub_dosyasi

# GRUB güncelleniyor
echo "GRUB güncelleniyor..."
update-grub
```

4.2.7.2. Önyükleme (Bootloader) İzinlerin Yapılandırılması

Bootloader yapılandırma dosyasının izinlerinin doğru şekilde ayarlanması, sistemin güvenliğini önemli ölçüde artıran bir adımdır. GRUB yapılandırma dosyası, sistemin açılış ayarlarını ve parola korumalı boot seçeneklerini içerdiğinden, bu dosyaya yalnızca yetkili kullanıcıların erişebilmesi kritik bir öneme sahiptir. Bu dosyaya izinsiz erişim potansiyel olarak sistemdeki güvenlik zayıflıklarını ortaya çıkarabilir ve kötü niyetli bir kullanıcının sistemin boot seçeneklerini değiştirmesine olanak tanıyabilir.

Bu güvenlik önlemini uygulamak için, öncelikle /boot/grub/grub.cfg dosyasının sahipliğinin yönetici (root) kullanıcısına verilmesi gereklidir. Bu işlem sadece sistem yöneticisinin bu dosyayı yönetebilmesini sağlar. Ardından dosyanın izinleri yalnızca yönetici (root) kullanıcısının okuma ve yazma erişimine sahip olacak şekilde ayarlanmalıdır. Bu kural dosyayı sadece yönetici erişimine açar ve diğer kullanıcıların dosyayı okumasını veya değiştirmesini engeller.

Bu işlemde chown komutu ile dosyanın sahipliğini yönetici (root) kullanıcısına atama ve chmod komutu ile dosyanın erişim izinlerini yalnızca yönetici (root) için okuma ve yazma olarak sınırlama adımlarını içerir. Bu sayede dosyaya yalnızca yetkilendirilmiş kullanıcılar erişebilir ve sistemin boot ayarları üzerinde herhangi bir izinsiz değişiklik yapılması engellenmiş olur.

CIS tedbirine göre bu adımlar, sistemin bootloader yapılandırma dosyasına yönelik yetkisiz erişimi engelleyerek güvenliği önemli ölçüde artırır. Bu tür güvenlik önlemleri, sistemin daha güvenli bir şekilde çalışmasını ve potansiyel saldırılara karşı korunmasını sağlamaktadır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemin bootloader yapılandırma dosyasının güvenliğini artırmaya yönelik iki temel adımı otomatikleştirir. İlk olarak, /boot/grub/grub.cfg dosyasının sahipliği yönetici (root) kullanıcısına atanır. Bu, sadece yönetici (root) kullanıcısının bu dosyayı yönetmesini sağlar. Ardından, dosyanın izinleri, yalnızca yönetici (root) kullanıcısının okuma ve yazma erişimine sahip olacak şekilde değiştirilir, diğer kullanıcıların dosyayı okuması veya değiştirmesi engellenir. Bu güvenlik önlemi, bootloader yapılandırma dosyasına yetkisiz erişimi önleyerek, sistemin açılış ayarlarının korunmasına yardımcı olur. Bu adımlar, potansiyel saldırılara karşı sistemin güvenliğini artırır.

```
#!/bin/bash

# 1.4.2 - Bootloader Yapılandırma Dosyasının İzinlerinin Ayarlanması
echo "Bootloader yapılandırma dosyasının izinlerini ayarlıyoruz..."

# GRUB yapılandırma dosyasının sahipliğini root kullanıcısına atıyoruz
echo "GRUB yapılandırma dosyasının sahipliğini root kullanıcısına atıyoruz..."
sudo chown root:root /boot/grub/grub.cfg

# GRUB yapılandırma dosyasının izinlerini yalnızca root için okuma ve yazma olarak ayarlıyoruz
echo "GRUB yapılandırma dosyasının izinlerini yalnızca root için okuma ve yazma olarak ayarlıyoruz..."
sudo chmod u-x,go-rwx /boot/grub/grub.cfg

echo "Bootloader yapılandırma dosyasının izinleri başarıyla yapılandırıldı."
```

4.2.7.3. Tek Kullanıcı İçin Kimlik Doğrulama Yapılandırılması

Tek kullanıcı modu (Single user mode) sistemin önyükleme sırasında bir sorunla karşılaştığında ya da kullanıcı tarafından manuel olarak seçildiğinde başlatılabilen bir moddur. Bu modda sistem yöneticisi olarak root yetkilerine sahip olan bir kullanıcı, sisteme müdahale edebilir ve sistemin bakımını yapabilir. Ancak bu mod özellikle fiziksel erişimi olan kötü niyetli bir kullanıcı için potansiyel bir güvenlik açığı oluşturabilir. Çünkü herhangi bir kimlik doğrulama yapılmadan yönetici (root) yetkileri elde edilebilir. Bu nedenle single user mode'da kimlik doğrulamanın zorunlu hale getirilmesi güvenlik açısından kritik bir önlemdir.

Bu güvenlik önlemi, yönetici (root) kullanıcısının bir parola belirlemesiyle başlar. Böylece single user mode'a geçildiğinde, sisteme yönetici (root) erişimi sağlamak isteyen bir kullanıcı, doğru parolayı girene kadar sisteme giriş yapamayacaktır. CIS Benchmark v2.0.1-1.4.3 tedbirine göre bu işlem yetkisiz kişilerin yönetici (root) yetkilerini elde etmesini engelleyerek sistemin güvenliğini artıracaktır.

Yapılan işlemlerde kimlik doğrulama gerekliliği, sistemin fiziksel erişimi olan kişilerden korunmasına yardımcı olur ve sadece yetkili kullanıcıların yönetici (root) erişimiyle sisteme müdahale etmelerini sağlar. Bu işlemler özellikle sunucular ve kritik altyapılarda güvenlik açısından çok önemli bir önlemdir.

Aşağıda bulunan iyileştirme modelindeki bash komutu, sistemin single user mode (tek kullanıcı modu) sırasında kimlik doğrulamanın zorunlu hale getirilmesi için gerekli adımları otomatikleştirir. İlk olarak, yönetici (root) kullanıcısı için bir şifre belirlenir. Bu, single user mode'a geçiş sırasında kimlik doğrulama yapılmasını sağlar. Ardından, /etc/default/grub dosyasının yedeği alınır ve dosya üzerinde single user mode için gerekli düzenlemeler yapılır. "GRUB_CMDLINE_LINUX" satırına single parametresi eklenerek, sistemin single user mode'da açılabilmesi sağlanır. Son olarak, GRUB yapılandırması güncellenir ve yapılan değişikliklerin etkili olması sağlanır.

```
1. #!/bin/bash
2.
3. echo "Single user mode için kimlik doğrulama yapılandırılıyor..."
4.
5. # 1. Root kullanıcısı için şifre ayarlama
```

```
6. echo "Root kullanıcısı için bir şifre belirleniyor..."
7. sudo passwd root
8.
9. # 2. /etc/default/grub dosyasının yedeğini alarak düzenleme
10. echo "Grub konfigürasyon dosyası yedekleniyor..."
11. sudo cp /etc/default/grub /etc/default/grub.bak
12.
13. # 3. Single user mode için grub konfigürasyonunda düzenleme
14. echo "Single user mode için GRUB konfigürasyonu güncelleniyor..."
15. sudo sed -i 's/^GRUB_CMDLINE_LINUX="[^"]*/& single/' /etc/default/grub
16.
17. # 4. Grub yapılandırmasını güncelleme
18. echo "GRUB yapılandırması güncelleniyor..."
19. sudo update-grub
20.
21. echo "Single user mode için kimlik doğrulama başarıyla yapılandırıldı."
```

4.2.8. Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi

GNU/Linux sistemlerinde, erişim kontrolü zorunlu erişim kontrolü (MAC) modeline göre yapılandırılmalıdır. Bu model de işletim sistemi üzerinde kullanılan servisler (SELinux, AppArmor vb.) aracılığıyla uygulanmalıdır. Zorunlu erişim kontrolü, kullanıcıların ve süreçlerin yalnızca yetkilendirilmiş kaynaklara erişebilmesini sağlayarak sistemin güvenliğini önemli ölçüde artırır. Ayrıca MAC modeli sayesinde, kullanıcı ve süreçlerin sistemdeki kritik dosya ve kaynaklar üzerinde yapabileceği işlemler sınırlandırılır.

