KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

YEREL ALAN AĞLARININ SİBER GÜVENLİK YÖNÜNDEN İNCELENMESİ VE DEĞERLENDİRİLMESİ

SEZER YILDIZ

KOCAELİ 2019

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ

ANABİLİM DALI

YÜKSEK LİSANS TEZİ

YEREL ALAN AĞLARININ SİBER GÜVENLİK YÖNÜNDEN İNCELENMESİ VE DEĞERLENDİRİLMESİ

SEZER YILDIZ

Dr.Öğr.Üyesi Umut ALTINIŞIK Danışman,	Kocaeli Üniversitesi	.....
Doç.Dr. Halil YİĞİT Jüri Üyesi,	Kocaeli Üniversitesi	.....
Prof.Dr. Celal ÇEKEN Jüri Üyesi,	Sakarya Üniversitesi	.....

Tezin Savunulduğu Tarih: 11.06.2019

ÖNSÖZ VE TEŞEKKÜR

Yerel alan ağlarını dış tehditlerden koruyan bir güvenlik duvarı ile koruma sağladığımız gibi yerel alan ağlarında da bir takım önlemler alınması gerekmektedir. Bu tez çalışmasında, büyük ölçekli ağlardaki hiyerarşik mimarinin, hizmet kalitesini sağlamak için yerel ağdaki siber güvenliğin farklı güvenlik sorunlarının pratik gereksinimler ile test edilmiş ve önemi ortaya konmuştur. Yerel alan ağlardaki açıklıkların ortaya çıkartabileceği sonuçları göstererek bu kapsamda siber tehditlere karşı bir farkındalık oluşturacağını ve bu alanda faaliyet gösteren herkese faydalı olmasını ümit etmekteyim.

Bu tez çalışmasının tüm aşamalarında görüşleri ile katkıda bulunan ve yol gösteren değerli hocam Dr.Öğr.Üyesi Umut ALTINIŞIK'a teşekkürlerimi sunarım. Ayrıca bu yoğun dönemde desteklerini benden esirgemeyen değerli akademisyen Dr.Öğr.Üyesi Ayşegül Nuriye BAYRAKTAR'a ve Öğr.Gör. Ersin ŞAHİN'e sonsuz teşekkür ederim. Her zaman yanımda olup en büyük destekçilerim sevgili babam ve anneme teşekkürlerimi sunarım.

Haziran – 2019 Sezer YILDIZ

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

Kısaltmalar

ACL : Access Control List (Erişim Kontrol Listesi)
AP : Access Point (Erişim Noktası)
APT : Advanced Persistent Threat (Gelişmiş Kalıcı Tehdit)
ARP : Address Resulation Protocol (Adres Çözümleme Protokolü)
BEC : Business E-Mail Compromise (Şirket E-Postaları Dolandırıcılığı)
BGP : Border Gateway Protocol (Sınır Geçit Protokolü)
CAM : Content Addressable Memory (İçerik Adreslenebilir Bellek)
CEO : Chief Executive Officer (Yönetim Kurulu Başkanı)
CPU : Central Processing Unit (Merkezi İşlem Birimi)
CVE : Common Vulnerabilities and Exposures (Yaygın Güvenlik Açıkları ve Maruziyetler)
DDoS : Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DoS : Denial of Service (Hizmet Engelleme)
DHCP : Dymanic Host Configuration Protocol (Dinamik Bilgisayar Yapılandırma Protokolü)
DNS : Domain Name System (Alan Adı Sistemi)
DUAL : Diffusing Update Algorihtm (Genel Güncelleme Algoritması)
DVA : Distance Vector Algorithm (Uzaklık Vektör Algoritması)
EIGRP : Enhanced Interior Gateway Routing Protocol (Arttırılmış Dahili Ağ Geçidi Yönlendirme Algoritması)
FTP : File Transfer Protocol (Dosya Transfer Protokolü)
FW : Firewall (Güvenlik Duvarı)
GNS3 : Graphical Network Simulator-3 (Grafik Ağ Similasyonu-3)
HSRP : Hot Standby Router Protocol (Hazır Yedekteki Yönlendirici Protokolü)
HSTS : Hypertext Strict Transport Security (Sıkı Metin Taşıma Güvenliği)
HTTP : Hyper-Text Transfer Protocol (Hiper-Metin Aktarma İletişim Kuralı)
HTTPS : Hyper-Text Transfer Protocol Secure (Hiper-Metin Aktarma Güvenli İletişim Kuralı)
ICMP : Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)
IEEE : The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IP : Internet Protocol (İnternet Protokolü)
IOS : Internetwork Operating System (Ağ İşletim Sistemi)
ISP : Internet Service Provider (İnternet Servis Sağlayıcı)

LAN	: Local Area Network (Yerel Alan Ağ)
LLMNR	: Link-Local Multicast Name Resolution (Yerel Bağlantı Çoklu İsimi Çözümlemesi)
LSA	: Link State Algorithm (Bağlantı Durumu Algoritması)
MAC	: Media Access Control (Medya Erişim Kontrolü)
MD5	: Message-Digest Algorithm 5 (Mesaj Özet Algoritması 5)
MDNS	: Multicast Domain Name System (Çoklu Alan Adı Sistemi)
MITM	: Man In The Middle (Ortadaki Adam)
MPLS	: Multi Protocol Label Switching (Çoklu Protokol Etiket Anahtarlama)
MSF	: Metasploit Framework (Güvenlik Rehber Yazılımı)
NAT	: Network Address Translation (Ağ Adres Çeviricisi)
NBT-NS	: NETBIOS Name Service (NETBIOS İsim Servisi)
NETBIOS	: Network Basic Input/Output System (Ağ Temel Giriş/Çıkış Sistemi)
OS	: Operating System (İşletim Sistemi)
OSI	: Open System Interconnection (Açık Sistemler Ara Bağlantısı)
OSPF	: Open Shortest Path First (En Kısa Yola Öncelik)
PVA	: Path Vector Algorithm (Yol Vektör Algoritması)
RAM	: Random Access Memory (Rastgele Erişilebilir Bellek)
RIP	: Routing Information Protocol (Yönlendirme Bilgisi Protokolü)
SCADA	: Supervisory Control And Data Acquisition (Uzaktan Kontrol ve Gözleme Sistemi)
SHA	: Secure Hashing Algorithm (Güvenli Özetleme Algoritması)
SMB	: Server Message Block (Sunucu İleti Bloğu)
SSH	: Secure SHELL (Güvenli Kabuk)
SSL	: Secure Sockets Layer (Güvenli Soket Katmanı)
STP	: Spanning Tree Protocol (Kapsayan Ağaç Protokolü)
SVI	: Switch Virtual Interface (Anahtar Sanal Ara yüzü)
TCP	: Transmission Control Protocol (Taşıma Kontrol Protokolü)
TLS	: Transport Layer Security (Aktarım Katmanı Güvenliği)
TTL	: Time to Live (Yaşam Zamanı)
VLAN	: Virtual Local Area Network (Sanal Yerel Alan Ağı)
VM	: Virtual Machine (Sanal Makine)
VPCS	: Virtual Personal Computer Simulator (Sanal Bilgisayar Simülatör)
VTP	: Virtual Trunking Protocol (Sanal Yerel Ağ Aktarım Protokolü)

YEREL ALAN AĞLARININ SİBER GÜVENLİK YÖNÜNDEN İNCELENMESİ VE DEĞERLENDİRİLMESİ

ÖZET

Teknoloji alanındaki hızlı gelişmeler ve çalışan kişi sayısındaki artışlar nedeniyle yerel alan ağları karmaşık hale gelmiştir. Bu durum siber güvenlik probleminin ortaya çıkmasına neden olmaktadır. Saldırganlar, farklı saldırı yöntemlerini kullanarak yerel alan ağlarındaki tespit ettikleri zafiyetleri kendi amaçları doğrultusunda kullanmaktadır. Saldırganların başkaları tarafından üretilmiş hazır teknolojik araç ve gereçleri kullanarak, detaylı teknik bilişim bilgisine gereksinim duymadan siber saldırılar yapabilmekte ve bu saldırılar yoluyla yüksek düzeylerde kazanç sağlamaktadırlar. Alınacak bir takım güvenlik tedbirleri ile yerel alan ağları güvenli hale getirilebilmektedir.

Tez çalışmasında siber güvenlik ve bilgi güvenliği farkındalığının önemini göstermek üzere, sanallaştırma temelli işletim sistemleri ve servislerinin kurulumları hazırlanarak, yedekli ve yük dağılım özelliklerini barındıran bir ağ prototipi gerçekleştirilmiştir. Ağ prototipi GNS3 (Graphical Network Simulation 3- Grafik Ağ Simülasyonu 3) benzetim programı kullanılarak tasarlanmıştır. Sanal işletim sistemleri ile GNS3 benzetim programlarının birbirlerine entegresi sağlanmıştır. Böylece siber saldırı senaryolarının yapılabileceği bir sistem gerçekleştirilmiştir. Bu sistem üzerinde en yaygın yerel alan ağ saldırı yöntemleri uygulanmış ve çıkan sonuçlar için değerlendirmeler yapılmıştır. Ağ yöneticisinin dikkat etmesi gereken noktalar ve koruma yöntemleri benzetim programı üzerinden gösterilmesi sağlanmıştır. Çalışmada ARP zehirleme saldırılarını tespit etmek ve önlemek için Python dili kullanılarak web tabanlı bir uygulama gerçekleştirilmiştir.

Anahtar Kelimeler: Benzetim, Bilgi Güvenliği Farkındalığı, Siber Saldırılar, Yerel Ağ.

INVESTIGATION AND EVALUATION OF LOCAL AREA NETWORKS FROM CYBER SECURITY STANDPOINT

ABSTRACT

Rapid developments in technology and the increase in the number of people working in this field have caused the Local Area Networks to become complicated. This situation leads to the emergence of cyber security problem. Attackers use the weaknesses they detected by using different attack methods in local area networks for their own purposes. Attackers are able to make cyber attacks without the need for detailed technical informatics information by using ready-made technological tools and equipment produced by others, and provides high levels of gains through these attacks. Local area networks can be brought as secured by taking a number of security precautions.

In order to show the importance of cyber security and information security awareness in the thesis study, a network prototype with redundant and load distribution features has been realized by preparing the installation of operating systems and services through virtualization technology. The network prototype was designed using the simulation program GNS3 (Graphical Network Simulation 3). Virtual operating systems and the GNS3 simulation program integration is provided. Thus, a system has been realized in which cyber attack scenarios can be made. The most common attacks over the local area networks were tried on this system and the evaluations were made on the results obtained. The points that the network administrator should pay attention to and the protection methods are shown through the simulation program. In order to detect and prevent ARP poisoning attacks in the study, a web-based application was carried out using Python language.

Keywords: Simulation, Information Security Awareness, Cyber Attacks, Local Area Networks.

GİRİŞ

Günümüzde siber tehditler sadece bilgi teknolojileri alanında faaliyet gösteren kurumları değil o ülkenin askeri, sağlık, otonom araçlar, havayolu ve hukuk gibi birçok alanlarda faaliyet gösteren kurum ve kuruluşları olumsuz olarak etkilemektedir. Siber saldırıların önlenmesine yönelik olarak kurumlar tarafından çeşitli çalışmalar gerçekleştirilmektedir. Bu çalışmalarda teknolojide meydana gelen hızlı değişim göz önüne alınarak güvenlik mekanizmasının tesis edilmesi gerekmektedir. Bilgisayar ve Ağ Güvenliği firması olan WatchGuard'ın 2018 yılının ilk çeyreğinde açıkladığı rapora göre o dönemde gerçekleşen ağ saldırısı 2017 yılının son çeyreğinde gerçekleşen ağ saldırılarına göre %52 artış göstererek 10 milyondan fazla ağ istismarı yaşanmıştır [1].

APT (Advanced Persistent Threat - Gelişmiş Kalıcı Tehdit) saldırı türü birçok saldırı tekniğinin karmaşık bir biçimde kullanılmasıyla tasarlanmış, büyük ölçekli kurumsal firmaları hedef alan saldırılardır. Kurumsal alanda yapılacak olan APT saldırılarının büyük bir çoğunluğunun gerçekleştikten sonra tespit edildiği görülmektedir [2]. Bunun nedeni, saldırının çok yavaş ve fark ettirmeden sisteme sızılarak gerçekleştirilmesidir. Bu saldırıya karşı korumanın daha üst seviyelerde olabilmesi için kurum bilgi teknolojileri uzmanlarının, günlük olağan ağ trafiğini izlemesi, yerel alan ağını mantıksal bölümlere ayırması, bal küpü ağlarını aktif etmesi ve sadece önceden tanımlanmış uygulamalara erişim sağlamaları gerekmektedir.

Sosyal mühendislik e-posta, telefon veya fiziksel yöntemlerin kullanılarak insanların kandırılması ile gerçekleştirilen saldırılardır. Sosyal mühendislik saldırı türlerinden olan oltalama saldırısı kurbanın e-postasına gönderilen bağlantı aracılığı ile sahte web adresine yönlendirerek kurbanın kişisel bilgilerini elde etmekte ve kurum içi iş sürecini bozmayı amaçlamaktadır. BEC (Business E-Mail Compromise - Şirket E-Postaları Dolandırıcılığı) saldırısı, üst düzey yöneticilerin kullandığı e-posta adresini taklit ederek veya kaba kuvvet saldırıları ile ele geçirerek gerçekleştirdiği bir oltalama saldırı

türüdür. Bu saldırının yapılışını senaryo şeklinde ifade ettiğimizde; A kurumu B kurumuna hizmet vermektedir. Her ayın sonunda hizmet bedeli olarak B kurumu, A kurumunun önceden belirlediği IBAN numarasına bir bedel ödemektedir. Saldırgan, B kurumunun muhasebeden sorumlu personeline A kurumunun finans yöneticisinden geliyor gibi göstererek "IBAN numaramız değişmiştir" içerikli e-postayı B kurumuna yollayarak atağı gerçekleştirmektedir. FBI (Federal Bureau of Investigation - Federal Soruşturma Bürosu) tarafından 2018 yılında yayınlanan rapora göre BEC tabanlı küresel kayıplar 2013-2018 yılları arasında 12 milyar doları aştığı, küçük orta ve büyük ölçekli işletme ve kişisel işlemleri hedef alarak %136 oranında arttığı vurgulanmaktadır. Bu tip saldırılar sonucunda kurum açısından verilerinin saldırganın eline geçmesiyle o verinin hazırlanması için geçen zamanın boşa gitmesine, maddi ve prestij kaybına sebep olmaktadır. BEC dolandırıcılığında e-posta sahtekarlığı, uzlaşma, veri hırsızlığı, sahte fatura, avukat kimliğine bürünme ve üst düzey dolandırıcılık gibi farklı tekniklerin kullanılması sonucunda diğer e-posta saldırılarından farklılaşarak APT olarak sınıflandırılmaktadır. MuddyWater, 2017 yılında tespit edilmiş oltalama saldırı mantığıyla çalışan özellikle resmi kurumlar hedeflenerek resmi bir kurumdan geliyor gibi e-posta eki olarak gönderilen makro tabanlı dokümanın kurban tarafından çalıştırılması sonucunda zararlının kurban bilgisayarı üzerinde arka kapı oluşturarak bilgi sızdırılması hedeflenmektedir.

Saldırganların gerçekleştirdiği saldırıların %18'lik bir bölümünü zararlı e-posta eklentilerini kullanarak, %16'lik bölümünü ise oltalama saldırı tekniği ile gerçekleştirmektedirler. Toplamda %34'lük bir bölümünü kapsamasından dolayı saldırganların gerçekleştirdiği her üç saldırıdan en az bir tanesinin e-posta kaynaklı olduğunun sonucuna varılmaktadır. Bu sebeple siber saldırıların bu e-posta kaynaklılardan en az bir tanesinin oltalama e-postalarından veya kurum çalışanlarına zararlı yazılım içeren e-posta eklentileri gönderilerek gerçekleştiğini göstermektedir. Kurumun personeline yönelik kurum içi bilgi güvenliği eğitimleri yapması ve siber risk taşıyan davranışlardan kaçınılması gerektiği anlatılmalıdır [3].

SSL (Secure Sockets Layer - Güvenli Soket Katmanı), web servislerinin hedef ile kaynak arasındaki haberleşmenin şifrelemesi için kullanılan bir güvenlik katmanıdır. OSI (Open System Interconnection - Açık Sistemler Ara Bağlantısı), farklı markadaki

tüm ağ kartı üreticilerinin haberleşmelerindeki uyum problemini ortadan kaldırmak için geliştirilmiş yedi katmanlı bir referans modelidir. OSI referans modelinin yedinci katmanında çalışan servislerin kullandığı portların kontrol edilmemesi ve süresi tamamlanan SSL sertifikalarıyla birlikte kullanılan yazılımların zamanında güncellenmemesi nedeniyle ağ güvenliği noktasında saldırganlara açık kapı bırakılarak sistem üzerinde zafiyetler oluşmaktadır. Bunun dışında, zafiyete neden olabilecek diğer etkenler ise son kullanıcıya yönelik yapılan sosyal mühendislik saldırıları, kurumun siber güvenliğe gereken önemi vermediği için bütçe ayırmaması veya bütçesinin olmaması, uzman personel eksikliği ve saldırı altındayken uygulanacak acil durum planının olmaması şeklinde sıralanmaktadır. Yerel alan ağlarına dahil olacak bilgisayarların, bağlanacak olduğu anahtar portunda cihaz bilgilerinin ağ yöneticileri tarafından doğrulanması ve bilgi güvenliği risk yönetim prosedür ölçütlerini taşıyan bilgisayarların bağlantısına izin verilmesi gerekmektedir. Ayrıca, kurum birimlerini ve kritik sunucuları birbirlerinden mantıksal olarak ayırmak ve ağ yönetiminin daha işlevsel olması için yerel alan ağlarında mutlaka VLAN (Virtual Local Area Network- Sanal Yerel Alan Ağı) yapılandırılmasının yapılması gerekmektedir.

DoS (Denial of Service- Hizmet Engelleme) saldırısının temel amacı saldırının belli bir zaman diliminde sürekli gerçekleştirilerek hedef kaynaklarının işlevsiz hale getirilmesi sonucunda kurbanın hizmet dışı kalmasını sağlamaktır. DoS saldırıları 2003 yılından bu yana kurumları tehdit etmeye devam etmektedir. Kurumu bu saldırıdan korumak için sınır cihaz görevi gören yönlendirici üzerinde yapılacak basit ayarlar ve uzman personelin TCP/IP (Transmission Control Protocol – Taşıma Kontrol Protokolü / Internet Protocol – İnternet Protokolü) bilgisi sayesinde koruma sağlayabilmektedir. Siber uzayda tam anlamıyla güvende olmamız mümkün değildir. Buradaki güvenliğin üst seviye çıkartılması için katmanlı güvenlik ağ tasarımları üzerinde durulması ve uluslararası kabul görmüş kurumlara yönelik hazırlanan siber güvenlik sağlama adımlarının uygulanması gerekmektedir.

Kurum güvenlik duvarının doğru ve zamanında yapılandırılmaması nedeniyle siber saldırıların başarı yüzdelerinin, doğru yapılandırma ve yetişmiş insan kaynağı ile ters orantılı olduğu görülmektedir. Bu kapsamda küçük ölçekli firmaların yetersiz teknik

alt yapı, bilgi güvenliği farkındalığının düşüklüğü ve teknik bilgi eksikliğinden dolayı saldırganların hedefine girdiği görülmektedir. Yapılan araştırmaya göre siber saldırıların %58'nin küçük ölçekli firmaları hedeflediği gözlenmektedir [4].

CVE-2018-4878 (Common Vulnerabilities and Exposures- Yaygın Güvenlik Açıkları ve Eksiklikleri) zafiyetinin giderilmesi için Adobe firması tarafından 1 hafta sonra gerekli yamalar yayımlanmıştır [5]. Yaması yayımlanmadan önce geçen zaman diliminde yapılmış siber saldırılar sıfırıncı gün saldırısı olarak adlandırılmaktadır. Sıfırıncı gün saldırılarından korunmak için gelen e-postaların içeriği ve gönderenin kim olduğuna, indirilen dokümanların korumalı görünümde açılmasına, Sadece HTTP (Hyper-Text Transfer Protocol – Hiper-Metin Aktarma İletişim Kuralı) ile başlayan web sitelerine tıklanmamasına ve web adresinin yanıltıcı bir adres olup olmamasına karşı dikkat edilmesi gerekmektedir. Siber güvenlik dünyasından yaşanan gelişmeler neticesinde sıfır gün saldırılarına, oltalama ve zararlı yazılımlara, kaba kuvvet saldırılarına, hizmet saldırılarına ve APT saldırılarına karşı kurum tarafından verilen önem kadar artık son kullanıcı bilinçlenmesi de önemli hale gelmektedir. Bu riskler göz önünde bulundurulduğunda hem yerel alan ağ güvenliğinin üst seviyelere çıkartılması hem de son kullanıcı farkındalıklarındaki olumlu gelişmelerin olması sayesinde yaşanacak tehlike ve risklerin ortadan kalmasındaki önemi ortaya çıkmaktadır. Önümüzdeki yıllarda gerçekleşecek olan siber saldırıları önlemeye yönelik olarak çok sayıda siber güvenlik uzmanlarına ihtiyaç doğacaktır. US News and World dergisinin 2015 yılında yayınladığı raporda, en iyi 100 meslek grubu içinden, bilgi güvenliği analistleri sekizinci sırada yer aldığı görülmektedir. Ayrıca bilgi güvenliği alanının 2022 yılına kadar %36,5 oranında büyüyeceği ön görülmektedir [6]. Bu sonuçlar dikkate alındığında kurumsal alandaki tüm sektörler için bilgi güvenliğinin çok önemli bir konsept olacağı görülmektedir. Teknolojideki hızlı gelişmelere paralel olarak tüm kurumların bu alanda hızlı bir biçimde gelişme göstermesi gerekmektedir. Bilgi güvenliği konusunda yeterli gelişimi sağlayamayan kurumlar bulundukları sektör içindeki pazardan pay alma yarışından elenmek durumunda kalacaklardır. Sektörlerin kurumsal olarak bilgi güvenliği gereksinimlerini karşılamak için nitelikli personellere ihtiyaç duyulmaktadır. Kurum çalışanlarının kendilerini bu değişimdeki güncelliği yakalamak ve bilgi güvenliği alanında kariyer yapmak için üniversitelerin Meslek Yüksekokulu bilgi güvenliği teknolojisi

programlarını, mühendislik bölümlerini, online platformları veya siber güvenlik alanına yönelik düzenlenen konferans, eğitim ve yarışma yöntemlerini kullandıkları görülmektedir.

