BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİMDALI
BİLGİSAYAR MÜHENDİSLİĞİ TEZLİ YÜKSEK LİSANS PROGRAMI

SİBER UZAY ORTAMINDA SALDIRI TEHDİTLERİNİN FARKINDALIĞI, TESPİTİ VE ÖNLENMESİ ÜZERİNE BİR GERÇEK-ZAMAN SİSTEM ÖNERİSİ

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

EMRECAN ARDA

ANKARA - 2020

BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİMDALI
BİLGİSAYAR MÜHENDİSLİĞİ TEZLİ YÜKSEK LİSANS PROGRAMI

SİBER UZAY ORTAMINDA SALDIRI TEHDİTLERİNİN FARKINDALIĞI, TESPİTİ VE ÖNLENMESİ ÜZERİNE BİR GERÇEK-ZAMAN SİSTEM ÖNERİSİ

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

EMRECAN ARDA

TEZ DANIŞMANI

PROF. DR. AHMET ZİYA AKTAŞ

ANKARA - 2020

BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 07 / 05 / 2020

Öğrencinin Adı, Soyadı : Emrecan Arda
Öğrencinin Numarası : 21010003
Anabilim Dalı : Bilgisayar Mühendisliği Anabilim Dalı
Programı : Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışmanın Unvanı/Adı, Soyadı : Prof. Dr. A. Ziya Aktaş
Tez Başlığı : Siber Uzay Ortamında Saldırı Tehditlerinin Farkındalığı, Tespiti ve Önlenmesi Üzerine Bir Gerçek-Zaman Sistem Önerisi

Yukarıda başlığı belirtilen Yüksek Lisans tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 97 sayfalık kısmına ilişkin, 07 / 05 / 2020 tarihinde danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı %8'dir. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:…….

ONAY

Tarih: … / … / 20…

Öğrenci Danışmanı Unvan, Adı, Soyadı, İmza:

……..

TEŞEKKÜR

Yazar, bu çalışmanın gerçekleşmesinde katkılarından dolayı, aşağıda adı geçen kişi ve kuruluşlara içtenlikle teşekkür eder.

Sayın Prof. Dr. Ahmet Ziya Aktaş'a (tez danışmanı), tez çalışması süresince gösterdiği sabrı, duyduğu güveni her daim hissettirmesi ve deneyimleri ile tez çalışmasına yol gösterdiği için…

ÖZET

Emrecan ARDA

SİBER UZAY ORTAMINDA SALDIRI TEHDİTLERİNİN FARKINDALIĞI, TESPİTİ VE ÖNLENMESİ ÜZERİNE BİR GERÇEK-ZAMAN SİSTEM ÖNERİSİ

Başkent Üniversitesi Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

2020

Teknolojinin hızla gelişmesi, bilgi teknolojilerine olan bağımlılığı her geçen gün arttırmaktadır. Bilgi önemini arttırdıkça, bilgi teknolojileri sistemleri üzerinde saklanan bilgiler potansiyel hedefler haline gelmiştir. Büyüyen ve entegre olan bilgi sistemleri 'siber uzay' kavramını doğurmuştur. Siber uzay içerisinde aynı zamanda 'siber saldırganları' da barındırmaktadır. Bilgi güvenliğinin önemi, bilgi sistemlerine saldırı yapmak için kullanılabilecek olan 'saldırı yüzeyinin' genişlemesiyle daha da artmıştır. 'Siber farkındalık' bilincinin oluşturulması, saldırıların önlenmesi için en büyük önlem olmuştur. Bu bilincin oluşturulabilmesi için teorik bilgi yanında pratik çalışmaların güvenli bir şekilde yapılabileceği bir ortama ihtiyaç duyulmaktadır. Bu tezde öneri olarak sunulan sistem ile güvenli bir ortamda siber tehditlerin anlatılması ve etkilerinin gösterilmesi mümkün olacaktır. Ayrıca yeni güvenlik tekniklerinin denenmesine de olanak sağlanacaktır.

ANAHTAR KELİMELER: Siber Uzay, Saldırı Yüzeyi, Siber Farkındalık, Saldırı Tespit Sistemleri, Saldırı Önleme Sistemleri.

ABSTRACT

Emrecan ARDA

A REAL-TIME SYSTEM PROPOSAL ON THE AWARENESS, DETECTION AND PREVENTION OF THREATS IN CYBER SPACE

Baskent University Institute of Science

Department of Computer Engineering

2020

The rapid development of technology increases the dependency on information technologies. As the importance of information increases, information stored on information technology systems has become potential targets. Integrating different systems together has given birth to the concept of 'cyber space'. Cyber space also contains 'cyber attackers'. The importance of information security has further increased with the expansion of the 'attack surface' that can be used to attack information systems. Raising 'cyber awareness' has become the biggest measure to prevent attacks. In order to create this awareness, there is a need for an environment where exercises can be done safely to support theoretical knowledge. With the system presented as a proposal in this thesis, it will be possible to explain cyber threats and show their effects in a safe environment. It will also be possible to try new security techniques.

KEYWORDS: Cyber Space, Attack Surface, Cyber Awareness, Intrusion Detection Systems, Intrusion Prevention Systems

İÇİNDEKİLER LİSTESİ

Sayfa

ÖZET ..... **i**

ABSTRACT ..... **ii**

İÇİNDEKİLER LİSTESİ ..... **iii**

TABLOLAR LİSTESİ ..... **vii**

ŞEKİLLER LİSTESİ ..... **viii**

SİMGELER VE KISALTMALAR LİSTESİ ..... **xi**

1. GİRİŞ **1**

1.1. Problemin Tanımı **1**

1.2. Literatür Taraması **3**

1.2.1. Temel güvenlik kavramları **4**

1.2.2. Temel güvenlik ilkeleri **7**

1.2.3. Saldırılar **10**

1.2.4. Varlık, zafiyet ve istismar **13**

1.2.5. Siber uzay **14**

1.2.6. Siber saldırı **14**

1.2.7. Siber tehdit yüzeyi **16**

1.3. Çalışmanın Yapısı **16**

2. SİBER FARKINDALIK **18**

2.1. Siber Farkındalık Nedir? **18**

2.2. Siber Farkındalık Nasıl Sağlanır? **19**

2.2.1. Eğitim **19**

2.2.2. Politikalar, standartlar, yönergeler ve prosedürler **21**

2.3. Siber Tehditler Nelerdir? **23**

2.3.1. Sosyal mühendislik 24
2.3.2. Oltalama (Phishing) 26
2.3.3. DDOS/Botnet 27
2.3.4. Malware/Ransomware/Virus 29
2.3.5. Rootkit/Bootkit 32
2.3.6. İçeriden gelen tehditler/İnsan hatası 33
2.4. Sistem Saldırı Tipleri 34
2.4.1. Uygulama saldırıları 34
2.4.2. İşletim sistemi saldırıları 38
2.4.3. Ağ yığını saldırıları 40
3. SİBER SALDIRI TESPİTİ 48
3.1. Saldırı Tespit Sistemleri Sınıflandırılması 48
3.1.1. Ağ tabanlı saldırı tespit sistemleri (Network-based Intrusion Detection Systems - NIDS) 48
3.1.2. Uç nokta tabanlı saldırı tespit sistemleri (Host-based Intrusion Detection Systems - HIDS) 50
3.2. Saldırı Tespit Sistemlerinin Tespit Yöntemleri 51
3.2.1. Desen eşleştirme 51
3.2.2. Protokol analizi 51
3.2.3. Anomali analizi 52
3.2.4. Evrensel tehdit korelasyon yetenekleri 52
3.2.5. Dosya bütünlük kontrolü 54
3.2.6. Kayıt defteri takibi 54
3.3. Ağ Denetimi 55
3.3.1. Akış kontrolü (Flow Control) 55
3.3.2. Ağ güvenlik takibi (Network Security Monitoring) 56
3.3.3. Vekil sunucu (Proxy Server) 58

3.4. Uç Nokta Denetimi 61
3.4.1. Kayıt (Log) yönetimi 61
3.4.1.1. Windows kayıt yönetimi 64
3.4.1.2. Linux kayıt yönetimi 65
3.4.1.3. Syslog 67
3.4.1.4. Kayıtların ayrıştırılması, indekslenmesi ve saklanması 67
3.5. SIEM (Security Information and Event Management) 72
3.6. Balküpleri ve Balküpü Ağları 73
4. SİBER SALDIRILARIN ÖNLENMESİ 77
4.1. Ağ Koruması 77
4.1.1. Güvenlik duvarı (Firewall) 78
4.1.2. Saldırı önleme sistemi (IPS – Intrusion Prevention System) 81
4.1.3. Kum havuzu (Sandbox) 81
4.1.4. E-posta ağ geçidi (Email Gateway) 82
4.1.5. Web uygulama güvenlik duvarı 83
4.1.6. Bulut tabanlı koruma 84
4.2. Uç Nokta Koruması 84
4.2.1. Antivirüs/Antimalware 87
4.2.2. Veri kaybı önleme (DLP – Data Loss Prevention) 88
4.2.3. Uç nokta tespit ve yanıt (EDR – Endpoint Detection and Response) 90
4.2.4. Sıkılaştırmalar 92
5. BİR GERÇEK-ZAMAN SİBER TEHDİTLER, SALDIRI TESPİTİ VE SALDIRILARIN ÖNLENMESİ İÇİN ÇALIŞMA ORTAMI SİSTEM ÖNERİSİ 93
6. SONUÇ VE ÖNERİLER 96
6.1. Özet 96
6.2. Sonuç 96

6.3. Öneriler 96

KAYNAKLAR..... 98

TABLOLAR LİSTESİ

Sayfa

Tablo 2.1. WannaCry kullanılan yöntemler 31
Tablo 3.1. Basit bir squid proxy yapılandırması 60

ŞEKİLLER LİSTESİ

Sayfa

Şekil 1.1. CIA (Confidentiality, Integrity and Availability) Üçlüsü 6
Şekil 1.2. Derinlemesine Güvenlik katmanları 9
Şekil 1.3. AAA (Authentication, Authorization and Accounting) İlkesi 10
Şekil 1.4. CIA üçlüsü ve saldırı kategorilerinin etkileşimi 11
Şekil 1.5. Zafiyet Çeşitleri ile İlgili Genel Kanı 16
Şekil 2.1. İyi bir poster örneği 21
Şekil 2.2. Politikalar, standartlar, yönergeler ve prosedürler 22
Şekil 2.3. Örnek Maltego uygulaması 25
Şekil 2.4. 2019 yılı sosyal saldırı eğilimleri 26
Şekil 2.5. Bir oltalama saldırısı örneği 27
Şekil 2.6. DDoS (Distributed Denial of Service) saldırısı 28
Şekil 2.7. Virüs Tipleri 30
Şekil 2.8. Edgescan Raporu İstatistikleri 36
Şekil 2.9. Uygulama Saldırıları test ortamı 36
Şekil 2.10. Çalışan uygulamaların tespiti 37
Şekil 2.11. Detaylı web hizmeti tarama sonuçları 37
Şekil 2.12. Kurban makineye uzaktan erişim 38
Şekil 2.13. Mimikatz Çalışma Ekran Görüntüsü 39
Şekil 2.14. PowerSploit Uygulaması Betikleri 39
Şekil 2.15. Windows 10 servisleri 40
Şekil 2.16. Windows sisteminin beklediği bağlantı örneği 40
Şekil 2.17. Ağ Yığını Saldırı Test Ortamı 41
Şekil 2.18. Windows 8 makinesinde varsayılan ağ geçidi 42
Şekil 2.19. Windows 8 makinesinde saldırı öncesi ARP tablosu 42
Şekil 2.20. Ettercap ekran görüntüsü 43
Şekil 2.21. ARP (Address Resolution Protocol) Zehirlemesi 43
Şekil 2.22. Saldırı başarılı olduktan sonra yeni ARP tablosu 44
Şekil 2.23. MAC (Media Access Control) adresi değiştirme uygulaması 44
Şekil 2.24. MAC adresi değişmeden önce 45
Şekil 2.25. Yeni MAC adresi atanması 45
Şekil 2.26. Yeni MAC adresinin doğrulanması 45

Şekil 2.27. Saldırı öncesi yapılan DNS (Domain Name System) sorgusu..... 46
Şekil 2.28. Ettercap DNS Sahteciliği saldırısı 46
Şekil 2.29. DNS Sahteciliği saldırısı sonrası 47
Şekil 3.1. Ağda NIDS (Network-based Intrusion Detection System) konumlandırılması.. 49
Şekil 3.2. Örnek kural listesi 49
Şekil 3.3. Bir kuralın incelenmesi 50
Şekil 3.4. Snort Tehdit İstihbaratı Toplama Ekranı 53
Şekil 3.5. Snort Tehdit Tespit Kuralı 53
Şekil 3.6. Şifreleme karması örneği 54
Şekil 3.7. Windows kayıt defteri..... 55
Şekil 3.9. Kurum Güvenlik Döngüsü..... 56
Şekil 3.8. Elastiflow Ekran Görüntüsü..... 57
Şekil 3.10. Zabbix Kullanıcı Arayüzü..... 59
Şekil 3.11. Vekil Sunucu Kullanımı 60
Şekil 3.12. Squid Proxy kayıt örneği 61
Şekil 3.13. CIS (Center of Internet Security) Kayıt Yönetimi 62
Şekil 3.14. CIS Kayıt Yönetimi Kuralları 63
Şekil 3.15. Yerel Güvenlik İlkesi 64
Şekil 3.16. Komut Satırı ile Olay Kaydı Etkinleştirme..... 65
Şekil 3.17. Olay Görüntüleyicisi..... 65
Şekil 3.18. Dosyanın denetlenmeye başlanması 66
Şekil 3.19. Dosya denetimi kayıtları 66
Şekil 3.20. dmesg komutu çıktısı 66
Şekil 3.21. journalctl komutu çıktısı 67
Şekil 3.22. Syslog kullanıcı yapılandırması 68
Şekil 3.23. Syslog sunucusunda toplanan kayıtlar 68
Şekil 3.24. Örnek Bir Grok Filtresi 69
Şekil 3.25. Elasticsearch veri yapısı..... 70
Şekil 3.26. Kibana üzerinde verinin görselleştirilmesi 71
Şekil 3.27. Kibana üzerinde verinin filtrelenmesi..... 71
Şekil 3.28. MHN (Modern Honey Network) Genel Saldırı Haritası 74
Şekil 3.29. MHN tehdit raporu..... 74
Şekil 3.30. MHN saldırı istatistikleri 75
Şekil 3.31. Maltrail tehdit raporu 76

Şekil 4.1. Güvenlik duvarı erişim kısıtı 78
Şekil 4.2. Ağ seviyesinde kum havuzu kullanımı 82
Şekil 4.3. Örnek bir e-posta ağ geçidi yerleşimi 83
Şekil 4.4. Web uygulama güvenlik duvarları 84
Şekil 4.5. Kurumların Uç Noktada Kullandıkları Cihazlar 86
Şekil 4.6. Kurumlarda başarılı bir saldırıya uğramış cihazlar 86
Şekil 4.7. Sophos DLP (Data Loss Prevention) Örnek Ekran Görüntüsü 89
Şekil 4.8. Kaspersky Lab Uygulanabilir Güvenlik Modeli 90
Şekil 4.9. Farklı Çözümlere göre Tehdit Engelleme ve Tespit Oranları 91
Şekil 5.1. Çalışma ortamı sistem önerisi bileşenleri 93
Şekil 5.2. Örnek eğitim ortamı tasarımı 94

SİMGELER VE KISALTMALAR LİSTESİ

AAA	Authentication, Authorization and Accounting
ARP	Address Resolution Protocol
CEH	Certified Ethical Hacker
CIA	Confidentiality, Integrity and Availability
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMDi	Command Injection
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DMZ	Demilitirized Zone
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
EDR	Endpoint Detection and Response
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GOP	The Guardians of Peace
HIDS	Host-based Intrusion Detection Systems
ICT	Information and Communication Technologies
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
KVKK	Kişisel Verilerin Koruması Kanunu
MAC	Media Access Control
MBR	Master Boot Record
MHN	Modern Honey Network
NAT	Network Address Translation
NCR	National Cyber Range
NGFW	Next Generation Firewall
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection Systems
NIPS	Network-based Intrusion Prevention Systems
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSM	Network Security Monitoring
OPM	Office of Personnel Management
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
RFC	Request for Comment
RST	Reset
SANS	SysAdmin, Audit, Network and Security
SEM	Security Event Management
SIEM	Security Information and Event Management
SIM	Security Information Management

SQLi	Structured Query Language Injection
STS	Saldırı Tespit Sistemi
TCP	Transmission Control Protocol
TOR	The Onion Router
UDP	User Datagram Protocol
UTM	Unified threat management
XSS	Cross Site Scripting
WAF	Web Application Firewall

1. GİRİŞ

1.1. Problemin Tanımı

Günümüzde ağ tabanlı sistemler hem sivil hem de askeri alanda büyük önem taşımaktadırlar. Bu sistemler telekomünikasyon ve televizyon hizmetleri, internet, sosyal medya, askeri sistemler vb. birçok karmaşık sistemin temelini oluşturmaktadırlar. Birbirine bağlı sistemlerin sağladığı servisler ev kullanıcılarını, firmaları, hükümetleri, vb. birbirlerine bağlamakta ve günlük akışın büyük bir parçasını oluşturmaktadır. Ağ tabanlı sistemlerin hızlı bir ölçüde büyümüş olması ve birbirine bağımlılığın bu denli artması beraberinde bazı tehlikeleri doğurmuştur. Yazılım test yöntemleri belli bir olgunlukta olsa da birçok farklı yazılımın ağ tabanlı sistemlerle birbirine bağlanıp oluşturduğu büyük sistemlerin test metodolojileri yeterli olgunluğa ulaşamamıştır [1]. Artan kullanıcı ihtiyaçlarının karşılanması için hızlı bir şekilde geliştirilen yeni servisler var olan sistemlerin karmaşıklığını git gide arttırmakta ve sistemlerin güvenliğini sağlamak her geçen gün daha da zorlaşmaktadır.

Bundan 50 yıl önce siber güvenlik denildiği zaman akla bilgisayar güvenliği gelmekteydi. Bilgisayar donanımı pahalı ve erişimi zor olduğu için, sistemleri fiziksel olarak korumak (erişim yetkileri, yangın önleme sistemleri, vb.) en önemli güvenlik uygulaması sayılıyordu. Günümüzde; internet kullanımının hızla artması, bilgisayar maliyetlerinin rahat karşılanabilir hale gelmesi, insanların kimliklerinin internet üzerinde önem kazanması vb. gelişmeler sonucunda artık bilgisayarların fiziksel güvenliği yerine asıl önemli olan bilgisayarların tuttuğu verilerin güvenliği olmuştur. Bu nedenle bilgisayar güvenliği terimi yerini bilgi güvenliği terimine bırakmıştır. Williams et al. [2] ’e göre bilgi güvenliği; bilginin izinsiz erişime veya değiştirilmeye karşı korunması ve aynı zamanda yetkili kişilerce erişilebilir olmasıdır. Bilgi güvenliği (information assurance); sadece bilginin korunması değil, sağlanan güvenliğin seviyesinin farkında olunması anlamına gelmektedir.

Her ne kadar bilgi güvenliği konusu önem kazanıyor olsa da ağ tabanlı sistemler üzerine kurulan servislerin birincil önceliği kullanım kolaylığı sağlamaktır. Özellikle IoT (Internet of Things) teknolojileri veya giyilebilir teknolojiler, kullanıcılara rahat ve kolay kullanılan hizmetler sunmayı hedeflemektedirler. Teknolojinin gelişmesi sonucunda doğan yeni ihtiyaçlar hızlı bir şekilde karşılanmaya çalışılırken bilgi güvenliği ikinci planda kalmaktadır. GDPR (General Data Protection Regulation), KVKK (Kişisel Verilerin Koruması Kanunu), vb. kanunlar kurumlara veri güvenliğini sağlamak için yükümlülükler getirse bile siber saldırganlar hedeflerine ulaşmayı başarmaktadırlar.

Kurumların bilgi güvenliğini sağlayabilmesi için, bütün kurum çalışanlarının temel güvenlik kavramları olan gizlilik, bütünlük ve kullanılabilirlik kavramlarına hakim olmaları gerekmektedir. Bu kavramlara hakimiyet, kurumların oluşturduğu güvenlik politikaları ve çalışanlarına sağladığı farkındalık eğitimleri sayesinde kazanılmaktadır. Kurum sistemlerini yöneten insanların ise bahsedilen kavramlara ek olarak siber uzay, siber saldırı, varlık, zafiyet ve istismar gibi kavramlara da hakim olmaları gerekmektedir. Örnek olarak hastane sistemleri işleten bir sistem yöneticisinin sağlık sektörünü hedef alan en son saldırılardan haberdar olması gerekmektedir. Böylece kendi varlıkları üzerinde bu saldırın hedef alabileceği zafiyetleri hızlı bir şekilde kapatabilmesi gerekmektedir. Temel güvenlik kavramları ve bu kavramlara bağlı olarak türeyen ilkeler ve tanımlar bölüm 1.2 Literatür Taraması altında verilmiştir.

Siber saldırıların kavram olarak bilinmesi, siber tehditlerin anlaşılması ve farkındalık yaratılması bilgi güvenliğinin önemli bir bölümünü oluşturmaktadır fakat bu unsurlar destekleyici unsurlardır. Ana unsurlar ise siber saldırıların tespit edilebilmesi ve önlenebilmesidir. Siber saldırı tespit ve önleme sistemlerinin kurulması, yeterli ve yetenekli personel ile işletilmesi bir kurumun bilgi güvenliği sağlayabilmesi için çok önemlidir. Hiçbir zaman %100 güvenlik olamayacağı bilinmelidir. Bu sistemler saldırganların işini zorlaştırmayı ve onları yıldırmayı hedeflemektedir. Ayrıca oluşabilecek bir veri sızıntısı sonrasında saldırganların hangi eylemleri gerçekleştirdiğinin tespit edilmesini sağlamaktadırlar.

Unutulmamalıdır ki bilgi güvenliğinin temelini oluşturan bütün sistemler o sistemleri kullanan ve yöneten insanların kabiliyetleri ve bilgileri ile sınırlıdırlar. Örneğin bir kurum çalışanı kendisine gelen oltalama e-postasını açtığı zaman güvenlik sistemleri yetersiz kalabilir ve kurum varlıkları saldırganlar tarafından ele geçirilebilir. Bu nedenle yukarıda bahsedilen ana unsurların destekleyici unsurlar ile tamamlanması çok büyük önem taşır.

Bu tezin amacı; yukarıda bahsedilen ana ve destekleyici unsurlar ile ilgili literatür taraması yaptıktan sonra detaylı açıklamalarını vermek ve bu unsurların çalışılabileceği ve/veya öğretilebileceği güvenli bir ortam önerisi sunmaktır. Bu ortam, farklı saldırı veya savunma senaryolarına göre çalışma altyapısı sağlayacak ve gerçek bir siber olayı güvenli bir alanda canlandırma imkanı sağlayacaktır. Bu ortam ile hedeflenen, siber farkındalığın arttırılmasını sağlamak, farklı güvenlik sistemlerinin test edilebilmesine olanak sağlamak, siber savunma yeteneklerini geliştirmek ve yeni güvenlik teknikleri oluşturabilmek için bir çalışma alanı sağlamaktır.

1.2. Literatür Taraması

Bilgi güvenliğinin önemini anlamak için bilgisayar suçlarına birkaç örnek vermek faydalı olacaktır. İlk örnek olarak Morris Solucanı (The Morris Worm) ile başlanabilir. Cornell Üniversitesi mezunu olan Robert Morris İnternet Solucanı (Internet Worm) ya da Morris Worm'u 1988 yılında yayınlamıştır. O zaman internete bağlı bulunan bilgisayarların %10'una (yaklaşık olarak 6000) bulaşan bu solucan, zararlı bir içerik içermese de bilgisayarları kullanılamaz hale getirmiştir [2].

Kevin Mitnick ismi siber güvenlik ile ilgilenen herkes tarafından bilinmektedir. Kendisi 1980'ler ve 1990'larda büyük bilgisayar suçları işlemiştir. 1995 yılında yakalandığı zaman suçlarını itiraf etmiş ve 46 ay hapis cezasına mahkum edilmiştir. İzinsiz erişim sağladığı firmalar arasında Motorola, Novell, Fujitsu ve Sun Microsystems bulunmaktadır [2].

1999 yılının Mart ayının sonunda e-posta ile yayılan Melissa Virüs'ü 1.2 milyon bilgisayarı, 53.000 sunucuyu, en az 200 bilgisayarı olan 7.800 Kuzey Amerika Firmasını etkilemiş ve 248 milyon dolardan fazla hasar vermiştir [3].

Code-Red (CRv2) solucanı 19 Temmuz 2001 yılında, 14 saatten kısa sürede İnternete bağlı olan 359.000 bilgisayara bulaşmış ve 2.6 milyar dolardan fazla hasar vermiştir [4].

Nisan 2009'da Amerikan Homeland Security sekreteri Janet Napolitano gazetecilere, Rusya ve Çin tarafından Amerikan enerji hatlarına yapılan siber saldırıların farkında olduklarını açıklamıştır. 'Kansas City Star' gazetesinin bu konuyla ilgili 1997 yılında yaptığı habere göre yerel enerji firması olan 'Kansas City Power and Light' bütün bir yıl boyunca 10.000 saldırıya maruz kalmıştır. 2009 yılı verilerine göre firma yılda 30 ila 60 milyon siber saldırıya maruz kalmıştır [2].

İnternet erişimi yaygınlaştıkça ve insanların veriye ulaşması kolaylaştıkça, siber tehdit yüzeyi de şekil değiştirmeye başlamıştır. Geçmişte siber tehdit yüzeyleri daha küçüktü ve saldırılar genelde belli bir hedefe yönelik yapılırdı. Günümüzde tehdit yüzeylerinin artması, devlet aktörlerinin (state actor) devreye girmesi vb. olaylar siber tehditlerin ciddiyetini ve bir saldırı sonrası doğabilecek sonuçların ciddiyetini büyük ölçüde arttırmıştır. Williams et. al. [2] 'e göre saldırganların iki amacı vardır. Bunlar;

1. Bilgisayar sistemlerini devre dışı bırakmaktır;
2. Ele geçirdikleri sistemleri finansal kazanç için kullanmaktır.

2010 yılının Haziran ayında keşfedilen 'Stuxnet' solucanı, İran Natanz'da bulunan bir nükleer fabrikayı hedef almıştır. Bu saldırının arkasında devlet aktörlerinin bulunduğu düşünülmektedir. Devletler siber suçlar tarafından gelişimi sağlanan teknolojilere yatırım

yapmaktadırlar. Siber saldırı araçları, konvansiyonel askeri saldırı araçlarına göre daha büyük potansiyel taşımaktadır [5].

2013'ten günümüze ulus-devletler (nation-state) siber güvenlik alanında tanınmış bir mesele haline gelmişlerdir. 'Great Firewall of China' ve benzeri kötü niyetli yazılımların arkasında ulus-devletler bulunmaktadır. Tehdit İstihbaratı artık teknik bir sözcük olmaktan çıkmıştır. CrowdStrike gibi firmalar aralarında Çin, Rusya ve başka ülkelerin de bulunduğu gelişmiş tehdit aktörlerini (threat actor) açıklamışlardır. 2014 yılında CrowdStrike 39 farklı tehdit aktörü raporlamıştır. Rapor, tehdit aktörleri olarak; suçluları, hactivistleri, devlet destekli (state sponsored) grupları ve ulus-devletleri içermektedir. 2015 yılında veri sızıntıları (data breach) ve ulus-devlet saldırıları sonucunda Amerika Office of Personnel Management (OPM) bilgisayarlarından 20 milyon kişisel veri dosyası kaybedilmiştir. Çin tarafından ele geçirildiği düşünülen bu dosyalar, güvenlik belgesi başvurusunda bulunan insanların detaylı bilgilerini içerdiği için, Amerika'ya büyük bir zarar vermiştir [2].

Veri sızıntıları büyük finansal ve itibar kayıplarına neden olmaktadır. 24 Kasım 2014 tarihinde kendilerine 'The Guardians of Peace (GOP)' diye hitap eden bir grup Sony Pictures Entertainment firmasının sistemlerine sızmış ve 100 terabayt'lık veri sızdırmışlardır. Bu veri, firma için büyük önem taşıyan; sosyal güvenlik numaraları, maaş bilgileri, filmler, vb. bilgileri içermektedir. Sony için bu sızıntı 35 milyon dolara ve büyük itibar kaybına neden olmuştur [6].

Günümüze kadar yaşanmış olaylardan anlaşılabileceği üzere bilgi güvenliği günlük hayatın bir parçası haline gelmek zorundadır. Bilgi güvenliğinin ne olduğunu tanımlamak için ilk olarak temel güvenlik kavramlarının tanımı yapılmalıdır.

1.2.1. Temel güvenlik kavramları

Bilgi Sistemleri (Information Systems); bilginin toplanması, işlenmesi, bakımı, kullanımı, paylaşılması, yayılması ya da dağıtılması için bir araya getirilmiş bilgi kaynakları kümesidir [7]. İngilizce kaynaklarda data/information/knowledge terimleri birbirleri ile ilintili ama aynı değildir. Tam olarak bilinmediği zaman 'information' terimi kullanılmaktadır. Türkçe'de de veri/haber/bilgi içinde benzer şekilde 'bilgi' terimi kullanılmaktadır. Bu çalışmada da bu tanıma uyulmuştur.

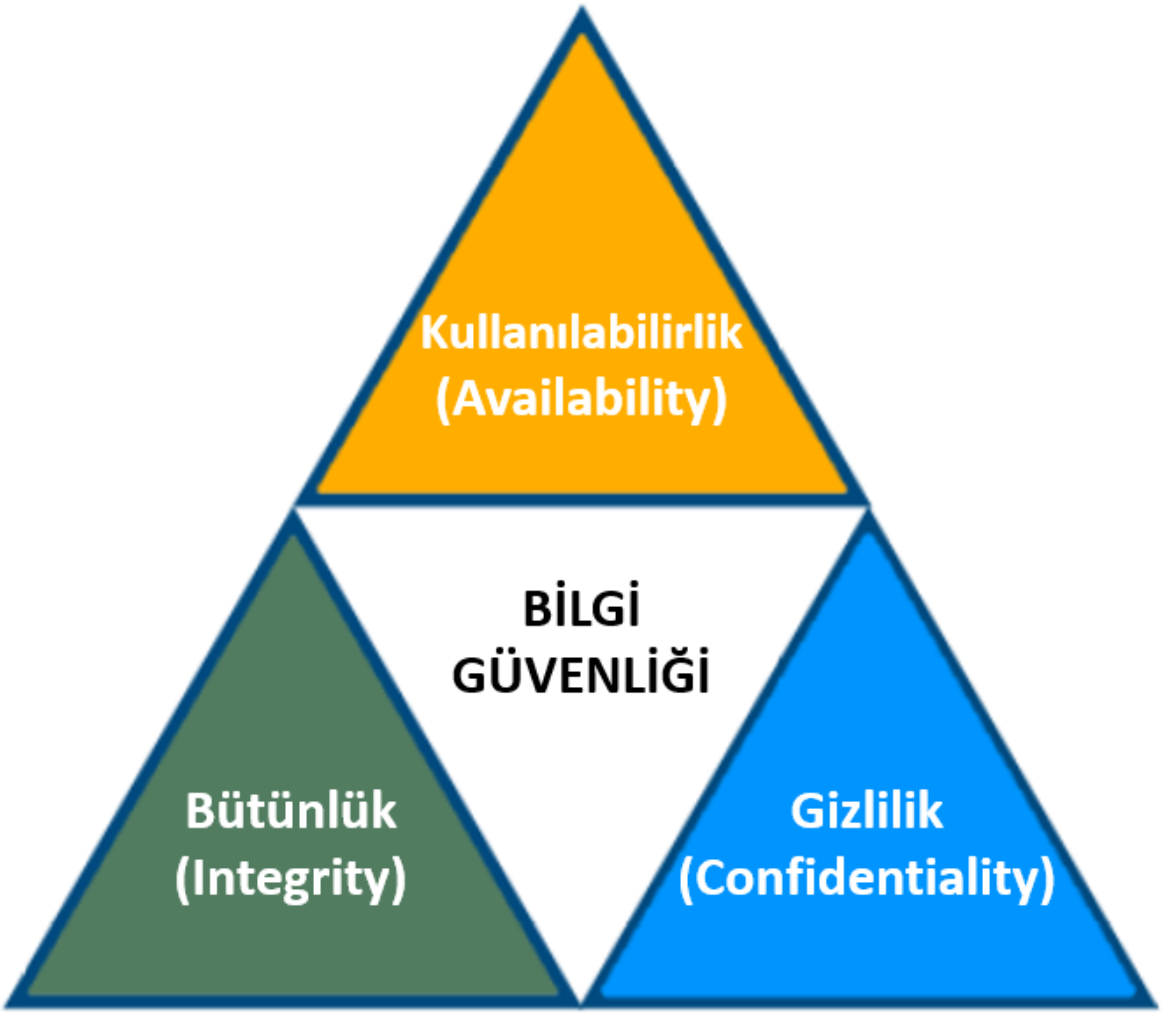
Aşağıda yer alan terimlerin tanımlanması önemlidir[1]:

[1] Bu terimler 6 Nisan 2015 tarihli CNSSI (Committee on National Security Systems (CNSS) Glossary) 4009'dan alınmıştır.

- **Bilgi:** İki şekilde tanımlanabilir;
    1. Farklı veri biçimlerinde ifade edilen fikir veya gerçekler.
    2. Herhangi bir ortam aracılığıyla sistemler arasında iletilebilen veri, komut vb. bilgiler (knowledge).
- **Bilgi Güvenliği:** Bilginin ve Bilgi Sistemlerinin gizlilik (Confidentiality), bütünlük (Integrity) ve kullanılabilirlik (Availability) sağlaması amacı ile herhangi bir izinsiz erişime, kullanıma, bilgi ifşa edilmesine, hizmet kesintisine, değiştirilmesine ya da yok edilmesine karşı korunmasıdır.
- **Gizlilik:** Kişisel verileri ve kuruma özel bilgileri korumak da dahil olmak üzere, veriye erişim yetkilerinin kısıtlanması ve bu kısıtlamaların istemsiz değişimlere karşı güvenliğinin sağlanmasıdır.
- **Bütünlük:** Verinin, usulsüzce değiştirilmeye ya da imha edilmeye karşı korunmasıdır. İnkar edilemezlik (non-repudiation) ve doğruluk (authenticity) kavramlarını da kapsar.
    1. **Veri Bütünlüğü:** Verinin saklanırken, işlenirken ve iletim halindeyken izinsiz bir şekilde değiştirilmediğinin gösterilmesidir.
    2. **Sistem Bütünlüğü:** Sistemin yetkisiz ya da kaza eseri değişikliğe maruz kalmadan, istenilen şekilde çalışması durumudur.
- **Kullanılabilirlik:** Bilginin ihtiyaç halinde erişilebilir ve kullanılabilir olmasıdır.
- **Güvenlik Kontrolleri:** Sistemin gizliliğinin, bütünlüğünün, kullanılabilirliğinin ve üzerinde bulunan verinin korunması ve aksi durumlara karşı önlem alınmasıdır.

Kurumların bilgi sistemleri üzerinde var olan bilgi, sürekli olarak tehdit altındadır. Günümüzde karşılaşılan siber tehditler çok karmaşık saldırı teknikleri içermektedir ve kurumlar için büyük tehdit oluşturmaktadır [8].

Bilgi güvenliğinin üç temel hedefi; gizliliğin, bütünlüğün ve kullanılabilirliğin sürekliliğini sağlamaktır. Birçok güvenlik kontrolü bu alanların bir ya da daha fazlasında bütünlüğü sağlamak için geliştirilmiştir. Bu üç temel hedef genelde CIA (confidentiality, integrity, availability) üçlüsü (Şekil 1.1) olarak adlandırılır. Sistem yöneticileri ve sahipleri bilgi güvenliğini sağlamak için gerekli olan kontrollerin uygulandığından emin olmalıdırlar [9]. Bu nedenle yukarıda kısaca bahsedilen bu üç temel hedefin detaylı tanımları aşağıda verilmiştir.



Şekil 1.1. CIA (Confidentiality, Integrity and Availability) Üçlüsü

- **Gizlilik:** Gizlilik mahremiyete benzeyen fakat aynı olmayan bir yaklaşımdır. Mahremiyet için gerekli bir bileşendir. Verinin yetkisiz kişiler tarafından erişiminin engellenmesidir. Gizliliğe örnek olarak banka ATM'sinden para çeken biri verilebilir. Bu kişi para çekerken kredi kartı numarası ve kart şifresini gizli tutmak isteyecektir. Aynı zamanda banka ATM'si de kişinin bankadan para çekmesi için gerekli olan hesap numarasını ve diğer bilgileri gizli tutmalıdır. Eğer para çekme işleminin herhangi bir adımında gizlilik bozulursa para çeken kişi ya da banka için kötü sonuçlar doğacaktır. Gizliliğin bozulmasına farklı örnekler olarak kişisel bir bilgisayarın kaybolması, parola girildiği sırada girilen parolanın başka bir kişi tarafından görülmesi, önemli bir e-posta eklentisinin yanlış kişiye gönderilmesi verilebilir [10].
- **Bütünlük:** Veri bütünlüğü güvenle ilişkilidir. Eğer sistemde olan bir verinin bütünlüğü garanti edilemiyorsa, o veriye güvenilemez. Sonuç olarak veri

bütünlüğüne önem veren kaynaklar belirlenmeli ve izinsiz değiştirilmeye karşı korumaya alınmalıdır. Bir örnek olarak *nix sistemlerde bulunan resolv.conf dosyası verilebilir. Bu dosya için gizlilik önemli değildir. Her kullanıcı dosyanın içeriğini görebilir fakat kullanıcılar yetkisiz bir şekilde bu dosyanın içeriğini değiştirememelidir. Bu dosya alan adlarının IP karşılıklarını bulmak için kullanılan DNS sunucuların yapılandırmasını tuttuğu için, dosya üzerinde izinsiz yapılacak bir değişiklik sonrası Internet sorgularının doğru şekilde çözümlenip çözümlenmeyeceği bilinemez. Sonuç olarak İnternet ile ilgili yapılan herhangi bir işleme güvenilemez. Bütünlük, veri hareket halindeyken de önemlidir. Verinin ağ üzerinde bir noktadan başka bir noktaya hareketi sırasında değiştirilememesi gerekmektedir [11].

- **Kullanılabilirlik:** Kullanılabilirlik, yetkili kişinin erişmek istediği kaynak ya da bilgiye kesintisiz ve zamanlıca erişebilmesidir. Örnek olarak banka hesaplarını çevrim içi şekilde kontrol etmek isteyen bir kişi, bankasının İnternet hizmetlerine erişebilmelidir. Eğer bankadan kaynaklı bir nedenden dolayı erişemezse, kullanılabilirlik etkilenmiş demektir. Bilgi güvenliği gözünden kullanılabilirlik, gizlilik ve bütünlük kadar önemlidir. Eğer bir nedenden ötürü istenilen veriye zamanlıca erişilemezse bunun maddi, sosyal, vb. etkileri olacaktır [12].

Temel güvenlik kavramlarına değindikten sonra bu kavramlara dayanarak oluşturulmuş olan güvenlik ilkelerinden bahsedilmesi gerekmektedir.

1.2.2. Temel güvenlik ilkeleri

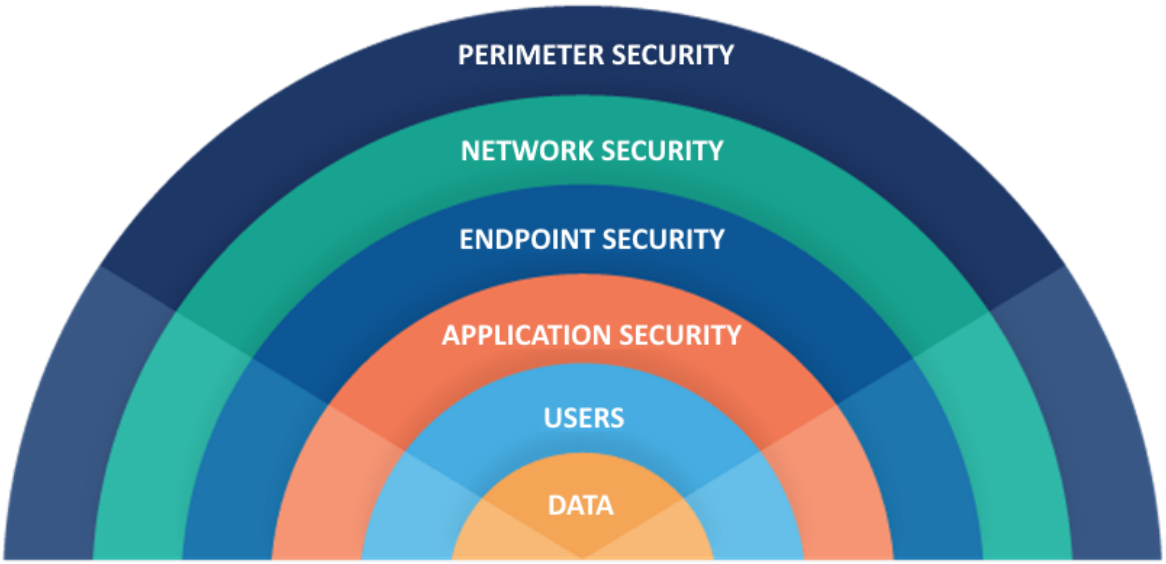
Bu ilkeler temel güvenlik kavramları üzerine kurulmuş güvenlik ilkeleridir. Bir sistemin veya kurumun güvenlik düzeyini yükseltmeyi hedefler. Temel güvenlik ilkeleri ve tanımları aşağıdaki gibidir:

- **En az yetki (Least Privilege):** Bu kavram bir kullanıcı ya da bir uygulamaya sadece çalışması için yetecek kadar yetki verilmesidir. Bu sayede güvenlik riskinin düşürülmesi hedeflenir. Bu yöntemi uygulamak saldırı yüzeyini küçültmenin bir yöntemidir. Sistem üzerinde yer alan her bileşende aynı şekilde sadece çalışmasına yetecek kadar yetkiye sahip olmalıdır. Eğer bir sistem bileşeni çok karmaşık ise bu bileşen önce daha basit parçalara bölünmeli daha sonra her bir yeni parçaya yetki tanımlaması yapılmalıdır. İnsanlar, uygulamalar ve sistem bileşenleri için gerekli olan en az yetkiyi belirlemek zor bir süreçtir ve çoğunlukla deneme yanılma yöntemine dayanır. Gereğinden fazla yetki vermek

işleri kolaylaştırıyormuş gibi görünse de saldırı yüzeyini büyük ölçüde arttırmaktadır [13]. Yetki bölümlemesi için bir örnek olarak kurum içinde yönetilen bir proje verilebilir. Proje yöneticileri projeye ait finans bilgilerine ve teknik bilgilere erişim sağlarken, proje mühendisleri sadece projenin teknik bilgilerine erişim sağlayabilirler. Kurumun diğer çalışanları ise proje ile ilgili herhangi bir bilgiye erişemezler.

