DÜZCE ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SİBER SALDIRILARIN LOGLAR ÜZERİNDEN TESPİT EDİLMESİ VE ÖNLENMESİ

SERKAN ÖZARGIN

YÜKSEK LİSANS TEZİ
SİBER GÜVENLİK ANABİLİM DALI

DANIŞMAN
DR. ÖĞR. ÜYESİ AHMET ALBAYRAK

DÜZCE, 2024

T.C.
DÜZCE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SİBER SALDIRILARIN LOGLAR ÜZERİNDEN TESPİT EDİLMESİ VE ÖNLENMESİ

Serkan ÖZARGIN tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Lisansüstü Eğitim Enstitüsü Siber Güvenlik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Dr. Öğr. Üyesi Ahmet ALBAYRAK

Düzce Üniversitesi

Jüri Üyeleri

Dr. Öğr. Üyesi Ahmet ALBAYRAK
Düzce Üniversitesi _____

Dr. Öğr. Üyesi Enver KÜÇÜKKÜLAHLI
Düzce Üniversitesi _____

Dr. Öğr. Üyesi Yasin ORTAKCI
Karabük Üniversitesi _____

Tez Savunma Tarihi: 04/06/2024

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

04 Haziran 2024

Serkan ÖZARGIN

TEŞEKKÜR

Öncelikle Yüksek Lisans öğrenimim boyunca örgün ve uzaktan eğitim sürecinde bu tezin hazırlanmasında gösterdiği her türlü destek, yardım ve emeklerinden dolayı, sürekli iletişim halinde olduğum, çok kıymetli tez danışmanım Dr. Öğretim Üyesi Ahmet Albayrak hocama en içten dileklerimle teşekkürlerimi sunarım.

Aynı zamanda araştırmalarımda bana şirket kapılarını açan BG-TEK firmasına, Kâmil Burlu hocama, COSLAT teknik ekibine ve arkadaşım Mustafa Tosyalı 'ya teşekkürlerimi iletirim. Yoğun çalışma ortamında siber güvenlik konularında yardımlarını esirgemeyen, bilgisayar donanımı programından değerli sınıf arkadaşım, Harun Şeker'e teşekkür ederim.

Ayrıca iş yoğunluğum ve tez çalışmalarım süreci içinde desteğini esirgemeyen her zaman yanımda olan çok kıymetli annemin ellerinden öperim.

04 Haziran 2024 **Serkan ÖZARGIN**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ viii

ÇİZELGE LİSTESİ x

KISALTMALAR xi

ÖZET xiv

ABSTRACT xv

1. GİRİŞ 1

1.1. LİTERATÜR TARAMASI 4

1.2. LİTERATÜRE KATKISI 9

2. MATERYAL METOT 11

2.1. LOG KAVRAMSAL ÇERCEVE, YASAL ZORUNLULUK VE GÜVENLİK STANDARTLARI 11

2.1.1. Log Kavramı, Log Kayıtları ve Dosya Türleri 11

2.1.1.1. Log Kavramı 11

2.1.1.2. Log Kayıtları 12

2.1.1.3. Log Kayıtlarında Yasal Zorunluluk 13

2.1.1.4. Log Kayıtlarının Amacı 13

2.1.2. Log Kayıtlarının Tutulduğu Farklı Sistemler 14

2.1.2.1. Linux Sistemlerinde Log Kayıtları 15

2.1.2.2. Windows Sistemlerinde Log Kayıtları 15

2.1.2.3. Ağ ve Güvenlik Sistemlerinde Log Kayıtları 16

2.1.2.4. Web Sunucu Log Kayıtları 16

2.1.2.5. Veri Tabanı Sistemlerinde Log Kayıtları 16

2.1.3. Log Dosya Türleri 16

2.1.3.1. Sistem Logları 17

2.1.3.2. Ağ Cihazı Logları 18

2.1.3.3. Uygulama Sunucu Logları 18

2.1.4. Logların Siber Güvenlik Açısından Kapsamı 20

2.2. LOGLAMA SİSTEMLERİ 21

2.2.1. Loglama Sistemlerinin Kullanıldığı Yerler 21

2.2.2. Loglama Sistemlerinde Kullanılan Donanımsal Cihazlar 22

2.2.3. Loglama Sistemlerinde Kullanılan Yazılımsal Araçlar 24

2.3. LOG YÖNETİMİ, ANALİZİ VE GÜVENLİĞİ 24

2.3.1. Log Yönetimi 24

2.3.1.1. Normalizasyon 25

2.3.2. Log Analizi 25

2.3.2.1. Log Analizi Metodoloji Adımları 26

2.3.2.2. Log Analizi Yazılımları 27

2.3.2.3. Log Yönetim Araçları 27

2.3.3. Log Güvenliği 28

2.4. SİBER SALDIRILAR 30

2.4.1. Siber Saldırılarda En Çok Kullanılan Yöntemler 31

2.4.1.1. DoS saldırı Çeşitleri 31

2.4.1.2. DDoS saldırı Çeşitleri 31

2.4.1.3. SQL Enjeksiyon Saldırıları 32

2.4.1.4. Kaba Kuvvet Saldırıları *32*
2.4.1.5. Yönetici Hesabı ile Oturum Açma *32*
2.4.1.6. Yetki Yükseltme *32*
2.4.2. Siber Saldırılara Karşı Alınan Loglama Önlemleri **33**
2.4.2.1. 5651 Log Sunucu *33*
2.4.2.2. Zaman Damgası *35*
2.5. SİBER SALDIRILARIN TESPİT EDİLMESİNDE LOGLARIN KULLANILMASI **35**
2.5.1. Siber Güvenlik Açısından Logların Önemi **35**
2.5.2. Siber Saldırıların Log Analizleriyle Önlenmesi **39**
2.5.3. Siber Saldırı Tespitinde İncelenmesi Gereken Loglar **40**
2.5.3.1. Siber Saldırıların Belirlenmesinde Kritik Log Kaynakları *43*
2.5.3.2. İç Ağ Log Kayıtlarından Üretilen Bazı Önemli Veriler *44*
2.6. SALDIRI TESPİT VE SALDIRI ÖNLEME SİSTEMLERİ **46**
2.6.1. Saldırı Tespit Sistemi **46**
2.6.1.1. Ana Bilgisayar Tabanlı IDS *47*
2.6.1.2. Ağ Tabanlı IDS *47*
2.6.1.3. Hibrit IDS *48*
2.6.1.4. İmza Tabanlı IDS *48*
2.6.1.5. Anomali Tabanlı IDS *48*
2.6.1.6. İlke Tabanlı IDS *48*
2.6.2. Saldırı Önleme Sistemi **49**
2.6.2.1. Ana Bilgisayar Tabanlı IPS *49*
2.6.2.2. Ağ Tabanlı IPS *49*
2.6.3. IDS/IPS Sistemlerinin Karşılaştırılması **50**
2.6.4. IDS/IPS Siber Güvenlik Sistemleri Nitelikleri **50**
2.6.4.1. IDS metodolojileri *51*
2.6.4.2. IDS/IPS Sistemi Çalışma Yapısı *51*
2.6.4.3. IDS/IPS Sistemi Mimari Yapısı *52*
2.6.4.4. IDS/IPS Sistemi Kod Yapısı *54*
2.6.5. Saldırı Tespit ve Önleme Sistemi Geliştirilmesi **54**
2.7. SALDIRI TESPİT VE ÖNLEME SİSTEMİ YAPILAN ÇALIŞMALAR **55**
2.7.1. Raspberry Pi Kullanarak IDS/IPS Geliştirme **55**
2.7.2. IPS ile Kullanılan Araçlar ve Çözümleri **57**
2.7.3. Python IDS/IPS Geliştirme **62**
3. SİBER SALDIRILARIN LOGLAR ÜZERİNDEN TESBİT EDİLMESİ VE ÖNLENMESİ ÇALIŞMALARI **65**
3.1. SALDIRI TESPİT VE ÖNLEME SİSTEMİ ÖNERİSİ **65**
3.1.1. Saldırı Tespit ve Saldırı Önleme Sistemi Mimari Yapısı **65**
3.1.1.1. Web Sunucu Loglarına Göre Mimari Tasarımı *66*
3.1.1.2. Yönlendirici Log Dosyalarına Göre Mimari Tasarımı *66*
3.1.2. Saldırı Tespit ve Önleme Sistemi Çalışma Yapısı **66**
3.1.3. Saldırı Tespit ve Önleme Sistemi Kod Yapısı **67**
3.2. SİBER GÜVENLİK SİSTEMİ ÖNERİLERİ **72**
3.2.1. Log Sistemleriyle IDS/IPS ve Güvenlik Duvarı Entegrasyon Önerisi **72**
3.2.2. Loglama Sistemleri için IPS Paket önerisi **76**
3.2.3. Misafirlerin Siber Güvenlik Sistemi Üzerindeki Hareketi **78**
4. SONUÇ **80**
5. KAYNAKLAR **82**
6. EKLER **91**

6.1. EK 1: IDS/IPS SALDIRI TESPİT SİSTEMİ KODLARI I 91
6.2. EK 2: SALDIRI TESPİT VE ÖNLEME SİSTEMİ KODLARI I 92
6.3. EK 3: SALDIRI TESPİT VE ÖNLEME SİSTEMİ KODLARI II..... 93
ÖZGEÇMİŞ..... 94

ŞEKİL LİSTESİ

Sayfa No

Şekil 1.1. Siber güvenlik unsurları. [4]. 2
Şekil 1.2. Siber saldırı konulu tez çalışmalarının yıllara göre dağılımı 10
Şekil 2.1. Logların güvenli IP erişim piramidi 14
Şekil 2.2. Log dosyaları türleri şeması [8]. 17
Şekil 2.3. Log dosya türlerinin görseller ile gösterimi [33]. 19
Şekil 2.4. Siber uzayda siber güvenlik. 21
Şekil 2.5. Log cihazlarının network üzerindeki yerleşim şeması. 22
Şekil 2.6. 5651 Loglama cihazı iç ve dış görünümü [34]. 23
Şekil 2.7. Log yönetimi kalite sistem şeması [17]. 24
Şekil 2.8. 2017-2021 Yılları arasında kritik 10 web uygulaması [40]. 30
Şekil 2.9. Cisco anahtarlama cihazının option 82 bilgisi [47]. 33
Şekil 2.10. 2017 Microsoft dijital savunma raporu [51]. 36
Şekil 2.11. Microsoft dijital savunma raporu siber suçların durumu [51]. 37
Şekil 2.12. Scalp raporu çıktısı [56]. 40
Şekil 2.13. Log cihazlarının konumlandırılması şeması [58]. 41
Şekil 2.14. Log dosya analizi [8]. 42
Şekil 2.15. Dıştan içe log analiz cihazları şeması [55]. 43
Şekil 2.16. Dıştan içe log analiz adımları [55]. 44
Şekil 2.17. DBF mimari yapısı [72]. 52
Şekil 2.18. Siber saldırı [72]. 53
Şekil 2.19. EBF' ye karşı mimari örneği [72]. 53
Şekil 2.20. IDS/IPS topolojileri [77]. 56
Şekil 2.21. IDS/IPS çözüm topolojisi [77]. 56
Şekil 2.22. Saldırı tespit sistemlerinin sınıflandırılması [8]. 62
Şekil 2.23. Saldırı desenleri. 63
Şekil 2.24. Saldırı yapılan web sitesi. 63
Şekil 2.25. IDS/IPS ile saldırgan IP tespit edilmesi ve bloke edilmesi. 64
Şekil 3.1. Siber güvenlik sistemi, (a) kullanılan sistem (b) önerilen sistem 67
Şekil 3.2. Açık kaynak uygulama login ekranı. 68
Şekil 3.3. Açık kaynak uygulama login giriş mesajı. 69
Şekil 3.4. Açık kaynak uygulama login giriş hatası mesajı. 69
Şekil 3.5. Açık kaynak uygulama başarılı login girişi. 70
Şekil 3.6. Açık Kaynak ile login denemesi IP'lerin kara listeye alınması. 70
Şekil 3.7. Log tablosu. 71
Şekil 3.8. Coslat 5651 Admin paneli. 72
Şekil 3.9. SSH IP tablosu. 72
Şekil 3.10 Network üzerinde firewall ve log sunucu konumlandırılması. 73
Şekil 3.11 Network üzerinde firewall, log sunucu ve IDS/IPS konumlandırılması. 73
Şekil 3.12. Siber güvenlik sistemi ve alt sistemleri şeması. 74
Şekil 3.13. IDS/IDS, güvenlik duvarı ve loglama sistemi çalışma şeması. 75
Şekil 3.14. Siber güvenlik sistemi diyagram şeması. 76
Şekil 3.15. Log çözümleri için IPS önerisi. 77
Şekil 3.16. Log çözümleri için en uygun IDS/IPS türleri 78
Şekil 3.17. Kullanıcıların siber güvenlik sistemi üzerinde ilerleyiş şeması. 79
Şekil 3.18. Kullanıcıların siber güvenlik sistemi üzerinde ilerleyiş şeması 79
Şekil 6.1 IDS/IPS Tespiti Açık Kaynak Uygulama Kodları [76]. 91

Şekil 6.2 Açık Kaynak Uygulama Kodları I 92
Şekil 6.3 Açık Kaynak Uygulama Kodları II 93

ÇİZELGE LİSTESİ

Sayfa No

Çizelge 2.1. Log kayıtları üzerinde yer alan açıklamalar [8]. 12
Çizelge 2.2. Log dosya türlerine göre kaynak türleri [33]. 20
Çizelge 2.3. Loglama araçları ve özellikleri. 28
Çizelge 2.4. Loglama kategorileri ve araçları [33]. 28
Çizelge 2.5. OWASP en kritik 10 web uygulaması [40]. 31
Çizelge 2.6. 5651 Log cihazları nitelikleri [49]. 34
Çizelge 2.7. 2023 Yılı Microsoft dijital savunma raporu [51]. 38
Çizelge 2.8. Siber güvenlik zafiyetleri ve sonuçları [52]. 38
Çizelge 2.8 (devamı). Siber güvenlik zafiyetleri ve sonuçları [52]. 39
Çizelge 2.9. IDS/IPS sistemlerinin karşılaştırılması. 50
Çizelge 2.10. IPS özellikleri ve çözümleri [77]. 59
Çizelge 2.11. IPS çözümlerinin log uyumluluğu 60
Çizelge 3.1. Log uyumluluğu olan IPS paketleri 78

KISALTMALAR

ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
BFA	Brute Force Attack (Kaba Kuvvet Saldırıları)
COBİT	Control Objectives For Information and Related Technology (Bilgi ve İlgili Teknolojiler Kontrol Hedefleri)
CSRF	Cross Site Request Forgery (Siteler Arası Talep Sahteciliği)
CSV	Comma Separated Variabies (Virgülle Ayrılmış Değişkenler)
DBF	Database Firewall (Veri Tabanı Güvenlik Duvarı)
DDoS	Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DHCP	Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)
DLP	Data Loss/Leak Prevention (Veri Kaybı/Sızıntısı Önleme)
DMZ	Demilitarized Zone (Silahsızlandırılmış Bölge)
FISMA	Federal Information Security Administration Act (Federal Bilgi Güvenliği Yönetim Yasası)
HIDS	Host-Based İntrusion Detection System (Ana Bilgisayar Tabanlı Saldırı Tespit Sistemi)
ID	Identification Number (Kimlik Numarası)
IDMEF	Intrusion Detection Message Exchange Format (İzinsiz Giriş Tespiti Mesaj Değişim Formatı)
IDPS	Intrusion Detection and Prevention Systems (Saldırı Tespit ve Önleme Sistemleri)
IDS	Intrusion Detection System (Saldırı Tespit Sistemi)
IMAP	Internet Message Access Protocol (İnternet Mesaj Erişim Protokolü)
IP	Internet Protocol (İnternet Protokol)
IPS	Intrusion Prevention System (İzinsiz Giriş Önleme Sistemi)
IPSec	Internet Protocol Security (İnternet Güvenlik Protokolü)
ISMS	Information Security Management System (Uluslararası Güvenlik Yönetim Sistemi)
ISS	Internet Information Service (İnternet Bilgi Hizmeti)
LLRP	Low Level Reader Protocol (Düşük Seviye Okuyucu Protokolü)
MAC	Media Access Protocol (Ortam Erişim Yönetimi)
NIDPS	Network Intrusion Detection And Prevention Systems (Ağa İzinsiz Giriş Tespit ve Önleme Sistemler)
OSI	Open Systems Interconnection (Açık Sistemler Ara Bağlantısı)
OSSEC	Open-Source Host-Based İntrusion Detection System (Açık Kaynak Ana Bilgisayar Tabanlı Saldırı Tespit Sistemi)
OWASP	Open Web Application Security Project (Açık Web Uygulama Güvenliği Projesi)
PCI DSS	Payment Card Industry Data Security Standard (Ödeme Kartı Sektörü Veri Güvenliği Standardı)
POP3	Post Office Protocol (Postane Protokolü)
R2L	Remote To Local (Uzaktan Yerel Bağlantı)
RDP	Remote Desktop Protocol (Uzak Masaüstü Protokolü)
RFID	Radio Frequency Identification (Radyo Frekansı Tanımlama)

RNN	Reccurrent Neural Network (Yinelemeli Sinir Ağı)
SaaS	Software as a Service (Hizmet Olarak Yazılım)
SDN	Software Defined Networking (Yazılım Tanımlı Ağ)
SIEM	Security Information and Event Management (Güvenlik Bilgisi ve Onay İzleme Sistemi)
SMTP	Simple Mail Transfer Protocol (Basit Mail Aktarım Protokolü)
SNMP	Simple Network Management Protocol (Basit Ağ Yönetim Protokolü)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SSH	Secure Shell (Güvenli Kabuk)
SSL	Secure Sockets Layer (Güvenli Yuva Katmanı)
SSLPP	Secure Sockets Layer Dynamic Preprocessor (Güvenli Yuva Katmanı Dinamik Ön İşlemci)
STÖS	Saldırı Tespit ve Önleme Sistemi
SUID	Set User ID
TCP	Transmission Control Protocol (İletim Kontrol Protokolü)
TLS	Transport Layer Security (Taşıma Katmanı Güvenliği)
U2R	User to Root (Kullanıcının Root Yapması)
UHF	Ultra High Frequency (Ultra Yüksek Frekans)
VLAN	Virtual Local Area Network (Sanal Yerel Alan Ağ)
VPN	Virtual Private Network (Sanal Özel Ağ)
WAF	Web Application Firewall (Web Uygulamaları Güvenlik Duvarı)
XGBoost	Extreme Gradient Boosting (Aşırı Gradyan Tahminleme)
XSS	Cross Site Scripting (Siteler Arası Betik Çalıştırma)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
BFA	Brute Force Attack (Kaba Kuvvet Saldırıları)
COBİT	Control Objectives For Information and Related Technology (Bilgi ve İlgili Teknolojiler Kontrol Hedefleri)
CSRF	Cross Site Request Forgery (Siteler Arası Talep Sahteciliği)
CSV	Comma Separated Variabies (Virgülle Ayrılmış Değişkenler)
DBF	Database Firewall (Veri Tabanı Güvenlik Duvarı)
DDoS	Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DHCP	Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)
DMZ	Demilitarized Zone (Silahsızlandırılmış Bölge)
DLP	Data Loss/Leak Prevention (Veri Kaybı/Sızıntısı Önleme)
FISMA	Federal Information Security Administration Act (Federal Bilgi Güvenliği Yönetim Yasası)
HIDS	Host-Based İntrusion Detection System (Ana Bilgisayar Tabanlı Saldırı Tespit Sistemi)
ID	Identification Number (Kimlik Numarası)
IDMEF	Intrusion Detection Message Exchange Format (İzinsiz Giriş Tespiti Mesaj Değişim Formatı)
IDPS	Intrusion Detection and Prevention Systems (Saldırı Tespit ve Önleme Sistemleri)
IDS	Intrusion Detection System (Saldırı Tespit Sistemi)
IMAP	Internet Message Access Protocol

	(İnternet Mesaj Erişim Protokolü)
IPS	Intrusion Prevention System (İzinsiz Giriş Önleme Sistemi)
IPSec	Internet Protocol Security (İnternet Güvenlik Protokolü)
ISMS	Information Security Management System (Uluslararası Güvenlik Yönetim Sistemi)
ISS	Internet Information Service (İnternet Bilgi Hizmeti)
LLRP	Low Level Reader Protocol (Düşük Seviye Okuyucu Protokolü)
MAC	Media Access Protocol (Ortam Erişim Yönetimi)
NIDPS	Network Intrusion Detection and Prevention Systems (Ağa İzinsiz Giriş Tespit ve Önleme Sistemler)
OSI	Open Systems Interconnection (Açık Sistemler Ara Bağlantısı)
OSSEC	Open-Source Host-Based İntrusion Detection System (Açık Kaynak Ana Bilgisayar Tabanlı Saldırı Tespit Sistemi)
OWASP	Open Web Application Security Project (Açık Web Uygulama Güvenliği Projesi)
PCI DSS	Payment Card Industry Data Security Standard (Ödeme Sektörü Kartı Veri Güvenliği Standardı)
POP3	Post Office Protocol (Postane Protokolü)
R2L	Remote to Local (Uzaktan Yerel Bağlantı)
RDP	Remote Desktop Protocol (Uzak Masaüstü Protokolü)
RFID	Radio Frequency Identification (Radyo Frekansı Tanımlama)
RNN	Reccurrent Neural Network (Yinelemeli Sinir Ağı)
SaaS	Software as a Service (Hizmet olarak yazılım)
SDN	Software Defined Networking (Yazılım Tanımlı Ağ)
SIEM	Security Information and Event Management (Güvenlik Bilgisi ve Onay İzleme Sistemi)
SMTP	Simple Mail Transfer Protocol (Basit Mail Aktarım Protokolü)
SNMP	Simple Network Management Protocol (Basit Ağ Yönetim Protokolü)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SSH	Secure Shell (Güvenli Kabuk)
SSL	Secure Sockets Layer (Güvenli Yuva Katmanı)
SSLPP	Secure Sockets Layer Dynamic Preprocessor (Güvenli Yuva Katmanı Dinamik Ön İşlemci)
STÖS	Saldırı Tespit ve Önleme Sistemi
TLS	Transport Layer Security (Taşıma Katmanı Güvenliği)
U2R	User to Root (Kullanıcının Root Yapması)
UHF	Ultra High Frequency (Ultra Yüksek Frekans)
VLAN	Virtual Local Area Network (Sanal Yerel Alan Ağ)
VPN	Virtual Private Network (Sanal Özel Ağ)
WAF	Web Application Firewall (Web Uygulamaları Güvenlik Duvarı)
XGBoost	eXtreme Gradient Boosting (Aşırı Gradyan Tahminleme)
XSS	Cross Site Scripting (Siteler Arası Betik Çalıştırma)
2FA	Two-Factor Authentication (İki Faktörlü Kimlik Doğrulama)

ÖZET

SİBER SALDIRILARIN LOGLAR ÜZERİNDEN TESPİT EDİLMESİ VE ÖNLENMESİ

Serkan ÖZARGIN

Düzce Üniversitesi
Lisansüstü Eğitim Enstitüsü, Siber Güvenlik Anabilim Dalı
Yüksek Lisans Tezi
Danışman: Dr. Öğr. Üyesi Ahmet ALBAYRAK

Haziran 2024, 93 sayfa

Teknoloji kullanımı giderek yaygınlaşmakta, insan hayatının vazgeçilmezleri arasında yer almaktadır. Teknolojinin tüm alanlarda yaygın olarak kullanılması bilgisayar sistemleri üzerinde güvenlik açıklarının oluşmasına neden olmaktadır. Sistemlere yapılan saldırıların nereden ne zaman kim tarafından yapılacağı bilinmemektedir. Bu bağlamda sistemler üzerinde gerçekleşen işlemlerin internet izlerinin tutulması, log kayıtlarının alınması, yaşanan birçok siber saldırıyı çözme konusunda uzmanlara fayda sağlamaktadır. Sistemler üzerindeki zafiyetlerin hackerlar tarafından fark edilmesiyle beraberinde çeşitli siber saldırılar ortaya çıkarmıştır. Tespit edilen bu zafiyetler üzerinden network sistemi üzerinde hakimiyet kurmaları, maddi kazanç elde etmeleri ve itibari sebepler yer alabilmektedir. Bu durum sistemlerin bilgi bütünlüğünü bozmaktadır. Bu çalışma kapsamında log kayıtları üzerinden siber saldırıların tespit edilebileceği ve siber saldırıların engellenebileceği araştırılmıştır. Bu çalışma loglar üzerinden siber saldırıların tespit edilmesi ve engellenmesi, siber saldırılara karşı çözümlerin üretilmesi bakış açısıyla literatüre katkı sağlayacağı düşünülmektedir.

Anahtar Sözcükler: Siber Saldırılar, Log tutma, Siber Saldırıların tespiti ve Önlenmesi,

ABSTRACT

DETECTION AND PREVENTION OF CYBER ATTACKS THROUGH LOGS

Serkan ÖZARGIN
Düzce University
Graduate School, Department of Cyber Security
Master's Thesis
Supervisor: Asst. Prof. Ahmet ALBAYRAK

June 2024, 93 pages

The use of technology is becoming increasingly widespread and is among the indispensables of human life. The widespread use of technology in all areas causes security vulnerabilities on computer systems. It is not known from where, when and by whom the attacks on the systems will be made. In this context, keeping internet traces of the transactions on the systems, taking log records, provides benefit to experts in solving many cyber attacks. With the vulnerabilities on the systems being noticed by hackers, various cyber attacks have emerged. Through these detected weaknesses, they can dominate the network system, gain financial gain and reputational reasons. This situation disrupts the information integrity of the systems. Within the scope of this study, it has been investigated that cyber attacks can be detected and cyber attacks can be prevented through log records. This study is thought to contribute to the literature from the perspective of detecting and preventing cyber attacks through logs and producing solutions against cyber attacks.

Keywords: Cyber Attacks, Logging, Detection and Prevention of Cyber Attacks,

1. GİRİŞ

Internet teknolojileri hızla gelişmekte, yeni trend teknolojileri beraberinde getirmektedir. Teknolojik gelişmeler, insanların hayatlarını sürdürmeleri için yaşamsal ortam sunmakta ve yaşamlarını kolaylaştırmaktadır. Bu bağlamda teknolojik gelişmeler, canlıların yaşam standartlarını üst seviyelere çıkartmaktadır. Teknolojik gelişmeler internet ortamında yer alan yeni paradigmaları da beraberinde getirmektedir. Aynı zamanda internete bağlanan cihaz sayısında müthiş bir artış yaşanmaktadır. Bu durum birçok sorunun oluşmasına ve probleme neden olmaktadır.

Yetkisiz kullanıcıların sistemlere erişiminin engellenmesi, saldırıların bertaraf edilmesi ve siber güvenliğin sağlanması bilgi bütünlüğü açısından önemlidir. Siber güvenlik alanı akademik çalışmalara açık konulardan oluşmaktadır. Siber güvenlik alanında, çalışmaların yapılamamasının bazı nedenleri içinde, araştırmacıların azlığı, çalışma konularının zor olması ve siber güvenlik sistem gereksinimlerinin maliyetli olması sebepleri yer almaktadır. Bu durum siber alanda uzman personelin yetişmesini engellemektedir. Literatür taramalarında siber güvenlik konulu 2013-2021 yılları arasında 225 tez çalışması bulunmaktadır [1]. 2013-2021 yılları arasında Bilgisayar Mühendisliği konu bazında 6097 adet tez yazılmıştır. Siber güvenlik konulu tez çalışmalarına göre Bilgisayar Mühendisliği alanında yapılan tez çalışmalarının daha yoğun olduğu görülmektedir. Siber güvenlik alanında yapılan tez çalışmaların giderek artacağı beklenmektedir. Yapılan çalışmaların artması uzman personelin yetişmesinde önemli bir rol oynayacağı düşünülmektedir.

Teknolojinin her alanda kullanılması kötü niyetli kullanıcılar tarafından hedef haline gelmiş siber saldırıların tetiklenmesine sebep olmuştur. Akıllı sistemler, sosyal medya platformları, devlet kurumları, e-ticaret siteleri, oyun siteleri, e-postalar, bulut sistemler ve stratejik kurumların sistemleri siber güvenlik açısından tehlike altındadır [2].

Akıllı sistemler üzerinde yapılan siber saldırıların maddi hasarı daha fazladır. Kişi veya kurumun sunucuları, mail adresleri sosyal medya hesapları siber saldırılar ile ele geçirilebilir. Daha da fazlası banka hesapları boşaltılabilir. Siber saldırıların bilgi güvenliği açısından, tespit edilmesi ve önlenmesi oldukça önemlidir. Sistemlere erişimlerin kayıt altına alındığı ve yapılan işlemlere ait verilerin tutulmasıdır [3].

Dijital ortamda oluşan verilerin işlenmesi, bilgi haline getirilmesi, bu bilgilerin güvenliğinin sağlanması en önemli alanlardan biridir. Sunucu bilgisayar sistemleri, web hizmetleri, ile akıllı sistemler, akıllı cihazlar IoT (Nesnelerin İnterneti), sağlık, eğitim, çevre, şehir, şebeke, enerji gibi birçok alanda çok yaygın olarak kullanılmaktadır. Bu sistemler için siber güvenlik en önemli yapıdır. Tüm sistemlerin sürdürülebilirliği ve bütünlüğü için en önemli olgu güvenlik tarafıdır. Siber güvenlik açısından bilgi güvenliği tüm internet teknolojilerini kapsamaktadır. Akıllı sistemler, web-mail sunucular, kamu veri tabanları, dijital devlet, sosyal medya tüm bu teknolojik yapıların sürdürebilirliği açısından bilgi güvenliği en hassas, en kritik ve en stratejik yapı içinde siber güvenlik kapsamında yer almaktadır. Tüm sistemlerde güvenlik, veri bütünlüğü açısından en değerli olgulardır. Aynı zamanda internet teknolojilerinin her geçen gün hızla gelişmekte ve internete bağlanan cihazların sayısı giderek artmakta olduğu bilinmektedir. Bu cihazların yönetimi kadar güvenliği de önemlidir.

Tez çalışma konusu içinde yer alan bölümlerde log kayıtlarının tutulması, loglama cihazları, network sistemleri üzerinde oluşan log verilerinin incelenmesi, siber güvenlik ve siber saldırılar açısından oluşabilecek zafiyetlere çözüm önerileri başlıklar halinde tez içinde yer alması düşünülmektedir [3].

Network sistemleri üzerinde, siber güvenlik önemli yapılar arasındadır. Akıllı sistemler de dahil olmak üzere tüm network sisteminin log kayıtlarının tutulması gerekmektedir. Bu bağlamda log kayıtlarının analiz edilmesiyle siber güvenlik tedbirlerinin alınmasını sağlanabilir. Siber güvenlik, donanım, yazılım, kullanıcı güvenliği başta olmak üzere tüm sistemleri içinde barındırır. Şekil 1.1'de yer alan siber güvenlik unsurları yer almaktadır. Siber güvenliğin tüm sistemlerde ilk sırada yer aldığı görülmektedir [4].

Şekil 1.1. Siber güvenlik unsurları. [4].

En yeni teknolojilerde bile siber güvenlik zafiyetlerinin çıkabileceği muhtemeldir. Bu bağlamda veri bütünlüğünün sağlanması için bilgi güvenliği sistemler içinde en üst seviyede yer almaktadır. Siber güvenlik zafiyetlerinin ne zaman ne şekilde ortaya çıkacağı bilinmemekte olup saldırıların ve zafiyetlerin tahmin edilmesi mümkün olmayabilir. Bu durumun sistemler üzerinde meydana gelebilecek siber saldırıların önceden tespit edilememesi, siber saldırıların oluşturacağı zararların tahmin edilememesi araştırmanın kısıtları arasında yer almaktadır [5].

Teknolojik bir sistemin güvenlik zafiyetlerinin incelenmesi, analizi ve güvenlik açıklıklarının tespit edilmesi bilgi güvenliği açısından birtakım prosedürlerin yerine getirilmesi, izinlerin alınması ve kanuni dayanakların olduğu bir sürece sahiptir. Bu durum siber güvenlik konuları üzerine araştırma yapan personele çalışma yapan araştırmacılara belirli ortam dahilinde bazı sınırlılıklar getirebilir [6].

Siber güvenlik çalışmaları yapmak için bazı yazılım ve donanım bazlı ihtiyaçlar söz konusudur. Daha güvenli siber sistemler için açık kaynak yazılım teknolojilerinin kullanılması maliyet ve güvenlik açısından daha uygun olmaktadır. Bu anlamda donanım ihtiyaçları açısından güçlü bilgisayar ve network sistem gereksinimlerine ihtiyaç duyulabilmektedir. Bu durum ve gereksinimler siber güvenlik konularının çalışma alanını daraltmakta ve sınırlılıklarını oluşturmaktadır.

Bu tez çalışması sonuç dahil 4 bölümden oluşmaktadır.

Birinci bölümde, saldırı tespit sistemleri konulu akademik çalışmalar yer almaktadır. Ayrıca tez çalışma konusunun amacı, kapsamı ve önemini belirten içerikler bulunmaktadır.

İkinci bölümde, log kavramı, log tanımı, loglama cihazları, log analiz araçları ve siber güvenlik için log kayıtlarının önemini içeren konu başlıkları bulunmaktadır. Ayrıca siber saldırı tespitinde kullanılan açık kaynak araçlar da incelenmiştir.

Üçüncü bölümde, siber saldırıların loglar üzerinden tespit edilmesi ve siber saldırıların önlenmesi için açık kaynak kod uygulamaları yer almaktadır. Siber saldırıların tespit edilmesi ve önlenmesi için çeşitli çözüm önerileri sunulmuştur.

Sonuç bölümünde, siber saldırıların loglar üzerinden tespit edildiği ve tespit edilen siber saldırıların önlendiği verileri yer almaktadır. Ayrıca siber saldırıların tespit edilmesinde kullanılan açık kaynak paketler incelenmiş ve çıkan sonuçlar açıklanmıştır.

1.1. LİTERATÜR TARAMASI

Kişi, kurum, işletme işlemlerinde dijital verilerin artması, kişisel verilerin dijital ortama taşınmasına olanak sağlamıştır. Bu bağlamda birçok veri dijitalleşmiştir. Bu verilerin dijital ortama taşınması bilgisayar korsanlarının dikkatinden kaçmamıştır. Bu durum dijital ortamda saklanan verilerin güvenlik sorununu ortaya çıkarmıştır. Dijital ortamda saklanan kişisel veriler korunması gereken veriler arasında ilk sıralarda yer almaktadır. Son kullanıcı verilerinin başında kullanıcı adı ve şifre gelmektedir. Bu verilerin korunmasında siber güvenlik açısından yeni yaklaşımlara ihtiyaç duyulmaktadır. Siber güvenlik çözümlerinin yapılabilmesi için loglama teknolojilerinin kullanılabileceği görülmektedir [7].

Internet ortamında birbirleriyle iletişim halinde olan bilgisayarların, iletişime geçtikleri bilgisayarlar ile ilgili loglar tutulmaktadır. Bu loglar siber saldırılar sonrası incelenmekte olduğu görülmektedir. Loglama teknolojilerinin geliştirilmesi yapılan siber saldırıları anlık olarak tespit etmesi için büyük bir öneme sahiptir. Siber saldırıların oluşturduğu maddi kayıplar büyüktür. Bilgisayar ağlarında kullanılan loglama teknolojileri günümüz internet ortamına giriş ve çıkışlarında hızla kullanılmaya başlandığı görülmektedir [8].

Loglama teknolojileri daha yaygın hale gelmektedir. Loglama teknolojileri daha donanımlı olması saldırıların tespit edilmesinde daha etkili olmaktadır. Network sistemleri üzerinde kullanılan loglama teknolojileri, analiz programları ve açık kaynak işletim sistemleridir. Bu sayesinde toplanan log verileri analiz edilmektedir. Güvenlik şirketleri, siber saldırıları tespit edebilmek için çeşitli yazılım ve donanım ürünleri geliştirmektedir. Toplanan loglar belirtilen açık kaynak işletim sistemleri ile incelenerek sistemlere sızmaya çalışan IP adresleri tespit edilmiştir [9].

Analiz yöntemiyle tespit edilen IP adresleri engellenerek sistemler daha güvenli hale getirilmeleri sağlanmıştır. Bu çalışmada tutulan loglara göre çok katmanlı bir yaklaşım sunulmuştur. 4 katmanlı bir tasarıma dayalı güvenlik ihlalleri tespitine yönelik analiz yaklaşımı yer verilmiştir. Bu dört katman saldırıların tespiti için kullanılmaktadır. Her katmanda farklı bir olay gerçekleşmektedir. Yapılan siber saldırıların katman yapısına göre değişlik gösterdiği görülmektedir. Yapılan çalışmada çözüm önerileri içinde her katmana göre farklılık gösterdiği yer almaktadır [10].

Log verileri çeşitli analiz yöntemleri kullanılarak siber güvenlik bağlamında birçok yol haritalarının oluşturabileceği görülmektedir. Bu çalışmada analiz edilen veriler bilgiye

dönüştürülürken veri madenciliği yöntemi kullanılmıştır. Ayrıca makale çalışmasında log analiz yazılımı geliştirilmiştir. Bu yazılımda algoritma olarak apriori algoritması kullanılmıştır. Geliştirilen yazılım ile üniversite bünyesinde bir analiz yapılmış ve çeşitli sonuçlar çıkartılmıştır. Bu yazılım ile veriler daha hızlı ve kolay bilgiye dönüştürülmüştür [11].