Kurumlar, güvenlik ve ağ cihazlarına büyük bütçeli yatırımlar yapmaktadırlar. Büyük bütçeler ile alımı sağlanan bu cihazların, ağa konumlandırılması yetmemektedir. Kurumsal yapılardaki yerel alan ağlarının ağ cihazları üzerine yapılacak siber saldırılar karşısında koruma sağlanması için kurumun bilgi teknolojileri uzmanları tarafından gerekli konfigürasyonları zamanında yapılması önemli bir problemdir. Yerel alan ağlarında kullanılan koruma yöntemlerinin, belirli aralıklarla güncel siber saldırılara karşı ne kadar direnç gösterdiği bilinmelidir. Ağ güvenliğinin sağlanması için, bilgi teknolojileri uzmanlarının önleyici bir yaklaşımla ve belirli zaman aralıklarıyla sızma testlerini yapması gerekmektedir. Bunun için, en hızlı ve düşük maliyete sahip olan yöntemlerden biri benzetim araçlarıdır. GNS3 benzetim aracı, olası saldırıların henüz gerçekleşmeden önce birbirinden farklı saldırı senaryoları kullanılarak başarıya ulaşıp ulaşamayacağı testiyle önleyici yaklaşımının kullanıldığı ve çıkan sonuçlara göre yeni bir koruma yöntemi belirlenmesine yardımcı olmaktadır. Gerçekleştirilen bu işlem, kurum ağına eklenecek yeni bir ağ cihaz alımı gerçekleşmeden önce de yapılarak kurum bütçesi anlamında olumlu katkı sağlayacağı düşünülmektedir.

Yapılan bu tez çalışmasında farklı siber saldırı senaryolarının, farklı mantıksal birimlerin olduğu, yedekli ve yük dengeli özelliklerini barındıran ağ prototipine uygulanarak elde edilen sonuçların incelenmesi ve neticesinde ağ güvenliği farkındalığı oluşturulması amaçlanmaktadır. Çalışma, toplam 5 bölümden oluşmaktadır. İkinci bölümde, ağ prototipinin hazırlanmasında kullanılan IP yönlendirme, adres çözümleme, ağ geçidi yedekliği, kapsayan ağaç, dinamik bilgisayar yapılandırma ve anahtar port birleştirme protokolleri, anahtarın çalışma prensibi, yerel ağlarda güvenlik ve saldırı tipleri açıklanmıştır. Üçüncü bölümde, yapılan çalışmaların deneysel haline gelmesine olanak oluşturacak sanallaştırma ve benzetim yazılımı anlatılmıştır. Ayrıca yerel alan ağ saldırılarının içeriğini oluşturacak temel kavramlara ve sanallaştırılan işletim sistemlerine yer verilmiştir. Dördüncü bölümde, yerel alan ağ saldırılarının her birini, benzetim ve sanallaştırma teknolojisinin yardımı ile uygulanmasına, tedbirlere, prensiplere ve geliştirilen ARP

zehirleme tespit ve koruma aracına ait bilgilerin anlatımı yapılmıştır. Son bölümde, saldırılar ile her an karşı karşıya kalınabileceğine, siber güvenlik farkındalığın davranışsal olarak içselleştirilmesini sağlanmasına ve yerel alan ağ saldırılarında karşılaşılan sonuçlara yer verilmiştir.

1. GENEL BİLGİLER

1.1. IP Yönlendirme

Yerel alan ağ haberleşmesi anahtara gelen çerçevenin hedef fiziksel adresi anahtar portlarında kayıtlı olan fiziksel adreslerden herhangi biri ile örtüştüğünde o porta anahtarlama yapılarak sağlanmaktadır. Bunun yanında, 3. katman ağ haberleşmesinde uzak veya farklı ağların devreye girmesinden dolayı yerel alan ağ haberleşmesinden farklı bir yöntemle gerçekleştirilmektedir. Yerel alan ağlar ile 3. katman ağlar arasındaki iletişimde köprü görevini ağ geçidi cihazları üstlenmektedir. Ağ geçidi cihazları kaynak adresin hedef adresten farklı olduğu haberleşmelerde önemli bir unsur olmaktadır. Yönlendiriciler, yerel alan ağlarda ağ geçidi görevini üstlenmekte ve hedef paketin en uygun rota ile uzak hedef ağa yönlendirilmesi için kullanılmaktadır.

Ethernet ara yüzleri, bulunduğu ağı bulmak için alt ağ maskesi ve IP adresini ikilik tabanda çarparak elde etmektedir. Bilgisayarda birden fazla ara yüz yer alıyorsa aynı işlemleri diğer ara yüzler için de yapmaktadır. Tüm bu bilgiler üzerine yönlendirme protokolünün elde ettiği bilgiler eklenerek yönlendirme tablosu oluşturulmaktadır. Yönlendirme tabloları hedef yönlendiriciye en uygun yoldan gitmek için kullanılacak olan rota bilgileri yer almaktadır. Ayrıca, yönlendirme tabloları farklı yerel alan ağlar arasındaki haberleşmenin gerçekleştirilmesinde kullanılmaktadır [7]. Bir paketin farklı bir yerel alan ağa gidebilmesi için yönlendirme tablosunda olması gerekenler;

- Hangi yönlendirme tekniğinin kullanıldığı,
- Hedef ağ bilgisi ve bu bilginin hangi ara yüzden öğrenildiği,
- Öncelik, mesafe ve hız birimlerini ifade eden bilgiler yer almaktadır.

Yönlendiriciler yönlendirme tablosunu, ihtiyaca göre farklılık gösteren öğrenme tekniklerinin kullanılmasıyla oluşturmaktadır. Yönlendirmenin gerçekleştirilmesinde kullanılan başlıca öğrenme teknikleri:

- Doğrudan yönlendirme.
- Sabit yönlendirme.
- Dinamik yönlendirmedir.

1.1.1. Doğrudan yönlendirme

Yönlendiricide bu öğrenme tekniğinin aktif olması için üzerinde yer alan ara yüzlerin ek yapılandırmaya gerek kalmadan yönlendirme tablosuna hedef ağ ile ilgili bilgiler eklenmektedir.

1.1.2. Sabit yönlendirme

Kurumun sınır cihaz görevi gören yönlendiricisi, bu öğrenme tekniği ile yönlendirme tablosunda bir eşleşmeye sahip olmayan ağlara bir yol sunarak internet çıkışının öğretilmesi işlemini varsayılan rota ile gerçekleştirmektedir. Bu yönlendirmede yönlendiriciler, yönlendirme kararlarını, mesafe, anlık bant genişliğine, ağ bağlantı biçimine ve ağ alt yapısına ilişkin ölçmelere dayandırmaz. Bunun yerine önceden varsayılan uzaklık ve güvenirlik değerlerinin kullanılarak hesaplanan bilgilerin yüklenmiş olduğu yönlendirici tablolarına göre yönlendirme yapmaktadırlar [7].

Bu öğrenme tekniği fazla sayıdaki farklı yerel alan ağını yönlendirmedeki zorluklarının olması, güvenirliğin ve bant genişliğini hesaba katmaması, değişen rota bilgilerini güncellemek için yönetici müdahalesi gereksinimi duyması ve olası hat kopmalarına karşı alternatif hattın tespit edememesinden dolayı yaygın bir şekilde kullanılmamaktadır. Ayrıca kurumun birden fazla ISP (Internet Service Provider-İnternet Servis Sağlayıcı)'den hizmet aldığı durumda ISP ile kurum yönlendiricisi arasında dinamik yönlendirme tekniğini tercih etmesi gerekmektedir. Fakat kurum bir adet ISP'den hizmet alıyorsa ISP ile kurum yönlendiricisi arasında doğrudan yönlendirme tekniği kullanılmaktadır.

1.1.3. Dinamik yönlendirme

Bu yöntemde, yönlendirici üzerindeki ara yüz ve en uygun rotaları belirlenmesini sağlayan yönlendirme verilerinin anlık güncellenmesinden dinamik yönlendirme protokolleri sorumludur. Uzaklık vektörü ve bağlantı durumu yönlendirme başlıca

dinamik yönlendirme protokolleridir. Dinamik yönlendirmede öğrenme işlemi otomatik olarak gerçekleşirken, sabit yönlendirme başlığı altında bahsedilen bazı temel işlemler için sabit yönlendirmenin kullanıldığı durumlarda ortaya çıkmaktadır. Dinamik yönlendirme öğrenme tekniğinin en olumlu özelliği ağ topolojisindeki değişikliklerde ve trafikte oluşacak tıkanma durumlarında uyarlayıcı yapısı sayesinde otomatik yeniden hesaplama yaparak trafiğin alternatif yol üzerinden devam etmesini sağlamasıdır [8].

Alternatif yol seçimi yönetimsel uzaklık ve metrik değerlerine göre gerçekleşmektedir. Yönetimsel uzaklık, hattın güvenirliğini ifade eder ve ağ yöneticisi tarafından değiştirilmediği sürece dinamik veya sabit yönlendirme protokolleri için varsayılan değerleri ile kullanılmaktadır. Bu değer sayısal olarak büyüdükçe o hattın güvenirliği de düşmektedir.

1.1.3.1. Uzaklık vektörü yönlendirme protokolü

Hedef ağa ulaşmak için kullanılan metrik değerinin belirlenmesindeki kriter düğümlerin geçtiği atlama noktası sayısıdır. Atlama sayısının miktarına göre hangi rotanın kullanılması gerektiğine karar verilmektedir. Bu protokolün çalışma prensibini temel alan yönlendirme protokolü genellikle atlama sayısına bakarak yönlendirme yapılmamaktadır. RIP (Routing Information Protocol- Yönlendirme Bilgisi Protokolü) ve EIGRP (Enhanced Interior Gateway Routing Protocol- Arttırılmış Dahili Ağ Geçidi Yönlendirme Algoritması) protokollerinin çalışması, uzaklık vektörü yönlendirme protokolünün çalışmasını temel almışlardır.

RIP protokolü için temel oluşturmuş olan Bellman-Ford algoritması, birçok özelliği korunarak RIP protokolüne entegre edilmiştir [9, 10]. RIP protokolünde hedef ağa ulaşmak için gereken rotanın belirlenmesinde sadece atlama sayısına bakılmaktadır.

EIGRP ve IGRP protokollerine temel oluşturmuş olan DUAL (Diffusing Update Algorithm- Genel Güncelleme Algoritması)'dır. EIGRP protokolünde, yönlendirme işleminin gerçekleştirilmesinde sadece atlama sayısına bakılmamaktadır. EIGRP'nin rota belirleme sürecinde kullandığı metrik değerleri birden fazla kriterden elde edilen sonuca göre belirlenmekte ve yönlendirme tablosu oluşturulmaktadır. Metrik

değerinin belirlenmesinde bant genişliği, gecikme, güvenilirlik, yük ve atlama sayısı parametreleri dikkate alınmaktadır [11]. Bu yöntem, uzaklık vektörü ve bağlantı durumu yönlendirme protokollerinin özelliklerini barındırmasından dolayı melez bir yapıda çalışmaktadır [12].

1.1.3.2. Bağlantı durumu yönlendirme protokolü

Bağlantı durumu yönlendirme protokolü ağ üzerinde bulunmakta olan tüm yönlendiricilerin, tüm ağ topolojisini öğrenmesine olanak sağlayan bir alt yapı sağlamaktadır. Bu yöntemde öğrenilen topolojiye göre, her yönlendirici önce en kısa yol hesaplamasını kullanarak yönlendirme tablosunu oluşturmaktadır [13]. Bu protokolde güvenirlik, referans bant genişliği ve hattın bant genişliği gibi parametrelerin etkili olmasıyla alternatif rotanın otomatik hesaplanması ve tüm marka cihazlarda çalışabilmesinden dolayı kurumlar tarafından daha çok tercih edilmektedirler. Bu yöntemde, birçok parametrenin işleme katılmasından dolayı yönlendiricilerin işlemci özelliklerinin daha güçlü olması gerekmektedir. Bu nedenle, kurumların bu protokolün kullanılması için ayırması gereken bütçe uzaklık vektör yönlendirme protokolünü çalıştıracak yönlendirici maliyetine göre daha yüksek olmaktadır. Dinamik bağlantı yönlendirme protokolü olan OSPF (Open Shortest Path First – Önce En Kısa Yolu Aç) protokolü için Dijkstra algoritması bir temel oluşturmuş ve kurum ağında yer alan tüm yönlendiricilerde aktif olarak kullanılabilmektedir [14, 15].

1.2. Adres Çözümleme Protokolü

Yerel alan ağlarında veri paketlerinin hedefe gönderilebilmesi için OSI referans modelinin ağ katmanından veri bağlantısı katmanına geçiş yapması gerekmektedir. Veri bağlantısı katmanında, MAC (Media Access Control- Medya Erişim Kontrolü) adres bilgisini kullanarak haberleşme gerçekleştirilmektedir. ARP (Address Resolution Protocol- Adres Çözümleme Protokolü) bu esnada devreye girerek ağ katmanında yer alan hedef IP bilgisine karşılık gelen MAC adresi bilgisini çift yönlü olarak bulmayı sağlamaktadır.

1.3. Anahtarın Çalışması

MAC protokolü Ethernet kartlarındaki fiziksel adresi temsil etmektedir. Anahtarlar yerel ağlardaki haberleşmeyi MAC adresi tablosundaki değerleri kullanarak gerçekleştirmektedir. MAC adres tablosunda MAC adresi ve bu adresi öğrendiği port numarası yer almaktadır. Anahtarların gelen trafiği doğru porta yönlendirebilmesi için o trafiğin gitmesi gereken MAC adresini biliyor olması gerekmektedir. MAC adres tablosunda hedef MAC adresi varsa tek nokta haberleşme gerçekleştirilmektedir. Fakat hedef MAC adresi tabloda yer almıyorsa, kendisi hariç herkese ARP isteği göndererek, hedefin MAC adresini tablosuna ekleyerek öğrenme sürecini tamamlanır. Anahtar üzerinde bulunan portta birden fazla fakat sınırlı bir sayıda MAC adres bilgisi yer alabilir. Bu kapsamda, marka çeşitliliğine göre farklılık göstermekle birlikte anahtarların hafızalarında kaydedebileceği MAC adres sayıları 16.000 – 32.768 değerleri arasında olabilmektedir.

1.4. Yerel Ağlarda Güvenlik

Güvenlik politikaları kurum yerel ağlarında güvenlik, gizlilik ve erişebilir olma ilkelerinin güvenlik yönünden seviyesinin belirlenmesini sağlayan, tüm çalışanların ve kurumun paydaşları tarafından uyması gereken kurallar bütünüdür [16]. Güvenlik politikasındaki asıl amaç değerli ve gizli dokümanların yetkisiz/kötü niyetli kişilerin eline geçmesini engellemek ve olası kötü bir durumda atılması gereken adımları önceden belirlemektir. Kurumlar tarafından uygulanmakta olan bazı temel güvenlik politikalarının içeriklerine örnek olarak;

- Görevlilerin sunucu odasına giriş politikası.
- Parola belirleme/koruma politikası.
- Son kullanıcıların hak ve sorumluluk politikası.
- Son kullanıcıları bilgi güvenliği farkındalık politikası.
- Yedekleme politikası verilebilir.

1.5. Sanal Yerel Ağ

İkinci katman cihazlarının fiziksel portlarının sanal ağlara bölünmesi ile birbirinden izole edilmiş birimlerin oluşturulması sağlamaktadır. Yerel ağların mantıksal olarak

birbirlerinden ayrılması saldırganların kurum ağında ilerlemesini ve kurumun kritik bilgilerini bulunduran sistemlere erişimini zorlaştırmayı amaçlamaktadır.

1.6. Hazır Yedekteki Yönlendirici Protokolü

HSRP (Hot Standby Router Protocol- Hazır Yedekteki Yönlendirici Protokolü) ağ geçidi görevi gören cihazın arızasına karşı koruma sağlar. Kaynak bilgisayar hedef bilgisayara ağ geçidi aracılığı ile ulaşamadığında veya farklı ağdaki DHCP (Dynamic Host Configuration Protocol- Dinamik Bilgisayar Yapılandırma Protokolü) sunucusundan IP alamadığında dinamik olarak yedekte bekleyen diğer ağ geçidi cihazının devreye girmesi için bu protokol tasarlanmıştır [17]. HSRP'nin kullanılması ile ISP tarafına bağlı 3. katman cihazın olası arızalanması durumunda yedekte bulunan diğer 3. Katman cihazın devreye girmesiyle internet bağlantısının kesintiye uğramadan devam etmesini sağlamaktadır.

1.7. Kapsayan Ağaç Protokolü

Yerel alan ağlarda olası hat problemlerine karşı otomatik olarak devreye alternatif hattın alınmasıyla zaman ve maddi kayıpların önüne geçmek hedeflenmektedir. Yedekli hattın kullanıldığı yerel alan ağlarında sonsuz döngü problemi ortaya çıkabilmektedir. Sonsuz döngü ARP genel yayın paketi ile TTL (Time to Live – Yaşam Zamanı) süresinden kaynaklanmaktadır. Sonsuz döngüyü durdurmanın tek yolu ilgili anahtar portlarını kapatmaktır. Sonsuz döngüye iki anahtar portun birbirlerine kısa devre yapılmasıyla ortaya çıkabilmektedir. Böylece son kullanıcı güvenliğinin olumsuz etkilenmesine ve yerel alan ağda genel yayın fırtınasının oluşmasına sebebiyet verilmektedir. Genel yayın fırtınası, aynı MAC adresinin birden fazla anahtar portlarına kayıt edilmesiyle meydana gelmektedir. Sonsuz döngüden korunmak için STP (Spanning Tree Protocol - Kapsayan Ağaç Protokolü) protokolünün kullanılması gerekmektedir.

Yerel alan ağlarda hem yedekli yapıda hem de anahtar portlarının kısa devre yapılmasıyla ortaya çıkacak olan sonsuz döngünün gerçekleşme ihtimalinin en aza indirilmesi ve alternatif hattın sağladığı avantajları elde etmek için yerel alan ağlarda STP protokolünün kullanılması önerilmektedir. STP protokolü 1985 yılında Radia

Perlman tarafından geliştirilmiştir. 1990'da IEEE (The Institute of Electrical and Electronics Engineers - Elektrik ve Elektronik Mühendisleri Enstitüsü), Perlman tarafından tasarlanan algoritmaya dayanarak, STP protokolü için 802.1D standardını yayınlamıştır. Bu standardın devam niteliğindeki diğer versiyonları 1998 ve 2004 yıllarında yayınlanmıştır [18, 19].

1.8. Dinamik Bilgisayar Yapılandırma Protokolü

DHCP sunucuları ağ adresi ayırma, ağ geçidi ve DNS (Domain Name Server - Alan Adı Sunucusu) gibi bilgilerin ağdaki cihazlara atanmasını gerçekleştirerek ağ yöneticisine destek aracı rolü oynamaktadır [20]. Böylece bilgi işlem personellerinin her bir son kullanıcı bilgisayarı için ayrıca IP belirleme yükünden kurtarmaktadır.

1.9. Port Birleştirme

Fiziksel birkaç anahtar portunun birleştirilmesiyle tek bir mantıksal hat oluşturarak veri aktarım hızı ve bant genişliğinin arttırılması hedeflenmektedir. Fakat bu veri aktarım hızı belirli bir noktanın üzerinde olamaz. Veri aktarım hızının belirli bir sınıra kadar yükseltilmesinin nedeni birleştirilecek fiziksel anahtar port sayısının en fazla 8 tane olabilmesidir.

1.10. Çoklu Protokol Etiket Anahtarlama

Yönlendiricilerin farklı VLAN'leri haberleşmelerini geleneksel VLAN veya tek hat yöntemini kullanılarak sağlamaktadır. Bu yöntemler VLAN sayısının fazla olduğu yerel alan ağların maliyeti, kullanılabilirliği ve hattın performansı olumsuz etkilemesinden dolayı tercih edilmemektedir.

