SİBER GÜVENLİK EĞİTİMİ

Birleşmiş Milletler Eğitim, Bilim ve Kültür Kurumu
UNESCO Türkiye Milli Komisyonu

ÖĞRETMEN YETİŞTİRME VE GELİŞTİRME GENEL MÜDÜRLÜĞÜ

TÜRKİYE CUMHURİYETİ MİLLİ EĞİTİM BAKANLIĞI

Millî Eğitim Bakanlığı
Öğretmen Yetiştirme ve Geliştirme
Genel Müdürlüğü Adına
Doç. Dr. Adnan BOYACI
Genel Müdür

Editör
Sibel AKBIYIK
Daire Başkanı

Yazarlar
Dr. Erdal ÖZDOĞAN
Dr. İbrahim EDİZ
Ali GÖKDEMİR
Arzu KİLİTÇİ CALAYIR
Hakan VOLKAN
Onur DEMİRKAPI

Grafik Tasarım
Kadir İbrahim BORA

Kapak Tasarım
Meliha BAKA ÇAKMAKLI

SİBER GÜVENLİK EĞİTİMİ

ISBN: 978-975-11-5609-9

Millî Eğitim Bakanlığı Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğünün yazılı izni olmadan bu kitap içeriğinin bir kısmı veya tamamı yeniden üretilemez, çoğaltılamaz, dağıtılamaz.

2020

SİBER GÜVENLİK EĞİTİMİ

Değerli Meslektaşım,

Biz öğretmenlerin iyi bildiği bir gerçek var ki o da öğretmenliğin aslında hayat boyu devam eden bir öğrenme süreci olduğudur. Her zaman söylerim "Öğretmenlik bir insanın kendi öğrenme yolculuğu, kendi olgunlaşma sürecidir." diye. Hayat şartlarının, mesleki sıkıntıların yeteri kadar izin vermediği bu sürecinin zaman zaman kesintiye uğradığını sizler kadar bizler de hissediyoruz. Her birimizin ilgi alanı, yetenekleri, birikimleri, tecrübeleri farklı olsa da değişen şartlara uyum konusunda ihtiyacımız ortak. Gerek mesleki gerekse bireysel olarak kimimiz yeni teknolojilere, kimimiz farklı yol ve yöntemlere, kimimiz materyale, kimimiz de ruhumuzu doyuracak, hayatımıza anlam katacak etkinliklere ihtiyaç duyuyoruz. Bu ihtiyaçların giderilerek sizlerin mesleki anlamda daha yetkin, fikren ve ruhen daha zengin olması için Bakanlığımızın da üzerine düşeni yapmaya çalıştığını ve sizler için birinci dereceden önemli kitap, kılavuz ve yardımcı ders materyallerini hızla hazırlamaya gayret ettiğini belirtmek isterim.

Öğretmeninden akademisyenine, okul yöneticisinden eğitim gönüllüsüne kadar alanında uzman kişilerce hazırlanan bu kitaplar teorik bilgiler yanında ders ve kazanımlara yönelik sınıf içinde ve dışında kolayca uygulayabileceğiniz etkinlik örnekleri içermektedir. Edinilen tecrübelerin, yaşanan problemlerden çıkarılan derslerin, geleceğe dair öngörülerin ve özverili bir çalışmanın ürünü olan bu kitaplar mesleki anlamda karşılaşabileceğiniz sorunlara çözüm, ilgi ve ihtiyaçlarınıza karşılık bulmanızda, derslerinize eğlence ve zenginlik katmanızda sizlere yardımcı olmak amacıyla hazırlandı. En büyük temennimiz, emeklerinizin, ilgi ve gayretlerinizin karşılıksız kalmaması ve elinizdeki kitabın ihtiyaçlarınıza, bilgi ve birikimlerinize katkıda bulunmasıdır.

Kitapların hazırlanmasında ve sizlere ulaştırılmasında emeği geçen tüm paydaşlarımıza teşekkür ediyor, meslek hayatınızda ve öğrenme yolculuğunuzda başarılar diliyorum.

Ziya Selçuk
Millî Eğitim Bakanı

ÖN SÖZ

Değerli Meslektaşlarım,

İnternetin gündelik hayatın hemen her alanında yaygın olarak kullanılması; önemli bilgi ve verilerin bilgisayar ve ağlar üzerinden yürütülmesi, bireylerin, kurumların ve devletlerin güvenlik kavramını farklı boyutlarıyla ele almasını gerekli kılmaktadır. Günümüz dünyasında dijital teknolojilerin geldiği nokta kullanıcılara birçok kolaylık sunarken güvenlik açıklarının oluşmasına ve verilerin kötü amaçlarla kullanılmasına da neden olmaktadır. Bu sorun hem bireysel hem de toplumsal güvenliği tehdit ettiği için siber güvenlik kavramı ortaya çıkmıştır. İnternet veya ağlar üzerinden aktarılan bilgi ve verilerin korunması, bireysel ya da kurumsal veri güvenliği kritik bir sorumluluk hâline gelmiştir.

Bu sorumluluk kapsamında Genel Müdürlüğümüz tarafından öğretmenlerimizin siber güvenlik konusunda bilgi sahibi olması, kötü amaçlı yazılım ve saldırı türlerini tanımaları, kişisel verilerin korunması için gerekli önlemleri almaları konusunda bilgi ve becerilerini geliştirmek amacıyla Siber Güvenlik Mesleki Gelişim Programı hazırlanmıştır. Eğitim programından daha çok öğretmenimizin yararlanabilmesi ve siber güvenlik konusunda öğrencilerine rehberlik edebilmesi amacıyla "Siber Güvenlik Eğitimi" kitabı hazırlanmıştır.

Siber Güvenlik Eğitimi kitabı on bölümden oluşmaktadır. Her bir bölümde siber güvenlik farklı boyutlarıyla ele alınmaktadır. Siber güvenliğin temel kavramları, zararlı yazılımlar, siber saldırı ve saldırı türleri, temel güvenlik önlemleri, internet ve sosyal medya güvenliği, ağ ve işletim sistemi güvenliği, kriptoloji, siber güvenlik ve bilişim hukuku, Python ile siber güvenlik uygulamalarına yer verilen kitap her alandan öğretmenlerimizin yararlanabileceği bir nitelikte tasarlanmıştır. Burada verilen bilgiler çerçevesinde öğretmenlerimiz hem kişisel verilerin korunması ve gerekli önlemleri alma konusunda bilgi ve beceri sahibi olabilecekler hem de bu konuda öğrencilerinin bilinçlenmesine yardımcı olabileceklerdir.

Kitabın hazırlanmasında emeği geçen tüm meslektaşlarıma teşekkür ediyor, siz değerli öğretmenlerimizin bireysel ve mesleki gelişine katkıda bulunmasını temenni ediyorum.

Adnan Boyacı

Öğretmen Yetiştirme ve Geliştirme
Genel Müdürü

İÇİNDEKİLER

TERİMLER 17

1. BÖLÜM: SİBER GÜVENLİĞE GİRİŞ ve TEMEL KAVRAMLAR 19

1.1 SİBER GÜVENLİĞE GİRİŞ 20
1.2 SİBER GÜVENLİKTE BİLGİ VE VERİ KAVRAMLARI 22
1.3 YAZILIM VE DONANIM BİLEŞENLERİ 25
1.3.1 Donanım 26
1.3.2 Yazılım 27
1.3.3 İşletim Sistemleri 27
1.4 TEMEL İLETİŞİM VE AĞ BİLEŞENLERİ 29
1.4.1 Ağ Türleri 29
1.4.2 Ağ Bileşenleri ve Donanımları 30
1.4.3 Bilgisayar Ağlarında İletişim ve OSI Referans Modeli 34
1.4.4 Ağ Protokolleri 38
1.4.5 Uçtan Uca Ağ İletişim Örneği 46

2. BÖLÜM: SİBER GÜVENLİK KAVRAMLARI 57

2.1 TEHDİT AKTÖRLERİ VE GÜVENLİK KAVRAMLARI 58
2.1.1 Amatörler 58
2.1.2 Bilgisayar Korsanı (Hacker) 59
2.1.3 Tehdit Aktörlerine İlişkin Kavramlar 60
2.2 ZARARLI YAZILIMLAR (MALWARE) 61
2.2.1 Virüsler 62
2.2.2 Solucanlar (Worm) 64
2.2.3 Truva Atları (Tojan Horse) 67
2.2.4 Diğer Zararlı Yazılımlar 68
2.2.5 RootKit Türleri ve Tespit Yöntemleri 72
2.2.6 Zararlı Yazılımın Belirtileri ve Korunma Yöntemleri 75

2.3 SİBER GÜVENLİK UNSURLARI 76
2.3.1 Gizlilik 76
2.3.2 Bütünlük 77
2.3.3 Erişilebilirlik 77
2.3.4 Bilgi Güvenliğinde Diğer Unsurlar 78
2.4 SİBER SALDIRILAR VE SALDIRI TÜRLERİ 79
2.4.1 Siber Saldırılar 79
2.4.2 Ağ Saldırıları 80
2.4.3 DoS ve DDoS Saldırıları 81
2.4.4 Sosyal Mühendislik Saldırıları 83
2.4.5 Uygulama Atakları 86
2.4.6 Gelişmiş Kalıcı Tehditler (APT) 89
2.4.7 Siber Ölüm Zinciri (Cyber Kill Chain) 90
2.4.8 Siber Saldırı Vektörleri ve Saldırı Yüzeyleri 93
2.5 SİBER SAVAŞ ÖRNEKLERİ 94

3. BÖLÜM: GÜVENLİK STRATEJİLERİ ve KORUNMA 97
3.1 SİBER GÜVENLİKTE BİLGİ TOPLAMA 98
3.1.1 Pasif Bilgi Toplama 98
3.1.2 Aktif Bilgi Toplama 105
3.1.3 Google Hack Veritabanı ile Veri Toplama 108
3.2 TEMEL GÜVENLİK ÖNLEMLERİ 110
3.2.1 Parola Güvenliği 112
3.2.2 İki Aşamalı (Faktörlü) Doğrulama 117
3.2.3 Biometrik Kimlik Doğrulama 118
3.2.4 Parola Kırma Teknikleri 119
3.3 GÜVENLİK ZAAFİYETİ DERECELENDİRME 120
3.3.1 CVE İsimlendirmesi 120
3.3.2 Zaafiyet Derecelendirmesi (CVSS) 123

İÇİNDEKİLER

3.4 GÜVENLİK YAZILIMLARI 125
3.4.1 Antivirüs 125
3.4.2 AntiMalware 125
3.4.3 Konak Tabanlı Güvenlik Duvarı 125
3.4.4 Diğer Yazılımlar 126
3.5 GÜVENLİK OPERASYONLARI MERKEZİ 126
3.5.1 SOC Fonksiyonları 127
3.5.2 Olay Müdahale Yaşam Döngüsü 128

4.BÖLÜM: İNTERNET VE SOSYAL MEDYA GÜVENLİĞİ 131
4.1 İNTERNET ORTAMINDAKİ SİBER TEHDİTLER VE TEHLİKELER 133
4.1.1 İnternetteki Tehlikeler ve Tehditlerin Sınıflandırması 134
4.2 İNTERNETİN İSTİSMARI, SİBER TEHDİT VE TEHLİKELER 134
4.2.1 Veri Çalınması 134
4.2.2 Sistemlerin Hizmet Dışı Bırakılması 135
4.2.3 Zararlı Yazılım Yüklenmesi 136
4.2.4 Tehdit ve Şantaj Maksatlı Kullanım 136
4.3 SOSYAL MEDYANIN İSTİSMARI 137
4.3.1 Sosyal Medyada Güvenli İletişim 139
4.3.2 Sosyal Medyada ve Güvenlik Ayarları 139
4.4 İNTERNET TARAYICILAR 141
4.4.1 E-posta ve Web Tarayıcı Gizliliği 142
4.4.2 Tarayıcı Eklentileri 142
4.4.3 Çerez (Cookie) Yönetimi 144
4.4.4 Parola Yönetimi 144
4.5 İNTERNETTE GÜVENLİ İLETİŞİM 145
4.5.1 İnternette Tehlikelerden Korunma ve Güvenli İletişim Kurma 145
4.6 HTTP ve WEB GÜVENLİĞİ 146
4.6.1 http Protokolünün Temelleri 147

4.6.2 Web Güvenliği 151
4.7 DİJİTAL OYUNLAR VE TEHDİTLER 155
4.7.1 Dijital Oyunlar 155
4.7.2 Dijital Oyunlardaki Tehditler 156
4.7.3 Dijital Oyunlardaki Tehditlerden Korunma 157

5. BÖLÜM: AĞ GÜVENLİĞİ 159
5.1 TCP/IP PROTOKOLLERİNDEKİ ZAYIFLIKLAR 160
5.1.1 TCP Zayıflıkları 161
5.1.2 ARP Zayıflıkları 162
5.1.3 ICMP Zayıflıkları 164
5.1.4 DHCP Zayıflıkları 166
5.1.5 DNS Zayıflıkları 166
5.1.6 Diğer Protokollerdeki Zayıflıklar 168
5.2 KABLOSUZ AĞLARDA GÜVENLİK 168
5.2.1 Kablosuz Ağlar 168
5.2.2 Kablosuz Ağ Şifreleme Modelleri 169
5.2.3 Kablosuz Ağlara Yönelik Yapılan Saldırılar 170
5.2.4 Kablosuz Ağlarda Güvenlik Uygulamaları 171
5.3 DİĞER KABLOSUZ TEKNOLOJİLERDE GÜVENLİK 172
5.3.1 Bluetooth 172
5.3.2 NFC (Yakın Alan İletişimi - Near Field Communication) 173
5.3.3 RFID 174
5.4 MOBİL CİHAZ GÜVENLİĞİ 175
5.4.1 Mobil Cihazlara Yönelik Tehditler 175
5.4.2 Mobil Platformlara Yönelik Tehditler 178
5.5 AĞ GÜVENLİK CİHAZLARI 180
5.5.1 Saldırı Önleme (IPS) ve Saldırı Tespit (IDS) Sistemleri 180
5.5.2 Güvenlik Duvarı (Firewall) 182

İÇİNDEKİLER

5.6 VPN TEKNOLOJİLERİ 184
5.6.1 VPN Nedir 184
5.6.2 VPN Türleri 186

6. BÖLÜM: İŞLETİM SİSTEMİ GÜVENLİĞİ 189
6.1 WİNDOWS İŞLETİM SİSTEMİ GÜVENLİĞİ 190
6.1.1 Windows Yönetimsel Araçlar 192
6.1.2 PowerShell 211
6.1.3 Windows İşletim Sisteminde Zararlı Yazılım Analizi 215
6.2 LİNUX İŞLETİM SİSTEMİ VE GÜVENLİĞİ 222
6.2.1 Linux İşletim Sisteminde Güvenlik 223

7. BÖLÜM : GÜNLÜK DOSYALARI ve OLAY YÖNETİMİ 231
7.1 SIEM (Security Information Event Management) 232
7.1.1 Yaygın SIEM Yazılımları 234
7.2 SECURITY ONION YAZILIMI 234
7.2.1 Security Onion Araçları 235

8. BÖLÜM: KRİPTOLOJİ 239
8.1 KRİPTOLOJİYE GİRİŞ 240
8.2 ŞİFRELEME ALGORİTMALARI 243
8.2.1 Simetrik Şifreleme 245
8.2.2 Asimetrik Şifreleme 247
8.3 ÖZETLEME ALGORİTMALARI 249
8.3.1 MD5 250
8.3.2 SHA 251
8.3.3 Salting İşlemi 252
8.4 ÖRNEK UYGULAMALAR 252
8.5 DİĞER ALGORİTMALAR VE TEKNİKLER 254

9. BÖLÜM: SİBER GÜVENLİK ve BİLİŞİM HUKUKU 259
9.1 BİLİŞİM HUKUKU TANIMI 260
9.2 KİŞİSEL VERİLERİ KORUMA KANUNU 260
9.3 YASAL MEVZUAT 261
9.4 SİBER GÜVENLİK KURULU 263
9.5 ULUSAL SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANI 264
9.6 ISO 27001 264
9.6.1 ISO 27001 Faydaları 265
9.7 SİBER GÜVENLİKTE KARİYER 265

10. BÖLÜM: PYTHON ile SİBER GÜVENLİK UYGULAMALARI 267
10.1 SOKET PROGRAMLAMA 268
10.2 PYTHON İLE NMAP KULLANIMI 271
10.3 SHODAN İLE BİLGİ TOPLAMA 275
10.4 VİGENÈRE ŞİFRELEME UYGULAMASI 280
10.5 SCAPY ile PAKET MANİPLASYONU 282
10.5.1 Scapy Örnekleri 285

KAYNAKLAR 293

TERİMLER

Bu kitap içerisinde yer alan İngilizce terimlerin Türkçe karşılıkları aşağıdaki tabloda verilmiştir.

Access point	Erişim noktası
Adware	Reklam yazılımı
APT	Gelişmiş Kalıcı Tehditler
Baiting	Tuzağa düşürme
Baseline	Temel Çizgi
Broadcast	Yayın
Default route	Varsayılan rota
DNS	Alan Adı Sistemi
DoS	Hizmet Reddi
Exploit	İstismar
Firmware	Bellenim
Gateway	Ağ geçidi
Hacker	Bilgisayar korsanı
Hacking	Hacklemek
Host	Konak
Keylogger	Tuş tutucular
Malware	Zararlı yazılım
Master Boot Record	Ana Önyükleyici Kaydı
Multicast	Çoklu yayın
Protocol Data Unit - PDU	Protokol Veri Birimi - PVB
Phishing	Oltalama
Port	Bağlantı noktası
Pretexting	Bahane uydurma
Quid pro quo	Bir şey için bir şey
Ransomware	Fidye yazılımı
Router	Yönlendirici
Scareware	Korku yazılımı
Spear Phishing	Yemleme kancası
Spoofing	Aldatma
Spyware	Casus yazılım
SQL Injection	SQL enjeksiyonu
Subnet Mask	Ağ Maskesi
Switch	Anahtar
Unicast	Tekil yayın
Worm	Solucan

Siber Güvenlik

Siber Güvenlik

Siber Güvenlik

BÖLÜM 1

SİBER GÜVENLİĞE GİRİŞ ve TEMEL KAVRAMLAR

1.1 SİBER GÜVENLİĞE GİRİŞ

Güvenlik kavramı tarih boyunca önemli konularından ve ihtiyaçlarından biri olmuştur. Günümüz teknoloji temelli iletişim yapısında güvenlik ihtiyacı kavramı eskiye kıyasla önemli ölçüde farklılık göstermektedir. Bilişim teknolojilerinin ve özellikle internetin günlük hayatın hemen her alanındaki etkin kullanımının, bu kavramın değişiminde büyük etkisi vardır. Genel olarak bilişim teknolojileri, kişilerin hayatını kolaylaştırmak için geliştirilmektedir. Kişilere ait tıbbi veriler, eğitim verileri, mali veriler ve sosyal veriler gibi bilgiler dijital ortamda tutulmakta ve bilişim sistemlerinin işlevselliğinde kaynak teşkil etmektedir. Bilişim teknolojileri insan hayatını kolaylaştırmış olmasına rağmen, art niyetli kişilerin de hedefi ya da aracı olabilmektedır.

İnternetin ortaya çıkışı, günlük hayattaki hemen her alanda kullanımı ve yaygınlaşması, kritik, hassas verilerin ve altyapı sistemlerinin bilgisayarlar ve ağ üzerinden yürütülebilmesi, kurumların yanı sıra devletlerin de güvenlik kavramını farklı boyutlarla ele almalarına neden olmuştur. Kişisel açıdan ele alındığında, bireye ait finansal bilgiler, sağlık bilgileri gibi veriler "hassas" veriler olarak adlandırılabilir. Bireyler, çeşitli konumlarda depolanan ya da ağdan transfer edilen bu verileri yetkisiz kişilere karşı korumak yani güvenliğinden emin olmak isterler. Aynı biçimde kurumların da güvenliğini sağlama ihtiyacı duydukları verileri bulunmaktadır.

Şekil 1.1. Siber saldıralar altyapıları hedefleyebilir

Dijital ortamda tutulan, İnternet veya ağ üzerinden aktarılabilen bu verilerin korunması, eskiye oranla çok daha önemli bir hâle gelmiş, bu nedenle güvenliğinin sağlanması ihtiyacı da aynı derece kritik bir görev ve sorumluluk oluşturmuştur.

Güvenlik ihtiyacının hem kişisel hemde kurumsal düzeyde, hatta küresel ölçekte de dikkate alınması gerekmektedir. Bir kurumun ticari sırları, patentleri, mali kayıtları ve işlerin yürütülmesiyle ilgili bilgileri de

korunması gereken önemli verilerdir. Aynı şekilde ülke çapında da, kritik altyapı bilgileri ve askeri bilgiler gibi son derece değerli ve korunması gereken bilgiler bulunmaktadır.

Bireysel ya da kurumsal, depolanan ya da hareket halinde olan tüm veriler, bu verilerin tutulmasını, aktarımını sağlayan tüm altyapılar siber güvenliğin kapsamında ele alınması gerekmektedir.