Bilgi ve İletişim Güvenliği Rehberi (BİGR), CIS (Center for Internet Security) denetimlerine dayalı olarak, zorunlu erişim kontrolünün etkinleştirilmesini önerir. “Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi” tedbiri, SELinux, AppArmor gibi güvenlik servislerinin kullanılarak, sistemdeki erişim kontrolünün daha katı bir şekilde uygulanmasını sağlar. Bu önlem ile sistemdeki potansiyel güvenlik açıklarını kapatır ve izinsiz erişimleri önler. Çizelge 4.21’de, BİGR 5.1.2.8 maddesi, Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi tedbiri, CIS üzerindeki benzer tedbir maddeleri ile eşleştirilmiştir.

Çizelge 4.21. GNU/Linux işletim sistemi zorunlu erişim kontrolünün (MAC) aktif edilmesi

Tedbir No.	**Tedbir Adı**	**Tedbir Tanımı**	**CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1**
5.1.2.8	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	İşletim sistemi üzerinde erişim kontrolü, ilgili servisler (SELinux, AppArmor vb.) kullanılarak zorunlu erişim kontrolü (MAC) modeline göre yapılmalıdır.	1.6.1.1 Ensure AppArmor is installed 1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration 1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode 1.6.1.4 Ensure all AppArmor Profiles are enforcing

4.2.8.1. Zorunlu Erişim Kontrolleri İçin AppArmor Kurulumu

AppArmor, GNU/Linux işletim sistemlerinde güvenliği artırmak amacıyla kullanılan önemli bir güvenlik modülüdür. Uygulama düzeyinde erişim denetimleri sağlayarak, sistemde çalışan uygulamaların yalnızca yetkili ve güvenli işlemleri gerçekleştirmesine izin verir. Bu sayede potansiyel olarak zararlı yazılımlar ve hatalı uygulamalar sistemde kritik bir zarar verecek hareketleri gerçekleştiremez.

AppArmor, Zorunlu Erişim Kontrolleri (Mandatory Access Controls - MAC) sağlayan bir güvenlik sistemidir. Eğer bir MAC sistemi yüklü değilse, sadece varsayılan Takdirî Erişim Kontrolü (Discretionary Access Control - DAC) sistemi kullanılabilir ve bu şekilde daha zayıf bir güvenlik seviyesi sağlar. Güvenlik seviyesini üst düzeye çıkartmak için AppArmor'ın yüklü ve etkin olması gerekmektedir. CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1-1.6.1.1 maddesini iyileştirme modeline göre karşılamış olmaktadır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, Ubuntu sistemine AppArmor güvenlik modülünü kurmak için gerekli adımları otomatikleştirir. İlk olarak, sistemdeki paket listeleri güncellenir. Daha sonra, apparmor ve apparmor-utils paketleri yüklenerek AppArmor ve onun yardımcı araçları sisteme dahil edilir. Kurulum tamamlandıktan sonra, AppArmor servisinin durumu kontrol edilir. Bu işlem, Zorunlu Erişim Kontrolleri (MAC) sağlamak için gereklidir ve sistemde güvenliği artıran bir önlem olarak, yalnızca belirli uygulamalara güvenli işlemleri gerçekleştirme yetkisi vererek potansiyel zararlı yazılımlara karşı koruma sağlar.

```
#!/bin/bash

# Paket listelerini güncelle
echo "Paket listeleri güncelleniyor..."
sudo apt-get update

# AppArmor ve yardımcı araçları yükle
echo "AppArmor ve yardımcı araçlar yükleniyor..."
sudo apt-get install -y apparmor apparmor-utils

# Yükleme sonrası AppArmor servisini kontrol et
echo "AppArmor servisi durum kontrol ediliyor..."
sudo systemctl status apparmor
```

4.2.8.2. AppArmor Kurulumu Başlangıç (Bootloader) Etkinleştirilmesi

AppArmor'ın sağladığı güvenlik özelliklerinin etkin bir şekilde işlev gösterebilmesi için, sistem önyüklendiğinde (boot time) aktif olması gerekmektedir. Bunun sağlanabilmesi için, bootloader olarak bilinen yazılımın yapılandırmasında gerekli ayarlamaların yapılması şarttır.

Bootloader, işletim sistemini başlatan temel yazılımdır ve genellikle GRUB (Grand Unified Bootloader) kullanılır. GRUB, sistemin başlatılması sırasında hangi çekirdek ve modüllerin yüklenmesi gerektiğini belirler. Eğer AppArmor, sistemin bootloader yapılandırmasında doğru şekilde etkinleştirilmezse, sistem başlatıldığında bu güvenlik modülü devreye girmeyecek ve bu durumda saldırganlara sistemin güvenlik mekanizmalarına karşı bir açık sağlayacaktır. Bu sebeple AppArmor'ın bootloader parametreleri üzerinden devre dışı bırakılmaması ve her zaman etkin olarak başlaması gerektiği vurgulanmaktadır.

CIS Benchmark v2.0.1-1.6.1.2 maddesinde, AppArmor'ın etkin olmasının, sistemin güvenlik bütünlüğü için kritik bir gereklilik olduğu belirtilmiştir. Bu nedenle, GRUB bootloader'ı kullanılıyorsa, AppArmor'ın doğru şekilde yapılandırıldığından emin olunmalıdır. Eğer sistemde LILO veya farklı bir bootloader kullanılıyorsa, aynı güvenlik politikaları ve yapılandırmalar uygulanarak, AppArmor'ın etkin olması sağlanmalıdır.

Aşağıda bulunan iyileştirme modelindeki bash komutu, AppArmor güvenlik modülünün bootloader yapılandırmasına eklenmesi ve sistemin önyükleme sırasında

etkin olmasını sağlamak için gereken adımları otomatikleştirir. İlk olarak, mevcut GRUB yapılandırma dosyasının bir yedeği alınır. Ardından, GRUB yapılandırma dosyasındaki "GRUB_CMDLINE_LINUX" satırına apparmor=1 ve security=apparmor parametreleri eklenerek AppArmor'un etkin olacağı garanti altına alınır. Son olarak, GRUB2 yapılandırması güncellenir ve yapılan değişikliklerin doğruluğu, "GRUB_CMDLINE_LINUX" satırının son haliyle kontrol edilir. Bu işlem, sistemin güvenlik bütünlüğünü artırarak AppArmor'un her önyükleme sırasında aktif olmasını sağlar.

```
1. #!/bin/bash
2.
3. # GRUB yapılandırma dosyasını yedekle
4. echo "Yedekleme yapılıyor: /etc/default/grub"
5. sudo cp /etc/default/grub /etc/default/grub.bak
6.
7. # GRUB yapılandırma dosyasını düzenle
8. echo "GRUB_CMDLINE_LINUX satırına apparmor=1 ve security=apparmor parametreleri
ekleniyor..."
9. sudo sed -i 's/^GRUB_CMDLINE_LINUX="\(.*\)"/GRUB_CMDLINE_LINUX="\1 apparmor=1
security=apparmor"/' /etc/default/grub
10.
11. # GRUB2 yapılandırmasını güncelle
12. echo "GRUB yapılandırması güncelleniyor..."
13. sudo update-grub
14.
15. # Yapılandırmanın başarılı olduğuna dair mesaj
16. echo "AppArmor bootloader yapılandırmasına eklendi ve grub yapılandırması
güncellendi."
17.
18. # Yapılandırmanın doğru şekilde uygulandığını kontrol et
19. echo "GRUB_CMDLINE_LINUX satırının son hali:"
20. grep GRUB_CMDLINE_LINUX /etc/default/grub
```

4.2.8.3. AppArmor Profillerinin Uygulama veya Denetim Modu Yapılandırması

AppArmor profilleri, uygulamaların hangi kaynaklara erişebileceğini tanımlar. Güvenlik yapılandırma gereksinimleri, her site için farklılık gösterebilir ve bazı durumlarda varsayılan politikalardan daha katı bir politika talep edilebilir. Bu madde, sistemde var olan tüm AppArmor politikalarının etkinleştirildiğini ve doğru şekilde uygulandığını sağlamak için gereklidir.