MPLS (Multi Protocol Lable Switching - Çoklu Protokol Etiket Anahtarlama) teknoloji olarak bilenen 3. katman anahtarlama cihazı, etiket anahtarlama yöntemin kullanması ve anahtarlama sırasında donanımın da işin içine katılıyor olmasından dolayı anahtarlama kapasiteleri yönlendiricilere göre yüksek olmaktadır. Bu nedenle 3.katman anahtarlama cihazları yerel alan ağlarında hız ve güvenlik sağlamasından dolayı yaygın olarak kullanılmaktadır.

MPLS'in çalışma yapısındaki uyumluluk neticesinde 2. katman ve 3. Katman alt yapılarında yer alan teknolojilerin bir arada çalışmasını sağlamaktadır [21].

1.11. Saldırganların Güvenlik Saldırı Tipleri

1.11.1. Aktif saldırı

Bu yöntemde saldırgan aktif olarak rol oynamaktadır. Bu yöntemi kullanan saldırganın yakalanma veya tespit edilme ihtimali oldukça yüksektir. Aktif saldırı yönteminde tercih edilen saldırılar aşağıda gibi sıralanabilir [20]:

- Taklit
- Yanıt
- Mesaj içeriğini değiştirme

1.11.2. Pasif saldırı

Bu yöntemde saldırgan taraf pasif davranmakta ve çoğu zaman sadece sistemi gizlice dinlemektedir. Pasif saldırı yönteminde tercih edilen saldırılar aşağıda gibi sıralanabilir [20]:

- Mesaj içeriğinin açığa çıkartılması
- Trafik analizi

Pasif saldırı yönteminde saldırganın yakalanması aktif saldırıya göre daha zordur. Pasif saldırının belirlenebilmesi için saldırının gerçekleşebileceği sistem üzerindeki kayıtların ayrıntılı olarak incelenerek, olağan dışı durumların raporlanması gerekmektedir.

1.12. Çalışma ile İlgili Literatür Taraması

Bu tez çalışmasının konusu özelinde siber güvenlikle ilgili Türkiye ve dünyada yazılan toplam 18 adet tez ve makalelerin özetleri açıklanmıştır. Yapılan taramalar neticesinde uluslararası yayınlar incelendiğinde benzetim temelli siber güvenlik üzerine çalışmaların yapıldığı ve benzetim yazılımının önemine yer verildiği aynı zamanda siber saldırılarda benzetim ve sanallaştırmanın entegre edildiği çalışmaların yer aldığı

görülmektedir. Fakat Türkiye'de benzetim ve sanallaştırma temelli yerel alan ağlarının siber güvenlik süreçlerine ilişkin bir çalışmaya rastlanmamıştır.

Ahmet Bozgeyik, 2018 yılında yaptığı " Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi" konu başlıklı doktora tezinde Gaziantep'te yer alan 128 adet kurumun siber güvenliğe olan kurumsal yaklaşımlarının neler olduğuyla birlikte kurumların niteliklerine göre siber güvenliğe olan yaklaşımlarındaki farklılıkların bulunmasını amaçlamıştır. Büyük ölçekli kurumların siber güvenlik farkındalık düzeyleri küçük ölçekli kurumlara göre daha yüksek olduğunu belirtmiştir. Kurumun kritik birimlerinde çalışan personellerin iş değişikliğine gitme olasılığının düşük olması kurumun bilgi güvenliği zafiyetinin oluşmamasına olumlu katkı sağladığını vurgulamıştır. Ayrıca kurumun kendi yerel alan ağında barındırdığı, hem kendi personel bilgileri hem de paydaş kurumlara ait kritik bilgilerin kötü niyetli kişiler tarafından sızdırılması sonucu kurum imajına ve paydaşla olan ticari ilişkiye zarar vermekte olacağını belirtmiştir [22].

Mustafa Yasir Şentürk, 2018 yılında yaptığı "Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinde Uygulanması" konu başlıklı yüksek lisans tezinde teknolojinin hızla ilerlemesiyle bilişim suçlarını işleyen kişilerinde arttığını bu kapsamda yetişmiş personel ve doküman eksikliğini gidermek, kurumsal alt ağ yapısının saldırı yapılmadan önce sistem üzerinde yer alan zafiyetlerin önceden tespit edilerek güvenliğin sağlanması için güncel sızma testi senaryolar ile ortaya çıkan zafiyetlere karşı alınacak korumaların belirlenmesine olumlu katkı sağlaması açısından bir rehber olmasını amaçlamıştır. Siber farkındalığın kurumlarda ve toplumun tüm kesimine yayılması sağlamak için bir takım önerilerde bulunulmuştur. Ayrıca sızma testlerinin kurumlar açısından çok önemli olduğu ve yılda en az 4 kez güvenlik taraması ve yılda en az 2 kez sızma testinin yapılması gerektiğini belirtmiştir. Kurumdaki işletim sistemlerinin sanal ortam üzerinden çalışması, yerel alan ağ saldırılarını yapmaya yönelik art niyetli kurum personelinin yapacağı bir çok siber saldırının etkisiz hale geleceğini belirtmiştir [23].

Mevlüt Büyükkılıç, 2018 yılında yaptığı "Cybersecurity Framework For Small and Medium Size Enterprises" konu başlıklı yüksek lisans tezinde bilgi güvenliği farkındalığının önemi belirtilmiş fakat tek başına yeterli olmadığına yer verilmiştir.

Farkındalık çalışmalarından sonra gelen siber güvenlik uygulama çalışmaları kurum açısından önem kazandığı ifade edilmiştir. Büyük ölçekli firmalarda saldırı tespit ve önleyicilik konusunda rehberlik eden uluslararası standartların uygulanması gerektiğine değinmiştir. Fakat küçük ölçekteki firmaların kaynak yetersizliği ve burada faaliyet gösteren bilgi işlem personellerinin siber güvenlik alanındaki bilgi düzeylerinin yetersizliği nedeniyle uluslararası standartları uygulamayacaklarını vurgulamıştır. Hem kaynak problemini ortadan kaldıracak hem de bilgi işlem personelinin de kolay anlayabileceği bir siber güvenlik modelinin geliştirilmesi amaçlanmıştır [24].

Mustafa Kara, 2018 yılında yaptığı "Endüstriyel Nesnelerin İnternetinde Hızlı ve Güvenli Veri İletişimi" konu başlıklı yüksek lisans tezinde endüstriyel cihazların iletim alt yapısında yer almaya başlayan nesnelerin interneti teknolojisi ile ağda gerçekleşen işlemlerin güvenlik riskleri artmış ve bu risklerden önemli olanlardan biri olan ortadaki adam saldırısı sonucundaki sensörlerden gelen verilerdeki değişikliğin olup olmadığını tespitini sağlayan güvenli bir yazılım üretmiştir. Bir diğer amacı, saldırı sonrası sensörlerden gelecek yanlış bilgilerin engelleyerek yol açacağı sorunları ortadan kaldırmaktır. Kurulan yapıdaki farklı sensör sayıları göz önünde bulundurarak doğrulama mekanizmalarından olan MD5 (Message-Digest Algorithm 5 - Mesaj Özet Algoritması 5), SHA-1 (Secure Hashing Algorithm-1– Güvenli Özetleme Algoritması-1) ve SHA-256 yöntemleri ile ürettiği yazılım arasındaki hız performans farkları ölçülmüştür. Yapılan testler sonucunda önerilen yöntemin hem veri bütünlüğünün korunması hem de hız performans özelliği daha iyi sonuçlandığı ifade edilmiştir [25].

Bhargav Pingle, Aakif Mairaj ve Ahmad Y. Javaid, 2018 yılında yaptıkları "Real-World Man In The Middle Attack Implementation Using Open Source Tools For Instructional Use" konu başlıklı çalışmalarında siber güvenliğin WiFi ve Bluetooth gibi kablosuz ağlarda daha önemli hale geldiğini ifade etmişlerdir. Siber dünyanın bir çok saldırı karşısında savunmasız olduğunu bunlardan birinin de MITM (Man in the Middle – Ortadaki Adam) atağının olduğunu ve çalışmalarında açık kaynak OS (Operating System – İşletim Sistemi) olan Kali Linux'te ettercap aracını kullanarak gerçekleştirilen atakları incelemişlerdir. Ayrıca son kullanıcıların saldırganlar tarafından çok tercih edilen siber saldırılara karşı kendilerini korumaları ve

farkındalıklarının yüksek olması gerektiği vurgulanmıştır. Farkındalığın artması için önerilerde bulunmuşlardır [26].

Parinya Ekparinya, Vincent Gramoli ve Guillaume, 2018 yılında yaptıkları "Impact of Man-In-The-Middle Attack on Ethereum" konu başlıklı çalışmalarında herkese açık blok zinciri ile kurumsal özelliği barındıran ethereum yazılımının hem güvenlik açıklıklarını hem de önemli özelliklerini listelemişlerdir. Kurumsal ethereum yöntemine BGP protokolünün açıklarının kötüye kullanarak yapılan saldırıda elde edilen başarı ile herkese açık ethereum'a yapılan ARP sahtekarlığı saldırısında elde edilen başarı aynı olduğu sonucuna varmışlardır [27].

Ertuğrul Başaranoğlu, 2017 yılında yaptığı "Kurumsal Ağlardaki Windows Ortamlarına Saldırılar ve Sıkılaştırma Yöntemleri" konu başlıklı yüksek lisans tezinde etki alanı, yerel alan ağının merkezinde yer alması ve yönetiminde aktif rol oynaması gibi nedenlerden dolayı kötü niyetli kişilerin hedefine gireceğinin vurgusu yapılmıştır. Sızma testi içinde yer alan etki alanı sızma testleri için özel hazırlanan Microsoft etki alanı sızma testi metodoloji ile diğer metodolojiler arasındaki farkları incelemiştir. Yazarın sunduğu metodolojide etki alanına yönelik yapılacak saldıra karşı hangi savunma tekniklerinin kullanılması gerektiğini benzetim senaryoları ile göstermiştir [28].

Kemal Hajdarevic, Adna Kozic, Indira Avdagic, Zerina Masetic ve Nejdet Dogru 2017 yılında yaptıkları "Training Network Managers in Ethical Hacking Techniques to Manage Resource Starvation Attacks using GNS3 Simulator" konu başlıklı çalışmada tecrübeli çalışanların ağ yönetimi, siber saldırılar gerçekleşmeden önce proaktif eylemleri gerçekleştirdiklerini vurgulamışlardır. Yerel alan ağdaki sistem güvenliğini sıkılaştırmadan sorumlu yöneticilerin ve öğrencilerin deneyim kazanmaları için test becerilerini geliştirmelerini sağlayacak simülasyon temelli bir eğitim senaryosu hazırlamışlardır. Bu eğitim senaryosu ile DDOS (Distributed Denial of Service - Dağıtık Hizmet Engelleme) saldırısının etkilerini ve belirtilerini tecrübe etmeleri ve olası gerçek saldırılara hazırlıklı olunmasını amaçlamışlardır. Ayrıca beyaz şapkalı siber güvenlik uzmanlarının öğrenme deneyimlerine değer katmak ve hazırladıkları gerçek saldırı senaryoların yer aldığı dokümanlardan öğrenmeleri sayesinde tecrübelerinin artacağını belirtmişlerdir [29].

Rajneet Kaur Bijral, Alka Gupta ve Lalit Sen Sharma, 2017 yılında yaptıkları "Study of Vulnerabilities of ARP Spoofing and its Detection Using Snort" konu başlıklı çalışmalarında kurumlar, bilgilerin yetkisiz kişilerin eline geçmemesi için bütçenin önemli bir kısmını güvenlik için ayrılması gerektiğini ve saldırganlar ağa sızıp yetkisiz erişime sahip olmak için ağ uygulamalarının güvenlik açıklarından yararlanılarak yapıldığını vurgulamışlardır. Bu güvenlik açıkları, zayıf uygulama kodu veya tasarım nedeniyle ortaya çıkmaktadır. Bu çalışmada, ARP Zehirleme gibi bir tür tasarım düzeyinde güvenlik açığı tartışıyor olacağız. ARP Zehirleme saldırısını temel alarak Tarayıcı İstismarı ve Oturum Çalma saldırıları kullanılmıştır. Yerel alan ağlarına yapılan saldırıların tespitinde kullanılan ve açık kaynak kodlu Snort ile ARP Zehirleme tespit etmek için kullanmışlardır. Snort yazılımı, ağa giren saldırganın MAC adresini tespitini yapar ve bu MAC adresi tarafından paket gelmesini engellendiğini vurgulamışlardır. Ayrıca Snort yazılımının, yerel alan ağdaki cihaz sayısındaki artıştan etkilenmeyerek saldırı tespit edebildiği sonucuna varmışlardır [30].

Jabrayil Alizada 2016 yılında yaptığı "Kablosuz Yerel Alan Ağlarında Güvenlik ve Saldırı Yöntemleri Yüksek Güvenlikli Kablosuz Yerel Alan Ağının Tasarımı" konu başlıklı yüksek lisans tezinde farklı çalışma birimlerinin yer aldığı 5 katlı bir kurumun kablosuz yerel alan ağa gerçekleşme ihtimali olan siber saldırılara karşı güncel güvenlik konfigürasyonlarının ve ağ cihazlarının haberleşmesi için gerekli komutlarının yer aldığı bir ağın tasarımını Huawei firması tarafından geliştirilen eNSP (Enterprise Network Simulation Platform – Kurumsal Ağ Simülasyonu Platformu) V1.2.00.380 sürümü olan ağ benzetim programı aracılığı ile oluşturmuştur. Kullanılan benzetim aracının ücretsiz olması, simülasyon desteğine yer vermemesi ve sanal olarak kullanılması nedeniyle günümüz teknolojilere göre bazı eksikliklerin olabileceğini ifade etmiştir. Ağın tasarımında kullanılan benzetim yazılımın en önemli eksikliği AC ve FW cihazlarının komut satırı ile yönetmede bazı problemler ile karşılaşıldığı vurgulanmıştır [31].

R.Mohtasin, P.W.C. Prasad, Abeer Alsadoon, G.Zajko, A. Elchouecmi ve Ashutosh Kumar Singh, 2016 yılında yaptıkları "Development of a Virtualized Networking Lab Using GNS3 and VMware Workstation" konu başlıklı çalışmalarında bilgisayar ağları eğitiminin yapıldığı laboratuvar ve sınıflarda verimli bir öğrenme ortamı

sağlayamadıklarını bu nedenle bilgisayar ağları eğitiminin GNS3 benzetim programı üzerinden eğitim alan üniversite öğrencilerine gerçek ağ ekipmanları üzerinde uygulama yapma fırsatı sunduğunu ifade etmişlerdir. GNS3 ile diğer ağ benzetim yazılımları arasındaki avantaj ve dezavantaj durumları ile çalışma farklılıklarını vurgulamışlardır. Çalışmalarının amacı sanal laboratuvar yaratmak olduğunu ve öğrencilere bu yöntem ile gerçek ağ teknolojilerine ulaşabilme fırsatını sağlamak olduğunu ortaya koymuşlardır. GNS3 benzetim programı bir adet fiziksel bilgisayar ile çalışacağı için ucuz ve ulaşılabilirliğinin kolay olduğunu ifade etmişlerdir [32].

Matej Plch, 2015 yılında yaptığı "Practical Man-in-the-Middle Attacks in Computer Networks" konu başlıklı lisans tezinde MITM saldırısı, halka açık kablosuz ağları kullanan kullanıcıların gizliliği için gerçek bir tehdit oluşturacağı ve saldırgan tarafından işletilen kablosuz erişim noktalarının riskleri vurgulanmıştır. MITM saldırısı için sahte AP'lerin kullanım yöntemleri, sahte AP (Access Point – Erişim Noktası) oluşturmak için gereksinimlerin neler olduğunu, saldırılara karşı alınması gereken tedbirleri ve kurbanların bu sahte ağa bağlanmaya nasıl ikna edilebileceğini açıklamıştır. Saldırgan, kurbanın SSL/TLS (Transport Layer Security – Aktarım Katmanı Güvenliği) korumalı iletişimini tehlikeye atmak için hem saldırı hem de savunmada kullanılan yazılım araçları hakkında bilgiler vermiştir. HTTPS'in güvenlik testi yapılmıştır. Ayrıca HSTS (Hypertext Strict Transport Security – Sıkı Metin Taşıma Güvenliği) teknolojisinin kullanılması sayesinde internet tarayıcılarının güvenliğinde iyileştirmeler olduğu vurgulanmıştır. Sahte SSL sertifikaların güvenlik anlamında problem yaşattığını somut örnek olay olan Lenova dizüstü bilgisayarlarında yüklü gelen Superfish yazılımı üzerinden açıklamalarda bulunmuştur. Uygulamalı bölümde ise saldırı araçlarının başarısı ve etkisi değerlendirilmiştir [33].

Mustafa Meral, 2015 yılında yaptığı " Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi" konu başlıklı yüksek lisans tezinde siber saldırılar arasında SCADA (Supervisory Control And Data Acquisition - Uzaktan Kontrol ve Gözleme Sistemi) sistemleri saldırganların öncelikli hedefleri olduğunu belirtmiştir. Kritik altyapıların siber güvenliğini koordine edebilecek merkezi bir otoritenin eksikliği vurgulanmıştır. Bu kapsamdaki korunmaya yönelik olumlu katkı sağlayacak olan farkındalık çalışmalarına, Türkiye ve Dünya'da yaşanan siber saldırılara ve iyi

örneklerin incelenmesine yer vermiştir. Kritik altyapıların siber saldırılar karşısında korumasız kalması durumunda, ulusal güvenlik ve kamu düzeninin engellenmesine vurgu yaparak ve kritik altyapıların dahil olduğu sınıftan daha önemli ve kapsamlı olması gerektiğini ifade etmiştir [34].

Prema Arote, Karam Veer Arya, 2015 yılında yaptıkları "Detection and Prevention Against ARP Poisoning Attack Using Modified ICMP and Voting" konu başlıklı çalışmalarında ARP zehirlenmesi için önemli nokta olan LAN (Local Area Network – Yerel Alan Ağ)'da MITM ve DOS atakları konularını işlemişlerdir. Çalışmada önerilen tespit mekanizmasında başlangıçta ağ üzerindeki trafik CS (Central Server – Merkezi Sunucu) tarafından kesileceği ve sonrasında CS tuzak ICMP (Internet Control Message Protocol - İnternet Kontrol Mesaj Protokolü) ping paketini göndereceği, geri gelen ICMP'nin cevabının analiz edilerek ve saldırganın başarılı bir şekilde tespit edileceği ifade edilmektedir [35].

Nikhil Tripathi ve BM Mehtre, 2014 yılında yaptıkları "Analysis of Various ARP Posoning Mitigation Techniques: A Comparison" konu başlıklı çalışmada ARP, bilgisayar iletişimi ile ilgili temel ve en sık kullanılan protokollerden biridir. LAN içinde, ARP Mesajları IP adreslerine karşılık gelen MAC adreslerini çözümlemek için kullanıldığı ve bu protokoldeki bazı sınırlamaları nedeniyle savunmasız kalacağı ifadesine yer vermişlerdir. ARP'ın en belirgin iki önemli sınırlamaları kimlik doğrulama yöntemi kullanmaması ve durumsuz tablo tutmasıdır. ARP zehirlenmesi, temel saldırıların en başında gelir ve daha yüksek seviyeli saldırıları başlatmak için kullanıldığını belirtmişlerdir. Literatürde, bunları tespit etmek ve önlemek için birkaç çözüm önerilmiştir. Ancak, önerilen çözümlerin tümü bir dereceye kadar sınırlıdır. Bazı çözümler özel senaryolarda etkiliyken, diğerleri farklı bir gruba hitap eden senaryolar için uygundur. ARP zehirlenmesinin yeni teknikleri zaman içinde geliştikçe, araştırmacılar yeni çözümler önereceği bilgisini vurgulamışlardır. Bu çalışmada, literatürde oldukça popüler olan önerilen farklı çözümlerin karşılaştırmalı bir analizini yapmışlardır. Önerilen çözümlere sınırlama olarak kabul edilen bazı önemli faktörlere dayanarak farklı azaltma tekniklerini karşılaştırılmışlardır. Farklı tablolar arasında karşılaştırmaya hızlı bir genel bakış sunan kısa tablo formatı da sunulmuştur. Bu karşılaştırmalı çalışma, bir yandan, farklı etki azaltma tekniklerinin

birleşik avantajlarından yararlanan ve diğer yandan eski kısıtlamaları taşımayan daha verimli ve etkili bir şema sunmak ve oluşturmak için kullanılacağı bilgisine yer vermişlerdir [36].

Muhammed Alparslan Akyıldız, 2013 yılında yaptığı "Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi" konu başlıklı yüksek lisans tezinde kurum ağ tasarımlarına yapılma ihtimali olan siber saldırıların ortaya çıkaracağı kötü sonuçları ortadan kaldırmak için sızma testinin önemi vurgulanmış ve senaryolar geliştirilmiştir. Siber güvenlik alanındaki milli yazılımların önemini vurgulamıştır. Bunun için eğitim içeriklerinin yeniden gözden geçirilerek uygulama ağırlıklı olması, siber güvenlik derslerinin ilköğretimde yer alması ve olası büyük siber saldırılara karşı afet durum planı çıkartılarak farklı senaryolar ile benzetim ortamında değerlendirilmesi gerektiğini ifade etmiştir [37].