Bu bölümde, siber güvenliğin ne olduğu, kişisel ya kurumsal verilerin neler oldukları, neden korunması gerektiğine değinileccektir. Ayrıca siber güvenliğin anlaşılabilmesi için ele alınması gereken donanım, yazılım, işletim sistemi ve ağ iletişimi gibi temel kavramlar siber güvenlik çerçevesinde incelenecektir.

Siber kelimesi, İngilizcedeki **"Cyber"** kelimesinden dilimize geçmiş, bilgisayar veya bilgisayar ağları ile ilgili ya da bunları içeren kavram yahut varlıkları tanımlamak için kullanılan bir ifadedir [1] . Diğer bir deyişle birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır [2].

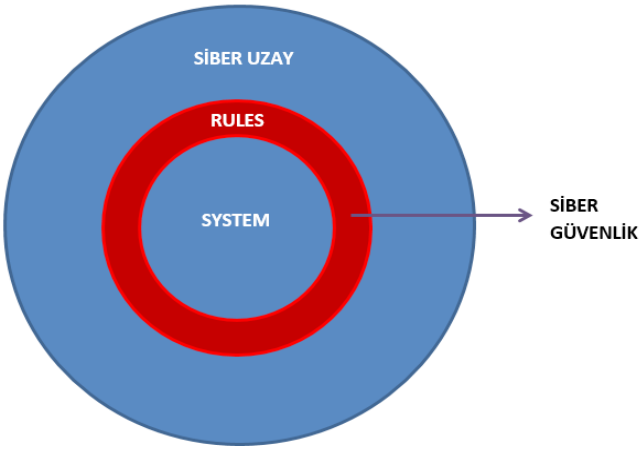
Şekil 1.2. Siber güvenlik her bireyi ilgilendiren bir kavramdır.

İnsanların farklı yollarla iletişim kurabildiği, bilgisayar ağları tarafından oluşturulan fiziksel olmayan alanlara **siber uzay** denir. Bu tanım sanal bilgisayar dünyasını ifade eder. Siber uzay, iletişim ve veri alışverişi faaliyetlerinin yapılabilmesi için iletişim protokollerini kullanan dünya çapındaki birçok bilgisayar alt ağından oluşan ağlararası büyük bir ağı içerir. Siber uzay, kullanıcıların diğer birçok faaliyetlerinin yanı sıra birbirleri ile bilgi paylaşmasına, iletişim kurmasına, etkileşimde bulunmasına, oyun oynamasına, tartışmalara veya forumlara katılmasına ve iş yapmasına olanak tanır.

Siber uzay, her ne kadar sadece İnternet ile sınırlı olmasada, genellikle İnternet olarak bilinen İnternet Servis Sağlayıcıların oluşturduğu ağlar arası ağ olarak algılanır. Siber güvenlik ise bir sistemin bu siber uzayın tehditlerinden korunması için gereken kuralların bütünü olarak ifade edilir.

Siber Güvenlik kavramı, üzerinde fikir birliğine varılmış yaygın bir tanımı olmamakla birlikte [3], bilgisayar güvenliği, bilgi güvenliği ve ağ güvenliği gibi birçok alanla ilişkili geniş bir perspektifte incelenmektedir. Bu kitap kapsamında siber güvenlik kavramı için, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında belirtilen aşağıdaki tanımlama esas alınacaktır:

"Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder [4]"



Şekil 1.3. Siber uzay ve siber güvenlik

Bu tanımlamaya göre siber güvenliğe konu olan önemli unsurlarından *biri* bilgi ve dolayısıyla *veri* kavramlarıdır.

1.2 SİBER GÜVENLİKTE BİLGİ VE VERİ KAVRAMLARI

Bilgi kavramı başlangıçta sadece felsefenin ilgi alanında yer alırken, zamanla diğer bilim dallarının konusu haline gelmiştir [5]. Basit bir ifade ile bilgi, verinin (data) anlamlandırılmış şekli olarak görülebilir. Bilgi ve veri kavramlarına Siber güvenlik açısından bakıldığında, kişiye, kuruma, bir varlığa ilişkin çeşitli değerleri, yâni "anlamı" ifade eder. Bu kitap içerisinde veri ve bilgi ifadeleri, zaman zaman birbirinin yerine kullanılacak ve siber güvenlik literatüründe yer alan çerçeve kapsamında ele alınacaktır. Siber güvenlik kapsamında dikkate alınması gereken birçok veri türü bulunmaktadır. Aşağıda özellikle bireysel açıdan siber güvenliğin konusunu teşkil eden veriler yer almaktadır.

Kişisel Tanımlanabilir Veriler: Kişiyi tanımlayan herhangi bir bilgi, "kişisel veri" olarak kabul edilebilir. Kişisel Verileri Koruma Kanunu'nda (KVKK) kişisel veri, *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi "* olarak tanımlanmaktadır. Bu bilgiler, e-posta adresi, takma ad gibi genellikle zararsız bilgiler olduğu gibi, sağlık bilgileri, eğitim bilgileri, finansal bilgiler gibi kritik öneme sahip kişisel tanımlayıcı bilgiler de olabilir. Diğer taraftan, fotoğraflar, aileye ilişkin bilgiler, sosyal medyada paylaşılan yorumlar/mesajlar, anne kızlık soyadı, doğum tarihi ve yeri, adres bilgisi, banka bilgileri, parolalar ve TC Kimlik Numarası gibi bilgiler de yine kişisel tanımlanabilir verilerdir. Özetle siber güvenlik açısından kişisel tanımlanabilir veri, kişinin dijital parmakizidir.

Şekil 1.4. Kişisel tanımlanabilir bilgiler bireye ait birçok bilgiyi barındırır

Siber suçlular, bu tür verileri birçok farklı amaç için kullanabilirler. Örneğin bu tür kişisel bilgileri ele geçirilip, yasa dışı web sayfalarında satılabilmektedir. Bu nedenle kişisel bilgiler, saldırganlar açısından potansiyel gelir kaynağı olabilir. Bu yönüyle bireyler için değerli ve korunması önemli olan bu veriler, saldırgan açısından da değerlidir ve elde edilmesi çabaya değerdir.

Kişisel Verileri Koruma Kanunu'nda öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki veriler özel nitelikli kişisel veriler olarak adlandırılmıştır. Bu kitap kapsamında özel nitelikli kişisel verilerden sağlık, eğitim ve finansal veriler ele alınmaktadır.

Sağlık Verileri: Sağlık bilgileri, kişisel tanımlanabilir bilgilerin içerisinde en önemlisi belki de en gizli olması gereken bilgilerdendir. Sağlık kuruluşundan randevu alındığında, doktor ile yapılan görüşmelerde, tetkiklerde ve muayenelerde kişisel kayıtlar oluşmakta ve çoğu durumda bir bilişim sisteminde depolanmaktadır. Bu bilgiler, kritik ve hassas öneme sahip bedensel ve ruhsal bilgileri barındırır. Kişisel bilgilerin yanı sıra, aile hakkında da (geçmişteki olaylar dâhil) bilgiler barındırmaktadır.

Nesnelerin İnterneti uygulamalarının yaygınlaşması ve giyilebilir teknolojiler sayesinde, kalp atış hızı, kan basıncı değeri gibi çok sayıda klinik veriler üretilebilmekte, kişisel sağlık bilgileri gerçek zamanlı olarak izlenebilmektedir. Bu kritik bilgiler, doğru yerlerde hayati öneme sahip son derece faydalı amaçlar için kullanılabileceği gibi, yanlış kişilerin ellerinde oldukça zararlı sonuçlara da dönüşebilir. Siber güvenlik yönüyle bu verilerin güvenliğinin sağlanması hem bireysel hem de kurumsal bir sorumluluktur.

Eğitim Verileri: Kişisel tanımlanabilir bilgilerden biri de eğitime ilişkin kişisel verilerdir. Eğitim durumu ve mezuniyet bilgileri gibi yararlı bilgilerin yanı sıra, özellikle eğitimi devam eden kişiler için, başarısız olunan dersler, disiplin raporları gibi bilgiler de eğitim kayıtlarını teşkil eder. Ancak bu bilgiler, özellikle reklam amaçlı kullanılabileceğinden güvenliğinin sağlanması gerekir.

Finansal Veriler: Kişisel harcamaları, gelir ve gider durumunu, bankacılık işlemlerini, bireyin satın alım gücünü, kredi notu ve bankacılık bilgileri gibi kişisel bilgileri içerir. Bu bilgiler de yine saldırganların hedefi olabilir ya da saldırganlar tarafından kullanılabilir.

Kişisel tanımlanabilir bilgiler her zaman saldırganlar için cazip birer hedef olmuşlardır. Örneğin, 2019 yılında çevrimiçi bir grafik tasarım aracı web sitesi, 4 milyon hesap bilgilerinin bilgisayar korsanlarınca ihlal edildiğini bildirmiştir. 2020 yılında, Çinli bir sosyal medya şirketi siber saldırıya uğramış ve telefon numaralarını içeren 172 milyon kullanıcı bilgisi çalınmıştır. Yine sosyal ağlar için oyun geliştiren bir şirket siber saldırıya uğramış ve 218 milyon kullanıcı bilgisi çalınmıştır. Sadece bu üç örnekten de görüleceği üzere, saldırganlar ya da diğer bir ifade ile tehdit unsurları, çok farklı ve illegal amaçlarla kişisel tanımlanabilir verileri ele geçirmek için siber uzayı kullanmaktadır. Bu bilgileri ele geçirmek için doğrudan bireye siber saldırı yapabildiği gibi, kurumlara da saldırılar gerçekleştirmektedirler.

İster bir bireyi tanımlayan kişisel veriler olsun, ister bir kurumun siber güvenliğe esas teşkil eden bilgileri olsun, tüm bu veriler siber ortamda genellikle kayıtlı veriler ve hareket halindeki veriler olmak üzere iki farklı şekilde görülür.

Kayıtlı veriler, bir veri tabanında ya da bir depolama ünitesinde saklanan verileri ifade eder.

Bir iş başvurusu yapıldığında, kişisel bilgilerin dijital bir ortamda saklanması, internet ortamında yapılan bir sosyal medya yorumunun bulutta saklanması, bir hastaneye gidildiğinde hastaya ilişkin bilgilerin depolama ortamında saklanması bunun birer örneği olarak görülebilir. Bu tür saklanan veriler, saldırganların potansiyel hedefi olduğundan, bulunduğu noktada güvenliğinin sağlanması gerekmektedir.

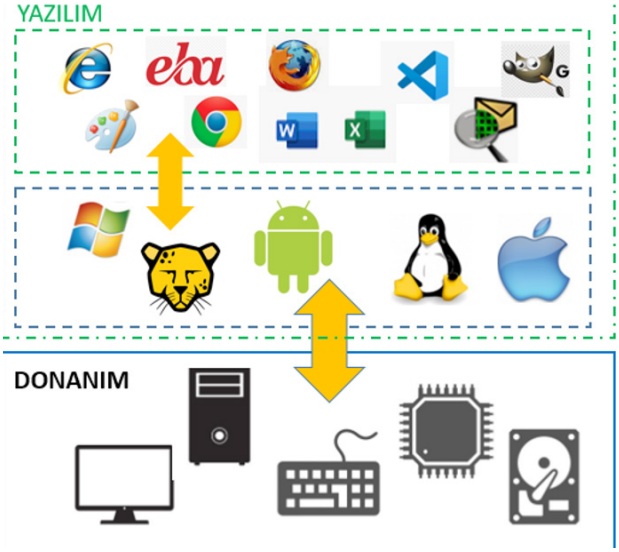
Hareket halindeki veriler, genellikle ağ ya da internet ortamından verinin hedef sisteme geçip kaydedilinceye kadar geçtiği süreci ifade eder. İnternet ortamında bir form doldururken, çevrimiçi alışveriş yaparken girilen verilerin, hedef adrese ulaşıncaya kadar güvenli olmayan ve herkese açık ağlardan transfer edilme olasılığı vardır. Bu tür hareket halindeki veriler de, yine saldırganlar için ilgi çekici olabilir, veriler hedefe ulaşmadan ele geçirilebilir, değiştirilebilir ya da tamamen silinebilir.

Hangi durumda olursa olsun verilerin güvenliğinin sağlanması siber güvenliğin amacıdır. İlerleyen bölümlerde, hem kayıtlı halde hem de hareket halinde bulunan verilerin güvenliğinin nasıl sağlandığına ilişkin teknolojiler ve kavramlar (şifreleme, veri bütünlüğü, VPN gibi) ele alınacaktır.

1.3 YAZILIM VE DONANIM BİLEŞENLERİ

Siber alan veya siber uzay sadece internet ile sınırlı değildir. Dijital ortamlar ve bilgi işlem donanımları, internete bağlı olsun ya da olmasın, siber güvenlik çerçevesinde ele alınması gerekmektedir. Çünkü saldırganlar, kişisel bilgileri elde etmek için İnternet üzerinden olsun veya olmasın farklı yöntemler denemektedirler. Üstelik her geçen gün daha farklı ve yeni teknikler ve senaryolar denemektedirler.

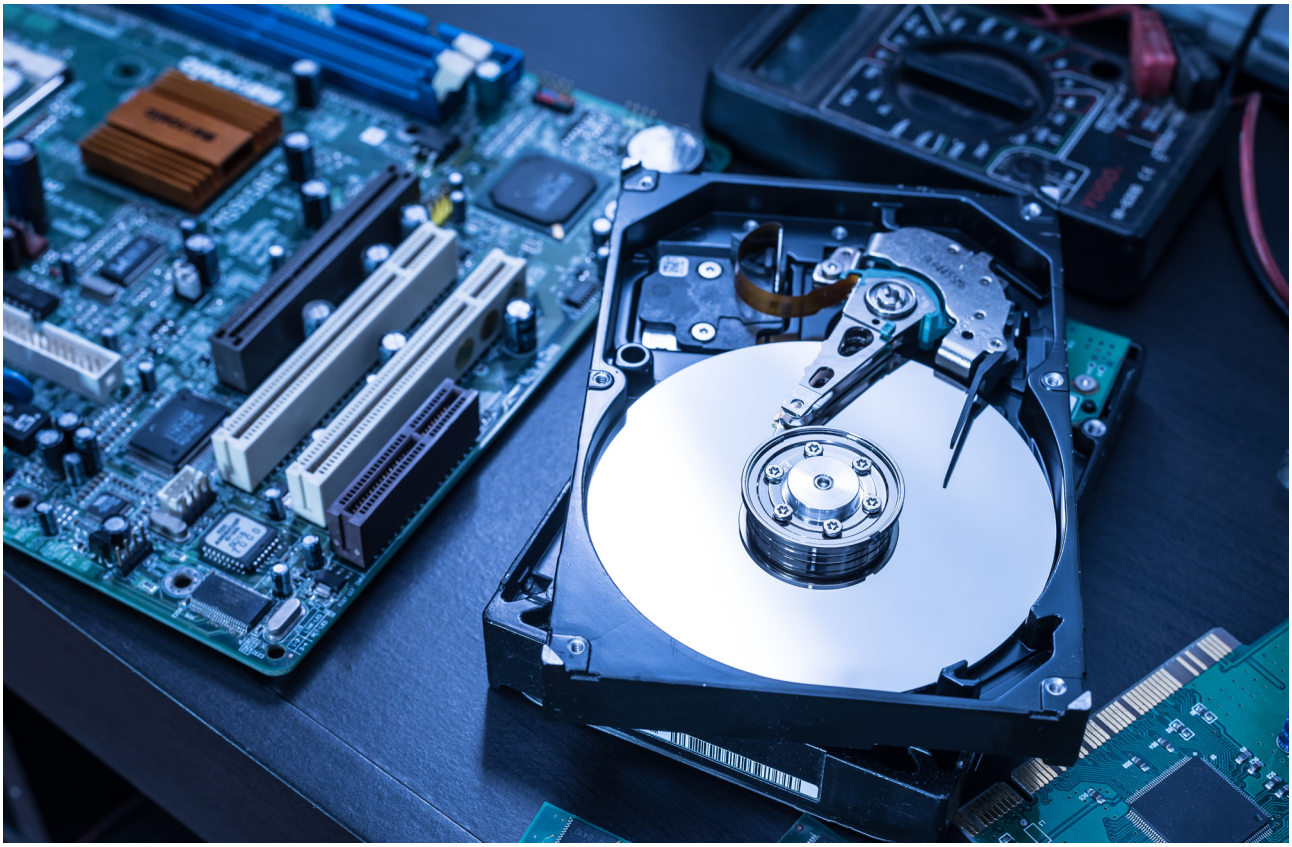
İlerleyen konularda anlatılacağı üzere, siber ortama yönelik olan bazı saldırılar internet olmadan da, taşınabilir bellekler gibi çeşitli donanımlar üzerinden gerçekleşebilmektedir. Bu nedenle, bilgisayar ya da daha geniş ifade ile bilgi işlem aygıtlarıdonanım ve yazılım yönüyle bilgi güvenliği çerçevesinde incelenmelidir.



Şekil 1.5. Yazılım ve donanım bileşenleri.

1.3.1 Donanım

Bir bilgi işlem cihazının mekanik ya da elektronik fiziki bileşenlerine donanım adı verilir. Bilgisayar açısından bakıldığında, genellikle dâhili bileşenler ve harici bileşenler olmak üzere iki kısımda incelenir.



Şekil 1.6. Dahili donanım bileşenleri

Dâhili Bileşenler: bilgisayar kasası içerisinde bulunan donanım bileşenleridir. Anakart, işlemci, RAM bellek, sabit sürücüler ve genişleme kartları bu bileşenler arasında yer alır.

Harici Bileşenler: Bilgisayar kasasına dışarıdan bağlanan bileşenlerdir. Monitör, yazıcı, kameralar, projeksiyon cihazı, harici disk sürücüler dış donanım bileşenleri arasında yer alır.

1.3.2 Yazılım

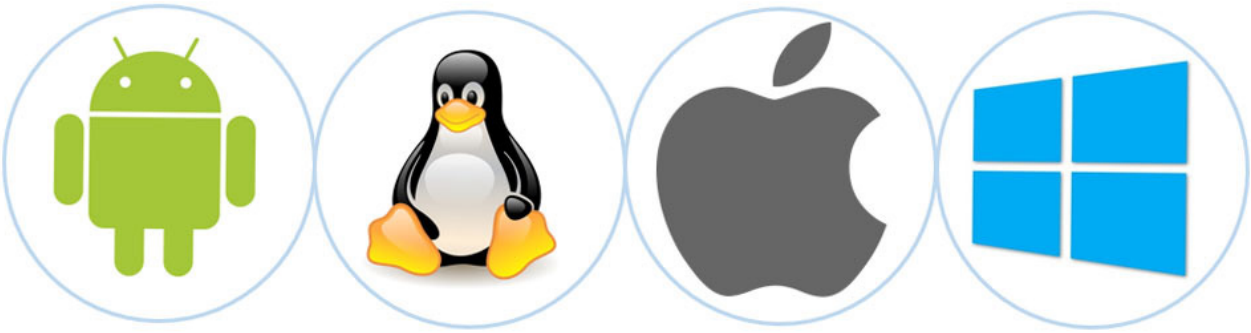
Donanım bileşenlerinin yapacağı işlemleri organize eden programlama dillerinden herhangi biri ile yazılmış kod parçaları veya bütünüdür. Yazılımlar da kendi içerinde iki kısımda incelenebilir.

Ana yazılımlar: Bilgisayar veya sistemin çalışması için gerekli olan yazılıma denir. Ana yazılım olmaz ise sistemin çalışması mümkün değildir. İşletim sistemleri bu kısımda değerlendirilebilir.

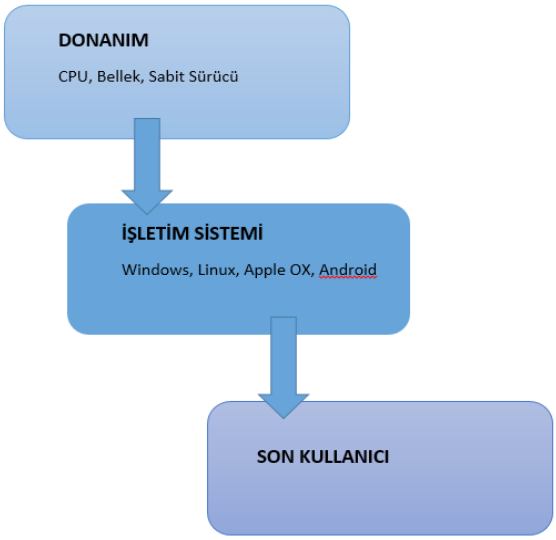
Yardımcı yazılımlar: Ana yazılım üzerinde çalışan, belirli alanlarda uzmanlaşmış ve yapılacak işlerde kolaylık sağlayan yazılımlara denir. Fotoğraf işleme yazılımı, video oluşturma yazılımları bu kısımda değerlendirilebilir.

1.3.3 İşletim Sistemleri

Bilgisayarlar sistemlerinin çalışabilmesi için gerekli temel yazılıma işletim sistemi denmektedir. İşletim sistemi olmadan donanım bileşenlerinin birbiri ile uyumlu çalışması mümkün değildir. Bilgisayar sistemlerinin doğru biçimde çalışabilmesi için işletim sistemine ihtiyacı bulunmaktadır. Kullanılan bilgisayarlar, tabletler, akıllı telefonlar, akıllı saatler, hatta beyaz eşyalarda bile işletim sistemi bulunmaktadır.



