
GAZİ ÜNİVERSİTESİ
Gazi
1926

LOG YÖNETİMİ İLE SİBER GÜVENLİK ARAÇLARININ GELİŞTİRİLMESİ

Emre GÜL

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EYLÜL 2019

Emre GÜL tarafından hazırlanan "LOG YÖNETİMİ İLE SİBER GÜVENLİK ARAÇLARININ GELİŞTİRİLMESİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Ercan Nurcan YILMAZ

Elektrik Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi ……..……..

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum

Başkan: Doç. Dr. İbrahim Alper DOĞRU

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi ...……

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye: Dr. Öğretim Üyesi Abdullah ORMAN

Bilgisayar Teknolojileri Bilimi, Yıldırım Beyazıt Üniversitesi ...……

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 17/09/2019

Jüri tarafından kabul edilen bu çalışmanın Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum

……..…….

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

……..
Emre GÜL
17/09/2019

LOG YÖNETİMİ İLE SİBER GÜVENLİK ARAÇLARININ GELİŞTİRİLMESİ

(Yüksek Lisans Tezi)

Emre GÜL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Eylül 2019

ÖZET

Siber saldırılardaki artış, siber dünya içerisinde olan hemen hemen herkesin bilgi güvenliği ve olay yönetimi konusunda yüksek seviyede farkındalığa sahip olmasını zorunlu kılmaktadır. Ayrıca kurumlarda da bu konuda gerekli çalışmaların yapılmasını mecbur hale getirmiştir. Yasal düzenlemeler ve kurumsal politikalar uyarınca, bilgi teknolojilerini içinde barındıran tüm sistemlerde ve bu sistemler üzerinde bulunan uygulamalarda kullanıcıların gerçekleştirdiği tüm işlemler kaydedilmektedir. Günümüzde siber güvenliğin en temel ve önemli birleşenlerinden biri olan bu kayıtlara log ismi verilmektedir. Bilginin gizliliği, bütünlüğü ve erişilebilirliği açısından kritik öneme sahip olan log analizi konusunda temel bilgi sahibi olmak zorunlu bir durum haline gelmiştir. Sistemler ve uygulamalar sürekli ve çok sayıda log üretmektedir. Bu logların analizinin yapılması ve anlamlandırılabilmesi için log yönetimi yapan yazılımlar kullanılmaktadır. Bu yazılımların yetenekleri doğrultusunda suistimal edilebilecek güvenlik açıklıkları ve saldırı girişimleri tespit edilebilir. Yapılan tespitler hakkında sistem ile ilgili sorumlu kişi otomatik olarak uyarılabilir ve gerekli önlemleri alması sağlanabilir. Yapılan bu tez çalışması ile logların yönetim süreçlerinin anlatılması aynı zamanda bilgi güvenliğinin sağlanması için gerçekleşen olayların yönetimi ve sistemlere karşı yapılacak saldırıların önceden tespit edilmesi için log analizinin nasıl yapılması gerektiği üzerinde durulmuştur. Çalışmada tercih edilen log yönetim aracı olan Graylog'un ve kablosuz ağlar için görüntüleme aracı olan NZYME uygulamalarının kullanımı konusunda bilgi sağlamak amaçlanmaktadır.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Log Yönetimi, Graylog, NZYME, Siber Güvenlik, Saldırı Tespiti, Bilgi Güvenliği Farkındalığı
Sayfa Adedi	:	43
Danışman	:	Prof. Dr. Ercan Nurcan YILMAZ

DEVELOPMENT OF CYBER SECURITY INSTRUMENTS WITH LOG MANAGEMENT

(M. Sc. Thesis)

Emre GÜL

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

September 2019

ABSTRACT

The increase in cyber attacks necessitates almost everyone in the cyber world to have a high level of awareness of information security and incident management. In addition, the institutions have made it compulsory to do the necessary work on this issue. In accordance with legal regulations and corporate policies, transactions performed by users are recorded in all systems containing information technologies and the applications on these systems. These records, which are one of the most fundamental and important compounds of cyber security today, are called log. Having basic knowledge of log analysis, which is critical to the confidentiality, integrity and accessibility of information, has become a must. Systems and applications are continuously producing lots of logs. In order to analyze and make sense of these logs, log management software is used. With this software, exploitable vulnerabilities and intrusion attempts can be detected. The person responsible for the system can be automatically alerted about the recognized attack attempts and it can be ensured to take the necessary precautions. In this thesis, it is aimed to explain the management processes of logs as well as to explain the management of events in order to ensure information security and how log analysis should be done in order to detect attacks against systems in advance. The study aims to provide information on the use of Graylog, the preferred log management tool, and nzyme, the imaging tool for wireless networks.

Science Code	:	92403
Key Words	:	Log Management, Graylog, NZYME, Cyber Security, Intrusion Detection, Information Security Awareness
Page Number	:	43
Supervisor	:	Prof. Dr. Ercan Nurcan YILMAZ

TEŞEKKÜR

Tezin hazırlanma aşamasında bana her türlü desteği veren danışmanım Sayın Prof. Dr. Ercan Nurcan YILMAZ'a, değerli katkılarından dolayı çalışma arkadaşım İbrahim Edib KÖKDEMİR ve mesai arkadaşlarıma, yüksek lisans çalışmam boyunca göstermiş oldukları sevgi ve anlayış ile bana destek olan çok değerli Babam, Annem ve Ablam'a sonsuz teşekkürlerimi sunmayı borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ANSI	American National Standart Institute
ASCII	American Standard Code for Information Interchange
CIFS	Common Internet File System
DB	Database
IDS	Intrusion Detection Systems
IP	Internet Protocol
ISO	International Organization for Standardization
JVM	Java Virtual Machine
MBPS	Megabits Per Second
MIB	Merkezi İşlem Birimi
MIMO	Multiple-Input and Multiple-Output)
NFS	Network File System
NMS	Network Management System
RFC	Request For Comments
SCP	Secure Copy Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network

1. GİRİŞ

Günümüzde hemen hemen bulunduğumuz her ortamda siber uzayın içinde yaşamımızı sürdürmekteyiz. Özellikle kişisel kullanımın yanında kurumlarda bilişim sistemlerinde mevcut olan cihazlar ve bu cihazlar üzerinde çalışan uygulamalar, hem yerel hem de geniş ağlar içerisinde diğer sistemler ile etkileşimli olarak çalışmaktadırlar. Bu durum siber güvenlik açısından birçok farklı alanların ayrı ayrı kontrol edilmesi ve geliştirilmesi gerekliliğini ortaya çıkarmaktadır. Bilgi sistemleri yönetimindeki gelişmeler ve oluşan ihtiyaçlar bu alanı bilimsel ve akademik bir araştırma konusu haline getirmiştir ve bu konuda birçok farklı yöntem ve standart oluşturulmuştur. Bilgi güvenliğinin sağlanması amacıyla belli standartlar dâhilinde, kullanılan sistemlerin izlenmesi zorunlu bir durum haline gelmiştir. Alınan tüm önlemlere rağmen kasıtlı veya istemsizce yapılan girişimler, sistemsel hatalar veya yazılımda mevcut olabilecek hatalı kodlamalar nedeniyle, sistemlerde birçok umulmadık durumlar meydana gelebilmektedir. Bunların yanında gelişen teknoloji ile beraber, farklı amaçlar doğrultusunda, sistemler üzerinde etkili olabilecek atak vektörleri oluşmaya devam etmektedir. Saldırıya uğrayan sistemler tarafından üretilen loglar, sistemin güvenliğinin sağlanması hususunda kritik değere sahip olsalar da sistem yönetcileri tarafında gerekli öneme sahip değildirler. Bu durum bilişim sistemleri alt yapılarına yönelik yatırımların doğru bir şekilde kullanılamamasına sebep olmaktadır.

Bilişim sistemleri yönetim süreçlerinin önemli bir bölümünü bilgi güvenliği yönetimi kapsamaktadır. Bilgi güvenliği yönetimi ile bilginin tehlikeye açık halini azaltacak yöntem ve talimatlar oluşturulmaktadır. Bir bilgi güvenliği yönetimi standardı olan ISO 27001 Bilgi Güvenliği Yönetim Standardında log yönetiminin önemi ayrıca belirtilmiştir [1]. Farklı sistemlerden alınan logların bir bütün olarak incelenmesi sonucunda sistemlerin güvenlik durumlarına ait daha kapsamlı ve farklı bir bakış açısı elde edilebilir. Önceden loglara sadece sistemlerde herhangi istenmeyen bir durum meydana geldiğinde veya geçmişe yönelik bir kontrol yapılacağı zaman bakılmakta idi. Ancak günümüzde bilginin bütünlüğünü bozacak herhangi bir eylem veya saldırının önlenebilmesi açısından logların analizinin yapılması büyük önem taşımaktadır.

Log kayıtlarının siber güvenlik alanında kullanılması ile ilgili daha önce bazı çalışmalar yapılmıştır. Snodgrass ve diğerleri [2] saldırıların önlenebilmesi için şifreleme temelli bir

veritabanı yönetim sistemi içerisinde mekanizmalar önermektedir. Yaptıkları çalışmada, kötü niyetli bir kurum çalışanı veya dışarıdan bir saldırganı engelleyen tek yönlü güçlü fonksiyonlar ile veritabanı yönetim sistemi içerisinde meydana gelecek hataların loglarının incelenmesini önermişlerdir. Bu araştırmada Snodgrass ve diğerleri, ayrıca geleneksel sistemlerde logların düzenli olarak kontrolünün yapılmadığını ve bu durumun meydana getirdiği zafiyetten bahsetmişlerdir. Schneier ve Kelsey [3] ise yaptıkları çalışmada log sunucularında sistemlerin log kayıtlarının tutulması için düşük maliyetli bir sistem önermişlerdir. Önerdikleri sistemde, saldırganın log kayıtlarına erişme imkânı bulunmamaktadır. Ancak yapılacak bir siber saldırının öncesinde tespit edilmesi ve önlenmesi ile ilgili herhangi bir geliştirmede bulunmamışlardır. Axelsson ve diğerleri [4] UNIX sistemlerine kolayca uygulanabilir, basit kurulumlu ve maliyeti düşük bir loglama yöntemi sunmaktadırlar. Geliştirdikleri yöntem temel olarak: sistemde gerçekleştirilen tüm işlemlerin ve bu işlemlerden etkilenen diğer sistemlerin loglarını tutmaya dayalıdır. Yazarlar, yaptıkları çalışmada gerçeğine uygun siber saldırı deneyleri yapmış ve bu deneylerden elde edilen verileri kullanmışlardır. Önerdikleri loglama yönteminin diğer sistemlere göre daha az sistem kaynağı tükettiğini savunmaktadırlar. Söderström ve Moradian ise yaptıkları çalışmada [5] güvenli log depolamak için tasarladıkları sistemden bahsetmişlerdir. Sistemlerinde dosya sistemi, veritabanı ve log izleme aracı parallel olarak log depolamak için test edilmiş ve bu sistemler güvenlik, esneklik, performans ve taşınabilirlik özellikleri bakımından karşılaştırılmıştır. Bu tez çalışması kapsamında: ise kurumlarda log yönetiminden sorumlu güvenlik ve sistem yöneticileri ile diğer paydaşların ihtiyaç duyabileceği genel kavramlar, kurallar, düzenlemeler ve diğer çeşitli konular ele alınmıştır. Çalışmanın gerçekleştirilmesi için açık kaynak bir log yönetimi aracı olan Graylog ve yine açık kaynak bir ürün olan kablosuz ağ çerçevelerinin izlenmesini sağlayan NZYME uygulaması kullanılmıştır. Çalışmada iki adet uygulama yapılmıştır. Birinci uygulama kurumlarda yetkisiz erişimlerin tespiti yapılmış, ikinci uygulama da ise bir sibere saldırı senaryo oluşturulmuş ve sonuçları irdelenmiştir. Senaryonun temelini WIFI deauthentication saldırısı oluşturmaktadır ve log analizi ile yapılan bu saldırının tespit edilebileceği gösterilmiştir. Log yönetimi ve siber güvenlik üzerine yapılan diğer çalışmalardan farklı olarak bu tez çalışmasında açık kaynak bir log yönetimi aracı ile kablosuz ağ görüntüle aracı tamamen ücretsiz olarak bir saldırı önleme ve saldırı tespit sistemi gibi kullanılmıştır.

2. LOG KAVRAMI

Log yönetimi ve analizinde kullanılan ifadelerin ve terimlerin çoğu farklı şekilde anlaşılabilir veya yanıltıcı bir anlam içerebilir. Log analizlerinde kullanılan terimlerin ifadeleri aşağı belirtilmiştir.

- Olay, sistemlerde meydana gelmiş herhangi bir değişimdir. Olay içeriğinde olayın nedeni, etkileri, olayın gerçekleştiği zaman aralığı gibi detaylar bulunmaktadır.
- Olay alanı, olayın gerçekleştiği sistemin tanımıdır. Olayın kaynak ve hedef bilgilerini içerir.
- Olay kaydı, sistemlerde meydana gelen hareketlerin tümünün ayrı ayrı tutulduğu kayıtlardır.
- Log, bir kurumun sistemlerinde ve ağlarında meydana gelen olay kayıtlarına denilmektedir [6].
- Loglama, logların merkezi bir yerde tutulması işlemidir.
- Güvenlik vakası, sistemlere yetkisi bulunmayan kişiler tarafından erişilebilme veya yetkili kişilerin manipülasyon ve kötü amaçlı kullanımlarıdır.
- Uyarı veya alarm, Sistemlerde meydana gelen ve normal olmayan olaylarda daha önceden bu tür olaylar için yapılan ayarlamalar doğrultusunda otomatik olarak sistem tarafından yapılan uyarılardır.

2.1. Gerekliliklerine Göre Loglama Türleri

Sistemlerin log üretmesinin 4 temel sebebi bulunmaktadır.

- Güvenlik Loglama: Siber saldırı girişimlerinin tespit edilmesi amaçlı üretilen loglardır. Bu loglama türüne örnek olarak: yetkisiz erişim olayları verilebilir. Tez çalışmasının uygulama alanında yetkisiz erişim örnekleri verilmiştir.
- Operasyonel Loglama: Sistem yöneticilerine, sistemlerde meydana gelen hatalar ve gerçekleşen diğer işlemler hakkında bilgi sağlamak amacıyla üretilirler.
- Uyumluluk Loglama: Sistemleri ve verileri daha güvenli bir hale getirmek için yapılan yasal düzenlemelere uyum amacıyla tutulan loglardır. Ülkemizde 5651 no'lu yasa

kapsamında kurumlar en az 2 yıl önceki log kayıtlarını eskiye dönük olarak saklamak mecburiyetindedir.

- Hata Ayıklama Loglama: Bu tür loglar sistem üreticileri tarafından kullanılırlar. Sistemleri kullanan sistem yöneticilerinin anlayabileceği loglar değildir. Bu loglar sistemlerde genelde kullanım dışıdır, ancak eğer istenilirse sistem üreticileri tafından etkinleştirilebilir. Sistemin kaynak kodlarına sahip sistem üreticileri tarafından analiz edilebilen loglardır.