Yapılan makale çalışmasında sistemler üzerinde yer alan hizmet sağlayıcılarının hizmet günlükleri/log kayıtları baz alındığında hizmet sistemlerine izinsiz girişlerin tespiti için uygulama katmanı kapsamında sisteme girişlerin bir örüntüsü oluşturulmuş ve bu örüntü kapsamında yetkisiz girişlerin saptanması için bir ChainSpot önerilmiştir. Bu bağlamda ağ katmanı tarafından sağlanan bilgiler ışığında uygulama katmanı sayesinde kullanıcı hizmet erişim davranışlarındaki sapmaları tespit edilmesi sağlanmaktadır. ChainSpot, kullanıcıların sıralı davranışlarını analiz etmeleri sağlanmıştır. Bu sayede siber saldırıların tespiti konusunda çeşitli önlemlerin alınabileceği görülmektedir [12].

Günümüz teknolojileri düşünüldüğünde siber saldırılarda yapay zekâ ve makine öğrenmesi yöntemleri kullanılmaktadır. Siber saldırılardan korunmak ve savunma teknikleri geliştirmek için log verilerini gözlemleyerek analiz edilmesiyle anormal davranışların tespit edilmesi mümkündür. NetFlow sistemi kullanılmıştır. Bu araç sayesinde network trafiği analiz edilerek siber saldırılar tespit edilmiş aynı zamanda networklerin daha sağlıklı çalışması sağlanmıştır. Bunun yanında Derin Sinir Ağı (DNN), Tekrarlayan Sinir Ağı (RNN) içinde XGBoost algoritması makine öğrenme yöntemi kullanılarak bir derin öğrenme modeli geliştirilmiştir [13].

Bulut sistemlerde ve dijital ortamda saklanan, dosya, klasör, video, mail gibi birçok veri bilgisayar ağlarında paylaşılmaktadır. Mevcut güvenlik sistemiyle veriler şifre kullanılarak güvenli hale getirilen birçok bilgi bulunmaktadır. Bu şifrelerin tahmin edilmesi siber saldırıları yapan kötü amaçlı kişileri tetiklemektedir. Bu saldırılar şifreli sistemlerin ana saldırılarını oluşturmaktadır. Bu kanallara yapılan siber saldırılara karşı bir güvenlik sistemine ihtiyaç vardır. Bu çalışmada kullanılan kanallarında şifreli hale getirilmesi önerisi yapılmıştır [14].

Günümüz teknolojilerinde internet kullanıcılarının hızlı artışı siber güvenlik gereksinimlerini de beraberinde getirmiştir. Bilgisayar korsanlarının sistemlere saldırılarını arttırmış ve saldırı metodolojileri ve tekniklerini arttırmıştır. Bu çalışmada öğrencilerin sanal ortamda Ağ Saldırı Tespit Sistemi kurulumu ve kullanımını

öğrenmeleri için bir platform geliştirilmiştir. Yapılan siber saldırıların IP adresleri üzerinden algoritmalar kullanarak siber saldırıları tespit etmesi sağlanmıştır. Bu sayede öğrenciler siber saldırıların belirlenmesi ve önlenmesi için birtakım kuralları öğrenmeleri sağlanmıştır [15].

Günlük tutulan logların analizi geleneksel yöntemlerle tespit edilmesi bir hayli zor olduğu bilinmektedir. Bu bağlamda log analizlerinin yapılması için profesyonel araçların kullanılması gerektiği ortaya koyulmuştur. Siber saldırı yönetimi için Güvenlik Bilgisi ve Onay İzleme Sistemi (SIEM) kullanılmaya başlandığı görülmektedir. SIEM içinde barındıran birtakım özelliklerin olması gerektiği bu çalışmada yer almaktadır. SIEM çalışma yapısı siber saldırılara karşı kullanılan bir araç haline gelmiş ve olayların gerçek zamanlı olarak izlenmesini sağlamaktadır [16].

Bilgi Teknolojileri, kullanıcıların sürekli artan istekleri doğrultusunda kullanımı gün geçtikçe artmaktadır. Bu doğrultuda işlemlerin akışı sırasındaki oluşan aksiyonların yasal dayanağa göre log kayıtlarının tutulması gerekmektedir. Bu anlamda tutulan log kayıtlarının yönetimi, güvenliği analizinin yasalar çerçevesinde bütünlüğünün sağlanması gerekmektedir. Tez çalışması kapsamında log kayıtları hakkında teorik ve pratik çalışmalar yapılmıştır. Aynı zamanda açık kaynak kod kullanarak log yönetim aracı geliştirilmiştir. Geliştirilen log kayıt aracının çalışma durumu, karşılaşılan zorluklar tez kapsamında değerlendirilip açıklamaları yapılmıştır [17].

Zafiyetlerin oluşturduğu en önemli siber risk faktörü yazılım sahteciliğidir. Bu yazılımlar kurulu olan veya üzerinde çalıştırılan sistemler üzerinde siber zafiyet oluşturarak birçok açıdan siber güvensiz ortamlara izin vermektedir. Sistemler üzerinde zararlı yazılımlar kullanılarak sistemler üzerinde oluşturduğu siber zafiyetler incelenmiştir. Zararlı yazılımlar incelenerek bir dizi önlemler sunulmuştur [18].

Makale çalışmasında ülkemizin siber suç anlamında durum tespiti yapılmış, yapılan siber saldırılara karşı yöntemler araştırılmıştır. Siber suçları kapsayan kanun ve yasaların 2016 yılında yapılmasından dolayı, çalışma 2016 yılı öncesini kapsamamaktadır. Makale çalışması kapsamında en çok çalışma yapılan ve aynı zamanda siber saldırı türü olan Hizmet Engelleme (DoS) ve Dağıtık Hizmet Engelleme (DDoS) saldırı türü olduğu sonucuna ulaşılmıştır. Siber saldırıların tespit yöntemi olarak Random Forest karar ağacı yöntemi kullanılmıştır [19].

Tez çalışmasında bilgi teknolojileri açısından bilgisayar ağları kritik altyapı sistemleri

incelenmiştir. Gelişen teknoloji karşısında bilgi teknolojileri alt yapısını güncel tutmak siber güvenlik için kaçınılmazdır. Genel olarak ulaşım, iletişim, tarım, enerji sistemleri kamu özel kurum koordinasyonlu çalışmaktadır. Siber saldırılara karşı önlemlerin arttırılması gerekmektedir. SIEM, siber saldırılara karşı koyma kabiliyetine sahiptir. Bu tez çalışmasında, öncelikli olarak kritik altyapı bilgileri yer almaktadır. Bu kritik sistem altyapılarının öncelikle ülkemizde gerekli önlemlerin alınmasını sağlamak için bir farkındalık oluşturmak amaçlanmıştır. [20].

Saldırı Tespit Sistemi (IDS), zararlı sistem faaliyetleriyle ilişkilendirilen IP (İnternet Protokol) adresleri gibi göstergelerin, Kontrolun Tersine Çevrilmesi (IoC) uygun ve doğru bir şekilde mevcut olmasına dayanır. Ancak, bu göstergelerin basit doğası ve sınırlı geçerliliği, siber tehditlere karşı korumayı zayıflatır. Taktikler, Teknikler ve Prosedürler, saldırgan davranışları hakkında soyut bilgiler sağlar, IDS kullanımı sayesinde otomatik algılamayı engeller ve ancak insanlar tarafı dan okunabilecek formatlarda bulunur. Bu makalede, karmaşık sistem davranışlarının algılanabilir desenlerini üreterek log verilerinden siber tehdit istihbaratı çıkaran ve IoC ve Taktik Teknik, Protokol (TTP) avantajlarını birleştiren bir yaklaşım önerilmiştir. Mevcut yaklaşımlardan farklı olarak, şüpheli log olaylarını ortaya çıkarmak için log verileri anormallik tespiti kullanılmış bu olaylar ardışık kümeleme, desen tanıma ve iyileştirme için kullanılır. Başka bir sistem üzerinde aynı saldırının algılanması için uygun çok adımlı bir saldırıya karşılık gelen otomatik olarak çıkarılan tehdit istihbaratının uygun olduğunu göstermektedir [21].

IoT, en çok siber saldırı alan sistemler arasındadır. Çalışmada IoT güvenliği incelenmiştir. Günümüz teknolojilerinin yeni trendi haline gelen IoT, aynı zamanda siber güvenlik açısından incelenmesi gereken teknolojiler arasındadır. IoT teknolojileri birçok alanda kullanılmakta olup, insan hayatında önemli bir yere sahiptir. IoT teknolojileri En çok siber saldırı alan sistemler arasında yer almaktadır. IoT cihazlarda güvenlik sorunu bu teknolojiyi biraz sınırlandırmıştır [22].

IoT teknolojilerine siber saldırı senaryoları uygulanmış ve analizleri yapılmıştır. IoT teknolojilerine yönelik siber saldırıların katmanlara yoğun olarak yapıldığı ortaya çıkmaktadır. Bu çalışmada yapılan analizler cihaz güvenliği, veri güvenliği, ağ ve sistem güvenliği olarak çalışmalar yapılmıştır. Araştırmaların daha derin olması için maliyet faktörü ve araştırmacı sayısı yetersiz olması, araştırmayı olumsuz etkilemiştir [23].

Internet teknolojilerindeki muazzam büyüme işlemlerin sürekli olarak dijital platformlara

taşınmasına olanak sağlamıştır. Bu teknolojik gelişmeler, evrende gerçekleşen tüm işlemlerin dijital ortama taşınmasıyla birlikte, siber saldırılara maruz bırakmıştır. Ne yazık ki işlemlerde gerçekleşen teknolojik gelişmeler güvenlik tarafında gerçekleşmemiştir. Dijitalleşen işlemlerin güvenlik açıklarının oluşması, siber uzayda siber saldırılara maruz kalmasını sağlamıştır. Siber saldırıların önlenmesi için geliştirilen sistemler bulunmaktadır. Ana Bilgisayar Tabanlı İzinsiz Giriş Sistemi (HIDS) kullanılarak, sistemleri izleyen, gerçekleşen olayları log kayıtlarını tutan, yetkililere bilgi veren bir sistemdir. Kurumlar gün geçtikçe virüsler, kötü amaçlı yazılımlar, izinsiz girişler vb. şekilde çok sayıda tehditle karşı karşıya kalmaktadır. Benzer saldırılardan korumak için saldırı tespit ve önleme sistemleri şeklinde birçok farklı mekanizma tercih etmektedirler. Bazı durumlarda tespit edilemeyen güvenlik zafiyetleri olabilmektedir. HIDS ana bilgisayar sisteminin davetsiz misafirler tarafından tehlikeye atılmasını önlemek için kullanılmaktadır. Ana bilgisayarda kötü amaçlı kodların yürütülmesini önlemek için HIDS sistem denetimini ve log kayıtlarını incelemektedir [24].

Bu makalede, Ağ İzinsiz Giriş Tespit ve Önleme Sistemleri (NIDPS), için kapsamlı bir mimari sunulmuştur. Hızla kontrolsüz bir şekilde büyüyen ve gelişen siber uzayda, NIDPS dünyanın en büyük olası saldırıları bulmak, trafiği izlemek, analiz etmek için temel ağ bileşenleri kullanılarak bir NIDPS mimarisi sunmak için çeşitli çalışmalar yapılmıştır. Ancak bu çalışmalar mevcut tüm NIDPS gereksinimlerini karşılayamamıştır. NIDPS mimarisi, Ana bileşenlerden ve bu bileşenler üzerinde veri akışından oluşmaktadır. Bu mimari tüm NIDPS bileşenlerinden kapsamaktadır. Siber saldırı olaylarında, yakalama, kod çözme modülü, ön işleme, tespit, müdahale ve yönetim dahil tüm işlevler çalıştırılmaktadır. Tespit modülü kötüye kullanım tabanlı ve anomali tabanlı yaklaşımların her ikisini de kapsamaktadır. Ayrıca anomali tabanlı algılama modülü trafik ve protokol kurallarını içerir. Anomali tespitinin yanı sıra öğrenme tabanlı yaklaşımlar da kullanılır. Önerilen mimari dört modda performans gösterecek şekilde tasarlanmıştır. Bu çalışma modları pasif yanıt modu, aktif yanıt modu, hızlı önleme modu ve mükemmel önleme modu olarak yer almaktadır. Aynı zamanda, bu varlığı nedeniyle yüksek hızlı ağlarda çalışabilen hızlı önleme modu, eksiksiz bir yönetim tasarladık daha kullanışlı işlevler sağlayan NIDPS için modül çalışmasına yardımcı olmak için diğer modüllerle ilişki kurmaktadır [25].

Teknolojinin hızlı gelişimi internet ortamında gerçekleşen bilinen ya da bilinmeyen ortamlardan yapılan siber saldırı oranlarının artmasına neden olmuştur. Bu durum siber

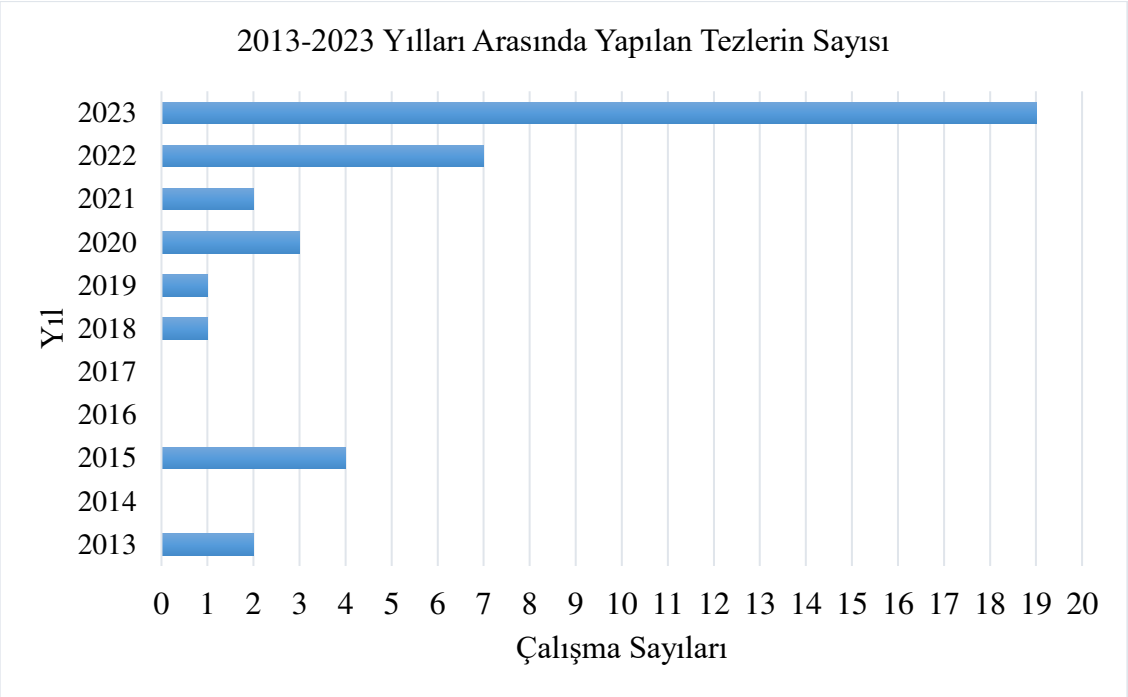
saldırıların tahribat boyutunu da aynı oranda attırmıştır. Farklı networklerden farklı siber saldırılar farklı boyutlarda hazarlar oluşturabilmektedir. Artık günümüz teknolojilerinde bu durum çok yaygın olarak rastlanılmaktadır. Yapılan siber saldırıların tespit edilmesinde birçok yöntem kullanılmakta olup kullanılan bu yöntemlerin ne kadar başarılı olduğu, doğru sonuçlar verdiği ve zaman açısından dezavantajlarının olduğu bilinmektedir. Bu çalışmada siber saldırıların doğru analizlerde daha başarılı sonuçların elde edilmesi için KDD Cup'99 saldırı tespiti veri setinin k-means kümeleme algoritması kullanılarak farklı k değerleri baz alınarak analizi ve silhouette metriği ile optimum küme sayısı belirlenmesi hedeflenmiştir. Bulunan bu metrik en iyi küme sayısı 4 ve silhouette sonucu 0.83 hesaplanmıştır. Ayrıca silhouette grafiği kalınlıkları ile küme boyutları görselleştirilmiştir [26].

Teknolojinin gelişmesi dünya, ülke ve bölgelerin kalkınmasında önemli bir role sahiptir. Ülkeler birbirleriyle diplomasi yoluyla haberleşmektedir. Teknolojinin gelişmesi ülkelerin diplomasiyi dijital ortamda yapmasına olanak sağlamıştır. Bu bağlamda dijital diplomasi birçok yönden fayda sağladığı bilinmektedir. Bu bağlamda birçok ülkede dijital diplomasi ön plana çıkmaktadır. Bu anlamda internet yönetişimi, ülkeler arası dijital iletişim, dijital devlet veriler, siber suçlar, dijital altyapı, siber casusluk, ülkeler arası siber saldırılar ülkelerin dijital diplomasi yapısını oluşturmaktadır. Scopus ve Web of Science (WoS) veri tabanlarında yer alan siber diplomasi çalışmaları bibliyometrik analizi yapılmıştır [27].

1.2. LİTERATÜRE KATKISI

Siber güvenlik hem araştırmacılar açısından hem de çalışma konusu olarak zorlanılan çok tercih edilmeyen alan olarak bilinmektedir. Bu bağlamda yapılan tez çalışması literatürdeki eklenerek, siber araştırmacılarına kaynak olacağı ve katkı sağlayacağı düşünülmektedir.

Akademik çalışmalar içinde, 2013-2022 yılları arasında siber saldırıları konulu 20 tez çalışması Şekil 1.2 de yer almaktadır. Şekil 1.2 de yer alan veriler Yükseköğretim Kurulu Başkanlığı tez merkezinden alınmıştır. Şekil 1.2 de yer alan verilere göre siber saldırı konusunda yapılan çalışmaların giderek artacağı düşünülmektedir.



Şekil 1.2. Siber saldırı konulu tez çalışmalarının yıllara göre dağılımı

Ayrıca son 10 yıl içinde yer alan tez çalışmalara ek olarak 2013-2023 yılı arasında yapılan TR Dizin makale çalışmaları incelenmiştir. Bu bağlamda siber saldırı konulu makale çalışmaları literatür taraması yapılmıştır. Çalışma yapılan veriler DergiPark veri tabanından alınmıştır. DergiPark 'tan alınan verilerine göre, 2023 yılında 2, 2022 yılında 1, 2020 yılında 2, 2018 ve 2017 yıllarında 1'er adet makale çalışması yapıldığı görülmektedir.

2. MATERYAL METOT

2.1. LOG KAVRAMSAL ÇERCEVE, YASAL ZORUNLULUK VE GÜVENLİK STANDARTLARI

2.1.1. Log Kavramı, Log Kayıtları ve Dosya Türleri

2.1.1.1. Log Kavramı

Log kavramı, kelime olarak kütük, günlük tutmak anlamlarına gelmektedir. Türk Dil Kurumu (TDK)' ya göre birlikte işlenen ve bu işlemler üzerinden oluşan ilgili kayıtların oluşturduğu verilerdir. Log kayıtları, günümüz sistemlerinde internet teknolojilerinin kullanılması sanal ortamda gerçekleşen tüm aksiyonların kayıtlarını tutmak için kullanılmaktadır. Ayrıca günümüzde log için kullanılan birçok tanım bulunmaktadır. Log, olayda gerçekleşen tüm yapılan işlemlerin hepsidir [28].

Log kayıtlarının tutulmasının altında birçok gerekçe yer almaktadır. Bu gereksinimler, siber güvenlik, adli analiz, sistem hatalarının tespit edilmesi ve giderilmesi, kullanıcı hataları, network sistemleri iyileştirilmesi, analiz ve raporlama işlemlerinin yapılabilmesini sağlamaktadır. Log kayıtları adli bilişim analizleri, siber güvenlik, sistemlerin üzerinde gerçekleşen olayların kayıtlarından oluşan günlük zamansal dosyalardır. Network sistemleri üzerinde log kayıtlarının tutulması bu sistemlerin iyileştirilmesinde, güvenliğinin sağlanmasında, sistemlerin analizinde kullanılmaktadır. Ayrıca network sistemlerinde oluşabilecek davranışların tahmin edilmesi süreçlerinde yol haritası olarak kullanılabileceği düşünülmektedir.

Log kayıtlarının önemi ilk olarak, Amerika Birleşik Devletleri (ABD) Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), tarafından vurgulanmıştır. Bu anlamda bilgisayar güvenliği log yönetimi için en iyi uygulamaları ve önerileri oluşturmaktadır. NIST, 2002 tarihli Federal Bilgi Güvenliği Yönetimi Yasası (FISMA), Kamu Hukuku 107-347 bünyesinde yasal açıdan gerekli olan işlemlerin yerine getirilmesi amacıyla oluşturmuştur. Bu yayın, kuruluşların bilgisayar güvenliği günlük yönetimi ihtiyacını anlamalarına yardımcı olmayı amaçlamaktadır. Günlük log kayıtlarının yönetimi uygulamalarının geliştirilmesi, uygulanması ve sürdürülmesi konusunda pratik bilgiler

bulunur. Yayın, logların kaydetme teknolojilerini üst düzey bir bakış açısı sunar [29].

Loglar, cihaz, yazılım, işletim sistemi veya sunucular üzerinden gelen olayların kayıtlarını oluşturan verileri, belirli periyotlarla haftalık, günlük, saatlik olarak tutulan dosyalardır. Log, bilişim sistemlerinde meydana gelen işlemlerden üretilen kayıt bilgileridir. Örneğin bir uçağın log kayıtları kara kutusudur. Aslında internet sistemleri üzerinde yer alan log kayıtları da aynı durumdadır. Log dosyalarını açmak için bir kelime işlemci programına ihtiyaç duyulur. Bunlar, Microsoft Word, LibreOffice, OpenOffice, Notepad ++ programları kullanarak log dosyalarını açılabilir [28].

2.1.1.2. Log Kayıtları

Log kayıtları, sistemler üzerinde gerçekleşen aksiyonların bilgilerini tutmaktadır. Log kayıtlarında, kullanıcı bilgilerini, zaman bilgilerini, adres bilgilerini yer almaktadır. Sistemler üzerinde oluşan işlemlerin kayıt bilgilerini, bu sayede yapılan işlemler hakkında tüm aksiyonlar verileri loglar ile ortaya çıkartılmaktadır. Tutulan log kayıtları ile sisteme erişim sağlayan cihazların, kullanıcı bilgileri, IP adresi, MAC adresi, erişim zaman bilgileri, işletim sistemi bilgileri, işlem yaptıkları hizmet bilgileri gibi birçok veri kaydı tutulur. Çizelge 2.1.'de yer alan log kayıtlarında yer alan önemli veriler yer almaktadır [8].

Çizelge 2.1. Log kayıtları üzerinde yer alan açıklamalar [8].

Alan Adı	Örnek Değer	Açıklama
Date	2015-11-20	Aktivitenin gerçekleştiği tarih
Time	00:22:31	Aktivitenin gerçekleştiği saat
c-ip	212.154.80.164	İstekte bulunan IP adresi
s-ip	193.140.180.4	Web sitenin yer aldığı sunucunun IP adresi7
cs-url-stem	/Default.aspx	İstekte bulunan web adresi
cs-status	200	İsteğe verilen cevabın durum kodu
cs(user-agent)	Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;)	İstemci tarafından kullanılan tarayıcının tipi ve diğer özellikler
cs-referrer	-	Aktif sayfaya hangi kaynaktan geldiğini gösterir

Log kayıtlarında en çok kullanılan ve incelenen veriler aşağıdaki gibidir,

- Log girdilerinin türü,
- Üreten sistem bilgileri,
- Üretildiği uygulama ve bileşen bilgileri,
- Log mesajının önem düzeyi,
- Logların kullanıcı bilgileri,
- Kullanıcıların IP ve MAC adres bilgileri,
- Zaman damgası,

2.1.1.3. Log Kayıtlarında Yasal Zorunluluk

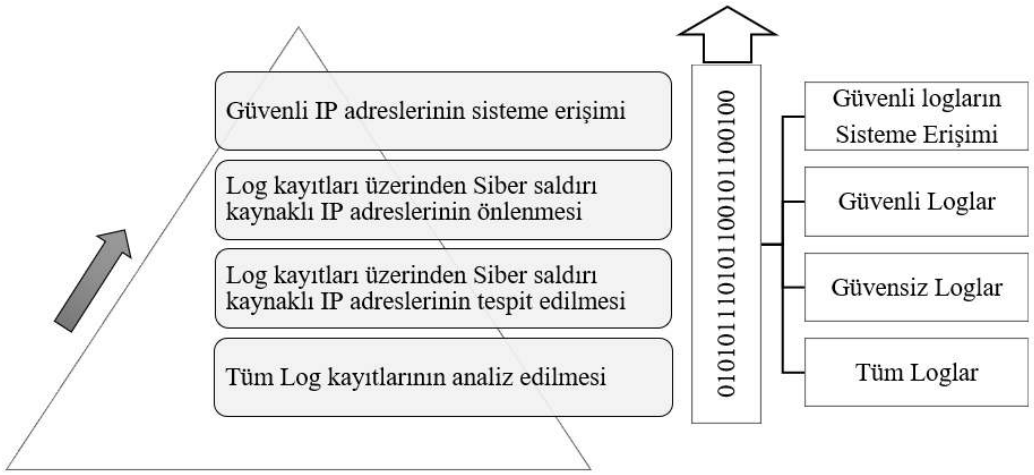
Log kayıtları, 5651 sayılı kanun kapsamında tutulmaktadır. Tutulan loglar loglama sistemleri yöntemiyle yasa gereği belirli süre saklamaktadır. Log kayıtları internet üzerinde gerçekleşen aksiyonları kontrol ve kayıt altına almak için yapılmaktadır. 5651 sayılı yasaya göre loglamanın iki önemli amacı bulunmaktadır. İlk önemli amacı, internete yön veren içerik sağlayıcı, alan sağlayıcı, erişim sağlayıcı, topluma açık internet sağlayıcıların görev ve sorumluluklarını belirlemektir. Diğer amacı ise, siber uzayda gerçekleşen suçların tespit edilmesi yer almaktadır. Log kayıtları sonraki süreçte arşivlenerek sıkıştırılıp sistem veya bulut üzerinde tutulmaktadır. Log kayıtları veri tabanında ne kadar süre kalması gerektiğiyle ilgili herhangi bir madde yer almamaktadır. Ayrıca log kayıtları 6 aydan az, iki yıldan uzun olmamak şartıyla kanun gereği saklanmak zorundadır. Saklanan log kayıtları yetkili merciler tarafından incelenmesi sağlanır. Bu doğrultuda kurumlar log kayıtlarını 5651 yasaya uygun bir şekilde log tutmakla yükümlüdürler. [30].

2.1.1.4. Log Kayıtlarının Amacı

Log kullanımı, sistem yöneticileri, adli analiz, bilişim analizleri gerçekleştirmek için kullanılmaya başlanmıştır. Akabinde günümüz teknolojilerinde log kayıtları ve log analizleri giderek artmaktadır. Bilişim sistemlerinin verimliliğin ve bilgi bütünlüğünün arttırılması gibi birçok işlemler için kullanılmaktadır. Şekil 2.1 de log kayıtlarının siber güvenliğe etkisi yer almaktadır. Kullanıcılar güvensiz ortamdan güvenli ortama doğru ilerlemekte ve güven vermeyen loglar üzerinden bazı kullanıcıların engellenebildiği yer almaktadır.

Log kayıtları, siber suçların tespit edilmesinde hayati öneme sahiptir. Bu anlamda log kayıtlarının tüm sistemler üzerinde yer alması ve tüm işlemler doğrultusunda log kayıtlarının tutulması gerekmektedir. Log kayıtlarının tutulmasındaki en önemli amaçlar içinde yer alan olağan dışı işlemlerin tespit edilmesinde kullanılmasıdır [30]. Log kayıtlarının amaçlarından bazıları,

- Güvenlik zafiyeti tespit etme,
- Zamandan tasarruf,
- Güvenli veri transferi,
- Sistem üzerinde otorite sağlama,
- Siber saldırılara karşı caydırıcı etkisinin olması
- Sistemler üzerinde oluşan hataları giderme,
- Sistem üzerinde Performans arttırma,
- Sistem üzerinde iyileştirme,
- Analiz ve raporlama,



Şekil 2.1. Logların güvenli IP erişim piramidi

2.1.2. Log Kayıtlarının Tutulduğu Farklı Sistemler

Sistemler üzerinde tutulan log kayıtları cihaz, görev, sunucu, bulut sistem, veri tabanı, kullanıcı işlemleri, login gibi yapılan çeşitli işlemlere göre değişiklik gösterebilir. Bu anlamda web sunucu, veri tabanı ve işletim sistemleri üzerinde farklı dosya formatlarında log dosyaları oluşmaktadır [31].

2.1.2.1. Linux Sistemlerinde Log Kayıtları

Linux işletim sistemi, dosya tabanlı dosya sistemine sahiptir. Linux sistemlerinin bu özelliği farklı dosya formatlarının kullanılmasını sağlayan araç bulunmaktadır. Bu araçlar, *cut, awk, grep, ngrep, less, tail, head, sort, sed, cad unig, strings, multitail, urlsnarf.* Log kayıtlarının, linux sistemleri üzerinde tutulması, hız, performans, esneklik gibi bazı avantaları beraberinde getirmektedir. Ayrıca bazı dezavantajları bulunmaktadır. Bu dezavantajlar veri tabanı özelliği olmadığı için yapılan her işlem tekrar etmesi gerekmektedir. Kapasitesi büyük log dosyalarının alınmasında süre kaybı ve performans kaybı yaşayabilir. Sistemler üzerinde hayati önem arz eden dosyalar arasında log dosyaları da yer almaktadır. Linux sistemlerde log kayıtları /var/log/ dizini içinde tutulmaktadır. Linux ortamında log kayıtları dört farklı türde tutulmaktadır [32].

Bu log türleri,

- Sistem Logları
- Servis logları
- Olay logları
- Uygulama logları

2.1.2.2. Windows Sistemlerinde Log Kayıtları

Sysmon (system monitor) yüklenen sistem üzerindeki aksiyonları kayıt altına alarak kullanılan Microsoft firmasının geliştirdiği loglama aracıdır. Kurulum ve gerekli konfigürasyon yaparak kullanılır [31].

Linux ve Unix sistemlerde yorumlanması analiz edilmesi açısından daha rahat yapılmaktadır. Windows tabanlı sistemlerde log düzenlemek için komut satırı olmadığı için bazı sorunlar ortaya çıkmaktadır. Windows tabanlı sistemleri inceldiğimizde log yönetimi için syslog aracının Windows desteği yoktur. Bunun için üçüncü parti yazılımlar kullanılmaktadır.

Windows Olay Günlüğü: Windows işletim sistemleri üzerinde, sistemi yöneten ve kullanan kullanıcıların günlük olaylarını lokal ya da bulut üzerinden işlenmesini ve görüntülenmesini sağlayan sistemdir [31].

Uygulama programları ve İşletim Sistemi yöneticinin işletim sistemlerinden kaynaklanan problemleri gidermek için kullanılan donanım ve yazılım hareketlerinin kaydedilmesini

sağlayan log kayıtlarıdır. Windows logları, çalışan uygulamaları, güvenlik uzmanları, sistem kurulum olayları, sorunları aynı zamanda hataları yazmaktadır [32].

2.1.2.3. Ağ ve Güvenlik Sistemlerinde Log Kayıtları

Firewall, Router, Switch, Wireless, Sanal Özel Ağ (VPN) sistemleri, IPS'ler bu tür network cihazlarında log kayıtları tutmak için program tutulması için syslog aracı kullanılmaktadır. Bu sayede uzak sistemlere log gönderilerek log kayıtları tutulmak ve saklanmaktadır [33].

2.1.2.4. Web Sunucu Log Kayıtları

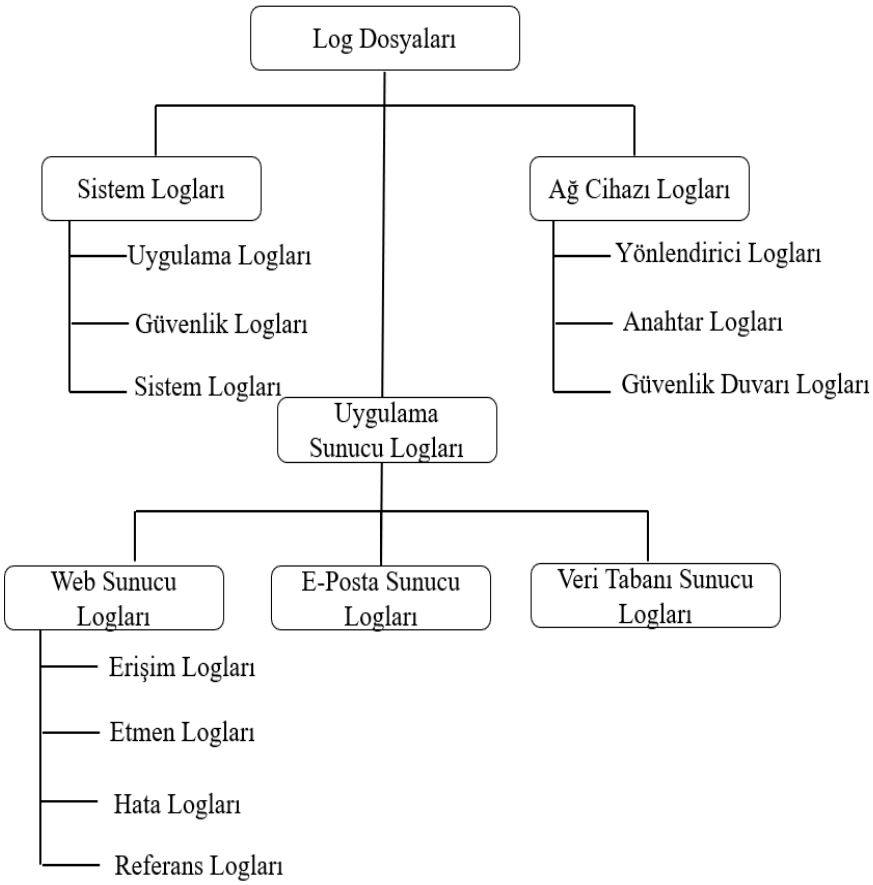
Web sunucu üzerinde oluşan loglar, düz metin ASCII dosyalarıdır. Bu loglar, browserlar üzerinden sunuculara erişim sağlayan istemcilerin aksiyonlarını düz metin olarak saklar. Sistemler üzerinde oluşan bu loglar önemli birçok veriyi oluşturmaktadır [33].

2.1.2.5. Veri Tabanı Sistemlerinde Log Kayıtları

Loglama, veri tabanı sistemlerinde iki farklı yolla yapılmaktadır. Bunlar Audit ve veri tabanı sunucusuna giden trafiği pasif olarak izleyen ve sorgulamaları anlamlı bir şekilde kaydeden sistemlerdir. Audit, incelemek ve denetlemek gibi anlamlara sahiptir. İşletim sistemleri üzerinde kullanıcı ve sistem aksiyonlarını kayıt altına alarak ileriye dönük inceleme yapılabilmesine olanak sağlayan bir altyapıdır. Log kayıtları veri tabanı yapısına ve gereksinimlere göre log kayıtları tutulmaktadır. Performans ve hız sorunları olan sistemlerde aktif olmayan/pasif loglama sistemleri tercih edilmektedir. Pasif sistemlerin maliyeti aktif loglama sistemlerine göre daha fazla maliyet getirmektedir. Veri tabanı sistemlerinde Audit sistemi kullanılıyorsa gereksiz log kayıtlarından uzak durulması gerekmektedir [33].

2.1.3. Log Dosya Türleri

Literatürde birçok log türü bulunmaktadır. Bu tez çalışmasında, siber saldırıların tespitini yapabilecek log kayıtları araştırılmıştır. Bu sayede tezin çalışma amacına ulaşılması hedeflenmektedir. Loglar farklı sistemlerde farklı içerikler ve farklı isimler oluşturabilir. Bu log çeşitleri Web Sunucu, mail sunucu, veri tabanı, sistem logları, güvenlik duvarı logları olarak tanımlanmaktadır [8]. Şekil 2.2' de gösterilen görselde log çeşitleri üç ana başlılıkta incelenmektedir. Log dosya türleri incelendiğinde genel olarak en çok karşımıza çıkan log dosya türleri Şekil 2. 2'de yer almaktadır.



Şekil 2.2. Log dosyaları türleri şeması [8].

2.1.3.1. Sistem Logları

Windows tabanlı işletim sistemleri üzerinde gerçekleşen aksiyonlardan oluşan log dosyalarıdır. İşletim sistemleri üzerinde gerçekleşen bazı olaylardan oluşmaktadır. Bu olaylar/aksiyonlar, sürücü işlemleri, sistem bilgileri üzerindeki işlemlerden oluşan log dosyalarını oluşturur. Sistem logları üç başlıkta incelenmektedir [8].

Uygulama logları: İşletim sistemi üzerinde çalışan programların kullanımından oluşan verilerin kaydedildiği log dosyalarıdır [33].

Güvenlik logları: Güvenlik logları sistemler üzerindeki, dosya, oturum ve kaynak kullanım işlemlerinin oluşturduğu loglardan meydana gelmektedir. Güvenlik logları incelemelerinde yönetici oturumuyla sisteme erişim sağlamak gerekebilir [33].

Sistem logları: Windows işletim sistemi araçları üzerindeki işlemlerden kaynaklanan verilerin tutulduğu log dosyalarıdır [33].

2.1.3.2. Ağ Cihazı Logları

Birden fazla bilgisayarın haberleşmesini sağlayan, bilgisayar ağlarını oluşturan network cihazlarıdır. Bilgisayar ağları üzerinde oluşan işlemlerden kaynaklanan verileri oluşturan log dosyalarıdır. Bilgisayar ağları üzerinde konumlandırılan, anahtar (Switch), yönlendirici (Router), güvenlik duvarı (Firewall) cihazları üzerindeki işlemlerden oluşan log dosyalarıdır. Bu log dosyaları içinde, cihaz arayüzleri işlemleri, konfigürasyon bilgileri, ağ üzerindeki trafikten kaynaklanan işlemler den oluşan verilerdir. Sistemlerin güvenliği açısından, tutulan log kayıtları içinde önemli veriler yer alır. Ağ cihazı logları üç farklı log türüyle incelenmektedir [33].