Şekil 1.7. Yaygın kullanılan işletim sistemleri



Şekil 1.8. Donanım, yazılım ve kullanıcı etkileşimi

İşletim sistemleri genellikle satın alınan herhangi bir bilgisayara önceden yüklenmiş olarak gelir. Pek çok kişi bilgisayarlarıyla birlikte gelen işletim sistemini kullanır, ancak işletim sistemlerini yükseltmek ve değiştirmek mümkündür.

İşletim sistemi, bilgisayar dilini bilmeden bilgisayarla iletişim kurulmasına yardımcı olur. Kullanıcılar yardımcı yazılımlar aracılığıyla işletim sistemleri ile iletişime geçerler. İşletim sistemleri, kendisine gelen istekleri sıraya koyarak yerine getirmeye çalışır. Bu sırada işletim sistemi, işleri tamamlamak için ilgili donanım bileşenleri ile irtibata geçerek donanım bileşenlerinin isteklerinin tamamlanması ister. Yani işletim sistemi, kullanıcı ile donanım arasında bir köprü bir aracı gibi çalışır. O halde işletim sisteminin, donanım ile ilişkili bir bileşeni (çekirdek) ve kullanıcı ile ilişkili diğer bir bileşeni (kabuk) olduğu söylenebilir.

Çekirdek (Kernel) : Çekirdek, İşletim sistemlerinin bileşenlerinden biri olup, donanım ve yazılım arasındaki iletişimi sağlayan kısımdır. Donanım kaynaklarının yönetimi, kaynakların uygulamaları arasında paylaştırılması gibi işletim sistemi görevleri çekirdek tarafından yürütülür. Siber güvenlik açısından, güvenlik zaafiyeti barındıran bir çekirdek, son derece kritik sorunlara neden olabilir.

Kabuk (Shell) : İşletim sisteminin kullanıcı ile etkileşiminin sağlandığı kısmı kabuk (Shell) olarak adlandırılır. Kullanıcı işletim sistemi ile etkileşimini komutlar aracılığıyla (CLI) yapabildiği gibi, düğmeler, pencereler gibi görsel arayüzden (GUI) de yapabilir. Güvenliği sağlanmayan bir kabuk, kullanıcı ile işletim sistemi etkileşiminin şüpheli olarak değerlendirilmesine neden olur.

Şekil 1.9. Kullanıcıdan donanıma akış şeması

Günümüzde kullanılan bazı işletim sistemi tipleri ve kullanım bilgileri şunlardır:

Toplu İşletim Sistemi: Gerçekleştirilen işlem sürecini hızlandırmak için benzer görevleri gruplandırarak çalıştıran işletim sistemleridir.

Çoklu Görev/Zaman Paylaşımı İşletim Sistemi: Farklı bir kabukta bulunan kullanıcıların tek bir bilgisayarı veya bilgisayar sistemini kullanmasına izin veren işletim sistemleridir. Çoklu kullanıcı olmasından dolayı bilgisayar kaynakları belirli zaman paylaşımı yapılarak dağıtılmaktadır.

Gerçek Zamanlı İşletim Sistemi: Önemli görevler için geliştirilmiş işletim sistemleridir. Verilen girdiye çok hızlı tepki vermesi amacıyla özellikle askeri ve uzay sistemleri tarafından kullanılan sistemlerdir.

Dağıtılmış İşletim Sistemleri: Daha hızlı işlem gücü sağlamak için farklı bilgisayarların işlemcilerini kullanan işletim sistemleridir. Veri madenciliğinde yaygın olarak kullanılır.

Ağ İşletim Sistemi: Ağ sistemlerinin en etkili şekilde kullanılması için geliştirilmiş işletim sistemleridir. İleride ele alınacak olan yönlendirici, anahtar ve erişim noktası gibi ağ donanımlarının görevlerini yapmalarını sağlar.

Mobil İşletim Sistemleri: Taşınabilir ve giyilebilir cihazlar için geliştirilmiş işletim sistemlerdir. Sistem kaynaklarını en az kullanarak daha az enerji tüketmesi üzerine odaklanmışlardır. Andorid, IOS, WebOS bunlara örnek verilebilir.

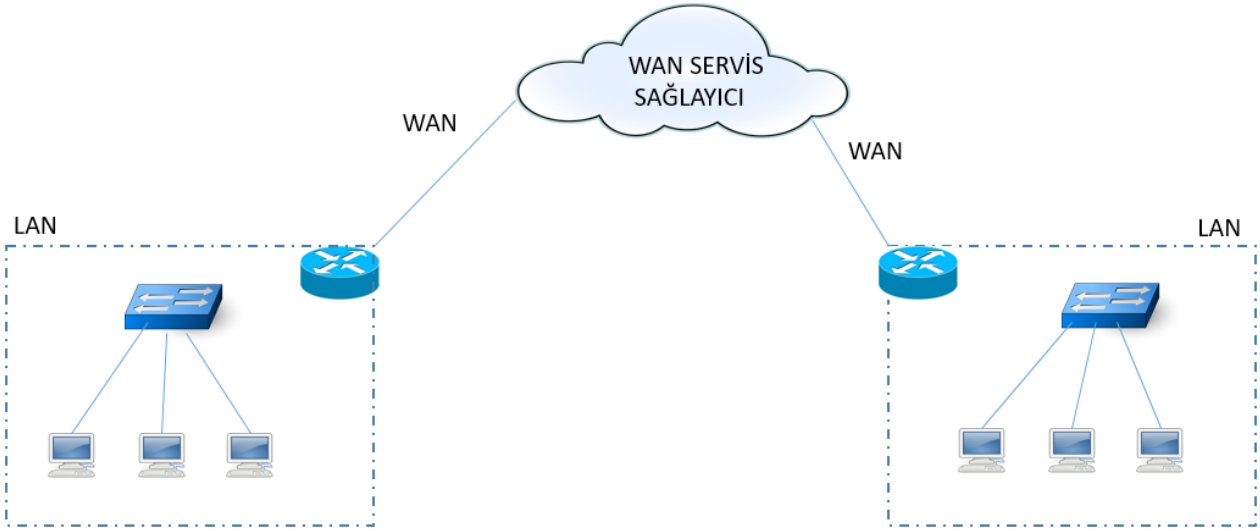
1.4 TEMEL İLETİŞİM VE AĞ BİLEŞENLERİ

Siber uzayın ve dolayısıyla siber güvenliğin en çok kullanıldığı alan bilgisayar ağlarıdır. Bilgisayar ağları (Network), birden fazla cihazın veri paylaşımı ya da çeşitli nedenlerle etkileşimde bulunmaları için oluşturulan fiziksel yapılardan, mantıksal kurallardan ve işleyişlerden oluşan bir yapıdır. Çok genel bir amaç olarak bilgisayar ağları, insanların bilgiye kolay ulaşımını sağlamaktadır. Başlangıçta, özellikle soğuk savaş döneminde, olası bir saldırı durumunda en hızlı şekilde hassas verilerin bir noktadan uzak bir noktaya transfer edilmesi için tasarlanmış, askeri bir proje olarak geliştirilmiştir. Ancak sonraki aşamalarda akademik olarak da kullanıma açılmış ve nihai olarak günümüzde herkesin kullandığı ağların ağı yani İnterneti oluşturmuştur.

1.4.1 Ağ Türleri

Bilişim sistemlerindeki iletişimi anlayabilmek için bilgisayar ağlarını, ağ mimarilerini ve türlerini de bilmek gerekir. Ağ türleri ile ilgili sınıflandırma yaparken çok çeşitli ölçütlere bakılabilir.

Boyutlarına göre ağlar, kullanım senaryolarına göre ağlar, kullanılan teknolojiye göre ağlar gibi farklı sınıflandırmalar mümkündür. Boyutlarına ve kullanım senaryolarına göre bakıldığında ağları Yerel Alan Ağları (LAN) ve Geniş Alan Ağları (WAN) olarak ayırmak mümkündür.



Şekil 1.10. LAN ve WAN kavramları

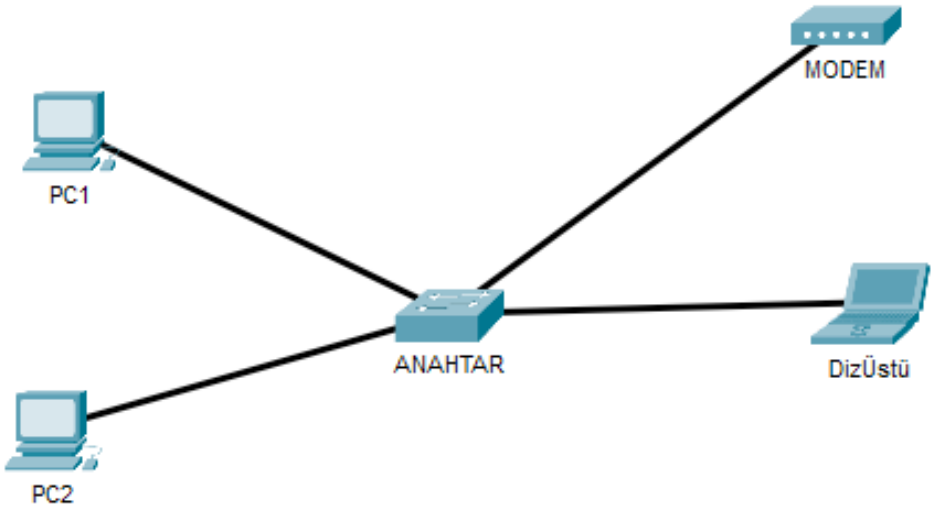
Yerel Alan Ağları, genellikle coğrafi olarak küçük bir bölgeye yayılmış olan, yönetiminin ve kontrolünün bir otoride tarafından sağlandığı yapılardır. Küçük ve orta ölçekli şirketlerde kullanılan, birden fazla cihazın birbirine bağlandığı yapılar ya da evlerde kullanılan ağlar LAN olarak ifade edilir. Günümüzde en yaygın yerel alan ağı teknolojisi Ethernet teknolojisidir. İnternet dünyasına bakıldığında milyonlarca birbirine bağlı yerel alan ağından bahsedilebilir. Bu ağlarının birbirine bağlanabilmesini sağlayan yapılar da Geniş Alan Ağları (WAN) olarak ifade edilir. Geniş Alan Ağları, bir telekomünikasyon kurumunun desteği ile sağlanan, LAN'lara göre daha düşük hızlarda çalışan ağlardır.

1.4.2 Ağ Bileşenleri ve Donanımları

İster yerel alan ağında yer alan bilgisayar ya da dizüstü gibi bilgi işlem cihazları olsun, ister İnternet sitelerinin barındığı sunucular olsun, yerel alan ağını oluşturan cihazların birbirleri ile

iletişime geçebilmesi yani geniş alan ağı aracılığıyla ağların ağını (İnterneti) oluşturabilmesi için birçok farklı aracı cihaz kullanılmaktadır. Bu başlıkta bu aracı cihazlardan bazıları tanıtılacaktır.

Anahtar (Switch) : Aynı ortamda yer alan cihazların birbirine bağlanabilmesini ve iletişim kurabilmesini sağlayan donanımlardır. Okullardaki bilgisayar laboratuarında yer alan öğrenci bilgisayarları ya da dersliklerde yer alan etkileşimli tahtalar ilk olarak bu anahtar denen cihaz ile bağlantıya geçerler. Bilgisayarlar, anahtarların portlarına takılır ve bu sayede birbirleri ile iletişime geçebilmeleri sağlanır.



Şekil 1.11. Ethernet anahtarına bağlı cihazlar

Ethernet anahtarlar, MAC adres olarak bilinen her bir cihazın belirleyici tekil tanımlayıcısı olan adreslere göre cihazları tanır ve kendilerinin hangi bağlantı noktasına (portuna) bağlı olduğunu belirlerler. Anahtarlar ağda kullanılan cihaz sayısına göre 4 portlu, 8 portlu, 24 portlu ya da daha fazla portlu olabilir. Aşağıdaki şekilde 24 kullanıcı portu bulunan bir anahtar gösterilmektedir.

Şekil 1.12. Ethernet anahtar

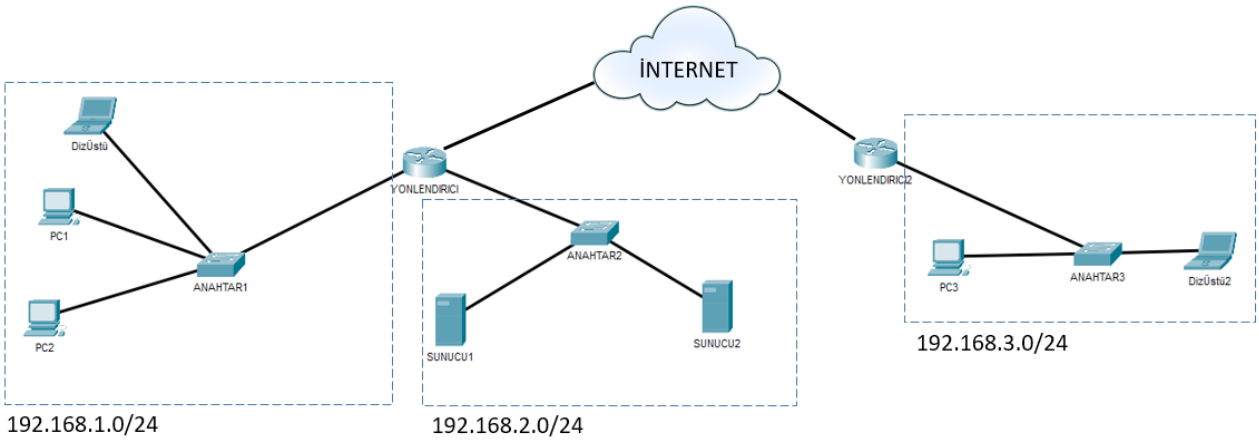
Siber güvenlik açısından ele alındığında anahtarlar son derece önemli cihazlardır. Çünkü kullanıcıların ağla ilk temasları kablolu ortamda anahtarlar aracılığıyla olur. Anahtarın çalışma prensibinin anlaşılması, anahtar üzerinden yapılan (genellikle ağın zayıf noktalarından biridir) saldırıların anlaşılmasını ve dolayısıyla önlem alınmasını kolaylaştıracaktır. Anahtarlar, MAC tablosu olarak adlandırılan, port-MAC eşleşmesini tutan ve cihazların haberleşmesi esnasında dinamik olarak oluşan bir tablo ile çalışır. Bu sayede hangi portta hangi cihazın bulunduğu anahtar tarafından bilinir. Bu tablonun boyutunun bir sınırı olması, MAC adreslerin hangi portta olduğunu öğrenme mekanizması ve tabloda bir adresin bulunmaması durumundaki işleyiş, anahtarları siber güvenliğin konusu yapmaktadır. Kitabın ileriki kısımlarında bu çalışma prensibi detaylı olarak örnek bir iletişim üzerinden anlatılacaktır.

Cihazlar anahtar üzerinden haberleşirken bazen tüm cihazlar ile haberleşmeleri ya da sadece bir cihaz ile haberleşmeleri gerekebilir. Bilgisayar ağlarında bu iletişim, hedefin türüne göre farklı isimlerle anılır. Bir cihazdan sadece bir cihaza yapılan iletişime tekli yayın **(unicast)**; o ağdaki her cihaza yapılan iletişime yayın **(broadcast)** ve belirli bir gruba yapılan iletişime de çoklu yayın **(multicast)** denir. Bilgisayar ağlarında bu yayın türleri sıklıkla kullanılmaktadır.

Yönlendirici (Router) : Yerel ağda yer alan cihazlar genellikle birbirleri ile anahtar üzerinden haberleşirler. Ancak farklı ağlarda yer alan cihazların haberleşmesi yönlendirici olarak adlandırılan ağ donanımları üzerinden gerçekleşir. Örneğin bir ev kullanıcısı, kendi evi dışındaki cihazlar ile haberleşmek istediğinde, örneğin İnternetteki bir sayfaya erişmek istediğinde evindeki ADSL cihazından geçerek internete ulaşır. O halde bu cihaz temel olarak bir yönlendiricidir ve kullanıcının ağın dışına çıkış kapısını, yani **ağ geçidini** (gateway) temsil eder.

Şekil 1.13. Örnek bir yönlendirici

Yönlendiriciler farklı ağları birleştirirler. İlerideki kısımlarda anlatılacağı üzere, her bir LAN ağının bir tanımlayıcı adresi vardır. Yönlendiriciler **ağ adresi** olarak adlandırılan bu adreslerin yer aldığı bir tablo sayesinde trafikleri doğru hedefe yönlendirirler. Şekil 1.14'te yer alan örnekte ağ adresleri 192.168.1.0/24, 192.168.2.0/24 ve 192.168.3.0/24 olarak gösterilmiştir.



Şekil 1.14. Yönlendiriciler farklı ağları bağlar

Yönlendirme tablosu olarak adlandırılan bu tablo, hangi ağa gitmek için hangi porttan çıkılacağını belirten bir yol tabelası olarak düşünülebilir. Yönlendiriciler, bu tabloya göre kendilerine gelen trafikleri hedef adreslere ilgili portu kullanarak yönlendirirler.

Erişim Noktası (Access Point) : Kablosuz teknolojilerin gelişmesi ile yerel ağlarda kullanılan dizüstü bilgisayar, akıllı telefon ya da tablet gibi kablolu yapı kullanmayan donanımların ağa bağlanma ihtiyacı doğmuştur.

Erişim noktaları, bu kablosuz istemcilerin ağa bağlanmasını sağlayan donanımlardır. Kablosuz erişim noktalarının sunduğu ve genellikle WiFi teknolojisi ile bağlanılan ağ esasında bir yerel alan ağıdır. Bu nedenle kablosuz yerel alan ağı anlamında gelen WLAN (Wireless LAN) olarak ifade edilir. Çoğu erişim noktasının (AP) aynı zamanda birden çok kablolu bağlantı noktaları da vardır.

Şekil 1.15. Erişim noktası birçok mobil cihazı kablosuz ağa bağlar.

Bu temel cihazların haricinde ağda çeşitli amaçlarla kullanılan birçok farklı cihaz türleri vardır. Bazıları iletişimi sağlayan aracı cihazlar iken, bazıları da iletişimin ya da ağın güvenliğini sağlayan donanımlardır. Örneğin bu aracı cihazlardan biri de Modem'dir. Bir ağda cihazların iletişimi kablolu ağlardaki sinyallerle sağlanır. Bazı durumlarda bu sinyallerin uzak mesafeye telefon hatlarından gönderilebilmesi modülasyon teknikleri ile mümkündür. Yani gönderilen sinyallerin MODülasyonu; alıcı tarafta da telefon hattından gelen sinyalin de DEModülasyonu gerekir. Gönderirken modülasyon alırken de demodülasyon yapan bu aracı cihazlara MODEM adı verilir. Yine ağda kullanılan diğer bir cihaz türü de, özellikle siber güvenlikte önemli olan Saldırı Tespit Sistemi (IDS) ve Saldırı Önleme Sistemleridir (IPS). Bu sistemler ileriki bölümlerde ele alınacaktır.

1.4.3 Bilgisayar Ağlarında İletişim ve OSI Referans Modeli

Görüldüğü üzere, ağda (ya da ağlar arası ağ olan internette) iletişimin sağlıklı kurulabilmesi için birçok cihaz uyumlu bir şekilde çalışması gerekmektedir. Ancak bilgisayarlarda yer alan yazılımlar dâhil, bu cihazların ve sistemlerin haberleşebilmesi için modellere, iletişim standartlarına ve haberleşmesinin nasıl olacağını tanımlayan protokollere ihtiyaç vardır. Bu bölümde, birçok kavram ve protokolden genel olarak bahsedilecektir. Protokollerin detayları kitabın sonraki bölümlerinde özellikle siber güvenlik açısından ayrıntılı olarak ele alınacaktır.

Bir ağda iletişimin gerçekleşebilmesi için konak cihazların mantıksal ve fiziksel olmak üzere iki adrese ihtiyacı vardır. Mantıksal adres, cihazın bulunduğu yere ve konumuna göre değişen adrestir. Bu amaçla kullanılan adres genellikle IP adreslerdir. Fiziksel adres ise, cihazın değişmeyen, üretici tarafından atanan adresidir. Ethernet ağlarında bu adres için Media Access Control (MAC) adresi kullanılır. MAC adres 48-bitlik bir sayıdır ve NIC üreticisi tarafından atanan tekil bir adrestir. Aşağıda örnek bir MAC adresi gösterilmiştir.

A0-88-B4 -68-DC-3C	
A0-88-B4	**68-DC-3C**
Üretici Kısmı	**Üreticinin atadığı değer**

Bu 48 bitlik sayı onaltılık sayı sistemi şeklinde gösterilir. İlk 24-bit IANA tarafından tahsis edilen üreticinin kodu iken sonraki 24 bit üreticinin atadığı seri numarası olarak düşünülebilir.

Bilgisayarın fiziksel adresi (MAC) ve mantıksal adresini (IP) görmek için Windows işletim sistemlerinde komut satırından **ipconfig /all** komutu kullanılır.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : erdHome
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Physical Address. . . . . . . . . : 48-45-20-F3-ED-41
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4a45:20ff:fef3:ed41%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.103(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 8 Ocak 2021 Cuma 11:57:27
   Lease Expires . . . . . . . . . . : 9 Ocak 2021 Cumartesi 15:50:21
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 122176800
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-14-C2-F5-1C-39-47-A3-ED-EF
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Şekil 1.16. Windows işletim sisteminde ipconfig komut çıktısı.