- **Görevlerin Ayrımı:** Bir sistem üzerinde yetkili kişilerin görev alanları belirli olmalıdır. Kurumlarda sistem yönetme yetkisine sahip her kişinin görevi aynı olamayacağı gibi yetkileri de farklı olmalıdır. Bazı sistem yöneticileri bütün kurum çapında gerçekleşen operasyonlardan sorumluyken diğerleri sadece sistem üzerinde bulunan bir bileşenden sorumlu olabilir. Bu durumlarda kişilerin sorumlulukları doğru şekilde belirlenmeli ve yetkileri görevlerine göre tanımlanmalıdır [8]. Görev ayrımı aynı zamanda bir kurumda iş akışı üzerinde yer alan farklı noktalarda da olmalıdır. Örneğin bir finans biriminde fatura kesen kişi ile faturanın ödemesini yapan kişi ayrı olmalıdır. Eğer ayrı olmazsa, fatura kesen kişi hayali bir firmaya fatura kesip bunun ödemesini yaparak kişisel çıkar sağlayabilir ve çalıştığı kurumu mali sıkıntıya sokabilir.
- **Derinlemesine Güvenlik:** Güvenlik, farklı yöntemler bir arada kullanıldığı zaman daha verimli olmaktadır. Hiçbir güvenlik kontrolü mükemmel değildir. Derinlemesine Güvenlik ilkesi; farklı güvenlik uygulamalarının bir arada kullanılmasının ortalama güvenlik düzeyini arttıracağını ifade etmektedir. Bunun nedeni ise bir güvenlik uygulamasının gözden kaçırabileceği bir tehdidi, başka bir güvenlik uygulamasının yakalama ihtimali olmasıdır. Birbirinden bağımsız denetim yöntemleri olan güvenlik uygulamaları ile katmanlı bir savunma oluşturulması, zafiyetlerin istismar edilmesini güçleştirecektir. Derinlemesine Güvenlik katmanları Şekil 1.2'de gösterilmiştir [2].

[2] https://www.fairwarning.com/wp-content/uploads/2019/03/Defense-in-Depth-for-Cloud-Security-Rainbow-Diagram.png

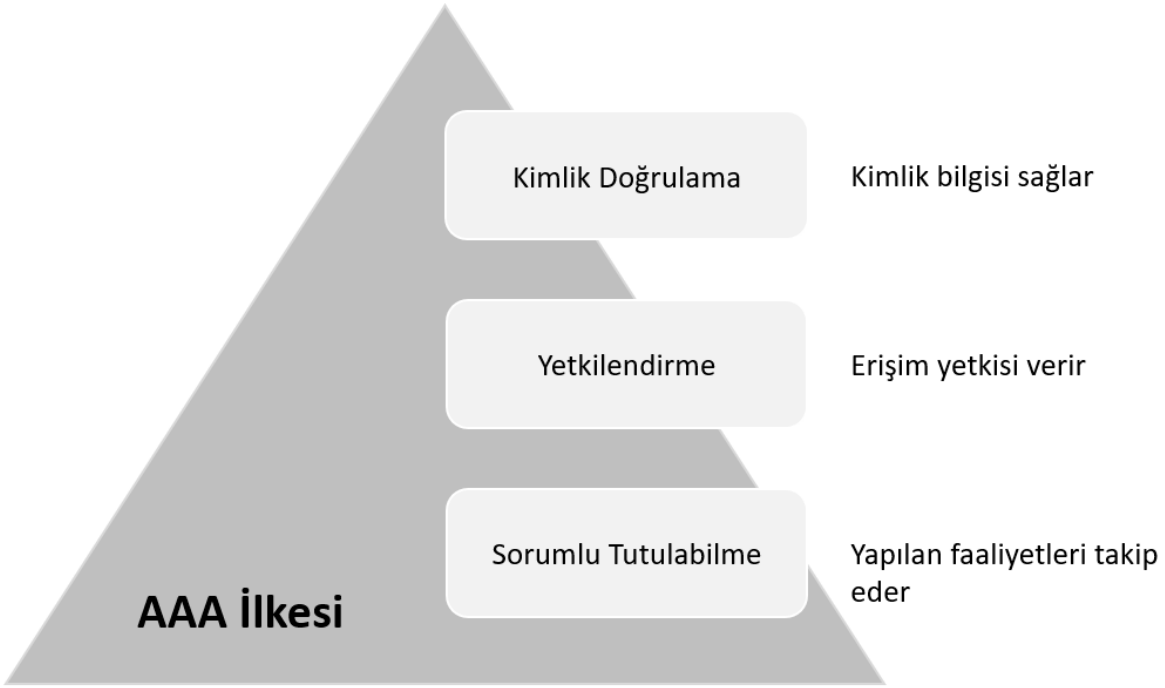


Şekil 1.2. Derinlemesine Güvenlik katmanları

- **İnkar Edilemezlik:** Bu ilke kişinin yaptığı bir işi inkar edememesini hedefler. Kayıtlar ve dijital imzalar inkar edilemezlik sağlamak için yaygın olarak kullanılan yöntemlerdir. Örnek olarak dosya dizini üzerinde kayıt tutan bir işletim sistemi verilebilir. Bahsi geçen kayıtlarda dosyalar üzerinde yapılan okuma, yazma ve silme işlemlerini bulmak mümkündür. Bu kayıtlar ayrıca yapılan işlemi kimin yaptığını da tutacağı için kişilerin hangi saatte dosya dizini üzerinde ne yaptığı tespit edilebilir. Dijital imzalarda benzer bir inkar edilemezlik sağlama yöntemidir. E-posta gönderilirken kişi bu postayı kendi dijital imzası ile imzalayabilir. Bu sayede gönderilen e-postanın kendisine ait olduğu inkar edilemez bir şekilde gösterilmiş olur [9].

- **AAA (Authentication, Authorization, Accountability):** AAA ilkesi erişim kontrol sistemlerinin üç temel servisini belirtir (Şekil 1.3) [9]. Bunlar; kimlik doğrulama (Authentication), yetkilendirme (Authorization) ve sorumlu tutulabilmedir (Accountability). Kimlik doğrulama, tanılama (identification) ve kimlik doğrulama olarak iki aşamadan oluşmaktadır. Tanılama; kişinin kendisine ait olan kimlik bilgisini (ör: kullanıcı adı) sisteme sunmasıdır. Kimlik doğrulama ise sunulmuş olan bu kimlik bilgisinin doğrulanmasıdır. Sisteme kullanıcı adı ve parola girişi tanılama ve kimlik doğrulama aşamalarını gösteren bir örnektir. Yetkilendirme; bir uygulamaya ya da kullanıcıya atanmış hakların ve yetkilerin tanımlanmasıdır. Bir sistem kullanıcının kimliğini doğruladıktan

sonra sistem üzerinde neler yapabileceğini belirlemek için kullanıcıyı yetkilendirir. Sorumlu tutulabilme; kullanıcıları ve uygulamaları yaptıkları işlemler ile eşleştirmektir. Sistem kayıtları sorumlu tutulabilme bileşenlerindendir [14].



Şekil 1.3. AAA (Authentication, Authorization and Accounting) İlkesi

Bilgi sistemleri ile ilgili temel kavramlarını tanımladıktan sonra, sistemlere yapılan saldırıların bu kavramları nasıl etkilediğini ve saldırganların kimler olduğunu incelemek gerekmektedir.

1.2.3. Saldırılar

Bilgi sistemlerine birçok farklı açıdan ve teknik kullanılarak saldırılar gerçekleştirilmektedir. Bu saldırılar incelendiği zaman dört farklı kategori altında sınıflandıkları görülmektedir. Bunlar; Dinleme (Interception), Kesme (Interruption), Değiştirme (Modification) ve Üretmedir (Fabrication). Her bir kategori altında yer alan saldırı, CIA üçlüsünden birini etkilemektedir. Bu etkileşim Şekil 1.4'te gösterilmiştir [10].

Yukarıda tanımlanmış dört kategorinin açıklamaları aşağıdaki gibidir [10]:

- **Dinleme:** Dinleme saldırıları; verilere, uygulamalara veya ortamlara yetkisiz kişilerin erişimine olanak veren saldırılardır ve öncelikli olarak gizlilik ilkesini hedef alırlar. Dinleme, yetki dahili dışındaki bir dosyayı inceleme ya da

kopyalama, telefon konuşmasına kulak misafiri olma, e-postayı okuma, vb. şekillerde olabilir. Dinleme veri saklanırken veya hareket halindeyken gerçekleşebilir.

Şekil 1.4. CIA üçlüsü ve saldırı kategorilerinin etkileşimi

- **Kesme:** Kesme saldırıları sahip olunan varlıkların (asset) geçici ya da kalıcı olarak kullanılamaz veya erişilemez hale gelmesini hedefler. Kesme saldırıları genellikle kullanılabilirlik ilkesini hedef alır fakat bütünlük ilkesini de etkileyebilmektedir. E-posta sunucusuna yapılan hizmet kesme saldırısı kullanılabilirlik ilkesini hedef almış olarak sınıflandırılabilir. Veri tabanı uygulamasında değişikliğe sebep olan ve veri tabanında tutulan verilere erişimi kısıtlayan bir saldırı ise bütünlük ilkesini hedef almış olarak sınıflandırılabilir.
- **Değiştirme:** Değiştirme saldırıları sahip olunan varlıkların istemsiz değişikliğe uğratılmasıdır. Bu saldırı temel olarak bütünlük ilkesini hedef alsa da kullanılabilirlik ilkesini de tehdit etmektedir. Eğer bir dosyaya yetkisiz erişim sonucunda dosya değiştirilirse, bu saldırı bütünlük ilkesini hedef almıştır. Benzer bir olayda yetkisiz erişim sonucunda değişen dosya bir internet hizmeti konfigürasyon dosyası ise bu değişiklik internet hizmetinde kesintiye neden olabileceği için kullanılabilirlik ilkesini hedef almış olur.

- **Üretme:** Üretme saldırıları bir sistemde veri, işlem, iletişim, vb. aktiviteler üretilmesidir. Üretim saldırıları temel olarak bütünlük ilkesini hedef almaktadır fakat kullanılabilirlik ilkesini hedef aldığı durumlar da olabilir. Bir veri tabanında sahte bilgiler üretilmesi bu saldırı tipinin bir örneği olarak verilebilir.

Yukarıda anlatılmış olan saldırıları gerçekleştiren kişiler günümüzde bilgisayar korsanları olarak bilinmektedir. Birçok kişiye göre bilgisayar korsanı terimi 1950'lerin sonunda ortaya çıkmıştır. Erickson [15] 'a göre bu terimin çıkış nedeni "MIT Model Rail Club" üyeleridir. Bu grubun üyeleri kendilerine bağış olarak verilen parçaları (çoğunlukla eski telefon parçaları) kullanarak tren yolunun farklı bölümlerinin farklı operatörler tarafından kontrol edilmesine olanak veren karmaşık bir sistem geliştirmiştir. Grup eski telefon parçalarının bu şekilde yaratıcı kullanımına korsanlık (hacking) adını vermiştir. Korsanları diğer programcılardan ayıran şey ise, yazdıkları kodun işi daha verimli yapması (daha az kaynak harcaması) ve kodun zekice (zarif) olması olmuştur.

Radziwill et al. [16] 'in makalesinde açıkladığı üzere "Bilgisayar Korsanı" terimi yıllar içinde evirilmiştir. Zamanında bu kavram yukarıda açıklanan içeriğe sahipken günümüzde genel anlamda bu kavram Beyaz Şapka ve Siyah Şapka olmak üzere ikiye ayrılmıştır. Beyaz Şapka yeteneklerini suç teşkil eden unsurlar için kullanmazken, Siyah Şapka yeteneklerini yasal olmayan işler için kullanır. Beyaz ve siyah şapka bilgisayar korsanı tanımları aşağıda verilmiştir.

- **Beyaz Şapkalı Bilgisayar Korsanları:** Amaçları kişilere/kurumlara zarar vermek olmayan, yasal yöntemleri kullanarak bilgi toplayan ve topladığı bilgiyi gerekli kişiler/kurumlar ile paylaşan kişiler/takımlardır. Jagnarine [17] 'in tezinde bahsettiği üzere Beyaz Şapkalı Bilgisayar Korsanlarının amacı sistemlerdeki açıklıkları bularak bu açıklıkların kötü niyetli kişiler tarafından istismar edilmeden önce yamalanmasını sağlamaktır. Harper et al. [18] 'e göre Beyaz Şapkalı Bilgisayar Korsanları bir etik anlayışı çerçevesinde saldırılarını gerçekleştirirler. Saldırılarının amacı düşmanlarını (test yapılan ortam) alt etmek değil, gerekli bilgiyi elde ettikten sonra bu bilgiyi yetkili kişilerle paylaşıp daha bilgili insanlar yaratmak ve daha güvenli sistemler oluşturmaktır.
- **Siyah Şapkalı Bilgisayar Korsanları:** Vacca [19] 'ye göre eskiden "Siyah Şapkalı Bilgisayar Korsanları" ismi saatlerini bilgisayar başında şöhret kazanmaya ya da birinden öç almaya adamış gençlere verilmiştir. Günümüzde ise bu isim amaçları şöhret ya da öç almak olmayan, bunun yerine bilgisayar başında yasadışı yöntemler kullanarak menfaat ve para kazanmaya çalışan

kişilere verilmiştir. Sabih [20] 'de bahsedildiği üzere "Siyah Şapkalı Bilgisayar Korsanları" sistemleri sadece kendi çıkarları için ele geçiren kişilere denmektedir. Erickson [15] 'a göre iyi Bilgisayar Korsanını kötü Bilgisayar Korsanından ayırmak için kırıcı (cracker) terimi türetilmiştir. Bilgisayar Korsanları etik kurallarına bağlı kalırken, kırıcılar kanunları çiğneyip maddi menfaat elde etmektedirler.

Kötü niyetli saldırganlar artık sadece eğlenmeyi ya da ün kazanmayı hedeflememektedirler. Amaçları saldırılarından maddi menfaat elde etmektir. Buna örnek olarak 2009 yılında bir Rus bilgisayar korsanı grubunun Citibank'tan bir kötücül yazılım (malware) aracılığı ile çaldığı onlarca milyar doları örnek verebiliriz[3]. 2008 yılında Symantec var olan kötücül yazılımların gelişme hızına yetişmek için her 20 saniyede bir yeni bir kötücül yazılım imzası yazmak zorunda kalmışken bu rakam 2009 yılında her 8 saniyede bire düşmüştür.

Genel anlamı ile saldırılara değindikten sonra daha detaylı kavramlara değinmeden varlık, zafiyet ve istismar kavramlarının açıklanması faydalı olacaktır.

1.2.4. Varlık, zafiyet ve istismar

Bu kavramlar Baloch [21] 'un bahsettiği şekilde aşağıda aktarılmıştır:

- **Varlık:** Bir varlık, verilere erişmesine izin verilen kişilerin dışında herhangi birinden korunması gereken, bilgi ile ilgili faaliyetleri destekleyen herhangi bir veri, cihaz veya ortamın diğer bileşenidir.
- **Zafiyet:** Zafiyet, varlıkların içinde yetkisiz erişim sağlamak için kullanılabilecek bir kusur veya zayıflık olarak tanımlanır. Bir zafiyetin başarılı bir şekilde istismar edilmesi, veri değiştirilmesine, yetki arttırılmasına vs. neden olabilir.
- **İstismar:** İstismar, bir varlık üzerinde istenmeyen veya beklenmeyen değişikliklere neden olarak hedef üzerinde yetki kazanmayı amaçlayan aksiyondur.

Güvenlik ile ilgili yeterli altyapıyı oluşturduktan sonra günümüzde sıkça bahsedilen siber kavramının güvenlik ile nasıl birleştiğine bakılmalıdır ve bu birleşim sonucunda ortaya çıkan siber güvenlik kavramı incelenmelidir. Siber güvenlik kavramını tanımlamak için

[3] https://www.theguardian.com/technology/2009/dec/22/russian-hackers-citigroup-cyber-security

aşağıda bu kavramı oluşturan öğeler tanımlanmıştır. Bu öğeler; Siber Uzay, Siber Saldırı ve Siber Tehdit Yüzeyidir.

1.2.5. Siber uzay

İlk olarak William Gibson tarafından 1982 yılında yazılmış olan 'Burning Chrome' isimli kısa hikayede ortaya çıkmıştır. 'Siber' Yunan 'kybernetes' kelimesinden gelmektedir ve pilot, yönetici ve hükümdar anlamını taşımaktadır. Günümüzde bilgisayar ağlarının oluşturduğu sanal uzayı ifade etmek için kullanılmaktadır. Gibson, Neuromancer romanında siber uzayı; saf bilginin bilgisayar ve bilgisayar öbeklerinin (cluster) oluşturduğu üç boyutlu düzlemde hareketi olarak hayal etmiştir. Gibson'ın hayal ettiği bu yapı; bilgisayarları hem işlem hem de iletim aracı, insanları bilgi üreten ve tüketen varlıklar ve saf bilgiyi ise birbirinden bağımsız iletim araçlarında hızla ilerler olarak tanımlar. Bilgi, iletim araçları üzerinde bulunan protokol adı verilen yazılımlar sayesinde kaynaktan hedefe doğru hareket eder [22].

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından yayınlanan '2016-2019 ULUSAL SİBER GÜVENLİK STRATEJİSİ' dokümanına[4] göre siber uzay aşağıdaki şekilde tanımlanmaktadır:

"Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamıdır."

Nesnelerin İnterneti de (IoT) günümüzde siber uzayın bir parçası olmuştur. Akıllı cihazların hayatımızdaki etkilerinin artması ile vazgeçilmez hale gelen bu cihazlar, siber uzay unsurlarını yoğun şekilde kullanmaktadır.

1.2.6. Siber saldırı

Siber Uzay olanakları kullanılarak yapılan saldırıdır. Hizmet kesmek, veri sızdırmak, finansal zarara uğratmak vb. amaçları olabilir. Birçok siber saldırı büyük tehdit oluşturmasa da bazıları insan hayatını etkileyebilecek ölçüde tehlikelidir. Günümüzde siber tehdit yüzeyinin hızla artmasından dolayı, siber saldırılar ICT yaşam döngüsünün gündelik bir parçası haline gelmektedir. Botnet saldırıları bir rutin haline gelmişken hizmet kesme

[4] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

saldırıları çok yaygın şekilde yapılmaktadır. Siber tehdit yüzeyini açıklamadan önce değinilmesi gereken önemli bir konu bulunmaktadır: hedefli siber saldırılar.

İnternete açık ağların ve teknolojilerin istismar edilerek istihbarat toplanması gündelik olaylar halini almıştır. Bu saldırılar kurum bilgilerinin çalınması, espiyonaj, kritik altyapıların zarar görmesi vb. gibi sonuçlar doğurmaktadır. Anlatılan benzeri bir saldırı yapmak için fiziksel bir yakınlaşma gerekmediği için stratejik ve taktiksel açıdan siber saldırıların geleceğin savaş alanını değiştireceği düşünülmektedir. Günümüzde birçok ulus-devletin siber savaş kabiliyeti bulunmaktadır. Sıfır-gün (Zero-Day) zafiyetleri, rakibin altyapısını ele geçirmek ya da çalışmasını aksatmak için kullanılabilecek silahlar haline gelmiştir [23].

Bu noktada siber saldırılar için büyük önem arz eden sıfır-gün açıklıklarından bahsetmek faydalı olacaktır. Libicki et al. [24], Sıfır-Gün açıklıklarını henüz yamaları yayınlanmamış yazılım zafiyetleri olarak tanımlamıştır. Sıfır-gün terimini ise, yazılım sahibinin zafiyetten haberdar olduğu gün sayısı olarak belirtmiştir. Saldırganlar sıfır-gün açıklıklarından faydalanarak güvenlik seviyesi üst düzeyde olan kurumları hedeflemektedirler. Bu kurumlar en güncel yamaları sistemlerine uygulayan ve verilerine en iyi şekilde sahip çıkan kurumlar olarak tanımlanabilir. Bu nedenle sıfır-gün açıklıkları; saldırganların, orduların ya da hükümetlerin siber operasyonlarında büyük rol oynamaktadır [25].

Enbody and Sood [23], ülkelerin istihbarat teşkilatlarının tanımlanan sıfır-gün açıklıklarına milyonlarca dolar yatırdıklarını ve Amerika'nın en büyük siber silah alıcısı olduğunu ifade etmiştir. Buna ek olarak yasal firmaların sıfır-gün açıklıkları bulup, buldukları açıklıkları büyük paralar karşılığında hükümetlere sattıklarını belirtmiştir. Ulus-devletler hedefli siber saldırılar için hazırlık yaparken siber uzayda yalnız değillerdir. Hedefli siber saldırılar dünya üzerinde bulunan birçok farklı kurum, kuruluş ya da saldırgan tarafından da gerçekleştirilmektedir.

Siber tehdit yüzeyinin tanımına geçmeden, siber saldırı yapmak için kullanılan zafiyetlerle ilgili bir tanımı daha vermekte fayda vardır: zafiyet envanteri. Ablon and Bogart [25], genel kanı olarak iki çeşit zafiyet olduğu görüşü yaygın olsa da bu görüşün gerçeği çok fazla basite indirgediğini belirtmektedir. Bahsedilen iki zafiyet çeşidi: (1) özel kullanım için bilgisi saklı tutulan zafiyetler ve (2) halka açık zafiyetlerdir. Şekil 1.5'te zafiyet çeşitleri gösterilmektedir [25].

Şekil 1.5. Zafiyet Çeşitleri ile İlgili Genel Kanı

1.2.7. Siber tehdit yüzeyi

Dulaney and Easttom [26] 'a göre bir uygulamanın siber tehdit yüzeyi, o uygulamaya yetkili ya da yetkisiz kullanıcıların erişebildiği alanlardır. Bu alanlar servisler, protokoller, ara yüzler ve kodun kendisi olabilir. Santanam [27] 'a göre ise bilgisayarlarda uygulamalara saldırganların erişimi olan kısmı hedef teşkil etmektedir. Kodun bir kısmı ya da uygulamanın bir parçası dış dünyaya ara yüzler vasıtasıyla açık olabilir ve bu açık kısımlar saldırıların hedefidir. Bir uygulamanın siber tehdit yüzeyi; kullanıcıların erişebildiği kod, ara yüz, servis ve protokollerin birleşimidir. Örneğin kurumun dışarı verdiği bir FTP servisi kurum için bir tehdit yüzeyi oluşturur çünkü bu servis saldırganlar tarafından istismar edilebilir. Benzer şekilde yeterli güvenlik önlemleri ile korunmayan bir uç nokta, kullanıcı hatası nedeniyle saldırganlar tarafından ele geçirilebilir ve bir tehdit yüzeyi haline gelebilir. Siber tehdit yüzeyi kavramı önemlidir çünkü her geçen yıl yeni teknolojiler eklenmesiyle beraber kurumların siber tehdit yüzeyi genişlemektedir.

Siber uzayı ve siber saldırıları daha detaylı bir şekilde tanımlamak için varlık, zafiyet ve istismar tanımlarının yapılması gerekmektedir.

1.3. Çalışmanın Yapısı

Bu tez çalışmasında önce siber uzay ortamında var olan saldırılar ve tehditler anlatılmıştır. Bu kavramların anlaşılabilmesi için bir temel oluşturmak adına literatür taraması yapılmış ve temel kavramlar tezin başında sunulmuştur. Temel kavramların anlatılmasının ardından siber farkındalığın tanımı yapılmış ve siber uzay ortamında var olan

tehditler anlatılmıştır. Bahsedilen tehditlerin anlatımı sırasında güncel olan güvenlik ve tehdit raporlarından yararlanılmıştır.

Siber uzay ortamında yer alan tehditler belirlendikten sonra bu tehditlerin nasıl tespit edilebileceği anlatılmıştır. Bu anlatım sırasında yine literatür kaynaklarından yararlanılmış ve sanallaştırma teknolojileri yardımıyla farklı bir test ortamı kurulmuştur. Kurulan test ortamlarında siber saldırılar gösterilmiş ve saldırı tespiti için kullanılan araçlara ait çalışmalar yapılmıştır.

Siber saldırıların önlenmesi aşamasında ise güncel uygulamalar saptanmış ve bu uygulamaların örnekleri sunulmuştur.

Son olarak anlatılan bütün kavramların bir arada kullanılabileceği bir eğitim ortamının tasarımı öneri olarak sunulmuştur. Bu öneri ile hedeflenen amaç siber farkındalığın arttırılması için bir çalışma ortamı sağlanması ve güvenli bir ortam üzerinde siber yeteneklerin geliştirilmesidir.

2. SİBER FARKINDALIK

Bilgi güvenliğinin en önemli parçalarından biri kullanıcılardır. Kullanıcılar, gündelik yaşamlarının bir parçası olan bilgi sistemlerini kullanırken belirli kurallara uymaları gerektiğini bilseler bile bu kurallara uymazlar. Schroeder [28] 'in bahsettiği üzere kullanıcılar bu sistemleri kullandıkları süre boyunca çeşitli alışkanlıklar geliştirmişlerdir. Örnek olarak 20 seneyi aşkın süredir İnternet hesapları kullanan kullanıcılar verilebilir. Büyük olasılıkla bu kullanıcılar, kullanıcı adı ve parolalarını hatırlamak için bir yöntem geliştirmişlerdir ve büyük olasılık ile bu yöntem çalıştıkları kurumun güvenlik politikalarına uymamaktadır. Benzer bir örnek olarak kullanıcıların uzun yıllar boyunca e-postalara ve anlık mesajlaşmalara cevap verme alışkanlıkları verilebilir. Kullanıcı, her ne kadar kurum adına bir e-postaya cevap verirken kurum güvenlik politikalarına dikkat etmesi gerektiğini bilse de alışkanlıkları nedeniyle her zaman güvenlik politikaları çerçevesinde cevap verememektedir. Kötü alışkanlıkların bilgiyi ve mantığı yenmesi küçümsenecek bir problem değildir. 2015 yılında A.B.D. Anayurt Güvenliği (Homeland Security) Departmanı CISO'su (Chief Information Security Officer) Paul Beckman'ın yaptığı açıklamaya göre; kullanıcılara bir oltalama saldırısı tatbikatı sırasında gönderdikleri e-postalar tamamen gerçek dışı olsa bile, kullanıcılar hâlâ tuzağa düşmüşlerdir. Tuzağa düşen kullanıcılar defalarca farkındalık eğitimi almış olsalar bile alışkanlıklar bilginin önüne geçebilmektedir.

Her ne kadar alışkanlıklar bilginin önüne geçse de kullanıcıları bilgilendirmek saldırganlara ve saldırılara karşı çok güçlü bir önlemdir. Bahsi geçen bilgilendirme siber farkındalık bölümü altında toplanmıştır. Bu bölümün amacı farkındalığın ne olduğunun tanımlanması, nasıl sağlanacağının anlatılması, bilgi güvenliğini tehdit eden siber tehditlerin açıklanması ve sistemlere yapılan saldırıların nasıl gerçekleştiğinin gösterilmesidir.

İlk olarak siber farkındalığın tanımı yapılacaktır.

2.1. Siber Farkındalık Nedir?

INFOSEC [29] makalesinde belirtildiği üzere, siber farkındalık, bir kurumun yapacağı en önemli yatırımlardan biri sayılmaktadır. Siber farkındalık kurum çalışanlarının bilgi güvenliği hakkında eğitilmesi sürecidir. Bu süreç aşağıdakileri kapsamaktadır:

- Kurum çalışanlarını eğitmek için eğitim programları hazırlanması,
- Kurum güvenlik kurallarına uymak için kişisel sorumluluk bilinci oluşturulması,
- Yukarıda bahsedilen konuların ölçülebilir şekilde denetlenmesi.

IFOSEC [29]'ye göre eğitim programlarının hazırlanması siber güvenlik farkındalığı yaratmak için ana bileşendir. Kurum çalışanlarının güvenlik kurallarına uyumunun takip edilmesi ve kurumun güvenlik seviyesinin arttırılabilmesi için kurallara uymayanların hesap verebilmesi de eşit derece önem taşımaktadır. Siber farkındalık dört aşamadan oluşmaktadır. Bunlar aşağıdakilerdir:

1. Mevcut durumun belirlenmesi,
2. Bir güvenlik farkındalığı programının geliştirilmesi ve içeriğinin hazırlanması,
3. Çalışanların söz konusu programa atanması,
4. Çalışanların, eğitim programı sayesinde gelişiminin ölçülmesi ve gerektiğinde gözden geçirilmesi.

Kurumlarda siber farkındalık yukarıdan-aşağı yaklaşımını benimsemelidir. Günümüzde oltalama saldırılarının hedefinde genelde kurumların üst düzey yetkilileri bulunmaktadır. Bu nedenle siber farkındalık kurumlarda en üst düzeyden başlayıp en alt düzeyde yer alan çalışanlara kadar verilmelidir. Kurumlar çalışanlarında bu farkındalığı yaratabilmek için belli bir bütçe ayırmalıdır. Kurumların siber farkındalık yaratmak için ayırdıkları bütçelere bakılarak bu konuya ne kadar önem verdikleri anlaşılabilir.

2.2. Siber Farkındalık Nasıl Sağlanır?

Yukarıda da bahsedildiği üzere siber farkındalık sağlanması için kurumların güvenlik politikaları, standartları, yönergeleri, prosedürleri ve çalışan eğitim programları olmalıdır. Ayrıca sürekli denetlemelerle kurumun güvenlik düzeyi tespit edilmeli ve gerekli düzenlemeler yapılmalıdır. Aşağıda eğitim programları ile kurum güvenlik politikaları detaylandırılmıştır.

2.2.1. Eğitim

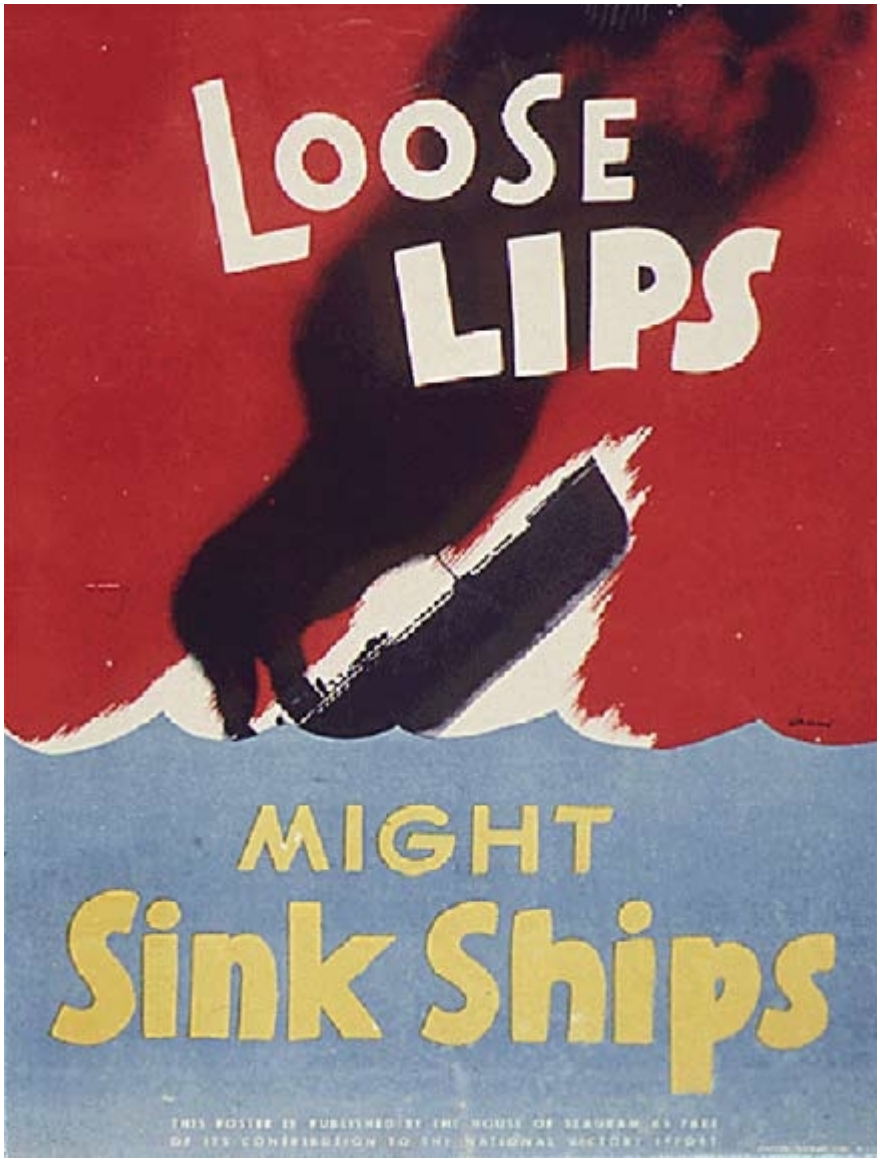
Eğitim içeriği değişken olsa da siber farkındalık eğitimleri kurum çalışanlarını siber tehditlere karşı bilinçlendirmeyi hedefler. Siber tehditler ve tanımları gelecek bölümlerde yapılmıştır. Bu başlık altında siber farkındalık eğitimlerinin kurum içinde hangi yöntemler ile verilebileceği anlatılmıştır.

Siber farkındalık eğitim içeriği hazırlanılması ve sunulması için birkaç farklı yöntem bulunmaktadır. Bu yöntemler resmi ve resmi olmayan olarak iki kategoriye ayrılmaktadır. Resmi eğitimler; yüz yüze eğitim, bilgisayar tabanlı eğitim ve internet tabanlı eğitimdir.

Resmi olmayan eğitimler ise öğle yemeği ve öğrenme oturumları, kurum tarafından çekilmiş videolar ve posterlerdir [30].

Yüz yüze eğitim ya da eğitmen ile eğitim en geleneksel eğitim yöntemi kabul edilmektedir. Bu eğitim kurum için konuya özel olarak hazırlanmış yansıların sunulmasını içerir. Yansılar; videolar ve konu ile ilgili olayların anlatımı ile güçlendirilir. Eğitime katılan çalışanların etkileşimde bulunması için onları teşvik etmek, eğitimin başarı oranını arttıran bir yöntemdir. Örnek olarak katılımcılara farklı e-postalar gösterip, gösterilenler arasında hangisinin bir oltalama e-postası olduğunun sorulması, katılımcıların konuya hakimiyetini arttıracaktır. Bilgisayar tabanlı eğitim, günümüzde yaygınlaşmaya başlamış bir eğitim yöntemidir. Bir bilgisayar aracılığı ile verilen eğitim ses, video, etkileşimli sınavlar, vb. birçok yöntem kullanılarak konunun anlatılmasına olanak sağlamaktadır. Eğitim içeriği genel olarak kurumun ihtiyaçları doğrultusunda hazırlanır ve taşınabilir bir ortamda kurumlara teslim edilir. İnternet tabanlı eğitimler, bilgisayar tabanlı eğitimlerde olduğu gibi bilgisayar aracılığıyla yapılmaktadır. İçerik bir eğitim ortamı üzerinden çevrim içi olarak sunulacağından eğitim küçük parçalar halinde ve hedef kitleye yönelik verilebilir. Örnek olarak yardım masası için hazırlanan içerik ile satış danışmanları için hazırlanan içerik birbirinden farklı olabileceği gibi sadece oltalama saldırılarına yönelik bir eğitim vermek de örnek olarak verilebilir [30].

Resmi olamayan eğitimleri açıklamak için öğle yemeği ve öğrenme oturumlarından başlamak faydalı olacaktır. Bu oturumların süreleri kısa tutulur ve gönüllülük esasına göre katılım sağlanır. Amaç katılımcıların dikkatini çekecek bir konu üzerinde bilgi paylaşmaktır. ‘Çocuklarınızı çevrim içi ortamda nasıl korursunuz?’ benzeri bir başlık bahsi geçen oturumlar için bir örnektir. Kurum tarafından çekilmiş videolar ise kurumun yerel ağından sunulur ve resmi eğitim yöntemleri ile öğrenilmiş bilgileri destekler. İçerik hazırlama aşamasında kurum çalışanlarından yardım alınarak, onlarında farkındalık eğitiminin bir parçası olması sağlanabilir. Posterler ise iyi güvenlik uygulamalarını pekiştirmek için kullanılan düşük bütçeli bir yöntemdir. Bir posterin içeriğini başarılı bir şekilde aktarabilmesi için önemli olan iki unsur içerik ve yerleşimdir. İçerik olarak çok az kelime içermeli ve mesajı açık olmalıdır. İkinci dünya savaşı sırasında Amerika tarafından kullanılan “gevşek dudaklar gemileri batırabilir” posteri (Şekil 2.1) iyi bir poster örneğidir [30].



Şekil 2.1. İyi bir poster örneği[5]

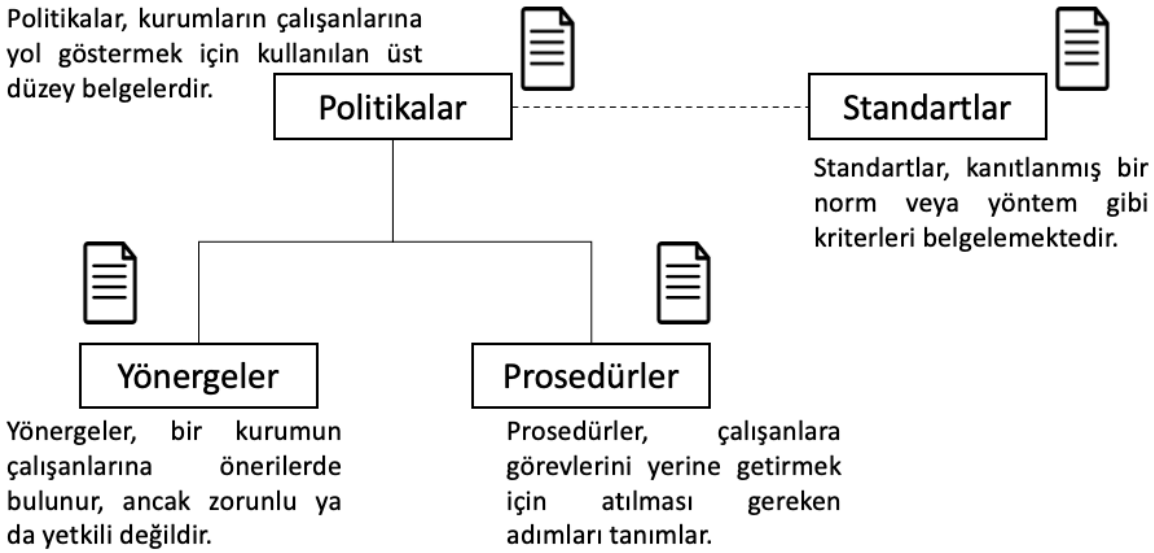
2.2.2. Politikalar, standartlar, yönergeler ve prosedürler

Landoll [31] 'ye göre güvenlik politikaları, kurumların bilgi güvenliği ile ilgili en üst seviye bilgiyi içeren dokümanlarıdır. Bu politikalar, genel güvenlik programı, sistem kontrolleri ve kullanıcı davranışı beklentilerini içerir. Kuruluşun üst yönetimi tarafından onaylanır ve yayınlanır. Bilgi güvenliği politikaları zorunludur, çünkü tüm bilgi sistemleri ve kullanıcıların politika beyanlarına uyması beklenir. Örnek bir politika maddesi olarak aşağıdaki cümle verilebilir:

[5] https://upload.wikimedia.org/wikipedia/commons/f/f8/Loose_lips_might_sink_ships.jpg

"Kurum, bütün bilgi sistemlerinin, amacına uygun şekilde kullanılabilmesi için gerekli kimlik doğrulama mekanizmalarının uygulandığını garanti etmelidir."

Gibson [9] 'e göre ise politikalar, kurumların çalışanlarına yol göstermek için kullanılan üst düzey belgelerdir. Politika, çalışanlara yön verir ve doğası gereği yetki sahibi bir belgedir. Standartlar, kanıtlanmış bir norm veya yöntem gibi kriterleri belgelemektedir. Genellikle kurum tarafından belirlenmez, ancak kurumun politikalarını, yönergelerini ve prosedürlerini etkileyebilir. Yönergeler, bir kurumun çalışanlarına önerilerde bulunur, ancak zorunlu ya da yetkili değildir. Prosedürler, çalışanlara görevlerini yerine getirmek için atılması gereken adımları tanımlar. Bahsi geçen belgeler arasındaki ilişki Şekil 2.2'de verilmiştir [9].



Şekil 2.2. Politikalar, standartlar, yönergeler ve prosedürler

Landoll [31], güvenlik politikalarının, kurumsal seviye, bilgi güvenliği programı seviyesi, kullanıcı seviyesi ve sistem seviyesi politikalardan oluştuğunu ifade etmiştir. Kurumsal düzeyde bilgi güvenliği politikaları, genel bilgi güvenliği programını ve verilerin hassasiyetini ele alır. Bilgi Güvenliği Programı politikasında, üst yönetim bilgi güvenliği programının gerekli unsurlarını belirler, sorumluluklar atar ve gözetim kontrolleri oluşturur. Sistem Sınıflandırma Politikasında, üst yönetim, verilerin hassasiyeti ve sistemin kritikliğine bağlı olarak hem veri hem de bilgi sistemleri için sınıflandırma düzeylerini tanımlar.

Güvenlik politikaları aşağıdaki adımlardan geçerler [9]:

- **Başlangıç aşaması:** Güvenlik politikası kuruluşun ihtiyaçlarına göre hazırlanır. Bu çalışma neredeyse tamamlanmış bir taslak veya üst yönetimin görüşüne sunulacak bir teklif halinde olabilir.

- **Onay aşaması:** Üst yönetim politikayı onaylar. Üst yönetimin onayladığı bir belge oluşturmak için başlangıç aşaması ile onay aşaması arasında birkaç yineleme gerekebilir. Onaylandıktan sonra, kurum çalışanlarına politikayı uygulaması için yönlendirme sağlar.
- **Yayın aşaması:** Politika ilgili kurum yetkilisine teslim edilir, böylece yetkili kişi politikayı uygulayabilir ve takip edebilir.
- **Uygulama aşaması:** Güvenlik politikası kurumda güvenlik sağlamak için önemli bir ilk adımdır ama kesinlikle son adım değildir. Üst yönetimin onayladığı güvenlik politikasının uygulanması ve zorunlu kılınması için kurum içinde gerekli çalışmalar yapılmalıdır.
- **Bakım aşaması:** Dönemsel takipler ile yayınlanmış güvenlik politikalarının güncelliğinin korunması ve güncel tehditleri içermesi sağlanmalıdır.

Siber farkındalığın ne olduğu ve nasıl sağlandığı tanımlandıktan sonra siber tehdit tanımı yapılmalı ve tehditlerin neler olduğu açıklanmalıdır.

2.3. Siber Tehditler Nelerdir?

Siber uzay alanında en yetkin ülkelerden biri Amerika Birleşik Devletleridir. NIST (National Institute of Standards and Technology), Amerika Birleşik Devletleri'ndeki en eski fiziksel bilim laboratuvarlarından biridir. Çeşitli endüstriler ve alanlarda devlet kurumları için standartlar önerilmesine odaklanmaktadır. Blank and Gallagher [32] 'da yazdığı üzere NIST siber tehdidi şu şekilde tanımlamıştır:

"Kurumsal işleyişi ve varlıkları, bireyleri, diğer kuruluşları veya ulusal bilgi sistemleri üzerinden yetkisiz erişim, imha etme, ifşa etme, veri değiştirme veya hizmet reddi yoluyla olumsuz yönde etkileme potansiyeli olan herhangi bir durum veya olaydır".

Siber tehditler; tehdit kaynakları tarafından yapılan tehdit eylemleridir. Bir tehdit kaynağı şöyle tanımlanır [32]:

- Bir güvenlik açığından yararlanılmasını hedefleyen niyet ve yöntem veya,
- Yanlışlıkla bir güvenlik açığından yararlanabilecek bir durum ve yöntem.

Tehdit kaynağı türleri şunlardır:

- Siber veya fiziksel saldırılar,
- İnsanların ihmalkarlıkları,
- Kurum tarafından idame edilen kaynaklarda yaşanacak yapısal hatalar (ör: donanım, yazılım, çevresel kontroller),

- Kurumun kontrolü dışındaki doğal ve insan kaynaklı felaketler, kazalar ve başarısızlıklar.

Dulaney and Easttom [26] 'a göre tehdit; kaynaklara zarar verebilecek herhangi bir şeydir ve üç türü vardır:

- **Çevresel:** Çevresel tehditler; su baskınları, hortumlar, fırtınalar, vb. doğa olaylarıdır. Örnek olarak; kurumun bulunduğu bina başka bir kurum ile paylaşılıyorsa ve diğer kurum katında çıkan bir yangın, sistem odasında bulunan yangın söndürme sistemini harekete geçirip sunucuları su baskınına maruz kalmasıdır.
- **İnsan Yapımı:** Bir kişinin elindeki çakmağı halka açık bir alanda yer alan yangın alarmını tetiklemek için kullanıp, sunucu odasını sular altında bırakması insan yapımı bir tehdide örnek olarak verilebilir.
- **İç ve Dış Tehditler:** Eğer tehdit unsurunu oluşturan kişi kurumun bir çalışanıysa iç tehdit değil ise dış tehdit olarak tanımlanır.

