



**T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

**SİBER GÜVENLİK, BİLGİSAYAR AĞLARI, KİMLİK AVI,
KÖTÜ AMAÇLI YAZILIM, FİDYE YAZILIMI, SOSYAL
MÜHENDİSLİK BİÇİMİNDE KORSANLIKTAN KORUNMAYA
YÖNELİK İNCELEMELER VE BİR UYGULAMA**

**YÜKSEK LİSANS TEZİ
Mehmet Özer BAŞESKİOĞLU
195113002**

**Adli Bilişim Anabilim Dalı
Adli Bilişim (Tezli) Programı**

Tez Danışmanı: Doç.Dr. Abdülkadir TEPECİK

EYLÜL 2021



**T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

**SİBER GÜVENLİK, BİLGİSAYAR AĞLARI, KİMLİK AVI,
KÖTÜ AMAÇLI YAZILIM, FİDYE YAZILIMI, SOSYAL
MÜHENDİSLİK BİÇİMİNDE KORSANLIKTAN KORUNMAYA
YÖNELİK İNCELEMELER VE BİR UYGULAMA**

**YÜKSEK LİSANS TEZİ
Mehmet Özer BAŞESKİOĞLU
195113002**

**Adli Bilişim Anabilim Dalı
Adli Bilişim (Tezli) Programı**

Tez Danışmanı: Doç.Dr. Abdülkadir TEPECİK

EYLÜL 2021



ÖNSÖZ

Hayat boyu öğrenme hedefiyle çıktığım bu yolda Tezi yazmamda emeği ve bilgisi ile her zaman destek olan Danışmanım Doç. Dr. Abdülkadir TEPECİK'e Yüksek Lisansa başlayıp bu zamana kadar bilgisi ve sabrıyla desteklerini esirgemeyen Prof. Dr. Murat GÖK Hocama başta teşekkürlerimi sunarım. Bu süreçte destekleriyle her zaman yanımda olan Aileme sonsuz şükranlarımı sunarım. Mensubu olmaktan gurur duyduğum Hazine ve Maliye Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü'ndeki amirlerim başta olmak üzere Koordinatörüm Mehmet GÖĞEBAKAN'a desteklerinden dolayı oda arkadaşlarım İsa ERKORKMAZ, Ali KARASU ve Murat Emin SAYAN'a tezdeki yazım yanlışlarını düzelterek yardımlarını esirgemeyen arkadaşım Buhar TULUM'a sevgi saygı ve şükranlarımı sunarım. Beni bu Yüksek Lisans yolunda üzen tek şey olan Covid-19 sebebiyle aramızdan ayrılan Hasan İŞLEK abimi rahmet ve özlem ile anmak isterim.

Kasım 2021

Mehmet Özer BAŞESKİOĞLU

Bilgisayar Mühendisi

Sistem Uzmanı



İÇİNDEKİLER

	Sayfa
	No
ÖNSÖZ	iii
İÇİNDEKİLER.....	v
KISALTMALAR.....	xv
ŞEKİL LİSTESİ	xvii
ÖZET	xx
ABSTRACT	xxii
1.GİRİŞ	1
2.SİBER GÜVENLİK VE NEDEN ÖNEMLİDİR.....	9
2.1 Siber Güvenlik Nedir?	9
2.2 Siber Güvenlik Neden Önemlidir?	11
2.3 Siber Güvenlik Senaryoları	12
2.4 Her Şeyin Buluta Taşındığı Bulut nedir?.....	13
3.SİBER SALDIRILAR VE HACKERLER.....	14
3.1 Siber Suçların Sınıflandırılması	15
3.1.2 İçeriden Bilgilendirme Saldırısı	15
3.1.3 Harici Saldırı	15
3.2 Yapılandırılmamış Saldırıları	16
3.3 Yapılandırılmış Saldırıları.....	16
3.4 Siber Suçların Nedenleri	16
3.4.1 Para	17
3.4.2 İntikam	17
3.4.3 Tanınma	17
3.4.4 Siber casusluk.....	17
3.5 Siber Hacker Türleri	17
3.5.1 Beyaz Şapkalı Hackerler.....	18
3.5.2 Siyah Şapkalı Hackerler.....	18
3.5.3 Gri Şapkalı Hackerler	18
3.5.4 Lamerler	18
3.5.5 Yeşil Şapkalı Hackerler	19
3.5.6 Red Hat Hackerleri	19
3.5.7 Devlet Destekli Hackerler	19
3.5.8 Hacktivist	19



3.6 Bilgisayar Korsanları Tarafından Kullanılan Genel Araçlar	20
3.6.1 Rootkit.....	20
3.6.2 Tuş kaydediciler (Keylogger).....	20
3.6.3 Güvenlik Açığı Tarayıcıları	20
3.7 Siber Suç Türleri	21
3.7.1 Siber taciz.....	21
3.7.2 Siber terörizm	21
3.7.3 Siber Vandalizm	21
3.7.4 E-dolandırıcılık.....	22
3.7.5 Hacklemek (Bir Bilgisayar veya sisteme sızarak ele geçirmek)	22
3.7.6 Kötü Amaçlı Yazılım Yayımak.....	22
3.7.7 Siteler Arası Komut Dosyası.....	23
3.7.8 Spam yapma	23
3.7.9 Siber İşgal	23
3.7.10 Çevrimiçi Açık Artırma Sahtekârlıkları.....	23
3.7.11 İnternet Zaman Hırsızlığı	23
3.7.12 Web Krikosu.....	24
3.7.13 Hizmeti engelleme saldırısı (DDoS).....	24
3.7.14 E-posta Sahtekârlığı.....	24
3.7.15 Salam Saldırısı.....	24
3.7.18 Veri Karıştırması	24
3.7.19 Mantık Hatası	25
4.BİR KİMLİK AVI SALDIRISINI TANIMA VE ÖNLEME	26
4.1 Kimlik avı nedir?	26
4.2 Kimlik avı için kullanılan yöntemler	26
4.3 Kimlik Avı Saldırılarıyla Mücadele Etmenin Yaygın Yolları	27
4.3.1 Aldatıcı Kimlik Avı	27
4.3.2 Yemleme kancası (Spear phishing)	28
4.3.3 Balina Saldırısı (Whale Attack)	28
4.3.4 Vishing – Smishing	29
4.3.6 Pharming	29
4.4 Bir Kimlik Avı E-postasını Tanımlama.....	30
4.4.1 E-posta Sahtekârlığı.....	30
4.4.2 Sahte Bir E-postayı Tanımlama	31
4.4.3 Alınan-SPF.....	31



4.4.4 X-CMAE Puanı - 100	31
4.4.5 Referans E-postası: (Kullanılan Şablon).....	32
5. KÖTÜ AMAÇLI YAZILIM NASIL BELİRLENİR VE KALDIRILIR.....	34
5.1 Kötü Amaçlı Yazılım Türleri.....	34
5.1.1 Virüsler	34
5.1.2 Solucanlar-Wormlar	36
5.1.3 Truva Atları.....	38
5.1.4 Hibrit Kötü Amaçlı Yazılım.....	39
5.1.5 Fidyeye Yazılımı.....	39
5.1.5.1 Enfekte Olunursa Ne Yapılmalıdır.	40
5.1.5.2 Fidyeye Yazılımından Nasıl Korunuruz.....	41
5.1.6 Dosyasız Kötü Amaçlı Yazılım.....	42
5.1.7 Reklam Yazılımı ve Kötü Amaçlı Reklamcılık	42
5.1.8 Casus Yazılım.....	43
5.2 Sistemde Virüs Veya Kötü Amaçlı Yazılım Olduğu Nasıl Anlaşılır?	45
5.3 Antivirüs Ve Kötü Amaçlı Yazılımdan Korunmak Gereklimi?	46
5.4 Kötü Amaçlı Yazılımlardan Koruma	46
5.4.1 Antivirüsünüzü Kurun / Güncelleyin.....	47
5.4.2 Sistem Geri Yükleme.....	47
5.4.3 İnternet Bağlantısını Kesin.....	47
5.4.4 Taşınabilir Bir Antivirüs Çözümü Edinin.....	48
6.BİR SOSYAL MÜHENDİSLİK SALDIRISI NASIL TESPİT EDİLİR VE DURDURULUR.....	50
6.1 Sosyal Mühendislik Metodolojileri	50
6.2 Bir Sosyal Mühendislik Saldırısını Tespit Etme	51
6.2.1 Bir Arkadaştan E-posta.....	51
6.2.2 Güvenilir Bir Kaynaktan Bir E-posta	52
6.3 Sosyal Mühendisliğe Düşmekten Nasıl Kaçınılır?.....	54
6.3.1 Ağırdan Almak	55
6.3.2 Araştırmaya Biraz Zaman Harcayın	55
6.3.3 Bağlantılara Körü Körüne Tıklamayın	55
6.3.4 E-posta Hack'lerinin Farkında Olun	55
6.3.5 Körü Körüne İndirme.....	55
6.3.6 Piyangoların Sahte Olduğunu Bilin	55
6.3.7 Banka Dolandırıcılıklarına Dikkat Edin	56
6.3.8 Yardım Tekliflerini Reddet	56

6.3.9 Spam Filtrelerinizi Yapılandırın.....	56
6.3.10 Tüm Cihazlarınızı Koruyun	56
7.AĞ GÜVENLİĞİ VE KORUMA TEKNİKLERİ.....	57
7.1 Ağ Güvenliği.....	57
7.2 Ağ Güvenliği Nasıl Çalışır?.....	57
7.3 Ağ Güvenliğinin Faktörleri.....	57
7.3.1 Fiziksel Ağ Güvenliği.....	58
7.3.2 Teknik Ağ Güvenliği	58
7.3.3 İdari Ağ Güvenliği.....	58
7.4 Bir Ağ Üzerinden İşletmenizi Etkileyebilecek İlk Beş Saldırı	58
7.4.1 Gelişmiş Kalıcı Tehdit (APT)	59
7.4.2 Hizmet Reddi Saldırısı (DoS)	59
7.4.3 Nesnelerin İnterneti (IoT) Hacking	60
7.4.4 Yapılandırılmış Sorgu Dili (SQL) Enjeksiyonu	60
7.4.5 Ortadaki Adam	60
7.6 Bir İşletmeyi Siber Saldırıdan Koruma	61
7.7 Donanım Aracılığıyla Siber Güvenlik	61
7.7.1 Güvenlik Anahtarları	61
7.7.2 VPN Güvenlik Duvarları	62
7.8 Yapılandırmalar ve Ayarlar aracılığıyla Siber Güvenlik.....	63
7.8.1 Çok Faktörlü Kimlik Doğrulama.....	63
7.8.2 Şifre Kasası	63
7.8.3 Otomatik Güncellemeler	64
7.8.4 Tam Disk Şifreleme	64
7.8.5 Kötü Amaçlı Yazılım Tarayıcıları.....	65
7.8.6 IP Adresi Sabitleme	65
7.8.7 Sistem Yedeklemeleri	65
7.9 Güvenlik Eğitimi	65
8.WEB UYGULAMASI GÜVENLİĞİ.....	66
8.1 Web Uygulama Güvenliği	66
8.2 Web Uygulamalarını Nasıl Güvenceye Alınır	67
8.3 Web Güvenlik Açığı Tarayıcıları	68
9. KALİ LİNX	70
9.1 Kali Linux Nedir?.....	70
9.2. Canlı Sistem (Live ISO)	74



9.3 Adli Araç Modu (Forensic Tool Mod)	74
9.4. Özel Bir Linux Çekirdeği.....	74
9.5. Özelleştirilebilme Özelliği	75
9.6. Güvenilir Bir İşletim Sistemi	75
9.7. ARM Cihazları	75
9.8. Önemli Kali Linux Toolları	76
9.8.1 Nmap.....	76
9.8.2 Burp Suite	76
9.8.3 Wireshark	77
9.8.4 Metasploit Çerçevesi	77
9.8.5 Aircrack-ng	77
9.8.6 John the Ripper	77
9.8.7 Sqlmap	77
9.8.8 Autopsy	78
9.8.9 Social Engineering Toolkit	78
10 UYGULAMA	79
10.1 NMAP Nedir ?.....	80
10.2 NMAP Tarama Teknikleri	82
10.3 NMAP Tarama Teknikleri - NSE Scripts	88
10.4 Essential NetTools	96
10.5 NMAP Uygulama Taraması ve Essential NetTools Taraması.	98
10.6 Phishing Saldırı Uygulaması.	106
11. SALDIRI TESPİT VE ÖNLEME SİSTEMLERİ	109
11.1 Firewall Cihazı Nedir? Ne İşe Yarar?	109
11.2 DDOS Koruma Ürünleri	109
11.2 IPS ve IDS Nedir? Nasıl Çalışır?	110
11.3 WAF Nedir?	111
11.4 EDR ve MDR Nedir?.....	113
11.5 Database Firewall (Veri tabanı Güvenlik Duvarı).....	114
11.6 SIEM Nedir? (Security Information and Event Management)	115
12. SONUÇ VE ÖNERİLER	117
12.1 Uygulama Sonuçları	117
12.2 Öneriler	120
KAYNAKLAR.....	128
ÖZGEÇMİŞ.....	135



KISALTMALAR

API	: Application Program İnterface
BT	: Bilgi Teknolojileri
CEH	: Certified Ethical Hacker
CPU	: Central Processing Unit
DoS	: Denial of Service
İSS	: İnternet Servis Sağlayıcısı
ISO	: International Organization for Standardization
GDPR	: General Data Protection Regulation
PDA	: Personal Digital Assistant
PCI	: Ödeme Kartları Sektörü Veri Güvenliği Standartları
PLC	: Lojistik kontrol unsurları
URL	: Uniform Resource Locator
VPN	: Virtual private network
SQL	: Structured Query Language
STS	: Saldırı Tespit Sistemleri
URL	: Uniform Resource Locator
USB	: Universal Serial Bus
SPF	: Sender Policy Framework
SSL	: Secure Sockets Layer
DNS	: Domain Name Service
TXT	: Extension for a file in the text-only format
TLS	: Transport Layer Security
Wi-Fi	: Wireless Fidelity



ŞEKİL LİSTESİ

	Sayfa
	No
Şekil 1.1. Veri ihlallerinin sınıflarına ayrılması.	3
Şekil 1.2. TÜİK Bilgi Toplumu istatistikleri.	4
Şekil 3.1 Cyber Attack.....	14
Şekil 5.1 Truva Atı.....	39
Şekil 5.2 Kötü Amaçlı Reklamcılık.....	43
Şekil 5.3 Virüs Tehdidi Altkümesi	45
Şekil 6.3 2020 Yılında Q3 tarafından bildirilen Fidyeye Yazılım ihlallerinde açığa çıkan veri türleri.....	48
Şekil 6.4 2020 Yılında Q3 tarafından bildirilen Yıllara göre Tüm ihlallerde açığa çıkan veri türleri.....	49
Şekil 8.1 Ortadaki Adam Saldırısı.....	61
Şekil 8.2 Şifre Kasası.....	64
Şekil 11.1 Kali Linux Ekranı.....	71
Şekil 10.1 Nmap Nedir 1.....	81
Şekil 10.2 Nmap Nedir 2.....	81
Şekil 10.3 Nmap Nedir 3.....	83
Şekil 10.4 Nmap Nedir 4.....	84
Şekil 10.5 Nmap Nedir 5.....	84
Şekil 10.6 Nmap Nedir 6.....	85
Şekil 10.7 Nmap Nedir 7.....	86
Şekil 10.8 Nmap Nedir 8.....	86
Şekil 10.9 Nmap Nedir 9.....	87
Şekil 10.10 Nmap Nedir 10.....	88
Şekil 10.11 Nmap Nedir 11.....	89
Şekil 10.12 Nmap Nedir 12.....	90
Şekil 10.13 Nmap Nedir 13.....	91
Şekil 10.14 Nmap Nedir 14.....	93
Şekil 10.15 Nmap Nedir 15.....	94
Şekil 10.16 Nmap Nedir 16.....	95
Şekil 10.17 Essential NetTools.....	97
Şekil 10.18 VMware Ekranı	98
Şekil 10.19 Metasploit2 Ekranı	99
Şekil 10.20 Kali Linux Terminal Ekranı.....	99
Şekil 10.21 Kali Linux Ekranı Sonuç Ekranı	100
Şekil 10.22 Google Tarama Keranı	101
Şekil 10.23 Kali Linux Terminal Saldırı Ekranı	101
Şekil 10.24 Kali Linux Saldırı Aracı Ekranı	102
Şekil 10.24 Kali Linux Saldırı Ekranı Aracı Sonucu.....	102
Şekil 10.25 Kali Linux Atak Sonucu Ekranı.....	102
Şekil 10.26 Essential NetTools Ekranı	103
Şekil 10.27 Essential NetTools Tarama Ekranı.....	104



Şekil 10.28 Bağlanılan ModemTarama Ekranı	104
Şekil 10.29 Bağlanılan Modem Arayüz Ekranı.....	105
Şekil 10.29 Güvenlik Kamerası Arayüz Ekranı	105
Şekil 10.30 Güvenlik Kamerası Ekranı.....	106
Şekil 10.31 Sahte Banka Web Sitesi Ekranı	107
Şekil 10.32 Mail Adresi Ekranı	107
Şekil 10.33 Mail adresine Gelen Şifreler	108
Şekil 11.1 IDS ve IPS	110
Şekil 11.2 WAF	112
Şekil 11.3 EDR ve MDR.....	114
Şekil 11.4 Database Firewall.....	115
Şekil 12.1 Kamu Murumları Tarama Sonuçları	117



SİBER GÜVENLİK, BİLGİSAYAR AĞLARI, KİMLİK AVI, KÖTÜ AMAÇLI YAZILIM, FİDYE YAZILIMI, SOSYAL MÜHENDİSLİK BİÇİMİNDE KORSANLIKTAN KORUNMAYA YÖNELİK İNCELEMELER VE BİR UYGULAMA

ÖZET

Günümüzde iletişim teknolojilerinin ve internetin yaygınlaşması ile tabletlerden, bilgisayarlardan, cep telefonlarına çeşitli cihazların, ağlar ile birbirlerine bağlanması, veri ihlaller ve siber saldırılara neden olmaktadır. Bu saldırı türlerinde bilgisayar donanımları, yazılımları, virüsler ve zararlı yazılımlar internetin olduğu her yer de karşılaşılmaktadır. Siber alan çoğaldıkça, veri ihlalleri de önem kazanmaya başlamıştır. Bu ihlallerin engellenmesine verilen önem artmış olsa da, teknoloji ile birlikte sistemlerin saldırılara ve istismara karşı kalma ihtimalleri çok daha yüksek bir orana çıkmıştır. Teknoloji hayatımızı kolaylaştırırken, siber güvenlik önlemlerine dikkat edilmez ve hayata geçirilmez ise yeni ihlallere ve saldırılara fırsat verilmiş olur.

Bu çalışmada siber suç türleri, çeşitleri, amaçları ve zararlı yazılımlar ile birlikte kullanılan araçlar ayrıntılı bir şekilde araştırılmış ve bunlara karşı alınacak önlemler tezde belirtilmiştir. Bunun yanında kamu kurumlarının olası açıkları ve alması gereken tedbirlere ve bilgi güvenliği için yapılması gerekenlere bu çalışma da yer verilmiştir. Ayrıca teknolojik olarak ne gibi tedbirlerin alınması gerektiği de açıklanmıştır. Hangi tedbir alınırsa alınsın en zayıf halka olan insanın, eğitim ile olası zararları en aza indirebileceği vurgulanmıştır.

Anahtar Kelimeler: Siber Güvenlik, Siber Saldırı Yöntemleri, Nmap tarama, Kali Linux, Fidye Yazılımı, Saldırı Tespit Sistemleri



CYBER SECURITY, NETWORKING, PHISHING, MALWARE, RANSOMWARE, SOCIAL ENGINEERING HACKING PROTECTION REVIEWS AND AN APP

ABSTRACT

Today, with the widespread use of communication technologies and the internet, the connection of various devices from tablets, computers to mobile phones with networks causes data breaches and cyber attacks. In these attack types, computer hardware, software, viruses and malicious software are encountered wherever there is internet. As the cyberspace proliferates, data breaches have started to gain importance. Although the importance given to the prevention of these violations has increased, with the technology, the probability of the systems to be exposed to attacks and abuse has increased to a much higher rate. While technology makes our lives easier, if cyber security measures are not taken into account and are not implemented, new breaches and attacks are given the opportunity. In this study, cybercrime types, types, purposes and tools used together with malicious software were investigated in detail and the precautions to be taken against them were stated in the thesis. In addition to this, the possible shortcomings of public institutions and the precautions to be taken and the things to be done for information security are also included in this study. It is also explained what kind of technological measures should be taken. It has been emphasized that no matter what precautions are taken, the weakest link, the human being, can minimize the possible harms through education.

Keywords: Cyber Security, Cyber Attack Methods, Nmap scanning, Kali Linux, Ransomware, Intrusion Detection Systems



1.GİRİŞ

Bu çalışmada son zamanlarda büyük artış gösteren veri hırsızlığı ve siber saldırılara karşı alınması gereken tedbirler ve bu tedbirlerin neler olduğu incelenmiştir. Siber güvenlik neden önemlidir? Bir fidye yazılımından nasıl korunulur? Sosyal Mühendislik saldırısı nasıl tespit edilir? gibi sorular ile başlanmıştır. Kötü amaçlı yazılımların nasıl yapıldığı ve kimlik avı saldırısına karşı nasıl davranılması gerektiği açıklanmıştır.

Siber güvenlik farkındalığı tehdit ve tedbir unsurlarının karşılaştırmalı sonuçlarıyla anlatılmıştır. Çalışma kapsamında siber uzay, siber güvenlik, siber suç gibi kavramlar, dünyada yankı bulmuş bilişim suçlarına giren olaylar ve siber tehditler incelenmiştir. Siber olayların nasıl gerçekleştirildiği uygulamalı olarak anlatılmıştır. Kamu kurumları ve özel sektörün bilişim sistemlerini nasıl koruyacakları, saldırılara karşı alacakları tedbirler ve kullanacakları “Saldırı Tespit ve Önleme” sistemleri anlatılmıştır.

Birinci bölümde, genel kavramlar ile birlikte istatistiki bilgiler verilmiştir. Çalışmanın bu bölümünde internet kullanım oranlarındaki artış ile dünya çapında yankı bulmuş veri ihlalleri ele alınmıştır.

İkinci bölümde, Siber güvenlik nedir? Siber güvenlik neden önemlidir? Siber güvenlik senaryolarının neler olduğuna değinilmiştir.

Üçüncü bölümde; siber suçların sınıflandırılması, siber suçların nedenleri, siber saldırıları kimlerin gerçekleştirdiği ve bu saldırıların türleri anlatılmıştır. Ayrıca bu bölümde siber taciz, terörizm ve vandalizm hakkında tanımlamalara yer verilmiştir.

Dördüncü bölümde, kimlik avı saldırısının tanımlanması ve bu saldırıları önleme konusu ele alınmıştır. Bu saldırıların çeşitliliği ile hangi yöntemleri kullandıkları hakkında da bilgi verilmiştir.

Beşinci bölümde; kötü amaçlı yazılım olan virüsler, solucanlar, truva atları, fidye yazılımları ve casus yazılımlardan bahsedilmiş, sistemde bu virüslerden birisi varsa bu konuda nelerin yapılması gerektiği anlatılmıştır.

Altıncı bölümde, Sosyal Mühendislik Saldırılarına dikkat çekilmiştir. Bu saldırıların yapılma şekli ve bunlara karşı alınacak tedbirler ele alınmıştır.

Yedinci bölümde; bir sistemin en mahrem alanı kabul edilen ağ güvenliği konusunda bilgiler verilmiştir. Aynı zamanda "Ağ güvenliği nedir ve nasıl çalışır, ağda gerçekleştirilebilecek saldırılar nelerdir?" sorularına değinilmiştir.

Sekizinci bölümde; resmi kurumların ve özel sektörün web sayfalarının güvenliği ele alınmıştır. Özellikle veri tabanı güvenliği ve SQL enjeksiyon konusuna dikkat çekilmiştir.

Dokuzuncu bölümde; siber saldırılarda en çok kullanılan yazılım ve bu yazılımın içindeki araçlar hakkında bilgiler verilmiştir. En çok kullanılan saldırı araçları tanıtılmıştır.

Onuncu bölümde; siber atakları gerçekleştirmek için hangi tarama aracının kullanıldığı ve bu tarama sonucu uygulanacak ataklar uygulamalı olarak gösterilmiştir. Kamu kurumlarının port zaafiyetleri araştırılmış, ilgili açıklar listelenmiştir.

On birinci bölümde; kamu kurumlarının ve özel sektörün siber saldırılara nasıl karşı koyması gerektiği anlatılmış, konu hakkında önerilerde bulunulmuştur. Siber saldırıların tespiti ve bu saldırıları önlemeye yarayan cihazlar anlatılmıştır.

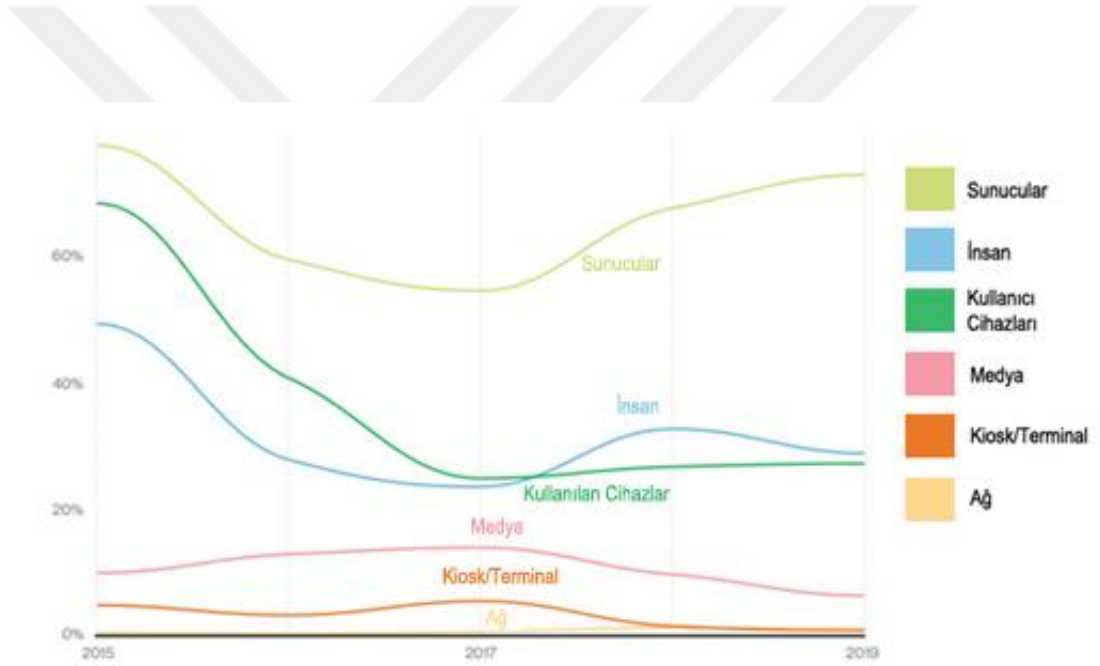
İnternet, insanların sosyalleşmeleri için "mükemmel" hale gelirken, aynı zamanda siber suçlulara da büyük fırsatlar sunmaktadır. Suçlular, her şeyin dijitalleşmesiyle bu duruma uyum sağlamışlar ve dijital ortama geçmişlerdir. İnternet tarafından sağlanan programların alışveriş, bankacılık, yemek siparişi vb. faaliyetler için kullanıldığını, tüm bu bilgilerin dijital ortamda saklandığını, herşeyin buradan yönetildiğini anlamaları çok hızlı şekilde gerçekleşmiştir. Milyarlarca dolarlık onlarca para birimi her gün internet üzerinden hareket etmekte ve bu suçlular için büyük bir cazibe ve suç işlemek için alternatif bir yol haline gelmektedir. Artık para çalmak, soygun yapmak bankaya gidilerek değil internet üzerinden kolayca yapılmaktadır.

Genel Durum

Veriyi korumak teknolojik unsurlarla mümkün olsa da harcanan paralar kimi zaman veriyi korumada etkili olamamaktadır. Günümüzde teknolojinin getirdiği savunma mekanizmaları yapay zekâ ile donatılsa da en zayıf halka olan insan faktörü alınan tüm önlemlerin önüne geçmektedir. Saldırganlar artık gelişmiş duvarları ve cihazları aşmaya uğraşmaktansa insan faktörünün daha kolay bir hedef olduğunu düşünmektedir. Şekil 1.1'de 2015-2019 yılları arasında veri ihlalleri grafiği yer

almaktadır. Grafikte insan ve kullanıcı cihazları yönünden veri ihlallerinin 2017 yılında azaldığı gözlemlenirken, 2019 yılında bu ihlallerin arttığı gözlemlenmiştir. Diğer ihlallerin hepsinde 2015 yılı verilerine göre çok az bir farkla azalma olmuştur. Bu artışta, kullanıcıların farkındalık düzeylerinin düşük olmasına sebep olan kullanıcı artışının büyük etkisi olmuştur [1].

Ülkemizde 2019 yılında kamu kurumlarında yapılan veri ihlallerine yönelik bir ankette, 980 kullanıcının %92,3'lük çok büyük bir kısmı “kişisel verilerim benim için önemlidir” demiştir, %61,4'ü kullandıkları bilgisayar veya telefonlara yönelik saldırılardan bilgileri olmadığı cevabını vermiştir. Bu sonuç bize veri ihlallerinin önlenmesinde insanların farkındalık eğitimlerinin artırılması gerektiğini göstermiştir [2].



Şekil 1.1. Veri ihlallerinin sınıflarına ayrılması.

2020 yılında IBM Güvenlik İş Birimi, veri ihlallerinin kuruluşlar üzerindeki maliyetini inceleyen yıllık araştırmasına göre Türkiye'deki her veri ihlalinin ortalama maliyeti, bir yılda yüzde 10,3 oranında artış göstermiş ve 12,3 milyon TL'ye ulaşmıştır. TÜİK'in 16-74 yaş arası fertleri kapsayan, hanelerde ve işyerlerinde bilişim teknolojileri kullanımına yönelik istatistiki çalışmaları neticesinde elde edilen bulgular Çizelge 1.1'de listelenmiştir. Bu tabloda işletmelerin hemen hemen hepsinin işlemlerini bilgisayarlar aracılığı ile sanal ortamda gerçekleştirdiği görülmüştür [3] .

Rakamlar % olarak verilmiştir		2015	2016	2017	2018	2019	2020
Kurumlarda	Bilgisayar Kullanımı	95,2	95,9	97,2	97	96,7	98,2
	İnternet Erişimi	92,5	93,7	95,9	95,3	94,9	94,9
	Web Sayfası Barındırma	65,5	66	72,9	66,1	66,6	53,7
Hanelerde	Bilgisayar Kullanımı	54,8	59,3	57	57,1	55,5	53,2
	İnternet Kullanımı	55,9	61,2	66,8	72,9	75,3	79
	İnternette Alışveriş yapma Oranları	18,4	20,9	24,9	29,3	34,1	36,5

Şekil 1.2. TÜİK Bilgi Toplumu istatistikleri.

Web sitesi sahiplik oranı %53,7 olmuştur. Hane kullanıcılarının ise 2019 yılına göre yaklaşık %5'lik bir artışla %79 gibi bir oranda internet erişiminin olduğunu, bir diğer istatistiki veride hanelerin %90,7'sinin evden internete erişim imkânına sahip olduğu gözlenmiştir. Ancak aynı oran bir önceki yılda %88,3 olarak belirlenmiştir. İşletmelerin %92,5'i 2020 yılında internete erişimde sabit geniş bant bağlantı kullanmıştır. İnternet üzerinden kişisel kullanım amacıyla mal veya hizmet siparişi veren ya da ürün satın alan 16-74 yaş grubundaki bireylerin oranı, 2019 yılı Nisan ayı ile 2020 yılı Mart ayını kapsayan on iki aylık dönemde %36,5 olmuştur. Bu oran önceki yılın aynı döneminde %34,1 olarak ölçümlenmiştir.

Bu bilgiler bize göstermektedir ki bireylerin internet bağımlılığı ve internete erişimleri her geçen gün artmaktadır. Bu artış verilerin korunmasını zorlaştırmanın yanında saldırılara açık olan verilerin de her geçen gün artmasına neden olmaktadır. WatchGuard'ın 2020 yılı için hazırladığı rapora göre Türkiye'de bir yılda 1,692,320 adet kötü amaçlı yazılım saldırısı düzenlenmiştir. Geçen yıla göre %81 oranında artışın gerçekleştiği Türkiye'de, dakikada 3 adet kötü amaçlı yazılım saldırısı yaşanmıştır. Gerçekleşen saldırıların birçoğunu "Truva Atı" ve "Exploit" türünde saldırıların oluşturduğu belirtilmiştir. COVID-19 beraberinde dijital ortamda faaliyet gösteren ve verilerini ağlara taşıyan şirketler, değerli verileri çalmak isteyen siber suçlular tarafından her geçen gün daha çok tehdiye maruz bırakılmıştır. 2019 yılında 38.858

adet ağ saldırısı gerçekleşirken 2020 yılında ise 200.647 adet saldırının meydana geldiği raporlanmıştır. WatchGuard Tehdit Laboratuvarı tarafından elde edilen verilere göre, 2021'in ilk 6 ayında Türkiye'de 288 bin 445 adet siber saldırı gerçekleşmiştir [4].

Tüm dünyada artan teknolojik ürünlerinin kullanımları ile internete bağlanma oranları, siber zaafiyetlerin ve saldırıların artmasına neden olmaktadır. Bireysel kullanıcıların ve kurumsal kullanıcıların 2015-2020 yılında maruz kaldığı siber saldırılara yönelik hazırlanan istatistikler incelenmiş, incelenen bu sonuçların ışığında aşağıdaki olayların gerçekleştiği ve yine burada da insan faktörünün ne kadar önemli olduğu görülmüştür.

1. Yahoo, 3 milyar güvenliği ihlal edilmiş hesaplara (Statista) tüm zamanların en büyük veri ihlali rekorunu kırmıştır [5].
2. 2019 yılında First American Financial Corp. Bankacılık işlemleri, sosyal güvenlik numaraları ve daha fazlası dâhil olmak üzere çevrimiçi olarak 885 milyon kişi ile rekor kıran bir başka şirket olmuştur [6].
3. 2019' yılında Facebook, 2012 yılından beri 600 milyon kullanıcının, kullanıcı şifrelerini güvence altına almadığını itiraf etmiştir [7].
4. 2019' yılında Georgia Tech'in mevcut ve eski öğrenci, personel ve öğrenci adaylarının kişisel bilgilerine bir hacker tarafından merkezi bir veri tabanı üzerinden erişildi. 1.3 milyon kişi bu siber saldırıdan etkilendi. Saldırıya uğrayan veri tabanı; isimleri, adresleri, sosyal güvenlik numaralarını ve doğum tarihlerini içeriyordu [8].
5. 2020' Wawa adlı Amerikan hipermarket zincirinin, alışveriş siteleri üzerindeki açık nedeni ile 30 milyon Amerikalının ve 1 milyon yabancı müşterinin kart bilgileri DarkWeb üzerinden satışa sunuldu [9].
6. 2020 yılında ünlü MGM Resorts 142 milyon adet misafir kayıtları ve kişisel verileri DarkWeb'te ortalama 2.500 dolar üzerinden satışa sunuldu [10].
7. 2020 yılında Nintendo oyun sektöründe hem de e-posta servislerinde kişisel verilerin yayılmasına neden oldu. Nisan ayında, oyun devi 160 bin kullanıcısının hesaplarının saldırı altında olduğunu duyurdu [11].
8. 2021 yılında 533 milyon Facebook kullanıcısının kişisel bilgileri ve telefon numaraları düşük seviye hackerların yer aldığı bir forumda yayınlandı. Bu tarz veriler

genellikle dark web'de ücret karşılığında satılıyor. Ancak forumda verilerin ücretsiz olarak yayınlanması dikkat çekti [12].

9. 2021 yılında LinkedIn adlı çevrim içi kariyer platformu büyük boyutta bir veri ihlali yaşandığını duyurdu. Saldırganlar, platformu kullanan 700 milyondan fazla kullanıcının verisini açığa çıkardı. Platformun toplam kullanıcı sayısı 756 milyon civarındadır [13].

Bu kadar büyük çaptaki veri ihlalleri ve siber saldırılar, küresel anlamda alınması gereken tedbirlerin ve bu tedbirler kapsamında büyük yatırımların yapılması gerektiğini gözler önüne sermektedir. Ancak ne kadar yatırım yapılırsa yapılsın insan faktörünün ve insanların farkındalıklarının artırılmasının ne kadar önemli olduğu görülmektedir.

Tüm bu durumlar değerlendirildiğinde kullanıcı sayıları, saldırı yöntemleri ve saldırı türleri, veri sızıntıları neticesinde ortaya çıkan zararlar gözlemlendiğinde önemli seviyelerde maliyet artışı görülmektedir. Korsanlar güvenlik duvarları ya da sistemleri aşmak yerine maliyet gerektirmeyen insan faktörü üzerinden hedeflerine kolayca ulaşmaktadır. Buradan da anlaşılıyor ki teknolojiye ne kadar yatırım yapılırsa yapılsın insan faktörü tüm güvenlik cihazlarının önündedir. Bu durumu aşmak için bireysel ve kurumsal kullanıcıların farkındalıklarını artırmak amacıyla eğitimleri her geçen gün artırmak gerektiği değerlendirilmektedir.

Literatür Taraması

Son yıllarda Veri Güvenliği ve Siber Güvenlik alanında birçok çalışma ve akademik araştırma yapılmıştır. Teknoloji ilerledikçe siber zaafiyet şekilleri ve türleri de değişmiştir. Yapılan araştırmalar meydana gelecek veri kayıpları konusunda alınacak tedbirler ile bu tedbirlerin güncellenmesine yardımcı olmuştur. Yapılan bu çalışmalar şu şekilde özetlenmiştir;

Kamu kurumlarının veri güvenliğinin sağlanması için bilişim sistemlerinin güncel tutulması, mevcut veri açıklarının tespit edilip belirli zamanlarda bu işlemin tekrar edilmesinin gerekliliği vurgulanmıştır. Ayrıca veri güvenliğini sağlamak amacıyla gerekli eğitimlerin alınması için teknik personelin eğitimi ve fiziksel güvenlik önlemleri de dikkate alınmalıdır [14].

Veri fidyeciliği'ne (Ransomware) ve çeşitliliğine dikkat çekmiştir. Bilgisayar kullanıcılarının son zamanlarda verilerinin şifrelendiğini belirterek bu şifreler karşılığında para istendiğini ve bu hususta alınması gereken tedbirler hakkında öneriler sunulmuştur [15].

Veri güvenliği ihlallerinden biri olan sosyal mühendislik üzerine incelemeler yapılmıştır. Sosyal mühendisliğin ne olduğu, kapsadığı saldırı çeşitlerinin neler olduğu, sosyal mühendislik saldırılarına karşı alınacak önlemlerin neler olduğu ve bu konuda nelere dikkat edilmesi gerektiği anlatılmıştır [16].

Kimlik avı (phishing) saldırılarının önlenmesi için üç sütunlu bir stratejiyi savunmaktadır. 1. Tek seferlik parolalar, 2. Çok düzeyli masaüstü engelleri, 3. Davranış değişikliği. Bu yaklaşımları kullanarak bireyler ve kurumlar veri güvenliklerini koruyabilmeli, neden olabilecek zararları en aza indirebilmelidir [17].

Günümüz modern dünyasında basit kötü amaçlı bir yazılım saldırısı felaketle sonuçlanabilir. Piyasada bulunan birçok virüs programı, kötü amaçlı yazılımları tespit edemediği için sorunlar yaşanabilir. Bu saldırılardan nasıl korunacağı hakkında basit yöntemlerle ilgili bilgiler verilmiştir [18].

Bilgi güvenliğinin önemi. Kişi, kurum ve kuruluşların bilgiyi saklayarak ve mahremiyetini koruyarak bu bilgileri yetkili kişilere ulaştırması oldukça önemlidir. Bu çalışmada bilgi güvenliği sistemlerinin vazgeçilmez unsuru olan STS (Saldırı Tespit Sistemleri) araçları ayrıntılı şekilde incelenmiştir [19].

Güvenlik eksikliklerini bulma ve hedef işletim sisteminin açıklarını keşfetmek amacıyla Nmap tarama aracı hakkında bilgi verilmiştir. Ayrıca hedef portlar ve diğer faydalı hizmetler hakkında bilgiler sağlanmıştır. Nmap herhangi bir sızma testinin ilk aşaması olan keşif veya bilgi toplama aşamasında kullanılır. Bu aşamalar ve ayrıntılı tarama hakkında bilgiler aktarılmıştır [20].

Yukarıdaki çalışmalarda kişi, kurum ve kuruluşların bilgi ve bilişim sistemlerinin güvenliğini sağlaması için birçok yöntem mevcuttur. Bu çalışmanın amacı ise siber saldırıların nasıl yapıldığı, kimler tarafından yapıldığı, hangi araçların kullanıldığı konusunda güncel bilgiler sunarak farkındalık yaratmak ve uygulama ile bunu ortaya koymaktır. Veri ihlallerinin önüne geçmek siber saldırı yöntemlerini bilmek davranış ve hareketlerini incelemekten geçmektedir. Bu ihlaller konusunda teknik olarak ne kadar tedbir alınırsa alınsın en zayıf halka olan insan, eğitimlerle elde edeceği

farkındalıklarla bu ihlallerin önüne geçecektir. Bir sahte site uygulaması yapılarak en zayıf halkanın insan olduğu gösterilmiştir. Bu çalışmada ayrıca diğer çalışmalardan farklı olarak kamu kurumlarının port açıklıkları Nmap aracı ile taranmış, olası açıklıklardan yararlanılmaya çalışılmıştır. Bu doğrultuda port açıklıkları ilgili bölümde listelenmiştir. Yine aynı kurumların SQL açıklıkları taranmış elde edilen bulgular açıklanmaya çalışılmıştır. Sanal bir ortamda saldırı gerçekleştirilmiş bunun nasıl gerçekleştirildiği ayrıntılı olarak anlatılmıştır. Tüm bu yapılanlar, tezin içerisinde bir bütün olarak yer almaktadır. Bu araştırmalar ve anlatılanlar ışığında elde edilen bulgular göstermektedir ki en büyük zafiyet insan faktörüdür. İnsan faktörünün de bütün bu bilgilere sahip olması, geçmişte karşılaşılan tecrübelerden haberdar olmasının çok önemli bir durum olduğu değerlendirilmektedir.



2.SİBER GÜVENLİK VE NEDEN ÖNEMLİDİR

2.1 Siber Güvenlik Nedir?

Bilgi güvenliği olarak da bilinen siber güvenlik, Bilgisayar sistemlerini, ağları, programları ve verileri siber saldırılara veya dijital saldırılara karşı koruma uygulaması anlamına gelir. Bu nedenle, siber güvenlik, bilgisayarları, bilgi teknolojisini, sanal gerçekliği vb. koruyan her şeyi ifade eder. “Etkili siber güvenlik, siber saldırı riskini azaltır ve sistemlerin, ağların ve teknolojilerin yetkisiz kullanımına karşı korur.” Siber güvenlik, **Bilgi Güvenliği** teriminin bir parçasıdır. Bilgi güvenliği, tüm dijital ve basılı kopya bilgi varlıklarını korumayı amaçlamaktadır [21].

Siber güvenlik sürecinin parçaları vardır ve şu şekildedir.

İnsanlar; İnsanlar bir sistemin parçasıdır. 2019 yılında yapılan bir araştırma da, İnsan Faktörü raporuna göre saldırganlar, zararlı yazılım yüklemek, gizli bilgileri çalmak veya dolandırmak amacı ile çoğunlukla çalışan sistemler yerine insanları hedef almaktadır. Yapılan ihlallerin %99’unda insan faktörüne yoğunlaşan saldırganlar e-posta, sosyal medya ve bulut uygulamaları hedeflerine saldırmak için sosyal mühendisliği kullanmaktadır. E-postaların sahtelerini göndermek, kimlik bilgilerini ele geçirmek veya kötü amaçlı ekleri bulut uygulamalarına yüklemek, başarısız olma ihtimali yüksek maliyetli, zaman alıcı saldırıdan daha kolay ve çok daha avantajlıdır. Saldırıların önemli bir oranın olmasına e-postasındaki bir linke tıklama veya kötü amaçlı bir dosyayı açma gibi insan etkileşimine bağlı olduğuna dikkat çekilmektedir. Güvenlik uzmanları, saldırılarda sosyal mühendisliğin önemli rol oynadığını ve güvenlik teknolojileri ne kadar gelişirse gelişsin bu saldırıların devam edeceğini belirtmişlerdir. 2018’de gerçekleşen her dört kimlik avı e-postasından birinin Microsoft ürünleriyle ilişkili olması da araştırmada öne çıkanönemli detaylardan biridir [22].

Süreçler; Kuruluşların, hem denenmiş hem de başarılı olan siber saldırıların üstesinden gelmek için belirli birimlere sahip olması gerekmektedir. En üst seviyede bilgi güvenliği stratejisi ve politikaları, bu politikaları destekleyici süreç, prosedür ve talimatların organizasyon yapısına uygun olarak oluşturulması ve hayata geçirilmesi önem arz etmektedir. Tüm politika, süreç, prosedür ve talimatları burada yazmak mümkün değildir, ancak siber güvenliğin sağlanması açısından bu tip bir yaklaşımın sürece özel oluşturulması gerekmektedir. Burada süreç ile kastedilen kısım, bir

durumun kim tarafından, nasıl ele alınması gerektiğinin incelenmesidir. Ayrıca süreçler göz önüne alındığında, bu süreçlerin de bir olgunluk modeli üzerinden oluşturulması ve devamlı olarak iyileştirilmesi gerekmektedir. Kurumsal bir operasyonu verimli bir şekilde yönetebilmek için tanımlı süreçlere ihtiyaç vardır. Bu süreçler organize, etkili ve tutarlı bir şekilde yürütülmesi gereken ve kişilerin hangi işleri nasıl yapacağına dair yol gösterir. Siber güvenlik alanında kuruluşların faaliyetlerini yürütebilmesi için gerekli olan süreçlerden bazıları aşağıda listelenmiştir [23].

- Sürekli Güvenlik İzleme
- Siber Olay Yönetimi ve Müdahale
- Kimlik ve Erişim Yönetimi
- Log Yönetimi
- Çağrı Yönetimi
- Değişiklik Yönetimi
- Siber Tehdit ve İstihbarat Yönetimi
- Zafiyet Yönetimi
- Risk Yönetimi

Teknoloji; Teknoloji olmasaydı, kuruluşlar sistemlerinin güvenliği için kendilerini siber saldırılara karşı korumak adına gerekli araçlara sahip olamazlardı. Siber güvenliğin sağlanması için bir takım teknolojileri temin etmek gerekli hale gelmiştir. Bu teknolojileri yönetecek olan siber güvenlik uzmanlarını yetiştirmek gerekir. Süreçlerin oluşturulmasından sonra teknolojik gelişmelerin hayata geçirilmesi gerekmektedir. Bu kapsamda korunacak varlıkları 3 başlık altında toplayabiliriz.: yönlendiriciler, akıllı cihazlar ve bilgisayarlar gibi kişisel uç nokta cihazları, ağ ve bulut. Bu varlıkları korumak için kullanılan yaygın teknolojiler arasında güvenlik duvarları, DNS filtreleri, kötü amaçlı yazılımdan koruma çözümleri, antivirüs çözümleri ve e-posta güvenlik çözümleri bulunmaktadır [24].