Yukarıda tanımlanmış loglar sistemler tarafından üretilirler; ancak farklı sistem ve kişiler tarafından analiz edilirler.

2.2. Loglama Süreçleri

Loglamanın mantıksal olarak dört farklı süreci vardır.

- Log iletimi
- Log biçimi
- Log içeriği (taksonomi)
- Log konfigürasyonu

2.2.1. Log iletimi

Log mesajlarının üretilen sistem üzerinden merkezi log sunucusuna iletimidir. Syslog protokolü gibi iletim protokolleri bulunmakla beraber kendisine özgü iletim protokolü bulunmayan loglama yöntemleri de mevcuttur. Log iletim protokolünde log bilgisinin bütünlüğü, erişilebilirliği ve gizliliği korunmalıdır. Bu aşamada log bilgisinin olay akışının sıralaması da muhafaza edilmelidir. Burada en önemli husus ise log bilgilerinin doğru zaman damgası ile tutulmasıdır.

Genel olarak kullanılan bazı log iletim protokolleri aşağıda belirtilmiştir.

- Syslog
- Simple Network Management Protocol
- Simple Object Access Protocol
- Secure Copy Protocol, Common Internet File System, Network File System vb.

Syslog, ağ cihazlarının olay kayıtlarını bir log sunucusuna gönderme yoludur. Syslog protokolü, geniş bir cihaz yelpazesi tarafından desteklenir ve farklı olay türlerini log olarak kaydetmek için kullanılabilir. Örneğin, bir yazıcıdan çıktı alınırken, yazıcı tarafından üretilen loglar syslog ile log sunucusuna iletilir [7].

Router, switch, güvenlik duvarı, yazıcılar, Apache web sunucuları gibi birçok ağ cihazı Syslog mesajı gönderebilmektedir. Windows tabanlı sunucular Syslog'u desteklemez, ancak çok sayıda üçüncü parti ürün ile Windows tabanlı sunucularda da Syslog desteklenebilir hale gelebilmektedir [8].

2.2.2. Log biçimi

Log dosyaları farklı biçimlerde söz dizilimlerine sahiptir. Yapı olarak logların söz dizilimleri Türkçenin söz dizilimine benzemektedir. Çizelge 2.1'de yaygın olarak kullanılan loglama mekanizmalarının karşılaştırılması gösterilmektedir.

Çizelge 2.1. Loglama mekanizmalarının karşılaştırılması [9].

	XML Loglama	Syslog Loglama	Metin Dosyası Loglama	Tesciili Loglama
Okuma şekli	Genellikle makine tarafından anlaşılabilir.	Genellikle el yardımı ile anlaşılabilir	Sadece el yardımı ile anlaşılabilir	Sadece makine tarafından anlaşılabilir
Yaygın kullanım	Güvenlik amaçlı loglama	İşlem loglaması hata loglaması	Hata loglaması	Performans gereksinimi yüksek loglamalar
Örnekler	IPS	Router ve Switch	Uygulamalar	Firewall
Uyarı	Yapılandırılmış logların iletiminde	İncelemeyi basitleştirmek için ad, değer benzeri bir ifade eklenebilir	Operasyonlar sırasında belirginleştirici bir yapı eklenmelidir.	Performansın önemli olduğu durumlarda kullanılır
Olumsuzlukları	Log mesajının boyutu yüksek olduğu için performansı düşürür	Yapısı bulunmadığı için analiz performansını düşürür	Loglar genelde sadece uygulamayı geliştiren kişiler tarafından anlaşılabilabilir	İkili mesaj yapısına döndürmeden okunamaz

Log mesajlı farklı bilgi alanlarını barındırır ve yaygın olarak kullanılan alanlar aşağıda belirtilmiştir.

- Meydana gelme zamanı
- Türü
- Üretildiği kaynak sistem
- Sonuç göstergesi
- Logun kritikliği
- Operatör bilgisi

Log analiz uygulamaları çeşitli logların biçimlerini tanımlamak için mesaj şemaları oluşturmaktadır. Oluşturulan bu şemalar uygulamalar, sistemler, cihazlar log için uygundur.

2.2.3. Log içeriği (Taksonomi)

Log taksonomisi, loglanan olayları kategorize etmek demektir. Eğer bir biri ile eş iki olay farklı sistemler tarafından loglanırsa bu logların taksonomilerinin bir birleri ile aynı olması gerekmektedir.

log taksonomileri için günümüzde tanımlanmış bir standart mevcut değildir. Piyasada mevcut olan log analizi ürün üreticileri bu ürünler için log taksonomisi oluşturmaktadırlar. Ancak farklı üreticiler farklı formatlara sahip taksonomiler oluşturdukları için genel olarak kullanılan standart bir taksonomi bulunmamaktadır [9,10].

2.3. Loglama Kriterleri

Log içeriğinin eksik olduğu veya loglanan bilginin faydasız bulunduğu durumlar mevcuttur. Siber saldırılara karşı hangi önlem alabilmek için log içeriğinde hangi bilgilerin bulunması gerektiği önem arz eden bir konudur.

Loglar saldıralara karşı savunma yapabilmek için aşağıdaki bilgileri içermelidir.

- Gerçekleşen olay?
- Olayın gerçekleştiği yer?
- Olayın gerçekleştiği zaman?
- Olayı gerçekleştiren kişi?

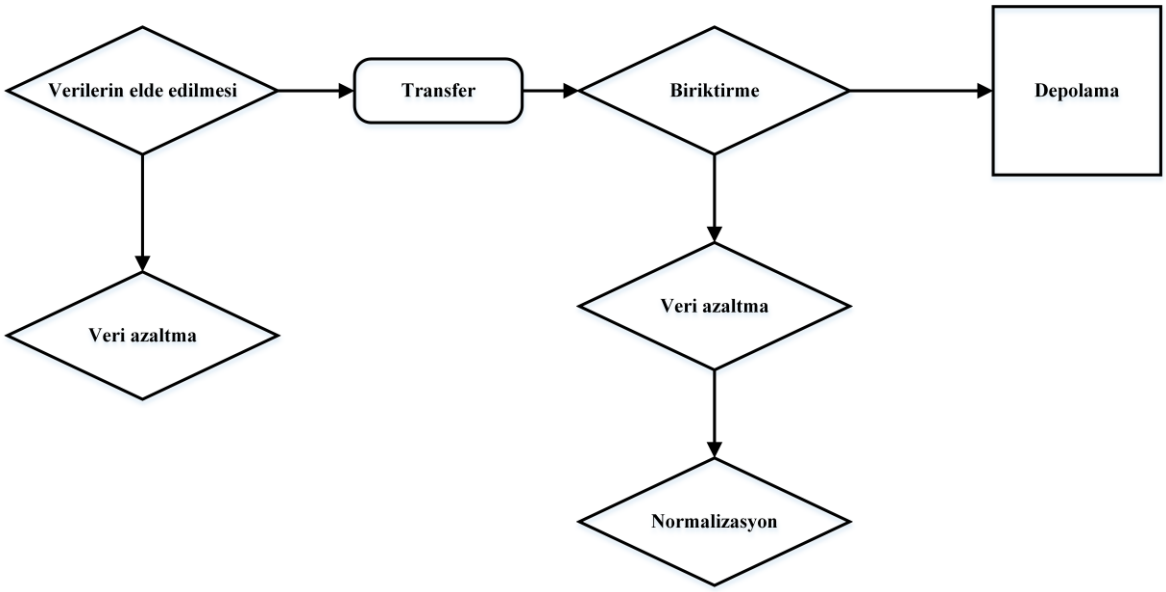
Yukarıda belirtilen bilgiler log mesajının içeriğinde olmazsa olmaz bilgilerdir. Ayrıca gerçekleşen olayın tam olarak anlaşılabilmesi için aşağıda belirtilen bilgilerin de bilinmesi gereklidir.

- Gerçekleşen olaydan etkilenen nedir?
- Gerçekleşen olay ile ilgili hangi kaynaktan bilgi edinilebilir?
- Gerçekleşen olay ile ilgili bilgilerin doğruluğundan nasıl emin olunabilir?
- Gerçekleşen olayın sonuçları ne olacak?
- Gerçekleşen olay ile ilgili hangi önlemlerin alınması gereklidir?
- Gerçekleşen olayın etkilerini en aza indirebilmek için nelere dikkat edilmelidir [10].

2.4. Log Analizi

Bilişim sistemlerinin alt yapısında mevcut olan sunucu, istemci ve ağ cihazları gibi tüm yapılar üzerinde yürütülen işlemler hakkında kayıt yapma özelliğine sahiptir. Bu kayıtların analizi yapılarak sistemler üzerinde mevcut güvenlik olaylarının belirlenmesi ve bir bilgi güvenliği ihlal olayı var ise, bu duruma karşı önlem alınması sağlanmaktadır. Bu yapılan çalışmaya log analizi denilmektedir. Log analizi ile sistemlere dışarıdan veya içeriden yapılan saldırlar tespit edildiği gibi aynı zamanda sistemlerdeki mevcut kullanıcıların yaptıkları işlemlerin de kayıt altına alınması ve gözlemlenmesi mümkündür.

Log analiz sürecinde öncelikle logun hangi sistem veya uygulama tarafından üretildiğinin, yani log kaynağının ne olduğunun anlaşılması gerekmektedir. Bazı sistem veya uygulamalarda log gönderimi otomatik olarak yapılırken, bazılarında log gönderimi için farklı ayarların yapılması gerekmektedir. Uygulama veya sistem log gönderse bile karşısında bu gönderdiği logları alacak hiçbir şey bulamayabilir [11].



Şekil 2.1 Log verilerinin toplanmasının yaşam döngüsü

Loglar, logları oluşturan sistemin kendi üzerinde veya bir başka sisteme aktarılarak tutulabilir. Şekil 2.1'de log verilerinin elde edilme süreci gösterilmiştir. Tüm sistemlerde oluşturulan logların tek bir ortamda kaydedilmesi işlemine log depolaması denilmektedir [12]. Log kayıtlarının yönetimi aşağıda belirtilen nedenlerden dolayı zorlaşmaktadır.

- Birden çok sistem tarafından çok sayıda ve büyüklükte üretilen loglar,
- Farklı sistemlerden farklı türde logların oluşturulması,
- Log içeriklerinin birbirinden farklı olması.

Log kayıtlarının değerlendirilmesi süreci, çok sayıda event (olay-hareket) kaydının yer alacağı ortamlarda, bu konuda çalışanı, verilerin ele alınması ve yönetilmesinin zorluğu ile karşı karşıya bırakacaktır [12]. Hangi sistemlerden veya uygulamalardan gelen logların ne sıklıkla okunacağı, hangi atak türlerinde sistemlerin/uygulamaların nasıl ve ne sıklık ile log ürettiği hakkında bilgi/deneyim eksikliği de bir sorun olarak karşımıza çıkmaktadır. Sadece siber atakların değil, sistemlerdeki diğer çeşitli hataların çözülmesi de log analizi ile mümkün olabilmektedir. Mevcut log dosyaları sistemler hakkında belli ölçülerde görünürlük sağlarlar. Log dosyaları yorumlanırken, sistemler ve uygulamalar üzerinde gelişen eylemlere farklı yaklaşımlarda bulunulması, yeni olayların farkına varılması için önemlidir. Logların bütün olarak incelenmesi ve karşılaştırması ile bütünleşik bir bilgi elde edilebilir. Eğer olaylar bütün olarak ele alınmaz ve yeterli bir şekilde analiz edilmez ise, bu olayların etkisi ve önemi açığa çıkartılmayabilir [13].

2.5. Loglama Yöntemleri

Loglama yöntemleri genel olarak iki kategoriye ayrılır.

- Ajansız yöntem
- Ajanlı yöntem

2.5.1. Ajanlı yöntem:

Avantajları: Bu yöntemde logların depolandığı log sunucusu çalışmıyor durumda olduğu zamanlarda bile bilgi kaybı yaşanmamaktadır. Log sunucusu, istemcinin kapalı mı açık mı olduğunu anlayabilir.

Dezavantajları: Ajanlı yöntemde log alınması istenilen sistemlerde ayarlama yapılması gerekmektedir. Eğer sistem kötü niyetli kişiler tarafından başarılı bir saldırıya uğrarsa ajan tarafından sistem loglarının gönderilmesi kapatılabilir.

2.5.2. Ajansız yöntem:

Avantajları: Sistemden log alabilmek için ayarları hızlı ve kolay bir şekilde yapılabilir. Dolayısıyla çok büyük sistemler tarafından kullanılması mantıklıdır.

Dezavantajları: Ajansız yöntemde Syslog protokolü kullanılmaktadır. Syslogda ise UDP kullanıldığı için log bilgisinin karşı tarafa kesin olarak gönderilip gönderilmediği bilinemez ve bilgi kaybı yaşanabilir.

Ajansız yöntem ile sistem tarafından sunucuya log mesajı gönderilir. Ağ üzerinde gönderilen bu mesajı log sunucusu alır. Mesajın iletilmesinde kullanılan üç farklı protokol mevcuttur: Bunlar Syslog, Snmp ve Windows Olay Günlüğü protokolleridir [13]. Aşağıda bu protokoller ile ilgili detaylı bilgi verilmiştir.
Bir diğer yöntem olan ajanlı yöntemde ise log mesajı uygulama tarafından kaynaktan alınır.

2.6. Syslog

Syslog, Sistem Günlüğü Protokolü anlamına gelmektedir. Sistem loglarını veya olay mesajlarını syslog sunucusuna göndermek için kullanılan standart bir protokoldür. Öncelikli olarak, izleme ve gözlemleme için merkezi konumda bulunan birkaç farklı makineden çeşitli cihaz loglarını toplamak için kullanılır [13].

Bu protokol routerlar, switchler, güvenlik duvarları ve hatta bazı yazıcı ve tarayıcılar gibi çoğu ağ donanımında etkindir. Ek olarak, Syslog Unix ve Linux tabanlı sistemlerde ve Apache dâhil birçok web sunucusunda kullanılabilir. Syslog, varsayılan olarak Windows tabanlı sistemlere yüklenmemektedir. Bu olaylar üçüncü parti programları veya Syslog protokolü kullanan farklı yapılar aracılığıyla iletilebilmektedir. Syslog protokolü RFC 5424'de tanımlanmıştır [14].

Syslog Bileşenleri: Her bir cihazda, değişen koşulları takip edip gözlemlemek için sistem tarafından çeşitli olaylar üretilir. Bu olaylar bir yönetici tarafından incelenip analiz edilebilmeleri için kaydedilmektedir. Bununla birlikte, çok fazla miktarda router, switch ve sistemler üzerinden logların izlenmesi, takip edilmesi zaman alıcı olmakla beraber pratikliğini de kaybetmektedir. Syslog, bu olayları merkezi bir sunucuya ileterek çok sayıda cihazın gözlemlenmesi sorununu ortadan kaldırmaktadır [15].