Genel anlamda tehdit tanımı yaptıktan sonra siber uzayda sıkça gözlemlenen siber tehditlerin neler olduğunun açıklanması faydalı olacaktır.

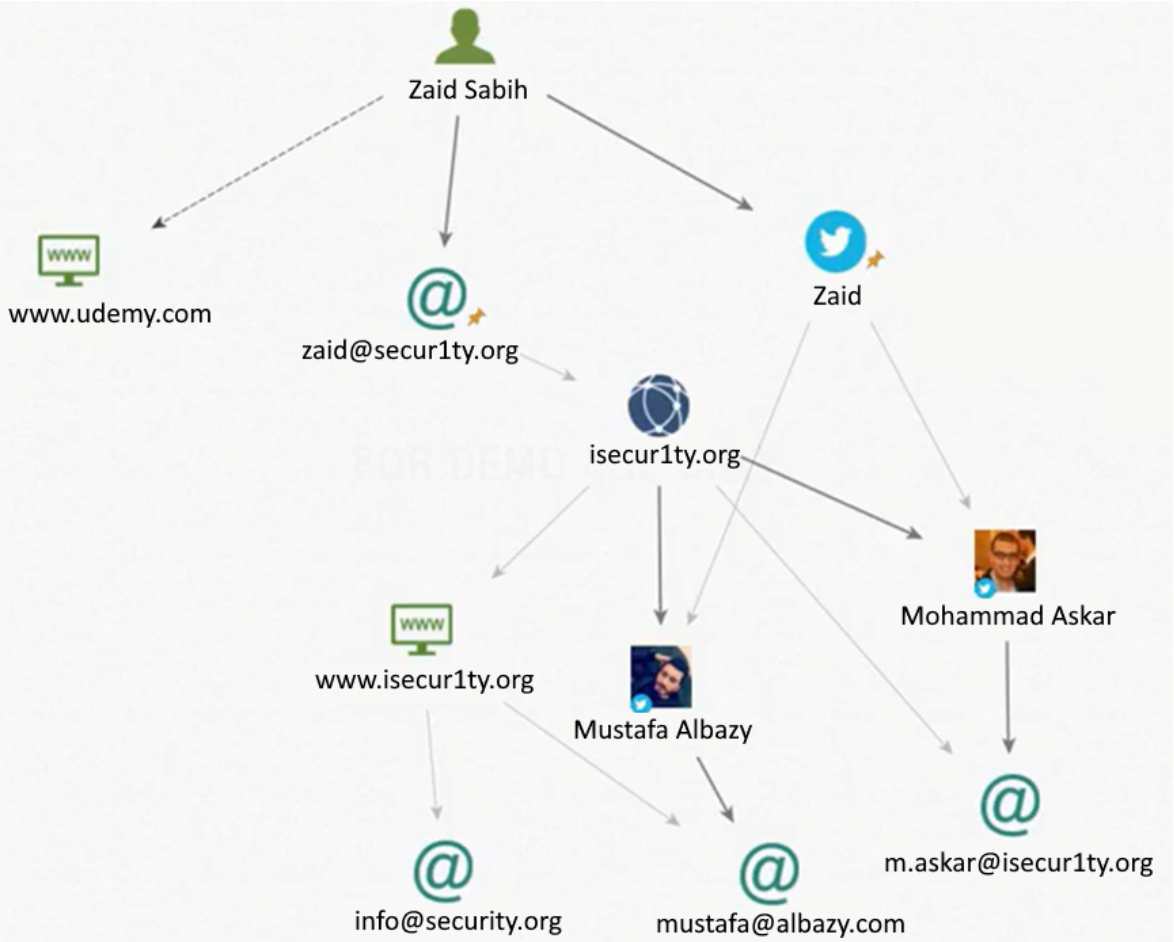
2.3.1. Sosyal mühendislik

Neil [33] 'e göre sosyal mühendislik saldırıları, birinin kişiliğinin sömürülmesine dayanır. Çeşitli yöntemler kullanarak insanlardan gizli bilgi elde etmeye ya da insanları güvenlik ihlali yapmaya yönlendirmeye verilen genel isimdir. Sabih [20] 'e göre ise sosyal mühendislik geniş bir kavramdır; saldırı tipi hedefe bağlı olduğu için yapılabilecek çok fazla saldırı vardır. Sosyal mühendislik saldırıları kurban hakkında yeterli bilgi toplamaya dayanmaktadır. Bu bilgileri toplamak için açık kaynaklı bilgi istihbaratı verilerinden yararlanılabileceği gibi fiziksel bir çalışma da yapılabilir. Fiziksel çalışmalara örnek olarak çöp karıştırma (dumpster diving) ve omuz üzerinden izleme (shoulder surfing verilebilir) verilebilir. Neil [33] çöp karıştırmayı ve omuz üzerinden izlemeyi aşağıdaki şekilde tanımlamaktadır:

- **Çöp karıştırma:** Kurbanın çöp kutusunda ona ait olan ve kişisel olarak tanımlanabilir bilgi (personally identifiable information) içeren bir içerik aramaktır. Örnek olarak posta vasıtası ile gelmiş bir zarf üzerinde yer alan bilgiler verilebilir.

- **Omuz üzerinden izleme:** Bir örnek olarak, bilgisayar kullanan birinin arkasında bekleyip, kullanıcının haberi olmadan gizli bilgilerini öğrenmek gösterilebilir. Başka bir örnek ise ATM'den para çeken birinin arkasında yaptığı işlemleri telefonu ile kameraya çeken biri olarak verilebilir.

Açık kaynaklı bilgi istihbaratı, kurban hakkında internet üzerinde var olan ve herkesin erişebildiği bilgileri içerir. Bu bilgileri toplamak için farklı araçlar kullanılabilir. Bu araçlardan biri Maltego'dur. Bu araç bilgi toplamak için mükemmeldir ve insanlar, web siteleri, bilgisayarlar, şirketler, telefon numaraları, vb. bilgi toplanmasına izin verir. Örnek bir uygulama Şekil 2.3'te gösterilmiştir. Örnek olarak uygulamada Zaid Sabih hakkında bilgiler toplanmıştır [20].

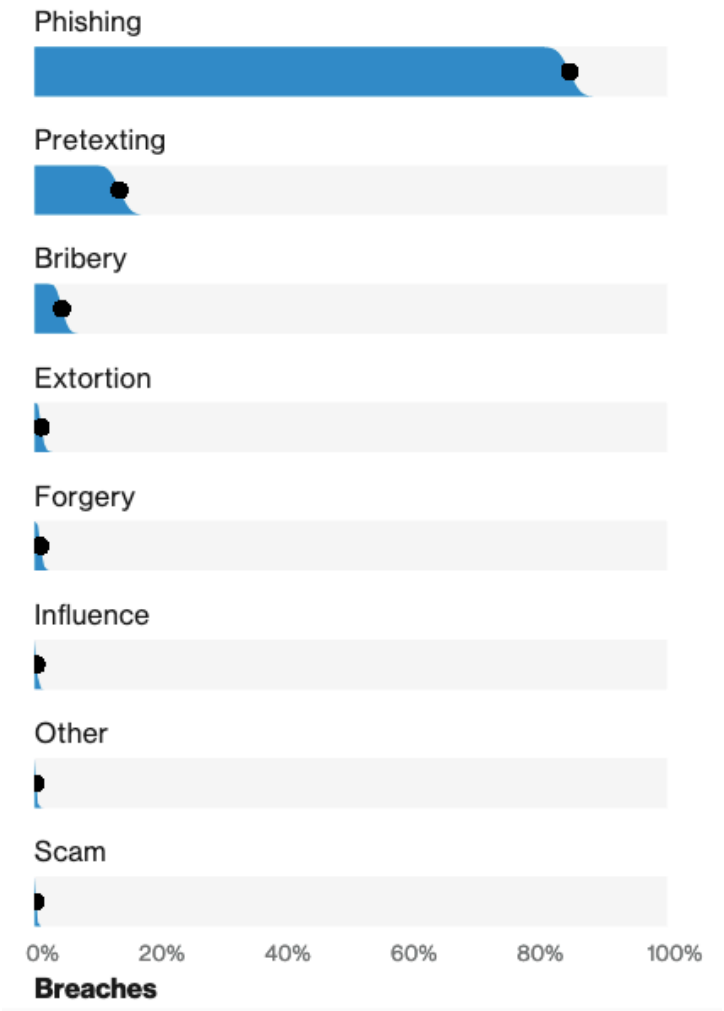


Şekil 2.3. Örnek Maltego uygulaması

Sosyal mühendisliğin hedefi, saldırganın, kurbanı tuzağa düşürmek için gerekli bilgiyi toplayıp saldırısının inandırıcılığını arttırmaktır. Sosyal mühendislik siber tehditlerin birçoğu için ilk aşamadır. Örnek olarak sosyal mühendislik sonrasında yapılan bir oltalama saldırısı verilebilir. Oltama saldırısının tanımı aşağıda verilmiştir.

2.3.2. Oltalama (Phishing)

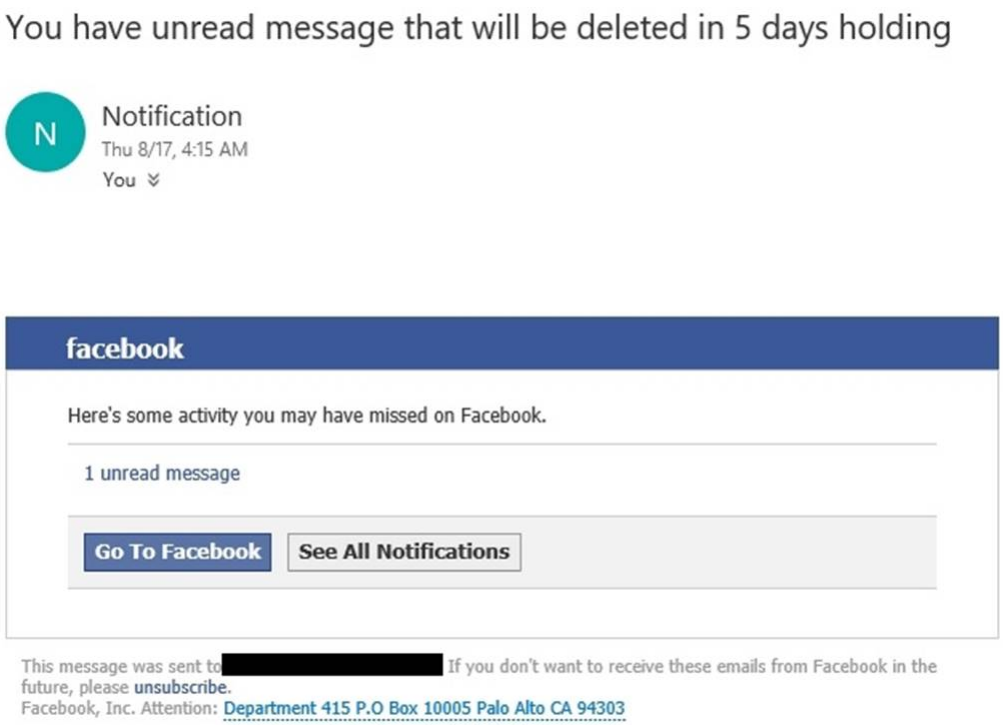
E-posta, kısa mesaj gibi araçlar kullanarak insanlar üzerinde bir çeşit merak, korku, acele tepki verme vb. duygular tetikleyip, gizli bilgi elde etmeyi hedefleyen saldırı türüdür. Bu saldırı bir sisteme giriş sağlamak için en yaygın kullanılan yöntemdir. Verizon [34] 'a göre sosyal saldırı yöntemlerinin %80'inden fazlası oltalama saldırılarından oluşmaktadır. Şekil 2.4'te 2019 yılı verilerine göre sosyal mühendislik kullanarak yapılan saldırıların eğilimlerini göstermektedir.



Şekil 2.4. 2019 yılı sosyal saldırı eğilimleri

Oltalama saldırısı bir kurumu hedef aldıysa bu gerçek saldırı öncesi hazırlık amaçlı da olabilir saldırının kendisi de olabilir. Saldırgan genellikle kendisini güvenilen biri/kurum gibi (ör: banka) göstererek kurbanın bilgilerini vermesini sağlamaya çalışır. Eğer saldırı bir sisteme sızma amacı güdüyorsa, genellikle içinde zararlı bir içerik içerir. Saldırganlar e-

postalara eklenmiş bir belgeyi ya da e-posta içinde geçen bir bağlantıyı kullanarak oltalama saldırısını gerçekleştirebilirler. Çoğu zaman e-postaların içerdikleri PDF veya WORD dosyaları zararsız olarak kabul edilir fakat bu dosyalar zararlı içerik taşıyan kod parçacıkları içerebilirler. Bu kod parçacıkları çalıştırıldıkları bilgisayarın saldırganlar tarafından ele geçirilmesini sağlamak amaçlıdır. Son zamanlarda sosyal medya uyarı mesajları kullanımı artan oltalama saldırı tekniklerinden biridir. Örnek olarak Şekil 2.5'te gösterilene benzer bir saldırı ile saldırgan kurbanın gönderilen bağlantıya tıklamasını sağlayıp, kurbanın Facebook parolasını ele geçirmeyi hedeflemektedir [35].



Şekil 2.5. Bir oltalama saldırısı örneği

2.3.3. DDOS/Botnet

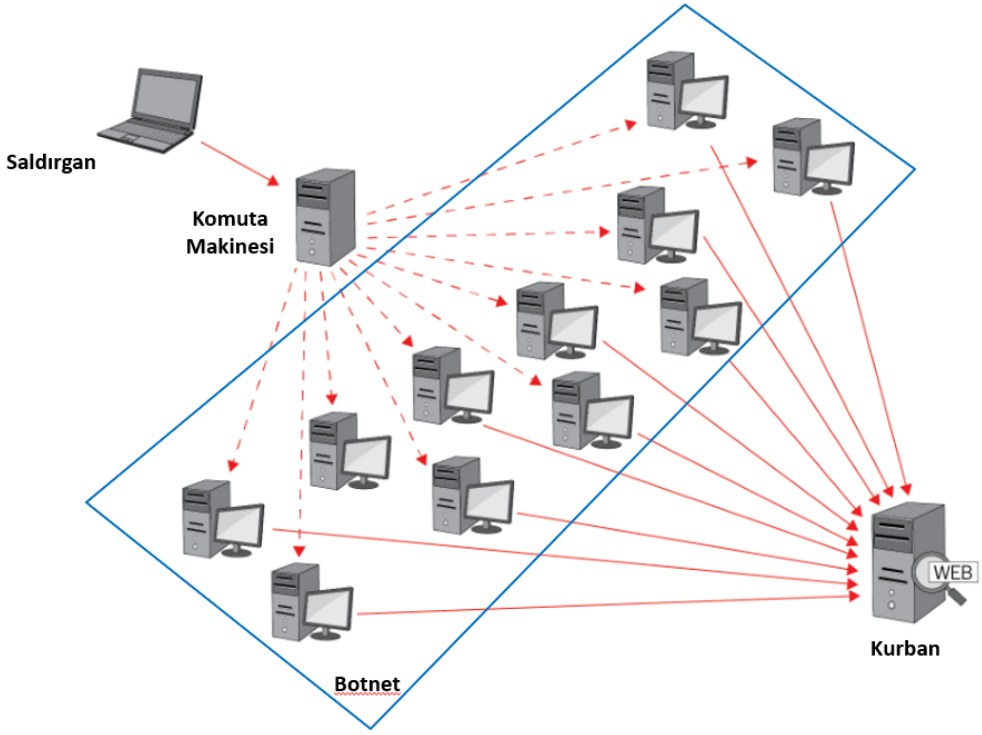
Servis dışı bırakma (DoS – Denial of Servis) saldırısı, meşru bir kullanıcı ulaşması gereken bir servise, cihaza veya başka bir ağ kaynağına, bir siber saldırı nedeniyle ulaşamadığı zaman oluşur. Bu servisler e-posta, internet, çevrim içi hesaplar, vb. servisler olabilir. Bir servis dışı bırakma saldırısı hedefi, gelecek meşru isteklere cevap veremeyecek kadar çok ağ paketi yollama ile gerçekleştirilir. Bir DoS saldırısı gerçekleştirmek için birçok farklı yöntem vardır. Smurf saldırısı ve SYN baskını (SYN flood) saldırıları örnek olarak verilebilecek iki yöntemdir [36]. Vikipedi [37] Smurf saldırısını aşağıdaki gibi tanımlamıştır:

“Paketlerin belirli bir ağdaki tüm ana makinelere; belirli bir makineden gönderilmesi yerine ağın yayın adresi aracılığıyla gönderilmesini sağlayan hatalı yapılandırılmış aygıtlarına dayanır. Saldırgan, hedefin adresi gibi görünmesi için kaynak adrese çok sayıda IP paketi gönderir. Böylece ağın bant genişliği hızlıca tükenir ve yasal paketlerin hedeflerine ulaşması engellenir.”

Yine Vikipedi [37] SYN baskını saldırısını aşağıdaki gibi tanımlamıştır:

“Host, genellikle sahte bir gönderen adresi olan aşırı miktarda TCP / SYN paketleri gönderdiğinde bir SYN flood oluşur.”

Bir hedefe saldırmak için birden fazla makine birlikte çalıştığında dağıtılmış hizmet reddi (DDoS) saldırısı gerçekleşir. DDoS saldırganları, büyük ölçekli saldırılar gerçekleştirmek için genellikle bir botnet (ele geçirilmiş internet bağlantılı cihazlar) grubundan yararlanır. Saldırganlar, komuta-kontrol (command and control) yazılımları kullanarak çok sayıda cihazı kontrol etmek için güvenlik açıklarından yararlanır. Güvenliği ihlal edilmiş cihazlardan oluşan botnet’ler diğer potansiyel saldırganlara da kiralanabilir. Botnet genellikle vasıfsız kullanıcıların DDoS saldırıları başlatmasına izin veren “kiralık saldırı” hizmetlerine sunulur. [36]. Neil [33], DDoS saldırısını anlatmak için Şekil 2.6’yı kullanmıştır.



Şekil 2.6. DDoS (Distributed Denial of Service) saldırısı

2.3.4. Malware/Ransomware/Virus

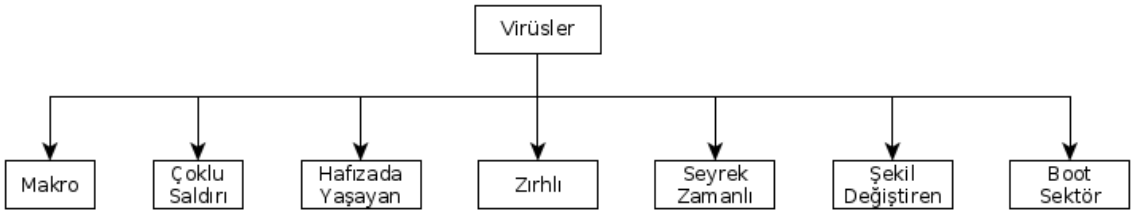
Malware/Ransomware/Virus bir sistemde kullanıcının isteği dışında değişlik yapan ve kötü amaç güden yazılımlardır. Sistemden bilgi kaçırmak, çalışmasını engellemek, vb. için kullanılırlar.

Virüs, tanım olarak kendi kendine çoğalabilen program demektir. Genellikle virüslerin kendilerini çoğaltmak dışında başka yan etkileri de bulunmaktadır; fakat çoğalma ve hızlı bir şekilde yayılma her virüsün sahip olduğu niteliklerdir. Çok hızlı yayılan bir virüs ağ trafiğinin işleyişini kötü yönde etkiler. Sadece çoğalmak için oluşturduğu trafik bile ağın izin verdiğinden fazla bir yük oluşturup, bütün ağı kullanılmaz kılabilir. Yıllar öncesinin 'ILOVEYOU' virüsünün kötü niyetli bir yükü (payload) olmasa bile, sadece yarattığı e-posta trafiği birçok ağı kullanılamaz hale getirmiştir. Virüsler birkaç yol ile yayılırlar. ; [38].

- **E-posta:** Bulaştıkları bilgisayarın sahibinin e-posta adres defterinde bulunan herkese kendini gönderebilir,
- **Ağ Bağlantısı:** Bulaştığı bilgisayarın ağ bağlantısını kullanarak aynı ağ üzerinde bulunan diğer bilgisayarlara sıçramaya çalışabilir,
- **Taşınabilir Cihazlar:** USB, CD, DVD, vb. taşınabilir ortamlar içeriklerinde virüs taşıyabilir. Bu ortam bir cihaza takıldığında, kendini cihaza kopyalayabilir,
- **Maskeleme:** Virüs kendisini meşru (legit) bir dosya içerisinde gizleyebilir. Dosya çalıştırıldığı zaman arka planda kendini bilgisayara aktarabilir,
- **İnternet:** Bir İnternet sayfasına bulaşan virüs ziyaret edildiği zaman, ziyaretçi bilgisayara kendini kopyalayabilir.

Anlatılan yöntemlerden en sık kullanılanı e-posta yöntemidir. Virüslerin e-posta göndermek için en sık yararlandıkları uygulama ise Microsoft Outlook'tur. Bunun nedeni Outlook uygulamasının zafiyetleri değildir. Microsoft programcılara kolaylık sağlamak için kendi uygulamalarında birçok ara yüz geliştirmiştir. Bu sayede bir kişi küçük bir kod parçası ile oluşturduğu bir dokümanı hızlıca adres defterinde bulunan insanlara e-posta olarak gönderebilir. Virüsler de bu kolaylıktan faydalanabildikleri için Outlook çok sık tercih ettikleri bir uygulama olmaktadır [38]. Günümüzde virüsler yayılmak için sadece tek bir yöntemi kullanmak yerine birden fazla yöntemi kullanmaya başlamışlardır. Virüsler tasarımcılarının dehası sayesinde bilgisayarlara bulaşmaktan ziyade, kullanıcıların yapmaması gereken davranışları yapması (kötü niyetli içerik sitelerinden dosya indirmek gibi) sonucunda yayılabilmektedirler.

Virüsler tipleri Şekil 2.7'de gösterdiği şekildedir ve açıklamaları aşağıda verilmiştir.



Şekil 2.7. Virüs Tipleri

- **Makro:** Ofis uygulamaları kullanıcıların belirli işlerini kolaylaştırmak için oluşturdukları dokümanlar içinde kod yazmaya izin veren altyapılar içerebilir. Örneğin Microsoft Office uygulamaları içinde Visual Basic kodu çalıştırılmasına imkan tanır. Bu imkan sayesinde yazılan programlara 'makro' denir. Kötü niyetli bir kişi makrolar aracılığı ile ofis dokümanına zararlı bir kod parçası ekleyerek, doküman çalıştırıldığı zaman çalıştırıldığı bilgisayara virüs bulaşmasını sağlayabilir. Bu yöntem genellikle yukarıda bahsedilen e-posta yöntemi ile birleştirilir.
- **Çoklu Saldırı (Multi-partite):** Virüs, bir bilgisayara bulaşmak için sadece bir yöntem kullanmayabilir. Örneğin; ofis dokümanı içinde gelen bir kod Windows Powershell'i kullanarak internetten zararlı bir içerik indirip, indirilen içeriği çalıştırabilir. Ardından ağ üzerinde diğer bilgisayarlara yayılmaya çalışırken, bulunduğu bilgisayar üzerinde kalıcılık sağlamak için kendini birden fazla dosyaya bulaştırmaya çalışabilir.
- **Hafızada Yaşayan:** Virüsler izlerini gizlemek için geride bir artık bırakmak istemeyebilirler. Bu nedenle dosya sistemi üzerinde bir değişiklik yapmak yerine kendilerini bilgisayarın hafızasında çalıştırabilirler.
- **Zırhlı:** Araştırmacılar tarafında anlaşılması zor olsun diye virüsler tasarlanırken farklı yöntemler izlenebilir. Bir virüs yazılırken kod şifrelenip, çalışma anında kendi şifresini açan bir yapı, virüsün nasıl çalıştığını anlamak için tersine mühendislik yapıldığı sırada kodun takip edilmesini zorlaştırabilir.
- **Seyrek Zamanlı (Sparse Infector):** Bazı virüsler bulunmalarını zorlaştırmak için sürekli çalışmak yerine seyrek aralıklarla çalışmayı tercih edebilirler. Örneğin bulaştıkları bilgisayarda günde sadece bir kere gece saat 10'da çalışarak güvenlik uygulamaları tarafından bulunmayı zorlaştırmaya çalışabilirler.
- **Şekil Değiştiren (Polymorphic):** Çalışma süreleri boyunca belli zaman aralıklarında formlarını değiştirerek güvenlik yazılımlarını atlatmaya çalışırlar.

- **Boot Sektör:** Bu virüsler bilgisayarların boot sektöründe var olurlar. Bilgisayar başlarken çalıştıkları için kendilerini diğer tip virüslere göre daha rahat gizleyebilirler çünkü güvenlik uygulamaları bilgisayar açıldıktan sonra devreye girmektedirler.

Yukarıda tanımı yapılan virüsler kullanım yöntemi/amacına göre Malware ya da Ransomware olarak ta adlandırılabilirler. Bir virüs bulaştıktan sonra bilgisayar üzerindeki verileri şifreleyebilir ve tekrar açılması için kullanıcıdan belli bir ücret talep edebilir. Bu virüsler Ransomware olan adlandırılmaktadır. Ransomware'ların etkili örneklerinden biri 'WannaCry'dır. Elizabeth Dwoskin ve Karla Adam tarafından yapılan 'The Washington Post' haberine göre (https://www.washingtonpost.com/business/ economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710 b69_story.html) WannaCry 150'den fazla ülkeyi ve 200.000'den fazla kişiyi etkilemiştir. MITRE ATT&-CK™ saldırı veri tabanına göre (https://attack.mitre.org /software/S0366/) bu Ransomware Tablo 2.1'de yer alan saldırı tekniklerini kullanmıştır:

Tablo 2.1. WannaCry saldırısında kullanılan yöntemler

Domain	ID	Name	Use
Enterprise	T1024	Custom Cryptographic Protocol	WannaCry uses a custom cryptographic protocol over the Tor circuit.
Enterprise	T1486	Data Encrypted for Impact	WannaCry encrypts user files and demands that a ransom be paid in Bitcoin to decrypt those files.
Enterprise	T1210	Exploitation of Remote Services	WannaCry uses an exploit in SMBv1 to spread itself to other remote systems on a network.
Enterprise	T1083	File and Directory Discovery	WannaCry searches for variety of user files by file extension before encrypting them using RSA and AES, including Office, PDF, image, audio, video, source code, archive/compression format, and key and certificate files.
Enterprise	T1222	File Permissions Modification	WannaCry uses attrib +h and icacls . /grant Everyone:F /T /C /Q to make some of its files hidden and grant all users full access controls.
Enterprise	T1158	Hidden Files and Directories	WannaCry uses attrib +h to make some of its files hidden.
Enterprise	T1490	Inhibit System Recovery	WannaCry uses vssadmin, wbadmin, bcdedit, and wmic to delete and disable operating system recovery features.

Domain	ID	Name	Use
Enterprise	T1188	Multi-hop Proxy	WannaCry uses Tor for command and control traffic.
Enterprise	T1079	Multilayer Encryption	WannaCry uses Tor for command and control traffic and routes a custom cryptographic protocol over the Tor circuit.
Enterprise	T1050	New Service	WannaCry creates the service "mssecsvc2.0" with the display name "Microsoft Security Center (2.0) Service."
Enterprise	T1120	Peripheral Device Discovery	WannaCry contains a thread that will attempt to scan for new attached drives every few seconds. If one is identified, it will encrypt the files on the attached device.
Enterprise	T1076	Remote Desktop Protocol	WannaCry enumerates current remote desktop sessions and tries to execute the malware on each session.
Enterprise	T1105	Remote File Copy	WannaCry attempts to copy itself to remote computers after gaining access via an SMB exploit.
Enterprise	T1018	Remote System Discovery	WannaCry scans its local network segment for remote systems to try to exploit and copy itself to.
Enterprise	T1489	Service Stop	WannaCry attempts to kill processes associated with Exchange, Microsoft SQL Server, and MySQL to make it possible to encrypt their data stores.
Enterprise	T1016	System Network Configuration Discovery	WannaCry will attempt to determine the local network segment it is a part of.
Enterprise	T1047	Windows Management Instrumentation	WannaCry utilizes wmic to delete shadow copies.

2.3.5. Rootkit/Bootkit

Kök kullanıcı takımı (Rootkit); çalışan uygulamaları, servisleri, açık olan portları vb. bilgileri sistemden gizlemek için kullanılır. Kötü niyetli kişiler Rootkit kullanarak sistemlerde varlıklarını gizleyebilirler. Bootkit ise sistemin MBR (Master Boot Record) kayıtlarını hedef alır ve kendini buraya yerleştirir. Böylece işletim sistemi yüklemeden önce zararlı faaliyetlerini harekete geçirebilir.

Bettany and Halsey [39] ise Bookit'i şu şekilde tanımlamıştır; bu kötü amaçlı yazılım türleri kendilerini bir bilgisayardaki önyükleme bölümlerine yerleştirir. Daha sonra rootkit, işletim sistemini sanallaştırma ortamı benzeri bir ortamda başlatır ve işletim sisteminin tam kontrolünü sağlar. Aynı zamanda yüklenilen herhangi bir güvenlik yazılımından ve işletim sisteminin kendisindeki güvenlik özelliklerinden kendisini saklar. Rootkit bulaştığı bir sistemde bütün uygulama akışlarına erişebilir ve eriştiği uygulamaların kabiliyetlerini ve yetkilerini kullanabilir. Rootkit ve bootkit'ler diskteki gizli ve korumalı bölümlerde bulunduğu ve algılanması son derece zor olduğu için kaldırılması çok güçtür.

2.3.6. İçeriden gelen tehditler/İnsan hatası

İçeriden biri, kuruluşun varlıklarına erişim yetkisi olan bir çalışan, danışman veya satıcı gibi bir kuruluşta çalışan kişidir. İçeriden gelen tehditler önemli miktarda hasara neden olma imkanına ve fırsatına sahiptir ve bir kuruluşun kaynaklarının gizlilik, bütünlük ve kullanılabilirliğini kaybetmesine neden olabilirler. Kurum içerisinde yer alan kişiler hata yapabilir veya kayıplara neden olan güvenlik uygulamalarını görmezden gelebilirler. İntikam almak amaçlı kötü niyetli faaliyetlerde bulunabilirler. Ticari sırları, müşteri bilgilerini veya kuruluştan diğer hassas bilgileri çalmak gibi veri hırsızlığına neden olabilir ve daha sonra kişisel kazanç için satma girişiminde bulunabilirler. Tüm içeriden gelen tehditler kasıtlı olarak veri çalınması veya verilerin yok edilmesi değildir. Bunun yerine, genellikle güvenlik protokollerini veya uygulamalarını izlemeyerek kayıplara neden olan kullanıcılardır. Örnek olarak, bir organizasyon düzenli olarak çalışanlarına bilinmeyen kaynaklardan gelen e-postalarda yer alan bağlantılara tıklamamalarını söylese bile bu bağlantılardan birine tıklayan bir kullanıcı içeriden gelen bir tehdittir [9].

Başka bir tanım olarak Easttom [38] 'a bakılabilir. Bu tanım şöyledir; içeriden gelen tehditler bir tür güvenlik ihlalidir. Bir kurum çalışanı, verilere erişimini kötüye kullandığında veya erişim yetkisi olmadığı verilere eriştiğinde içeriden bir tehdit oluşur. İçeriden tehditlere en büyük örneklerden biri Edward Snowden'dir. 2009 yılında Edward Snowden, birkaç ABD devlet kurumunun bilgisayar sistemlerini yöneten Dell için çalışmıştır. Mart 2012'de Hawaii'de bir NSA konumuna atanmıştır. Orada çalıştığı sırada, ağ idari görevlerini yerine getirme bahanesiyle, ona kendi kullanıcı adı ve parola bilgilerini sağlamak için birkaç kişiyi ikna etmiştir, erişme yetkisi olmadığı binlerce belgeye erişmiştir ve indirmiştir.

2.4. Sistem Saldırı Tipleri

Bir ağ yapısı; birine fiber, bakır ya da kablosuz bir şekilde bağlı olan sistemler bütünüdür. Bir ağ oluşturma için sadece fiziksel olarak bağlı olmak yetmez. Buna ek olarak sistemlerin gerekli ağ donanımlarını içermesi, ağ farkındalığı olan işletim sistemlerinin ve yazılımların kullanılması gerekmektedir. Bu yapıyı gerçekleştirmek için sistemler birbirinden bağımsız dört özellikten oluşmaktadır. Bunlar [40]:

- Ağ farkındalığı olan yazılımlar,
- Ağ farkındalığı olan işletim sistemleri,
- Gelen ve giden paketleri yönetmek için bir ağ yığını (network stack),
- Ağ arayüzü için gerekli sürücülerdir.

Bu gereklilikler nedeniyle, bir ağa bağlı olan sistemler aşağıda belirtilen saldırı tiplerine açıklardır:

1. Uygulama Saldırıları
2. İşletim Sistemi Saldırıları
3. Ağ Yığını Saldırıları

Sistem güvenliğini anlamak ve saldırıların tespit aşamasına geçebilmek için bu saldırı tiplerinin anlanması gerekmektedir.

2.4.1. Uygulama saldırıları

Günümüzde ağa bağlı sistemlerde çalışan bir uygulama dendiği zaman akla ilk gelen uygulama çeşidi Web uygulamalarıdır. Kullanım yaygınlıkları ve sunulan hizmetler için temel oluşturduklarından dolayı Web uygulama saldırıları en yaygın görülen uygulama saldırı tipidir [41].

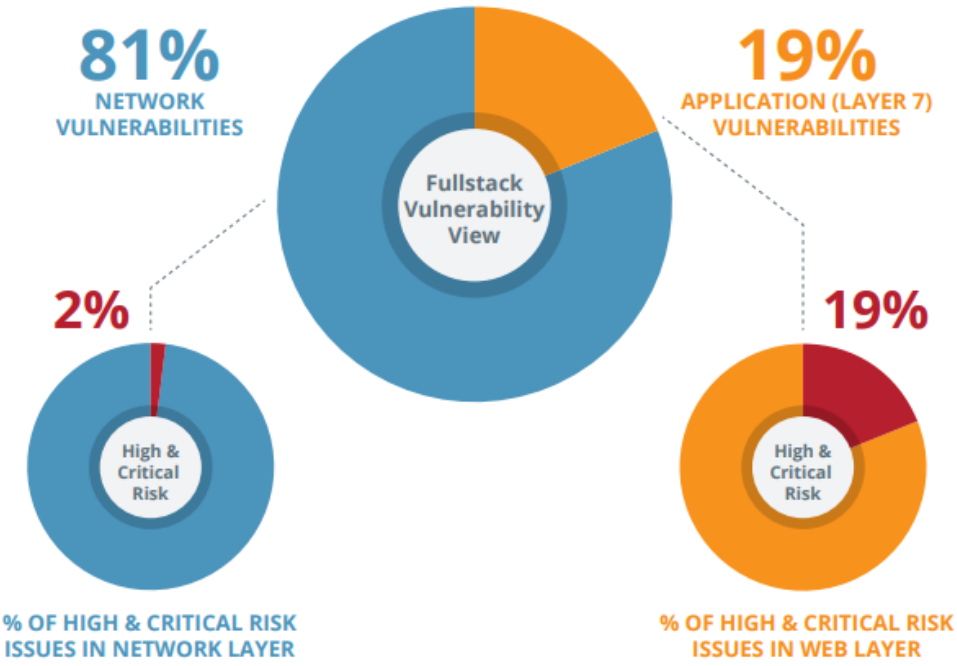
Web uygulama saldırıları istatistiklerine bakıldığına, bir kısım saldırı ön plana çıkmaktadır. Rapid7 [42] tarafından hazırlanmış olan rapora göre bu saldırılar aşağıdakilerdir:

- Cross-Site Scripting (XSS),
- SQL Enjeksiyonu (SQL Injection - SQLi),
- Otomatikleştirilmiş Tehditler (Automated Threats),
- Dosya Yolu Geçişi (File Path Traversal),
- Komut Enjeksiyonu (Command Injection - CMDi).

Bu rapora göre bahsi geçen saldırıların tanımları aşağıda verilmiştir [42]:

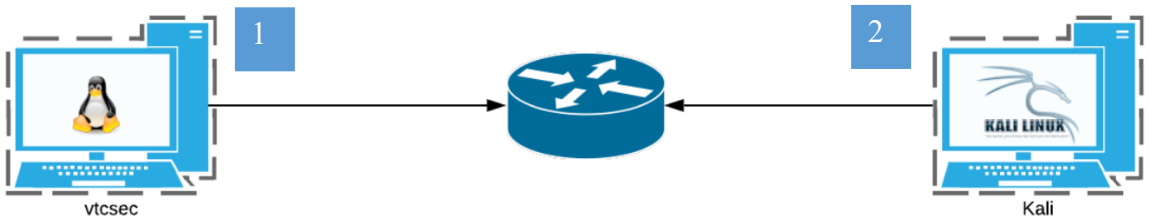
1. **Cross-Site Scripting (XSS):** Bu saldırı tipi web saldırıları arasında en yaygınıdır. XSS zafiyetleri sunucuların üzerinde çalışan kod yerine kurbanların internet tarayıcılarını hedef almaktadır. Arkasında yatan mantık ise, kurbanın internet tarayıcısı üzerinde çalışan kod parçacıklarını manipüle ederek, saldırganın isteklerinin gerçekleştirilmesidir. Bir web uygulamasına zararlı bir kod parçacığı gömülerek, sayfa her ziyaret edildiğinde bu zararlı kodun çalışması tetiklenebilir. XSS ayrıca saldırganların erişim kontrol kurallarını atlatmalarını sağlayabilir.
2. **SQL Enjeksiyonu (SQL Injection):** Bu saldırı tipi veri güdümlü uygulamalarda (data-driven application) geçerlidir. Saldırgan veri okuyan bir giriş alanına zararlı bir SQL sorgusu yazarak uygulama veri tabanında sahte kimlikler yaratabilir, var olan veriyi değiştirebilir ya da silebilir ve veri tabanının yönetimini ele geçirebilir.
3. **Otomatikleştirilmiş Tehditler (Automated Threats):** Bu tehditler özel olarak tasarlanmış yazılımlar ile gerçekleştirilir. Bu yazılımlar bir sunucu başka bir sunucudan veri istediğinde bunu tespit eder ve kendisini gerçek bir kişiymiş gibi gösterip aynı veriyi sunucudan ister. Zamanla toplanan veri sayesinde sunucuya yapılan isteklerin gerçek bir kişi tarafından mı yoksa otomatikleştirilmiş bir kod parçası tarafından mı yapıldığı tespit edilebilir. Bu çıkarım sayesinde gerçek istekler ve saldırılar ayrıştırılabilir ve bu saldırı tipi engellenebilir.
4. **Dosya Yolu Geçişi (File Path Traversal):** Bu saldırı başarılı olduğu taktirde kaynak kod, sunucu yapılandırması, işletim sistemi kullanıcı bilgileri gibi hassas verilerin sızmasına neden olabilir. Bu saldırı kullanılarak başka saldırılara zemin hazırlanabilir.
5. **Komut Enjeksiyonu (Command Injection):** Bu saldırı doğru veri kaynağı kontrolü yapılmadığı zaman gerçekleştirilebilir. Eğer veri uygulamaya kabul edilirken hangi kaynaktan geldiği kontrol edilmezse, bu saldırgana normalde yetkisi olmayan komutları çalışma yetkisi verebilir.

Edgescan [43] 'a göre ağ katmanı zafiyetleri uygulama katmanı zafiyetlerinden yüzde olarak daha fazladır: fakat uygulama katmanı zafiyetleri daha kritik olarak değerlendirilmektedir. Bu rapora göre istatistikler Şekil 2.8'de gösterilmiştir.



Şekil 2.8. Edgescan Raporu İstatistikleri

Uygulama saldırılarına örnek bir test ortamın oluşturmak için VulnHub üzerinde bulunan 'Basic Pentesting: 1' makinesi kullanılmıştır. Bu makine ve Kali Linux makinelerinden oluşan bir test ortamı Şekil 2.9'da gösterilmiştir. Bu test ortamında Şekil 2.9'da 1 ile gösterilmiş makine üzerinde çalışan bir web uygulamasına Şekil 2.9'da 2 ile gösterilmiş makine ile saldırı gerçekleştirilip 1 numaralı makine ele geçirilecektir.

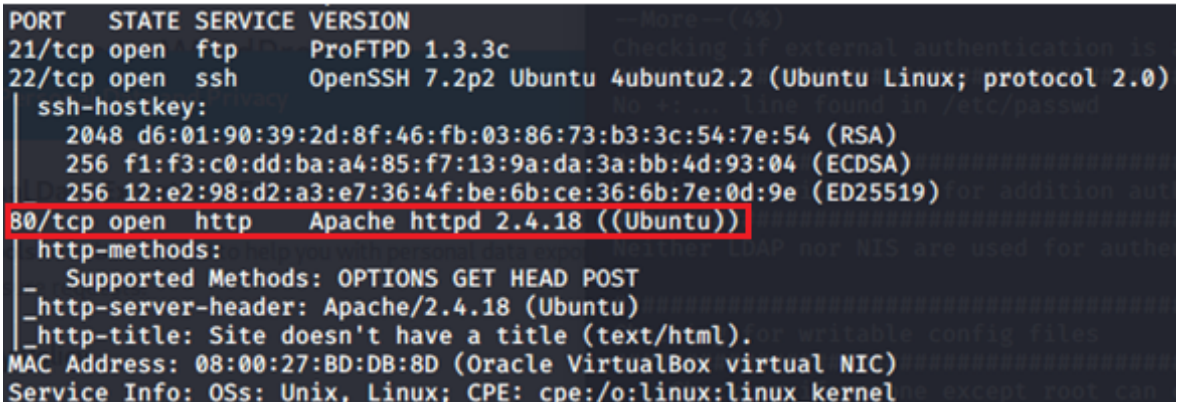


Şekil 2.9. Uygulama Saldırıları test ortamı

İlk olarak 2 numaralı makine üzerinden 1 numaralı makinede çalışan uygulamalar tespit edilmiştir. Bu tespitin sonuçları Şekil 2.10'da gösterilmiştir. Bu sonuçlara göre kurban makine üzerinde 80 portundan bir web uygulaması sunulmaktadır.

Saldırgan makinesinden kurban makinesine internet tarayıcısı ile bağlanıldığı zaman sıradan bir internet sayfası ile karşılaşılmaktadır. Bu aşamada saldırgan daha detaylı bilgi elde etmek için kurban makinesi üzerinde yer alan web hizmetinin başka neler içerdiğini taramıştır. Bu tarama sonuçları Şekil 2.11'de gösterilmiştir. Bu sonuçlara bakıldığında

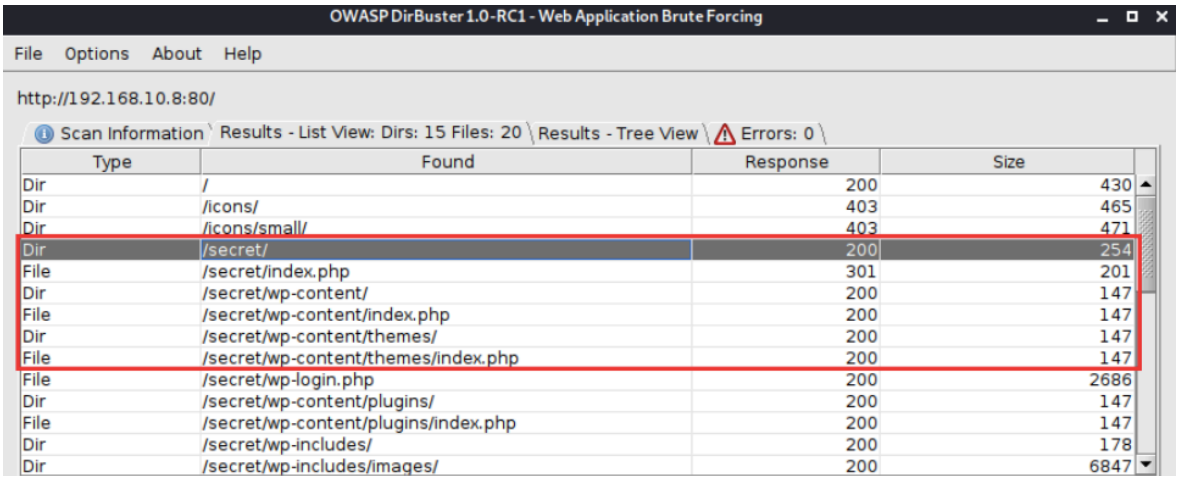
kurban makine üzerinde bir WordPress uygulaması çalıştığı ve bu uygulamaya hangi internet adresinden erişilebileceği gözükmektedir.