2.2 Siber Güvenlik Neden Önemlidir?

Dünya; teknolojiye, geçmiş yıllarda olduğundan daha fazla bağımlı hale gelmiştir. Bu, dijital verilerin oluşturulmasında büyük bir artışa neden olmuştur. Veriler, bireyler, işletmeler, devlet kurumları vb. tarafından bilgisayarlarda depolanır ve günlük olarak bir ağ üzerinden diğer bilgisayarlara aktarılmaktadır. Bilgisayarlar ve bağlı sistemlerinde güvenlik açıkları bulunabilmektedir. Bunlar bir saldırgan tarafından istismar edilebilir ve bu da bir yapının çökmesine yol açabilir. Bu nedenle siber güvenlik hayati önem taşımaktadır.

2010 yılının Haziran ayında ortaya çıkan bilgisayar solucanının hem yayılma biçimi hem de siyasi olarak kullanım şekli dikkat çekmiştir. Microsoft'un Windows tabanlı işletim sistemi aracılığıyla dağılan bu solucan, Siemens'in S7 300 modüllerini hedef almıştır. –*Simatic WinCC SCADA* kodlu bu yazılımdaki SCADA'nın açılımı '*Supervisory Control and Data Acquisition Systems*' şeklindedir. Tanım olarak, veri sağlama ve denetim sistemidir. Bu sistemler, çeşitli sanayi işlemlerini otomatik olarak çalıştıran programlanabilir lojistik kontrol unsurlarını (PLC) denetlemektedir. Nükleer reaktörlerdeki basıncı kontrol edip artırabilen, petrol boru hatlarının kontrol edilmesi ile aynı zamanda kapatabilen bu zararlı yazılım, sistem operatörlerine de her şeyin normal seviyede olduğu bilgisini vererek sıkıntıların son ana kadar anlaşılmamasına sebep olmuştur. Stuxnet, standart virüslerin aksine, sisteme girişi gerçekleştirmek için sahte güvenlik sertifikası kullanmıştır. Dünyanın en büyük teknoloji şirketleri, Realtek'in güvenlik sertifikasını kullanmaktadır. Bu olay, sistemlere sızarak bir süre habersizce beklemesini ve sonra çalışmasını açıklamaktadır. Stuxnet'in işleyişini değerlendiren uzmanlar, bulaştığı sistemin yöneticileri tarafından haberdar olmadığı açıkları kullandığını görmüşlerdir. Bu açıklara "*Zero Day*" adı verilmekle birlikte, bir sistemdeki "*Zero Day*" açığı, 200.000'den fazla bilgisayara bulaşmış ve 1.000 makinenin fiziksel olarak bozulmasına neden olmuştur. Stuxnet, çok sayıda "*Zero Day*" açığı kullandığı için dikkat çekmiştir.

İhlalden etkilenen ülkeler arasında İran (% 58,85) ve Endonezya (%18,22)'nin ilk sıralarda yer alması nedeni ile virüsün doğrudan bu ülkeleri hedef aldığı görülmüştür. Özellikle de nükleer santrallerinin zarar gördüğü İran'ı hedef aldığı iddia edilmiştir. Saldırılan ülkenin İran olması ve virüsün etkili olduğu zamanlarda İran'ın açıklama yapmadan nükleer faaliyetlerine ara vermesi nedeniyle Stuxnet'i kimin yazdığının

tahmin edilmesi zor değildir. Fakat bunu kesin kanıtlarla ortaya koymak mümkün değildir [25].

Sistemdeki bir saldırganın ve erişimine izin verilen bir ihlalin çok kapsamlı sonuçları olabilmektedir. Müşteri verilerinin sızması, kuruluşun itibarını etkilemekte ve iş ortakları ile müşteriler arasında güven kaybına yol açmaktadır. Yazılım kaynak kodunun çalınması, rakiplerine göre rekabet avantajına mal olabilmektedir.

Orta düzeyde veri ihlali bir kuruluşa milyon dolarlara mal olabilir. Dahası, yüksek düzeyde veri ihlalleri, orman yangını gibi aslı olmayan haber başlıklarını değiştirerek, bir şirketin itibarını zedeler. Bu nedenle kuruluşların siber güvenliğe güçlü ve hassas bir yaklaşım göstermesi gerekmektedir.

2.3 Siber Güvenlik Senaryoları

Dünyada siber güvenliğin kullanıldığı birkaç yaygın senaryo bulunmaktadır. Bu senaryoların etkileri her geçen gün artmaktadır. İşletmelerin sorunsuz çalışması için tüm dijital ihtiyaçlarını karşılayacak en son teknolojiye ve güvenlik ekipmanlarına sahip olunması gerekmektedir. Bu ekipmanlar ile altyapısının günün her saati çalışır durumda olması önemlidir. Kuruluşun, genel erişim ağı ve kişisel verilerin dışında diğer verilerin, ağı, ekipmanların ve ürünlerin güvence altına alınmasını sağlaması gerekmektedir. Halka açık verilerin kendisi de şifrelenmeli ve veriler güvence altına alınmalıdır. Birçok kuruluş dijital ortama geçti. Bu nedenle bir kuruluşun amaçlarını ve hedeflerini gerçekleştirmek için birlikte çalışan birçok sistem vardır. (Sunucular, güvenlik duvarları, switchler vb.) Dijitalleşme aynı zamanda bir kuruluşun sınırlarını genişleterek bağlantılarını ve çevresini artırmaktadır. Bu durum elbette bugün avantajdır, ancak ilerleyen zamanlarda kuruluşa zarar verecektir.

Üç bakış açısı dijitalleşmeyi ve bağlanabilirliği tanımlar:

- **Kimlik** : Kullanıcıların etkileşimde bulunabileceği bir özelliktir.
- **Veri** : Kullanıcı, işletme, sistem veya müşteri ile ilgili verilerdir.
- **Ağ** : Herkesin bağlı olduğu ve erişim seviyeleriyle kısıtlandığı bölümdür.

Bu üç tanım, donanım, yazılım ve iş süreçleri aracılığıyla birbirine bağlıdır. Daha önce de belirtildiği gibi, bir yapı bu seviyeyi kontrol eden bir kullanıcının kimlik için geliştirilen erişim yoluyla verileri oluşturması, görüntülemesi veya değiştirmesi gerekmektedir. Hem statik hem dinamik verilerin güvenliğinin de sağlanması

gerekmektedir. Son olarak, ister fiziksel ister bulut ortamında, bu altyapının ağ çevresinin güvenliğinin de sağlanması gerekmektedir.

2.4 Her Şeyin Buluta Taşındığı Bulut nedir?

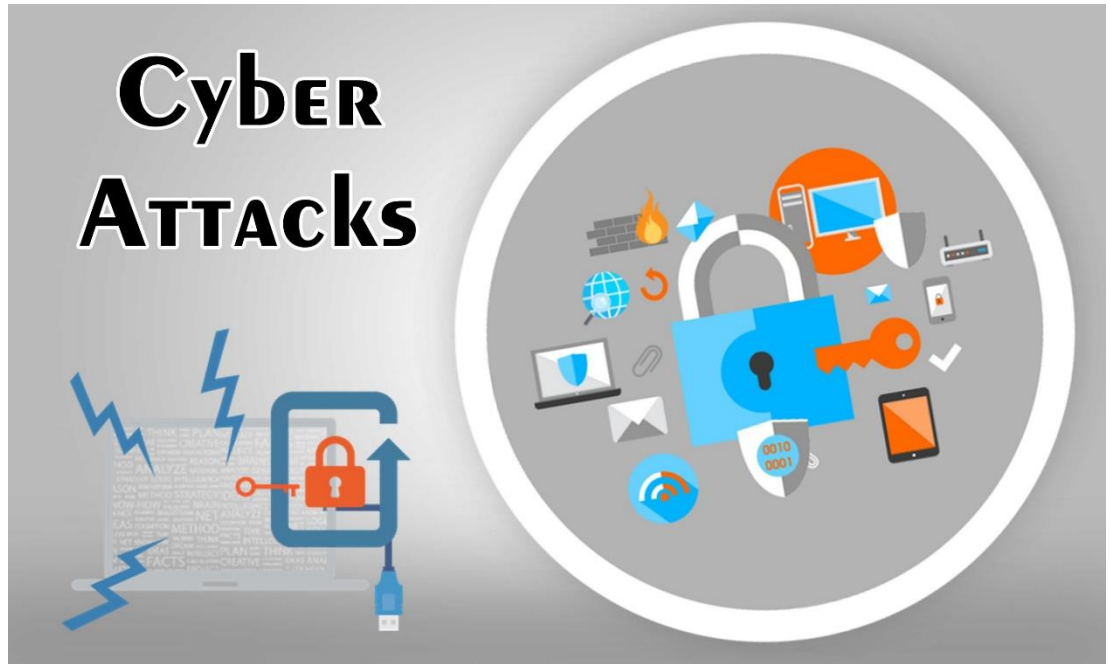
“Bulut Bilişim” (Cloud), kişisel verilerinizi uzak bir sunucuda barındırıp, depolayabileceğiniz bir alandır. Yüksek donanımlı özellik gerektiren ancak sahip olmadığımız uygulamaları çalıştırabileceğimiz, web tabanlı uygulamalara erişebileceğimiz, yüksek donanımlı bilgisayarların olduğu, herhangi bir yerden herhangi bir zamanda erişerek hizmet almamıza imkân veren teknolojidir. Bulut bilişim ülkemizde yeni gelişmektedir. Bu kategoride faaliyet gösteren birçok şirket bulunmaktadır ve bu şirketlerin sayısı her geçen gün artmaktadır. Bulut bilişim servislerine ve uygulamalarına örnek olarak Apple iCloud, Ubuntu One, Google Mail, Google Docs, Picasa, Microsoft SkyDive, Flickr, TTNET NETDISK vb. olarak verilmektedir. Bulut teknolojisi standart olmayan bir yapıyla, kullanıcıların istek ve ihtiyaçlarını göz önünde bulundurarak kullanılan, çeşitli servisleri sunan bir yapı olarak bilinir [26].

Bulut altyapısı kesinlikle daha fazla hız, kontrol, doğruluk, güç ve kullanılabilirlik ile yeni bir çağ açmıştır. Ancak bu konuda birçok güvenlik riski de bulunmaktadır. Bulut yapısı güvenlik açısından farklı bir yapıya sahip değildir. Bir altyapı gerekli şekilde güvenli değilse sorunlar olabilmektedir. Bulut altyapısının en büyük avantajı, hizmet alanının gerekli altyapıya sahip olmasının gerekmemesidir. “Bulutta bulunan verilere kimler erişebilir? Bulut, PCI veya GDPR gibi hükümet düzenlemeleriyle nasıl uyumlu tutulabilir?” soruları ilk olarak akla gelmektedir. Hizmet sağlayıcının iş modeli aynı zamanda bulut altyapısıyla ilgili felaket kurtarma politikasını da yönetmektedir. Bu nedenle bir kuruluşun bu konuda güncel olması gerekmektedir. Kuruluş, bu servis sağlayıcının veri merkezinin nerede olacağı konusunda herhangi bir söz hakkına sahip olmamaktadır.

3.SİBER SALDIRILAR VE HACKERLER

Bugün kullandığımız İnternet 1960'larda ortaya çıkmıştır. O zamanlar sadece birkaç bilim adamı, araştırmacı ve savunma departmanı tarafından erişilebiliyordu. İnternet veri yapısı o zamandan beri katlanarak gelişim gösterdi. İlk zamanlarda bir **siber suç**, bir bilgisayara ve altyapısına fiziksel hasar verilmesi olarak tanımlanmaktaydı. Bu tanım, 1980'lerde bilgisayarın arızalanmasına neden olacak eylemler şeklinde değiştirildi.

İnternet ilk başta genellikle savunma sanayi, büyük kuruluşlar ve araştırma topluluklarıyla sınırlıydı. Dolayısı ile siber suçun etkisi o zamanlar düşüktü. İnternet 1996 yılında halka açık olarak kullanılmaya başlanmıştır. İnsanların hayatlarını değiştirecek kadar popüler hale gelmiştir. İnternet için grafik kullanıcı arayüzü basit bir şekilde tasarlanarak, kullanıcıların işlevlerini ve özelliklerini anlaması kolaylaştırılmıştır. Kullanıcılar, tarayıcılarındaki köprülere tıklayarak veya tarayıcıya URL'leri yazarak veriye ulaşmaktaydı. Verilere başka birinin erişimi olup olmadığını veya ulaştıkları verilerin bir saldırgan tarafından izinsiz şekilde tahrif edilip edilmediğini bilmiyorlardı. Siber suçların odağı olan internet geliştikçe bir bilgisayara fiziksel olarak zarar vermek yerine, verilere müdahale ederek mali suçlar işlenmeye yönelinmiştir.



Şekil 3.1 : Cyber Attack

İnternet 2013 yılına kadar zirveye ulaştı ve siber suçların oranı hızla arttı. Her saniye yirmi beş bilgisayar saldırıya uğramış aynı zamanda 900 milyon kullanıcı da siber suçların kurbanı olmuştur. Dünya genelinde herkesin artık akıllı telefona sahip olmasıyla, kurbanların sayısı büyük ölçüde artmıştır. Bu telefonlara güvenlik önlemleri alınmaması ve kullanıcı hataları milyar dolarlara varan saldırılara ve zararlara yol açmıştır [27].

3.1 Siber Suçların Sınıflandırılması

Kuruluşlar, çalışanları ve müşterileri hakkında önemli veriler içeren büyük ölçekli veri tabanı veya sunucu bulundurlar. Siber suçlular için veri tabanları önemli veriler olduğu için bu kuruluşlara saldırmaktadırlar. Bir siber suçlu, kuruluşun çalışanı veya dışından olabilir. Bu duruma göre siber suçları iki türe ayırabiliriz:

3.1.2 İçeriden Bilgilendirme Saldırısı

Bir sisteme veya bilgisayar altyapısına erişimi olan birinin saldırısı, içeriden yapılan bir saldırdır. Bu saldırganlar, hırs ve intikam gibi çeşitli nedenlerle saldırıyı gerçekleştirmektedir. İçeriden biri, güvenlik sisteminin altyapısının, politikalarının ve zayıflıklarının farkında olduğu için sisteme kolayca saldırabilmektedir. Bu kişinin ayrıca kuruluşun ağına erişim yetkisi vardır. Bu nedenle, içeriden birinin bilgi çalması veya altyapıya zarar vermesi oldukça kolaydır. İçeriden biri, özellikle sisteme yeni roller atandığında, genellikle saldırı için bir fırsat penceresi bulmaktadır. Örneğin, bir şirket yeni bir uygulama geliştirdiğinde, uygulamadaki verileri korumak için gerekli kontrollere ve politikalara sahip değildir. İçeriden bir kişi bu güvenlik açığını, hedefini gerçekleştirmek için kullanır. Kurum içi güvenlik sistemleri dâhili olarak kullanılarak saldırıyı tespit etmekte ve önlemektedir [28].

3.1.3 Harici Saldırı

Kuruluşun içinden veya dışından kuruluşun ağına ve sistemlerine saldırmak için bir bilgisayar korsanı tutulduğunda harici saldırılar ortaya çıkmaktadır. Bir sistemde mali ve itibar kayıplarına neden olmak için harici saldırılar yapılmaktadır. Dışarıdan yapılan saldırı, içeriden yapılan saldırıya kıyasla daha fazla planlamaya ve araştırmaya ihtiyaç duymaktadır. Her harici saldırı aşağıdaki aşamalardan geçmektedir:

- Planlama
- Keşif

- Tarama
- Erişim Elde Etme
- Erişimi Sürdürme

Kuruluşun ağ yöneticisi, güvenlik duvarı günlüklerini sürekli kontrol etmelidir. Güvenlik açıklarını belirlemek için sistemleri ve ağı sürekli olarak taraması gerekmektedir. İçeriden saldırıların ve harici saldırıların yanında, iki tür siber saldırı daha vardır: Yapılandırılmış veya yapılandırılmamış saldırılar. Bu sınıflandırma, saldırganın deneyimine ve bilgisine dayanmaktadır. İnsanlar bu saldırıları dış saldırılar olarak sınıflandırmaktadır. Bir çalışan, kişisel kazanç sağlamak için kuruma yapılandırılmış saldırılar gerçekleştirir. Bu tür saldırılar genellikle rakip şirketler tarafından yapılmaktadır. Bunu, çalışanlarından birini rakip şirkete gönderip o şirketten bilgi toplamasını isteyerek gerçekleştirirler. Bu kurumsal casusluk olarak bilinmektedir [29].

3.2 Yapılandırılmamış Saldırıları

Önceden tanımlanmış bir nedeni olmaksızın amatör bir saldırgan tarafından gerçekleştirilen bir saldırı, *yapılandırılmamış saldırı* olarak sınıflandırılmaktadır. Bu saldırılar internette kolayca bulunabilen bir sızma aracı kullanılarak gerçekleştirilmektedir. Salırgan bu aracı şirketin ağında kullanarak gerekli sızma işlemlerini gerçekleştirir.

3.3 Yapılandırılmış Saldırıları

Yapılandırılmış saldırı, hedefleri net olan deneyimli ve profesyonel biri tarafından dikkatlice planlanır ve yürütülür. Salırganlar, saldırı tespit sistemi tarafından tespit edilmeden, hedef sisteme veya ağı erişmelerine yardımcı olan araçlara ve teknolojilere erişebilmektedir. Bir salırgan, mevcut bir aracı belirli saldırı şekline uyacak şekilde değiştirmek için gerekli bilgiye sahiptir.

3.4 Siber Suçların Nedenleri

Bir salırgan, çeşitli nedenlerle bir kuruluşun sistemine veya ağına erişmektedir. Siber suçların meydana gelmesinin yaygın nedenlerinden bazıları şunlardır:

3.4.1 Para

Saldırganlar, para kazanmanın daha kolay ve hızlı bir yolu olduğunu düşündüğü için siber suçlar işlemektedirler. Birinin hesap bilgilerini ifşa etmek ve kandırmak için kimlik avı sahtekârlığı yöntemini kullanmaktadırlar. Saldırgan, bu bilgileri, kurbanın hesabından kendi hesabına para aktarmak için kullanmaktadır.

3.4.2 İntikam

Bazı saldırganlar kişi, kuruluş, din veya hükümete karşı intikam almak için saldırı düzenlemektedirler. Mali ve fiziksel kayıplara neden olmak için bu saldırıyı gerçekleştirmek öncelikli amaçlarıdır. Bu saldırı biçimi ‘‘Siber Terörizm’’ olarak adlandırılmaktadır.

3.4.3 Tanınma

Bazı saldırganlar popülerlik kazanmak, toplumda ün kazanmak için saldırılar gerçekleştirmektedir. Büyük kuruluşların sistemlerine ve ağlarına, kendilerine bir isim vermek için (anonimlik) saldırırlar. Siber suçlular, bilgisayarı ya da sistemi ele geçirdiklerinde (hack yaptıklarında) anonim kalmak isterler. Bu kişiler kendilerine takma isimler vererek ‘‘t4cs1zkr4l’’ gibi bazı sitelerde kendilerine yer bulmaya veya başarı sırası kazanmaya çalışırlar. Bu anonimlik, saldırganları kişisel kazanç sağlamak için siber suç işlemeye teşvik etmektedir.

3.4.4 Siber casusluk

Bazı devletler, veri gizliliği yasasını görmezden gelmeyi ve vatandaşlarının yaptığı her şeyi izlemeyi seçebilirler. Bunu, siyasi veya ekonomik nedenlerin yanında istihdam sağlamak, kendi nam ve hesaplarına çalıştırmak için kullanırlar.

3.5 Siber Hacker Türleri

Bilgisayar korsanları yapıları gereği ağların ve bilgisayar sistemlerinin nasıl çalıştığını merak etmektedirler. Programlama ve kodlama konusunda yeteneklidirler. Becerilerini geliştirmek için ellerinden gelenin en iyisini yapmaktadırlar. Ayrıca bilgisayarı ve sistemleri ele geçirmek için kullanabilecekleri çeşitli araçlar ve teknolojiler hakkında bilgi sahibidirler. Bilgisayar korsanları genellikle işletim sistemlerine saldırdıkları için, farklı sistem türleri hakkında fazla bilgi edinmektedirler. Herhangi bir güvenlik açığını belirlemek için sistemde kendi yollarını bulmaktadırlar. Günümüzde ‘‘Hacker’’ denildiğinde herkesin aklına genellikle yıkıcı,

kötü amaçlı bilgisayar saldırganları gelmektedir. Bu her zaman böyle değildir. Bilgisayar ve internet ile azıcık haşır neşir olan çoğu insanın kafasında oluşturduğu bu kavram doğru değildir. Hacker'ın kelime anlamı: "Bilgisayar korsanı" demektir. Bu korsanların da kendi içlerinde zararlı olanı ve zararsız olanları bulunmaktadır [30].

3.5.1 Beyaz Şapkalı Hackerler

Beyaz Şapkalı Hackerler, bilişim suçları işleyen kötü niyetli kişilerin kullanmış oldukları teknik ve yöntemleri iyi bir şekilde bilmektedirler. Siber korsanların eylemleri sırasında kullandıkları araçları ve yazılımları tanıyan, aynı bilgi ve beceriye sahiptirler. İyi niyetli siber güvenlik uzmanlarıdır. Bu kişilere "Etik Hacker" veya "Güvenlik Uzmanı" da denilmektedir. "CEH" ya da tam ismiyle "Certified Ethical Hacker" adı ile dünya çapında tanınmaktadırlar. Hacking becerilerini, savunma amaçlı kullanırlar. Danışmanlığını yaptığı kurum ve kuruluşların saldırıya uğramasını engellemeye çalışırlar. Bu saldırıları en az zararla atlatmalarını sağlarlar [31].

3.5.2 Siyah Şapkalı Hackerler

Bilgisayar korsanları olarak da bilinen siyah şapkalı korsanlar, sisteminize ve ağınıza erişmek, verilerinizi çalmak, değiştirmek veya yok etmek isteyen kötü niyetli saldırganlardır. Saldırıları için ortak hackleme uygulamaları kullanırlar. Kanunlara aykırı davranırlar ve suça eğilimlidirler. Hedeflerine göre beyaz şapka ile siyah şapka korsanını birbirinden ayırmak oldukça kolaydır [32].

3.5.3 Gri Şapkalı Hackerler

Kullandığı illegal yöntemlerle sistemin açıklarını bulan ancak bulduğu açıkları zararsız ve masum kullanıcılara zarar vermek için kullanmayan hacker sınıfıdır. Gri şapkalı hackerler buldukları açıklarla kullanıcılara zarar vermezler. Bunun yerine kendini o açığı kapatmaya ve kullanıcılar için tehdit olmaktan çıkarmaya çalışırlar. "Gri Şapka" veya "Gray Hat" kavramı ilk defa 1998 yılında ortaya çıkmıştır. Bir grup hacker bir sistemin açığını fark etmişlerdir. Ancak açığı kullanmak yerine şirkete bildirmeyi tercih etmişlerdir. Daha sonradan bir felsefe haline gelen gri şapkalı eylemler günümüzde dahi hala devam etmektedir [33].

3.5.4 Lamerler

Lamerler, deneyim ve bilgiden yoksun oldukları için bilgisayar korsanlığı dünyasındaki en tehlikeli kişiler olarak bilinmektedirler. İnternette bulunan herhangi

bir kötü amaçlı aracın veya yazılımın ne için kullanıldığını bilmeden kullanılmaktadırlar. Ağa veya sisteme verebilecekleri zarar hakkında hiçbir fikirleri yoktur. Bilgisayar korsanlığı dünyasındaki varlıklarını sürdürmek isteyen bilgisayarlara ve ağlara saldırırlar.

3.5.5 Yeşil Şapkalı Hackerler

Yeşil şapka bilgisayar korsanları da bilgisayar korsanlığı dünyasının amatörleridir. Ancak onlarla lamerler arasında bir fark vardır. Hackleme konusunda çok az bilgiye sahiptirler. Profesyonel bilgisayar korsanları olma konusunda tutkulu olduklarından, hacklemek için gerekli becerilerini geliştirmeye çalışmaktadırlar. Diğer bilgisayar korsanlarından ilham almakta ve saldırıları öğrenmek için onlarla iletişim halinde kalmaktadırlar.

3.5.6 Red Hat Hackerleri

Kartal gözü korsanları olarak da bilinen kırmızı şapkalı bilgisayar korsanları, beyaz şapka korsanları gibi çalışmaktadırlar. Siyah şapka bilgisayar korsanları tarafından gerçekleştirilen saldırılara karşı koymak için ellerinden geleni yaparlar. Aradaki fark, kırmızı şapka korsanlarının acımasız olmaları ve siyah şapka korsanlarının kullandığı ağı ve sistemi yok etmeleridir.

3.5.7 Devlet Destekli Hackerler

Farklı ülkelerden korsanlar kullanılmaktadır. Savunma sistemleri ile ilgili bilgileri elde etmek için diğer ülkelerin sistemlerine girmeleri hedeflenmektedir. Hükümetin maaşlı elemanlarıdır.

3.5.8 Hacktivist

Hacktivism (aktivizm), “hackleme” ve “aktivizm” kelimelerinin karışımından oluşmaktadır. İnsanların interneti genellikle siyasi veya sosyal nedenlerle kullandıkları belirlenmiştir. Bu insanlara bazen sosyal adalet savaşçıları denilmektedir. Hacktivism ve aktivizm birbiriyle ilişkilidir. Bununla birlikte, bu saldırılar çoğunlukla dijital olarak yapılmamaktadır. Hacktivistler (bu çabalara katılan insanlar) genellikle finansal kazançlar peşinde değildirler. Bunun yerine bir tür açıklama yapma çabası içindedirler. Bilgisayar korsanlığının ardındaki asıl amaç açıklama yapma çabası için saldırmaktır. Sivil itaatsizlik yerine, internet mesajlarını tüm dünyaya yaymak, onlar için çok önemli bir araçtır [34].

3.6 Bilgisayar Korsanları Tarafından Kullanılan Genel Araçlar

Bilgisayar korsanları, mükemmel bir saldırı gerçekleştirmek için çok sayıda araç kullanır. Bu araçlar şu şekilde listelenmektedir:

3.6.1 Rootkit

Dosyaları, çalışan süreçleri veya sistem içindeki bilgileri işletim sisteminden gizleyerek varlığını hissettirmeden sürdüren programların bütününe verilen addır. Asıl amacı sistem üzerinde yayılmak değil bulunduğu sistem içinde varlığını gizlemektir. Bu durum tipine göre değişmekle birlikte genellikle erişim yetkisi dâhilinde sisteme kurabilecek rootkit'ler vardır. Güvenilir bir kaynaktan geldiğine inandığınız bir programı haddinden fazla yetki ile çalıştırmak (Ör: root veya root yetkili bir grubu üyesi) zararlı bir rootkit'in sisteme kurulmasına sebep olmaktadır [35].

3.6.2 Tuş kaydediciler (Keylogger)

Keylogger'lar, klavyede basılan her tuşu kaydedebilen araçlar olarak bilinmektedir. Keylogger'lar herhangi bir uygulamanın, uygulama programlama ara yüzüne gizlenir. Uygulamaya eriştiklerinde kullanıcı tarafından yapılan her tuş vuruşunu kaydetmektedirler. Kaydedilen tuş vuruşları, kullanıcı adları, şifreler, web sitesi URL'leri, açık uygulamalar vb. gibi hassas verileri bir dosyaya kaydederler. Tuş kaydediciler ayrıca, klavye kullanılarak yazılmaları şartıyla kredi kartı bilgilerini, cep telefonu numaralarını, e-posta uygulamalarına yazılan kişisel mesajları vb. kaydedebildikleri için oldukça tehlikelidir. Keylogger'lar, hedef bilgisayara truva atları gibi kötü amaçlı yazılımlar kullanılarak yerleştirilir [36].

3.6.3 Güvenlik Açığı Tarayıcıları

Güvenlik açıklarını veya boşlukları belirlemek, ağları ve bilgisayar sistemlerini taramak için güvenlik açığı tarayıcısı kullanılmaktadır. Bilgisayar korsanları, bir sistemdeki boşlukları tespit etmek için genellikle bu aracı kullanırlar. Böylece açıklar mümkün olan en kısa sürede düzeltilecektir. Siyah şapkalı bilgisayar korsanları, bir hedefin sistemindeki veya ağındaki zayıflıkları keşfetmek için güvenlik açığı tarayıcılarını kullanırlar.

3.7 Siber Suç Türleri

Bilgisayar ve internet gibi dijital platformları kullanarak bir kişinin işleyebileceği suçları anlamak, gerekli tedbirleri almak için önemlidir. İnsanların bugün işlediği siber suç türlerini şu şekilde sıralayabiliriz:

3.7.1 Siber taciz

Siber zorbalık; başka bir kişiyi taciz etmek, tehdit etmek, utandırmak veya hedef almak için teknolojik platformların kullanılmasıdır. Siber zorbalık tanımı gereği genelde genç insanlar arasında gerçekleşmektedir. Bir yetişkin söz konusu olduğunda buna ‘‘Siber Taciz’’ ya da ‘‘Siber Saldırı’’ denir. Hukuki sonuçlara yol açabilecek ve hapis cezası gerektirebilecek bir suçtur. Siber zorbalığı fark etmek bazen oldukça kolaydır. Örneğin, çocuğunuz size kırıcı, kaba ya da acımasız bir mesaj, tweet veya Facebook yorumu gösterdiğinde bunun siber zorbalık olduğu anlaşılabilmektedir. Ancak, mağdurun kimliğini ele geçirmek, mağdura zarar vermek, onu utandırmak adına kişisel bilgilerini, fotoğraflarını ve videolarını yayınlamak gibi eylemleri fark etmek daha güç olabilmektedir. Bazı çocuklar sahte bir hesabın, web sitesinin ya da çevrimiçi kişiliğin yalnızca kendilerine yönelik taciz ve zorbalık amacıyla oluşturulduğu hakkında şikâyetler de bulunmaktadır [37].

3.7.2 Siber terörizm

Teknolojinin gelişmesiyle birlikte terörizm kendisine yeni alanlar ve yeni yöntemler bulmuştur. Terör örgütleri bir yandan kırsalda ve şehirlerde terör faaliyetlerini devam ettirirken diğer yandan da kendilerine yeni bir alan yaratmışlardır. Siber alanda da faaliyet göstermeye başlamışlardır. Bu çerçevede ‘‘Siber Terörizm’’, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere karşı kullanılmasıdır. Ayrıca bir hükümetin veya toplumun yıldırılması, baskı altında tutulması amacıyla da kullanılmaktadır. Siber terörizmde, ulusal bankacılık sistemlerinin çökertilmesi, insanlara ait hesapların ele geçirilmesi, devlete ait gizli bilgilerin bu yolla elde edilmesi, resmi ve sivil internet sitelerinin çökertilmesi gibi birçok faaliyet icra edilebilmektedir [38].

3.7.3 Siber Vandalizm

Siber Vandalizm, dijital biçimde meydana gelen hasar veya yıkım olarak adlandırılır. Siber Vandallar bir web sitesini bozabilir, elektronik dosyaları veya normal kullanımı

kesintiye uğratabilirler. Bilgisayar sistemini devre dışı bırakmak için bir disk sürücüsünü kaldıran kötü amaçlı yazılımlar oluştururlar. Siber Vandalizm, müşterilerin, hizmetlere erişmesini engellemekle beraber finansal kayıp, markaya zarar vermek, itibara etkisi de dâhil olmak üzere işletmeleri önemli ölçüde etkilemektedir.

3.7.4 E-dolandırıcılık

Kimlik avı, bir kişiyi, banka hesabı bilgileri gibi hassas bilgilerinin e-posta yoluyla ifşa edilmesi için kandırma işlemidir. Saldırgan, bankanın web sitesine benzer bir etki alanı kullanır. Bankadan veya diğer finans kuruluşlarından gönderilen e-postalara benzeyen bir e-posta gönderir. Kurbandan hesap numarası, hesap şifresi vb. gibi hassas bilgileri sağlamasını ister. Saldırgan daha sonra bu bilgileri, kurbanın hesabından kendi hesabına para aktarmak için kullanır. Bilgisayar korsanı saldırıyı telefon kullanarak gerçekleştirirse, vishing veya sesli kimlik avı olarak bilinir. Ülkemiz, telefon dolandırıcılığının en etkili kullanıldığı ülkeler arasındadır. Kendini savcı, hâkim, polis olarak tanıtan kişiler “Terör olaylarına karıştınız, hesaplarınızı kontrol ediyorlar” yalanıyla her gün binlerce kişiyi dolandırmaktadır. Bu mağdurlar arasında hâkim, doktor ve akademisyenler bulunmaktadır [39].

3.7.5 Hacklemek (Bir Bilgisayar veya sisteme sızarak ele geçirmek)

Bilgisayar korsanlığı, size ait olmayan bir bilgisayara, üzerinde bulunan verileri çalmak, değiştirmek veya yok etmek için erişme eylemidir. Bilgisayar korsanlığı yapmanın ardındaki neden kazanç elde etmekle beraber politik ya da sosyal olabilmektedir.

3.7.6 Kötü Amaçlı Yazılım Yaymak

Bilgisayar korsanları kötü amaçlı yazılımları yaymak için birçok web sitesi kullanmaktadırlar. Bunu kendilerini geliştirmek için yâda belirledikleri hedeflere ulaşmak için yaparlar. Kötü amaçlı yazılımlar, sistemleri çökerterek birey veya işletme için mali kayıplara neden olabilmektedir. Kayıplar, sistemin onarım maliyetini ve imha edilen verileri içerir. Bilgisayar korsanı yakalanırsa zarar gören taraf, zararlarının tazmini için dava açabilir.

3.7.7 Siteler Arası Komut Dosyası

Bazı saldırganlar, web sitesinin koduna gizli şekilde bir komut dosyası yerleştirir. Bu web sitesini ziyaret eden kullanıcı, bu komut dosyasını çalıştırır. Komut dosyası, kullanıcının bilgisayarındaki bilgilerini tarar. Saldırgan, komut dosyasını mağdurun bilgisayarına aktarmak için çerezleri kullanır. Bu sayede hassas bilgiler toplanır ve bu bilgiler saldırganın sistemine aktarılır. Saldırgan, bu bilgileri kullanıcının bilgisayarına veya bir web sitesindeki oturumlara erişmek için kullanır. Bu saldırı neticesinde kullanıcıyı finansal zarara uğratır.

3.7.8 Spam yapma

İnternet üzerinden istenmeyen ve gereksiz e-postaları toplu olarak gönderme eylemi “Spam” olarak adlandırılmaktadır. Aşağıdaki e-posta çeşitleri spam olarak adlandırılır:

- Anonim: Gönderen anonim kalır.
- Toplu Posta: Gönderen, birden çok kullanıcıya bir e-posta gönderir.
- İstenmeyen e-posta: Gönderen e-postayı istememiştir.

Spam e-postalar yalnızca kurbanın gelen kutusunu doldurmakla kalmaz, aynı zamanda tüm ağı da meşgul etmektedir.

3.7.9 Siber İşgal

Bir alanı (adresi), daha sonra yüksek bir maliyetle sahibi olan kuruluşa satmak amacıyla başka bir kuruluşun ticari markasını kullanarak kaydettirme eylemi siber işgal olarak adlandırılır.

3.7.10 Çevrimiçi Açık Artırma Sahtekârlıkları

İnternet üzerindeki çeşitli web siteleri çevrimiçi müzayedeler düzenlemekte ve siber suçlular bu web sitelerinden yararlanmaktadırlar. Web sitesini birebir kopyalayarak açık artırma sırasında yapılan tüm para akışı, böylece bilgisayar korsanının hesabına geçmektedir.

3.7.11 İnternet Zaman Hırsızlığı

İnternet saati hırsızlıkları çoğunlukla, bir kullanıcının ISS (İnternet Servis Sağlayıcısı) bilgilerinin çalındığı ve bu bilgilerin zamanın bedeli karşılığında internette gezinmek

için kullanıldığı bir suç türüdür. Bu, kullanıcının internette geçirdiği süre için ücretlendirildiği anlamına gelmektedir.

3.7.12 Web Krikosu

Web krikosu, bir saldırganın ilgili olmayan bilgileri görüntülemek için bir kuruluşun web sitesini ele geçirme yöntemidir. Bu durumu kuruluşun faaliyetleri hakkında farkındalığı yaymak için de kullanabilirler. Web krikosu politik, sosyal veya ekonomik çıkarlara hizmet etmektedir.

3.7.13 Hizmeti engelleme saldırısı (DDoS)

DDoS (DistrubutedDenial of Service Attack), sunucuların tüm hizmetlerine yönelik anlık ciddi bir yoğunluk oluşturulması ile meydana gelmektedir. Bir başka deyişle kaynak tüketiminin doruk noktalara çıkarılması demektir. Ele geçirilmiş olan milyonlarca IP adresi, bu yapay trafikleri oluşturmak için yaygın olarak kullanılmaktadır. Siber saldırı modeli olarak dikkat çeken DDoS, hackerler tarafından oluşturulan botnetler ile yapılmaktadır. Sunucularda açıklar verilmesini sağlayan saldırı tipidir [40].

3.7.14 E-posta Sahtekârlığı

Bir e-postanın içeriğini değiştirerek yapılan saldırı şeklidir. Kaynağını gizleyerek, bankadan geliyormuş gibi izlenim vererek kişisel bilgileri çalmayı hedeflemektedir. Bu, alıcının hassas bilgileri vermesi için yapılmaktadır.

3.7.15 Salam Saldırısı

Salam saldırısı doğası gereği marjinal bir yapıdadır. Uzun süre fark edilmeden kalabilmektedir. Salam saldırısına örnek olarak, saldırganın birden fazla banka hesaplarından her gün 1 TL çekmeyi hedeflemesi verilebilir. Kullanıcılar bunun farkına varmayacaktır. Ancak birçok kullanıcının banka hesabından birkaç gün içinde elde edilen 1 TL, birkaç ay veya yıl içinde çok miktarda para birikimine neden olacaktır. Bankalar artık olağandışı para çekme işlemlerini izlemekte ve işlem hakkında hesap sahibini hemen bilgilendirmektedir.

3.7.18 Veri Karıştırması

Verileri bir bilgisayar sistemine girmeden önce değiştirme eylemi, “*Veri Karıştırma’dır.*” Örneğin, bir saldırgan maaş bordrosunu değiştirerek şirketten alması

gereken maaş miktarını değiştirebilmektedir. İşyerinden daha yüksek maaş alabilmekte ancak şirket raporlarında, kendisine ödenmesi gereken miktarın ödendiği görülmektedir.

3.7.19 Mantık Hatası

Orijinal yazılımın içerisine gizlenen kötü amaçlı bir kod, mantık hatası olarak adlandırılmaktadır. Kötü amaçlı kod, kullanıcının gerçekleştirdiği bir işlemle tetiklenmektedir. Kötü amaçlı kod tetiklendiğinde, sistemdeki veriler yok edilebilmekte veya sistemi etkisiz hale getirebilmektedir.



4.BİR KİMLİK AVI SALDIRISINI TANIMA VE ÖNLEME

4.1 Kimlik avı nedir?

Çevrimiçi kimlik avı (phishing), bir e-posta iletisi veya web sitesi aracılığı ile kişisel ve finansal bilgileri elde etmek amacıyla, kullanıcıları kandırmak için kullanılan bir yöntemdir. En sık kullanılan kimlik avı dolandırıcılığıdır. Banka, kredi kartı şirketi veya bilinen bir online-çevrimiçi satıcı gibi bir kaynaktan gönderilmiş bir e-posta iletisiyle başlamaktadır. E-posta içerisinden, hesap numarası veya parola gibi kişisel bilgilerin istendiği sahte bir web sitesine yönlendirilmektedir. Bu bilgiler genellikle kimlik hırsızlığı amacıyla kullanılmaktadır [41].

Kimlik avı saldırıları, hem bireysel kullanıcılar hem de kuruluşlar için sorun teşkil etmektedir. Bir kişi veya kuruluştan elde edilen her türlü bilgi, saldırganın finansal avantajlar elde etmesine yol açmaktadır. Kimlik avı dolandırıcılığı siber ihlallerin en çok kullanıldığı yöntemler arasındadır.

4.2 Kimlik avı için kullanılan yöntemler

Bilgisayar korsanlarının kimlik avı saldırısını gerçekleştirmek için kullandığı bazı yöntemler şu şekilde sıralanmaktadır:

- Saldırgan, size gönderilen e-postalardaki bağlantıları değiştirmektedir. Bunu, URL'yi değiştirerek yapmakta, böylece kullanıcı kötü amaçlı bağlantı ile gerçek web sitesi arasındaki ayrımı yapamamaktadır. Örneğin, birçok web tabanlı uygulama "Şifremi Unuttum" özelliği sunmaktadır. Düğme tıkladığında, web sitesi şifre sıfırlamak için bir e-posta göndermektedir. Bilgisayar korsanı e-postayı yeniden yönlendirmeyi başarırsa, kullanıcı adınının ve güvenlik sorusunun cevabının girildiği farklı bir bağlantı gönderecektir. Bilgisayar korsanı daha sonra hesaba erişmek için bu bilgileri kullanacaktır.
- Bazı bilgisayar korsanları, web sitesi sahteciliğini bir kimlik avı dolandırıcılığı aracı olarak da kullanmaktadır. Saldırgan orijinal görünen sahte bir web sitesi geliştirmek için JavaScript komutlarını kullanmaktadır. Bu, kullanıcıyı izlemeyi kolay hale getirmektedir.
- Saldırganlar gizli yönlendirme olarak bilinen bir tekniği kullanmaktadırlar. Bu süreçte, pop-up'lar atmak için (istem dışı açılan web sayfaları) gerçek web

sitelerini kullanırlar. Bir kullanıcı, pop-up'ta açılan pencerede, kendisini saldırganın web sitesine yönlendiren bağlantılara tıklayarak veri ihlallerinin hedefi olmaktadır.

- Saldırganlar, virüslü EXE ekleri, PDF'ler ve Microsoft Office ekleri ile kullanıcının sistemine veya ağına kötü amaçlı yazılımları veya fidye yazılımlarını dağıtabilmektedirler.
- Saldırganlar, metin mesajları, telefon görüşmeleri, sosyal mecralar ve diğer medya yolları ile kimlik avı saldırıları gerçekleştirebilmektedirler [42].

4.3 Kimlik Avı Saldırılarıyla Mücadele Etmenin Yaygın Yolları

Sisteminizi ve ağınıza kimlik avı saldırılarından korumaya yönelik farklı yöntemler vardır. Kullanılan yaygın yöntemlerden bazıları şunlardır:

- Kötü Amaçlı Yazılım Tarayıcıları
- Otomatik Güncellemeler
- Çok Aşamalı Kimlik Doğrulama
- Sistem veya Veri Yedeklemeleri

Yukarıda bahsedilen yöntemlere ek olarak, sisteminizi ve ağınıza kimlik avı saldırılarından korumak için kullanabileceğiniz başka teknikler de vardır.

4.3.1 Aldatıcı Kimlik Avı

Aldatıcı kimlik avı, en yaygın kimlik avı saldırısı türlerindendir. Saldırgan, kullanıcının kişisel bilgilerini veya giriş bilgilerini vermesi için gerçek bir e-posta göndereni veya kuruluşu taklit etmektedir. Bu, e-postalar kullanılarak yapılmaktadır. E-posta içeriği, kullanıcının paniğe kapılmasına neden olmakta ve saldırganın yapmak istediği şeyi tam olarak yapmasına neden olan bir aciliyet duygusu yaratmaktadır.

Örneğin, saldırgan bir veya daha fazla kullanıcıya e-posta gövdesindeki bağlantıyı kullanarak ödeme yapmazlarsa kredilerinin devre dışı bırakılacağını bildiren bir e-posta göndermektedir. Kullanıcı bağlantıyı tıkladığında, bankanın veya ödeme ağ geçidinin bir kopyası, kullanıcıyı saldırganın web sitesine yönlendirmektedir. Kullanıcı daha sonra son kullanma tarihi ve güvenlik kodu dâhil olmak üzere kredi

kartı bilgilerini girer. Saldırgan artık, kullanıcının kredi kartında hileli işlemler yapmak için gerekli tüm bilgilere sahip olmuştur [43].

Aldatıcı bir kimlik avı saldırısının başarısı, kimlik avı e-postasının gerçek kuruluşun e-postasına ne kadar benzediğine bağlıdır. Kullanıcıların, bağlantıyı tıklamadan veya herhangi bir bağlantıyı indirmeden önce kendilerini korumak için hem e-posta adresinin hem de e-posta gövdesindeki bağlantıların URL'lerinden geçmesi gerekir. Aldatıcı bir kimlik avı e-postasının sahteliği yazım ve dilbilgisi hataları ile genel selamlamalardan anlaşılmaktadır.

4.3.2 Yemleme kancası (Spear phishing)

Teknolojilerin sağladığı imkânları kullanmak suretiyle, hedef alınan kişilerin aldatılarak, ikna edilerek kişisel veya gizli verilerinin ele geçirilmesidir. Bu söz konusu verilerin kötü niyetle kullanılması olarak da tanımlanmaktadır. Bunun ilk örneklerinden birisi 1960'larda telefon sistemlerine yetkisiz olarak giren kişilerin kendilerini "Phone Phreaks" olarak isimlendirmesiyle görülmüştür. Burada ucube, garabet, çılgın gibi anlamlar taşıyan "Freak" kelimesi dönüştürülüp "Phreak" şeklinde yazılarak bu terim türetilmiş ve yaygın olarak kullanılmıştır. "Phishing" kelimesinin de bu şekilde türetilmiş bir terim olduğu düşünülmektedir [44].

4.3.3 Balina Saldırısı (Whale Attack)

Bir yapıdaki üst düzey yöneticiler dahil herkese saldırmak için kullanılmaktadır. Saldırgan, bilgileri ve oturum açma kimlik bilgilerini çalmak için patronları ve üst düzey yöneticileri hedef almaktadır. Başarılı bir balina avı saldırısı, CEO dolandırıcılığına yol açmaktadır. Adından da anlaşılacağı gibi, CEO dolandırıcılığı, saldırırganın banka bilgilerini aldıktan sonra büyük finansal işlemleri onaylamak için CEO'nun e-postasını kullandığı yerdir. Balina avının bir başka uygulaması da, saldırırganların yöneticinin e-posta hesabını kullanarak, diğer çalışanların kişisel bilgilerini talep etmesidir. Çalışanların bilgilerini kullanarak, sahte vergi beyannamesi düzenleyerek finansal anlamda veri sahteciliği yapılmaktadır. Ayrıca saldırırgan bu bilgileri çevrimiçi olarak satmaktadır [45].