Gopi Nath Nayak ve Shefalika Ghosh Samaddar, 2010 yılında yaptıkları "Different Flavours of Man in the Middle Attack, Consequences and Feasible Solutions" konu başlıklı çalışmada MITM saldırısı, bilişim suçluları tarafından kullanılan temel tekniklerden biridir. MITM saldırısı ile DoS, DNS sahtekarlığı ve port çalma gibi saldırıları başarılı bir şekilde başlatabileceğini ifade etmişlerdir. MITM saldırısı, LAN ortamında, özellikle de ARP zehirlenmesiyle gerçekleştiği yerlerde daha müsait olduğu vurgulamışlardır. Her türden MITM saldırısı, çevrimiçi hesap kullanıcı kimliği, parola, yerel FTP (File Transfer Protocol – Dosya Transfer Protokolü) kimliğinin çalınması, SSH (Secure SHELL Güvenli Kabuk) veya telnet oturumu elde etme gibi durumları incelemişlerdir. ARP sahtekarlığı ve bir LAN ortamındaki etkisi, belirtilen amaca ulaşmak için detaylı olarak incelenmiş alternatif çözüm önerilerinde bulunmuşlardır [38].

Zouheir Trabelsi ve Khaled Shuaib, 2006 yılında yaptıkları "Man in the Middle Intrusion Detection" konu başlıklı çalışmada LAN güvenliği, ağ yöneticilerinin uzman olması gereken kritik ve zorunlu bir unsur olduğunun altını çizmişlerdir. Ağ güvenliğinin, ağı dış saldırılara ve izinsiz girişlere karşı koruduğu düşünüldüğünü ancak, iç saldırılar da dış saldırılar kadar zararlı olabileceğini belirtmişlerdir. Ağ iletişiminde iyi bilinen saldırılardan biri, farklı ağ katmanlarında paket aldatma saldırısıdır. Bu çalışmada, sahte ARP paketlerinin kötü niyetli kullanıcılar tarafından,

kullanıcıların ana bilgisayarlarına yönelik bir saldırı başlatmak için ağ trafiğini yönlendirmenin nasıl kullanacağını ele almışlardır. Trafik yönlendirme saldırılarının tespitinde mevcut IDS sınırlamaları da tartışılmaktadır [39].

2. KULLANILAN TEKNOLOJİLER

2.1. Çalışmada Kullanılan Yazılımlar

Bu çalışmada yerel alan ağı saldırılarında en çok tercih edilen açık kaynak yazılımlarından Kali Linux OS ve GNS3 ağ benzetimi ile VMware yazılımı kullanılmıştır.

2.1.1. GNS3 ağ benzetim aracı

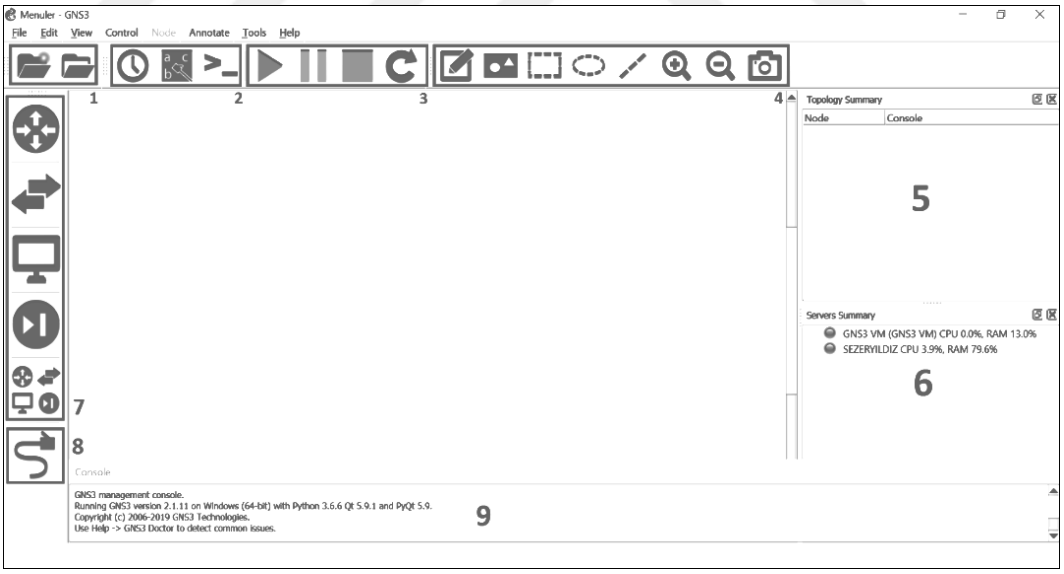
Yerel alan veya geniş alan ağlarının ağ konfigürasyonlarında ve siber güvenlik uygulamalarında tercih edilen açık kaynak kodlu ağ benzetim aracıdır [40]. GNS3 ağ benzetim aracında, marka bağımsız gerçek IOS (Internetwork Operating System – Ağ İşletim Sistemi) barındıran ağ cihazının çalışmasını, komut satırı ile işlem yapan VPCS (Virtual Personal Computer Simulator – Sanal Bilgisayar Simülatörü) bileşenini ve VMware sanal işletim sistemlerini bir arada çalıştırabilmektedir. Bu ağ benzetim aracı ile düşük bütçeli fakat büyük ölçekli ağ prototiplerinin hazırlanması, kurumun siber varlıklarından biri olan ağ güvenliğinin siber güvenlik yönünden incelenmesi veya ağ performans ölçümleri gerçekleştirilebilmektedir. Benzetim yazılımı ile ağın testi yapılarak ağ tasarımları ile ortaya çıkabilecek krizler engellenebilmekte veya yönetilmesine katkı sağlamaktadır. Ağ benzetim teknolojisinin gelişmesinin nedenleri aşağıdaki gibi sıralanabilir:

- Ağ cihazlarının sayısının artmasıyla kurum bütçesinin olumsuz etkilenmesi,
- Ağ tasarımı değişikliğinin gerekmesi,
- Karmaşık ağlarda hata kontrolü ve performans testlerinin öneminin artması,
- Yerel alan ağda alınan güvenlik önlemleri zaman içerisinde değişiklik göstermesi,
- Ağ cihazlarının yapılandırma ayarlarındaki güncelleme ihtiyaçlarıdır.

GNS3 ağ benzetim aracının kullanıcı ara yüzü Şekil 2.1'de gösterilmektedir. Şekil 2.1'deki GNS3 ağ benzetim ara yüzünün kullanılmasına ait açıklamaların yapılması

için şekil üzerinde numaralandırılmış parçaların açıklaması aşağıda sırası ile yer almaktadır.

- 1 numaralı yerden yeni bir proje veya daha eski yapılmış proje yüklenebilmektedir.
- 2 numaralı yerden o andaki ayarların kaydedilmesini, topoloji alanındaki tüm cihazlara bağlantı yapılabilmesini veya port etiketlerinin gösterimi/gizlenmesi işlevini yerine getirmektedir.
- 3 numaralı yerden ağ cihazlarının çalışmasını, dondurulmasını, durdurulmasını veya topoloji alanındaki tüm cihazların yeniden başlatılmasını sağlamaktadır.
- 4 numaralı yerden çizim araçlarına ulaşılmaktadır.
- 5 numaralı yerde cihazların açık/kapalı ve portların nereye bağlantı yaptığı bilgileri yer almaktadır.
- 6 numaralı yerde sunucuların listesi yer almaktadır.
- 7 numaralı yerden topoloji alanını eklenebilecek aygıtların listesine erişilmektedir.
- 8 numaralı yerden ağ cihazlarını birbirine bağlayan araca ulaşılmaktadır.
- 9 numaralı yerde cihazlarda oluşacak hata bilgileri yer almaktadır.



Şekil 2.1. GNS3 ağ benzetim yazılımının kullanıcı ara yüzü

2.1.2. VMware

Sanallaştırma, mevcut fiziksel makineyi mantıksal bölümlere ayırarak birden fazla makine olarak kullanılmasını sağlayan, işlemci performansını daha verimli hale getiren, sanal sistem üzerinde kullanılan yazılımların fiziksel makine bağımlılığını

azaltarak fiziksel ve sanal makinede çalışan programların güvenli kalmasını sağlayan ve harici problemler ile karşılaşılmasını en aza indiren bir yöntemdir [41].

2.1.3. Kali linux

Kali Linux işletim sistemi, sızma testi çalışmaları için geliştirilmiş bir açık kaynak yazılımıdır. İçerisinde farklı türde çeşitli sızma testlerini içeren gerekli uygulamaları barındırmaktadır [42].

2.1.4. Metasploit framework

Metasploit, sızma testlerinde kullanılmak için geliştirilmiş içinde auxiliary, payload, post exploit ve exploit modüllerini içeren ve ruby programlama dili ile geliştirilmiş bir güvenlik yazılımıdır. Bu yazılım; 1825 adet exploits, 1033 adet auxilary, 318 adet post, 541 adet payloads, 44 adet encoders ve 10 adet nops özelliklerini barındırmaktadır. Bu özellik sayıları, yeni zafiyetlerin tespiti, zafiyetlerin sömürülmesi veya eklenti yapılması durumunda gerekli araçların yüklenmesi ile değişebilmektedir.

2.2. MAC Güvenliği

MAC güvenliği 2. katman ağlar için büyük bir önem arz etmektedir. Kötü niyetli kişilerin ciddi teknik bilgiye ihtiyaç duymadan ağın trafiğini askıya uğratmak ve mevcut verileri çalmak için bu güvenliğin aşılması teknikleri kullanılmaktadır. CAM (Content Addressable Memory- İçerik Adreslenebilir Bellek) tablosunun içeriği, anahtar portlarında kayıtlı olan MAC adreslerinden oluşmaktadır. İkinci katman haberleşmenin güvenliği sahte MAC bilgilerinin CAM tablosuna eklenmesi ile riske girmektedir. Böylece anahtarın bir göbek gibi çalışmaya başlamasıyla hem yerel alan ağ güvenliği hem de ağ performansı olumsuz etkilenmesiyle sonuçlanmaktadır [43].

2.3. DHCP Güvenliği

Genel veya özel ağ trafiğinde haberleşmenin temelini oluşturan IP, alt ağ maskesi, ağ geçidi ve DNS bilgileri ağdaki bilgisayarın talep etmesi ile DHCP servisi tarafından gönderilmektedir [44]. DHCP sunucusu DHCP keşif paketinin içinde yer alan MAC adres bilgisine göre IP eşleştirmesi ve rezerve işlemini gerçekleştirmektedir. DHCP sunucusunun rezerve edeceği IP adres sayısı ilgili ağda kullanılan alt ağ maskesine

bağlı olup sınırlı sayıda olmaktadır. Ayrıca DHCP sunucusu bu süreçte kullanılan paketler için kimlik doğrulamasını yapmamaktadır. Kimlik doğrulamadaki eksiklik DHCP protokolünde güvenlik açıklığına neden olmaktadır.

2.4. Ağ Geçidi Güvenliği

Bilgisayarlar MAC adres bilgisini hem yerel alan ağdaki haberleşmelerinde hem de kaynağın bulunduğu ağdan farklı bir ağa erişilmesi istenmesi durumunda ağ geçidine ulaşmak için kullanmaktadırlar. Bunun nedeni, hedef ağa gidilecek rotayı sadece ağ geçidi cihazının bilmesidir. Bilgisayar, ağ geçidinin IP bilgisini DHCP sunucusundan öğrendikten sonra bu öğrendiği IP adresine karşılık gelen MAC adresi öğrenme süreci başlamaktadır. Öğrenme süreci tamamlandıktan sonra ARP tablosuna ilgili MAC bilgisi eklenmektedir. ARP mekanizması içinde kimlik doğrulama olmadığı için kötü niyetli birinin kurbanın ARP tablosunu yaygın kullanılan araçlar yardımıyla değiştirmesi mümkün olmaktadır. Bu süreçte ağ geçidi güvenliği alınmadığı taktirde kurbandan hedefe giden tüm paketlerin bir kopyasının saldırgana gitmesinden dolayı bilgi güvenliği zafiyeti ortaya çıkacaktır.

2.5. Son Kullanıcı Güvenliği

ARP ve DHCP protokollerine yönelik gerekli güvenlik önlemleri alınmadığı durumlarda yerel alan ağlarında bazı güvenlik açıklıkları meydana gelmektedir. Bunların yanı sıra, MITM saldırı temelli olan çoklu ve genel yayın adreslerini kullanan popüler protokollerin bazıları arasında NetBIOS (Network Basic Input/Output System (Ağ Temel Giriş/Çıkış Sistemi), NBT-NS (NetBIOS Name Service – NetBIOS İsim Servisi), LLMNR (Link Local Multicast Name Resolution- Yerel Bağlantı Çoklu İsimi Çözümlemesi) ve mDNS (Multicast Domain Name Server – Çoklu Alan Adı Sistemi) bulunmaktadır. NBT-NS, LLMNR ve mDNS, bir ağ içindeki kaynakların isim çözümlemesi yapmak için kullanılan protokollerdir. Bu protokoller DNS protokolünün isim çözümlemesi başarısız olduğunda otomatik olarak devreye girer ve isim çözümleme işini gerçekleştirirler. NBT-NS ve LLMNR, Windows işletim sisteminde, mDNS ise Macintosh işletim sisteminde kullanılmaktadır. NBT-NS, UDP genel yayınını kullanırken LLMNR ve mDNS, UDP çoklu gönderim yayınını kullanmaktadır. UDP mesajlarının kopyalanmasının kolay olması ve saldırgan

tarafından veri iletim trafiğine kolayca müdahale edebilmesinden dolayı son kullanıcının oturum güvenliği riske girmektedir. Bu protokolleri kullanan popüler saldırılar ise MITM çalışma prensibine benzer SMB (Server Message Block – Sunucu İleti Bloğu) geçişi saldırılarıdır [45].

3. DENEYSEL ÇALIŞMA

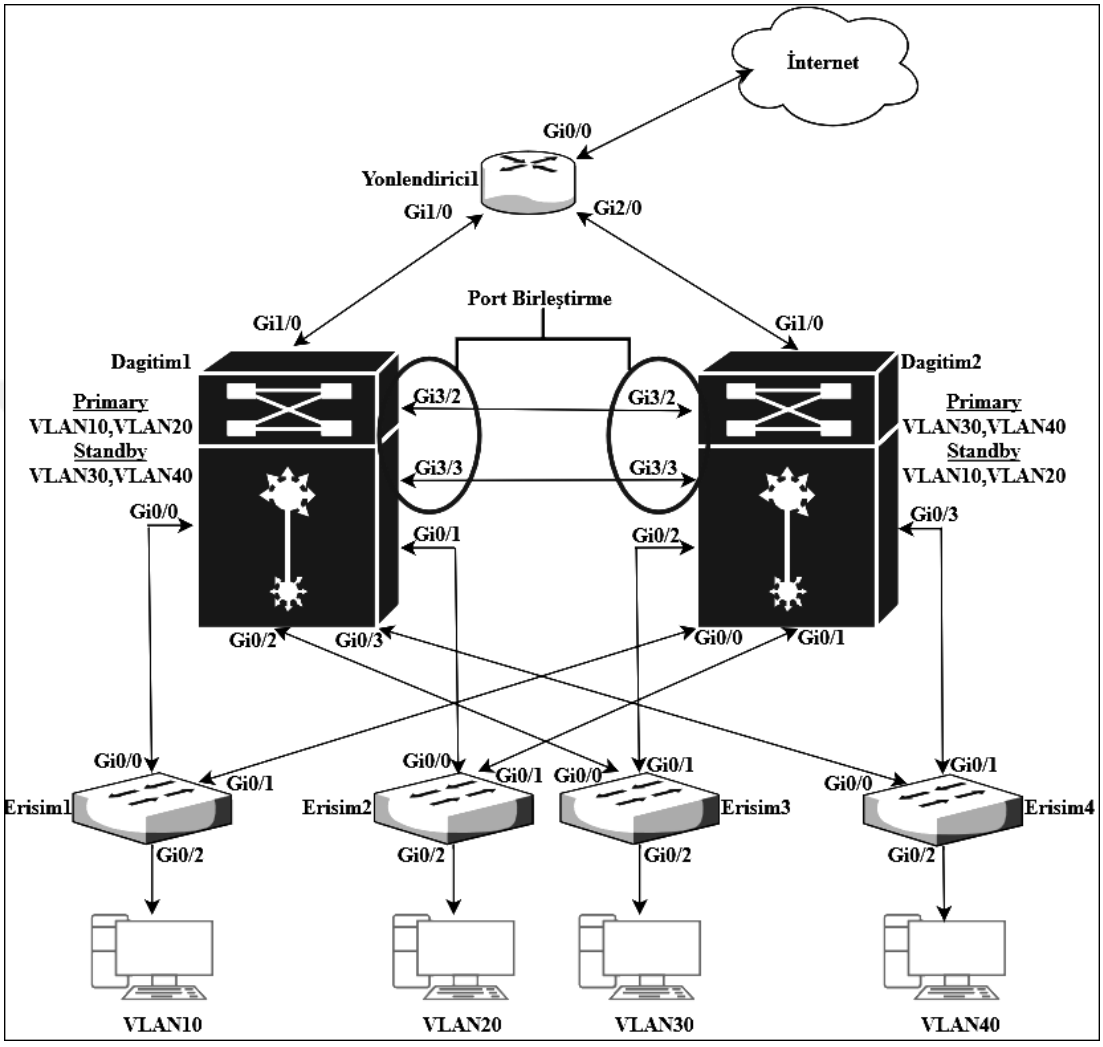
3.1. Çalışmanın Ağ Tasarımı

Bu çalışmada yerel alan ağlarındaki atakların test edilebilmesi için sanal hacking laboratuvarı kurulmuştur. Bu laboratuvar, GNS3 benzetim yazılımı ve Vmware sanallaştırma içinde yer alan Kali Linux, Windows 10 ve Windows 7 bileşenlerinin de yer aldığı ekipmanlar yardımı ile bir ağ prototipi oluşturarak gerçekleştirilmiştir. Ağ prototipi içinde yer alan bileşenler aşağıda maddeler haline sıralanmaktadır:

- 1 adet yönlendirici
- 2 adet 3. katman anahtar
- 4 adet 2. katman anahtar
- 4 adet GNS3 ile entegre edilmiş VMware üzerinde çalışan sanal bilgisayar

GNS3 benzetim yazılımı aracı ile birlikte kullanılabilen GNS3 VM (Virtual Machine – Sanal Makine) aracının yüklenmesi sağlanarak benzetim aracının içinde kullanabilecek cihazların çalışacağı ikinci bir sunucu görevi gören sanal bir sunucu sisteme eklenmektedir. Böylece hem fiziksel bilgisayarın işlemci ve RAM (Random Access Memory – Rastgele Erişilebilir Bellek) yüklerinin bir kısmı sanal sunucuya aktarılarak verim elde edilmiş hem de NAT (Network Address Translation – Ağ Adres Çeviricisi) işlemi gerçekleştirilerek yerel alan ağındaki sanal bilgisayarların yönlendirici cihazı üzerinden internete çıkması sağlanmıştır. VLAN, kurum ağında yer alan birimler için mantıksal bölümlerin yer aldığı sanal ağlar oluşturmaktadır. Böylece kurum ağının yönetimi kolay hale gelmesi hem de genel yayın adresi aracılığı ile yerel alan ağı tehdit edecek siber saldırı riskini azaltılması amaçlanmaktadır. Ağ geçidi yedekliliği için HSRP protokolü tercih edilmiştir. HSRP protokolü ile hangi VLAN'lerin aktif (primary) hangisi beklemede (standby) olduğunu ayarlama imkanı sağlamaktadır. Böylece hem ağ geçidi yedekliliği hem de yük dengeleme sağlanması amaçlanmaktadır.

Şekil 3.1'de GNS3 benzetim aracı üzerinde hazırlanan ağ prototipi yer almaktadır. Kali ve kurban makinelerinin yerleri her atakta değişkenlik göstermesinden dolayı şekle eklenmemiştir.



Şekil 3.1. VMware ve GNS3 entegrasyonu ile yapılan ağ prototipi

3.1.1. Ağ cihazlarının işlevleri

Şekil 3.1'de kullanılan ağ prototipi üzerinde kullanılan yönlendirici, dağıtım anahtarları ve erişim anahtarlarının işlevleri ve konfigürasyonları kısaca özetlenmektedir. Yönlendirici cihazı üzerinde tanımlanan konfigürasyonlar ve işlevleri aşağıdaki gibidir:

- Sanal işletim sistemlerinin internete çıkması için NAT, ACL (Access Control List – Erişim Kontrol Listesi) ve varsayılan rota yapılandırması,

- Dinamik yönlendirme için OSPF yapılandırmasıdır.