Yönlendirici log dosyaları: Bilgisayar ağlarını oluşturan sistemlerin birbirleriyle iletişimini sağlayan network cihazlarıdır. Yönlendirici cihazlar OSI referans modelinin üçüncü katmanında çalışmaktadır. Bilgisayar ağları arasında oluşan trafiğin loglarını oluşturur [33].

Anahtar log dosyaları: Bilgisayar ağları üzerinde kullanılan network cihazlarıdır. Açık Sistemler Arası Bağlantı (OSI) referans modelinin 2. ve 3. Katmalarında çalışmaktadır. Bu cihazlar üzerindeki işlemlerin verilerini tutan log dosya türüdür [8].

Güvenlik Duvarı logları: Bilgisayar ağları üzerinde çalışan sistemler güvenliğini sağlayan yazılımsal ve donanımsal cihazlardır. Güvenlik duvarı üzerinde gerçekleşen logları oluşturur [33].

2.1.3.3. Uygulama Sunucu Logları

Sunucu işletim sistemleri üzerinde gerçekleşen aksiyon/olaylardan oluşan log dosyalarıdır. Sunucu işletim sistemi üzerinde gerçekleşen, veri tabanı işlemleri, işlemleri, hata mesajları, bağlantılar, sunucu erişimleri, çalıştırılan araçlar, çalışan komutlar, sistem giriş bilgileri işlemlerinden oluşan log dosyalarıdır [33].

E-Posta Sunucu Logları: E-Posta sunucuyu incelediğimizde mail işlemleri için Postane Protokolü (POP3), Basit Mail Aktarım Protokolü (SMTP), İnternet Mesaj Erişim Protokolü (IMAP) gibi protokoller kullanılmaktadır [31].

E-Mail gönderilmesi ve alınması için POP3, SMTP ve IMAP protokolleri kullanılmaktadır. Sunucu ile sunucu ve user ile sunucu arasında mail gönderimi SMTP için 25 nolu port şifrelenmemiş ve 465 nolu port SSL ile şifrelenmiş olarak mail gönderimi gerçekleşir [32].

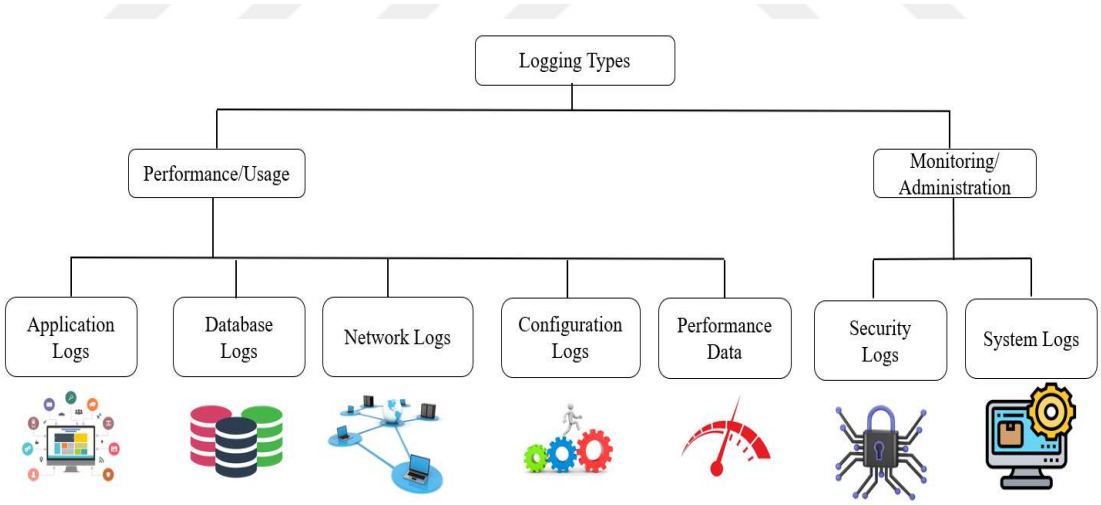
Günümüzde mail sunucuda kimlik doğrulama işlemi gerektirdiği durumlarda 587 nolu port kullanılmaktadır. Spam maillerinin artması yüzünden 25 numaralı port yerine 587 numaralı port kullanılmaktadır. 3. Parti mail programları da 465/587 numaralı portlar kullanmaktadır [32].

POP3 ve IMAP 3. Parti mail istemcilerinde kullanılan protokollerdir. Bu işlemler sunucu işlemlerinde log dosyalarını oluşturur [32].

Veri Tabanı Sunucu Logları: Log kayıtlarının kalıcı tutulduğu veri tabanlarını oluşturur. Log kayıtlarının analizi için log kayıtlarının belirli süre saklanması gerekmektedir. Bu log kayıtları sistem üzerinde veri taban sistemlerinde tutulur. Veri tabanı üzerinde gerçekleşen işlemlerin dosyalarını oluşturan loglarıdır [33].

Web sunucu logları: Dört farklı sunucu log tipi bulunmaktadır. Bu loglar, Erişim bilgileri logları, Faktör logları, Hata mesajı logları, Referans bilgileri loglarıdır [33].

Sistemler üzerinde tutulan logların, kullanıldıkları teknolojilere göre farklılık gösterebilir. Farklı bir kaynaktan alıntı yapılan log dosya türleri Şekil 2.3 de yer almaktadır. Log türleri iki başlıkta incelenmektedir. Log türleri içinde güvenlik log türleri, sistem log türleri, performans log kayıt türleri göze çarpmaktadır [33].



Şekil 2.3. Log dosya türlerinin görseller ile gösterimi [33].

Log dosya türleri, kaynağı ve kullanım bilgileri Çizelge 2.2'de yer almaktadır.

Çizelge 2.2'de farklı sistemler üzerinden elde edilen log kayıtları ve kaynakları yer verilmiştir.

Çizelge 2.2. Log dosya türlerine göre kaynak türleri [33].

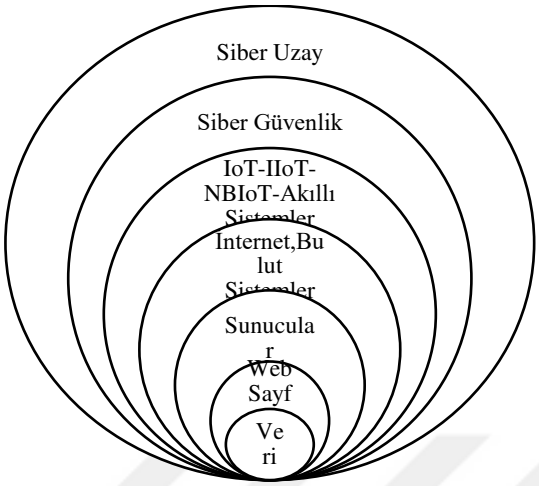
SN	Log Türü	Source	Usage
1	System Log	Operating Systems Like Windows Or Linux Etc.	Operating Systems Activites Logs
2	Network Log	Network Devices	Network Communiction Logs
3	Security Log	Authentiction Schemes	Security Related Logs
4	Web Server Log	Web Servers	Related To Web Server Activities
5	Appliction Log	Custom Appliction Logs	Developers Monitor Applictions
6	Setup Log	Application İnstallers	Installer Logs
7	VM Log	Virtual Resource Managers Like VM Ware Etc	Log Used By Virtual Machines
8	Custom Audit Log	Custom Appliction Logs	Miscellanecus Authentiction Requests

Ayrıca farklı log dosya türleri burada göze çarpmaktadır. Log dosya türlerinin sayısının artması siber saldırıların tespit edilmesini ve log analizini kolaylaştırdığı görülmektedir. Bu bağlamda network sistemleri üzerinde kullanılan loglama teknolojileri network sistemlerinin analiz ve yorumunu hızlandırmaktadır.

2.1.4. Logların Siber Güvenlik Açısından Kapsamı

Sistemler üzerinde bilgi güvenliğinin kullanıcılar acısından ne kadar hayati öneme sahip olduğu bilinmektedir. Dijital veriler içinde, kişisel bilgiler, sağlık bilgileri, ticaret, bankacılık, eğitim ve sosyal alanlarda birçok veri yer almaktadır. Bu anlamda bilgi güvenliğinin sağlanması açısından tüm verilerde gizlilik esastır. Ayrıca ülkeler, kurumlar, işletmeler, dijital ortamda hizmet sunan tüm dijital verilerini daha kapsamlı korumak ve veri bütünlüğünü sağlamak için sistemlerinin siber anlamda güvenliği sağlamak için yüksek bütçeler harcamaktadır. Log sistemlerinin geliştirilmesi ve yaygınlaşması bu harcamaların önüne geçebileceği düşünülmektedir [32].

Siber güvenlik, donanım, yazılım, kullanıcı güvenliği başta olmak üzere tüm sistemleri içinde barındırır. Şekil 2.4'de yer alan siber güvenlik kapsamı yer almaktadır. Siber güvenliğin tüm sistemlerde ilk sırada yer aldığı görülmektedir.



Şekil 2.4. Siber uzayda siber güvenlik.

2.2. LOGLAMA SİSTEMLERİ

Loglama cihazları internet kullanıcılarına açık ve ücretsiz giriş izni veren network sistemleri üzerine konumlandırılan yazılımsal ve donanımsal cihazlardır. Log sistemleri yazılımsal olarak da network sistemleri üzerinde konumlandırılırlar. Bu nedenle loglama sistemleri üzerinde yazılımsal araçlar, donanımsal anlamda harddisk işlemci ram gibi elektronik cihazlarda kullanılabilmektedir. Bu anlamda kullanıcıların loglama sistemlerini kullanarak internete erişimi sırasında bazı prosedür işlemlerini onaylamaları gerekmektedir. Buradaki amaç internet kullanıcısının gerçek kullanıcı olduğunu öğrenip, internete giriş bilgilerini kayıt altına almaktadır. Aynı zamanda bu durum kullanıcıların internete güvenli bağlanmalarını ve kişisel verilerinin kayıt altına alınarak korunmasını sağlamaktadır. Bu bürokrasi durumu 5651 sayılı yasa ile düzenlenmiş olup, kanun gereği kullanıcıların log kayıtları tutulmaktadır [34].

2.2.1. Loglama Sistemlerinin Kullanıldığı Yerler

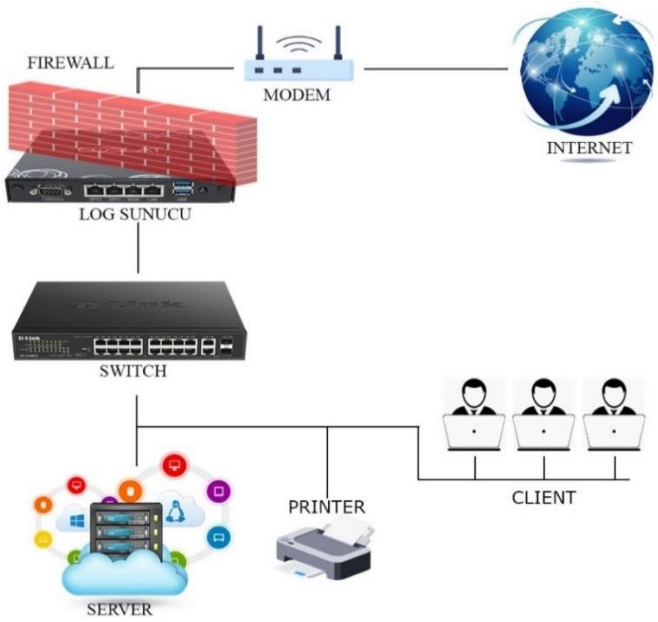
Loglama cihazları, internet kullanımının halka açık olduğu ortamlarda kullanılmaktadır. Kullanıcıların internete erişimi sırasında kimlik doğrulama yöntemleri kullanılarak internete erişimleri söz konusudur. Ayrıca kullanıcıların internet erişimleri sırasında

meydana gelen tüm işlem ve süreçlerin loglama yöntemiyle kayıt altına alınmaktadır.

2.2.2. Loglama Sistemlerinde Kullanılan Donanımsal Cihazlar

Log kayıt cihazları, network sistemleri üzerine konumlandırılan, cihazlardır. Network sistemleri üzerine konumlandırılan log kayıt cihazları network üzerinde gerçekleşen aksiyonların log kayıtlarının tutulmasını sağlar. Bu cihazların belli bir disk kapasitesi, işlemcisi, ram kapasitesi gibi donanımsal birtakım özelikleri bulunmaktadır. Bu özellikler loglama sistemi üzerindeki donanımsal özellikleri oluşturur. Loglama sistemleri, network sistemleri üzerinde modem cihazı ile Hub/Switch arasına konumlandırılır. Şekil 2.5 incelendiğinde log sistemlerinin network ortamında nereye konumlandırıldıkları yer almaktadır. İnternet üzerinden gelen kullanıcılar modem den sonra loglama sistemine erişimleri sağlanır. Kullanıcı bilgileri loglama sistemi sayesinde kayıt altına alınarak kullanıcıların sistemlere erişimi sağlanır.

Donanımsal loglama araçları modem sonrasında kurulan, network ortamına dahil olan cihazlardır. Bu cihazların içinde logların tutulması için gerekli yazılımsal araçlar yer almaktadır. Loglama cihazları, kamuya açık kablosuz internet hizmeti sağlayan, otel, restoran, belediye, kafe, eğitim kurumları gibi yerlerde internet erişimini daha güvenli hale getiren, kullanıcıların birtakım bilgilerini kayıt altına alan sistemdir [34].



Şekil 2.5. Log cihazlarının network üzerindeki yerleşim şeması.

Loglama Cihazlarındaki Önemli Özellikleri

- Web arayüzünde Türkçe dil desteği ve raporlama
- Kişisel Verilerin Korunması Kanunu (KVKK) ve 5651 uygunluğu, Elektronik Zaman Damgası ile imzalı kayıt
- Virgülle Ayrılmış Değişkenler (CSV) ile toplu kullanıcı ekleme
- TC, SMS ve doğum tarihi ile kimlik doğrulama seçenekleri
- Çoklu kayıt seçeneği ve Yönetici bilgilendirmesi
- Kota ve bant genişliği yönetimi ve Radius Sunucu ile entegrasyon
- İzinli Medya Erişim Protokolü (MAC) ve IP adresi tanımlaması
- Active Directory (AD) entegrasyon
- Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) sunucu desteği
- Üçüncü parti uygulamalar ile entegrasyon
- Hiper Metin Transfer Protokolü (HTTPS) karşılama ekranı
- Güvenlik Duvarı özelliği ve External Portallar ile entegrasyon

Şekil 2.6'de güncel olarak kullanılan log server görselleri yer almaktadır. 5651 log cihazları bir modemi, switch andırmaktadır.

Şekil 2.6. 5651 Loglama cihazı iç ve dış görünümü [34].

2.2.3. Loglama Sistemlerinde Kullanılan Yazılımsal Araçlar

Log kayıtlarının tutulması için sunucu ve güvenlik duvarı cihazlarına yüklenen üçüncü parti loglama yazılım araçlarıdır. Yazılımsal araçlarda kullanıldıkları sistemlere entegrasyonu ve uyumluluğu sağlanmalıdır. Belirli lisans kapsamında alınarak kullanılmaktadır. Bu araçların çeşitleri aşağıda yer almaktadır [32].

Loglama Araçlarındaki Önemli Özellikler;

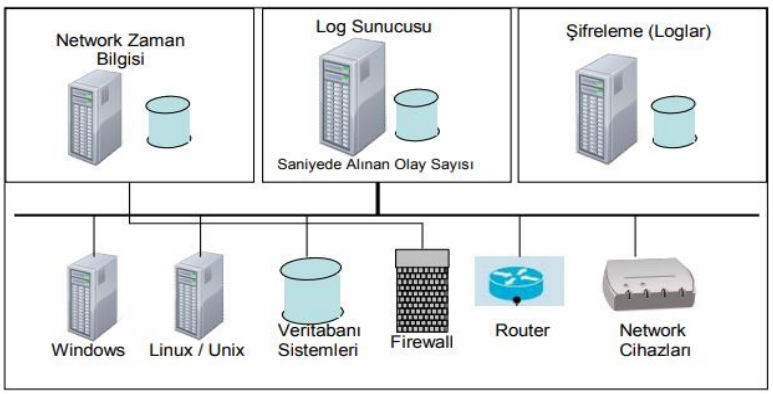
- Donanım maliyetinin olmaması, Türkçe ve farklı dil desteği,
- Fiziksel ve enerji kullanımı açısından ergonomik olması,
- Üçüncü parti uygulamalar ile entegrasyon
- Güvenlik Duvarı özellikleri
- External Portallar ile entegrasyon

2.3. LOG YÖNETİMİ, ANALİZİ VE GÜVENLİĞİ

2.3.1. Log Yönetimi

Sistemler üzerinden toplanan loglar yönetim anlamında, log toplama kadar önemli bir yere sahiptir. Log yönetimi, sistemler üzerinde gerçekleşen logların doğru yönetilmesi, güvenliğinin sağlanması, filtreleme, doğrulama ve analizi gibi işlemleri kapsamaktadır. Log yönetimi, log toplama standartlarına uygun olarak yapılmalıdır. Farklı sistemlerinde yer aldığı log yönetim şeması Şekil 2.7'de yer almaktadır [17].

Siber güvenlik anlamında log yönetimi ve analizi organizasyonlara göre farklılık gösterebilir. Yetkili personel dahilinde log yönetimi gerçekleştirilir. Analizler sonucu sistemler üzerinde iyileştirmeler yapılabilir [32].



Şekil 2.7. Log yönetimi kalite sistem şeması [17].

2.3.1.1. Normalizasyon

Normalizasyon, veri tabanında yer alan verilerin tekrarlardan ayrıştırma işlemidir. Aynı zamanda loglar üzerinde kaynak verilerin bütünlüğünü etkilemeyecek şekilde, log kayıtlarından kullanılabilecek bir veri çıkarmak için, korelasyon aracının belirlenen düzeyde kabiliyetinde olması gerekir. Log verilerinin düşürülmesi için, belirlenen nitelikler doğrultusunda veriye filtre uygulamaktır. Çalışma kapsamında, log verilerinin sayısında meydana gelen azalma, işlemlerin hem logların incelenmesi hem de logların veri tabanı üzerinde kayıtlarının tutulma süreçleri log standartları doğrultusunda yapılması, gereksiz zaman ve performans açısından sistem üzerinde kolaylık sağlayacaktır [17].

2.3.2. Log Analizi

Dijital sistemler üzerindeki hareketlerin loglama yapısına uygun olarak kayıtlarının tutulduğu loglar, cihazların sistemler üzerinde oluşturduğu izlerdir. Log analizleri birçok amaç için kullanılmaktadır. Ayrıca log analizlerini yapan, açık kaynak yazılımlar, ücretli ve ücretsiz birçok log analizi yazılımı mevcuttur. Log analizi yapan birçok yazılım aynı zamanda log yönetimi özelliği de bulunmaktadır. Log analiz programları bir veri tabanı ile bağlantılı bir şekilde çalışmaktadır. Ayrıca oluşan loglar veri tabanı olmadan belirli dosya formatlarında tutulabilmektedir. Bu uzantılar log analizi programına göre değişebilmektedir. Log analizinde en önemli bileşen log içinde ne aradığının bilinmesidir. Bunun için daha önce yapılan log analizlerinden tecrübe edinilebilir [34].

Log Analiz çalışmalarının düzenlenmesi

- Log standartlarının düzenlenmesi,
- Log yönetimi ve analizinin yaygınlaştırılması,
- Log analizlerinin hangi IP adresinden başarılı giriş sağladığı ve başarısız girişlerinin incelenmesi,
- Sistemler üzerinde log analizinin arttırılması,
- Güvenlik duvarı üzerindeki log analiz araçlarının geliştirilmesi ve desteklenmesi,
- Açık kaynak kodlu yazılım ile siber saldırı analizi yapan uygulama geliştirilmesi,

Küçük ve orta ölçekli işletmelere yapılan siber saldırılar, işletmeler açısından, siber tehdit ve endişe yaratmıştır. Ortaya çıkan siber güvenlik problemleri gelişmekte olan ülkeler

için sorun olusturmaktadır. Siber güvenlik araştırılmaya açık konulardan birisidir. Bu çalışmada Afrika'daki Küçük ve Orta Büyüklükteki İşletme (KOBİ) işletmeleri açısından siber güvenlik olgusu araştırılmıştır. Üç vaka incelemesi yapılmış, nitel yaklaşımlar ve siber güvenlik verileri incelenmiştir. Yaklaşık 150 çalışanı olan KOBİ işletmeleri üzerinde araştırmalar yapılmıştır. Bu kobiler üzerinde KOBİ'lere izinsiz giriş tespiti ve sunucu logları incelenmiştir. Bu bağlamda güvenlik mekanizmaları oluşturulmuştur [35].

Log analizleri, sistemler üzerinde oluşan problemlerin ortaya çıkarılmasında ve giderilmesinde önem arz eden verilerin elde edilmesinde kullanılmaktadır. Bu oluşan log verileri analiz edilerek, sorunlara çözüm önerileri veya anormallikleri tespit edebilir. Ayrıca network işleyişini sistem uzmanlarına loglar ile anlatmaya çalışır. Sistemler üzerinde gerçekleşen log analizleri, sistemin performansına ve davranışına ilişkin değerli içgörüler sağlayabilir. Network üzerinde oluşan günlük işlemlerinizi analiz ederek, network sistemi üzerinde gerçekleşen olumlu olumsuz davranışların haritasını çıkartmanıza yardımcı olur. Log analizleri, kanun kapsamında yapılmaktadır. Log verilerini ilgili yasaya uygun olarak analiz ederek, sistem üzerinde oluşan güvenlik ihlallerini ve anormal davranışları tespit etmek için log kayıtlarının tutulmaktadır. Bu anlamda elde edilen analiz sonuçları siber saldırıların tespiti ve engellenmesinde kullanılabilir olduğu görülmektedir [36].

2.3.2.1. Log Analizi Metodoloji Adımları

Adım 1 Log dosyasının elde edilmesi – Log dosyalarının normalleştirilmesi

- Bir web sunucu üzerindeki logların toplanması, logların normalleştirilmesi

Adım 2 Log analiz amacının belirlenmesi – Log analizinin teknik dile çevrilmesi

- Saldırgan ip adresinin belirlenmesi,
- Saldırı yönteminin belirlenmesi, gereksiz logların ayıklanması

Adım 3 Log analizi yazılımları kullanarak istenilen verilerin çıkarılması- sonuç

- Elde edilen verilerin ayıklanması ve doğrulanması
- Saldırgan ip adresinin tespit edilmesi ve saldırı türünün belirlenmesi
- Saldırgan ip adresinin sisteme daha önceki girişlerinin tespit edilmesi

Log analizi sonucunda logların tarih, boyut, ip adresi gibi bilgileri bir dosyada saklanması daha sonraki işlemlerde kullanılmasına olanak sağlanması gerekebilir. Siber saldırıların

belirlenmesinde en büyük eksiklik yeterli loglamanın tutulmamasıdır. Ücretsiz log analiz programları da kullanılabilinir. Ayrıca logların varlığını kanıtlayan tüm işlemlerin yapıldığını onaylayan zaman damgası özelliğinin yer almasıdır. Siber saldırıların belirlenmesinde kullanılacak olan veri kümeleri yüksek oranda satırlar içeren log dosyalarından oluşmaktadır. Dağıtık hizmet dışı bırakma eski bir siber saldırı yöntemi olmasına nazaran günümüzde kötü niyetli kullanıcılar tarafından hala kullanılmaktadır. Siber saldırıların belirlenmesi için log dosyaları büyük veriler olmasına rağmen analiz edilmesi gerekmektedir [37].

2.3.2.2. Log Analizi Yazılımları

Log analiz araçları, sistemler ağ trafiği üzerinde oluşan aksiyonların log kayıtlarının analizini sağlayan yardımcı programlardır. Log analizi sistemler üzerinde gerçekleşen olayların kimler tarafından hangi sistemlerde gerçekleştiğini bilgisini tutan günlüm dosyalardır. Açık kaynak ve kapalı kaynak olarak iki ana yapıda incelenebilir.

Açık kaynak analiz araçları linux/Unix sistemleri desteklemektedir. Kapalı kaynak log analiz programları genelde Windows tabanlı olmaktadır. Bazı log araçları Windows ve Linux tabanlı da hizmet vermektedir. Bazı log analiz araçları,

- Kali analiz araçları (WRESHARK, WHARKSARK, TSHARK, NMAP),
- Kali açık kaynak kod analiz araçları (TCPDUMP, LIBCAP),
- Açık kaynak araçlar (NXLOG, LOGSTASH, GRAYLOG2),

2.3.2.3. Log Yönetim Araçları

Kanun gereği tutulan log kayıtları birçok firma tarafından ticari program boyutuna taşınmıştır. Yazılım firmaları tarafından geliştirilen programların log yönetimi açısından birçok özelliği bulunmaktadır.

Log kayıtlarını tutan bazı programlar özellikleriyle birlikte Çizelge 2.3'de yer almaktadır.

Loglama sistemleri yönetim yapısı olarak üç farklı kategoride hizmet vermektedir.

Bu kategoriler Log Management, Güvenlik Bilgisi ve Onay İzleme Sistemi (SIEM), Hizmet olarak yazılım (SaaS) Logging olarak sistemler üzerinde yer almaktadır [38].

Çizelge 2.3. Loglama araçları ve özellikleri.

Log Aracı	Platform	Dağıtım	Lisans	Tutar
FLUENTD	Windows, Mac, Linux	-	-	Ücretsiz
SOLARWINDS	Windows	-	30 Gün Deneme Sürümü	1500$
SEMATEXT	Windows, Mac, Linux	Local ve Bulut	14 Gün Deneme Sürümü	50-60
DATADOG	Windows, Mac, Linux	Local ve Bulut	Ücretsiz Versiyon	Aylık 60$
SPLUNK	Windows, Mac, Linux	Local ve Bulut	Deneme Sürümü ve Ücretsiz Version	AylıkGB/150$
EVENTLOG	Windows, Mac, Linux	Local	30 Gün Deneme Sürümü	595-2495
LOGDNA	Windows, Mac, Linux	Local ve Bulut	14 Gün Deneme Sürümü	Aylık GB/3$

Log yönetimi açık kaynak sistemlerden farklı olarak, Çizelge 2.4'de günlük log yönetimi için SIEM ürünleriyle yapıldığı yer almaktadır. Log yönetimi için farklı analiz programları kullanılabilmektedir.

Çizelge 2.4. Loglama kategorileri ve araçları [33].

Log Management	SIEM Ürünleri	SAAS Logging
Tibco The Power Of Now	Hp Arcsight	Sumolgic
Balabit It Security	Attachmate	Papertrail
Keyw Sensage	Solarwınds	Loggly
Splunk	Blackstratus	Logentrie
Tripwire	Rsa	Torch

2.3.3. Log Güvenliği

Loglama sistemlerinin güvenliği en üst seviyede tutulmalıdır. Log kayıtlarının bütünlüğü, analizi, siber saldırılara karşı alınması gereken tedbirleri, logların değiştirilmesi ve silinmesi gibi birçok önemli konuyu kapsamaktadır. Log kayıtları sistemlerin işleyiş,

güvenlik, strateji ve iyileştirme gibi kavramlar hakkında bilgi vererek sistemlere yol haritası oluşturmaktadır.

Kanuni düzenleme ile log kayıtları tutulmaya başlanmıştır. Tutulan logların kriptolu güvenlik standartlarına uygun bir şekilde kayıtlarının tutulması gerekmektedir. Adli analiz ve işlem olaylarının izlenmesinde log kayıtları önemli bir yere sahiptir. Log kayıtları, bilgi güvenliği açısından sistemler üzerinde büyük rol oynamaktadır. Log kayıtlarının yönetimi, sistemlerin siber güvenliği açısından birbiriyle yakından ilgilidir. İncelenen log kayıtları üzerinden güvenlik stratejileri geliştirilebilir.

Açık kaynak sistemler siber güvenlik sistemlerinin yapılandırılması işlemlerinde yoğun bir şekilde kullanılmaktadır. Kapalı kaynak yazılımlar siber güvenlik açıklarının taranması, belirlenmesi ve açıkların kapatılması konusunda açık kaynak kod ve yazılımları karşısında yeterli performans göstermediği literatür taramalarında görülmektedir. Yukarıda yer alan yöntemlerin siber saldırıların tespit edilmesinde kullanıldığı ve analizlerin yapıldığı, yapılan çalışmalarda yapıldığı görülmekte olup bu çalışmalara yapılan atıflar kaynakçada belirtilmiştir. Tez çalışmasında siber saldırıların loglar üzerinde tespit edilmesinde kullanılması uygun olduğu literatür taramalarında görülmektedir. Bu bağlamda tez çalışmasını yukarıda yer alan analiz yöntemlerini kullanarak siber saldırılara karşı koyma yöntemleri belirlenmesi hedeflenmektedir [38].

Sistemler üzerinde yer alan logların yönetiminde SIEM çözümleri kullanılmaktadır. Birçok sistem üzerinde log kayıtları SIEM yöntemiyle tutulmaktadır SIEM yöntemiyle kaydedilen loglar indekslenmiş düz metin dosyalarında şifrelenmiştir. SIEM üzerinde toplanan loglar biçimde normalleştirilerek tutulmaktadır. Bu özellik sayesinde log yönetimi ve analizi kolaylaşmaktadır. Bu anlamda log kayıtlarında SIEM ürünlerinin kullanılması daha doğru sonuçlar vermesi sağlanır [38].

Sistemlerin siber güvenliği açısından, sistemler üzerinde oluşan siber saldırıların tespit edilmesinde log sistemlerine ihtiyaç olmakla birlikte, siber saldırıların tespiti açısından çok önemli bir yere sahiptir. Sitemler üzerinde tutulan logların, yönetimi, güvenliği, analizi, siber güvenlik tespiti açısından birbiri ile ilişkili bir yapıya sahiptir. Network sistemleri üzerinde bilgi güvenliğini sağlamanın en önemli verileri siber güvenlik raporlarıdır. Siber güvenlik raporları zafiyetlerinin giderilmesi için kullanılması gerekmektedir. Ayrıca birçok loglama cihazı günümüz şartlarında bir güvenlik duvarı gibi çalışmaktadır [39].

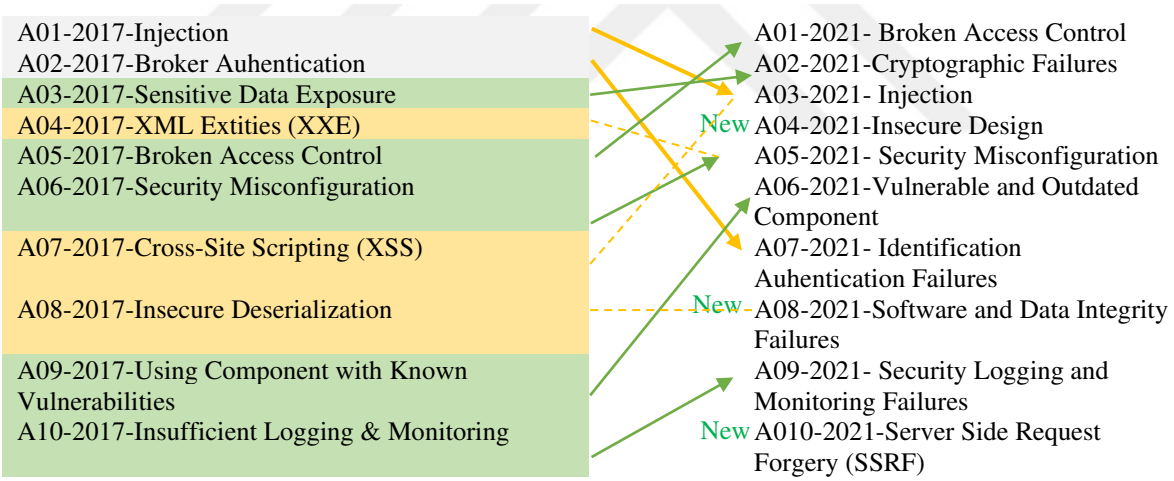
2.4. SİBER SALDIRILAR

Siber saldırılar, aktif ve pasif bilgi toplama, güvenlik açıklarının taranması, web saldırıları, şifre denemeleri, yem saldırıları, sosyal mühendislik gibi siber uzayda kullanılan birçok metot yer almaktadır [40].

Log kayıtları, dijital verileri oluşturan ve kullanan kullanıcıların siber güvenlik açısından kuvvetli bir bağa sahiptir. Bu yüzden siber saldırıların tespiti için dijital veriler üzerinde oluşan kullanıcı logları hayati öneme sahiptir [41].

Open Web Application Security Project (OWASP), 2017 yılında kritik 10 web uygulamasına ait güvenlik zafiyetlerini belirlenmiştir.

Şekil 2.8'de İncelendiğinde yıllara göre saldırı türlerinin değişiklik gösterdiği görülmektedir. Bu anlamda hangi saldırı türünün hangi zamanda oluşacağını önceden kestirilememektedir. Her saldırı türünün farklı savunması olabilmektedir. Bu anlamda siber saldırıların network sistemleri üzerine etkisinin azaltılması için güvenlik sistemlerinin yaygın ve güncel olarak kullanılması gerekmektedir [42].



Şekil 2.8. 2017-2021 Yılları arasında kritik 10 web uygulaması [40].

Ayrıca 2017-2021 yılları arasındaki siber zafiyet olan uygulamaların değişimi Şekil 2.8'de yer almaktadır. OWASP raporuna göre kritik ilk 10 web saldırısı adı ve kodları Çizelge 2.5'da yer almaktadır. Raporda saldırı uygulamaları yıllara göre değişim gösterilmektedir. Saldırı raporlarından elde edilen verilere göre siber saldırıların haritası çıkartılarak gerekli önlemlerin alınması sağlanır. [40].

Çizelge 2.5. OWASP en kritik 10 web uygulaması [40].

Saldırı Kodu	Saldırı Türü
A01:2021	Kırık Erişim Kontrolü
A02:2021	Şifreleme Hataları
A03:2021	Enjeksiyon
A04:2021	Güvensiz Tasarım
A05:2021	Güvenliğin Yanlış Yapılandırılması
A06:2021	Hassas ve Güncel Olmayan Bileşenler
A07:2021	Kimlik Doğrulama ve Kimlik Doğrulama Hataları
A08:2021	Yazılım ve Veri Bütünlüğü Arızaları
A09:2021	Güvenlik Günlüğü Kaydetme ve İzleme Hataları
A10:2021	Sunucu Tarafı İstek Sahteciliği

2.4.1. Siber Saldırılarda En Çok Kullanılan Yöntemler

2.4.1.1. DoS saldırı Çeşitleri

Denial of Service (DOS) Dağıtık Hizmet Engelleme, siber saldırılar içinde yaygın olarak kullanılan siber saldırı türüdür. İnternet üzerindeki sistemin kendi kullanıcıları tarafından ulaşılmasını engellemek amacıyla yapılan sistem yavaşlatma saldırısıdır [43].

İnternet üzerinden hizmet veren sistemin geçici olarak servis dışı bırakılması saldırısı olarak da açıklanabilir. Saldırganların, sistemlere erişilmesini engellemek için belirli zaman dilimlerinde sıkça kullandıkları saldırı türüdür.

2.4.1.2. DDoS saldırı Çeşitleri

Distrubuted Denial of Service (DDoS), DoS saldırılarından daha fazla sayıda, farklı sistemler üzerinden yapılan saldırı türüdür. DDoS saldırıları spoofing edilmiş IP adreslerinden ve internet korsanları tarafından ele geçirilmiş, yem olarak tabir edilen bilgisayarlar üzerinden yapılan saldırı türüdür [43].

Domain Name System (DNS) spoofing, kullanıcılarının hedef web site yerine sahte siteye giriş yapmalarını sağlayan, kişisel verilerinin gerçek siteye giriyormuş izlenimi vererek bu verilerin çalınmasını, başkalarının eline geçmesini sağlayan, siber saldırı türüdür [44].

2.4.1.3. SQL Enjeksiyon Saldırıları

Siber uzayda birçok siber suç işlenmektedir. Veri tabanlarına sızma, Siber casusluk, ülkelerin stratejik bilgilerini öğrenme girişimi gibi siber uzayda en yoğun yaşanan saldırılardır. Bu saldırılardan korunmak için ülkeler stratejik siber politikalar geliştirmektedir [42].

Sistemlerin veri tabanı bölümlerinde oluşan güvenlik açıklıklarından meydana gelen siber zafiyetlerdir. Yapılandırılmış Sorgu Dili (SQL) Enjeksiyon zafiyetleri veri tabanında yer alan çeşitli verilerin siber saldırgan/hacker tabir ettiğimiz kötü niyetli kişilerin eline geçmektedir [43].

SQL enjeksiyon zafiyetleriyle, ile kullanıcı bilgileri, şifreler, kişisel veriler vb. birçok veri kötü niyetli kullanıcıların eline geçmektedir. Bu zafiyetler, OWASP tarafından yüksek seviyeli güvenlik zafiyetini oluşturduğu belirtilmiştir [40].

Veri tabanında yer alan açıkların kurumlar, ülkeler arasında saldırı yoğunluğuna neden olmaktadır. Bu anlamda siber uzayda gerçekleşen saldırı türleri artmaktadır. Bu anlamda siber uzayda gerçekleşen siber saldırılar gerçek savaşların yerini almaya başlamıştır [41].

2.4.1.4. Kaba Kuvvet Saldırıları

Erişim sağlanacağı sistem üzerinde kullanıcı adı ve şifre bilgilerinin sürekli olarak denenmesiyle yapılan saldırı türüdür. Kaba kuvvet saldırıları, saldırganların, erişim sağlanacağı sistem üzerine elle veya açık kaynak araçlar ile deneme yapılması da mümkündür [43].