Kuruluşlardaki üst düzey yönetim, bilgi güvenliği konusunda eğitilmiş olduğundan çoğu saldırırganın balina avı saldırılarından kurtulmaktadır. Üst düzey yönetim de dâhil olmak üzere tüm çalışanlar için güvenlik bilinci eğitimi zorunlu hale getirilerek balina avcılığından kaçınılabilecektir. İşletmelerin ayrıca finansal işlemlerini yalnızca e-

posta yoluyla gerçekleştirmemeleri için iki faktörlü kimlik doğrulama veya çok faktörlü kimlik doğrulama süreçleri uygulanması daha doğru olacaktır.

4.3.4 Vishing – Smishing

Vishing yöntemi, kurbanı ses ile aldatma yöntemidir. Bu nedenle “Phishing” kelimesindeki “p” harfinin yerine “Voice” kelimesinin ilk harfi kullanılarak “Ses Aldatmacası” anlamında kullanılmaktadır. Vishing dolandırıcılık metodu, müşterilerin kişisel bilgilerini elde etmeye yönelik gönderilen e-postalar olarak nitelendirilmektedir. Bu e-postaların içeriklerinde verilen çeşitli telefon numaralarına yönlendirmeler yapılmaktadır. Bu sahte telefon numaraları kurban tarafından arandığında, dolandırıcının daha önceden hazırladığı sesli yanıt sistemlerine yönlendirilmektedir. Bunlar banka sesli yanıt sistemini ve çağrı merkezini taklit eden bir sistem olarak tanımlanmaktadır. Dolandırıcılar bu yöntem sayesinde kurbanı ait kişisel bilgileri ele geçirmektedir. Vishing saldırıları sadece e-posta yoluyla değil, cep telefonlarına gönderilen bir mesaj ile de yapılabilmektedir. Bunada “Smishing” denir. “Ücretsiz sms gönderin, X TL puan kazanmak için kaydolun.” tarzında faaliyet gösteren dolandırıcılık yöntemidir. Bir site gibi kayıt sırasında, kullanıcı bilgileriyle beraber cep telefonu numaranızı elde edip, daha sonra kiralanan bir hat üzerinden toplu sms gönderilerek yapılabilmektedir. Cep telefonlarına ulaşan mesajın içeriği, gönderilen e-posta içeriğine benzer olmakta ve yine benzer senaryolarla bilgilerinizi ele geçirmeyi hedeflemektedir [46].

Pandemi döneminde bu saldırı yöntemi artış göstermiştir. Aşı randevusu adı altında mesajlar yollanarak, dolandırıcılar kişisel bilgilerin girildiği yerlere yönelenerek insanların bilgilerini almaya çalışmışlardır. Vishing'i önlemenin en basit yolu, bilinmeyen numaralardan gelen aramaları asla yanıtlamamak, arayan kimlik bilgisi için bir uygulama kullanmak ve kişisel bilgileri telefon üzerinden kimseye ifşa etmemektir. Smishing saldırısından kaçınmanın en basit yolu ise size mesaj gönderen numaraya bakmak ve ardından bununla ilgili bir şeyler yapmaya karar vermektir. Alternatif olarak, mesajda belirtilen şirketi aramak ve gerçekten böyle bir mesaj gönderip göndermediklerini kontrol etmek bir çözüm olacaktır.

4.3.6 Pharming

“Pharming” web sitesi trafiğinin manipüle edildiği ve gizli bilgilerin çalındığı kimlik avına benzer bir siber suç türüdür. Site trafiği yönlendirme, internet taramasının

çalıştığı zeminden faydalanmaktadır. Bağlantı kurulabilmesi için “www.google.com” gibi bir internet adresini oluşturan harflerin sırasının DNS sunucusu tarafından bir IP adresine dönüştürülmesi gerekmektedir. Bu tehdit için iki saldırı yöntemi vardır: Birincisi, korsan bir kullanıcının bilgisayarına trafiği asıl hedeften başka yere yönlendirmektir. Sahte bir web sitesine göndermek için, bilgisayarın ana bilgisayardaki dosyalarını değiştiren bir virüs veya truva atı yüklenmektedir. İkincisi ise, korsan bir DNS sunucusunu değiştirerek, birden çok kullanıcının farkında olmadan bu sahte siteyi ziyaret etmesine neden olmaktadır. Sahte web sitesi, kullanıcının bilgisayarına virüs veya truva atı yüklemek amacıyla kullanılmaktadır. Kimlik hırsızlığında kullanılmak üzere kişisel ve finansal bilgileri toplama girişimi de olabilmektedir. “Site Trafiği Yönlendirme,” özellikle endişe verici bir siber suç biçimidir. Çünkü DNS sunucusunun değiştirilmesi durumunda bundan etkilenen kullanıcı hiç kötü amaçlı yazılım bulunmayan bir bilgisayara sahip olsa bile kurban haline gelebilmektedir. Web sitesi adresini manuel olarak girme veya daima güvenilen yer imlerinin kullanılması gibi önlemler almak yeterli olmamaktadır [47].

Bu tür dolandırıcılıktan korunma; şüpheli web sitelerinden kaçınma ve şüpheli e-posta iletilerindeki bağlantılara asla tıklamamaktır. Bilgisayar kullanma uygulamalarıyla birlikte kullanılmak üzere, güvenilir bir kötü amaçlı yazılım ve virüs karşıtı çözümün yüklenmesiyle korunulabilmektedir. Bu adımlar çoğu kötü amaçlı yazılımın bilgisayara erişmesini ve ana bilgisayar dosyalarını değiştirmesini önlemektedir.

4.4 Bir Kimlik Avı E-postasını Tanımlama

Bir kimlik avı e-postasının neye benzediğini, nasıl tanımlanacağını ve bu tür e-postalarla kandırılmamak için hangi önlemlerin alınması gerektiğinin bilinmesi gerekmektedir.

4.4.1 E-posta Sahtekârlığı

Saldırganın, bir e-postanın başlıklarını manipüle ederek e-postanın kaynağının, saldırganın sistemi gibi meşru olmayan bir kaynaktan geliyor gibi gösterilmesidir. Bu e-postanın gerçek görünmesini sağlayan kimlik avı çatısı altında bir metodolojidir. Saldırganlar, gönderenin e-posta adresini daha önce gördükleri bir adrese benzediği için, kullanıcıların e-postaya güvendiklerinin farkındadır. E-posta sahtekârlığının amacı, kullanıcıyı aldıkları e-postanın önemli olduğuna ve gönderenin gerçekten bilgi talep ettiğine inandırmaktır.

4.4.2 Sahte Bir E-postayı Tanımlama

Sahte bir e-postayı belirlemenin iki yolu vardır:

Konu satırı verilen örneklerden herhangi birine benziyorsa, e-posta gerçek değildir:

- abc@example.com e-posta hesabınız saldırıya uğradı.
- Acil: E-posta hesabınızın şifresini hemen değiştirin.
- Banka hesabınız ele geçirildi.
- Güvenlik Uyarısı: E-posta hesaplarınızı kaydedin.

Size yollanan E-posta içeriği aşağıdaki bilgileri isterse, sahte bir e-postadır:

- Kişisel bilgileriniz veya banka hesabı ayrıntılarınız,
- Belirli bir hesaba para göndermenizin istenmesi,
- Parola değişikliği istememiş olmanıza rağmen parola sıfırlama bağlantısı gelmesi,
- Ayrıntıları doğrulamak için diğer bilinmeyen bağlantılara yönlendirilmek.

“E-postanın gerçekten de e-posta başlıklarından gelen sahte veya spam bir e-posta olduğunu nasıl doğrularsınız?” diye bir soru gelmektedir. E-posta kaynağında aşağıdaki parametrelerden birine bakarak e-postanın gerçekliği doğrulanmaktadır.

4.4.3 Alınan-SPF

SPF (Sender Policy Framework) Domain DNS kayıtlarında, o domain adının hangi IP adreslerinden e-posta gönderdiğini belirten TXT kayıtlarına verilen isimdir. E-posta gönderimlerinde gönderici için "Kimlik İbrazı" da denir. Özellikle Hotmail, Yahoo, Gmail gibi e-posta servislerinin kontrol ettiği SPF kayıt doğrulaması ile ISS'ler, aldıkları e-posta mesajının, gönderim yapılan sunucu ile gönderici e-posta adresinin gerçek gönderici olduğunu teyit etmek ister. Bu kaydı oluşturmanın amacı, e-postaların gerçekten doğru yerden geldiğini teyit etmek ve spoof sahte e-postaları engelleyerek, phishing saldırılarını engellemektir [48].

4.4.4 X-CMAE Puanı - 100

Bu, e-postanın spam puanıdır. Alıcı e-posta sunucusu, e-postaya hangi spam puanını atadığına bağlı olarak belirli spam kontrollerine sahiptir. En yüksek değer 100'dür. Bir

e-postanın başlığı bu şekilde görünmektedir. Üstbilgiye, e-posta sağlayıcısının arayüzünde, bir e-postanın orijinal kaynağını “gmail.com” gibi görüntüleyerek erişilebilmektedir.

Bir kullanıcı böyle bir e-posta aldığında akıllara bazı sorular gelmektedir:

Böyle bir e-posta alınırsa hesap tehlikeye girer mi?

- Hayır, e-posta hesabı hiçbir şekilde tehlikeye girmez. Alınan e-posta ya spam ya da sahte bir e-postadır.

Sunucu neden bu tür e-postaları SPAM olarak sınıflandırmıyor?

- Çoğu sunucu, bu e-postaları SPAM olarak sınıflandıran sıkı e-posta kontrollerine sahiptir. Bu e-postalar otomatik olarak kullanıcının e-postasının spam klasörüne taşınır, ancak bu kontrollerin bir e-postayı atlayabileceği unutulmamalıdır.

Sahte bir e-posta almaktan tamamen kaçınılabilir mi?

- Hayır, her durumda, spam yapan kişi farklı bir konu ve farklı bir gövde kullanabilir. Bu nedenle genel bir filtre oluşturmak işe yaramayacaktır. Bu filtre yasal e-postaları engelleyebilmektedir.

4.4.5 Referans E-postası: (Kullanılan Şablon)

Merhaba yabancı!

Size bu mesajı hesabınızdan gönderdiğim için cihazınızı hackledim. Şifrenizi zaten değiştirdiyseniz, kötü amaçlı yazılımım her seferinde onu yakalar. Beni tanımıyor olabilirsiniz ve büyük olasılıkla bu e-postayı neden aldığınızı merak ediyorsunuz, değil mi?

Aslında, bazı web sitelerinin yetişkinleri (pornografi) üzerine kötü amaçlı bir program yayınladım ve bu web sitelerini eğlenmek için ziyaret ettiğinizi biliyorsunuz (ne demek istediğimi biliyorsunuz). Siz video klipleri izlerken, benim Trojan'ım hem ekranınıza hem de bir web kamerasına erişmeye izin veren bir keylogger ile bir RDP (uzak masaüstü) olarak çalışmaya başladı.

Bundan hemen sonra, programım tüm bağlantılarınızı messenger, sosyal ağlar ve ayrıca e-posta yoluyla topladı. Ben ne yaptım Çift ekranlı bir video yaptım. İlk bölüm izlediğiniz videoyu gösterir (iyi bir zevkiniz var,

evet ama diğer normal insanlar ve benim için garip) ve ikinci bölüm web kameranızın kaydını gösterir.

Ne yapmalısın?

Küçük sırrımız için 608 \$ 'ın (USD doları) makul bir fiyat olduğunu düşünüyorum. Bir Bitcoin ödemesi yapacaksınız (bilmiyorsanız, Google'da "Bitcoins nasıl alınır" konusuna bakın).

BTC Adresi: 1GjZSJnpU4AfTS8vmre6rx7eQgeMUq8VYr (Bu CASE duyarlıdır, lütfen kopyalayıp yapıştırın)

Açıklamalar: Ödemek için iki gününüz (48 saat) var. (Özel bir kodum var ve şu anda bu e-postayı okuduğunuzu biliyorum). Bitcoin alamazsam, videonuzu aile üyeleri, iş arkadaşları vb. dahil tüm kişilerinize göndereceğim.

Ancak, ödeme alırsam videoyu hemen yok edeceğim ve Truva Atım kendi kendini yok edecek.

Kanıt almak istiyorsanız, "Evet!" ve bu mektubu kendinize tekrar gönderin. Ve kesinlikle videonuzu on iki kişiye göndereceğim. Bu, pazarlık konusu olmayan bir tekliftir, bu nedenle lütfen bu e-postayı yanıtlayarak kişisel ve başkalarının zamanını boşa harcamayın. Hoşçakal! Lütfen sorunu araştırın ve bana geri dönün.

Saldırgan bu e-postayı, gönderdiği kişinin kendi e-posta adresini taklit etmektedir. Kullanıcının e-posta hesabına erişimi olduğuna inandırarak e-postayı göndermektedir. İçeriğe bakarsanız, saldırgan masum bir kullanıcıyı, kullanıcının bilgisayarına erişemediği zaman bile, erişebileceğini söyleyerek ikna etmeye çalışmaktadır. Kullanıcı dikkatli olmazsa saldırganı inanarak, isteklerini yerine getirecektir. Ancak, e-postanın başlıklarını incelemek, kullanıcının bu saldırganın gerçekten e-postalarına erişimi olup olmadığını veya blöf yapıp yapmadığını anlamasına yardımcı olacaktır.

Her kimlik avı girişimini tanıyabileceğinizin garantisi yoktur. Saldırganlar ayrıca araştırma yaparak, kullanıcı davranışları hakkında daha fazla bilgi edinmektedirler. Bu bilgileri, saldırılarını iyileştirmek için kullanmaktadırlar. Bunu unutmayarak, kullanıcılar, korsanların bugün kullandığı yeni kimlik avı teknikleri hakkında daha fazla bilgi edinmeli ve bu konuda kendilerini eğitmelidirler.

5. KÖTÜ AMAÇLI YAZILIM NASIL BELİRLENİR VE KALDIRILIR

Kötü amaçlı yazılım, farklı kötü amaçlı yazılımlar için (casus yazılımı, fidye yazılımı ve virüsler gibi) kullanılan genel bir terimdir. Kötü amaçlı yazılım, saldırganlar tarafından bir sisteme ve ilgili verilere saldırmak için geliştirilen bir koddur. Kötü amaçlı yazılımları dağıtmak için kullanılan araç genellikle bir e-posta olmaktadır. E-posta, tıklandığında veya indirildiğinde kötü amaçlı yazılım kodunun yürütülmesine neden olan bağlantılar veya ekler çalıştırılmış olmaktadır.

Kötü amaçlı yazılım, bireysel kullanıcıları ve kuruluşları tehdit eden “Creeper Virüsü” 1970’lerin sonunda ortaya çıkmıştır. O zamandan beri dünya, hepsi aynı amaca sahip milyonlarca kötü amaçlı yazılım görmüştür. Bunların amacı hep aynıydı. Hizmetlerin kesintiye uğratılması ve yok edilmesi idi. Kötü amaçlı yazılım, çeşitli şekillerde hedef sistemlere dağıtılan yükleri içermektedir. Bir saldırganın güdülere para istemekten bilgi çalmaya kadar uzanmaktadır. Saldırı teknikleriyle daha da akıllı hale gelmeye başlamaktadırlar.

5.1 Kötü Amaçlı Yazılım Türleri

Birinci bölümdeki siber güvenlik terminolojisi bölümünde bu terimlerin bazılarında daha önce kısaca bahsetmiştik. Bunlardan şimdi biraz daha ayrıntılı bahsedelim.

5.1.1 Virüsler

Bilgisayar virüsleri biyolojik virüsler gibidir. Çalışmanızı engeller ve iyileşmek için birçok yola başvururuz. Bu nedenle “virüs” olarak adlandırılırlar. Biyolojik virüslerin bir insandan diğerine geçmesi gibi bilgisayar virüsleri de bir bilgisayardan diğerine geçmektedirler.

Bilgisayar virüsleri durmak bilmeden çoğalmak amacıyla geliştirilmiştir. Kendilerini başka bir programa, belgeye veya önyükleme kısmına kopyalayarak çoğaltan kötü amaçlı yazılımlardır. Bu virüsler, bilgisayarın çalışma şeklini, işletim sisteminin bütünlüğünü ve gizliliğini tehdit etmektedir. Bilgisayar virüslerinin, kendilerini bir kullanıcının bilgisi veya izni olmadan çoğaltmaları gerekmektedir. Bu anlamda bilgisayar virüsleri birer bağımsız program değildirler. Bu virüsler Fidye Yazılımları, Truva Atı (Trojan Horse Virus), Solucan Virüsü gibi birçok kötü amaçlı yazılım bünyesinde bulundurmaktadır. Bilgisayar virüsü diğer kötü amaçlı yazılım türleri gibi bilgisayarınıza zarar vermek ve ele geçirmek amacıyla saldırganlar tarafından

oluşturulmuştur. Bilgisayar virüslerinden korunma konusunda ne kadar dikkatli ve bilinçli olursanız olun nereden geldiğini tahmin edemeyeceğiniz yerlerden bilgisayarınıza virüs bulaşabilir. İnternet kullanımı henüz yaygın değilken virüsler, genellikle virüslü disklerden bilgisayarınıza ve oradan da başka bilgisayarlara yayılıyordu. Modern zamanda ise bunlar, sizinle paylaşılan müzikler, fotoğraflar, e-postalar, indirilen oyunlar, programlar, uygulamalar ya da virüs bulaşmış bir web sitesi ziyaretinden kaynaklı olmaktadır. Virüsün bulaşma işlemi genellikle kullanıcının kendi isteğiyle ya da farkında olmadan virüslü bir program yürütmesiyle gerçekleşmektedir. Bilgisayar virüsü içeren bir program çalıştırıldıktan sonra, bu virüs belleğe taşınmaktadır. İşte tam bu noktada virüs, bilgisayardaki diğer uygulamalara hızla bulaşmakta ve kötü amaçlı kodunu yayabildiği kadar yaymaktadır. Bilgisayarların disket önyükleme kısımlarına bulaşan önyükleme virüsleri bu aşamada özellikle zararlı bir teknik kullanılmaktadırlar. Bu kodları ön yüklemeye yerleştirerek bilgisayarın normal bir şekilde çalışmasını bile imkânsız hale getirmektedirler.

Bazen bir e-posta eki açarak veya virüslü bir reklama tıklayarak yayılabilen bilgisayar virüsleri, ana makineye ulaştıktan sonra kendini belleğe yüklemekte ve çalıştırılan her programa bulaşmaktadır. Bu virüsler sistem yazılımlarına ulaşp verileri kopyalayabilir, silebilir veya şifreleyebilirler. Bilgisayar virüsleri bulaştıkları programları ya anında ya da zaman içinde işlemez duruma getirmektedir. Bilgisayar virüslerinin bazıları, programların tamamen silinmesine, dosyalara erişilmemesine ve sistemin çökmesine neden olmaktadır. Eğer bilgisayarınızda sebebini bilmediğiniz veri kaybı, performans düşüşü, sık sık bilgisayar çökme problemi yaşıyorsanız bilgisayarınıza virüs bulaşmış demektir. Elbette bilgisayarınıza virüs bulaşmaması için birçok yöntem vardır. Anti-virüs programları ve casus yazılımları bu konuda en büyük etkenlerdendir. Ayrıca kullanılan işletim sisteminin ve tarayıcıların güvenlik ayarlarını sürekli güncel tutarak, yalnızca güvenilir sitelerden yazılım indirerek veri güvenliği sağlanabilir [49].

Ayrıca tanımadığınız adreslerden gelen e-postalar açılmamalı ve spam mailleri silinmelidir. Çünkü gönderilen basit bir e-postada bile zararlı yazılımlar olabilir. Bilinçsizce bu işlemler yapıldığında virüslü uygulama yürütülmekte ve virüs CPU belleğinize kadar yayılabilmektedir. Böylece bilgisayar virüsü diğer uygulamalarınıza da bulaşarak kötü amaçlı yazılım kodu ulaşabildiği her yere yayılmaktadır.

- Bu virüsler banka kimlik bilgilerinizi tarayabilir,

- Şifrelerinizi çalmak için tuş hareketlerinizi izleyip kaydedebilir,
- Verilerinizi şifreleyip geri alabilmeniz için sizden fidye/bitcoin ödemesi isteyebilirler.

Bilgisayarda ücretsiz anti-virüs programları olsada korunmak için güvenilir ve güncel bir korumaya ihtiyaç duyulmaktadır. Anti-virüs programları virüslere karşı koruma sağlayan, kurtarma ve temizleme işlerini yapan koruyucu programlardır. Bu programlar bilgisayarınızdaki virüsleri tespit edip karantina ve silme işlemlerini gerçekleştirmektedir.

5.1.2 Solucanlar-Wormlar

Solucanların bilinen tarihi virüslerden öncedir. Bilgisayarların geliştirilmesinden bu yana varolmuşlardır. 1990'larda e-postanın kullanıma girmesiyle popüler hale gelmişlerdir. Birçok kullanıcı e-posta ekleri ile birlikte gelen solucanlarla ciddi sorunlar yaşamıştır. Bir çalışan, solucan içeren bir e-postayı açtığında tüm kuruluş kısa sürede etkilenmektedir. Solucanlar bulaştıkları sistemlerde kendilerini çoğaltarak sistemde yayılmaya başlarlar. Teknik anlamda katlanarak çoğaldıkları (kendini kopyalama) için çok kısa bir zaman içinde çok büyük rakamsal değerlere ulaşırlar. Wormlar temel anlamda insanlara benzerler kendi soylarını devam ettirme çabası içinde kendi kopyalarını (klon) ulaştığı her ortama yaymaya çalışırlar. Böylece hayatta kalma süreleri uzayarak verdiği zararlar katlanarak artmaktadır. Gerçek hayatta solucan gibi canlılar ortadan ikiye bölündüğünde iki farklı yeni canlı oluşmaktadır. Bu zararlı ise bölünmek yerine kendini çoğaltarak sayısını arttırır. Wormlar kodlandığı dile göre çeşitlilik gösterse de özünde normal dosya kopyalama şeklinde olduğu gibi çoğalmaktadırlar. Wormlar çalıştırılan makinede zararlı kodların bir kopyasını oluşturup daha sonra farklı bir konumda tekrar bir araya getirirler. Kendisinin aynısı (klon) olan bir worm meydana getirirler. Kopyalama işlemi bilinen dillerde olan sistem kütüphanelerini işleyerek tek satırda gerçekleştirilebilir. Worm virüsünün önemli noktalarından biri olan insan faktörünü kullanması onu olduğundan daha tehlikeli hale getirmektedir. Bir klasör altına klasör ile aynı isimde bir kopyasını meydana getirerek aktif olması ile, wormun tekrar tetiklenmesi için insanların zafiyetini kullanır. Worm bunun yanında kendisini disk, çıkarılabilir medya, harici bellek, disk gibi ortamlara “Özel Dosyalar” ismiyle çoğaltmaktadır. Bu durumdaki amaç meraklı kişilerden faydalanılarak kendisinin sisteme bulaştırılmasını sağlamaktır. Wormların diğer bir

özelliği de “autorun. inf” adında otomatik başlatma için kullanılan bir dosyayı harici belleğe yazarak, bellek sisteme takıldığında otomatik tetiklenmeyi sağlar. (Eski sistemler için geçerli). E-Posta içindeki ekleri ile de yayılabilen bu wormlar, kullanıcıların kişiler listesindeki kişilere otomatik oluşturulan bir e-mail atarak ekine kendisinin bir kopyasını yerleştirirdi. Her yönüyle kendi kopyalarını olası bütün koşullarda çoğaltmayı hedefleyen bu zararlı yazılımların spesifik olarak birçok özelliği daha bulunmaktadır. Bu virüs çeşitleri genel olarak ilk başlarda kendilerini çoğaltmayı amaçladıklarından bilgisayara zarar verdikleri düşünülmeyebilir. Zamanla kullanıcının birçok bileşenine erişimini engelleyerek kendisinin sisteme olabildiğince fazla zarar vermesini sağlıyor. Bunlara örnek olarak:

- Görev yöneticisini devredışı bırakma
- Regeditin (kayıt defteri) kapatılması
- “Gizli dosyaları göster” seçeneğini aktif hale getirildiği halde tekrar pasif hale getirme
- Masaüstü dosyalarına erişimi engelleme
- Başlat menüsündeki araçların bağlantılarını değiştirme
- usb belleklerde kendisinin gizli bir kopyasını oluşturma
- Bilgisayardaki CPU (Merkezi İşlem Birimi) yük artırma
- Bilgisayardaki Ram’e (Rastgele Erişim Belleği) yük bindirme
- Bilgisayarda ikincil diskin (HDD, SSD) devamlı kullanılmasına neden olma (kopyalama ve kontrol işlemlerinden dolayı)
- Bilgisayarın Hafızasında yer işgal etme (her oluşturulan kopya depolama biriminde bir yer tayin eder.)

Daha birçok etkisi olmasının yanında bunlar genel anlamda kabul görenleridir. Solucanlar (worm) diğer virüslerle kıyasla daha kolay dezenfekte edilebilen virüslerdir. Bilgisayarlardaki güncel olan antivirüsler neredeyse tüm worm virüslerini tanır ve temizler. Yalnız önem verilmesi gereken kısım, disklerin dizinlerle birlikte tarama işlemine tabi tutulmasıdır. Bunun nedeni virüsün yayılması sonucu olası her dizin altına bir kopyasının oluşturmuş olma ihtimalidir. Diğer virüslere kıyasla bilgisayardan temizlenme süreci oldukça uzun sürmektedir. Bunun nedeni antivirüsün

bütün alt dizinleri ayrı ayrı tarayarak virüsün varlığını kontrol ediyor olmasıdır. Manuel bir şekilde temizlemek olası bir ihtimal olsa da en pratik yol bu tür virüslere karşı üretilmiş antivirüs ve antimalware yazılımlarıdır. Genellikle temizleme işlemi ardından bazı bölümler (regedit, task manager) kendiliğinden düzeltilemez. Bunun için kolaylıkla bulunacak birçok düzeltme aracı vardır. Virüsün temel olarak yaptığı regedit (kayıt defteri) değerlerini değiştirerek ilgili görev yöneticisine erişimi kısıtlamaktır. Burada diğer üçüncü parti araçlarla bu kayıtlar düzeltilebilmekle birlikte script ile sorunlar düzeltilmektedir. Bazı worm türleri antivirüslerini de engellediğinden bilgisayarı “güvenli” modda başlatmak sorunu çözmek için en iyi çözümlerden biridir. Genelde insanlar arasında bilgisayara format atmak da olası çözümler arasında yer alsada format (sistem sıfırlama) işleminden sonrası alınan yedekler için detaylı bir virüs taraması yapmak gerekmektedir [50].

5.1.3 Truva Atları

Saldırganlar, yeni saldırılar uygulamak için bir silah olarak solucanlardan Truva atlarına geçti. Truva atları, gerçek programlar veya dosyalar gibi görünseler de içlerinde kötü amaçlı kodlar bulunmaktadır. Truva atları dijital dünyada virüslerden önce mevcuttu ve bugün siber suçlar arasında en popüler kötü amaçlı yazılımlardandır. Virüsler gibi, Truva atları da yürütülmesi için kullanıcı etkileşimine ihtiyaç duymaktadır. Truva atı, hedef sisteme ulaşmak için bir araç olarak e-postaları veya kötü amaçlı web sitelerini kullanmaktadır. En yaygın ve popüler Truva atı türü sahte bir virüsten koruma yazılımıdır. Belirli web sitelerini ziyaret ederken bilgisayarınıza virüs bulaştığını söyleyen bannerler vardır. Sizden virüsü temizlemek için yazılımın indirilmesini isteyecektir. Bunun doğru olduğuna inanarak, Truva atı indirilip yüklenebilir. Truva atı daha sonra sisteminizin kontrolünü ele geçirmektedir. Kendinizi bir Truva atına karşı savunmanız iki nedenden dolayı zordur:

1. Truva atlarını kodlamak kolaydır ve siber suçlu grupları bugün Truva atı oluşturma kitleri bile geliştirmiştir.
2. Truva atları, kullanıcıları kandırarak bir sisteme yerleştirilir ve bu nedenle bir güvenlik duvarı gibi geleneksel savunmalardan rahatlıkla kaçarlar.

Kelimenin tam anlamıyla her ay geliştirilen milyarlarca Truva atı bulunmaktadır. Virüsten korunmak için geliştiriciler, Truva atlarına karşı koymak için ellerinden

geleni yapmakta, ancak imzaları izlenemeyecek kadar fazla olduğundan bu konuda zorlanmaktadırlar.



Şekil 5.1 : Truva Atı

5.1.4 Hibrit Kötü Amaçlı Yazılım

Hibrit kötü amaçlı yazılım; diğer kötü amaçlı yazılımların, Truva atlarının ve hatta virüslerin karma bir kombinasyonudur. Kötü amaçlı yazılım başlangıçta bir Truva atı gibi görünebilir. Ancak yürütüldüğünde, solucanlar tarafından ağdaki tüm kullanıcılara saldırmaktadır. Günümüzde kötü amaçlı yazılım programları, gizli programlar veya rootkit'ler olarak kabul edilmektedir. Bu da günümüzde kötü amaçlı yazılımın temel amacının, bilgisayarın işletim sisteminin kontrolünü ele geçirmek ve kötü amaçlı yazılım önleme programlarının bile algılayamayacağı şekilde onu manipüle etmek olduğu anlamına gelmektedir. Bu tür kötü amaçlı yazılımlardan kurtulmanın tek yolu, sistemin kontrolüne sahip olan bellek bileşeninin bağlantısının kesilmesidir. [36] Botlar kendilerini ayrı bilgisayar sistemlerine yerleştirir ve ardından bot ağı için komuta ve kontrol sunucuları olan bot yöneticilerinden talimat beklerler. Botnet olarak bilinen bot ağları, tek bir botmaster tarafından kontrol edilmektedir. İnternet üzerinden binlerce sunucudan oluşan bir ağla birkaç yüz bilgisayarı istila edebilirler. Bot yöneticileri genellikle bu botnet'leri, onları özel ihtiyaçları için kullanan diğer suçlulara kiralamaktadırlar [51].

5.1.5 Fidyeye Yazılımı

Fidyeye yazılımı, her geçen gün gelişen ve daha da yaygınlaşan bir zararlı yazılım türüdür. Temelde iki türü vardır: Şifreleyiciler ve kilitleyiciler. Bilgisayarınıza

şifreleyici bulaştığı zaman, bilgisayarınızda bulunan her türlü veriyi (dosyalar, fotoğraflar, oyunların save dosyaları, veri tabanları vs.) şifrelemektedir. Dosyalar bir defa şifrelendiğinde dosyaları açamazsınız ve dosya içerisinde bulunan verilere ulaşamazsınız. Bu saldırıları düzenleyen suçlular, dosyalarınızı açabilecek özel anahtar karşılığında fidye talep etmektedirler. Talep edilen ortalama fidye miktarı 3000 TL civarındır. Diğer türe kilitleyici denilmesinin sebebi ise, bu zararlı yazılımların bütün cihazı kilitlemesidir. Yani sadece dosyalarınız değil, bütün sistem erişilmez olmaktadır. Kilitleyicilerin istedikleri fidye miktarı şifreleyicilerinki kadar yüksek olmamaktadır. Tüm Windows, Mac OS X, Linux ve Android cihazları tehdit etmektedirler. Kısacası tüm masaüstü ve mobil cihazlar tehdit altındadır. Ancak fidye yazılımları ağırlık olarak Windows ve Android cihazları hedef almaktadır. Aynı zamanda cihazınıza bulaşması da çok kolaydır. Çok yaygın olarak, fidye yazılımları bilgisayarda açılan şüpheli eklerden, tıklanan şüpheli linklerden ve uygulama indirilen üçüncü parti mecralardan bulaşmaktadır. Ayrıca fidye yazılımları yasal internet sitelerine de bulaşabilmektedir. Güncel olarak, siber suçlular fidye yazılımlarını kullanıcılara bulaştırmak için reklam ağlarını kullanırlar. Kullanıcılara önemli bir şey indirtip açtığını düşündürmek çok zor olmamaktadır. Bankadan gelmiş bir mail ya da önemli bir program yüklemesi bunlardan bazılarıdır. Dosya açıldığında ya da program kurulduğunda, kullanıcı kendi bilgisayarına fidye yazılımı kurmuş olmaktadır [52].

Fidye yazılımlarının temel sorunu şu ki zararlı yazılımı silmeniz ile problem çözülüyor. İyi bir antivirüs programı ve özellikle belli uygulamalar, genellikle fidye yazılımlarına karşı çok etkili çözüm sunmaktadır. Eğer zararlı yazılım dosyalarınızı şifrelerse, verilerinize erişebilmek için şifreyi bilmeniz gerekmektedir. Bu şifreyede ancak para ödeyerek erişebilirsiniz.

5.1.5.1 Enfekte Olunursa Ne Yapılmalıdır.

Fidye yazılımı kurbanı olunursa uyulması gereken temel kural, asla fidye ödememektir. “Emniyet Siber Suçlar Birimi” bile fidye ödememenizi tavsiye etmektedir. Fidye ödenirse, saldırganların yapmak istediği şeyler yapılmış olunmaktadır. Bu nedenle, onları gelecekte fidye yazılımı saldırıları planlamaya teşvik edersiniz. Ücretsiz dosya şifre çözme yazılımlarını kullanarak şifrelenmiş dosyalardan bazılarını geri alma olasılığı ne yazık ki düşüktür. Ancak, bu araçların tersine çevirebileceği veya önleyebileceği bazı fidye yazılımı saldırıları vardır. Ayrıca, bir şifre çözücü varsa, sisteminizde zaten mevcut olan fidye yazılımlarından korumaya

yardımcı olduğundan emin olunmalıdır. Dosyalarınız daha fazla şifreleneceğinden herhangi bir şifre çözme yazılımının bilgisizce çalıştırılmaması gerekmektedir. Fidyeye yazılımlarını temizlemenin diğer bilinen yöntemleri ise, sisteminizi taratmak ve bulaşımı ortadan kaldırmak için fidye yazılımı önleme ürünlerini kullanmaktır. Bu çözümler dosyalarınızı geri almanıza yardımcı olmayacaktır. Ancak sisteminizin temizlenmesine yardımcı olacaktır. Ekran kilidi durumunda, sistemi önce, sağlıklı bir geri yükleme noktasına geri yüklemeyi denemeli veya ön yüklenebilir bir USB sürücüden veya DVD'den bir tarama yapması denenmelidir.

Devam eden bir fidye yazılımı saldırısını bertaraf etmek istiyorsanız, her zaman tetikte olunmalıdır. Sisteminizde sebepsiz yere yavaşlama olduğunu fark ederseniz, en iyisi sistemi yeniden başlatmak ve internet bağlantısını kesmek olacaktır. Bu, sistemi başlattığınızda kötü amaçlı yazılımın etkin olmamasını sağlayacaktır. Ayrıca komuta edilen sunucudan veya saldırgandan talimat alamayacak veya gönderemeyecektir. Saldırganın, etkinliği tamamlamadığı için sistemdeki tüm dosyaları şifreleyemeyeceği ve dolayısıyla para talep edemeyeceği anlamına gelmektedir. Bu noktada, kötü amaçlı yazılımdan koruma çözümü yüklenmeli ve sistemde tam bir tarama gerçekleştirilmelidir.

5.1.5.2 Fidyeye Yazılımdan Nasıl Korunuruz

Bir fidye yazılımı bulaşmasıyla mücadele etmenin birkaç yöntemi bulunmaktadır. Ancak bunların işe yaradığına dair bir kanıt bulunmamaktadır. Bunların çoğu üst düzey teknik uzmanlık gerektirir ve orta düzeyde bir kullanıcı bu tür araçları kullanamaz. Bu nedenle, aşağıdaki çözüm yolları izlenmelidir.

İlk adım olarak, gerçek zamanlı koruma sağlayan ücretli yazılımlar satın alınmalıdır. Bu çözüm aynı zamanda gelişmiş fidye yazılımlarından gelen saldırıları da algılayacaktır. Çözüm, savunmasız dosyaları ve yazılımları koruyabilmeli ve aynı zamanda fidye yazılımının herhangi bir dosyayı şifrelemesini engellemelidir. Bir sonraki adım zaman ve çaba gerektirir. Verilerin düzenli olarak yedekleri oluşturmalı ve bunların harici bir ortamda depolanması sağlanmalıdır. Uzmanlar, yedeklemelerin şifreleme ve çok faktörlü yetkilendirme ile korunan bulut tabanlı bir çözümde depolanmasını önermektedir. Diğer bir seçenek de yedeklemeleri USB sürücüler veya sabit diskler gibi harici ortamlarda saklamaktır. Ancak, yedeği aldıktan sonra bunların bağlantılarının kesildiğinden emin olunmalıdır. Aksi takdirde, fidye yazılımının bu

harici cihazlara da bulaşma ihtimali yüksektir. Sonraki adım, işletim sisteminizin ve diğer yazılımların güncel olmasını sağlamaktır. Popüler WannaCry fidye yazılımı, Microsoft işletim sistemindeki bir güvenlik açığından yararlandı. Microsoft, Mart 2017'de güvenlik açığını düzeltmek için bir güncelleme yayınladı ancak çoğu kişi bu güncelleştirmeyi görmezden geldi ve indirmede. Bu, sistemlerin saldırıya açık hale gelmesine sebep oldu. İşletim sistemini ve diğer yazılımları manuel olarak güncellemenin zor olduğu, bu nedenle işletim sistemi ve diğer yazılımlar için otomatik güncellemelerin etkinleştirilmesinin en güvenilir olduğu anlaşılmaktadır [53].

Fidye yazılımı dağıtmak için kullanılan en yaygın teknik sosyal mühendisliktir. Herkes kötü amaçlı web sitelerini, malspam'ı ve diğer zararlı yazılımları nasıl tespit edeceği konusunda eğitilmelidir. Her zaman içgüdünüze güvenin. Bir şey zararlı görünüyorsa, kesinlikle öyledir.

5.1.6 Dosyasız Kötü Amaçlı Yazılım

Bu gerçekten kötü amaçlı bir yazılım türü değildir. Ancak kötü amaçlı yazılımın, bir kullanıcıyı istismar etmek için kullanılma biçimine dayalı olarak yapılmıştır. Geleneksel kötü amaçlı yazılım, dosya sisteminin kontrolünü ele geçirerek sistemlere bulaşmaktadır. Diğer yandan, dosyasız kötü amaçlı yazılım ise dosya sistemine dokunmaz, ancak sistem belleğine yayılır veya API'ler (Application Program Interface) , zamanlanmış görevler ve kayıt defteri anahtarları gibi dosya dışı diğer bileşenleri kullanmaktadır. Dosyasız kötü amaçlı yazılım, sistemde çalışan bir programı alt süreci haline getirmek için kullanır veya Microsoft Windows tabanlı işletim sistemlerinde PowerShell gibi sistem araçlarını kullanmaktadır. Saldırganlar, tespit edilmesi zor olduğu için dosyasız kötü amaçlı yazılımlar kullanmaya başladılar. Örneğin, "Operasyon Kobalt Kitty", altı ay boyunca PowerShells'e bulaşmak ve Asya şirketlerine saldırmak için popüler hale gelen dosyasız kötü amaçlı yazılımdır. Kötü amaçlı yazılım, hedef sistemlere hedefli kimlik avı e-postaları kullanılarak yerleştirildi.

5.1.7 Reklam Yazılımı ve Kötü Amaçlı Reklamcılık

Kötü amaçlı yazılımlara yalnızca reklam yazılımı biçiminde rastlanılmamaktadır. Adware, kullanıcının bilgisi olmaksızın ve çoğu zaman başka bir yazılımla birlikte bilgisayara yüklenen programlardır. Bir bilgisayara bulaşır ve istenmeyen reklamları göstermeye devam eder. Reklam yazılımı aracılığıyla görünen en yaygın reklamlar,

kullanıcıları diğer ürünler için promosyonlar içeren web sitelerine yönlendirirler. Reklam yazılımı potansiyel olarak zararsızdır ancak çok can sıkıcı olabilmektedir.



Şekil 5.2 : Kötü Amaçlı Reklamcılık

Bu reklam yazılımlarıyla karıştırılmamalıdır. Ancak kötü amaçlı reklamcılık, kötü amaçlı dosyaları hedef sisteme göndermek için gerçek reklamları kullanırlar. Örneğin; bir saldırgan, web sayfasına kötü amaçlı bir reklam yerleştirmesi için bir web sitesine ödeme yapar. Bu reklamı tıklayan bir kullanıcı saldırganın web sitesine yönlendirilerek, kötü amaçlı yazılımı anında kendi sistemine indirecektir. Çoğu zaman, reklamlardaki kötü amaçlı yazılımlar herhangi bir kullanıcı etkileşimi olmadan yürütülmektedir. Bu teknik "by-download" olarak adlandırılır. Saldırganların, reklamlar aracılığıyla "Spotify, Hepsiburada, Amazon" gibi daha büyük web sitelerine kötü amaçlı yazılım dağıtmak için "Yahoo" gibi büyük reklam motorlarına saldırdığı durumlar olmuştur.

5.1.8 Casus Yazılım

Casus yazılım, saldırganlar tarafından insanların faaliyetlerini gözetlemek için kullanılan kötü amaçlı bir yazılımdır. Çoğunlukla bir ilişkideki ortaklar tarafından birbirlerini gözetlemek için kullanılır. Ancak saldırganlar aynı zamanda hedefin etkinliğini anlamak ve tuş vuruşlarını kaydetmek için casus yazılım kullanırlar. Casus yazılımların siber zaafiyet kapsamında da kullanılması, sebep olduğu zararları gün

geçtikçe artırmaktadır. ABD’de ‘‘Federal Soruřturma B rosu’’ tarafından 2005 yılında 2000’den fazla firma ile yapılan bir arařtırmada, bu řirketlerin %64’ n n bilgisayarlar ve casus yazılım iliřkili zaafiyetlerden finansal zararlara maruz kaldıęı belirlenmiřtir. ‘‘Federal Soruřturma B rosu’’ oluřan bu finansal kaybın yaklaşık 62 milyar ABD doları olduęunu a ıklamıřtır. Webroot, 2005 yılı boyunca 420 binden fazla web sitesinde casus yazılım tespit etmiřtir. Casus yazılımlar bu kadar etkin ve yaygın olduęu i in, bu konuda alınması gereken tedbirlerin ve yapılacakların belirlenmesi gerekmektedir. Casus yazılımlar, ilgili sisteme bulařtıktan sonra bulařtıęı yerde arka planda iřlevini s rd rmeye devam etmektedir. Fakat  oęu zaman, casus yazılım olgusunu dile getirmek bazı  nemli ve genel belirtiler ortaya  ıkarmaktadır.

Eęer;

- Kullandıęınız bilgisayar bařlamada bařarısızlıęa d ř yor ya da kısa zamanda durduk yere yavařlama eęilimi g steriyorsa,
- Web sayfalarında gezinirken sizin istemedięiniz web siteleri karřınıza  ıkıyorsa,
-  nternete girmek istedięinizde sizin istedięiniz sayfa deęil de s rekli reklam i erikli sayfalar geliyor,
- Tarayıcınızın yer imi y da sık kullanılanlar b l m nde tarafınızca ekledięiniz farklı web site baęlantıları ekliyse,
- Tarayıcınıza bařlangı ta ayarladıęınız web sitesi olan ‘‘Bařlangı  Sayfası’’, sizin ayarlanmadıęınız farklı bir web sitesine y nleniyorsa ve bu ayarı tarafınızca deęiřtirseniz de yine farklı web siteleri ortaya  ıkıyorsa,
- Tarayıcınızda daha  nce sizin tarafınızdan g rmedięiniz yer imi varsa,
- Ara   ubuęunuzda daha  nce g zlemedięiniz bir uygulama simgesi varsa,
- Kullanmakta olduęunuz bilgisayarda bir iřlem olmadıęı zaman birden ortaya  ıkan ve size hitap eden tanıtım sayfaları  ıkıyorsa,
- Tarayıcınızda bazı tuřlar ( rneęin bir web sayfası formu doldururken bir sonraki yazım alanına ge mek i in kullandıęınız sekme tuřu) kullanılmıyorsa,
- Kullanmakta olduęunuz bilgisayar  alıřmakta iken bilgisayarınızın hard diski hareketlilięini g steren ıřık devamlı yanıp s n yorsa,

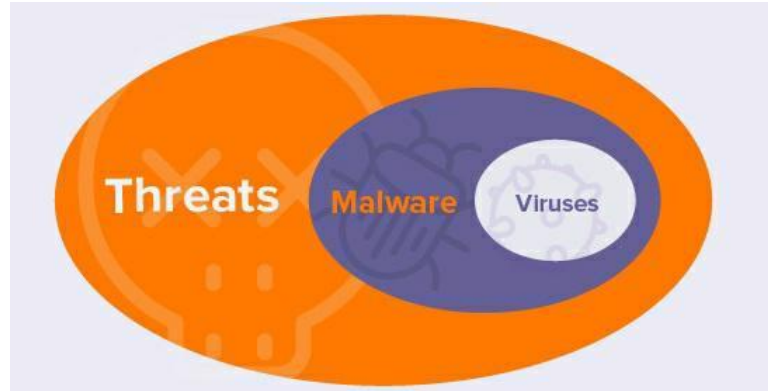
- Kullanmakta olduğunuz bilgisayarda herhangi bir işlem olmadığı anda araç çubuğundaki ağ bağlantısını gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren ışıklar yanıp sönüyorsa,

- Bilgisayar kasasındaki dâhili CD-RW sürücüsü kendiliğinden açılıp kapanıyorsa,

- Bilgisayar ekranınıza durup dururken hata iletileri geliyorsa,

Sistemde çok büyük ihtimalle casus yazılım bulunmaktadır. Sistemine casus yazılımın bulaştığını bu tür bulgular sonucunda farkedene bir kullanıcının aklına gelen ilk soru “Acaba bu yazılım sistemime nasıl bulaştı?” olacaktır [54].

Sıradan bir tarayıcı casus yazılımları algılayıp, kaldırmanıza yardımcı olabilmektedir. Günümüzde kötü amaçlı yazılımları ve virüsleri birbirinin yerine kullanmak yaygın bir uygulamadır. Fakat bunlar aynı şeyler değildir. Aradaki fark, kötü amaçlı yazılımın ana terim olması ve virüsün bir tür kötü amaçlı yazılım olabilmesidir. Basit bir ifadeyle, bir virüs kötü amaçlı yazılım olabilir, ancak tüm kötü amaçlı yazılımlar bir virüs olmamaktadır. Bir “Venn Diyagramı” olarak temsil edilirse, aşağıdaki şekle benzeyecektir. Virüs, bir tehdidin alt kümesi olan kötü amaçlı yazılımın alt kümesidir.