Yapılan testlerde halihazırda bulunan Ubuntu 20.04 makinesi için CIS Benchmark v2.0.1-1.6.1.3 maddesi, tüm AppArmor profillerinin uygulama veya denetim modunda olduğu tespit edilmiştir. Bu nedenle, sistemdeki mevcut profillerin

doğru bir şekilde yapılandırılmış ve güvenli olduğu için iyileştirme modelinde uygulanan sıkılaştırma kodu yazılmamıştır.

4.2.8.4. AppArmor Profillerinin Zorunlu Uygulama Modu Yapılandırması

AppArmor profilleri, hangi uygulamaların hangi kaynaklara erişebileceğini belirleyerek sistem güvenliğini sağlamada önemli bir rol oynar. Birçok güvenlik yapılandırması, bu profillerin doğru şekilde etkinleştirilmesini gerektirir. Bu madde, sistemde bulunan tüm profillerin uygulama modunda olduğunu ve bu profillerin uygulamaları denetlediğini garanti etmeye yöneliktir.

Yapılan testlerde halihazırda bulunan Ubuntu 20.04 makinesi için CIS Benchmark v2.0.1-1.6.1.4 maddesi, tüm AppArmor profillerinin uygulama modunda olduğu ve uygulamaların güvenlik politikalarına uygun şekilde çalıştığı doğrulanmıştır. Bu nedenle mevcut yapılandırmalar güvenli olduğu için iyileştirme modelinde herhangi bir sıkılaştırma kodu yazılmamıştır.

5. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

İşletim sistemi sıkılaştırma tedbirleri kapsamında Bilgi ve İletişim Güvenliği Rehberi (BİGR) GNU/Linux işletim sistemi ve Windows İşletim Sistemi için denetim tedbir maddeleri sunmuştur.

5.1. Bilgi ve İletişim Güvenliği Rehberi Sıkılaştırma Denetim Yöntemleri

5.1.1. Linux İşletim Sistemi Sıkılaştırma Tedbirleri Denetim Yöntemleri

BİGR 5.1. İşletim Sistemi Sıkılaştırma Tedbirlerine göre Linux işletim sistemleri için 1.seviye 2 adet, 2.seviye 5 adet, 3.seviye 1 adet olmak üzere toplamda 8 adet denetim yöntemi bulunmaktadır. Bu denetim önerileri Çizelge 5.1'de gösterilmiştir.

Çizelge 5.1. Linux işletim sistemi sıkılaştırma tedbirleri denetim yöntemleri

Tedbir No	Tedbir Seviyesi	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soruları Önerileri
5.1.2.1	1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) etkisiz hale getirilmiş midir?
5.1.2.2	1	Yetkili Kullanıcı Hesap Yönetimi	Mülakat, Güvenlik Denetimi	Kullanıcılar ve yetkileri nasıl yönetilmektedir? Gereksiz kullanıcılar bulunmakta mıdır? Sistem ve servis kullanıcıları hariç diğer kullanıcıların parolaları bulunmakta mıdır? Root ile uzaktan erişim mümkün müdür? UID değeri 0 olan kullanıcı bulunmakta mıdır? Aynı isme ve UID değerine sahip kullanıcılar ve gruplar bulunmakta mıdır? Sistem kullanıcıların kabuğu /sbin/nologin midir? Sudoers kullanıcıları değişikliklere karşı takip edilmekte midir?
5.1.2.3	2	Dosya Sistemi Güvenli Erişim Düzenlemeleri	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sistemlerde yer alan kritik dosyalar belirlenmiş midir? Dosya sistemlerine güvenli erişim kapsamında tanımlanmış bir politika var mıdır? Politika içeriğinde hangi hususlar ele alınmaktadır?
5.1.2.4	2	Güvenli Disk Bölümlendirme	Mülakat, Güvenlik Denetimi	Disk bölümlendirme nasıl yapılmaktadır?
5.1.2.5	2	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	CD/DVD ve USB gibi medya cihazları otomatik olarak başlatılmakta mıdır? Bunu engellemek için ne gibi bir yapılandırma ayarı yapılmıştır?
5.1.2.6	2	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	Mülakat, Güvenlik Denetimi	Sistemlerde bütünlüğü kritik olan dosyalar belirlenmiş midir? Belirlenen bu dosyaların kontrolünü yapmak için hangi araçlardan/programlardan faydalanılmaktadır? Dosyaların bütünlüğünün bozulduğu durumlar için ne gibi bir süreç işletilmektedir?
5.1.2.7	2	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	Mülakat, Güvenlik Denetimi	Önyükleyici için güvenli bir yapılandırma var mıdır? Boot cihazlarının yönetimi nasıl yapılmaktadır?
5.1.2.8	3	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	Mülakat, Güvenlik Denetimi	Zorunlu erişim kontrolü (MAC) için hangi servilerden faydalanılmaktadır? Bu servislerin yönetimi nasıl sağlanmaktadır?

Bu tedbirlere göre, sıkılaştırma kurallarının ilk hali ile, bu çalışmadaki iyileştirme modelinin uygulanmasından sonraki aşamalar değerlendirildiğinde, kapsam dahilindeki tedbirlerin başarılı bir şekilde uygulandığı ve olumlu sonuçların

gözlemlendiği görülmüştür.

BİGR 5.1.2.4 Güvenli Disk Bölümlendirme tedbiri iyileştirme modelinde uygulanamamıştır. Güvenli disk bölümleme işlemi işletim sistemi kurulurken başlangıçta ayarlanması gerekmektedir.

5.1.2. Windows İşletim Sistemi Sıkılaştırma Tedbirleri Denetim Yöntemleri

BİGR 5.1. İşletim Sistemi Sıkılaştırma Tedbirlerine Windows işletim sistemleri için 1.seviye 6 adet tedbir, 2.seviye 7 adet olmak üzere toplamda 13 adet denetim yöntemi bulunmaktadır. Bu denetim önerileri Çizelge 5.2'de gösterilmiştir.

Çizelge 5.2. Windows işletim sistemi sıkılaştırma tedbirleri denetim yöntemleri

Tedbir No	Tedbir Seviyesi	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soruları Önerileri
5.1.3.1	1	Kullanıcı Haklarının Kısıtlanması	Mülakat, Güvenlik Denetimi	Kullanıcı haklarının kısıtlanması son kullanıcı bilgisayarlarına uygun olarak yapılandırılmış mıdır?
5.1.3.2	1	Otomatik Güncellemenin Aktif Olması	Mülakat, Güvenlik Denetimi	İşletim sisteminin otomatik güncelleme ayarı açık mıdır?
5.1.3.3	1	SMB Protokolü Güvenliği	Mülakat, Gözden Geçirme	SMB versiyon 1 protokolü sunucu ve istemcilerde kapatılmış mıdır, SMB protokolü hangi versiyon u kullanılmaktadır?
5.1.3.4	1	Yerel Yönetici Hesapları Yönetimi	Mülakat, Gözden Geçirme	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmış mıdır? Yerel yönetici hesaplarının parolaları nasıl değiştirilmektedir?
5.1.3.5	1	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Mülakat, Gözden Geçirme	Ayrıcalıklı hesap sayıları sınırlandırılmakta mıdır?
5.1.3.6	1	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Mülakat, Gözden Geçirme	Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında ne sıklıkla ve ne gibi işlemler yapılmaktadır? Yerel bilgisayarlarda tutulan hesaplara ait parola özetlerinin tutulma sayısı 0 olarak ayarlanmış mıdır? Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) Grubuna alınmış mıdır?
5.1.3.7	2	Kullanılmayan Hesapların Devre Dışı Bırakılması	Mülakat, Gözden Geçirme	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmış mıdır?
5.1.3.8	2	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Mülakat, Güvenlik Denetimi	Varsayılan yönetici ve misafir hesaplarının yapılandırılması en iyi çözüm önerilerine uygun olarak yapılmış mıdır?