Syslog İletimi: Syslog 514 portundan UDP protokolünü kullanarak çalışmaktadır, ancak herhangi bir portdan çalışmak için de yapılandırılabilir. Ek olarak, bazı cihazlar onaylı ileti teslimini almak üzere Syslog verilerini göndermek için TCP protokolünü 1468 portundan kullanabilmektedir.

Syslog paket iletimi eşzamansızdır. Bir Syslog mesajının oluşturulma işlemi router, switch veya sunucunun kendisinde yapılandırılmıştır. SNMP gibi diğer izleme, gözlemleme protokollerinden farklı olarak, sistem log verilerini sorgulama mekanizması yoktur. Bazı uygulamalarda, SNMP, Syslog parametrelerini uzaktan ayarlamak veya değiştirmek için kullanılabilmektedir.

Syslog mesaj formatı: Syslog mesajı üç kısımdan oluşmaktadır: PRI (hesaplanmış öncelik değeri), HEADER (tanımlayıcı bilgilerle birlikte) ve MSG (mesajın kendisi).

Syslog protokolü aracılığıyla gönderilen PRI verileri, mesajı kategorize etmeye yardımcı olan iki sayısal değerden gelir. Birincisi Facility (Tesis) değeridir. Bu değer mesaj türünü veya olayı hangi sistemin oluşturduğunu sınıflandırmaktadır. İkinci değer ise mesajın önemini veya ciddiyetini 0'dan 7'ye sınıflandıran sayısal bir değerdir.

Her iki kısmın da değerleri kesin tanımlara sahip değildir. Bu nedenle, bir olayın (uyarı, bildirim, alarm gibi) nasıl loglanacağını ve hangi sisteme kaydedileceğini belirlemek sisteme bağlıdır.

Bu iki değer, mesajla birlikte gönderilen bir Öncelik Değeri (PRI) üretebilmek için birleştirilmektedir. Öncelik Değeri, Tesis değerinin sekiz ile çarpılması ve ardından Önem Değerinin sonuca eklenmesiyle hesaplanmaktadır. Öncelik Değeri ne kadar düşük olursa, önceliği o kadar yüksek olmaktadır [15].

2.7. SNMP

Ağdaki yönetilen cihazlar hakkında bilgi toplamak ve düzenlemek ve bu cihazların davranışını kontrol etmek için kullanılan protokoldür. Genellikle SNMP'yi destekleyen cihazlar arasında modemler, routerlar, switcher, sunucular, iş istasyonları, yazıcılar bulunur. SNMP, ağ izlemede ve ağ yönetiminde geniş bir yelpazede kullanılmaktadır. SNMP protokolünün üç farklı sürümü geliştirilmiş ve yaygınlaştırılmıştır. SNMPv1 protokolün orijinal sürümüdür. Yeni sürümler olan SNMPv2 ve SNMPv3 performans ve güvenlik açısından daha elverişlidir [16].

2.8. Windows Olay Günlüğü

Window Olay Günlüğü, Microsoft'un Windows işletim sistemlerinde, yöneticilerin ve kullanıcıların olay günlüklerini yerel veya uzak bir makinede görmelerini sağlayan bir bileşendir.

Uygulamalar ve işletim sistemi (OS), yöneticinin işletim sistemiyle ilgili sorunlarını inceleyip gidermek için kullanabileceği önemli donanım ve yazılım eylemlerini, hareketlerini kaydetmek için bu olay günlüklerini kullanmaktadır. Windows olay günlükleri, uygulama yüklemeleri, güvenlik yönetimi, başlangıçtaki sistem kurulum işlemleri ve sorunlar veya hatalar gibi belirli olayları yazmaktadır [17].

2.9. Log Yönetim Araçları

Log analizi bilişim süreçlerinde ne olduğunu anlamamıza yardımcı olur ve sistemlerde meydana gelen olayların izlenmesi, değerlendirilmesi ve varsa sorunların çözümü için rehberlik eder. Log yönetimi araçları büyük boyutlardaki log verilerinden kolaylıkla bilgi edinmemize yardımcı olur. Bu araçlar tüm verileri birleştirir ve merkezi, erişilebilir ve kullanımı kolay bir arayüz ile yönetmemize imkân tanır. Böylece veriler tek bir yerde toplanır, saklanır ve verimli bir şekilde yönetebiliriz. Log yönetim araçları ile mevcut log verilerinden faydalı eğilimler çıkartılabilir. Siber saldırı gibi zor bir durum ile karşı karşıya kalındığında ortamda mevcut txt dosyalar ile uğraşmak yerine log yönetim aracı kullanmak daha kolaydır. Tek bir sorgu ile bu araçların yardımı ile herhangi bir uygulama veya yazılımın kök nedeni belirlenebilir. Log yönetimi ile bir siber saldırı gerçekleşmeden önce vereceği zararlar en aza indirilebilir. Aşağıda yer alan Çizelge 2.2.'de popüler log yönetim araçlarının mevcut avantajları ve dezavantajları belirtilmiştir.

Çizelge 2.2. Log yönetim araçlarının avantajları ve dezavantajları

Log Yönetim Aracı	Avantajları	Dezavantajları
Splunk	Dâhili alarm ve raporlama aracı	Kurulumu ve yeni kaynaklar eklenmesi kolay değil. Her bir yeni kaynak manuel olarak eklenmeli
	Yapılandırılabilir grafikler ve gösterge tabloları	Ücretli
	SaaS çözümü	
	Tek bir sunucudan birden çok veri merkezine veri aktarımı	
	Gerçek zamanlı arama, analiz ve görselleştirme Çok hızlı indeksleme imkanı sağlar Bu durum kullanım rahatlığı oluşturur. Kodlama bir log yönetim aracı için önem arz etmektedir. Bu yönetim aracında yer alan gerçek zamanlı arama analiz ve görselleştirme ise log yönetim aracının indekslemesinin çok hızlı yapıldığından kaynaklanmaktadır.	

Çizelge 2.2. (Devamı) Log yönetim araçlarının avantajları ve dezavantajları

Log Yönetim Aracı	Avantajları	Dezavantajları
LogPacker	100'den fazla log tipi için destek sağlamaktadır.	Web arayüzü mevcut değil
	Birden fazla depolama sağlayıcısı imkânı sunar	Ücretli
	e-Posta, Slack veya SMS ile uyarı ve raporlama sistemi	
	Paketler üzerinden kolay kurulum	
	Güvenilir cluster yapısı	
	Geniş platform desteği: Unix, Windows, Mobile, JS	
	Kaydedilen verilere dayalı özel çözümler oluşturmak için REST API	
	Olayları toplama, çözümleme ve güvenlik	
	Yüksek performans	
	Disk tabanlı bulut kontrol paneli	
LogRhythm	Gerçek zamanlı akıllı arama	Yüksek maliyet
	Uygulamalar ve veritabanlı dâhil olmak üzere yaklaşık 700 kaynaktan log toplar	Şeffaf olmayan kullanıcı kılavuzu ve dokümantasyonu
	Gerçek zamanlı izleme ve esnek, rol tabanlı uyarılar.	
	Herhangi bir aramadan tek tıkla korelasyon	
	Konsol, kullanıcıların verileri hızlı bir şekilde ilişkilendirmesini, aramasını ve verilerini hızla döndürmesini sağlar.	
Logentries	Birden fazla PaaS ve IaaS ile çalışır.	Manuel kurulum ve manuel log kaynakları yönetimi.
	Gerçek zamanlı akıllı arama	3. parti kütüphanelerinde hataların kaynağı izlenemiyor.
	Loglara özel etiketler	Yeterince güvenli olmayan web istemcisi loglaması
	Arama için SQL Benzeri Sorgu Dili (LEQL).	JavaScript için özel bir raporlama mevcut değil.
	e-Posta raporları	
	Çeşitli programlama dilleri grubunu destekler. Farklı kodlarda ve arayüzlerde kod çalıştırılabilir. Kod farkındalığı yüksek bir log yönetim aracıdır	

Çizelge 2.2. (Devamı) Log yönetim araçlarının avantajları ve dezavantajları

Log Yönetim Aracı	Avantajları	Dezavantajları
	Ücretsiz ve açık kaynak	Az sayıda log türleri için destek
	Akışlar, olayları gerçek zamanlı olarak tanımlamayı ve eylemleri gerçekleştirmeyi sağlar.	
	Kolay kurulum	
	Sunucu tarafı işlevselliği eklentiler aracılığıyla genişletilebilir.	
Graylog	Ücretsiz ve açık kaynak	Az sayıda log türleri için destek
	Akışlar, olayları gerçek zamanlı olarak tanımlamayı ve eylemleri gerçekleştirmeyi sağlar.	
	Kolay kurulum	
	Sunucu tarafı işlevselliği eklentiler aracılığıyla genişletilebilir.	
	Rest API	
	Kullanıcılar ve rolleri için özel izin yönetimi.	
	Kapsamlı bir işlem algoritması kullanarak loglar zenginleştirilebilir ve ayrıştırılabilir.	
	Günlük verilerinin ve sorguların görsel çıkışı için özel panolar.	
	Sezgizel arama arayüzü	
Scalyr	Kolay kurulum ajahı veya API	Ücretsiz bir sürümü mevcut değil
	Heroku, Amazon RDS veya Amazon CloudTrail'den günlükleri içe aktarabilme	Bulut çözümü yok
	Özelleştirilebilir grafikler	
GoAccess	Terminal ortamındaki milisaniye içindeki günlük verilerini günceller.	Zor kurulum
	Özel günlük dizeleri.	Sunucu ve İstemciler ile entegrasyon mevcut değil
	Sayfaları yanıt süreleri için izleyin; uygulamalar için ideal.	

3. KABLOSUZ AĞLAR VE KABLOSUZ AĞ SALDIRILARI

Günümüzde kablosuz ağların kullanımı giderek artmaktadır. Kablosuz ağlar havaalanları, kafeteryalar, kamu kuruluşları ve neredeyse her evde kullanılmaktadır. Kablosuz ağlar kullanım açısından kolaylık sağlasa da güvenlik açısından birçok risk barındırmaktadır [18]. Kablosuz ağların avantajları:

- Kablo dağınıklığı ve kablolama sorunlarını ortadan kaldırmıştır.
- Cep telefonları, tabletler ve diğer akıllı cihazların kullanımı ile uyumludur.
- Haberleşmeyi kolaylaştırmıştır ve daha pratik bir hale getirmiştir.

Kablosuz ağların dezavantajları

- Düşük bant genişliğine sahiptirler.
- Saldırganlar tarafından kablolu ağa göre daha fazla suistimal edilebilir olması.

3.1. Kablosuz Ağ Standartları

802.11a: 802.11 in artık yetmemesi sebebiyle 2000'li yıllarda kullanılmaya başlanmıştır. 5GHz frekans aralığında çalışmaktadır. 54Mbps veri aktarım hızı sunar. Bununla birlikte erişim mesafesi açık alanlarda 80 metrenin üzerine çıkabilmektedir. Kanal hacmi birden fazladır böylece daha büyük bant genişliği sunmaktadır [19].

802.11b: 802.11a ile birlikte kullanıma sunulmuştur. 2.4 GHz frekans bandından çalışmaktadır ve 11 Mbps veri aktarım hızı ile çalışır.

802.11g: 2004 yılının başlarında kullanıma açılan üçüncü nesil bir kablosuz ağ teknolojisidir. 2.4 GHz frekans aralığında çalışmaktadır. Veri aktarım hızı 54 Mbps'dir ve açık alanlarda 150 metreye kadar bağlantı imkânı tanımaktadır.

802.11n: MIMO teknolojisini kullanarak gönderilen veya alınan paketlerde işlemleri parçalar haline ayırır ve böylece daha hızlı bir şekilde haberleşme sağlamaktadır. Haberleşme hızı 500 Mbps'nin üzerine çıkabilmektedir. Açık ortamlarda 300 metreye kadar iletişim ağı oluşturabilmektedir [20].

3.2. Kablosuz Ağ Terimleri

Erişim Noktası (Access Point): Kablosuz bağlantıların WLAN oluşturabilmesi için geliştirilmiş araçlardır.

Hizmet Kümesi Tanımlayıcı (SSID) : Kablosuz ağın adıdır.

BSSID (Basic Service Set Identifier): Her kablosuz aygıt için aygıtın MAC adresidir.

PWR (POWER): Ethernet kartı tarafından bildirilen sinyal seviyesidir.

Beacons: Erişim noktaları (Access Point) tarafından gönderilen duyuru paketlerinin sayısıdır.

Data: Ethernet kartı tarafından yakalanan bilgi paketi sayısıdır.

#/s: Son 10 saniyede ölçülen saniyede geçen toplam veri paketi sayısıdır.

CH: İşaret (Beacon) paketlerinden alınan kanal numarasıdır.

MB: Erişim noktası (Access Point) tarafından desteklenen maksimum hız değeridir.

ENC: Kullanılan şifre algoritmasıdır.

CIPHER: Algılanan şifrenin türünü belirtmektedir.

AUTH: Kullanılan kimlik doğrulama protokolüdür.

ESSID: Kablosuz ağ adını göstermektedir. SSID adı etkin ise boş bırakılabilir.

Çerçeve (Frame): Kablosuz ağlarda iletişim çerçeveler ile yapılır.

Probe: Ağa bağlanmak isteyen istemcilerin gönderdiği pakettir.

Probe Replay: Erişim noktalarının istemciye döndüğü cevaptır.

İstasyon (Station): Kablosuz ağa bağlanacak bilgisayarlar, cep telefonları, tabletler vb. cihazların tümüne verilen isimdir.
Kanal (Channel): 11 adettir ve kablosuz haberleşmenin gerçekleştiği yerdir. Aynı kanalda bulunan iki sisteminin haberleşmesi daha verimli olur.

Doğrulama (Authentication): Kablosuz bir ağa bağlanmadan önce istemcinin doğrulanması istenir.

İş birliği (Association): İstemcinin kablosuz ağa bağlanabilmesi için erişimin verilmesidir.

WEP: En basit şifreleme türüdür. Güvensiz olduğu için günümüzde neredeyse hiç kullanılmamaktadır.

WPA: Dinamik anahtar ile şifreleme yöntemidir. WEB'e göre daha güvenlidir.

WPA2: WPA'dan daha gelişmiş AES şifrelemesi de kullanan protokoldür. Zayıflıkları WPS pin açıklığıdır. WPS pin kilidi aktif olmayan modemler bu saldırıya maruz kalmaktadır [21].

Geçici Anahtar Bütünlüğü Protokolü (Temporal Key Integrity Protocol / TKIP): Statik anahtar yerine her paketin farklı bir anahtarla gönderilmesini sağlar [22].

3.3. Kablosuz Ağlarda Paket (Frame) Yapısı

Kablosuz ağlarda kullanıcı ile erişim noktası arasındaki iletişimi sağlamak için 802.11 de kullanılan üç ayrı paket tipi mevcuttur. Bu paketler aşağıd a detalı olarak anlatılmıştır.