Günlük hayatımızda bilgisayarlar ve bilgisayar ile yapılan işlemler arttıkça, bilgilerin bir bilgisayardan diğerine taşınması ve haberleşmesi ihtiyacı da artmaktadır. Belli bir işte ortak bir dosya üzerinde çalışma, doküman paylaşımı gibi birçok özellik artık kaçınılmaz hale gelmişti. İlk önceleri bu tür çok kullanıcının üzerinde çalışması gerektiği ortak dosyalar, disketler aracılığıyla aktarılıyordu. Daha sonraları bilgisayarların kendi aralarında haberleşmesi için çalışmalar başlatıldı. Birçok üretici kendi ağ donanımını geliştirmeye başladı. Ancak farklı üreticilerin donanımları kendi aralarında haberleşmesi ciddi sıkıntılar doğuruyordu. Bu sıkıntıyı aşmak ve bir standardizasyon sağlamak adına ISO, Open System Interconnection (OSI) adında bir model geliştirdi.

Bu modele göre, ağların çalışması yedi adımda incelenmektedir. Her adımın işlevi ve bu adımda yapılması gerekenler kesin olarak tanımlanmış ve standardizasyon sağlanmıştır. Ağın çalışma prensiplerinin belirlendiği bu adımlara **"Katman** (Layer)" denir. Geliştirilen bu standardizasyon sayesinde farklı üreticilerin ürünleri birbirleri ile haberleşebilmektedir.

Uygulama Katmanı (Application Layer), kullanıcı ile etkileşimin olduğu, uygulamaların bulunduğu katmandır. Örneğin bir web sayfasına bağlanmak için Internet Explorer, Firefox, Chrome gibi bir web tarayıcı uygulaması çalıştırmak gerekir.

Sunum Katmanı (Presentation Layer), uygulama katmanından gelen verilerin şekillendirildiği (sıkıştırma, şifreleme vb.), yani karşıdaki uygulamanın ya da hizmetin anlayabileceği bir biçimde sunulmasının gerçekleştiği katmandır.

Oturum Katmanı (Session Layer), cihazlar arasında sanal oturumların kurulduğu, yönetildiği ve sonlandırıldığı katmandır.

Bu üç katmana, üst katmanlar denir.

Taşıma Katmanı (Transport Layer), üst katmanlardan gelen verilerin alt katmanları ile iletişimini sağlayan katmandır. Diğer bakış açısıyla, alt katmanlardan gelen verinin, üst katmanlarda hangi uygulama ya da servis ile iletişime geçeceğinin belirlendiği katmandır. Bu belirleme temelde bir sayı olan port numaraları ile sağlanır.

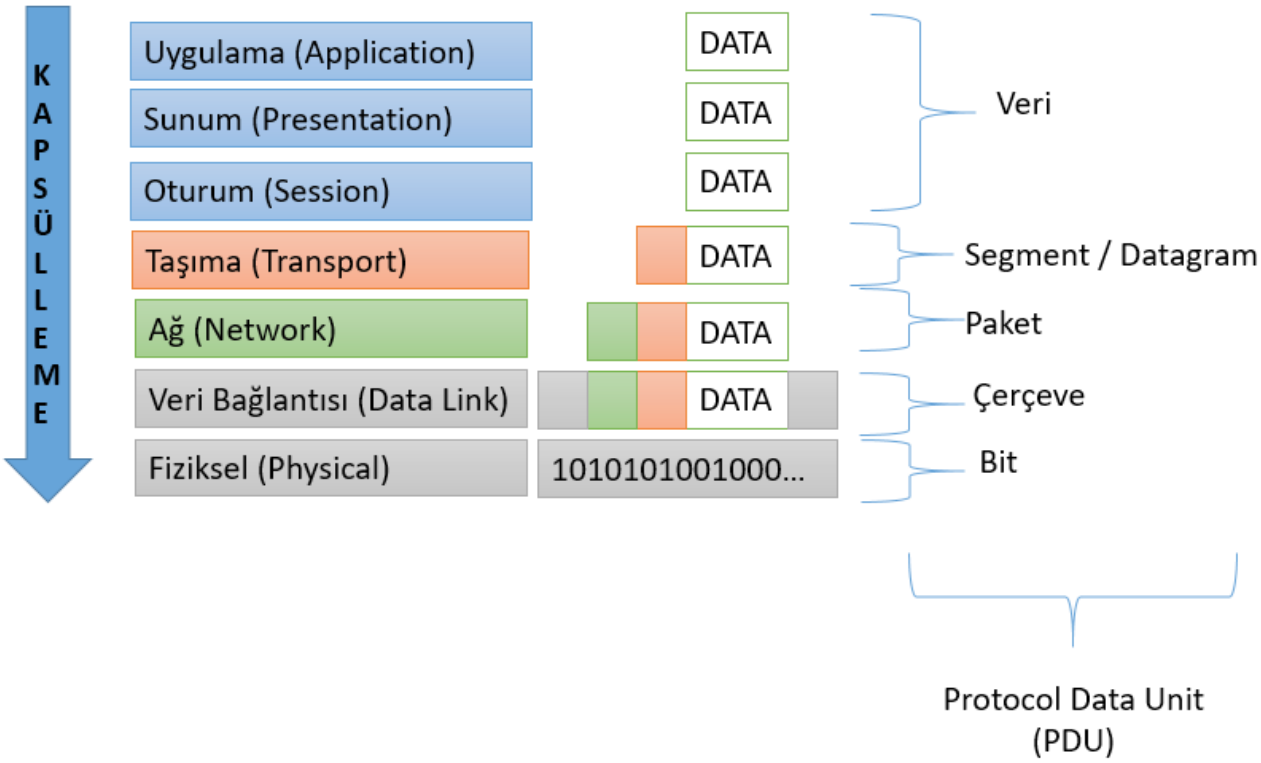
Ağ Katmanı (Network Layer), mantıksal adreslemenin yapıldığı katmandır. Burada veriyi gönderen ve alacak olan cihazların mantıksal adresleri bulunur. Mantıksal adres olarak burada Internet Protocol (IP) adresleri eklenecektir. IP adresi dışında IPX, AppleTalk gibi mantıksal adresler bulunmakla beraber büyük bir çoğunlukla IP kullanıldığı için bu kitap boyunca IP adresleri örnek olarak gösterilecektir.

Veri Bağı Katmanı (Data – Link Layer), Veri bağlantısı olarak da adlandırılan bu katman fiziksel adreslemelerin yapıldığı yerdir. Yerel ağdaki, gönderici ve alıcı cihazların fiziksel adreslerinin belirlendiği aşamadır. Burada Fiziksel Adres olarak MAC adresleri kullanılır.

Fiziksel Katman (Physical Layer), verilerin taşınacak ortama (kablo, hava gibi) aktarılmak üzere sinyallere dönüştürüldüğü katmandır.

İsimlendirmede kolaylık olsun diye tüm katmanlara aşağıdan yukarıya olmak üzere numaralar verilmiştir. Buna göre örneğin Fiziksel Katman: **1. Katman (K1),** Uygulama Katmanı: 7. Katman **(K7)** olarak adlandırılmıştır.

Bir ağ uygulamasını kullanan bir kullanıcı, başka bir bilgisayar veya cihaz ile iletişim kurmak istesin. Bu durumda kullanıcının göndereceği bilgiler **(data)** her katmanda, bulunduğu katmana özgü değişikliğe uğrar yani veriye katmanla ilgili bazı başlık bilgileri **(header)** eklenir ve bir alt katmana aktarılır. En son fiziksel ortama aktarılıncaya kadar bu işlem devam eder. Buna kapsülleme (encapsulation) denir. Her katmanda, şekillenen bu veriye **Protokol Veri Birimi – PVB (Protocol Data Unit - PDU)** adı verilir. Buna göre katmanlar ve bu katmanlara ait PVB'lerin isimleri Şekil 1.17'de verilmiştir.



Şekil 1.17. OSI modeli ve kapsülleme

Alıcı tarafta ise bu işlemin tersi gerçekleşir. Yani fiziksel ortamdan alınan sinyaller, başlık bilgileri her katmanda çıkarılıp bir üst katmana aktarılır. Bu işleme de **kapsül açma (de-encapsulation)** denir.

OSI Modeline göre, uygulamalardan gelen veri, 7., 6. ve 5. katmanlarda büyük bir değişikliğe uğramadan taşıma katmanına gelir. Bu katmanda uygulamanın türüne göre TCP ya da UDP başlık bilgisi eklenir ve **Segment /Datagram** oluşur.

Eklenen bu başlık bilgisinde özetle göndericinin ve alıcının bağlantı noktası numaraları bulunur. Bu sayede hedef ile kaynak arasında hangi uygulamaların veya servislerin haberleşeceği belirlenmiş olur. Segment olarak kapsüllenmiş veri bir alt katmana aktarılır.

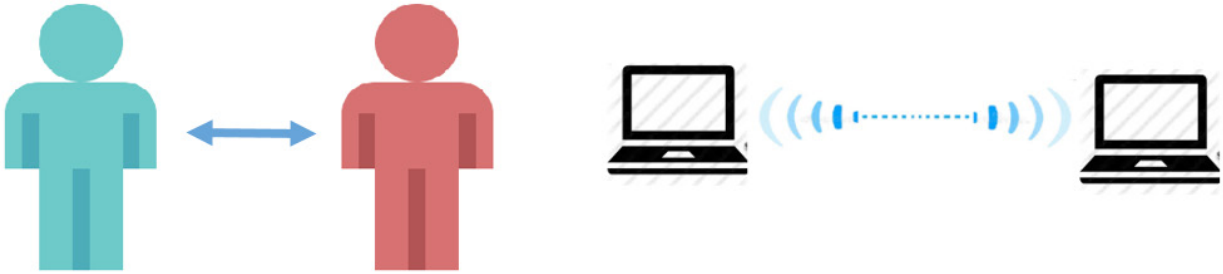
Ağ katmanında, gönderen IP adresi ve alıcı IP adresi gibi bir takım bilgiler eklenir.

IP başlık bilgisi eklenip paket oluşur. Ethernet teknolojisinde bir paketin boyutu 46 Byte ile 1500 Byte arasında olmalıdır.

İkinci katmanda (Data Link Layer) 3. Katmandan gelen paket yapısına bu kez Kaynak MAC adresi, Hedef MAC adresi, Tür/Uzunluk başlık bilgisi eklenir. Ayrıca sonuna da, bit bazında hata kontrolü için FCS alanı eklenir. Toplamda 18 byte eklendiği için bir Ethernet çerçevesi 64 Byte ile 1518 Byte arasında olmalıdır.

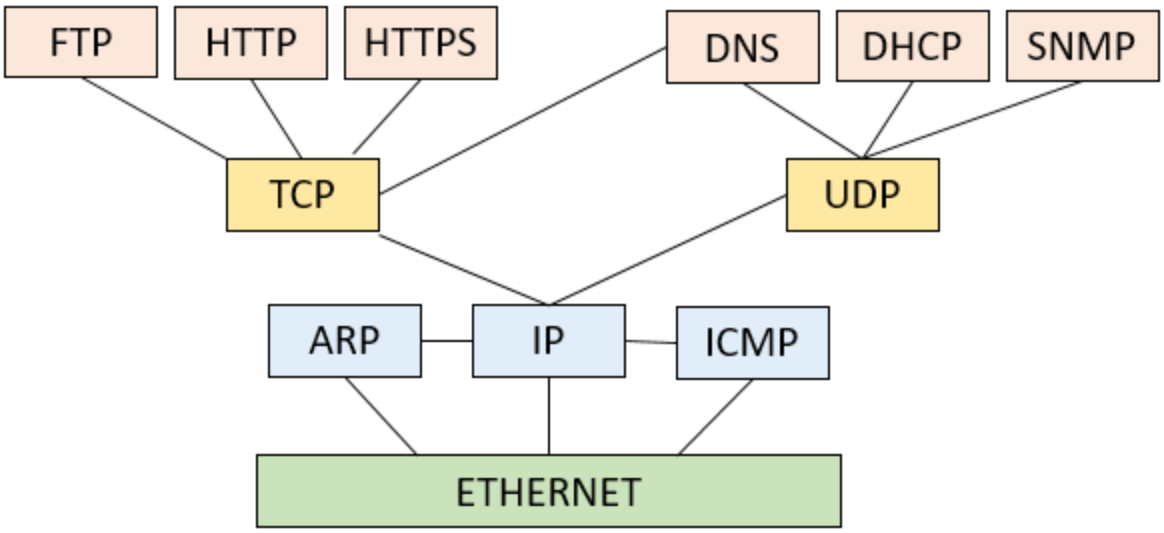
1.4.4 Ağ Protokolleri

İnsanlar arasındaki iletişim esnasında; dil, konuşma hızı, cümle yapısı, konuşma sırasını bekleme, karşıdakinin sözünü kesmeme, anlaşılmadığı durumda tekrar etme, anlaşıldığına dair karşıdan bir onay bekleme gibi kuralları bilgisayar ağları dünyasına uyarlamak mümkündür. Bir iletişimin gönderici ile alıcı açısından anlaşılır hale getirilmesinden sorumlu olan kurallara protokol denir. Ayrıca, protokoller farklı üreticilerin farklı ürünlerinin aynı platformda iletişimini yani standardizasyonu sağlar.



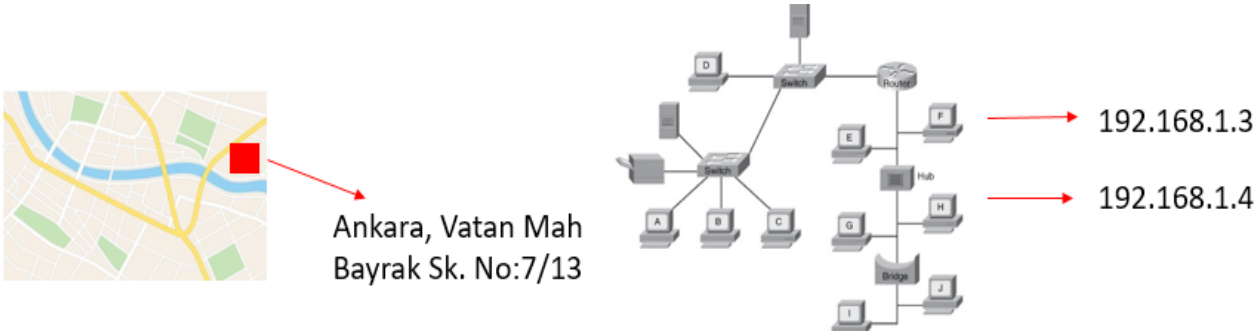
Şekil 1.18. İnsan- İnsan iletişimi ve Makine-makine iletişimi

Bilgisayar ağları söz konusu olduğunda birçok üretici firmanın ve ürününün olması kaçınılmazdır. Standartlar oluşmadan önce, her üretici sadece kendi cihazları arasındaki iletişimi destekliyor, farklı üreticilerin ürünleri ile iletişim kurmakta zorlanıyor ya da kuramıyordu. ISO tarafından geliştirilen referans model sayısında bu zorluk aşılabilmektedir. Diğer bir referans modeli de Amerikan Savunma Bakanlığı tarafından geliştirilen TCP/IP referans modelidir. Bu kısımda, iletişimin nasıl gerçekleşeceğini, aslında bir anlamda standardizasyonunu sağlayan protokollerden TCP/IP protokolleri ve ilişkili bazı temel kavramlar ele alınacaktır.



Şekil 1.19. Bazı TCP/IP protokolleri ve Ethernet

Internet Protokolü Adresi (IP Adresi): İnternet ortamında ya da bilgisayar ağlarında, her ağ cihazını eşsiz olarak tanımlayan bir adres bilgisine ihtiyaç vardır. Bu adres bilgisi, ağ cihazlarının göndermiş oldukları verilerin kaynağını ve hedefini belirlemek üzere kullanılan mantıksal bir adrestir. Günümüz ağlarında, bu amaç doğrultusunda ağ cihazlarının adreslemesinde IP adresi kullanılır.



Şekil 1.20. İnternet Protokollerinin bir amacı da adreslemedir

Şekil 1.20'de gösterilen adres bir ev için hangi anlama geliryorsa, IP adresi de bir ağ cihazı için aynı anlamdadır. Ancak, ev adreslerinden farklı olarak bilgisayar dünyasında adreslemeler için ikilik sayı sistemleri kullanılır. Günümüzde sürüm 4 (IPv4) ve sürüm 6 (IPv6) olmak üzere iki

farklı IP protokolü adresleme amacıyla kullanılmaktadır. 32-bitlik bir sayıdan oluşan IPv4 adresi örneği aşağıda gösterilmiştir. IPv6 adresi ise 128-bitten oluşur.

Örnek bir IPv4 adresi : 11000000101010000000000100000011

Günlük hayatta onluk sayı sistemi kullanıldığı için, bilgisayarlar açısından bir-sıfırlar dizisi olarak görünen yukarıdaki adres, kolay kullanım için onluk sayı sistemine dönüştürülür. Öncelikle yukarıdaki adres, 8 bitlik gruplar (oktetler) olarak ayrılır, her bir grup onluk sayı sistemine dönüştürülür ve gruplar arasına nokta (.) konarak gösterilir. Bu işlem adımları aşağıdaki tabloda ifade edilmiştir.

İkilik gösterim	11000000101010000000000100000011			
Oktetlere ayırma	11000000	10101000	00000001	00000011
Onluk sisteme dönüştürme	192	168	1	3
Onluk noktalı gösterim	192.168.1.3			

Tablo 1.1. IP adresinin ikilik ve onluk gösterimi

IP adresinden bahsederken ele alınması gereken diğer bir kavram ağ maskesidir. **Ağ maskesi** (subnet mask), aynı ağda bulunan cihazların soldan itibaren kaç bitlerinin aynı olması gerektiğini gösteren bir değerdir. Bu değer belirli kurallar dâhilinde değiştirilebilen bir sayıdır. Örneğin, Tablo 1.1'deki örnekteki 192.168.1.3 IP adresli bir cihaz ile 192.168.1.129 IP adresli bir cihazın ilk 24 bitleri aynıdır. Bu nedenle eğer maske 24 bit uzunluğunda olursa (teknik olarak /24 olarak gösterilir) bu iki cihaz aynı ağda olacaktır. Ancak maske /25 olursa bu iki cihaz aynı ağda olmayacaktır. Çünkü bit olarak yazıldığında 25. bitlerin her iki adreste farklı olduğu görülecektir.

Ağ cihazları, ağının sınırlarını belirlemek üzere bu maskeyi kullandıklarından, her zaman IP adresi ile beraber kullanılırlar. Yukarıdaki örnek için bu ifade 192.168.1.3/24 olarak gösterilebilir. Bu ifade, 192.168.1.3 cihazı açısından şu anlama gelir:

"Bir cihazın benimle aynı ağda olması için ilk 24 bitinin benimle birebir aynı olması gerekir, geri kalan 8 bit ne olursa olsun…"

Yukarıdaki ifade bit olarak 24 tane "1" ve 8 tane "0" olarak göstermek mümkündür:

11111111111111111111111100000000

Tıpkı IP adreslerinde olduğu gibi, yapılandırma esnasında ağ maskeleri de ikilik sayı sistemlerinden onluk sayı sistemlerine dönüştürülürse, "255.255.255.0" onluk gösterimli maske ifadesi elde edilir.

Internet Protokolünün diğer bir görevi de, kaynak cihaz ile hedef cihaz arasında veriyi paketler halinde taşımaktır. Bu nedenle IP, taşınan verinin ne olduğunu, hangi adresten gelip hangi adrese gideceğini, paketin parçalara ayrılıp ayrılmadığı gibi özellikleri belirtecek bir yapıda tasarlanmıştır. Bu bilgiler, IP paketinin başlık bilgilerini oluşturur. Aşağıda bir IP paketinin başlık bilgisi yer almaktadır.

1								2								3								4							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
VERSION				IHL				DSCP						ECN		TOTAL LENGTH															
IDENTIFICATION																FLAGS	FRAGMENT OFFSET														
TIME TO LIVE								PROTOCOL								HEADER CHECKSUM															
SOURCE IP ADDRESS																															
DESTONATION IP ADDRESS																															
OPTIONS (IF IHL > 5)																															

Şekil 1.21. IP Paket başlığının yapısı

Internet Protokolünün tasarlanması aşamasında güvenlik dikkate alınmamıştır. Bu nedenle, bu başlık bilgisinde yer alan bazı kısımlar, siber saldırganlar tarafından saldırı amacıyla manipüle edilebilmekte (Ör. **Sahte Kaynak IP Adresi**), alıcı cihazın kandırılmasına neden olabilmektedir. Bir siber güvenlik uzmanının bu yapıyı bilmesi, olası tehditlere karşı hazırlıklı olmasını sağlayacaktır. Aşağıda başlıca TCP/IP protokolleri özetle ele alınmıştır, protokollere ilişkin güvenlik zafiyetleri kitabın sonraki bölümlerde daha detaylı olarak sunulmaktadır.