5.1.3.9	2	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Mülakat, Güvenlik Denetimi	Cmd, powershell gibi betik çalıştırma motorlarına erişimler kısıtlandırılmış mıdır?
5.1.3.10	2	Aktif Dizin Sorguları Güvenliği	Mülakat, Gözden Geçirme	Aktif dizin sorguları güvenli LDAPs protokolü ile yapılmakta mıdır?
5.1.3.11	2	Yönetici Hesaplarının İzlenmesi	Mülakat, Gözden Geçirme	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmekte midir?
5.1.3.12	2	Güvenli Yönetici İş İstasyonu Kullanımı	Mülakat, Gözden Geçirme	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu kullanılmakta mıdır?
5.1.3.13	2	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Mülakat, Gözden Geçirme	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmekte midir?

5.2. İyileştirme Modeli Öncesi ve Sonrası Bulgu Durumu

5.2.1. Windows 10 Enterprise

Windows 10 Enterprise işletim sistemi üzerinde CIS-CAT aracı ile yapılan testlerde, önce Şekil 5.1'deki iyileştirme modeli öncesi kullanıcı hakları ataması tedbirleri analiz edilmiştir. Ardından, Şekil 5.2'de ise iyileştirme modeli sonrası kullanıcı hakları ataması tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

2.1 Audit Policy		
2.2 User Rights Assignment		
1.0	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	Pass
1.0	2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	Fail
1.0	2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	Pass
1.0	2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'	Fail
1.0	2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	Pass
1.0	2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	Fail
1.0	2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	Pass
1.0	2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'	Pass
1.0	2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators'	Pass
1.0	2.2.11 (L1) Ensure 'Create a token object' is set to 'No One'	Pass
1.0	2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Pass
1.0	2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One'	Pass
1.0	2.2.14 (L1) Configure 'Create symbolic links'	Pass
1.0	2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators'	Pass
1.0	2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'	Fail
1.0	2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	Fail
1.0	2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests'	Fail
1.0	2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests'	Fail
1.0	2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	Fail
1.0	2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'	Pass
1.0	2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'	Pass
1.0	2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Pass
1.0	2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'	Pass
1.0	2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'	Pass
1.0	2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One'	Pass
1.0	2.2.28 (L2) Ensure 'Log on as a batch job' is set to 'Administrators'	Fail
1.0	2.2.29 (L2) Configure 'Log on as a service'	Fail
1.0	2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'	Pass
1.0	2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One'	Pass
1.0	2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'	Pass
1.0	2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	Pass
1.0	2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators'	Pass
1.0	2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	Pass
1.0	2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	Fail
1.0	2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users'	Fail

Şekil 5.1. İyileştirme modeli öncesi kullanıcı hakları ataması tedbirleri

2.2 User Rights Assignment		
1.0	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	Pass
1.0	2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	Pass
1.0	2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	Pass
1.0	2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'	Pass
1.0	2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	Pass
1.0	2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	Pass
1.0	2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	Pass
1.0	2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'	Pass
1.0	2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators'	Pass
1.0	2.2.11 (L1) Ensure 'Create a token object' is set to 'No One'	Pass
1.0	2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Pass
1.0	2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One'	Pass
1.0	2.2.14 (L1) Configure 'Create symbolic links'	Pass
1.0	2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators'	Pass
1.0	2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'	Pass
1.0	2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	Pass
1.0	2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests'	Pass
1.0	2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests'	Pass
1.0	2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	Pass
1.0	2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'	Pass
1.0	2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'	Pass
1.0	2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Pass
1.0	2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'	Pass
1.0	2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'	Pass
1.0	2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One'	Pass
1.0	2.2.28 (L2) Ensure 'Log on as a batch job' is set to 'Administrators'	Fail
1.0	2.2.29 (L2) Configure 'Log on as a service'	Fail
1.0	2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'	Pass
1.0	2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One'	Pass
1.0	2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'	Pass
1.0	2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	Pass
1.0	2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators'	Pass
1.0	2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	Pass
1.0	2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	Pass
1.0	2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users'	Pass

Şekil 5.2. İyileştirme modeli sonrası kullanıcı hakları ataması tedbirleri

Şekil 5.3'te iyileştirme modeli öncesi kullanıcı hesapları tedbirleri analiz edilmiştir. Ardından, Şekil 5.4'de iyileştirme modeli sonrası kullanıcı hesapları tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

17.2 Account Management		
1.0	17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	Fail
1.0	17.2.2 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'	Pass
1.0	17.2.3 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	Fail

Şekil 5.3. İyileştirme modeli öncesi kullanıcı hesapları tedbirleri

17.2 Account Management	
1.0 17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	Pass
1.0 17.2.2 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'	Pass
1.0 17.2.3 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	Pass

Şekil 5.4. İyileştirme modeli sonrası kullanıcı hesapları tedbirleri

Şekil 5.5'te iyileştirme modeli öncesi Microsoft güvenlik rehberi tedbirleri analiz edilmiştir. Ardından, Şekil 5.6'da iyileştirme modeli sonrası Microsoft güvenlik rehberi tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

18.4 MS Security Guide	
1.0 18.4.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'	Fail
1.0 18.4.2 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	Fail
1.0 18.4.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	Fail
1.0 18.4.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'	Fail
1.0 18.4.5 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled'	Fail
1.0 18.4.6 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	Fail
1.0 18.4.7 (L1) Ensure 'LSA Protection' is set to 'Enabled'	Fail
1.0 18.4.8 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'	Fail
1.0 18.4.9 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	Fail

Şekil 5.5. İyileştirme modeli öncesi Microsoft güvenlik rehberi tedbirleri

18.4 MS Security Guide	
1.0 18.4.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'	Fail
1.0 18.4.2 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	Fail
1.0 18.4.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	Pass
1.0 18.4.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'	Pass
1.0 18.4.5 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled'	Fail
1.0 18.4.6 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	Fail
1.0 18.4.7 (L1) Ensure 'LSA Protection' is set to 'Enabled'	Fail
1.0 18.4.8 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'	Pass
1.0 18.4.9 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	Fail

Şekil 5.6. İyileştirme modeli sonrası Microsoft güvenlik rehberi tedbirleri

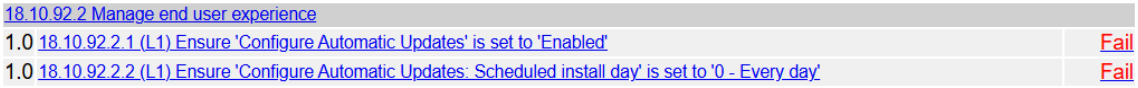
Şekil 5.7'de iyileştirme modeli öncesi Windows Powershell tedbirleri analiz edilmiştir. Ardından, Şekil 5.8'de iyileştirme modeli sonrası Windows Powershell tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

18.10.86 Windows PowerShell	
1.0 18.10.86.1 (L2) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled'	Fail
1.0 18.10.86.2 (L2) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled'	Fail

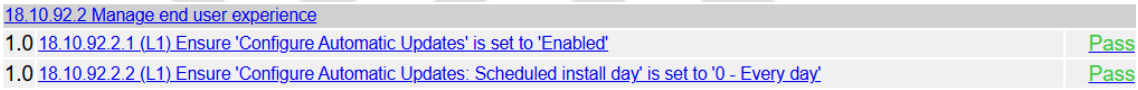
Şekil 5.7. İyileştirme modeli öncesi Windows Powershell tedbirleri

Şekil 5.8. İyileştirme modeli sonrası Windows Powershell tedbirleri

Şekil 5.9'da iyileştirme modeli öncesi son kullanıcı deneyimi tedbirleri analiz edilmiştir. Ardından, Şekil 5.10'da iyileştirme modeli sonrası kullanıcı deneyimi tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.



Şekil 5.9. İyileştirme modeli öncesi son kullanıcı deneyimi tedbirleri



Şekil 5.10. İyileştirme modeli sonrası kullanıcı deneyimi tedbirleri

CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)' profili üzerinde yapılan tüm testler başarılı bir şekilde sonuçlandırılmıştır.