3.3.1. Management frame

802.11 management frameleri ağ üzerinde iletişimi başlatmak ve kurulan bu iletişimin sürekliliğini sağlamak için kullanılmaktadır. Bu paketler aşağıda detaylı olarak ifade edilmiştir.
Authentication Frame: Bu paket ağ üzerinde istemcinin kimliğini doğrulamak için kullanılmaktadır [23].

Deauthentication Frame: Erişim noktası ile istemci arasındaki mevcut iletişimin bitirilmesi istenildiğinde bu paket gönderilir.

Association Request Frame: Bu paket içerisinde SSID bilgisi taşınır.

Association Response Frame: Erişim noktası tarafından istemcinin bağlantı teklifi kabul veya reddedilebilir. Eğer bağlantı teklifi erişim noktası tarafından kabul edilirse client bu ağa artık erişim sağlayabilir.

Beacon frame: IEEE 802.11 tabanlı WLAN'lardaki yönetim paketlerinden biridir. Ağla ilgili tüm bilgileri içerir. Beacon çerçeveleri periyodik olarak iletilir, kablosuz bir LAN varlığını duyurmak ve servis grubunun üyelerini senkronize etmek için kullanılırlar. Beacon çerçeveleri, erişim noktası (AP) tarafından bir altyapı temel servis setinde (BSS) iletilir. IBSS şebekesinde işaret üretimi istasyonlar arasında dağıtılmıştır. 2.4 GHz spektrumu için, üst üste binen kanallarda (veya toplamda 45'ten fazla) 15'ten fazla SSID'ye sahip olması ve işaret çerçeveleri, çoğu şebeke boştayken bile önemli miktarda hava süresi tüketmeye ve performansı düşürmeye başlar [24].

3.3.2. Control frame

Kullanıcı ve erişim noktasının iletişimde paketlerin iletilmesini sağlarlar. 3 farklı kontrol çerçevesi mevcuttur

- Request to Send (RTS) frame:.
- Clear to Send (CTS) frame
- Acknowledgement (ACK) frame:

3.3.3. Data Frame

Kablosuz bağlantılarda bilgiyi taşımak için kullanılır.

3.4. Kablosuz Ağlarda Atak Vektörleri

3.4.1. Sahte bağlantı noktası (hotspot) tehditi

Aynı ağ içerisindeki kullanıcılar birbirlerine ulaşım sağlayabilirler. Bu nedenle saldırganlar saldırı yapacakları kişi ile aynı ağda olmaya çalışırlar. Bu saldırı yönteminde kurban önce ağdan düşürülür. Daha sonra ise kurbanın önceden bağlı olduğu SSID ile aynı numaraya sahip saldırgan tarafından oluşturulan sahta erişim noktasına bağlanması amaçlanır [25].

3.4.2. Kimlik doğrulamayı kaldırma (deauthentication) WPA atak

Çoğu kablosuz ağ kilitleyicisinin aksine, Kimlik Doğrulamayı Kaldırma (Deauthentication) benzersiz bir şekilde hareket eder. IEEE 802.11 (Wi-Fi) protokolü bir kimlik doğrulama çerçevesinin hazırlanması için bir hüküm içerir. Çerçeveyi erişim noktasından bir istasyona gönderme “sahte bir istasyonu ağdan kopuk olduklarını bildiren onaylanmış teknik” olarak adlandırılır.

Bir saldırgan, kurban için sahte bir ağda bulunan herhangi bir zamanda bir kablosuz erişim noktasına bir deşifre paketi gönderebilir. Protokol, veri gizliliği için oturum WEP ile kurulduğunda bile bu paket için herhangi bir şifreleme gerektirmez ve saldırganın yalnızca kablosuz ağ bağlantısı yoluyla açık olan mağdurun MAC adresini bilmesi gerekir [25].

4. GRAYLOG VE NZYME

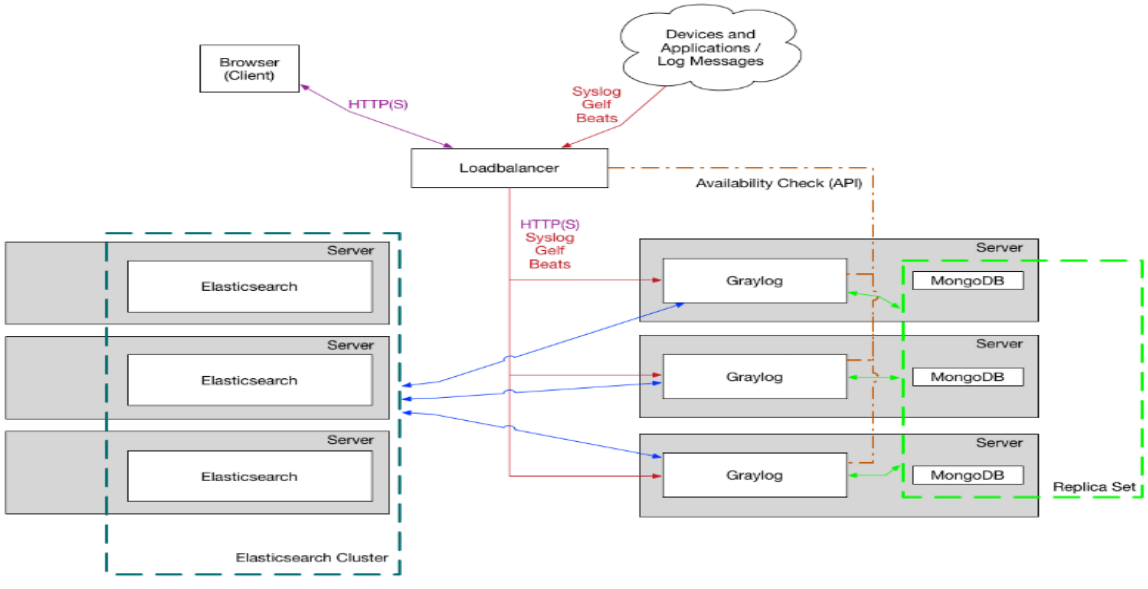
4.1. Graylog

Graylog, yapılandırılmış veya yapılandırılmamış verilerin hemen hemen her kaynaktan toplanması, dizine eklenmesi ve analiz edilmesi için tamamen bütünleşmiş bir açık kaynak bir platformdur. 2010 yılından beri geliştirilmektedir. Xing geliştirilmesine destekleyici olmuştur.

Graylog uygulama birleşenleri:

- Graylog sunucusu
- Graylog wep arayüzü
- Mango DB
- ElasticSearch

Graylog uygulaması Java ile geliştirilmiştir. Mesajları ElasticSearch üzerinde depolar. İstatistikleri ve grafikleri MangoDB üzerinde saklamaktadır. İç mesaj kuyruklama sistemi mevcuttur. Gecikmeli veya toplu indeksleme yapabilmektedir. IT dünyasında yer alan programlar, bash scriptleri, syslog vb. hemen her yerden logları alınabilinir ve bu logların takibi web arayüzü üzerinden yapılabilir [26]. Graylog toplama mimarisi Şekil 4.1'de görülmektedir [26].



Şekil 4.1. Graylog log toplama mimarisi.

4.2. NZYME

Nzyme, 802.11 yönetim frame'lerini doğrudan havadan toplar ve bunları WIFI IDS izlemek için Graylog uygulamasına gönderir. Nzyme, sadece bir sanal makine ve monitör modunu destekleyen bir WIFI adaptöre ihtiyaç duyar.

Nzyme, tüm ilgili 802.11 aşağıda belirtilen yönetim frame'lerini toplar, ayrıştırır ve iletir. Yönetim frame'leri şifrelenmez, bu nedenle gönderilen bir istasyona (erişim noktası, bilgisayar, telefon vb.) yeterince yakın olan herkes nzyme ile bu frame'leri alabilir [27].

- İlişki isteği
- İlişki yanıtı
- Prob isteği
- Prob yanıtı
- Beacon
- Ayrışma
- Kimlik doğrulama
- Yetkiyi kaldırma

5. UYGULAMA

Bu tez çalışmasında 2 farklı uygulama yapılmıştır. Birinci uygulamada log yönetimi ile yetkisiz erişimlerin tespiti yapılmış ve proaktif alarm oluşturularak mail yoluyla yetkisiz erişim anlık olarak ilgili kişilere bildirilmiştir. İkinci uygulamada ise, kablosuz Ağlarda yapılan Deauth saldırılarının oluşan loglar NZYME uygulaması ile Graylog'a yönlendirilmiş ve Graylog üzerinde stream oluşturularak saldırı tespit edilmiştir. Yapılan 2 farklı uygulamanın detayları aşağıda belirtilmiştir.

5.1. Yetkisiz Erişim Saldırı Tespiti

Çalışmada Graylog uygulaması, Tübitak Bilgem YTE kurumundaki Active Directory sistemi ile entegre edilmiş ve bu sisteme ait olan 3 adet DC'nin logları Graylog'a yönlendirilmiştir. Tutulan bu loglar ile parolası arka arkaya 5 defa hatalı girilen hesaplar tespit edilmiş; böylece hesaba yapılacak brute force tarzı bir saldırının farkına varılması sağlanmıştır. Ayrıca Çizelge 5.1'de gösterilen olay numaraları ile AD'de mevcut durumlar için alarmlar oluşturulabilir [28].

Çizelge 5.1. Active Directory olay numaraları.

Olay No	Tanım
4776	Etki alani denetleyicisi, bir hesap için kimlik bilgilerini dogrulamayi denedi
4777	Etki alani denetleyicisi bir hesabin kimlik bilgilerini dogrulayamadi
4768	Kerberos kimlik dogrulama bileti (TGT) talep edildi
4769	Kerberos servis bileti talep edildi
4770	Kerberos servis bileti yenilendi
4741	Bir bilgisayar hesabi olusturuldu.
4742	Bir bilgisayar hesabi degistirildi.
4743	Bir bilgisayar hesabi silindi.
4739	Etki Alani Politikasi degistirildi.
4782	Bir hesaba erisilen sifre hash.
4727	Güvenlik özellikli bir genel grup olusturuldu.
4728	Güvenligi etkinlestirilmis bir genel gruba üye eklendi.
4729	Güvenlik özellikli bir genel gruptan üye çikarildi.
4730	Güvenlik özellikli bir genel grup silindi.
4731	Güvenligi etkin bir yerel grup olusturuldu.
4732	Güvenligi etkinlestirilmis bir yerel gruba üye eklendi.
4733	Güvenlik etkin bir yerel gruptan üye çikarildi.
4734	Güvenligi etkinlestirilmis bir yerel grup silindi.

Çizelge 5.1. (Devamı) Active Directory olay numaraları

Olay No	Tanım
4735	Güvenligi etkinlestirilmis bir yerel grup degistirildi.
4737	Güvenligi etkinlestirilmis bir genel grup degistirildi.
4754	Güvenlik özellikli bir evrensel grup olusturuldu.
4755	Güvenlik özellikli bir evrensel grup degistirildi.
4756	Güvenlik özellikli bir evrensel gruba üye eklendi.
4757	Güvenlik özellikli bir evrensel gruptan üye çikarildi.
4758	Güvenlik özellikli bir evrensel grup silindi.
4720	Bir kullanici hesabi olusturuldu.
4722	Bir kullanici hesabi etkinlestirildi.
4723	Bir hesabin sifresini degistirme denemesi yapildi.
4724	Bir hesap sifresini sifirlama girisiminde bulunuldu.
4725	Bir kullanici hesabi devre disi birakildi.
4726	Bir kullanici hesabi silindi.
4738	Bir kullanici hesabi degistirildi.
4740	Bir kullanici hesabi kilitlendi.
4765	Bir hesaba SID Geçmisi eklendi.
4766	Bir hesaba SID Geçmisi ekleme denemesi basarisiz oldu.
4767	Bir kullanici hesabinin kilidi açildi.
4780	ACL, yönetici gruplarinin üyesi olan hesaplara kuruldu.
4781	Bir hesabin adi degistirildi:
4934	Bir Active Directory nesnesinin öznitelikleri çogaltildi.
4935	Çogaltma hatasi baslar.
4936	Çogaltma hatasi sona eriyor.
5136	Bir dizin hizmeti nesnesi degistirildi.
5137	Bir dizin hizmeti nesnesi olusturuldu.
5138	Bir dizin hizmeti nesnesi silindi.
5139	Bir dizin hizmeti nesnesi tasindi.
5141	Bir dizin hizmeti nesnesi silindi.
4932	Bir Active Directory adlandirma baglaminin bir kopyasinin senkronizasyonu basladi.
4933	Bir Active Directory adlandirma baglaminin bir kopyasinin senkronizasyonu sona erdi.
34	Bir hesap kapatildi.
4647	Kullanici oturumunu baslatti.
4624	Bir hesap basariyla giris yapildi.
4625	Bir hesap oturum açamadi.
4648	Açik kimlik bilgileri kullanilarak bir oturum açma denemesi yapildi.
4675	SID'ler süzüldü.
4649	Bir tekrarlama saldirisi tespit edildi.
4778	Bir oturum bir Window Station'a yeniden baglandi.
4779	Bir oturumun bir Pencere Istasyonundan baglantisi kesildi.
4800	Is istasyonu kilitlendi.