İletim Denetim Protokolü (Transmission Control Protocol- TCP): OSI modelinin dördüncü katmanında çalışan, uygulamalar / hizmetler arası bağlantıyı kuran güvenilir bir protokoldür. Verinin kaynaktaki hangi uygulamadan çıkıp, hedefteki hangi uygulamaya gittiği, TCP başlık bilgisinde yer alan ve her biri 16-bit olan kaynak ve hedef bağlantı noktası numaraları tarafından belirlenir. TCP'nin güvenilir olması, veri transferinde alıcı cihazın veriyi aldığını doğrulaması (Onay-Ack) ve olası paket kayıplarında paketi tekrar göndermesi ile ilişkilidir. Yani verinin karşı uygulama tarafından alınıp alınmadığı bilinir, bu da TCP'yi güvenilir yapar. TCP aynı zamanda, verilerin parçalar halinde gönderildiği durumlarda, parçalara sıra numarası (Sequence Number) ekleyerek alıcı tarafta doğru bir şekilde sıralanmasını sağlar.

0 15 16 31

Kaynak Bağlantı Numarası (Source port)			**Hedef Bağlantı Numarası** (Destination port)
Sıra Numarası (Sequence Number)			
Onay Numarası (Ack Number)			
Başlık Uzunluğu (Header length)	**Rezerve**	**Bayraklar** (Flags)	**Pencere Boyutu** (Windows size)
Doğrulama (Checksum)			**Acil İşaretçi** (Urgent Pointer)
Seçenekler (Options)			
Veri (Data)			

Tablo 1.2. İletim Denetim Protokolü başlık bilgisi

Uygulamalar tarafından üretilen verinin, hedefteki doğru uygulamaya güvenilir bir şekilde iletilmesini sağlamak amacıyla OSI modelinin 4.katmanında veriye başlık bilgileri eklenir. TCP başlık bilgileri Tablo 1.2'de gösterilmiştir.

TCP veri iletişimini başlatmadan önce bayraklar alanında yer alan bitleri, sıra ve onay numaralarını kullanarak ***3-yönlü el sıkışma*** işlemini yapar. Böylece gönderici ile alıcı arasında bir anlaşma niteliğinde olan oturum kurulmuş olur.

Kullanıcı Datagram Protokolü (User Datagram Protocol - UDP): Uygulamalar ya da hizmetler arasında veri iletimini sağlayan diğer bir 4.katman protokolü de UDP'dir. UDP, yine bağlantı noktası numaralarını kullanarak uygulama verilerini iletir ancak TCP'ye göre oldukça basit bir yapıdadır. Verilerin ulaşıp ulaşmadığını kontrol etmez, gönderilmeyen paketleri tekrar iletmez, sıralı değildir. Bu nedenle güvensizdir, başlık yapısı basittir.

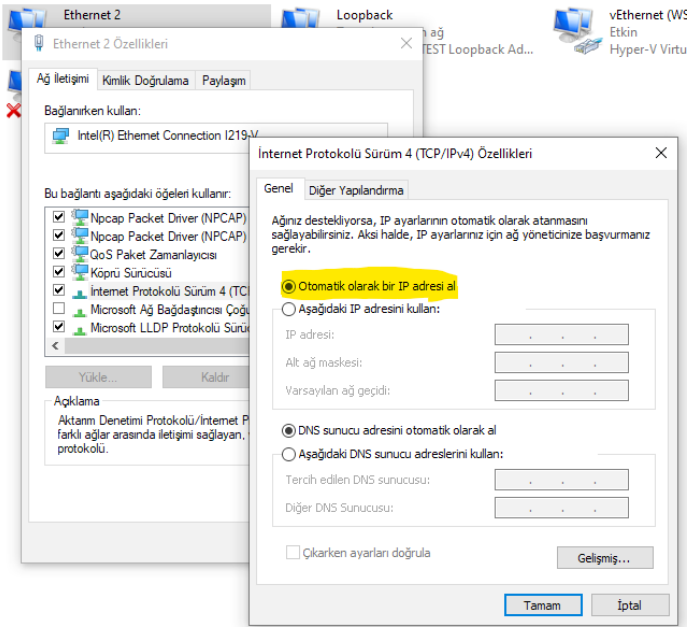
0 15 16 31

Kaynak Bağlantı Noktası	Hedef Bağlantı Noktası
UDP Uzunluğu	UDP Doğrulama
Veri	

Tablo 1.3. Kullanıcı Datagram Protokolü başlık bilgisi

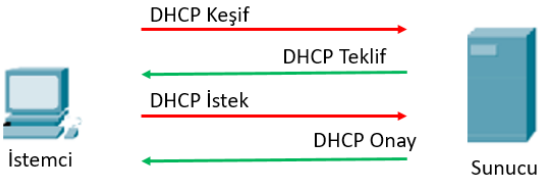
Hız gerektiren ve paket kayıplarının tolere edilebildiği ses akışı, video akışı gibi uygulamalarda kullanılır.

Dinamik Konak Yapılandırma Protokolü (DHCP): Önceki bölümde değinildiği gibi, cihazların ağ iletişimi kurabilmeleri için benzersiz IP adreslerinin olması gerekir. Bu adresler cihazlara statik olarak atanabildiği gibi, otomatik olarak alınması da sağlanabilir. DHCP, bu amaç doğrultusunda geliştirilen, 7.katman bir uygulama protokolüdür. Cihazların ihtiyaç duyduğu, IP, Ağ Maskesi, Ağ Geçidi ve DNS adresi gibi bilgileri cihazlara kiralar. Windows işletim sistemlerinde ihtiyaç duyulan bu bilgiler, Şekil 1.22'deki IP yapılandırma ekranında gösterilmiştir.



Şekil 1.22. Windows bilgisayarda IP yapılandırma ekranı

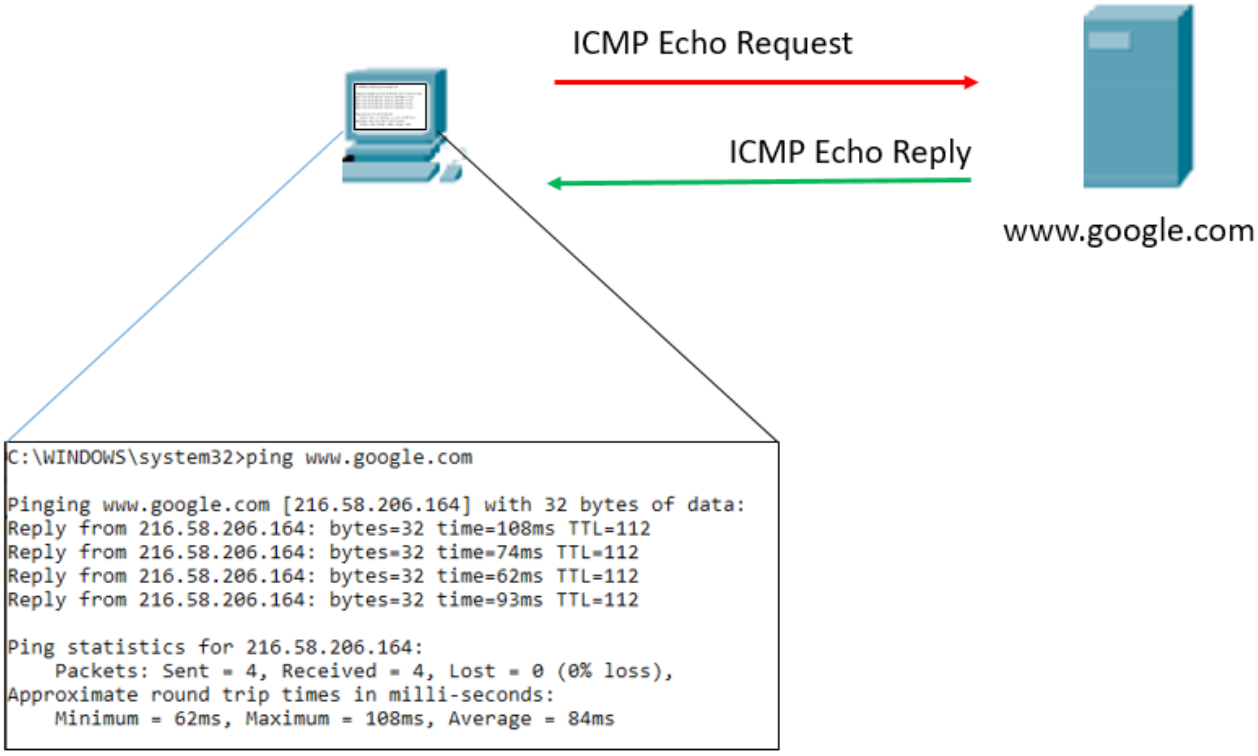
"Otomatik olarak bir IP adresi al" seçeneği belirlendiğinde DHCP devreye girecek ve ihtiyaç duyulan bilgileri bulmak üzere DHCP işlemini başlatacaktır. İstemci cihazlara verilecek olan IP yapılandırma bilgileri ***DHCP sunucusu*** olarak adlandırılan bir cihazda önceden tanımlı olmalıdır. İstemci ile sunucu arasında toplamda dört aşamadan oluşan DHCP'nin işlem akışları ve isimleri Şekil 1.23'te gösterilmiştir.



Şekil 1.23. DHCP protokolünün aşamaları

Küçük ağlarda (örneğin ev ağlarında) modem-yönlendiriciler, IP dağıtmak üzere hazır olarak tasarlanmış DHCP sunucuları olarak çalışmaktadır. Bu nedenle ev ağlarında modeme bağlanan cihaz ek bir yapılandırmaya gerek kalmadan IP adresi alabilmektedir. DHCP sunucusu tarafından sağlanan bilgiler, bir istemcinin doğru iletişim kurmasını sağladığından, siber saldırganlar için bu protokol bir hedeftir. DHCP'ye yönelik olarak yapılan saldırılar kitabın sonraki bölümlerinde ele alınacaktır.

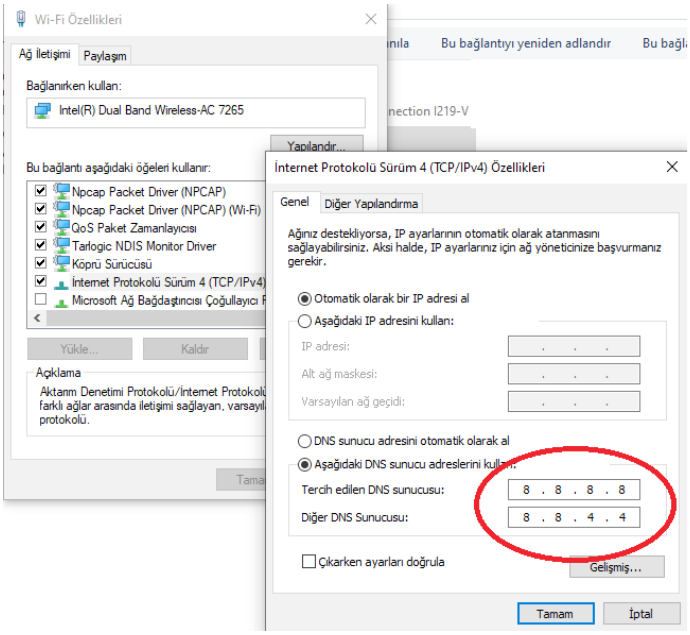
Internet Kontrol Mesaj Protokolü (Internet Control Message Protocol - ICMP): Bir ağ ortamında gerek sorun giderme için gerek iletişimin varlığının doğrulanması için kontrol edilmesi ihtiyacı vardır. ICMP, bu amaç doğrultusunda geliştirilmiş, belirli bir IP'nin erişilebilir olup olmadığını doğrulamak için kullanılan bir protokoldür. Erişimin olup olmadığının yanı sıra, erişim ile ilgili, erişiminin olmamasının olası nedeni, erişilen cihaza ve uzaklığına dair çeşitli bilgiler de sunan yararlı bir protokoldür. Örnek iletişim bölümünde bahsedilecek olan **ping** ve **traceroute** (Windows'ta **tracert**) gibi komutlar bu protokolü kullanır.



Şekil 1.24. İletişimin varlığını doğrulamak için kullanılan ping komutu ICMP'yi kullanır

İletişimin varlığını doğrulamak isteyen kaynak, ICMP yankı isteği **(Echo Request)** gönderir. Bu isteği alan hedef cihaz, (cevap vermemek üzere yapılandırılmadığı sürece) ICMP yankı cevabı **(Echo Reply)** ile cevap verir. Cevaptaki TTL değeri cihazın işletim sistemi hakkında ipucu ve uzaklığı **(hop count)** hakkında yaklaşık bir bilgi verir.

Hiper Metin Transfer Protokolü (Hyper Text Transfer Protocol - HTTP): İnternet ortamında en yayın kullanılan uygulama protokolüdür. World Wide Web'de (WWW) metin, grafik görüntü, ses, video ve diğer multimedya dosyalarını değiş tokuş etmek için bir dizi kuralın tanımlandığı protokoldür. İnternet uygulamalarında en çok kullanılan uygulama protokolü olduğundan, kitabın 4.7 bölümünde detaylı olarak ele alınmıştır.



Şekil 1.25. DNS yapılandırma ekranı

Alan Adı Sistemi (Domain Name System - DNS): İnternet ve ağ ortamında cihazları adresleyen benzersiz tanımlayıcı IP adresidir. Ağ aracılığıyla iletişime geçilmek istenen cihazın IP adresi yazılarak iletişim kurulur. Ancak özellikle internet ortamında IP adresi yerine daha akılda kalıcı olduğu için isim kullanmak (daha teknik bir ifade ile alan adı) daha kullanışlıdır. Ancak IP paketlerinde hedef adres kısmına alan adları değil, IP adresleri yazılabilir. Bu nedenle, alan adı ile IP adreslerinin dönüştürülmesi gerekir. DNS, bu amaç doğrultusunda geliştirilmiş UDP kullanan bir uygulama protokolüdür. Erişilmek istenen alan adının IP adresine dönüştürülmesinin ardından, IP-alan eşleşmesi kaynak cihazın belleğinde tutulur.

İnternet ortamında bir ağ adresine ismi ile erişilmek istendiğinde, işletim sistemi öncelikle bu ön belleği araştırır. Önceden bir çözümleme yapıldıysa, bellekte yer alacaktır ve doğrudan bu adres kullanılacaktır. Aksi durumda, konak cihazın IP yapılandırma penceresinde belirtilen DNS sunucusuna isim çözümlemesi için hiyerarşik bir sorgu süreci başlatılacaktır.

Adres Çözümleme Protokolü (Address Resolution Protocol - ARP): Adres Çözümleme Protokolü, bir IPv4 adresi ile donanım adresi (MAC adresi) arasında dinamik adres eşlemesi sağlar. Ethernet veri iletişiminde, İnternet gibi farklı bir ağ ile iletişime geçiliyorsa ağ geçidinin MAC adresi; aynı ağda yer alan bir cihaz ile iletişime geçiliyorsa doğrudan hedef cihazın MAC adresinin bilinmesi gerekir. Bu işlem, kaynak cihaz tarafından başlatılan bir ARP İsteği **(ARP Request)** ile