Dağıtım anahtarları üzerinde tanımlanan konfigürasyonlar ve işlevleri aşağıdaki gibidir:

- Tanımlanan her birim için VLAN'ların oluşturulması,
- Farklı VLAN'lerdeki birimlerin haberleşmesi için SVI (Switch Virtual Interface – Anahtar Sanal Ara yüzü) için IP yapılandırması,
- VTP (Virtual Trunking Protocol – Sanal Yerel Ağ Aktarım Protokolü) sunucu görevi.
- Yedekli DHCP sunucusunun oluşturulması,
- Yedekli ağ geçidinin oluşturulması,
- Darboğazı engellemek için kullanılan port birleştirme yapılandırmasının gerçekleştirilmesi,
- Dinamik yönlendirme işlevi için OSPF yapılandırmasının yapılması,
- VLAN'ler için STP yapılandırmasıdır.

Erişim anahtarları üzerinde tanımlanan konfigürasyonlar ve işlemler aşağıdaki gibidir:

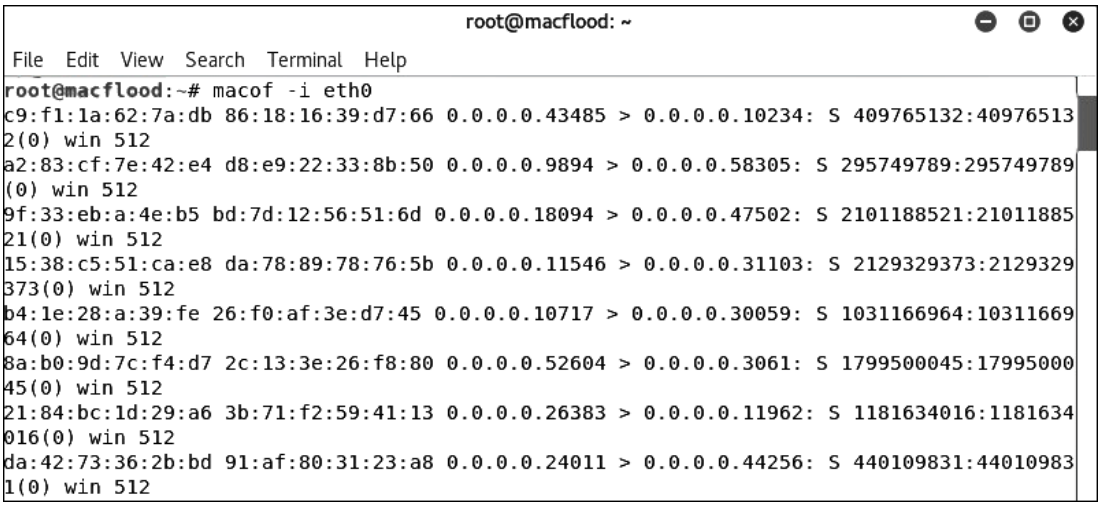
- VTP istemci görevinin tanımlanması,
- Mantıksal olarak bölünmesi için portlar üzerinde VLAN ataması işleminin gerçekleştirilmesidir.

3.2. Tasarlanan Ağ Üzerinde Gerçekleştirilen Yerel Ağ Atakları

3.2.1. MAC taşma atağı

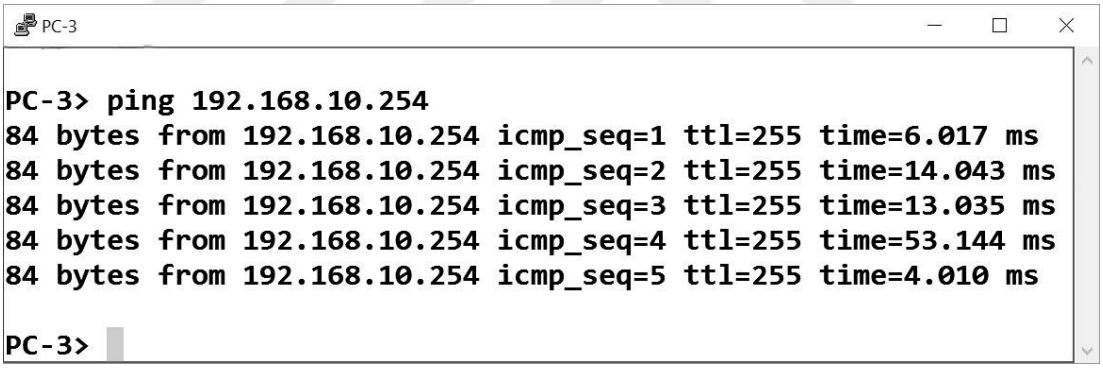
3.2.1.1. MAC taşma saldırısının başlatılması

Bu saldırı iki farklı senaryo gerçekleştirilerek değerlendirilmiştir. İlk senaryoda, saldırgan bilgisayarı tarafından VLAN 10'a üye olan porta bağlantı sağlanmakta ve ilgili VLAN üzerinden saldırı gerçekleştirilmektedir. Saldırı gerçeklemesinde test aracı olarak macof test aracı kullanılmıştır. Şekil 3.2'de macof test aracının kullanımı ve saldırı anındaki bilgiler görüntülenmektedir.

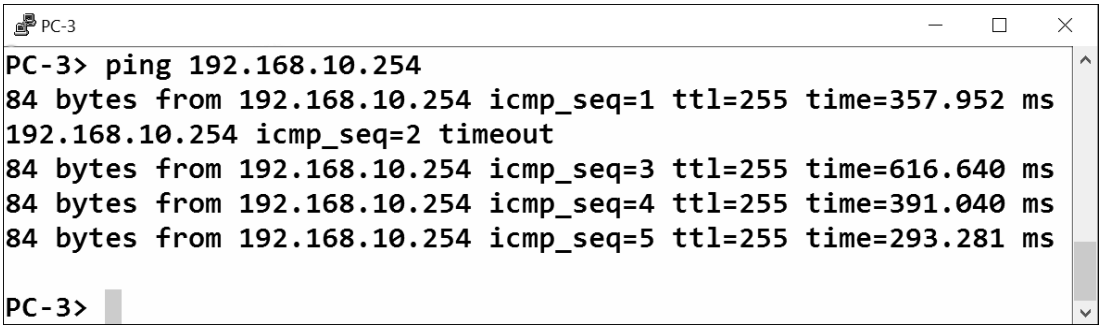


Şekil 3.2. Test aracının anlık görüntüsü

Saldırı öncesinde VLAN 30'a üye olan bilgisayardan VLAN 10'un sanal IP adresine Şekil 3.3'te görüldüğü gibi ping paketleri gönderilmiştir. Saldırı aşamasında ise aynı noktalar arasında tekrar ping paketi gönderilmiş ve çıkan sonuçlar Şekil 3.4'de gösterilmektedir.



Şekil 3.3. Saldırı öncesi ping paket durumu



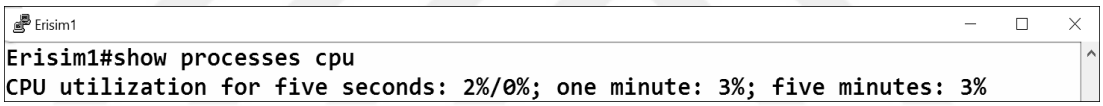
Şekil 3.4. Saldırı aşaması ping paket durumu

Saldırı esnasında yerel alan ağ trafiğinde paket gecikmelerinin ve kayıplarının yaşandığı Şekil 3.4'de görülmektedir. Bu yapıda, kurgulanan ağ prototipi üzerinde yer alan yönlendirici hariç diğer ağ cihazlarının MAC tabloları sahte MAC bilgileri ile dolmaktadır.

İkinci senaryoda, aynı yöntemler kullanılarak yapılan saldırılar yerli VLAN (VLAN 1)'a üye olan porta bağlanarak gerçekleştirilmiştir. Saldırgan kurum ağı ile hiç ilgisi olmayan bir VLAN'a dahil edildiği için DHCP'den IP alamamıştır. Fakat bu saldırı tipi ile 2. katman ağı etkilenmekte ve IP adresine gereksinim olmadığı için dahil olduğu anahtar portuna MAC taşma saldırısı başarıyla tamamlandığı görülmektedir.

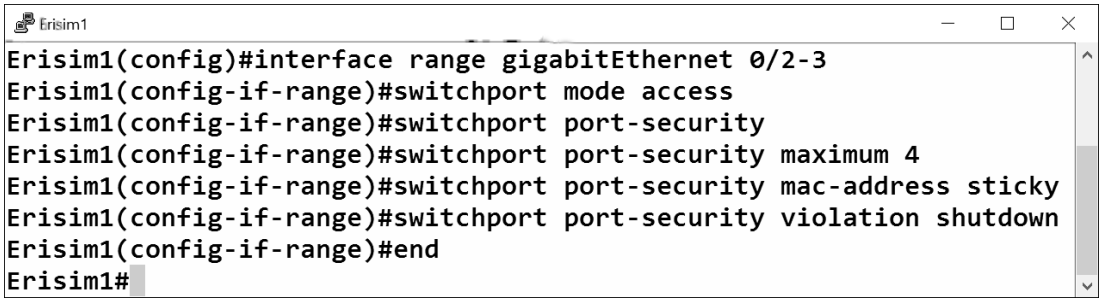
3.2.1.2. MAC taşma saldırısından korunmak

Mac taşıma atağı, MAC erişim kural listesi veya anahtar port güvenliği özelliklerinin aktif edilmesi neticesinde başarısız olmaktadır. Şekil 3.5'te saldırı öncesi anahtarın CPU kullanım değerleri gösterilmektedir.



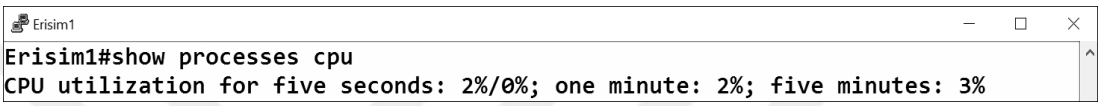
Şekil 3.5. Saldırı öncesi CPU değerleri

Anahtar port güvenliği koruma yöntemi, porttaki MAC adres sayısına bağlı olarak erişim için sınırlama getirmektedir. Bu koruma yöntemi, belli sayıdaki MAC bilgisinin ilgili portta kayıt edilmesini ve yabancı MAC bilgisi ile karşılaştığında trafiğin o hattan gelmemesini sağlamaktadır. Ağ yöneticisi, MAC adreslerini statik veya dinamik yöntemi kullanarak anahtarın portlarına kaydedebilmektedir [46]. Anahtar port güvenliği özelliğini aktif edebilmeyi sağlayan örnek konfigürasyon Şekil 3.6'da gösterilmektedir. Bu konfigürasyon incelendiğinde, ilk satırdaki komut arayüzlere bağlantı için kullanılır. İkinci satırdaki komut, ilgili ara yüze tek bir cihaz bağlantı yapılacağını ve bir adet VLAN'nin geçişini izin verilmesi için kullanılır. Üçüncü satırdaki komut, ilgili porta toplam en fazla 4 adet MAC adresi kayıt edilmesi için kullanılır. Dördüncü satırdaki komut, öğrenme yöntemi dinamik olarak gerçekleşmesini ve beşinci satırdaki komut ise olası ihlal durumunda port kapatılır ve olay kayıt sunucusuna bu ihlal bilgisi gönderilerek işlem tamamlanmaktadır.



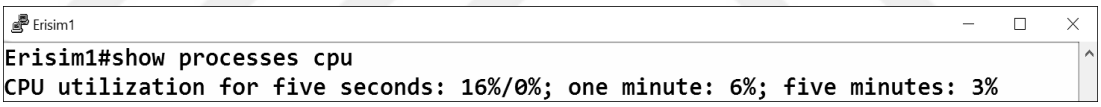
Şekil 3.6. Port güvenliği için gerekli konfigürasyon

Anahtar üzerinde sadece anahtar port güvenliği özelliği aktif iken saldırı başlatılmıştır. Anahtarın anlık CPU değerleri Şekil 3.7'de görüntülenmektedir.



Şekil 3.7. Anahtar port güvenliği tekniği için anahtarın CPU değerleri

MAC erişim kural listesi sayesinde sadece tanımladığımız MAC'ler ilgili porttan geçiş yapabilmektedir. Anahtar üzerinde sadece MAC erişim kural listesi özelliği aktif iken saldırı başlatılmıştır. Anahtarın anlık CPU değerleri Şekil 3.8'de görüntülenmektedir.



Şekil 3.8. MAC erişim kural tekniği için anahtarın CPU değerleri

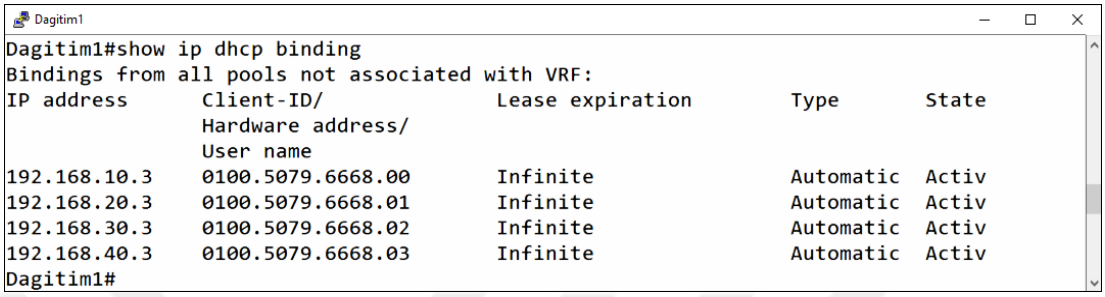
Anahtar port güvenliği tekniğindeki CPU kullanım değerlerinin MAC erişim kural listesi tekniğinde çıkan CPU kullanım değerine göre daha düşük çıktığı görülmektedir.

3.2.2. DHCP açlık saldırısı

DHCP açlık saldırısının amacı yetkili DHCP sunucusunun hizmet dışı kalmasını sağlamaktır. Bunun için yetkili DHCP sunucunun IP havuzunun bitirilmesi gerekmektedir. Saldırgan tarafından DHCP keşif paketi ile sürekli MAC adresi değiştirme işlemi ile IP talebinde bulunarak gerçekleştirmektedir [47]. Saldırgan bu atağı başarıyla tamamladığında, sahte bir DHCP sunucu kurarak istemcilerin ağ geçit bilgilerini bu sahte DHCP sunucunun IP'si yaparak MITM atağını daha geniş çapta yapabilmektedir.

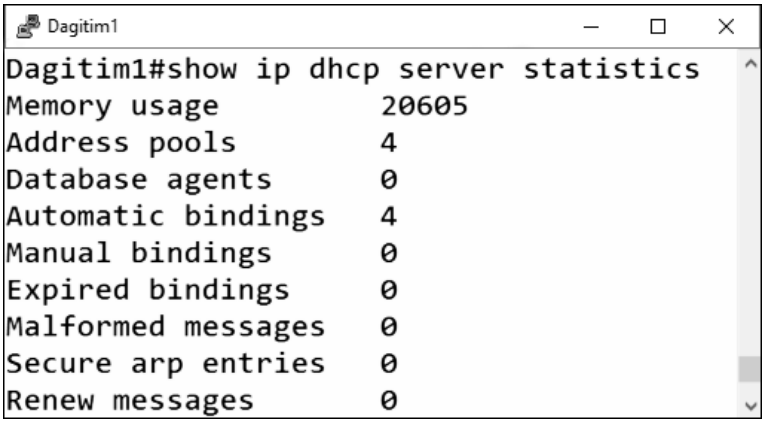
3.2.2.1. DHCP açlık saldırısının başlatılması

DHCP açlık saldırısının başlatılmadan önce dagitim1 anahtarının IP havuzu ve tasarlanan ağdaki VLAN'larinde yer alan toplam 4 bilgisayar için IP ataması gerçekleştirilmesi Şekil 3.9'da gösterilmektedir.



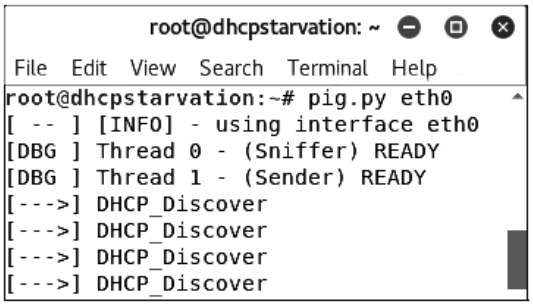
Şekil 3.9. Saldırı öncesi dagitim1'in IP havuzu

Tasarlanan ağ için DHCP sunucusunun IP havuzuna ait sayısal verilerinin yer aldığı bilgiler Şekil 3.10'da görülmektedir. IP havuzunda yer alan 4 adet bilgisayarın istatistik tablosu ile aynı sayıda olması DHCP açlık saldırısının henüz başlamadığını göstermektedir. Açlık atağı yapılmış olsaydı hem havuzdaki IP sayısının hem de istatistik tablosundaki adres havuz sayısında artış gözlenmesi beklenmektedir.



Şekil 3.10. Saldırı öncesi DHCP sunucu istatistik verileri

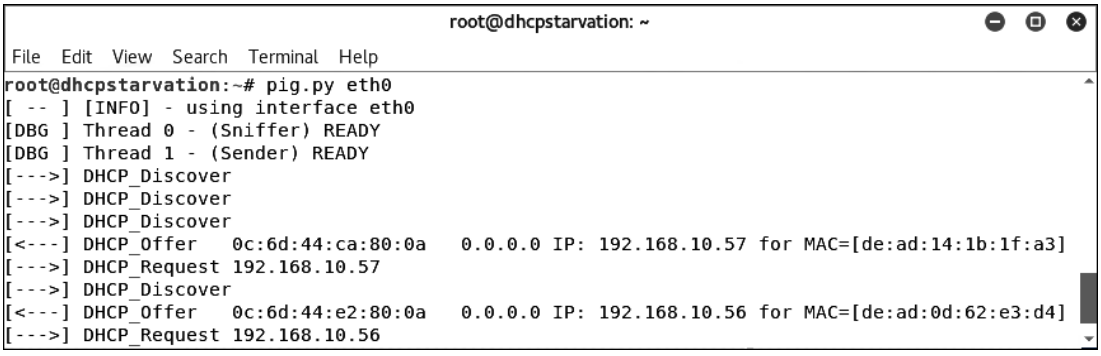
Tasarlanan ağ için DHCP açlık saldırısı iki farklı senaryo üzerinde değerlendirilmiştir. Birinci senaryoda anahtar portunun fiziksel katmanın aktif olduğu durumun değerlendirilmesi yapılmıştır. Saldırının gerçekleştirilmesinde Python dili ile geliştirilmiş pig.py aracı kullanılmıştır. Bu aracın kullanılması ile Şekil 3.11'de görüldüğü gibi sürekli DHCP keşif paketleri ağ üzerinde anons edilmektedir.



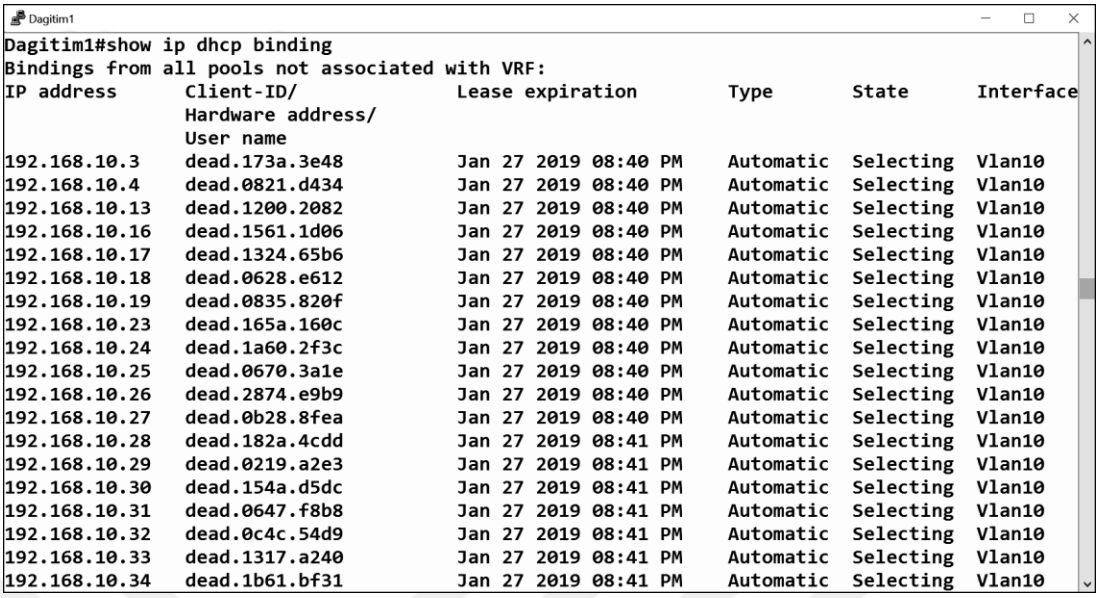
Şekil 3.11. Birinci senaryo için saldırının başlatılması

Bu senaryoda tasarlanan ağın DHCP sunucusunda sadece ilgili VLAN'lere IP ataması yapılabilmesi ve saldırgana ait bilgisayarın bağlı olduğu porta VLAN ataması yapılmaması bu saldırıdan yetkili DHCP sunucusu etkilenmemiştir. Fakat saldırganın bağlı olduğu anahtar üzerinde port güvenlik yapılandırmasının olmayışı nedeniyle anahtarın ilgili portuna DOS atağı yapıldığı görülmüştür.