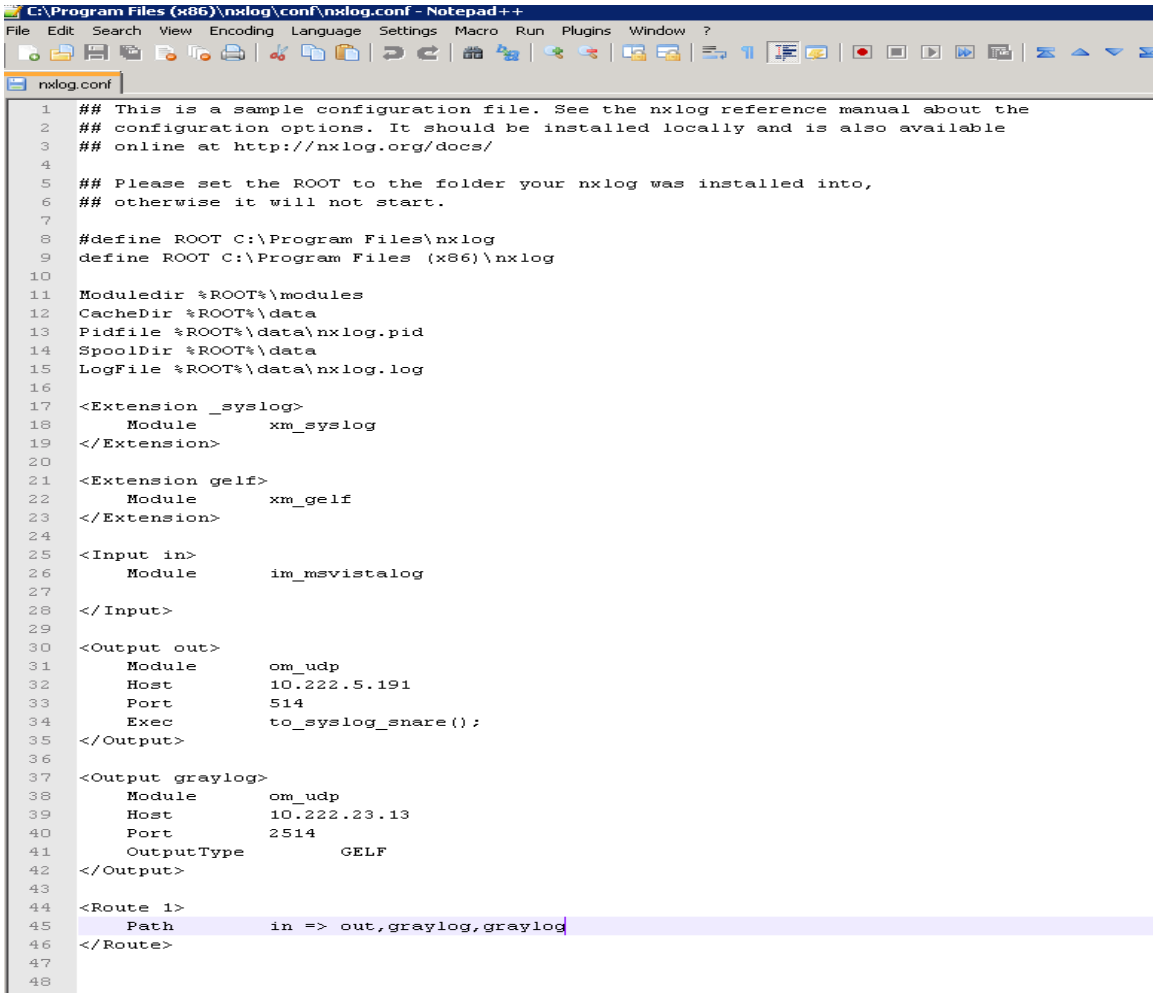
Çizelge 5.1. (Devamı) Active Directory olay numaraları

Olay No	Tanım
5632	Bir kablosuz agin kimligini dogrulamak için bir istek yapildi.
5633	Kablolu bir agin kimligini dogrulamak için bir istek yapildi.
5140	Bir ag paylasim nesnesine erisildi.
4664	Sert bir baglanti olusturma girisiminde bulunuldu.
4985	Bir islemin durumu degisti.
5051	Bir dosya sanallastirildi.
5031	Windows Güvenlik Duvari Hizmeti, bir uygulamanin agdan gelen baglantilari kabul etmesini engelledi.
4698	Zamanlanmis bir görev olusturuldu.
4699	Zamanlanmis bir görev silindi.
4700	Zamanlanmis bir görev etkinlestirildi.
4701	Zamanlanmis bir görev devre disi birakildi.
4702	Zamanlanmis bir görev güncellendi.
4657	Bir kayit defteri degeri degistirildi.
5039	Bir kayit defteri anahtari sanallastirildi.
4660	Bir nesne silindi.
4663	Bir nesneye erisme girisiminde bulunuldu.
4715	Bir nesne üzerindeki denetim politikasi (SACL) degistirildi.
4719	Sistem denetim politikasi degistirildi.
4902	Kullanici basina denetim politikasi tablosu olusturuldu.
4906	CrashOnAuditFail degeri degisti.
4907	Nesne üzerindeki denetim ayarlari degistirildi.
4706	Bir etki alanina yeni bir güven olusturuldu.
4707	Bir etki alanina duyulan güven kaldirildi.
4713	Kerberos politikasi degisti.
4716	Güvenilir etki alani bilgisi degistirildi.
4717	Bir hesaba sistem güvenligi erisimi verildi.
4718	Sistem güvenlik erisimi bir hesaptan kaldirildi.
4864	Bir ad alani çarpismasi tespit edildi.
4865	Güvenilir bir orman bilgisi girisi eklendi.
4866	Güvenilir bir orman bilgisi girisi kaldirildi.
4867	Güvenilir bir orman bilgisi girisi degistirildi.
4704	Bir kullanici hakki atandi.
4705	Bir kullanici hakki kaldirildi.
4714	Sifreli veri kurtarma politikasi degistirildi.
4944	Windows Güvenlik Duvari baslatildiginda asagidaki politika etkindi.
4945	Windows Güvenlik Duvari baslatildiginda bir kural listelenmistir.
4946	Windows Güvenlik Duvari özel durum listesinde bir degisiklik yapildi. Bir kural eklendi.
4947	Windows Güvenlik Duvari özel durum listesinde bir degisiklik yapildi. Bir kural degistirildi.
4948	Windows Güvenlik Duvarında yönetici hesabından farklı bir hesap ile giriş yapıldı
4949	Windows Güvenlik duvarın kapatıldığında aşağıdaki politika kapandı

Çizelge 5.1. (Devamı) Active Directory olay numaraları

Olay No	Tanım
4951	Ana sürüm numarasi Windows Güvenlik Duvari tarafindan taninmadigindan bir kural yok sayildi.
4952	Kuralin bazi bölümleri göz ardi edilmistir, çünkü küçük sürüm numarasi Windows Güvenlik Duvari tarafindan taninmamistir. Kuralin diger kisimlari uygulanacak.
4953	Kural, Windows Güvenlik Duvari tarafindan yoksayildi, çünkü kurali ayristiramadi.
4954	Windows Güvenlik Duvari Grup Ilkesi ayarlari degisti. Yeni ayarlar uygulandi.
4956	Windows Güvenlik Duvari aktif profili degistirdi.
4957	Windows Güvenlik Duvari uygulamadi
4958	Windows Güvenlik Duvari asagidaki kurali uygulamamaktadir, çünkü kural bu bilgisayarda yapilandirilmamis ögelere atifta bulunmustur:
6144	Grup ilkesi nesnelerindeki güvenlik ilkesi basariyla uygulandi.
6145	Grup ilkesi nesnelerinde güvenlik ilkesi islenirken bir veya daha fazla hata olustu.
4670	Nesne üzerindeki izinler degistirildi.
4672	Yeni oturum açmaya atanmis özel ayricaliklar.
4673	Ayricalikli bir servis çagrildi.
4674	Ayricalikli bir nesne üzerinde bir islem denendi.
24	Windows Güvenlik Duvari Hizmeti basariyla baslatildi.
5025	Windows Güvenlik Duvari Hizmeti durduruldu.
5027	Windows Güvenlik Duvari Hizmeti, güvenlik ilkesini yerel depolama biriminden alamadi. Hizmet mevcut politikayi uygulamaya devam edecek.
5028	Windows Güvenlik Duvari Hizmeti, yeni güvenlik ilkesini ayristiramadi. Hizmet su anda uygulanan politikalarla devam edecek.
5029	Windows Güvenlik Duvari Hizmeti sürücüyü baslatamadi. Hizmet mevcut politikayi uygulamaya devam edecek.
5030	Windows Güvenlik Duvari Hizmeti baslatilamadi.
5032	Windows Güvenlik Duvari, kullaniciya bir uygulamanin agdan gelen baglantilari kabul etmesini engelledigini bildiremedi.
5033	Windows Güvenlik Duvari Sürücüsü basariyla baslatildi.
5034	Windows Güvenlik Duvari Sürücüsü durduruldu.
5035	Windows Güvenlik Duvari Sürücüsü baslatilamadi.
5037	Windows Güvenlik Duvari Sürücüsü kritik çalisma zamani hatasi algiladi. Sonlandiriliyor.
4608	Windows basliyor.
4609	Windows kapaniyor.
4616	Sistem zamani degistirildi.
4621	Yönetici CrashOnAuditFail'den sistemi kurtardi. Yönetici olmayan kullanicilarin oturum açmasina artik izin verilecek. Bazi denetlenebilir faaliyetler kaydedilmemis olabilir.
4697	Sistemde bir servis kuruldu.
4618	Izlenen bir güvenlik olay kalibi olustu.

Yapılan bu uygulamada ayrıca Graylog'un kullanımı detaylı olarak açıklanmaya çalışılmıştır. Graylog uygulamasının web ara yüzünde Search, Stream, Alerts, Dashboards, Sources ve System sekmeleri mevcuttur. Mevcut sistemlerin loglarını Graylog a göndermek için Windows makinelerde Nxlog uygulaması kurulmalı ve bu programın Conf dosyasında gerekli tanımlamaların yapılması gerekmektedir. DC makinesi üzerinde mevcut örnek bir conf dosyası aşağıda Şekil 5.1.de gösterilmiştir.

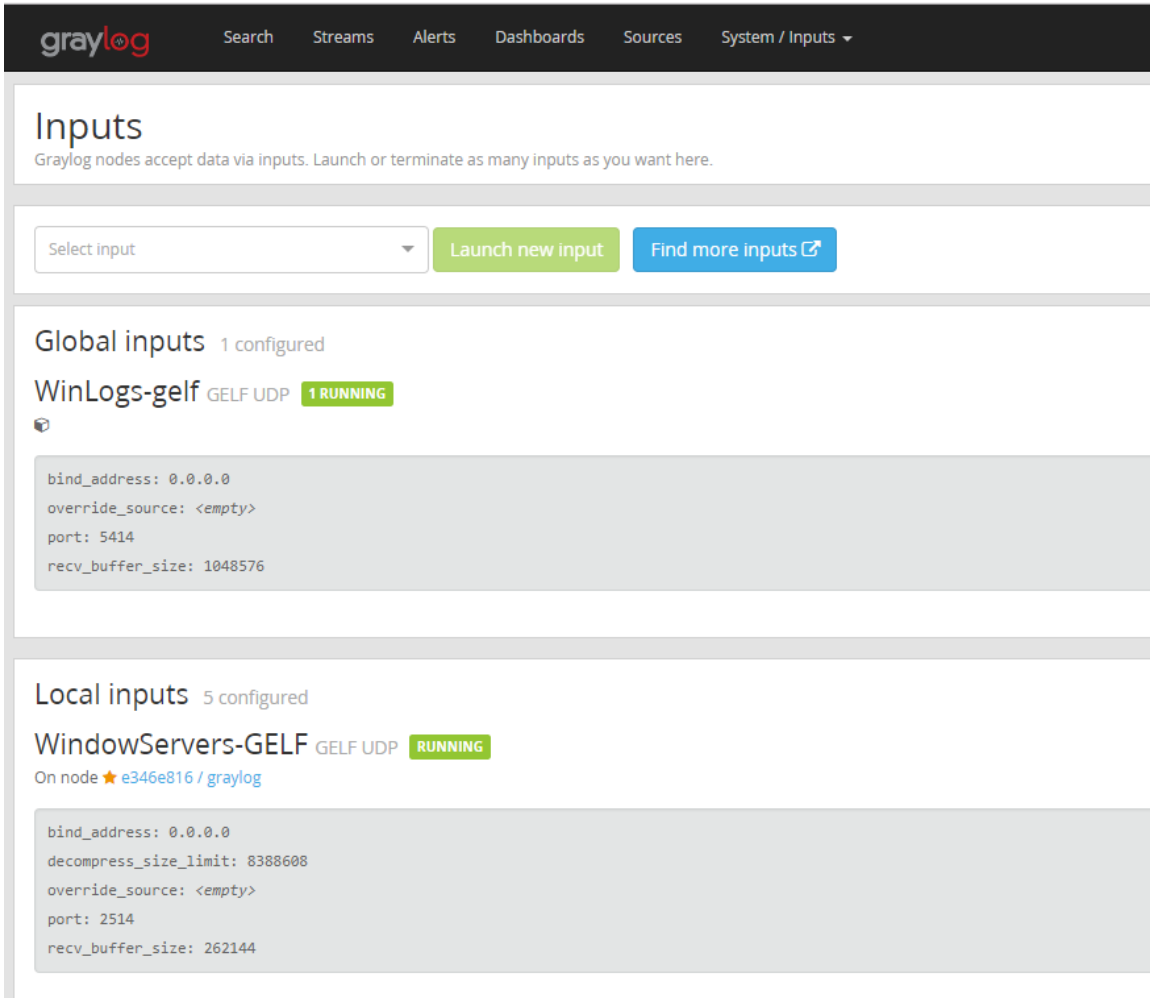


Şekil 5.1. Nxlog Conf dosyası örneği

Conf dosyası içinde gerekli değişiklikleri yaptıktan sonra sunucu işletim sisteminin servislerinin Nxlog un aktif olabilmesi için yeniden çalıştırılması gerekmektedir.

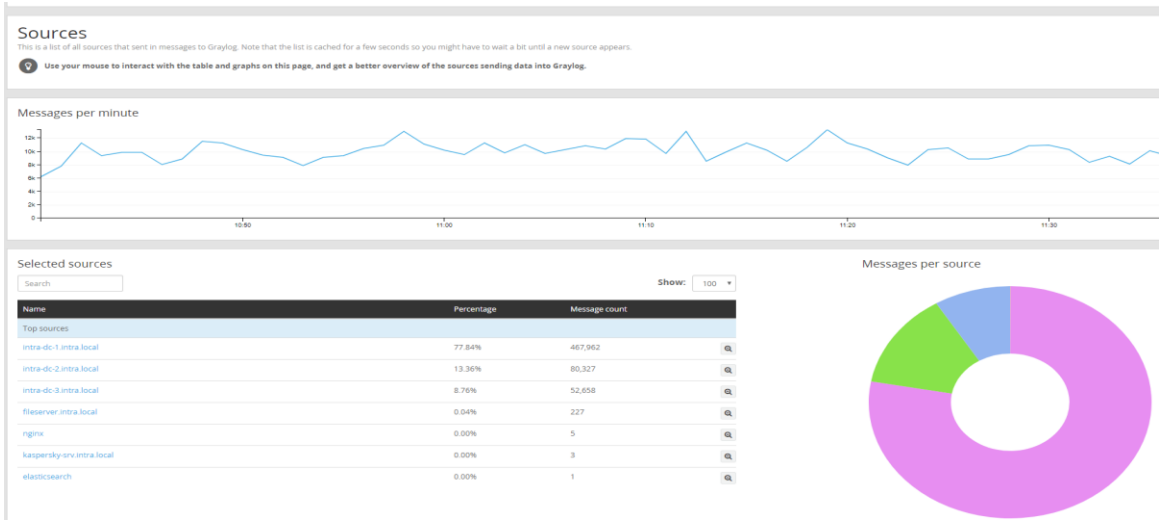
Nxlog üzerinde gerekli çalışmalar yapıldıktan sonra sistem artık Graylog uygulamasına log göndermeye başlayacaktır. Gönderilen logların Graylog ekranında görülmesi için ise Graylog web arayüzünde gerekli bazı tanımlamaların yapılması gerekmektedir. Şekil 5.2 de

ekran görüntüsü mevcut olan Input sekmesinde port ve log dosyalarının türü belirtilmelidir. Uygulamamızda GELF protokolü ile loglar alınmıştır.