başlar. Bu istek bir yayın mesajdır ve bu nedenle ağdaki tüm cihazlara gidecektir. MAC adresi öğrenilmek istenen cihaz (aslında IP) ister doğrudan aynı ağdaki cihaz olsun, ister ağ geçidi olsun bu ağdaki tüm cihazlarda olduğu gibi bu mesajı alır. Olması gereken ARP işleyişine göre, sorgulanmak istenen IP adresine sahip cihaz dışındakilerin bu mesajı dikkate almaması ve cevap vermemesidir. Doğru cihaz, kendi MAC adresini içeren tekli yayın (unicast) bir cevap verir **(ARP Reply)**. Böylece trafiği ilk başlatan cihaz, istediği MAC adresi öğrenecek ve bunu çoğu zaman bu IP - MAC eşleşmesini belirli bir süreliğine belleğinde (arp cache) tutacaktır.

```
C:\>arp -a

Interface: 192.168.56.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.1.103 --- 0xe
  Internet Address      Physical Address      Type
  192.168.1.1           5c-63-bf-06-d0-13     dynamic
  192.168.1.100         48-44-f7-51-46-df     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

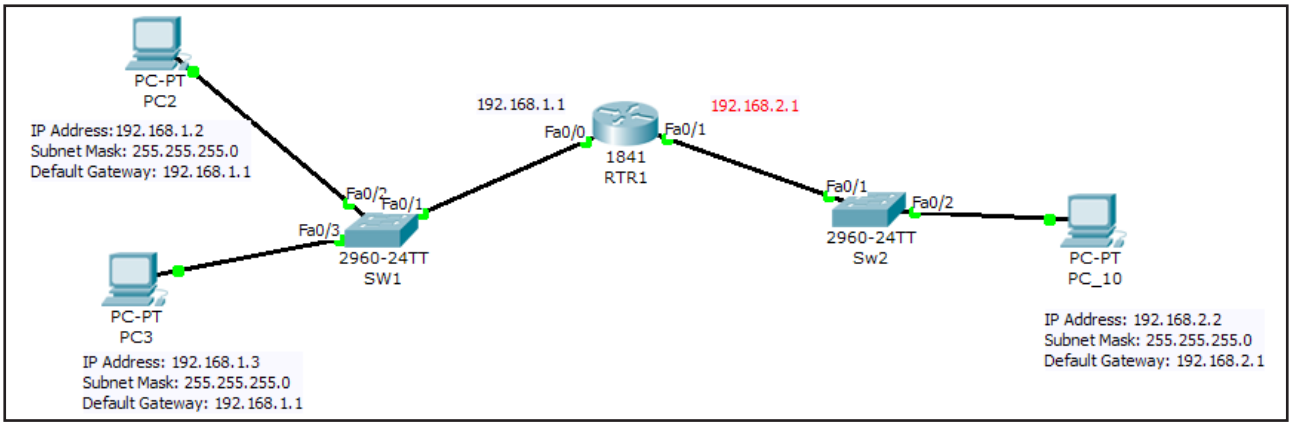
Şekil 1.26. Windows işletim sisteminde Arp önbelleği

Windows işletim sisteminde arp önbelleğini görüntülemek için, Şekil.1.26'daki ekran görüntüsünde olduğu gibi ***arp –a*** komutu kullanılabilir.

1.4.5 Uçtan Uca Ağ İletişim Örneği

Siber güvenlikte yapılan saldırıların analiz edilebilmesi ve anlaşılabilmesi için, iki cihaz arasındaki uçtan uca iletişimde cihazların rolleri, işlevleri ve protokollerin çalışma mantığının

anlaşılması gerekmektedir. Bu başlıkta, iki cihaz arasındaki uçtan uca iletişim, önceki bölümlerde ele alınan protokoller ve cihazlar dâhilinde Şekil 1.27'deki topoloji temel alınarak ayrıntılı olarak incelenecektir.



Şekil 1.27. Uçtan uca iletişim için örnek topoloji

Bu topolojide, ortada RTR1 olarak adlandırılan bir Yönlendirici (Router), sağında ve solunda birer anahtara (srasıyla SW1 ve SW2) bağlıdır. SW1 anahtarında PC2 ve PC3, SW2 anahtarında ise PC_10 bilgisayarları bulunmaktadır. SW1'e bağlı cihazlar 192.168.1.x IP adreslerine sahip olduklarından yönlendiricinin tablosunda bu ağın tanımlayıcı adresi 192.168.1.0/24 olarak yer alır. Aynı şekilde SW2'nin bulunduğu ağın adresi de 192.168.2.0/24 olarak belirtilmiştir. Yine hangi cihazın hangi fiziksel bağlantı noktası aracılığıyla diğer bir cihaza bağlı olduğu topolojiden görülebilmektedir.

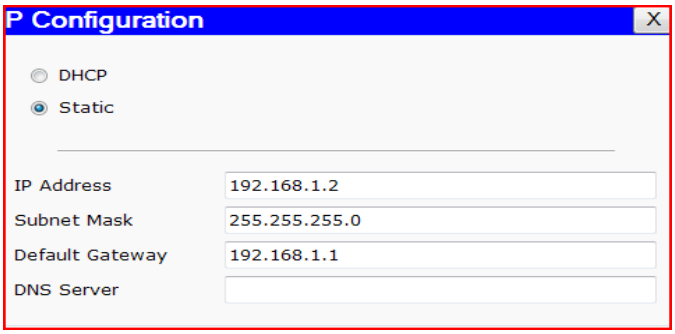
Tüm cihazların yeni açıldığını varsayalım. Yönlendirici, kendisine bağlı olan ağlar hakkında bilgi sahibidir. Bu durumda Yönlendirici için yönlendirme tablosu aşağıdaki gibi olacaktır.

Routing Table for RTR1

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0

Şekil 1.28. RTR1 için yönlendirme tablosu

Yönlendirici kendisine gelen bir paketin hedef IP adresini bu tabloyla karşılaştırır ve bir eşleşme bulunursa, fiziksel bağlantı noktası (port) olarak belirlenen arayüzden bu paketi iletecektir. Örneğin, hedef IP adresi 192.168.1.5 olan bir paket bu cihaza geldiğinde, 192.168.1.0/24 ile belirtilen FastEthernet0/0 isimli bağlantı noktasından iletilecektir.

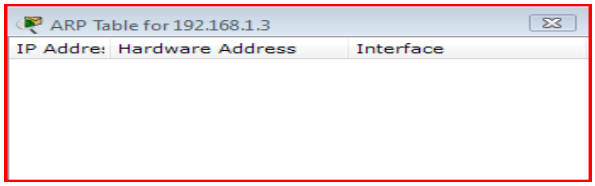


Şekil 1.29. IP yapılandırma penceresi

Varsayılan haldeki anahtarların da MAC tablosu boştur. Çünkü bu tablo, cihazdan trafik geçtikçe dinamik olarak doldurulan ve belirli bir süreliğine tutulan bir tablodur.

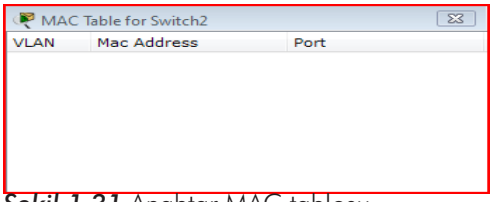
Bilgisayarlar kendi IP, Ağ Geçidi ve Ağ Maskesi bilgilerini bilir. Bu bilgiler ya bir DHCP sunucusundan alınmış ya da statik olarak yapılandırılmıştır.

İlk açıldıklarında PC lerin ARP tablosu (ARP Cache) boştur. Çünkü cihazlar yeni açılmış ve herhangi bir IP-MAC eşleşmesi bellekte yoktur.



Şekil 1.30. Konuk cihazın ARP önbelleği

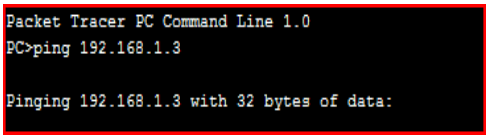
Not: *Aşağıda yer alan iletişim örneklerinde anahtarlar tarafından yapılabilen çerçeve kontrolü (Frame Check) işlemi atlanmıştır.*



Şekil 1.31. Anahtar MAC tablosu

A. AYNI AĞDA İLETİŞİM

Şekil 1.27 de PC2, aynı ağda bulunan PC3 ile iletişime geçmeye, örneğin PING **(ICMP Echo Request)** atmaya çalışsın. "Ping atma" kavramı, iletişimi test etmek amacıyla hedef IP adresine ICMP yankı iletisi göndermek anlamına gelir.



Şekil 1.32. Ping atma işlemi

PC2, hedef IP (192.168.1.3) ile kendi ağ maskesi bilgisini (255.255.255.0) AND (mantıksal VE) işlemine tâbi tutacaktır. Bu sayede hedefin kendisi ile aynı ağda olup olmadığını anlayacaktır.

192.168.1.3 AND 255.255.255.0 = **192.168.1.0 (Hedef Ağ Adresi)**

Kendi IP adresi ile Ağ Maskesini AND işlemine alacaktır.

192.168.1.2 ^255.255.255.0 = **192.168.1.0 (Kendi Ağ Adresi)**

Her iki değer eşit olduğuna göre, PC2 hedefin (PC3'ün) kendisi ile aynı ağda olduğunu anlayacaktır.

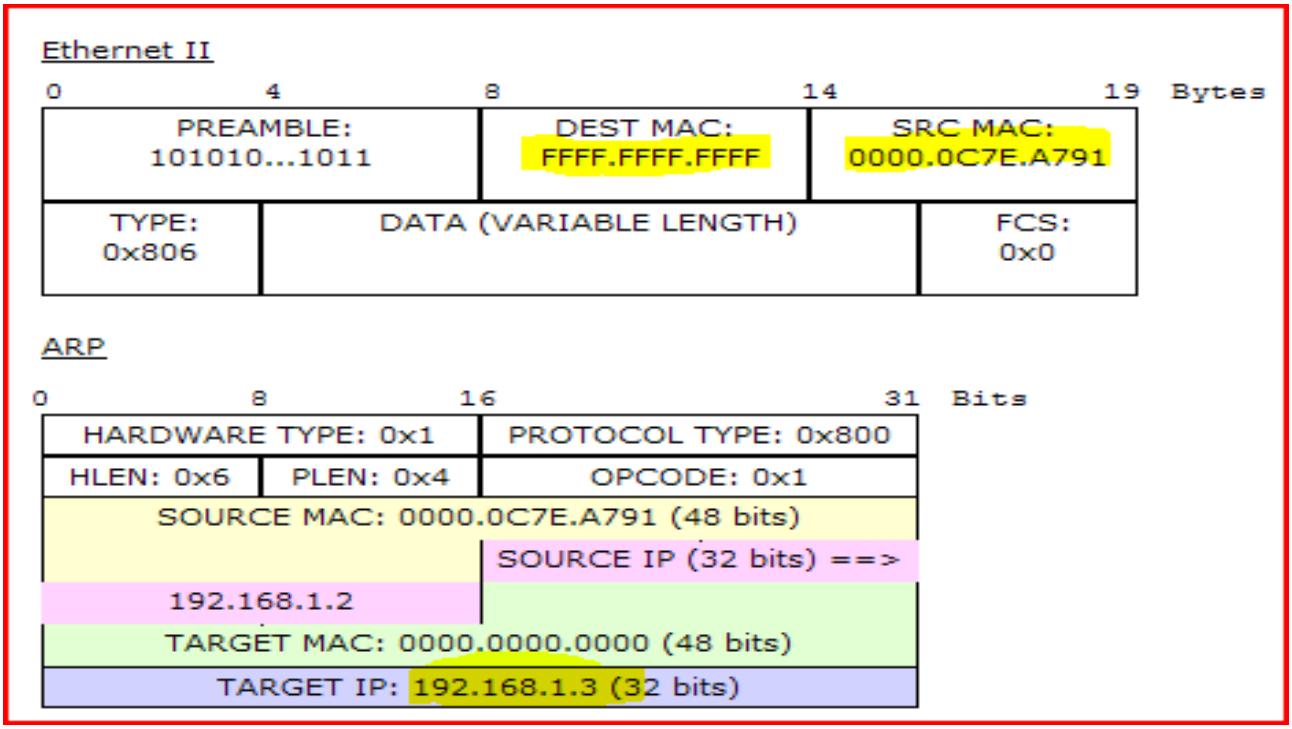
Her iki cihaz aynı ağda olduğuna göre oluşturulacak çerçevenin anahtar aracılığıyla hedefe ulaşılabilir olduğu (hedef MAC adresini kullanarak) anlaşılır. Bu durumda PC2, bir çerçeve oluşturamaya çalışacaktır. Daha önceki bölümlerde bahsedildiği gibi, Ethernet iletişimi için hem IP hem MAC bilgisi gereklidir. Ancak hedef IP bilinmesine rağmen hedef MAC bilinmemektedir.

Hedef IP : 192.168.1.3

Hedef MAC: ????

PC2, Hedef MAC **(Destination MAC)** için 192.168.1.3'e karşılık gelen MAC adresini öğrenmek için kendi ARP tablosuna bakacaktır.

ARP tablosu boş olduğundan, **192.168.1.3** e karşılık gelen MAC adresi öğrenmek için ARP isteği **(ARP Request)** yayınlayacaktır. Bu ARP isteği bir yayın (broadcast) mesajdır. Bu mesajın hedef MAC adresi FFFF.FFFF.FFFF, kaynak MAC adresi ise, PC2'nin MAC adresidir. (Örnekte 0000.0C7E.A791)



Şekil 1.33. Arp çerçevesi

MAC Table for SW1

VLAN	Mac Address	Port
1	0000.0C7E.A791	FastEthernet0/2

Şekil 1.34. SW1 için MAC tablosu

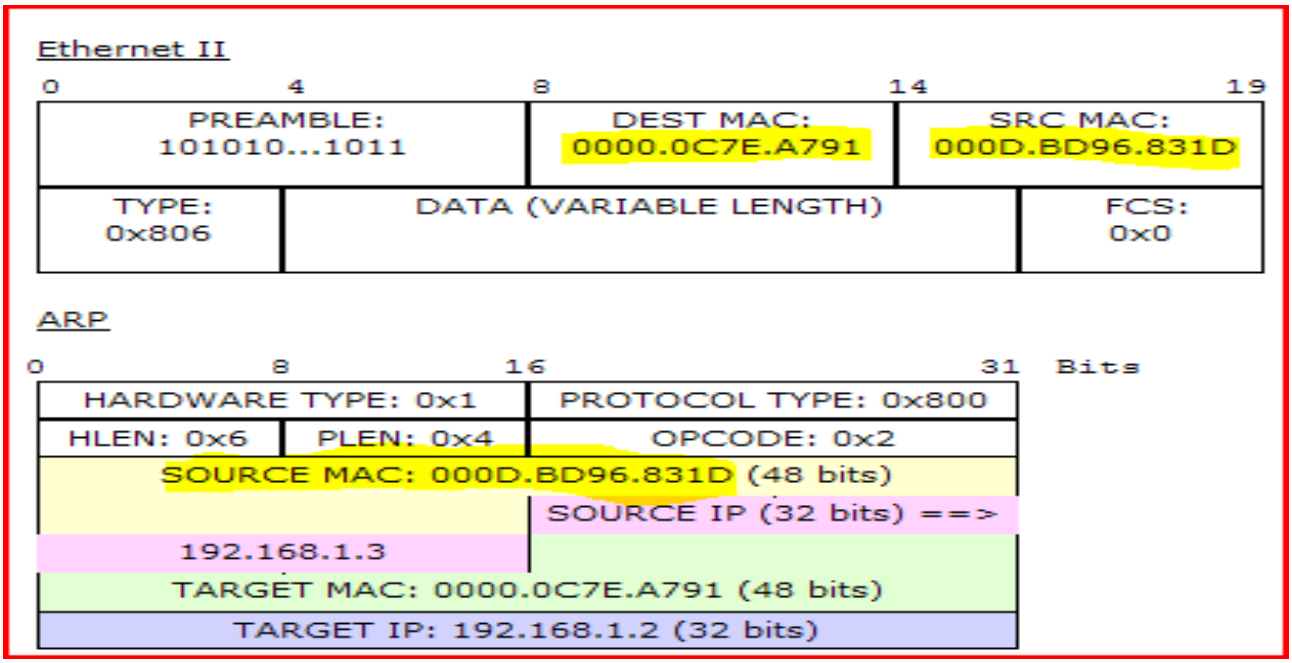
Arp mesajı yayınlanıp anahtara ulaşacaktır. Anahtar, ilk işlem olarak gelen çerçevedeki kaynak MAC adresine **0000.0C7E.A791** bakıp bunu gelen bağlantı noktası **(FastEthernet 0/2)** ile eşleştirecektir. Bu sayede MAC tablosunda Şekil 1.34'deki gibi bir kayıt oluşacaktır.

ARP Table for PC3

IP Address	Hardware Address	Interface
192.168.1.2	0000.0C7E.A791	FastEthernet

Şekil 1.35. PC3 için ARP tablosu

Ardından anahtar gelen ARP çerçevesinin hedef MAC adresine bakıp **FFFF.FFFF.FFFF** (yayın) bunu gelen haricindeki tüm aktif bağlantı noktalarına gönderecektir. Dolayısıyla çerçeve hem PC3'e hem yönlendiriciye gidecektir. Yönlendirici gelen ARP mesajını dikkate almaycak ve çöpe atacaktır. PC3 ise bu ARP mesajındaki hedef IP nin kendi IP si olduğu için cevap verecektir. Bu arada PC3 PC2 ile iletişime geçtiği için MAC- IP eşleşmesini bilecektir. Yani ARP tablosu aşağıdaki gibi olacaktır.



Şekil 1.36. ARP cevabı

PC3, PC2'nin hem MAC hem IP adresini bildiği için Şekil 1.36'daki gibi bir tekil yayın ARP cevabı yayınlayacaktır.

ARP cevabı mesajında PC2'nin ihtiyaç duyduğu PC3 MAC adresi bulunmaktadır.

MAC Table for SW1

VLAN	Mac Address	Port
1	0000.0C7E.A791	FastEthernet0/2
1	000D.BD96.831D	FastEthernet0/3

Şekil 1.37. SWI için MAC tablosu

Bu tekil yayın ARP cevabı anahtara ulaşacaktır. Anahtar ilk işlem olarak, gelen çerçevedeki kaynak MAC (Source MAC) alanına bakacak ve geldiği bağlantı noktası ile eşleştirip MAC tablosuna aktaracaktır. Bu durumda anahtarın MAC tablosu aşağıdaki gibi olacaktır.

Anahtar, bağlantı noktası – MAC adresi eşleştirmesi yaptıktan sonra Hedef MAC adresine bakacaktır. Hedef MAC (örnekte 0000.0C7E.A791) adresinin hangi bağlantı noktasında olduğu (FastEthernet 0/2) bilindiği için anahtar gelen çerçeveyi sadece bu bağlantı noktasına yönlendirecektir. Dolayısıyla sadece PC2 bu cevabı alacaktır.

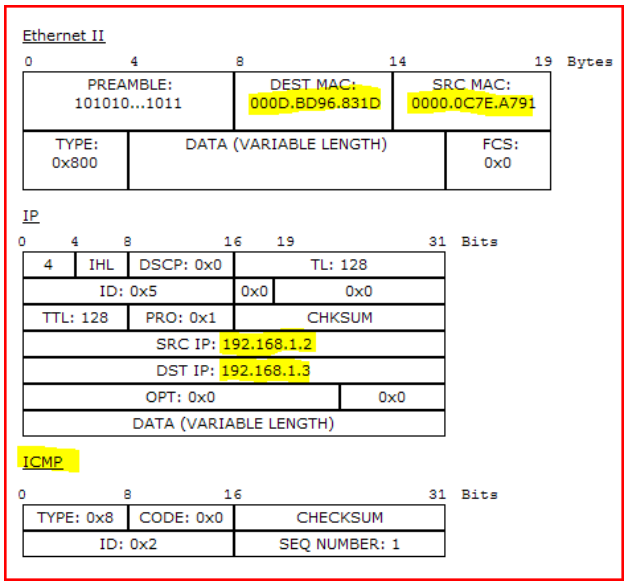
Gelen cevaptan yola çıkarak PC2, 192.168.1.3 IP adresinin MAC adresini (000D.BD96.831D) öğrenecek ve ARP tablosuna yazacaktır. Bu durumda PC2'nin ARP tablosu aşağıdaki gibi olacaktır.

ARP Table for PC2

IP Address	Hardware Address	Interface
192.168.1.3	000D.BD96.831D	FastEthernet

Şekil 1.38. PC2 için ARP tablosu

Artık PC2, PC3'e PING paketi (ICMP Yankı İstemi) göndermek için hem IP hem MAC bilgisine sahip olduğu için ICMP paketi oluşturabilecektir. Oluşan paket Şekil 1.39'daki gibidir.



Şekil 1.39. PING (ICMP) paketinin yapısı

ICMP paketi anahtarlara ulaşacaktır. Anahtar öncelikle gelen çerçevenin kaynak MAC adresine bakıp bunun ilgili bağlantı noktasına işlenip işlenmediği kontrol edilecektir. Ardından hedef MAC adresine bakacak ve bu MAC adresin hangi bağlantı noktasında olduğu bilgisine göre iletecektir. Örnekteki hedef MAC bilgisi ve anahtar MAC tablosundan yola çıkarak anahtarın bunu FastEthernet 0/3 bağlantı noktasına ileteceği görülebilir. Bu sayede ICMP

paketi PC3'e ulaşacaktır. PC3 gelen ICMP isteğinin hedef MAC adresine bakarak kendisine ait olduğunu öğrendikten sonra PING isteğine cevap (ICMP Echo Reply) verecektir.

Gönderilen 4 ICMP Yankı İsteği paketine karşılık verilen ICMP Yankı Cevabına göre PC2'de durum aşağıdaki gibi olacaktır.

Bazen ilk ICMP paketi ARP istekleri sebebiyle cevapsız kalabilir, ancak diğer paketlere cevap gelecektir.

```
PC>
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=8ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

Şekil 1.40. Başarılı bir Ping işlemi

B. FARKLI AĞLARDA İLETİŞİM

Şekil 1.27'de yer alan topolojide PC1, farklı bir ağda bulunan PC_10 ile Ping aracılığıyla iletişim kurmak istesin.

Bu durumda AND işlemi sonunda 192.168.2.2 cihazının PC2 ile aynı ağda olmadığı anlaşılacaktır. PC2, PC_10'un farklı ağda olduğunu anladıktan sonra oluşturacağı çerçevenin hedef IP ve hedef MAC yerine aşağıdaki gibi bir paket oluşturacaktır.

```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
```

Şekil 1.41. Uzak ağa Ping atma

Hedef IP : 192.168.2.2 (PC_10 IP)

Hedef MAC: Yönlendirici FastEthernet 0/0 (Ağ Geçidi) MAC Adresi

PC2, Hedef MAC adresi yerine ağ geçidi MAC adresini yazacaktır. Daha önce PC2 ile ağ geçidi iletişim kurmadığı için PC2 ARP tablosunda ağ geçidi IP adresi için MAC kaydı yoktur. Sadece daha önce iletişim kurduğu PC3'e ait IP ve MAC bilgileri vardır.

IP Address	Hardware Address	Interface
192.168.1.3	000D.BD96.831D	FastEthernet

Şekil 1.42. PC2 için ARP tablosu

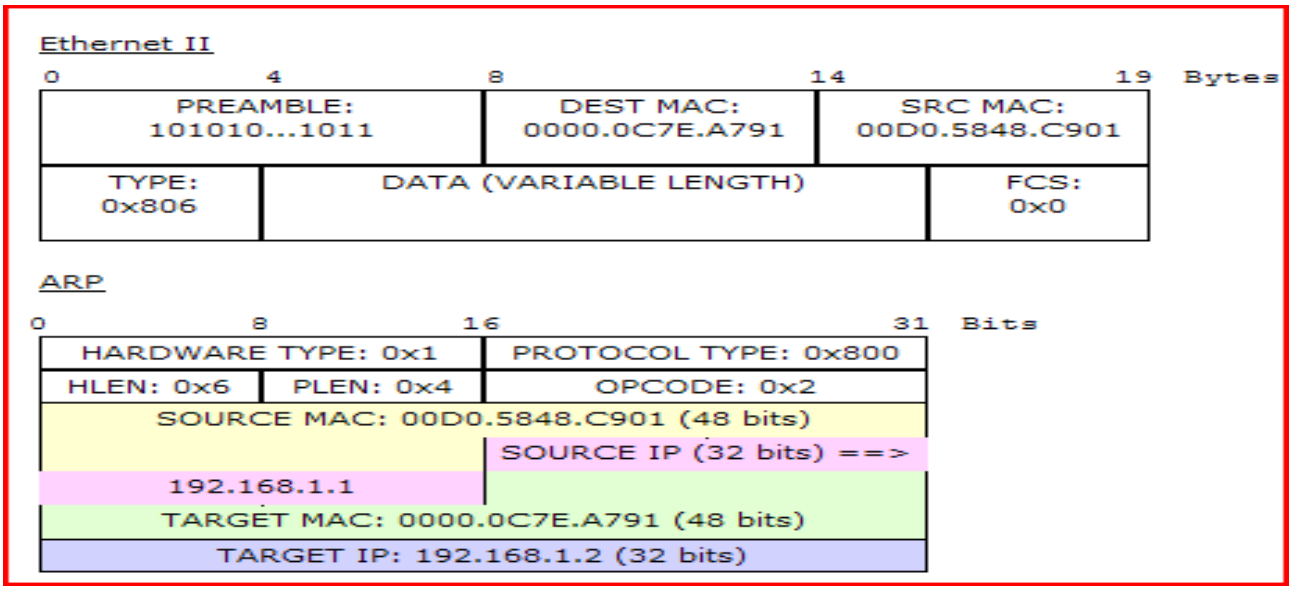
Bu nedenle PC2, ag geçidi adresine (192.168.1.1) karşılık gelen MAC bulmak için ARP isteği yayınlayacaktır. Bu yayın anahtardan geçecektir. Anahtar, gelen bağlantı noktasındaki Kaynak MAC ile bağlantı noktası eşleştirmesi olup olmadığına bakacak, kayıt yoksa MAC tablosuna ekleyecektir. Bu örnekte daha önceki iletişimden dolayı ilgili kayıt vardır. Anahtar hedef MAC adresine bakacaktır. Hedef MAC adres, ARP istekleri için FFFF.FFFF.FFFF dir. Dolayısıyla anahtar bunu gelen haricindeki tüm aktif bağlantı noktalarına gönderecektir. PC3 de bu isteği alacak ancak ARP cevabı vermeyecektir. Ağ geçidi ise bu ARP mesajına cevap verecektir.

Gelen cevap anahtardan geçerken, Kaynak MAC ile gelen bağlantı noktası (FastEthernet 0/0) eşleştirecek ve MAC tablosuna yönlendirici MAC ve ilgili bağlantı noktasını işleyecektir. Bu durumda anahtar PC2, PC3 ve ag geçidi MAC adreslerinin (örnekte ağ geçidi için 00D0.5848.C901) hangi bağlantı noktasında olduğunu bilecektir. Anahtarın MAC tablosu Şekil 1.43'deki gibidir.