İkinci senaryoda kurum çalışanının işten ayrılması veya birim değişikliği yapması nedeniyle bağlı olduğu port üzerinde bir takım güvenlik önlemlerinin alınmadığı durum değerlendirilmiştir. Şekil 3.12'de ve Şekil 3.13'te atağın başarılı bir şekilde gerçekleştirildiği hem saldırgan tarafından hem de katman 3 anahtar tarafında görülmektedir.



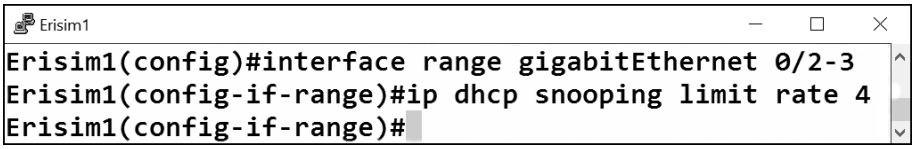
Şekil 3.12. İkinci senaryo için saldırının başlatılması



Şekil 3.13. İkinci senaryo için 3. katman cihazının DHCP havuzu

3.2.2.2. DHCP açlık saldırısından korunmak

Erişim anahtarlarında yapılacak teknik yapılandırmalar; DHCP açlık saldırısının çalışma mantığı MAC değiştirerek yapılmasından dolayı anahtar port güvenliği yapılandırılması ve DHCP paketlerinin saniyedeki gönderim hızını sınırlandırmak için yetkili DHCP sunucusunun bağlı olmadığı portlara Şekil 3.14'deki komutun çalıştırılması ile yapılan ağ tasarımında atağın önüne geçilebildiği görülmüştür.



Şekil 3 14. DHCP keşif paket gönderim sınırlama

DHCP keşif paket sınırlama komutu tek başına bir önlem alamadığı görülmüş, port güvenliği ile birlikte kullanıldığında anahtar üzerinde DOS atağını engelleyerek DHCP açlık atağının da engellenmesi sağlanmaktadır.

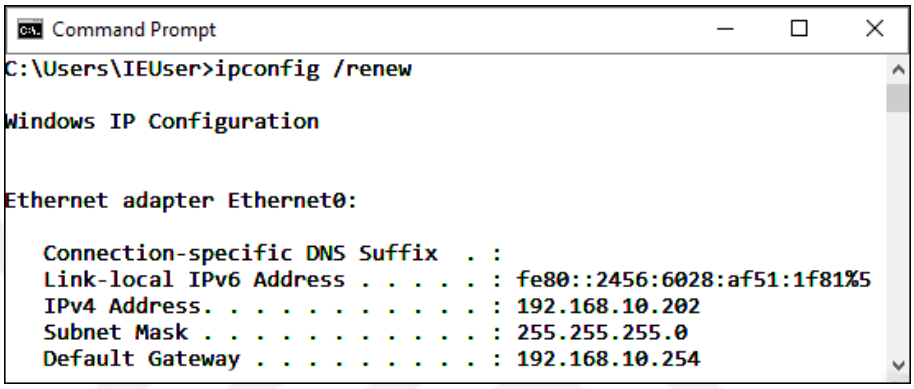
3.2.3. Sahte DHCP saldırısı

DHCP istemcisi DHCP keşif ile IP talebinde bulunduğunda, bu istekler sisteme zarar vermek isteyenler tarafından da görülür. Sahte DHCP sunucusu kurban bilgisayara yetkili DHCP sunucudan konum olarak daha yakın, yetkili DHCP sunucusu meşgul

olduğunda veya bu sunucuya ait havuzda IP kalmadığı durumlarda, IP talep cevabı sahte DHCP sunucusu tarafından verilir. Böylece saldırgan istediği ip, alt ağ maskesi, ağ geçidi ve DNS bilgilerini kurban bilgisayarına gönderir. Kurban bilgisayar DHCP bilgilerini sahtenin gönderdiği bilgilerine göre günceller [48].

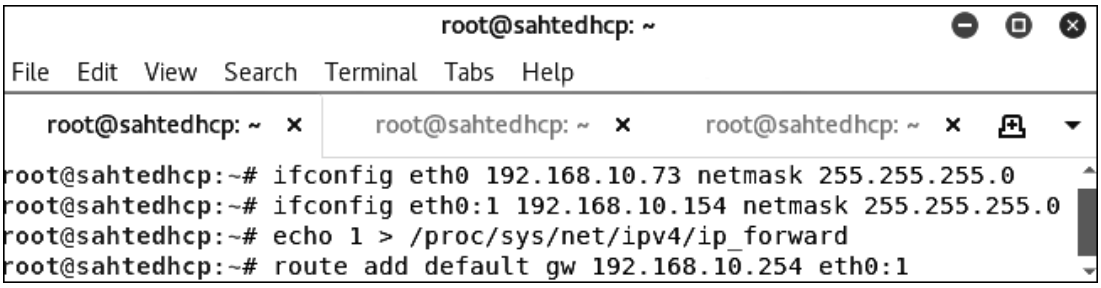
3.2.3.1. Sahte DHCP saldırısının başlatılması

Şekil 3.15'te saldırı öncesi kurbanın IP bilgileri yer almaktadır.



Şekil 3.15. Kurbanın saldırı öncesi IP bilgileri

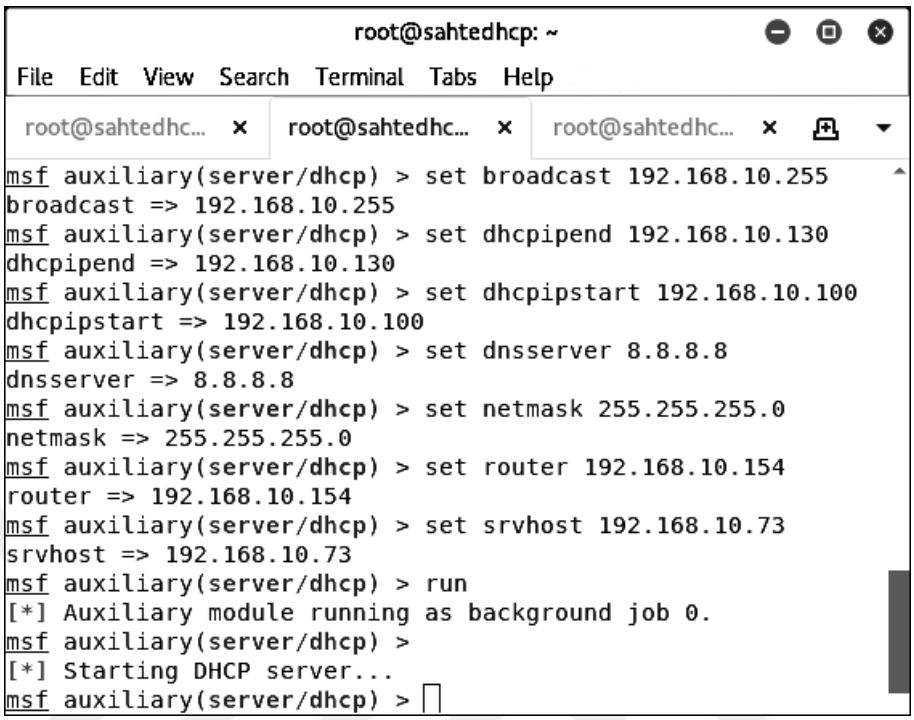
Saldırgan, kurbanın ağ geçidinin IP adresini sahte IP adresi ile değiştirebilmesi için alt arayüz tanımlaması yapması gerekmektedir. Saldırgan, kurbanın saldırı altında olduğunu anlamaması için sahte ağ geçidi adresini belirlerken doğru ağ geçidi bilgisine benzer bir IP adresi seçer ve üzerine gelen paketi ISP yönlendiricisine yönlendirir. Bu işlemlerin gerçekleşmesini sağlayan ayarlar Şekil 3.16'da yer almaktadır.



Şekil 3.16. Saldırganın arayüz ayarları

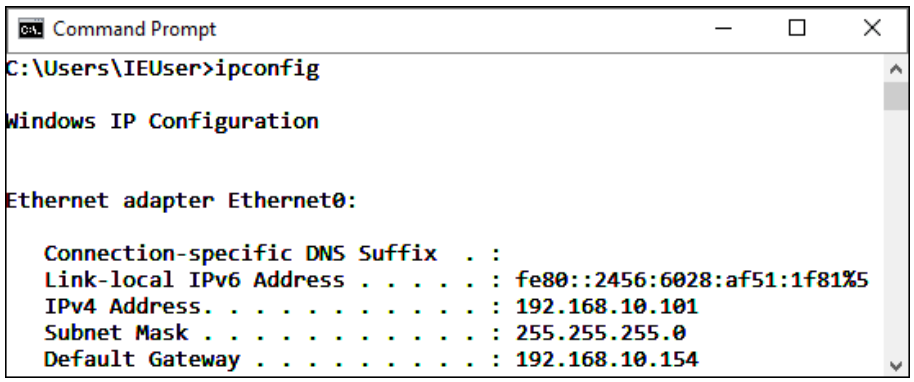
Yetkili DHCP sunucusu için hangi ayarlar gerekli ise sahte DHCP sunucusu için de aynı ayarlar gereklidir. MSF (Metasploit Framework – Güvenlik Rehber Yazılımı)

yazılımı ile sahte DHCP sunucusunu aktif hale gelmesini sağlayan ayarlar Şekil 3.17'de yer almaktadır.



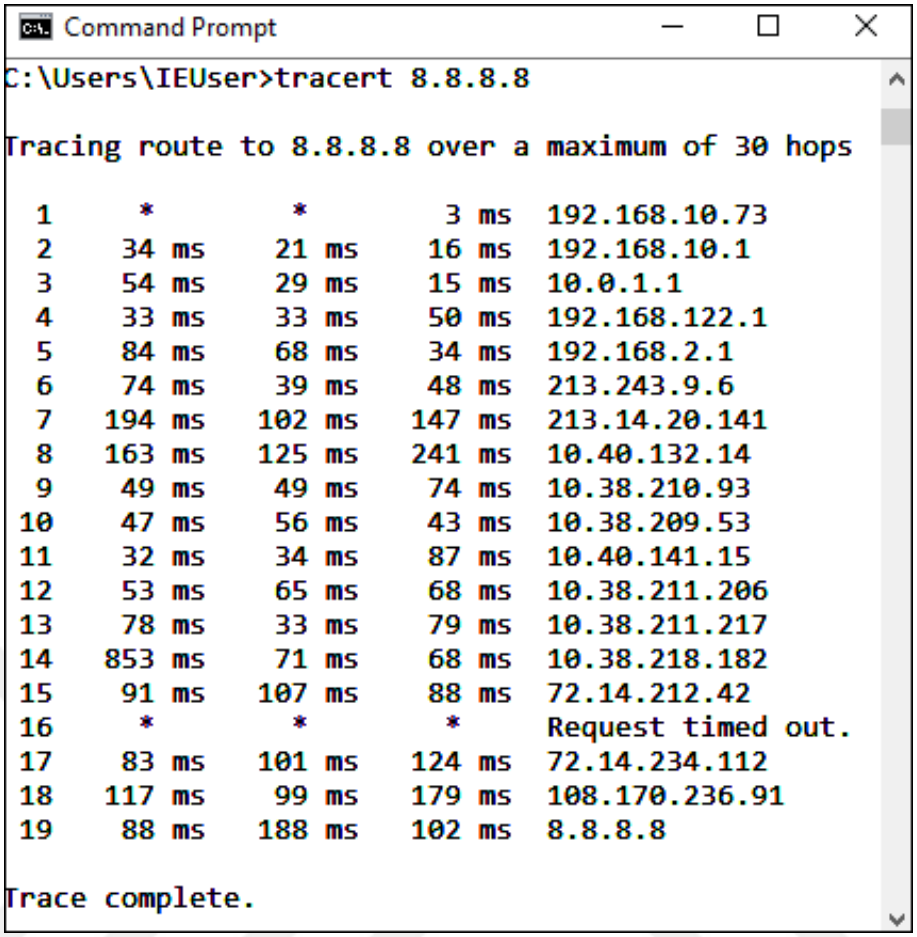
Şekil 3.17. MSF ile sahte DHCP ayarları

Sahte DHCP sunucusu aktif hale gelmesi ile birlikte açlık atağı başlatılır. O sırada yeni eklenen bir Windows bilgisayarın alacağı yeni IP bilgileri Şekil 3.18'deki gibi olmaktadır.



Şekil 3.18. Kurbanın saldırı sonrası IP bilgileri

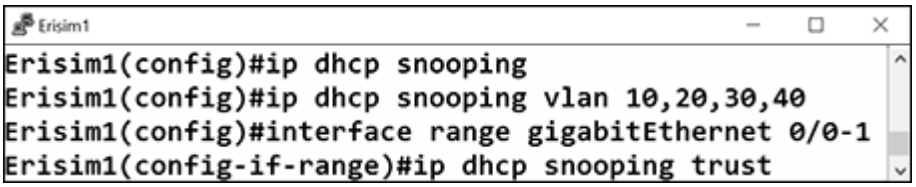
Kurban ile google.com arasındaki rota normal şartlar altında ilk uğraması gereken durak yetkili ağ geçidi olması gerekirken Şekil 3.19'da da görüldüğü gibi saldırgan bilgisayarına uğramaktadır.



Şekil 3.19. Kurbanın internet trafik rotası

3.2.3.2. Sahte DHCP saldırısından korunmak

Burada dikkat edilmesi gereken en önemli nokta IP bilgilerinin gerçek DHCP sunucusundan geldiğini garanti altına alınmasıdır. Eğer DHCP Teklif veya DHCP Onay paketlerini anahtarın güvenilir portundan gönderiliyorsa gerçek DHCP sunucudur. DHCP Keşif veya DHCP İstek paketleri anahtarın güvenilmeyen portundan gönderiliyorsa DHCP istemcisidir. Güvenilmeyen port DHCP sunucu paketlerini geçirmez ve sadece DHCP istemci paketlerinin geçmesini sağlar. IP adresinin güvenilmeyen porttan alınmaması gerekmektedir. Güvenilir port kullanılarak DHCP sunucu paketlerini geçirilmesi sağlanmalıdır [49]. Şekil 3.20'de bu ataktan korunmayı sağlayan konfigürasyonlar yer almaktadır. Cisco marka anahtarların tüm portları varsayılanda güvenilmeyen port olarak ayarlı olduğu unutulmaması gerekmektedir.



Şekil 3.20. Sahte DHCP sunucudan korunma

3.2.4. ARP zehirleme saldırısı

HTTPS (HyperText Transfer Protocol Secure – Hiper-Metin Aktarma Güvenli İletişim Kuralı) sitelerinin HTTP'ye indirgenerek parola ve kullanıcı adı bilgilerini elde edilebilmesi mümkündür. DNS sahtekarlığı ile de kurbanın bağlanmak istediği web sitesine kullanıcının bilgisi haricinde zararlı yazılım içeren web sitesine yönlendirilmektedir. Kurbanın ekran görüntüleri ve klavye tuşlarından gelen bilgilerin takibi gerçekleştirilmektedir. Bunun yanında kurbanın girdiği herhangi bir web sitesi içerisine javascript kodu enjekte edilerek kurbanın dikkatini çekecek uyarı ekranları ile veri ihlali işlemi devam etmektedir [50]. Görülmektedir ki bu saldırı yöntemi diğer saldırılara temel olmakta ve tehlikenin daha çok büyümesine neden olmaktadır. Tüm bu anlatılan risklerin gerçekleşmesine temel oluşturan saldırıyı yapmak için sadece tek satır komutu kullanmak yeterli olmaktadır. Bilgi anlamında hem kurum hem de çalışan zarar görmektedir. Ağın performansı da bu saldırıdan olumsuz etkilenmektedir. Bu gibi durumlar ile karşılaşılmaması için ARP zehirlenmesi saldırısına yönelik gerekli teknik önlemlerin alınması gerekmektedir.

3.2.4.1. ARP zehirleme saldırısının başlatılması

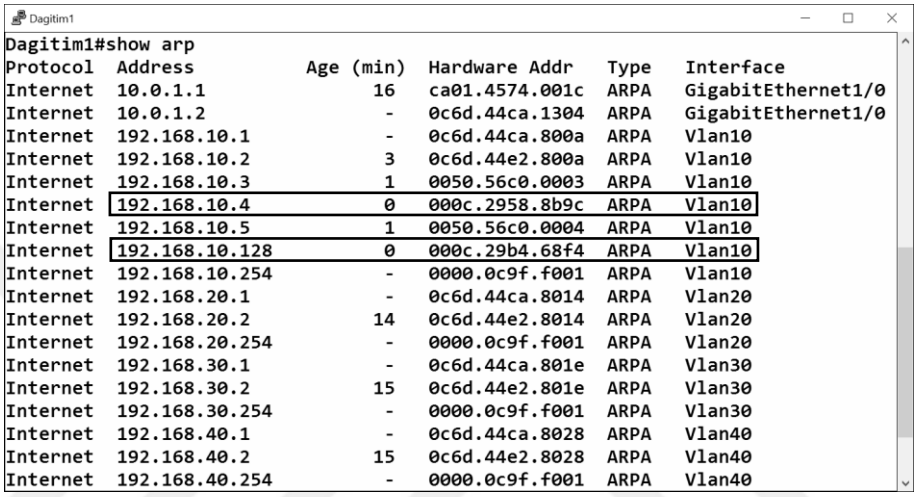
Saldırgan bilgisayarının bağlı olduğu anahtar portunun kurumda kullanılan VLAN'lerden herhangi birine dahil edilmediğinde ARP zehirleme saldırısı başarısız olmaktadır. Saldırgan bilgisayar, kurumda kullanılan VLAN'lerden her hangi birine dahil edilmiş anahtar portuna bağlantı yapması durumunda saldırının yapılması süreci değerlendirilecektir.

Saldırgan ve kurban bilgisayarlarının MAC ve IP bilgilerinin yer aldığı bilgiler Tablo 3.1'de yer almaktadır.

Tablo 3.1. Tasarlanan ağda yer alan bilgisayarların IP ve MAC bilgileri

Host	IP Adresi	MAC Adresi
Kurban	192.168.10.4	00:0c:29:58:8b:9c
Saldırgan	192.168.10.128	00:0c:29:b4:68:f4

Şekil 3.21'de saldırı öncesi dağıtım1 anahtarının ARP tablosu listelenmektedir.

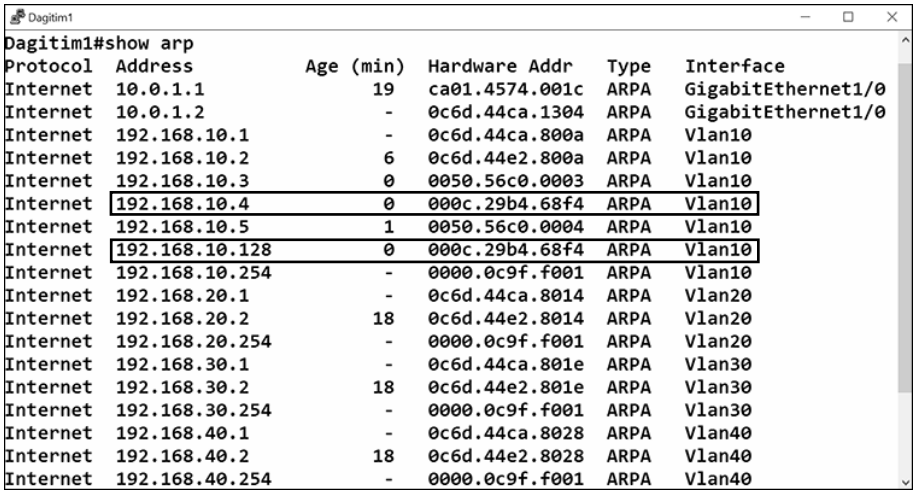


Şekil 3.21. Saldırı öncesi dağıtım1 anahtarının ARP tablosu

ARP zehirleme saldırısı Şekil 3.22'deki ettercap aracı kullanılarak saldırgan tarafından başlatılmaktadır.

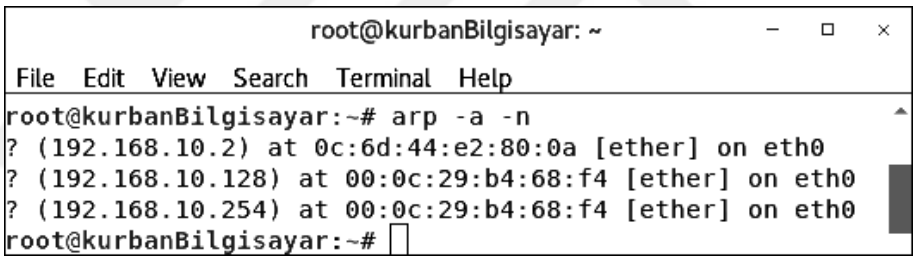
Şekil 3.22. Ettercap iki yönlü ARP zehirleme atağının başlatılması

Anahtar1 üzerinde tanımlı olan anahtar port ve DHCP güvenliğini sağlamada kullanılan koruma yöntemlerinin bu saldırı türüne karşı herhangi bir koruma sağlayamadıklarını ve zehirlenmenin gerçekleştiği Şekil 3.23'de iki farklı IP adresine karşılık iki aynı MAC adresinin eklenmesi ile anlaşılmaktadır.