2.4.1.5. Yönetici Hesabı ile Oturum Açma

Erişim sağladığı sistem üzerinde yetkisi olmadığı halde sisteme erişerek, sisteme giriş sağlamasıdır. Çok fazla sayıda kullanılan Uzaktan Yerel Bağlantı (R2L) olay saldırılar içinde Dictionary, Guest, Imap, Named, Sendmail, Xlock, Xsnoop 'tur [44].

2.4.1.6. Yetki Yükseltme

Erişim sağladığı sistem üzerinde kullanıcı oturum yetkisi olduğu halde, sistem zafiyetlerinden yararlanarak, yönetici yetkilerini ele geçirerek sistem üzerinde yönetici yetkisiyle sistem üzerinde işlem yapmasıdır. Çok fazla sayıda kullanılan Kullanıcının Root Yapması (U2R) örnek saldırıları Eject, Ffbconfig, Fdformat, Loadmodule, Perl, Ps, Xterm'dir [45].

2.4.2. Siber Saldırılara Karşı Alınan Loglama Önlemleri

Sistemler üzerinde log kayıtlarının alınması, sistemin çalışma yapısını olumlu etkileyeceği aşikardır. Loglama yöntemleri, sistemler üzerinde çeşitli konumlara yerleştirilerek, network üzerindeki hareketlerin dijital izlerinin alınmasını sağlamaktadır. Bu sayede log kayıtları, siber saldırılara karşı istihbarat çalışması yapmasının önünü açarak çoğu siber saldırıyı başlamadan engellediği görülmektedir [46].

Kablosuz ağlarda, 802.1x kimlik denetimi en yaygın kullanılan yöntemlerden biridir. Kimlik denetimi süreci, belirli zaman diliminde Radius server incelenerek kullanıcı tespitti yapılmasına olanak sağlar. Kullanıcıların MAC adresleri ile tespitti de yapılabilir. Option 82 bilgisi ile MAC adresi ve bağlanılan port numarası loglanabilir. Log kaydı için Cisco anahtarlama cihazının Option 82 seçeneğinin aktif olması gerekmektedir. Şekil 2.9'da Cisco anahtarlama cihazının Option 82 bilgisi detaylarına yer verilmiştir [47].

```
! Snooping'i devreye alma komutu
ip dhcp snooping
ip dhcp snooping vlan <vlan no>
!
! option 82bilgisinin taşınmasının devreye alınması için gereken komut
ip dhcp snooping information option
!
interface <int adı> <int.no>
description Istemci bilgisayar portu – Bir konfigurasyon yapmaya gerek yoktur.
!
interface <int adı> <int.no>
description DHCP sunucusunun portu veya Uplink portu
ip dhcp snooping trust
```

Şekil 2.9. Cisco anahtarlama cihazının option 82 bilgisi [47].

Loglama sistemleri üzerinde yer alan birçok özellik sayesinde, siber saldırıları karşı birçok önlem alınmasını sağlamaktadır. Coslat 5651 log server cihazını incelediğimizde birçok önemli özelliğe sahip olduğu görülmektedir. Sistemler üzerinde, siber saldırılara karşı bir kalkan görevi üslendiği görmektedir. Bu yüzden sistemler üzerinde loglama sistemleri kullanımının daha yaygın hale getirilmesi gerekmektedir.

2.4.2.1. 5651 Log Sunucu

Ağ trafiğini üzerinde gerçekleşen işlemleri kayıt altına alarak Elektronik Zaman Damgası (EZD) ile imzalanarak 5651 sayılı kanun hükümleri yerine getirilmektedir. Sistemler üzerindeki yasal zorunluluğu yerine getirmektedir. Aynı zamanda birçok siber saldırıya

karşı korumaktadır.

Log sunucuların önemli özellikleri aşağıda yer almaktadır [48].

- Mirror-Span Port özelliği ile pasif durumda lokalde log işlemi
- Router ile katman 2'de log işlemi, Sanal Yerel Alan Ağ (VLAN) işlemleri
- Elektronik Zaman Damgası ile lokal ve nitelik ile imzalama
- Turk Trust, KamuSM ve EZD özelliği
- Syslog ile Log Korelasyon yapısına uygun log gönderme
- Harddisk (HDD) ile 2 yıla kadar kayıt desteği

Log cihazları kullanıcı sayısına göre belirlenmekte ve network sistemleri üzerine yerleştirilmektedir. Log cihazları incelendiğinde bu cihazların içinde, linux tabanlı bir işletim sistemi, kullanıcı sayılarına göre (Rasgele Erişim Bellek) RAM, Merkezi İşlem Birimi (CPU) ve HDD kapasiteleri belirlenmektedir. Ethernet kartı, veri aktarım ve bağlantı hızları yer almaktadır [49].

Kullanıcı sayıları arttıkça log cihazının donanımsal açıdan kapasitesi artmakta ve kullanıcı sayısına oranla değişim göstermektedir. Bu anlamda network trafiğinin band genişliği önemli bir yere sahiptir. Log cihazlarının kullanıcı sayısına göre belirlenmesi network sistemlerine entegre edilmesini kolaylaştırmaktadır. Çizelge 2.6'da log cihazlarının donanımsal kapasiteleri ve kullanıcı sayıları yer almaktadır.

Çizelge 2.6. 5651 Log cihazları nitelikleri [49].

Özellik	RMIDS1000	RM2DS2000
Ram	8 GB	16 GB
Port(1Gb)	6	6
Port (10 Gb)	x(Ops)	x(Ops)
Disk	240 GB	512 GB
Boyut	1U	1U
Güvenlik duvarı aktarım hızı	6.8 Gbps	9.6 Gbps
Eşzamanlı oturum sayısı	7.2 Milyon	15 Milyon
IPsec VPN aktarım hızı	2.2 Ghz	2.4 Ghz
Kullanıcı Sayıları	500	2500

2.4.2.2. Zaman Damgası

Zaman damgası, gerçekleşen işlemlerin zaman acısından oluştuğunun kanıtıdır. Zaman Damga Sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisi kullanır. Böylece verilerin belirtilen tarihteki varlığı onaylanarak, bütünlüğü sağlanır [49].

Dijital sözleşmelerin imzalandığı, para transferi, e-devlet gibi birçok dijital işlemlerin güvenli bir şekilde gerçekleşmesi için zaman damgası alınmaktadır. Bu dijital işlemler içinde, resim, çizim, fotoğraf, kitap gibi veriler yer alabilir [48].

5070 Elektronik İmza Kanunu göz önüne alındığında bir elektronik verinin oluşturulduğu, değişiklik yapıldığı, gönderildiği zamanların tespit edilmesini sağlayan elektronik imzayı doğrulayan dijital kayıtları ifade etmektedir [50].

2.5. SİBER SALDIRILARIN TESPİT EDİLMESİNDE LOGLARIN KULLANILMASI

2.5.1. Siber Güvenlik Açısından Logların Önemi

Log kayıtları network sistemi içinde yer alan siber güvenlik olgusunu ve dijital veriler arasında önemli bir yer sahiptir. Log kayıtları siber güvenlik ve dijital veriler arasında kuvvetli bir bağa sahiptir.

Verilerin sürekliliği ve bütünlüğü açısından verilerin en üst seviyede güvenliğinin sağlanması gerekmektedir. Bu anlamda sistemler üzerinde log kayıtlarının tutulması aslında misafir kullanıcılara güvenli ortam mesajı vermektedir. Loglama sistemlerinin kullanılması saldırganlara caydırıcı etki oluşturmaktadır. Bu etki saldırıların sayısını düşürdüğü görülmektedir.

Logların tutulması siber güvenliğin temel taşını oluşturmaktadır. Bu anlamda sistemler üzerinde log kayıtlarının tutulması siber güvenlik anlamında bir bütünlük olarak bilgi güvenliğini sağlamaktadır.

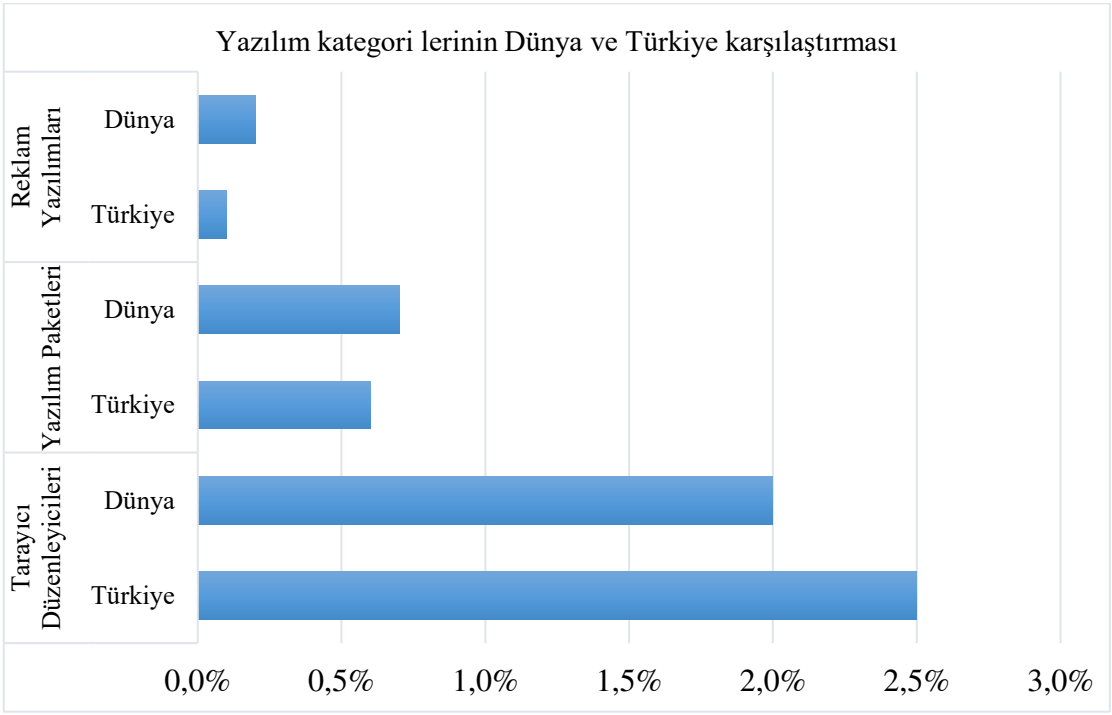
Microsoft siber saldırı raporları incelendiğinde, 2017 yılına ait veriler kullanılmıştır. 2017 yılına ek olarak son iki yıl olan 2022 ve 2023 yıllarında yayınlanan saldırı raporlarına da yer verilmiştir. Bu yıllarda yaşanan bazı siber saldırı türlerinde hızlı artışın olduğu görülmektedir.

Şekil 2.10 incelendiğinde Microsoft siber raporuna göre Türkiye de siber suçların durumu gösterilmektedir. Şekil 2.10'da 2017 yılında hazırlanan Microsoft siber raporuna göre,

siber saldırılar incelendiğinde yıllara göre saldırı türlerine göre çeşitli siber saldırı verileri bulunmaktadır.

Şekil 2.10'da 2017 Microsoft siber raporuna göre dünya ve Türkiye istenmeyen yazılım kategorileri grafiği yer almaktadır.

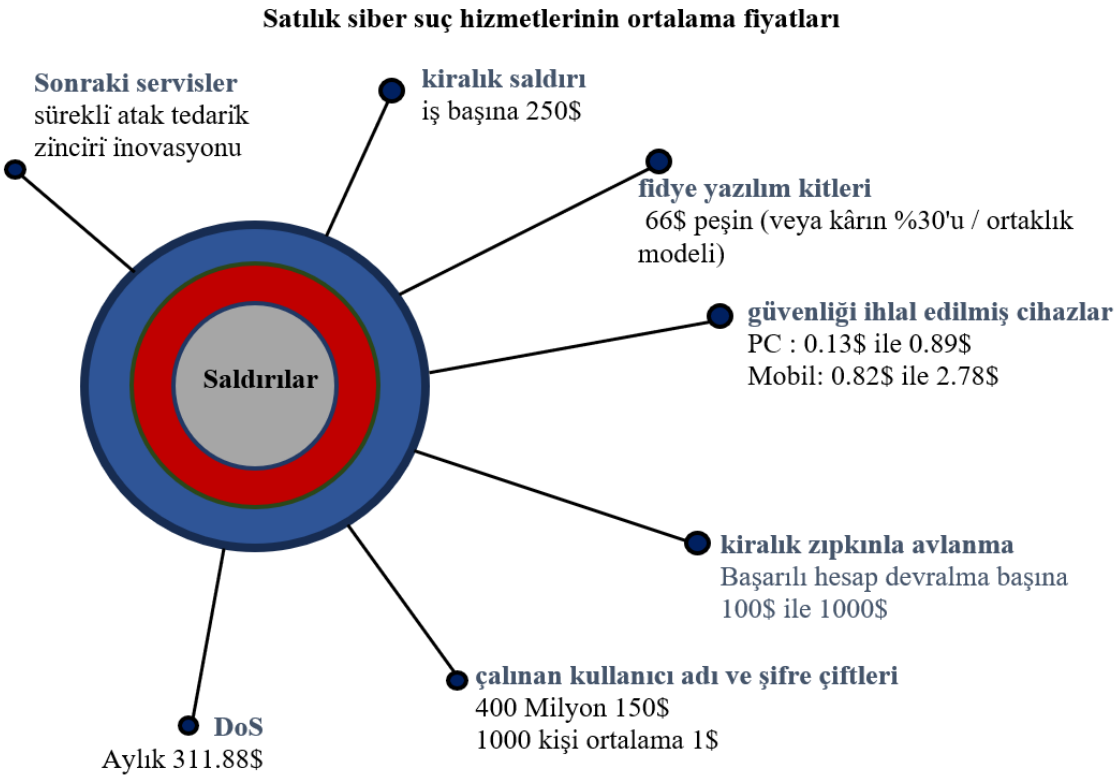
2017 yılında yayınlanan rapora göre yazılım türlerine göre saldırı oranları ülke bazında verilmiştir [51].



Şekil 2.10. 2017 Microsoft dijital savunma raporu [51].

Şekil 2.11 incelendiğinde Microsoft Dijital Savunma Raporuna göre, 2021 yılı içinde gerçekleşen kimlik avı saldırı verileri incelendiğinde, 15000'den fazla kimlik avı web sitesi imha edilmiştir.

Raporda 25'den fazla kimlik avı saldırı tekniği olduğu yer almaktadır. Ayrıca raporda kimlik avı simülasyon eğitimi alan personelin 50% oranda, kimlik avı saldırılarına karşı önlem aldığı ve bu saldırıların azaldığı görülmektedir [51].



Şekil 2.11. Microsoft dijital savunma raporu siber suçların durumu [51].

Siber suçların işlenmesindeki ana sebep maddi kazanç elde etmektir. Bu durum tüm dünyada dijital sistemler için büyük bir tehdittir. Dünyada birçok ülke siber saldırıları engellemek, önlemek ve bertaraf etmek için bir dizi çeşitli önlemler almaktadır. Alınan bu önlemler büyük bütçelerden oluşmaktadır. Sistemler üzerinde konumlandırılan loglama teknolojileri, birçok siber saldırıyı engelleyeceği görülmektedir. Eğitim alan personelin siber saldırılara karşı daha bilinçli olduğu görülmektedir. Loglama teknolojileri siber saldırıların habercisi konumundadır.

Log kayıtlarının incelenmesi, periyodik analizlerinin yapılması planlanan siber saldırıların önüne geçebilir. Log kayıtları bu anlamda uzmanla network sisteminin gizemli yanları hakkında bilgiler vermektedir. Log kayıtları siber saldırıları anlık engellemese de sonraki süreçte zafiyetlerin tespit edilmesinde önemli rol üslenir. Siber saldırılardan bankalar, e-ticaret siteleri, sosyal medyanın yanı sıra ülke ve kurumları da nasibini almıştır.

Microsoft firmasının 2023 Yılına ait dijital savunma raporuna göre fazla yapılan ilk dört saldırı türü Çizelge 2.7'de yer almaktadır.

Çizelge 2.7. 2023 Yılı Microsoft dijital savunma raporu [51].

Saldırı Yüzdeleri	Saldırı Türleri
42,00%	Başarılı Kimlik saldırıları (A)
29,00%	Fidye yazılımı karşılaşmaları (B)
25,00%	Başarılı hedefli kimlik avı girişimleri (C)
4,00%	İş e-postalarının ele geçirilmesi (D)

Microsoft yayınladığı raporda 2022 Yılında yapılan fidye yazılımı saldırıları 2023 yılında 2 kat artığı yer almaktadır. Rapora göre kimlik avı saldırıları 2023 yılında parola deneme saldırı saniyede 4000 ortalaması ile en yüksek seviyeye çıkmıştır. Aynı zamanda uzaktan şifre deneme sayısında 2022 yılına göre arttığı görülmektedir. Zafiyet oranı yüksek olan siber saldırıların bilgi toplama ve keşif süreleri diğer saldırılara göre biraz daha uzun sürmektedir. Bu durumun izlenmesini log kayıtları üslenmektedir. Çizelge 2.8'de yer alan verilere göre farklı yıllardaki ülkelere yapılan siber saldırı türleri ve hedef alınan kurumlar yer almaktadır. Tablo verileri incelendiğinde siber saldırıların kişi, kurum, işletme, şehir, ülke bazında olduğu giderek arttığı görülmektedir [52].

Çizelge 2.8. Siber güvenlik zafiyetleri ve sonuçları [52].

SN	**Saldırı Adı**	**Saldırı Yılı**	**Saldırı Yapılan Ülke**	**Saldırı Hedefi**	**Saldırı Türü**
1	Bakü-Tiflis Ceylan Boru Hattı	2008	Azerbaycan, Türkiye, Gürcistan	Yer altı maden tesisleri	Mantık Bombası
2	Conficker	2009	Tüm Dünya ve Türkiye	İstanbul Hava Limanı Dış Hatlar	Virüs
3	TİB	2011	Türkiye	TİB Web Siteleri	DDoS
4	Hastaneler	2016	Türkiye	33 Devlet Hastanesi	Veri Hırsızlığı
5	Muddy Water (APT)	2018	Irak, S. Arabistan, Afganistan, Pakistan	Kamu, TSK, Telekom, Üniversiteler	Otlama Saldırıları
6	Telekom	2020	Türkiye	DNS Servisleri	DDoS

Çizelge 2.8 (devamı). Siber güvenlik zafiyetleri ve sonuçları [52].

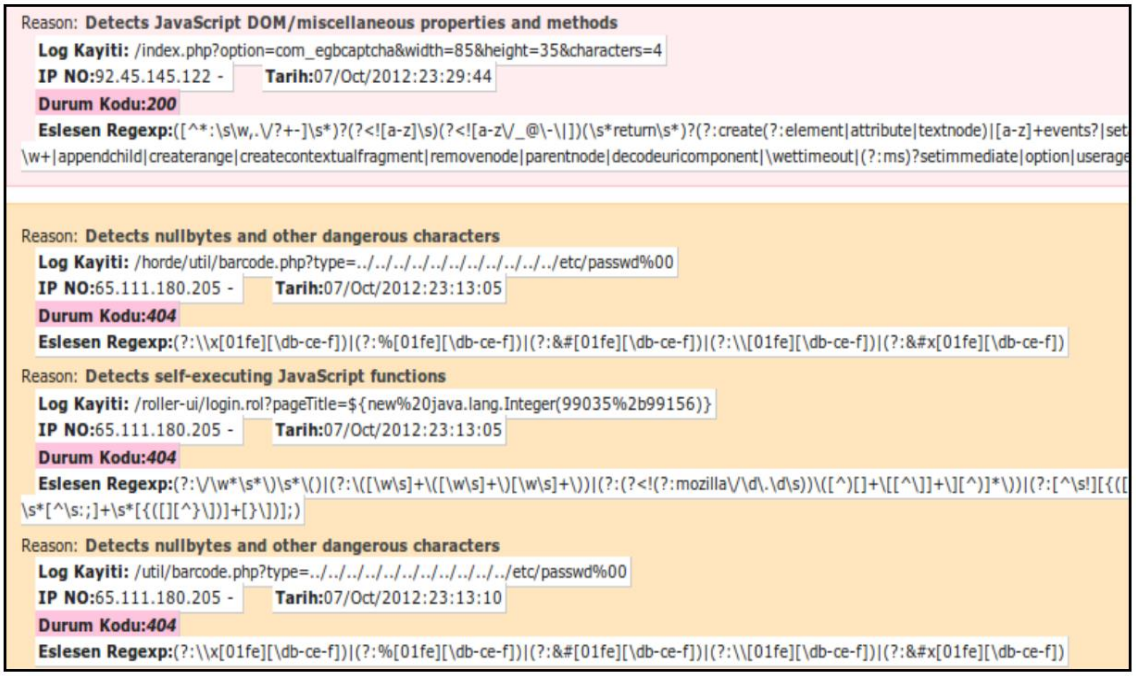
7	Yemek Sepeti	2021	Türkiye	Müşteri Veri Tabanları	Fidye Yaz, Veri Hırsızlığı, Backdoor
8	Konya Belediyesi	2021	Türkiye	Kurum Veri Tabanları	Fidye Yazılımları, Backdoor
9	Sağlık Kurumları	2022	Türkiye	Hasta Bilgi sistemleri	Veri Hırsızlığı, Backdoor
10	Pegasus	2022	Türkiye	Müşteri bilgileri	Backdoor
11	ALtahıca	2022	Türkiye	Türkiye, AHA, TSK	DDoS
12	Baydöner	2022	Türkiye	Web Servisleri	Malware
13	TÜBİTAK	2022	Türkiye	E-Mail adları	Trojan
14	MurenShark	2022	Türkiye	Milli Denizaltı Yönetim Sistemi	Casus Yazılım, Trojan
15	THY	2022	Türkiye	Müşteri Bilgileri	DDoS

2.5.2. Siber Saldırıların Log Analizleriyle Önlenmesi

Log kayıtlarının incelenmesi, yorumlanması ve analizi, siber saldırıların bulunmasında kolaylık sağlamaktadır. Siber saldırı tespitinde log kayıtları önemli bir yere sahiptir. İlk bölümde yer alan log kayıtlarının yasal zorunluluğunda yer aldığı gibi log kayıtları siber saldırıların tespit edilmesi anlamında sistemlerin kripto kutusudur [53]. Log kayıtlarının doğru yorumlanması, olağan dışı davranış sergileyen kullanıcıların tespit edilmesinde kullanılmasını sağlamaktadır [54]. Bu anlamda tespit edilen kullanıcı adreslerine kural uygulanması sağlanır. Siber güvenlik zafiyetlerinin giderilmesi için birçok çalışma bulunmaktadır. Bu çalışmalar arasında web loglarının analiz edilmesi de yer almaktadır. Güvenlik uzmanları tarafından web logları analiz edilerek değerlendirilmiştir [55].

Log analizi ve değerlendirmesinde Scalp aracı kullanılmıştır. Şekil 2.12'de Scalp raporu çıktısı görseli bulunmaktadır. Bu raporda log hakkında önemli veriler yer almaktadır. Scalp, Python dili ile yazılmış bir scripttir. Web uygulamaları, Scalp aracı ile SQL enjeksiyon, Siteler Arası Betik Çalıştırma (XSS), Siteler Arası Talep Sahteciliği (CSRF) saldırılar karşısında hedef alınıp alınmadıkları analiz edilmiştir. Log kayıtları içinde belirlenen saldırı desenleri aranmıştır. Tespit edilen karakter dizileri hangi IP adresinden

geliyorsa o IP adresi engellenmiştir. Scalp aracı, Apache aracı içinde yer almasından dolayı, web logları saldırı tespitinde kullanıldığı görülmektedir. Scalp aracı saldırıların en çok XSS ve SQL atakları olduğunu ortaya çıkarmıştır [56].



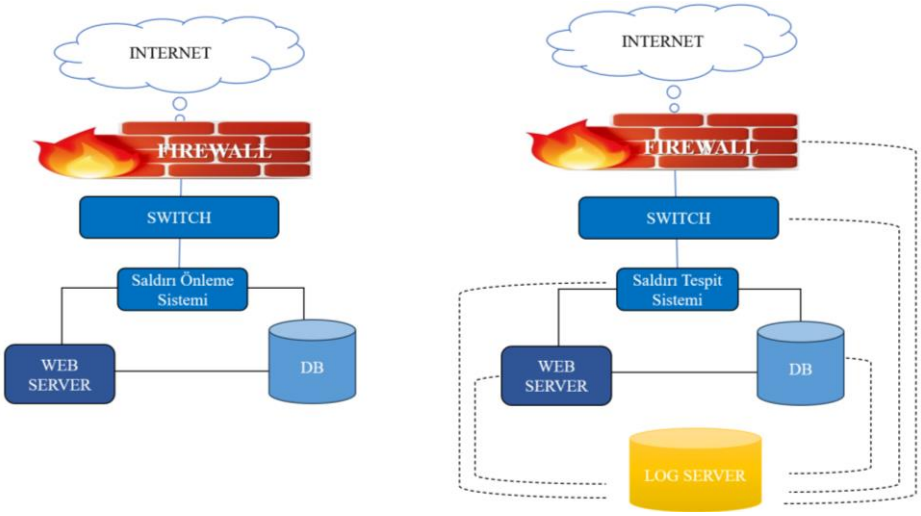
Şekil 2.12. Scalp raporu çıktısı [56].

2.5.3. Siber Saldırı Tespitinde İncelenmesi Gereken Loglar

Log analizleri siber saldırıların tespiti için dış ortamdan iç ortama doğru incelenerek analiz edilmelidir. En dışta yer alan güvenlik duvarından başlanarak içe doğru analiz edilerek gelinmelidir. Saldırgan kendi kimlik bilgilerini gizleyerek çeşitli saldırı yöntemleri deneyerek sisteme sızma girişimi gerçekleştirebilir. Log kayıtlarının, analiz yöntemleri kullanılarak incelenmesi birçok yol haritalarının oluşturduğu yapılan çalışmalardan bilinmektedir. Log kayıtlarının incelenmesinde ve analizinde siber güvenlik uzmanları yer alabilir. Ayrıca açık kaynak saldırı tespit ve önleme sistemi kullanılmaktadır. Log kayıtlarının incelenmesi ve yorumlanmasında güvenlik uzmanı personelinin kullanılması zaman açısından verimli olmayabilir. Zaman açısından personel kullanılması siber saldırıların tespit edilmesinde gecikmeler yaşanabilir. Zaman açısından Saldırı Tespit Sistemi kullanılması siber saldırıların zamanında ve yerinde tespit edilmesini sağlamaktadır. Bu anlamda Saldırı Tespit Sistemi kullanan personel saldırı tespitinde daha etkili olacağı düşünülmektedir. Bu çalışmada analiz edilen veriler bilgiye dönüştürülürken web madenciliği ile yapıldığı görülmektedir. Ayrıca makale

çalışmasında log analiz yazılımı geliştirilmiştir. Bu yazılımda algoritma olarak apriori algoritması kullanılmıştır. Geliştirilen yazılım ile üniversite bünyesinde bir analiz yapılmış ve çeşitli sonuçlar çıkartılmıştır. Bu yazılım ile veriler daha hızlı ve kolay bilgiye dönüştürülmüştür [57].

Log analizlerinde en son veri tabanı loglarının incelenmesi gerektiğini de ekleyebiliriz. İnternet üzerinden gelen saldırıların belirlenmesinde Şekil 2.13'de yer alan log cihazlarının network içindeki sıralaması takip edilerek konumlandırılmaktadır [58].



Şekil 2.13. Log cihazlarının konumlandırılması şeması [58].

Logların tek merkezde toplanması aşağıda belirtilen maddelerde kolaylık sağlamaktadır.

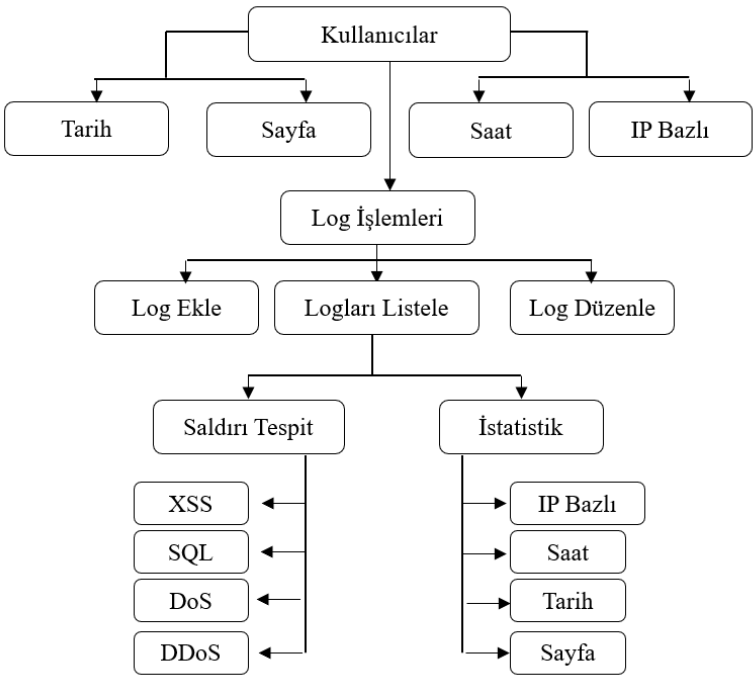
- Farklı sistemlere ait logların bir merkezde toplanması yönetimini ve güvenliği,
- logların sınıflandırılması, analiz ve yorumlanması,
- Logların tek merkeze toplanması, korelasyon kuralını uygulanmasını,

Basit Mail Aktarım Protokolü (SNMP) destekleyen cihazlardan istenilen aralıklarda log alınmasını sağlamak amacıyla "WALKBEE" isimli bir yazılımın geliştirilmiştir. Yazılım sistemi kullanılarak merkezi üçüncü katman anahtarlama cihazı Adres Çözümleme Protokolü (ARP) kayıtları tutularak 5651 sayılı loglama kanunu kapsamında log kayıtlarının alınması sağlanmıştır [59].

Siber güvenlik tatbikatı log analizleri incelenerek gerçek siber saldırılarda kullanılmak için çeşitli yol haritaları çıkarılmıştır. Bu çalışmada Professional siber güvenlikçilerin tecrübelerinden faydalanılmış oluşabilecek siber saldırılara karşı daha fazla önlen

alınması sağlanmıştır [60].

Log analizleri veri madenciliği yöntemleriyle daha kapsamlı analiz edilerek siber saldırıların azalacağı kaçınılmazdır. Log dosya analizi Şekil 2.14'de yer almaktadır. Log analizlerinin yapılmasında gerekli Profesyonel personelin önemi burada bir kez daha öne çıkmaktadır [61].



Şekil 2.14. Log dosya analizi [8].

Web üzerinde olan veriler kontrolsüz hızlı bir şekilde artmaktadır. Bu durum web üzerinde oluşan logların analiz ihtiyacı aynı doğrultuda artmıştır. Siber saldırıların günümüz şartlarında uygulama katmanına yapılması web sayfalarına saldırıların arttığını işaret etmektedir. Web logları aynı zamanda veri madenciliği analiz yöntemleriyle de analiz edilebileceği, siber saldırı oranlarının aynı şekilde düştüğü görülmektedir. Web logları veri madenciliği yöntemleriyle 3 kısımda analiz edilmiştir. Bu adımlar,

- İstatistiksel analiz,
- Kullanıcı logların analizi,
- Saldırı tespiti analizleri olarak yapılmıştır.

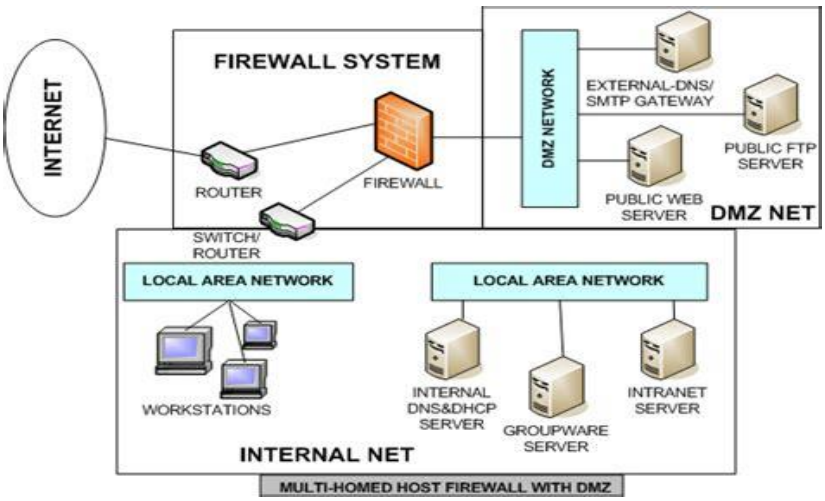
Teknolojik gelişmelerin özel ve tüzel işlemler ile kişi, kurum ve devlet işlerinde kullanılması, en basit bir evrak işleminden tutunda, yer, zaman ve maliyet kavramlarını

bürokrasi işlemlerinde kişi kurum ve devlet tarafından birçok fayda sağladığı görülmektedir. Aynı zamanda teknolojik gelişmeler sistemler üzerinde bazı siber zafiyetleri oluşturmaktadır. Sistemler üzerinde tutulan log kayıtları oluşan siber güvenlik zafiyetlerinin büyük bölümünü engelleyeceği, azaltabileceği, sistemlerin siber güvenlik konusunda daha güvenli hale getirebileceği bilinmektedir [61].

Sistemler üzerindeki log kayıtlarının doğru analizi siber saldırıların tespit edilmesinde büyük yere sahiptir. Bu sebeple sistem üzerinde donanımsal ve yazılımsal log sistemlerinin doğru konumlandırılmaları gerekmektedir. Bu durum siber saldırıların birçoğunun yapılmasını engelleyeceği düşünülmektedir. Bilgisayar ağlarına yapılan siber saldırıların tespiti için bir dizi yaklaşımların geliştirilmesi için çeşitli çalışmalar yer almaktadır. Siber saldırıların veri madenciliği yöntemleriyle tespit edilmesinde önemli bir faktör olarak görülmektedir. Siber saldırıların veri madenciliği yöntemlerini kullanarak engellendiği görülmektedir [62].

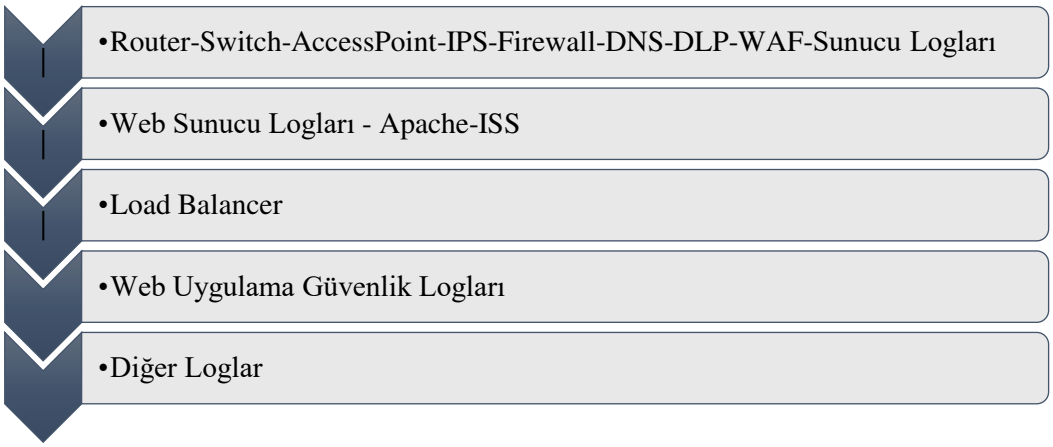
2.5.3.1. Siber Saldırıların Belirlenmesinde Kritik Log Kaynakları

SIEM ve MONITORING (İzleme) sistemlerinin bileşenleri içinde yer alan iç ve dış network trafiklerinden oluşan şüpheli aksiyonların izlenmesine olanak sağlayan ve aynı zamanda sistemlere zarar vermenin önüne geçilmesini sağlayan kritik ve önemli bir yapıya sahiptir. Şekil 2.15'de dış ortamdan içe doğru log analiz cihazları yer almaktadır. Bu anlamda log cihazlarının dıştan içe doğru konumlandırıldığı görülmektedir. Ayrıca şekil 2.16'da loglama sisteminin dıştan içe analiz adımları kullanılmaktadır [65].



Şekil 2.15. Dıştan içe log analiz cihazları şeması [55].

Sistemlerin güvenliği açısından iç ağa hangi servislerin çalıştırıldığı, dış ağa giden ve gelen trafiğin hangi sistemler üzerinden sağlandığı loglarının tutulmasını sağlamaktadır. Ayrıca iç ve dış ağada oluşan trafiğin log kayıtlarının incelenmesi analiz edilmesi, çeşitli siber saldırıların önüne geçilmesi için bir dizi kurallar oluşturulmasını, siber güvenlik politikalarının geliştirilmesinde büyük bir öneme sahip olduğu görülmektedir. İç ağ log kayıtlarından elde edilen önemli veriler alt başlıklarıyla aşağıda yer almaktadır. [55].



Şekil 2.16. Dıştan içe log analiz adımları [55].

2.5.3.2. İç Ağ Log Kayıtlarından Üretilen Bazı Önemli Veriler

Kimlik doğrulama sistemlerinin kullanıldığı bazı durumlar;

Sistemlere erişimler sırasında birçok kimlik doğrulama yöntemi kullanılmaktadır. Kimlik doğrulama kavramları aşağıda yer almaktadır [55].