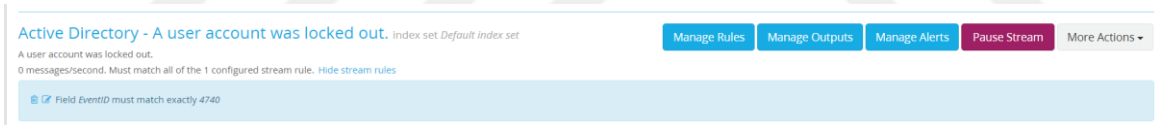
Şekil 5.2. Graylog Input Sekmesi

Sources kısmında Graylog uygulamasına log gönderen sistemleri görebilirsiniz. Şekil 5.3'te Graylog uygulamasının Source kısmının ekran görüntüsü görülmektedir.



Şekil 5.3. Graylog Sources Sekmesi

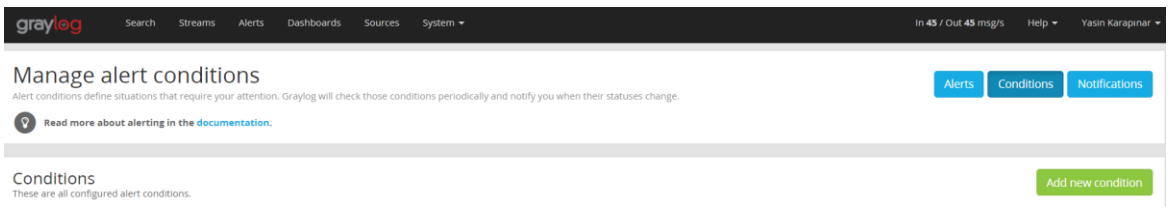
Yapılan çalışmada kurumda mevcut olan 3 adet DC makinesinin logları sisteme gönderilmiştir. Graylog web arayüzünde Şekil 5.4'te gösterilen Stream sekmesinde istenilen sistemler için loglar filtrelenebilir. Belirtilen bir event ID ile logları filtreleyerek görüntülenmek istenilen olaylar daha rahat takip edilebilir.



Şekil 5.4. Oluşturulan bir stream

Dashboard ekranında ise oluşturulan streamlar ile görseller hazırlanabilir.

Ayrıca oluşturulan streamler kullanılarak istenilen loglar için alarmlar oluşturulabilir ve istenilen durumlar mail olarak gönderilebilir. Alarm durumlarına ait ekran görüntüsü Şekil 5.5'te görülmektedir.



Şekil 5.5. Proaktif alarm oluşturma

Graylog'un kullanıcı dostu arayüzü ile alarmlar kolay bir şekilde oluşturulabilmektedir. Oluşturulan alarmlar mail ile ilgili kişilere yönlendirilebilir. Graylog sunucu üzerinde aşağıdaki mail ayarları yapılır.

Transport_email_enabled = true
Transport_email_hostname = exchange-srv.intra.local
Transport_email_port = 25
Transport_email_use_auth = false
Transport_email_use_tls = false
Transport_email_use_ssl = false

Aşağıda Şekil 5.6'da 5 defa yanlış parola girilmiş bir hesabın kilitlendiğinin Graylog tarafından mail ile bildirimi gösterilmiştir.

Şekil 5.6. Proaktif alarmın mail ile bildirilmesi

Proaktif alarmların bu şekilde mail ile bildirilmesi sayesinde yetkisiz bir erişim yapılmasının önüne hızlı bir şekilde geçilmiş olur.

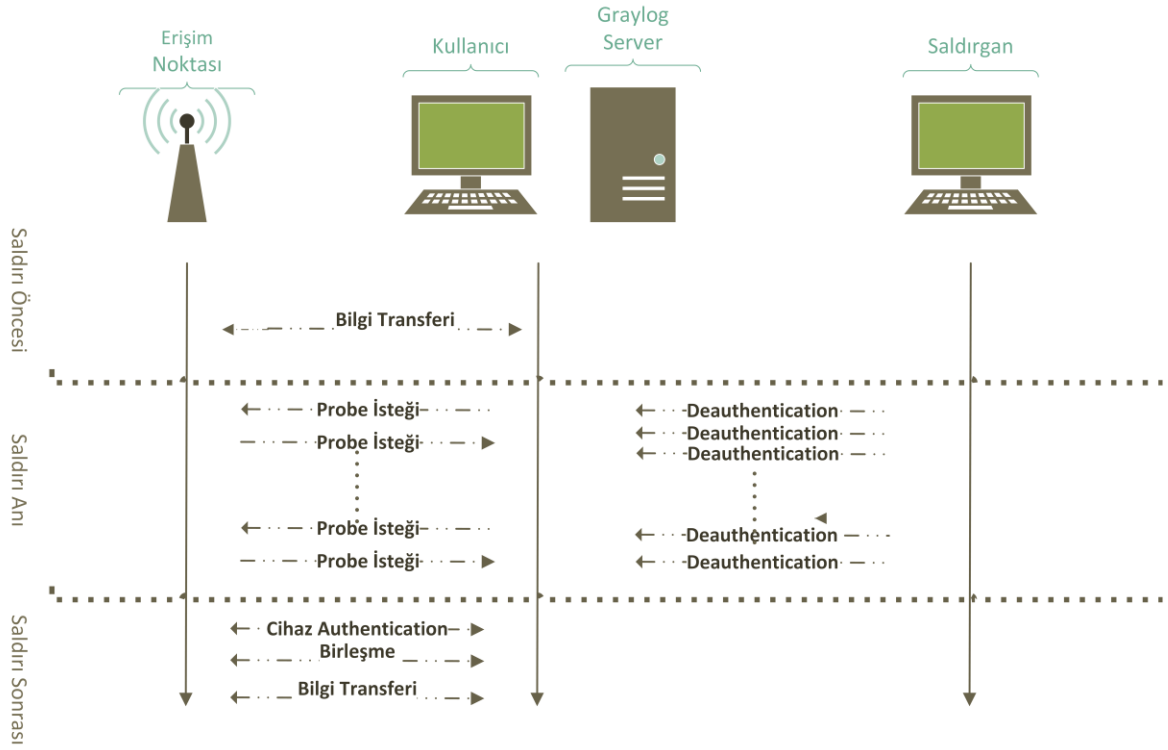
5.2. Deauthentication Saldırısı ve Tespiti

Öncelikle sanal ortamda VirtualBox üzerine Graylog sunucu OVA imajı üzerinden kurulmuştur. Saldırı yapacağımız Kali işletim sistemi kali.org/ üzerinden yine OVA imajı olarak indirilmiş ve biri saldırı yapmak için diğeri de kurban olacak şekilde iki adet sanal makine oluşturulmuştur. Hem kurban hem de saldırgan makineler üzerine WIFI görüntüleme aracı olan NZYME kurulumu yapılmış ve conf dosyası logları Graylog

sunucusuna gönderecek şekilde düzenlenmiştir. Saldırı sırasında kurban olan makinede TP-LINK WN722N model kablosuz USB adaptörü ve saldırgan olan makinede ise ASUS N14 model kablosuz USB adaptörü kullanılmıştır.

Kablosuz ağ adaptörleri hangi amaç ile kullanıldıklarına bağlı olarak dört farklı modda çalışabilirler [29].

- Master Mod: Erişim noktası olarak kullanılan cihazlarda, etraftaki istemcilere kablosuz ağ hizmetini verebilmek amacıyla kullanılan moddur.
- Managed Mod: Bir erişim noktasına bağlanarak hizmet alan istemcide kablosuz adaptör bu modda kullanılır. Uygulamada kurban bilgisayarına bağlı olan kablosuz adaptör Managed modda kullanılmıştır.
- Ad-Hoc Mod: İstemcilerin herhangi bir erişim noktası olmaksızın haberleşebilmeleri için kullanılan moddur.
- Monitor Mod: Herhangi bir ağa bağlanmadan, pasif olarak tüm kablosuz ağ trafiğinin izlenmesine olanak sağlayan moddur. Uygulamamızda saldırı yapılan makinenin kablosuz adaptörü bu modda çalıştırılmıştır.



Şekil 5.7. Deauth atak simülasyon düzeni

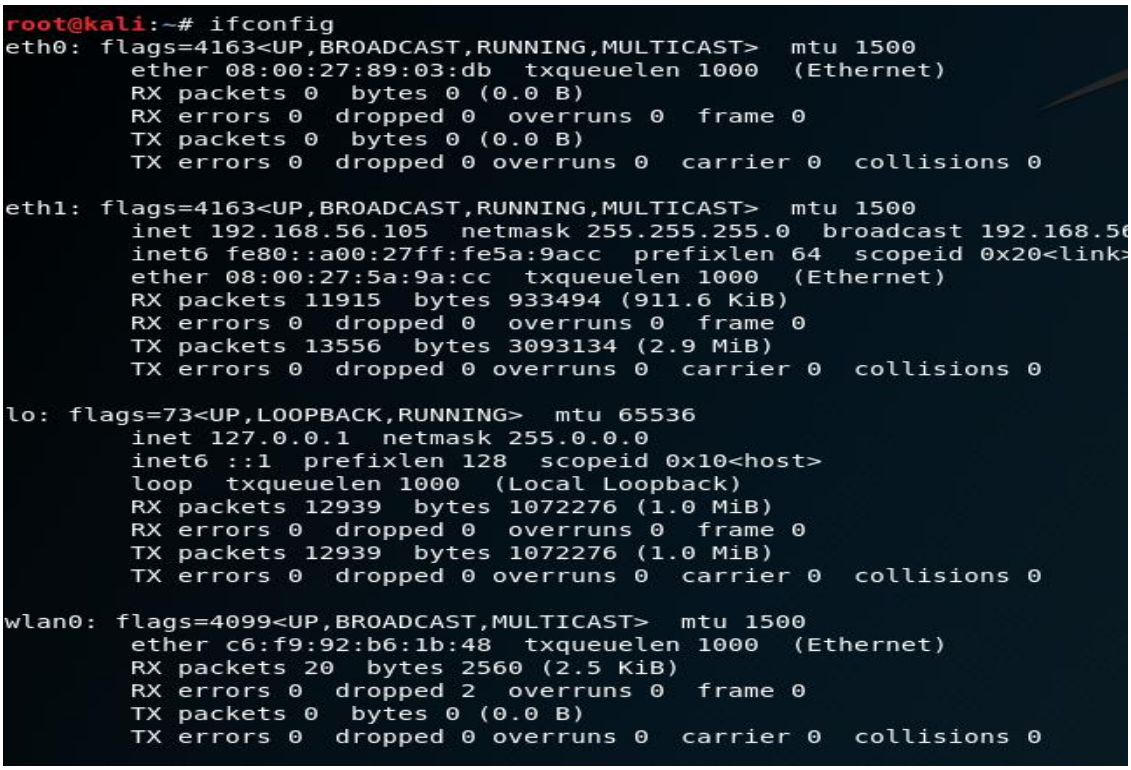
Atak türü olarak Deauthentication atak seçilmiştir. Bu atak bir tür denial of service (DOS) atağıdır [30]. Kullanıcı ile WIFI erişim noktası arasındaki iletişimin kesilmesini hedeflemektedir. Şekil 5.7'de saldırı diagramı gösterilmiştir. Bir istemci mevcut bağlantısını sonlandırmak istediğinde kablosuz ağa bir deatuhentication paketi gönderir. Eğer başkasının adına bağlı olduğu kablosuz ağa deauthentication paketi gönderilirse kurbanın bağlantısı

sürekli olarak kopacaktır. Bu saldırının en güzel yanı, tüm ağların WPA2 şifrelemesi kullandığı 2019 yılında bile, herhangi bir cihaza bağlı olduğu network içerisinde bulunmadan bile saldırının yapılabiliyor olmasıdır. WPA2 şifreli olmasına rağmen bu atağı yapabiliyor olmamızın nedeni 802.11'de şifrelemenin kullanımının yalnızca veri taşıma yükleri ile sınırlandırılmış olmasıdır. Şifreleme 802.11'de mesaj trafiğinin normal çalışması için paket başlıkları şifrelenmez ve bu nedenle kolayca taklit edilebilirler [30].

Aslında deauth saldırısı çoğu zaman daha büyük bir saldırının ön adımıdır. Saldırganların genellikle kurbanlarını ağdan çıkarmaları gerekir. Böylece, kullanıcıyı ağa yeniden bağlamaya çalışarak ortadaki adam saldırısını yapabilirler. Kurbanlarını Rogue erişim noktalarına bağlanmaya zorlayabilirler veya kullanıcıları manipüle ederek bir esir portale bağlayabilirler.

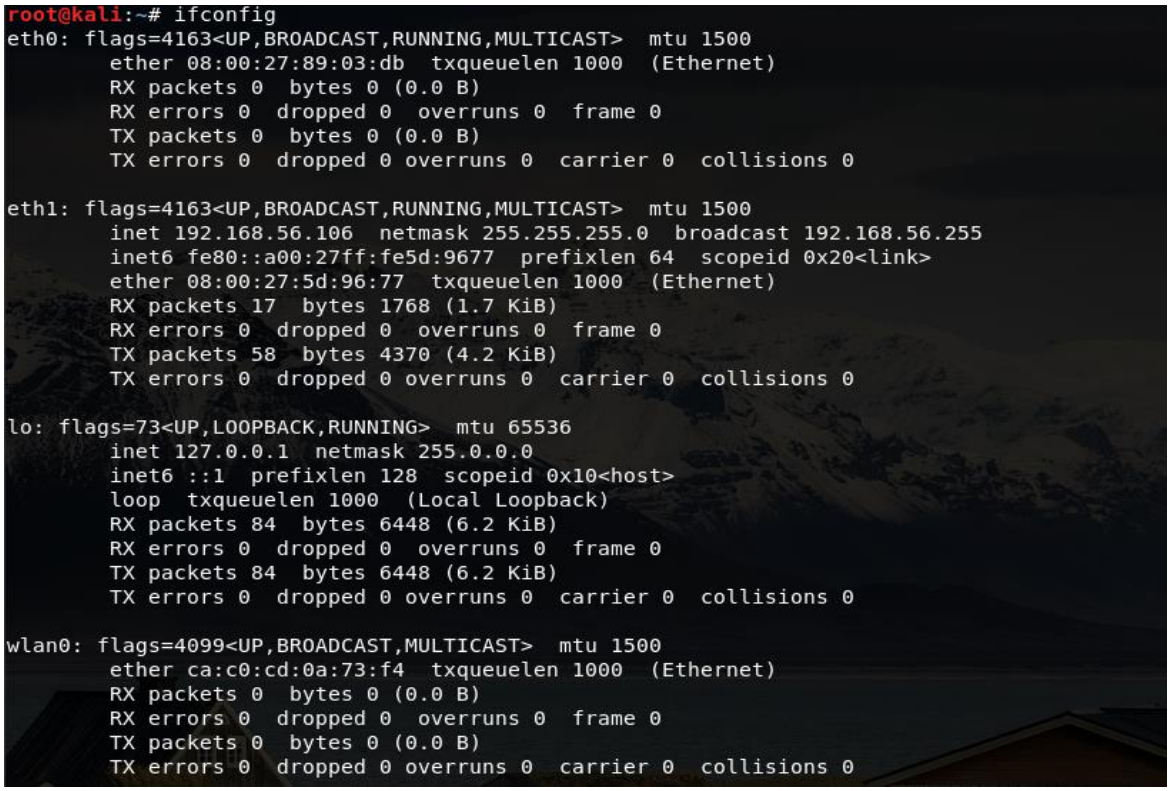
5.2.1. Deauthentication saldırısı ve tespiti

1. Adım: Kali terminali açılır. Terminale ifconfig yazılarak ağ ayarları kontrol edilir. Şekil 5.8'de saldırı öncesi, saldırılacak sanal makinenin, Şekil 5.9'da saldırgan sanal makinesinin, Şekil 5.10'da ise graylog sunucusunun ağ ayarlarının kontrol sonucu gösterilmiştir.