Şekil 5.3 Virüs Tehdidi Altkümesi

5.2 Sistemde Virüs Veya Kötü Amaçlı Yazılım Olduğu Nasıl Anlaşılır?

Bir virüs çoğunlukla bir dosyaya bulaşır ve kendisini diğer dosyalara çoğaltır. Bununla birlikte, virüs kötü amaçlı yazılım olarak dağıtıldıysa, en yaygın gösterge sisteminizin yavaşlaması olacaktır. Bazıları sabit sürücünüzdeki mevcut tüm depolama alanı dolana dek kendini çoğaltır ve bilgisayarınızı bir tuğlaya dönüştürür. Bazıları verilerinizi

çalışmaz hale getirip, bilgisayarınızın stabilitesini bozmaktadır. Ve hatta bazıları bilgisayarınızdaki kişi listesini kullanarak kendini başka bilgisayarlara da yaymaya çalışır. Tabii tüm bunların yanında yazılımın uzaktan erişim için bir altyapı kurabileceği de söylenebilir. Normal bir durum olarak kimse virüs bulaşmış bilgisayara sahip olmak istemez. Bu nedenle güvenilir alışkanlıklar edinmek ve bilindik antivirüs yazılımlarını kullanmak önemlidir. Neredeyse tüm kötü amaçlı yazılımlardan biraz dikkat ve biraz bilgi ile kaçınılabilmektedir. Antivirüs yazılımınız da güncelse bilgisayarınızın çok iyi durumda olduğu söylenebilir. Yine de çeşitli durumlarda bu kötü amaçlı yazılımlar savunmamızı aşabilir. Belki antivirüs yazılımınız güncel değildir ya da zekice hazırlanmış bir kod parçası ile atlatılmıştır. Belki de yanlışlıkla bir bağlantıya tıklanmıştır. Ya da başka birisi bilgisayarınızı kullanıp kötü amaçlı yazılımlar indirmiştir. Genellikle bir virüs söz konusu olduğunda antivirüs yazılımınız alarm durumuna geçip size bilgi verecektir. Ancak çeşitli durumlarda atlamalar olabilmektedir. Böyle bir durumda ilk olarak “Bilgisayarınızda virüs olup olmadığını anlatan bir işaret var mı?” sorusu akla gelmektedir. Aslında, bilgisayarınızda kötü amaçlı yazılımların varlığını gösterebilecek birkaç işaret bulunmaktadır [55].

- Bilgisayarınızdaki çökmeler ve donmalar virüse işaret eder.
- Bilgisayarınızdaki sürücüye erişim engeli virüse işaret eder.
- Bilgisayarınızdaki kaybolan dosyalar virüse işaret eder.
- Bilgisayarınızdaki sizce yüklenmeyen programlar virüse işaret eder.

5.3 Antivirüs Ve Kötü Amaçlı Yazılımdan Korunmak Gereklimi?

Bugün, virüsten koruma ve kötü amaçlı yazılımdan koruma çözümleri aynı şeydir. Hiçbir sağlayıcı yalnızca virüsleri kontrol etmez. Solucanları, truva atları, fidye yazılımları gibi diğer kötü amaçlı yazılımları taramayan bir çözüm sunmazlar. İyi bir güvenlik çözümü, sistemdeki yerel dosyaları tarayacak ayrıca e-posta ve internette gezinme yoluyla çevrimiçi etkinlikleri gözlemleyecektir. Kötü niyetli bir web sitesine ziyarette bulunursanız güvenlik çözümü tarayıcının yüklenmesine izin vermeyecektir.

5.4 Kötü Amaçlı Yazılımlardan Koruma

Sisteminize virüs bulaştığı düşünülüyorsa yapılması gereken birkaç şey vardır. Bunlar bazıları şu şekildedir:

5.4.1 Antivirüsünüzü Kurun / Güncelleyin

Bir antivirüs çözümü yok ise, bir tane satın alınmalı ve hemen kurulmalıdır. Sisteminizin sağlığı ve içerdiği önemli veriler için ödenmesi gereken küçük bir bedeldir. Diğerlerinin yanı sıra “Norton Security, Kaspersky, McAfee ve Avast” gibi sağlayıcılara genellikle güvenilmelidir. Bu çözümlerin çoğu 4,5 yıldızla derecelendirilmiştir. Virüsten koruma yazılımını yükledikten sonra derinlemesine bir tarama yapılmalı ve çok zaman alsa bile çalışmasına izin verilmelidir. Tek sorun, kötü amaçlı yazılımın çok gelişmiş olmasıdır, antivirüsün nasıl devre dışı bırakılacağını bilir. Zaten bir antivirüs çözümünüz varsa ve kötü amaçlı yazılımı tespit edemediyse, bu çoğunlukla programı güncellemediğiniz anlamına gelmektedir. Bu süreç yalnızca bir antivirüs çözümü yüklenerek bitmez. Her gün yeni kötü amaçlı yazılım geliştirilir. Bu nedenle, yeni kötü amaçlı yazılımı algılayabilmeleri için antivirüs programlarının güncellenmesi gerekmektedir. Virüsten koruma yazılımı güncellenmediğinde bir gün bile geçse sistemi yeni kötü amaçlı yazılımlara açık hale getirilmiş olunur.

5.4.2 Sistem Geri Yükleme

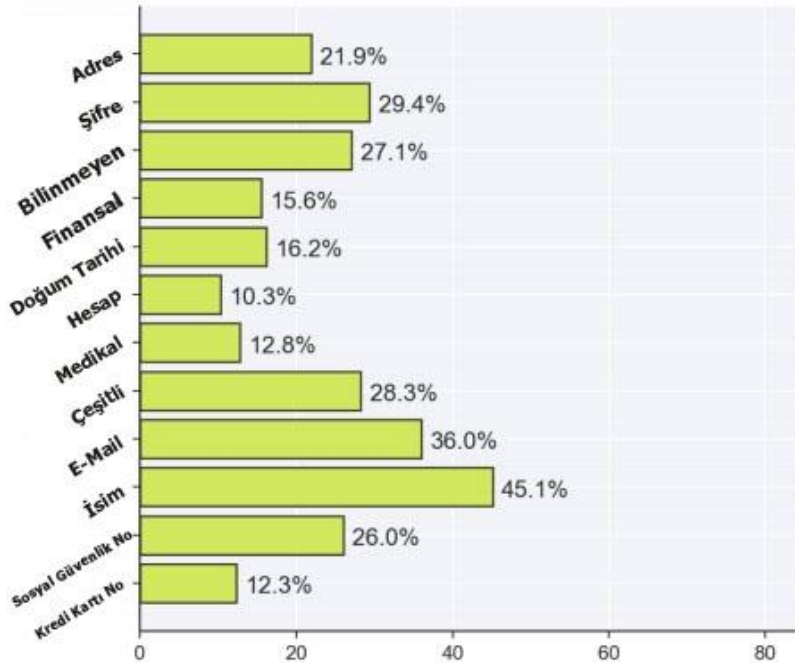
Microsoft Windows gibi çoğu işletim sistemi, sistem geri yükleme adı verilen bir özelliğe sahiptir. Bu, temel olarak tüm sistemin bir yedeğini düzenli aralıklarla depolamaktadır. Sisteme bugün kötü amaçlı yazılımlar bulaştıysa ve dün için kullanılabilir bir sistem geri yükleme noktası varsa, sistem dün olduğu gibi geri yüklenebilmektedir. Bu da kötü amaçlı yazılımı kaldıracağı anlamına gelmektedir. Ancak bazen kötü amaçlı yazılım kodu, sistem geri yüklemesini çalıştırılmasına izin vermeyecek şekilde yazılır. Bu gibi durumlarda, güvenli modu etkinleştirmek için sistemin yeniden başlatılması ve ardından bir sistem geri yükleme noktası çalıştırılması gerekmektedir.

5.4.3 İnternet Bağlantısını Kesin

Sistemde bilgi çalmak için kullanılan kötü amaçlı yazılım varsa, bu birisinin İnternet üzerinden onu uzaktan kontrol ettiği anlamına gelmektedir. Bununla başa çıkmanın ilk adımı İnternet bağlantısını tamamen kesmektir. Ethernet kablosunu çıkarılmalı, Wi-Fi devre dışı bırakılmalıdır. Hatta gerekirse modem kapatılmalıdır. İnternet bağlantısı kesildiyse antivirüs güncellenmeyeceği iddia edilmektedir. Antivirüs bir çevrimdışı-offline çözüm yoluyla yüklenmelidir. En azından, saldırgan artık bilgisayara, tablete, erişemeyecektir.

5.4.4 Taşınabilir Bir Antivirüs Çözümü Edinin

Her şey başarısız oluyorsa ve antivirüs kurmanıza bile izin verilmiyorsa, bu kötü amaçlı yazılımın işletim sisteminin kontrolünü ele geçirdiği anlamına gelmektedir. İşletim sistemiyle uğraşmak zorunda kalmadan kontrolü ele almanın bir yolunun bulunması gerekmektedir. Bu gibi durumlarda, bir USB sürücüsüne yüklenebilen, taşınabilir offline-çevrimdışı antivirüs çözümleri kullanılmalıdır. Bunlardan bazıları “ClamWin, Kaspersky Security Scan, McAfee Stinger ve Microsoft Safety Scanner'dır.” Aslında, bunların tümü bir USB sürücüsünde tutulabilir ve herhangi bir çakışmaya neden olmadan ayrı taramalar yapılabilir. Kötü amaçlı yazılımın bulaşmasının sonucu tekrar başlangıç da zor olacaktır. Soyulmuş bir evde yaşamak için geri dönmek gibi nitelendirilebilmektedir. Tekrar güvende hissetmek zaman alacaktır. Sistem geri yüklendiğinde, sistemin güvenliğini artırmak için adımlar atılmalıdır. Biraz maliyetli olsalar bile en iyi güvenlik çözümleri satın alınmalıdır. Ayrıca, istenmeyen yazılımlar düzenli aralıklarla kaldırılmalı ve geçici dosyalar silinmelidir. Bu süreçten sonra daha titiz ve dikkatli olunmalıdır.



Şekil 6.3 : 2020 Yılında Q3 tarafından bildirilen Fidye Yazılımı ihlallerinde açığa çıkan veri türleri

Data Type	2020	2019	2018
E-Mail	36%	64%	46%
İsim	45%	29%	36%
Şifre	29%	58%	42%
Bilinmeyen	27%	11%	14%
Çeşitli	28%	23%	19%
Sosyal Güvenlik No	26%	15%	19%
Adres	22%	14%	20%
Doğum Tarihi	16%	9%	12%
Finansal	16%	8%	12%
Medikal	13%	7%	9%
Kredi Kartı No	12%	12%	15%
Hesap	10%	9%	7%

Şekil 6.4 : 2020 Yılında Q3 tarafından bildirilen Yıllara göre Tüm ihlallerde açığa çıkan veri türleri

6.BİR SOSYAL MÜHENDİSLİK SALDIRISI NASIL TESPİT EDİLİR VE DURDURULUR

Sosyal Mühendislik, insanları size onlar hakkında ihtiyacınız olan bilgileri vermeleri için manipüle etme veya kandırma sürecidir. Siber suçlular her türlü bilgiyi ararlar, ancak en yaygın olanları, banka bilgileri, çeşitli uygulamalara giriş kimlik bilgileridir. Bilgisayarınıza erişmek ve şifrelerinizi ifşa etmeye ikna etmek için sosyal mühendislik kullanılır. Bu bilgileri, kendi hesaplarınızdan kendi hesaplarına para aktarmak veya sisteminize kötü amaçlı yazılım yüklemek için kullanılır. Siber suçlular; sosyal mühendisliğin, bir kişinin güvenini kazanmanın bilgisayara fidye yazılımı yüklemekten daha kolay olduğunu bilirler. Örneğin, herhangi bir kurbanı şifresini vermek üzere manipüle etmek için basit konuşmaları kullanılır. Bir şifre veya başka bir teknik işlem kullanarak sistemi hacklemeye çalışmazlar. Kullanıcının zayıf bir şifresi varsa sisteme saldırabilirler. Güvenliğin temel ilkesi kime ve neye güvenileceğini bilmektir. Bir kişiye ne zaman güvenileceğini bilmeli ve onlarla iletişim kurduğunuzda, göz teması kuramayacağınız için uyanık olmak gerekir. Bu, güvenilen uygulamalar için de geçerlidir. Sisteminize veya web sitenize indirip yüklediğiniz bir uygulamanın orijinal olup olmadığını ve size zarar verip vermeyeceğini bilmeniz gerekmektedir [56].

Herhangi bir güvenlik uzmanı, işletmelere, bir güvenlik zincirindeki en zayıf halkanın, başka bir kullanıcıyı itibari değerde kabul eden ve ona güvenen bir kullanıcı olduğunu söylemektedir. Basit bir deyişle, eviniz için çoklu kilitler, bekçi köpekleri, projektörler, alarm sistemleri, dikenli teller, çitler vb. ile birinci sınıf güvenliğinizin olması fark etmez. Eğer bir yabancının sadece tesisatçı olduğunu iddia ettiği için evinize girmesine izin verirsiniz, herhangi bir kontrol yapmadan evinize girme tehdidi güçlendirilmektedir.

6.1 Sosyal Mühendislik Metodolojileri

Sosyal mühendislik için kullanılan üç tür metodoloji vardır:

- Kimlik avı
- Vishing
- Kimliğe Bürünme

Kimlik Avı ve Vishing, daha önce ayrıntılı olarak önceki bölümlerde anlatılmıştı. Ancak, ‘‘Kimliğe Bürünme,’’ bir saldırganın zaten tanıdığınız biri gibi davranarak ve sizi kandırarak bilgisayarınıza, ağınıza vb. erişim sağlamasıdır. Saldırgan, kimliğe bürünme tekniğini hesaplarınızı ve sistemlerinizi hacklemek için kullanmadan önce çok fazla araştırma yapar. Saldırganlar, insanları sosyal medyada ve şirket web sitelerinde takip eder ve kurbanın arkadaşları ve meslektaşları hakkında bilgi toplarlar. Ayrıca konuşmalarınızı dinler ve çöpe attığınız belgeleri incelerler.

6.2 Bir Sosyal Mühendislik Saldırısını Tespit Etme

Bir sosyal mühendislik saldırısının genellikle nasıl yapıldığını anlamak zor değildir. Sosyal mühendisliğin nasıl çalıştığını anlamak için bazı yaygın senaryolar vardır.

6.2.1 Bir Arkadaştan E-posta

Saldırgan, bir kullanıcının e-posta şifresini yazılım veya sosyal mühendislik yoluyla ele geçirmeyi başarır, o kullanıcının kişi listesine erişebilir. Çoğu kullanıcının çok sayıda web uygulaması veya sosyal medyası için aynı şifreyi kullandığı bilinmektedir. Saldırgan kullanıcının sosyal medyasına ve sosyal medyadaki kişilerine de erişebilir. Bundan sonra her şey saldırgan için kendi alanıdır. Kullanıcının kişi listesine e-postalar veya sosyal medyadan anlık mesajlar gönderebilir. Saldırgan tarafından gönderilen mesajların çoğu aşağıdaki özelliklere sahiptir:

- Saldırgan arkadaş gibi davranarak, ilgili olabileceğiniz bir şey söyleyip sizi heyecanlandıran bir URL’den bahsedebilir. Size bir bağlantı gönderebilir ve bu bağlantı aracılığıyla sizden bazı bilgiler vermenizi isteyebilir. Şüphesiz ve masum. Çünkü bir tanıdığınızdan geliyor. Bağlantıya tıklanıyor ve bilgisayara bulaşan kötü amaçlı yazılımlar indiriliyor. Artık sisteme erişebilir ve istediği herhangi bir işlemi gerçekleştirebilir. Saldırganlar kişi listenizdekiler hakkında bilgi toplamaya ve sizi aldattıkları gibi onları da aldatmaya çalışacaklardır. Türkiye’de sosyal medya mesajlaşmalarında genellikle ‘‘Hediye çeki dağıtıyorum.’’ yalanıyla telefon numarası istenmekte ve bu sayede kişiler dolandırılmaktadır.
- Dosya içeriğine kötü amaçlı kod parçacığı gizlenmiş bir görüntü, video veya müzik dosyası olduğu bir mail yollanmıştır. Dosya bir arkadaşınızdan geldiği için tereddüt etmeden indirilir ve sonunda sisteminize kötü amaçlı yazılım bulaşmış olur. Saldırganın artık bilgisayarınıza ve üzerinde bulunan verilere erişimi vardır [57].

Bu tip saldırılardan korunmak için tüm sosyal medya şifrelerinin aynı yapılmaması gerekmektedir. Her biri için ayrı ve güçlü parola belirlemek daha güvenli olacaktır. Eğer yapılabiliyorsa two faktör güvenlik önlemi alınmalıdır. Bu sayede saldırgan sadece sınırlı sayıda kitleye ulaşacaktır. Kimden gelirse gelsin yakın akrabalarınızdan bile olsa gönderdikleri dosyayı bilgi almadan indirmemeli veya farklı bir işlem yapmamalıdır.

6.2.2 Güvenilir Bir Kaynaktan Bir E-posta

Sosyal mühendislik, saldırganların hassas bilgileri ifşa etmek, kullanıcıları kandırmak için güvenilir bir kaynağı taklit ettikleri kimlik avı saldırısıdır. Webroot'tan gelen raporlar, çoğu saldırganın finansal kurumların kimliğine büründüğünü gösteriyor. Verizon'dan gelen veriler, bugün meydana gelen ihlallerin %93'ünün başarılı bir sosyal mühendislik girişiminin sonucu olduğunu da göstermektedir.

Güvenilir kaynaklardan gelen e-postalar aşağıdaki temalara sahip olabilir:

E-postalar acil yardım isteyebilir: Bazı e-postalarda acil mesajlar olabilir ve aciliyet duygusu sizi e-postadaki eylemi yapmaya zorlayabilir. Korktuğunuz için, parayı saldırganın hesabına aktarabilirsiniz.

E-posta, bir amaç için bağış isteyebilir: E-postalar cömertliğinizi veya nezaketinizi istismar etmeye çalışabilir. İçerik, bir vakfa veya amaca yönelik bir miktar fon aktarmanız gerektiğini söyleyebilir, ancak para doğrudan saldırganın hesabına gitmektedir.

Gerçek bir arka plan kullanan kimlik avı girişimleri: Bir saldırgan size para göndermenizi isteyen bir mesaj veya e-posta gönderebilir. Mesajın veya e-postanın kaynağı tanınmış bir şirket, okul veya kurum olabilir izlenimi verilebilir.

E-posta bir sorun olduğunu söyleyecek ve düzeltmek için bir bağlantıya tıklamanızı isteyecektir: E-postayı göndermek için kullanılan URL gerçekmiş gibi görünebilir. E-postanın gövdesinde saldırganın aitmiş gibi davrandığı kuruluşa benzer bir logo kullanılabilir. Saldırganın e-postayı doğrudan kaynak web sitesinden göndermesi, ancak bu web sitesine erişmek için farklı yöntemler kullanması mümkündür. Her şey yasal görüldüğünden, sizi saldırganın web sitesine yönlendiren URL'ye tıklayabilirsiniz. Saldırgan, hesabınıza girmek için ihtiyaç duyduğu bazı bilgileri isteyen bir form sunacaktır. E-posta ayrıca, URL'yi tıklamazsanız sonuçların ne

olabileceğini söyleyen bir uyarı da içerir. Bunun amacı sizi korkutarak bağlantıya tıklamanızı sağlamaktır.

Yöneticiniz veya meslektaşınız gibi davranmak: E-posta, ofisinizde üzerinde çalıştığınız bir projenin ayrıntılarını içerebilir. Bu güveninizi kazanmak için yapılmış bir harekettir. Bir sonraki bölüm, geçmişte yapmış olduğunuz bir şirket kartını kullanarak bir tür ödeme ile ilgili olacaktır. Bunun doğru olduğuna inanıyorsunuz ve ödemeyi yapıyorsunuz.

Sana bir şey kazandığını söyleyen bir posta: Ölen bir akrabanızdan, bir piyango şirketinden veya başka herhangi bir işletmeden e-posta almış olabilirsiniz. Bazı e-postalar, web sitesini ziyaret eden 100. kişi olduğunuzu ve bir şey kazandığınızı da söyleyebilir. E-posta, kim olduğunuzu kanıtlamak için sosyal güvenlik numaranız gibi bazı hassas belgeler sağlamanızı ister. Bu istekler sizi şüpheli kılmalıdır. E-postalara güvenmeyin. Bu tür saldırı, açgözlülük kimlik avı olarak bilinir. Açgözlü olduğunuz için saldırganlara gerekli bilgileri vermek isteyebilirsiniz. Sonuç olarak, saldırganın banka hesabınızı boşaltmak için kullanabileceği hassas bilgileri ona sunmuş olabilirsiniz.

Ücretsiz film ve müzik indirme: Bu sosyal mühendislik senaryosunda, saldırganlar, özellikle hassas bilgiler elde etmek istiyorlarsa kullanıcıyı tuzağa düşürebileceklerini bilirler. Bu tür yemler genellikle ücretsiz filmler veya müzik indirmeleri sunan web sitelerinde bulunur. Saldırganlar bu tür dolandırıcılıkları kötü amaçlı web sitelerinde, sosyal medyada ve çoğu kullanıcının arama sonuçlarında rastladığı diğer web sitelerinde çalıştırabilir.

Tuzak planı; bir telefon satmayı teklif eden bir web sitesinde de ortaya çıkıyor: Gerçek maliyeti 1.000 TL olan telefon için sizden yalnızca 100 TL istenmiş olması dikkat düşündürücüdür. Şüphelenebilirsiniz, birçok kullanıcıdan teklifin doğru olduğunu ifade eden yorumlar yapılmış gibi gösterilmektedir. Saldırgan bunu şüphelerden uzak olunması için zekice tasarladı. Bu yemlemeden hoşlanan kullanıcılar bilgisayarlarına kötü amaçlı yazılım indirir. Bu sayede kullanıcı hakkındaki ayrıntıları ve iletişim kurduğu diğer kullanıcılar hakkındaki diğer verileri ortaya çıkarır. Onlara 100 TL ödeyebilirsiniz, ancak karşılığında vaat edilen telefonu asla alamazsınız.

Sormadığınız Soruları Yanıtlamak: Saldırganlar, bazen bir şirketten avantajlar sağlamak ve yardım etmek için sizinle iletişime geçerler. Size gelen E-posta kimliği,

tanınmış bir şirket veya bankaya benziyor olabilir. Ürünün tüketicisi değilseniz, e-postayı silersiniz. Ancak, ürünü kullanıyor olma ihtimaliniz yüksektir. Aslında yardım için şirketle iletişime geçmeniz planlanıyordur. Örneğin, işletim sisteminizdeki bir sorunla ilgili yardım istenmiş olunabilir, ancak aniden Microsoft'tan bir e-posta gelir. E-posta, sorunu ücretsiz olarak çözmeyi teklif etmektedir. Onlara yanıt verirsiniz ve onlara güvenirsiniz, kendinizi saldırganın önceden planladığı çeşitli istismarlara açmış olursunuz. Saldırgan sizden kimliğinizi doğrulamanızı, sistem veya uygulamada oturum açmak için gerekli bilgileri sağlamanızı isteyecektir. Diğer zamanlarda, sorunu çözmek için sisteminizde birkaç komut çalıştırmanız istenebilir. Bunu yapmalarına izin verdiğinizde, sisteminize erişirler.

Güvensizlik Yaratma: Bazı sosyal mühendislik uygulamaları yalnızca güvensizlik veya çatışmalar yaratmak için uygulanır. Bunlar tanıdığınız ve sorun yaşayan kişiler tarafından ya da dünyanın yanmasını izlemekten zevk alan kişiler tarafından yapılır. Bu saldırganlar, kafanızı tanıdığınız diğer insanların yanlış izlenimleriyle dolduracak ve ardından güveninizi kazanmak için kurtarıcı olarak gelecektir. Bu tür kötü uygulamalar, başlangıçta sizi manipüle etmek ve daha sonra size saldırmak isteyen gaspçılar tarafından da kullanılır. Bu tür bir sosyal mühendislik saldırısı hesaplarınızdan birine erişim sağlayarak başlatılır. Bu, şifrenizi kırarak, sosyal mühendislik yaparak veya sadece şifrenizi tahmin ederek elde edilebilir.

Artık sosyal medyanıza, videolara ve resimler gb uygulamalara erişimi olan saldırgan, bunları ihtiyaçlarına göre düzenler ve güvensizlik ortamı yaratmak için kişilerinize iletebilir. İçeriği yanlışlıkla iletili gibi davranırlar. Saldırgan, çalınan medya içeriğini saldırıya uğrayan kullanıcıya şantaj yapmak için de kullanabilir [58].

Sosyal mühendislik saldırılarının birçok çeşidi vardır. Saldırganın hayal gücü, birisini sömürme yöntemlerinin tek sınırır. Tek bir saldırı, birden fazla sayıda istismar içerebilir. Saldırgan, daha sonra istismar edilebilmeniz için bilgilerinizi sizden hoşlanmayan kişilere para karşılığı satabilir.

6.3 Sosyal Mühendisliğe Düşmekten Nasıl Kaçınılır?

Bir sosyal mühendislik saldırısının raf ömrü kısadır ve başarılı olması için sadece birkaç kullanıcıya ihtiyacı vardır. Ancak kendinizi buna karşı koruyabilirsiniz. Çoğu zaman çevrenizden haberdar olmanız gerektiğinden çok fazla çaba gerektirmez.

6.3.1 Ağırdan Almak

Bazı saldırılar karşısında durmak ve biraz düşünmek iyi bir fikirdir. Saldırganlar, düşünmeden acilen hareket etmenizi beklemektedirler. Çoğu sosyal mühendislik saldırısı sizi acil görünen bir duruma sokar. Bu, durumu doğru bir şekilde yavaşlatmak ve gözden geçirmek için ipucunuz olmalıdır.

6.3.2 Araştırmaya Biraz Zaman Harcayın

Bildiğiniz birinden veya güvendiğinizi düşündüğünüz bir işletmeden e-posta alabilirsiniz. Sadece e-postanın gövdesi değil, aynı zamanda "gönderen" adresi, imzası vb. iyice gözden geçirilmelidir. Şirketi tanımıyorsanız, gerçekten var olup olmadıklarını görmek için basit bir araştırma yapılmalıdır.

6.3.3 Bağlantılara Körü Körüne Tıklamayın

E-postada bir bağlantı alırsanız, bağlantıya tıklamayın. Bir arama yoluyla bu web sitesi URL'sini bulmak için biraz çaba sarf edin ve temel URL'nin sizi nereye götürdüğünü görün. Bu şekilde, bağlantının kontrolü sizde olacaktır. Bunun tersi olması durumunda araştırılmadan tıklanan linkler, kötü niyetli kişilerin amaçlarına ulaşmalarını sağlayacaktır.

6.3.4 E-posta Hack'lerinin Farkında Olun

Saldırganlar e-posta hesaplarını ele geçirir ve saldırıya uğramış hesabın kişi listesindekilerin güvenlerine dayanarak saldırıda bulunurlar. Bu nedenle, tanınan birinden bir e-posta alındığında, bu mailin beklenip beklemediğinin sorulması gerekmektedir. Postayı beklemediyseniz postadaki herhangi bir bağlantıya tıklamayın. Kişiyi aramak ve size postayı gerçekten gönderip göndermediğini doğrulamak güvenli bir seçenektir.

6.3.5 Körü Körüne İndirme

Göndereni tanımıyorsanız, e-postadaki hiçbir eki indirmeyin. Eklerin ne olduğuna özellikle dikkat edilmelidir. Uzantılarına bakılmalı exe, pdf ya da makro çalışacak, çalışabilme ihtimali olan hiçbir ek indirilse bile çalıştırılmamalıdır.

6.3.6 Piyangoların Sahte Olduğunu Bilin

Kimse size bedavadan bir sürü para vermiyor. Yani, bir e-posta alırsanız özellikle herhangi bir yarışmaya katılmadan bir şey kazandığınızı söylemek bir aldatmacadır.

Klasik bir örnek, Harry Potter ve Zümrüdüanka Yoldaşlığından Tonks'un Dursley'lere en iyi çim için bir yarışma kazandıklarını söyleyen bir mektup gönderdiği sahnedir. Bunu sadece Dursley'ler Harry'yi Kovuk'a götürmeye çalışırken yollarına çıkmamaları için yaptı. Böyle bir e-posta alırsanız sahtedir ve tedbirli olunması gerekmektedir.

6.3.7 Banka Dolandırıcılıklarına Dikkat Edin

Size gelen bir e-posta kişisel bilgilerinizi ve banka bilgilerinizi soruyorsa, büyük olasılıkla bir dolandırıcıdır. Bu e-postayı silin, ayrıca bu gönderenden gelecek tüm e-postaları almamak için bir filtre oluşturun.

6.3.8 Yardım Tekliflerini Reddet

Gerçek şirketler sizinle proaktif olarak iletişime geçmezler. Herhangi birinden e-posta alırsanız, sohbeti başlatmadığınızda, özellikle aşağıdakileri yapabileceklerini söylerlerse bu bir aldatmacadır:

1. Kredi puanınızı iyileştirmenize yardımcı olmayı teklif eder.
2. Sisteminizdeki bir uygulamayı veya yazılımı düzeltmeyi teklif eder.

Bir hayır kurumundan tanımadığınız bir e-posta veya mesaj alırsanız silinmelidir. Bir hayır kurumuna gerçekten bağış yapmak istiyorsanız, biraz araştırma yaparak meşru bir hayır kurumuna bağışta bulunulmalıdır.

6.3.9 Spam Filtrelerinizi Yapılandırın

İstenmeyen posta filtreleri, e-postaları meşru veya istenmeyen posta olarak sınıflandırmanıza yardımcı olan bir özelliktir. Biraz zaman ayrılmalı ve spam filtreleri güncellenmelidir. Yalnızca istenilen e-postalara izin vermek için kurallar belirlenmelidir. E-posta sağlayıcınız aracılığıyla istenmeyen posta filtrelerinizi nasıl ayarlayacağınıza dair kılavuzlar vardır. Otuz dakika kadar kısa bir zaman ayırımı, "e-posta hayatınızı" sonsuza kadar kolaylaştıracaktır.

6.3.10 Tüm Cihazlarınızı Koruyun

Tüm cihazlara virüsten koruma ve kötü amaçlı yazılımdan koruma programları yüklenmelidir. Yazılım rutin bir tarama yapacak şekilde ayarlanmalıdır ve gelen herhangi bir e-posta için gerçek zamanlı taramalar çalıştırılmalıdır. Otomatik güncelleştirmeleri etkinleştirerek işletim sisteminin ve diğer yazılımların güncel tutulması sağlanmalıdır.

7.AĞ GÜVENLİĞİ VE KORUMA TEKNİKLERİ

Ağ güvenliği siber dünyada korunması gereken en önemli varlıklardandır. Yıkıcı bir kaybı önlemek istiyorsanız ağınıza güvenli hale getirmeniz gerekmektedir.

7.1 Ağ Güvenliği

Ağ güvenliği, çeşitli süreçleri, teknolojileri ve cihazları kapsayan genel bir terimdir. Ağ güvenliği, bilgisayar verilerinin bütünlüğünü, erişilebilirliğini ve gizliliğini güvence altına almak için önemlidir. Bu önem herhangi bir web uygulamasının veya aracın hem donanım hem de yazılımındaki kurallarının ve politikalarının yapılandırılmış halidir. Bu, ağ altyapısıyla yakından ilişkilidir. Bilgisayar verileri ve ağları çok sayıda siber saldırıya karşı savunmasızdır. Bu nedenle, büyüklüğü, altyapısı veya endüstrisi ne olursa olsun her işletmenin yerinde ağ güvenliği önlemleri olması gerekmektedir. Ağ mimarisi her geçen gün gelişmekte ve daha karmaşık hale gelmektedir. Sistemdeki güvenlik açıklarından yararlanmak için daha yeni yöntemler bulmaya çalışan saldırganlar vardır. Bunlar sürekli olarak değişmekte ve kendilerini yenilemektedir [59].

Güvenlik açıkları, veriler, cihazlar, uygulamalar ve kullanıcılar gibi ağ altyapısının çeşitli varlıklarında bulunur. Bu göz önüne alındığında, bu varlıkları güvence altına almak için ayrı araçlar mevcuttur. Bu araçlar, işletmenin şartlarına uygun olduğundan emin olmak için uygulamaları test etmek de kullanılır. Birkaç dakikalık kesinti süresi bile kuruluşun itibarına ve maliyesine zarar verebileceğinden, ağ güvenliği son derece önemlidir.

7.2 Ağ Güvenliği Nasıl Çalışır?

Bir kuruluştaki ağ güvenliğinin birden çok katmanı vardır. Bir saldırgan, ağ güvenlik modelindeki herhangi bir katmanı hedef alabilir. Bu nedenle, işletmelerin savunmasız alanların üstesinden gelmek için hem donanım hem de yazılım için ağ güvenlik modellerini tanımlamaları gerekmektedir.

7.3 Ağ Güvenliğinin Faktörleri

Ağ güvenliği faktörleri üç kısımda incelenmektedir: Fiziksel, teknik ve idari.

7.3.1 Fiziksel Ağ Güvenliği

Bu konu, ağla ilgili farklı fiziksel erişim türleriyle ilgilenmektedir. Kablolar, modemler, anahtarlar ve yönlendiriciler gibi aygıtlardır. Bir kuruluş, yalnızca yetkili çalışanların, özellikle bilgi teknolojileri uzmanı veya ağ ekibinin bir parçası olanların bu bileşenlere erişmesini sağlamalıdır. İşletmenin erişime izin verebileceği bazı yaygın yollar; biyometri, güvenlik kilitleri vb. gibidir.

7.3.2 Teknik Ağ Güvenliği

Bu yöntem, bir ağda depolanan veya ağ üzerinden geçiş halindeki verilerin korunmasıyla ilgilidir. İşletme, verileri ve ilişkili sistemlerini yetkisiz erişime karşı korumak için iki yönlü koruma kullanmalıdır. Verilere, dahili çalışanların kötü niyetli faaliyetlerinden korumak için de özen gösterilmelidir. Dahili çalışanlar bunu kasıtlı olarak yapmayabilir, ancak şirket mülkünde kişisel bir USB sürücü kullanmak gibi eylemler bir tehdit içermektedir.

7.3.3 İdari Ağ Güvenliği

Bu özellik, kullanıcı davranışını kontrol altında tutmak için süreçler ve güvenlik politikaları ile ilgilenmektedir. Bu, kullanıcıların kimlik doğrulamasını ve kuruluştaki kullanıcının rolüne ve atamasına bağlı olarak erişim düzeyini içermektedir. Örneğin, bir banka yönetici kullanıcısının bir sunucuya veya ağ cihazına teknik erişime ihtiyacı yoktur.

7.4 Bir Ağ Üzerinden İşletmenizi Etkileyebilecek İlk Beş Saldırı

Önceki bölümlerde, farklı siber saldırı türlerini kısaca anlattık. Bu bölümde, bir ağ üzerinden işletmeleri yok edebilecek ilk beş siber saldırı türü anlatılmaktadır. İşe alımların planlanmasından müşteri ilişkileri yönetimine kadar, çoğu kuruluş tüm görevlerini çevrimiçi olarak gerçekleştirir. Otomasyon sistemleri, insan gücünü azaltmakta ve süreçleri çok daha verimli hale getirmektedir. Tüm sistemi kullanışlı hale getirerek siber saldırganlar için bir fırsat penceresi açmaktadır. “Stratejik ve Uluslararası Araştırmalar Merkezi” tarafından yayınlanan bir raporda, siber saldırıların neden olduğu hasarın yıllık 600 milyar dolar olduğu belirtilmektedir. Teknolojinin evrimi, saldırganların bir işletmeyi dolandırması için yeni yöntemler geliştirmesine yol açtı. İşte işletmelerin uğraşması gereken ilk beş siber saldırı türü şu şekilde sıralanabilir.

7.4.1 Gelişmiş Kalıcı Tehdit (APT)

Bu saldırının amacı, kuruluşun ağını ve yazılımını güvenlik açıklarına karşı taramak ve bu güvenlik açıklarını verileri çalmak için kullanmaktır. Gelişmiş ve kalıcı bir tehdit, uzun süre tespit edilemeyebilir. Bu saldırı, hükümet bilgilerini çalmak isteyen saldırganlar tarafından tasarlanmıştır. Salırganlar artık sistemden hassas bilgileri çalmak ve fidye talep etmek için bu yöntemi kullanmaktadırlar. Kuruluşunuzun gelişmiş kalıcı bir tehdidin kurbanı olup olmadığını belirlemenize yardımcı olacak bazı göstergeler şunlardır:

- Düzensiz Bilgi Akışı - Altyapının gelen veya giden trafikte ani bir artışa tanık olduğu fark edilmektedir. Veri akışı düzensiz bir modele sahiptir ve bu ağlar, sunucular veya sunucudan istemci bağlantıları arasında gerçekleşebilir.
- Veri Paketi Kullanımı - Gelişmiş bir kalıcı tehdit, çalınan verileri istenen bilgisayara aktarmadan önce bir araya getirir. Ağınız üzerinden büyük hacimlerde veri veya sıkıştırılmış veri aktarıldığı gözlemlenebilir, bu ağınıza virüs bulaşmış olabileceğini gösterir.
- Beklenmedik saatlerde artan kullanıcı girişi sayısı.
- Ağda ve ilişkili aygıtlarda arka kapı truva atları keşfi.

7.4.2 Hizmet Reddi Saldırısı (DoS)

Hizmet reddi saldırısı, gerçek bir kullanıcının banka hesapları veya e-posta hesapları gibi hizmetlerden erişimini engellemeye yönelik bir saldıdır. Bir saldırgan ağa ve sunucuya saldırarak ardından bant genişliğini gereksiz isteklerle doldurmaktadır. Bir Hizmet Reddi saldırısının nedeni herhangi bir bilgiyi çalmak değil, sunucuya veya web sitesine erişimi engellemektir. İşletmeler, bu durum nedeniyle büyük mali kayıplara uğratılmaktadır.

Bir kullanıcının çevrimiçi banka hesabına erişmeye çalıştığını varsayın. İnternet bağlantısı iyi olmasına rağmen bunu yapamamaktadır. Bu, hizmetin bir DoS saldırısı altında olduğunu ve gerçek kullanıcının hesaplarına erişiminin engellendiğini göstermektedir.

7.4.3 Nesnelerin İnterneti (IoT) Hacking

Nesnelerin interneti, internete doğrudan veya dolaylı olarak bağlanan cihazları ifade eder. Bu cihazlar, termostatlar, kilitler, kameralar, buzdolapları, temizlik robotları vb. gibi çeşitli IoT cihazlarını içerir. Bir saldırgan, bir işletmeye saldırmak için IoT cihazlarından yararlanabilir. Örneğin; işletmelerin güvenlikle güncellemeyi unuttuğu ve birçok güvenlik açığı içeren birkaç IoT cihazı vardır. Bir çalışanın akıllı saatini iş yerindeki bir bilgisayara bağladığı düşünülmektedir. Akıllı saatte güvenlik açıkları varsa, saldırgan iş yerindeki tüm altyapıya erişmek için bunları kullanabilir. Bir saldırganın bunlardan yararlanamamasını sağlamak için eski ve kullanılmayan IoT cihazlarındaki uygulamaların kaldırması gerekmektedir.

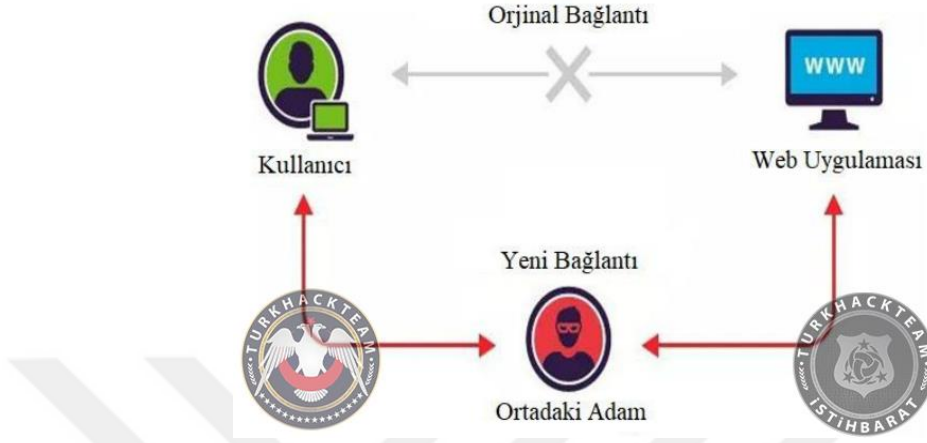
7.4.4 Yapılandırılmış Sorgu Dili (SQL) Enjeksiyonu

“Yapılandırılmış Sorgu Dili SQL Enjeksiyonu,” yıllar önce keşfedilen ancak günümüzde hala etkili olan bir hackleme yöntemidir. “SQL, Oracle, MySQL veya Microsoft SQL'de” programlanan veri tabanları ve tablolar üzerinde çalıştırılan bir dildir. Enjeksiyon, bu veri tabanlarından birini kullanan herhangi bir uygulamayı etkiler, ancak saldırganlar bu veri tabanlarını kullanan web sitelerini hedef almaktadır. Geçtiğimiz on yılda birçok SQL enjeksiyon saldırısı meydana geldi. Bir SQL enjeksiyon saldırısı başarılı olursa, saldırgan bir web sitesinin içeriğini değiştirebilir ve kullanıcı hesabı ayrıntıları gibi hassas bilgilere erişebilmektedir. SQL enjeksiyonunun iki aşaması vardır: İlk aşamada, saldırgan hedef altyapıyı gözlemler ve bunun hakkında olabildiğince fazla bilgi toplar. Bu aşama aynı zamanda “Keşif” olarak da bilinir. Bir sonraki aşama, saldırganın toplanan bilgileri hedef sisteme girmek için kullandığı saldırı aşamasıdır. Bir SQL enjeksiyon saldırısında, saldırgan, komutlarını yürütmek için bir SQL komutuna kötü amaçlı kod yerleştirir.

7.4.5 Ortadaki Adam

Ortadaki adam, üçüncü bir tarafın iki taraf arasındaki iletişimi durdurması yöntemidir. Saldırganın web siteleri, sosyal medya, e-postalar, haberciler vb. gibi verileri ele geçirmek için hackleyebileceği çeşitli çevrimiçi kanallar bulunmaktadır. Bu saldırıyı gerçekleştiren bir saldırgan, kişisel ve ticari faaliyetlere, verilere erişebilmektedir. Ortadaki adam saldırısında, bir mesajın ulaşması engellenebilir veya mesaj başka birine yönlendirilebilir. Çoğu iletişim uygulamasının uçtan uca şifreleme kullanmasının nedeni budur. Bu, bir mesaj gönderdiğinizde, bir algoritmanın düz

metni, şifreli karakterlere dönüştürdüğü anlamına gelmektedir. Alıcı bu komut dosyasını aldıktan sonra, cihazındaki algoritma, karakterlerin şifresini tekrar düz metinlere dönüştürür. Bu şekilde, bilgi, ortadaki biri tarafından ele geçirilse bile, şifresini nasıl çözeceklerini bilmedikleri için etkili olamaz [60].



Şekil 8.1 : Ortadaki Adam Saldırısı

7.6 Bir İşletmeyi Siber Saldırıdan Koruma

Birden fazla işletme düzenli olarak siber saldırılara maruz kalmaktadır. Çoğu saldırgan, güncel olmayan güvenlik özelliklerine sahip işletmeleri hedef almaktadır. İşte siber saldırılardan kaçınmanın çeşitli yolları:

- Donanım yoluyla siber güvenlik
- Yapılandırmalar ve ayarlar aracılığıyla siber güvenlik

7.7 Donanım Aracılığıyla Siber Güvenlik

Siber güvenlik dünyasında hem saldırı yapmak hem de saldırıları bertaraf etmek için gerekli donanımlara ihtiyaç duyulmaktadır. Bu donanımlar ne kadar kuvvetli olursa hem saldırmak hem de savunmak o derece etkili olmaktadır.

7.7.1 Güvenlik Anahtarları

İnsanların tüm hesapları için aynı parolaya sahip oldukları bir gerçektir. Ayrıca şifrelerin doğum yılları veya başka basit kelimeler olduğu genellikle tahmin edilir. Bu nedenle, şüphesiz siber güvenlik alanındaki en büyük güvenlik açığı insanlardır. Yubikeys aracı, çalışanların hesaplarına şifre kullanmadan erişmesine olanak tanır.

Ayrıca, deęiřtirmeleri gereken řifre sayısını ynetmeleri de gerekmez. Saldırganlar bu yazılımı hacklemek iin kaba kuvvet saldırıları kullanabildięinden, bu tr uygulamalar ok poplerlik kazanmaktadır. Doęru řifreyi bulana kadar farklı bir harf, sayı ve karakter kombinasyonu kullanabilirler. İřletmeler, hassas projelerde alıřan tm alıřanlar ve ekip yeleri iin bir anahtar satın almalıdır. Bunu yaptıklarında, anahtarı bir cihaza takıp gerekli aralara, uygulamalara, belgelere vb. eriřebilmektedir. oęu zaman, bir saldırgan, hassas bilgileri elde etmek iin bir alıřanı kimlik avı yoluyla da kandırabilmektedir. Maksimum hasara yol aan saldırılar, gvenlik bayraklarını atlayan ve herhangi bir alarm vermeyen sosyal mhendislik yoluyla kurulan tuzakların sonularıdır [61].

Deneyimli bir saldırgan, bir alıřan hakkında bilgi edinmeye ve onlar hakkındaki karmařık ayrıntıları ęrenmeye alıřır. Dzenli olarak iletiřim kurdukları kiřiler hakkında bilgi edinirler. Saldırgan daha sonra kurbanın tanıdıęı biri olarak kendini gizler ve tanıdıklarının e-postasına benzer bir kimlikten size bir e-posta gnderir. Saldırgan bu e-postaları, kurbanların hakkında bilgi almak iin kt amalı baęlantılara tıklamaya ikna etmek iin kullanmaktadır. Yubike'y'ler, bu tr senaryolardan kaınmaya yardımcı olmakta ve kt amalı dosyaları veya baęlantıları tanımlama gibi ek gvenlik zellikleri saęlamaktadır.

7.7.2 VPN Gvenlik Duvarları

Kapıları ve pencereleri kilitleyerek evinizi hırsızlardan korursunuz. Bu aynı zamanda evdeki insanların korumasına da yardımcı olmaktadır. Sisteminize ve aęınıza yetkisiz eriřimi nlemek iin sisteminizde ve aęınızda da bu kilitleri korumalısınız. oęu, "Bilgisayarımın yerleřik gvenlik duvarı beni korumaz mı?" gibi sorularla karřı karřıya kalmaktadır. Evet, kısmen korumaktadır ancak bir iřletmenin gvenlik taleplerini karřılamamaktadır. Konumdan baęımsız olarak tm iletiřim bir "VPN Gvenlik Duvarı" kullanılarak řifrelenebilir. Ofisinizde veya kafenizde otururken internet ile gvenli bir baęlantınız bulunabilir. Gvenlik duvarı, konuřmak istedięiniz herkesle gvenli iletiřim hatları kurabilir. Bu, en yaygın fideye yazılımı saldırısı tr olan "Uzak Masast" kaba kuvvet saldırılarının stesinden gelmeye yardımcı olmaktadır. Bir VPN gvenlik duvarı ayrıca zorla girme giriřimlerini izler ve gnlęe kaydeder. alıřanların eriřimini filtrelemek iin zellikler saęlar, bylece zararlı web sitelerine eriřimleri engellenir [62].