5.2.2. GNU/Linux Ubuntu 20.04 LTS

GNU/Linux Ubuntu Linux 20.04 LTS işletim sistemi üzerinde CIS-CAT aracı ile yapılan testlerde, ilk olarak Şekil 5.11'de iyileştirme modeli öncesi dosya sistemi yapılandırması tedbirleri analiz edilmiştir. Ardından, Şekil 5.12'de iyileştirme modeli sonrası dosya sistemi yapılandırması tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

1.1.1 Disable unused filesystems		
1.0	1.1.1.1 Ensure mounting of cramfs filesystems is disabled	Fail
1.0	1.1.1.2 Ensure mounting of freevxfs filesystems is disabled	Fail
1.0	1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	Fail
1.0	1.1.1.4 Ensure mounting of hfs filesystems is disabled	Fail
1.0	1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	Fail
1.0	1.1.1.6 Ensure mounting of squashfs filesystems is disabled	Pass
1.0	1.1.1.7 Ensure mounting of udf filesystems is disabled	Fail

Şekil 5.11. İyileştirme modeli öncesi dosya sistemi yapılandırması tedbirleri

1.0	1.1.1.1 Ensure mounting of cramfs filesystems is disabled	Pass
1.0	1.1.1.2 Ensure mounting of freevxfs filesystems is disabled	Pass
1.0	1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	Pass
1.0	1.1.1.4 Ensure mounting of hfs filesystems is disabled	Pass
1.0	1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	Pass
1.0	1.1.1.6 Ensure mounting of squashfs filesystems is disabled	Pass
1.0	1.1.1.7 Ensure mounting of udf filesystems is disabled	Pass

Şekil 5.12. İyileştirme modeli sonrası dosya sistemi yapılandırması tedbirleri

İyileştirme modeli sonrası yapılan çalışmada Şekil 5.13'te iyileştirme modeli öncesi dosya sistemi yapılandırması tedbirleri analiz edilmiştir. Ardından, Şekil 5.14'te iyileştirme modeli sonrası dosya sistemi yapılandırması tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

1.0	1.1.10 Disable USB Storage	Fail

Şekil 5.13. İyileştirme modeli öncesi dosya sistemi yapılandırması tedbirleri

1.0	1.1.10 Disable USB Storage	Pass

Şekil 5.14. İyileştirme modeli sonrası dosya sistemi yapılandırması tedbirleri

İyileştirme modeli sonrası yapılan çalışmada Şekil 5.15'te iyileştirme modeli öncesi dosya sistemi bütünlüğü tedbirleri analiz edilmiştir. Ardından, Şekil 5.16'da iyileştirme modeli sonrası dosya sistemi bütünlüğü tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

1.2 Filesystem Integrity Checking		
1.0	1.2.1 Ensure AIDE is installed	Fail
1.0	1.2.2 Ensure filesystem integrity is regularly checked	Fail

Şekil 5.15. İyileştirme modeli öncesi dosya sistemi bütünlüğü tedbirleri

1.2 Filesystem Integrity Checking		
1.0	1.2.1 Ensure AIDE is installed	Pass
1.0	1.2.2 Ensure filesystem integrity is regularly checked	Pass

Şekil 5.16. İyileştirme modeli sonrası dosya sistemi bütünlüğü tedbirleri

Şekil 5.17'de iyileştirme modeli öncesi güvenli önyükleme (boot) tedbirleri analiz edilmiştir. Ardından, Şekil 5.18'de iyileştirme modeli sonrası güvenli önyükleme (boot) tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

1.4 Secure Boot Settings		
1.0	1.4.1 Ensure bootloader password is set	Fail
1.0	1.4.2 Ensure permissions on bootloader config are configured	Fail
1.0	1.4.3 Ensure authentication required for single user mode	Fail

Şekil 5.17. İyileştirme modeli öncesi güvenli önyükleme (boot) tedbirleri

1.4 Secure Boot Settings		
1.0	1.4.1 Ensure bootloader password is set	Pass
1.0	1.4.2 Ensure permissions on bootloader config are configured	Pass
1.0	1.4.3 Ensure authentication required for single user mode	Pass

Şekil 5.18. İyileştirme modeli sonrası güvenli önyükleme (boot) tedbirleri

Şekil 5.19'da iyileştirme modeli öncesi zorunlu erişim kontrolü tedbirleri analiz edilmiştir. Ardından, Şekil 5.20'de iyileştirme modeli sonrası zorunlu erişim kontrolü tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

1.6 Mandatory Access Control		
1.6.1 Configure AppArmor		
1.0	1.6.1.1 Ensure AppArmor is installed	Fail
1.0	1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration	Fail

Şekil 5.19. İyileştirme modeli öncesi zorunlu erişim kontrolü tedbirleri

1.6 Mandatory Access Control		
1.6.1 Configure AppArmor		
1.0	1.6.1.1 Ensure AppArmor is installed	Pass
1.0	1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration	Pass

Şekil 5.20. İyileştirme modeli sonrası zorunlu erişim kontrolü tedbirleri

Şekil 5.21'de iyileştirme modeli öncesi erişim tedbirleri analiz edilmiştir. Ardından, Şekil 5.22'de iyileştirme modeli sonrası erişim tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

4 Access, Authentication and Authorization		
4.1 Configure time-based job schedulers		
1.0	4.1.1 Ensure cron daemon is enabled and active	Pass
1.0	4.1.2 Ensure permissions on /etc/crontab are configured	Fail
1.0	4.1.3 Ensure permissions on /etc/cron.hourly are configured	Fail
1.0	4.1.4 Ensure permissions on /etc/cron.daily are configured	Fail
1.0	4.1.5 Ensure permissions on /etc/cron.weekly are configured	Fail
1.0	4.1.6 Ensure permissions on /etc/cron.monthly are configured	Fail
1.0	4.1.7 Ensure permissions on /etc/cron.d are configured	Fail
1.0	4.1.8 Ensure cron is restricted to authorized users	Fail
1.0	4.1.9 Ensure at is restricted to authorized users	Pass

Şekil 5.21. İyileştirme modeli öncesi erişim tedbirleri

4 Access, Authentication and Authorization		
4.1 Configure time-based job schedulers		
1.0	4.1.1 Ensure cron daemon is enabled and active	Pass
1.0	4.1.2 Ensure permissions on /etc/crontab are configured	Pass
1.0	4.1.3 Ensure permissions on /etc/cron.hourly are configured	Pass
1.0	4.1.4 Ensure permissions on /etc/cron.daily are configured	Pass
1.0	4.1.5 Ensure permissions on /etc/cron.weekly are configured	Pass
1.0	4.1.6 Ensure permissions on /etc/cron.monthly are configured	Pass
1.0	4.1.7 Ensure permissions on /etc/cron.d are configured	Pass
1.0	4.1.8 Ensure cron is restricted to authorized users	Pass
1.0	4.1.9 Ensure at is restricted to authorized users	Pass

Şekil 5.22. İyileştirme modeli sonrası erişim tedbirleri

Şekil 5.23'te iyileştirme modeli öncesi PAM tedbirleri analiz edilmiştir. Ardından, Şekil 5.24'te iyileştirme modeli sonrası PAM tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

4.4 Configure PAM		
1.0	4.4.1 Ensure password creation requirements are configured	Fail
1.0	4.4.2 Ensure lockout for failed password attempts is configured	Fail
1.0	4.4.3 Ensure password reuse is limited	Fail

Şekil 5.23. İyileştirme modeli öncesi PAM tedbirleri

4.4 Configure PAM		
1.0	4.4.1 Ensure password creation requirements are configured	Pass
1.0	4.4.2 Ensure lockout for failed password attempts is configured	Pass
1.0	4.4.3 Ensure password reuse is limited	Pass

Şekil 5.24. İyileştirme modeli sonrası PAM tedbirleri

Şekil 5.25'te iyileştirme modeli öncesi kullanıcı hesapları ve ortam tedbirleri analiz edilmiştir. Ardından, Şekil 5.26'da iyileştirme modeli sonrası kullanıcı hesapları ve ortam tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

4.5 User Accounts and Environment		
4.5.1 Set Shadow Password Suite Parameters		
1.0	4.5.1.1 Ensure minimum days between password changes is configured	Fail
1.0	4.5.1.2 Ensure password expiration is 365 days or less	Fail