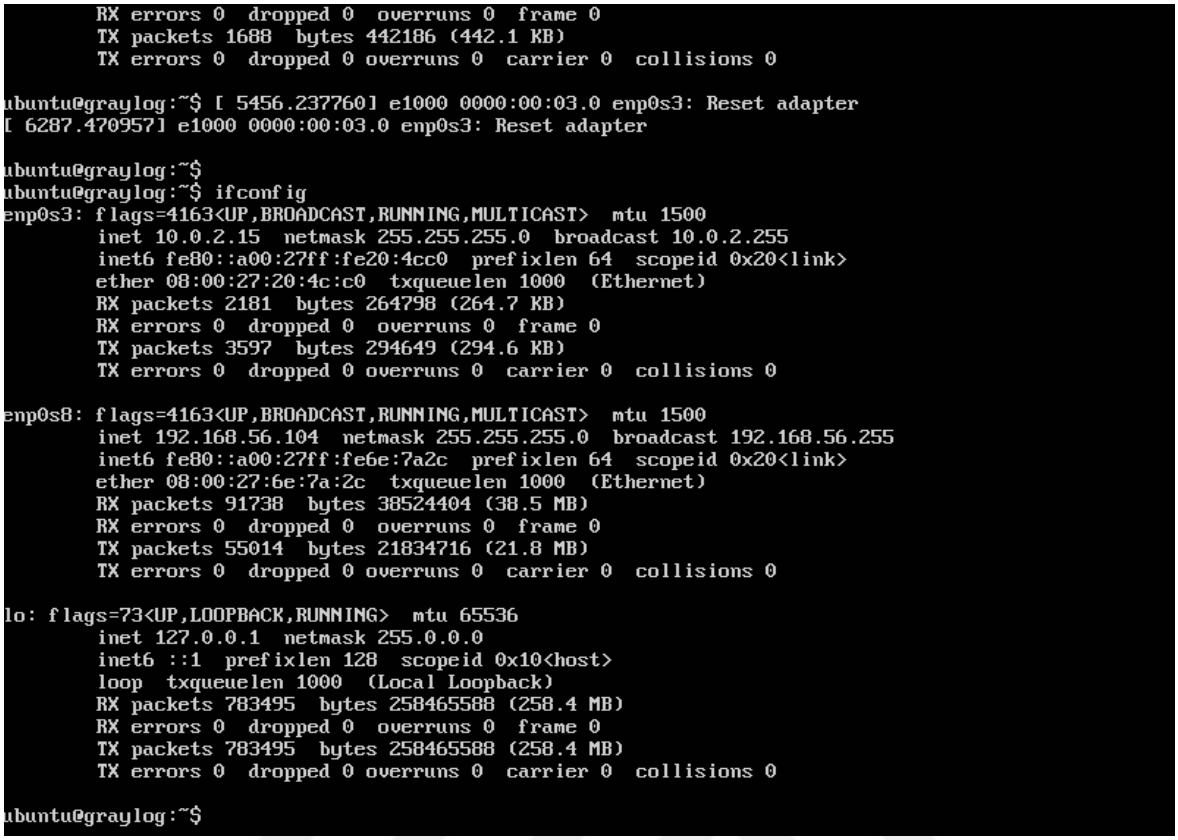


Şekil 5.8. Kurban Ağ Arayüzü Ayarları

Sanal makinemizde bulunan tüm kartların bilgilerini böylece görebiliriz. Burada eth0 sanal makinemize bağlı olan ilk network kartıdır. Lo olarak görülen ise loopback kartımızdır. Ifconfig komutu sadece IP ile ilgili bilgileri değil, her kartın kullandığı interrupts, PCI Bus ID ile ilgili bilgileri de ekrana döker. Network kartlarının çalışmadığı durumlarda bu buradaki interrupt noktalarının kontrol edilmesi fayda sağlayabilir.



Şekil 5.9. Saldırgan Ağ Arayüzü Ayarları



Şekil 5.10. Graylog ağ arayüzü ayarları

İfconfig çıktısının eth1 bölümünde saldırganın IP'sinin 192.168.56.106 olduğu, kurban IP'sinin 192.168.56.105 ve Graylog'un ise 192.168.56.104 olduğu görülmektedir. Saldırgan ve Kurban makinelerinin her ikisinden de Graylog'a ilgili logları düşürübilmek için tüm makineler aynı alt ağ içerisine kurulmuştur. Burada hem saldırı yapanın, hem de kurbanın loglarını görmek amaçlanmıştır. Normal canlı sistemlerde saldırganın IP'sini görmeye gerek olmayacaktır.

2. Adım: Bu aşamada kurban kablosuz adaptörü manage mod, saldırgan kablosuz adaptörü ise monitor moda'a alınmalıdır. Bunun için aşağıda belirtilen komutlar kullanılabilir.

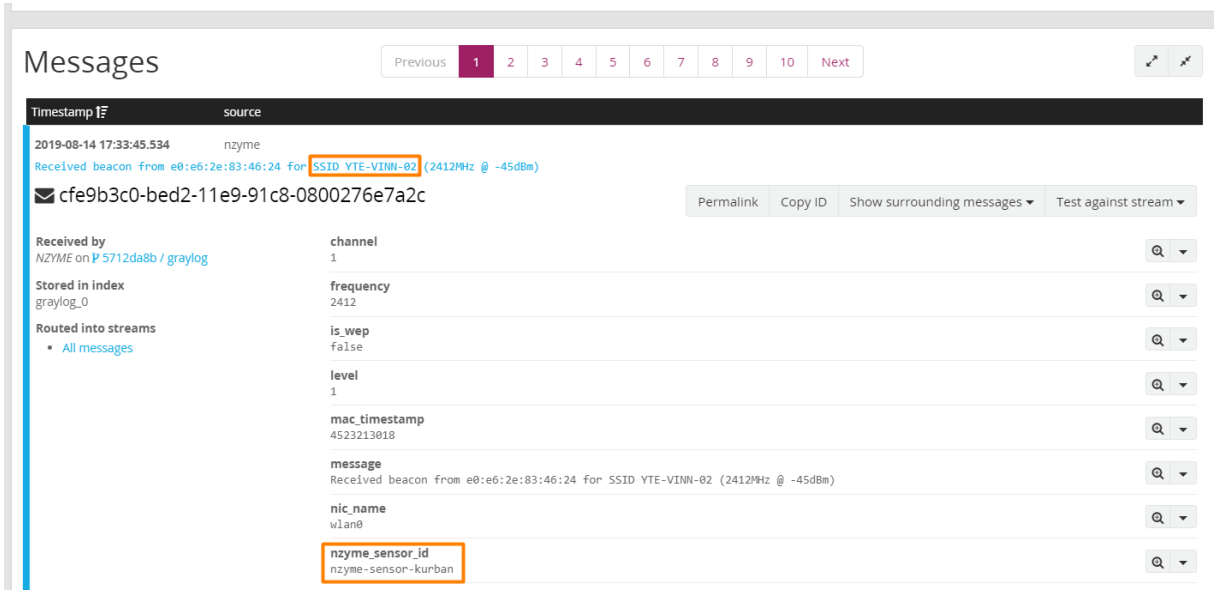
İfconfig wlan0 down
İwconfig wlan0 mode monitor (kurban için burada "manage" kullanılmalıdır.)
İfconfig wlan0 up

Artık kurban üzerinden kablosuz ağa bağlantı yapılabilir. Bağlantı sırasında erişim noktası ile makine arasındaki paketleri görüntülemek için NZME'nin aktif olarak çalıştığının

kontrolü yapılmalıdır. Bunun için systemctl status nzyme komutu kullanılabilir. Şekil 5.11 de saldırılacak sanal makinedeki NZYME'nin durum kontrolü gösterilmiştir.

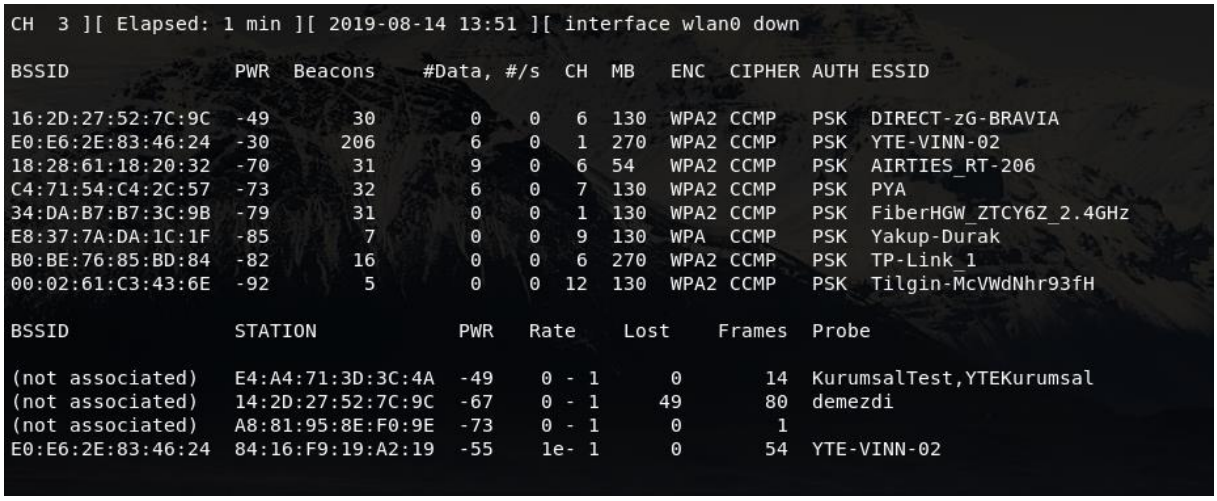
Şekil 5.11. Kurban makinesi üzerinde NZYME'nin aktif olarak çalıştığı kontrol edilmiştir.

YTE-VINN-02 kablosuz ağına kurban makinesi üzerinden bağlanmıştır. Bu bağlantının da logları Graylog üzerine düşmüştür. Kontrol edildiğinde bazen NZYME'nin aktif olarak çalışmadığı görülebilir. Böyle bir durum ile karşılaşılır ise systemctl start nzyme ile NZYME'nin tekrar çalışltırılması sağlanabilir. NZYME eğer çalışmıyor ise loglar Graylog'a aktarılmayacaktır. Bu da veri kaybına neden olacaktır. Dolayısıyla NZYME'nin istikrarlı olarak çalışması uygulama açısından kritik bir durumdur. Şekil 5.12'de saldırılan sanal makine üzerinden NZYME aracılığı ile kablosuz ağ ile yapılan bağlantı bilgilerinin Graylog'a gönderilen log bilgileri gösterilmiştir.



Şekil 5.12. Kurbanın kablosuz ağa bağlantısının Graylog üzerinde görülmesi

3. *Adım:* Etrafta mevcut kablosuz ağları aramak için saldırgan bilgisayarında terminale airodump-ng wlan0mon komutu girilir. Şekil 5.13'te saldırı esnasında bulunulan konumdaki mevcut kablosuz ağlar gösterilmiştir.

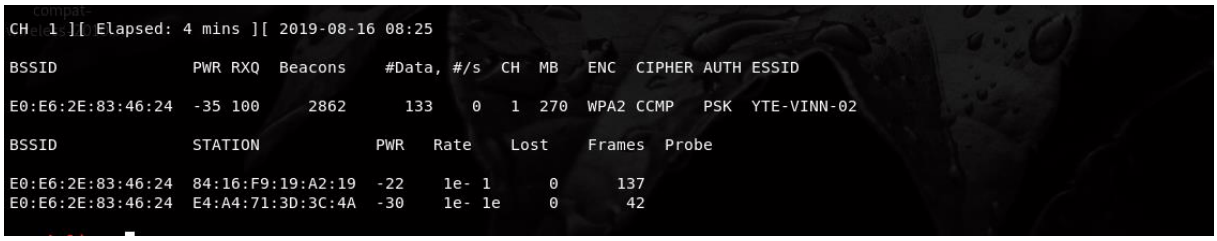


Şekil 5.13. Bulunduğumuz alanda mevcut olan kablosuz ağ ve bilgileri

4. Adım: Saldırı yapacağımız WIFI ağının seçilmesi

Saldırı yapacağımız ağ hakkında gerekli bilgiye sahip olunduktan sonra aşağıdaki komut ile ağa bağlı olan herhangi bir cihaz bulunur. Şekil 5.14'te YTE-VINN-02 kablosuz ağına bağlı bulunan istemciler gösterilmiştir. Burada komutu yazarken saldırı yapacağımız ağın kanal bilgisi doğru belirtilmelidir.

airodump-ng -d E0:E6:2E:83:46:24 -c 1 wlan0mon



Şekil 5.14. Saldırı yapılacak ağa bağlı cihazlar

5. Adım: Cihazı bağlı olduğu ağdan deauthentice etmek.

Cihazı bağlı olduğu ağdan düşürmek için aşağıdaki komutu gireriz.

aireplay-ng --deauth 2000 -a E0:E6:2E:83:46:24 -c 84:16:F9:19:A2:19 wlan0mon

Komuttaki talimatların açıklaması aşağıda belirtilmiştir.

-- deauth: Deauthentice etmek anlamına gelmektedir. 2000 adet deauth paketi gönderir..

-a E0:E6:2E:83:46:24 hedeflediğimiz erişim noktasının MAC adresidir.

-c 84:16:F9:19:A2:19 Deauthentice etmek istediğimiz ağa bağlı olan cihazın MAC adresidir. Bu adres belirtilmez ise ağa bağlı olan tüm cihazlara Deauth sinyallari gönderilir.