Yenilenmiş bir güvenlik duvarı satın alarak maliyetlerden tasarruf edebilirsiniz. Ancak, satın alma işleminden sonra, çalışanları güvenlik politikalarına eklemekten önce en son ürün yazılımı ile güncellendiğinden emin olun. Güvenlik duvarının varsayılan parolasının değiştirildiğinden ve yönetici erişimi için iki faktörlü kimlik doğrulaması yapılandırıldığından emin olunmalıdır. Günümüzde birçok güvenlik duvarında, çalışanların resmi cihazlarına kurmaları için bir yazılım bileşeni de bulunmaktadır. Bu işlem, oturum açma işlem süresini birkaç saniye uzatabilir ancak daha iyi güvenlik sağlamaktadır.

7.8 Yapılandırmalar ve Ayarlar aracılığıyla Siber Güvenlik

7.8.1 Çok Faktörlü Kimlik Doğrulama

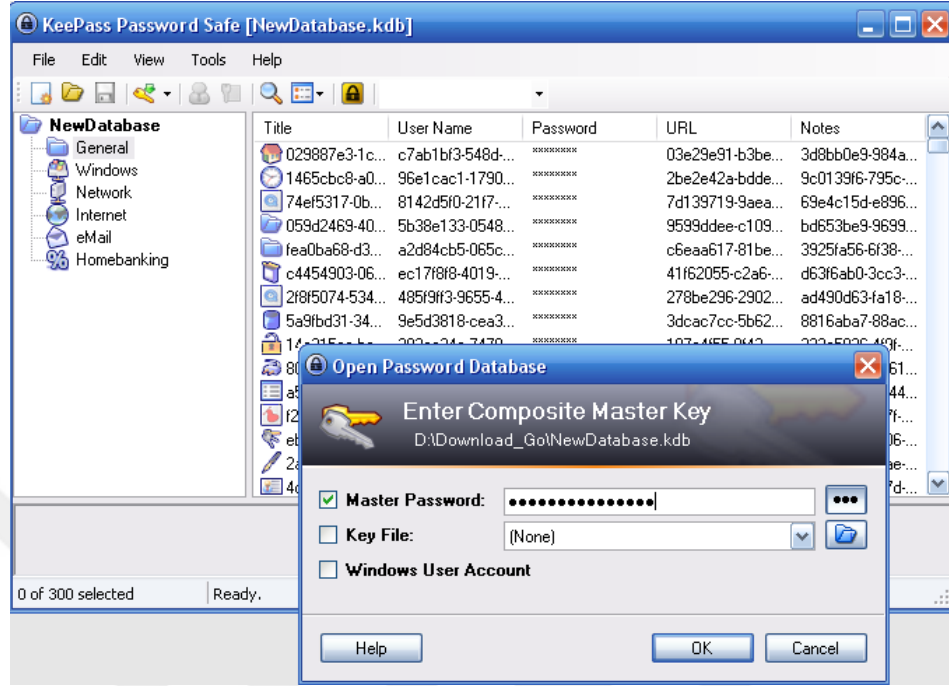
Çoğu uygulama iki faktörlü kimlik doğrulama sunar, ancak kullanıcılar bunu kullanmak konusunda oldukça isteksizdir. Ancak, bu güvenlik ayarı bugün çok etkilidir ve çok ihtiyaç duyulmaktadır. Kullanıcı ilk olarak kendi kullanıcı adı ve şifresini kullanarak uygulamasında oturum açar. Bundan sonra, sistem veya uygulama, akıllı telefonu gibi uygulamaya ve kullanıcıya bağlı başka bir cihaza gönderilen tek seferlik geçici bir şifreyi tetikler. Kullanıcı, yalnızca bu şifreyi girdikten sonra uygulamaya erişebilir.

Bu, bir saldırganın e-posta kimlik avı, kötü amaçlı yazılım veya tuş kaydediciler gibi yöntemlerle, kullanıcının kullanıcı adını ve şifresini ele geçirme olasılığından kaynaklanan riskleri ortadan kaldırmaktadır. Bu, saldırganın kullanıcı adınızı ve parolanızı girdiği, ancak tek seferlik parolayı almadığı anlamına gelir. Bu, saldırganı uygulamadan engeller. Saldırgan uygulamayı birçok kez hacklemeye çalışırsa uygulama kullanıcıya bir bildirim göndermektedir.

7.8.2 Şifre Kasası

Kullanıcılar birden fazla uygulamaya eriştiği için, farklı parolaları korumaları gerekmektedir. Ancak çoğu kullanıcı tüm uygulamalarda ve cihazlarda aynı parolayı kullanmaktadır. Bunu şifreyi unutmamak için yapmaktadırlar. Günümüzde kullanıcıların kendi cihazlarında saklamalarına olanak tanıyan parola kasası uygulamaları bulunmaktadır. Bu şekilde yalnızca kasa için bir şifre belirlemeniz ve hatırlamanız gerekmektedir. Parola kasası, karmaşık parolalar oluşturma, parolaları yönetme ve formları, uygulamaları, web sitelerini ve sistem oturum açma bilgilerini

otomatik olarak doldurma özelliklerine sahiptir. Bu parolalar rastgele ve karmaşık olarak belirlenmektedir ve bu nedenle bir saldırganın kırması oldukça zordur.



Şekil 8.2 : Şifre Kasası

7.8.3 Otomatik Güncellemeler

Çoğu işletme yazılımlarını ve uygulamalarını güncellememektedir. Bu da sistemi ve ağı savunmasız ve saldırılara açık hale getirmektedir. Yazılım sağlayıcıları, oluşan güvenlik açıkları ve uygulamaların güvenliğini sağlamak için düzenli olarak yama ve yazılım güncellemeleri sağlamaktadırlar. Yazılımda yeni bir güvenlik açığı keşfedildiğinde, satıcılar uygulamayı veya yazılımı güvence altına almak için bir yama oluşturmaktadırlar. Bu nedenle, yazılım düzenli olarak güncellenemez ise, yazılım ve uygulama herhangi bir saldırıya açık bırakılmış olur. Bu nedenle, tüm yazılımınızın otomatik güncellemede bırakılması güvenlik açısından doğru olacaktır. Böylece güvenlik açıklarının kapatılması için yazılım firmaları tarafından geliştirilen yamalar otomatik olarak indirilmiş olur.

7.8.4 Tam Disk Şifreleme

Bir işletmenin ulaşılabilen tüm verileri her zaman tamamen şifrelenmelidir. Cep telefonları, dizüstü bilgisayarlar, sabit sürücüler ve ağ depolama gibi cihazların her

zaman bir şifreleme katmanına sahip olması gerekmektedir. Çoğu işletme, çalışanlarının evden çalışmasına izin verdiğinden, tüm iş cihazlarının ve verilerin şifrelenmesi sağlanmalıdır. Düşük bir maliyet ile tam disk şifreleme, verilerinizin çalınması durumunda güvende olunmasını sağlamaktadır.

7.8.5 Kötü Amaçlı Yazılım Tarayıcıları

Kötü amaçlı yazılım tarayıcıları düşük maliyetlerle sunulur. Herhangi bir kötü amaçlı yazılım tehdidini tespit etmeye yardımcı olmaktadır. Günümüzde, farklı türde kötü amaçlı yazılım tarayıcıları vardır. Bunlar, işlevlerine ve fiyatlarına göre sınıflandırılmaktadır. Kötü amaçlı yazılım tarayıcısının yeni güvenlik açıklarını tespit ettiğinden emin olmak için düzenli olarak güncellenmeniz gerekmektedir.

7.8.6 IP Adresi Sabitleme

Genellikle çevrimiçi uygulamalar üzerinde çalışıldığında, özellikle uygulamaya erişenlerin IP adreslerinin sabitlenmesi gerekmektedir. Ayrıca, kullanıcının erişip erişmediğini belirlemek için uygulamaya iki faktörlü kimlik doğrulama uygulanmalıdır. Üçüncü taraf uygulamaları ticari amaçlarla kullanıyorsanız, uygulamalara erişimi olan IP adresleri de sabitlenmelidir. Bu, yetkisiz IP'lerden girişlerin engellenmesine yardımcı olmaktadır.

7.8.7 Sistem Yedeklemeleri

Sisteminizde çok fazla veriniz varsa, bir yedekleme yaparak onları saldırılardan ve felaketlerden korumuş olursunuz. Bunun rutin olarak yapılması ve yedeklemelerin tamamen farklı bir ağdaki şifreli disklerde depolanması gerekmektedir. Yedekleme cihazlarının, diğer cihazlarla aynı oturum açma kimlik bilgilerinin kullanılarak açılmadığından emin olunması gerekmektedir. Yedekleme şifrelerinin, saldırganlar tarafından kolayca kırılmaması için, farklı parolalar oluşturulması ve saklanması gerekmektedir.

7.9 Güvenlik Eğitimi

Ekipleriniz için eğitim rutinleri oluşturulmalı ve onlara en iyi güvenlik uygulamaları öğretilmelidir. Kimlik avı, adres sahteciliği, sosyal mühendislik vb. gibi konularda on beş dakikalık küçük eğitim videoları hazırlanmalıdır. Bu videolar çalışanların çeşitli siber saldırı türlerine karşı bilgi edinmelerini sağlayacaktır.

8.WEB UYGULAMASI GÜVENLİĞİ

Teknolojideki ilerleme, web uygulamalarının geliştirilmesine yol açmıştır. Günümüzde çoğu işletmenin web uygulamaları var ve birçoğu da verileri güvenli bir şekilde depolamak için bulutu kullanıyor. Modern Web 2.0 ve HTML5 tabanlı web uygulamalarının başlangıcından bu yana müşterilerin talepleri hızlı bir şekilde artmıştır. Müşteriler anlık olarak verilere ve bilgilere erişmek istemektedir. Bu talepler, işletmelere verilerini ve web uygulamalarını buluta taşımaları için baskı yapmıştır. Örneğin, bankacılık ve alışveriş işlemleri çevrimiçi ortama taşındı. Artık fiziksel olarak bir bankaya veya süpermarkete gidilmesine gerek kalmamıştır. Bu, işlemleri koltuklarının rahatlığında yapabildikleri için hayatı kolaylaştırdı, ancak bazı dezavantajları da ortaya çıkarmıştır. Bu durum bilgisayar korsanlarının yaptığı siber saldırıların çeşidini ve girişimlerin sayısını artırdı. Aynı zamanda güvenlik alanında “*Web Uygulama Güvenliği*” olarak bilinen başka bir bölümün ortaya çıkmasına yol açtı.

8.1 Web Uygulama Güvenliği

Bir web uygulaması güvenlik duvarı WAF, HTTP ve HTTPS trafiğini filtrelemek için uygulama düzeyinde çalışan bir güvenlik protokolüdür. Böylece uygulama katmanındaki saldırılardan korumaktadır. Basit bir deyişle, bir saldırgan bir web uygulamasındaki bilinen bir güvenlik açığından faydalanmaya çalışırsa, bu tür saldırıları engelleyebilir. Web sitesini veya uygulamayı bir saldırıdan koruyabilir. Ancak, bu sürecin bazı dezavantajlarının olduğu bilinmektedir. Yalnızca bilinen güvenlik açıklarını tespit edebilir. Bir web uygulaması güvenlik duvarının kendi ayarlarında yapılandırılmış belirli kuralları bulunmaktadır. Web trafik kurallarıyla eşleşir ve trafiğin bu kurallarla eşleşip eşleşmediğine göre uygulamayı sınıflandırır. Bu göz önüne alındığında, bir web uygulaması güvenlik duvarı sizi web ‘de yeni keşfedilen güvenlik açığına karşı koruyamaz. Ancak, web uygulaması güvenlik duvarları, hizmet reddi saldırılarına karşı etkilidir. Bir web uygulaması güvenlik duvarının bir kullanıcı tarafından yapılandırılmış kuralları vardır. Bu, zincirdeki en zayıf halka ve güvenlik duvarını yapılandıran kullanıcı kadar iyi olduğu anlamına gelmektedir. Sistem içinde herhangi bir sorun olup olmadığını belirlemek zordur. Bu nedenle, deneyimli bir kullanıcı web uygulamasını yapılandırmazsa, tamamen güvensiz olur. Web uygulamasındaki güvenlik sorunlarını çözemez; web uygulaması kodunu otomatik olarak düzeltemez. Dolayısıyla, uygulamada boşluklar varsa, bu

boşlukları yalnızca yapılandırılan kurallara göre saldırgandan koruyabilir. Kodun hala bir geliştirici tarafından düzeltilmesi gerekmektedir. Bir web uygulaması güvenlik duvarı normal bir uygulamadır ve güvenlik zaafiyetleri bulunmaktadır. Saldırganların güvenlik açığı nedeniyle web uygulaması güvenlik duvarına yönetici erişimi elde ettiği ve kapattığı istismar durumları vardır. Bu nedenle, web uygulaması güvenlik duvarları ek bir güvenlik katmanıdır ancak nihai çözüm değildir. Bir web uygulaması güvenlik duvarına (WAF) sahip olmak iyi bir güvenlik çözümüdür, ek güvenlik katmanları ve uygulamaları kullanmak veri ihlalleri için her zaman iyi bir çözümdür [63].

Sistemdeki veya web uygulamasındaki güvenlik açıklarına dikkat etmek ve bir web uygulaması güvenlik duvarının varlığına bakılmaksızın bunları düzeltmek önemlidir. İşletmeler, ürün kalitesi test süreçlerinin ayrılmaz bir parçası olarak web uygulaması güvenlik açığı testine sahip olmalıdır.

8.2 Web Uygulamalarını Nasıl Güvenceye Alınır

Web uygulamasının tamamen güvenli olup olmadığını anlamak için, bir saldırgan bunları bulup kullanmaya başlamadan önce sistemdeki güvenlik açıkları belirlenmelidir. Bir web uygulaması, yalnızca uygulama yayınlandığında değil, tüm yazılım geliştirme döngüsü boyunca güvenlik açıklarına karşı test edilmelidir. Bir web uygulamasını güvenlik açıklarına karşı test etmenin çeşitli yöntemleri vardır. Bu yöntemlerden bazıları şu şekildedir:

- Web uygulamasını taramak için bir kara kutu tarayıcı kullanılmalıdır.
- Uygulama koduyla ilgili sorunları tespit etmek için otomatik olarak beyaz kutu tarayıcı kullanılmalıdır.
- Uygulamanın kaynak kodu manuel olarak denetlenmelidir.
- Manuel sızma testi ve güvenlik denetimi yapılmalıdır.

Hiçbir yöntem yüzde 100 tespit oranını garanti etmemektedir. Sistemin güvenlik açıklarını test etmek için tek bir yöntem kullanamazsınız. Her yöntemin artıları ve eksileri vardır. Örneğin, otomatik bir araç, manuel bir test cihazına kıyasla kodla ilgili neredeyse tüm güvenlik açıklarını keşfedebilir. Ancak herhangi bir mantıksal boşluk tespit edemez. Araç bir saldırgan gibi düşünemez ve testi gerçekleştirmek için temel bir koda veya uygulamaya sahip olması gerekir. Koddaki mantıksal kusurları belirlemek için manuel müdahale gereklidir. Tersine, teknik boşlukları manuel olarak

belirlemek çok zaman, çaba ve para gerektirir. Manuel test uzmanının sistemdeki tüm güvenlik açıklarını tespit ettiği garanti edilemez.

Zaman ve bütçe kısıtlaması yoksa bir web uygulamasını test etmek için mevcut her aracı kullanmanız önerilmektedir. Ancak bu yalnızca ideal bir senaryoda olur. Bu nedenle, bir işletmenin bir saldırıyı simüle etmek için zaman ve para açısından en etkili çözümü seçmesi gerekmektedir. Çoğu işletme, web güvenlik açığı tarayıcısı olarak bilinen bir kara kutu tarayıcı kullanır. Manuel bir denetimin otomatik bir web güvenlik açığı tarayıcısı kullanması gerektiğini söylemeye gerek yoktur. Bu, hem teknik hem de mantıksal güvenlik açıklarının belirlenmesini sağlamaktadır.

8.3 Web Güvenlik Açığı Tarayıcıları

Kara Kutu Tarayıcıları, web güvenlik açığı tarayıcıları olarak da bilinmektedir. Kara kutular, güvenlik açıkları ve diğer güvenlik sorunları için web sitelerini ve web uygulamalarını tarayan otomatik uygulamalardır. Web güvenlik açığı tarayıcılarının kullanımları kolaydır ve bunlar tüm tarama sürecini otomatikleştirdikleri için popüler hale gelmişlerdir. Beyaz kutu tarayıcı kullanıyorsanız, temel koda erişmeniz ve uygulama geliştirmeyi anlayan birinin yardımını almanız gerekmektedir. Ancak kara kutu tarayıcılarla, minimum teknik bilgiye sahip herkes web güvenlik açığı tarayıcısını çalıştırabilir ve bir web uygulamasını test edebilmektedir.

Doğru web güvenlik açığı tarayıcısını nasıl seçersiniz?

İnternet, hem ticari hem de ticari olmayan kullanıcılar için web güvenlik açığı tarayıcılarıyla doludur. Size en uygun tarayıcıyı seçmek zordur. Bu nedenle, uygulamanıza hangisinin uygun olduğunu anlamak için mevcut her tarayıcı test edilmelidir. Önünüzde birçok seçenek olabilir, bir web güvenlik açığı tarayıcısı seçin. İlk ve açık soru, ücretsiz bir tarayıcı mı yoksa ticari olarak ödenen bir lisansa sahip tarayıcı mı kullanılacağıdır. Düzenli güncellemeleri olduğundan, profesyonel olarak eğitilmiş ekiplerden destek sağladığından vb. her zaman ticari bir tarayıcı kullanmanız önerilmektedir.

Web uygulaması saldırı yüzeylerini ne kadar iyi tanımlayabilir?

Tarayıcıyı test ederken, hangisinin en iyi tarayıcıya sahip olduğu dikkatlice incelenmelidir. Tarayıcı, saldırganın saldırıyı başlatabileceği tüm giriş noktaları için

uygulamayı tarayan bir tarayıcı bileşenidir. Güvenlik açığını yalnızca giriş noktaları belirlendiğinde tanımlamak daha kolay olduğu için kritik bir bileşendir.

Bir tarayıcının web uygulamasının tüm yüzeyini tarayamama olasılığı vardır. Bu genellikle tarayıcının manuel olarak yapılandırılması gerektiğinde meydana gelir ve bu da bir sonraki noktaya götürmektedir.

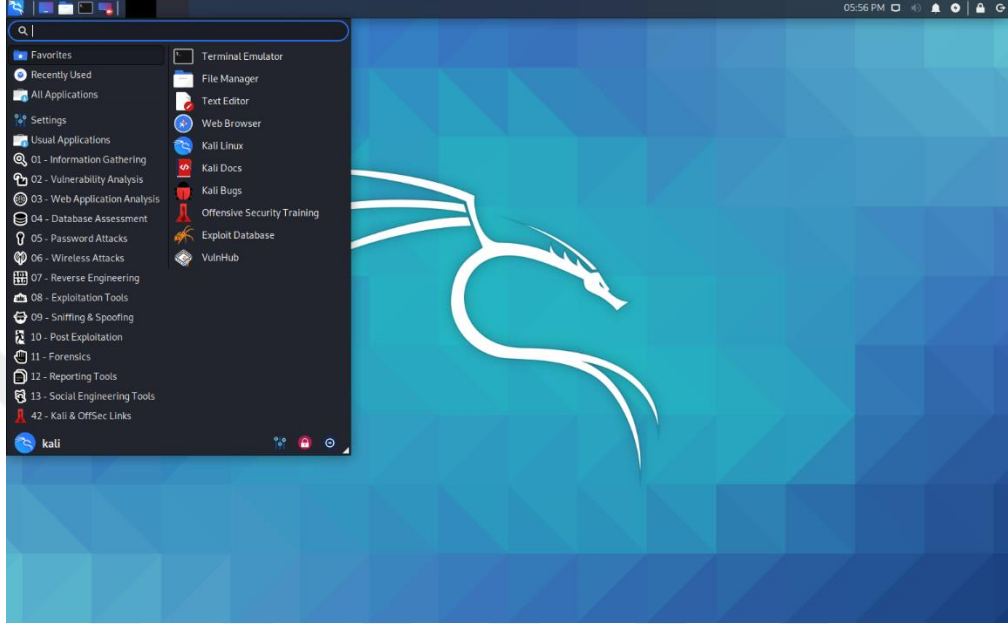


9. KALİ LINUX

9.1 Kali Linux Nedir?

Kali Linux projesi 2012'de, Offensive Security'nin manuel olarak sürdürülen o zamanki adıyla BackTrack Linux'un, gerekli tüm altyapı ve iyileştirilmiş paketleme teknikleri ile tasarlanmış halidir. Geliştiricilerin Debian türevi olabilecek bir projeyi değiştirmek istediklerine karar vermesiyle ortaya çıktı. Kali'yi Debian dağıtımının üzerine kuruldu çünkü kalitesi, kararlılığı ve geniş yazılım seçenekleriyle tanınmaktaydı. İlk sürüm (sürüm 1.0), bir yıl sonra, Mart 2013'te gerçekleştirildi ve Debian'ın o zamanki kararlı dağıtımı olan Debian 7 “Wheezy” adıyla biliniyordu. Geliştirmenin ilk yılında, kalem testiyle ilgili yüzlerce uygulamayı bir araya getirip altyapıyı oluşturuldu. Kali 1.0 sürümünü çıkmasını takip eden iki yıl boyunca daha yeni çekirdek geliştirilebilir ve mevcut uygulamaların çeşidini ve donanım desteğini geliştirerek birçok güncelleme yayınlandı. Sürekli entegrasyona yapılan yatırımla, tüm önemli paketler kurulabilir durumda tutuldu. 2015 yılında Debian 8 “Jessie” çıktığında, Kali Linux'u bunun üzerine yeniden kurmak için çalışıldı. Kali Linux 1.x, GNOME Shell'den kaçınırken (bunun yerine GNOME Fallback'e güvenerek), bu sürümde onu önemsemeye ve geliştirmeye karar verildi. Eksik özellikleri, özellikle de Uygulamalar menüsünü elde etmek için bazı GNOME Shell uzantıları eklendi. Bu çalışmanın sonucu, Ağustos 2015'te yayınlanan Kali Linux 2.0 oldu. Kali Linux'un her zaman tüm kalem testi uygulamalarının en son sürümüne sahip olması sağlandı. Ne yazık ki, bu hedef, dağıtım için bir temel olarak Debian Stable'ın kullanılmasıyla biraz çelişiyordu, çünkü birçok paketi desteklenmesi gerekliydi. Bunun nedeni, Debian Stable'ın yazılımının kararlılığına öncelik vermesi ve genellikle yukarı akış güncellemesinin yayınlanmasından dağıtıma entegre edilmesine kadar uzun bir gecikmeye neden olmasıdır. Bu, özünde Kali Rolling'in konseptidir. Döner dağıtım bir süredir mevcut olsa da, Kali 2016.1, bu dağıtımın yuvarlanan doğasını resmi olarak benimseyen ilk sürümdü. En son Kali sürümü yüklendiğinde, sistem aslında Kali Yuvarlama dağıtımını izler ve aldığınız yeni güncellemeler aslında Kali sürümleri, içine Kali'ye özgü paketlerin enjekte edildiği temel Debian dağıtımının anlık görüntüleri idi. 2017 yılına gelindiğinde Kali'deki paketlerin sayısı nispeten düşük olsa da, ek paketlerin sayısı 400'dü. Bu paketlerin çoğu Debian Özgür Yazılım Yönergeleri ile uyumlu ücretsiz yazılımlardı.

Kali'nin odak noktası “sızma testi ve güvenlik denetimi” olarak hızlıca özetlenebilirken, bu faaliyetlerin arkasında birçok farklı görev vardır. Kali Linux bir çerçeve olarak oluşturulmuştur, çünkü çok farklı kullanım durumlarını kapsayan birçok araç içerir (ancak bunlar bir penetrasyon testi sırasında birlikte kullanılabilirlerdi).



Şekil 11.1 : Kali Linux Ekranı

Kali Linux çeşitli bilgisayar türlerinde, sızma test cihazlarının dizüstü bilgisayarlarında, aynı zamanda ağlarını izlemek isteyen sistem yöneticilerinin sunucularında, adli analistlerin iş istasyonlarında ve daha da beklenmedik bir şekilde bir kablosuz ağın kapsama alanında kullanılmaktadır. Kali Linux, taşınabilir penetrasyon testine izin vermek için cep telefonları ve tabletlerde hızlı bir şekilde bir parola kırma makinesi oluşturmak için bulutta da konuşlandırılabilir. Penetrasyon test cihazlarının ayrıca sunuculara ihtiyacı vardır. Kalem testçileri yazılımı kullanmak, kimlik avı süreçlerini yönetmek üzere bir web sunucusu kurmak, güvenlik açığı tarama araçlarını çalıştırmak ve diğer ilgili faaliyetler için bu sunucuya ihtiyaç duymaktadır.

Bu görevler ve faaliyetler şunları içerir:

- Bilgi Toplama: Hedef ağ ve yapısı hakkında veri toplama, bilgisayarları, işletim sistemlerini ve çalıştırdıkları hizmetleri tanımlama. Bilgi sisteminin potansiyel olarak hassas bölümlerinin belirlenmesi. Çalışan izin hizmetlerinden her türlü listeyi çıkarmak.

- **Güvenlik Açığı Analizi:** Yerel veya uzak bir sistemin bir dizi bilinen güvenlik açığından veya güvenli olmayan yapılandırmadan etkilenip etkilenmediğini hızla test etme. Güvenlik açığı tarayıcıları, olası güvenlik açıklarını belirlemek için binlerce imza içeren veritabanlarını kullanır.
- **Web Uygulaması Analizi:** Web uygulamalarındaki yanlış yapılandırmaların ve güvenlik zafiyetlerinin belirlenmesi. Bu uygulamaların kamuya açık olmasının onları saldırganlar için ideal hedefler haline getirdiği göz önüne alındığında, bu sorunları belirlemek ve azaltmak çok önemlidir.
- **Veri tabanı Değerlendirmesi:** SQL enjeksiyonu kimlik bilgilerinden saldırıya kadar, veri tabanı saldırıları saldırganlar için çok yaygın bir unsurdur. SQL enjeksiyonundan veri çıkarma ve analize kadar çeşitli saldırı vektörlerini test eden araçlar burada bulunabilir.
- **Parola Saldırıları:** Kimlik doğrulama sistemleri her zaman saldırı hedefi içindedir. Çevrimiçi parola saldırı araçlarından şifreleme veya karma sistemlere yönelik çevrimdışı saldırılara kadar birçok yararlı araç burada bulunabilir.
- **Kablosuz Saldırıları:** Kablosuz ağların yaygın olarak kullanılması, her zaman saldırıya açık olacakları anlamına gelir. Birden çok kablosuz kart için geniş desteğiyle Kali, birden çok kablosuz ağ türüne karşı saldırılar için bariz bir seçimdir.
- **Tersine Mühendislik:** Tersine mühendislik birçok amacı olan bir faaliyettir. Saldırgan faaliyetleri desteklemek için, güvenlik açığı tanımlama ve geliştirmeden yararlanılmaktadır. Savunma tarafında, hedefli saldırılarda kullanılan kötü amaçlı yazılımları analiz etmek için kullanılır. Bu kapasitede amaç, belirli bir ticari zanaat parçasının yeteneklerini belirlemektir.
- **Sömürü Araçları:** Bir güvenlik açığından yararlanmak ve bu güvenlik açığını kullanarak, uzaktaki bir makinenin (veya aygıtın) kontrolünü ele geçirmenize olanak tanır. Bu erişim daha sonra, güvenliği ihlal edilmiş makinede yerel olarak veya yerel ağından erişilebilen diğer makinelerde daha fazla ayrıcalık yükseltme saldırıları için kullanılabilir. Bu kategori, kendi istismarlarınızı yazma sürecini basitleştiren bir dizi araç ve yardımcı program içerir.
- **Sniffing & Spoofing:** Veriler ağda dolaşırken erişim elde etmek genellikle bir saldırgan için avantajlıdır. Burada, meşru bir kullanıcının kimliğine bürünmenize izin

veren sahtekârlık araçlarını ve verileri anında yakalamanıza ve analiz etmenize olanak tanıyan araçları bulabilirsiniz. Birlikte kullanıldığında, bu araçlar çok güçlü olabilir.

- Sömürü Sonrası: Bir sisteme erişim kazandıktan sonra, genellikle bu erişim seviyesini korumak veya ağ üzerinde yanlamasına hareket ederek kontrolü genişletmek istenecektir. Bu hedeflere yardımcı olan araçlar burada bulunur.
- Adli Araçlar: Adli Linux canlı önyükleme ortamları yıllardır çok popüler olmuştur. Kali, ilk triyajdan veri görüntülemeye, tam analiz ve vaka yönetimine kadar her şeyi yapmanızı sağlayan çok sayıda popüler Linux tabanlı adli araç içerir.
- Raporlama Araçları: Sızma testi ancak bulgular rapor edildikten sonra tamamlanır. Bu kategori, bilgi toplama araçlarından toplanan verileri derlemeye, açık olmayan ilişkileri keşfetmeye ve her şeyi çeşitli raporlarda bir araya getirmeye yardımcı olan araçları içermektedir.
- Sosyal Mühendislik Araçları: Teknik güvenlik olduğunda, genellikle insan davranışını bir saldırı biçimi olarak kullanma olasılığı vardır. Doğru etki göz önüne alındığında, insanlar sıklıkla çevrenin güvenliğini tehlikeye atan eylemlerde bulunmaya teşvik edilebilmektedir. Sekreterin az önce taktığı USB anahtarı zararsız bir PDF içeriyor mu? Yoksa aynı zamanda bir arka kapı kuran bir Truva atı mıydı? Muhasebecinin beklenen web sitesine giriş yaptığı bankacılık web sitesi mi yoksa kimlik avı amacıyla kullanılan mükemmel bir kopya mı? Bu kategori, bu tür saldırılara yardımcı olan araçları içerir.
- Sistem Hizmetleri: Bu kategori, arka planda sistem hizmetleri olarak çalışan uygulamaları başlatmanıza ve durdurmanıza izin veren araçları içerir.

Kali Linux, hedef kullanıcıları için özel olarak tasarlanmış sızma test edicileri ve diğer güvenlik uzmanları için yüzlerce yazılım aracı koleksiyonunu içeren bir Linux dağıtımdır. Ayrıca Kali Linux'u herhangi bir bilgisayarda ana işletim sistemi olarak tamamen kurmak için bir kurulum programı ile birlikte gelmektedir. Bu, mevcut tüm diğer Linux dağıtımlarına oldukça benzer, ancak Kali Linux'u farklı kılan, çoğu penetrasyon testçilerinin özel ihtiyaçlarına göre uyarlanmış başka özellikler de bulunmasıdır [64].

9.2. Canlı Sistem (Live ISO)

Çoğu Linux dağıtımının aksine, indirdiğiniz ana ISO görüntüsü sadece işletim sistemini kurmaya yönelik değildir; ön yüklenebilir bir canlı sistem olarak da kullanılabilir. Başka bir deyişle, Kali Linux'u yüklemeyen, sadece ISO görüntüsünü önyükleyerek (genellikle görüntüyü bir USB cihazına kopyaladıktan sonra) kullanılabilir.

Canlı sistem, penetrasyon test cihazları tarafından en sık kullanılan araçları içerir. Bu nedenle kullanılan sistem Kali Linux olmasa bile, diski veya USB cihazını takıp Kali'yi çalıştırmak yeterli olacaktır. Ancak, varsayılan yapılandırmanın yeniden başlatmalar arasındaki değişiklikleri korumayacağını unutmayın. Kalıcılığı bir USB cihazı yapılandırırsanız “Bir USB Cihazı Canlı ISO'ya Kalıcılık Ekleme” o zaman sistem istenildiği gibi ayarlanabilmektedir.

9.3 Adli Araç Modu (Forensic Tool Mod)

Genel olarak, bir sistem üzerinde adli çalışma yaparken, analiz edilen sistemdeki verileri herhangi bir şekilde değiştirecek faaliyetten kaçınmak istenir. Modern masaüstü ortamları, algıladıkları herhangi bir diski/diskleri otomatik olarak bağlamaya çalışarak bu amaca müdahale etme eğilimindedir. Bu davranışı önlemek için Kali Linux, önyükleme menüsünden etkinleştirilebilen bir adli tıp moduna sahiptir. Canlı sistem, özellikle adli tıp amaçları için kullanışlıdır, çünkü herhangi bir bilgisayarı, sabit disklerine erişmeden veya değiştirmeden Kali Linux sistemine yeniden başlatmak mümkündür.

9.4. Özel Bir Linux Çekirdeği

Kali Linux, her zaman Debian Un-stable'daki sürüme dayalı olarak özelleştirilmiş yeni bir Linux çekirdeği sağlamaktadır. Bu, özellikle çok çeşitli kablosuz cihazlar için sağlam donanım desteği içermektedir. Birçok kablosuz güvenlik değerlendirme aracı bu özelliğe dayandığından, çekirdek kablosuz enjeksiyon desteği için yamalanmıştır. Birçok donanım aygıtı güncel belenim dosyaları gerektirdiğinden (/lib/firmware/ içinde bulunur), Kali, Debian'ın özgür olmayan bölümünde bulunan belenim dahil, hepsini varsayılan olarak yükler. Bunlar, kapalı kaynak oldukları ve dolayısıyla Debian'ın uygun bir parçası olmadıkları için Debian'da varsayılan olarak kurulmazlar.

9.5. Özelleştirilebilme Özelliği

Kali Linux, penetrasyon test cihazları için penetrasyon test cihazları tasarımcıları tarafından oluşturulmuştur. Kali Linux'un kendi ihtiyaçlarınıza ve tercihlerinize göre kolayca özelleştirilebilmesini sağlıyoruz. Bu amaçla, resmi Kali görüntülerini oluşturmak için kullanılan canlı oluşturma yapılandırması yayınlanıyor, böylece kullanım şekline göre özelleştirilebilir. Yayınlanan bu yapılandırmadan başlamak ve canlı derlemenin çok yönlülüğü sayesinde ihtiyaçlara göre çeşitli değişiklikleri uygulamak kolaydır. Live-build, kurulu sistemi değiştirmek, ek dosyalar kurmak, ek paketleri kurmak, isteğe bağlı komutları çalıştırmak ve debconf için önceden tohumlanmış değerleri değiştirmek için birçok özellik içermektedir.

9.6. Güvenilir Bir İşletim Sistemi

Bir güvenlik dağıtımının kullanıcıları, haklı olarak güvenilir olabileceğini ve herkesin kaynak kodunu incelemesine izin verecek şekilde açıkça geliştirildiğini bilmek ister. Kali Linux, şeffaf bir şekilde çalışan ve en iyi güvenlik uygulamalarını takip eden bilgili geliştiricilerden oluşan küçük bir ekip tarafından geliştirilmiştir: imzalı kaynak paketleri yüklerler ve bunlar daha sonra özel yapım arka plan programları üzerine kuruludur. Paketler daha sonra sağlama toplamı ve imzalı bir havuzun parçası olarak dağıtılır. Paketler üzerinde yapılan çalışma, Kali kaynak paketlerini oluşturmak için kullanılan Git depoları¹⁴ (imzalı etiketler içeren) aracılığıyla tam olarak gözden geçirilebilir. Her paketin gelişimi Kali paket takipçisi aracılığıyla da takip edilebilir.

9.7. ARM Cihazları

Kali Linux, armel, armhf ve arm64 ARM mimarileri için ikili paketler sağlar. Offensive Security tarafından sağlanan kolayca kurulabilen görüntüler sayesinde Kali Linux, akıllı telefonlar ve tabletlerden Wi-Fi yönlendiricilere ve çeşitli şekil ve boyutlardaki bilgisayarlara kadar birçok ilginç cihaza kurulabilir.

Kali Linux Özette

- Kali Linux¹⁷, Debian GNU/Linux tabanlı, kurumsal kullanıma hazır, güvenlik denetimi yapan bir Linux dağıtımıdır. Kali, güvenlik uzmanlarına ve BT yöneticilerine yönelik olup, onların gelişmiş sızma testi, adli analiz ve güvenlik denetimi yapmalarını sağlar.

- Çoğu yaygın işletim sisteminin aksine, Kali Linux sürekli bir dağıtımdır, bu da her gün güncellemeler alacağınız anlamına gelir.
- Kali Linux dağıtımı, Debian Testing18'e dayanmaktadır. Bu nedenle Kali Linux'ta bulunan paketlerin çoğu doğrudan bu Debian deposundan gelir.
- Kali'nin odak noktası “sızma testi ve güvenlik denetimi” ile hızlı bir şekilde özetlenebilirken, ağlarını izlemek isteyen sistem yöneticileri, adli analiz, gömülü cihaz kurulumları, kablosuz izleme, mobil platformlarda kurulum, ve dahası.
- Kali'nin menüleri, güvenlik açığı analizi, web uygulaması analizi, veri tabanı değerlendirmesi, parola saldırıları, kablosuz saldırılar, tersine mühendislik, istismar araçları, koklama ve sahtekarlık, istismar sonrası araçlar dahil olmak üzere çeşitli görev ve etkinlikler için araçlara erişmeyi kolaylaştırır, adli tıp, raporlama araçları, sosyal mühendislik araçları ve sistem hizmetleri.

9.8. Önemli Kali Linux Toolları

Kali Linux dağıtımı içinde birçok tool içermektedir. Bunlar saldırganların işini kolalaştıracak hazır paketlerdir. Bunların en önemlileri şunlardır.

9.8.1 Nmap

Nmap, ağları yeniden yapılandırmak/taramak için kullanılan açık kaynaklı bir ağ tarayıcısıdır. Bir ağ üzerinden ana bilgisayarları, bağlantı noktalarını ve hizmetleri sürümleriyle birlikte keşfetmek için kullanılır. Paketleri ana bilgisayara gönderir ve ardından istenen sonuçları üretmek için yanıtları analiz eder. Ana bilgisayar keşfi, işletim sistemi tespiti veya açık portları taramak için bile kullanılabilir. En popüler keşif araçlarından biridir.

9.8.2 Burp Suite

Burp Suite, en popüler web uygulaması güvenlik test yazılımlarından biridir. Bir proxy olarak kullanılır, bu nedenle proxy ile tarayıcıdan gelen tüm istekler bunun üzerinden geçer. İstek burp paketinden geçerken, XSS veya SQL gibi güvenlik açıklarını ve hatta web ile ilgili herhangi bir güvenlik açığını test etmek için iyi olan ihtiyacımıza göre bu isteklerde değişiklik yapmamıza olanak tanır. Kali Linux, ücretsiz olan burp suite topluluk sürümüyle birlikte gelir, ancak burp suite profesyonel olarak bilinen ve burp suite topluluk sürümüne kıyasla birçok işlevi olan ücretli bir sürümü vardır.

9.8.3 Wireshark

Wireshark, bir ağ üzerinden gönderilen verileri analiz etmek veya bunlarla çalışmak için kullanılan bir ağ güvenlik aracıdır. Bir ağ üzerinden iletilen paketleri analiz etmek için kullanılır. Bu paketler, kaynak IP ve hedef IP, kullanılan protokol, veriler ve bazı başlıklar gibi bilgilere sahip olabilir. Paketler genellikle Wireshark aracı kullanılarak okunabilen bir “.pcap” uzantısına sahiptir.

9.8.4 Metasploit Çerçevesi

Metasploit, Rapid7 teknolojileri tarafından tasarlanmış açık kaynaklı bir araçtır. Dünyanın en çok kullanılan sızma testi çerçevelerinden biridir. Bir ağ veya işletim sistemi üzerindeki güvenlik açıklarından yararlanmak için birçok istismarla birlikte gelir. Metasploit genellikle yerel bir ağ üzerinden çalışır ancak Metasploit'i “**port forwarding**” kullanarak internet üzerinden hostlar için kullanabilmektedir. Temel olarak Metasploit, CLI tabanlı bir araçtır, ancak Metasploit'in kullanımını daha rahat ve uygulanabilir kılan “**armitage**” adlı bir GUI paketi bile vardır.

9.8.5 Aircrack-ng

Aircrack, hepsi bir arada paket dinleyicisi, WEP ve WPA/WPA2 kırıcı, analiz aracı ve karma yakalama aracıdır. Wifi kesmek için kullanılan bir araçtır. Paketi yakalamaya ve bunlardan hashleri okumaya ve hatta sözlük saldırıları gibi çeşitli saldırılarla bu hashleri kırmaya yardımcı olur. Hemen hemen tüm en yeni kablosuz ara yüzleri destekler.

9.8.6 John the Ripper

John the Ripper, sözlük saldırısı veya özel kelime listesi saldırısı vb. saldırılar için bazı ünlü kabukuvvet kullanarak şifreleri kırmak için harika bir araçtır. Hatta sıkıştırılmış dosyalar ve hatta kilitli dosyalar için karmaları veya şifreleri kırmak için kullanılmaktadır. Karma veya şifreleri kırmak için birçok mevcut seçeneğe sahiptir.

9.8.7 Sqlmap

sqlmap, SQL enjeksiyon saldırılarını gerçekleştirmek için en iyi araçlardan biridir. Yalnızca SQL enjeksiyonu için bir parametreyi test etme sürecini otomatikleştirir ve hatta savunmasız parametreden yararlanma sürecini otomatikleştirir. Veri tabanını kendi başına algıladığı için harika bir araçtır, bu yüzden URL'deki parametrenin savunmasız olup olmadığını kontrol etmek için bir URL sağlamamız gerekiyor, hatta POST parametrelerini kontrol etmek için istenen dosyayı bile kullanabiliriz.

9.8.8 Autopsy

Otopsi, adli tıptan bilgi toplamak için kullanılan bir dijital adli tıp aracıdır. Veya başka bir deyişle, bu araç, sistemle tam olarak ne yapıldığını öğrenmek için dosyaları veya günlükleri araştırmak için kullanılır. Dosyaları bir hafıza kartından veya bir kalem sürücüden kurtarmak için bir kurtarma yazılımı olarak bile kullanılabilir.

9.8.9 Social Engineering Toolkit

Sosyal Mühendislik Araç Takımı, sosyal mühendislik saldırılarını gerçekleştirmek için kullanılabilecek bir araçlar topluluğudur. Bu araçlar, bilgi toplamak için insan davranışını kullanır ve manipüle eder. web sitelerini bile phishing için harika bir araçtır [65].



10 UYGULAMA

Siber saldırılarda insan etkisi ve zafiyeti her zaman ön planda olmuştur. Alınan ve alınması gereken tedbirler ve bunların uygulanması, denetlenmesi verilerin güvenliği için oldukça önemlidir. Kişisel verilerin sızdırılması ya da kritik öneme haiz bilgi ve belgelerin zafiyete uğraması tüm çevreler tarafından kabuledilemez bir olaydır. Sızdırılan kişisel veriler yanında önemli ölçüde prestij ve para kayıplarına yol açmaktadır. Siber saldırılardan korunmak için öncelikle siber saldırıların nasıl gerçekleştirildiğinin bilinmesi ve bu yöntemlerin incelenmesi önem teşkil etmektedir. Siber saldırı modellemeleri nasıl yapılır ve nelerden yararlanılır hangi araçlar ve hangi açıklıklar kullanılır bunları bilmek zafiyetleri en aza indirecektir.

Siber saldırıların başlangıcı bilgi toplama ile başlar. Toplanan bilgiler doğru araç kullanımı etkin bir saldırıyı tetikler. Etkin bir saldırı toplanan verilerin ışığında siber zafiyetleri beraberinde getirmektedir. Birçok saldırgan Linux sistemlerini ve araçlarını etkili bir saldırı aracı olarak kullanmaktadır.

Burada amacımız bir siber zafiyetin nasıl gerçekleştirildiğinin ve bilgi toplama araçlarının nasıl kullanıldığının etkin bir biçimde kullanılarak bu yöntemleri gözler önüne sermektir. Ayrıca tarama araçlarını kullanarak zafiyet içeren portları ve diğer açıklıkları tespit etmek, bu portların açıklıklarından faydalanarak ilgili zafiyetleri kullanarak sistemin nasıl zafiyete uğratıldığını göstermektir. Bilgi toplama araçlarından NMAP ve Essential NetTool kullanılmıştır. Bu araçlar etkili ve aktif olarak kullanılmaktadır. Bu saldırıları gerçekleştirmek için öncelikle her zaman bir IP adresine veya IP aralığına ihtiyaç duyulmaktadır. Bu nedenle bu araçlar bu IP adreslerini kullanarak açıklıkları tespit etmektedir. Hedef belirleme en basit yöntemiyle CMD (Command) ekranı ile ilgili web sitesine ping atarak bulunmaktadır. Ping www.google.com yazdığımızda Google sunucusunu IP adresi çıkmaktadır. Bu yöntemle belirli sayfalara atak düzenlemek için ilk kaynak olan IP adresine ulaşılmaktadır. Aynı şekildeki ağda bulunan diğer bilgisayarlarında IP leri bu şekilde bulunmaktadır. Essential NetTools ya da farklı programlar aracı aynı ağda kullanılan IP bloğu aralığı yazılarak aktif olan bilgisayarlar belirlenerek ilgili araçlar ile saldırılar düzenlenmektedir.

Uygulamada bir zafiyetli bilgisayara NMAP yardımı ile tarama yapılarak port açıklıkları belirlenecektir. Bu ataklar için Kali Linux ve araçları kullanılacaktır. Hedef

IP ler bağılı bulunulan ağda taranacak ilgili portlar incelenecektir. Açık olan portlara göre hangi atakları düzenleneceği değerlendirilecektir. Bu açıklıklar çoğunlukla insan zafiyeti yüzünden ya da kullanılan bir uygulama için açık bırakılan portlardır. Bu portların kullanılmıyorsa belirli zamanlarda taranarak kapatılması, kullanılıyorsa ilgili zafiyetler için tedbirlerin alınması gerekmektedir. Essential NetTool ile yine public IP taraması yaparak kullanılan modemlere ya da güvenlik kameralarına atak düzenlenmektedir. Ataklar gerçek zamanlı kullanılan IP bloklarına ve cihazlara yapılacaktır. Bu ataklar insan zafiyetini gözler önüne sermek için yapılmıştır. Bu atakların bertaraf edilmesi için fabrika çıkışı (default) şifrelerin değiştirilmesi gerekmektedir.

10.1 NMAP Nedir ?

Nmap ("Network Mapper"), ağdaki farklı bağlantı noktalarını (port) tarayarak güvenlik açıklarını bulmak için kullanılan açık kaynaklı bir yazılımdır. Nmap ile bir hedef sistemin ağ haritasını çıkartılarak, hedef sistemlerde hangi cihazların çalıştığını belirlemek, mevcut ana bilgisayarları ve sundukları hizmetleri keşfetmek, açık bağlantı noktaları bulmak ve güvenlik risklerini tespit etmek için de kullanılır. Nmap yapılan isteklerden gelen yanıtları dinler ve bağlantı noktalarının bir güvenlik duvarı tarafından açık, kapalı filtrelenmiş olup olmadığını belirleyebilir. Kurumsal ölçekli ağlar için geliştirilmiştir ve binlerce bağılı cihazı tarayabilir.