- Kullanıcı hesapları ve hesap kilitlenmesi denetimi
- Grup işlemleri denetimi, bilgisayar hesapları denetimi
- Giriş işlemleri ve özel giriş aktivitelerinin denetimi
- Kimlik doğrulama sisteminde meydana gelen sapmaların denetimi

Güvenlik Duvarı;

- Network trafiğinin denetimi
- İletilen veri kapasitesi, bant genişliği ve tercih edilen protokoller
- Kara listede yer alan web adreslerine erişim isteği ve SMTP bağlantıları

DNS Sunucuları;

- İnternet erişimini izleme, aşırı istek yapan cihazlar
- Kara listedeki web sitelerini açma isteği
- DNS tünelleme ve DNS kayıtları ve DDoS saldırı ataklarının tespiti

DHCP Sunucuları

- Cihazlara atanan MAC, IP ve Hostname adresleri
- Sisteme bağlanan sistem dışı cihazların tespiti

Web Sunucuları

- IP, Zaman damgası ve HTTP kodları, Fazla login olmak ve İzinsiz denemeler
- Erişim kaynağı ve istemciye gönderilen veri boyutları
- XSS, SQL enjeksiyon, bellek saldırısı, komut çalıştırma ve zararlı program denemeleri tespiti

Web Proxy

- Kullanıcı davranışları ve Kural ihlalleri
- Erişime izin verilecek web sitelerini sınıflandırılması
- Dış sistemleri saldırı atağı gerçekleştiren lokal hesaplar
- Zararlı yazılımların bulaştığı cihazlar

Saldırı tespit sistemleri

- Sistemlere yapılan yoğun saldırılar
- Sistemler üzerinde en çok saldırı alan cihazlar
- Veri kayıpları

Router

- DoS, ortadaki adam ve TCP reset saldırıları
- Admin girişlerine yapılan atak saldırılar, network trafiği

Switch

- TCP, UDP ve ICMP trafiğinin izlenmesi

- ARP Poisoning ve MAC Flooding saldırıları

Altyapı

- Konumlandırma, network haritaları ve siber zafiyet raporları
- Ağ Segmentasyonu ve Kablosuz Ağlar, Bulut sistemler ve WAN

Riskli Aksiyonlar

- İzin verilen portların dışındaki portların hareketlerini izlememek
- İşletim sistemi açıkları, Sosyal mühendislik ve oltalama saldırılarıyla karşılaşmak

Dış Network Kaynaklı Gerçekleşen Riskler

- Network dinleme ve zararlı yazılımlar
- Kimlik doğrulama ve oturum hesaplarının izinsiz girişleri
- Sahte SSL sertifika ile saldırı, IP/Port, ağ keşif ve Botnetler

2.6. SALDIRI TESPİT VE SALDIRI ÖNLEME SİSTEMLERİ

Siber saldırılar, elektronik ortamda yer alan bilgilerin, bütünlüğünü bozulması, gizliliğin ihlal edilmesi, yetkisiz erişim sağlanması ve bu bilgilerin kullanılması gibi durumlarıyla karşı karşıya kalınan olaylar bütünüdür. Saldırı Tespit Sistemi, bilgisayar ağları üzerinde yetkisiz kullanıcılar tarafından gerçekleşen her türlü olayın tespit edilmesini ve önlenmesini sağlayan siber güvenlik sistemlerdir. Bu sistemler, Saldırı Tespit Sistemi (IDS) İzinsiz Giriş Önleme Sistemi (IPS) birlikte kullanılan iki saldırı sistemidir. Bu sistemler siber saldırıların tespit edilmesi ve önlenmesinde kullanılmaktadır.

2.6.1. Saldırı Tespit Sistemi

IDS, yazılım veya donanım sistemi olabilir. Bilgisayar ağlarındaki meydana gelen şüpheli trafiği keşfeden belirleyen siber güvenlik sistemidir. Ağ üzerindeki trafiği sürekli olarak taramayan güvenlik aracıdır. Ağda yer alan izinsiz girişleri tespit etmek için kullanılır. Sistemler üzerindeki anormal network trafiğini aramak için çalışır. IDS, network üzerindeki paketleri inceleyerek siber saldırı tespit eden sistemlerdir. Genellikle ağ üzerinde veri girdi çıktılarının yapıldığı yerlere, aynı güvenlik duvarı gibi konumlandırılırlar [64].

Konumlandırıldıkları yerdeki paketleri inceleyerek siber saldırıların tespit edilmesini

sağlarlar. IDS sistemlerinin bazı dezavantajları da bulunmaktadır. Büyük yapılı ağlarda bazı incelenmeyen paketler kalabilir. Kriptolu paketlerin iç yapısı incelenmez [65].

Aynı zamanda güvenlik seviyesi yüksek olan sunucu paketlerinin incelenmesinde ve siber saldırı tespitinde kullanılmaktadır. Bilgisayar ağlarında hızlı çalışmaktadır. Saldırı tespit uyarı sistemi gerçek zamanlı çalışmaktadır. Ağ trafiği içinde kriptolu paketlerin içeriğini incelemektedir. Kurulu olan bilgisayar üzerinde çalışmaktadır [66].

Log dosyaları bir network sisteminde kullanılan durumu hakkında bilgiler içermektedir. Ayrıca sistemler üzerinde anormal olayların tespit edilmesi kolaylaşır. Bu durum heterojen kaynaklardan oluşan büyük miktarda yapılandırılmamış ve çeşitli paketler içerdiğinden, log verilerini otomatik olarak analiz etmek daha zordur [67].

İnternet üzerinden bilgisayar sistemlerine yapılan siber saldırıların önlenmesini sağlayan güvenlik sistemidir. Sunucu üzerine kurulu olan yazılım sistemi de olabilir. Ağ trafiğini çok hızlı inceleyerek saldırıların gerçek zamanda tespit edilmesini sağlar [68].

2.6.1.1. Ana Bilgisayar Tabanlı IDS

Sunucu bilgisayar tabanlı izinsiz giriş tespit sistemi (Host-Based, HIDS), kurulu olduğu bilgisayar sistemi üzerinde gerçekleşen olayları izleyerek izinsiz girişleri tespit edilmesini sağlayan yazılım tabanlı bir saldırı tespit sistemidir. HIDS çalışma yapısı istemci-sunucu mimarisi kullanılmıştır. Bu anlamda görev ve sorumluluk alanı kuvvetli olan sunucu bilgisayarlarda daha yaygın olarak kullanılmaktadır. Gerçek zamanlı çalışmaktadır. Kurulu olan ana bilgisayarın güvenliğinden sorumludur. Kriptolu paketleri çözme kabiliyetine sahiptir. Aynı zamanda hassas bir yapıya sahiptir. Sistemlere izinsiz giriş yapılması ve kötüye kullanım tespit edildiğinde, gerçekleşen olayları loglara kaydederek gerekli sisteme bilgi vermektedir [25].

Ana bilgisayarlar herhangi bir saldırı için en uygun bilgisayarlardır. Bu anlamda erişim sağlayan kullanıcılar hakkında kilit bilgileri içermektedir. Bu çalışmada sistemler üzerinde gerçekleşen olay ve verilen dijital hizmetlerin gerçekleşmesinde oluşan log kayıtları kullanılarak sisteme erişim sağlayan kullanıcılar tespit edilir. Ayrıca bilgisayar tabanlı izinsiz giriş tespit sistemi (HIDS) geliştirilmiştir [69].

2.6.1.2. Ağ Tabanlı IDS

Network sistemleri üzerine daha önceden konumlandırılmış alan üzerindeki network trafiğini izlemek ve analiz etmek için kullanılır. Sistemler üzerinde izinsiz girişlerin tespit

edilmesini gösteren saldırı imzaları aranır [25].

Siber saldırı imzaları sistemler üzerinde gerçek zamanlı olarak izleme sağlar. Sistemler üzerinde anormal İletim Kontrol Protokolü/İnternet Protokol (TCP/IP) paket başlıklarını tespit eder. Bu anlamda sistemler üzerinde gerçekleşen aksiyonlar/olaylar gerçek zamanlı IDS sistemi ile tespit edilir. Büyük network ortamında bazı paketleri incelemeye bilmektedir. Aynı zamanda kriptolu paketleri çözme kabiliyeti yoktur [69].

2.6.1.3. Hibrit IDS

Hibrit Saldırı Tespit Sistemi (HIDS) ana sunucu bilgisayara gelen ve giden tüm paketlerin ağ trafiğini inceleyen güvenlik sistemidir. HIDS, ağ tabanlı IDS sisteminden daha fazla çalışmaktadır Ağ tabanlı IDS sisteminden farklı çalışmaktadır. Hibrit sistem daha fazla alan işgal etmektedir. Ayrıca HIDS sistemi donanım kullanımı daha fazladır [69].

2.6.1.4. İmza Tabanlı IDS

Kayıt altına alınan veriler üzerinden saldırı tespiti saldırı türüne göre karşılaştırılır. Saldırıların özellikleri önceden bilindiği üzere saldırı türü ile karşılaştırılarak siber saldırılar engellenmesi sağlanır. Saldırı ilk defa yapılıyorsa bu saldırı tespit edilemez. Bu sınıflandırma yapılan saldırı türünün önceden tanıtılması gerekmektedir. Olası saldırı ve tehditleri belirlemek için network içinde zararlı byte ve paket dizileri incelenerek daha önceden tespit edilmiş atak imzalar ile karşılaştırılarak saldırı tespit edilmektedir [69]**.**

2.6.1.5. Anomali Tabanlı IDS

Kayıt altına alınan veriler, önceki zamanlarda kayıt altına alınan veriler ile karşılaştırılmaktadır. Bu karşılaştırma sonrası veriler arasında anormal durumlar incelenerek saldırı tespit edilir. Sistem kayıtları üzerinde performans değerleri de incelenmektedir [70]. CPU, IO birimleri, RAM zaman ve kullanım değerleri değişiklikleri saldırı olarak tanımlanabilir. Aynı zamanda yeni saldırı türleri tespit edilebilmektedir. Kullanılan bu sınıflandırma kendi kendine öğrenme yeteneğine sahiptir. Bu durumda hata oranı düşük değildir [71].

2.6.1.6. İlke Tabanlı IDS

İlke tabanlı IDS, İmza tabanlı ve anormal tabanlı yönteme göre daha az kullanılmaktadır. Dışarıdan gelen misafirlerin, güvenlik ilkelerini tehdit eden veya şüpheli durum oluşturan faaliyetleri engellenir. İlke tabanlı IDS, daha önce belirlenen kurallar ve güvenlik ilkeleri belirlenip, yapılandırarak kullanılır [69].

2.6.2. Saldırı Önleme Sistemi

IPS, yazılım ya da donanım sistemi olabilir. Bilgisayar ağlarında tespit edilen yetkisiz kullanıcıları önlemek için kullanılan siber güvenlik aracıdır. IPS, sistem üzerine gelen ve giden tüm paketleri inceleyen bir sınıfa sahiptir. Bu sayede siber anlamda network sistemleri üzerinde bir hakimiyet sağlar [71].

IPS layer 2-7 katmanları arasında çalışır. İki farklı durum şeklinde çalışmaktadır. Karşı tarafa engelle geri dön, engelle geri dönme şeklinde çalışmaktadır. Tespit edilen kullanıcılara çeşitli kurallar uygular. Bu kurallar, sisteme erişim kısıtlaması, sisteme erişimi engellenmesi gibi bir dizi hizmet engellemesine gidilmektedir. IPS, network üzerindeki tespit edilen yetkisiz kullanıcıları engelleyen aktif, gerçek zamanlı siber güvenlik sistemidir [58].

Ayrıca yanlış-pozitif (false-pozitive) ve yanlış negatif (false-negative) değerleri imza tabanlı IDS'lere karşısında yeterince iyidir. Anormallik tespitinde, istatistiksel anormallik tespiti, veri madenciliği ve yapay zekâ özelliklerinden yararlanılmaktadır [67].

IDS sistemleri network trafiğini izlemek için başarılı sistemler olmasına karşın, ilerleyen süreçte oluşabilecek saldırılara karşı savunmasız kalabilirler. IPS sistemleri buna nazaran gelen siber saldırılara karşı hemen tepki göstererek tedbir alırlar, lakin network içinden meydana gelen tehditlere karşı koyma yeteneklerine sahip değillerdir [71].

IPS güvenlik sistemi kullanımı günümüz yıllarında yaygın olarak kullanılmaya başlanmıştır. Geleneksel saldırı tespit sistemleri ağ üzerinde bazı saldırılar karşısında kayıtsız kalmaktadır. IPS network üzerine gelen ve giden tüm paketleri inceleme kabiliyetine sahiptir.

2.6.2.1. Ana Bilgisayar Tabanlı IPS

Popüler bir teknoloji olarak literatüre geçmiştir. Sunucu ve işletim sistemi üzerinden aktiviteleri kontrol etmektedir. Bu sayede saldırı gerçekleşmeden işletim sistemi üzerinden önlenir. Ana bilgisayar üzerinden işlem gerçekleştiği için geniş bant genişliği gerekmektedir. Aynı zamanda bilgisayarın performansını etkileyecektir [73].

2.6.2.2. Ağ Tabanlı IPS

Kurulu sistem üzerindeki tüm network paketlerini inceler adeta koklamaktadır. Farklı güvenlik sistemleri ile entegrasyonu sonucu ortamın daha güvenli hale gelmesini sağlar. Aynı zamanda network sistemi üzerinde farklı düğüme kurulması yeterlidir. [73].

2.6.3. IDS/IPS Sistemlerinin Karşılaştırılması

IDS ve IPS siber güvenlik sistemleri Çizelge 2.9'da karşılaştırılmış, aynı zamanda önemli görev ve tanımlı özelikleri yer almaktadır. Sistemler üzerinde görev ve sorumluluk alanlarına yer verilmiştir. IDS ve IPS güvenlik sistemleri, network üzerinde birlikte kullanılması bu sistemleri daha güvenli hale getirmektedir. Aynı zamanda yeni nesil ağ teknolojileri içinde yer alan Yazılım Tanımlı Ağlar (SDN) için IDS/IPS birlikte kullanılması güvenliği artıracağı bir yapı önermektedir. SDN yazılım tabanlı olmasıyla birlikte açık kaynak güvenlik sistemleriyle entegreli çalışabilmektedir. Ayrıca IDS/IPS ve güvenlik duvarının siber güvenlik sistemi bünyesinde entegreli çalışması sistemlerin güvenlik düzeyini üst seviyelere çıkartabileceği gibi yapay zekâ teknolojilerinin de entegre edilmesiyle daha üst seviyeye çıkarabileceği yer almaktadır [74].

Çizelge 2.9. IDS/IPS sistemlerinin karşılaştırılması.

Saldırı Tespit Sistemi IDS	Saldırı Önleme Sistemi IPS
Saldırı tespit sistemidir.	Saldırı önleme sistemidir.
Ağ trafiğini analiz ederek yetkisiz kullanıcıları tespit eder.	Ağ trafiğini analiz edilen yetkisiz kullanıcıları engeller.
Güvenlik duvarı arkasında çalışır.	Güvenlik duvarı arkasında çalışır.
Bilgisayar ağlarında şüpheli ve risk faktörü oluşturan trafiği izler.	Bilgisayar ağlarında şüpheli ve risk faktörü oluşturan trafiği oluşturan kullanıcıları engeller.
Ağ trafiği içindeki paketleri engellemez.	Ağ trafiği kullanıcıları engelleyebilir.
Bilgisayar ağlarında şüpheli ve risk faktörü oluşturan trafiği analiz ve yorum için insan faktörü gerekebilir.	Bilgisayar ağlarında şüpheli ve risk faktörü oluşturan kullanıcıları engellemek için insan faktörü gerekmeyebilir.
IDS güvenlik duvarı ile entegreli çalışabilir.	IPS güvenlik duvarı ile entegreli çalışabilir.
Bilgisayar ağlarında şüpheli ve risk faktörü oluşturan trafiği analiz ve yorum gerekebilir.	Önceden belirleniş kuralları uygular.

2.6.4. IDS/IPS Siber Güvenlik Sistemleri Nitelikleri

Farklı zamanlar içinde aniden oluşabilen siber saldırılar karşısında sistemler savunmasız kalabilir. Network sistemlerin heterojen bir yapıya sahip olmaları bu durumu tetiklemektedir. Saldırı tespit sistemleri saldırıyı tespit etmeye çalışmaktadır. Saldırı önleme sistemi, tespit edilen saldırıları önlemeye çalışmaktadır. Her iki sistem üzerinde

gerçekleşen olaylar gerçek zamanlıdır. IDS/IPS sistemlerinin amacı, saldırıların bir an önce tespit edilmesinde önlenmesini sağlamaktır [72].

IDS ve IPS siber güvenlik sistemlerinin tek bir sistem üzerinde bileştirilmesinden yanadır. Bunun sebebi her iki güvenlik sisteminin Güçlerini birleştirmesidir. Böylece sistemler üzerinde güvenlik seviyesi biraz daha arttırılabilir. Ayrıca TOPASE dediğimiz bu sistem sayesinde kullanılan protokoller ile güncel siber saldırıların engellenebildiği görülmektedir. Bu durumda ana bilgisayardan gelen ağ trafiği kontrol altına alınabilmektedir [71].

IDS/IPS Sistemleri, ağ ve sistem katmanındaki şüpheli faaliyetleri tespit ederek siber anlamda risk değerlendirmesi yapan gerçek zamanlı siber güvenlik yazılımlardır. Yazılım aracı sistem üzerinde zafiyetleri tarayıp, sistem uzmanlarına sunmaktadır. Bu anlamda saldırıların önüne geçilmesi sağlanır [75]. İzinsiz Giriş Önleme Sistemi (IPS) ve Saldırı Tespit Sistemi (IDS), siber saldırıları belirleme önlemek ve tespit etmek amacıyla geliştirilmiş güvenilir saldırı önleme ve tespit etme sistemleridir. Siber tarafta yaygın olarak bilinen ve kullanılan sistemlerdir. IDS/IPS Sistemi Python programlama dili kullanılarak yazılmıştır. Python açık kaynak programlama dili olduğu için bu tür sistemlerin kod ile entegre edilerek Saldırı Tespit Sistemi (STS) geliştirilmiştir [76].

2.6.4.1. IDS metodolojileri

IDS güvenlik sistemi olası siber saldırılara karşı önlemler alarak networkleri korumaktadır. IDS güvenlik sistemi çalışma metodolojileri inceleyelim [72].

İmza tabanlı tespit**:** Siber tehditleri deşifre etmek, network içinde zararlı içerik ve paketleri önceden tespit edilmiş saldırı atak imzaları ile karşılaştıran sistemdir.

Anomali tabanlı tespit**:** Network sistemleri üzerinde normal davranışların dışında oluşan anormal davranışları tespit eden sistemdir. Network üzerinde normal dışı gerçekleşen aksiyonları belirler.

Durum protokol analizi**:** Zararsız protokol hareketlerinden oluşturulan hesaplar ile gözlenen şüpheli davranışları karşılaştıran ve sistem üzerinde oluşan normal dışı hareketlerin tespit edilmesi analizidir.

2.6.4.2. IDS/IPS Sistemi Çalışma Yapısı

IPS ve IDS Saldırı tespit ve önleme sistemlerinde, log kayıtlarını filtre uygulaması yaparak, kullanıcı bilgileri, hedef ve kaynak IP aynı zamanda hedef ve kaynak port,

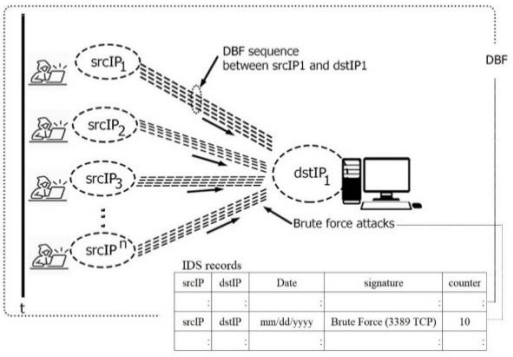
protokol ve MAC adres bilgileri filtreleyerek logların detaylı bir şekilde incelenmesine olanak sağlamaktadır [13].

IPS güvenlik duvarı arka planında çalışan tespit ve önleme sistemi olarak görev yapan, tehlikeli gördüğü ve güvenilir tüm içerikleri analiz ederek tehdit içeren verileri ayırmak üzerine geliştirilmiş bir katman bünyesinde çalışmaktadır. TCP protokolünde veri alışverişi katmanlar sayesinde yapılmaktadır. Bu katmanlar verileri paketler içinde taşımaktadır. Sistem üzerinde çalıştırılan bir güvenlik katmanı IPS devreye girerek, ağ trafiği üzerinde oluşan paketleri analiz ederek, kaynak ve hedef sistem arasındaki bağlantıyı sürekli kontrol etmektedir. Siber saldırı tespiti durumunda iletişimi, bağlantıyı ve veri akışı işlemini keserek, bağlantıyı sonlandırarak ve sistem yöneticisine saldırı hakkında bilgi verir. IPS gerçek zamanlı çalışan bir sistemdir. Analizlerin doğru tespit edilmesi sistemler için daha sağlıklı olur. Bu sistem hızlı çalışmasına rağmen bazen zararsız içeriklerinde siber tehdit unsuru olarak görebilmektedir. Bu durum sistemler üzerinde ağ performansı düşürebilir [72].

Sistemler üzerinde ağ trafiğinin izlenmesi için ve web sunucuya gelecek olan saldırı isteklerin içerisinde belirli saldırı desenlerini bulmaya çalışan, bulduğu saldırı tiplerini ve desenlerini kayıt altına alarak ve istendiği taktirde saldırı yapan IP adresini engelleyecek siber saldırıları engellemesi beklenmektedir. Python dili ile yazılmış bir IDS/IPS programıdır [76].

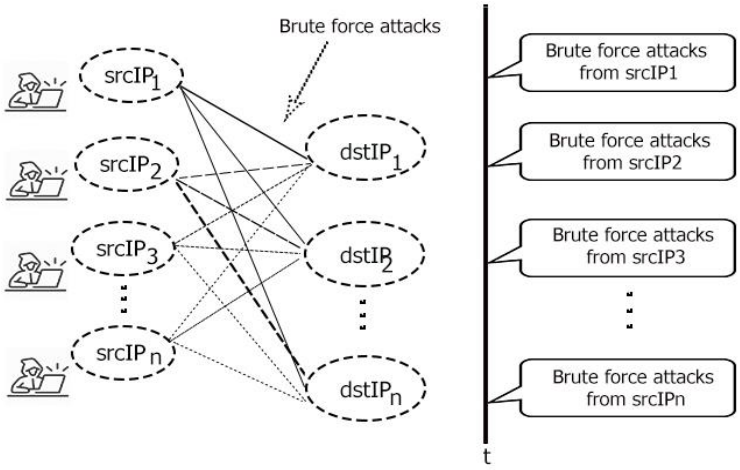
2.6.4.3. IDS/IPS Sistemi Mimari Yapısı

Veri Tabanı Güvenlik Duvarı (DBF), Şekil 2.17'de gösterildiği gibi bir tür dağıtılmış kaba kuvvet saldırısıdır. DBF, çoğul srcIP'ler hedeflenen dstIP'lere belirli sürelerle giriş yapmaya çalışır ve giriş denemelerinin sıklığını belirler. IDS kayıtları, her srcIP'nin bir dstIP'yi kaba kuvvet saldırılarının hedefi olarak belirlediğini göstermektedir. [72].



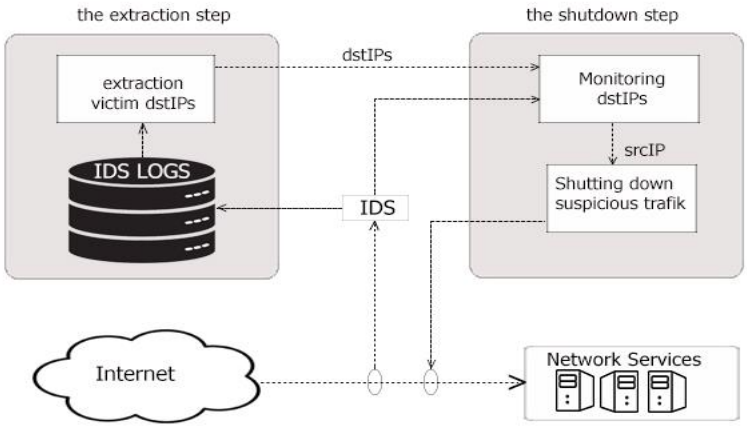
Şekil 2.17. DBF mimari yapısı [72].

Şekil 2.18'de yer alan görselde kullanıcılardan gelen Kaba Kuvvet Saldırıları (BFA) yer almaktadır. Aynı kullanıcıdan farklı hesaplara saldırılar yapılmaktadır. Kullanıcılardan gelen kaynak IP ve saldırıya maruz kalan hedef IP adresleri yer almaktadır. Hedef alınan IP adreslerine farklı kaynaklardan siber saldırıların BFA yapıldığı görülmektedir. Kullanıcılardan gelen n IP adresi kadar saldırı denemesi yapılmıştır [72].



Şekil 2.18. Siber saldırı [72].

Şekil 2.19' da yer alan görselde EBF ye ait bir mimari önerisi yer almaktadır. Kullanılan mimari yapıda IDS/IPS güvenlik sistemleri korunmak istenen network sistemi ile internet arasında konumlandırılmıştır.



Şekil 2.19. EBF' ye karşı mimari örneği [72].

2.6.4.4. IDS/IPS Sistemi Kod Yapısı

Sistemler üzerine yapılan kaba kuvvet saldırıları kullanıcıların kullanıcı adı ve şifrelerini deneyerek sistemlere erişim sağlanması için yüzlerce deneme yaparak oluşan saldırı türüdür. Kaba kuvvet saldırıların engellenmesinde en önemli güvenlik önleme sistemlere kullanıcı bilgilerini deneme sayısı koymasıdır. Sistemlere giriş noktasında IPS sistemi devreye girerek kaba kuvvet saldırıların trafiğini engelleyebilir. Son zamanlarda günümüz saldırılarında IPS ve IDS sisteminden kaçabilen saldırı türlerinde çıkmıştır.

Saldırganlar, sunucu makinalara erişim saldırıları gerçekleştirerek kaba kuvvet saldırıları engellemek için kullanılan panel şifre denemelerini değiştirmektedir. Bu makale çalışmasında web sayfalarına sistemlere entegre edilen IDS sistemi log analizleri yaparak Uzak Masaüstü Protokolüne (RDP) karşı bir tür dağıtılmış kaba kuvvet saldırı olayını gerçekleştirilmiş kaba kuvvet saldırıları yapan kullanıcıların IP-DBF adresleri rapor edilmektedir. DBF, belirli sayıda saldırı ana makinadan bir hizmete belirli bir süre otomatik olarak tekrar eder. Yapılan siber saldırılara karşı TOPASE önerilmiştir. TOPASE, ana bilgisayar ile hedef bilgisayar arasındaki oturum açma denemelerini analiz eder. TOPASE, kaba kuvvet saldırısının yapıldığı kaynak bilgisayardan gelen ağ trafiğini belirli bir süre keser. IDS sistemi kullanılarak log dosyalarından siber saldırılara karşı performans tahmini analizi yapılması sağlanır [71].

2.6.5. Saldırı Tespit ve Önleme Sistemi Geliştirilmesi

Siber uzay, bilişim sistemlerinin gelişmesi ve büyümesiyle karmaşık hale gelmektedir. Bu büyük uzayda homojen ve heterojen ağlar giderek yaygınlaşmaktadır. Bu anlamda gerçekleşen tüm işlemler dijital ortamda yapılmaktadır. Dijital ortamda oluşan verilerin siber uzayda bilinmeyen tespit edilemeyen tehlikelere yol açmaktadır. Bu durum siber uzayda bilgi güvenliğini gizlilik ve bütünlüğü tehlikeye atmaktadır. Bu tehlikeye karşı koymak için IDS sistemi kullanılmıştır. Bu sistem sayesinde kullanıcılara siber uzayda güvenli ortam sağlar. Sistemler üzerinde gerçekleşen olaylarda kimlik doğrulama sistemi ve güvenlik duvarı hayati öneme sahiptir [72].

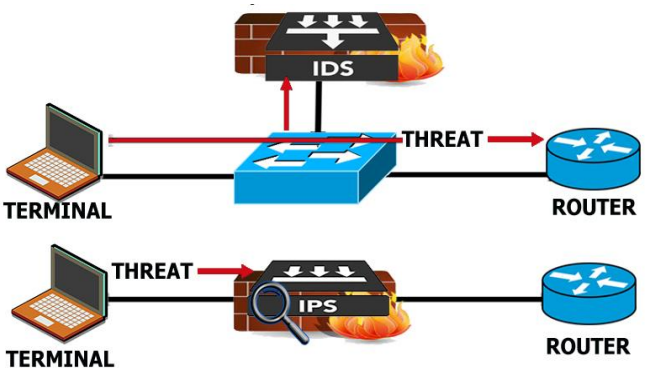
Saldırganlar sistemlere sımak için siber uzayda tüm yeteneklerini ve araçları kullanır. Bu bağlamda saldırganlar güvenlik duvarını atlatarak sistemler üzerinde istedikleri yetkiye sahip olarak istedikleri işlemleri yaparlar. Bu anlamda network içinde hareketleri izlemek ve tespit etmek için IDS sistemi kullanılması ve güvenlik duvarı ile entegre halinde çalışması sağlanabilir. Aynı zamanda saldırı tespit sistemi sayesinde IPS sisteminin kural

uygulamasıyla karşı karşıya kalan saldırganın engellenmesi sağlanır. Bu bağlamda tez kapsamında 3.bölümde saldırı tespit ve önleme sistemi önerisi yer almaktadır.

2.7. SALDIRI TESPİT ve ÖNLEME SİSTEMİ YAPILAN ÇALIŞMALAR

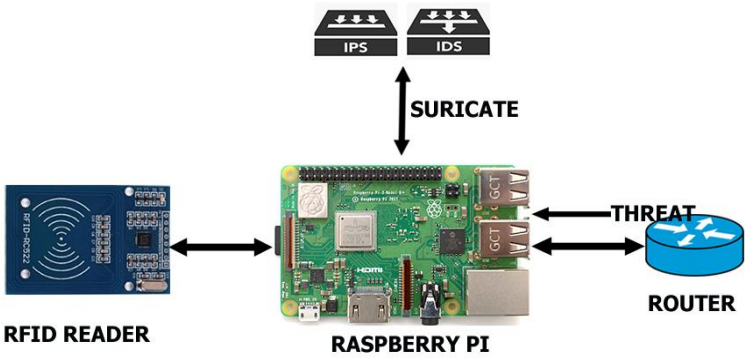
2.7.1. Raspberry Pi Kullanarak IDS/IPS Geliştirme

Bu çalışmada, Düşük Seviye Okuyucu Protokolü (LLRP) arayüzü için geliştirilen algılama kuralları, Raspberry Pi 3 kullanarak Ultra Yüksek Frekans (UHF), Radyo Frekansı Tanımlama (RFID), IDS ve IPS çözümleri uygulanmıştır. Geliştirilen güvenlik çözümü, LLRP destekleyen mevcut Radyo Frekansı Tanımlama (RFID) okuyucuların güvenliğini sağlamak için kullanılmaktadır. Ayrıca IPS/IDS çözümlerinin karşılaştırılmasını sağlamaktır Şekil 2.20'de IDS/IPS topolojisine yer verilmiştir. Genellikle piyasada herhangi bir şifreleme desteği olmadan kullanılabilir. İşlevsellik düzeyi metasploit framework yazılımı ile test edilmiştir. IoT ve Endüstri 4.0 konseptlerindeki cihazlar ve hizmetler geniş bir uygulama yelpazesinde (örneğin evler, fabrikalar ve şehirler) kullanılmaktadır. Bu cihazlar ve hizmet üretebilmeleri için, internet altyapısını kullanarak bir dizi bilgiyi kullanıcılarına iletmektedir. Bu veriler içinde birçok kişisel bilgiler, mahrem ve gizli bilgiler bulunmaktadır. Bu nedenle bu cihazların siber saldırılara karşı korunması muhtemeldir. IoT ve Endüstri 4.0 uygulamalarındaki cihazlar genellikle antivirüsler tarafından korunmaz ve standart işletim sistemlerinden bilindiği gibi güvenlik açığı düzeltmeleri içeren aylık güncellemeleri almazlar. Bu durum, botnetlere bağlı saldırıya uğramış cihazlarla ilgili birçok vakaya yol açmaktadır. Dolayısıyla bu akıllı cihazları geleneksel güvenlik çözümlerinden farklı bir şekilde korumak gerekmektedir Yazılım Tanımlı Ağ (SDN), mevcut kapalı ağ ortamlarını bireysel ağ sağlayıcılarının teknolojilerine dayalı olanlardan, ağ soyutlaması yoluyla basitleştirilmiş, programlanabilir bir esnek, merkezi yönetim ortamına dönüştüren ağ teknolojisidir. Bu nedenle, geleneksel ağların aksine, SDN bazı güvenlik sorunlarına karşı avantajlara sahiptir [77].



Şekil 2.20. IDS/IPS topolojileri [77].

Bununla birlikte, mevcut ağ güvenlik sorunlarının çoğu ve zayıf noktaları SDN ortamında bulunmaktadır ve buna yönelik çeşitli saldırılar gerçekleşmektedir. Şekil 2.21'de IDS/IPS çözüm topolojisi çalışmasına yer verilmiştir. Raspberry Pi kullanılarak topoloji çözümü geliştirilmiştir [77].



Şekil 2.21. IDS/IPS çözüm topolojisi [77].

Saldırı Tespit ve Önleme Sistemleri (IDPS) teknolojilerinin temel türleri, tehditlerin analiz edildiği bir konuma göre belirlenebilir. Belirli ağ segmentleri veya cihazlar için ağ trafiğini izleyen ve şüpheli etkinlikleri tanımlamak için ağ ve uygulama protokolü etkinliğini analiz eden Ağ Tabanlı Saldırı Tespit ve Önleme Sistemleri (NIDPS) olarak kullanılmaktadır. Sunucu bilgisayar üzerinde şüpheli davranışları olan kullanıcıları tespit edilmesinde ve bu ana bilgisayar üzerinde meydana gelen olayları izleyen sisteme Ana Bilgisayar Tabanlı Saldırı Tespit ve Önleme Sistemleri (HIDPS) denir. Tehdit analizi için temel tespit metodolojileri, bilinen güvenlik olaylarının imzalarına (İmza Tabanlı tespit), ağ veya cihazların olağandışı davranışlarına Anomali Tabanlı Tespit (ATT) ve gelen veya

giden verilerin protokol tanımlarının profilleriyle karşılaştırılmasına Durum Tespitli Protokol Analizi dayanır. Mevcut IDPS'ler doğru tespit sağlamak için tespit metodolojilerini birleştirir [77].

IDS/IPS çözüm önerisinde görüldüğü üzere açık kaynak donanım cihazları ve siber sistemler entegre edilerek yeni bir siber saldırı tespiti yapabilen ve bu saldırıları önleye bilen bir cihaz geliştirilmiştir. Bu tür sistemlerin geliştirilmesi siber saldırıların tespit ve önlenmesi adına SSTS geliştirmek isteyen araştırmacılar için faydalı olacağı düşünülmektedir [78].

2.7.2. IPS ile Kullanılan Araçlar ve Çözümleri

ACARM-ng: Alert Correlation, Assessment and Reaction Module-next generation (ACARM-ng) bilgisayar ağları analizi için geliştirilen bir yazılımdır. ACARM-ng içerik uyarıları oluşturur ve aynı zamanda ilişkilendirir. İlişkili uyarıları benzer olaylar olarak gruplar halinde sıralar. ACARM-ng mimarisi, uyarı korelasyonu için filtreler, uyarı toplama için tetikleyiciler ve veri depolamak için veri tabanından oluşur. ACARM-ng, toplanan uyarıları Saldırı Tespit Mesajı Değişim Formatı (IDMEF) biçiminde girdi olarak okuyabilmektedir [79].

Bro-IDS Bro: Bro sisteminin yapısı, paket yakalamak için libpcap, paket analizine dayalı olaylar oluşturmak için olay motoru ve komut dosyalarına dayalı olayları işleyen komut dosyası yorumlayıcısından oluşur. Geçersiz paket tespit edilirse atılır ve olay oluşturulur. Bro IDS GNU/Linux sistemlerini desteklemektedir [80]. Network güvenlik monitörü, izinsiz girişleri gerçek zamanlı olarak tespit eden bir ağ analiz programıdır [81].

eXpert-BSM: eXpert-BSM monitör içeriden kötüye kullanımı, kural ihlallerini, ayrıcalıkların kötüye kullanımını, yasadışı kaynak manipülasyonunu vb. tespit etmek için bilgi tabanını kullanan ana bilgisayar tabanlı bir saldırı tespit sistemidir [82]. eXpert-BSM veri toplama, saldırı tespit analizi, uyarı yönetimi arayüzü ve ayrıntılı yanıt direktifleri sağlar. Solaris işletim sistemi için geliştirilmiştir. Bu sebeple gömülü sistemler için uygun değildir [81].

Fail2ban: Log dosyalarını tarar ve izinsiz girişlere karşılık gelebilecek saldırıları tespit eder. Daha sonra bir güvenlik duvarı zincirine yeni bir kural ekler ve gönderilen bir e-posta bildirimi ile sistem yöneticisini bilgilendirir. Fail, 2 bölümden oluşur: Bu bölümler istemci ve sunucu bölümleridir. Sunucu çok iş parçacıklarından oluşur. Komutlar için bir Unix soketini dinler. İstemci sunucu soket dosyasına bağlanır ve sunucuyu yapılandırmak

ve çalıştırmak için komutlar gönderir. Tanımlanan filtre ve eylem kombinasyonu bir gizli dosya olarak temsil edilir. Fail2an GNU/Linux platformunda desteklenmektedir. Python ile yazılmıştır [83].

OSSEC: Open Source SECurity (OSSEC) Açık kaynak güvenlik, dosya bütünlüğü izleme, günlük izleme, rootcheck ve süreç izleme gibi işletim sistemi olaylarını izleyen ana bilgisayar tabanlı saldırı önleme sistemidir. OSSEC, açık kaynak ve kapalı kaynak sistemler üzerinde bağımsız bir HIDS olarak çalışabilir [84].