Şekil 3.23. Saldırı sonrası dağıtım1 anahtarının ARP tablosu

Şekil 3.24'de kurbanın ARP tablosu görülmektedir. Bu şekle göre, saldırgan bilgisayarına ait MAC adresi, kurban bilgisayarının ağ geçidine karşılık eklendiği görüntülenmektedir.



Şekil 3.24. Saldırı sonrası kurbanın ARP tablosu

Saldırgan, hem ağ geçidi görevi gören dagitim1 anahtarının ARP tablosunu hem de kurbanın ARP tablosunu zehirlemiştir. Böylece iki yönlü olarak arp zehirleme saldırısı tamamlanmış olmaktadır. Saldırgan, ARP zehirleme atağına karşı ağ geçidi cihazlarına tanımlanan güvenlik önlemlerini atlatmak için atağı sadece kurban bilgisayarına doğru yaparak hedefine ulaşmayı denemektedir. Şekil 3.25'te tek yönlü ARP zehirleme için kullanılan yöntem yer almaktadır.

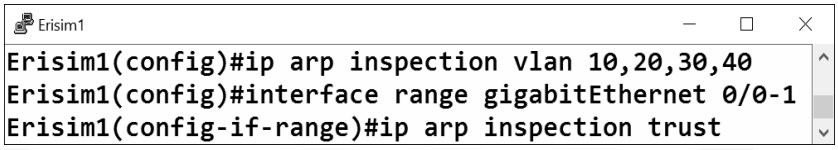
Şekil 3.25. Ettercap tek yönlü ARP zehirleme atağının başlatılması

İki yönlü ile tek yönlü atağın yapılmasında kullanılan komutların arasındaki tek fark tek yönlüde ilk önce zehirlenecek bilgisayarın IP adresi yazılmasıdır. İki yönlü de ise

hangi IP adresinin önce yazılacağının bir önemi olmamaktadır. Tasarlanan ağda gerçekleştirilen tek yönlü yapılan atağın sonucunda sadece kurban bilgisayarının etkilendiği görülmektedir.

3.2.4.2. ARP zehirleme saldırısından korunmak

Erisim1 anahtarı üzerine tanımlanacak güvenlik konfigürasyonuna ait komutlar Şekil 3.26'de yer almaktadır.



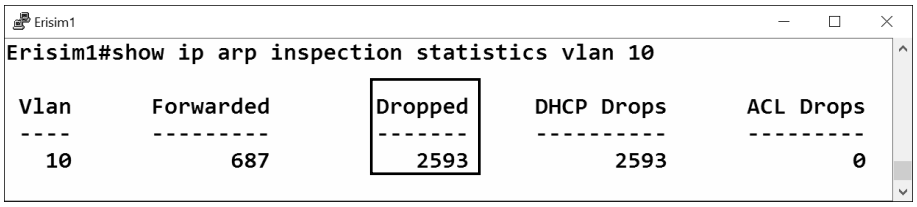
Şekil 3.26. Erişim1 anahtarına tanımlanan ARP korumanın aktif edilmesi

Şekil 3.26'da yer alan komutlardan ilk satırdaki komut ARP zehirlemeye karşı kullanılan genel ARP koruma için kullanılmaktadır. Erişim1 anahtarına tanımlanan bu komutların yönetimi doğru yapıldığında yapılan ARP zehirleme atağına karşı koruma sağlamaktadır. Sadece genel ARP koruma komutu kullanıldığında bu atağa karşı koruma başarısızlıkla sonuçlanmasına neden olmaktadır. Buna göre Tablo 3.2'te zehirleme atağına karşı alınan korumanın hangi durumlarda başarılı veya başarısız olduğu gösterilmektedir.

Tablo 3.2. ARP koruma yönteminin başarımı

Kurban / Saldırgan	Güvenli Port	Güvensiz Port
Güvenli Port	Korunmaz	Korunmaz
Güvensiz Port	Korunur	Korunur

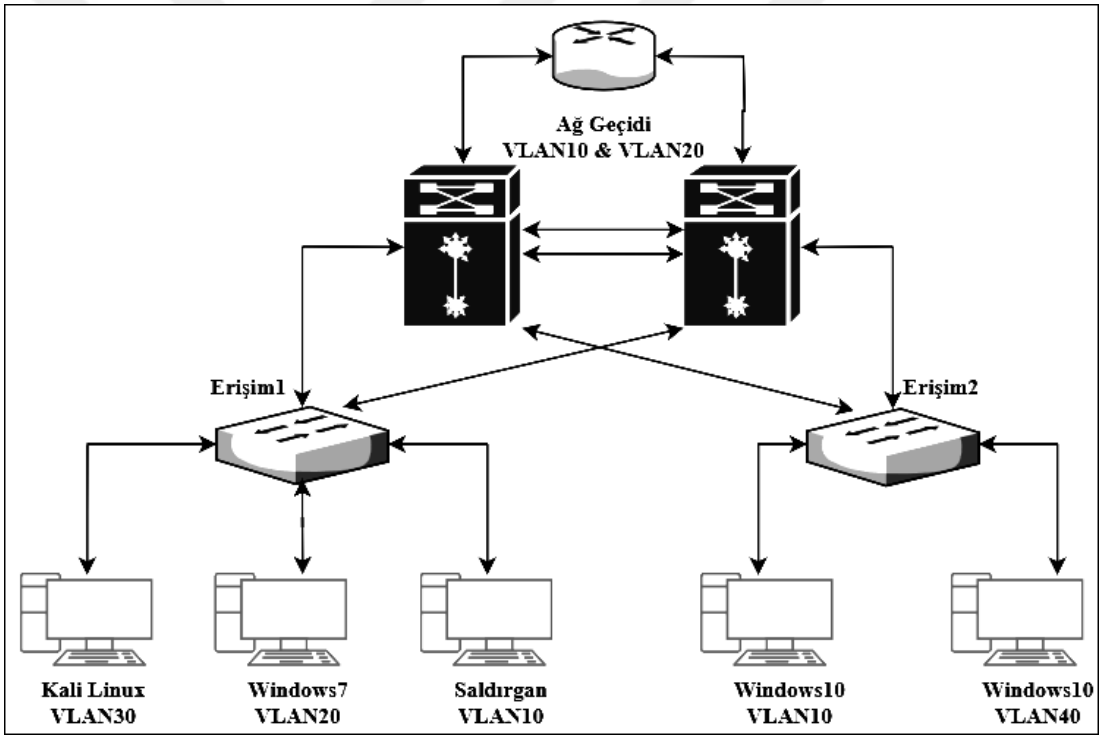
Tablo 3.2'deki verilere göre saldırgan bilgisayarının bağlı olduğu anahtar portu mutlaka güvensiz portta olması gerekmektedir. Eğer saldırgan güvenli porta bağlantı sağlar ve o porttan atağı başlatırsa ağdaki güvenli/güvensiz portlara bağlı tüm bilgisayarların bu ataktan olumsuz etkilendiği görülmektedir. Ayrıca atak sırasında pasif hale getirilen sahte ARP paketlerinin sayısı Şekil 3.27'de gösterilmektedir.



Şekil 3.27. Durdurulan paket sayısı

3.2.5. LLMNR ve NBT- NS zehirleme saldırısı

Bu zehirlenme saldırısının amacı son kullanıcıların parola özetlerini elde etmek ve bu parola özetini parola kırma araçlarında kullanarak asıl parolaya ulaşmaktır. Saldırının gerçekleşmesini Şekil 3.28'de yer alan örnek ağ senaryosu üzerinde gerçekleştirilmiştir.

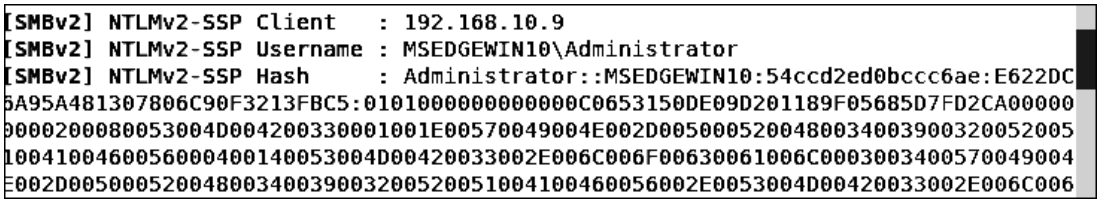


Şekil 3.28. Bu zehirlenme tekniği için örnek ağ senaryosu

3.2.5.1. LLMNR ve NBT- NS zehirleme saldırısının başlatılması

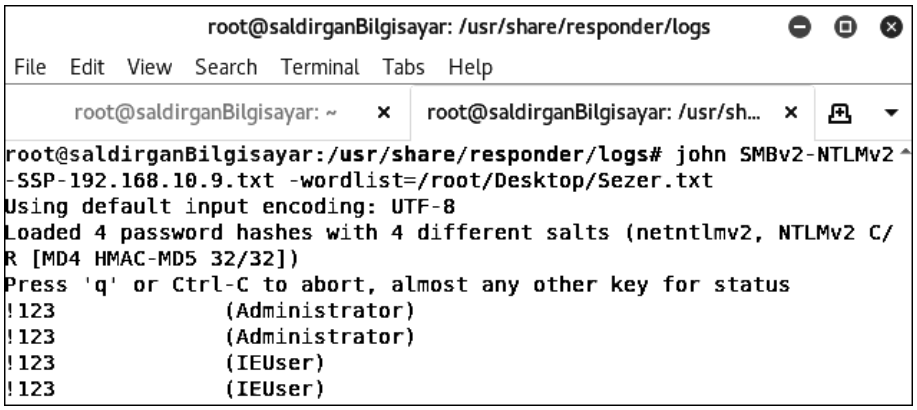
Saldırgan ile kurban(Windows10) bilgisayarı aynı VLAN'dedirler. DNS servisi, isim çözümlemesini gerçekleştirerek yazıcı veya dosya sunucusuna ulaşmayı sağlamaktadır. Böylece hedef ile ilgili isim bilgisi elde edilmektedir. Kurban çalıştır alanına ulaşmak istediği yerin adını yanlış yazması, dosya sunucusunda veya

yazıcıdaki bağlantı problemi nedeniyle ulaşılamaması durumunda LLMNR/NBT-NS servisleri devreye girerek ikinci DNS görevini başlatır ve saldırgan bu görevi üstlenerek isim çözümleme sorgusuna cevap vermektedir. Kurban, verilen cevaba karşı kendi kullanıcı adı ve parola özetlerini saldırgana göndererek süreç tamamlanmaktadır. Saldırganın elde ettiği parola özetleri şekil 3.29'da görülmektedir.



Şekil 3.29. Parola özetleri

Saldırgan bu süreçten sonra parola kırma tekniklerini devreye alır ve bu parola özetinden açık parolaya ulaşmaya çalışmaktadır. Son kullanıcı, parolasını belirlerken karmaşık ve en az 8 karakter olması kuralına uymasının önemi bu saldırı tekniğinde karşımıza çıkmaktadır. Şekil 3.30'de kullanılan yöntem ile elde edilen hash değerlerinin yaygın olarak kullanılan parola kırma araçlarından john the ripper aracına giriş olarak verilen değerler ile kelime listesindeki kelimelerden türetilen hash değerleri karşılaştırır. Eğer eşleşme sağlanırsa kullanıcıya ait parola saldırganın eline geçmesiyle sonuçlanmaktadır.



Şekil 3.30. Parola özetinden açık parolanın bulunması

Parolanın bu kadar çabuk bulunmasının en önemli nedeni, parola kısalığı ve karmaşık karakterleri barındırmamasıdır. Bu saldırı senaryosu diğer VLAN'lerde yer alan farklı işletim sistemleri üzerinde de denemeler yapılmıştır. Saldırganın bulunduğu VLAN'den farklı olanlar bu saldırıdan etkilenmediği sonucuna varılmaktadır.

3.2.5.2. LLMNR ve NBT- NS zehirleme saldırısından korunmak

Son kullanıcıları LLMNR/NBT-NS saldırılarına karşı sömürülmeye karşı korumak için bilgi toplama modüllerini kullanarak LLMNR ve NBT-NS servislerinin aktif olduğu bilgisayarları belirlemek ve aktif olan bu servisleri devre dışı bırakmak gerekmektedir. Tasarlanan ağda saldırgan bilgisayarından NBT-NS sorgusu VLAN10'daki Windows 10 bilgisayarına Şekil 3.31'deki gibi yapılmaktadır.

```
msf auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 192.168.10.5->192.168.10.5 (1 hosts)
[+] 192.168.10.5 [MSEDGEWIN10] OS:Windows Names:(MSEDGEWIN10, WORKGROUP)
 Addresses:(192.168.10.5) Mac:00:0c:29:44:d8:40 Virtual Machine:VMWare
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/netbios/nbname) >
```

Şekil 3.31. VLAN10 windows 10 için NBT-NS sorgusu

Sorgu sonucunda NBT-NS servisinin VLAN10 ağındaki bilgisayarda devrede olduğu görülmektedir. NBT-NS sorgusu tasarlanan ağda yer alan VLAN20'deki Windows 7 bilgisayarına Şekil 3.32'deki gibi yapılmaktadır.

```
msf auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 192.168.20.3->192.168.20.3 (1 hosts)
[+] 192.168.20.3 [WIN7-BILGISAYAR] OS:Windows Names:(WIN7-BILGISAYAR, WORKGROUP, □□□
 MSBROWSE_ □□ Addresses:(192.168.20.3) Mac:00:0c:29:89:aa:fa Virtual Machine:VMWare
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/netbios/nbname) >
```

Şekil 3.32. VLAN20 ağındaki windows 7 için NBT-NS sorgusu

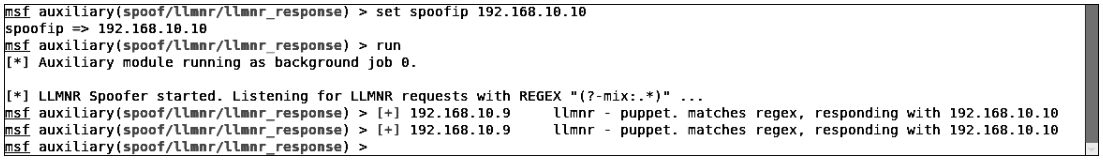
Sorgu sonucunda NBT-NS protokolünün VLAN20 ağındaki bilgisayarda devrede olduğu görülmektedir.

Örnek senaryoda VLAN10 ağına dahil olan saldırgan bilgisayarının NBT-NS sorgusunda karşılaşılan durumlar aşağıda sıralanmaktadır:

- Hedef bilgisayarın işletim sistemi Windows 7 olması durumda VLAN'nin burada bir önem arz etmediğini ve sorguya her zaman cevap verdiği sonucuna varılmaktadır.
- Hedef bilgisayarın işletim sistemi Windows 10 ve sorgunun yapıldığı bilgisayar ile aynı VLAN'de olduğunda hedefin NBT-NS sorgusuna cevap verdiği fakat farklı VLAN'de olduğunda ise sorguya cevap vermediği görülmektedir.

- Hedef bilgisayarın işletim sistemi Linux olması durumda VLAN'nin burada bir önem arz etmediğini ve sorguya hiç bir zaman cevap vermediği görülmektedir.

Bir diğer sorgulanması gereken servis LLMNR servisidir. Tasarlanan ağda yer alan saldırgan bilgisayarından, VLAN10 ağında yer alan Windows 10 ve Windows 7 bilgisayarlarına Şekil 3.33'de de görüldüğü gibi LLMNR sorgusu yapılmaktadır.



Şekil 3.33. VLAN10 LLMNR sorgusu

Sorgu sonucunda LLMNR servisinin VLAN10 ağdaki bilgisayarlarda devrede olduğu görülmektedir. Bu sorgunun farklı VLAN'lere gönderilmesi durumunda cevap dönülmediği sonucuna varılmaktadır.

NBT-NS zehirlenmesine karşı son kullanıcı bilgisayarında NBT-NS servisinin kapatılması önerilir. Bunun için IPv4'ün gelişmiş TCP/IP ayarlarının WINS sekmesinde yer alan "TCP/IP üzerinde NetBIOS'u devre dışı bırak" seçeneğinin seçilmesi gerekmektedir. LLMNR zehirlenmesine karşı son kullanıcı bilgisayarında LLMNR servisinin kapatılması önerilir. Bunu için Yerel Grup İlkesi Düzenleyicisi ekranından yönetim şablonları, ağ , DNS istemcisi yolunu izleyerek "Çoklu noktaya ad çözümlemesini kapat özelliğinin" devreye alınması gerekmektedir. Örnek senaryoda yer alan son kullanıcı bilgisayarlarında yukarıda bahsedilen önlemler alındıktan sonra bilgi toplama yöntemlerine hiçbir şekilde cevap alınamadığı sonucuna varılmaktadır.

3.3. ARP Zehirleme Saldırısı için Geliştirilmiş Test Ortamı

ARP zehirlemeye karşı alınması gereken güvenlik önlemleri yönetilebilir ağ cihazları üzerinde tanımlanabilmektedir. Yerel alan ağında kullanılan ağ cihazlarının yönetilebilir olmayanların büyük çoğunluğu ARP zehirleme saldırısına yönelik koruma yöntemlerini desteklememektedir. Bu kapsamda ARP zehirleme saldırısına karşı son kullanıcıların ARP atağı durum bilgisini görüntülemesi ve atağın durdurulmasına yönelik Python dili ile hazırlanmış web görünümüne sahip koruma

aracı geliştirilmiştir. Ayrıca saldırının gerçekleştirilebilmesi için de bir araç geliştirilmiştir. Şekil 3.34'te bu aracın ara yüzü yer almaktadır.

Şekil 3.34. Ortadaki adam saldırı aracı

Bu saldırı aracı ile hem tek yönlü hem de iki yönlü zehirleme gerçekleştirilmektedir. Şekil 3.35'te ise geliştirilen koruma aracının saldırı öncesi web görünümü yer almaktadır.

Şekil 3.35. Saldırı öncesi koruma yazılımının web görünümü

Python dili ile geliştirilen yazılım öncelikle ağın yetkili ağ geçidinin MAC adresini öğrenmektedir. Sonraki süreçte ise yerel bilgisayarın güncel ARP tablosundaki

durumun takibini gerçekleştirmektedir. ARP tablosunda istenmeyen bir hareket algıladığı anda yazılım devreye girerek hem uyarı bilgisini hem de ARP zehirleme için son kullanıcıyı koruma altına almaktadır. Koruma yazılımı devredeyken saldırganın ARP zehirleme atağını devam ettiriyor olsa da yerel bilgisayarın gönderdiği hiçbir paketi kendi üzerine çekemediği sonucuna varılmaktadır. Koruma yazılımı devreye alınmadan önce veya çalışıyorken ARP atağı başladıysa Şekil 3.35'deki ekranın son kullanıcının ekranına düşmesi sağlanmaktadır.

Şekil 3.36. Saldırı sonrası koruma yazılımının web görünümü

4. SONUÇLAR VE ÖNERİLER

Kurum çalışanı kaynaklı siber saldırıların gün geçtikçe artmaya devam ettiği görülmektedir. Bundan dolayı saldırganların en çok hedefledikleri çalışanların parolaları veya diğer kişisel bilgileri olmaktadır. Ayrıca siber tehditler ile mücadele etmeyi sağlayan yerel alan ağlarda kullanılan cihazların doğru yapılandırılmaması sonucunda siber saldırının tespit edilmesi neredeyse imkansız olmaktadır. Kurumların bu kapsamda hem gerekli güvenlik yapılandırma süreçleri hem de teknolojik olmayan süreçlerinin etkin ve verimli yönetmesi sağlanmalıdır.

Bu çalışmanın temel amacı, benzetim ortamı ve işletim sistemi sanallaştırmanın bir arada olduğu yapı üzerinden; yerel alan ağdaki siber saldırıların nasıl gerçekleştiğini, bu saldırılardan korunmak için gerekli güvenlik adımlarını uygulamalı bir biçimde ifade edilmesi ve kurum çalışanlarının bilgi güvenliği farkındalıklarına yönelik katkıda bulunmaktır.

Kurum ağına kimliği belirsiz kötü niyetli kişilerin bağlanmaması gerekmektedir. MAC taşma saldırısı ile yerel alan ağlarının çalışamayacak bir seviyeye geldiği görülmektedir. Bu durumdan hem son kullanıcı güvenliği riske girmekte hem de kurumun genel işleyişi olumsuz etkilenmektedir. Farklı VLAN'lerin de bu saldırıdan etkilenmesi VLAN'in bu tip bir saldırıda güvenlik önlemi olarak kullanılamayacağını göstermektedir. MAC taşma atağından korunmak için teknik konfigürasyonların yanında kullanılmayan anahtar portların mutlaka kapatılması gerekmektedir. Çünkü saldırgan herhangi bir VLAN'de olmaması veya IP almamasına rağmen bu saldırıyı gerçekleştirebilmektedir. MAC taşma saldırısına yönelik anahtar port güvenliği ve MAC erişim liste teknikleri kullanılarak koruma sağlanmıştır. Anahtar port güvenliği tekniğinin kullanıldığı anahtarda, saldırı sırasındaki CPU kullanım değerleri diğer tekniğe göre daha iyi sonuçlar verdiği görülmüştür. Bu nedenden dolayı anahtar port güvenliği tekniğinin kullanılması önerilmektedir.