Hedef Belirleme

- Nmap'in en temel işlevlerinden biridir. Ağınızdaki etkin ana bilgisayarları tanımlamak için ping taraması yapılması gerekmektedir. Bunun için ilgili IP bloğunu girilir. Ping taramasını -sn parametresi kullanarak gerçekleştireceğiz. Bu parametre bağlantı noktası taramadan IP taraması yapacaktır. Bunu için kullanılacak parametre: `nmap -sn 192.168.1.0/24`
- Sadece belli bir IP adresi taraması gerçekleştireceksek `nmap 192.168.1.1` gibi parametre girilir. Bu ilgili IP de açık olan portları ve servisleri listeleyecektir. Host taramak içinde aynı şekilde `nmap Google.com` gibi taramalar gerçekleştirilebilir. İlgili parametreler ile örnekler aşağıda gösterilmektedir.

```
root@kali:~# nmap 192.168.1.39
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 02:21 +03
Nmap scan report for 192.168.1.39
Host is up (0.0013s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp

root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 02:25 +03
Nmap scan report for MitraStar.Home (192.168.1.1)
Host is up (0.0027s latency).
MAC Address: 5C:6A:80:A0:EA:E2 (Zyxel Communications)
Nmap scan report for 192.168.1.33
Host is up (0.0015s latency).
MAC Address: 70:54:B4:D2:FC:2E (Vestel Elektronik San ve Tic. A..)
Nmap scan report for 192.168.1.34
Host is up (0.015s latency).
MAC Address: B8:B7:F1:0B:71:6F (Wistron Neweb)
Nmap scan report for 192.168.1.40
Host is up (0.00021s latency).
MAC Address: 00:0C:29:C5:E8:46 (VMware)
Nmap scan report for 192.168.1.41
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.54 seconds
root@kali:~#
```

Şekil 10.1 : Nmap Nedir 1

- Belirli bir IP aralığını/bloğunu, bağlantı noktası taramayı devre dışı bırakarak, yalnızca ana bilgisayarları bulmak için `nmap 192.168.1.0/24 -sn` parametresi kullanılır.
- Bir dosyadan hedefleri taramak için `nmap -iL targets.txt` parametresi kullanılır.

```
root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 0
Nmap scan report for MitraStar.Home (192.168.1.1)
Host is up (0.0028s latency).
MAC Address: 5C:6A:80:A0:EA:E2 (Zyxel Communications)
Nmap scan report for 192.168.1.33
Host is up (0.0028s latency).
MAC Address: 70:54:B4:D2:FC:2E (Vestel Elektronik San ve Tic. A..)
Nmap scan report for 192.168.1.34
Host is up (0.015s latency).
MAC Address: B8:B7:F1:0B:71:6F (Wistron Neweb)
Nmap scan report for 192.168.1.36
Host is up (0.012s latency).
MAC Address: 00:0C:29:C5:E8:46 (VMware)
Nmap scan report for 192.168.1.40
Host is up (0.00034s latency).
MAC Address: 00:0C:29:C5:E8:46 (VMware)
Nmap scan report for 192.168.1.41
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.3
```

Şekil 10.2 : Nmap Nedir 2

10.2 NMAP Tarama Teknikleri

Nmap kullanarak bağlantı noktası taraması yapmanın birkaç yolu vardır. En yaygın olarak kullanılanlar:

- sS TCP SYN scan
- sT TCP connect scan
- sU UDP scans
- sY SCTP INIT scan
- sN TCP NULL Bu tür taramalar arasındaki en büyük fark TCP veya UDP bağlantı noktalarını kapsayıp kapsamadıkları ve bir TCP bağlantısı yürütüp yürütmedikleri. Temel farklılıklar şunlardır:
 - Bu taramalardan en temel olanı -sS TCP SYN taramasıdır ve bu çoğu kullanıcıya ihtiyaç duydukları tüm bilgileri verir. Saniyede binlerce bağlantı noktasını tarar ve bir TCP bağlantısını tamamlamadığından şüphe uyandırmaz.
 - Bu tarama türünün ana alternatifi, her ana bilgisayarı etkin bir şekilde sorgulayan ve yanıt isteyen TCP Connect taramasıdır. Bu tür tarama bir SYN taramasından daha uzun sürer, ancak daha güvenilir bilgiler döndürebilir. -sT
 - UDP taraması TCP bağlantı taramasına benzer şekilde çalışır, ancak DNS, SNMP ve DHCP bağlantı noktalarını taramak için UDP paketleri kullanır. Bunlar, bilgisayar korsanları tarafından en sık hedeflenen bağlantı noktalarıdır ve bu nedenle bu tür tarama, güvenlik açıklarını kontrol etmek için yararlı bir araçtır. -sU
 - SCTP INIT taraması farklı bir hizmet grubunu kapsar: SS7 ve SIGTRAN. Bu tür bir tarama, tüm SCTP işlemini tamamlamadığı için harici bir ağı tararken şüpheyi önlemek için de kullanılabilir. -sY
 - TOP NULL tarama aynı zamanda çok kurnaz bir tarama tekniğidir. TCP sisteminde, bağlantı noktalarını doğrudan sorgulamadan gösterebilen bir boşluk kullanır, bu da bir güvenlik duvarı tarafından korundukları yerlerde bile durumlarını görebileceğiniz anlamına gelir. -sN

İlgili resimde, en çok kullandığımız ve çoğu kullanıcıya da ihtiyaç duyduğu tüm bilgileri veren, saniyede binlerce bağlantı noktasını tarayan ve bir TCP bağlantısını

tamamlamadığından şüphe uyandırmayan -sS parametresi kullanıldı. nmap -sS 192.168.1.0/24 komutu ile ağımızdaki bütün cihazların taramasını gerçekleştirildi. Örnekte de görüldüğü gibi ev ağında buluna cihazlar listelenerek açık port ve servisler tespit edildi. Birden fazla portun açık olduğu görüntülenen 192.168.1.40 IP adresi, test için kurduğum metasploitable2 sistemimin IP adresidir. Sızma testi uzmanları veya saldırganlar bu çıktılar doğrultusunda ilgili blokta açık bulunan, tespit ettikleri port ve servisler üzerinden saldırılar gerçekleştirir. Tespit edilen servislerde zafiyetler bulunabilir ve bu zafiyetler ile sistem ele geçirilebilir veya bir sonraki adımlar için daha detaylı bir saldırı yol haritası çıkartılabilir.

```
root@kali:~# nmap -sS 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 18:04 +03
Nmap scan report for MitraStar.Home (192.168.1.1)
Host is up (0.0049s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
23/tcp    filtered  telnet
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
5431/tcp   open      park-agent
MAC Address: 98:8B:6E:4E:88:6A (Zyxel Communications)

Nmap scan report for 192.168.1.33
Host is up (0.011s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
3030/tcp   open      arepa-cas
12345/tcp  open      netbus
MAC Address: 98:8B:6E:4E:88:6A (Vestel Elektronik San ve Tic. A..)

Nmap scan report for 192.168.1.34
Host is up (0.019s latency).
All 1000 scanned ports on 192.168.1.34 are closed
MAC Address: 98:8B:6E:4E:88:6A (Wistron Neweb)

Nmap scan report for 192.168.1.35
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.35 are closed
MAC Address: 98:8B:6E:4E:88:6A (Wistron Neweb)

Nmap scan report for 192.168.1.40
Host is up (0.0012s latency).
Not shown: 977 closed ports
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    open      smtp
53/tcp    open      domain
80/tcp    open      http
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
512/tcp   open      exec
513/tcp   open      login
514/tcp   open      shell
```

Şekil 10.3 : Nmap Nedir 3

Yapılan taramaları çıktı almamız, daha sonra farklı araçlar ile saldırı yöntemleri geliştirmemize de yardımcı olacaktır. TXT ve XML çıktılarımızı metasploitable2 sistemimiz IP adresinde alacağız. XML için nmap -oX xml.xml 192.168.1.38 ve TXT çıktısı içinde nmap -oN output.txt 192.168.1.38 parametreleri kullanılmaktadır.

```
# Nmap 7.80 scan initiated Sat May 16 18:33:42 2020 as: nmap -oX xml.xml 192.168.1.38
output.txt 192.168.1.38
Nmap scan report for 192.168.1.38
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
```

Şekil 10.4 : Nmap Nedir 4

Daha hızlı tarama yapabilmemiz için ters DNS çözümlemesini devre dışı bırakmayı seçebilirsiniz. Bunun için “-n” parametresini eklemeniz yeterli olacaktır. -n parametresi DNS çözümlemesi yapma anlamına gelmektedir. Sağdaki resimde kullanılan parametreler, «-p 80» sadece 80 portunu, -n parametresi ile DNS çözümlemesi yapmadan gerçekleştirmesi istenmektedir. nmap -p 80 -n 8.8.8.8

```
root@kali:~# nmap -p 80 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 19:00 +03
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.055s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
root@kali:~# nmap -p 80 -n 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 19:01 +03
Nmap scan report for 8.8.8.8
Host is up (0.14s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
root@kali:~#
```

Şekil 10.5 : Nmap Nedir 5

İşletim sistemi ve versiyon tespiti yapabilmemiz için -A parametresi kullanacağız. -A parametresi İşletim sistemi algılama, sürüm algılama, komut dosyası tarama ve traceroute'u etkinleştirir. Sağdaki resimlerde metasploitable sistemimize yaptığımız istek yer almaktadır. Burada altı çizilen yerlerde, tespit edilen servisler, tracerouter taraması ve işletim sistemi ile ilgili bilgiler ön plana çıkartılmıştır. Tespit edilen işletim

sistemi ve servis versiyonları ile zafiyet araştırılması yapılarak, exploit çalışmaları gerçekleştirilir.

```
rootkali:~# nmap -A 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 19:22 +03
Nmap scan report for 192.168.1.38
Host is up (0.0042s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.1.41
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
IME, DSN,
|_ssl-date: 2020-05-15T21:38:19+00:00; -18h44m46s from scanner time.
|_ssl2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -18h44m46s, deviation: 0s, median: -18h44m46s
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_smb-security-mode: ERROR: Script execution failed (use -d to debug)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 4.24 ms 192.168.1.38

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.74 seconds
```

Şekil 10.6 : Nmap Nedir 6

- Hedef bağlantı noktasında çalışan hizmetlerin sürümünü belirlemek için nmap -sV 192.168.1.38 parametresi kullanılır. Sürüm tespit seviyesi 0 ile 9 arasındadır. -sV --version-all komutu, Yoğunluk seviyesi 9'u etkinleştirin ve daha yavaş bir tarama ile doğruluk olasılığı artırır.
- -O İşletim sistemi algılamayı etkinleştir. -O --osscan-limit parametresi TCP bağlantı noktası bulunursa işletim sistemi algılama çok daha etkilidir. Bu parametre kullanıldığında Nmap, ölçütleri karşılamayan ana bilgisayarlara karşı işletim sistemi algılamayı bile denemez. Bu, özellikle birçok ana bilgisayara karşı yapılan taramalarda önemli ölçüde zaman tasarrufu sağlayabilir.

```
root@kali:~# nmap -sV 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-17 00:01 +03
Nmap scan report for 192.168.1.38
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)

root@kali:~# nmap 192.168.1.38 -O --osscan-limit
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-17 00:04 +03
Nmap scan report for 192.168.1.38
Host is up (0.00092s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:C5:E8:A6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Şekil 10.7 : Nmap Nedir 7

- Gönderilen ve alınan tüm paketleri göstermesi için --packet-trace komutu kullanılır. Tarama sonunda hedef makinede açık portları ve servisleri listeler.
- -v, -vv, -vvv komutları, ekrana gösterilecek detayları artırır.
- Hızlı tarama gerçekleştirmek için -F parametresi kullanılır. Varsayılan taramadan daha az sayıda bağlantı noktası tarar.
- -T <0-5>: Zamanlama şablonunu ayarlar. Ve taradığı bloktaki bütün portları ve servisleri listeleyebilir.
- --open: Sadece açık Portları gösterir.
- nmap -P0 parametresi portlara ping atmadan açık olup olmadığını kontrol eder. ICMP kapalı sistemlerde bu parametre işe yarayabilir.
- TCP Connect Scan; nmap -sT ip_adres aynı şekilde portun açık olup olmadığını kontrol eder. Daha yavaştır ama güvenilirdir.

```
Nmap scan report for 192.168.1.40
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.1.40 are closed

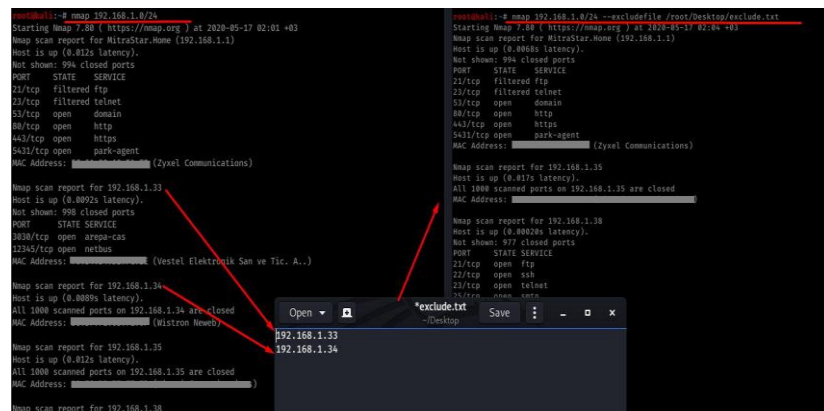
Nmap done: 256 IP addresses (4 hosts up) scanned in 4.71 seconds
root@kali:~#

Nmap scan report for 192.168.1.40
Host is up (0.000088s latency).
All 1000 scanned ports on 192.168.1.40 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.60 seconds
root@kali:~#
```

Şekil 10.8 : Nmap Nedir 8

- --host-timeout <zaman> parametresi 1s; 4m; 2s süreleri belirlenerek, belirlenen süre içerisinde hedeften yanıt gelmez ise vazgeç anlamına gelmektedir.
- --min-rate <number> ve --max-rate <number> parametreleri, tarama hızlarını doğrudan kontrol eder. Hedef ağın tarama hızının ne kadar olacağını veya ne kadar sürede bitebileceğini biliyor veya tahmin ediyorsanız bu parametreler bu gibi durumlar için çok uygundur. Veya nmap taramaların hızlı bir şekilde gerçekleşmemesi için kullanabilirsiniz. Örneğin belirtmek --min-rate 300, Nmap'ın gönderme hızını saniyede 300 paket veya üstünde tutmaya çalışacağı anlamına gelir. Benzer şekilde, --max-rate taramanın gönderme hızını belirli bir maksimuma sınırlar. Örneğin --max-rate 100 hızlı bir ağda saniyede 100 paket gönderiyle sınırlamak için kullanılır.
- XMAS Scan «-sX» komutu diğer komutların açık port bulamadığı zaman devreye girer. Hedef sisteme bütün bayrakları içeren bir paket yollar, kapalı olan portların RST cevabı beklenir. Kapalı portlar cevap verdikten sonra cevap gelmeyen portlar açık olarak kabul edilir. nmap -sX ip_adres
- UDP taramaları gerçekleştirebilmek için «-sU» komutu kullanılır. Bu komut açık olan UDP portlarını tespit için kullanılır. nmap -sU ip_adres
- Tarama yapılacak bir blokta, tarama yapılmaması istenilen IP adreslerini –excludefile parametresi ile hariç tutulur. nmap 192.168.1.0/24 –excludefile exclude.txt Aşağıdaki örnek tarama resminin bir kısmında, normal taradığımızda elde ettiğimiz IP adresleri ve bu adreslere bağlı bilgiler yer almaktadır. Diğer bir kısmında ise –excludefile komutu kullanarak, normal taramada elde ettiğimiz birkaç IP adresini bir TXT dosyasına ekleyerek, --excludefile komutu ile taramasını engellediğimiz sonuç yer almaktadır.



Şekil 10.9 : Nmap Nedir 9

- Nmap güvenlik duvarı TCP ACK taraması yapmak için, hedef bağlantı adresi ve `-sA` komutu ile Nmap çağrılmalıdır. Herhangi bir portun filtreleneip filtrelenmediğini belirlemeye çalışır. Bu teknik, herhangi bir ana bilgisayarı koruyan güvenlik duvarının durum bilgisini kontrol etmek için kullanışlıdır. `nmap -sA «ip_adres»` bu taramaya `-p80` komutu ekleyerek, ilgili IP adresteki sadece istenilen portu taramasını isteyebilirsiniz. Veya başka komutlar ile taramanızın kapsamını genişletebilirsiniz.
- Firewall ile koruna bir hosts `--PN` parametresi ile taranabilir. Bu seçenek, Nmap keşif aşamasını tamamen atlar.

```

root@kali:~# nmap -sA 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-17 02:22 +03
Nmap scan report for MitraStar.Home (192.168.1.1)
Host is up (0.016s latency).
Not shown: 998 unfiltered ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
23/tcp    filtered  telnet
MAC Address: 9C:60:08:00:00:02 (Zykel Communications)

Nmap scan report for 192.168.1.33
Host is up (0.0067s latency).
All 1000 scanned ports on 192.168.1.33 are unfiltered
MAC Address: 08:00:27:00:00:00 (Vestel Elektronik San ve Tic. A..)

Nmap scan report for 192.168.1.34
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.34 are unfiltered
MAC Address: 08:00:27:00:00:00 (Wistron Neweb)

Nmap scan report for 192.168.1.40
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.1.40 are unfiltered
MAC Address: 08:00:27:00:00:00 (VMware)

Nmap scan report for 192.168.1.37
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.1.37 are unfiltered

Nmap done: 256 IP addresses (5 hosts up) scanned in 3.09 seconds

```

Şekil 10.10 : Nmap Nedir 10

10.3 NMAP Tarama Teknikleri - NSE Scripts

Nmap Scripting Engine” (NSE) dosyası oluşturma altyapısı, kullanıcıların önceden tanımlanmış bir komut dosyası seti kullanmalarına veya Lua programlama dilini kullanarak kendi komut dosyalarını yazmalarına olanak tanır. Sistem ve güvenlik açığı

taramalarını otomatikleştirmek için NSE kullanmak çok önemlidir. NSE ile güvenlik açığı taramasını, güvenlik zafiyetlerin bulunduğu metasploitable2 sistemimiz üzerinden test edeceğiz. Kullanılacak komut: `nmap -Pn --script vuln 192.168.1.40` Sağdaki resimde görüldüğü üzere tespit ettiği güvenlik zafiyetlerini CVE kodları ve zafiyet referansları ile birlikte bildirmektedir. İlgili zafiyetli makinede daha fazla güvenlik zafiyeti tespit edilmiştir. Bu görüntülerde örnek amaçlı bir kısım gösterilmektedir.

```
root@kali: ~ 192x33
or insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
  WEAK DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: Unknown/Custom-generated
    Modulus Length: 1024
    Generator Length: 8
    Public Key Length: 1024
  References:
    https://weakdh.org
- ssl-poodle:
  VULNERABLE:
  SSL POODLE information leak
  State: VULNERABLE
  IDs: CVE:CVE-2014-3566 BID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
    products, uses nondeterministic CBC padding, which makes it easier
    for man-in-the-middle attackers to obtain cleartext data via a
    padding-oracle attack, aka the "POODLE" issue.
  Disclosure date: 2014-10-14
  Check results:
    TLS_RSA_WITH_AES_128_CBC_SHA
  References:
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
    https://www.openssl.org/~bodo/ssl-poodle.pdf
    https://www.securityfocus.com/bid/70574
    https://www.insecure.org/p3k/ssl/3.0/faq/faq3.html
- Slowloris DOS attack
  State: LIKELY VULNERABLE
  IDs: CVE:CVE-2007-6750
    Slowloris tries to keep many connections to the target web server open and hold
    them open as long as possible. It accomplishes this by opening connections to
    the target web server and sending a partial request. By doing so, it starves
    the http server's resources causing Denial Of Service.
  Disclosure date: 2009-09-17
  References:
    http://ha.ckers.org/slowloris/
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
- MAC Address: 00:0C:29:C5:E8:46 (VMware)
Host script results:
  _smb-double-pulsar-backdoor: ERROR: Script execution failed (use -d to debug)
  _smb-vuln-cve-2017-7494: ERROR: Script execution failed (use -d to debug)
  _smb-vuln-ms06-025: ERROR: Script execution failed (use -d to debug)
  _smb-vuln-ms07-029: ERROR: Script execution failed (use -d to debug)
  _smb-vuln-ms08-067: ERROR: Script execution failed (use -d to debug)
  _smb-vuln-ms10-054: false
  _smb-vuln-ms10-061: false
  _smb-vuln-ms17-010: ERROR: Script execution failed (use -d to debug)
  _smb-vuln-regsvcs: ERROR: Script execution failed (use -d to debug)
```

Şekil 10.11 : Nmap Nedir 11

Nmap taramalarını XML çıktısı olarak metasploit gibi içerisinde ürün ve servislerin zafiyetleri bulunduğu araçlarda otomatik taramalar gerçekleştirebilirsiniz. Sızma

testlerinde yapılan önemli işlemlerden birisidir. Bir bloğa Nmap taraması yaparak XML çıktısını bu gibi araçlarda zafiyet kontrolleri oldukça faydalıdır.

```
or insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
  WEAK DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: Unknown/Custom-generated
    Modulus Length: 1024
    Generator Length: 8
    Public Key Length: 1024
References:
  https://weakdh.org
ssl-poodle:
VULNERABLE:
  SSL POODLE information leak
  State: VULNERABLE
  IDs: CVE-2014-3566 BID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
    products, uses nondeterministic CBC padding, which makes it easier
    for man-in-the-middle attackers to obtain cleartext data via a
    padding-oracle attack, aka the "POODLE" issue.
  Disclosure date: 2014-10-14
  Check results:
    TLS_RSA_WITH_AES_128_CBC_SHA
  References:
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
    https://www.openssl.org/~bodo/ssl-poodle.pdf
    https://www.securityfocus.com/bid/70574
    https://www.exploit-db.com/exploits/6944/ssl-poodle.html

Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE:2007-6750
  Slowloris tries to keep many connections to the target web server open and hold
  them open as long as possible. It accomplishes this by opening connections to
  the target web server and sending a partial request. By doing so, it starves
  the http server's resources causing Denial Of Service.

  Disclosure date: 2009-09-17
  References:
    http://hackers.org/slowloris/
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
MAC Address: 00:0C:29:C5:E8:46 (VMware)

Host script results:
_smb-double-pulsar-backdoor: ERROR: Script execution failed (use -d to debug)
_smb-vuln-cve-2017-7494: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms06-025: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms07-029: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms08-067: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: false
_smb-vuln-ms17-010: ERROR: Script execution failed (use -d to debug)
_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
```

Şekil 10.12 : Nmap Nedir 12

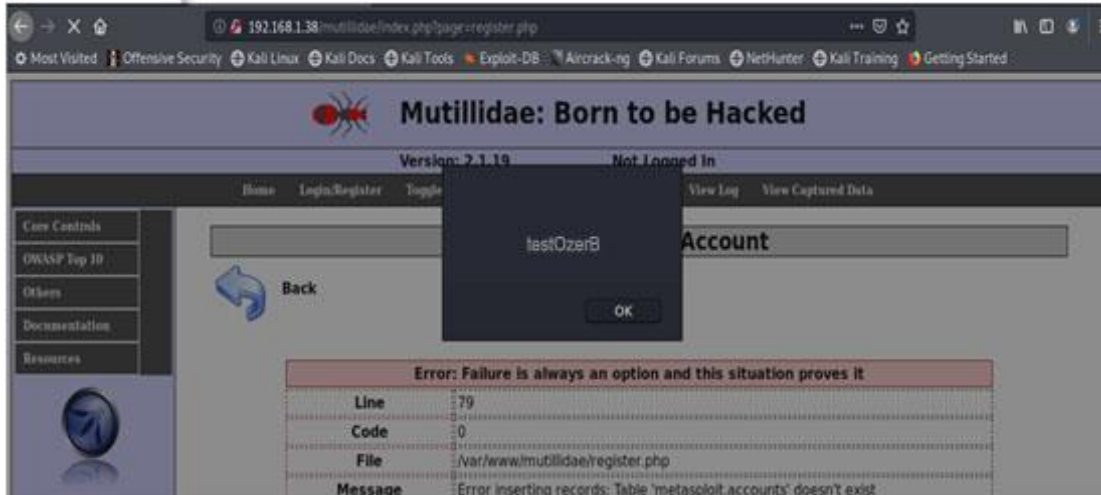
- Tek bir komut dosyası ile taramak için -- script=banner komutu kullanılır. Sağdaki görüntüde ilgili komut kullanıldığında elde edilen sonuç gösterilmektedir.
- Özel bir karakter taramak için --script=http* komutu kullanılır.
- Standar tarama yapmak fakat ilgili zafiyete müdahale etmesini istemiyorsanız --script "not intrusive komutu kullanılabilir.
- Whois sorgulaması için nmap --script whois* domain.com komutu kullanılır.

- Hedef adreste SQL injection olup olmadığını kontrol eden komut: `nmap -p80 --script http-sql-injection scanme.nmap.org`
- XSS tespiti için `nmap -p80 --script http-unsafe-output-escaping site_adı.com` veya `IP_adres` komutu kullanılabilir. Sağdaki komut satırında metasploitable2 makinemizde XSS keşfettiğimize dair bilgiler mevcut. Burada yer alan URL'lere giderek XSS denemeleri gerçekleştirebilirsiniz. Bir alt görüntüde XSS tespit edilen URL'de (`http://192.168.1.38:80/mutillidae/index.php?page=register.php`) XSS denemesi gerçekleştirilerek başarılı sonuç elde edilmiştir.

```
root@kali:~# nmap -p80 --script http-unsafe-output-escaping 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-17 05:27 +03
Nmap scan report for 192.168.1.38
Host is up (0.00029s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-unsafe-output-escaping:
| Characters [ > " ' ] reflected in parameter page at http://192.168.1.38:80/mutillidae/index.php?page=home.php
| Characters [ > " ' ] reflected in parameter page at http://192.168.1.38:80/mutillidae/?page=show-log.php
| Characters [ > " ' ] reflected in parameter page at http://192.168.1.38:80/mutillidae/index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
|_ Characters [ > " ' ] reflected in parameter page at http://192.168.1.38:80/mutillidae/index.php?page=register.php
MAC Address: 00:0C:29:C5:E8:46 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
root@kali:~#
```



Şekil 10.13 : Nmap Nedir 13

- Yapılan Nmap taramalarında, Firewall/IDS sistemlerinden gizlenerek tarama gerçekleştirebilmek için `-f` komutu kullanılabilir. Bu komut ile yapılan tarama (ping

taramaları dahil) küçük parçalanmış IP paketleri kullanır. Paket filtreleri için daha zordur. Nmap 192.168.1.1 -f

- Nmap'de -S komutu kimlik kaynağı, kaynak adresi anlamına gelmektedir. Bir başka kullanımı ise hedeflerin başka birinin olduğunu düşünmesini sağlamak için taramayı taklit etmektir. Bu işlemleri yaparken -e <iface>, ve -Pn komutlarında kullanılır. İface alanına belirtmek istenilen arabirim kullanılır. Yukarıdaki resimde ilgili komut kullanılmıştır. Windows cihazının IP adresi olan 192.168.1.36'den, 192.168.1.37 (Metasploitable2) sistemine istek yapılmıştır. Tcpdump ile de o anki ağ trafiği dinlenerek sonuç görüntülenmiştir. -Pn, tüm ana bilgisayarlara çevrimiçi olarak davran - ana bilgisayar keşfini atla anlamına gelmektedir.

Proxychains uygulaması ile Tor ağı kullanılarak nmap taraması yapmak için ilk önce tarama yapacağımız sistemde tor yüklü olması gerekmektedir. Apt-get install tor komutu ile yüklenebilir. Proxychains uygulaması TOR network'ünü kullanacak şekilde yapılandırılması gerekmektedir. nano /etc/proxychains.conf komutu ile konfigürasyon dosyasına ulaşarak, socks4 127.0.0.1 9050 değeri socks5 127.0.0.1 9050 olarak değiştirebiliriz. Socks4 ve socks5 arasında authentication vb. farklılıklar vardır. Tor ağıımız aktif olduğunu ve ilgili IP adres ve port'un tor ile ilişkilendirildiğini sağ alttaki resimde görebilirsiniz. Burada ilk önce IP kontrol yapıyoruz daha sonra tor doğru IP ve port ile ilişkisini kontrol ediyoruz. Şimdi taramayı kali sistemimizden metasploitable sistemimize gerçekleştireceğiz. Kullanacağım komut: proxychains nmap -p 1-65535 -T4 -A -v -Pn 192.168.1.41 Ayrıca direkt socks4 veya socks5 ile nmap -p22 -Pn -n --proxies socks4://127.0.0.1:9050 192.168.1.41 komutu ile direkt taramada gerçekleştirebilirsiniz. İlgili taramalarda kullandığımız -n parametresi, bir proxy üzerinden tarama yaparken, Nmap'e her zaman keşfettiği IP'lerde ters DNS çözümlemesi yapmaktan kaçınmasını söylemeliyiz. Bunun nedeni, IP adresinizin DNS istekleri aracılığıyla dolaylı olarak sızdırılabilmesidir. Tünel olmadan ters DNS çözümlemesi yapmak istemezsiniz. Bu nedenle, ad çözümlemesini atlamak önemlidir. Nmap taraması yaparken -n parametresini bir proxy ile bu yüzden kullanırız. Not: Tor tarayıcıyı kullanmadığınızda tor üzerinden trafik gönderme konusunda son derece dikkatli olun. Şifrelenmemiş trafik potansiyel olarak kötü amaçlı bir çıkış düğümü tarafından görülecektir.

```
root@kali:~# proxychains nmap -p 1-65535 -T4 -A -v -Pn 192.168.1.41
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 06:53 +03
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:53
Completed NSE at 06:53, 0.00s elapsed
Initiating NSE at 06:53
Completed NSE at 06:53, 0.00s elapsed
Initiating NSE at 06:53
Completed NSE at 06:53, 0.00s elapsed
Initiating ARP Ping Scan at 06:53
Scanning 192.168.1.41 [1 port]
Completed ARP Ping Scan at 06:53, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:53
Completed Parallel DNS resolution of 1 host. at 06:53, 0.02s elapsed
root@kali:~# proxychains nmap -Pn -n -sT 192.168.1.41
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 06:53 +03
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:1723-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:143-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:8888-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:110-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:5900-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:22-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:80-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:25-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:113-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:443-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:23-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:3389-<->
S-chain|<-127.0.0.1:9050-<->-192.168.1.41:3306-<->
root@kali:~# tcpdump -i any -n | grep 192.168.1.41

root@kali:~# proxychains curl http://icanhazip.com
ProxyChains-3.1 (http://proxychains.sf.net)
DNS-request| icanhazip.com
S-chain|<-127.0.0.1:9050-<->-4.2.2.2:53-<->-OK
S-chain|<-127.0.0.1:9050-<->-4.2.2.2:53-<->-OK
DNS-response| icanhazip.com is 116.202.55.106
S-chain|<-127.0.0.1:9050-<->-116.202.55.106:80-<->-OK
188.213.49.176
root@kali:~#

root@kali: ~ 106x14
06:16:37.669932 IP 167.172.147.227.443 > 192.168.1.36.6874: Flags [.], ack 2043482466, win 501, options
op,nop,sack 1 {0:1}], length 0
06:16:38.079567 IP 157.240.9.53.443 > 192.168.1.36.6858: Flags [.], ack 3476572574, win 205, length 0
06:16:38.197685 IP 157.240.9.53.443 > 192.168.1.36.6858: Flags [P.], seq 0:38, ack 1, win 205, length 38
06:16:39.252672 ARP, Request who-has 192.168.1.39 tell 192.168.1.1, length 46
^C
7 packets captured
7 packets received by filter
0 packets dropped by kernel
root@kali:~# netstat -tanp | grep tor
tcp        0      0 127.0.0.1:9050        0.0.0.0:*               LISTEN      46797/tor
tcp        0      0 192.168.1.37:48472    5.189.181.61:443      ESTABLISHED 46797/tor
```

Şekil 10.14 : Nmap Nedir 14

- Nmap ile düzenli bir ARP paket isteği gerçekleştirerek, cihazın IP adresini ile MAC adresini aramak için kullanılan komut -PR'dir. Örnek komut kullanımı: nmap -sP -PR 192.168.1/24 burada ek olarak kullanıla -sP komutu, ping'e yanıt veren makineleri listeleterek ağı taraması için verilebilir. Kullanılan komut sonrası elde edilen sonuç yukarıdaki resimdedir.

- `nmap -sn --send-ip 192.168.0.*` komutu, tarama kuvvetleri ve ip bir arp taraması üzerinde, yine joker karakteri kullanarak son sekizli üzerinde tarar.
- `nmap -sn --disable-arp-ping 192.168.0.*` komutundaki – Disable-arp-ping bayrağını ekleyerek, ARP protokolünü devre dışı bırakırsanız benzer bir çıktı ve zamanlama gerçekleştirilebilir. Yerel ağda Nmap kullanırken, resmi verilere göre daha hızlı ve daha güvenilir olması için ARP protokolü varsayılan olarak uygulanır, Nmap'yi yerel bir ağ içinde Internet Protokolü'nü kullanmaya zorlamak için flag `-send-ip`'i kullanılabilir.

```

root@kali:~# nmap 192.168.1.1/24 -PR
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 23:15 +03
Nmap scan report for MitraStar.Home (192.168.1.1)
Host is up (0.0097s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
23/tcp    filtered telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
5431/tcp  open  park-agent
MAC Address: 00:0C:87:00:EA:E2 (Zyxel Communications)

Nmap scan report for 192.168.1.33
Host is up (0.0036s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
3030/tcp  open  arepa-cas
12345/tcp open  netbus
MAC Address: 08:00:27:00:02:FC:2E (Vestel Elektronik San ve Tic. A..)

Nmap scan report for 192.168.1.34
Host is up (0.0079s latency).
All 1000 scanned ports on 192.168.1.34 are closed
MAC Address: 08:00:27:00:0B:71:6F (Wistron Neweb)

Nmap scan report for 192.168.1.39
Host is up (0.0067s latency).
Not shown: 799 filtered ports, 200 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync
MAC Address: 08:00:27:00:06:2:7C (Apple)

```

Şekil 10.15 : Nmap Nedir 15

Nmap, tarama hızını kontrol etmek için birçok ayrıntılı seçenek sunar. Çoğu kişi bu seçenekleri Nmap'i hızlandırmak için kullanır, ancak Nmap'ı yavaşlatmak için de oldukça yararlıdır. Bu özellikler ile IDS sistemlerinden kaçınmak, ağ yükünü azaltmak veya hatta ağ koşullarına göre doğruluğu artırmak için de yapıyoruz.

- Nmap, birden çok ana bilgisayarı paralel olarak bağlantı noktası tarama veya sürüm tarama özelliğine sahiptir. Nmap bunu hedef IP alanını gruplara bölerek ve ardından bir kerede bir grup tarayarak yapar. `--min-hostgroup <numhosts>;` komutu ile Paralel tarama grubu boyutlarını ayarlayabilirsiniz. Dezavantajı, tüm grup bitene kadar ana bilgisayar sonuçlarının sağlanamamasıdır. Bu nedenle, Nmap 50 kişilik bir grupla başlarsa, kullanıcı ilk 50 ana bilgisayar tamamlanana kadar herhangi bir rapor almaz.
- `--min-parallelism <numprobes>;` komutu, bir ana makine grubu için olağanüstü olabilecek toplam prob sayısını kontrol eder. Bağlantı noktası tarama ve ana bilgisayar bulma için kullanılır. Paketler düşürülüyorsa, Nmap yavaşlar ve daha az olağanüstü prob sağlar.
- Tarama hızını doğrudan kontrol eden, kullandığım Nmap komutu ise `--min-rate <number>;`'dir. Tarama yapılırken uygun bir hız bulmak için idealdir. Bununla birlikte, bazen, bir ağ için uygun bir tarama hızı biliyor olabilirsiniz veya bir taramanın belirli bir zamana kadar biteceğini garanti etmeniz gerekebilir. Ya da Nmap'in çok hızlı bir şekilde taramasını engellemelisiniz. `--min-rate` ve `--max-rate` seçenekleri bu tür durumlar için tasarlanmıştır. Örneğin, Nmap'ın gönderme hızını saniyede 300 paket veya üstünde tutması için `--min-rate 300` kullanılır [66].

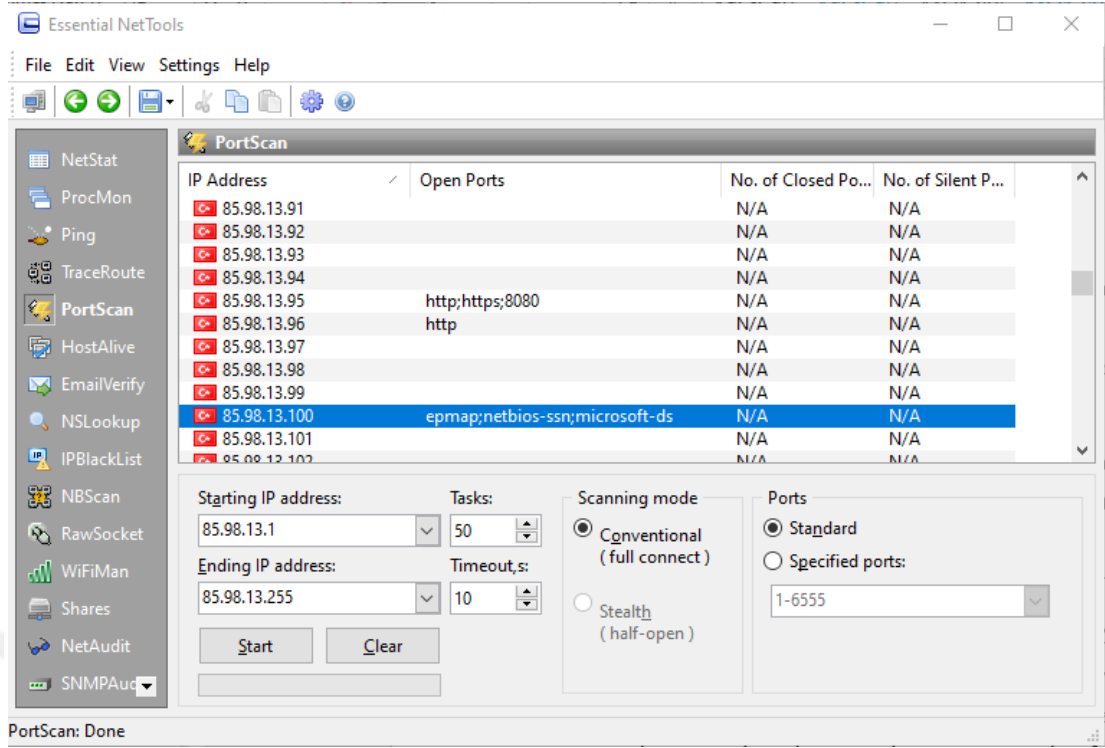
```
root@kali:~# nmap 192.168.1.37 -sT -sV -Pn -n -vvv --min-rate 5000 --min-hostgroup 256 --min-parallelism 1000
Warning: You specified a highly aggressive --min-hostgroup.
Warning: Your --min-parallelism option is pretty high! This can hurt reliability.
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 05:18 +03
NSE: Loaded 45 scripts for scanning.
Initiating Connect Scan at 05:18
Scanning 192.168.1.37 [1000 ports]
Discovered open port 111/tcp on 192.168.1.37
Discovered open port 23/tcp on 192.168.1.37
Discovered open port 3306/tcp on 192.168.1.37
Discovered open port 445/tcp on 192.168.1.37
Discovered open port 139/tcp on 192.168.1.37
Discovered open port 53/tcp on 192.168.1.37
Discovered open port 25/tcp on 192.168.1.37
Discovered open port 22/tcp on 192.168.1.37
Discovered open port 80/tcp on 192.168.1.37
Discovered open port 21/tcp on 192.168.1.37
Discovered open port 5900/tcp on 192.168.1.37
Discovered open port 2049/tcp on 192.168.1.37
Discovered open port 1524/tcp on 192.168.1.37
Discovered open port 8180/tcp on 192.168.1.37
Discovered open port 513/tcp on 192.168.1.37
Discovered open port 6000/tcp on 192.168.1.37
Discovered open port 6667/tcp on 192.168.1.37
Discovered open port 512/tcp on 192.168.1.37
Discovered open port 8009/tcp on 192.168.1.37
Discovered open port 514/tcp on 192.168.1.37
Discovered open port 5432/tcp on 192.168.1.37
Increasing send delay for 192.168.1.37 from 0 to 5 due to 265 out of 881 dropped probes since last
Discovered open port 2121/tcp on 192.168.1.37
Discovered open port 1099/tcp on 192.168.1.37
Completed Connect Scan at 05:18, 0.28s elapsed (1000 total ports)
Initiating Service scan at 05:18
```

Şekil 10.16: Nmap Nedir 16

10.4 Essential NetTools

Essential NetTools, ağları tanılamada ve bilgisayarınızın ağ bağlantılarını izlemede yararlı olan bir dizi ağ tarama, güvenlik ve yönetici aracıdır. Günlük kullanım için güçlü bir ağ araç kitiyle ilgilenen herkes için bir İsviçre Çakısıdır.

- NetStat: açık TCP ve UDP bağlantı noktaları, IP adresi ve bağlantı durumları hakkındaki bilgiler de dahil olmak üzere bilgisayarınızın gelen ve giden ağ bağlantılarının bir listesini görüntüler. Onu diğer NetStat yardımcı programlarından farklı kılan şey, açık bağlantı noktalarını sahip olunan uygulamayla eşleme yeteneğidir. Gelen ve giden bağlantılar için yapılandırılabilir uyarılar da mevcuttur.
- NBScan: güçlü ve hızlı bir NetBIOS tarayıcısı. NBScan, belirli bir IP adresi aralığındaki bir ağı tarayabilir ve NetBIOS kaynak paylaşım hizmeti sunan bilgisayarların yanı sıra ad tabloları ve MAC adreslerini listeleyebilir. Windows ile sağlanan standart nbtstat yardımcı programından farklı olarak, bu araç bir grafik kullanıcı arabirimi ve lmhosts dosyasının kolay yönetimini sağlar ve paralel tarama özelliğine sahiptir, bu da C sınıfı bir ağı bir dakikadan daha kısa sürede kontrol etmeye olanak tanır. NBScan, genellikle sistem entegratörleri, yöneticiler ve analistler tarafından gerçekleştirilen rutin görevleri kolaylaştırabilir.
- PortScan : ağınıza aktif portlar için taramanıza izin veren gelişmiş bir TCP port tarayıcı. Bu araç hem geleneksel (tam bağlantı) hem de gizli (yarı açık) tarama modlarına sahiptir.
- HostAlive : bir ana bilgisayarın canlı olup olmadığını ve HTTP veya FTP sunucusu gibi ağ hizmetlerini çalıştırıp çalıştırmadığını düzenli olarak kontrol eden bir ağ izleme aracı.
- EmailVerify : SMTP üzerinden ilgili posta sunucusuyla iletişim kurarak bir e-posta adresinin geçerli olup olmadığını kontrol eder.
- Paylaşımlar : Bilgisayarınızın paylaşılan kaynaklarına yapılan harici bağlantıları izler ve günlüğe kaydeder, yerel paylaşımları listeler ve ayrıca uzak kaynaklara bağlanmak için hızlı ve kolay bir yol sağlar.
- SysFiles : beş önemli sistem dosyası için uygun bir düzenleyici: hizmetler, protokol, ağlar, ana bilgisayarlar ve lmhost'lar.



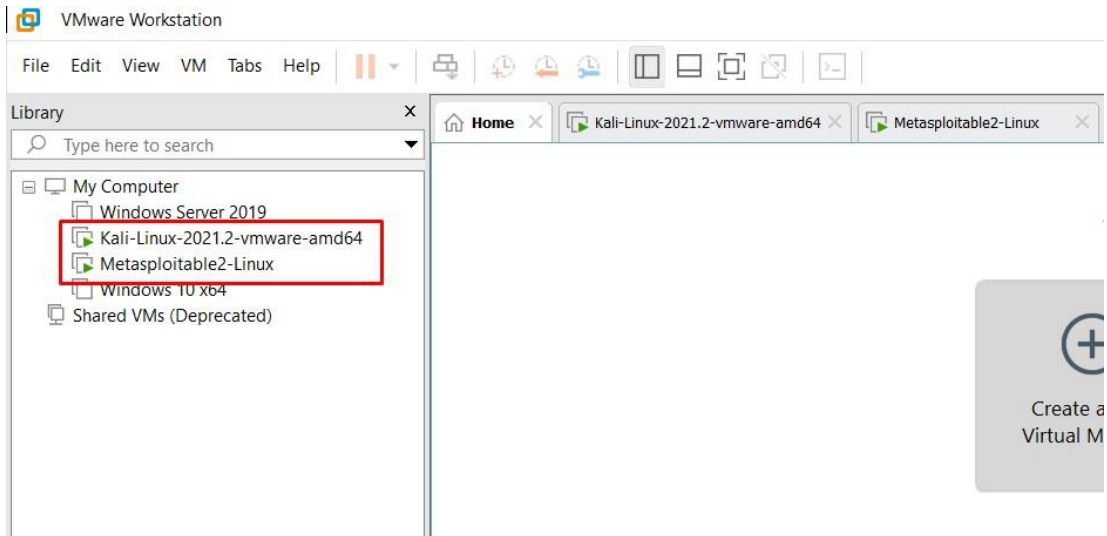
Şekil 10.17: Essential NetTools

- NetAudit (NetBIOS Denetim Aracı): ağınızda ve/veya NetBIOS dosya paylaşım hizmeti sunan bireysel bilgisayarlarda çeşitli güvenlik kontrolleri yapmanızı sağlar. Bu araç, olası güvenlik açıklarını belirlemenize yardımcı olabilir.
- RawSocket: farklı ağ hizmetlerinde sorun gidermek ve test etmek için size düşük seviyeli TCP ve UDP bağlantıları kurma yeteneği sağlar. Çok renkli çıktı ve kullanışlı bir arayüz, onu her ağ yöneticisi veya bilgisayar programcısı için harika bir araç haline getirir.
- WiFiMan: bir bilgisayarda kurulu kablosuz bağdaştırıcıları gösterir, kullanılabilir kablosuz ağları listeler ve bağlantı profillerini yönetmenize olanak tanır.
- TraceRoute ve Ping: Özelleştirilebilir seçenekler ve kullanışlı sonuç sunumu içeren bu tanıdık yardımcı programlar, İnternet'i keşfetmenize ve bağlantı sorunlarını gidermenize olanak tanır.
- NSLookup: IP adreslerini ana bilgisayar adlarına veya tam tersine dönüştürmenize, takma adlar almanıza ve MX veya CNAME gibi gelişmiş DNS sorguları gerçekleştirmenize olanak tanır.

- IPBlackList: bir IP adresinin farklı IP adresi kara listelerinde olup olmadığını kontrol eder: SPAM veritabanları, açık proxy'ler ve posta geçişleri, vb. Bu araç, belirli bir IP adresinin posta sunucuları gibi bazı ağ kaynakları tarafından neden reddedildiğini anlamamıza yardımcı olur.
- ProcMon: Programın konumu, üretici ve işlem kimliği ile yüklenen modüller hakkında tam bilgilerle birlikte çalışan işlemlerin listesini görüntüler. Bu araçla, CPU kullanım istatistiklerini görüntüleyebilir, gizli uygulamaları belirleyebilir, çalışan işlemleri sonlandırabilir ve bilgisayarınızın kaynaklarının kullanımını daha etkin bir şekilde yönetebilirsiniz.
- SNMPaudit: Gelişmiş SNMP cihaz tarayıcısı. Seçilen ağ segmentindeki SNMP cihazlarını hızlı bir şekilde bulmanıza ve her bir cihazdan özelleştirilebilir veri örnekleme almanıza olanak tanır. Bir cihazı detaylı olarak incelemek için SNMP tarayıcısını kullanabilirsiniz. Diğer özellikler arasında HTML, metin ve virgülle ayrılmış biçimlerde rapor oluşturma; farklı araçlar arasında hızlı IP adresi paylaşımı; IP adresi coğrafi konumu; kapsamlı bir Sistem Özeti penceresi ve özelleştirilebilir bir arayüz bulunmaktadır [67].

10.5 NMAP Uygulama Taraması ve Essential NetTools Taraması.

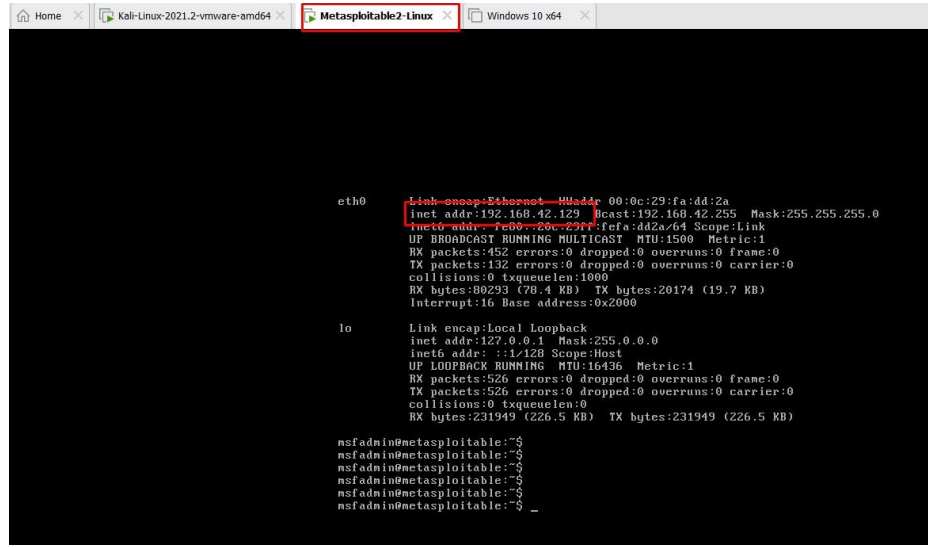
Kali Linux toolu olan NMAP uygulamasının, bilgi toplama ve saldırı konusundaki etkilerini göstermek için bir uygulama gerçekleştirilmiştir. Bu uygulama şu şekilde gerçekleştirilmiştir.



Şekil 10.18: WMware Ekranı

Windows İşletim sistemlerinde Kali Linux tarzı işletim sistemlerini birlikte kullanmak için VMware uygulaması kullanılmaktadır. VMware Windows işletim sistemleri için sanallaştırma teknolojisini kullanan bir yardımcı programdır. Windows işletim sistemlerine birden fazla sanal işletim sistemi kurmak için kullanılmaktadır.

Test amaçlı, Kali Linux araçları ve saldırı yapmak için açıkları bulunan Metasploit işletim sistemi kuruldu. Metasploit genellikle labarotuar ortamında test amaçlı kullanılan ve açık portları bulunan Linux tabanlı bir işletim sistemidir.



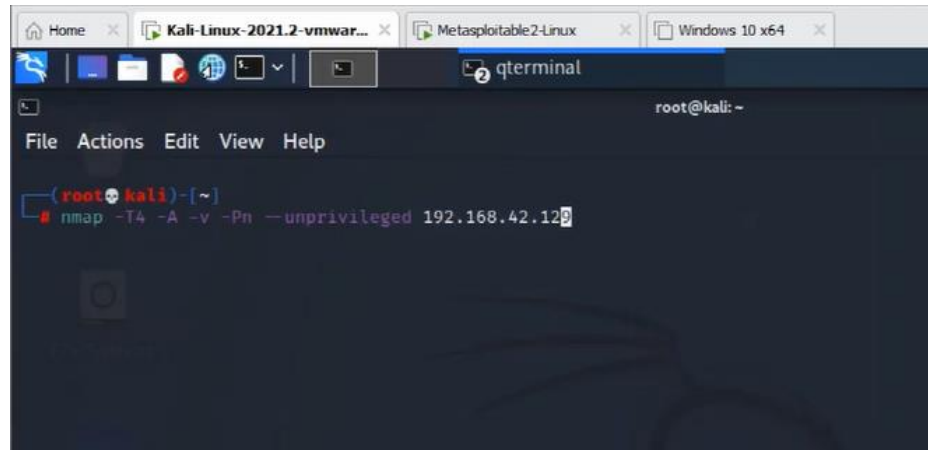
```
eth0      Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.42.129 Bcast:192.168.42.255 Mask:255.255.255.0
          inet6 addr: fe80::c00:720c:2314:fe64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:452 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:80293 (78.4 KB)  TX bytes:20174 (19.7 KB)
          Interrupt:16 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:526 errors:0 dropped:0 overruns:0 frame:0
          TX packets:526 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:231949 (226.5 KB)  TX bytes:231949 (226.5 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

Şekil 10.19: Metasploit2 Ekranı

Şekil 10.19 da Metasploit sisteminin IP adresi görülmektedir. Kali Linux işletim sisteminden bu IP numarasına ilgili NMAP taraması gerçekleştirilecektir.