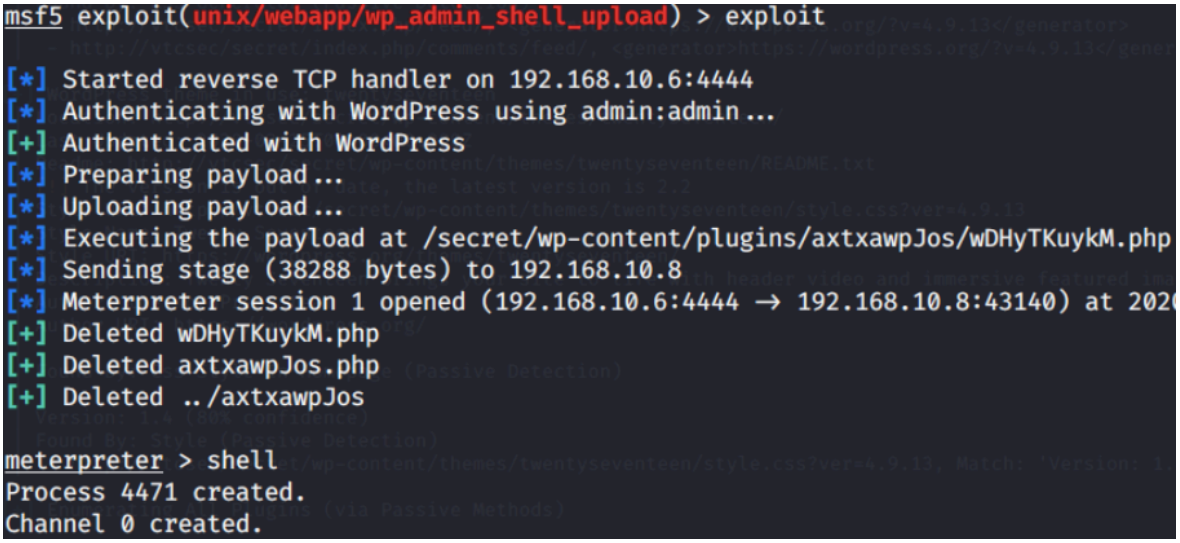
Şekil 2.10. Çalışan uygulamaların tespiti

Saldırgan makinesinden kurban makinesine internet tarayıcısı ile bağlanıldığı zaman sıradan bir internet sayfası ile karşılaşılmaktadır. Bu aşamada saldırgan daha detaylı bilgi elde etmek için kurban makinesi üzerinde yer alan web hizmetinin başka neler içerdiğini taramıştır. Bu tarama sonuçları Şekil 2.11'de gösterilmiştir. Bu sonuçlara bakıldığında kurban makine üzerinde bir WordPress uygulaması çalıştığı ve bu uygulamaya hangi internet adresinden erişilebileceği gözükmektedir.

Saldırgan bahsi geçen WordPress uygulamasını internet tarayıcısından açmış ve varsayılan birkaç kullanıcı adı ve parola kombinasyonunu denemiştir. Denemeleri sonucunda uygulama yöneticisinin kullanıcı adı ve parolasını bulabilmiştir. Bu bulgudan sonra saldırgan 'Metasploit Framework' aracı yardımı ile kurban makineye uzaktan erişim sağlamıştır. Şekil 2.12'de bu erişim gösterilmiştir.



Şekil 2.11. Detaylı web hizmeti tarama sonuçları



Şekil 2.12. Kurban makineye uzaktan erişim

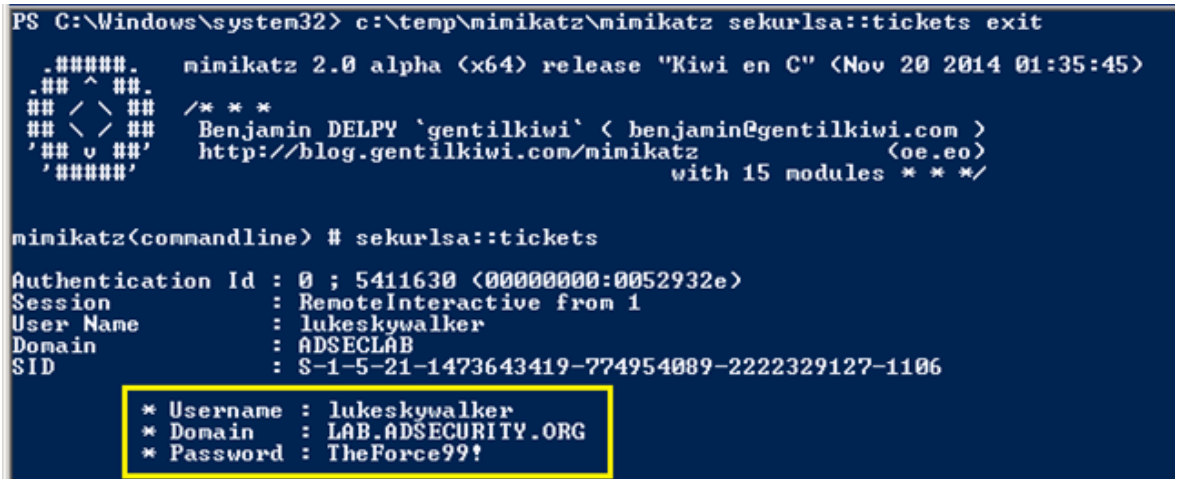
Bu çalışmada uygulama saldırılarının ne kadar kritik olduğu görülmektedir. Uygulamada yapılacak konfigürasyon, kodlama, vb. hatalar bir bilgisayarın saldırganların eline geçmesi için uygun ortam hazırlamaktadır.

2.4.2. İşletim sistemi saldırıları

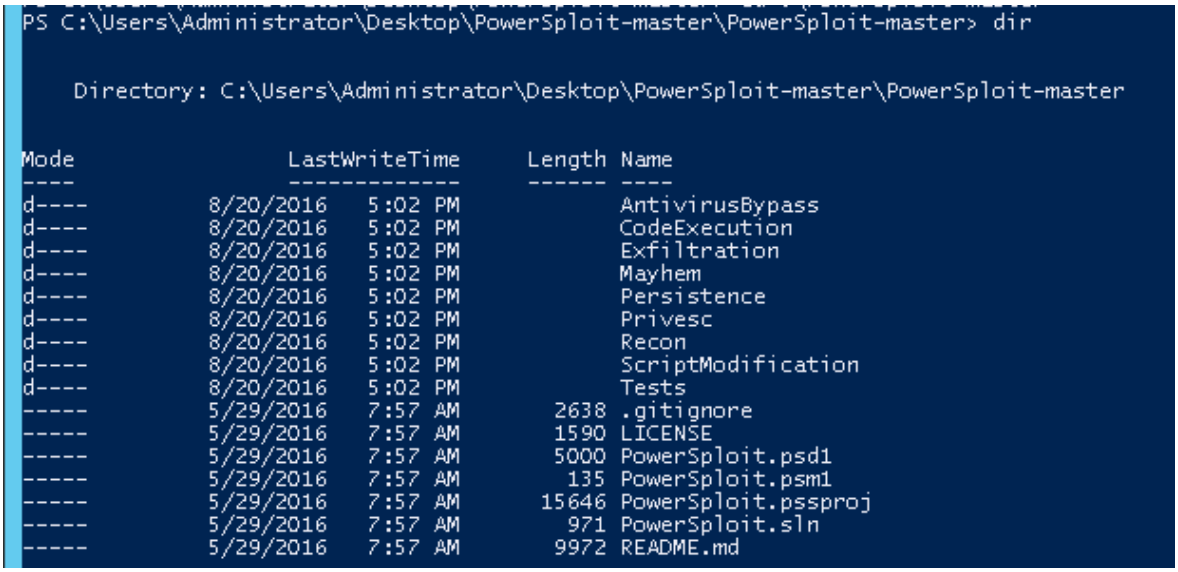
Günümüz işletim sistemleri birçok saldırıya dayanıklıdırlar. Bu dayanıklılığın nedeni; işletim sistemi sahibi firmaların zamanında yama yayınlamasıdır. Bu nedenle işletim sistemi saldırıları, ilk saldırı vektörü tercihlerinden biri değildir. Dikkat edilmesi gereken husus ise yayınlanmış olan yamaların sistemlere yüklenmesidir çünkü bir zafiyetin yaması var olsa bile eğer sistemde yüklü değil ise o sistem hala bahsi geçen zafiyeti içermektedir. Eğer yönetilen sistemin doğru bir yama yönetim politikası yoksa işletim sistemi saldırı tekniklerinin başarılı olma olasılığı yüksektir [40].

Bu tip altında iki saldırı yöntemi ön plana çıkmaktadır:

1. **Hak yükseltme (Privilege Escalation):** Hak yükseltme saldırıları; sistemin kullanıcıya atadığı hakları değiştirmeyi ve daha yetkili haklara sahip bir kullanıcı yetkisi elde etmeyi hedefler. Yetkili bir kullanıcı hakkı ele geçirildiği zaman saldırgan normal bir durumda izin verilmeyen zararlı kodları çalıştırabilir ve ICT ortamında istediği değişikleri yapmaya yetki kazanmış olur [33]. Örnek olarak bir Windows ortamında hak yükseltmeyi sağlayacak iki adet araç verilebilir: Mimikatz ve PowerSploit. Bu araçların örnek ekran görüntüleri Şekil 2.13'te ve Şekil 2.14'te verilmiştir.



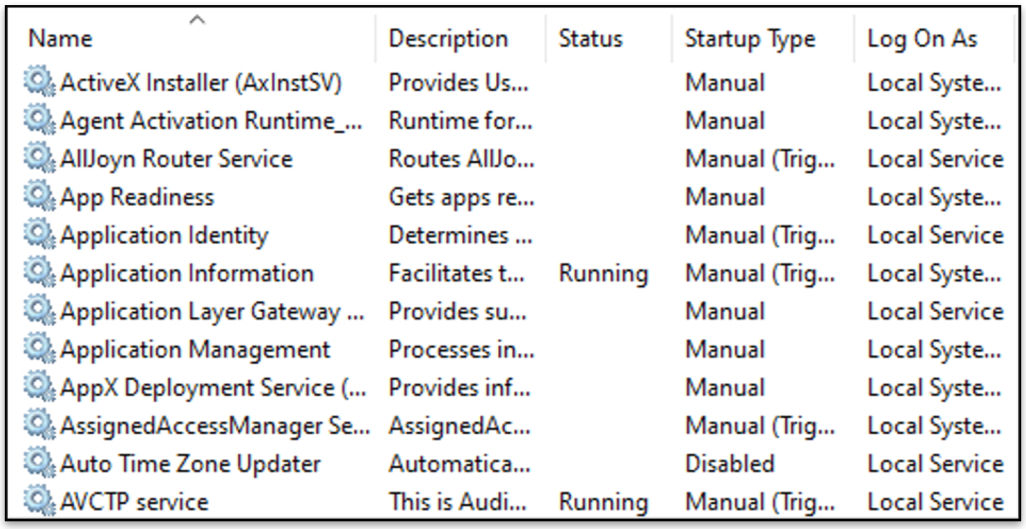
Şekil 2.13. Mimikatz Çalışma Ekran Görüntüsü



Şekil 2.14. PowerSploit Uygulaması Betikleri

2. **Servis Zafiyetleri:** Servis zafiyetleri farklı anlamlarda anlaşılmaktadır. Bir Windows sistem yöneticisi için servis Windows işletim sistemi altında çalışan servisler olabilirken (Windows 10 altında çalışan servislerin ekran görüntüsü Şekil 2.15'de verilmiştir), bir DevOps için servis kurumun dış dünyaya verdiği hizmetler olarak anlaşılabilmektedir (bir Windows sistemin dinlediği dış dünya bağlantıların ekran görüntüsü Şekil 2.16'da verilmiştir). Her iki durum için de bir servis zafiyeti aslında bir uygulama zafiyeti anlamı taşımaktadır; çünkü aslında her bir servis işletim sistemi üzerinde çalışan bir uygulamadır. Bu uygulamalara yapılabilecek saldırı tipleri ortadaki adam saldırısı (man-in-the-middle), hak yükseltme, vb. olabilir. Servis zafiyetlerine yapılan saldırılar

sadece yerel saldırılar olmayabilir. Bu saldırılardan ağ yığını da etkilenebilmektedir [40].



Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Agent Activation Runtime_...	Runtime for...		Manual	Local Syste...
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
App Readiness	Gets apps re...		Manual	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
AssignedAccessManager Se...	AssignedAc...		Manual (Trig...	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
AVCTP service	This is Audi...	Running	Manual (Trig...	Local Service

Şekil 2.15. Windows 10 servisleri

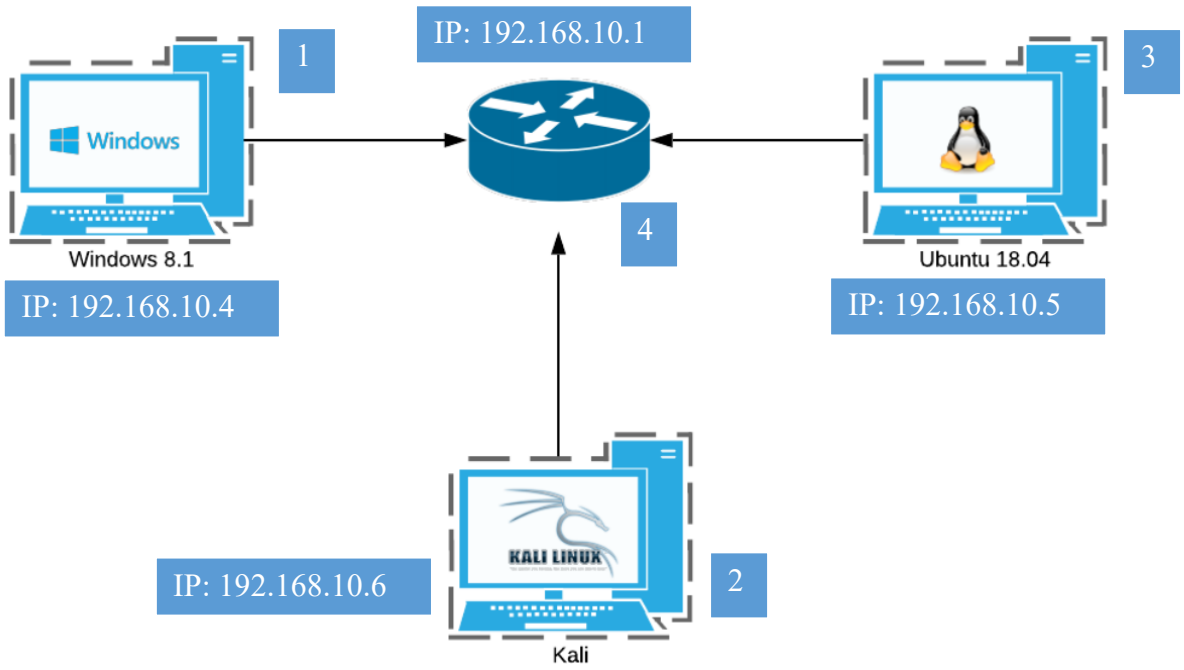
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1368
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:2179	0.0.0.0:0	LISTENING	3380
TCP	0.0.0.0:4000	0.0.0.0:0	LISTENING	6332
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	6972
TCP	0.0.0.0:5041	0.0.0.0:0	LISTENING	3992
TCP	0.0.0.0:5473	0.0.0.0:0	LISTENING	3992
TCP	0.0.0.0:10801	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	1036
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	112
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1812
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1856
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3564
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	772

Şekil 2.16. Windows sisteminin beklediği bağlantı örneği

2.4.3. Ağ yığını saldırıları

Bu saldırılar uygulama saldırıları gibi çok görülen saldırı tiplerindendir. Bilinmesi gereken en önemli ağ yığını saldırıları; ARP Zehirlemesi, MAC kafesleme (MAC Spoofing) ve DNS Sahteciliğidir (DNS Spoofing). Bu saldırıları tanımlamak ve etkilerini göstermek için Şekil 2.17'de gösterilen test ortamı kullanılmıştır. Bu test ortamında üç adet sanal makine ve bu makineleri birbirine bağlayan bir adet sanal yönlendirici kullanılmıştır. Saldırılar Şekil 2.17'de 2 numara ile gösterilmiş 'Kali' makinesi üzerinden gerçekleştirilmiştir.

Kurban makine olarak Şekil 2.17'de 1 ile gösterilen Windows 8 makine kullanılmıştır. Saldırıları takip etmek için Şekil 2.17'de 3 ile gösterilen 'Ubuntu' makine kullanılmıştır. Saldırı için Ettercap isimli araç kullanılmıştır. Bu araç yukarıda bahsi geçmiş olan üç ağ yığın saldırı çeşidini de gerçekleştirebilmektedir ve bu nedenle yaygın olarak kullanılmaktadır. Saldırıları takip etmek için 'Wireshark' uygulaması kullanılmıştır. Bu uygulama ağ trafiğini takip etmek bu trafik içinde şüpheli durumları tespit etmek için kullanılmaktadır.



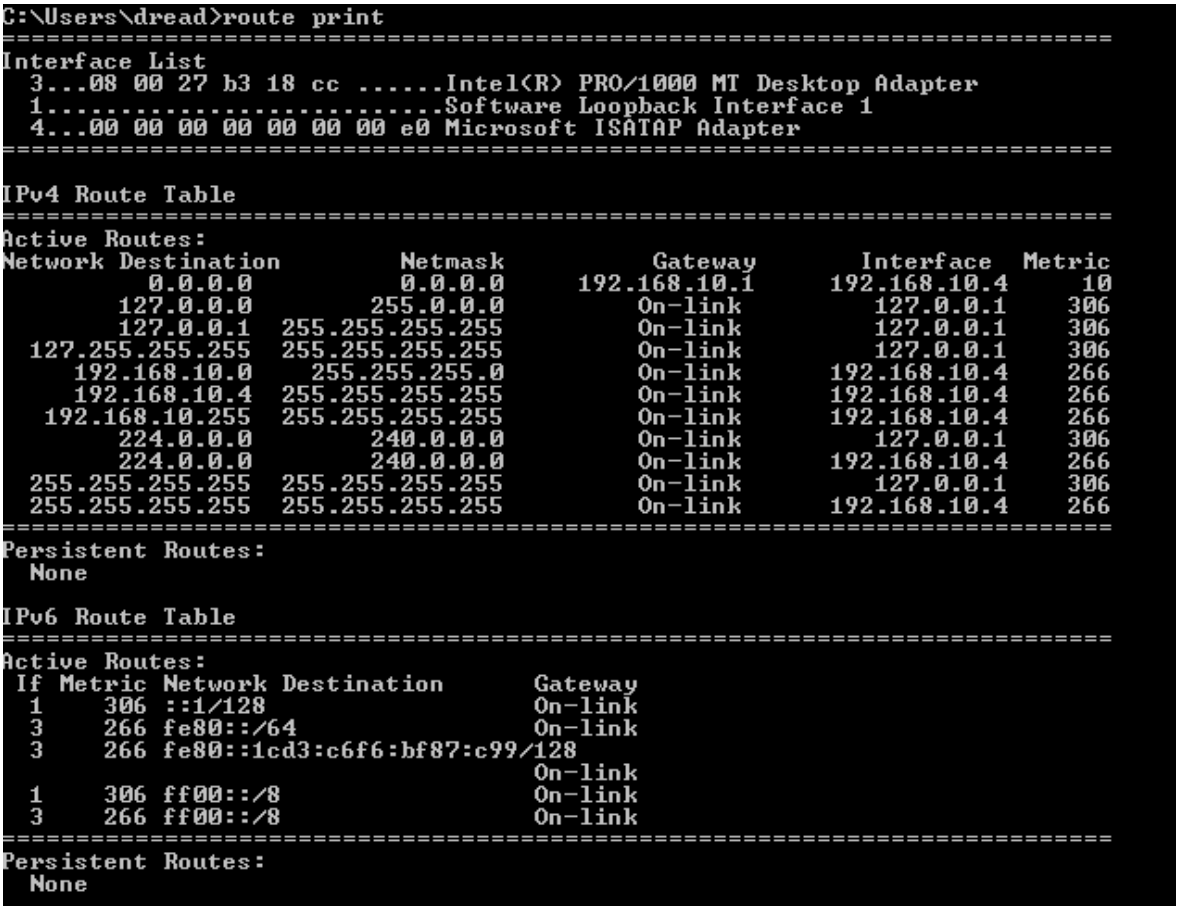
Şekil 2.17. Ağ Yığını Saldırı Test Ortamı

İlk olarak ARP Zehirlemesi tanımlaması yapılacaktır. ARP; OSI modelinin ikinci katmanında yer almaktadır ve MAC adreslerini kullanır. 'ARP Zehirlemesi' lokal ağda yapılması gereken bir saldırıdır. Bir saldırgan lokal ağa sahte ARP paketleri göndererek, bahsi geçen ağ trafiğini dinleyebilir, değiştirebilir ya da ağı tamamen kullanılamaz hale getirebilir [33]. Test ortamında gerçekleştiren saldırı senaryosu aşağıda anlatılmıştır:

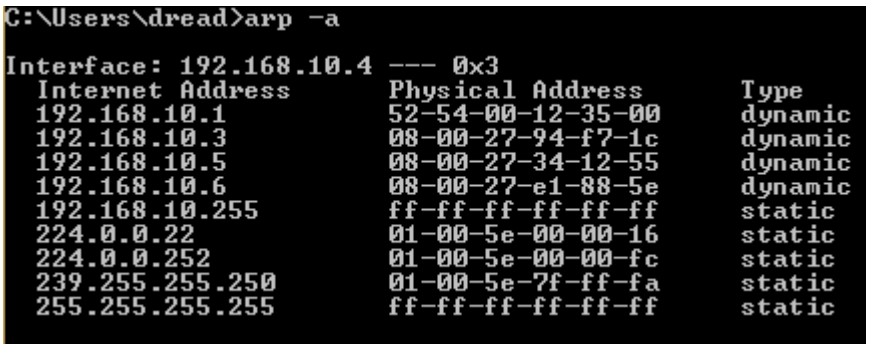
- Şekil 2.17'de 1 ile gösterilen Windows 8 makinenin dış ağa çıkmak için Şekil 2.17'de 4 ile gösterilen yönlendiriciyi kullanmaktadır,
- Saldırgan (Şekil 2.17'de 2 ile gösterilmiştir) Windows 8 makineye ortadaki adam saldırısı yapmak istemektedir,
- Bu nedenle Windows 8 makinesinin ağ trafiğini kendi üzerine yönlendirmek için 'ARP Zehirlemesi' saldırısını yapacaktır,

- Bu saldırı başarılı olduğu zaman Windows 8 makinesinin ağ trafiği saldırgan makineye yönlendirilmiş olacaktır.

Saldırgan saldırıya başlamadan önce Windows 8 makinesinin varsayılan ağ geçidi ve ARP tablosu sırası ile Şekil 2.18'de ve Şekil 2.19'da gösterilmiştir. Şekil 2.18'de görüleceği üzere Windows 8 makinesinin varsayılan ağ geçidi IP adresi 192.168.15.1'dir. Şekil 2.19'da görüleceği üzere ise 192.168.15.1 IP adresinin MAC adresi 52-54-00-12-35-00'dır.

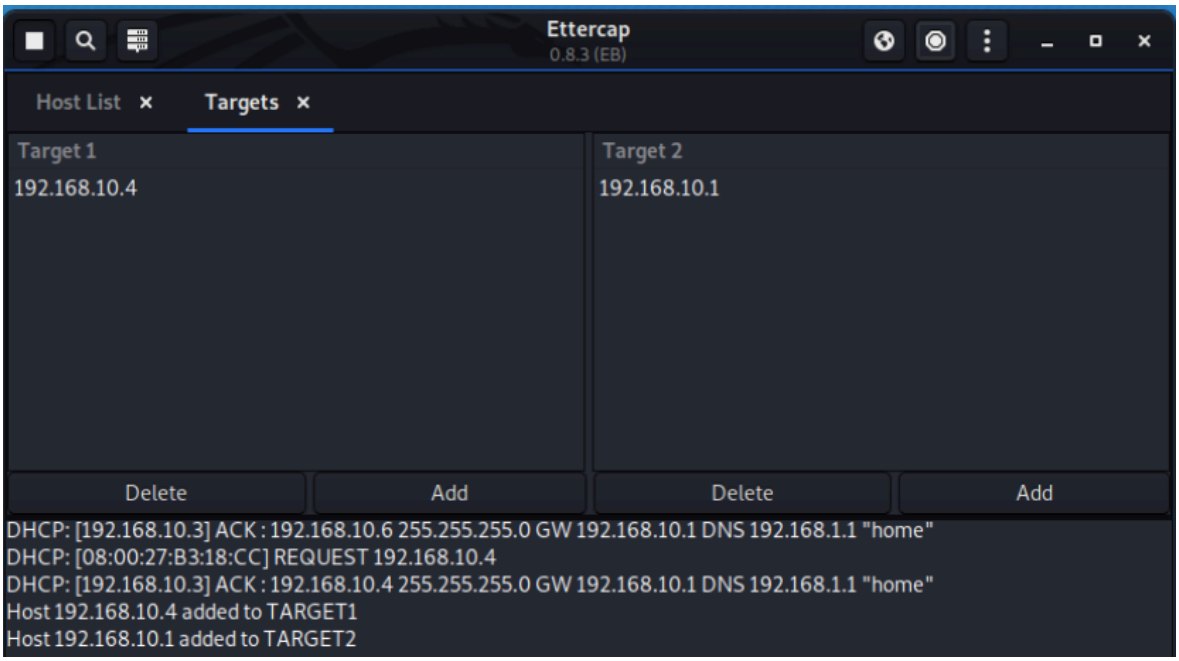


Şekil 2.18. Windows 8 makinesinde varsayılan ağ geçidi



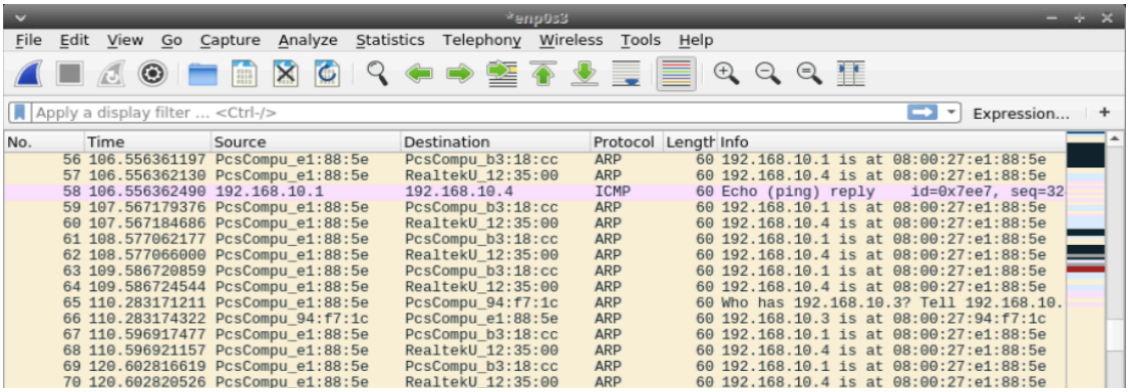
Şekil 2.19. Windows 8 makinesinde saldırı öncesi ARP tablosu

Saldırgan ‘ARP Zehirlemesi’ saldırısını kullanarak Windows 8 makinesi üzerinde bulunan 192.168.15.1 IP adresine ait MAC adresini kendi MAC adresi ile değiştirecektir. Saldırganın kullandığı Ettercap uygulamasına ait ekran görüntüsü Şekil 2.20’de gösterilmiştir.

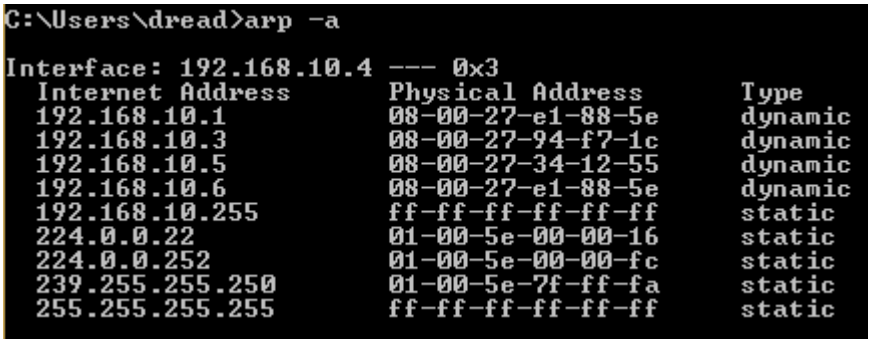


Şekil 2.20. Ettercap ekran görüntüsü

Saldırgan tarafından yapılan saldırıyı takip etmek için kullanılan Wireshark uygulamasında saldırı sırasında yakalanan ağ trafiği Şekil 2.21’de gösterilmiştir. Saldırgan başarı ile saldırısını gerçekleştirdikten sonra Windows 8 makinesi üzerindeki varsayılan ağ geçidine ait MAC adresi değiştirilmiş ve Windows 8 makinesinin ağ trafiği artık saldırgan makinesine yönlendirilmiştir. Saldırı sonrası Windows 8 makinesi üzerinde yer alan ARP tablosu Şekil 2.22’de gösterilmiştir.

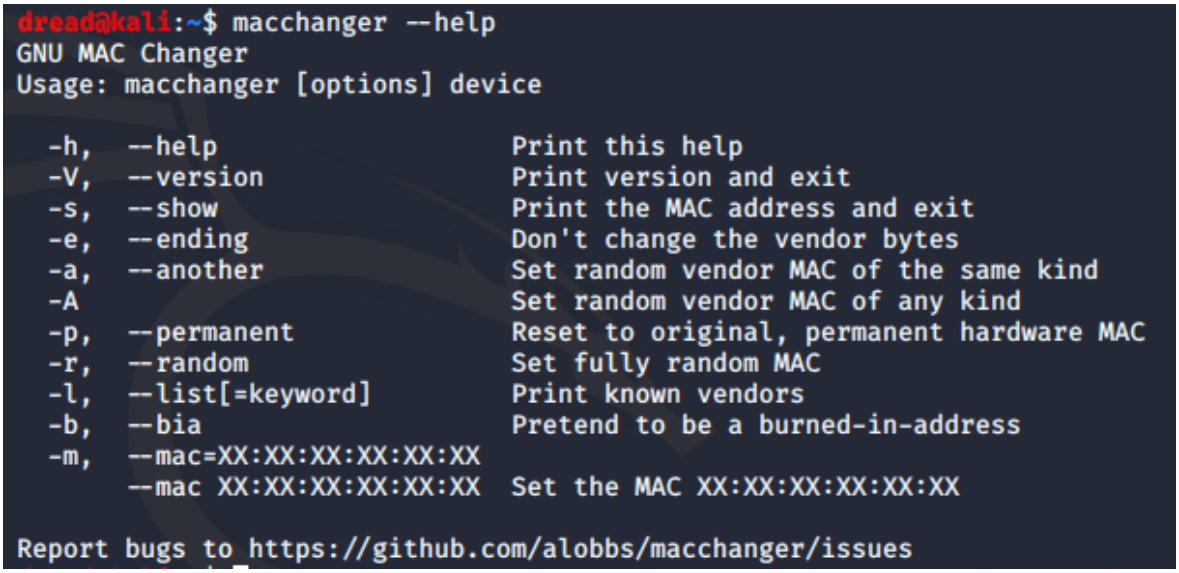


Şekil 2.21. ARP (Address Resolution Protocol) Zehirlemesi

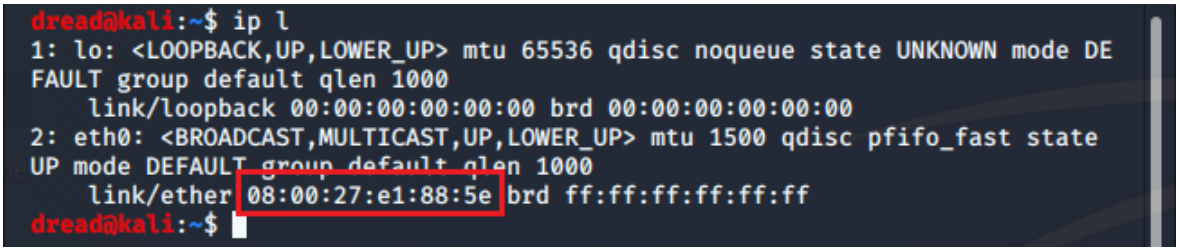


Şekil 2.22. Saldırı başarılı olduktan sonra yeni ARP tablosu

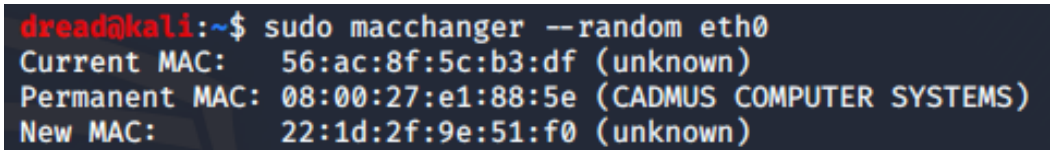
İkinci olarak MAC kafesleme saldırısı tanımlanacaktır. Bu saldırının amacı ağ üzerinde var olan bir MAC (Media Access Control) adresini kopyalayıp erişim kontrol kurallarını atlatmaktır [33]. Bir saldırgan yetkili bir bilgisayarın MAC adresini kopyalayarak ağ üzerinde servis dışı bırakma, oturum çalma (session hijacking), vb. saldırılar yapabilir. MAC adresleri ağ ara yüz donanımlarına üretildikleri fabrikalar tarafından tanımlanır ve her bir ağ arayız cihazının MAC adresi tekildir. Buna rağmen belli yazılımlar kullanılarak MAC adreslerini değiştirmek mümkündür. Şekil 2.23'te MAC adresi değiştirmek için kullanılabilecek uygulamalardan biri olan 'macchanger' gösterilmiştir. Bu uygulama kullanılmadan önce bilgisayarın MAC adresi Şekil 2.24'te 08:00:27:e1:88:5e olarak görülmektedir. Örnek teşkil etmesi amacı ile uygulamayı çalıştırıp rastgele bir MAC adresi atamasını istedikten (Şekil 2.25'de gösterilmiştir) sonra MAC adresinin değiştiği Şekil 2.26'da gösterilmiştir



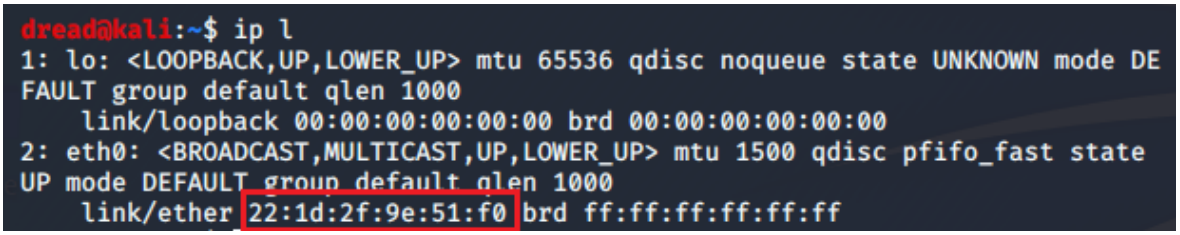
Şekil 2.23. MAC (Media Access Control) adresi değiştirme uygulaması



Şekil 2.24. MAC adresi değişmeden önce



Şekil 2.25. Yeni MAC adresi atanması



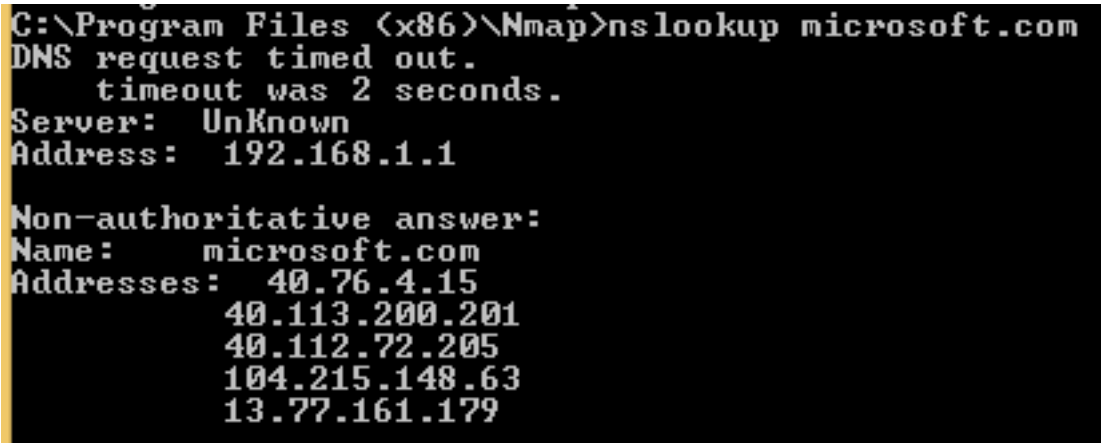
Şekil 2.26. Yeni MAC adresinin doğrulanması

Son olarak DNS Sahteciliği saldırısı tanımlanacaktır. DNS (Domain Name System – Alan Adı Sistemi); İnternet üzerinde bulunan alan adlarının tanımlanmasını sağlar. Örnek olarak microsoft.com alan adına ait bir A sınıf kaydı sorgu yapıldığı zaman, bu alan adına karşılık gelen IPv4 adresi öğrenilebilir. Bu sorgunun yapıldığı sistem, sorgu yapılan alan adından sorumlu olan DNS'tir. Anlaşılacağı üzere DNS'ler İnternet üzerinde çok önemli bir rol oynamaktadır.

DNS Sahteciliği saldırısının amacı; kurban bilgisayar üzerindeki DNS önbelleğini bozmaktır. Bu sayede saldırgan kurbanının sahte İnternet adreslerine yönlendirebilir. Bu teknik ortadaki adam saldırıları sırasında sıkça kullanılmaktadır [44]. Test ortamında gerçekleştiren saldırı senaryosu aşağıda anlatılmıştır:

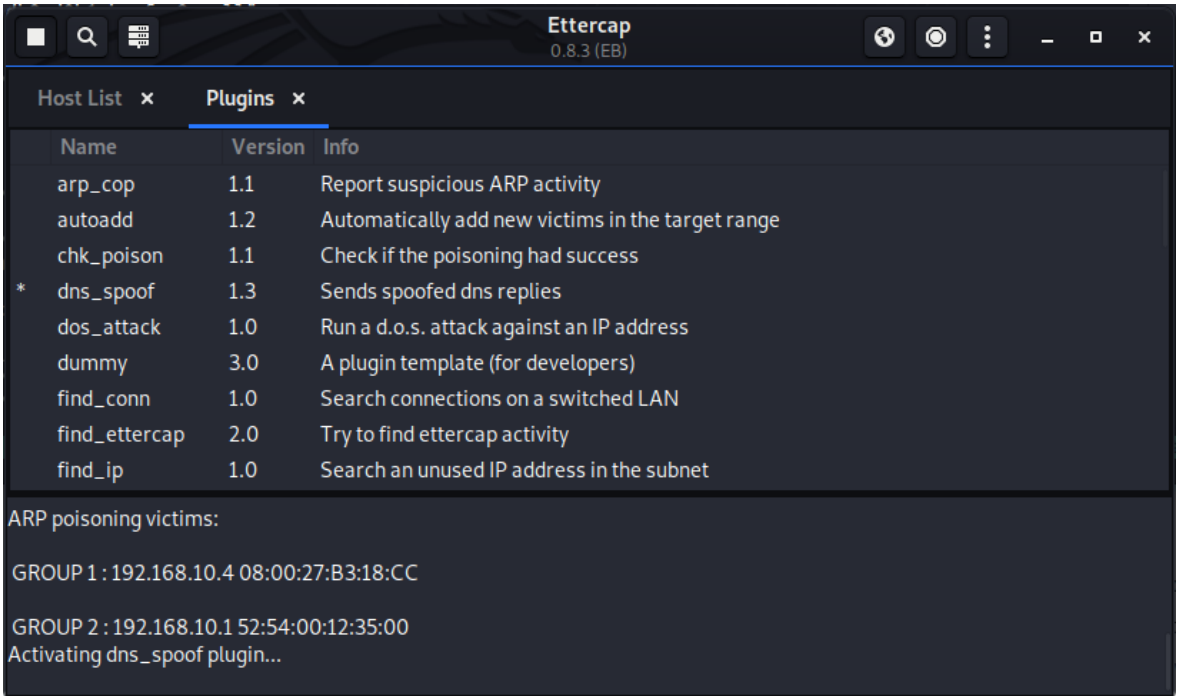
- Şekil 2.17'de 2 ile gösterilmiş olan saldırgan Şekil 2.17'de 1 ile gösterilen kurbanın Microsoft giriş bilgilerini elde etmek istiyordur.
- Bu nedenle saldırgan microsoft.com alanını DNS Sahteciliği saldırısını kullanarak kendi sunduğu alana yönlendirecektir.

DNS Sahteciliği saldırısını yapmadan önce kurban makinesinden microsoft.com alanının IPv4 adresini sorgulandığında Şekil 2.27'de gösterilen cevap alınacaktır.



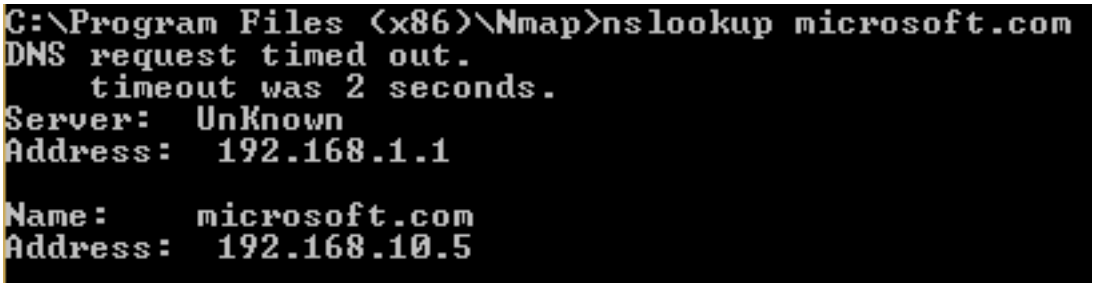
Şekil 2.27. Saldırı öncesi yapılan DNS (Domain Name System) sorgusu

Saldırgan, saldırısı için Ettercap aracını kullanacaktır. Bu saldırıyı başarılı bir şekilde yapabilmek için önce ARP Zehirlemesi yaparak DNS sorgularını kendine yönlendirecek, daha sonra ise gelen DNS sorgularından kendi seçtiklerini zararlı içeriğe yönlendirecektir. Saldırı yapılışı Şekil 2.28'de gösterilmiştir.



Şekil 2.28. Ettercap DNS Sahteciliği saldırısı

Saldırı başladıktan sonra kurbanın makinesinden microsoft.com DNS sorgusu tekrarlandığında Şekil 2.29'da gösterilen sonuç dönecektir. Bu saldırı sayesinde saldırgan başarılı bir şekilde microsoft.com alanını farklı bir IP'ye yönlendirmiştir.