DHCP açlık saldırısından korunmak için sadece DHCP'ye yönelik tedbirlerin yeterli olmadığı görülmüştür. Bu nedenle bu saldırıdan korunmanın ilk şartı ağda kullanılan anahtarlar üzerinde mutlaka anahtar port güvenlik yapılandırması yapılması gerekmektedir. Dağıtım1 anahtarında tanımlı VLAN'lere yönelik IP teklifleri gönderildiği için saldırganın IP talebi karşılık görmemektedir. Bu nedenle çalışanın işten ayrılması veya birim değiştirmesi gereken durumlarda o çalışan için ayrılan anahtar portunun mutlaka kapatılması gerekmektedir. Böylece saldırganın tanımlı VLAN'lerin yer aldığı anahtar portlarına bağlantı yapılmasının önüne geçilmesi sağlanmaktadır.

Tasarlanan ağ üzerinde sahte DHCP saldırısının başarıya ulaşmasında açlık saldırısının rolü olduğu görülmektedir. Sahte DHCP sunucusundan bir kez IP alan kurban bilgisayarının yeniden başlatılması ve açlık atağının durdurulmasına rağmen IP bilgilerini sahte DHCP sunucusundan almaya devam etmektedir. Bu durumun asıl nedeni anahtar üzerinde port güvenliği alınmadığından kaynaklandığı görülmektedir. Tek bir koruma yöntemi tehditlere karşı yetersiz kalmaktadır. Bu nedenle gelen atağın barındırdığı işlevlere göre koruma yöntemleri seçilmelidir.

Saldırgan, ağda tanımlı VLAN'lerden birine dahil olmadığı sürece ARP zehirleme atağının tanımlı diğer VLAN'leri etkilemediği görülmektedir. Bu nedenle VLAN'lerin doğru yönetmenin önemi ortaya çıkmaktadır. Ayrıca saldırgan native VLAN üyesi anahtar portuna bağlanması durumunda ise IP hizmeti alamadığı ve diğer VLAN'leri ARP tablolarını zehirleyemediği görülmektedir. Saldırganın hangi porttan bağlantı yapacağı tam olarak bilinememesi Erişim1 anahtarına tanımlanan ARP koruma yönteminin zorlukları arasında yer almaktadır. Bu koruma yönteminde sadece genel koruma ayarını aktif edilmesi ve güvenli/güvensiz port tanımlaması yapılmadığı durumda yapılan ARP zehirlemesi atağı sonucunda kurban bilgisayar ağ geçidine ulaşamamakta ve bu nedenle bağlantı kaybına neden olmaktadır. ARP zehirleme atağının yapılmasının basit ve bir çok atağa temel oluşturması nedeniyle dikkatleri üzerine çekmiş ve bu nedenle kurum personeli bilgisayarlarına karşı da ayrıca bir koruma yapılması ihtiyacı ortaya çıkmaktadır. Anahtar üzerine tanımlanan koruma yönteminin kullanımı sırasında dikkat edilmesi gerekenler; genel koruma komutunun

tek başına kullanılmaması, ağ geçidi tarafına bakan tüm portlar güvenli ve son kullanıcının bağlı olduğu portlar ise güvensiz olarak ayarlanması gerekmektedir.

Yerel alan ağında MAC taşma, DHCP ve ARP saldırılarına karşı gerekli önlemlerin alınmasının yanında her birim için farklı VLAN tanımlamaları yer almaktadır. Tüm bu güvenlik önlemleri LLMNR/NBT-NS zehirlemesinin önüne kısmen geçebildiği sonucuna varılmaktadır. Son kullanıcı tarafında ilgili servislerin kapatılarak kullanıcıların parola belirlerken tahmin edilmesi zor hatırlanması kolay sayı ve karakterlerin birleşiminden oluşturmalarını ve daha güçlü parolalar kullanmaları gerektiği noktasında farkındalık düzeylerinin arttırılmasına yönelik eğitimler verilmesi önerilmektedir.

KAYNAKLAR

[1] Navhreiner C., Laliberte M., Internet Security Report, *WatchGuard,* 1, 4, 2018.

[2] Chen J., Su C., Yeh K., Yung M., Special Issue on Advanced Persistent Threat, *Future Generation Computer Systems,* DOI: 10.1016/j.future.2017.11.005.

[3] Wiele T.V., Email Inboxes Still The Weakest Link in Security Perimeters, Helpnetsecurity, https://www.helpnetsecurity.com/2018/02/23/weakest-link-security-perimeters/ (Ziyaret tarihi: 10 Ekim 2018).

[4] Widup S., Spitler M., Hylender D., Bassett G., 2018 Verizon Data Breach Investigations Report, *Verizon,* 11, 5, 2018.

[5] Sridhar M., Mohanty A., Yilmaz F., Tendulkar V., Hamlen K. W., Inscription: Thwarting ActionScript Web Attacks From Within, IEEE International Conference On Big Data Science And Engineering, DOI: 10.1109/TrustCom/BigDataSE.2018.00078.

[6] Morgan S., One Million Cybersecurity Job Openings in 2016, https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#733ce48e27ea, (Ziyaret tarihi: 12 Ekim 2018).

[7] Uçan O.N., Osman O., *Bilgisayar Ağları ve Ağ Güvenliği,* 1.Baskı, Nobel, Ankara, 2006.

[8] Çölkesen R., *İnternet Omurgasının Altyapısı Network TCP/IP Unix,* 10.Baskı, Papatya, İstanbul, 2013.

[9] Yuan X., On the Extended Bellman-Ford Algorithm to Solve Two-Constrained Quality of Service Routing Problems, *IEEE Proceedings Eight International Conference on Computer Communications and Networks,* DOI: 10.1109/ICCCN.1999.805535.

[10] Ma Q., Steenkiste P., Routing Traffic with Qualityof Service Guarantees in Integrated Services Networks, Researchgate, https://www.researchgate.net/publication/2331725_Routing_Traffic_with_Quality-of-Service_Guarantees_in_Integrated_Services_Networks (Ziyaret tarihi: 20 Ekim 2018).

[11] Tayeb S., Latifi S., An Evaluative Analysis of DUAL, SPF, and Bellman-Ford, *River Publishers,* DOI: 10.13052/jsn2445-9739.2017.001.

[12] Krishnan Y.N., Shobha G., Performance Analysis of OSPF and EIGRP Routing Protocols for Greener Internetworking, *IEEE 2013 International Conference on Green High Performance Computing*, DOI: 10.1109/ICGHPC.2013.6533929.

[13] RFC 3626, Optimized Link State Routing Protocol, *INRIA,* Villeneuve-d'Ascq, 2003.

[14] Apostolopoulos G., Guerin R., Kamat S., Implementation and Performance Measurements ff QoS Routing Extensions to OSPF, *IEEE IEEE INFOCOM '99. Conference on Computer Communications*, DOI: 10.1109/INFCOM.1999.7514554.

[15] Rastogi R., Breitbart Y., Garofalakis M., Kumar A., Optimal Configuration of OSPF Aggregates, *IEEE ACM Transactions on Networking*, 2003, **11**(2), 181-194.

[16] Kalman S., *Web Security Field Guide*, 1st ed., Cisco Press, New York, 2002.

[17] Udhayamoorthi M., Mohan K.S., Karthik S., Dinesh P. S., Senthilkumar C., Enhanced Designing of Network Using IPv6 Protocol And Enabling HSRP for Redundancy, *IEEE 2015 International Conference on Soft-Computing and Networks Security*, DOI: 10.1109/ICSNS.2015.7292431.

[18] Carroll D.A., Adams K.J., Potter K.H., Jain P., Token Ring Spanning Tree Protocol, 2001, US 6.304.575 B1, *U.S. Patent Application Publication.*

[19] Perlman R., Breitbart Y., Garofalakis M., Kumar A., An Algorithm for Distributed Computation Of a Spanningtree in an Extended LAN, *ACM SIGCOMM*, 1985, **15**(4), 44-53.

[20] Droms R.E., Automated Configuration of TCP/IP with DHCP, *IEEE Internet Computing*, DOI: 10.1109/4236.780960.

[21] Kırcı P., Toka Ç.Ö., Erdem F., IP/MPLS Ağlar Üzerinde Sanal-Yerel Servisler ve Yönlendirici Konfigürasyonları, *Uludağ University Journal of The Faculty of Engineering*, DOI: 10.17482/uujfe.33352.

[22] Bozgeyik A., Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi, Doktora Tezi, Hasan Kalyoncu Üniversitesi, Sosyal Bilimler Enstitüsü, Gaziantep, 2018, 498778.

[23] Şentürk M.Y., Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinde Uygulanması, Yüksek Lisans Tezi, Türk Hava Kurumu Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2018, 527395.

[24] Büyükkılıç M., Cybersecurity Framework For Small and Medium Size Enterprises, Master's Thesis, Bahcesehir University, Graduate School of Natural And Applıed Scıences Cyber Securıty, İstanbul, 2018, 510056.

[25] Kara M., Endüstriyel Nesnelerin İnternetinde Hızlı ve Güvenli Veri İletişimi, Yüksek Lisans Tezi, İskenderun Teknik Üniversitesi, Mühendislik ve Fen Bilimleri Enstitüsü, Hatay, 2018, 502475.

[26] Pingle B. Mairaj A., Javaid A.Y., Real-World Man In The Middle Attack Implementation Using Open Source Tools For Instructional Use, 2018 *IEEE International Conference on Electro/Information Technology,* DOI: 10.1109/EIT.2018.8500082.

[27] Ekparinya P., Gramoli V., Jourjon G., Impact of Man-In-The-Middle Attack on Ethereum, 2018 IEEE 37th Symposium on Reliable Distributed Systems, DOI: 10.1109/SRDS.2018.00012.

[28] Başaranoğlu E., Kurumsal Ağlardaki Windows Ortamlarına Saldırılar ve Sıkılaştırma Yöntemleri, Yüksek Lisans Tezi, İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2017, 457667.

[29] Hajdarevic K., Kozic A., Avdagic I., Masetic Z., Dogru N., Training Network Managers in Ethical Hacking Techniques to Manage Resource Starvation Attacks using GNS3 Simulator, *IEEE,* DOI: 10.1109/ICAT.2017.8171634.

[30] Bijral R.K., Gupta A., Sharma L.S., Study of Vulnerabilities of ARP Spoofing and its Detection Using Snort, *IEEE,* 2017, **8**(5), 2074-2077.

[31] Alizada J., Kablosuz Yerel Alan Ağlarında Güvenlik ve Saldırı Yöntemleri Yüksek Güvenlikli Kablosuz Yerel Alan Ağının Tasarımı, Yüksek Lisans Tezi, İstanbul Aydın Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2016, 483758.

[32] Mohtasin R., Prasad P.W.C., Alsadoon A., Zajko G., Elchouecmi A., Singh A.K., Development of a Virtualized Networking Lab Using GNS3 and VMware Workstation, *IEEE,* DOI: 10.1109/WiSPNET.2016.7566205.

[33] Plch M., Practical Man-in-the-Middle Attacks in Computer Networks, Lisans, Masaryk Unıversıty, Faculty of Informatics, 2015.

[34] Meral M., J., Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi, Yüksek Lisans Tezi, Harp Akademileri, Stratejik Araştırmalar Enstitüsü, İstanbul, 2015, 398413.

[35] Arote P., Arya K.V., Detection and Prevention Against ARP Poisoning Attack Using Modified ICMP and Voting, *IEEE,* 2015, DOI: 10.1109/CINE.2015.34.

[36] Tripathi N., Mehtre B.M, Analysis of Various ARP Posoning Mitigation Techniques: A Comparison, *IEEE,* DOI: 10.1109/ICCICCT.2014.6992942.

[37] Akyıldız M.A., Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Isparta, 2013, 353566.

[38] Nayak G.N., Samaddar S.G., Different Flavours of Man in the Middle Attack, *IEEE*, DOI: 10.1109/ICCSIT.2010.5563900.

[39] Trabelsi Z., Shuaib K., Man in the Middle Intrusion Detection, *IEEE*, DOI: 10.1109/GLOCOM.2006.282.

[40] Yılmaz T., Karaarslan E., Akın G., GNS3 Tabanlı Ağ Emülasyonlarının Bilgisayar Ağları Eğitiminde Kullanımı: Senaryolar ve Öneriler, *Akademik Bilişim Konferansı*, Eskişehir, 4-6 Şubat 2015.

[41] Çalışkan M., Sanallaştırma Teknolojilerinin Saldırı Tespit ve Önleme Sistemlerinin Performansı Üzerine Etkisi, Yüksek Lisans Tezi, Hava Harp Okulu, Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul, 2014, 364103.

[42] Yüksek M., Öztürk N., SIP Saldırıları ve Güvenlik Yöntemleri, *Bilişim Teknolojileri Dergisi*, 2017, **10**(3), 301-310.

[43] Wilkins S., Smith F., *CCNP Security Secure 642-637 Official Cert Guide*, 2.Baskı, Cisco Press, 2013.

[44] Akın G., DHCP Servisine Yeni Bir Bakış, *XIII. Türkiye'de İnternet*, Ankara, Türkiye, 22-23 Aralık 2008.

[45] Vissamsetty V., Lakshmanan M., Penupolu S.S., Rungta A., Detecting Man in the Middle Attacks, 2018, US 2018 / 0013788 A1, *U.S. Patent Application Publication.*

[46] Kiravuo T., Sarela Mikko, Manner J., A Survey of Ethernet LAN Security, *IEEE*, 2013, **15**(3), 1477-1491.

[47] Tripathi N., Hubballi N., Exploiting DHCP Server-Side IP Address Conflict Detection: A DHCP Starvation Attack, *IEEE*, DOI: 10.1109/ANTS.2015.7413661.

[48] Conti M., Dragoni N., Lesyk V., A Survey of Man in the Middle Attacks, *IEEE Communications Surveys & Tutorials*, 2016, **18**(3), 2027-2051.

[49] Bhaiji Y., Understanding, Preventing, and Defending Against Layer 2 Attacks, Cisco,https://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf (Ziyaret tarihi: 20 Ocak 2019).

[50] Dalabasmaz H., Man in the Middle Framework Kullanarak Çalıştırılabilir Dosyalara Arka Kapı Yerleştirme, Bilgi Güvenliği Akademisi, https://www.bgasecurity.com/2014/12/mitmf-man-in-middle-framework/ (Ziyaret tarihi: 20 Ocak 2019).

EKLER

EK-A

```
hostname Yonlendirici1
!
interface GigabitEthernet0/0
 ip address dhcp
 ip nat outside
!
interface GigabitEthernet1/0
 ip address 10.0.1.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet2/0
 ip address 10.0.2.1 255.255.255.0
 ip nat inside
!
router ospf 1
 passive-interface GigabitEthernet0/0
 network 10.0.1.0 0.0.0.255 area 0
 network 10.0.2.0 0.0.0.255 area 0
!
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip nat inside source list 2 interface GigabitEthernet0/0 overload
ip nat inside source list 3 interface GigabitEthernet0/0 overload
ip nat inside source list 4 interface GigabitEthernet0/0 overload
!
ip route 0.0.0.0 0.0.0.0 192.168.122.1
```

```
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 2 permit 192.168.20.0 0.0.0.255
access-list 3 permit 192.168.30.0 0.0.0.255
access-list 4 permit 192.168.40.0 0.0.0.255
!
end
```

EK-B

```
hostname Dagitim1
!
ip dhcp pool LAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
 dns-server 8.8.8.8
 lease infinite
!
ip dhcp pool LAN20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 8.8.8.8
 lease infinite
!
ip dhcp pool LAN30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.254
 dns-server 8.8.8.8
 lease infinite
!
ip dhcp pool LAN40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.254
 dns-server 8.8.8.8
 lease infinite
```

```
spanning-tree vlan 10,20 priority 24576
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0
 no switchport
 ip address 10.0.1.2 255.255.255.0
!
```

```
interface GigabitEthernet3/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet3/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 standby version 2
 standby 1 ip 192.168.10.254
 standby 1 priority 200
 standby 1 preempt
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
 standby version 2
 standby 2 ip 192.168.20.254
 standby 2 priority 200
 standby 2 preempt
!
interface Vlan30
```

```
 ip address 192.168.30.1 255.255.255.0
 standby version 2
 standby 3 ip 192.168.30.254
 standby 3 priority 150
 standby 3 preempt
!
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
 standby version 2
 standby 4 ip 192.168.40.254
 standby 4 priority 150
 standby 4 preempt!
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 10.0.1.1
!
end
```

EK-C

```
hostname Dagitim2
!
ip dhcp pool LAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
 dns-server 8.8.8.8
 lease infinite
!
ip dhcp pool LAN20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 8.8.8.8
 lease infinite
!
ip dhcp pool LAN30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.254
 dns-server 8.8.8.8
 lease infinite
!
ip dhcp pool LAN40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.254
 dns-server 8.8.8.8
 lease infinite
```

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0
 no switchport
 ip address 10.0.2.2 255.255.255.0
!
interface GigabitEthernet3/2
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet3/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby version 2
 standby 1 ip 192.168.10.254
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan20
 ip address 192.168.20.2 255.255.255.0
 standby version 2
 standby 2 ip 192.168.20.254
 standby 2 priority 150
 standby 2 preempt
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
 standby version 2
 standby 3 ip 192.168.30.254
```

```
 standby 3 priority 200
 standby 3 preempt
!
interface Vlan40
 ip address 192.168.40.2 255.255.255.0
 standby version 2
 standby 4 ip 192.168.40.254
 standby 4 priority 200
 standby 4 preempt
!!
router ospf 1
 network 10.0.2.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 10.0.2.1
!
end
```

EK-D

```
hostname Erisim1
!
ip arp inspection vlan 10,20,30,40
!
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip dhcp snooping
!
errdisable recovery cause dhcp-rate-limit
errdisable recovery interval 35
!
interface GigabitEthernet0/0
ip dhcp snooping trust
ip arp inspection trust
!
interface GigabitEthernet0/1
ip arp inspection trust
ip dhcp snooping trust
!
interface GigabitEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security
```

```
 ip dhcp snooping limit rate 4
!
interface GigabitEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security
 ip dhcp snooping limit rate 4
!
end
```

EK-E

```
import sys
import os
import time
import pyautogui
os.system("apt-get install figlet")
os.system("clear")
os.system("figlet ARP Zehirleme Tespit ve Engelleme Araci")
pyautogui.typewrite("-----Tespit Islemi Baslatiliyor------", interval=0.2)
pyautogui.press("enter")
agGecidi_ipadres =net.gateways()["default"][2][0]
print(agGecidi_ipadres)
def macadres(ip_adres):
        vol1,vol2=srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst=ip_adres),timeout=1,retr
y=1)
        for s,r in vol1:
                return r[ARP].hwsrc
                return None
agGecidi_macadres = macadres(agGecidi_ipadres)
while True:
        uyari=" "
        os.system("arp -a | grep -w 192.168.0.2 |cut -d ' ' -f 4 > macListesi.txt")
        MACKontrol=open("macListesi.txt")
        guncelMAC=MACKontrol.read().strip()
        print(guncelMAC)
        if(guncelMAC==agGecidi_macadres):
```

```
        print("Korunuyorsunuz")
else:
        uyari=pyautogui.alert(text="ARP zehirleme atağı başlatıldı. Sisteminiz koruma altına alınmıştır.", title="ARP Uyari Ekrani", button="Tamam")
        islev="arp -s {0} {1}".format(agGecidi_ipadres,agGecidi_macadres)
        os.system(komut)
if(uyari=="Tamam"):
        os.system("clear")
        os.exit()
```

KİŞİSEL YAYIN VE ESERLER

[1] **Yıldız S**., Altınışık U., Yerel Alan Ağlarında Ortadaki Adam Saldırısının Tespit Edilmesi ve Önlenmesi, *Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi*, Kocaeli, 23-25 Kasım 2018.

[2] **Yıldız S**., Altınışık U., Yerel Alan Ağlarının Siber Güvenlik Yönünden GNS3 Ağ Emülasyonu ile İncelenmesi, *TBD Bilişim 35. Ulusal Bilişim Kurultayı,* Ankara, 21-22 Kasım 2018.

[3] **Yıldız S**., Altınışık U., Detecting and Preventing Cyber Attacks on Local Area Networks : A Working Example, *International Journal of Computer Sciences and Engineering*, 2018, **6**(11), 1-6.

ÖZGEÇMİŞ

2010 yılında Karabük Üniversitesi Elektronik ve Bilgisayar Eğitimi Bölümü Bilgisayar Öğretmenliği Programından ve 2015 yılında İstanbul Üniversitesi Bilgisayar Mühendisliği bölümünden mezun olmuştur. 2010-2014 yılları arasında özel sektörün bilgi teknolojileri biriminde görev yapmıştır. 2014 yılı itibari ile Beykoz Üniversitesi Meslek Yüksekokulu Bilgi Güvenliği Programında Öğretim Görevlisi olarak görev yapmaktadır. İlgi alanları siber güvenlik, bilgisayar ağları, ve oyun programlamadır.