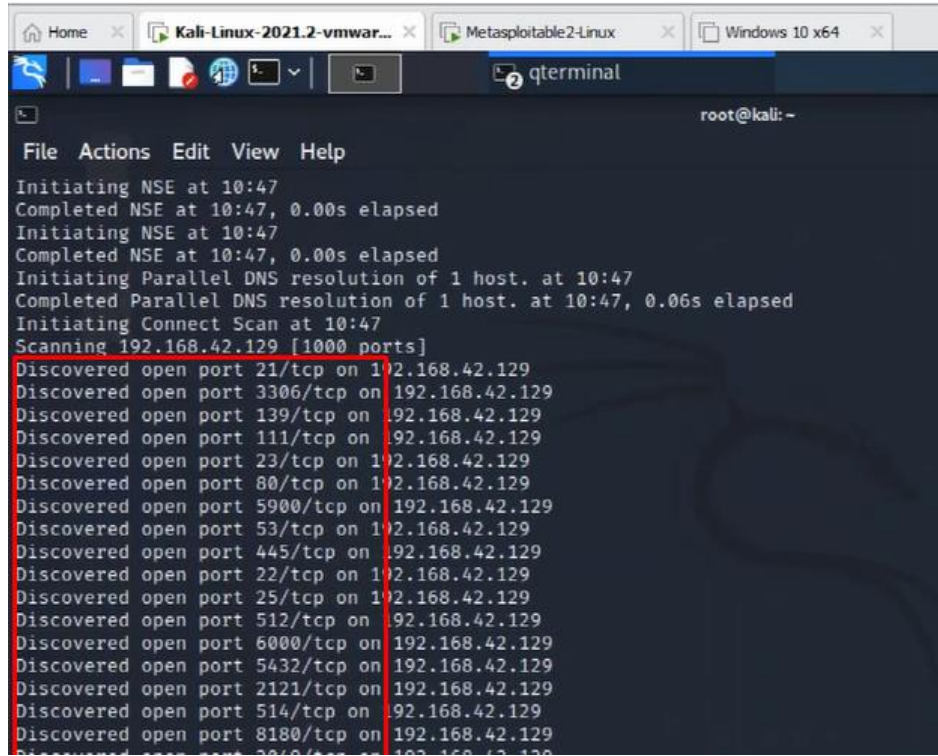


```
root@kali: ~
File Actions Edit View Help

(root@kali)~[~]
# nmap -T4 -A -v -Pn --unprivileged 192.168.42.129
```

Şekil 10.20: Kali Linux Terminal Ekranı

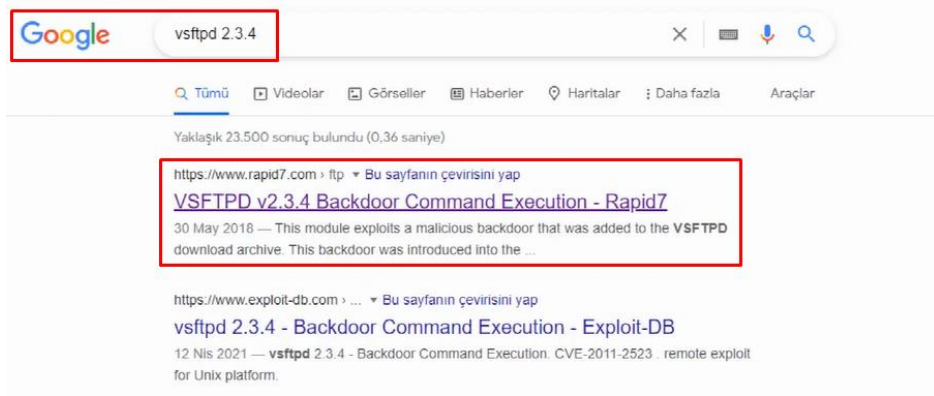
Nmap -T4 -A -v -Pn -unprivileged 192.168.42.129 komutuyla NMAP taramamızı başlatıyoruz. Şekil 10.20’de tarama sonrası ortaya çıkan port açıkları görülmektedir. Bu açıklıklara hangi saldırı türlerini kullanarak atak yapacağımız görülmektedir. Bu açıklıklara exploit yapılacaktır. Exploit’in kelime anlamı incelendiği zaman “istismar etmek”, “faydalanmak”, “sömürmek” anlamlarına gelmektedir.



```
File Actions Edit View Help
Initiating NSE at 10:47
Completed NSE at 10:47, 0.00s elapsed
Initiating NSE at 10:47
Completed NSE at 10:47, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 10:47
Completed Parallel DNS resolution of 1 host. at 10:47, 0.06s elapsed
Initiating Connect Scan at 10:47
Scanning 192.168.42.129 [1000 ports]
Discovered open port 21/tcp on 192.168.42.129
Discovered open port 3306/tcp on 192.168.42.129
Discovered open port 139/tcp on 192.168.42.129
Discovered open port 111/tcp on 192.168.42.129
Discovered open port 23/tcp on 192.168.42.129
Discovered open port 80/tcp on 192.168.42.129
Discovered open port 5900/tcp on 192.168.42.129
Discovered open port 53/tcp on 192.168.42.129
Discovered open port 445/tcp on 192.168.42.129
Discovered open port 22/tcp on 192.168.42.129
Discovered open port 25/tcp on 192.168.42.129
Discovered open port 512/tcp on 192.168.42.129
Discovered open port 6000/tcp on 192.168.42.129
Discovered open port 5432/tcp on 192.168.42.129
Discovered open port 2121/tcp on 192.168.42.129
Discovered open port 514/tcp on 192.168.42.129
Discovered open port 8180/tcp on 192.168.42.129
```

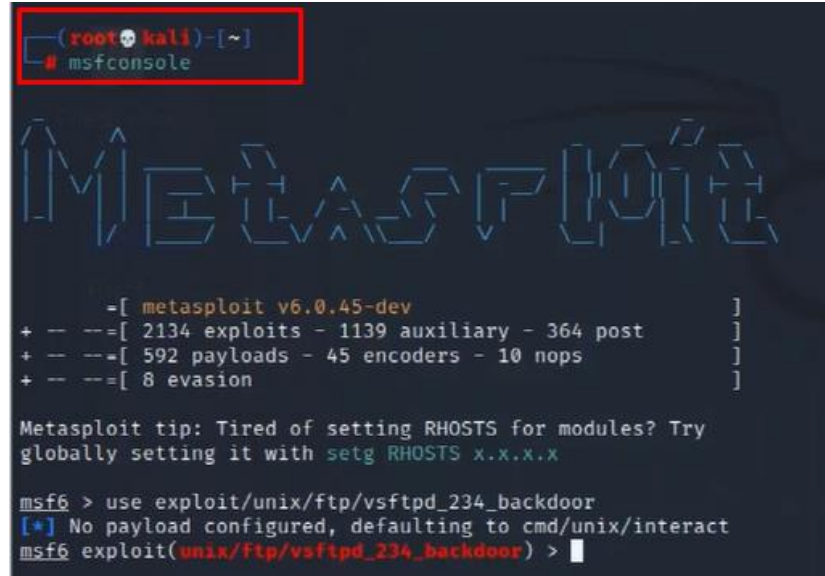
Şekil 10.21: Kali Linux Ekranı Sonuç Ekranı

Bu taramadan elde edilen bilgiler ışığında 21 portunun açıklıklarından faydalanarak saldırı yapılacaktır. Tarama sonrası 21 Portunun karşısında “vsftpd 2.3.4” yazmaktadır. Bu kodu web tarayıcısına yazıp, çıkan sayfada ilgili linke tıklayarak exploit’in nasıl kullanıldığına bakılmaktadır.



Şekil 10.22: Google Tarama Keranı

Kali Linux'un terminal penceresinden ilgili komutları yazarak saldırı gerçekleştirilecektir.



Şekil 10.23: Kali Linux Terminal Saldırı Ekranı

msfconsole yazarak ilgili araç aktive edilmektedir. Daha sonra `use exploit/unix/ftp/vsftpd_234_backdoor` komutu yazılır. Komut sonucu ilgili port için kullanılacak bilgiler çıkmaktadır.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    21               yes       The target host(s), range CIDR identifier, or hosts file
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Şekil 10.24: Kali Linux Saldırı Aracı Ekranı

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.42.129
RHOST => 192.168.42.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.42.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.42.129:21 - USER: 331 Please specify the password.
[*] 192.168.42.129:21 - Backdoor service has been spawned, handling...
[*] 192.168.42.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.42.129:6200) at 2021-09-04 10:50:09 -0400
```

Şekil 10.24: Kali Linux Saldırı Ekranı Aracı Sonucu

“Set RHOST <IP Numarası>” komutunu kullanıyoruz. Daha sonra “run” komutu ile atağı başlatıyoruz.