Şekil 2.29. DNS Sahteciliği saldırısı sonrası

3. SİBER SALDIRI TESPİTİ

Saldırı tespit sistemleri (IDS - Intrusion Detection System), bir kişinin bir sistemi ihlal etmeye çalıştığını gösteren işaretleri algılamak ve sistem yöneticisine şüpheli bir etkinlik olduğunu bildirmek üzere tasarlanmıştır. STS'ler son yıllarda çok daha yaygın bir şekilde kullanılmaktadır. STS, bir uç nokta, güvenlik duvarı veya sistem üzerinde, bütün iç yönlü ve dış yönlü ağ trafiğini inceler ve güvenlik ihlali oluşturabilecek kalıpları (pattern) arar. Örneğin, STS bir sistem üzerinde her porta aynı kaynak IP adresinden sırayla bir dizi paket gönderildiğini tespit ederse, bu muhtemelen bahsedilen sistemin Cerberus gibi bir ağ tarama yazılımı tarafından tarandığını gösterir. Bu da genellikle sistemin güvenliğini ihlal etme girişimi için bir başlangıç olduğundan, birisinin sisteme sızmak için yaptığı hazırlık tespit edilmiş olur. STS, aynı IP adresinden kısa bir süre içinde anormal derecede büyük bir paket akışını da algılayabilir. Bu bir DoS saldırısına işaret edebilir. Her iki durumda da bunlar ağ yöneticisinin bilmesi gereken ve önlemek için adımlar atması gereken durumlardır [45].

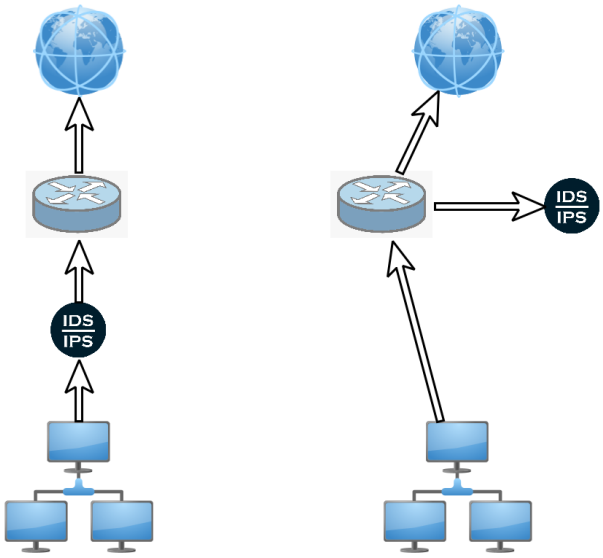
3.1. Saldırı Tespit Sistemleri Sınıflandırılması

Bu sistemler; ‘Uç Nokta Tabanlı’ ve ‘Ağ Tabanlı’ olmak üzere iki ana kategoride sınıflandırılırlar.

3.1.1. Ağ tabanlı saldırı tespit sistemleri (Network-based Intrusion Detection Systems - NIDS)

NIDS; ağ trafiğini dinleyip, bu trafik içinde zararlı ya da daha fazla analize ihtiyaç olan veri olup olmadığını kontrol eder. NIDS, dinleme (promiscuous) modunda olan bir ağ ara yüz kartına, ağ trafiğinin bir kopyası yönlendirilerek kullanılır. Bu sayede canlı ağ trafiği, üzerinde hiçbir değiştirme yapılmadan pasif bir şekilde incelenmiş olur. Ağ trafiğinin kopyalanması için ağ anahtarları üzerinde aynalama portu (mirror port) oluşturulur. Bu portun amacı ağ anahtarı üzerinden geçen bütün paketlerin bir kopyasının oluşturulması ve bu porta yönlendirilmesidir. Böylece birçok port üzerinden geçen ağ trafiği tek bir port üzerinden izlenebilmektedir. NIDS, zararlı trafiği tanımlayabilmek için bir çeşit imza ya da parmak izi verisi kullanır. Bu veriler genellikle paketlerin veri taşıyan veri yükü (payload) bölümünde yer alan zararlı içeriğe aittir. Buna ek olarak paketlerin başlık kısmında yer alan IP ve TCP/UDP bilgileri de incelenebilir. Bunun nedeni; bilinen bir zararlı komuta kontrol sunucusu adresi gibi bilgilerin başlık kısmında içerilmesidir [46].

Snort ve Suricata yaygın olarak kullanılan NIDS teknolojileridir. İmza tabanlı çalışan bu uygulamalar, veri akışına seri ya da paralel olarak bağlanabilirler. Şekil 3.1'de bahsi geçen uygulamaların ağda konumlandırılması gösterilmiştir. İki uygulamada önceden belirlenmiş bir imza veri tabanı kullanmaktadır. Bu imzalar sık sık güncellenerek sistemlerin en güncel zararlı trafiğe karşı korunmasını amaçlamaktadır. Şekil 3.2'de örnek bir Snort kural listesi ve Şekil 3.3'te bir kuralın detayları gösterilmiştir.

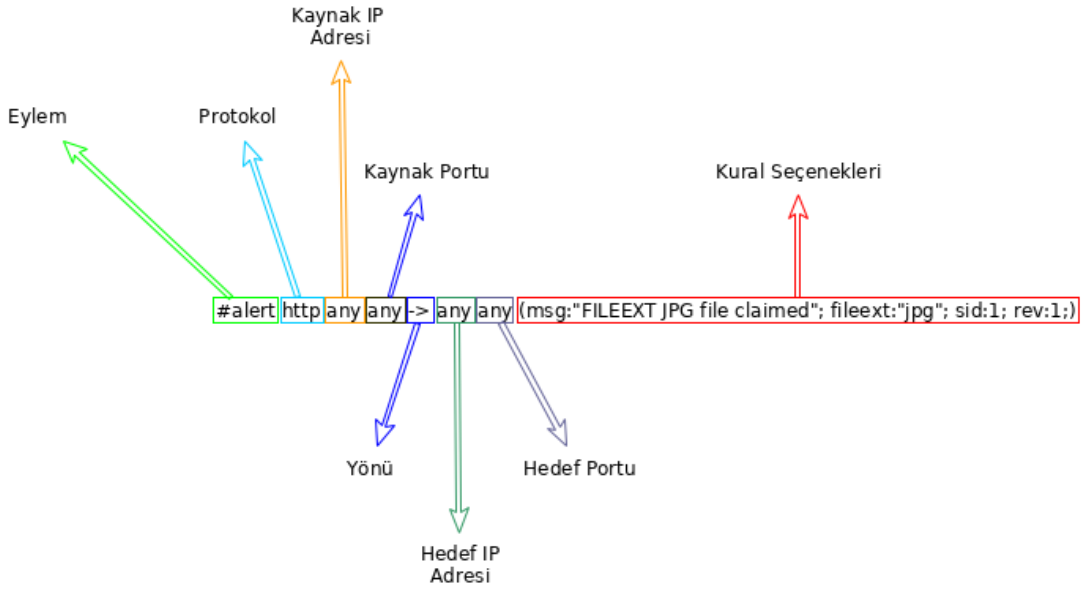


Şekil 3.1. Ağda NIDS (Network-based Intrusion Detection System) konumlandırılması

Legend: Default Enabled · Enabled by user · Auto-enabled by SID Mgmt · Action/content modified by SID Mgmt · Rule action is alert · Default Disabled · Disabled by user · Auto-disabled by SID Mgmt · Rule action is drop

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	⚠	1	2260000	ip	any	any	any	any	SURICATA Applayer Mismatch protocol both directions
✓	⚠	1	2260001	ip	any	any	any	any	SURICATA Applayer Wrong direction first Data
✓	⚠	1	2260002	ip	any	any	any	any	SURICATA Applayer Detect protocol only one direction
✓	⚠	1	2260003	ip	any	any	any	any	SURICATA Applayer Protocol detection skipped
✓	⚠	1	2260004	tcp	any	any	any	any	SURICATA Applayer No TLS after STARTTLS
✓	⚠	1	2260005	tcp	any	any	any	any	SURICATA Applayer Unexpected protocol

Şekil 3.2. Örnek kural listesi



Şekil 3.3. Bir kuralın incelenmesi

3.1.2. Uç nokta tabanlı saldırı tespit sistemleri (Host-based Intrusion Detection Systems - HIDS)

HIDS; sadece takip edeceği bilgisayara uygulama olarak kurulabilir. HIDS gibi sadece önemli birkaç noktaya kurulmak yerine birçok bilgisayara kurulur. Bunun avantajları ve dezavantajları vardır. Eğer HIDS'in kurulu olduğu bilgisayar ele geçirilmişse, zararlı aktiviteler kendilerini HIDS'den saklayabilirler. Buna rağmen HIDS doğrudan kaynak üzerinde çalıştığı ve kaynak üzerinde bulunan dosyalara ve çalışan uygulamalara erişebildiği için NIDS'e göre daha fazla bilgiyi inceleyebilir. En bilinen açık kaynak HIDS'ler OSSEC ve Samhain'dır. Bu iki uygulama da kayıt dosyaları, dosya bütünlüğü takibi, bilinen rootkit'leri tespit teknikleri ve diğer zararlı trafik tespit teknikleri gibi yerel kaynaklara yönelik incelemeler yapmaktadırlar [46].

HIDS, NIDS'e ek olarak bütün bağlantı akışını inceleyebilir. NIDS'i atlatmak için kullanılan parçalama saldırıları (fragmentation attacks) veya oturum birleştirme (session splicing) gibi teknikler uygulanamaz. Çünkü HIDS işletim sistemine sunulduğu şekliyle tamamen yeniden birleştirilen oturumu inceleyebilir. HIDS kaynakta ağ trafiği şifrelenmeden veya şifresi açıldıktan sonra inceleyebilir. Bu sayede şifreleme kullanan ağ trafiğini de kurallara tabi tutup imza taraması yapabilir [45].

3.2. Saldırı Tespit Sistemlerinin Tespit Yöntemleri

Ağ tabanlı saldırı tespit sistemleri farklı tespit metotları kullanırlar. Bu metotlar aşağıda sıralanmıştır [47]:

- Desen Eşleştirme (Pattern Matching)
- Protokol Analizi
- Anomali Analizi (Anomaly-based Analysis)
- Evrensel Tehdit Korelasyon Yetenekleri (Global threat correlation capabilities)
- Dosya Bütünlük Kontrolü
- Kayıt Defteri Denetimi

Bahsi geçen metotların kısa açıklamaları aşağıda yapılmıştır.

3.2.1. Desen eşleştirme

Bir veri paketi ağda hareket ederken üzerinde belli bir bit sıralaması içeriyor mu diye incelenir. Genelde bu inceleme belli bir prokol için yapılmaktadır. Protokoller ve bu protokollerin eşleştiği servisler; hedef IP adresi, hedef port kaynak IP adresi, kaynak port, vb. bilgiler ile belirlenebilir. Desen eşleştirme yöntemi ile her ağ paketi üzerinde yapılan işlem yoğunluğu azaltılmış olsa da bu yöntem kısıtlı bir tespit imkanı sağlar.

Bu yöntem imza tabanlı bir denetim mekanizmasıdır. Örneğin 5656 numaralı hedef portuna gönderilen ‘deadbeaf’ söz dizimi bir imza örneği olarak verilebilir. Desen eşleştirme yöntemi eğer bir ağ paketinde bu bilgileri bulursa o zaman alarm üretir [47].

Bu yöntem çok fazla sahte pozitif veri üretebilmektedir. Örnek olarak Suricata sisteminin kullandığı imzalardan bir kısmı Linux işletim sistemi güncellemeleri ile ilgidir. Bu imzalar geçerli olan bir güncelleme işlemini bir tehdit olarak gösterebilmektedir.

3.2.2. Protokol analizi

Saldırı tespit sistemleri genellikle ağ verisine bulunan IP, port ve protokol bilgileri ile ilgilenirler. Gelişmiş sistemler ise bu bilgilerin yanında ağ trafiğini oluşturan verinin protokolünü detaylı bir şekilde inceleme kabiliyetine sahiplerdir. Bu kabiliyet, sistemin bahsi geçen protokolün bütün detaylarına hakim olması ile olur. Eğer saldırı tespit sistemi protokolün resmi tanımlı halini bilirse, veri paketini bu bilgiye göre işleyip protokolde olabilecek aykırılıkları tespit edebilir. Bu yöntem ile hem bilinen hem de bilinmeyen saldırılar engellenebilmektedir. Bu yöntem saldırı imzası gerektirmediği için sezgisel tespit yöntemleri arasında yer almaktadır [48].

3.2.3. Anomali analizi

Anomali ya da aykırılık alışıla geldik dışında bir faaliyeti ifade eder. Bu faaliyetler genelde bir saldırı göstergesi olabilir. Eğer bir kullanıcının davranışı beklenen davranıştan farklılık gösterirse burada bir aykırılık oluşmuştur. Anomali analizinde bir sıkıntı, bu tespit sistemlerinin çok fazla yanlış pozitif değer üretebilmesidir. İzinli bir faaliyet bu sistemler tarafından bir aykırılık olarak algılanabilmektedir. Buradaki zorluk normal davranışı ifade eden bir model oluşturmaktadır çünkü normal davranışı ifade edebilecek bütün seçeneklerin tanımlanması gerekmektedir. Bir modelleme yapmak için bütünsel yaklaşmak yerine aşağıda bahsi geçen üç yöntemden birinin kullanılması, bir model oluşturulmasını kolaylaştırmaktadır [49]:

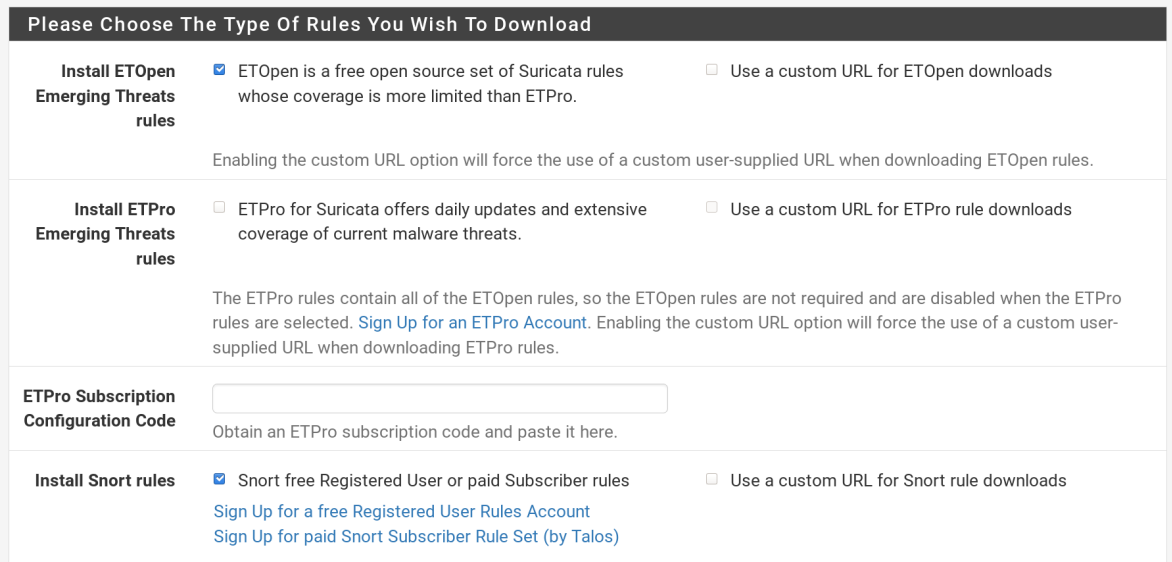
1. Genel, herkes tarafından uygulanan, davranışı modellemek yerine aynı işi yapan grupların davranışlarının modellenmesi daha kolaydır. Burada amaç bütün kullanıcıları bir arada modellemek yerine, birbirine benzer işler yapan kullanıcıları gruplayıp bu grupların davranışsal modellerini çıkarmaktır. Küçük gruplar halinde davranışsal model çıkarmak, bütün kullanıcıları bir bütün olarak modellemekten daha kolaydır.
2. Davranışların tek tek elle modellenmesi yerine doğru davranışı kendi kendine öğrenen bir sistem modellenebilir.
3. Bir saldırıyı gerçek zamanlı olarak tespit etmek çok zordur. Saldırıyı gerçekleştirmek için kullanılacak komut serisi farklı şekillerde girilebilir. Birçok durumda kullanıcıların bir oturumluk hatta bir günlük davranışlarını izlemek, saldırı tespiti için yeterli olmaktadır.

3.2.4. Evrensel tehdit korelasyon yetenekleri

Yeni nesil Saldırı Tespit Sistemleri, evrensel verilere anlık olarak erişip bu veriler doğrultusunda uyarı üretebilmektedirler. Tehdit istihbarat firmaları büyük veri analizi yaparak bir tehdit verisi oluşturmaktadır. Bu veri ücretsiz olduğu gibi bir üyelik te gerektirebilmektedir. Yeni nesil sistemler, tehdit istihbarat sağlayıcılarının kaynaklarına erişip en güncel veriyi çekebilmektedir. Tehdit istihbaratı firmaları, dünyanın farklı bölgelerine yayılmış detektörlerinden topladıkları veriyi korelasyon kurallarından geçirdikten sonra bir itibar bilgisi üretmektedirler. İtibar bilgisi; bir IP'nin geçmiş

eylemlerini de göz önünde bulundurarak oluşturulmaktadır. Günümüzde IP itibar bilgisi güvenilir bir kaynak olarak kullanılmaktadır [47].

Örnek olarak Snort isimli Saldırı Tespit Sisteminin kullanımı verilebilir. pfSense güvenlik duvarı ile bütünleşmesinden sonra Snort, internet üzerinde bulunan tehdit istihbarat kaynaklarından veri toplayıp, bu verileri saldırı tespitinde kullanabilmektedir. Şekil 3.4'te Snort'a ait tehdit istihbarat verilerinin ayarlanması görülmektedir.



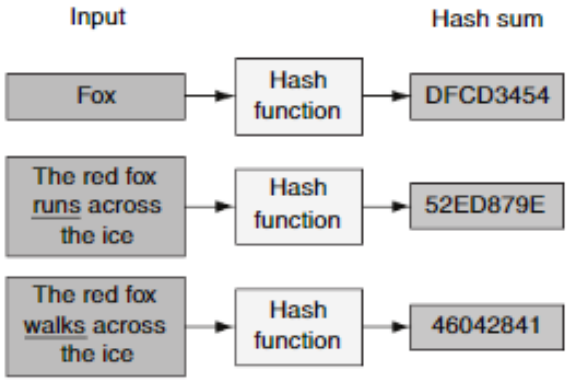
Şekil 3.4. Snort Tehdit İstihbaratı Toplama Ekranı

Evrensel kaynaklardan elde edilen veriler Snort'un kural veri tabanında saklanmaktadır. Şekil 3.5'te bu kaynaklardan elde edilen bir kural gösterilmiştir.

Şekil 3.5. Snort Tehdit Tespit Kuralı

3.2.5. Dosya bütünlük kontrolü

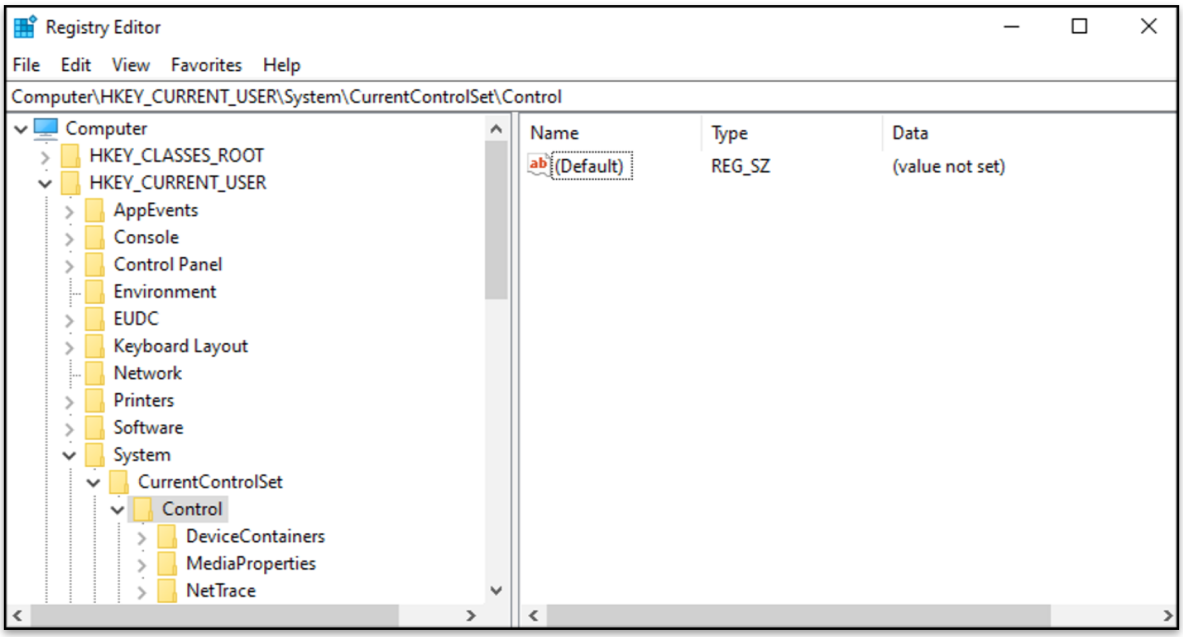
Bir işletim sistemindeki her dosya, şifreleme karması (cryptographic hash) olarak da bilinen benzersiz bir dijital dosya oluşturur. Bu dosya parmak izi, dosyanın adı ve içeriği temel alınarak oluşturulur. HIDS, birisi ya da bir şey dosya içeriğini değiştirdiğinde ya da dosyayı tamamen farklı bir dosya sürümüyle değiştirdiğinde, bu dosyadaki değişiklikleri tespit etmek için önemli dosyaları izleyebilir. Şekil 3.6'da şifreleme karması ile ilgili bir görsel paylaşılmıştır. [50].



Şekil 3.6. Şifreleme karması örneği

3.2.6. Kayıt defteri takibi

Sistem kayıt defteri, Microsoft Windows işletim sistemindeki tüm donanım ve yazılım ayarları, işletim sistemi yapılandırmaları ve kullanıcılar, gruplar ve tercihlerin tutulduğu bir dizin listesidir. Kullanıcılar ve sistem yöneticileri tarafından sistemde yapılan değişiklikler sistem kayıt defteri anahtarlarına kaydedilir, böylece oturum kapatıldığında veya sistem yeniden başlatıldığında değişiklikler kaybolmamış olur. Kayıt defteri ayrıca sistem çekirdeğinin (kernel) donanım ve yazılımla nasıl etkileşime girdiğine de bakılmasına olanak tanır. HIDS, bir kullanıcının veya uygulamanın yeni bir yükleme yapmadığından veya mevcut bir uygulamayı kötü amaçlı bir uygulamayla değiştirmediğinden emin olmak için önemli kayıt defteri anahtarlarında yapılan bu değişiklikleri izleyebilir. Örneğin, bir parola yönetimi yardımcı programı, kötü amaçlı bir yürütülebilir dosya ile değiştirilebilir ve kayıt defteri anahtarı, kötü amaçlı kopyaya işaret edecek şekilde değiştirilebilir [50]. Şekil 3.7'de Windows kayıt defteri ve içinde yer alan dizin yapısı gösterilmiştir.



Şekil 3.7. Windows kayıt defteri

3.3. Ağ Denetimi

Her bir ağ cihazı üzerinden akan trafiğin kaydını merkezi bir kayıt toplama aracına göndermelidir. Ağ cihazlarının farklı kabiliyetleri olduğu için bu kayıtlar farklılık gösterebilir. Ayrıca ham ağ trafiği de kayıt edilebilir.

3.3.1. Akış kontrolü (Flow Control)

Akış; aynı kaynak adresi, hedef adresi, kaynak portu, hedef portu ve protokol bilgisine sahip ağ paketleridir. Akış kaydı, akış bilgisinin bir özetidir. Hangi kaynak, hangi hedefle, saat kaçta, hangi protokolü kullanarak haberleştiğini göstermektedir. Bir akış analiz sistemi bahsi geçen bütün bu bilgileri toplar, saklar ve üzerinde arama yapılabilecek bir yapıda kullanıcısına sunar. Akış kayıtları bir ağ üzerinde olan bütün olayları özetler. Akış bilgisi özet olduğu için büyük bir veri kaynağı değildir. Örneğin yazarın çalışmış olduğu veri merkezine üç yılda saklanan toplam akış verisi 100 GB boyutundadır ki bu boyut modern veri kaynakları ile karşılaştırıldığı zaman çok küçük kalmaktadır. Bir paket süzme uygulaması ağ trafiği üzerinde çok detaylı (istemcileri eriştiği web adresleri, indirdikleri dosyalar vb.) veri elde edebilmesine rağmen bu verinin büyüklüğü nedeniyle üzerinde analiz yapmak zorlaşmaktadır. Akış verisi bu bilgilerin bir özeti niteliğinde olduğu için, bu bilgi kullanılarak analiz yapmak çok daha kolaydır. Akış bilgisi her ne kadar limitli bir bilgi gibi

görünse de NSA benzer bir yaklaşımı teröristleri yakalamak için kullanmaktadır. Benzer olarak AT&T firması akış analizi yaparak birçok olayı çözmüştür [51].

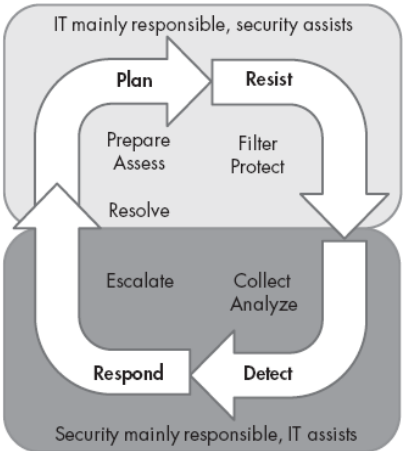
Birçok ağ cihazı akış verisi üretebilmektedir. Bu verinin üretilemediği durumlarda ağ anahtarları üzerinde oluşturulacak bir ayna portu ile veri toplanması sağlanabilir. 'nprobe' isimli uygulama veri toplamak için kullanılabilecek uygulamalara bir örnektir.

Akış verisi üretilmeye ya da toplanmaya başladıktan sonra merkezi bir yerde toplanmalı ve kullanıcı için analiz imkanı sağlanmalıdır. Elastiflow uygulaması ile akış verileri bir merkezde toplanıp görselleştirilebilir. Şekil 3.9'de Elastiflow'un akış verisini nasıl görselleştirdiği gösterilmiştir.

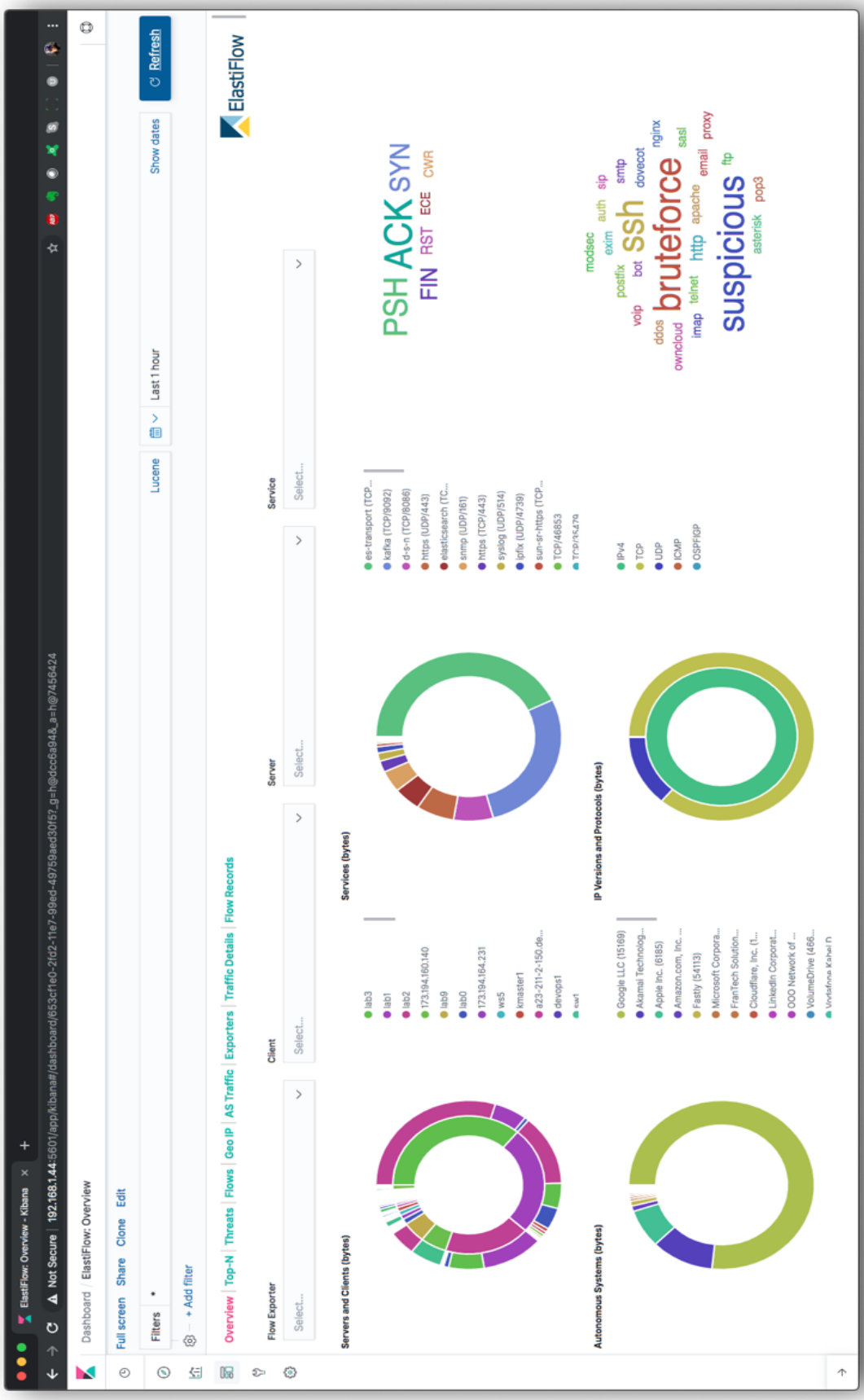
AT&T ve NSA örneklerinden anlaşılabileceği gibi akış verisi bir ağ üzerinde olan olayların takibi ve tespiti için önemli bir rol oynamaktadır.

3.3.2. Ağ güvenlik takibi (Network Security Monitoring)

Ağ güvenlik takibi kavramı ilk olarak 1988'de Todd Heberlein tarafından geliştirilen 'Network Security Monitoring' aracı sonrasında ortaya çıkmıştır. Bu araç ağ verisini kullanarak saldırı tespit yapan ilk araçtır. Günümüzde siber güvenliğe önem veren kurumlar bünyelerinde 'Bilgisayar Olaylarına Müdahale Ekipleri' bulundurmaktadırlar. Bu ekiplerin amacı kurum içinde bir siber olay yaşandığı zaman, olayın kaynağını tespit etmek ve tehdit hala aktif ise bu tehdidin giderilmesinde rol almaktır. Şekil 3.8'da siber güvenlik ekipleri ile sistem yöneticileri arasındaki bağ gösterilmektedir [52]. Güvenlik ekipleri korudukları sistem ile ilgili veri toplayıp bu veri üzerinde analizler yapmaktadırlar. Analizleri sonucunda bir olay olduğu sonucuna varırlarsa, bu olaya müdahale için sistem yöneticilerinden destek alırlar.



Şekil 3.8. Kurum Güvenlik Döngüsü



Şekil 3.9. Elastiflow Ekran Görüntüsü

Bir olayın tespit edilebilmesi için gerekli olan veri ‘Ağ Güvenlik Takibi’ sistemleri tarafından sağlanabilmektedir. Bu sistemler; Anti Virüsler, Güvenlik Duvarları, Saldırı Önleme Sistemleri, vb. gibi engelleme ya da filtreme yapamazlar. Bu sistemlerin amacı bahsi geçen sistemlerin sürekliliğini takip etmek ve bahsi geçen sistemlerde beklenmeyen bir durum oluşması halinde uyarı üretmektir.

ICT sistemlerinde birbirinden farklı ve çok sayıda güvenlik ürünü kullanılsa da bu ürünlerde birer yazılımdır ve her yazılım gibi kötü niyetli kişiler tarafından istismar edilebilmektedirler. Bir yazılım beklenmeyen bir durumla karşılaştığı zaman bunu raporlamakta sıkıntı yaşayabilir. Bu nedenle ‘Ağ Güvenliği Takip’ sistemleri bu yazılımların takibini yaparak olası bir tersliği raporlayabilir ve bir zafiyet oluşmasını engelleyebilir.

Yaygın olarak kullanılan ‘Ağ Güvenliği Takip’ sistemlerinden biri Zabbix’tir[6]. Bu uygulama ağ üzerinde bulunan cihazları otomatik olarak bulup takip etmeye başlayabildiği gibi kullanıcı tanımlamaları yapılmasına müsaade ederek cihaz tanımlanmasını sağlayabilir. Şekil 3.10’da görülen örnek arayüzde, ICT sisteminde yer alan bir cihazın periyodik takibi görünmektedir.

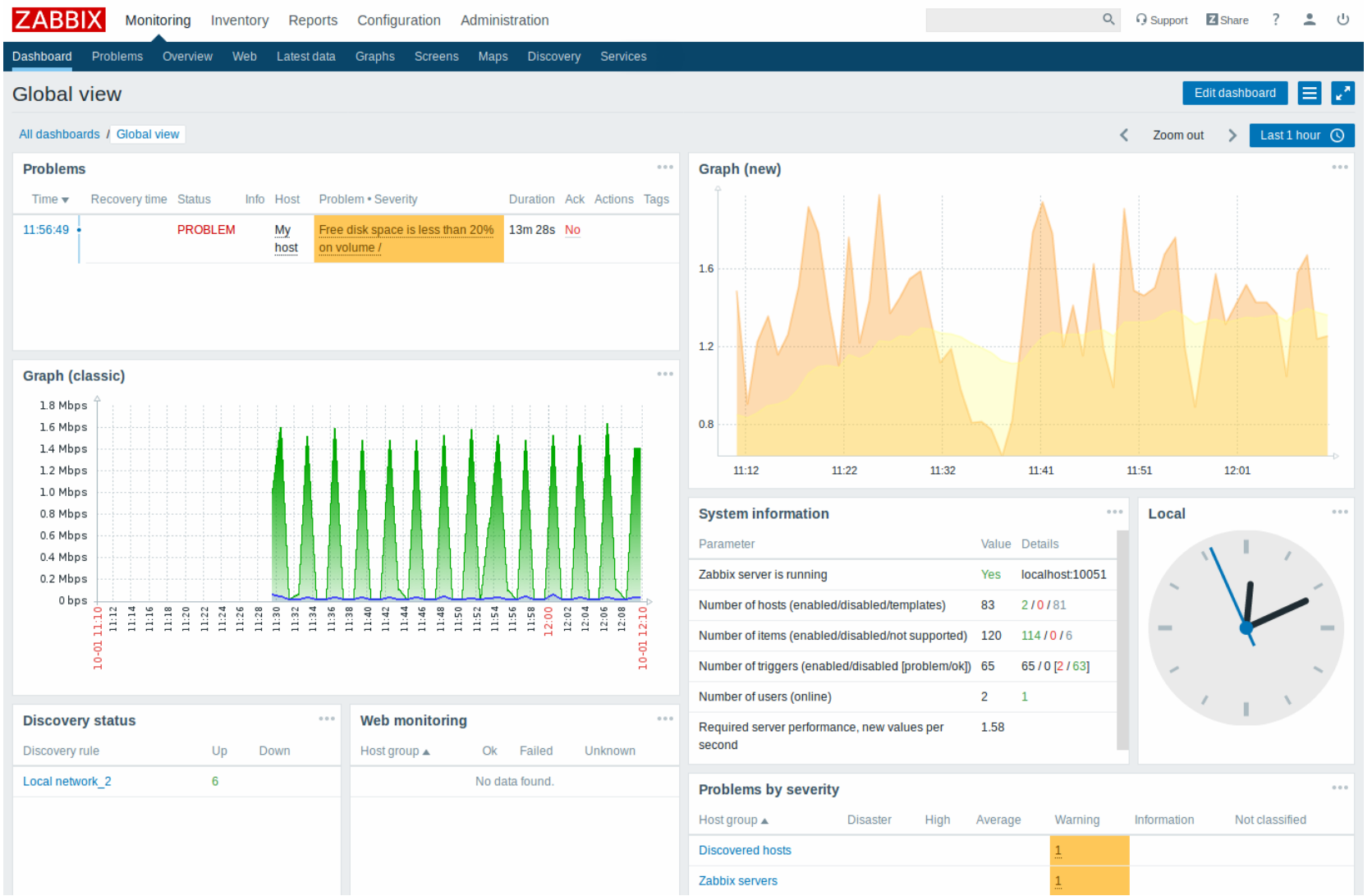
3.3.3. Vekil sunucu (Proxy Server)

Vekil sunucu istemciler ile sunucular arasında yer alır. İstemci, bir sunucuya doğrudan erişmek yerine önce vekil sunucuya erişir. Vekil sunucu istemcinin isteğini sunucuya iletir ve sunucudan gelen cevabı istemciye iletir. Vekil sunucular istemci istekleri üzerinde bir değişiklik yapmaz. Gelişmiş vekil sunucuların bir kural setine göre istekleri filtreleme özellikleri bulunabilmektedir.

Vekil sunucular aşağıdaki işlemleri gerçekleştirebilirler [53]:

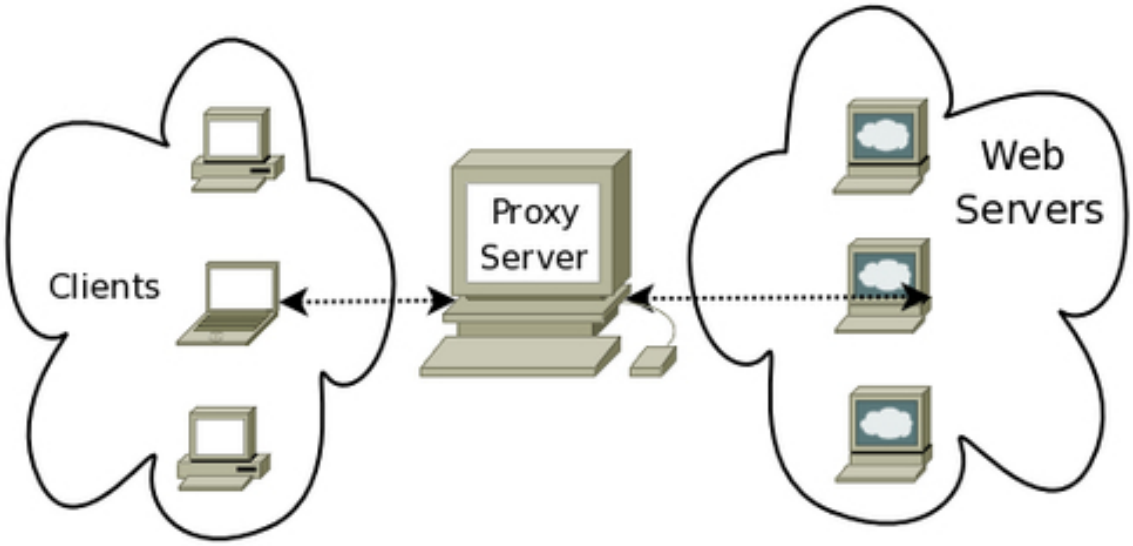
- İstemcilere ağ erişim kurallarının zorlaması,
- Kullanıcı trafiğinin izlenmesi ve kullanıcı/grup bazında rapor üretilmesi,
- Anti Virüs uygulamaları ile entegre olup, istemci istekleri ya da sunucu cevapları içerisinde var olabilecek zararlılara engel olunması,
- Kullanıcı ağının diğer ağlardan izole edilmesi.

[6] https://www.zabbix.com/documentation/4.2/_media/manual/web_interface/dashboard3.png? cache=



Şekil 3.10. Zabbix Kullanıcı Arayüzü

Şekil 3.11'de bir vekil sunucunun ICT sistemi içinde nasıl yerleştiği görülmektedir [53].



Şekil 3.11. Vekil Sunucu Kullanımı

Squid Proxy, vekil sunucular içinde çok yaygın olarak kullanılan bir vekil sunucudur. Önceden tanımlanmış kurallara göre istemciler ile sunucular arasındaki bağlantıyı yönetebilmektedir. Squid Proxy kullanılarak verinin istemci ve sunucu arasındaki trafiğini kontrolü yapılmasına ek olarak kullanıcı yönetimi de yapılabilmektedir. Yapılan bir istemin hangi kullanıcı tarafından yapıldığının bilinmesi, bir olay anında elde olması gereken önemli bir bilgidir. Squid Proxy için örnek bir yapılandırma Tablo 3.1'de gösterilmiştir.

Tablo 3.1. Basit bir squid proxy yapılandırması

```
1. acl ogretmenler src 192.168.10.0/255.255.255.0
2. acl ogrenciler src 192.168.70.0/255.255.255.0
3. acl ogle_arasi time MTWHF 12:00-13:30
4. http_access deny localhost
5. http_access allow ogretmenler
6. http_access allow ogrenciler ogle_arasi time
7. http_access deny all
```

Bu yapılandırma incelendiğinde:

- 'acl' direktifleri ile üç adet filtre kuralı tanımlanmıştır.
  - Birinci satır ile öğretmenler ağı tanımlanmıştır.
  - İkinci satır ile öğrenciler ağı tanımlanmıştır.
  - Üçüncü satır ile Pazartesi'den Cuma'ya kadar her gün saat 12:00 ile 13:30 arası öğle arası zamanı olarak tanımlanmıştır.

- ‘http_access’ direktifi ile yetkili ve yetkisiz erişimler tanımlanmıştır.
    - Dördüncü satır ile yerel bağlantılar kısıtlanmıştır.
    - Beşinci satır ile birinci satırda tanımlanmış olan öğretmenler ağının istemlerine izin verilmiştir.
    - Altıncı satırda; ikinci satırda tanımlanan öğrenciler ağına, üçüncü satırda tanımlanan zaman aralığında istem yapma izni verilmiştir.
    - Yedinci satırda hiçbir kurala uymayan bağlantılar engellenmiştir.

Şekil 3.12’de tanımlı kurallara göre Squid Proxy’nin tuttuğu kayıtlar gösterilmiştir.

```
1586171819.198 171076 1.1.1.1 TCP_TUNNEL/200 5720 CONNECT adservice.google.com:443 earda
HIER_DIRECT/216.58.206.162 -
1586171819.199 170821 1.1.1.1 TCP_TUNNEL/200 5641 CONNECT adservice.google.com.tr:443 earda
HIER_DIRECT/216.58.206.162 -
1586171820.214 171576 1.1.1.1 TCP_TUNNEL/200 4762 CONNECT googleads.g.doubleclick.net:443
earda HIER_DIRECT/216.58.206.162 -
1586171822.245 171434 1.1.1.1 TCP_TUNNEL/200 5438 CONNECT fonts.googleapis.com:443 -
HIER_DIRECT/172.217.11.10 -
1586171823.261 171299 1.1.1.1 TCP_TUNNEL/200 1726095 CONNECT lh3.googleusercontent.com:443
earda HIER_DIRECT/172.217.169.161 -
1586171824.261 172663 1.1.1.1 TCP_TUNNEL/200 21973 CONNECT ssl.google-analytics.com:443 earda
HIER_DIRECT/172.217.169.168 -
1586171824.261 177157 1.1.1.1 TCP_TUNNEL/200 135134 CONNECT www.gstatic.com:443 earda
HIER_DIRECT/172.217.169.163 -
1586171825.276 170362 1.1.1.1 TCP_TUNNEL/200 68277 CONNECT encrypted-tbn0.gstatic.com:443
earda HIER_DIRECT/216.58.206.174 -
1586171856.309 209985 1.1.1.1 TCP_TUNNEL/200 2876879 CONNECT www.google.com:443 earda
HIER_DIRECT/172.217.12.132 -
```

Şekil 3.12. Squid Proxy kayıt örneği

Yukarıdaki örnekte görülebileceği gibi vekil sunucular bir ağ üzerinde oluşan olayların takibi ve kayıt altına alınmasında önemli rol oynamaktadır.