Şekil 5.25. İyileştirme modeli öncesi kullanıcı hesapları ve ortam tedbirleri

4.5 User Accounts and Environment		
4.5.1 Set Shadow Password Suite Parameters		
1.0	4.5.1.1 Ensure minimum days between password changes is configured	Pass
1.0	4.5.1.2 Ensure password expiration is 365 days or less	Pass

Şekil 5.26. İyileştirme modeli sonrası kullanıcı hesapları ve ortam tedbirleri

Şekil 5.27'de iyileştirme modeli öncesi denetim kuralları tedbirleri analiz edilmiştir. Ardından, Şekil 5.28'de iyileştirme modeli sonrası denetim kuralları tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

5.2.3 Configure auditd rules		
1.0	5.2.3.1 Ensure changes to system administration scope (sudoers) is collected	Fail
1.0	5.2.3.2 Ensure actions as another user are always logged	Fail
1.0	5.2.3.3 Ensure events that modify the sudo log file are collected	Fail
1.0	5.2.3.4 Ensure events that modify date and time information are collected	Fail
1.0	5.2.3.5 Ensure events that modify the system's network environment are collected	Fail
1.0	5.2.3.6 Ensure use of privileged commands are collected	Fail
1.0	5.2.3.7 Ensure unsuccessful file access attempts are collected	Fail
1.0	5.2.3.8 Ensure events that modify user/group information are collected	Fail
1.0	5.2.3.9 Ensure discretionary access control permission modification events are collected	Fail
1.0	5.2.3.10 Ensure successful file system mounts are collected	Fail
1.0	5.2.3.11 Ensure session initiation information is collected	Fail
1.0	5.2.3.12 Ensure login and logout events are collected	Fail
1.0	5.2.3.13 Ensure file deletion events by users are collected	Fail
1.0	5.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected	Fail

Şekil 5.27. İyileştirme modeli öncesi denetim kuralları tedbirleri

5.2.3 Configure auditd rules		
1.0	5.2.3.1 Ensure changes to system administration scope (sudoers) is collected	Pass
1.0	5.2.3.2 Ensure actions as another user are always logged	Fail
1.0	5.2.3.3 Ensure events that modify the sudo log file are collected	Pass
1.0	5.2.3.4 Ensure events that modify date and time information are collected	Fail
1.0	5.2.3.5 Ensure events that modify the system's network environment are collected	Pass
1.0	5.2.3.6 Ensure use of privileged commands are collected	Fail
1.0	5.2.3.7 Ensure unsuccessful file access attempts are collected	Fail
1.0	5.2.3.8 Ensure events that modify user/group information are collected	Pass
1.0	5.2.3.9 Ensure discretionary access control permission modification events are collected	Fail
1.0	5.2.3.10 Ensure successful file system mounts are collected	Fail
1.0	5.2.3.11 Ensure session initiation information is collected	Fail
1.0	5.2.3.12 Ensure login and logout events are collected	Pass
1.0	5.2.3.13 Ensure file deletion events by users are collected	Fail
1.0	5.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected	Pass

Şekil 5.28. İyileştirme modeli sonrası denetim kuralları tedbirleri

Şekil 5.29'da iyileştirme modeli öncesi sistem bakım tedbirleri analiz edilmiştir. Ardından, Şekil 5.30'da iyileştirme modeli sonrası sistem bakım tedbirlerinin başarılı bir şekilde uygulandığı ve BİGR maddelerine göre bulguların kapatıldığı gözlemlenmiştir.

1.0	6.1.11 Ensure world writable files and directories are secured	Fail

Şekil 5.29. İyileştirme modeli öncesi sistem bakım tedbirleri

1.0	6.1.11 Ensure world writable files and directories are secured	Pass

Şekil 5.30. İyileştirme modeli sonrası sistem bakım tedbirleri

CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1 Level 2 – Workstation profili üzerinde yapılan tüm testler başarılı bir şekilde sonuçlandırılmıştır.

6. SONUÇLAR VE ÖNERİLER

Bu bölümde tez çalışmasının sonuçları ve öneriler hakkında bilgi verilmektedir.

6.1 Sonuçlar

Bu tez çalışmasında, Windows ve GNU/Linux işletim sistemlerinde güvenlik sıkılaştırma süreçleri detaylı bir şekilde ele alınmıştır. Çalışmada her iki işletim sisteminin güvenlik risklerini tespit etmek ve bu riskleri gidermek amacıyla çeşitli analizler yapılmış ve güvenlik iyileştirme stratejileri uygulanmıştır. Elde edilen bulgulara göre, her iki işletim sistemindeki güvenlik açıklarının büyük bir kısmı, sistem yapılandırmalarındaki eksikliklerden ve yazılım güncellemelerinin ihmal edilmesinden kaynaklanmaktadır. Özellikle, Windows işletim sistemlerinde kullanıcı hesap yönetimi, grup ilkeleri ve ağ yapılandırmalarındaki eksiklikler büyük güvenlik açıkları yaratırken, GNU/Linux sistemlerinde ise kullanıcı hakları yönetimi, sudo konfigürasyonları ve gereksiz servislerin açık bırakılması gibi unsurlar ciddi riskler taşımaktadır.

Geliştirilen güvenlik iyileştirme modeli, her iki işletim sistemi için adım adım uygulanabilir bir yaklaşım sunmaktadır. İlk aşamada temel güvenlik yapılandırmalarının yapılması, kullanıcı haklarının yönetilmesi ve ağ yapılandırmalarının güvence altına alınması önerilmektedir. İkinci aşamada ağ güvenliği önlemlerinin güçlendirilmesi ve sistemdeki zayıf noktaların tespiti için sızma testlerinin yapılması gerektiği vurgulanmıştır. Üçüncü aşamada ise sistem izleme ve saldırı tespiti yöntemlerinin devreye alınması gerektiği belirtilmiştir. Yapılan testler, güvenlik sıkılaştırma adımlarının, işletim sistemlerinin güvenlik düzeylerini anlamlı bir şekilde artırdığını göstermektedir.

6.2 Öneriler

Bu çalışmanın bulgularına göre, güvenlik sıkılaştırma süreçlerinin etkinliği yalnızca teknik yapılandırmalarla sınırlı kalmamalıdır. Kullanıcıların ve sistem yöneticilerinin güvenlik konularında eğitilmesi, siber güvenlik önlemlerinin başarıyla uygulanabilmesi için kritik bir adımdır. Özellikle sosyal mühendislik saldırıları gibi insan faktörüne dayalı tehditler göz önüne alındığında, güvenlik eğitimleri daha da

önemli hale gelmektedir. Kullanıcıların güçlü parolalar kullanmaları, kimlik avı saldırılarına karşı dikkatli olmaları ve güvenlik güncellemelerini takip etmeleri gibi temel güvenlik önlemleri hakkında bilgilendirilmeleri gerekmektedir.

Bu çalışmada geliştirilen güvenlik iyileştirme modeli, Windows ve GNU/Linux işletim sistemleri üzerinde test edilmiştir. Ancak, modelin daha geniş bir kapsamda test edilmesi, farklı işletim sistemlerinde de uygulanabilirliğinin değerlendirilmesi gerekmektedir. Özellikle macOS, BSD gibi diğer popüler işletim sistemlerinde de bu modelin uygulanarak, güvenlik iyileştirme stratejisinin evrenselliği test edilmelidir. Ayrıca, uzaktan bağlantılar üzerinden yapılacak testler, dış tehditlere karşı alınması gereken güvenlik önlemleri konusunda daha fazla bilgi sunacaktır.

Güvenlik iyileştirme süreçlerinin etkinliğini artırmak ve sürdürülebilirliğini sağlamak için otomasyon ve izleme araçlarının kullanımı büyük önem taşımaktadır. Otomatik güncellemeler ve sistem izleme araçları, güvenlik açıklarının hızla tespit edilmesini ve giderilmesini sağlayacaktır. Otomasyon, özellikle sistem yöneticilerinin iş yükünü hafifletecek ve insan hatasından kaynaklanan güvenlik açıklarını azaltacaktır. Ayrıca, izleme araçları sayesinde, ağdaki anormal aktiviteler ve potansiyel tehditler erkenden tespit edilebilir ve hızla müdahale edilebilir.