```
cd home
ls
ftp
msfadmin
service
user
ifconfig
ethtool

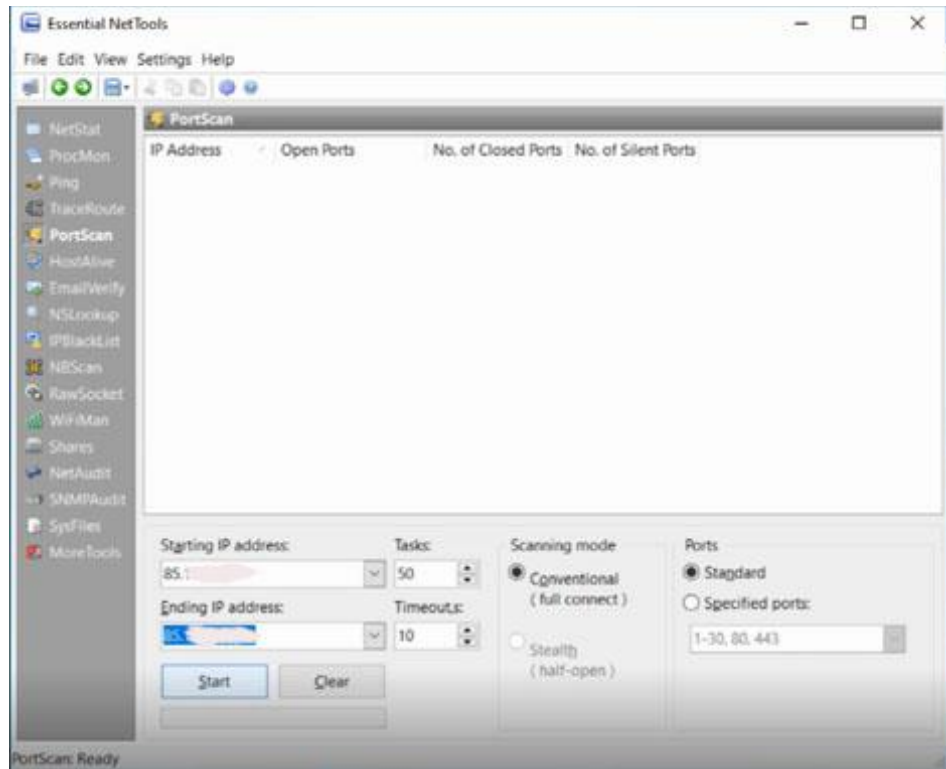
Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a
inet addr:192.168.42.129 Bcast:192.168.42.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:8579 errors:2 dropped:29 overruns:0 frame:0
TX packets:6963 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:809581 (790.6 KB) TX bytes:1411641 (1.3 MB)
Interrupt:16 Base address:0x2000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1114 errors:0 dropped:0 overruns:0 frame:0
TX packets:1114 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:520685 (508.4 KB) TX bytes:520685 (508.4 KB)
```

Şekil 10.25: Kali Linux Atak Sonucu Ekranı

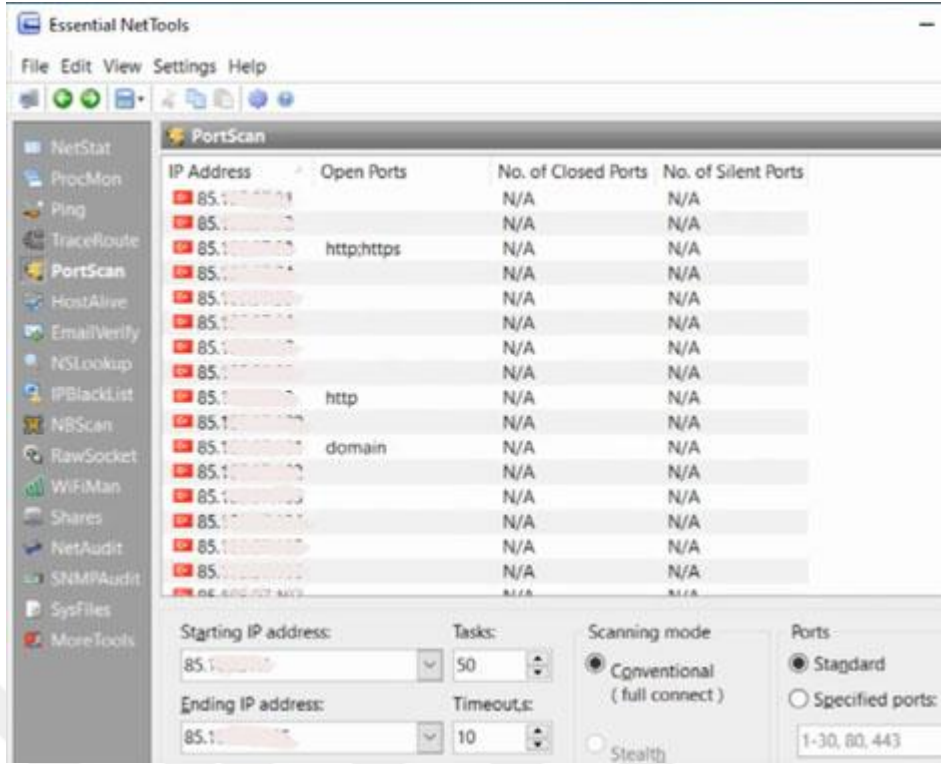
Şekil 10.25’de görüldüğü gibi Metasploit işletim sistemine Back Door açığını kullanarak girmiş bulunuyoruz.

Saldırı amaçlı bilgi toplamak için kullandığımız diğer bir uygulama olan Essential NetTools taraması için ilgili programın kurulumu yapıldıktan sonra rasgele public IP’ler taranmaktadır. Tarama sonucu IP bloğundaki açık olan ya da saldırılması muhtemel IP’lerin yanında http, https, domain vb. gibi açıklamalar yazmaktadır. Bu yazılar muhtemel saldırı yapılacak bir donanım olduğu anlamına gelmektedir.



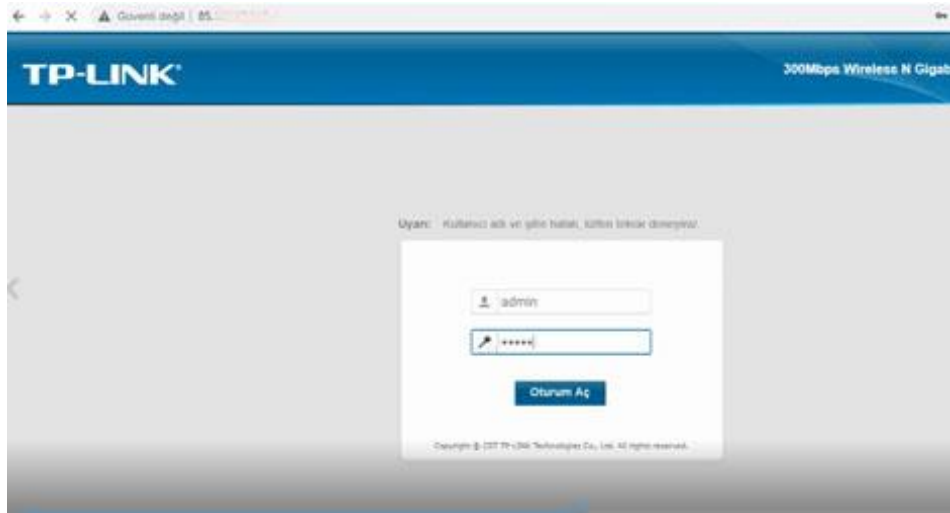
Şekil 10.26: Essential NetTools Ekranı

İlgili public IP yazdıktan sonra “start” ile tarama işlemi başlatılmaktadır. Burada IP bloğundaki aktif IP’leri sıralayacaktır. Şekil 10.27



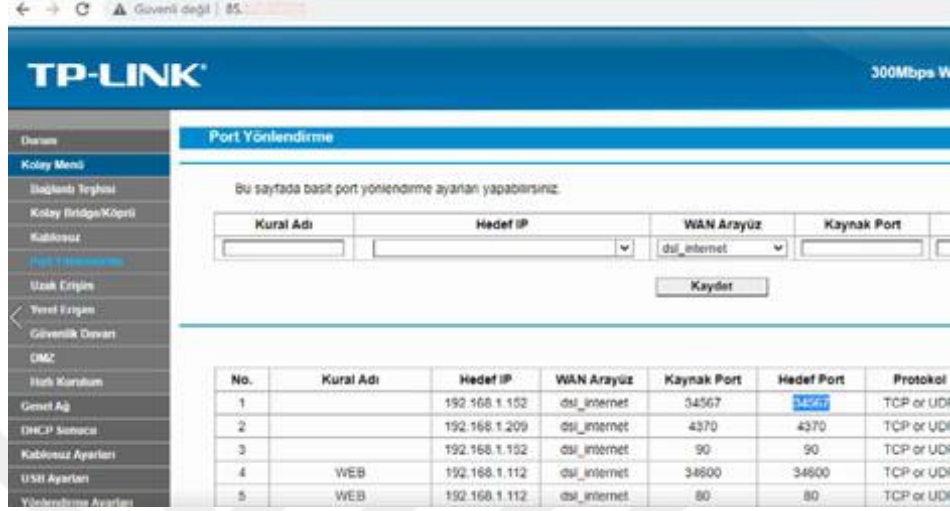
Şekil 10.27: Essential NetTools Tarama Ekranı

Atak yapılacak aktif olan IP'ler yanlarındaki yazılardan belirli olanlardır. Explorer (Diğer tarayıcılar genellikle sağlıklı bağlantı yapılamamaktadır) tarayıcısından bu IP'leri kullanarak bağlanılacaktır.



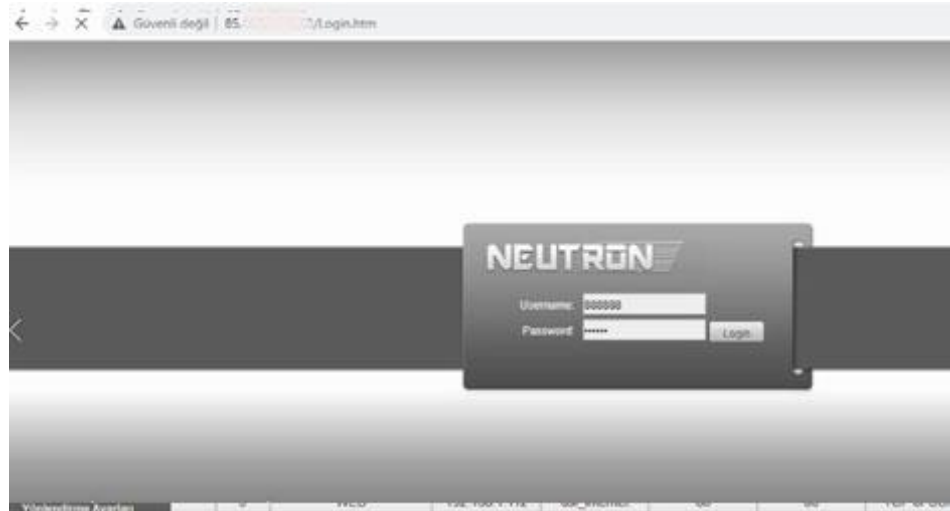
Şekil 10.28: Bağlanılan ModemTarama Ekranı

Kullanılan bu IP’de modem arayüzü gelmiştir. Burada genellikle fabrika ayarlarındaki şifreler bırakıldığı için giriş denemeleri yapılmaktadır. Her modem kendine göre bir kullanıcı adı ve şifresi bulunmaktadır. Bunlar değiştirilmediği sürece tehlike arz etmektedir.



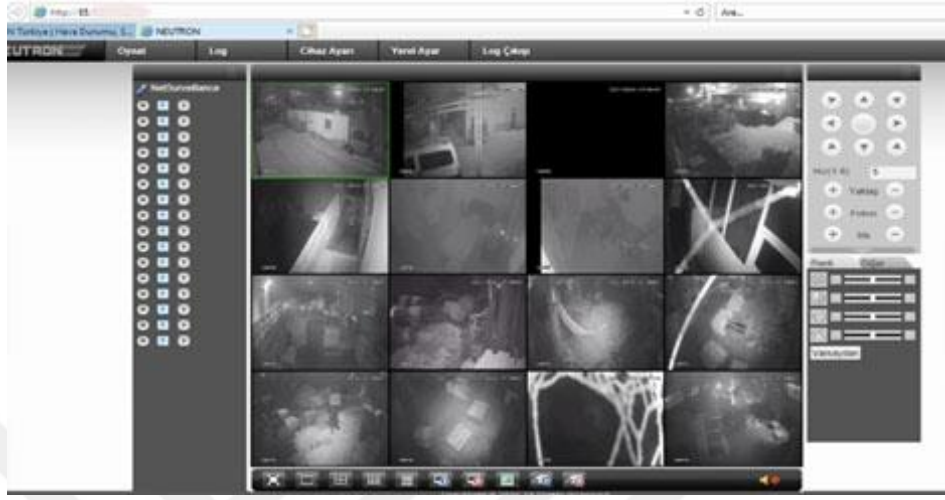
Şekil 10.29: Bağlanılan Modem Arayüz Ekranı

Şekil 10.29’da görüldüğü gibi modeme standart kullanıcı adı ve şifreleri ile giriş yapılmıştır. Burada kullanıcı adı ve şifreleri değiştirerek ya da diğer bağlı olan cihazların bilgilerini alarak saldırı düzenlenebilir ya da internet kesintilerine yol açılabilir.



Şekil 10.29: Güvenlik Kamerası Arayüz Ekranı

Diğer bir IP kontrol edildiğinde bir güvenlik kamerası olduğu anlaşılmıştır. Yine modemlerde olduğu gibi standart olarak bırakılan şifreler denenerek giriş yapılmaya çalışılmaktadır. Bu kamera ya da modemlerin standart şifreleri internet sayfalarından bulunabilmektedir.



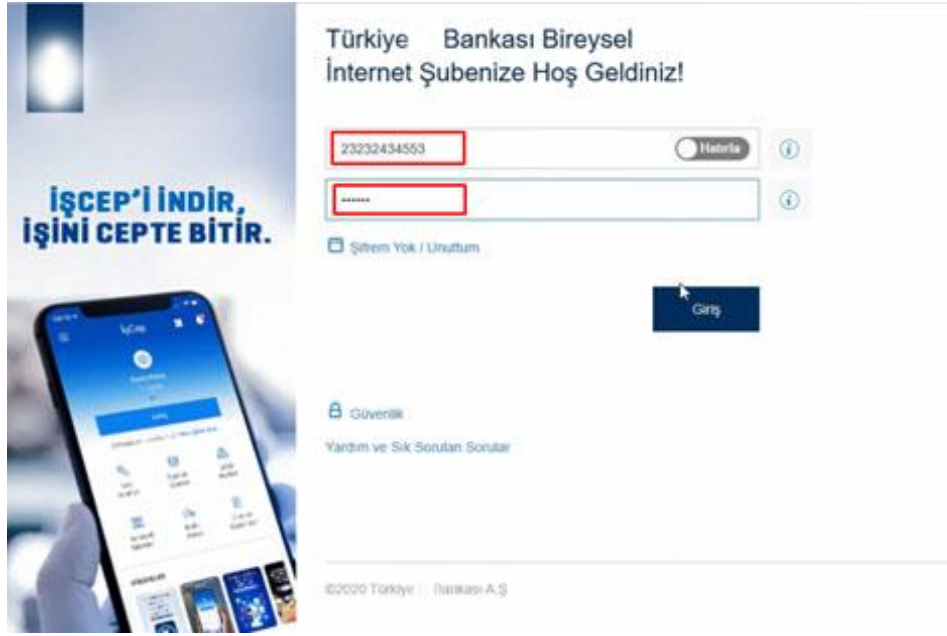
Şekil 10.30: Güvenlik Kamerası Ekranı

Şekil 10.30'da görüldüğü gibi sisteme girilmiş ve kamera kayıtlarına erişilmiştir. Bir kurumun kamera kayıtlarına erişilmesi olabilecek ihlallerin en büyüğü olarak nitelendirilmektedir. Bu görüntüler üzerinden her türlü saldırı gerçekleştirilebilir.

Burada gösterilmek istenen insan zaafiyetidir. Kullanılan cihazların şifreleri standart olarak bırakılmıştır. Kurulan ve kullanılan cihazların şifreleri standart olarak bırakılmamalıdır. Kurulum yapıldıktan sonra farklı şifreler ve farklı kombinasyonlar kullanılmalı ve bunlar karmaşık olarak belirlenmelidir.

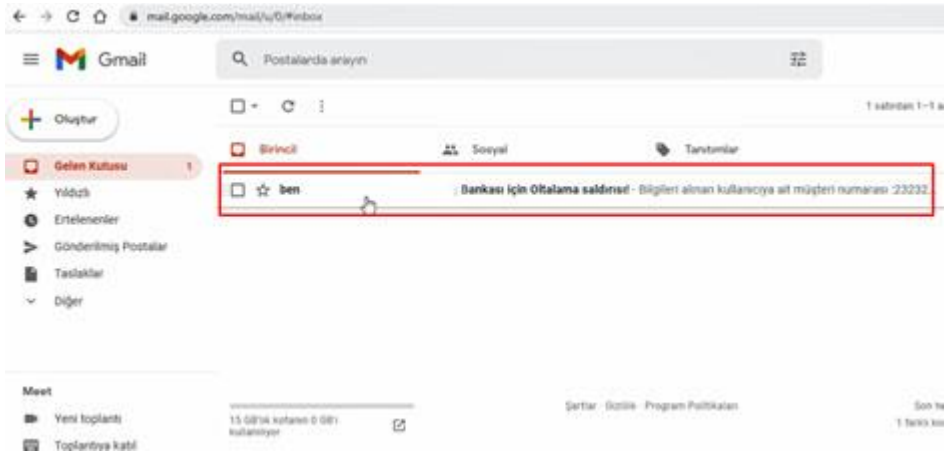
10.6 Phishing Saldırı Uygulaması.

Siber saldırılarda en zayıf halka olan insan faktörü olduğunun kanıtlanması için yapılan phishing saldırı uygulaması yapılmıştır. Burada bir bankanın web sayfası kopyalanmış ve kurbanı cazip bir kredi teklifi ya da güvenlik ihlali e-postası ile yollanan linke tıklaması sağlanmaya çalışılmıştır.



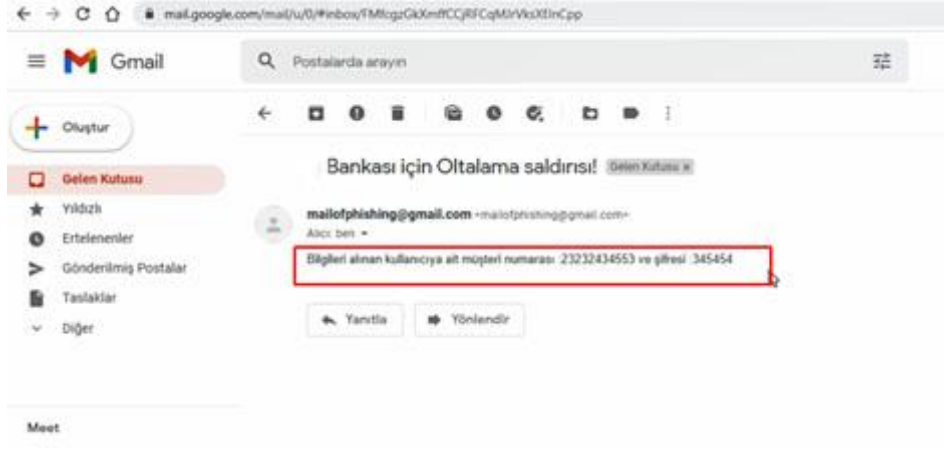
Şekil 10.31: Sahte Banka Web Sitesi Ekranı

Kopyalanan bir banka sitesi kodları değiştirilerek kurbanın bilgilerini girmesi sağlanmaktadır. Girilen bilgiler ilgili değişikliklerle belirlediğimiz bir mail adresine gelmesi sağlanmaktadır.



Şekil 10.32: Mail Adresi Ekranı

Sahte web sayfasının yönlendirmesi ile mail adresine gelen bilgiler mail kutusunda gözükmemektedir. Bu bilgiler hızla bankanın web sitesine girilerek ilgili siber saldırı gerçekleştirilir.



Şekil 10.33: Mail adresine Gelen Şifreler

11. SALDIRI TESPİT VE ÖNLEME SİSTEMLERİ

Kamu ve özel sektör firmalarının siber saldırılara karşı korunmak için alması gereken birçok tedbir vardır. Alınması gereken bu tedbirler teknolojinin gelişmesi ile bulut teknolojisi ve yapay zekâ ile donatılmış cihazları içermektedir. Bu cihazlar genellikle yabancı üretim ürünler olsa da artık yerli ürünlerde de bu saldırılara karşı koyulabilmektedir.

11.1 Firewall Cihazı Nedir? Ne İşe Yarar?

Dışarıdan gelebilecek tehlikeleri ve saldırıları önlemeye yarayan cihazlara verilen genel addır. Kişilerin internet üzerinden zararlı sitelere erişmesini engellemektedir. Dış ortamdan gelebilecek trojen ve virüs gibi zararlıları ilk engellenme noktasıdır. Fiziksel firewall cihazı ile tüm ağın ve sistemin verisini kontrol etmek ve kayıt altına almak mümkündür. Sistemin genel anlamda güvenliğini tek merkezden yönetmek firewall cihazları ile sağlanmaktadır. Firewall cihazlarla sağlanan güvenlik alt yapısının getirisi, güvenliğin sağlanması yanında kaynakların da en verimli şekilde kullanılmasının sağlanmasıdır. Özellikle düşük alt yapıya sahip internet hızlarının mevcut olduğu yerlerde gereksiz trafiğin engellenmesi veya kontrol altına alınması, internetin verimli kullanımı adına önemlidir. Firewall, belirlenmiş güvenlik politikalarına bağlı olarak, hem gelen hem de giden trafiğini gözlemleyen ve bu trafiği belirli politikalar dizisine uygun olarak yöneten güvenlik cihazına veya güvenlik yazılımına verilen addır. Firewall'ın temel prensibi, gelen veri trafiğinin incelenmesi ve uygun olmayanların, geçişlerinin engellenmesi şeklinde özetlenebilir. Hardware firewall (donanımsal firewall), ve Software firewall (yazılımsal firewall) olmak üzere iki çeşit firewall vardır. Hardware firewall (donanımsal firewall) cihazları yazılımı üzerinde barındıran ve üzerindeki yazılımlar ile trafiği yönlendiren münferit cihazlar olarak tanımlanmak mümkündür. Software firewall (yazılımsal firewall), işletim sistemi üzerinde yazılım temelli çalışan firewall olarak tanımlanmaktadır. Bu yazılımlar, bağlantı noktalarını kullanarak internet trafiğini düzenlemektedir [68].

11.2 DDOS Koruma Ürünleri

Persistent Threat (APT - Gelişmiş Sürekli Tehdit), bir grup veya kişinin ağa izinsiz erişim sağladığı ve uzun süre anlaşılmayan bilgisayar ağı saldırısıdır. Seviyesindeki karmaşık ve dinamik DDoS saldırılarına karşı bir savunma mekanizması olarak tasarlanmıştır. Teknolojisi ağdaki anormallikleri, 34'den fazla sensörü, geçmişe dayalı

veri toplama ve sezgisel algoritmalar tarafından desteklenen benzersiz anormali motoruyla algılamaktadır. Eş zamanlı ve otomatik olarak kirli trafiği hattınıza zarar vermeden önce temizler. Bu ürün yerli üretim ve milli üretim olarak kullanılmaktadır.

11.2 IPS ve IDS Nedir? Nasıl Çalışır?

IDS, sisteminiz ve ağıңыз içerisindeki zararlı olguların veya zararlı erişimlerin tespiti için kullanılan sistemlere verilen addır. Intrusion Detection Systems kelimelerinin kısaltması olarak kullanılır. IDS sisteminin amacı zararlı hareketi tanımlama ve loglama yapmaktır. IPS sistem ve ağ trafiğinizdeki zararlı hareketlerin veya zararlı erişimlerin tespiti ile birlikte önlenmesi için kullanılan sistemlerdir. Intrusion Prevention Systems kelimelerinin kısaltması olarak kullanılır.



Şekil 11.1: IDS ve IPS

IPS sistemlerinin amacı zararlı erişimlerin veya hareketlerin ağ üzerinde durdurulması ve engellenmesidir. Kısaca tanımlamak gerekirse IDS (Intrusion Detection System) saldırıları tespit etmeyi amaçlarken IPS (Intrusion Prevention System) saldırıyı durdurma ve berteraf etmek üzerine kurgulanmıştır. Son yıllarda artan gelişmiş siber saldırılara karşı yeni nesil Firewall cihazları ile bütünleşik olarak kullanılan IPS ve IDS sistemleri ciddi saldırıları engellemektedir. Doğru konfigüre edildiğinde saldırıların tespiti ve önlenmesi konusunda etkili bir rol oynamaktadır. IDS derinlemesine paket içeriğini analiz ederek saldırıyı tespit etmekte loglama işlevi de yürütmektedir. IPS saldırıları yapay öğrenme ile öğrenerek, kural listesi üzerinden tespit etmekte ve engellemektedir. Saldırı tespit ve önleme sistemleri olarak bilinen IPS ve IDS ürünleri birlikte kullanılırsa Intrusion Detection and Prevention Systems

yani IDPS olarak tanımlanmaktadır. Gelişmiş sistemlerde IPS ve IDS sistemleri bütünleşik olarak kullanılmaktadır. Firewall cihazları paketlerin geçmesini kısıtlayabildikleri halde, bir saldırı gerçekleştirilmesi durumunda otomatik olarak kendilerini yeniden programlama yetisine sahip değildirler. Bu durumu önlemek için genel olarak IPS ve IDS özellikleri ile birlikte gelmektedir. Intrusion Detection Sistem (IDS) teknolojisi sayesinde hem korumak istediğiniz kurum ağının saldırıya uğradığı anlaşılabilir, hem de Intrusion Prevention Systems (IPS) sayesinde saldırıyı gerçekleştiren kaynağın sisteme tekrar erişmesi engellenir [69].

11.3 WAF Nedir?

Web uygulaması güvenlik duvarı (WAF), veri ihlallerini önlemek için web uygulamalarını, API'leri ve sunucuları kötü amaçlı saldırılardan korur. Web uygulamalarını siber zaafiyetlere karşı koruyarak, web sitesi sunucularına saldıran gelen ve giden trafiği filtrelemekte ve izlemektedir. Kamu kurum ve özel sektör firmaları insanlarla iletişim halinde olmak ve kazanç elde etmek için web uygulamalarının üst düzeyde güvenli bir hale gelmesini istemektedir. Bununla birlikte, potansiyel güvenlik açıklarını belirlemek için giderek daha karmaşık teknikler geliştiren ve kullanan siber suçlular, web uygulamalarının en büyük tehditlerinin başında gelmektedir. WAF, saldırıları engellemek ve önlemek amacıyla ağdaki trafiği inceleyen bir güvenlik duvarı türüdür. Web uygulamalarına yönelik tehditler ile oluşan veri ihlalleri önemli konulardandır. İşletmeler, uygulamalarının pazara sunma süresini giderek kısaltmaya yönelmekte ve bu da genellikle insan hatasına ve güvenlikte boşluklara yol açan geliştirme sorunlarına neden olmaktadır. Bu nedenle WAF, işletmelerin hassas ve gizli verilerinin güvende olmasını sağlayan hayati bir araçtır. WAF kullanmak, kod güvenlik açıklarını keşfettiğinden dolayı kullanılan karmaşık siber saldırılar karşısında giderek önemli rol oynamaktadır. Diğer yandan, web uygulamaları ve kodları daha karmaşık hale geldikçe, HTTP ve HTTPS trafiğindeki sorunları analiz edebilen, keşfedebilen ve azaltabilen bir sisteme daha bağımlı hale gelmektedir. WAF, internet ve web uygulaması arasındaki kötü amaçlı trafiği engellemektedir. Aynı zamanda filtreleyerek ve izleyerek web uygulamalarını korur. Yetkisiz verilerin web uygulamasından çıkmasını da engellemektedir. WAF, işletmelerin aşağıdakiler gibi çok çeşitli gelişmiş güvenlik tehditlerinden korunmasına yardımcı olur:

WEB APPLICATION FIREWALL



Şekil 11.2: WAF

Siteler arası komut dosyası çalıştırma (XSS) saldırıları: Bir XSS saldırısı, saldırganın bir web uygulamasından kaynaklı güvenlik açığındaki boşluklardan yararlandığını görür. Bir kullanıcı saldırıdan etkilenen sitesini ziyaret ettiğinde veri ihlalleri veya kötü amaçlı eylem ile karşılaşabilir.

Kötü amaçlı yazılım saldırıları: En çok kullanılan saldırı biçiminden biri, kötü amaçlı yazılımlardır. (Malware attacks) Saldırganlar, web uygulamasındaki zaafiyetlerden yararlanır ve web sitelerine fidye yazılımı, casus yazılım bulaştırmak için kimlik avı gibi yöntemlerle saldırılar başlatırlar.

SQL enjeksiyon saldırıları: Bu saldırı türü, iletişim ve gönderim formları gibi web sitesindeki formlara karşı yapılmaktadır. Bu zaafiyet türünde saldırgan, kullanıcının doldurduğu alanlara kötü amaçlı SQL kodları ekler, bu da web sitesinin back-end kısmına erişmesine ve verileri çalmasına olanak tanımaktadır.

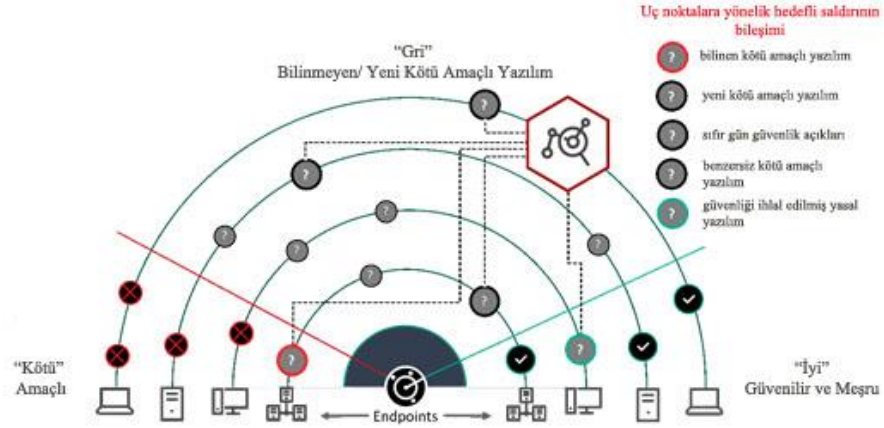
Sıfır gün saldırıları: Bir uygulamadaki savunmasız kod parçalarını hedef almaktadır. O kadar hızlı gerçekleşir ki, kuruluş sorunun varlığından haberdar olamaz. Saldırgan, olabilecek güvenlik açıklarını tarar. Bu boşluktan faydalanmak, şirketin gizli bilgilerine ve kaynaklarına erişim sağlamak için ataklar düzenler. Sıfır gün saldırıları, kurumsal sistemlerde genellikle aylarca ve hatta yıllarca tespit edilemeyebilir.

WAF ayrıca bir saldırganın kullanabileceği web uygulamalarındaki açıklıkları da tarayacaktır. Bir açığı keşfettiğinde, bilgisayar korsanlarının açığı bulmasını otomatik olarak engellemekte ve hemen düzeltmeye odaklanmaktadır. WAF'ın, güvenlik açıklarını tespit edebilmesi ve ortaya çıkan, önceden bilinmeyen tehditleri önleyebilmesi için WAF araçlarının her zaman güncel tutulması gerekmektedir. WAF olağan trafiği tanıyabildiğinden, bir kuruluşun güvenlik zaafiyetlerindeki aksak

noktaları keşfetmek için de kullanılabilir. Mevcut açıkları keşfedip, düzeltebilir ve kuruluşların web uygulamaları üzerindeki güvenlik testlerini gerçekleştirebilir [70].

11.4 EDR ve MDR Nedir?

EDR (Endpoint Detection and Response-Son Kullanıcı Tespit ve Geri Dönüşleri) Farklılaşan saldırı çeşitleri ve geleneksel anti-virüs sistemlerinin etkisizliğinden kaynaklı saldırıların fazlaştığı bilinmektedir. Yeni ortaya çıkan ihlallerin, sistemleri ve son kullanıcıları zaman zaman etkisi altına aldığını gözlemliyoruz. Özellikle powershell kullanılarak saldırıların yoğun olarak kullanılması bir çok anti-virus uygulamasını devre dışı bırakmaktadır. EDR ile yapabileceklerimiz Local-Remote-Malware-Ransomware-ZeroDay saldırılarından korunmadır. Eksik updateler, yanlış ya da eksik yapılandırmalar, BoTNet, eski versiyon uygulama kullanımından kaynaklı saldırılar. Atak ne zaman gerçekleşti? Atakdan etkilenenler/etkilenen kim? EDR Davranış analizi (Behaviour Monitoring) ve makine öğrenme (Machine Learning) teknolojilerini kullanarak olay tespit zamanını ve zararlının bulunduğu sisteme ve ağa zarar vermesinin önüne geçmektedir. Powershell saldırıları örn; pdf dosyası görünümlü aslında arka planda bir exe dosyası olarak yapılandırılmış ve kullanıcının makinesinden backdoor veya botnet gibi ataklara maruz bırakabilmektedir. Bilinmeyen uygulama veya dosyaların tespiti ve sanal ortamlarda testlerini sağlayarak ağda yer alan diğer ürünlerin bu konuda bilgilendirilmesini sağlamaktadır. Uç noktalarda faaliyet gösteren eylemlerin monitörlemesi yapılıp, durum analizleri anlık gözlemlenmektedir. Adli izlerin izlenmesi süreçlerinde önemli bir tespit imkanı sunmaktadır. Windows makinelerinde Registry kayıtlarının izlenmesini sağlamaktadır. Sıra dışı olayları arka planda anlık tespit etmektedir. Processler, servisler detaylı olarak takip edilir. IP,URL,Domain,DNS ve SHA Hash, File Name ve File Path gibi araştırmaların yapılmasına olanak tanımaktadır. Kolay yönetilebilmekte, olay zamanına ve tüm nedenlerine kolay erişilebilirlik sağlamaktadır. Görünmeyen detayları gözler önüne sermektedir. MDR (Managed Detection and Response-Yönetilebilir Tespitler ve Geri Dönüşler) tehdit ve saldırı algılaması, saldırının tespiti-müdahalesi ve düzenleme süreçlerinin uygulandığı ve yönetildiği servistir. MDR özellikle kurum içinde siber güvenlik elemanları bulunmuyorsa, süreç müdahale ve karar alma işlemlerinin hızlandırılmasının hedeflen-

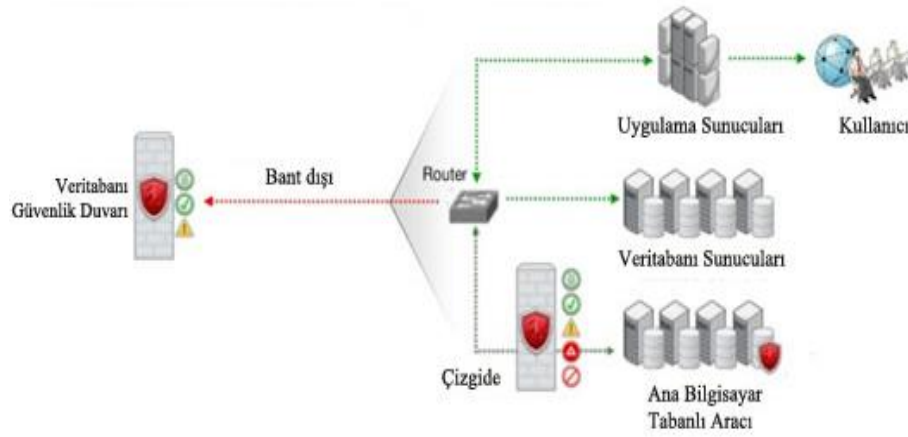


Şekil 11.3: EDR ve MDR

diği uygulama olarak adlandırılır. Saldırı engelleme ve verinin korunması gerektiği uç noktalarda işlem yapmayı merkezileştiren bir yapıya sahiptir. Özellikle DLP, SIEM ve Incident Forensics uygulamalarına kolayca entegre edilebilecek güvenlik çözümüdür. MDR ile güvenlik olaylarının incelenmesi, yorumlanması ve sonrasında kurum ve kuruluşlarda alınabilecek tedbirlerin uygulanması sağlanabilmektedir. Genel bakacak olursak, EDR ve MDR birbirine entegre benzer iki güvenlik ürünüdür[71].

11.5 Database Firewall (Veri tabanı Güvenlik Duvarı)

Veri tabanı sunucusuna yapılan tüm sorguları, sunucudan gelen yanıtları izleyen ve veri tabanına yetkisiz erişimi veya değiştirilmesini algılayan, önleyen bir Web Uygulaması Güvenlik Duvarı veya WAF türüdür. Database Firewall, önceden tanımlanmış ve özelleştirilebilir, güvenlik denetim politikaları içermekte ve veri tabanı saldırılarını "imzalar" adı verilen geçmiş olaylara tehdit modellerine göre tanımlayabilmektedir. Bu nedenle, SQL girdi ifadeleri sorguları, veri tabanında bilinen saldırıları tanımlamak için sık sık güncellenen bu imzalarla karşılaştırılmaktadır. Ancak veri tabanlarına yapılan tüm saldırılar bilindik olmamaktadır. Bu nedenle, veri tabanı güvenlik duvarı, güvenli olan onaylanmış SQL komutlarının ifadelerinin beyaz listesini oluşturmaktadır. Kullanıcılarının önemli bilgilerini saklayan şirket ve kurumlar için veri tabanı güvenliği son derece önemli bir yere sahiptir. Veri tabanının kullanıcı bilgilerini ve finansal anlamdaki belgeleri kayıt altında tutmalarından ötürü bu sistem ve kurumlar siber saldırı tehditlerinin merkez hedefi haline gelmektedir. Özellikle maddi açıdan değerli bilgilerin saklanma ihtiyacından dolayı veri tabanı güvenliği, günümüzde birçok kurum ve şirket için son derece önem arz etmektedir.



Şekil 11.4: Database Firewall

Database Firewall sistemlerine yapılan saldırılara örnek vermek gerekirse, SQL enjeksiyonu bu konuda en doğru örnek olabilir. SQL enjeksiyonu tehditleri, veri tabanına bağlı ara yüz sistemlerini doğrudan hedef alabilmektedir. Bu sayede sistemlere erişmeye çalışan, fakat web ara yüzü üzerinden yapılmaya çalışılan SQL enjeksiyon tehditleri daha çok görülmektedir. SQL zaafiyetleri kullanıcılardan alınmış bilgilerin denetleme işlemlerinin yapılmadan, veri tabanı uygulamalarında ya da veri tabanını yöneten web uygulamalarında çalıştırılmasından kaynaklanmaktadır. SQL enjeksiyon tehditleri, saldırgan yapının veri tabanı üzerinde önemli bilgilere ulaşması ve kullanıcıların haklarını yüksek seviyeye çıkarması gibi riskli işlemleri yapmasına sebep olmaktadır[72].

11.6 SIEM Nedir? (Security Information and Event Management)

Güvenlik Bilgileri ve Olay Yönetimi (SIEM) yazılımı, güvenlik teknolojisindeki en önemli yeniliklerden biridir. Güvenlikle ilgili olayları, uyarıları ve raporları toplama, analiz etme ve bunlara göre hareket etme sürecini içermektedir. Sadece tek bir konuya ya da etkinliğe odaklanmamaktadır. Bunun yerine, BT altyapısı içindeki herhangi bir kötü amaçlı etkinliği tespit etmek için bir kuruluş içindeki tüm kaynaklardan gelen etkinlikleri toplamaktadır. SIEM kavramı nispeten yeni olmasına rağmen, hali hazırda var olan iki teknoloji üzerinde geliştirilmiştir. Güvenlik Olay Yönetimi (SEM) ve Güvenlik Bilgi Yönetimi (SIM). SEM, olay korelasyonu, tehdit izleme ve olay yanıtı sağlamak için günlük ve olay verilerini gerçek zamanlı olarak analiz eden bir yazılım çözümüdür. Öte yandan SIM, günlük verilerini toplar, analiz eder ve raporlar. Bu teknolojinin genişletilmiş kapsamının ele alınması oldukça karmaşık olabilir ve uzman

BT teknisyenlerinin becerilerini gerektirir. Bununla birlikte, bir işletme veya kuruluştaki her paydaşın, SIEM'in işletmeyi nasıl etkilediğinin temellerini anlaması gerekir. Güvenlik Bilgileri ve Olay Yönetimi, öncelikle beş adımlık bir süreçte çalışır:

Veri topla,

Toplam veri,

Veri analizi,

Güvenlik ihlallerini tespit edin,

Tespit edilen ihlal hakkında uyarı.

Veri, teknolojinin nasıl çalıştığının temelinde yer alır. Bu nedenle SIEM, sunuculardan, ağ cihazlarından, etki alanı denetleyicilerinden, güvenlik duvarı günlüklerinden, virüsten koruma olaylarından vb. veri toplamaya başlar. Bir kuruluşun sistemi ve ağları boyunca çok büyük miktarda veri toplar. Bir sonraki adım, toplanan verilerin birleştirilmesini içerir. Verileri depolar ve birleştirir, böylece personel tarafından kolayca erişilebilir. Ardından analiz gelir. SIEM, kullanıcı davranışının yanı sıra ağ davranışını da analiz eder. Başarısız ve başarılı oturum açmalardan, kötü amaçlı yazılım etkinliğine ve diğer sıralanmış veri kategorilerine kadar tüm etkinlikleri merkezi bir platformda izler. Yazılım, analiz süreci sırasında olağandışı etkinlik olarak algılıyor. Örneğin, 5 dakikadan daha kısa sürede yapılan 100 başarısız oturum açma girişimi, kaşları çatar ve büyük olasılıkla saldırı girişimi olarak işaretlenir. Son olarak, tespit edilen bu tür anormallikler, potansiyel güvenlik sorunlarına işaret ettikleri için güvenlik uyarılarını tetiklemektir. Bu uyarı özelliği, BT personelinin dış tehditlerle erkenden mücadele etmede ve hatta ilk etapta onları önlemede daha proaktif olmasını sağlar [73].

12. SONUÇ VE ÖNERİLER

12.1 Uygulama Sonuçları

Kamu Kurumlarının almış olduğu tedbirleri gözler önüne sermek için uygulamanın içinde yapılan taramalar Şekil 12.1’de sergilenmiştir. Kali Linux NMAP aracı ile genel keşif ve bilgi toplama işlemi yapılmıştır. Yapılan bu taramada zaafiyet amaçlı açık port olup olmadığına bakılmıştır. Tarama sonrası, saldırı amaçlı açık bir port olmadığı gözlenmiştir. Genelde açık olan 80 portu’nun (HTTP listening port) web sayfası amaçlı kullanıldığı bilinmektedir. Bir diğer açık olan port 443’ün ise mail trafiği için (HTTPS - TLS/SSL üzerinden HTTP Protokolü Kriptolanmış aktarımı) kullanıldığı anlaşılmaktadır. 2000 ve 5060 portlarının ise (Cisco SCCP) öncelikli olarak IP telefonlar ile Cisco Unified Communications Manager arasındaki iletişimi sağladığı bilinmektedir. Bu bilgi VoIP santral olduğunu göstermektedir. 8080 ve 8081 portları ise genel olarak kullanılan güvenlik DVR cihazları ya da farklı basit cihazlar için yönlendirilmiş portlardır. SQL açıkları veri güvenliği için önemli yer teşkil etmektedir. Bu nedenle Kali Linux SQLMAP aracı ile Kamu kurumlarının WEB sayfalarına SQL açıkları için tarama yapılmıştır. Yapılan tarama sonucunda herhangi bir açıklık tespit edilememiştir. Yine taramalar neticesinde birçok kurumda F5 Networks veya nginx güvenlik cihazları tespit edilmiştir.

Kurum Adı	Açık Olan Portları
Adalet Bakanlığı	80,443
Aile ve Sosyal Hizmetler Bakanlığı	80,443
Çalışma ve Sosyal Güvenlik Bakanlığı	80,443
Çevre ve Şehircilik Bakanlığı	80,443
Dışişleri Bakanlığı	80,443
Enerji ve Tabii Kaynaklar Bakanlığı	80,443,2000,5060
Gençlik ve Spor Bakanlığı	80,443,8081
Hazine ve Maliye Bakanlığı	80,443
İçişleri Bakanlığı	80,443
Kültür ve Turizm Bakanlığı	80,443
Millî Eğitim Bakanlığı	80,443
Millî Savunma Bakanlığı	80,443
Sağlık Bakanlığı	80,443
Sanayi ve Teknoloji Bakanlığı	80,443
Tarım ve Orman Bakanlığı	80,443
Ticaret Bakanlığı	80,443,8080
Ulaştırma ve Altyapı Bakanlığı	80,443

Şekil 12.1: Kamu Kurumları Tarama Sonuçları

Elimizdeki tarama verilerine bakarak tarama yapılan kurumların %100'ünün güvenlik cihazları ile korunduğu gözlenmiştir. Kamu kurum ve kuruluşları kendi güvenlik personelinin yanı sıra USOM ve BTK tarafından 24 saat sürekli izlenerek korunmaktadır.

Genel sonuçlar değerlendirilecek olursa;

- Alınan tedbirlerin yanında kamu kurumları ve özel sektörün kullandığı sunucular ile kullandıkları uygulamaların uyumluluğu önem arz etmektedir. Birçok saldırgan uygulamaların kullandığı sunucuların güncel olmamasından kaynaklı açıklardan yararlanmaktadır. Bu nedenle sunucuların güncellemeleri tam ve eksiksiz olmalıdır. Kullanılan uygulamaların zamanımızın teknolojisine uygun yazılımlarına entegre olacak şekilde yenilenmesi ve tasarlanması gerekmektedir. Güncel olmayan sunucu her zaman tehlike arz etmektedir. Genellikle siber saldırılara maruz kalan sistemler açıkları kapatılmamış sunuculardan kaynaklanmaktadır.
- Tüm sistemin etkin bir antivürüs yazılımı ile korunması gerekmektedir. Bu korunma yerel bilgisayarlar ve taşra teşkilatı bulunan tüm kurumlar için muhakkak uygulanması gerekmektedir.
- E-posta hesapları için kullanılan şifre, diğer hesaplarındaki şifrelerden farklı yapıda olmalıdır. Kullanılan bu şifreler sosyal medyalar ya da alışveriş sitelerinde kullanılan şifreler olmamalıdır.
- Kişisel bilgileri isteyen e-postalara yanıt verilmemelidir. Gelen e-postanın kimden geldiği bilinmiyorsa dikkate alınmamalıdır. Unutulmamalıdır ki hiç bir kurum veya kuruluş, çalıştığınız işyeri bile asla kişisel verilerinizi ve parolanızı soran e-posta göndermez.
- Şüpheli görülen e-postalardaki URL linkleri tıklanmamalıdır. E-posta mesajlarındaki kısaltılmış URL linklerine (bit.ly, ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs vb.) herhangi bir internet tarayıcı ile açılması tehlikeli hale gelebilmektedir.
- Şüpheli veya bilinmeyen web sitelerine kişisel bilgiler ve kredi kartı bilgileri verilmemelidir.
- Bankaların kredi kartı ve servis sağlayıcılarının web siteleri ziyaret edildiğinde, kişisel bilgileri girmek için web sitesinin URL'si internet

tarayıcısına doğrudan yazılmalıdır. Güvenli olarak görülen sitelerde çevrimiçi olarak bir form doldurmadan, ilgili sitenin üçüncü kişilerle kişisel bilgileri paylaşp paylaşmadığını belirten gizlilik anlaşmasının var olup olmadığının kontrolü sağlanmalıdır.

- Yasal olmayan veya kaynağı belirsiz yazılımlar yüklenmemeli ve çalıştırılmamalıdır. Ücretli olarak satılan ticari programları kullanmak için crackleri gelişi güzel çalıştırılmamalıdır.
- Kredi kartlarının numaraları, özel veriler dâhil her türlü parola asla e-posta ile açıkça iletilmemelidir. Bir e-posta teknik anlamda gideceği yere ulaşana kadar birçok yerden geçmektedir. Bu yerlerden geçerken e-postaların içeriğinin "dinlenmesi" mümkün olabilir.
- Halka açık kablosuz erişim ağının kullanıldığı yerlerde mecbur olmadıkça bankaların web sitelerine girilmemeli, kart bilgileri, parola vs. ile ilgili hiçbirşey yapılmamalıdır. Sinyaller üçüncü şahıslar tarafından dinlenebilir. Bu sinyaller şifreli bile olsa unutulmamalıdır ki tüm şifreleme yöntemleri sadece kırılıncaya kadar güvenlidir. Bankalardaki hesapların güvenliğini sağlamak ve bu tip saldırıları önlemek için Kare kod tarama uygulaması ya da cep telefonunuzdaki banka uygulamasına giriş yapıldığında doğrulama onayı vererek giriş yapmak bu tip tehditlerin önüne geçecektir.
- Kendini savcı, polis, asker olarak tanıtan kişiler “kumpas kuruldu hakkınızda dosyalar var” gibi ifadelerle para istemektedir. Hiçbir savcı, polis veya asker telefon yolu ile sizden para istemez.

Siber zaafiyetlerin giderilmesinde insan faktörü ve insanların eğitimi çok önemlidir. Bu farkındalık eğitimlerinin artırılması için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi öncülüğünde BTK ile birlikte tüm kamu kurum ve kuruluşlarında çalışmalar yürütülmektedir. Ayrıca 27001 Bilgi güvenliği kapsamında BGYS (Bilgi Güvenliği Yönetim Sistemi) kamu kurumlarında denetimler yapılmaktadır. En önemli gelişme Siber güvenlik eğitimlerinin ilkokul çağından itibaren başlanarak verilmesi amacıyla Milli Eğitim Bakanlığının bünyesindeki EBA sisteminde “Siber Güvenlik Portalı” oluşturulmuştur. Bu portal öğretmenlere, ailelere ve öğrencilere yol gösterecek bir rehber niteliğinde olacaktır.

Tüm bu değerlendirmelere göre siber saldırılara karşı alınacak tedbirler kişisel olsa da “Saldırı Tespit ve Önleme Sistemleri’nin” varlığı çoğu kuruluşun güvenlik zaafiyetlerini azaltmıştır. Yapılan saldırılar ve bunların çeşitliliği göz önüne alındığında her saldırı tipine ve çeşidine göre cihaz almanın da bir maliyeti olmaktadır. Ancak hiçbir maliyet veri güvenliğinden daha önemli değildir. Yaptığım incelemelerde kamu kurumlarında alınan güvenlik tedbirleri ile Siber Güvenlik personelinin varlığı, son dönemde yapılan siber saldırılarda çok etkili ve etkin olmuştur.

12.2 Öneriler

Ülkemizde internet; kişi, kurum ve kuruluşların, gerek günlük işlerde gerekse eğitim kapsamında ve gerekse de özel sektör ve kamu kurum faaliyetleri kapsamında, binlerce araştırma ve incelemelerin yürütüldüğü bir platform haline gelmiştir. Bu bağımlılık alınması gereken tedbirleri de beraberinde getirmiştir. Bu tedbirlerden bazıları;

E-Posta Güvenlik Tedbirleri

Bir kurumun en kritik iletişim araçlarından biri e-posta hesaplarıdır. Basitliği ve hızı nedeni ile e-posta hesapları yanlış kullanıma açık bir kanaldır. E-posta hesaplarının güvenliğinin sağlanabilmesi adına kurumlarda alınması gerekli olan tedbirlerin bazılarını şu şekilde sıralayabiliriz:

- Kurumun e-postasını kullanırken insanları taciz eden, rencide edici veya e-posta alan kişinin haklarına zarar vermeye yönelik öğeler içermemelidir. Bu türden iletiler alındığında birim yöneticilerine bilgi verilmesi gerekmektedir.
- E-postanın iletildiği kişiden başka bir kişiye iletilmemesi için adres kısmına azami şekilde özen gösterilmelidir. İlgilisi olmayan bir kişiye e-posta gönderildiğinde, ilgili amirlere bilgi verilmeli, Exchange operatörü yardımı ile e-posta geri çekilmelidir.
- Kurum mailinden özellikle saldırı mailleri olduğu düşünülen maillere cevap verilmemelidir.
- Size gelen e-posta içeriğinde kullanıcı adınızı ve şifrenizi talep eden e-postalar cevaplanmamalıdır. Gelen e-posta güvenlik birimine iletilmelidir.

- Kamu personeli, kurumsal e-posta hesaplarının ve içeriğinin kurum dışındaki 3. şahısların ve yetkisi olmayan kişiler tarafından okunmasına ve görülmesine engel olmakla sorumludur.
- Nereden geldiği belli olmayan e-posta ve ekleri açılmamalıdır. Şüpheli işlemler Siber Güvenlik personeline bildirilmelidir.
- Kamu kurumlarına ait e-posta adresleri, alışveriş siteleri ve banka gibi yerlerde kullanılmamalıdır. Zira oluşabilecek veri ihlallerinden e-posta sahibi sorumlu olacaktır.

Şifre Güvenlik Tedbirleri

Kamu personeli için şifreleme, bilgisayar güvenliği için çok önemlidir. Son kullanıcı hesapları adına ilk alınan güvenlik tedbiridir. Güçsüz bir şifre tercihi, kurum ağını ve güvenliğini tümüyle tehlikeye atabilir. Tüm sistem güçlü şifrelerle kurulmalı ve son kullanıcı seviyeli şifreler belirli periyotlarla yenilenmelidir. Yenileme süresi en az 6 ayda bir olmalıdır.

- Kurum içindeki Sistem uzmanı her bir sistem için farklı şifreler kullandırmaya zorlamalıdır.
- Son kullanıcı şifrelerinin başkaları ile paylaşılmaması, kâğıtlara ya da elektronik ortamlara yazılmaması gerektiği konusunda personele bilgi verilmelidir.
- Kurum içinde şifre seçimleri yapılırken büyük-küçük harfler ve rakamlar kullanılmalıdır. Şifreler içinde #, !, %, & gibi karakterler seçilmeli ve en az 8 karakter olmalıdır.

Anti-Virüs Güvenlik Tedbirleri

- Kamu kurumlarının bütün bilgisayarlarında anti-virüs yazılımı olmalıdır. Belirli aralıklarla düzenli olarak güncelleştirilmelidir.
- Antivirüs güncellemeleri sadece bu iş için kullanılan Sunucular tarafından yapılmalıdır. Antivirüs sunucuları internete çevrimiçi bağlantılı olmalı ve otomatik olarak veri tabanını güncelleyebilmelidir.
- Kaynağı bilinmeyen diskler ve usb'ler daima virüslere karşı taranmalıdır.

- Önemli veriler içeren datalar ve sistemler belirli aralıklar ile yedeklenmelidir.
- Kurum içinde Virüs bulaştığı düşünülen bilgisayarlar tam olarak temizleninceye kadar bulunduğu ağdan çıkarılmalıdır.
- Son kullanıcı sebebi ne olursa olsun anti-virüs programını bilgisayarından kaldıramamalıdır.

Sunucu Güvenlik Tedbirleri

Kurum içinde bulunan sunucularının gerekli güvenlik konfigürasyonları için bazı standartlar bulunmaktadır.

- Sunucular üzerindeki uygulamalar ve servisler kullanılmıyorsa kapatılmalıdır.
- Sunucu üzerindeki servislere erişimleri ilgili şekilde loglanmalıdır. Erişim kontrol sistemiyle korumalıdır.
- Sistem uzmanları özel durumlar haricinde yetkili olan “root” ve “Administrator” gibi kullanıcı hesaplarını kullanmamalıdır. İlgili yetkilerin sağlandığı kendi hesapları ile erişim sağlamalıdır. Sistem Yönetimi hesapları farklı şekilde isimlendirilmelidir. Gerekli durumlarda ilk önce kendi şahsi hesapları ile giriş yapılmalı daha sonra genel yönetici hesaplarına geçiş yapılmalıdır.
- Kurumda ayrıcalıklı bağlantılar teknik anlamda daha güvenli olan kanal (SSH veya SSL, VPN, IPSec gibi şifrelenmiş özel ağ) üzerinden yapılmalıdır.
- Sunucuların barındırıldığı alanlar özel ve yerden soğutmalı olmalıdır. Giriş ve çıkışlar kontrol altında tutulmalı, yetkisiz kişilerin girişleri engellenmelidir.

Ağ Yönetimi Tedbirleri

Ağ yönetimi bir kurumun en önemli yapılarından biridir. Ağın trafiği ve ağda dolaşan bilgiler göz önüne alındığında, güvenlik, gizlilik, bütünlük yapıları sağlanmalıdır. Uzak bağlantı noktasına özel önem gösterilmelidir. İzinsiz ve yetkisiz girişler engellenmelidir.

- Kurum ağlarının ve bağlı olan sistemlerin iş sürekliliğinin sağlanması için ilgili kontrollerin sağlanması ve uygulanması gerekmektedir.

- Kurum Ağındaki servis standartlarında erişime izin verilen ağlara ve ağın servislerine erişim için yetkilendirme yöntemleri belirlenmelidir.
- Kurum uygulamaları ve kullanılan diğer uygulamalar için ilgili portlara ağ geçitlerine veya uygulama servislerine otomatik olarak bağlanması sağlanmalıdır.
- Kurum içi ağ trafiğinin sınırsız olması engellenmelidir.
- Kurum içinde ve dışında izin verilen kaynaklar ve hedef ağlar arasındaki iletişimi aktif olarak izleyen teknik cihazlar bulundurulmalıdır. (ör. Firewall)
- Kurum içi ağ erişimi, VLAN ve VPN gibi ayrı alanlar oluşturularak sınırlandırılmalıdır.
- Kurum içi ağ bağlantıları periyodik olarak izlenmeli ve kontrol edilmelidir.
- Ağ üzerinde bulunan firewall'lar ilgili konfigürasyon dokümanlarında ilgili servislerin dışında kalan tüm servisler kapatılmalıdır. Firewall için kullanılan cihazlar başka bir amaç için kullandırılmamalıdır.
- Kurum ağıyla ilgili sorumlulukların paylaşılması amacıyla ağ ile ilgili dokümanlar hazırlanmalı ve ağ ekipmanlarının güncel konfigürasyonları saklanmalıdır.
- Kurum ağı üzerinde gerçekleşen işlemler ile veri hareketliliği izlenmeli loglar saklanmalıdır.

Kablosuz İletişim Tedbirleri

Kablosuz erişimin Kurum içinde paylaşımının sağlanmasında kullanılan erişim cihazlarının (Access Point) güvenlik politikaları belirlenmediğinde saldırı için büyük zaafiyet içerdiği görülmüştür. Bu koşul bilgi güvenliği açısından tehdit oluşturacak ve zaafiyet oluşmasına neden olacaktır. Kablosuz iletişimin sağlanması için alınması gereken tedbirler şu şekilde olmalıdır.

- Kurum ağına erişen bütün cihazlar ve ağ arabirim kartları sistem yöneticileri tarafından kayıt edilmelidir. Kablosuz ağa erişen cihazlar belirli sürelerde güvenlik testlerine tabi tutulmalıdır. Mac adresleri kayıt altına alınan cihazların kurum ağına erişmesi sağlanmalıdır.

- Kurum ağına erişim sağlayan cihazların firmware'leri güncel olmalıdır. Bu durum donanımı üreten firmanın güvenlik açıkları ile ilgili yamaları yayınlayarak zaafiyetlerin önüne geçmesini sağlayacaktır.
- Kablosuz cihazların kişilerin kolayca ulaşabilecekleri bir yerde bulunmaması gereklidir. Kablosuz cihazlar resetlendiği takdirde fabrika ayarlarına dönmekte ve güvenlik zaafiyeti oluşturmaktadır.
- Kablosuz Cihaza erişim için güçlü bir şifre verilmelidir. Erişim şifreleri varsayılan ayarda unutulmamalıdır.
- Kablosuz cihazların SSID numaralarının yayınlanması engellenmelidir. Böylece sniffer tarzı cihazların SSID numaralarını otomatik olarak çözmesi engellenecektir.
- Kablosuz cihazlarda fabrika çıkışı SSID isimleri kullanılmamalıdır. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi bulunmamalıdır (Mesela kurum ismi, ilgili bölüm çalışanın ismi vs. gibi).
- Kablosuz cihazlar üzerinden gelen kullanıcılar Firewall üzerinden ilgili ağa dâhil olmalıdırlar.
- Kullanıcılar ve kablosuz ağlar statik ip adresleri kullanmalıdır. Ayrıca donanım adresleme sistemi (örnek mac adresleme) kullanılmalıdır.

Kimlik Doğrulama ve Yetkilendirme Tedbirleri

Kurumun ilgili sistemlerine erişimde yetkilendirme ve kimlik doğrulaması tedbirleri şu şekilde olmalıdır:

- Kurumda bilgi sistemine erişecek kullanıcıların kurumsal kimlikleri doğrultusunda erişebilecekleri sistemler ve hangi kimlik doğrulama yöntemi ile erişebileceği belirtilmeli ve dokümente edilmelidir.
- Kurumda sistemler üzerindeki kullanım hakları sürekli olarak gözden geçirilmeli ve gereksinimler, gerekli minimum yetkinin verilmesi ve kullanılması prensibi doğrultusunda güncellenmelidir.
- Kurumda sistemlere erişim ve yetki seviyelerinin devamlı olarak güncelliği sağlanmalıdır.

- Kurumda sistemlere yetkili ve yetkisiz, başarılı ve başarısız erişim logları düzenli olarak tutulmalı, başarısız log-on girişimleri gözden geçirilmelidir.
- Kullanıcılar kendilerine verilen ilgili erişim şifrelerini deşifre etmemeli ve kimseyle paylaşmamalıdır.
- Sistemlere giriş yaparak log-on olan kişilerin yetki aşımına yönelik hareketleri gözlenmeli ve yetki ihlalleri kontrol edilmelidir.
- Her kullanıcıya yalnızca kendisine ait olacak şekilde hesap açılmalı ve bu hesaba ait hareketler izlenilmelidir.

Veri Tabanı Güvenlik Tedbirleri

- Kurumlarda kritik olan verilere erişim işlemleri (değiştirme, silme, okuma ve ekleme) ilgili programlar ile loglanmalıdır. Alınan loglara izin alınmadan hiçbir zaman erişim sağlanmamalıdır. DVD, CD ve Manyetik kartuş ile tutulan loglar belirtilen en az 5 (beş) yıl süre ile güvenli ortamlarda muhafaza edilmelidir.
- Veri tabanı için alınan sistem log hareketleri tutulmalı idare tarafından istenildiğinde izlenmelidir.
- Veri tabanı sistemlerinde olan bilgiler ayrıştırılmalı ve yedekleme araçları ile saklanmalıdır, yedeklemeden sorumlu personel belirlenmelidir. Yedeklemelerin düzenli olarak alınması sağlanmalı ve kontrol edilmelidir.
- Veri tabanı bilgilerinin tutulduğu sistemler kurum tarafından her türlü güvenliği sağlanmış sistem muhafaza odalarında saklanmalıdır.
- Kurum içindeki bilgi saklama araçları kurum dışına çıkartılmamalıdır.
- Veri tabanı sunucusuna zorunlu kalınmadıkça root veya admin olarak erişim sağlanmamalıdır.
- Veri tabanına erişecek kişilerin kendi adlarına ait kullanıcı adı olmalı ve yetkilendirme yapılmalıdır.
- Kullanıcıların hepsinin yaptıkları işlemler loglanmalıdır.

- Veri tabanı yöneticiliği yetkisi kurum içinde sadece bir kullanıcıda bulunmalıdır.
- Veri tabanı sunucusunda olan şemaların, yetkili kişiler dışındaki diğer kişilerin erişmemesi sağlanmalıdır.
- Veri tabanı sunucularına kod geliştiren kişiler dışında hiçbir hesap bağlanıp sorgu yapamamalıdır. İstekler ara yüzden yapılmalıdır.

İnternette her saniye siber suçlar oluyor. Siber suçlular, ister parasal kazançlar olsun, ister dijital dünyanın huzurunu bozmak için olsun, sürekli olarak suçlar planlıyor. Bu nedenle, siber güvenlik bugün her zamankinden daha önemlidir. İşletmeler, bilgisayar korsanlarının sistemlerinde ve ağlarında başlatabilecekleri çeşitli saldırı türlerinden kendilerini korumalıdır.

Göz önüne serilen veriler, incelenen istatistikler doğrultusunda;

- Hanelere Göre internet erişimi 2021 Yılında %92,0 olmuştur.
- Teknoloji internete olan bağımlılık 2021 yılında %82,6 olmuştur.
- İnterneti düzenli olarak kullananların oranı %80,5 olmuştur
- E-devlet hizmeti kullananların oranı 2021 yılında 58,9 olmuştur.
- İnternet üzerinden mal ve hizmet siparişi verme ya da satın alma oranı ise 2021 yılının son üç ayında %49,0 olmuştur. Bunlardan %19,6 sı ödeme güvenliği veya gizlilik endişeleri duymaktadır.
- 2021'in ilk 6 ayında Türkiye'de 288 bin 445 adet siber saldırı gerçekleşmiştir.

Bu verilerin ışığında internet kullanım oranlarının artması ayrıca internet ortamındaki alışveriş oranlarının yüksek olması zaafiyet oranlarının artması beklenmektedir. Bu oranların artmasına rağmen alınan önlemler ve tedbirler ülkemiz için önemli ölçüde etkili olmuştur. Ülkelerin siber güvenlik güç kapasitelerine önemli bir dayanak olan ve bu alanda gelişim seviyelerini gösteren “GCI (Küresel Siber Güvenlik Endeksi)” Uluslararası Telekomünikasyon Birliği (ITU) verilerine göre; [74]

- 2017 verilerine göre Türkiye 164 ülke arasında 43.sırada,
- 2018 verilerine göre ise 175 ülke arasında 20.sırada
- 2019 verilerine göre 176 ülke arasında 14. Sırada
- 2020 verilerine göre 182 ülke arasında 11. Sırada yer almaktadır.

Bu verilerin ışığında 2017-2020 yılları arasında alınan önlemler ve tedbirler ile yapılan farkındalık eğitimlerinin etkili olduğu görülmektedir. Ancak her geçen gün değişen siber saldırı çeşitliliği ve bu saldırılardan korunmak için alınan tedbirler ile eğitimlerin sürdürülebilir olması değerlendirilmektedir. **“Siber zafiyetlerde ve veri ihlallerinde en büyük etkenin insan faktörü olduğu unutulmamalıdır.”**



KAYNAKLAR

- [1] Verizon business resources reports – Verizon şirketler raporu
<https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf>, 2021
- [2] TC. Hazine ve Maliye Bakanlığı 27001 Bilgi güvenliği eğitimleri kapsamında alınması gereken tedbirler ve incelemeler.
www.hmb.gov.tr/btgm/guvenlik/bilgi_guvenligi_raporlari.pdf, 2021
- [3] Tuik Raporu - Bilişim Teknolojileri Kullanım Araştırması
<https://data.tuik.gov.tr/Kategori/GetKategori?p=Bilim,-Teknoloji-ve-Bilgi-Toplumu-102> , 2020
- [4] Saprikin, Oleksandr Sergiyovich. " Models and methods for diagnosing Zero-Day threats in cyberspace." Current information technology bulletin 4.2: 155-167. 2021
- [5] Trautman, Lawrence J. ve Peter C. Ormerod. "Kurumsal yöneticilerin ve memurların siber güvenlik bakım standardı: Yahoo veri ihlali." *NS. UL Rev.* 66 : 1231.2016.
- [6] Marsilya, Emmanuel. Günümüz Toplumunda Veri İhlallerinin Hızlı Büyümesi. Dis. Utica Koleji, 2020.
- [7] Ergen, Yunus. "Büyük veri, sosyal medya ve etik: Facebook örneğinde bir değerlendirme. " Ege Üniversitesi İletişim Fakültesi Yeni Düşünceler Hakemli e-Dergisi 10:53-64, 2018.
- [8] Singh, Ajay. CyberStrong: İşletme Yöneticileri için Siber Risk Yönetimi Üzerine Bir Başlangıç . Adaçayı Yayınları Pvt. Sınırlı, 2020.
- [9] Wertheim, Steven. "Tips for Fighting Off Cybercrime in 2020." *The CPA Journal* 90.3:64-66 , 2020.
- [10] Yee, George OM. "Reducing the Attack Surface for Sensitive Data." *International Journal on Advances in Security* Volume 13, Number 3 & 4, 2020.

- [11] Parizi, Reza M., et al. "Security in online games: Current implementations and challenges." Handbook of Big Data and IoT Security. Springer, Cham,: 367-384, 2019.
- [12] Radzuik, Aliaksei. "Yana Kurto Aliaksei Radziuk." Publishing Board: Dr. Yury Holubeu (chairperson); Ms. Volha Zhuravskaya (vice-chairperson); Dr. Katsiaryna Lushneuskaya; Ms. Rita Rusina: 165, 2021.
- [13] Gökalp, Ömer Melik. "Sosyal Medya Şifre Güvenliğinin Önemi." Gazi Üniversitesi, Gazi Bilişim Enstitüsü, Adli Bilişim Bölümü, 10.13140/RG.2.2.23985.10080, 2021.
- [14] Vural, Yılmaz, and Şeref SAĞIROĞLU. "Kurumsal bilgi güvenliği ve standartlari üzerine bir inceleme." Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 2008.
- [15] Arif, S. A. R. I., et al. "Bilişim Sistemleri Etiğine Aykırı Zararlı Yazılımların İncelenmesi." , 2014
- [16] Acilar, Ali, and Ayse Bastug. "Social Engineering: Anformation Secrity Threat In Enterprises." PressAcademia Procedia 2.1: 289-297, 2016
- [17] Miller, Bryon, et al. "Prevention Of Phishing Attacks: A Three-Pillared Approach." Issues in Information Systems, 2020.
- [18] Mirza, Qublai Khan Ali, Ghulam Mohi-Ud-Din, and Irfan Awan. "A cloud-based energy efficient system for enhancing the detection and prevention of modern malware." 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2016.
- [19] Baykara, Muhammet, and D. A. Ş. Resul. "Saldırı tespit ve engelleme araçlarının incelenmesi." Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi 10.1: 57-75, 2019.
- [20] Kaur, Gurline, and Navjot Kaur. "Penetration Testing--Reconnaissance with NMAP Tool." International Journal of Advanced Research in Computer Science, 2017.

- [21] Quinn Kiser, Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering, New York, 2020.
- [22] Korucu, Onur. "Yeni Normal Dünya Düzeninin Siber Güvenlik Ve Bilgi Güvenliğine Etkileri." *Yönetim Bilişim Sistemleri Dergisi* 7.1: 44-60.M.Nezir Yücesoy, Evren Pazoğlu “ Siber Güvenlik Operasyonları Merkezi -süreçler-bölüm-3” , Gazi Kitabevi, 2021
- [23] R. A. Clarke, R.K. Knake, “Cyber War-The Next Threat to National - Security and What to Do About It”, New York: HarperCollins - Publishers, 74-85, 2010.
- [24] Quinn Kiser, Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering, New York, 2020.
- [25] Stuxnet, Baezner, Marie, and Patrice Robin. *Stuxnet*. No. 4. ETH Zurich, 2017.
- [26] Yıldız E. Ve Şahin S. Bulut bilişimde güvenlik riskleri ve önlemleri. II. Uluslararası Bilişim Hukuku Kurultayı İzmir, 2011.
- [27] Quinn Kiser, Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering, New York, 2020.
- [28] Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014 - Fırat Üniversitesi Sosyal Bilimler Dergisi Fırat University Journal of Social Science Cilt: 25, Sayı: 2, Sayfa: 229-248, ELAZIĞ-2015.
- [29] Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi - Fulya ASLAY - Pages: 24 – 28, 2017.
- [30] Kirsch, Cassandra. "The Grey hat hacker: Reconciling cyberspace reality and the law." *N. Ky. L. Rev.* 41, 383, 2014.
- [31] Pillay, Rishalin. *Learn Penetration Testing: Understand the art of penetration testing and develop your white hat hacker skills*. Packt Publishing Ltd, 2019.
- [32] O.Değirmenci,“Bilişim Suçlar”, (Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), İstanbul, 2002.

- [33] Matulesky, Andik, and Nabilla H. Humaira. "Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits." *Psychology and Behavioral Sciences* 5.6:137-142, 2016.
- [34] Tanczer, Leonie Maria. "The terrorist–hacker/Hackivist distinction: an investigation of self-identified hackers and Hacktivists." M. Conway, L. Jarvis, O. Lehane, S. Macdonald & L. Nouri (Eds.), *Terrorists' Use of the Internet*: 77-92, 2017.
- [35] Ankara Üniversitesi – <https://acikders.ankara.edu.tr/> Ankara Üniversitesi Nallıhan Meslek Yüksekokulu Sızma belirleme testleri.pptx, 2021
- [36] Quinn Kiser, *Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering*, New York, 2020.
- [37] Ergenlerin Siber Zorbalık ve Siber Mağduriyete İlişkin Algıları. Source: Gaziantep University Journal of Social Sciences, Vol. 11 Issue 3, p819-833, 2012
- [38] Siber Terörizm Tehditleri, C Hatipoğlu - (International Congress on Political, Economic and Social Studies), 2017
- [39] ÖZTÜRK, Mahmut Sami. "SİBER SALDIRILAR, SİBER GÜVENLİK DENETİMLERİ VE BÜTÜNCÜL BİR DENETİM MODELİ ÖNERİSİ." *Muhasebe ve Vergi Uygulamaları Dergisi* : 208-232, 2018.
- [40] Bilgi Üniversitesi - <https://it.bilgi.edu.tr/tr/guvenlik/ddos/> , 2021
- [41] ÇELİK, Soner, and Barış Çelikaş. "Güncel Siber Güvenlik Tehditleri: Fidyeye Yazılımlar." *Cyberpolitik Journal* 2.4 : 296-323, 2017.
- [42] Quinn Kiser, *Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering*, New York, 2020.
- [43] Vural, Y. Kurumsal Bilgi Güvenliği ve Sızma Testleri, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2007.
- [44] Ünver, M. ve Mirzaoglu, A.G. Yemleme ("Phishing"), *Bilgi Teknolojileri ve İletişim Kurumu*, 2011.

- [45] Canbek, G., Sağiroğlu, Ş. Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri. Türkiye: Grafiker, 2006.
- [46] Özdemir, Murat, and Erdal Kılıç. "A mail discrimination study using network basis tools." 2016 24th Signal Processing and Communication Application Conference (SIU), spf, IEEE, 2016.
- [47] Ilchenko, O. V., et al. "Fishing as a cybercrime in the Internet banking system: economic and legal aspects.", 2019.
- [48] Karlof, Chris, et al. "Dynamic pharming attacks and locked same-origin policies for web browsers." Proceedings of the 14th ACM conference on Computer and communications security, 2007.
- [49] Shah, Darsh, Vaibhav Shah, and Harsh Shah. "Survey on Computer Worms." International Journal on Recent and Innovation Trends in Computing and Communication 5.8: 184-194, 2017.
- [50] Yiğit, T., Akyıldız, M., A. Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitü Dergisi, 18(21), 14-21, 2012
- [51] Microsoft-<https://support.microsoft.com/tr-tr/topic/virüsler-ve-diğer-kötüamaçli-yazilimlar-nasil-engellenir-ve-kaldirilir-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5>, 2020
- [52] Güncel Siber Güvenlik Tehditleri: Fidyeye Yazılımları Soner ÇELİK-Barış ÇELİKTAŞ, Cyberpolitik Journal Vol. 3, No. 5, 2021.
- [53] Casus Yazılımlar: Buluşma Yöntemleri ve Önlmeleri-Gürol CANBEK ve Şeref SAĞIROĞLU-Gazi Üniv. Müh. Mim. Fak. Der.- Cilt 23, No 1, 165-180, 2008.
- [54] Quinn Kiser, Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering, New York, 2020.
- [55] Çelik, Soner, and Barış Çeliktaş. "Güncel Siber Güvenlik Tehditleri: Fidyeye Yazılımlar." *Cyberpolitik Journal* 2.4: 296-323, 2017.
- [56] Hatfield, Joseph M. "Social engineering in cybersecurity: The evolution of a concept." *Computers & Security* 73: 102-113, 2018

- [57] Wilson, Brent. "Introducing cyber security by designing mock social engineering attacks." *Journal of Computing Sciences in Colleges* 34.1 (2018): 235-241, 2018.
- [58] Karamollaoglu, Hamdullah, İbrahim Alper Dogru, and Murat Dorterler. "Detection of Spam E-mails with Machine Learning Methods." 2018 Innovations in Intelligent Systems and Applications Conference (ASYU). IEEE, 2018.
- [59] Canbek, G., Sağiroğlu, Ş., *Bilgisayar Sistemlerine Yapılan Saldırıları ve Türleri: Bir İnceleme*, Erciyes Üniversitesi, Fen Bilimleri Dergisi, Cilt : 22, Sayı : 1–2, Basımda, 2007.
- [60] Quinn Kiser, *Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering*, New York, 2020.
- [61] Hilm, David, and David Rahim. "Two-factor Authentication and Digital Signing for an Enterprise System utilizing Yubikey.", 2019.
- [62] Kosiur, David (Çeviri:Tansel Akyüz); *Özel Sanal Ağlar (VPN) inşa etme ve yönetme*, 2001.
- [63] Tekerek, A. D. E. M. and O. F. Bay. "Design and implementation of an artificial intelligence-based web application firewall model." *WAF, Neural Network World* 29.4: 189-206, 2019.
- [64] Kali Linux – Kali Linux Nedir nasıl kullanılır.
<https://www.kali.org/docs/introduction/what-is-kali-linux/> ,2021
- [65] *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux* - G Najera-Gutierrez, JA Ansari – 2018
- [66] *Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark* - GD Singh – 2019
- [67] Essential NetTools – Tarama aracı Essential NetTools Nedir?
<https://www.tamos.com/products/nettools/> , 2021
- [68] A. X. Liu and M. G. Gouda, "Diverse Firewall Design," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 9, pp. 1237-1251, doi, 2008

- [69] Khadafi, Shah, Budanis Dwi Meilani, and Samsul Arifin. "Sistem keamanan open cloud computing menggunakan ids (intrusion detection system) dan ips (intrusion prevention system)." *Jurnal IPTEK* 21.2: 67-76, 2017.
- [70] V. Clincy and H. Shahriar, "Web Application Firewall: Network Security Models and Configuration," *IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 2018, pp. 835-836, doi, 2018.
- [71] W. U. Hassan, A. Bates and D. Marino, "Tactical Provenance Analysis for Endpoint Detection and Response Systems," *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 1172-1189, doi, 2020.
- [72] R. K. Sharma, H. K. Kalita and B. Issac, "Different firewall techniques: A survey," *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1-6, doi, 2014.
- [73] I. Anastasov ve D. Davcev, "Küresel ve dağıtılmış ortamlar için SIEM uygulaması", *Dünya Bilgisayar Uygulamaları ve Bilgi Sistemleri Kongresi (WCCAIS)*, s. 1-6, doi, 2014.
- [74] Aldemir, Ceray, and K. A. Y. A. Merve. "Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları." *Kamu Yönetimi ve Politikaları Dergisi* 1.1: 6-27, 2019.

ÖZGEÇMİŞ

Ad Soyad: Mehmet Özer BAŞESKİOĞLU

Lisans: Bilgisayar Mühendisliği

Yüksek Lisans: İş Sağlığı ve Güvenliği (Tezsiz)

Mesleki Deneyim ve Ödüller:

Yayın ve Patent Listesi:

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR

Bildiri:

- [1] M.Özer Başeskioğlu, Abdülkadir Tepecik, Siber Güvenlik, Bilgisayar Ağlarında Kimlik Avı, Kötü Amaçlı Yazılım, Fidyeye Yazılım ve Sosyal Mühendislik - Korsanlıktan Korumaya Yönelik İncelemeler, 3rd İnsan-Bilgisayar Etkileşimi, Optimizasyon ve Robotik Uygulamaları Uluslararası Kongresi, Hora 2021, 11-13 Haziran 2021, Türkiye

<https://ieeexplore.ieee.org/abstract/document/9461272>