3.4. Uç Nokta Denetimi

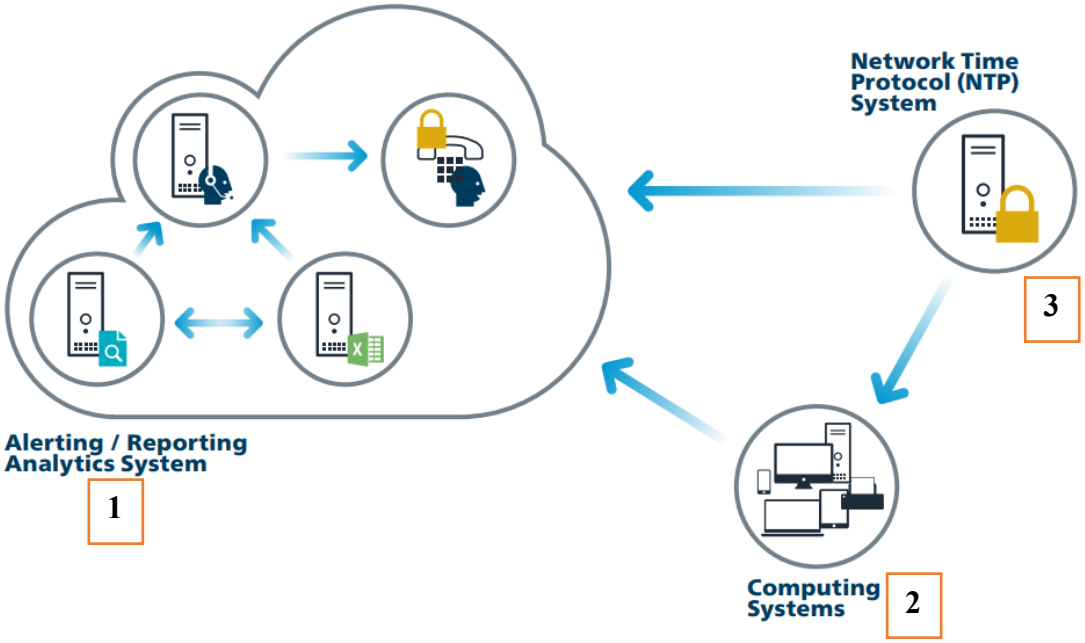
Uç noktalar üzerinde denetleme politikaları uygulanarak, uç noktaya giriş yapmış insanların kimlikleri, yapmış oldukları eylemler vb. denetlenir. Bu denetlemeler sonucunda oluşacak olan kayıtlar merkezi kayıt sisteminde toplanabilir.

3.4.1. Kayıt (Log) yönetimi

Kayıt tutma, eski denizcilik yöntemlerinden biridir. Kaptanlar yaptıklarını bir kayıt defterine yazarak hem üstlerine rapor vermiş hem de keşiflerini belgelemiş olmuşlardır. Benzer şekilde kayıt yönetimi bir ICT sistemi için de çok büyük önem taşımaktadır. Karmaşık yapıya sahip ICT sistemleri; Güvenlik Duvarları, Yönlendiriciler, Ağ Anahtarı, Sunucular, İş İstasyonları gibi birçok farklı cihazdan oluşmaktadırlar. Bütün bu cihazlar

kendilerine özgü kayıt verileri tutmaktadırlar. Tutulan bu veriler, cihazların üzerinde gerçekleşen olayların bir kaydıdır ve bu kayıtlar incelenerek cihaz üzerinde gerçekleşen veya gerçekleşmiş olaylar incelenebilir. 2018 Verizon Data Breach Investigation Report'a göre bir ICT sistemini zafiyete uğratan saldırıların %87'si bir dakikanın altında sürmüştür ve bu saldırıların %68'nin fark edilmesi aylar sürmüştür [54].

Bu rakamlar göz önüne alındığı zaman, doğru kayıt tutmanın ne kadar önemli olduğu anlaşılmaktadır. Center of Internet Security (CIS), kar amacı gütmeyen bir kurum olup, kurumların siber tehditlerle baş edebilmesi için profesyonel ICT çalışanlarınca hazırlanmış kaynaklar içermektedir. Bu kaynaklardan biri olan 'CIS Controls', altıncı bölümünde kayıt yönetimine değinmektedir. Şekil 3.13'te CIS'in kayıt yönetimi için hazırlamış olduğu ilişki diyagramı gösterilmektedir [55].



Şekil 3.13. CIS (Center of Internet Security) Kayıt Yönetimi

Diyagram üzerinde 1 ile kayıt yönetim sistemleri, 2 ile ICT sistemleri ve 3 ile zaman sunucu sistemleri gösterilmiştir. 1 ve 2 numaralı sistemler, 3 numaralı sistemden zaman bilgisi almaktadırlar. Zaman bilgisinin doğruluğu kayıt yönetimi için çok önemlidir. Gerek arıza tespit ederken gerekse zararlı bir faaliyeti araştırırken kayıt altına alınan bütün olayların zamanlarının aynı kaynağa göre eşzamanlı olması, verinin doğru şekilde yönetilebilmesi için önemlidir. Eşzamanlılık sağlandıktan sonra; 2 numaralı sistemler, 1 numaralı sistemlere ürettikleri kayıt bilgilerini gönderirler. Bu sayede bütün ICT sistem bileşenlerinin ürettiği kayıtlar merkezi bir noktada depolanmış olmaktadır. Merkezi kayıt yönetimi sayesinde farklı

kaynaklardan gelen kayıtlar tek noktadan incelenebilir ve aşağıda anlatılacak olan Bilgi Güvenliği ve Olay Yönetimi sistemleri yardımıyla uyarılar ürettirilerek sistem üzerinde izin verilmeyen faaliyetlerin tespiti sağlanabilir.

CIS tanımına göre kayıt yönetiminde ve analizinde olabilecek zafiyetler; saldırganların yerlerini, kötücül yazılımlarını ve kurban cihazlar üzerindeki faaliyetlerini gizlemelerine olanak sağlar. Bu zafiyet kurban bir saldırı olduğunun farkında dahi olsa, saldırının nereden geldiğinin, ne yaptığının ve sonraki adımların ne olacağının anlaşılmasına engel teşkil eder. Kurumların sağlam bir kayıt yönetimi olmadığı sürece saldırganlar fark edilmeden faaliyetlerini gerçekleştirebilir ve kurumlara geriye dönüşü olmayan zararlar verebilirler. Bazı koşullarda başarı ile gerçekleşmiş bir saldırının fark edilmesi için tek yöntem iyi bir kayıt yönetimidir. Saldırganlar, kurumların kayıt yönetim zafiyetlerinden yararlanarak, kurum içinde aylarca hatta bazen yıllarca fark edilmeden kalabilmektedirler [55].

CIS Controls bölüm 6 kayıt yönetimi ile ilgili sekiz adet kural tanımlamaktadır. Bu kurallar Şekil 3.14'te gösterilmiştir [55].

CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions
6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
6.2	Network	Detect	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.
6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
6.4	Network	Detect	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.
6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
6.6	Network	Detect	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis.
6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.
6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

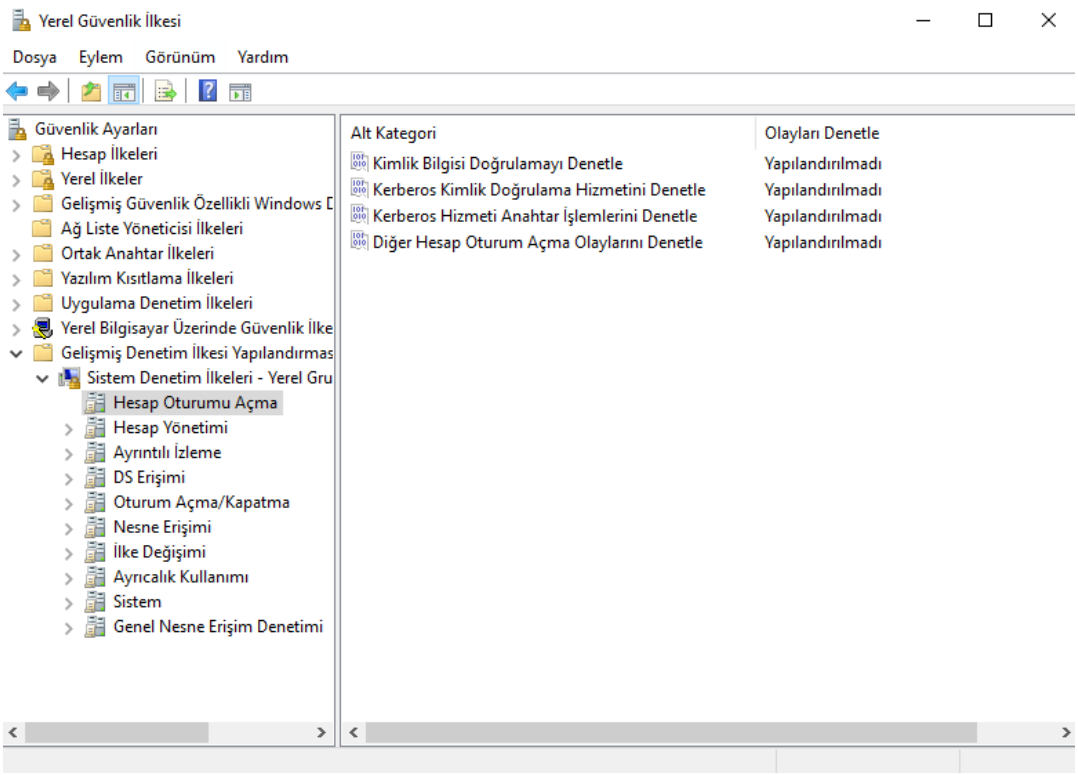
Şekil 3.14. CIS Kayıt Yönetimi Kuralları

Kayıt yönetimi her cihaz ve uygulamada farklı şekilde yapılmaktadır. Aşağıda Windows ve Linux sistemlerinde yerel kayıt yönetimi ve toplanan kayıtların merkezi bir sisteme gönderilmesinin nasıl olduğu tanımlanacaktır.

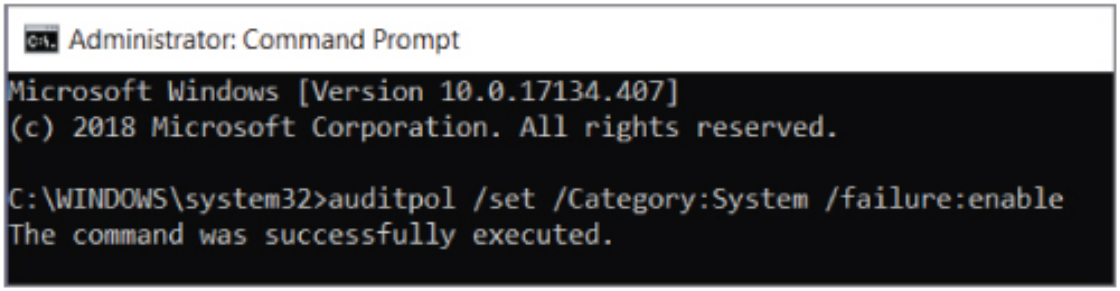
3.4.1.1. Windows kayıt yönetimi

Windows kayıt yönetimi, hangi olayların kayıt altına alınacağının belirlenmesi ile başlar. Kayıt altına alınan olaylar takip edilip istenilen düzeyde kayıt bilgisinin elde edildiği doğrulandıktan sonra kayıtlar merkezi bir sisteme gönderilmelidir.

Windows işletim sisteminde kayıt edilmesi istenen olaylar komut satırı, yerel grup politikaları, yerel güvenlik ilkeleri ya da etki alanı grup politikaları ile belirlenebilmektedir. Şekil 3.15'te Yerel Güvenlik İlkesi ile 'Hesap Oturumu Açma' olayı için kayıt oluşturulması gösterilmiştir. Şekil 3.16'da ise komut satırı ile sistem kategorisinde yaşanabilecek başarısız olayların kaydının tutulmasının etkinleştirilmesi gösterilmiştir.

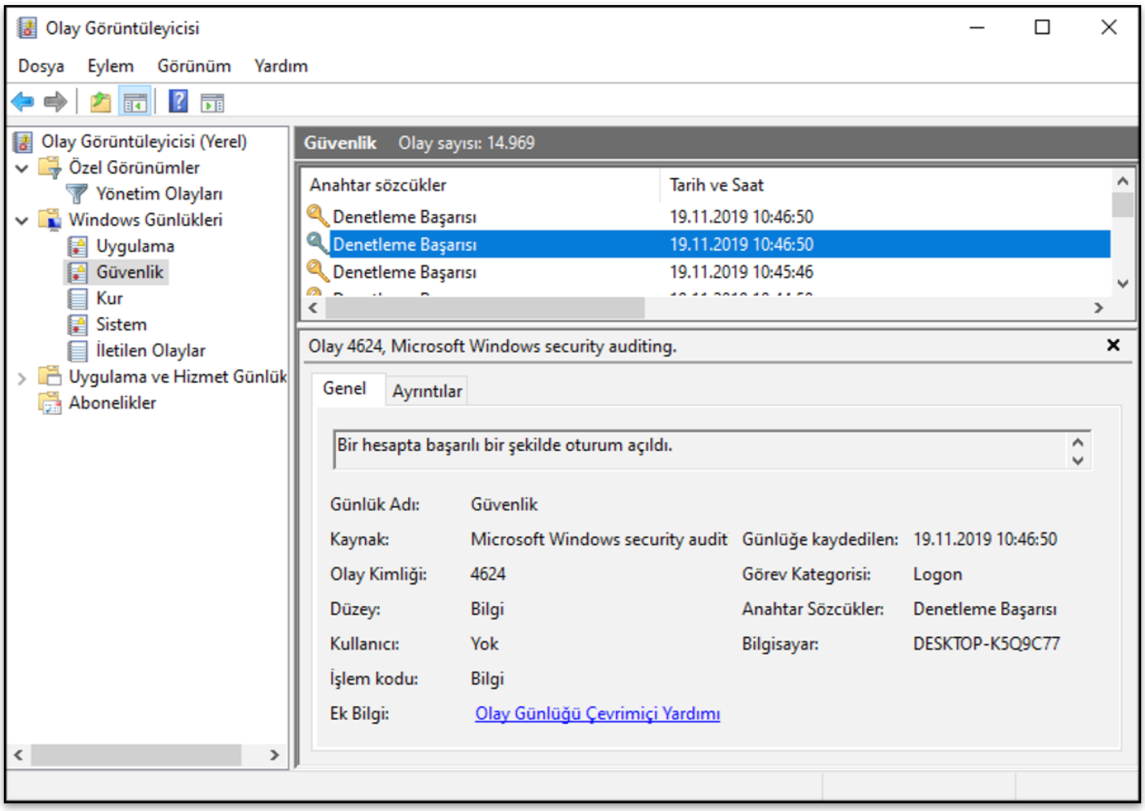


Şekil 3.15. Yerel Güvenlik İlkesi



Şekil 3.16. Komut Satırı ile Olay Kaydı Etkinleştirme

Windows, ürettiği olay kayıtlarının görüntülenmesine olanak sağlayan Olay Görüntüleyici aracını içermektedir. Bu araç kullanılarak kayıt edilen olaylar yerel olarak incelenebilmektedir. Şekil 3.17'de Olay Görüntüleyicisi ve kayıt altına alınmış başarılı bir 'sisteme giriş' kaydı gösterilmiştir.



Şekil 3.17. Olay Görüntüleyicisi

3.4.1.2. Linux kayıt yönetimi

Linux işletim sistemlerinde denetleme (audit) 'audit daemon' uygulaması ile sağlanır. 'auditd' olarak adlandırılan bu uygulama belirtilen kurallara göre işletim sistemi üzerinde olan olayların kaydını '/var/log/' dizini altına kayıt eder. 'auditd' komut satırı komutları ile

de yönetilebilmektedir. Şekil 3.18'de '/etc/passwd' dosyası bütün değişimlere karşı kayıt altına alınmaya başlanmış ve Şekil 3.19 ile de ilgili dosya ile alakalı oluşan olay kayıtları gösterilmiştir.

```
root@dread:/home/dread/Downloads# auditctl -w /etc/passwd -p rwxa
```

Şekil 3.18. Dosyanın denetlenmeye başlanması

```
root@dread:/home/dread/Downloads# ausearch -f /etc/passwd
----
time->Sun Apr  5 20:20:57 2020
type=PROCTITLE msg=audit(1586114457.978:82): proctitle=636174002F657
4632F706173737764
type=PATH msg=audit(1586114457.978:82): item=0 name="/etc/passwd" in
ode=3672753 dev=08:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype
=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1586114457.978:82): cwd="/home/dread/Downloads"
type=SYSCALL msg=audit(1586114457.978:82): arch=c000003e syscall=257
 success=yes exit=3 a0=ffffff9c a1=7ffdc9a9b803 a2=0 a3=0 items=1 pp
id=8647 pid=8970 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 e
gid=0 sgid=0 fsgid=0 tty=pts5 ses=4294967295 comm="cat" exe="/usr/bi
n/cat" key=(null)
```

Şekil 3.19. Dosya denetimi kayıtları

Bu uygulama haricinde 'journalctl' uygulaması kullanılarak işletim sistemi üzerinde koşan yazılımların/servislerin tutulan kayıtları takip edilebilir. Ayrıca 'dmesg' uygulaması yardımı ile çekirdek seviyesine olan olayların kayıtları incelenebilir. Şekil 3.20 ve Şekil 3.21'de sırası ile 'dmesg' ve 'journalctl' komutları çıktıları gösterilmiştir.

```
[61018.738063] 20:39:29.884187 control  Closing all guest files ...
[61018.738992] usb 2-1: USB disconnect, device number 4
[61019.438520] usb 2-1: new full-speed USB device number 5 using ohc
i-pci
[61019.772531] usb 2-1: New USB device found, idVendor=80ee, idProdu
ct=0021, bcdDevice= 1.00
[61019.772533] usb 2-1: New USB device strings: Mfr=1, Product=3, Se
rialNumber=0
[61019.772534] usb 2-1: Product: USB Tablet
[61019.772535] usb 2-1: Manufacturer: VirtualBox
[61019.788806] input: VirtualBox USB Tablet as /devices/pci0000:00/0
000:00:06.0/usb2/2-1/2-1:1.0/0003:80EE:0021.0004/input/input10
[61019.848216] hid-generic 0003:80EE:0021.0004: input,hidraw0: USB H
ID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
```

Şekil 3.20. dmesg komutu çıktısı

```
Apr 05 20:22:10 dread audit[8979]: SYSCALL arch=c000003e syscall=257
 success=yes exit=3 a0=ffffff9c a1=7f2d3b60f189 a2=80000 a3=0 items=
1 ppid=1387 pid=8979 auid=4294967295 uid=1000 gid=1000 euid=0 suid=0
 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=4294967295 co
mm="pkexec" exe="/usr/bin/pkexec" key=(null)
Apr 05 20:22:10 dread audit: CWD cwd="/home/dread"
Apr 05 20:22:10 dread audit: PATH item=0 name="/etc/passwd" inode=36
72753 dev=08:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMA
L cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
Apr 05 20:22:10 dread audit: PROCTITLE proctitle=706B65786563002F757
3722F6C69622F7570646174652D6E6F7469666965722F7061636B6167652D7379737
4656D2D6C6F636B6564
Apr 05 20:22:10 dread audit[8979]: SYSCALL arch=c000003e syscall=257
 success=yes exit=3 a0=ffffff9c a1=7f2d3b60f189 a2=80000 a3=0 items=
1 ppid=1387 pid=8979 auid=4294967295 uid=1000 gid=1000 euid=0 suid=0
 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=(none) ses=4294967295 co
mm="pkexec" exe="/usr/bin/pkexec" key=(null)
Apr 05 20:22:10 dread audit: CWD cwd="/home/dread"
```

Şekil 3.21. journalctl komutu çıktısı

3.4.1.3. Syslog

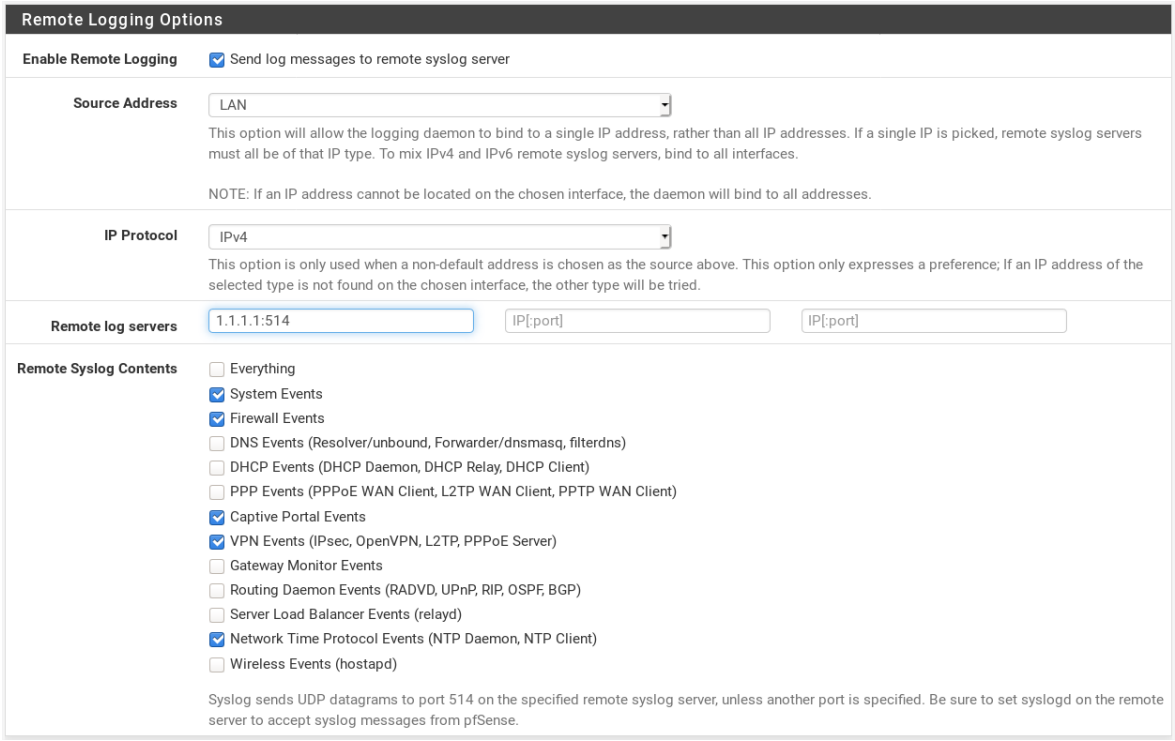
Syslog, ağ cihazlarının bir kayıt sunucusuna kayıtlarını göndermek için kullandıkları yöntemdir. Birçok cihaz tarafından desteklenir ve farklı kayıt çeşitlerini göndermek için kullanılabilir. Farklı kaynaklardan, farklı tipte kayıtları tek bir noktada toplamak syslog ile mümkündür. Syslog, merkezi sunucuda kayıtları toplamak için UDP kullanır. Cihazlar üzerinde oluşan olayları syslog ile merkezi bir noktaya iletmek, kayıtların birleştirilip incelenmesine olanak sağlamaktadır [54].

Örnek olarak Şekil 3.22'de bir güvenlik duvarı syslog yapılandırma ekranı ve Şekil 3.23'te syslog sunucusu tarafından toplanılan veri gösterilmektedir. Yukarıda bahsedildiği gibi syslog yapılandırma ekranı farklı tipte kayıtları seçmeye olanak tanımaktadır. Sunucu tarafından toplanan kayıtların ise farklı parametrelere göre sınıflandırılıp anlamlandırılması gerekmektedir. Örneğin kayıtlar önce kaynağa, daha sonra kayıt tipine göre sınıflandırılabilirler. Sınıflandırma işleminden sonra toplanan kayıtların ayrıştırılması gerekmektedir.

3.4.1.4. Kayıtların ayrıştırılması, indekslenmesi ve saklanması

Kaynaklar üzerinden kayıtlar merkezi bir sisteme yönlendirilip toplanmaya başlandıktan sonra işlenebilmeleri için öncelikle ayrıştırılmaları gerekmektedir. Daha sonra

ayrıştırılan bu verilerin hızlı bir şekilde erişilebilmesi için indekslenmesi gerekmektedir. Son olarak verinin gerektiğinde tekrar sorgulanabilmesi için saklanması gerekmektedir.



Şekil 3.22. Syslog kullanıcı yapılandırması

```
Apr  6 15:03:45 _gateway filterlog:
156,,,1542866113,em0.200,match,pass,in,4,0x0,,64,47878,0,DF,6,tcp,60,1.1.1.4,72.247.179.209
,59890,443,0,S,3768305822,,29200,,mss;sackOK;TS;nop;wscale
Apr  6 15:03:45 _gateway filterlog:
157,,,1542866113,em0.200,match,pass,in,4,0x0,,128,23950,0,none,17,udp,73,1.1.1.10,8.8.8.8,6
3721,53,53
Apr  6 15:03:45 _gateway filterlog:
157,,,1542866113,em0.200,match,pass,in,4,0x0,,128,23951,0,none,17,udp,73,1.1.1.10,8.8.8.8,5
0076,53,53
Apr  6 15:03:45 _gateway filterlog:
156,,,1542866113,em0.200,match,pass,in,4,0x0,,64,47878,0,DF,6,tcp,60,1.1.1.4,72.247.179.209
,59890,443,0,S,3768305822,,29200,,mss;sackOK;TS;nop;wscale
Apr  6 15:03:45 _gateway filterlog:
157,,,1542866113,em0.200,match,pass,in,4,0x0,,128,23950,0,none,17,udp,73,1.1.1.10,8.8.8.8,6
3721,53,53
Apr  6 15:03:45 _gateway filterlog:
157,,,1542866113,em0.200,match,pass,in,4,0x0,,128,23951,0,none,17,udp,73,1.1.1.10,8.8.8.8,5
0076,53,53
Apr  6 15:03:45 _gateway filterlog:
156,,,1542866113,em0.200,match,pass,in,4,0x0,,64,47878,0,DF,6,tcp,60,1.1.1.4,72.247.179.209
,59890,443,0,S,3768305822,,29200,,mss;sackOK;TS;nop;wscale
Apr  6 15:03:45 _gateway filterlog:
157,,,1542866113,em0.200,match,pass,in,4,0x0,,128,23950,0,none,17,udp,73,1.1.1.10,8.8.8.8,6
3721,53,53
```

Şekil 3.23. Syslog sunucusunda toplanan kayıtlar

Bir kayıtın ayrıştırılması için öncelikle kayıt gönderen kaynağın veriyi nasıl bir formatta gönderdiğinin bilinmesi gerekmektedir. Şekil 3.23'te gösterilen veri, Filter Log

Format for pfSense Software version 2.2[7] dokümanında tanımlanmaktadır. Bu ayrıştırmak için GROK desenleri kullanılabilir.

Şekil 3.23'te gösterilen veri, bahsi geçen dokümanda tanımlanan 'Grok' filtreleri yardımını ile ayrıştırılıp anlamlandırılabilir. Şekil 3.24'te, Şekil 3.23'te gösterilen veriyi ayrıştırmak için kullanılan Grok filtre kodunun bir parçası gösterilmektedir.

Kayıtlar ayrıştırıldıktan sonra üzerlerinde rahat ve hızlı işlem yapılabilmesi için indekslenmelidirler. İndeksleme işlemi; ayrıştırılmış verinin, o veriyi ifade eden veri yapısına göre saklanmasıdır. Örneğin Şekil 3.23'te gösterilen veri ayrıştırıldıktan sonra kaynak adresi 'src_ip' ve hedef adresi 'dst_ip' olarak indekslenebilir. Böylece bütün veriler üzerinde bir kaynaktan belli bir hedefe giden veri kolayca sorgulanabilir.

```
if [prog] =~ /^filterlog$/ {
    mutate {
        remove_field => [ "msg", "datetime" ]
    }
    grok {
        patterns_dir => "/etc/logstash/patterns"
        match => [ "message",
"%{PFSENSE_LOG_DATA}%{PFSENSE_IP_SPECIFIC_DATA}%{PFSENSE_IP_DATA}%{PFS
ENSE_PROTOCOL_DATA}",
            "message",
"%{PFSENSE_LOG_DATA}%{PFSENSE_IPv4_SPECIFIC_DATA_ECN}%{PFSENSE_IP_DATA
}%{PFSENSE_PROTOCOL_DATA}" ]
    }
    mutate {
        lowercase => [ 'proto' ]
    }
    geoip {
        add_tag => [ "GeoIP" ]
        source => "src_ip"
    }
}
```

Şekil 3.24. Örnek Bir Grok Filtresi

Elasticsearch, günümüzde indeksleme yapmak için standart hale gelmiştir. Elasticsearch ayrıştırılmış veriyi indekslemek için, her indeksi tanımlayan ve JSON formatında tutulan veri tipleri kullanır. Yukarıda verilen örnek veriyi indekslemek için Şekil 3.25'te verilen veri tipi tanımlaması yapılmalıdır (bütün tanımlama verilmemiştir).

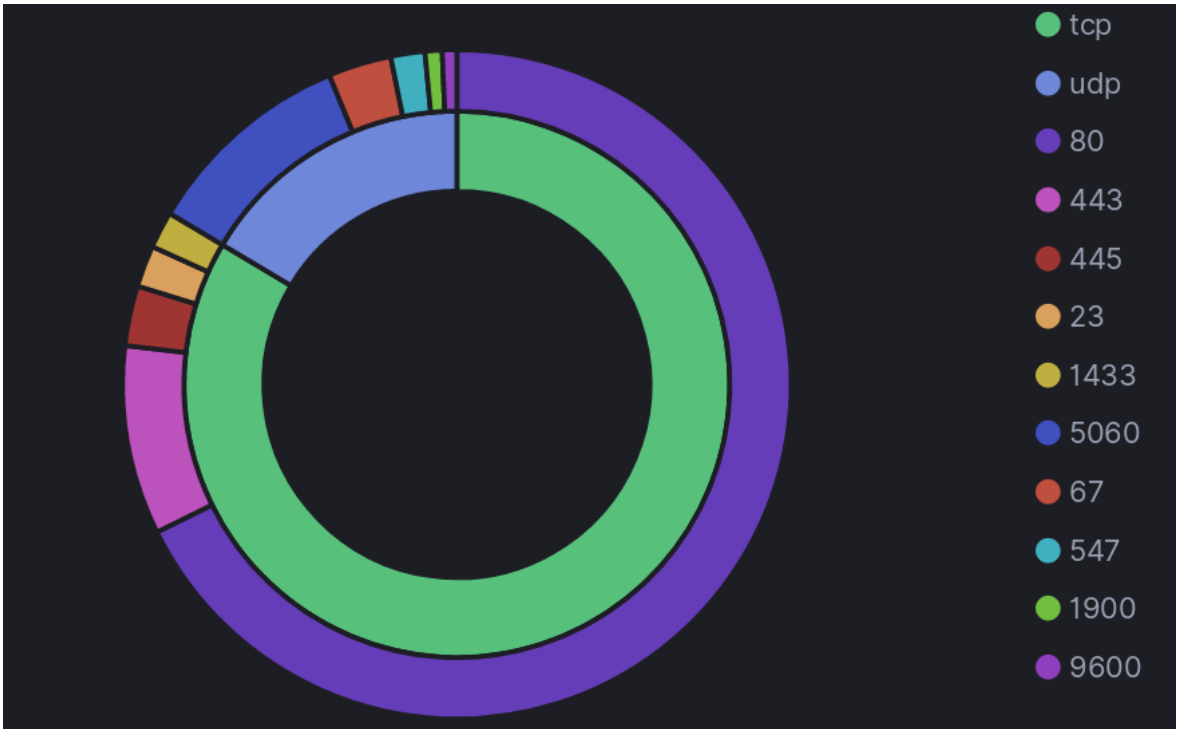
[7] https://docs.netgate.com/pfsense/en/latest/monitoring/filter-log-format-for-pfsense-2-2.html

Tanımlana veri yapısına bakıldığı zaman ‘dest_ip’, ‘dest_port’, vb. alanlar ve bu alanlara yerleştirilecek olan verinin tipleri görülebilmektedir. İndekslenen bu veri aynı zamanda dosya sisteminde saklanabilmektedir.

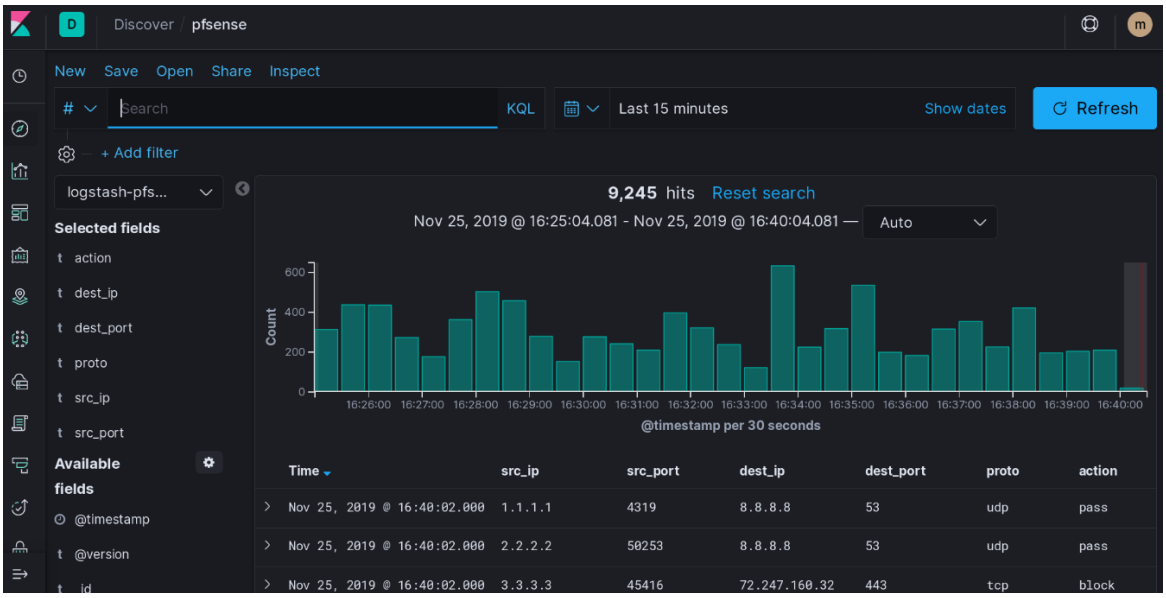
```
"properties" : {
  "dest_ip" : {
    "type" : "text",
    "norms" : false,
    "fields" : {
      "keyword" : {
        "type" : "keyword",
        "ignore_above" : 256
      }
    }
  },
  "dest_port" : {
    "type" : "text",
    "norms" : false,
    "fields" : {
      "keyword" : {
        "type" : "keyword",
        "ignore_above" : 256
      }
    }
  },
  "src_ip" : {
    "type" : "text",
    "norms" : false,
    "fields" : {
      "keyword" : {
        "type" : "keyword",
        "ignore_above" : 256
      }
    }
  },
  "src_port" : {
    "type" : "text",
    "norms" : false,
    "fields" : {
      "keyword" : {
        "type" : "keyword",
        "ignore_above" : 256
      }
    }
  }
}
```

Şekil 3.25. Elasticsearch veri yapısı

İndeksli veri üzerinde işlem yapabilmek önem arz eder. Verinin farklı şekillerde görselleştirmesi güvenlik uzmanlarının işini kolaylaştırmaktadır. Bunun yanında tehditlerin hızlı şekilde fark edilebilmesi içinde önemlidir. Kibana, Elasticsearch üzerinde tutulan verinin görselleştirilmesi için kullanılabilecek bir uygulamadır. Bu uygulama sayesinde veri filtrelenmesi, veriden grafikler oluşturulması, vb. işlemler yapılabilir. Şekil 3.26'da örnek bir görselleştirme ve Şekil 3.27'de örnek bir filtreleme işlemi gösterilmiştir.



Şekil 3.26. Kibana üzerinde verinin görselleştirilmesi



Şekil 3.27. Kibana üzerinde verinin filtrelenmesi

3.5. SIEM (Security Information and Event Management)

Bilgi Güvenliği ve Olay Yönetimi (SIEM - Security Information and Event Management); farklı kaynaklardan gelen kayıtları toplayarak, bu kayıtlar üzerinde anormallikleri ve saldırıları tespit eden bir olay yönetim sistemidir. Başka yerde örneği olmayan ve henüz imzası oluşturulmamış saldırıları tespit etmeye yardımcı olur. Topladığı kayıtlar üzerinde olay ilişkilendirmesi (ilgileşim) yaparak sistemde var olan tehditleri tespit etmeye yardımcı olur.

Salmon et. al. [44] 'ya göre SIEM, güvenlik bilgi yönetimi (SIM - security information management) ile güvenlik olayı yönetimini (SEM - security event management) birleştiren bir yazılıdır. SIEM, ağ donanımı ve sistem üzerinde koşan uygulamalar tarafından oluşturulan güvenlik uyarılarının gerçek zamanlı analizini sağlar. Üretilen uyarıları ve ağ güvenliğinin sağlığını kontrol etmek için merkezi bir nokta sağlar. SIEM, yalnızca altyapıya değil, aynı zamanda iş akışı, uyumluluk ve kayıt yönetimine de bütünsel ve birleşik bir bakış sunar. Bir SIEM verimli bir şekilde çok sayıda yetenek ve hizmet sağlayabilir. SIEM'in temeli, kayıt ve olay verilerinin toplanmasına dayanır.

SIEM'in temel yetenekleri aşağıdakilerdir [56]:

- **Toplama:** SIEM çözümünün temel işlevlerinden biri, güvenlik bilgi kaynaklarının toplanmasıdır. Toplama, analiz ve karar almayı kolaylaştırmak için ortak bir biçimde merkezi bir yerde bilgi toplanmasını ifade eder. SIEM'i besleyebilen kaynaklar, sistem olay günlükleri, güvenlik duvarı günlükleri, güvenlik uygulama günlükleri ve güvenlik aygıtlarından alınan belirli program akışları dahil çoktur. Bu materyalin, bir güvenlik analisti tarafından rahatça keşfedilmesini kolaylaştıran merkezi bir yere sahip olması, olay müdahale olayları sırasında çok faydalıdır.
- **Korelasyon:** Korelasyon, olayların ortak bir temele dayanarak birleştirilmesidir. Olaylar arasında zamana, ortak olaylara, davranışlara ve benzerlerine dayalı olarak ilişki kurulabilir. Birçok saldırı çok aşamalıdır ve saldırılar son adımlarına gelmeden önce varlıklarını belirlemek veya erken algılamak, korelasyonun kattığı en büyük değerlerinden biridir. Korelasyon son davranışa göre şüpheli IP adresleri gibi şeyleri tanımlayabilir. Örneğin, bir korelasyon kuralı port taramasını

belirleyebilir, bu da kendi içinde düşmanca olmasa bile normal olmayan bir davranıştır. Bu nedenle bu IP adresinden gelecekte gerçekleşecek ağ trafikleri şüpheli olarak kabul edilir.

- **Otomatik Uyarı ve Tetikleyiciler:** SIEM, önceden tanımlanmış kurallar ve analitik analizler kullanarak şüpheli davranışlar tespit ettiğinde uyarı üretebilir. Bu uyarılar sayesinde güvenlik önlemlerinin alınma süresi büyük ölçüde kısaltılmış olur. SIEM'ler STS'lerin geliştirilmiş hali gibi düşünülebilir; çünkü STS'ye göre çok daha fazla kaynaktan bilgi toplayıp işleyebilmektedirler.

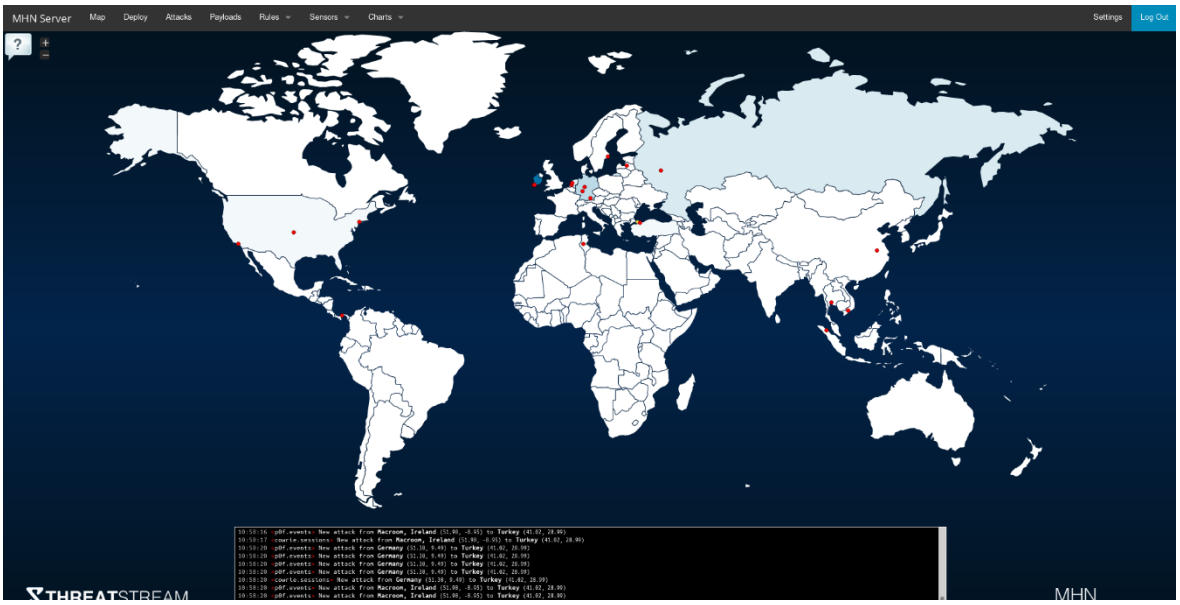
3.6. Balküpleri ve Balküpü Ağları

Balküpü; iç ve dış saldırganlar için cazip görünen fakat aslında saldırgan için tuzak olan bir hedeftir. Örnek olarak finans bilgilerini içeren veri bankası benzeri bir sunucu hazırlanabilir ve bu veri bankasına sahte bilgiler yerleştirilebilir. Bu sayede iki önemli hedef başarılmış olur. Birincisi, saldırgan değerli bir veriye ulaştığını düşündüğü için bir süreliğine diğer sistemlere odaklanamayacaktır. İkincisi, balküpü gerçek bir sistem olmadığından kimsenin erişmemesi gerekir. Bu nedenle balküpü sistemlerinde detaylı monitör ve kayıt verileri tutulabilir. Böylece bir saldırgan balküpü sistemine eriştiğinde kanıt olarak ve analiz amacıyla kullanılabilecek çok miktarda veri bulundurulabilir [26].

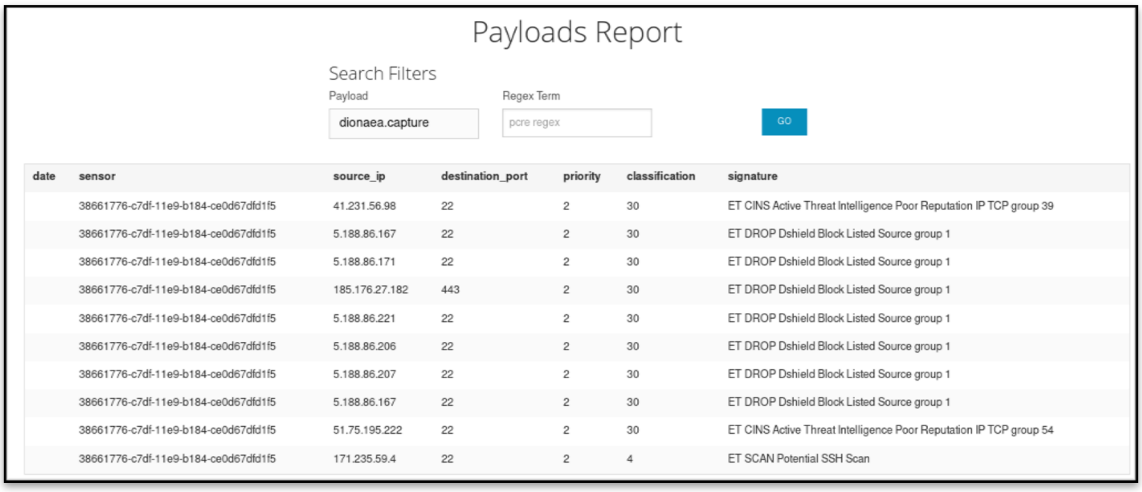
Balküpü ağları, balküplerinin mantıksal bir uzantılarıdır. Balküpü sistemlerinden oluşan sahte bir ağ segmenti kurulduğunda saldırganlar için cazip bir hedef oluşturulmuş olur. Bazı kurumların sadece bu amaç için sahte kablosuz erişim ağları kurdukları bilinmektedir [26].