VLAN	Mac Address	Port
1	0000.0C7E.A791	FastEthernet0/2
1	000D.BD96.831D	FastEthernet0/3
1	00D0.5848.C901	FastEthernet0/1

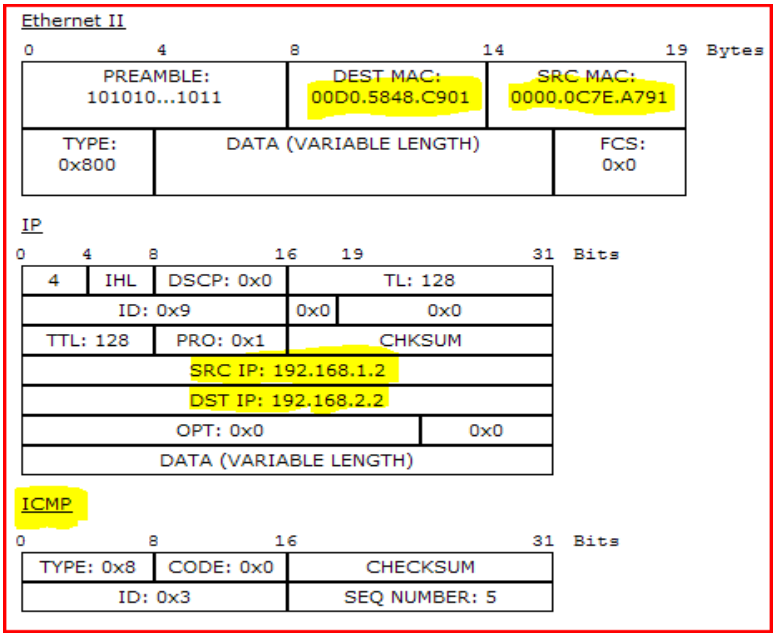
Şekil 1.43. Anahtar MAC tablosu

Gelen tekil yayın ARP cevabında hedef MAC adresi PC2'nin MAC adresidir. ARP cevabı paketi Şekil 1.44'deki gibidir.



Şekil 1.44. ARP cevabı yapısı

Anahtar hedef MAC adrese (0000.0C7E.A791) bakacak ve bunu MAC tablosu aracılığıyla ilgili bağlantı noktasına (FastEthernet 0/2) iletecektir. Gelen ARP cevabında ağ geçidi MAC adresi (00D0.5848.C901) bulunduğundan PC2, ağ geçidinin MAC adresini öğrenecek ve ICMP Yankı İsteği paketini oluşturabilecektir (Şekil 1.45).



Şekil 1.45. ICMP yankı isteği

Burada Hedef IP, PC_10 cihazının IP adresidir. Hedef MAC adresi ise, ağ geçidinin MAC adresidir. Kaynak IP, PC2'nin IP adresi, kaynak MAC ise yine PC2'nin MAC adresidir. Bu paket, anahtara ulaşacaktır. Anahtar kaynak MAC – Bağlantı Noktası eşleştirmesini kontrol ettikten sonra, hedef MAC adrese bakıp bunu ağ geçidine gönderecektir.

Yönlendirici (ağ geçidi), gelen paketteki hedef MAC adresine bakıp çerçevenin kendisine geldiğini anlayacak ve bu kez hedef IP adresine (192.168.2.2) bakacaktır. Bu IP adresini ağ maskesi ile mantıksal VE işlemine alacak ve 192.168.2.0 ağ adresini bulacaktır.

Yönlendirici hesapladığı bu adresi, yönlendirme tablosunda arayacaktır. Yönlendirme tablosunda bununla ilgili bir kayıt ya da varsayılan rota (default route) yoksa paketi silecektir. RTR1 yönlendiricisinin yönlendirme tablosu Şekil 1.46'da gösterilmiştir.

Routing Table for RTR1

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0

Şekil 1.46. RTR1 yönlendirme tablosu

Yönlendirme tablosunda 192.168.2.0 ağı için FastEthernet 0/1 arayüzünden çıkış yapması gerektiğini anlayacak, paketi bu arayüze yönlendirecek ve IP başlık bilgisindeki TTL değerini bir azaltacaktır. Yönlendirme tablosunda yer alan 192.168.2.0 ağı doğrudan bağlı olduğu için tür (type) alanında "C" ile gösterilmiştir.

Hedef IP adresi 192.168.2.2 tekil yayın bir adres olduğu ve FastEthernet 0/1 arayüzünün IP adresi ile (192.168.2.1) aynı ağda olduğu için doğrudan ulaşılabilirdir. Bu nedenle yönlendirici gelen çerçeveyi aşağıdaki bilgiler ile güncelleyecektir.

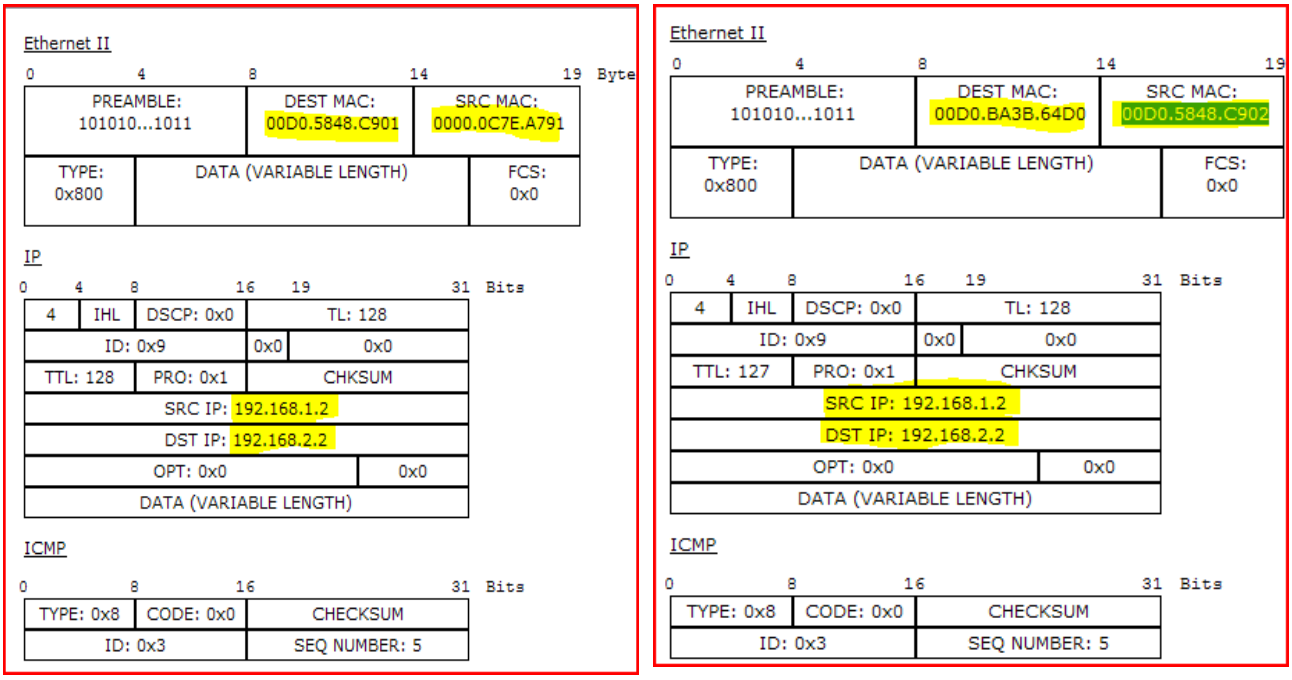
Hedef IP : 192.168.2.2 (Değişmez)

Hedef MAC : PC_10 MAC adresi

Kaynak IP: 192.168.1.2 (PC2 IP adresi)

Kaynak MAC: Yönlendirici FastEthernet 0/1 MAC adresi : 00D0.5848.C902

Bu durumda yönlendiriciye giren ICMP paketi ile çıkan ICMP paketi Şekil 1.47'de gösterildiği gibi olacaktır.



Şekil 1.47. Yönlendiriciye giren ve yönlendiriciden çıkan ICMP paketi

Burada hedef ve kaynak MAC adreslerin değiştiğine ama IP adreslerin değişmediğine; ayrıca TTL değerinin girerken 128, çıkarken 127 olduğuna (1 azaltıldığına) dikkat ediniz.

Yönlendiriciden çıkarken hedef MAC adresi için 192.168.2.2'ye karşılık gelen MAC adresi yazılacaktır. Bunun için yönlendirici ARP tablosuna bakacaktır. Yukarıdaki örnekte ARP tablosunda ilgili kayıt vardır. ARP tablosunda kayıt olmasaydı, yönlendirici ARP isteği yayınlayıp öğrenecekti.

Son olarak yönlendiricinin oluşturduğu bu paket anahtara ulaşacaktır. Anahtar gelen bağlantı noktası- kaynak MAC eşleştirmesi yaptıktan sonra hedef MAC adresine bakacak ve buna göre mesajı ilgili bağlantı noktasına iletecektir. Anahtar MAC tablosunda PC_10 için MAC adresi yoksa anahtar gelen bu tekil yayın çerçeveyi, gelen haricindeki aktif olan tüm bağlantı noktalarına gönderecektir. Bu işlem çoğu zaman yayın ile karıştırılır ancak işlem tekil yayın bir taşırma işlemidir. Siber güvenlikte anahtarlara yönelik olarak yapılan saldırılarda anahtarların bu özelliği yaygın olarak kötü amaçlarla kullanılmaktadır.

BÖLÜM 2

SİBER GÜVENLİK KAVRAMLARI

Bilişim araçların ve özellikle İnternetin günlük hayatın her alanına etkili bir şekilde nüfuz etmesi birçok avantajı ve kolaylığı sağlamıştır. Eğitimden, bankacılığa, oyunlardan sosyal medyaya birçok alanda üretilen veriler dijital ortamda tutulmakta ve dijital ortamlardan hareket etmektedir. Bu durum, tehdit aktörlerinin de iştahını kabartan bir durumdur. Çünkü hedef sektör sürekli olarak genişlemekte ve buna bağlı olarak hedef kitle de geniş bir yelpazeye dağılmaktadır. Tehdit aktörleri çeşitli teknikler, araçlar, yöntemler ve yazılımlar kullanarak kişisel ya da kurumsal olarak bu bilgilere ulaşmak istemektedirler.

Bu bölümde, başlıca siber güvenlik kavramları, saldırılar, saldırganlar, yaygın saldırı araçları, yaygın zararlı yazılımlar ve yöntemler ele alınacaktır.

2.1 TEHDİT AKTÖRLERİ VE GÜVENLİK KAVRAMLARI

Siber güvenlik söz konusu olduğunda, çok farklı amaç ve motivasyonla hareket eden bireyler, gruplar ve organizasyonlar yer almaktadır. Ancak genel itibariyle tehdit aktörlerini sınıflandırmak gerekirse, **amatörler, bilgisayar korsanları *(hacker)*, organize suç grupları (hacktivist), devlet destekli organizasyonlar ve terörist gruplar olarak** sınıflandırmak mümkündür.

Şekil 2.1. Tehdit aktörleri

Saldırganlar ya da daha geniş bir ifade ile tehdit aktörleri, siber saldırılar gerçekleştiren bireyler veya gruplardır. Siber saldırılar, başka bir kişiyi veya kuruluşu olumsuz yönde etkilemesi amaçlanan kasıtlı kötü amaçlı eylemlerdir.

2.1.1 Amatörler

Genellikle teknik bilgi düzeyleri kısıtlı olan, var olan çeşitli araçları kullanan ve script-kiddies olarak da isimlendiren bireylerdir. Amatörleri bir tehdit aktörü olmaya iten motivasyonları genellikle merak, heyecan, yeteneğini başkalarına gösterme isteği gibi daha çok psikolojik unsurlardır. Bilgi düzeyleri kısıtlı olsa bile, kullanabildikleri araçların yetenekleri ve bu grupta yer alan bireylerin sayısal

fazlalığı, bu saldırgan grubu tehlikeli gruplar yapmaktadır. Ayrıca, yıllar geçtikçe saldırı araçları da yetenek kazanmaya başlamış ve daha çok kişi tarafından erişilebilir olmuştur.

Amatörler grubunda ele alınabilecek diğer bir grup da **"Lamer"** olarak adlandırılan gruptur. İnternet dünyasında Lamer kavramı, şifre kıran, telekomünikasyon sistemlerine illegal yöntemlerle giren kişileri tanımlamaktadır. Ancak bu kavram zamanla değişmiş ve gereksizce rahatsızlık veren ve çocukça işler yapan daha amatör gruplar için kullanılmaktadır.

2.1.2 Hacker (Bilgisayar Korsanı)

Sistemlere girebilme yeteneğine sahip programlama ve ağ sistem bilgileri üst düzey olan kişiler "bilgisayar korsanı" olarak ifade edilmektedir. Bilgisayar korsanları kendi saldırı araçlarını geliştirebildiği gibi diğer saldırı araçlarını da yakından tanımaktadır.

Şekil 2.2. Bilgisayar korsanları kendi saldırı araçlarını geliştirebilirler

Bilgisayar korsanları yetkisiz erişim, hesap ihlali, yetkisiz dinleme, banka kartı dolandırıcılığı, internet bankası dolandırıcılığı gibi bilişim suçları işlerken sahte kimlik kullanma ya da kimlik taklit etme yöntemini kullanmaktadır. Bilgisayar korsanları, gizlenerek ya da normal kullanıcı gibi görünmeye çalışarak kullanıcıların kimlik bilgilerine ya da hesaplarına erişmeyi hedeflemektedirler. Bilgisayar korsanları literatürde beyaz şapkalı, siyah şapkalı, gri şapkalı olarak üçe ayrılmaktadır

- **Siyah Şapkalılar**: Sistemlere izinsiz girme, bilgileri çalma, verileri yok etme ya da sistemleri kendi istekleri doğrultusunda kullanma gibi işler için yeteneklerini kullanan kişilerdir.
- **Beyaz Şapkalılar**: (Etik Bilgisayar Korsanları) Siber güvenlik çalışanları olarak hizmet vermekte olup genel anlamda siber güvenlik açıklarını tarayarak, tespit edilen açıkları kapatmaya çalışan ve bilgilerini iyi yönde kullanan kişilerdir. Etik korsanlar ayrıca, her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kıran ancak daha sonra kırdığı sistemin açıklarını sistem yöneticisine ya da kurumlara bildirerek, o açıkların kapanmasına destek veren programcılardır. Bu hizmetlerinin karşılığında para da kazanabilirler.
- **Gri Şapkalılar**: Bazen siyah bazen beyaz şapkalı gibi davranan saldırganlardır.

Hacktivistler: Çeşitli politik ve sosyal fikirleri protesto etmek amacıyla eylemler düzenleyen bilgisayar korsanlarıdır. Hacktivistler, hassas ya da kritik bilgileri sızdırabilirler. Dağıtılmış hizmet reddi (DDoS) saldırılarıyla web hizmetlerini kesintiye uğratarak kuruluşlara karşı protesto eylemleri düzenlerler.

2.1.3 Tehdit Aktörlerine İlişkin Kavramlar

- **Hackleme (Hacking)**: Hackleme kavramı, bilgisayarlar, akıllı telefonlar, tabletler ve hatta tüm ağlar gibi dijital cihazları tehlikeye atmaya çalışan etkinlikleri ifade eder. Basitçe söylemek gerekirse, bazı yasa dışı amaçlarla bilgisayar ağ güvenlik sistemlerine yetkisiz erişim veya denetimdir.
- **Güvenlik Açığı (Vulnerability)**: İnternet protokolleri, uygulama yazılımları ve diğer sistemlerin istismar edilebilmesine olanak tanıyan zaafiyetlere denilmektedir.
- **Tehdit**: Sistemleri istismar edecek her türlü oluşum ve (hack grupları, virüsler, solucanlar, içeriden ve dışarıdan saldırı yapma ihtimali olan tüm kişiler...) tehdittir.

- **Risk:** Sistemlerdeki açıkların tehditler ile buluştuğu noktada risk oluşur.
- **İstismar (Exploit):** Zaafiyetlerin kullanılarak uzak makinaya erişim sağlanması, bilgi sızdırılması ya da farklı amaçlar ile hazırlanmış yazılımlara istismar kodu (exploit) denilmektedir.
- **Sunucu taraflı istismar kodları** (Server Side Exploits): Sunucuların zafiyetlerinden yararlanılmak üzere kullanılan kodlara verilen isimdir.
- **Kullanıcı İstismar Kodları (Client Side Exploits):** Internet tarayıcı gibi sistem üzerine kurulan yazılımların açıklarından faydalanan, yazılımlarının üzerine yerleştirilen zararlı kodların son kullanıcı tarafından yüklenmesi ile istismar edilmesidir.
- **Yetki Yükseltme İstismar Kodları (Local Privilige Escalation Exploits):** Bir bilgisayar sistemine normal kullanıcı yetkisiyle erişim yapıldıktan sonra yetkisini artırma işlemine olanak sağlayan yazılımlardır.
- **Metasploit:** İstismar kodlarını içerisinde bulunduran ve kullanmayı sağlayan yazılımlardır.
- **Yük (Payload):** Hedef makinaya erişim kazanan saldırganın istediği çalışmaları yapabilmesi için sisteme yüklediği yazılımlardır.
- **Yardımcı araç (auxilary):** Sisteme sızılma aşamasında port tarama, şifresiz hesapları bulma, basit şifreleri kırmak için kullanan yardımcı araçlardır.
- **Kodlayıcı (encoder):** Antivirüs, IDS/IPS, Firewall gibi sistemleri atlatmak için yükün (payload) şifrelenmesini sağlayan yazılımlardır.

2.2 ZARARLI YAZILIMLAR (MALWARE)

Zararlı yazılımlar (bazen kötü amaçlı yazılım da denir); sistemlerde kullanıcıların bilgisi olmadan bilgisayarlara sızıp verileri değiştirebilen, sistemin çalışmasını bozabilen ve sistemde tutulan kişisel bilgilere izinsiz erişim sağlayabilen tehlikeli yazılımlardır. Malware kelimesi, İngilizcedeki kötü niyetli (malicious) ve yazılım (software) kelimelerinden türetilmiştir. Günümüzde özellikle son kullanıcı cihazları kötü amaçları yazılım saldırılarına çok fazla uğramaktadır. Tehditlerin ana hedefi çoğunlukla son kullanıcı cihazları olmaktadır. Verilere, bilgisayarlara veya ağlara zarar vermek, veri ve sistemleri bozmak, verileri çalmak veya genel olarak başka bir "kötü" ya da yasadışı bir eylemde bulunmak için özel olarak tasarlanmış kod parçaları veya yazılımlarıdır.

Zararlı yazılımlar, çoğunlukla kullanıcıların güvenilir olmayan bağlantılar üzerinden yazılımın indirmesi ile ya da zararlı yazılım linkleri içeren oltalama mailleri üzerinden kullanıcı ya da kurum sistemlerine dâhil olmaktadır. Zararlı yazılımlar, sistemin güvenlik duvarları tarafından engellenemediğinde, sistemin kontrolü saldırgana geçebilir. *Bilişim sistemlerindeki korsanların en büyük motivastonları zararlı yazılımları kullanarak finansal kazanç sağlamaktır.*

Şekil 2.3. Zararlı yazılım kötü amaçlı kod parçacıklarıdır

Zararlı yazılım hakkında bilgi sahibi olmak, zararlı yazılımlardan korunmak için de oldukça önemlidir. Tehdit aktörleri ve çevrimiçi suçlular, güvenlik açıklarından yararlanarak kullanıcıları zararlı yazılım yüklemeleri için kandırmaya çalışır. Ayrıca, zararlı yazılımlar o kadar hızlı farklılaşıp, farklı bir yapıya dönüşür ki, koruma yazılımları her zaman bu yeni yapıya karşı koruma tarafında sahip olması gereken hıza yetişemez. Maalesef koruma yazılımları yeni tehditleri durduracak kadar hızlı bir şekilde güncellenmemektedir. Ayrıca; üretilen zararlı yazılım sayısı da koruma yazılımları sayısından fazladır. Üretilen istismarlar için https://www.exploit-db.com/ adresini ve zaafiyetleri incelemek için https://www.securityfocus.com/ adresini ziyaret edebilirsiniz.

2.2.1 Virüsler

Bilgisayar virüsleri biyolojik virüslerin insandan insana bulaşması gibi bir bilgisayardan diğerine kolaylıkla bulaşabilen zararlı yazılımlardandır. Başka bir yazılıma ya da çalıştırılabilir dosyaya kendini ekleyerek zararlı kodların çalışmasını sağlayan yazılımlardır. Belge açma, e-posta eki çalıştırma gibi bir etkileşim olmadan çalışmazlar.

Virüslerin karakteristik özelliği kendini kopyalaması **(çoğalma)** ve **bulaşmasıdır.** Zararlı kod kısmı ise her virüste farklılık gösterebilir. Kimlik bilgilerinin/verilerin çalınması, değiştirilmesi ya da silinmesi, donanımın işlevselliğinin zarar görmesi gibi etkiler gösterebilirler. Eskiden virüsler yayılmak için genellikle floppy diskler kullanırlardı. Günümüzde ise, USB Disk, CD/DVD ya da e-posta ekleri ile yayılabilirler. En sık karşılaşılan yöntem de e-posta ile yayılma yöntemidir.

Şekil 2.4. Virüs

İlk virüs, deneysel amaçla ARPAnet'te kendi kendini kopyalama amacıyla yazılmış Creeper (ARPAnet) virüsüdür. Bu virüs, TENEX OS işletim sistemlerinde etkili oldu. Bulaştığı bilgisayarlarda *"I'm the creeper, catch me if you can!"* diye bir mesaj görüntüleniyordu. Daha sonraları tespit edilip silinmesi amacıyla **Reaper** diye bir program yazıldı. Günümüzdeki anlamdaki ilk virüs, 1986 yılında ortaya IBM-PC tabanlı "Brain" ismi verilen bir sistemin başlangıç dosyasında çıkan bir virüstür.