Prelude Open Source Security (OSS): Prelude SIEM'in açık kaynaklıdır. Prelude OSS, belirli düzeyde büyüklükteki BT altyapıları, değerlendirme, araştırma geliştirme ve test uygulamaları için tasarlanmıştır. Saldırı tespit sistemi ve olay yönetim sisteminin temel yeteneklerine sahiptir [85]. Prelude OSS'nin mimarisi yönetici sunucu ve algılayıcılardan oluşur. PreludeLML Prelude OSS, OSSEC, Snort, Suricata vb. gibi diğer açık kaynaklı salgılayıcı uyumlu olmasını sağlayan IDMEF formatıyla uyumludur [86].

Sagan: Gerçek zamanlı günlük analizi ve korelasyon motoru sağlayan açık kaynaklı bir yazılımdır. GNU/Linux, UNIX ve Berkeley'in Yazılım Dağıtımı (BSD) işletim sistemlerini desteklemektedir. SIEM işlevlerine sahiptir. IDS olarak da yapılandırılabilir.

Ana bilgisayarlardan gelen loglar syslog-ng ve rsyslog programları aracılığıyla toplanır. Sagan, diğer cihazlardan ve sistemlerden örneğin, güvenlik duvarları, yönlendiriciler, Windows olay günlüklerini desteklemektedir.

Sagan, gözlemlenen olaylardan izinsiz girişleri tespit edebilir ve günlük olaylarını ilişkilendirebilen Snort IDPS ile benzer şekilde çalışır. Sagan, örneğin çoklu çıktı formatlarını ve izinsiz giriş tespitinde komut dosyası yürütmeyi destekler [87].

Samhain: Dosya bütünlüğü denetimi ve log kayıtları izleme/analiz, rootkit tespiti, bağlantı noktası izleme, hileli Set User ID (SUID) yürütülebilir dosyalarının tespiti ve gizli işlemler gerçekleştirebilen ana bilgisayar tabanlı bir saldırı tespit sistemidir. GNU/Linux için geliştirilmiştir. Veri tabanında log kaydı depolar ve istemci/sunucu mimarisine sahiptir. İstemci ve sunucu arasında şifrelenmiş ve kimliği doğrulanmış bağlantılar kullanılır [85].

Snort: İnternet ağlarında gerçek zamanlı trafik analizi ve log kayıtlarının tutulmasını sağlayan açık kaynaklı bir ağ saldırı önleme sistemidir. Snort Cisco Systems tabanlıdır. Snort, paket koklayıcı, ön işlemci, algılama motoru ve kaydediciden oluşur. Koklanan paketler TCPDUMP formatında saklanır ve incelenebilir.

Önbellek taşmaları, gizli bağlantı taramaları, CGI saldırı bulma, SMB probları, işletim sistemi girişi için parmak izi sistemi gibi çeşitli saldırıları ve probları tespit etmek için kullanılabilen protokol analizi, içerik arama, eşleştirme gerçekleştirilebilir.

Snort, yönetici tarafından oluşturulabilen imzaları kullanır. IPS işlevsellik için güvenlik duvarı ile iş birliği gerekir. TLS trafiğini çözen SSL Dynamic Preprocessor (SSLPP) özelliğine sahiptir [88].

Suricata: Gerçek zamanlı izinsiz giriş tespiti, hat içi izinsiz giriş önleme yapabilen açık kaynaklı bir motordur ve ağ güvenliği izleme özelliğine sahiptir. Suricata, kendinden imzalı veya sahte sertifika algılama yeteneğine sahip TLS Parser içerir. Kapsamlı protokol desteğine sahiptir (UDP, TCP, TLS/SSL, HTTP). Linux sistemleri desteklemektedir [89].

IPS araçlarının önemli özellikleri Çizelge 2.10'da yer almaktadır. Çizelge 2.10'de yer alan veriler incelendiğinde C, D ve J harfleri ile temsil edilen araçların ölçülebilirlik oranları yüksek çıkmıştır. Bu yüzden loglama sistemlerini destekledikleri için log analizleri üzerinden siber saldırıların tespit edilmesi ve önlenmesi uygulamalarında kullanılabilir oldukları görülmektedir.

Siber güvenlik açısından yazılım güvenliği sistemlerin en önemli kalkanıdır. Güvenlik önce sistem üzerinde kullanılan yazılım araçlarında başlar. SSTS kullanılan yazılım sistemlerinin üzerine entegre edilir. Sistemler üzerinde çalışan yazılımların zafiyetlerinin olması en sağlam güvenlik duvarı bile koruyamaz [77].

Çizelge 2.10. IPS özellikleri ve çözümleri [77].

Yazılım Araçları Sembolü	Yazılım Aracı	Açık Kaynak Desteği	Linux Desteği	Ağ Desteği	IPS	Çoklu Ağ	Ölçeklenebilirlik
A	ACARM-ng:	x	x	x	x	x	Düşük
B	Bro-IDS Bro:	x	x	x	-	-	Düşük
C	eXpert-BSM	-	-	x	-	-	Yüksek
D	Fail2ban	x	x	x	x	x	Yüksek
E	OSSEC	x	x	-	x	-	Düşük
F	Prelude OSS	x	x	x	-	-	Düşük
G	Sagan	x	x	x	-	x	Yüksek
H	Samhain	x	x	x	-	-	Yüksek
I	Snort	x	x	x	x	-	Orta
J	Suricata	x	x	x	x	x	Yüksek

Çizelge 2.11'de yer alan araçların log kayıtları üzerinden analiz edilerek siber saldırıların tespitini yapabilecek araçlar yer almaktadır. Bu araçlardan bazılarının log kayıtlarına olanak sağladığı görülmektedir. Son yıllarda kullanılmaya başlanan IDS Sistemi, saldırıların boyutunu göstermektedir.

İçerik Yönetim Sistemi olan WordPress 2013 yılında açıklamış olduğu rapora göre büyük çapta kaba kuvvet saldırıların hedefi olmuştur [90].

Rapora göre yaklaşık 9000 sunucudan kaba kuvvet saldırı yapılmış olup, 1 milyondan fazla oturum şifresi denenmiştir [90].

GitHub, büyük çapta kaba kuvvet saldırısına maruz kalmıştır. Bu saldırılar 40 bin IP üzerinden yapılmıştır [91].

Saldırılar, geçici IP'ler kullanılarak bir tür dağıtık ve gizli BFA rapor edilmiştir [92].

Log kayıtları üzerinden IDS Sistemi kullanılarak sistemlere yapılan siber saldırıların tespit edilmesi ve önlenmesi çalışması yer almaktadır. Bu çalışmayla tez önerisinin yapılabilirliğini daha da güçlenmiştir [92].

Çizelge 2.11. IPS çözümlerinin log uyumluluğu

SN	Yazılım Aracı	Ölçeklenebilirlik	Log Desteği
1	ACARM-ng:	Düşük	-
2	Bro-IDS Bro:	Düşük	-
3	eXpert-BSM	Yüksek	Var
4	Fail2ban	Yüksek	Var
5	OSSEC	Düşük	-
6	Prelude OSS	Düşük	-
7	Sagan	Yüksek	-
8	Samhain	Yüksek	-
9	Snort	Orta	-
10	Suricata	Yüksek	Var

Saldırı Tespit ve Önleme Sistemi (STÖS) kullanımının yaygınlaştırılması için, STSS kullanımının yaygınlaştırılması, geliştirilmesi için çeşitli olanakların sunulması gerekmektedir. Siber güvenlik disipliner bir yaklaşıma sahip olduğu için alan uzmanlarının bilgi ve tecrübeleri STSS Sistemlerinin daha iyi geliştirilmesine olanak

sağlayacaktır. Siber saldırıların vermiş olduğu zafiyetlerin maliyetleri yüksek olduğu gibi STSS geliştirilmesinde bir o kadar maliyetli ve sabır gerektiren konudur. Makale çalışmalarında geliştirilen STSS çözümlerini incelenmiştir. Çalışmada IDS ve IPS güvenlik sistemleri bir arada kullanılmıştır [93].

Kullanıcıların sistemler üzerinde oluşturdukları loglar, adli bilişim analizleri, siber saldırılar gibi konuların tespitinde önemli yere sahiptir. Sistemler üzerinde zafiyet tespitinde oluşan log kayıtları kullanıcılar hakkında ulaşılabilecek bilgilerin tek adresidir. İyi niyetli veya kötü niyetli kullanıcıların oluşturduğu log kayıtları birçok siber izi bulmada yardımcı olmaktadır. Toplanan logların analizleri incelendiğinde, siber saldırıların tespiti için loglama öncesi ve sonrası çeşitli bölümlerden oluşan adımlar yer almaktadır. Bu bölümlerde yer alan adımlar bütünden parçaya doğru hareket ederek logların kademe kademe işlenmesini sağlar.

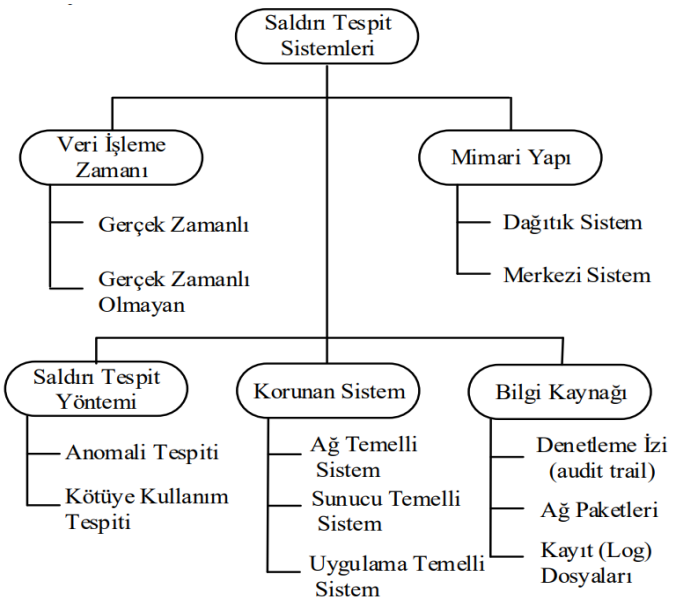
Ayrıca bu kademeler birbirini takip ederek, oluşabilecek siber saldırıların önlenmesi için IP adresleri belirlenerek sisteme zarar vermeleri engellenir. Önce veriler toplanır, normalleştirme işlemleri yapılır, uygulama kısmına geçilir, uygulamalardan loglar toplanır, loglar analiz edilir, daha sonra analiz sonuçları görselleştirilir, akabinde uygun olanların işlemleri yapılır, siber saldırı yaptığı düşünülen IP adresleri bloke edilir. Bu sayede kullanıcılardan oluşan loglar performans, izleme, dinleme, denetim, yönetim, engelleme, bloke etme, bilgi işlem süreçlerinin iyileştirilmesi konularında farklı yaklaşımlar ve farklı kararların alınmasını sağlar [94].

Open Web Application Security Project (OWASP), internet üzerinden çalışan uygulamaların daha güvenli hale getirilmesi, daha iyi şekilde geliştirilmesiyle standart yükseltmeye çalışan kâr amacı içermeyen bir kurumdur.

Uygulamaların büyük çoğunluğu web üzerinden çalışmaktadır. Web uygulamalarının dijital büyük bir ağ olan internet üzerinden erişim sağlanması, masaüstü uygulamalarından, web form uygulamalarına geçmesini sağlamıştır. Sistemlere erişim sağlanması siber uzayda birer tehdit unsuru haline getirmiştir [95].

Siber saldırı tespit sistemleri kapsamında, loglama sistemlerinin yer alması siber saldırı tespitini hızlandıracağı gibi daha güçlü hale getirecektir. Log kayıtları önerilen mimari yapıya uygun olarak tasarlanması düşünülmektedir. Siber güvenlik sistemi üzerinde yer alan alt kademelerde gerçekleşen olaylar ayrı ayrı log kayıtları alınması sağlanabilir. Siber saldırılar web sistemlerini daha fazla zarar vermektedir.

Web üzerinden hizmet veren teknolojiler homojen ve heterojen yapıya sahiptir. Bu anlamda daha fazla siber saldırılara maruz kalmaktadır. Microsoft siber raporu ve OWASP raporları siber saldırı konusunda bizlere yol haritası çıkarabilir. Önerilen saldırı tespit ve saldırı önleme sistemi bünyesinde IDS/IPS siber anlamda güvenlik sistemleri kullanılmıştır. Ayrıca Şekil 2.22'de saldırı tespit sistemlerinin sınıflandırılması yer almaktadır.



Şekil 2.22. Saldırı tespit sistemlerinin sınıflandırılması [8].

Önerilen her iki çalışmada sistem mimarisi, çalışma yapısı ve kullanılan kod yapısı ortak özellikler olarak karşımıza çıkmaktadır.

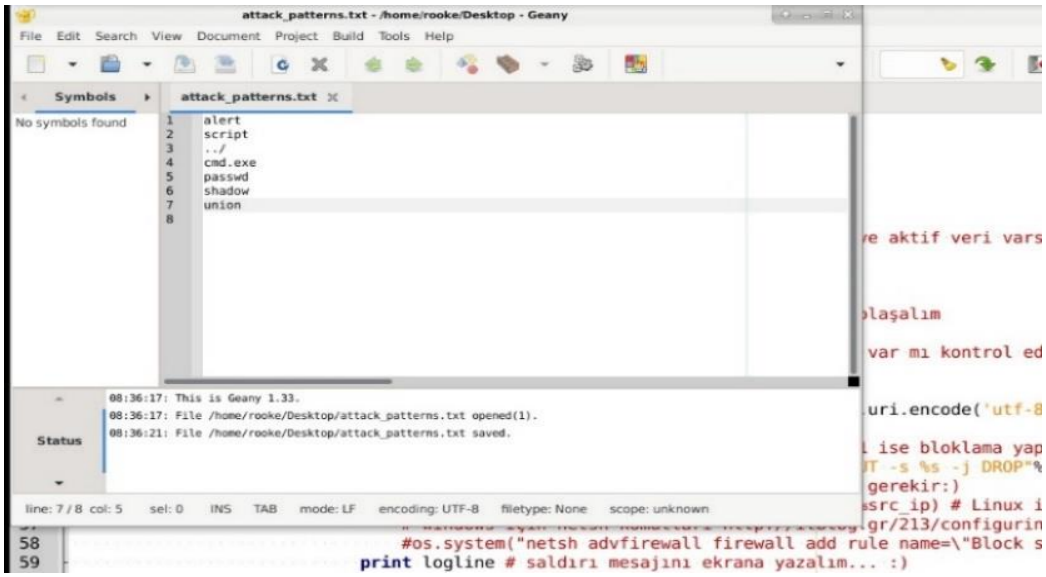
2.7.3. Python IDS/IPS Geliştirme

Açık kaynak platformlar neredeyse tüm sistemler üzerinde çalışabilmekte ve ayrıca açık kaynak yazılım dillerinin kütüphaneler ile desteklenmesi de bu durumu güçlendirmektedir.

Python programlama dili açık kaynak özelliği sayesinde IDS/IPS sistemi kullanılarak saldırı desenleri tespit edilmiştir. Siber saldırı tespitinde IDS sistemi hızlı ve doğru bir şekilde saldırı desenlerini tespit etme kabiliyetine sahiptir.

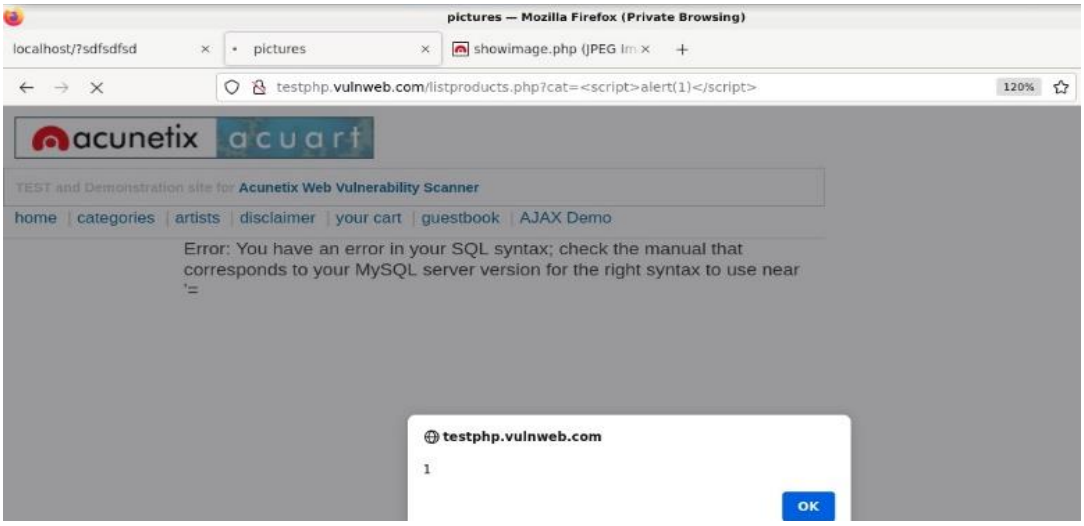
Saldırı desenlerine daha yeni saldırı desenleri eklenerek daha detaylı tespit yapılabilir. Python dili ile geliştirilen saldırı tespit sistemi kodları ekler bölümünde şekil 6.1'de yer almaktadır [76].

Saldırı desenleri saldırı türüne göre değişiklik gösterebilmektedir. Saldırı tespiti için yer alan saldırı desenleri Şekil 2.23'de yer almaktadır. Yapılan siber saldırıların sürekli değişim göstermektedir. Bu nedenle saldırı desenleri sürekli güncellenmesi gerektedir.



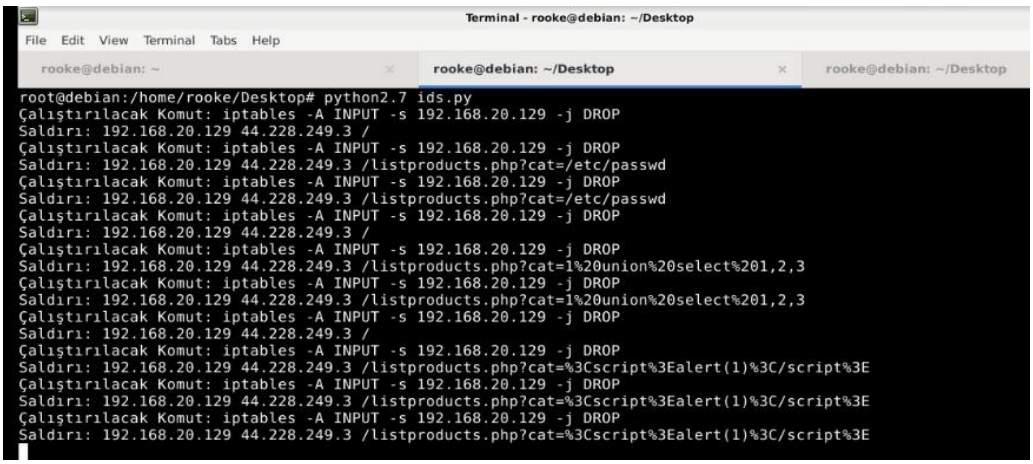
Şekil 2.23. Saldırı desenleri.

Python dili kullanılarak yazılan IDS/IPS sistemi gerçek zamanlı çalışmaktadır. Şekil 2.24'de yer alan web adresine kaba kuvvet saldırısı yapılmıştır. Yapılan bu saldırı gerçek zamanlı tespit edilmesi için şifre deneyen kullanıcıda saldırı desenleri anlık aranmıştır. Kaba kuvvet saldırısı gerçekleştiren kullanıcı üzerinde tespit edilen saldırı desenleri, şifre deneyen kullanıcı bilgilerini log kayıtları üzerinden IDS sistemi ile tespit edilerek IPS sistemi bünyesinde saldırı gerçekleştiren kullanıcı erişimi engellenmiştir.



Şekil 2.24. Saldırı yapılan web sitesi.

Python yazılım dilini kullanarak yazılan kod satırlarında IDS/IPS sistemlerinin eklenmesiyle bir saldırı tespit sistemi oluşturulmuştur. Yazılan saldırı tespit sistemi sayesinde, saldırı yapılan sisteme kaba kuvvet saldırı tekniği kullanılarak şifre denemesi yapan kullanıcı IPS/IDS sisteminin devreye girmesiyle engellenmiştir. Bu sayede saldırı yapan saldırgan cihazın IP adresi bloke edilmiştir. Bloke edilen IP adresleri Şekil 2.25'da yer alan görselde gösterilmektedir. Bu durum açık kaynak kod yapısının, açık kaynak saldırı tespit sistemlerinin entegre edilmesiyle doğru çalıştığı görülmektedir.



Şekil 2.25. IDS/IPS ile saldırgan IP tespit edilmesi ve bloke edilmesi.

3. SİBER SALDIRILARIN LOGLAR ÜZERİNDEN TESBİT EDİLMESİ VE ÖNLENMESİ ÇALIŞMALARI

3.1. SALDIRI TESPİT VE ÖNLEME SİSTEMİ ÖNERİSİ

Bu çalışmada siber uzayda network sistemlerini daha etkili korumak için iki çözüm önerisi sunulmuştur. İlk çözüm önerisi incelendiğinde, yazılımsal olarak tasarlanan, log teknolojileriyle entegreli çalışan açık kaynak IDS/IPS güvenlik sistemi önerisi yer almaktadır. İkinci çalışmada ise bu çalışmaya ek olarak güvenlik duvarı teknolojilerinin eklenmesi önerisi yer almaktadır. Bu sayede ikinci çalışmada yer alan sistem önerisi Siber Güvenlik Sistemi olarak karşımıza çıkmaktadır.

3.1.1. Saldırı Tespit ve Saldırı Önleme Sistemi Mimari Yapısı

Önerilen Siber Saldırı Tespit ve Önleme Sistemi (STÖS) açık kaynak uygulamanın çalışma/sistem mimarisi tasarlanmıştır. Siber saldırıların tespitinin yapılması için Python dili kullanılarak açık kaynak bir uygulama yapılmıştır.

Önerilen sistemde IDS/IPS birlikte kullanılması önerilmiştir. Uygulama kaba kuvvet saldırıları, sisteme erişim sağlama gibi siber saldırıların engellenmesi hedeflenmiştir. Bu sayede geliştirilen açık kaynak uygulama ile siber saldırılar tespit edilerek, gerekli önlemlerin alınması sağlanır. Bu sistemler siber saldırı durumlarında network ortamında gerçek zamanlı güvenlik sağlamaktadır. Network üzerinde anormal ve şüpheli davranış tespit edilmesi durumunda kullanıcıların network ortamına erişimi engellenir.

Aynı zamanda sistem kullanıcıları da aynı şekilde siber güvenlik sistemi üzerinde ilerleyeceklerdir. Sistem kullanıcıları kimlik doğrulama bilgilerini hatalı girmeleri ve tekrar eden giriş denemelerinden kaynaklı sisteme erişmeleri söz konusu olmayacaktır.

Kaba kuvvet saldırıları incelendiğinde siber saldırlar içinde yoğun bir şekilde kullanılan saldırı türüdür. Kaba kuvvet saldırıları popülerliğini sürdüren bir saldırı türü olarak karşımıza çıkmaktadır. Bu sayede kullanıcıların farklı saldırı türlerini kullansalar bile sisteme erişimi kısıtlanabilir ya da ilerleyişi durdurulabilir. Kısıtlanan ya da engellenen kullanıcılar sistem üzerinde bir işlem yapamaz hale gelir.

3.1.1.1. Web Sunucu Loglarına Göre Mimari Tasarımı

Geliştirilen STÖS uygulaması, web sunucu logları baz alınarak siber saldırı tespiti yapılmaktadır. Dışarıdan gelen kullanıcıların web, IP numarası, HTTP kodları, işlemlerin gerçekleştiği tarih-saat bilgileri ve byte olarak loglarda tutulmaktadır.

Sistem mimarisi log türüne göre değişiklik gösterebilir. Yönlendirici log dosyaları analiz edilerek saldırganların tespit edilmesi isteniyorsa, mimari bu log türüne göre oluşturulabilir. Ayrıca mimari oluşumunda tüm log dosya türleri kullanılması gerekmektedir. Web sunucularının yoğun olarak kullanılması siber saldırıların önünü açmaktadır. Bu anlamda web sunucu hizmeti sağlayan sistemler üzerinde log sunucuların kullanılması saldırı sayısını düşürmektedir.

3.1.1.2. Yönlendirici Log Dosyalarına Göre Mimari Tasarımı

Geliştirilen STÖS uygulaması mimari olarak, yönlendirici log dosyaları içeriği eklenebilir. Sistemlere yapılan siber saldırılar yönlendirici log dosyalarına göre hangi cihaza saldırı yapıldığı tespit edilir. Yönlendiriciler OSI Referans Modeli 3. Katmanında çalışmaktadır.

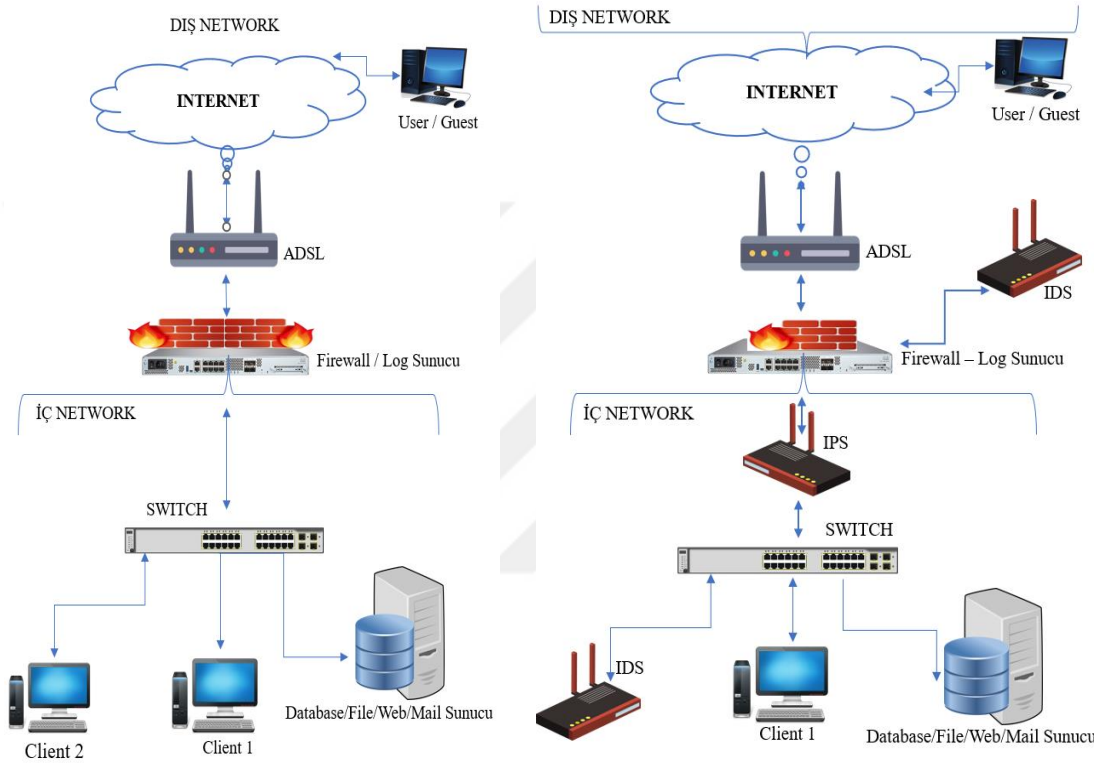
Bilgisayar ağlarında konumlandırılan bu cihazlar sistemler üzerinde iletişimi sağlamaktadır. Bu bağlamda cihazlara yapılan siber saldırılar yönlendirici log dosyaları kapsamında tespit edilir. Bu cihazlar ile iletişime geçen siber saldırganlar yönlendirici loglar sayesinde tespit edilerek engellenmesi sağlanır. Geliştirilen STÖS uygulaması log dosyaları türünde, sistem mimarisi daha kapsamlı oluşturulabilir [8].

Log türleri incelendiğinde OSI katmanları siber saldırılar hakkında önemli bilgiler vermektedir. OSI referans modelinde yer alan katmanlar incelendiğinde ağ yönlendirici cihazları 2. ve 3. katmanda çalışmaktadır. Network yönlendirici cihazlarıyla iletişime gecen kullanıcıların log kayıtları analiz edildiğinde yönlendirici kullanan saldırganlar hakkında veriler elde edilebilmektedir [8].

3.1.2. Saldırı Tespit ve Önleme Sistemi Çalışma Yapısı

Siber saldırıların tespiti için geliştirilen açık kaynak uygulamanın çalışma prensibi genel olarak, sisteme erişim sağlayan kullanıcının gerçek kişi veya kötü niyetli kullanıcı olduğunu birbirinden ayırmak için geliştirilmiştir. Sisteme erişim sağlayan kullanıcılar sistem üzerinde erişim bilgilerini yazarak sisteme giriş sağlarlar. Kullanıcıların network üzerindeki paketleri analiz eden ve bu kullanıcıların şüpheli hareketlerinin tespit

edilmesinde onlara kural uygulayan siber güvenlik sistemi önerilmiştir. Şekil 3.4'de siber güvenlik sistemi çalışma mantığı bulunmaktadır. Genel itibariyle kullanılan siber güvenlik sistemi Şekil 3.1 (a)'da ve önerilen sistem Şekil 3.1 (b)'de yer almaktadır. IDS/IPS sistemleri networklerde farklı konumlandırılabilmektedir. IDS/IPS sistemi network içinde network sisteminin yapısına göre farklı konumlandırılabilir. Bu bağlamda güvenlik duvarı, IPS ve IDS sistemleri kullanılarak bir siber güvenlik sistemi önerilmiştir. Bu öneri kuruluşların networklerini daha etkili korunması sağlanabilir.



Şekil 3.1. Siber güvenlik sistemi, (a) kullanılan sistem (b) önerilen sistem

Dışarıdan gelen kullanıcılar sisteme üzerinde 3 denemeden sonra sisteme erişim sağlayamaz. Bu kullanıcıların IP adresleri geliştirilen açık kaynak uygulama ile bloke edilir. Bloke edilen IP adresleri veri tabanına yazılır. Bloke edilen IP adresleri üzerinden sisteme erişim sağlayan kullanıcıların sisteme erişimi engellenir.

3.1.3. Saldırı Tespit ve Önleme Sistemi Kod Yapısı

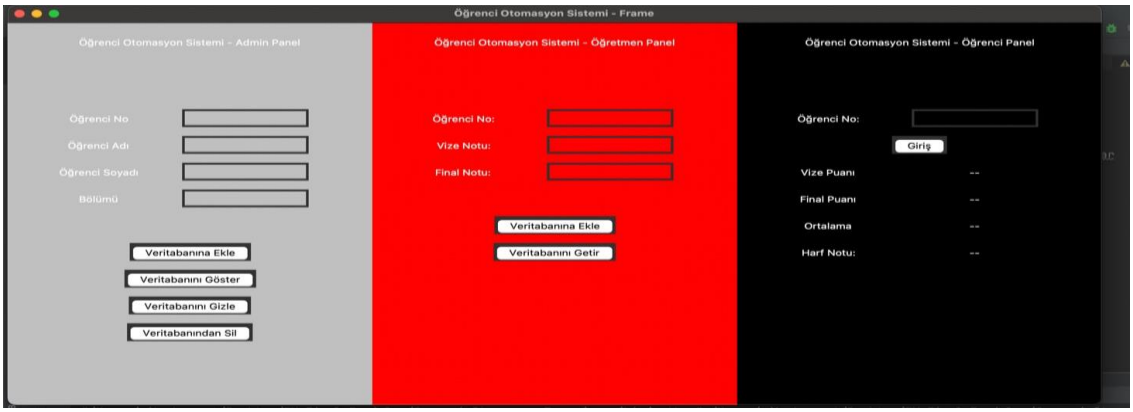
Geliştirilen açık kaynak uygulamanın kodları Şekil 6.2 ve Şekil 6.3 de ekler bölümünde yer almaktadır. Açık kaynak programlama dili Python kullanılmıştır. Uygulamada yazılan kodlar iki farklı .py uzantılı dosya olarak yer almaktadır. Kod editörü olarak PyCharm kullanılmıştır. Python 3.0 versiyonu kullanılmıştır. Gerekli kod, modül,

kütüphaneler kullanılarak yazılmıştır. Sisteme girmeye çalışan cihazlardan alınan log bilgileri veri tabanında saklanmaktadır. Log bilgileri içinde cihazların IP adresi, MAC adresi bilgileri bulunmaktadır. Kodların çalışma yapısına uymayan IP adreslerine ilgili işlemler uygulanmaktadır.

Log kayıtlarının alındığı sistem üzerinde login olmak isteyen kullanıcıların oluşturdukları aksiyonlardan elde edilen veriler log kayıtları olarak veri tabanında tutulmaktadır. Şekil 3.2'de yer alan sisteme giriş sağlayan kullanıcıların login ekranı yer almaktadır. Login giriş ekranı kullanıcı adı ve şifre den oluşmaktadır. Login giriş ekranı üç farklı yetkide giriş yapılmaktadır. Her kullanıcının yetki ve sorumluluk alanı farklıdır. Log kayıtlarını takip eden bu program geliştirilmeye açık, bir uygulamadır. Log kayıtları üzerinden gelen kullanıcıların gerçek kullanıcı veya sahte kullanıcı olduğunu ayırmak için yazılmıştır.

Kullanıcıların sisteme girişi için kullanıcı ID ve şifre ile girişleri mümkündür. Sisteme girişlerde kullanıcı ID ve şifre üç defa denenebilmektedir. Üçüncü denemeden sonra sisteme erişim yapamayan kullanıcıların IP adresleri bloke edilir. Log kayıtları IP adreslerini hemen engellemez. Siber saldırıların erken fark edilmesini sağlamaktadır. Bu sayede siber saldırıların örüntü verilerinin tespit edilmesinde önemli rol üslenmektedir. Buradan alınan örüntü verileri analiz edilerek siber saldırı raporları hazırlanarak, siber saldırılara karşı erken önlem alınması sağlanır.

Sistemlere yapılan siber saldırıların çoğu internet üzerinden, dış network olarak tabir ettiğimiz sistem ağı dışından, yapılmaktadır. Siber saldırılar, sistemlere uzak karmaşık yapıya sahip bilgisayar korsanları tarafından yapılmaktadır. Buna bağlı olarak geliştirilen açık kaynak uygulama web logları üzerinden sahte kullanıcıları tespit edip IP adreslerine bloke koymaktadır. Diğer log dosyalarına göre IP adreslerine göre engelleme ve bloke işlemleri yapılabilir.

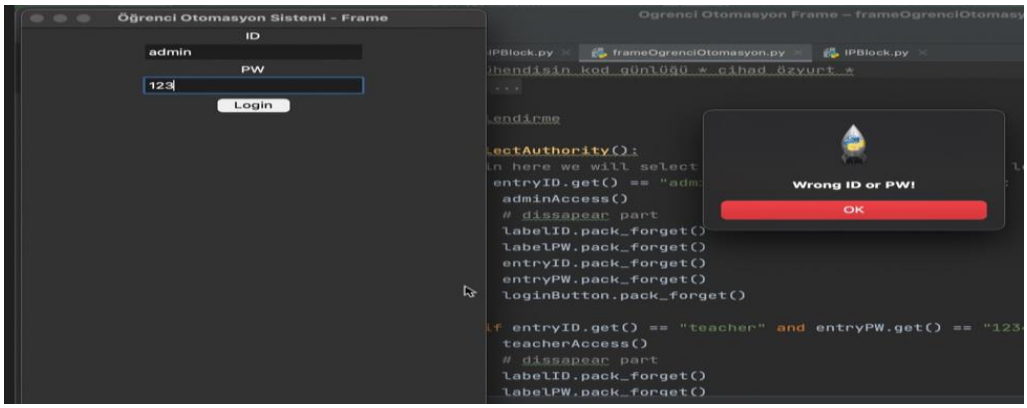


Şekil 3.2. Açık kaynak uygulama login ekranı.

Sisteme başarılı bir şekilde giriş sağlayan kullanıcılar Şekil 3.3'da yer alan ekran görüntüsü karşılamaktadır.

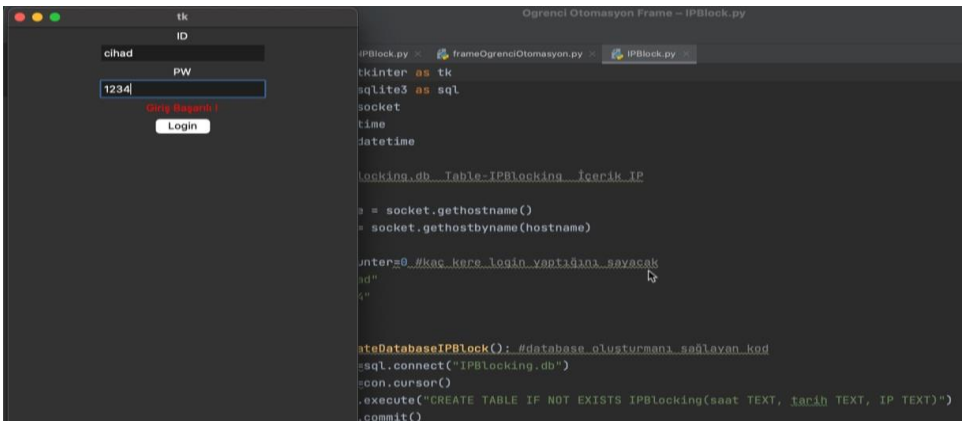
STÖS Çalışma Adımları,

- Sisteme giriş sağlanır.
- Kullanıcı bilgileri en fazla üç defa girilir ve üç denemeden sonra IP bloke edilir.
- İşlemlerin log kayıtları sisteme düşer ve Log kayıtları analiz edilir.
- Sonraki adımlarda analiz edilen log kayıtları siber tehdit durumu değerlendirilir.
- Sonraki adımlarda siber saldırı durumlarını tespit etmek için kullanılır.