Balküpü ağlarından yaygın olarak kullanılmakta olanlarından biri Modern Honey Network (MHN) projesidir. MHN projesi merkezi bir yönetim arayüzünden farklı balküplerini kurma ve bilgilerini toplama imkanı sunmaktadır. Yönetebildiği balküpleri arasında Snort, Cowrie, Dionaea, glastopf, vb. bulunmaktadır. Bu tuzak sistemleri; geniş ağda dolaşan otonom saldırı sistemlerinin (zombi bilgisayarlar) tespiti ve günlük eğilim istatistikleri toplanmasına yardımcı olabildiği gibi yeni saldırı yöntemlerinin yakalanmasına yardımcı olmaktadırlar. Büyük antivirüs firmaları kendi tasarladıkları balküpü sistemleri ile kötü niyetli insanları tuzağa düşürüp, ellerinde bulunan ve henüz geniş ağda dolaşmaya başlamamış zararlı içerikleri yakalamayı hedeflerler. MHN projesi, kullanıcısı tarafından istenmesi halinde, toplandığı verinin diğer sistemlere paylaşılmasına müsaade etmektedir.

Toplanan bu bilgiler sayesinde genel bir saldırı haritası oluşturmak mümkün olmaktadır. Şekil 3.28'de bu haritanın bir örneği gösterilmiştir. MHN tarafından yakalanan saldırıların içerikleri ve neden tehdit oluşturdukları belirlenebilmektedir. Şekil 3.29'da hazırlanmış olan bir tehdit raporu gösterilmiştir. Şekil 3.30'da MHN balküplerine takılan saldırılar hakkında tutulan istatistiksel veriler gösterilmiştir.



Şekil 3.28. MHN (Modern Honey Network) Genel Saldırı Haritası



date	sensor	source_ip	destination_port	priority	classification	signature
	38661776-c7df-11e9-b184-ce0d67dfd1f5	41.231.56.98	22	2	30	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 39
	38661776-c7df-11e9-b184-ce0d67dfd1f5	5.188.86.167	22	2	30	ET DROP Dshield Block Listed Source group 1
	38661776-c7df-11e9-b184-ce0d67dfd1f5	5.188.86.171	22	2	30	ET DROP Dshield Block Listed Source group 1
	38661776-c7df-11e9-b184-ce0d67dfd1f5	185.176.27.182	443	2	30	ET DROP Dshield Block Listed Source group 1
	38661776-c7df-11e9-b184-ce0d67dfd1f5	5.188.86.221	22	2	30	ET DROP Dshield Block Listed Source group 1
	38661776-c7df-11e9-b184-ce0d67dfd1f5	5.188.86.206	22	2	30	ET DROP Dshield Block Listed Source group 1
	38661776-c7df-11e9-b184-ce0d67dfd1f5	5.188.86.207	22	2	30	ET DROP Dshield Block Listed Source group 1
	38661776-c7df-11e9-b184-ce0d67dfd1f5	5.188.86.167	22	2	30	ET DROP Dshield Block Listed Source group 1
	38661776-c7df-11e9-b184-ce0d67dfd1f5	51.75.195.222	22	2	30	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 54
	38661776-c7df-11e9-b184-ce0d67dfd1f5	171.235.59.4	22	2	4	ET SCAN Potential SSH Scan

Şekil 3.29. MHN tehdit raporu

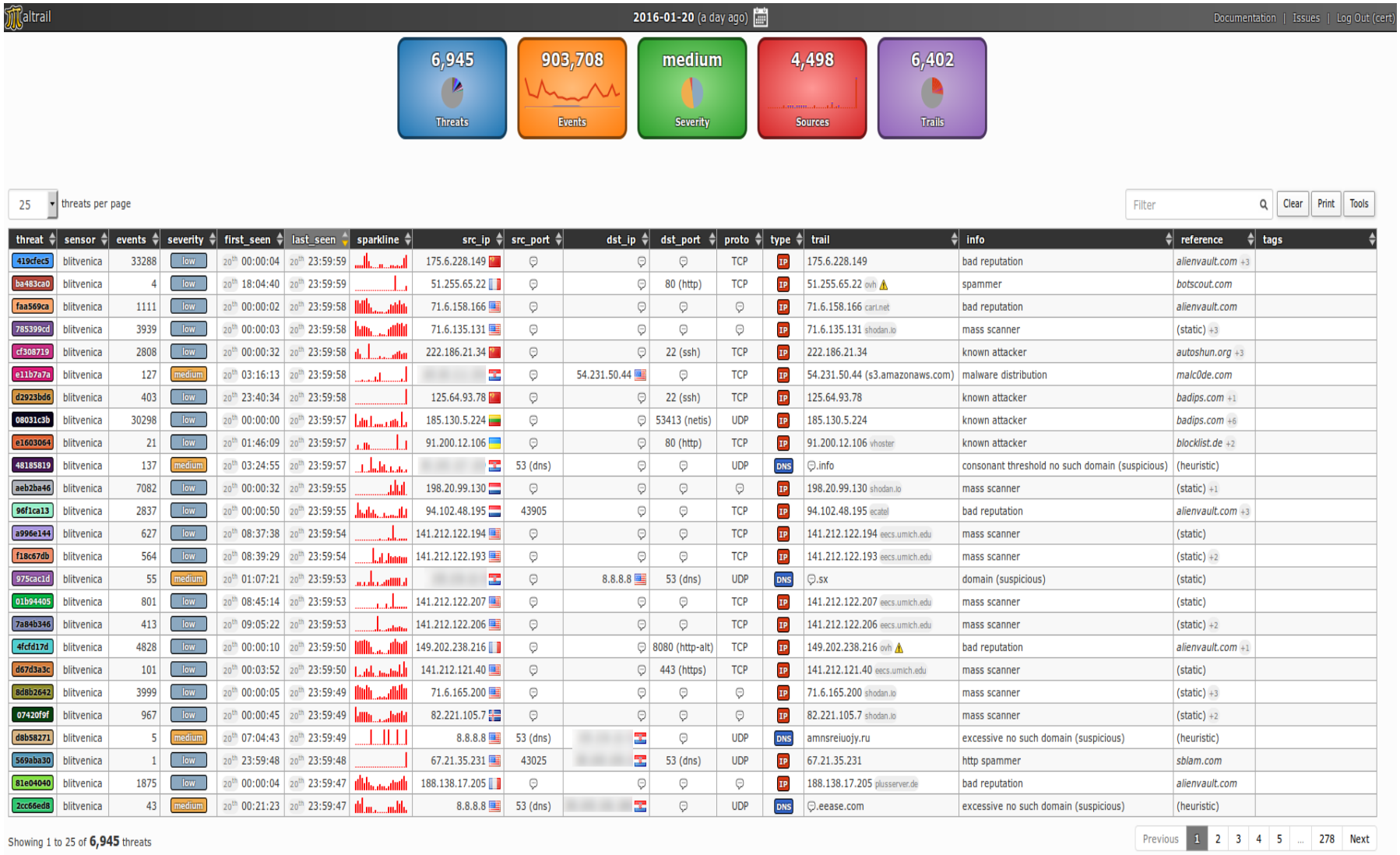
Balküperini desteklemek için internette var olan kara listelerden (blacklists) yararlanarak ağ trafiğini sınıflandıran sistemlerde mevcuttur. Bu sistemlerden bir tanesi Maltrail'dır. Maltrail, balküplerine ağ trafini üreten kaynakların kara listelerde olup

olmadığını kontrol ederek, tehdit unsuları hakkında ek bilgi sağlamaktadır. Şekil 3.31'de Maltrail[8] tarafından oluşturulmuş bir tehdit raporu gösterilmiştir.

Şekil 3.30. MHN saldırı istatistikleri

---

8 https://camo.githubusercontent.com/0038e0fd9c97e8a8552dac8c048e3efdce49afbe/68747470733a2f2f692e696d6775722e636f6d2f53643965716f612e706e67



Şekil 3.31. Maltrail tehdit raporu

4. SİBER SALDIRILARIN ÖNLENMESİ

Saldırı önleme hem makine seviyesinde hem de ağ seviyesinde birçok kabiliyet sağlamaktadır. Üst seviyeden bakıldığında bu kabiliyetleri iki ana kategoride toplayabiliriz: saldırı önleme ve mevzuata uygunluk. Tanımları aşağıda verilmiştir [57]:

- **Saldırı önleme:** Ağ seviyesinde saldırı önleme tarafından sağlanan temel özellik, kötü niyetli trafiğin hedef sisteme ulaşmasını önleme yeteneğidir. Saldırı tespit sistemleri yıllardır kullanılmaktadır, ancak doğaları gereği reaktif oldukları için belirli miktarda kötü niyetli trafiğin hedef sistemlere ulaşmasına izin vermişlerdir. Saldırı önleme sistemleri ile ağ seviyesinde saldırılara karşı önetkin bir savunma olanağı sağlanmaktadır. Saldırı önleme, saldırıları önlemenin yanı sıra RFC (Request for Comment) uyumluluğunun da güçlendirilmesini sağlar. Örneğin birçok uçbirimden uçbirime (peer-to-peer) uygulaması, güvenlik duvarlarından TCP 80 hedef portlu dış yönlü trafiğe izin verilmesinden faydalanır. RFC uyumluluğu kontrolü sağlamak için bahsi geçen dış yönlü trafik saldırı önleme sisteminden geçirilerek http (RFC2616) uyumluluğu kontrolü sağlanabilir.
- **Mevzuata uygunluk:** Düzenlemeler, belirli güvenlik kısıtlamalarının kurum ağında uygulanmasını garanti etmeye zorlar. Bu düzenlemeler, özellikle hastalar hakkındaki tıbbi bilgileri işleyen ağlar açısından çok önemlidir. Hem makine seviyesinde hem de ağ seviyesinde saldırı önleme sistemleri kullanılması, bu gereksinimlerin birçoğuna uymaya yardımcı olmaktadır.

Saldırı önleme sistemleri yukarıda bahsedildiği gibi makine seviyesinde ve ağ seviyesinde yer almaktadır. Bu iki seviyede aşağıda "Ağ Koruması" ve "Uç Nokta Koruması" başlıkları altında incelenmiştir.

4.1. Ağ Koruması

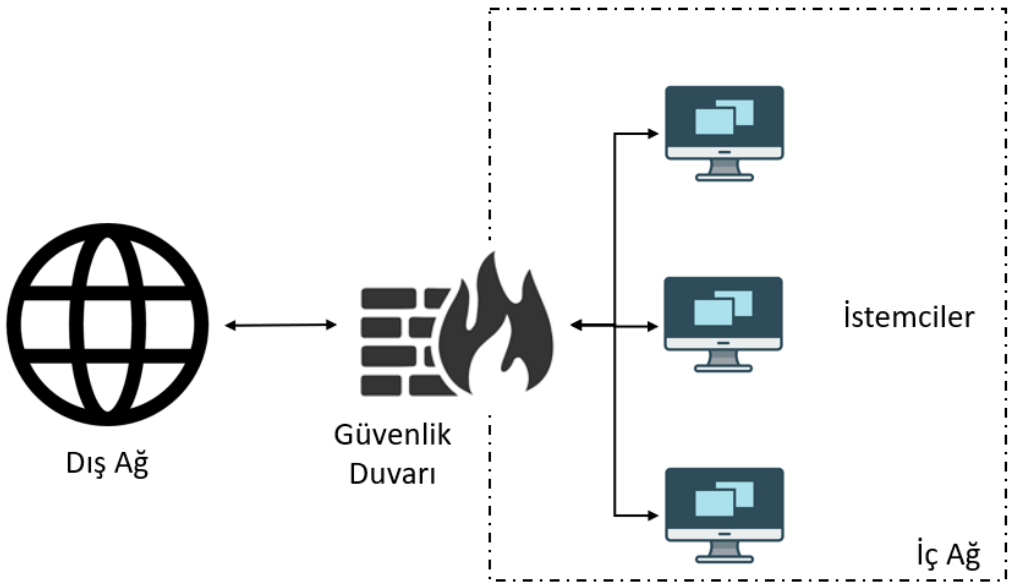
Bilgisayar ağı koruması, ABD Savunma Bakanlığı tarafından "bilgi sistemleri ve bilgisayar ağları içindeki yetkisiz etkinlikleri korumak, izlemek, analiz etmek, tespit etmek ve bunlara yanıt vermek için bilgisayar ağları kullanılarak yapılan işlemler" olarak tanımlanmaktadır [58].

Yetkisiz etkinliklerin engellenmesine yönelik olarak aşağıdaki alt bölümlerde özetlenen yöntemler kullanılmaktadır.

4.1.1. Güvenlik duvarı (Firewall)

Farklı ağlardan gelebilecek olan saldırıları kesmek ve/veya alarm üretmek için kullanılır. Kural tabanlı çalışır. Sadece IP, port ve protokol bilgilerine bakarak çalışabildiği gibi uygulamalara veya trafiğin içeriğine göre de denetleme yapabilir.

Güvenlik duvarları bir ağ korumasının ilk hattıdır. Farklı tür güvenlik duvarları bulunur ve bunlar ya tek başlarına (stand-alone) çalışan sistemlerdir ya da yönlendiriciler (router) veya sunucular içerisinde yer alan sistemlerdir. Güvenlik duvarının temel amacı bir ağı başka bir ağdan ayırmaktır. Örnek olarak Şekil 4.1'de gösterilen güvenlik duvarı, dış ağlardan gelen erişimi kısıtlarken, iç ağda yer alan kullanıcıların dış ağ kaynaklarına erişmesine izin vermektedir. Varsayılan ağ geçidi (gateway) olarak kullanılan bir güvenlik duvarı aynı zamanda Ağ Adresi Dönüştürme (Network Address Tranlation - NAT) işlemi de yapmaktadır. NAT işlemi sayesinde iç ağda bulunan IP adresleri, dış ağ adresine dönüştürülüp internet üzerinde yönlendirilebilir [26].



Şekil 4.1. Güvenlik duvarı erişim kısıtı

Güvenlik duvarı; kişisel bilgisayarları, ev ağlarını veya kurumsal ağlar ile internet arasında filtre görevi gören bir yazılım ya da donanımdır. Güvenlik duvarları, tanımlanan kurallara göre üzerlerinden hangi trafiğin geçip geçemeyeceğinin kontrolünü yaparlar. Güvenlik duvarlarının temel özellikleri aşağıdaki gibidir [59]:

- Gelen ağ trafiğini kaynağa ya da hedefe göre engellemek,
- Giden ağ trafiğini kaynağa ya da hedefe göre engellemek,
- Ağ trafiğini içeriğe göre engellemek,

- Kurumsal kaynakların dış ağdan erişimini kontrol altına almak,
- Ağ trafiğini ve güvenlik duvarı denetimlerini raporlayabilmek.

Firewall tipleri aşağıdaki gibidir [59]:

- Cihaz (Appliance)
- Sadece Yazılım
- Hepsi bir arada

Güvenlik duvarları, tanımlı kurallara göre ağ trafiğinin akışını belirlediği için yönetimlerinin büyük bir kısmı kural tanımlamaktır. Bu kurallara örnek olarak aşağıdakiler verilebilir [59]:

- Bütün kullanıcıların tüm Web sayfalarına erişimine izin ver;
- İç eposta sunucusundan dışarı giden bütün epostalara izin ver;
- Eğer yukarıda tanımlanan kurallara uymuyorsa dışarı çıkan bütün trafiği engelle;
- Halka açık Web sunucusuna gelen bütün http/https erişimlerine izin ver;
- Halka açık Web sunucusuna gelenler hariç dışarıdan gelen bütün erişim isteklerini engelle;
- Güvenlik duvarı tarafından reddedilen istekler dışında her isteğin kaydını tut;
- Dış dünyaya giden bütün Web erişim isteklerinin kaydını tut.

Güvenlik Duvarları aşağıdaki görevlerden bir veya daha fazlasını yapabilir:

1. Paket Filtresi;
2. Vekil Güvenlik Duvarı;
3. Durum Denetimli Güvenlik Duvarı (Stateful packet inspection).

Güvenlik duvarları bahsedilen görevleri yapmalarına ve konumlandırıldıkları yere göre aşağıda tanımlanan şekilde adlandırılırlar:

- **Paket Filtresi Güvenlik Duvarı:** Paket filtresi veya statik güvenlik duvarı olarak davranan bir güvenlik duvarı, belirli bir IP adresi ve port bilgisine göre veri trafiğine izin verir ya da engeller. Verinin içeriğine bakmaksızın paketin adres bilgisine göre karar verir. Örnek olarak bir paket filtresi port 80 üzerinden gelen web trafiğine izin verirken, port 23 üzerinden gelen Telnet trafiğini engelleyebilir. Bu tarz filtreleme çeşidi birçok yönlendirici (router) içinde yer almaktadır. Eğer gelen bir paket izinsiz bir porta erişmek istiyorsa, filtre bu paketi reddedebilir ya da görmezden gelebilir. Birçok paket filtresi hangi IP adreslerinin hangi portlara erişim sağlayabileceğinin tanımlanmasına olanak

tanır ve bu kurallar çerçevesinde gelen paketlerin geçmesini veya engellenmesini sağlar [26].

- **Vekil Güvenlik Duvarları:** Vekil sunucular yerel ağ ile diğer ağlar arasında bir aracı görevi görür. Vekil Güvenlik Duvarları dış ağlardan gelen istekleri işlemek için kullanılır. Kural tabanlı bir karar mekanizması gelen isteklerin iç ağa iletilip iletilmeyeceğine karar verir. Vekil, gelen bütün paketleri yakalar ve iç kullanım için tekrardan işler. Yapılan işlemler arasında IP adresinin gizlenmesi de bulunmaktadır. Vekil Güvenlik Duvarları, Paket Filtresi Güvenlik Duvarlarına göre daha iyi bir koruma sağlarlar. Bunun nedeni vekil güvenlik duvarlarının karar mekanizmalarının daha 'akıllı' olmasıdır. Vekil, istemleri (requests) tekrardan paketler ve öyle dışa aktarır. Böylece kullanıcıları dış ağlardan izole etmiş olur. Ayrıca vekil, önbellek olarak da çalışabilmektedir. Bu sayede gönderilen bir istem tekrarlanırsa önbellek kullanılarak veri iletiminin verimliliği arttırılır. Bir vekil güvenlik duvarı genelde iki tane ağ ara yüz kartı (network interface card - NIC) kullanır. Bu kartlardan biri dış ağa, diğeri ise iç ağa bağlanır. Vekil yazılımı bu iki kart arasındaki veri akışını yönetir. Bu yapı iki ağı birbirinden ayrı tutar ve daha yüksek güvenlik sağlar. Vekil fonksiyonu uygulama seviyesinde de olabilir, devre seviyesinde de. Uygulama katmanında yer alan vekiller, daha gelişmiş olurlar. Uygulama tarafından kullanılan kuralları ve kabiliyetleri bilmeleri gerekir. Örneğin bu tip vekiller http protokolünde yer alan *GET* ve *PUT* operasyonlarının ayrımını yapabilir, doğru kontrolleri gerçekleştirebilmelidir. Devre seviyesinde ise istemci (client) ve sunucu (server) arasında bağlantı sağlanır ve aralarında geçen veriye bakılmaz. Birçok vekil; denetleme, kullanıcı yönetimi ve devre seviyesi vekiller tarafından tutulamayan diğer kullanım bilgilerini sağlayabilir [26].
- **Durum Denetimli Güvenlik Duvarı:** Yukarıda bahsedilen güvenlik duvarlarının aksine sadece trafiğin o anki durumuna göre değil, geçmişine göre de karar verebilen sistemlerdir. Durum denetimi sayesinde sadece IP, port, protokol bilgilerine göre karar vermek yerine 'konuşmanın' (conversation) tamamını inceleyebilir. Böylece UDP ve ICMP gibi bağlantısız (connectionless) iletişim protokollerinin de denetimleri yapılabilmektedir. Servis dışı bırakma saldırıları (Denial of Service Attacks) bu güvenlik duvarları için zorluk oluşturabilmektedir; çünkü baskın (flooding) teknikleri kullanılarak güvenlik duvarının durum tablosu doldurulup, çalışamaz hale getirilebilinir [26].

- **UTM Cihazları:** UTM (Unified Threat Management) Birleştirilmiş Tehdit Yönetimi anlamına gelmektedir. Bu cihazlar 'hepsi bir arada' (all-in-one) çözümleri olarak kullanılmaktadır. Bir güvenlik duvarı; saldırı önleme, antivirüs, içerik filtreleme gibi farklı özellikler ile birleştirildiği zaman ortaya çıkan ürünler UTM ya da NGFW (next generation firewall) olarak bilinmektedir [26].

4.1.2. Saldırı önleme sistemi (IPS – Intrusion Prevention System)

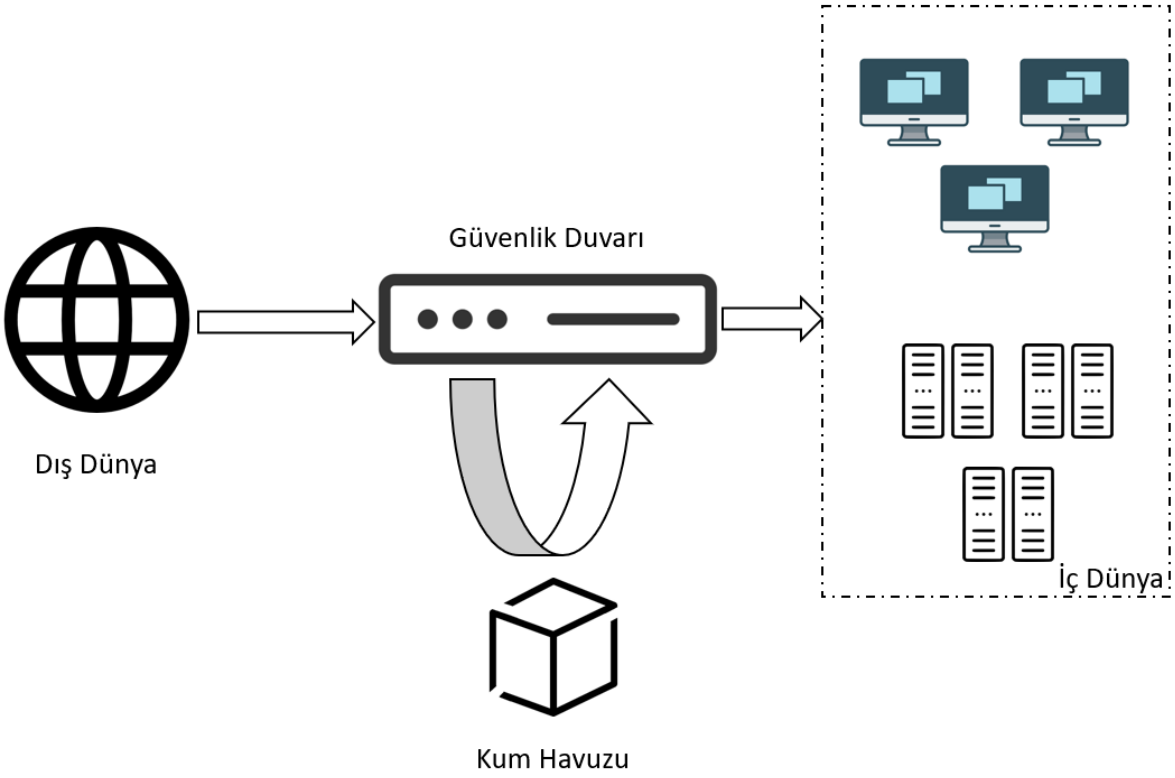
Saldırı Tespit Sistemleri mantığında çalışmaktadır. Alarm üretmek yerine çeşitli karar mekanizmalarına dayanarak saldırıya engel olurlar. Anti virüs gibi bir uç nokta üzerinde olan olayları yerel olarak incelemek yerine, ağ trafiğini izleyerek potansiyel tehditleri saptamaya çalışırlar. IPS tarafından üretilen her uyarı bir tehdit anlamı taşımaz. Uç nokta üzerindeki antivirüs izinli bir dosya indirme trafiğini tehdit olarak görmezken, IPS bu trafiği potansiyel bir tehdit olarak sınıflandırabilir. IDS ve IPS teknolojileri birbirilerine çok benzerlik gösterir. Aralarındaki temel fark şudur: IDS potansiyel bir tehdidi bulur, kaydını tutar ve alarm üretir. IPS buna ek olarak bahsi geçen trafiği engeller.

Ağ tabanlı saldırı önleme sistemleri (NIPS – Network Intrusion Detection System), NIDS sistemlerine benzer bir şekilde çalışırlar. NIDS'e ek olarak zararlı olduğu tespit edilen trafiği kesebilirler. IPS sistemleri genelde sıralı (inline) çalışırlar. Bir güvenlik duvarı gibi yetkisiz ağ trafiğini kesebilirler. Güvenlik duvarlarından farklı olarak trafiği engelleme kararını imza tabanlı bir eşleştirme mekanizmasına göre verirler. En çok bilinen açık kaynak IPS **Snort**'tur. 'Active Response' yöntemi ile zararlı olarak karar verdiği trafiği kesmek için TCP RST paketlerini kullanarak bağlantıyı düşürmeye çalışır [46].

4.1.3. Kum havuzu (Sandbox)

Fortinet [60] 'ün tanımına göre kum havuzu, son kullanıcı ortamının çoğaltılmış ve kurum sistemlerinden yalıtılmış bir halidir. Bu yalıtılmış ortamda bir kod; çalıştırılabilir, takip edilebilir ve faaliyetlerine göre sınıflandırılabilir. Kum havuzu ortamında zararlı olduğundan şüphelenilen uygulamalar çalıştırılıp dosya sistemi erişimleri, ağ bağlantıları, kayıt defteri ve sistem yapılandırma değişiklikleri takip edilebilir. Bu işlemin ağ katmanında yapılamasının avantajı, zararlı dosya son kullanıcıya erişmeden saldırının engellenebilmesidir.

Şekil 4.2'de ağ seviyesinde bir kum havuzu kullanımı gösterilmiştir. Bu şekle göre dış dünyadan gelen ağ trafiği içinde yer alan dosya iç dünyada bulunan istemcilere ve sunuculara ulaşmadan önce güvenlik duvarı tarafından kum havuzuna gönderilir. Kum havuzu analizleri sonucu dosyanın zararsız olduğuna karar verilirse, dosya iç dünyaya güvenlik duvarı üzerinden yönlendirilir.

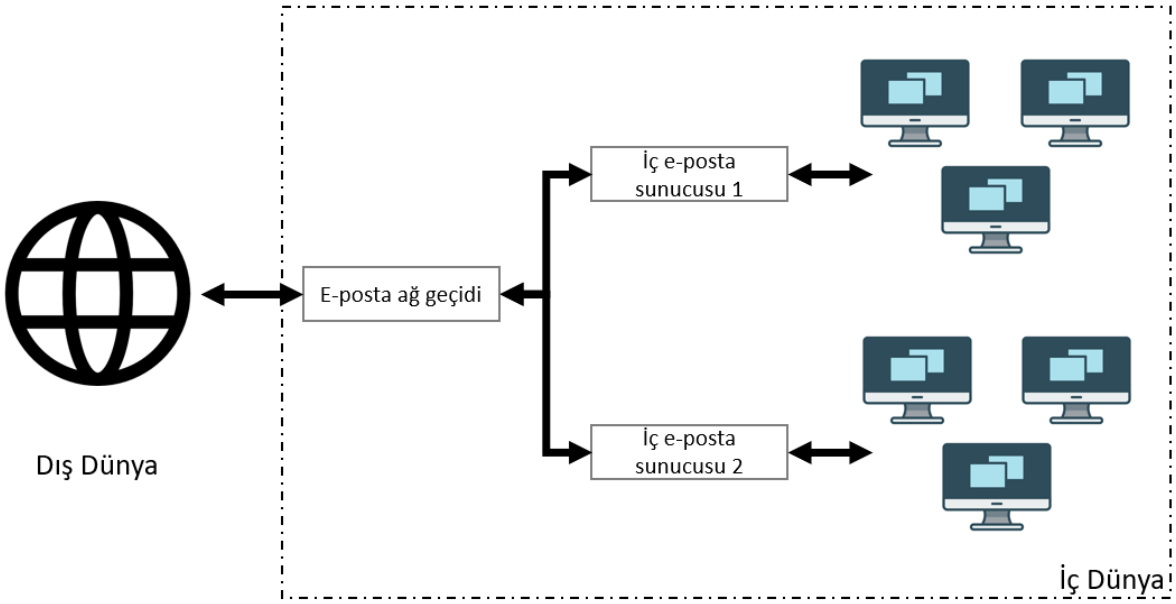


Şekil 4.2. Ağ seviyesinde kum havuzu kullanımı

4.1.4. E-posta ağ geçidi (Email Gateway)

E-posta ağ geçidi, iletileri kabul eden ve başka bir sisteme ileten bir e-posta sistemidir. Ağ geçitleri bir ağdan diğerine veya bir protokolden diğerine bir geçiş sağlayabilir. E-posta ağ geçidinin yaygın kullanımı, İnternet'ten bir kurum için gelen tüm postaları kabul eden ve bunu dahili posta sistemlerine ileten bir sunucudur. E-posta ağ geçitleri, İnternet'e doğrudan erişmesi gereken sunucu sayısını sınırlamak için genellikle güvenlik duvarı sistemleriyle birlikte kurulur [61].

Şekil 4.3'te örnek bir e-posta ağ geçidi yerleşimi gösterilmiştir. Dış dünyadan gelen iletiler önce e-posta ağ geçidine ulaşır. Oradan kurum içinde yer alan diğer e-posta sunucularına iletilir.



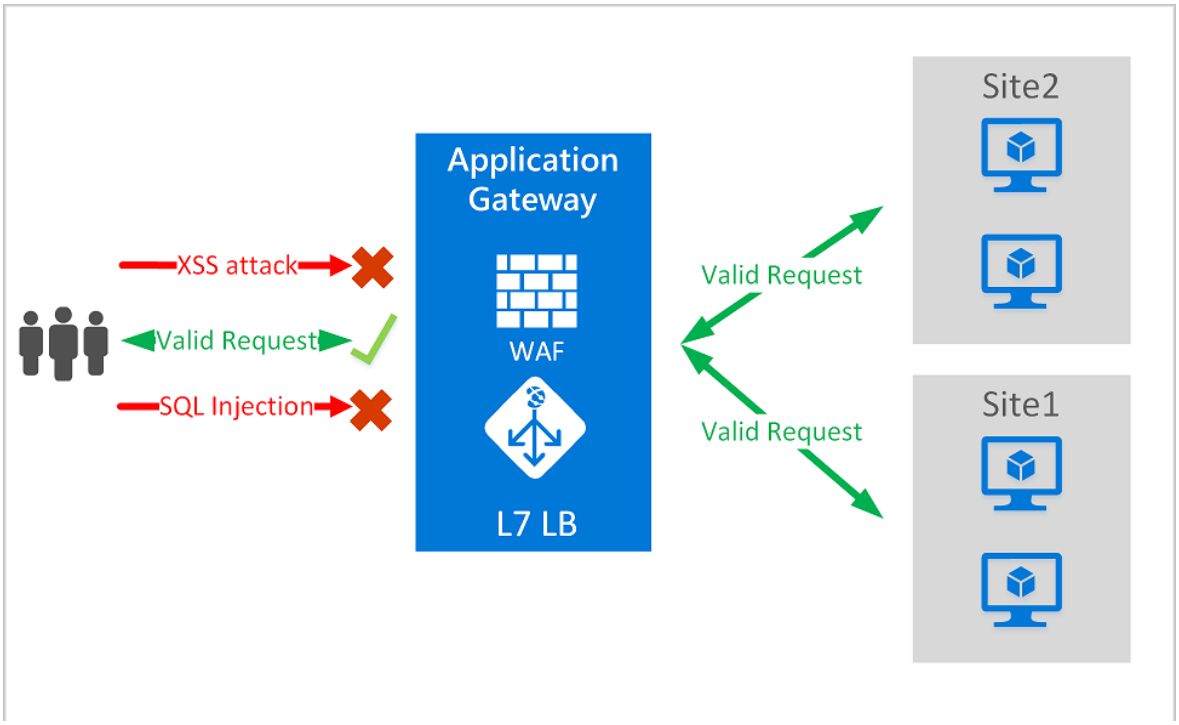
Şekil 4.3. Örnek bir e-posta ağ geçidi yerleşimi

E-posta günümüzde kurumların en sık kullandığı iletişim yöntemidir. Aynı zamanda saldırganların da kurumlara sızıp bilgi çalmak vb. faaliyetler için en sık kullandıkları yöntemdir. Her geçen gün e-posta saldırıları daha hedef odaklı, daha karmaşık ve daha tehlikeli olmaktadır. E-posta ağ geçidi tehditlerin bu denli tehlikeli olduğu bir ortamda çok gerekli bir güvenlik önlemidir. Yukarıda anlatıldığı üzere bu geçitler iç dünyadan dış dünyaya ve dış dünyadan iç dünyaya giden bütün iletileri aldıkları için iletiler üzerinde çeşitli güvenlik kontrolleri uygulayabilmektedirler. Bir e-posta ağ geçidi en az dört güvenlik kontrolü yapabilmelidir: virüs ve zararlı yazılım engelleme, istenmeyen e-posta (spam) filtreleme, içerik filtreleme ve arşivlemedir [62].

4.1.5. Web uygulama güvenlik duvarı

Web uygulama güvenlik duvarları genellikle bulut veya kurumsal ağlar üzerinde yer alan askerden arındırılmış bölgelere (DMZ) yerleştirilir. OSI modeline göre katman 7'de, uygulama katmanı, trafiğin derinlemesine denetlenmesini sağlamak için SSL sonlandırma yapabilirler. Sıfır gün saldırılarına karşı koruma sağlayan gelişmiş algılama yeteneklerine sahiptirler. Web uygulama güvenlik duvarları Açık Web Uygulaması Güvenlik Projesi (OWASP) en kritik 10 ve CWE/SANS en kritik 25 güvenlik açıklarını ve saldırılarını engelleme konusunda beceriklidirler. Modern web uygulama güvenlik duvarları, web saldırısı imzaları ve web güvenlik açığı imzaları içerir. Ayrıca güvenlik taraması sonuçlarını da kullanabilir. Web uygulama güvenlik duvarları uygulamalar için URL, parametre, çerez

ve form koruması sağlayabilir. Web uygulama güvenlik duvarları bir köprü veya vekil yapılandırmasında ağ trafiği akışı üzerinde sıralı (in-line) bağlanır. Sadece ağ trafiğini ayrıştırıp imza tabanlı bir tarama yapmazlar. Aynı zamanda uygulama davranışlarını analiz edebilir; kabul edilebilir davranış temelleri oluşturabilir ve bu iletişimde sapmalar arayabilirler [63]. Şekil 4.4'te bir web uygulama güvenlik duvarları uygulaması gösterilmiştir[9].



Şekil 4.4. Web uygulama güvenlik duvarları

4.1.6. Bulut tabanlı koruma

Geniş Alan Ağın'dan gelen dosyaların bulut tabanlı sistemlerde taranmasını sağlar. Bulut tabanlı sistemler işlem gücü açısından çok güçlü olduklarından tarama işlemi daha kolay ve hızlı bir şekilde yapılabilir. Tarama sonucunda elde edilen bilgiler, buluta bağlı diğer sistemlerle de paylaşılabilir.

4.2. Uç Nokta Koruması

Günümüzde sistemleri sadece ağ tabanlı korumak yeterli olmaz. Uç noktaların da aynı şekilde korunması gerekmektedir. Bir ICT sisteminde uç noktalar saldırı başlangıç noktası

[9] https://docs.microsoft.com/tr-tr/azure/web-application-firewall/ag/ag-overview

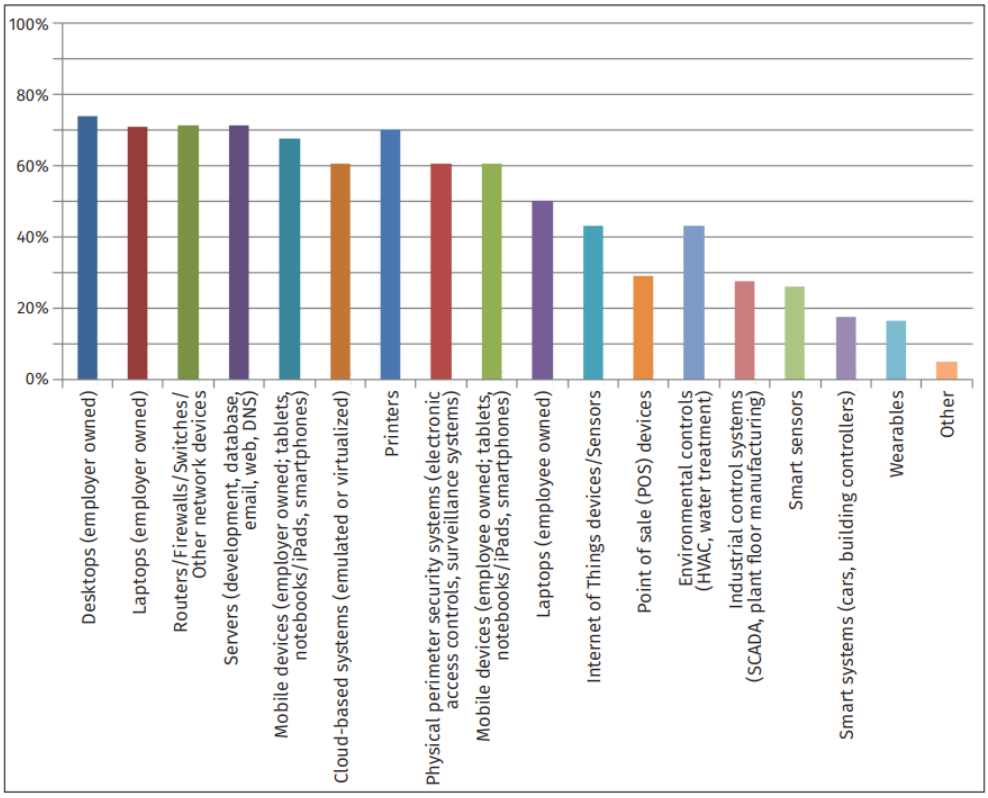
ya da hedef olmaktadır. Saldırganlar saldırı tespit sistemlerini mümkün olduğunca atlatmaya çalışırken, koruma zafiyeti olan ya da sosyal mühendislik saldırısı benzeri bir saldırı ile ele geçirdikleri bir uç nokta üzerinden hedeflerine ulaşmaya çalışırlar.

2018 yılında SANS tarafından yapılan Uç Nokta Güvenliği ve Yanıtı (Endpoint Protection and Response) araştırması, bu konunun önemini göstermektedir. Araştırmaya katılan kurumların Amerika, Avrupa ve Asya kıtalarına yayılmış uç noktaları bulunmaktadır. Bu kurumların %40'ı 1000 ve daha az çalışana sahipken %27'si 15000 ila 100000 çalışana sahiptir. Çalışma, kurumların uç noktada birçok farklı tipte cihaza sahip olduklarını göstermektedir. Şekil 4.5'te bu cihazlar gösterilmektedir [64].

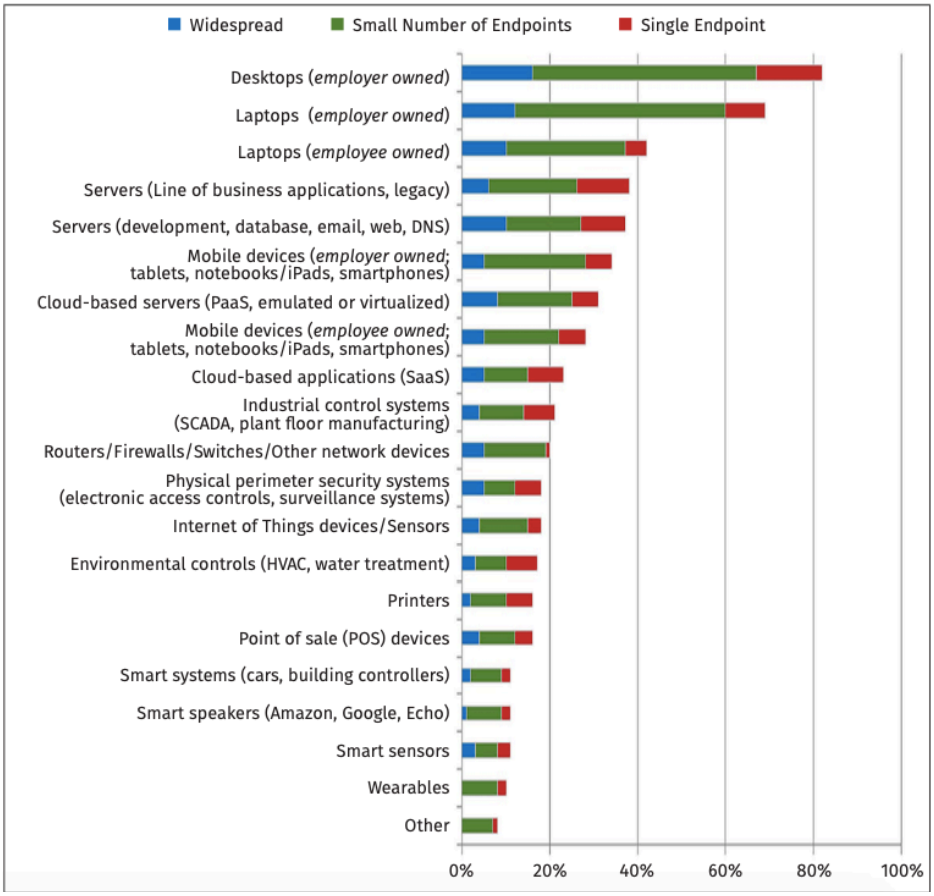
Şekil 4.5'te gösterilen rakamlara bakıldığında kullanıcıların sahip oldukları cihazların da kurumların sistemlerinin bir parçası olduğu görülmektedir. Bu noktada kurum tarafından yönetilen ve yönetilmeyen cihazların ayırımının yapılması gerekmektedir. Kurumların sistem yöneticileri, kuruma ait ICT cihazlarının her birine erişim yetkisine sahiplerdir. Bu yetki sayesinden uzaktan ya da yerinden bahsi geçen cihazları yönetebilmektedirler (güvenlik politikaları belirlenmesi, güncelleştirmelerin yapılması, yetkilerin kısıtlanması yönetimsel işlere örnek olarak verilebilir). Bu tip cihazlar, kurum tarafından yönetilen cihazlar olarak tanımlanmaktadır. Öte yandan kullanıcılara ait olan ve kurum ağına dahil olan cihazlar da bulunmaktadır. Tabletler, akıllı telefonlar ve kişisel dizüstü bilgisayarlar bu sınıfa giren cihazlara örnek olarak verilebilir. Bu cihazlar üzerinde sistem yöneticilerinin herhangi bir yetkisi bulunmamaktadır. Bahsi geçen cihazlar kullanıcılarının inisiyatifinde oldukları için kurum tarafından yönetilmeyen cihazlar olarak tanımlanmaktadırlar. Kullanıcının yönetiminde olan cihazlar, kurum ağına bağlandıkları andan itibaren kurum gözünden bir uç nokta haline gelmektedirler. Böylece istismar edildikleri takdirde kurum için tehdit oluşturabilmektedir.