Siber tehditlerin hızla evrimleşmesi, mevcut güvenlik standartlarının dinamik bir şekilde güncellenmesini zorunlu kılmaktadır. Bu çalışmada elde edilen bulgulara göre, ulusal ve uluslararası güvenlik standartlarının esnek ve güncel olması gerektiği sonucuna varılmıştır. Mevcut güvenlik protokollerinin hızla değişen tehditlere karşı yeterli olmadığı ve standartların sürekli olarak gözden geçirilmesi gerektiği vurgulanmıştır. Bu bağlamda, güvenlik standartlarının daha dinamik hale getirilmesi, sektördeki güvenlik boşluklarının hızla kapatılmasına yardımcı olacaktır.

Yapay zekâ (AI) destekli tehdit tespiti ve önleme sistemleri, gelecekteki araştırmalarda dikkate alınması gereken önemli bir konudur. Yapay zekâ, potansiyel tehditleri tespit etmek ve anormal davranışları izlemek konusunda daha etkili sonuçlar verebilir. AI tabanlı güvenlik sistemlerinin, özellikle bilinmeyen tehditler ve sıfırıncı gün saldırıları gibi karmaşık tehditlere karşı daha hızlı ve doğru çözüm geliştirebilmesi

mümkündür. Bu teknolojilerin, mevcut güvenlik araçlarıyla entegrasyonu, siber güvenlik alanında önemli bir gelişme sağlayacaktır.

Açık kaynak yazılımlarının güvenlik iyileştirilmesi konusu, genellikle göz ardı edilen ancak büyük güvenlik açıklarına yol açabilen bir alandır. Açık kaynak yazılımlarının güvenlik açıkları üzerine daha fazla araştırma yapılması gerektiği, bu çalışmanın bulgularından bir diğer önemli sonuçtur. Açık kaynak yazılımlarının güvenliği, ticari yazılımlar kadar ciddiyetle ele alınmalıdır. Geliştirici toplulukların güvenlik iyileştirmelerine daha fazla odaklanması, açık kaynak yazılımlarının yaygın kullanımının güvenli hale gelmesini sağlayacaktır.

Birçok güvenlik açığı, yazılım güncellemelerinin zamanında yapılmamasından kaynaklanmaktadır. Bu nedenle, sistem güncellemelerinin otomatikleştirilmesi büyük önem taşımaktadır. Güncellemelerin düzenli olarak yapılması, yazılımdaki güvenlik açıklarını hızlıca kapatacak ve sistemin genel güvenlik seviyesini yükseltecektir. Otomatik güncellemeler, kullanıcıların bu süreci ihmal etmelerinin önüne geçerek, güvenlik yönetimini daha verimli hale getirecektir. Bu sayede özellikle küçük güvenlik açıklarının büyük tehditlere dönüşmesi engellenebilir.

KAYNAKLAR

Ahmad, M. A., 2021, Worms. B. Warf. (Ed.), The sage encylopedia of the internet içinde (ss. 987-992), Sage Publications.

Akın, S., & Tanç, A., 2022, İşletmelerde Bilgi Sistemlerinin Denetiminde Siber Güvenlik Risklerinin Önemi, Erciyes Akademi, 36(2), 707-722.

Alkan, M., 2012, Siber Güvenlik ve Siber Savaşlar: Bilgi Güvenliği Derneği TBMM İnternet Komisyonu Sunumu, Tİ Komisyonu.

Aloul, F.A., 2012, The Need for Effective Information Security Awareness, Journal of Advances in Information Technology, 3(3), 176-183. DOI:10.4304/jait.3.3.

Andress, J., 2014, The Basics of Information Security (Second Edition), Waltham: Syngress.

Atasever, S., Özçelik, İ. ve Sağıroğlu, Ş., 2019, Siber terör ve DDoS, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23 (1), 238-244.

Banuls, V. A. ve M. Turoff., 2011, Scenario Construction via Delphi and Cross-Impact Analysis, Technological Forecasting & Social Change.

Beşkirli, A., Özdemir, D., & Beşkirli, M., 2019, Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme, Avrupa Bilim ve Teknoloji Dergisi, 284-291.

Bhanot, R., Hans, R., 2015, A review and comparative analysis of various encryption algorithms, International Journal of Security and Its Applications, 9(4): 289-306.

Bowles, S., Hernandez-Castro, J., 2015, The first 10 years of the Trojan Horse defence, Computer Fraud & Security, 2(1), 5-13. DOI:10.1016/S1361-3723(15)700059.

Center for Audit Quality, 2019, rep. 2019, Main Street Investor Survey (pp. 18–19).

Chuang, 2024, VMware Fusion and Workstation are Now Free for All Users https://blogs.vmware.com/cloud-foundation/2024/11/11/vmware-fusion-and-workstation-are-now-free-for-all-users/, [Ziyaret Tarihi: 02.12.2024].

CIS Critical Security Controls, 2023, CIS CSAT: A Free Tool for Assessing Implementation of CIS Critical Security Controls, [online], https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls, [Ziyaret Tarihi: 02.12.2024].

CIS, 2024, Getting to Know the CIS Benchmarks https://www.cisecurity.org/insights/blog/getting-to-know-the-cis-benchmarks, [Ziyaret Tarihi: 05.12.2024].

Cisco, 2024, Cisco Annual Internet Report (2018–2023) White Paper [Graph]. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, [Ziyaret Tarihi: 01.12.2024].

Clark, 2020, Security Automation for Windows Hosts: Hardening of Windows 10 Password Policy, Master's thesis, Jamk University of Applied Sciences.

CVE details, 2024, Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2024, [online], https://www.cvedetails.com/top-50-products.php?year=2024, [Ziyaret Tarihi: 01.12.2024].

Cybersecurity Insiders, 2024, Which types of security attacks against applications has your organization experienced over the past 12 months? Statista, https://www.statista.com/statistics/1463544/top-cyberattacks-against-applications-worldwide/, [Ziyaret Tarihi: 24.11.2024].

DDO, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2020, Bilgi ve iletişim güvenliği rehberi,[online],https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf , [Ziyaret Tarihi: 12.12.2023].

Demir, S., 2014., BT Süreç Yönetimi ve Deployment Yönetimi Uygulaması, Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü.

Elbahadır, H., 2011, Haching İnterface, Kodlab Yayınevi, İstanbul.

Elibol, M., 2021, İAU Bilişim Sistemlerinin ITIL Esaslarına Göre Performans Analizi, İletişim Çalışmaları Dergisi, 7(1), 93-108.

Ericsson, 2024, Number of connected devices worldwide in 2015 and 2029, by device (in billions) [Graph]. In Statista. Retrieved November 25, 2024, [online], https://www.statista.com/statistics/512650/worldwide-connected-devices-amount/, [Ziyaret Tarihi: 24.11.2024].

Federal Register, 2024, Cybersecurity Maturity Model Certification (CMMC) Program [online], https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program, [Ziyaret Tarihi: 24.11.2024].

Geeksforgeeks, 2024, manjeetks007, What is an Operating System? [online], https://www.geeksforgeeks.org/what-is-an-operating-system/, [Ziyaret Tarihi: 24.11.2024].

GNU, 2021, Richard Stallman, Linux ve GNU Sistemi [online], https://www.gnu.org/gnu/linux-and-gnu.html, [Ziyaret Tarihi: 24.11.2024].

Güntay, V., 2014, Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler, sayfa 83 sayı 27. Araştırma Makalesi Güvenlik Stratejileri (27), 79-111.

Harris R., 2006, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Indiana 2006, sf. 4.

ISACA, 2017, Auditing Cyber Security: Evaluating Risk and Auditing Controls, ISACA.

ISO, 2013, ISO/IEC 27001:2013, Information Security Management Systems Requirements, The International Organization for Standardization, Switzerland.