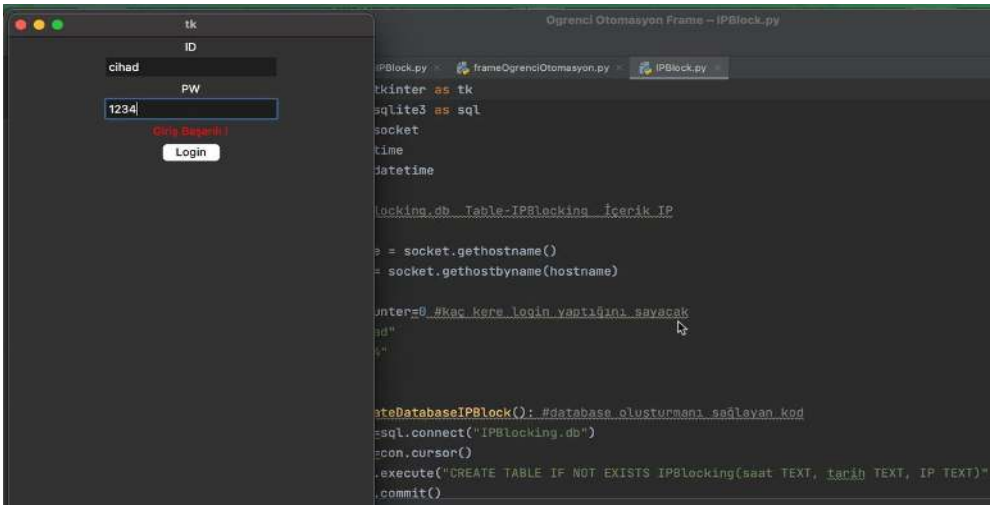
Şekil 3.3. Açık kaynak uygulama login giriş mesajı.

Şekil 3.4, Şekil 3.5'de login giriş ekranları yer almaktadır. Bu şekillerde kullanıcı sisteme girişi ve hatalı şifre bilgisi girerek oluştuğu görseller yer almaktadır. Login ekranı kullanıcıları, sisteme giriş yaptıkları sırada log kayıtları web sunucu log türleri içinde saklanmaktadır.



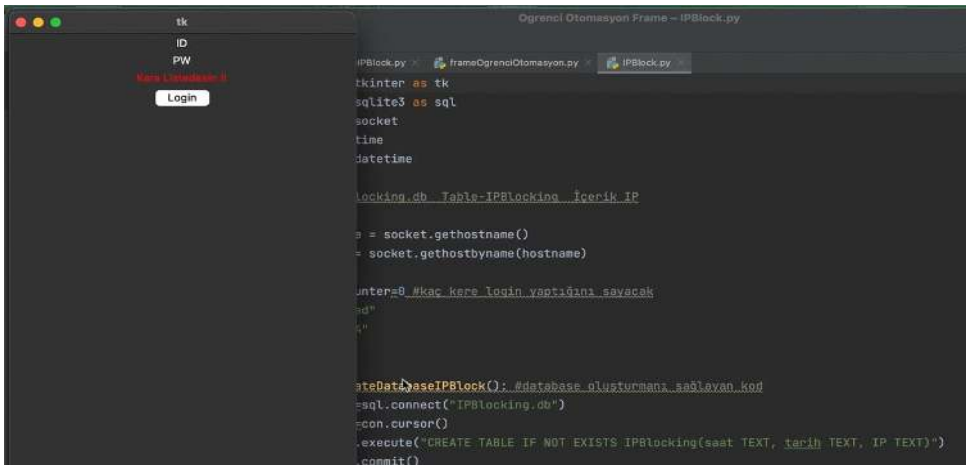
Şekil 3.4. Açık kaynak uygulama login giriş hatası mesajı.

Siber saldırıların belirlenmesinde log kayıtları büyük bir öneme sahiptir. Sistemler üzerinde log kayıtlarının alınması siber uzayda birçok siber tehdidi önleyeceği düşünülmektedir.



Şekil 3.5. Açık kaynak uygulama başarılı login girişi.

Siber saldırıların log kayıtları üzerinden tespit edilebileceği görülmektedir. Loglama cihazları siber güvenlik cihazları değildir. Tez çalışmasının hedefi, tutulan loglar üzerinden gelen kullanıcıların siber tehdit unsuru olup olmadığının belirlenmesidir. Şekil 3.6'da yer alan görselde login giriş ekranında şifre denemeleri başarısız olan kullanıcıların sisteme giriş yapamadıkları mesajı iletilir.



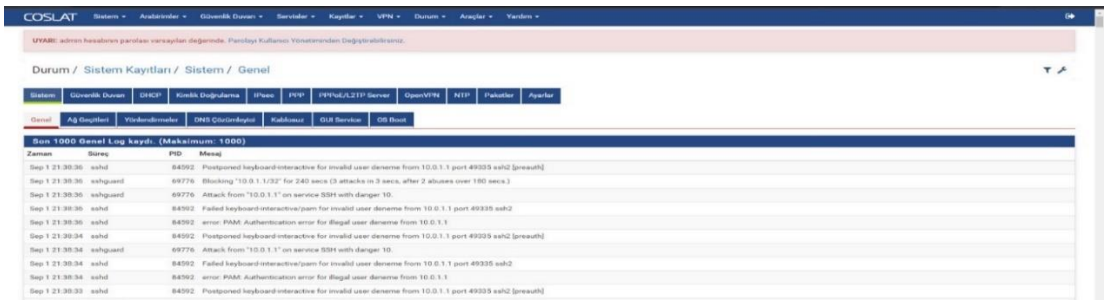
Şekil 3.6. Açık Kaynak ile login denemesi IP'lerin kara listeye alınması.

Log kayıtları için Coslat 6551 loglama cihazı kullanılmıştır. Şekil 3.7'de log tablosu yer almaktadır. STÖS uygulaması, internet üzerinden sistemlere erişim sağlayan

kullanıcıların gerçek kişi mi, siber korsan veya siber saldırı mı yapıldığını tespit edilmesi için geliştirilmiştir. Sistemler üzerinde yetkisiz kullanıcılarının sayısının artması siber saldırıları arttırmıştır.

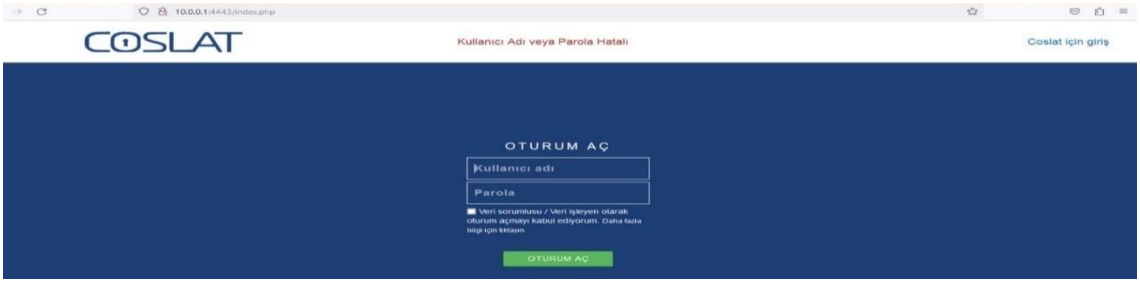
STÖS çalışma yapısı içinde olası kullanıcı ve yetkisiz kullanıcı denemeleri yapılmıştır. İnternet üzerinden erişim sağlanan admin panele kullanıcı bilgileri girilerek STÖS çalışması gözlemlenmiştir. STÖS çalışma yapısı incelendiğinde, sisteme erişim sağlayan kullanıcılar dört ve üzeri deneme sonrasında sisteme erişim sağlayamamışlardır. Bu sayede IP adreslerinden gelen kullanıcıların siber saldırı unsuru olarak tespit edilmesi sağlanır. Şekil 3.7'de log tablosu yer almaktadır. Fakat kısa bir süre sonra bu IP adresi blokesi kaldırılmaktadır. Loglama cihazı burada gelen IP'nin siber saldırımı veya gerçek kullanıcı mı olduğunu ayır edememektedir.

Loglama cihazlarına ve güvenlik duvarı sistemlerine log kayıtlarının incelenmesiyle, STÖS devreye girerek, siber saldırı için gelen IP adreslerini tespit etmesi ve engellemesi sağlanabilir. Tez çalışma kapsamında bu tür çalışmaların olduğu ve bu yapılan çalışmalara yer verilmiştir. Siber saldırılar genelde bir anda yapılmayan uzun vadede yapılan araştırmalar ve bilgi toplamalar sonucu oluşmaktadır. Bu yüzden log analizi uzun vadede birçok saldırıyı tespit edebilme özelliğine sahiptir. Bazı kısa süreli yapılan siber saldırılarında engelleme kabiliyetinin olduğu da görülmektedir.



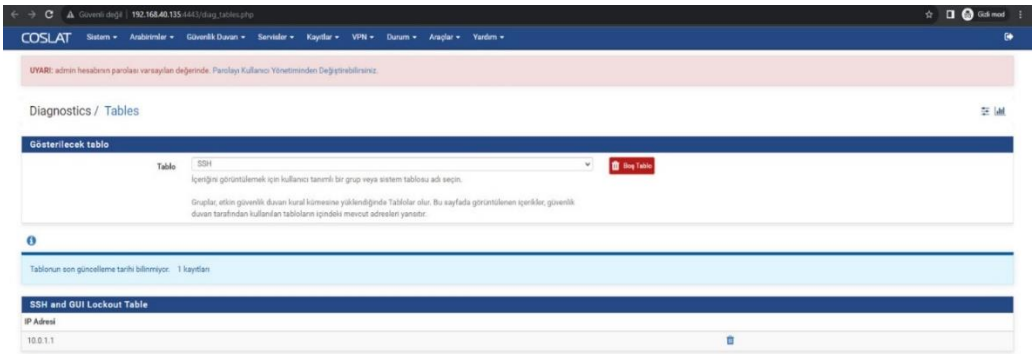
Şekil 3.7. Log tablosu.

Kullanıcılar, üç ve daha az deneme yaparak sisteme erişimleri sağlanmaktadır. Kullanıcılar, sistemlere dört ve üzeri deneme sonrasında IP adresleri bloke edilerek sistemlere erişimi engellenir. STÖS sayesinde olası bir siber saldırı tespit edilmesiyle kullanıcıların sisteme erişimi engellenir. Şekil 3.8'da Coslat admin paneli yer almaktadır.



Şekil 3.8. Coslat 5651 Admin paneli.

Log analiz yöntemleriyle saldırı yaptığı tespit edilen IP adresi, saldırı önleme sistemi sayesinde kural girilerek engellenmesi sağlanır. Saldırı tespit sistemi ile saldırı yapan IP adresi tespit edilir. Tespit edilen IP adresine kota koyma, engelleme getirme gibi kurallar saldırı önleme sistemi tarafından yapılır. Loglama cihazı, login olan kullanıcının IP adresini SSH tablosuna Şekil 3.9'de ki gibi yazmaktadır.



Şekil 3.9. SSH IP tablosu.

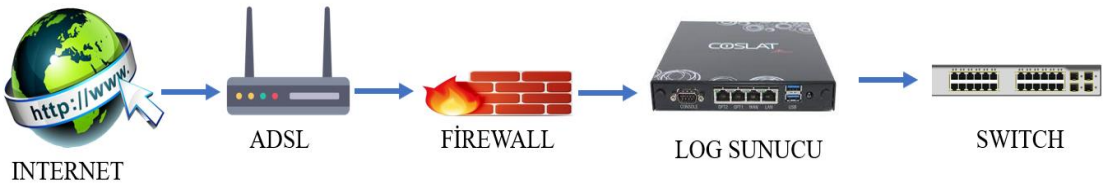
3.2. SİBER GÜVENLİK SİSTEMİ ÖNERİLERİ

3.2.1. Log Sistemleriyle IDS/IPS ve Güvenlik Duvarı Entegrasyon Önerisi

Siber Güvenlik Sistemi önerisi tüm güvenlik sistemlerini kapsamaktadır. Bu bağlamda network sistemleri daha güvenli hale gelecektir. Bir önceki çalışmada IDS/IPS Güvenlik Sistemi önerisi yer almaktadır. Bu çalışmada ise IDS/IPS ile kullanılan log teknolojilerine ek olarak güvenlik duvarı eklenmiştir. Bu güvenlik sistemine güvenlik duvarı entegrasyonunun yapılması önerisi yapılmıştır. Önerilen sistemin açık kaynak platform olması gelişime açık olması entegrasyonu kolaylaştırmaktadır. Ayrıca kullanılan loglama teknolojileri neredeyse tüm güvenlik duvarı sistemleriyle entegreli çalışmaktadır. Bu

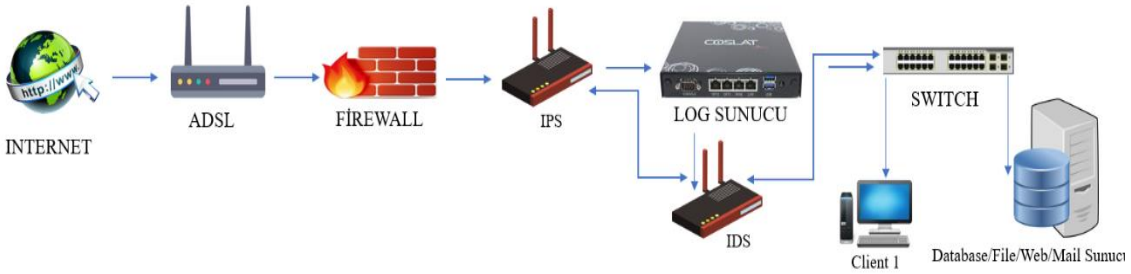
çalışmada diğer çalışmalardan farklı tüm güvenlik teknolojilerini tek çatıda toplamasıdır. Yapılan çalışmada güvenlik duvarı çalışma uygulaması sonuçları yer almamaktadır. Bunun nedeni güvenlik duvarı yazılımlarının kapalı sistem olması aynı zamanda tehdit oluşturan unsurlara direk kural uygulaması, açık kaynak desteğinin olmaması gibi temel ve önemli sorunlar nedeniyle uygulama yapma şansı olmamıştır.

Şekil 3.10'de genel olarak network üzerinde firewall ve loglama cihazlarının konumlandırılması yer almaktadır. Şekil 3.10'de yer alan konumlandırma yaygın olarak kullanılan cihaz dağılımını göstermektedir.



Şekil 3.10 Network üzerinde firewall ve log sunucu konumlandırılması.

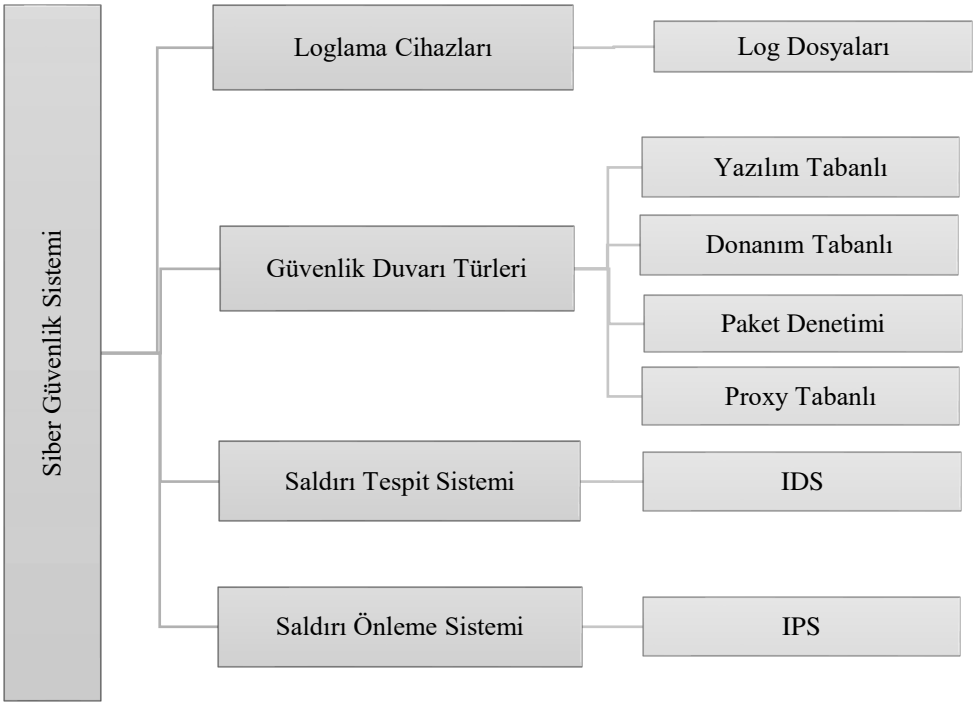
Network cihazları, loglama teknolojileri, firewall ve IDS/IPS sistemleri network üzerinde konumlandırılması bilgisayar ağlarına göre farklılık gösterebilir. Şekil 3.12'de network üzerinde firewall, loglama teknolojileri ve IDS/IPS sistemleri network üzerinde konumlandırılması yer almaktadır. Şekil 3.11'de yer alan konumlandırma bir öneri olarak sunulmuştur. Yaygın olarak kullanılan network cihazlarının konumlandırmasına ek olarak log sunucu öncesinde ve sonrasında IDS/IPS kullanımı önerilmektedir. Log çözümlerinin kullanıldığı network ortamında en verimli sonuçların alınması için IDS/IPS sistemlerinin doğru konumlandırılması gerekmektedir.



Şekil 3.11 Network üzerinde firewall, log sunucu ve IDS/IPS konumlandırılması.

İlk yapılan uygulamanın aksine açık kaynak kod yardımıyla IDS/IPS sistemi ile tehdit unsurları tespit edilmiş ve engellenmiştir. Ayrıca en çok kullanılan siber saldırı türleri

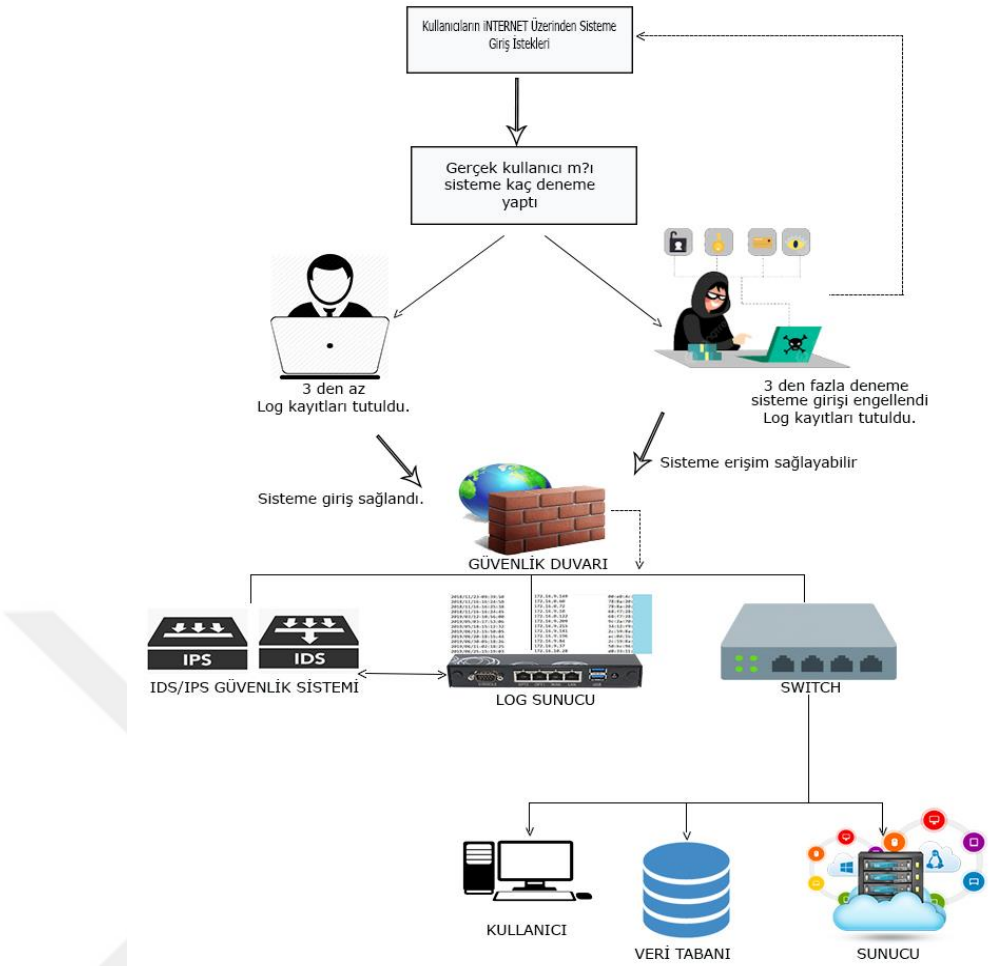
admin panel ekranında açık kaynak kod kullanılarak tespit edilmiş aynı şekilde engellenmiştir. İnternet üzerinde önerilen siber güvenlik sistemi çalışma yapısı Şekil 3.12'de yer almaktadır. Şekil 3.12'de yer alan şema incelendiğinde log teknolojisi, güvenlik duvarı teknolojisi ve ek olarak IDS/IPS güvenlik sistemleri bir bütün olarak verilmiştir. Önerilen bu sistem kullanılması düşünülen network sistemlere kolay entegrasyonu sayesinde siber uzayda, networkleri daha güvenli hale getirmektedir.



Şekil 3.12. Siber güvenlik sistemi ve alt sistemleri şeması.

Network sistemlerine erişim sağlayan kullanıcılar güvenlik duvarını aşmaları halinde loglama teknolojileri sayesinde IDS/IPS sistemiyle fark edilmeleri sağlanır. Bu anlamda güvenlik duvarı aşsalar bile log teknolojileri sayesinde IPS/IPS sistemine takılarak verilere erişimi söz konusu olmamaktadır. Güvenlik duvarı gerçek zamanlı çalışmadığı durumlar oluşabilmektedir. Bu anlamda kullanılan IPS güvenlik sistemi gerçek zamanlı çalışması sayesinde saldırı tehditleri bertaraf edilmesi sağlanır.

Geliştirilen açık kaynak uygulamanın çalışma şeması şekil 3.13'de yer almaktadır. Yapılan uygulama siber saldırıların tespiti için kullanılmaktadır. Tespit edilen siber saldırılar, sistemler üzerinde oluşan, oluşabilecek ve sonraki zaman dilimlerinde gerçekleşebilecek siber saldırılara karşı önlem alınmasını sağlayacaktır.

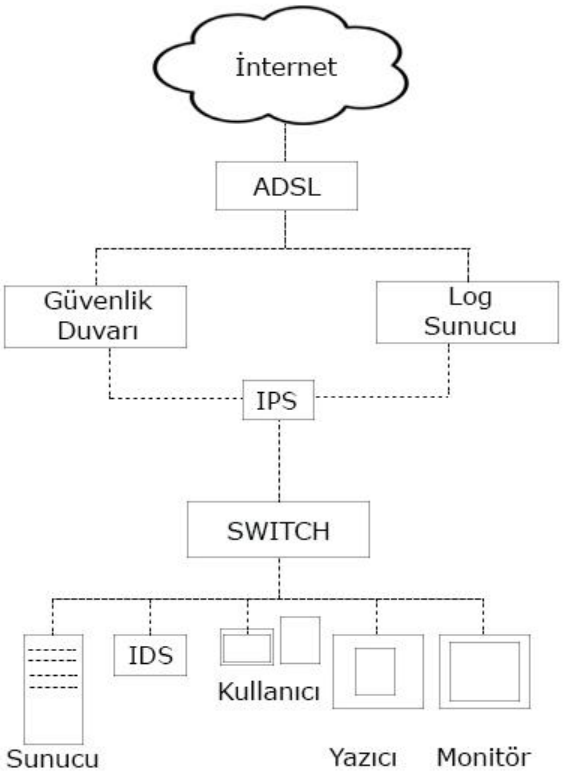


Şekil 3.13. IDS/IDS, güvenlik duvarı ve loglama sistemi çalışma şeması.

İnternet ortamından gelen misafirlerin güvenlik sistemi üzerindeki ilerleyişi adeta bir süzgeç gibi hareket etmesi sağlanır. Bu anlamda saldırganların basamaklar halinde ayrışması yapılır. Böylece zararlı yazılım ve saldırganlar siber güvenlik alt sistemleri üzerinde takılı kalmaları sağlanır. Siber güvenlik sistemi dışarıdan gelen davetsiz misafirleri bir huni misali süzerek elemesi sağlanır. IDS saldırı tespiti yapmakta, IPS ise saldırganı engellemekte yükümlüdür.

Şekil 3.14'de yer alan şema incelendiğinde siber güvenlik sistemi çalışma diyagramı yer almaktadır. Siber güvenlik sistemi çalışma diyagramı incelendiğinde loglama cihazı ve IDS/IPS siber güvenlik sistemi güvenlik duvarının arkasında konumlandırılır.

Misafir kullanıcıların güvenlik duvarını geçmeleri halinde tehdit unsurları IDS/IPS sistemi sayesinde bertaraf edilmektedir. Güvenlik duvarı gerçek zamanlı çalışmayabilmektedir. IIPS güvenlik sistemi gerçek zamanlı çalıştığı için saldırı tehdidi ve unsuru olan kullanıcıları engellemektedir.

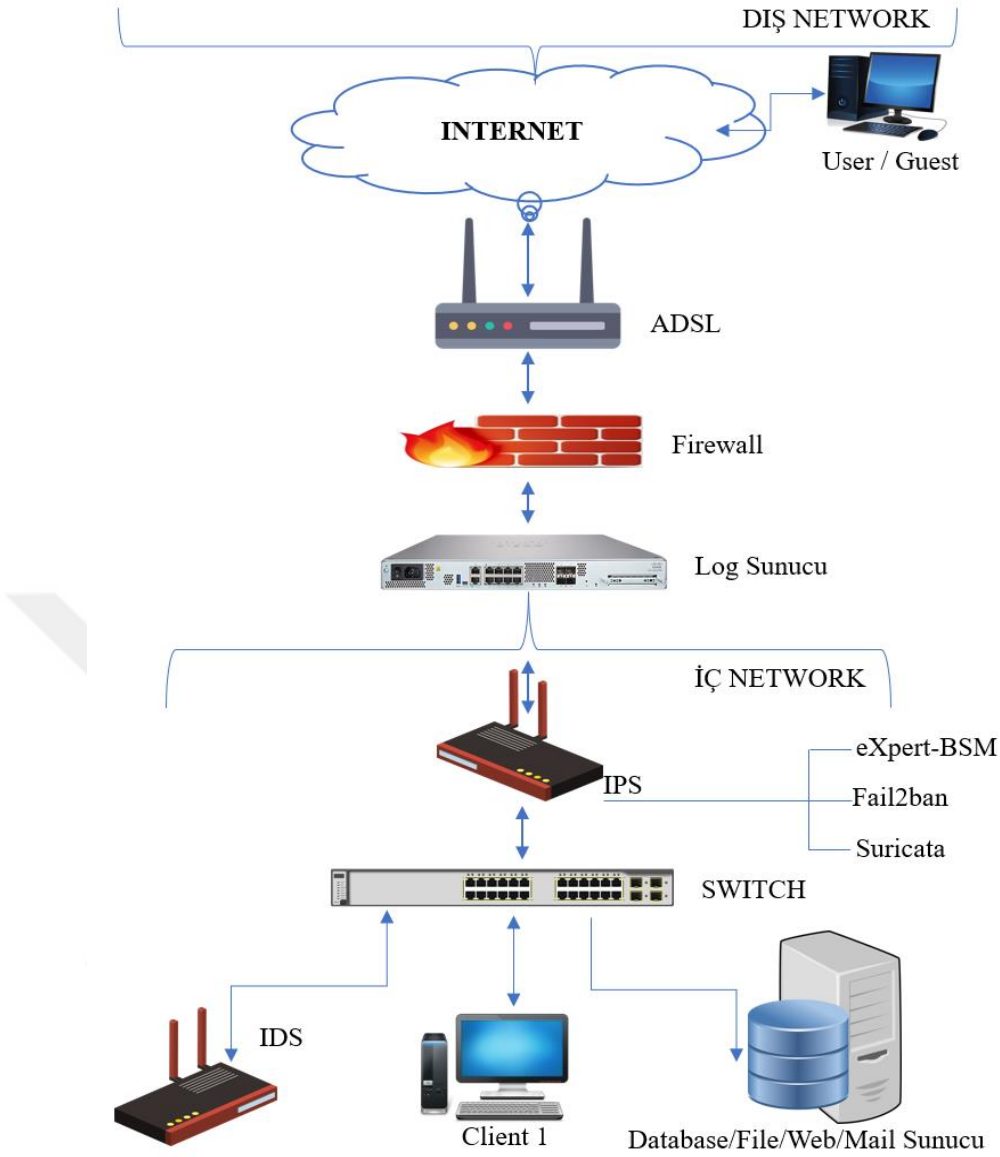


Şekil 3.14. Siber güvenlik sistemi diyagram şeması.

3.2.2. Loglama Sistemleri için IPS Paket önerisi

Bir önceki çalışmada IDS/IPS Güvenlik Sistemi önerisi yer almaktadır. Bu çalışmada ise IDS/IPS ile kullanılan log teknolojilerine ek olarak en uygun IPS paketleri kullanılmıştır. Bu çözüm önerisi loglama teknolojisi kullanan network sistemlerine öneri olarak sunulmuştur.

Önerilen bu mimari yapıda log analizlerine en uygun IPS paketleri kullanılmıştır. Daha önce yer alan konu başlıklarında IPS paketleri incelenmiş ve araştırılmış, log çözümlerine uygun IPS paketleri sunulmuştur. Şekil 3.15 incelendiğinde siber güvenlik sistemlerinde kullanılmak üzere log çözümleri için IPS önerisi yer almaktadır. Bu öneride log kayıtları incelenerek tespit edilen saldırı en uygun IPS paketleri kullanılarak engellenmesi sağlanır. Bu durum internet ortamından gelen saldırıların hızlı tespit edilmesi ve mimariye uygun paketlerin kullanılmasını sağlayacaktır.



Şekil 3.15. Log çözümleri için IPS önerisi.

Loglama teknolojileri ile uyum içinde çalışan IPS paketleri Çizelge 3.1'de yer almaktadır. Log kayıtları ile siber saldırıların önlenmesi için en uygun IPS paketlerinin kullanılması önerilmiştir. Bu sayede loglama sistemlerine uygun IPS paketleri kullanarak siber saldırıların daha hızlı önlenmesi sağlanabilir.

Loglama sistemlerinin yer aldığı network ortamlarında kullanılan eXpert-BSM, Fail2ban ve Suricata açık kaynak IPS paketlerinin daha fazla yaygınlaşması ve kullanılması siber güvenlik açısından daha iyi olacağı düşünülmektedir. Önerilen bu sistem sayesinde internet ortamında yer alan bilgisayar ve sunucu sistemlerinin daha kapsamlı korunmasını sağlar.

Çizelge 3.1. Log uyumluluğu olan IPS paketleri

SN	IPS Paketleri	Kural Ekleme Özelliği	Log Desteği
1	eXpert-BSM	Var	Var
2	Fail2ban	Var	Var
3	Suricata	Var	Var

Loglama çözümleri için en uygun IDS/IPS sistemleri Şekil 3.16'de yer almaktadır. Network yapılarına uygun IDS/IPS sistemlerinin kullanılması daha verimli sonuçlar oluşturacağı düşünülmektedir.

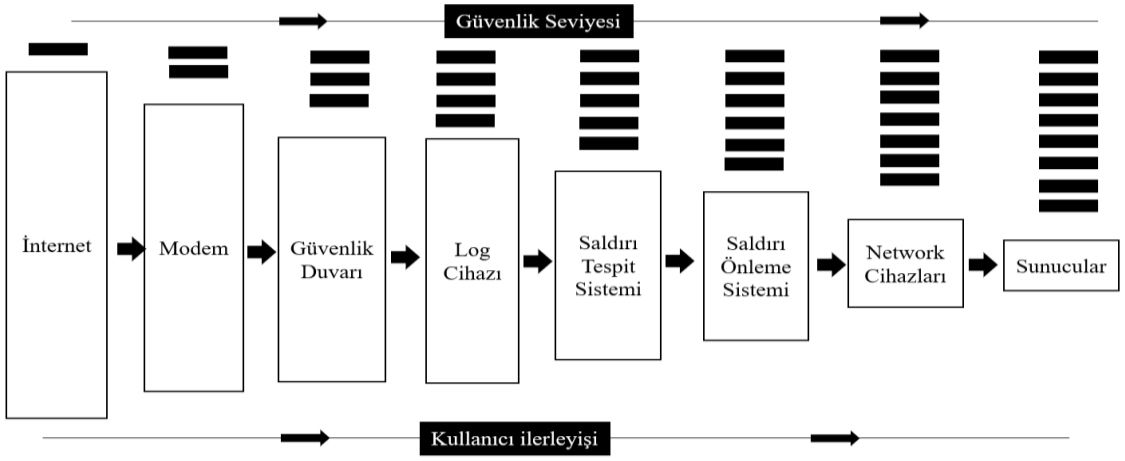
Şekil 3.16. Log çözümleri için en uygun IDS/IPS türleri

3.2.3. Misafirlerin Siber Güvenlik Sistemi Üzerindeki Hareketi

Siber güvenlik sistemi dışarıdan gelen davetsiz misafirleri bir huni misali süzerek elemesi sağlanır. Siber güvenlik sistemi üzerinde kullanıcılar kendi sistem bilgilerine ulaşana kadar şekil 3.18'de yer alan sistemlerden geçmektedir.

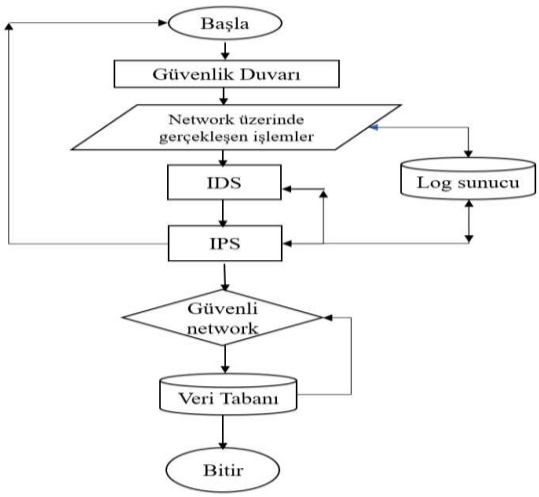
Siber güvenlik sistemi şeması incelendiğinde, her sistemin log kayıtları ayrı tutulmaktadır. Bu durum sistemin daha güvenli olmasını sağlamaktadır. Sistem üzerinde gerçekleşen anormal bir olay log kayıtları üzerinden tespit edilmesi sağlanır. Sonraki süreçte bu kullanıcıya siber güvenlik kuralları uygulanır.

Açık kaynak desteği olan güvenlik duvarı kullanılması daha iyi sonuçlar verebilir. Saldırı tespit sistemi ve saldırı önleme sistemi açık kaynak olduğu için güvenlik duvarı ile daha entegrasyon içinde çalışacağı düşünülmektedir. Bunlar, IP bloke, parola iptali, kullanıcıyı askıya alma gibi kurallardan oluşabilir. Dışarıdan gelen davetsiz misafirlerin siber güvenlik sistemi üzerindeki ilerleyişi şekil 3.17'de yer verilmiştir.



Şekil 3.17. Kullanıcıların siber güvenlik sistemi üzerinde ilerleyiş şeması.

Sistem mimarisi, IP adresi, MAC adresi, 802.1x Kimlik Denetim Protokolü, HTTP, URL bilgilerine göre değişiklik gösterebilir. Kablosuz ağlarda kullanılan protokolü incelediğimizde, 802.1x Kimlik Denetim Protokolü sistem üzerinden gelen kullanıcıların network sistemine erişimi olmadan kimlik denetimine tabi olmasıdır. Şekil 3.18'de saldırı tespit ve önleme sistemi hakkında şema önerileri bulunmaktadır.



Şekil 3.18. Kullanıcıların siber güvenlik sistemi üzerinde ilerleyiş şeması

4. SONUÇ

İnternet teknolojilerin hızlı gelişimi, kullanıcı sayısını ve kullanılan cihaz sayısını hızlı bir şekilde arttırmıştır. Bu durum internet üzerinden yapılan işlemlerin yönetimini, denetimini ve kontrolünü zorlaştırmıştır. Buna bağlı olarak sistemlere yapılan siber saldırılarda sistemlerin daha karmaşık bir hale sürüklemektedir. Loglama teknolojileri çeşitli yöntemler kullanarak sistemler üzerinde işlem yapan kullanıcıları daha düzenli, belirli kurallar ve güvenlik önlemleri alarak sistemlerin kontrolunu rahatlatmıştır. Siber güvenlik, çok disiplinli bir yapıya sahip çalışma alanıdır. Tez çalışmasında yukarıda bahsedilen tüm konulardan içerikler ulusal ve uluslararası makaleler ile desteklenmiştir. Bu bağlamda açık kaynak kod ile siber güvenlik sistemleri birbirine entegre edilerek bir öneri sunulmuş, log kayıtlarına göre siber saldırıların tespit edilmesi ve siber saldırı önleme sistemlerinin geliştirilmesi, STÖS uygulamaları yer almaktadır.

Tez çalışmasında sistemlere yapılan siber saldırılar incelenmiştir. Bu anlamda en popüler siber saldırılar DDoS, kimlik avı, parola denemeleri, yazılım sahteciliği ve oltalama saldırıları olarak tespit edilmiştir. Microsoft siber saldırı raporlarında 2016, 2017, 2021, 2022 ve 2023 yılları içinde yapılan saldırılar incelenmiştir. Ayrıca buna ek olarak OWASP siber saldırı raporları da incelenmiştir. Gerçekleştirilen bu siber saldırılar, hangi cihazlara daha çok siber saldırı yapıldığı, port numarası, protokol, katman, IP adresi, veri tabanı bilgileri araştırılmıştır. Bu verilere göre siber saldırının türü araştırılmış, saldırı yapılan siber saldırı türüne göre ve saldırı yapılan cihazın, port, katman, protokol bilgilerine göre loglama çözüm önerileri sunulmuştur. Bilgisayar ağları üzerinde farklı homojen ve heterojen yapıya sahip yazılım ve donanımsal sistemler bulunmaktadır.