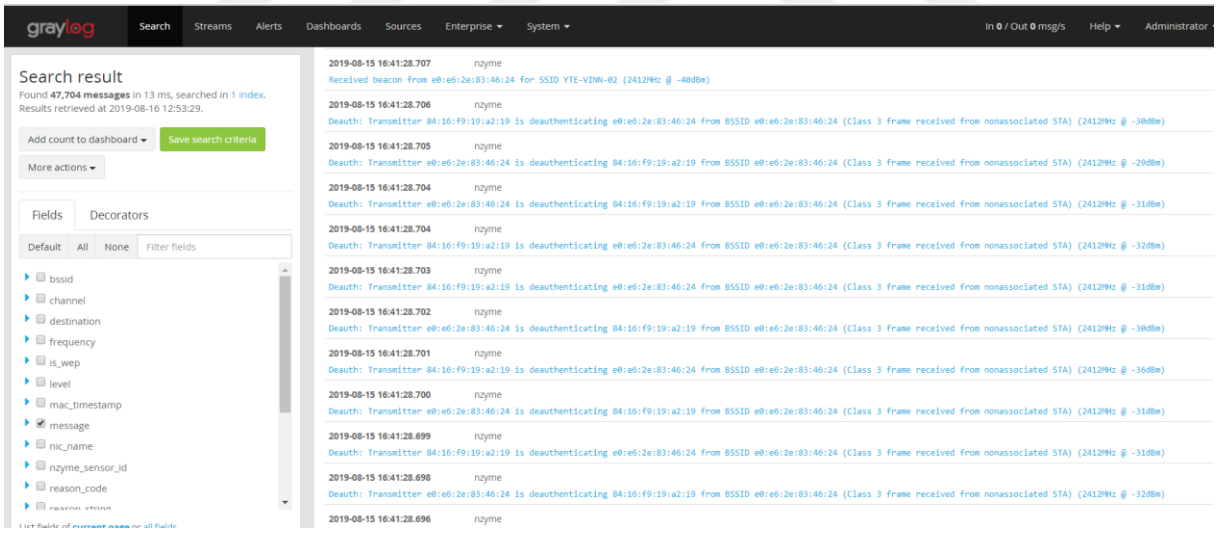
wlan0mon : arayüz adıdır. Şekil 5.15'te deauth paketlerinin istemci tarafına gönderilmesi gösterilmiştir.

```
root@kali:~# aireplay-ng --deauth 2000 -a E0:E6:2E:83:46:24 -c 84:16:F9:19:A2:19 wlan0mon
08:32:18  Waiting for beacon frame (BSSID: E0:E6:2E:83:46:24) on channel 1
08:32:18  Sending 64 directed DeAuth (code 7). STMAC: [84:16:F9:19:A2:19] [ 0| 0 ACKs]
08:32:19  Sending 64 directed DeAuth (code 7). STMAC: [84:16:F9:19:A2:19] [ 0| 0 ACKs]
```

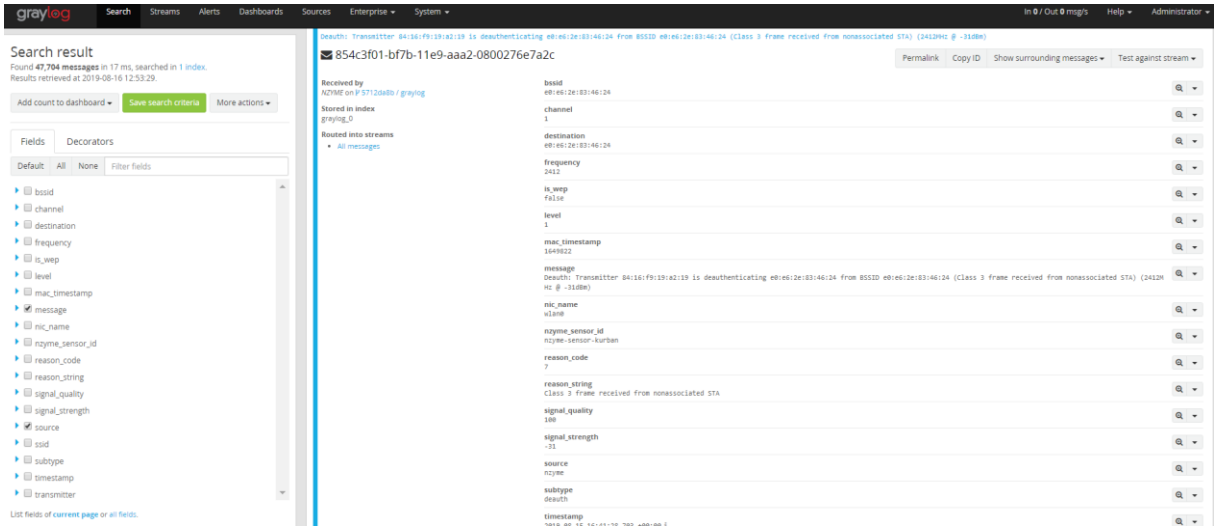
Şekil 5.15. Deauth paketlerinin istemci tarafına gönderilmesi

Kullanıcı ile erişim noktası arasındaki sinyal taklit edilmiştir. Burada modeme yeniden bağlantı istediği gönderilmiştir. Saldırı sonrasında kurbanın ağ ile bağlantısı kesilecektir. Deauth paketlerini göndermeye devam ettiğiniz sürece kurban sürekli ağdan düşmeye devam edecektir.

Deauthentication paketini gönderdikten sonra handshake paketi yakalanıp kontrol edilerek başka saldırılar da yapılabilir.



Şekil 5.16. Deauth mesajlarının geldiği graylog ekranına eş zamanlı olarak düşer.



Şekil 5.17. Deauth mesajının log içeriği

Yaptığımız saldırının logları Nzyme aracılığıyla anlık olarak Graylog'a düşecektir. Düşen loglar Şekil 5.16 ve Şekil 5.17'de gösterilmiştir. Graylog proaktif alarmlar üretmeye imkân tanımaktadır. Deauth ataklar daha büyük çaplı yapılacak saldırılar öncesinde log yönetimi ile tespit edilebilir.

6. SONUÇ

Bilişim sistemleri alt yapısındaki mevcut olan sistemlerin, bu sistemlerdeki uygulamaların ve sistemlerde mevcut bilginin güvenliğinin sağlanması konusunda bu sistemler ve uygulamaların ürettiği logların önemli bir yeri vardır. Log kayıtları adeta bir güvenlik kamerası olarak düşünülebilir. Kim ne zaman giriş yapmış ve ne yapmış gibi bilgilere güvenlik kameralarından erişilebildiği gibi sistemler ve uygulamalar için de bu bilgiler log kayıtlarında mevcuttur. Veriler korunması gerekli olan en önemli risk varlıklarıdır. Bu verilere erişimin log kayıtlarının alınması son derece önemlidir. Ancak sadece erişim ile ilgili logların tutulması verinin bütünlüğünün korunması hakkında bilgi vermez. Dolayısı ile verinin değiştirilip değiştirilmediğinden emin olunması için veri tabanlarının da loglarının tutulması gerekmektedir. Yani log analizinin sistemin bütününde yapılması önemlidir. Analizin yapılmasını ise log yönetim araçları oldukça kolaylaştırmaktadır. Çalışmamızda kullandığımız Graylog uygulaması ile sistemlerin oluşturduğu binlerce log içerisinden gerekli ve önemli olanını kolay bir şekilde elde edilebilmiştir. Tez çalışmasında yapılan uygulamalarda da görüldüğü gibi Graylog'da proaktif alarmlar oluşturularak bir bilgi güvenliği ihlal olayının önüne geçilmesi sağlanabilir.

Kablosuz ağlar artık hayatın her alanında kullanılıyor. Kamu kurumları ve özel sektör kurumlarında ve bireysel olarak kullanılan kablosuz ağların güvenliğinin sağlanması kurumların ve bireylerin siber dünyadaki güvenliği için önemli bir yer kaplamaktadır. Kablosuz ağların güvenliğini arttırmak için alınabilecek en temel önlem ağ parolasının karışık kombinasyondan oluşturulmasıdır. Günümüzde kablosuz modemlerde kullanılan WPA2 şifreleme protokolü kullanıcılara 8 karakterden 63 karaktere kadar parola belirleyebilme imkânı sağlamaktadır. Oluşturulan parolanın harf, sayı ve noktalama işaretleri kullanılarak oluşturulması güvenliğin daha iyi bir şekilde sağlanmasında faydalı olacaktır. Bunun yanında modem ayarları ile alınabilecek güvenlik önlemleri de vardır. Örneğin SSID yani kablosuz ağın bilgisayar veya mobil cihazlarda görünen adı gizlenerek ağ daha güvenli hale getirilebilir. Ayrıca modem üzerinde MAC filtreleme yapılarak da güvenlik önlemleri arttırılmış olur. Ancak bu tür önlemlerin yeterli olmadığı durumlar da meydana gelebilmektedir. Böyle bir durumun örneği olarak deauthentication atak uygulama olarak yapılmıştır. Graylog ve NZYME uygulamaları kullanılarak kablosuz ağ üzerinde iletilen paketler incelenmiştir. Deauthentication saldırısında erişim noktası yerine geçen ve

kullanıcıya deauth paketleri gönderen saldırgan makinemizin tespiti Graylog ile yapılmıştır. Böylelikle log analizi ile deauthentication ataklarının farkına varılabileceği ve önlenebileceğinin farkındalığı oluşturulmak istenmiştir. Bundan sonra yapılacak çalışmalarda makine öğrenmesi yönetimi kullanılarak normal olmayan durumların tespiti için log yönetimi araçları ile makine öğrenmesinin performans değerleri karşılaştırılabilir.

KAYNAKLAR

1. TSE (Türk Standartları Enstitüsü), (2006). TS ISO/IEC 27001 Bilgi Teknolojisi, Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler Standardı, Ankara.

2. Snodgrass, R. T., Yao, S.S., Collberg, C. (2004). *Tamper Detection in Audit Logs*, Proceedings Very Large Data Bases Conference, Toronto, Canada.

3. Schneier, B., Kelsey, J. (1998). *Cryptographic Support for Secure Logs on Untrusted Machines*, Proceedings of the 7th USENIX Security Symposium, San Antonio, Texas.

4. Axelsson, S., Lindqvist, U., Gustafsson, U., Jonsson, E., (1998). *An Approach to UNIX Security Logging*. Proccedings of the 21st National Information Systems Security Conference, Crystal City, Arlington VA, USA.

5. Söderström, O., Moradian, E. (2013). *Secure Audit Log Management*, International Conference in Knowledge Based and Intelligent Information and Engineering Systems, Kista, Sweden.

6. Souppaya, M., K. Kent, (2006). *Guide to computer security log management*. White Paper, NIST Special Publication 800-92, National Institute of Standards and Technology, USA.

7. Poole, O. (2002). *Network Security: A Practical Guide*, Syngress, Elsevier.

8. Hansen, J. B., Young, S. (2003). *The Hacker's Handbook*, CRC Press,

9. Chuvakin, A.A., Schmidt, K.J., Philips, C., (2013). *Logging and Log Management.* Massachusetts: Syngress.

10. Pouget. F., Dacier. M., (2003). White Paper: *Alert Correlation: Review of the state of the art 1*, France Institut Eurecom.

11. Forte Dario V., (2004) *The "ART" Of Log Correlation: Part 1: Tools And Techniques For Correlating Events And Log Files*, Computer Fraud & Security.

12. Herrerias J., Gomez H., (2007*), A Log Correlation Model to Support the Evidence Search Process in a Forensic Investigation*, Dept of Computer Science ITESM-CEM, IEEE, Computer Security.

13. Jacob Babbin, Dave Kleiman, (2006). *Security Log Management: Identifying Patterns in the Chaos*, Syngress Publishing.

14. İnternet: RFC 5424 URL: https://tools.ietf.org/html/rfc5424 (Son Erişim Tarihi: 12.08.2019)

15. Denis M, Zena C, Hayajneh T.(2016). *Penetration testing: concepts, attack methods, and defense strategies*. In Long Island Systems Applications and Technology Conference (LISAT) 1-6.

16. Hint, R. (1995), *SNMP, SNMPv2 and CMIP – The Technologies for multivendor network management*, Dept of Computer Science, University of Canterbury

17. Posey, B.,(2009). *GFI Network Security and PCI Compliance Power Tools*, Pages 347-362, Elsevier.

18. Y.-C. Hu , A. Perrig , D.B. Johnson.,(2003), *Packet leashes: a defense against wormhole attacks in wireless networks*, in: Proceedings of the IEEE Conference on Computer Communications (InfoCom).

19. S. ˇCapkun , J.-P. Hubaux, (2006). *Secure positioning in wireless networks*, IEEE J. Se- lected Areas Commun.

20. P. Kyasanur, N.H. Vaidya, (2005). *Selfish MAC layer misbehavior in wireless networks*, IEEE Transactions on Mobile Computing 4 (5) 502-516.

21. John Conti, G., (2006). *Counterıng Network Level Denıal Of Informatıon Attacks Usıng Informatıon Vısualızatıon*, In Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the College of Computing, Georgia Institute of Technology

22. N. Sastry , U. Shankar , D. Wagner , *Secure verification of location claims, in: Proceedings of the ACM* Workshop on Wireless Security (WiSe), 2003 .

23. N.O. Tippenhauer , H. Luecken , M. Kuhn , S. Capkun , (2015). *UWB rapid-bit-exchange system for distance bounding,* Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, June 22-26, New York, doi:10.1145/2766498.2766504

24. Masiukiewicz A, et al. (2016) *Security Threats in Wi-Fi Networks*. Engineering and Science.

25. L. Ma, A.Y. Teymorian, X. Cheng, (2008). *A hybrid rogue access point protection framework for commodity Wi-Fi networks*, in: IEEE INFOCOM, Pages.1220-1228

26. İnternet: Graylog URL: https://www.graylog.org/ (Son Erişim Tarihi: 12.05.2018)

27. İnternet: NZYME URL: https://github.com/lennartkoopmann/nzyme (Son Erişim Tarihi: 18.08.2019)

28. İnternet: https://social.technet.microsoft.com/wiki/contents/articles/15232.active-directory-services-audit-document-references.aspx (Son Erişim Tarihi: 17.07.2019.)

29. Lundin E., Erland Jonsson, (2000) *Anomaly-Based Intrusion Detection: Privacy Concerns And Other Problems* Computer Networks, Volume 34, Science Direct.

30. J. Katz , Y. Lindell, (2007). Introduction to Modern Cryptography (*Chapman & Hall/Crc Cryptography and Network Security Series*), Chapman & Hall/CRC, Boca Raton, FL 33487-2742.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : GÜL, Emre
Uyruğu : T.C.
Doğum tarihi ve yeri : 06.07.1987, Malatya
Medeni hali : Bekâr
Telefon : 0 (553) 348 63 94
Faks : 0 (312) 286 52 22
e-mail : egul.ee@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilgi Güvenliği Mühendisliği	Devam ediyor
Lisans	Gebze Teknik Üniversitesi/Elektronik Mühendisliği	2012

İş Deneyimi

Yıl	Yer	Görev
2015-Halen	Tübitak Bilgem YTE	Sistem Yöneticisi
2013-2015	Türk Telekomünikasyon A.Ş.	Mühendis

Yabancı Dil

İngilizce

Yayınlar

Gül, E., Yılmaz, E.N. (2019). *Log Management Wıth Open Source Tools*, International Symposium on Innovative Approaches in Scientific Studies (ISAS2019), Ankara, Turkey

Hobiler

Yüzme, Tenis, Fitness

GAZİ GELECEKTİR..