İnce, 2024, Makine Öğrenmesi Yöntemleri Kullanarak Dağıtık Hizmet Reddi (DDos) Saldırılarının Belirlenmesi, Yüksek Lisans Tez, Fırat Üniversitesi, Fen Bilimleri Enstitüsü.

Işık, 2021, Bulut Ortamlarında Hipervizör ve Konteyner Tipi Sanallaştırmanın Farklı Özellikte İş Yüklerinin Performansına Etkisinin Değerlendirilmesi.

Julisch, K., 2009, Security Compliance: The Next Frontier in Security esearch, Proceedings of the 2008 workshop on New security paradigms, p71-74, Rüschlikon, Switzerland.

Kara, İ., 2019, Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi, Sakarya University Journal of Computer and Information Sciences, 2(2): 61-69.

Kara, M., 2018, Kurumsal bilgi güvenliği, Papatyabilim Yayıncılık.

Karakoç, M.M. ve Varol A., 2016, Ulusal Dağıtım Projesi ve Pardus İşletim Sistemi, Türkiye Bilim ve Teknoloji Dergisi, Cilt: 11, Sayı: 2.

Kharraz, A., 2018, Ransomware. B. Warf. (Ed.), The sage encylopedia of the internet içinde (ss. 720-724), Sage Publications.

Koç, S., Şeker, S., & Şeker, F., 2019, Bilişim Teknolojileri (BT) Denetiminde Bilgi Güvenliği İle İlgili Uluslararası Standartlar ve Türkiye'deki Uyum Çabalarının İncelenmesi, Uluslararası Muhasebe ve Finans Araştırmaları Dergisi, 1(2), 121-139.

Kökoğlu, Ç., 2020, Bankacılık Sektöründe Bilgi Teknolojileri Altyapı Kütüphanesi (ITIL) Süreçlerinin İncelenmesi, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü.

Landeta J. ve J. Barrutia, 2011, People Consultation to Construct the Future: a Delphi Application, International Journal of Forecasting, 27,134–151.

Lapena, R., 2018, Two-Thirds of Organizations Don't Use Hardening Benchmarks to Establish a Secure Baseline, [online], https://securityboulevard.com/2018/08/two-thirds-of-organizations-dont-use-hardening-benchmarks-to-establish-a-secure-baseline-report-reveals/, [Ziyaret Tarihi: 18.12.2023].

Leyla Bilge, Tudor Dumitras, 2012, "Before We Knew It: An Emprical Study of Zero-Day Attacks in The Real World" Symantec Co.

Lustig, M., 2015, Compliance at Speed, Sebastopol, California: O'Reilly Media, Inc.

Mariano M., 2024, PCI DSS Versions Over the Years | Version 1.0 – 4.0, https://www.ispartnersllc.com/blog/pci-dss-versions/, [Ziyaret Tarihi: 22.12.2024].

Marion, N. E., & Twede, J., 2020, Cybercrime: An encyclopedia of digital crime. ABC-CLIO.

McAfee, 2006, Rootkits, Part 1 of 3: The Growing Threat, https://download.nai.com/products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf, [Ziyaret Tarihi: 22.12.2024].

Microsoft, 2009, Microsoft'un Geçmişi, [online], https://learn.microsoft.com/tr-tr/shows/history/history-of-microsoft-1985, [Ziyaret Tarihi: 24.12.2024].

Microsoft, 2023 Internet Explorer masaüstü uygulamasının desteği, https://learn.microsoft.com/tr-tr/lifecycle/announcements/internet-explorer-11-end-of-support, [Ziyaret Tarihi: 28.12.2023].

Microsoft 2024, Security baselines https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines, [Ziyaret Tarihi: 26.12.2023].

Microsoft, 2012, Microsoft Free Security Tools – Microsoft Baseline Security Analyzer [online], https://microsoft.com/en-us/security/blog/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/, [Ziyaret Tarihi: 25.12.2023].

Mitnick, Kevin D and Simon, William L., 2005, Aldatma Sanatı, (Çeviren: Nejat Eralp Tezcan), Ankara, Odtü Yayıncılık.

Ostrowski, 2020, OS Hardening, Seminar paper ,Ausgewählte Kapitel der IT-Security.

OWASP, 2021, SQL Injection, [online], https://owasp.org/www-community/attacks/SQL_Injection, [Ziyaret Tarihi: 03.12.2024].

Özbay, R., 2015, Aktif Siber Savunma Teknikleri ve Performans Analizi, Afyon Yüksek Lisans Tezi, Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü, 1,6,9- 10,12, Afyonkarahisar.

Pazoğlu, 2020, SOAR B4: Playbook, [online], https://evrenbey.medium.com/soar-b4-playbook-bc91bc8d927f, [Ziyaret Tarihi: 03.12.2024].

Proofpoint, 2024, What Is Privilege Escalation?, https://www.proofpoint.com/us/threat-reference/privilege-escalation, [Ziyaret Tarihi: 19.12.2024].

Resmî Gazete, 2013, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, [online], https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf, [Ziyaret Tarihi: 18.12.2023].

Sağıroğlu, Ş. ve Şenol M. (Ed.), 2018, Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Grafiker Yayınları.

Sausalito, 2024, 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics, [online], https://cybersecurityventures.com/cybersecurity-almanac-2024/ [Ziyaret Tarihi: 19.12.2024].

Savaş, S. ve Karataş, S., 2022, Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance, International Cybersecurity Law Review, 3 (1), 7-34.

Selinger, J., 2022, The Dod's Cybersecurity Maturity Model Certification and Resulting Tensions with U.S. Standard-Setting Policy and Established it Security Authorities. SSRN Electronic Journal, 3985000.

Shen Y.C., S.H. Chang, G.T.R. Lın, H.C. Yu, 2010, A Hybrid Selection Model for Emerging Technology, Technological Forecasting & Social Change, 77, 151–166.

Siik, P., 2017, Management of Operating System Hardening in Industrial Control Systems, Yüksek Lisans Tezi, Tampere Teknoloji Üniversitesi, Tampere, 40-43.

Şahin, Ali Ekber, Eğitim Araştırmalarında Delphi Tekniği ve Kullanımı, Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, XX, 2001, 215-220.

TBD Bilişim Sözlüğü, 2023, [online], https://bilisimde.ozenliturkce.org.tr/docs/TBD-Bilişim-Sözlüğü-İngilizce-Türkçe-2023-11-20.pdf, [Ziyaret Tarihi: 25.12.2023].

Tımartaş, 2022 Dijital Servis Dönüşümü ve Bilişim Teknolojileri Altyapı Kütüphanesi

Tofan, D.C., 2011, Informtion Security Standards, Journal of Mobile, Embedded and Distributed Systems, 128-135.

Tripwire, 2018, State of Cyber Hygiene Report, [online], https://static.fortra.com/tripwire/pdfs/guides/tw-dimensional-research-state-of-cyber-hygiene-gd.pdf, [Ziyaret Tarihi: 02.01.2024].

Tulgar, M., Zaim, A. H., & Aydın, M. A., 2022, Ulusal Bilgi ve İletişim Güvenliği Rehberi: Iot Güvenliği İçin Bir Uygulama Örneği, İstanbul Commerce University Journal of Science, 21(42), 353-382.

Uslu, 2009, Veri Madenciliği ile Bilgisayar Ağlarında Yeni Bir Saldırı Tespit Algoritması, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü.

Vural Y. ve Sağıroğlu, Ş., 2008, Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), 507-522.

Xenserver, 2024 XenServer Story, [online], https://www.xenserver.com/story, [Ziyaret Tarihi: 20.12.2024].

Wikipedia, 2023, Lynis, [online], https://en.wikipedia.org/wiki/Lynis, [Ziyaret Tarihi: 03.12.2024].

Yalpı, 2020, Güvenlik Uyumluluğu İçin Windows İşletim Sistemi Sıkılaştırma Kurallarının Uygulanması ve Denetimi, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü.

Yılmaz, H.,2014, TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi, Denetişim Dergisi, 15, ss 45-59.