Sistemlere yapılan siber saldırılar, log dosyaları türlerine göre tespit edilmesi mümkündür. Bu sebeple log dosyaları farklı katman ve protokollerde çalışmaktadır. Log kayıtları üzerinden siber saldırıların tespit edilmesi, katman ve protokol bilgilerinden belirlenmektedir. Log dosyaları, yazılım araçlarına ve donanım cihazlarına göre farklılık göstermektedir. Hangi cihaza kim tarafından erişim sağlandığı log bilgilerinden tespit edilmiştir. Sonuç olarak log verileri siber saldırıların tespitini kolaylaşmaktadır. Log kayıtları adli analizler içinde de çok yaygın olarak kullanılmaktadır. Loglamanın siber saldırıların tespiti için de ne kadar önemli olduğu burada ortaya çıkmaktadır.

Günümüz teknolojileri kullanılarak yazılımsal ve donanımsal olarak siber saldırı önleme araçları çalışmaları yapılmaktadır. Bu saldırıların tespiti ve önlenmesi için uluslararası çalışmalar yapılmaktadır. Siber saldırılar ülkeler boyutunda incelendiğinde siber saldırın önlenmesi için yüksek oranda bütçelerin ayrıldığı görülmektedir. Bu anlamda dijital verilerin toplanması, kaydedilmesi, saklanması, analiz edilmesi oldukça önemlidir. Veri bütünlüğünün sağlanması için siber uzayda güvenlik düzeyinin en üst seviyede olması gerekmektedir. Bu sebeple siber güvenlik araçlarının geliştirilmesi, siber güvenlik personellerinin yetiştirilmesi konusunda daha hassas adımların atılması gerektiği görülmektedir.

Açık kaynak sistemler siber saldırıların tespit edilmesinde ve önlenmesinde daha aktif rol oynadıkları ortaya çıkmaktadır. Bu sistemler için cihaz gereksinimi olarak aynı şekilde açık kaynak desteği olan donanımsal cihazların tercih edildiği uygulamalarda yer almaktadır. Açık kaynak destekli yazılım ve donanım birimlerinin tercih edilmesi, saldırı tespitini ve önlemesini hızlandırmıştır. Ayrıca açık kaynak desteği olan yazılım ve donanım birimlerine açık kaynak desteği olan IDS/IPS siber saldırı tespit ve önleme sistemlerinde kullanılması güvenlik duvarı üreticilerinin ilgisini çekmektedir. Açık kaynak yazılım ve donanım sistemleriyle birlikte IPS/IDS sistemlerinin kullanılması siber saldırıların tespit edildiği ve önlenmesi açısından verimli sonuçların verdiği gözlemlenmiştir.

Ayrıca önerilen SSTS sadece yazılım araçlarının olduğu da görülmektedir. ACARM-ng, Bro-IDS Bro, eXpert-BSM, Fail2ban, OSSEC, Prelude OSS, Sagan, Samhain, Snort, Suricata yazılım araçlarının SSTS entegre kullanılabildiği ve kullanıldığı görülmektedir. Bu yazılım araçlarının eXpert-BSM, Fail2ban ve Suricata log kayıtları üzerinden siber saldırıları tespit ettiği sonucu ortaya çıkmıştır. Bu tür araçların geliştirilmesi, geliştirilmiş bu tür yazılım araçlarının log kayıtları üzerinden STÖS üzerinde kullanılmasının araştırılması daha yaygın hale getirilmesi gerektiği görülmektedir. Aynı zamanda bu yazılım araçlarının IPS/IDS sistemleriyle entegreli çalışabilmesi en önemli özellikleri arasında yer almaktadır. Çalışmada saldırı tespit ve saldırı önleme sistemlerinde TCP/IP, MAC, HTTPS, ARP tablosu, protokol, port ve katman bilgilerinin yer almaktadır. Özellikle network cihazlarında kullanılan, network trafik akışının gerçekleştiği katman, port ve protokoller üzerinden siber saldırıların tespit edildiği ve engellendiği sonuçları ortaya çıkmıştır.

5. KAYNAKLAR

[1] Y. Kahriman, "Türkiye'de Siber Güvenlik Alanında Yapılan Tezlerin İncelenmesi, Bibliyografik Bir Çalışma", Yüksek Lisans Tezi, Eğitim Bilimleri Enstitüsü, Necmettin Erbakan Üniversitesi, Konya, 2022.

[2] O. Taş, "Nesnelerin İnterneti İçin Akıllı Saldırı Tespit Sistemleri Geliştirilmesi". Doktora Tezi, Lisansüstü Eğitim Enstitüsü, İstanbul Sabahattin Zaim Üniversitesi, İstanbul, 2022.

[3] E. Gül, "Log Yönetimi ile Siber Güvenlik Araçlarının Geliştirilmesi", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, 2019

[4] G., Canbek, & Ş. Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, 9(3), 165-174, 2020.

[5] M. D. Koyuncu, & Ü, Nafiz, "Yapay Zekâ Tekniklerinin Saldırı Tespit Sistemleri'nde Kullanımı", *Beykoz Akademi Dergisi*, *10*(1), 78-87, 2022.

[6] Ş. Sağıroğlu & M. Alkan, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, 1. Baskı, Ankara, Türkiye, Grafik-Ofset Matbaacılık, 2018.

[7] M.Z. Gündüz, & D. Resul, "Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi", *Dicle Üniversitesi MF Mühendislik Dergisi,* 13(3), 429-438, 2022.

[8] M. Baykara, "Web Sunucu Erişim Kütüklerinden Web Ataklarının Tespitine Yönelik Web Tabanlı Log Analiz Platformu", *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 28(2), 291-302, 2016.

[9] A. Kamal, "Log Necropsy: A Web-Based Log Analysis Tool", *IEEE 10th Conference on Systems, Process and Control* (*ICSPC*), 176-179, 2022.

[10] P. Malec, M. Piwowar, A. Kozakiewicz, & K. Lasota, "Detecting Security Violations Based on Multilayered Event Log Processing", *Journal of Telecommunications and Information Technology*, (4), 30-36, 2015.

[11] T. Özseven, & M. Düğenci, "Log Analiz: Erişim Kayıt Dosyaları Analiz Yazılımı

ve GOP Üniversitesi Uygulaması", *Bilişim Teknolojileri Dergisi*, *4*(2), 2011.

[12] JS, Wu, YJ, Lee, TE, Wei, CH, Hsieh, & CM, Lai, "ChainSpot: *Mining Service Logs for Cybersecurity Threat Detection", In 2016 at IEEE* Trustcom/BigDataSE/ISPA, 1867-1874, 2016.

[13] C. Yang, T., Y. W. Chan, J. C. Liu, E. Kristiani, & C. H. Lai, "Cyberattacks Detection and Analysis in a Network Log System Using XGBoost with ELK stack", *Soft Computing*, 26(11), 5143-5157, 2022.

[14] K. Shah, C. Parekh, & B. Gohil, "Private Cloud Security With Log Analysis and Encrypted Channel", *International Journal of Advanced Research in Computer Science*, 8 (5), 2017.

[15] C. K. Chan, & A. W. T. Yeoh, "Development of a Platform to Explore Network Intrusion Detection System (NIDS) for Cybersecurity", *Journal of Computer and Communications*, 6(1), 1-11, 2017.

[16] A. Benzekri, R. Laborde, A. Oglaza, D. Rammal, & F. Barrère, "Dynamic Security Management Driven by Situations: An Exploratory Analysis of Logs for the İdentification of Security Situations"*, In 2019 3rd Cyber Security in Networking Conference* (*CSNet*), 2019, ss. 66-72.

[17] E. Bayraktaroğlu, "Bilgi Sistemlerinde Log Yönetimi ve Logların Değerlendirilmesi", Yüksek Lisans Tezi Fen Bilimleri Enstitüsü, Bahçeşehir Üniversitesi, İstanbul, 2019.

[18] E. T. Kılıç, "Siber Saldırıları İzleme Yöntemleri ve Zararlı Yazılım Analizi", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, 2015.

[19] C. Hatipoğlu, & T. Tunacan, "Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması", *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, 8(1), 430-445, 2021.

[20] U. Göktürk, "Türkiye'nin Siber Güvenlik Politikalarının Yazılım Mühendisliği Açısından Değerlendirilmesi ve Kritik Altyapıların Siber Saldırılardan Korunmasına Yönelik Olay Yönetim Sistemi Tasarımı", Yüksek Lisans Tezi, Cerrahpaşa Enstitüsü, İstanbul Üniversitesi, İstanbul, 2021.

[21] M. Landauer, F. Skopik, M. Wurzenberger, W. Hotwagner, & A. Rauber, "A framework for cyber threat intelligence extraction from raw log data", In *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 3200-3209.

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

[23] J. Ma, X. Shangguan, & Y. Zhang, "IoT Security Review: A Case Study of IIoT, IoV, and Smart Home", *Wireless Communications and Mobile Computing*, 2022.

[24] U. K. Raut, "Log Based Intrusion Detection System", *IOSR Journal Of Computer Engineering*, *20*(5), 15-22, 2018.

[25] M. S. Mirpuryan, T. Tavizi, & H. Gharaee, "A Comprehensive Network Intrusion Detection and Prevention System Architecture", *In 6th International Symposium on Telecommunications* İstanbul, Türkiye, 2012, ss. 954-958.

[26] F. Topaloğlu, "Saldırı Tespit Sistemlerinde K-Means Algoritması ve Silhouette Metriği ile Optimum Küme Sayısının Belirlenmesi", *Bilişim Teknolojileri Dergisi,* 17(2), 71-79, 2024.

[27] N. Garakhanova, "Siber diplomasi çalışmaları üzerine bibliyometrik analiz", *Rumeli Dil ve Edebiyat Araştırmaları Dergisi,* 13(1), 2023.

[28] S. Can, (2023, 15 Haziran), *Log Analizi*, [Online]. Erişim: https://webdosya.csb.gov.tr/db/cbs/icerikler/samet-can-uzmanlik-tez--20180925134619.pdf

[29] K. Kent & M. Souppaya, "Guide To Computer Security Log Management Recommendations Of *The National İnstitute Of Standards And Technology*" NIST, 2006.

[30] Coslat Firewall, (2023, 10 Haziran), *logların yasal zorunluluğu*, [Online] Erişim: https://bg-tek.net/coslat-firewall.

[31] Bilgi Güvenliği Akademisi, (2023, 10 Haziran), log analizi, [Online]. Erişim: https://www.bgasecurity.com/makale/windows-sistemlerde-sysmon-ile-log-analizi/

[32] Myservername, (2023, 10 Haziran), *Log Analizi,* [Online]. Erişim: https://tr.myservername.com/top-8-best-log-management-software-log-analysis-tool-review-2021.

[33] A. Ali, M. Ahmed, & A. Khan, "Audit Logs Management and Security-A

Survey", *Kuwait Journal of Science*, 48(3), 2021.

[34] Coslat, (2023, 10 Haziran), *log cihazları özellikleri,* [Online]. Erişim: https://coslat.com/5651-hotspot-cozumleri

[35] C. Kent, M. Tanner, & S. Kabanda, "How South African Smes Address Cyber Security: The Case Of Web Server Logs And İntrusion Detection*". In 2016 IEEE International Conference On Emerging Technologies And Innovative Business Practices For The Transformation Of Societies* (*Emergitech*), 2016, ss. 100-105.

[36] R. G. Abbott, J. McClain, B. Anderson, K. Nauer, A. Silva, & C. Forsythe, "Log analysis of cyber security training exercises", *Procedia Manufacturing*, 3, 5088-5094, 2015.

[37] F. Ö. Çatak, "Topluluk Yöntemlerine Dayalı Dağıtık Hizmet Dışı Bırakma Saldırılarının Algılanması", *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi,* 22(1), 283-289, 2018.

[38] Ö. Ş. Fidancı, "Kurumlar İçin Bilgi Güvenliği Yönetim Sisteminin Oluşturulması", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, KTO Karatay Üniversitesi, Konya, 2022.

[39] R. Von Solms, & J. Van Niekerk, "From Information Security to Cyber security", *Computers end Security*, 38, 97-102, 2013.

[40] OWASP, (2023, 10 Ekim), *OWASP Güvenlik Raporu,* [Online]. Erişim: https://owasp.org/www-project-top-ten/

[41] R. Daş, D. Demirol, & G. A. Tuna, "Novel Tool for Mining Access Patterns Efficiently from Web User Access Logs", *In The International Conference on Engineering and Natural Sciences* (*ICENS*), 2836-2843, 2016.

[42] M. Kara, "Siber Saldırılar Siber Savaşlar", Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, İstanbul Bilgi Üniversitesi, İstanbul, 2013.

[43] R. Çankuş, "Veriyükü Üzerinden SQL Enjeksiyon Zafiyetlerin Belirlenmesi", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Düzce Üniversitesi, Düzce, 2022.

[44] A. Ünal, "Hizmet Reddi Saldırılarının Derin Öğrenme ile Tespiti", Yüksek Lisans Tezi, FBE, Necmettin Erbakan Üniversitesi, Konya, 2018.

[45] E. Bayraktaroğlu, "Bilgi Sistemlerinde Log Yönetimi ve Logların Değerlendirilmesi", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bahçeşehir Üniversitesi, İstanbul, 2019.

[46] Beyaz Bilgisayar, (2023, 10 Eylül, 2023), *log analiz adımları,* [Online]. Erişim: https://www.beyaz.net/tr/guvenlik/makaleler/tehdit_izleme_platformlarinda_kritik_log_kaynaklari.html

[47] G. Akın & S. Ketenci, "Kampüs Ağlarında Aranan Kullanıcıların Tespiti", *XI. Akademik Bilişim Konferansı, Harran Üniversitesi*. Şanlıurfa, Türkiye, 2009.

[48] Bilgem, (2023, 10 Eylül), *zaman damgası,* [Online]. Erişim: https://kamusm.bilgem.tubitak.gov.tr/urunler/zaman_damgasi/

[49] Ö. Sağlık, "Elektronik belge yönetimi uygulamalarındaki koşullar ışığında e-imzalı belgelerin delil değerinin arşivsel güvenilirlik açısından incelenmesi", Doktora Tezi, Sosyal Bilimler Enstitüsü, İstanbul Üniversitesi, İstanbul, 2021.

[50] Y. Başlar, "Elektronik Delilin Toplanması ve Muhafazası", *Hacettepe Hukuk Fakültesi Dergisi,* 10(1), 77-107, 2020.

[51] Microsoft, (2023, 5 Ekim), *Microsoft siber güvenlik raporu*, [Online]. Erişim: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2021#areaheading-oc4f81

[52] S. Tek, "Türkiye ve Dünyada Gerçekleştirilen Siber Saldırı Yöntemlerinin ve Bu Saldırılara Karşı Alınan Önlemlerin İncelenmesi", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Trakya Üniversitesi, Edirne, 2022.

[53] D. Kim, Y. H. Kim, D. Shin, & D. Shin, "Fast Attack Detection System Using Log Analysis and Attack Tree Generation", *Cluster Computing*, 22, 1827-1835, 2019.

[54] N. Sandilaç, "Siber Suç, Siber Terör ve Siber Savaş Üçgeninde Siber Dünya", *Bilişim Hukuku Dergisi*, 4(1), 81-140, 2006.

[55] N. Kaur, & H. Aggarwal, "Query Based Approach For Referrer Field Analysis Of Log Data Using Web Mining Techniques For Ontology Improvement", *International Journal of Information Technology*, *10*, 99-110. 2018.

[56] I. Çınar, I., & H. Ş. Bilge, "Web Madenciliği Yöntemleri ile Web Loglarının İstatistiksel Analizi ve Saldırı Tespiti", *Bilişim Teknolojileri Dergisi,* 9(2), 125-135,

2016.

[57] T. Özseven, & M. Düğenci, "Log Analizi: Erişim Kayıt Dosyaları Analiz Yazılımı ve GOP Üniversitesi Uygulaması", *Bilişim Teknolojileri Dergisi*, 4(2), 2011.

[58] BGA Security, (2023, 10 Eylül), *Loglama sistemi konumlandırma,* [Online]. Erişim: https://www.bgasecurity.com/makale/log-yonetimi-ve-saldiri-analizi-egitimi-bolum-2/

[59] U. Sezer, (2023, 10 Ekim), *Güvenlik amaçlı SNMP Walk ile Merkezi Loglama Yazılımı*, [Online]. Erişim: https://web.itu.edu.tr/akingok/inettr09/guvenlik_amacli_walkbee_yazilimi_sunumu.pdf

[60] R. G. Abbott, J. McClain, B. Anderson, K. Nauer, A. Silva, & C. Forsythe, "A log analysis of Cybersecurity Training Exercises", *Procedia Manufacturing,* 3, 5088-5094, 2015.

[61] E. T. Kılıç, "Siber Saldırıları İzleme Yöntemleri ve Zararlı Yazılım Analizi", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü Gazi Üniversitesi, Ankara, 2015.

[62] V. Platonov, & V. Semenov, "Detecting Network Attacks in Computer Networks by Using Data Mining Methods", *Интеллектуальные Технологии На транспорте*, (4), 16-21, 2016.

[63] BGA Security, (2023, 10 Ekim), *saldırı tespitinde kullanılan log kayıtları,* [Online]. Erişim: https://www.bgasecurity.com/2017/01/siber-tehditler-anketi-2016/

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

[65] W. Lee & S. J. Stolfo, "Data Mining Approaches for Intrusion Detection", *Proceedings of the 7th conference on USENIX Security Symposium,* Cilt 7, ss. 6, 1998.

[66] M. Landauer, F. Skopik, M. Wurzenberger & A. Rauber, "System log Clustering Approaches For Cyber Security Applications: A Survey", *Computers & Security*, *92*, 101739, 2020.

[67] L. Cornett, K. Grewal, M. Long, Millier, & S. Williams, "Network Security: Challenges And Solutions", *Intel Technology Journal*, *13*(2), 2009.

[68] K. Nam, & K. Kim, "A study on Sdn Security Enhancement Using Open Source IDS/IPS Suricata", *In 2018 International Conference on Information and Communication Technology Convergence* (*ICTC*), 2018, ss. 1124-1126.

[69] T. S. Sobh, Wired and Wireless Intrusion Detection System: Classifications, Good Characteristics and State-of-the-art, *Computer Standards & Interfaces*, 670-694, 2006.

[70] A. Patcha & J. M. Park J.M, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends", Computer Networks, 51(12), 3448-3470, 2007.

[71] S. Saito, K. Maruhashi, M. Takenaka, & S. Torii, "TOPASE: Detection and Prevention of Brute Force Attacks With Disciplined IPs from IDS logs", *Journal of Information Processing*, *24*(2), 217-226, 2016.

[72] Z. Wu, D. Xiao, H. Xu. & X. Peng, "Virtual Inline A Technique of Combining IDS and IPS Together in Response Intrusion", *Education Technology and Computer Science* (*ETCS* '09), 1, 1118- 1121, 2009.

[73] D. Stiawan., A.H. Abdullah, A. H., & M.Y. Idris, "The Trends of Intrusion Prevention System Network", *In 2010 2nd International Conference on Education Technology And Computer,* 2018*, ss.* 201-217.

[74] M. D. Koyuncu & N. Ünlü, " Yapay Zekâ Tekniklerinin Saldırı Tespit Sistemleri'nde Kullanımı", *Beykoz Akademi Dergisi*, *10*(1), 78-87, 2022.

[75] T. S. Huda & S. Subektiningsih, "Analisis Keamanan Jaringan Komputer Menggunakan Metode IDS dan IPS dengan Notifikasi Telegram", *Indonesian Journal of Computer Science (IJCS),* 13(1), 2024.

[76] H. Şeker, (2023, 10 Ekim), *IDS/IPS sistemi tasarımı,* [Online]. Erişim: http://www.harunseker.org/

[77] T. M. Zitta, Neruda, & L. Vojtech, "The security of RFID Readers With IDS/IPS Solution Using Raspberry Pi", In *2017 18th International Carpathian Control Conference (ICCC)*, 2017, ss. 316-320.

[78] K. Scarfone ve P. Mell, "Intrusion Detection and Prevention Systems (IDPS)", *NIST Special Publication* 800-94, 2007.

[79] Acarm-ng, [Online]. (2023, 1 Kasım), *IPS Araçları*, Erişim:

http://www.acarm.wcss.wroc.pl/index.php.

[80] V. Paxson, "Bro: A System for Detecting Network Intruders in RealTime", Journal Computer Networks: *The International Journal of Computer and Telecommunications Networking,* vol. 31, no. 23-24, pp. 2435-2463, 1999.

[81] U. Lindqvist and P. A. Porras, "EXpert-BSM: A Host-Based İntrusion Detection Solution For Sun Solaris", *in Seventeenth Annual Computer Security Applications Conference,* 2021, ss. 240-251.

[82] Emerald, (2023, 1 Kasım), *IPS Araçları*, [Online]. Erişim: http://www.csl.sri.com/projects/emerald/releases/eXpert-BSM/.

[83] fail2ban, (2023, 1 Kasım), *IPS Araçları,* [Online]. Erişim: http://www.fail2ban.org/wiki/index.php/MANUAL_0_8.

[84] D. Teixeira, L. Assunção, T. Pereira, S. Malta & P. Pinto, OSSEC IDS extension to improve log analysis and override false positive or negative detections. *Journal of Sensor and Actuator Networks*, *8*(3), 46, 2019.

[85] lasamhna, (2023, 10 Ekim), *IPS Araçları,* [Online]. Erişim: http://www.lasamhna.de.

[86] Blog, (2023, 1 Kasım), *IPS Araçları,* [Online]. Erişim: http://www.preludesiem.com/en/products/prelude-oss/.

[87] Sagan, (2023, 1 Kasım), *IPS Araçları,* [Online]. Erişim: https://quadrantsec.com/sagan_log_analysis_engine/.

[88] snort (2023, 1 Kasım), *IPS Araçları,* [Online]. Erişim: https://www.snort.org.

[89] suricata (2023, 1 Kasım), *IPS Araçları,* [Online]. Erişim: https://suricata-ids.org/.

[90] Blog, (2023, 10 Ekim), *SUCRI, Mass WordPress Brute Force Attacks-Myth or Reality (2013)*, [Online]. Erişim: (http://blog.sucuri.net/2013/04/masswordpress-brute-force-attacks-myth-or-reality.html).

[91] Blog, (2023, 10 Ekim), SUCRI, *WordPress Brute Force Attack Timeline (2013),* [Online]. Erişim: (http://blog.sucuri.net/2013/04/the-wordpress-bruteforce-attack-timeline.html).

[92] Lucian Constantin, (2023, 10 Ekim), Github Ban Sweak Passwords After Brute-Force Attack Results in Compromised Accounts (2013), [Online]. Erişim: (http://www. pcworld.com/article/2065340/github-bans-weak-passwords-after- bruteforce-attack-results-in-compromised-accounts.html).

[93] Z. Wu, D. Xiao., H. Xu, X. Peng & X. Zhuang, "Virtual inline: a technique of combining IDS and IPS together in response intrusion", *In 2009 First International Workshop on Education Technology and Computer Science*, 1118-1121, 2009.

[94] H. Koca, "Türkiye'de Siber Güvenlik Uygulamaları", Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Hatay Mustafa Kemal Üniversitesi, Hatay, 2022.

[95] M. Of, "Siber Güvenlik Üzerine Bir Araştırma: Yazılım Güvenliği", Bayburt Üniversitesi Fen Bilimleri Dergisi, 2(2), 254-260, 2019.

6. EKLER

6.1. EK 1: IDS/IPS SALDIRI TESPİT SİSTEMİ KODLARI I

```
#!/usr/bin/env python
# coding: utf-8
#-------------------------------------------------
# packet capture & decoding
import pcapy,dpkt   # bu kütüphaneleri yüklemek gerekiyor. standart python ile gelmiyorlar.
import socket, sys, os
attack_pattern='' #saldırı desenlerini taşıyan değişken
ipban=1 # ipban değeri 1 olursa saldırgan IP adresi iptables ile engellenenir.
def create_attack_pattern(): #3. adım saldırı desenleri oluşturulur
    global attack_pattern
    F=open("attack_patterns.txt","rb")
    attack_pattern=F.read().split("\n")
class network_monitor:
    def __init__ (self):
        pass
    def start (self): # 5. adım...
        # TODO: specify a device or select all devices
        # dev = pcapy.finddevs()[0] # ağ aygıtlarından ilk aygıtı seçmeyi sağlar.
        dev = 'wlan0' #Dinleyeceğiniz aygıt adı
        p = pcapy.open_live(dev, 65536, False, 1)
        p.loop(-1, self.handle_packet)
    def handle_packet (self, header, data):
        global attack_pattern,ipban,banned_ips
        eth = dpkt.ethernet.Ethernet (data) #etherner datasını almak için kullanıyoruz.
        if eth.type == dpkt.ethernet.ETH_TYPE_IP: #ethernet tipine bakıyoruz. IP paketiyse işleme alıyoruz.
            ip = eth.data
            tcp = ip.data
            src_ip = socket.inet_ntoa(ip.src) #kayna ip adresini buluyoruz.
            dst_ip = socket.inet_ntoa(ip.dst) #hedef ip adresini buluyoruz.
            try:
                if tcp.dport == 80 and len(tcp.data) > 0: #tcp portu 80 ise ve aktif veri varsa aşağıdakiler yapılacak...
                    http = dpkt.http.Request(tcp.data)
                    # saldırı desenleri uri de var mı bakalım...
                    for i in attack_pattern: # saldırı desenleri içerisinde dolaşalım
                        if http.uri.find(i)>0: # gelen istekte saldırı var mı kontrol edelim.
                            # desen eşleşiyorsa saldırı var diyelim..
                            # bu kısımda veritabanına ekleme yapılacak...
                            logline= "Saldırı: %s > %s %s %s%s " %(src_ip,dst_ip,http.method,http.headers['host'],http.uri)
                            if ipban==1: # saldırı varsa ve ipban değişkeni 1 ise bloklama yapalım
                                print "Çalıştırılacak Komut: iptables -A INPUT -s %s -j DROP"%src_ip
                                # komutu çalıştırmak için alt satırı açmanız gerekir:)
                                #os.system("iptables -A INPUT -s %s -j DROP"%src_ip) # Linux için saldırgan IP adresini engelleyelim...
                                # windows için netsh komutları http://itblog.gr/213/configuring-windows-firewall-from-the-command-line/
                                #os.system("netsh advfirewall firewall add rule name=\"Block some stuff\" dir=in action=block remoteip=%s enable=yes"%src_ip)
# Windows için saldırgan IP adresini engelleyelim...
                            print logline # saldırı mesajını ekrana yazalım... :)
            except:
                pass
def main():
    create_attack_pattern() # 2. adım
    network_monitor ().start () # 4 .adım
if __name__=="__main__":
    main () #1. adım
```

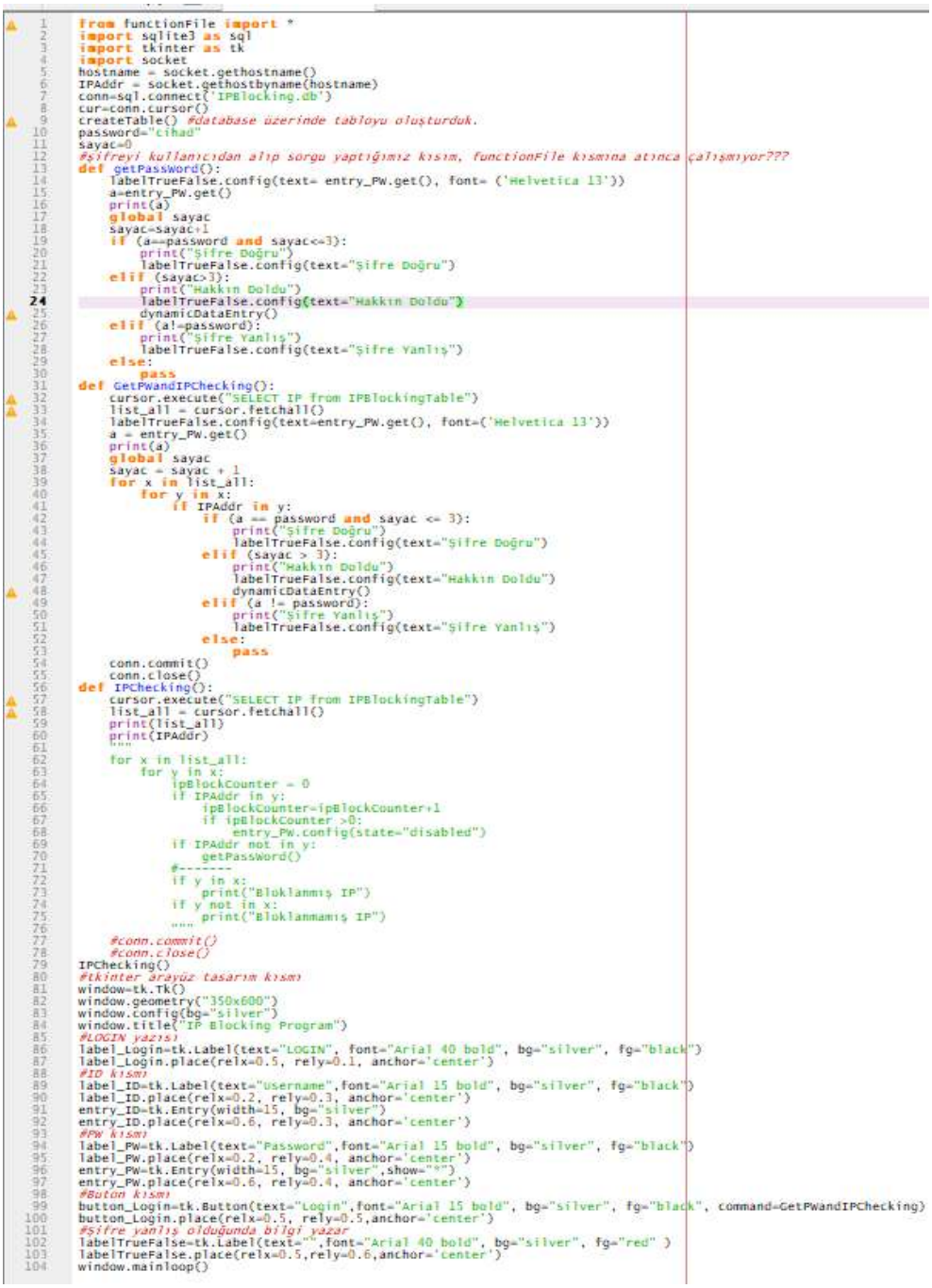
Şekil 6.1 IDS/IPS Tespiti Açık Kaynak Uygulama Kodları [76].

6.2. EK 2: SALDIRI TESPİT VE ÖNLEME SİSTEMİ KODLARI I

```
import sqlite3 as sql
import socket
from datetime import datetime
conn=sql.connect('IPBlocking.db')
cursor=conn.cursor()

def createTable(): #tabloyu oluşturan fonksiyon
    cursor.execute("CREATE TABLE IF NOT EXISTS IPBlockingTable(IP TEXT, saat TEXT, tarih TEXT)")

def getIpAdress(): #IP adresi alan fonksiyon
    hostname = socket.gethostname()
    IPAddr = socket.gethostbyname(hostname)
    print("Your Computer Name is:" + hostname)
    print("Your Computer IP Address is:" + IPAddr)

def dynamicDataEntry(): #IP adresini ve saati database'e yazan fonksiyon
    #IP adresini alan kodlar
    hostname = socket.gethostname()
    IPAddr = socket.gethostbyname(hostname)

    #şuanki saati alan kod
    now = datetime.now()
    current_time = now.strftime("%H:%M:%S")

    #şuanki tarihi alan kod
    current_date=datetime.today().strftime('%Y.%m.%d')

    add_commmand="INSERT INTO IPBlockingTable VALUES {}"
    isim=(IPAddr, current_time, current_date)
    cursor.execute(add_commmand.format(isim))
    conn.commit()
    conn.close()
```

Şekil 6.2 Açık Kaynak Uygulama Kodları I

6.3. EK 3: SALDIRI TESPİT VE ÖNLEME SİSTEMİ KODLARI II



```
from functionFile import *
import sqlite3 as sql
import tkinter as tk
import socket
hostname = socket.gethostname()
IPAddr = socket.gethostbyname(hostname)
conn=sql.connect('IPBlocking.db')
cur=conn.cursor()
createTable() #database üzerinde tabloyu oluşturduk.
password="cihad"
sayac=0
#şifreyi kullanıcıdan alıp sorgu yaptığımız kısım, functionFile kısmına atınca çalışmıyor???
def getPassWord():
    labelTrueFalse.config(text= entry_PW.get(), font= ('Helvetica 13'))
    a=entry_PW.get()
    print(a)
    global sayac
    sayac=sayac+1
    if (a==password and sayac<=3):
        print("Şifre Doğru")
        labelTrueFalse.config(text="Şifre Doğru")
    elif (sayac>3):
        print("Hakkın Doldu")
        labelTrueFalse.config(text="Hakkın Doldu")
        dynamicDataEntry()
    elif (a!=password):
        print("Şifre Yanlış")
        labelTrueFalse.config(text="Şifre Yanlış")
    else:
        pass
def GetPWandIPChecking():
    cursor.execute("SELECT IP from IPBlockingTable")
    list_all = cursor.fetchall()
    labelTrueFalse.config(text=entry_PW.get(), font=('Helvetica 13'))
    a = entry_PW.get()
    print(a)
    global sayac
    sayac = sayac + 1
    for x in list_all:
        for y in x:
            if IPAddr in y:
                if (a == password and sayac <= 3):
                    print("Şifre Doğru")
                    labelTrueFalse.config(text="Şifre Doğru")
                elif (sayac > 3):
                    print("Hakkın Doldu")
                    labelTrueFalse.config(text="Hakkın Doldu")
                    dynamicDataEntry()
                elif (a != password):
                    print("Şifre Yanlış")
                    labelTrueFalse.config(text="Şifre Yanlış")
                else:
                    pass
    conn.commit()
    conn.close()
def IPChecking():
    cursor.execute("SELECT IP from IPBlockingTable")
    list_all = cursor.fetchall()
    print(list_all)
    print(IPAddr)
    """
    for x in list_all:
        for y in x:
            ipBlockCounter = 0
            if IPAddr in y:
                ipBlockCounter=ipBlockCounter+1
                if ipBlockCounter >0:
                    entry_PW.config(state="disabled")
            if IPAddr not in y:
                getPassWord()
            #-------
            if y in x:
                print("Bloklanmış IP")
            if y not in x:
                print("Bloklanmamış IP")
            """
    #conn.commit()
    #conn.close()
IPChecking()
#tkinter arayüz tasarım kısmı
window=tk.Tk()
window.geometry("350x600")
window.config(bg="silver")
window.title("IP Blocking Program")
#LOGIN yazısı
label_Login=tk.Label(text="LOGIN", font="Arial 40 bold", bg="silver", fg="black")
label_Login.place(relx=0.5, rely=0.1, anchor='center')
#ID kısmı
label_ID=tk.Label(text="username",font="Arial 15 bold", bg="silver", fg="black")
label_ID.place(relx=0.2, rely=0.3, anchor='center')
entry_ID=tk.Entry(width=15, bg="silver")
entry_ID.place(relx=0.6, rely=0.3, anchor='center')
#PW kısmı
label_PW=tk.Label(text="Password",font="Arial 15 bold", bg="silver", fg="black")
label_PW.place(relx=0.2, rely=0.4, anchor='center')
entry_PW=tk.Entry(width=15, bg="silver",show="*")
entry_PW.place(relx=0.6, rely=0.4, anchor='center')
#Buton kısmı
button_Login=tk.Button(text="Login",font="Arial 15 bold", bg="silver", fg="black", command=GetPWandIPChecking)
button_Login.place(relx=0.5, rely=0.5,anchor='center')
#şifre yanlış olduğunda bilgi yazar
labelTrueFalse=tk.Label(text="",font="Arial 40 bold", bg="silver", fg="red" )
labelTrueFalse.place(relx=0.5,rely=0.6,anchor='center')
window.mainloop()
```

Şekil 6.3 Açık Kaynak Uygulama Kodları II

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Serkan ÖZARGIN

Yabancı Dili : İngilizce

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezun Yılı
Y. Lisans	Siber Güvenlik (Tezli)	Düzce Üniversitesi	2024
Y. Lisans	Yönetim Bilişim Sistemleri (Tezli)	Bandırma Onyedi Eylül Üniversitesi	2023
Y. Lisans	Bilgisayar ve Bilişim Mühendisliği ABD. Bilişim Teknolojileri BD. (Tezsiz)	Sakarya Üniversitesi	2017
Sertifika	Pedagojik Formasyon/Öğretmenlik	Bartın Üniversitesi	2015
Lisans	Yönetim Bilişim Sistemleri	Anadolu Üniversitesi	2019
Lisans	İşletme	Anadolu Üniversitesi	2008
Önlisans	Bilgisayar Donanımı	Afyon Kocatepe Üniversitesi	2003
Lise	Fen Bilimleri	Keles Lisesi	1999

YAYINLAR

Tez Kapsamında Çıkan Yayınlar

1. S. Özargın, & A. Albayrak “Log Kayıtları Üzerinden Siber Saldırı Tespit Sistemi Geliştirilmesi”, *Akıllı sistemlerin endüstriyel uygulaması I,* 1. Baskı, Ankara, Türkiye: BİDGE Yayınları, 2023, böl.8, ss. 150-187.