Yine Neely [64] 'nin raporunda bahsettiği üzere, kurum tarafından yönetilmeyen uç noktalar, kurumun güvenliğine kötü yönde etki etmektedir. Şekil 4.6, kurumlarda başarılı bir siber saldırıya uğramış cihazları ve bu saldırının ne kadar yayılabildiğini göstermektedir. Rakamlara bakıldığı zaman kurum tarafından yönetilen bilgisayarların en yoğun şekilde saldırılardan etkilendiği görülmektedir. Aynı rakamlar, kullanıcıların kurum ağına dahil ettikleri cihazların ek bir tehdit yüzeyi oluşturduğunu da göstermektedir.

Uç noktaların korunması, kurumlar için büyük önem arz eder. Aşağıda, uç nokta güvenliği için kullanılan uygulamalar açıklanmıştır.



Şekil 4.5. Kurumların Uç Noktada Kullandıkları Cihazlar



Şekil 4.6. Kurumlarda başarılı bir saldırıya uğramış cihazlar

4.2.1. Antivirüs/Antimalware

Bölüm 2.3.4'te de anlatıldığı üzere virüsler ve kötücül yazılımlar uç nokta cihazları için büyük birer tehdit unsurudur. Chauhan [65] tarafından bahsedildiği üzere kullanıcıların bu tehditlere karşı bilgi sahibi olmaları ve kendilerini nasıl koruyacaklarını bilmeleri önemlidir. Doğaları gereği virüsler ve kötücül yazılımlar kendilerini kopyalayarak etrafa yayılmak isterler. Bu yayılmayı sadece ağ cihazlarının kabiliyetlerini kullanarak engellemek mümkün değildir. Uç noktalara kurulacak antivirüs yazılımı büyük önem arz etmektedir.

Chauhan [65] bir antivirüs yazılımının aşağıdaki özelliklere sahip olması gerektiğini söylemektedir:

- Fidye yazılımı koruması;
- Kötücül yazılım koruması;
- Web güvenliği;
- E-posta güvenliği;
- Tarama motoru ve
- Anti tuş kaydedici (keylogger).

Chu [66], uç noktalara kurulan antivirüslerin üç yöntem kullanarak tespit yaptığını belirtmiştir. Bu yöntemler aşağıda sırası ile verilmektedir:

- **İmza tabanlı tespit:** Geleneksel antivirüs yazılımları bu yöntemi kullanmaktadırlar. Bu yöntem tespit için bilinen tehditlerin karmalarını (hash) kullanır. Virüs ve kötücül yazılım tasarımcıları gitgide daha karmaşık yöntemler kullanmaya başladığı için bu yöntemin verimliliği her geçen gün daha da düşmektedir. Kötücül yazılımlar kendilerini karmaşıklaştırmak için aşağıdaki yöntemleri kullanmaya başlamıştır:
    - **Oligomorphic:** Bu yöntemi kullanan kötücül yazılımlar kendilerini şifreleyerek saklamayı denerler. Yazılım içinde kötü niyetli kod şifrelenmiş bir şeklide saklanmıştır ve yazılımın koştuğu esnada kendi kendini şifresini çözerek bir sonraki safhayı icra etmeyi hedefler. Bir kötücül yazılım içinde birden farklı şifreleme yöntemi kullanılabilmektedir. İmza tabanlı antivirüs yazılımları bahsi geçen kötücül yazılımı tespit etmek için, kötücül yazılımın içerdiği bütün şifreleme yöntemlerinin karmasını bulundurur.
    - **Polymorphic:** Bu yöntemi kullanan kötücül yazılımlar kendilerini şifrelemek için rastgele bir anahtar üretirler. Bu sayede antivirüs

yazılımlarının imza oluşturmasını zorlaştırmış olurlar. Ancak çalışabilmek için bir aşamada şiflerini çözmeleri gerektiğinden antivirüs yazılımları tarafından bir imza çıkarma imkanı doğmaktadır.

- **Metamorphic:** Bu yöntem imza tabanlı antivirüs yazılımlarını en çok zorlayan yöntemdir; çünkü kötücül yazılım kodunun çalışması her seferinde farklı bir kod koşma sırası izlemektedir.

- **Kum Havuzu ile Tespit:** Kum havuzu, özel olarak hazırlanmış kapalı bir ortamdır. Programların çalışma yöntemlerini analiz etmek için özel olarak tasarlanmıştır. Kum havuzu uygulamaları kullanılarak kötücül bir yazılımın ne yapmaya çalıştığı tespit edilebilir. Kum havuzu içerisinde çalıştırılan kötücül yazılımın, ağ trafiği, çağırdığı sistem çağrıları, dosya sistemi üzerinde eriştiği dosyalar vb. takip edilebilir. Bu yöntem detaylı bir analiz olduğu için uç nokta güvenliğinde çok nadir kullanılmaktadır.
- **Veri Madenciliği (Data Mining) Teknikleri:** İmza tabanlı tespit ve kum havuzu ile tespit yöntemlerinin arasında bir yöntem olarak değerlendirilmektedir. Bilinen tehditlere karşı bir analiz yaptıktan sonra dosyadan elde ettiği verilere dayalı olarak bir tehdit sınıflandırması yapmaktadır. Bu yöntem yapay zeka çalışmalarına bağlı olarak geliştirilmiş bir yöntemdir.

4.2.2. Veri kaybı önleme (DLP – Data Loss Prevention)

Nickel [67] ’e göre bir kurumun sahip olduğu verinin hangi noktalardan hangi noktalara iletilebileceğine karar veren sistemlere Veri Kaybı Önleme (DLP) sistemleri denmektedir. Kurum içinde yer alan bir verinin belli kurallar çerçevesinde işlenmesi gerekmektedir. Yetkisiz bir şekilde değiştirilecek, silinecek ya da yetkisiz kişilere iletilecek bir veri kurum için büyük bir tehdit oluşturmaktadır.

Veri ihlalleri aşağıda belirtilen üç aşamadan birinde gerçekleşmektedir:

1. Veri hareket halindeyken,
2. Veri saklanırken,
3. Veri kullanılırken.

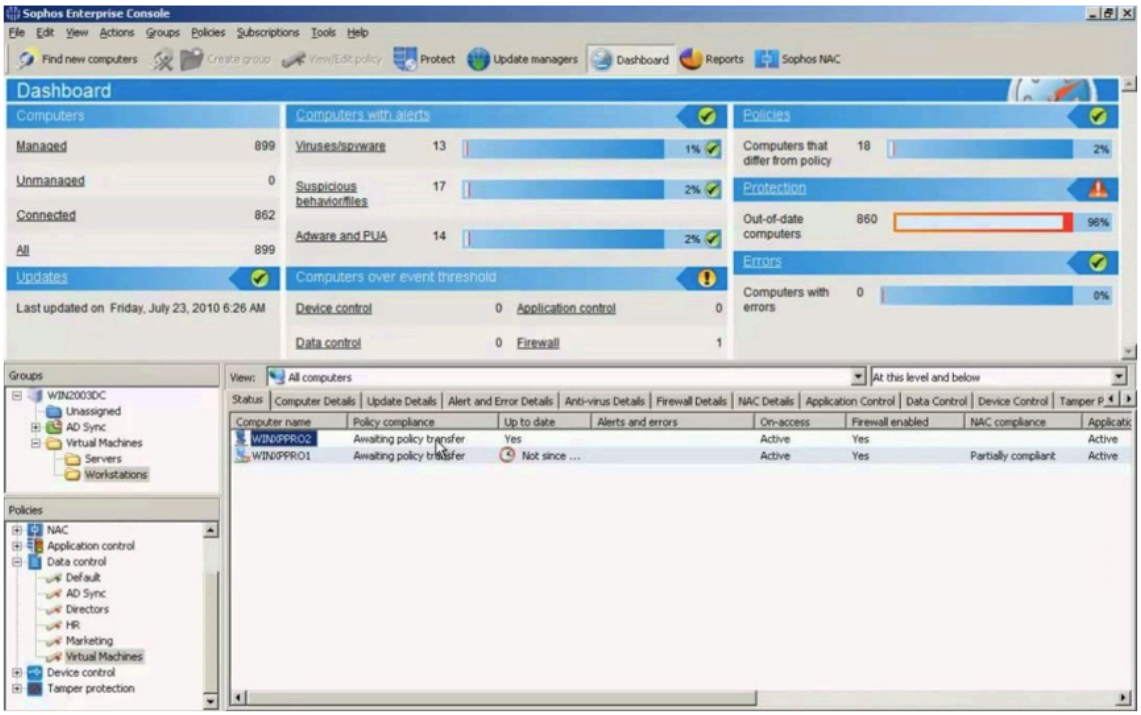
Srinivasan [68] tarafından bahsedildiği üzere veri kaybı önleme kontrolleri engelleyici ve tespit edici olmak üzere ikiye ayrılmaktadır. Engelleyici kontroller; verinin sınıflandırılmasına göre erişim kısıtlamaları getirmektedir. Bu kontrol yöntemi 100% verimlilik sağlamamaktadır. Bir ICT sisteminde birçok farklı uygulama kullanıldığı ve bu

uygulamalar veriyi farklı şekillerde sakladığı için verilerin sınıflandırılması bir problem oluşturmaktadır. Nickel [67] 'de benzer bir önerme yapmış ve DLP sistemlerinin veriyi sınıflandırmasının kurum çalışanlarına ek bir yük getirdiğinden söz edilmiştir. Bu nedenle DLP sistemlerinin potansiyellerinin çok altında bir verimlilikte çalıştıkları belirtilmiştir.

Srinivasan [68], DLP kontrollerinin aşağıdaki soruların yanıtına göre yapıldığını söylemektedir:

- Bilgi ne kadar hassas bir bilgidir ya da bilginin kurum için değeri nedir?
- Bir olaya neden olan kişi kimdir?
- Bahsi geçen olaya neden olan kişi, bu olayın oluşması için hangi faaliyetlerde bulunmuştur?
- Başka biri bu olaya karışmış mıdır? Eğer karışmışsa hangi aşamada dahil olmuştur?
- Hangi faaliyet gerçekleşmiştir?

Bennett [69] de benzer bir şekilde DLP uygulamalarının kurumlardan izinsiz veri çıkışına engel olmayı hedeflediğinden bahsetmiştir ve örnek bir DLP uygulaması olarak Sophos'tan bahsetmiştir. Şekil 4.7'de Bennett [69] tarafından verilmiş Sophos Enterprise Console'un ekran görüntüsü bulunmaktadır.



Şekil 4.7. Sophos DLP (Data Loss Prevention) Örnek Ekran Görüntüsü

4.2.3. Uç nokta tespit ve yanıt (EDR – Endpoint Detection and Response)

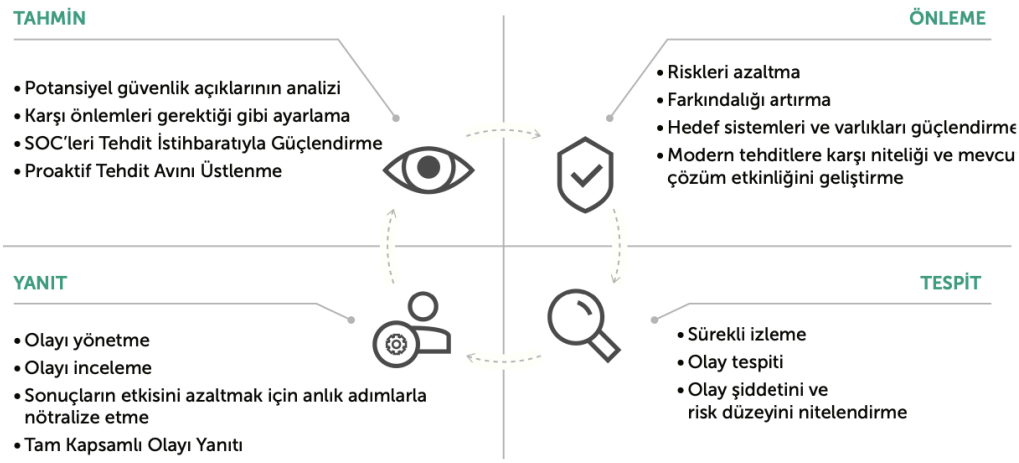
İlk olarak Uç Nokta Tehdit Tespiti ve Yanıtı (ETDR – Endpoint Threat Detection and Response) kavramı Gartner çalışanı Anton Chuvakin tarafından Temmuz 2013 tarihinde ortaya atılmıştır. Anton Chuvakin tarafından ETDR aşağıdaki şekilde tanımlanmıştır[10]:

"Temel amaçları uç noktalar üzerinde şüpheli faaliyetleri tespit etmek ve tespit ettiği şüpheli faaliyeti araştırmak olan araçlar."

ETDR günümüzde EDR (Endpoint Detection and Response) yani 'Uç Nokta Tespit ve Yanıt' olarak bilinmektedir. Amacı sürekli takip ve yanıt gerektiren ileri düzey tehditlere karşı güvenlik sağlamaktır.

Kaspersky Lab [70], EDR aşamalarını aşağıdaki gibi tanımlar ve Şekil 4.8'de gösterilen güvenlik modelini uygular:

- Önleme: Gelişmiş tehdit riskini azaltmak için yaygın tehditlerin engellenmesi ve temel sistemlerin güçlendirilmesi
- Tespit Etme: hedefli bir saldırının veya mevcut bir ihlalin belirtisi olabilecek etkinliklerin hızlı bir şekilde keşfedilmesi
- Yanıtlama: tehdidi tam olarak kontrol altına alma, incelemeler gerçekleştirme ve saldırılara uygun şekilde yanıt verme
- Tahmin Etme: yeni hedefli saldırıların nerede ve nasıl ortaya çıkabileceğini öğrenme



Şekil 4.8. Kaspersky Lab Uygulanabilir Güvenlik Modeli

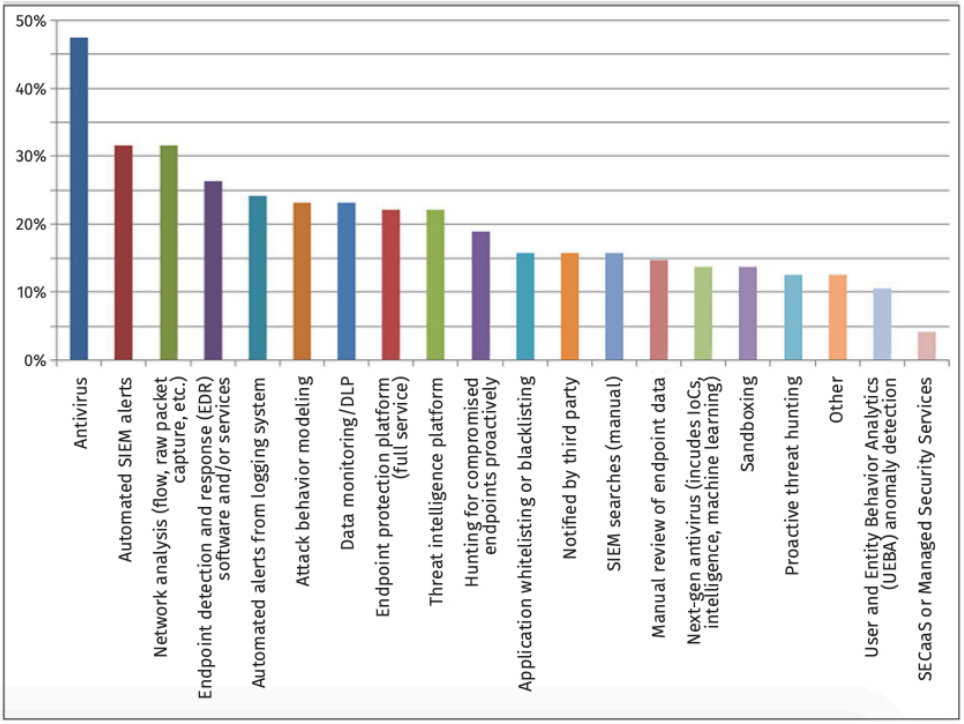
---

[10] https://digitalguardian.com/blog/what-endpoint-detection-and-response-definition-endpoint-detection-response

Crowdstrike tarafından yayınlanan ‘CrowdStrike Endpoint Protection Buyers Guide[11]’ makalesi de EDR için benzer bir yaklaşımdan bahsetmektedir. Crowdstrike’a göre bir EDR aşağıdaki beş özelliğe sahip olmalıdır:

- Engelleme: Kötücül yazılımları mümkün olduğunca uzak tutabilme;
- Tespit: Saldırganları bulup sistemden uzaklaştırma;
- Yönetilebilen tehdit avcılığı: Tespit yöntemlerini otomasyonun ötesine götürmek;
- Tehdit İstihbaratı Entegrasyonu: Saldırganları anlamak ve bir adım önlerinde bulunabilmek;
- BT Sağlığı ve Zafiyet Analizi: Saldırıları önlemek ve gelebilecek olan saldırılara karşı önlem almak;

Chauhan [65] ’ın araştırma verilerine göre uç nokta koruması için sadece bir antivirüs kullanmak yeterli olmamaktadır. Yukarıda bahsedilen güvenlik önlemleri bir arada kullanıldığı zaman daha bütüncül bir uç nokta güvenliği sağlanabilmektedir. Şekil 4.9’da gösterildiği üzere antivirüsler saldırıların sadece %47’sini engellenmesinde ve tespit edilmesinde kullanılmıştır.



Şekil 4.9. Farklı Çözümlere göre Tehdit Engelleme ve Tespit Oranları

[11] https://www.crowdstrike.com/resources/white-papers/crowdstrike-endpoint-protection-buyers-guide/

4.2.4. Sıkılaştırmalar

Kurumların ICT sistemleri sürekli olarak tehdit altındadırlar. Bu nedenle sistemlerin mümkün olduğunca kısıtlı bir saldırı yüzeyine sahip olmaları gerekmektedir. Bunu sağlamak için sistemler üzerinde gereksiz servislerin kapatılması, kullanıcıların kısıtlanması vb. işlemler uygulanır. Bu işlemlerin tümüne sıkıştırma denir.

Bir NIST yayını olarak Scarfone et. al. [71] 'a göre sistem yöneticileri bir işletim sisteminin güvenliğini sağlamak ve sıkılaştırmak için aşağıdaki adımları izlemelidirler:

- **Gereksiz servislerin, uygulamaların ve ağ protokollerinin kaldırılması:** İdeal olarak bir sunucu sadece bir amaca hizmet etmelidir. İşletim sistemi yapılandırılırken gereksiz olan bütün uygulamalar, servisler ve ağ protokolleri (Ör: IPv4, IPv6) kaldırılmalı, kaldırılamadığı takdirde etkisiz (disabled) hale getirilmelidir. Mümkünse işletim sisteminin minimal hali yüklenmeli ve bunun üzerinde gerekli uygulamalar eklenmelidir. Gerekmediği takdirde kaldırılması gereken servislere örnek olarak; dosya ve yazıcı paylaşma servisi, kablosuz ağ servisi, dizin servisleri, web servisleri, e-posta servisleri ve sistem geliştirme araçları verilebilir.
- **Kullanıcı kimlik doğrulamasının yapılandırılması:** Sunuculara yetkili erişim sistem yöneticileri ile kısıtlanır; fakat sunuculara normal erişim herkese açık olabilir. Güvenlik politikalarının doğru şekilde uygulanması için gerektiği takdirde kullanıcılardan ek kimlik doğrulama yöntemleri kullanmaları istenebilir. Doğru bir şekilde kimlik doğrulaması yapılması için gereksiz varsayılan hesapların kapatılması veya etkisizleştirilmesi, etkileşimsiz (non-interactive) hesapların etkisizleştirilmesi, kullanıcıların doğru kullanıcı gruplarına atanması, hangi kullanıcının hangi servisi kullanabileceğinin belirlenmesi ve bütün sunucular arasında zaman eşlemesi olması gerekmektedir.
- **Kaynak yönetiminin yapılandırılması:** Bütün modern işletim sistemleri dosyalara, dizinlere, cihazlara ve diğer kaynaklara erişim için yetkilendirme ataması yapabilmektedir. Kaynak erişimleri doğru şekilde yapılandırıldığı takdirde kullanıcıların istemli veya istemsiz bir kaynak erişimi yapması kontrol altına alınmış olur. Örnek olarak dosya ya da dizinlere okuma yetkisi verilmemesi gizlilik prensibinin sağlanmasına yardımcı olurken, yazma yetkisi verilmemesi ise bütünlük ilkesinin sağlanmasına yardımcı olur.

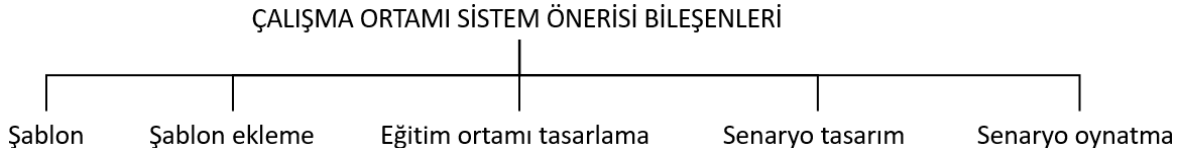
5. BİR GERÇEK-ZAMAN SİBER TEHDİTLER, SALDIRI TESPİTİ VE SALDIRILARIN ÖNLENMESİ İÇİN ÇALIŞMA ORTAMI SİSTEM ÖNERİSİ

Kullanıcıların bilgi güvenliği ile ilgili bilgi düzeylerini arttırmak ve edindikleri yetenekleri güvenli bir ortamda deneme ihtiyaçları vardır. Bu ortamın sağlanması için alınan eğitimlere yönelik araçları kullanabilecekleri veya zararlı eylemleri gözlemleyebilecekleri bir platform kurulmalıdır. Bu platform dinamik bir şekilde isteğe göre şekillendirilebilmelidir. Kullanıcıların önceden tanımlanmış olan senaryolar doğrultusunda en verimli şekilde yeteneklerini deneyimlemeleri sağlanmalıdır.

Bu ortamın yaratılabilmesi gerekli olan donanımların tanımlanması gerekmektedir. Bu tanımlama yapılırken çalışma ortamının sınırları çizilmelidir. Aynı amaca hizmet eden birçok farklı teknoloji bulunmaktadır. Bu teknolojilerin bir kısmı açık kaynak projelerden oluş da büyük bir çoğunluğu ücretli ürünlerdir. Örnek olarak güvenlik duvarları ile ilgili bir çalışma ortamı hazırlanırken açık kaynak PfSense gibi bir ürün kullanılabileceği gibi Sophos gibi paralı bir üründe kullanılabilmektedir.

Dikkat edilmesi gereken başka bir unsur ise kullanılacak teknolojilerin sanallaştırılabilir olmasıdır. Öneri olarak sunulan çalışma ortamı mümkün olduğunca sanallaştırılabilir teknolojiler içermelidir. Bunun nedeni günümüz teknolojileri ile sanal ortamların hızlı bir şekilde ihtiyacı karşılamaya yönelik kurulup kaldırılabilmesidir.

Önerilen çalışma ortamı beş bileşenden oluşacaktır. Bu bileşenler Şekil 5.1'de gösterilmiştir ve açıklamaları aşağıda verilmiştir.

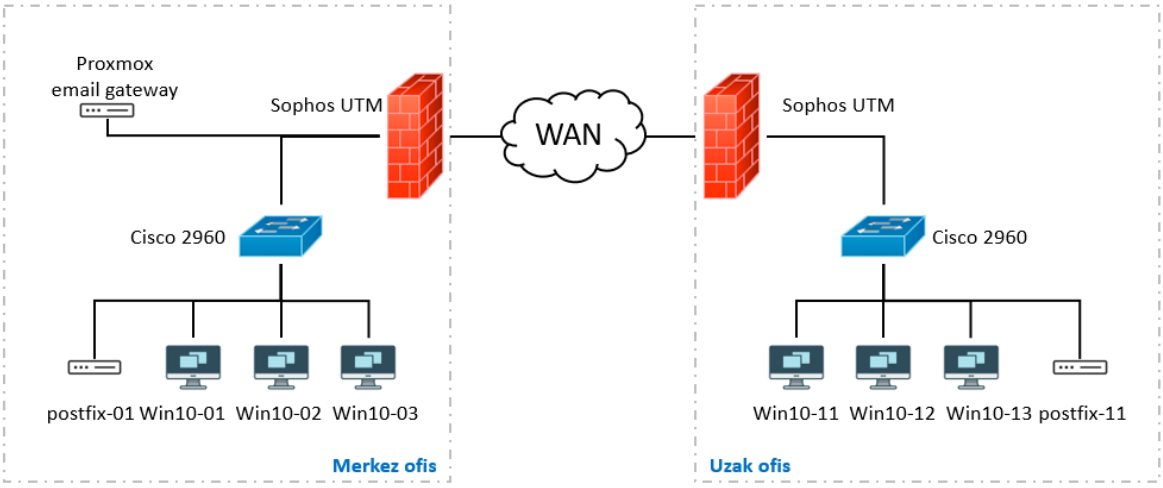


Şekil 5.1. Çalışma ortamı sistem önerisi bileşenleri

Önerilen çalışma ortamının temel taşını bu sanal ortamda yer alan şablonlar oluşturmaktadır. Bir şablon; çalışma ortamı hazırlanırken kullanılacak olan en küçük yapı taşıdır. Şablon içerisinde sanallaştırılması istenen teknolojiyi ve çalışma ortamı oluşturma araçlarının yönetimini sağlayacak araçları içermelidir. Örnek olarak Windows 10 şablonu verilebilir. Bu şablon temel Windows 10 işletim sistemini, uzaktan kurulum sağlamak için gerekli kullanıcıyı ve uzaktan yönetime olanak sağlayacak yetkileri içermelidir.

Önerilen çalışma ortamının ikinci önemli bileşeni ise şablon ekleme ortamıdır. Bu ortam yeni teknolojileri şablon olarak eklemeye olanak sağlayacaktır. Şablonlar yaygın olarak kullanılan sanallaştırma teknolojilerinin desteklediği disk görüntüsü dosya tiplerinde yaratılabilecektir. Bu dosya tipleri; vmdk, vdi, vdh, hdd ve qcow2'dir. Eğitim ortamı sistem yöneticisi, önceden hazırlanmış olan şablonları bu bileşen yardımı ile sisteme aktarabilecektir.

Üçüncü önemli bileşen eğitim ortamı tasarlama bileşenidir. Bu bileşen aracılığı ile sistem üzerinde bulunan şablonlar, eğitim ortamının gereksinimlerine göre bir araya getirilecektir. Bir araya getirilen şablonların bir ağ oluşturacak şekilde birbirleri ile bağlantılarının tanımlaması bu bileşen kullanılarak yapılacaktır. Tez önerisi olarak sunulan sistem görsel olarak Şekil 5.2'de gösterilen şema benzeri bir tasarım ortamı sağlayacaktır.



Şekil 5.2. Örnek eğitim ortamı tasarımı

Yukarıdaki örnekte bir e-posta ağ geçidi uyum çalışması gösterilmiştir. Bu çalışmada iki farklı merkezde yeri bulunan bir kurum gösterilmiştir. Bu kurumlara gelen e-postalar öncelikle merkez ofiste yer alan e-posta ağ geçidine gönderilecektir. Daha sonra güvenlik kontrolünden geçen e-postalar iç ağda yer alan posta sunucularına gönderilecektir. Bu çalışma alanı farklı teknolojilerin birbirlerine eğitim ortamı tasarlama bileşeni kullanılarak nasıl etkileşim kuracaklarını tasarlama imkanı tanımaktadır. Şekil 5.2'de Cisco ağ anahtarları, Sophos UTM güvenlik duvarları, Windows 10 işletim sistemleri, postfix eposta sunucuları ve Proxmox e-posta ağ geçidi kullanılmıştır.

Önerilen çalışma ortamının dördüncü bileşeni senaryo tasarım bileşenidir. Bu bileşen sayesinde her bir şablon özelleştirilir. Bu özelleştirme şablonlar üzerine kurulacak uygulamalar, yapılacak yapılandırmaları içermektedir. Özelleştirmeler belli bir betik dilinde

yazılacaktır ve her bir şablona senaryo tasarım bileşeni aracılığı ile uzaktan yüklenecektir. Bu bileşen ayrıca tasarlanmış senaryoların kaydedilmesine ve tekrardan yüklenebilmesine olanak sağlayacaktır. Bu sayede bir senaryo farklı zamanlarda tekrar oynatılabilecektir.

Beşinci bileşen senaryo oynatma bileşenidir. Bu bileşen tasarlanmış senaryonun başlatılmasına ve senaryoya dahil olan kişilerin eylemlerinin takip edilmesine olanak sağlayacaktır. Bu bileşen sayesinde eğitim ortamında eğitmen, öğrencilerin yaptıklarını takip edebilecektir ve gerektiğinde müdahale edebilecektir.

6. SONUÇ VE ÖNERİLER

6.1. Özet

"Bilgi" anlamı ve değeri son yıllarda önem kazanmıştır. Ona paralel olarak "Bilgi Güvenliği" de dikkat çeker ve önem kazanır olmuştur. Küçük-büyük ayırt edilmeksizin tüm kurum ve kuruluşlar için ihmal edilmesi çok pahalı bedel ödenmesi gereken bir konudur. Bu çalışmada Bilgi Güvenliğinin ne olduğu, ne gibi yazılım ve donanım bileşenlerinden oluştuğu titizlikle incelenmiş ve gereken kaynakları da sunarak özetlenmiştir.

6.2. Sonuç

Birçok hizmet ve servisin altyapısı bilgi sistemlerine dayanmaktadır. Böyle bir sistemde yer alan bilginin güvenliğinin önemi her geçen gün katlanarak artmaktadır. Bilgi güvenliği yeterli seviyeye ulaşmadığı takdirde oluşabilecek bir siber saldırının etkisi büyük ve yıkıcı olmaktadır. Yapılan çalışma sonucunda literatürde var olan siber güvenlik kavramları tanımlanmıştır. Bu tanımlama ile siber farkındalığın yükseltilmesi ve bilgi güvenliğinin öneminin anlaşılması hedeflenmiştir. Sunulan çözüm önerisi ile de bilgi güvenliği alanında çalışan insanlara veya kurumlara bilgi güvenliği kavramlarının anlatılması, eğitim ortamlarının sağlanabilmesi ve çeşitli senaryolar ışığında etkinlikler düzenlenebilmesi hedeflenmiştir.

6.3. Öneriler

Bilgi güvenliği her çalışma alanı için büyük önem arz etmektedir. Bu alanlarının en önemlilerinden biri ise medikal alandır. Medikal cihazların tasarımında teknolojinin ilerlemesi, hasta bilgi yönetimi ve ağ entegrasyon yeteneklerine sahip daha fazla cihaza yol açmıştır. Buna iyi bir örnek kalp içine yerleştirilen elektronik cihazlar olacaktır. Teknolojinin ilerlemesi ile birlikte bu cihazlar kablosuz bağlantı teknolojilerini kullanarak sakladıkları verinin sorgulanmasına, değiştirilmesine ve erişilmesine olanak sağlamaya başlamışlardır. Bu gelişme sayesinde hastaların iyileşme ve hastanede yatırılma zamanlarında büyük iyileşmeler gözlemlenmiştir [72]. Fakat iyileşmelerin yanında bu cihazlar siber saldırganların hedefleri haline gelmeye başlamıştır. Modern sağlık kuruluşları, hasta bakımını verimli ve etkili bir şekilde sunmanın yeni yollarını aradıkça, tıbbi cihazlar giderek daha fazla birbirine bağlanmaktadır [73].

Sağlık sistemleri çeşitli nedenlerden dolayı siber saldırılara karşı savunmasızdır. Bu sistemler birbirine bağlı birçok cihaz içermesine rağmen, kullanılan ürünler güvenlik standartlarına sahip değildirler ve ekipman tedarik edilirken siber güvenliğin bir öncelik olması pek mümkün değildir. Bu sistemlerin işleyişi sırasında yaşanabilecek başarısızlıklar, hastalar için hem klinik hem de kişisel verilerin ihlali açısından derin sonuçlar doğurur. Gelecek çalışma alanı olarak sağlık sistemlerinde siber güvenlik sağlanabilmesi için gerekli olan standartlar araştırılacak ve tez önerisi olarak sunulan sisteme sağlık sistemlerinin entegrasyonu incelenecektir.

KAYNAKLAR

[1] L. Pridmore, P. Lardieri, R. Hollister, "National Cyber Range (NCR) automated test tools: Implications and application to network-centric support tools," 2010 IEEE AUTOTESTCON, Orlando, FL, pp. 1-4, Sept. 2010, doi: 10.1109/AUTEST.2010.5613581

[2] D. Williams, R. L. Davis, C. Cothren, G. White and A. Conklin, *Principles of Computer Security: CompTIA Security+ and Beyond, Fifth Edition, 5th Edition*. NY, USA: McGraw-Hill, 2018.

[3] L. Garber, "Melissa Virus Creates a New Type of Threat," *Computer*, vol. 32, no. 6, pp. 16-19, Jun. 1999, DOI: 10.1109/MC.1999.769438

[4] H. Berghel, "The Code Red Worm," *Commun. ACM*, vol. 44, no. 12, pp. 15-19, Dec. 2001, DOI: https://doi.org/10.1145/501317.501328

[5] J.P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, vol. 53, no. 1, s. 23-40, 2011, DOI: 10.1080/00396338.2011.555586

[6] G. Sanchez, "Case Study: Critical Controls that Sony Should Have Implemented," Sans Institute, Jun. 22, 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022

[7] M. Nieles, K. Dempsey and V. Y. Pillitteri, "An Introduction to Information Security," NIST Special Publication 800-12 Revision 1, Jun., 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

[8] D. Death, *Information Security Handbook*. Birmingham, UK: Pact Publishing, 2017.

[9] D. Gibson, *SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Third Edition.* NY, USA: McGraw-Hill Education, 2018.

[10] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Waltham, MA, USA: Elsevier, 2011.

[11] Y. Korff, P. Hope and B. Potter, *Mastering FreeBSD and OpenBSD Security: Building, Securing, and Maintaining BSD Systems*. Sebastapol, CA, USA: O'Reilly Media, Inc., 2005.

[12] S. Rahalkar and S. Jetty, *Securing Network Infrastructure*. Birmingham, UK: Packt Publishing, 2019.

[13] J. Ingeno, *Software Architect's Handbook*. Birmingham, UK: Packt Publishing, 2018.

[14] P. Gregory and L. Miller, *CISSP For Dummies, 4th Edition*. Hoboken, NJ, USA: John Wiley & Sons, 2012.

[15] J. Erickson, *Hacking: The Art of Exploitation, 2nd Edition*. San Francisco, CA, USA: No Starch Press, Inc., 2008.

[16] N. Radziwill, J. Romano, D. Shorter and M. Benton, "The Ethics of Hacking: Should It Be Taught?," *Software Quality Professional,* vol. 18, no. 1, pp. 11-15, Dec. 9, 2015. [Online]. Available: https://arxiv.org/pdf/1512.02707.pdf

[17] A. A. Jagnarine, "The Role of White Hat Hackers in Information Security," Pforzheimer Honors College, Pace Univ., 2005.

[18] A. Harper, S. Harris, J. Ness, C. Eagle, G. Lenkey and T. Williams, *Gray Hat Hacking The Ethical Hacker's Handbook Third Edition*. NY, USA: The McGraw-Hill Companies, 2011.

[19] J. R. Vacca, *Computer and Information Security Handbook*. Waltham, MA, USA: Morgan Kaufman Publishers, 2012.

[20] Z. Sabih, *Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing.* Birmingham, UK: Packt Publishing, 2018.

[21] R. Baloch, *Ethical Hacking and Penetration Testing Guide*. Boca Raton, FL, USA: CRC Press, 2015.

[22] J. M. Kizza, *Computer Network Security and Cyber Ethics Fourth Edition*. Jeferson, North Carolina, USA: McFarland & Company, Inc., Publishers, 2014.

[23] R. Enbody and A. Sood, *Targeted Cyber Attacks*. Waltham, MA, USA: Syngress, 2014.

[24] M. C. Libicki, L. Ablon and T. Webb, "Defender's Dilemma: Charting a Course Toward Cybersecurity," RAND Corporation, 2015. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf

[25] L. Ablon and A. Bogart, "Zero Days, Thousands of Nights The Life and Times of Zero-Day Vulnerabilities and Their Exploits," RAND Corporation, 2017. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf

[26] E. Dulaney and C. Easttom, *CompTIA Security+ Study Guide Seventh Edition*. Indianapolis, IN, USA: Sybex, 2017.

[27] R. Santanam, *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives*. Hershey, PA, USA: Information Science Reference, 2010.

[28] J. Schroeder, *Advanced Persistent Training: Take Your Security Awareness Program to the Next Level.* Edinburgh, UK: Apress, 2017.

[29] "Security Awareness -- Definition, History, And Types." INFOSEC. https://resources.infosecinstitute.com/category/enterprise/securityawareness/#gref (Accessed: Apr. 02, 2020).

[30] B. Gardner and V. Thomas, *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats 1st Edition*. Waltham, MA, USA: Syngress, 2014.

[31] D. J. Landoll, *Information Security Policies, Procedures, And Standards: A Practitioner's Reference*. Boca Raton, FL, USA: CRC Press, 2017.

[32] R. M. Blank and P. D. Gallagher, "Information Security," NIST Special Publication 800-30 Revision 1, Sept. 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[33] I. Neil, *CompTIA Security+ Certification Guide.* Birmingham, UK: Packt Publishing, 2018.

[34] Verizon, "2019 Data Breach Investigations Report," [Online]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[35] Y. Diogenes and E. Ozkaya, *Cybersecurity – Attack and Defense Strategies Infrastructure Security with Red Team and Blue Team Tactics.* Birmingham, UK: Pact Publishing, 2018.

[36] "Security Tip (ST04-015) Understanding Denial-of-Service Attacks," Cybersecurity and Infrastructure Security Agency (CISA). https://www.us-cert.gov/ncas/tips/ST04-015 (Accessed: Apr. 04, 2020)

[37] "Denial-of-service attack." Vikipedi. https://tr.wikipedia.org/wiki/Denial-of-service_attack (Accessed: Apr. 04, 2020)

[38] C. Easttom, *Computer Security Fundamentals, 4th Edition*. Indianapolis, IN, USA: Pearson IT Certification, 2019.

[39] A. Bettany and M. Halsey, *Windows Virus and Malware Troubleshooting.* New York, NY, USA: Apress, 2017.

[40] M. Meyers and S. Jernigan, *Comptia Security+ Certification Guide Second Edition.* NY, USA: McGraw-Hill Education, 2018.

[41] EC-Council, "Most Common Web Application Attacks And How To Defend Against Them." EC-Council Blog. https://blog.eccouncil.org/most-common-web-application-attacks-and-how-to-defend-against-them/ (Accessed: Mar 22, 2020)

[42] "Security Report for In-Production Web Applications," Rapid7, 2018. [Online]. Available: https://information.rapid7.com/tCell-web-application-security-report.html

[43] "2019 Vulnerability Statistics Report," Edgescan, 2019. [Online]. Available: https://www.edgescan.com/wp-content/uploads/2019/02/edgescan-Vulnerability-Stats-Report-2019.pdf

[44] A. Salmon, W. Levesque and M. McLafferty, *Applied Network Security.* Birmingham, UK: Packt Publishing, 2017

[45] C. Easttom, *Network Defense and Countermeasures: Principles and Practices, Third edition.* Indianapolis, IN, USA: Pearson IT Certification, 2018.

[46] L. Brotherston and A. Berlin, *Defensive Security Handbook.* Sebastopol, CA, USA: O'Reilly Media, Inc., 2017.

[47] O. Santos and M. Gregg, *Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd Edition.* Indianapolis, IN, USA: Pearson IT Certification, 2019.

[48] A. K. Pathan, *The State of the Art in Intrusion Prevention and Detection.* Boca Raton, FL, USA: CRC Press, 2014.

[49] J. Ryan, M. J. Lin and R. Mikkkulainen, "Intrusion Detection with Neural Networks, Advances in neural information processing systems," 1998. Accessed: May, 08, 2019. [Online]. Available: http://www.cs.utexas.edu/~ai-lab/pubs/ryan.intrusion.pdf

[50] A. Hay, D. Cid and R. Bray, *OSSEC Host-Based Intrusion Detection Guide.* Burlington, MA, USA: Syngress Publishing, Inc., 2008.

[51] M. W. Lucas, *Network Flow Analysis*. San Francisco, CA, USA No Starch Press, 2010.

[52] R. Bejtlich, *The Practice of Network Security Monitoring*. San Francisco, CA, USA No Starch Press, 2013.

[53] K. Saini, *Squid Proxy Server 3.1 Beginner's Guide*. Birmingham, UK: Packt Publishing, 2011.

[54] N. H. Tanner, *Cybersecurity Blue Team Toolkit*. Indianapolis, IN, USA: Wiley, 2019.

[55] "CIS Controls v7.1," Center for Internet Security, Inc., 2019. [Online]. Available: https://learn.cisecurity.org/cis-controls-download

[56] W. A. Conklin, G. White, D. Williams, C. Cothren and R. L. Davis, *CompTIA Security+ All-in-One Exam Guide, Fifth Edition (Exam SY0-501), 5th Edition*. New York, NY, USA: McGraw-Hill Education, 2018.

[57] E. Carter and J. Hogue, *Intrusion Prevention Fundamentals*. Indianapolis, IN, USA: Cisco Press, 2006.

[58] S. Winterfeld and J. Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham, MA, USA: Syngress, 2012.

[59] B. Komar, R. Beekelaar and J. Wettern, *Firewall For Dummies 2nd Edition*. Wiley Publishing, Inc., 2003.

[60] "Why Do You Need Sandboxing for Protection?," Fortinet, 2014. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/Why-Do-You-Need-Sandboxing.pdf

[61] K. D. Dent, *Postfix: The Definitive Guide.* North Sebastopol, CA, USA: O'Reilly Media, Inc., 2003.

[62] "What is a Secure Email Gateway? Secure Email Gateway Defined and Explored," Forcepoint. [Online]. Available: https://www.forcepoint.com/cyber-edu/secure-email-gateway

[63] C. Russell, *Web Application Firewalls: Securing Modern Web Applications.* North Sebastopol, CA, USA: O'Reilly Media, Inc., 2018.

[64] L. Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, Jun. 12, 2018. [Online]. Available: https://www.sans.org/reading-room/whitepapers/clients/paper/38460

[65] A. S. Chauhan, *Practical Network Scanning*. Birmingham, UK: Packt Publishing, 2018.

[66] A. Chu, *CCNA Cyber Ops SECOPS – Certification Guide 210-255*. Birmingham, UK: Packt Publishing, 2019.

[67] J. Nickel, *Mastering Identity and Access Management with Microsoft Azure - Second Edition*. Birmingham, UK: Packt Publishing, 2019.

[68] M. L. Srinivasan, *CISSP in 21 Days - Second Edition*. Birmingham, UK: Packt Publishing, 2016.

[69] M. Bennett, *CompTIA A+ Certification Guide (220-901 and 220-902)*. Birmingham, UK: Packt Publishing, 2017.

[70] "Büyük Ölçekli İşletmeler İçin Uç Nokta Tespit ve Yanıt Çözümlerine Yönelik Yatırım Rehberi 2017-2018," AO Kaspersky Lab, 2017. [Online]. Available: https://media.kaspersky.com/tr/business-security/enterprise/KEDR_Product_Whitepaper_Customer_TR.pdf

[71] K. Scarfone, W. Jansen and M. Tracy, “Guide to General Server Security: Recommendations of the National Institute of Standards and Technology,” NIST Special Publication 800-123, Jul 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-123.pdf

[72] A. Kapoor, A. Vora and R. Yadav, “Cardiac devices and cyber attacks: How far are they real? How to overcome?,” *Indian Hearth Journal*, vol. 71, no. 5, s. 427-430, 2019. [Online] Available: https://www.sciencedirect.com/science/article/pii/S0019483220300237?via%3Dihub

[73] A. J. Coronado and T. L. Wong, “Healthcare Cybersecurity Risk Management: Keys To an Effective Plan.,” Biomedical Instrumentation & Technology: Cybersecurity In Healthcare, vol. 48, no. 1, s. 26-30, 2014. [Online] Available: https://www.aami-bit.org/doi/full/10.2345/0899-8205-48.s1.26