Virüsün Belirtileri

- Bilgisayarın olağan dışı yavaşlaması,
- Yeni ya da daha önce kullanılan harici disklerin çalışmaması,
- Ekranda daha önce görünmeyen olağan dışı görüntü ve mesajların oluşması,
- Kullanılan programların anlam verilemez bir şekilde çökmesi ya da yavaşlaması,
- Dosya isimlerinin, boyutlarının ve kayıt tarihlerinin kendi kendine değişmesi,
- İnternete dosya yükleme ve internetten dosya indirme hızında düşüş.

Virüslerden Korunma Yolları

- Virüslerin en sık yayılma yolları e-postalar aracılığıyla olmaktadır. Gönderenin kim olduğu bilinmeyen kişilerden gelen e-postalar açılmamalıdır. Özellikle e-postalar ile birlikte gelen dosya ekleri de çalıştırılmamalıdır.
- Bilgisayarda ve cep telefonunda lisanslı bir antivirüs programı kullanılmalıdır. İşletim sisteminin güvenlik duvarı yazılımı açık tutulmalıdır. Virüslerden korunmak için farklı üretici firmalar tarafından sunulan antivirüs programı kullanılabilir. Örnek; Avast, Nod32, Kaspersky, Panda ve Symantec gibi üreticilerin antivirüs programları bulunmaktadır.
- Antivirüs her zaman güncel tutulmalıdır. Güncel olmayan antivirüs yazılımları, yeni çıkan virüsler için sistemleri korumada yetersiz kalacaktır.
- Harddisk, CD, flashdisk vb. gibi donanımlar üzerinden bilgisayara veri yüklemeden önce veya bu donanımlardan bilgisayara veri almadan önce bu donanımların antivirüs yazılımları ile taratılması gerekmektedir.
- İşletim sistemi sürekli güncel tutulmalı ve bilgisayarda orijinal (lisanslı) yazılım programları kullanılmalıdır.

İnternet tarayıcısında kilit işareti olmayan, güvenli olmayan web sayfalarını ziyaret ederken güvenlik zafiyetlerinin olabileceğini düşünerek, bu sayfalardan program ya da dosya bilgisayara ya da cep telefonuna indirilmemelidir. İndirildiği takdirde de, kullanmadan ya da açmadan önce indirilen dosyalar mutlaka bilgisayardaki antivirüs yazılımları ile taratılmalıdır. İndirilen dosyalar **https://www.virustotal.com/** sistemine yüklenerek tüm antivirüs yazılımlarını kullanarak çevrimiçi olarak da tarama gerçekleştirilebilir.

2.2.2 Solucanlar (Worm)

Kullanıcı etkileşimine ihtiyaç duymadan, çoğunlukla ağdaki, işletim sistemlerindeki açıklardan yararlanarak kendi kendini çoğaltma yeteneğine sahip olan zararlı yazılımlardır. Ağın performansını düşürürler. Veri çalma, kimlik hırsızlığı gibi çeşitli amaçlarla kullanılabilirler.

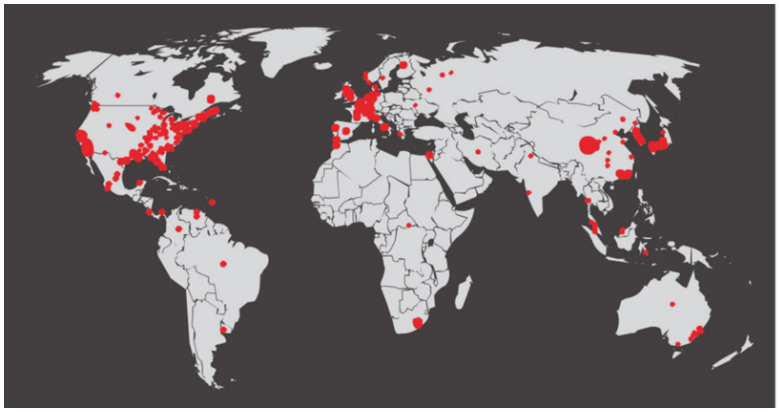
Şekil 2.5. Worm (Solucan) sistemdeki açıklardan yararlanır

Solucanlar bilgisayarlara kendisini kopyalayarak ve çalıştırılmasına gerek duyulmadan kendi kendine otomatik çoğalabilen zararlı yazılımlardır. Solucanlar sisteme bir kez bulaştıktan sonra kendi başlarına ilerlemekte ve kendini kopyalayarak çoğaltmaktadır. Solucanlar öncelikle bulaştıkları bilgisayar sistemlerinin denetimini ele geçirmektedir. Solucanların en büyük tehlikesi kendilerini çok fazla sayılarda çoğaltmalarıdır. Solucanlar e-posta eki olarak gönderilen dosyalar, web veya FTP kaynağı bağlantısı ile anlık mesajlaşma yazılımları ile gönderilen bağlantılar ile ya da P2P dosya paylaşım ağları üzerinden yayılabilmektedir. Bazı solucanlar ise ağ paketleri olarak yayılabilmektedir.

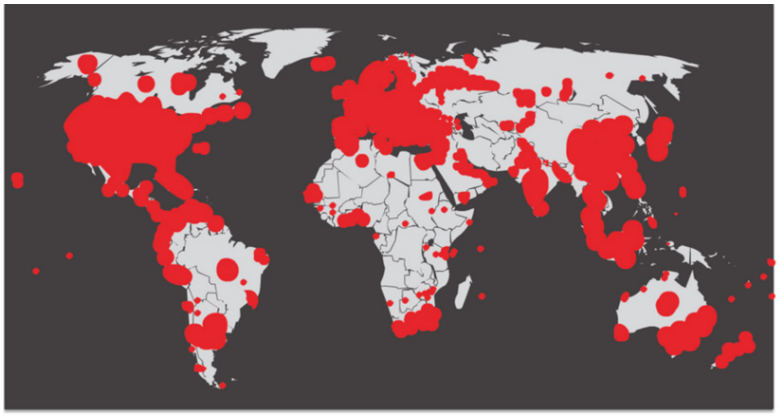
Bilgisayar solucanları virüsler gibi çoğalırlar ve aynı tür hasara neden olabilirler. Solucanlar özellikle ağlardaki güvenlik açıklarından yararlanarak bağımsız olarak kendilerini çoğaltırlar. Solucanlar, sistemden sisteme yayılırken de ağları yavaşlatabilirler.

Bir virüsün çalışması için bir kullanıcı etkileşimi gerekir fakat solucanlar kendi kendilerine çalışabilirler. Solucanlar ilk bulaşma sonrasında herhangi bir kullanıcı etkileşimine ihtiyaç duymazlar. Bir bilgisayara bulaştıktan sonra, ağ üzerinden çok hızlı bir şekilde yayılabilirler.

İnternetteki en yıkıcı saldırıların bazılarında solucan etkin rol oynamıştır. 2001 yılında, **Code Red** (kırmızı kod) solucanı başlangıçta 658 sunucuya bulaşmış, 19 saat içinde ise solucan 300.000'den fazla sunucuya bulaşmayı başarmıştır.



İlk Code Red Solucanı Yüklendiğinde



Code Red Solucanı Yüklendikten 19 Saat Sonrası

SQL Slammer solucanı, interneti yiyen solucan olarak bilinmektedir. SQL Slammer, Microsoft'un SQL Sunucusundaki bir arabellek taşma hatasından yararlanan bir hizmet reddi saldırısına neden olmaktadır. En bulaşıcı olduğu tepe noktasında, virüslü sunucuların sayısı her 8,5 saniyede iki katına çıkmıştır. Bu nedenle 30 dakika içinde 250.000'den fazla bilgisayara bulaşmayı başarmıştır. 25 Ocak 2003 hafta sonu piyasaya çıktığında, internet bağlantılarını, finans kurumları, ATM makinelerinin çalışmasının akmasına neden oldu. Garip olan ise, bu güvenlik açığının kapatılması için 6 ay öncesinde bir yama (patch) yayınlanmıştı. Yamayı kullanmayan sunucular etkilendi. Bu durum birçok kurumun; güncellemelerin ve yamaların önemli olduğu, zamanında uygulanmasını gerektiren bir güvenlik politikası olarak benimsenmesi gerektiği ile ilgili bir farkındalık oluşturdu.

Solucanlar benzer karakteristik özellikler gösterir. Hepsi etkinleştiren bir güvenlik açığından yararlanır ve kendilerini yaymanın bir yolunu bulur ve hepsi hedef sistem üzerinde yıkıcı bir eylem gerçekleştirerek, kendilerine ayrıcalıklı erişim ve izinler sağlayacak kötü niyetli kodları (payload) içerir.

Solucanların Bileşenleri

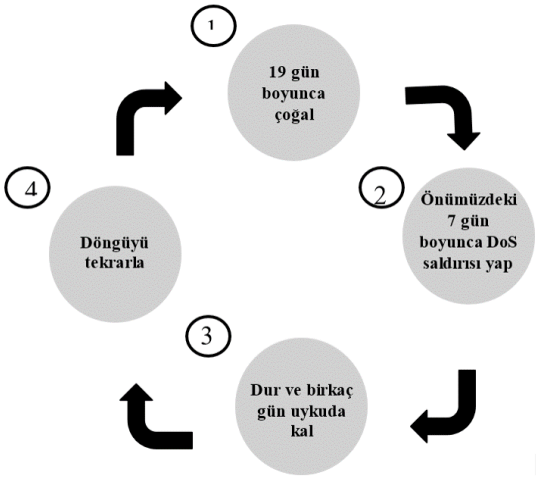
Yıllarca solucanları azaltmak için geliştirilen tekniklerine rağmen, solucanlar gelişmeye ve kalıcı bir tehdit oluşturmaya devam etmeyi başarmıştır. Hatta zamanla daha karmaşık yapılar haline gelmiştir. Fakat halen temelde yazılım uygulamalarındaki zaafiyetlerden yararlanma eğilimindedirler.

Solucan saldırılarının çoğu, **üç bileşenden** oluşur.

Güvenlik zaafiyetini etkinleştirme - Solucan, savunmasız bir sistemde bir e-posta eki, çalıştırılabilir bir dosya veya bir Truva atı gibi silahlar kullanarak kendisini yükler.

Yayılma mekanizması - Bir cihaza erişim sağladıktan sonra, solucan kendini çoğaltır ve artık kendine yeni hedefler bulur.

Ayrıcalıklı erişim ve izinler sağlayacak kötü niyetli kodlar - Bir eylemle sonuçlanan herhangi kötü amaçlı kodlardır. Çoğu zaman bu, tehdit aktörü



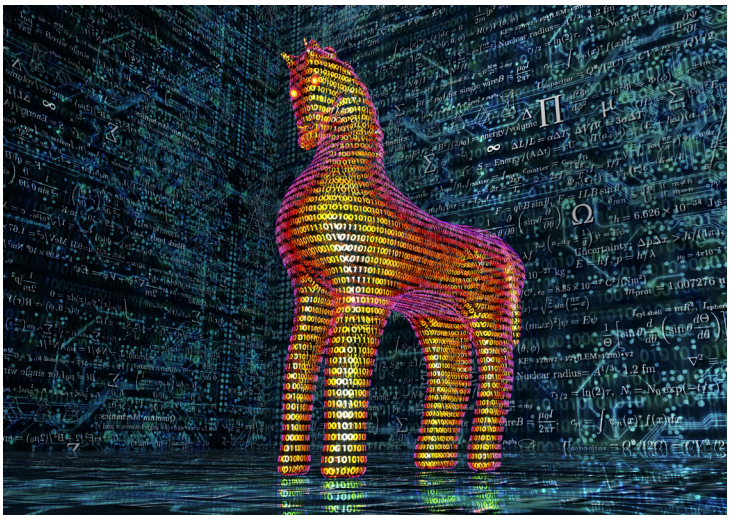
Şekil 2.6. Kırmızı Kod solucanının kullandığı yayılma tekniği

tarafından virüslü bilgisayara erişmesine izin veren bir arka kapı (back door) oluşturmak veya bir DoS saldırısı oluşturmak için kullanılır.

Solucanlar, bilinen bir güvenlik açığından yararlanmak için bir sisteme saldıran bağımsız programlardır. Başarıyla bulunan güzenlik açığı sonrasında, solucan kendini sisteme kopyalar ve yayılır. Çoğunlukla yayılma mekanizmalarını tespit etmek zordur. Bulaşabilecekleri tüm olası kaynakları uygun şekilde yamalanana kadar yayılmaya devam ederler.

2.2.3 Truva Atları (Tojan Horse)

Truva atı (veya kısaca trojan), yararlı gibi görünen ancak aslında zarara yol açan kötü amaçlı yazılımlardır. Mitolojideki Truva atı nasıl bir armağan gibi görünüp, aslında Troya kentini ele geçirecek askerleri taşıyorduysa; bu truva atları da yararlı yazılımlar gibi görünen bilgisayar programlarıdır. Çalıştırıldığında faydalı bir program gibi görünen ama aslında zarar veren programlardır.



Şekil 2.7. Trojan atı yararlı gibi görünen zararlı bir yazılımdır

Truva atları, eklendikleri program dosyasının çalıştırılması sonucu aktif olurlar ve kullanıcıların dosyaları kopyalamasıyla yayılırlar. Normal virüsler gibi tespit edilmeleri kolay değildir. Etkilerini bulaştıktan sonra gösterirler. Truva atları, interneti yavaşlatabilir, bilgisayardaki dosyaları silebilir veya dosya üzerinde değişiklikler yapabilir.

Truva atı klavyeden basılan tuşları kayıt altına alan programlar (keylogger) gibi programları da içerisinde barındırdığı için kullanıcının parolalarını ve banka hesapları gibi kişisel verilerini de sızdırabilirler. Truva atı zararlı yazılımı, genellikle e-posta veya hacklenmiş web siteleri ya da hack amaçlı tasarlanmış web sayfaları kullanılarak sisteme sızar. Truva atının tespit edilmesi diğer zararlı yazılımların tespit edilmesi kadar kolay değildir. Bazen antivirüs programlarının içerisine de saklanabildiği için bu zararlı yazılımın farkına varılması güçleşir.

Truva atları, genellikle neden oldukları hasara veya bir sistemi ihlal etme şekillerine göre sınıflandırılır. Tespiti zor olmasına rağmen, sistem ve ağ kaynaklarını kullandıklarından sistemde ve ağda oluşan anormal yavaşlıklardan anlaşılabilirler. Uzak erişim sağlamak, dosya göndermek, bağlantı noktası açmak (Ör: 21), Proxy sunucusu yapmak, DoS saldırısı yapmak gibi birçok farklı amaçlarla kullanılabilirler.

2.2.4 Diğer Zararlı Yazılımlar

Fidye Yazılımı (Ransomware)

Siber suçlar arasında bilgisayar korsanlarının en çok kazanç sağladığı yazılım türüdür. Siber saldırganlar kullanıcının ilgisini çekmek için onların takip ettiği, ilgilendiği paylaşımlar içeren bağlantılar ve e-posta göndermektedirler. İlgilerini çeken bu bağlantılara tıklayan veya gönderdikleri bağlantıları bilgisayarına indiren kullanıcıların indirdikleri dosya sisteme sızıp onların tüm kişisel bilgi ve verilerine izinsiz bir biçimde erişim sağlamaktadırlar. Fidye yazılımın en tehlikeli özelliklerinden biri, yazılım sisteme sızana kadar hiçbir biçimde anlaşılmamasıdır. Anladıkları zaman özel verileri siber saldırganların eline geçmiş durumdadır. Saldırganlar bu özel bilgi ve verilerinin karşılığında kullanıcıdan ücret istemektedirler.

Şekil 2.8. Fidye yazılımları en tehlikeli zararlı yazılımlardandır.

Şu anda kişisel ve kurumsal kullanıcılar için en fazla tehditi fidye yazılımları oluşturmaktadır. Fidye yazılımı, virüs bulaşmış bilgisayar sistemindeki verilere erişimi engelleyen kötü amaçlı bir yazılımdır. Siber suçlular bilgisayar sistemini şifreleyerek rehin almakta ve serbest bırakmak için de yüksek miktarlarda ödeme talep etmektedir. 2016'nın ilk yarısı ile birlikte, hem bireysel hem de kurumsal kullanıcıları hedefleyen fidye yazılımları daha yaygın ve güçlü hale geldi.

Düzinelerce fidye yazılımı çeşidi bulunmaktadır. Fidye yazılımları, sistem dosyalarını ve verilerini şifrelemek için sıklıkla bir şifreleme algoritması kullanır. Bilinen fidye yazılımı şifreleme algoritmalarının çoğunun şifresi kolayca çözülememektedir ve kurbanlara çok az seçenek bırakmaktadır. Kurbanlar talep edilen ödemeyi yapmaya zorlanmaktadır. Genellikle ödemelerin bir kripto para olan Bitcoin ile yapılması istenir. Çünkü blokzinciri (blockchain) teknolojisinin finansal alanda bir uygulaması olarak karşımıza çıkan bitcoin (değer saklama aracı) ile kullanıcılar kimliklerini saklayabilir. Bitcoin, herhangi bir merkez tarafından yönetilmeyen, merkezileştirilmiş, kontrol edilmeyen, anonim, şifreli ve açık kaynak bir kripto para birimidir.

E-postalar üzerinden kullanıcılara ulaştırılan kötü amaçlı reklamlar fidye yazılımlarının yayılım vektörleridir. Kimi zaman kendilerini güvenlik teknisyeni olarak tanımlayan siber suçlular, kişilerin evleri arayıp fidye yazılımını bilgisayarına indirmesi için bir web sitesine bağlanmaya ikna etmek için sosyal mühendislik de kullanabilmektedir.

Fidye yazılımından korunmak için;

- Şüpheli göndericinin e-postaları ve ekleri açılmamalıdır,
- Güvenli olmayan internet siteleri ziyaret edilmemelidir,
- Resmi kaynaklar harici yerlerden herhangi bir uygulama indirilmemelidir,
- Oltalama saldırılarındaki linklere tıklanmamalıdır,
- Düzenli olarak bilgisayardaki dosyalar yedeklenmelidir. Eğer güncel yedekler varsa, bilgisayardaki fidye yazılımı antivirüs programı ile temizlendikten sonra, bulutta ya da harici disklerde tutulan bu güncel yedek dosyalardan geri yüklenebilir.
- Lisanslı, düzenli günceleme yapılan bir antivirüs programı kullanılmalıdır.

Casus Yazılım (Spyware)

Bir kullanıcı hakkında bilgi toplamak ve bilgileri kullanıcının izni olmadan başka bir yere göndermek için kullanılır. Casus yazılımlar, kullanıcının gezindiği siteleri, indirdiği dosyaları, önemli bilgilerini, etkinliklerini izleyerek toplayıp izinsiz bir biçimde üçüncü taraflara bilgi vermek amacıyla yazılan tehlikeli yazılımlardır.

Şekil 2.9. Casus yazılım

Casus yazılım bir sistem monitörü, truva atı, reklam yazılımı, izleme çerezleri veya klavye tuşu kaydedicileri olabilir.

Reklam Yazılımları (Adware)

Reklam yazılımları gelir elde etmek amacıyla kullanıcılar için can sıkıcı olan açılan pencereleri (pop-up) görüntüler. Zararlı yazılım, kullanıcının ziyaret ettiği web sitelerini izleyerek kullanıcının ilgi alanlarını analiz edip sonrasında kullanıcıya uygun reklamlar gönderebilir.

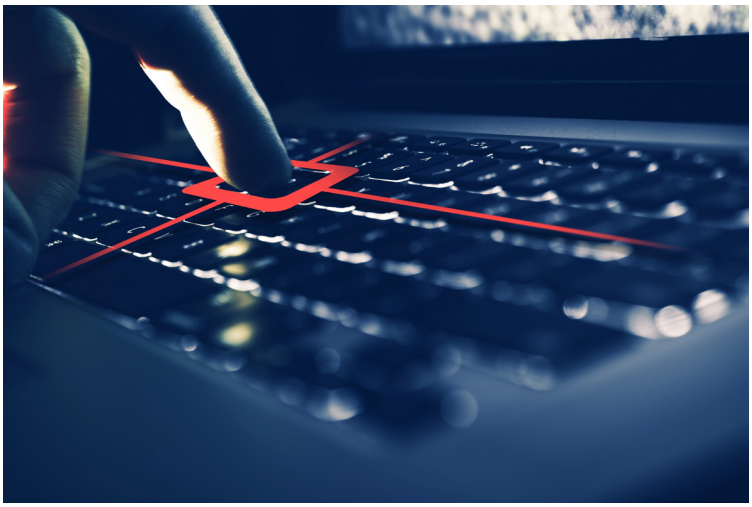
Korku Yazılımları (Scareware)

Kullanıcıda tehdit ve korku algısı oluşturarak onu şok etmek veya endişe uyandırmak için sosyal mühendislik kullanan dolandırıcılık yazılımlarıdır. Genellikle şüphelenmeyen bir kullanıcıya yönelik yapılır. Sahte tehdide karşı harekete geçerek kullanıcının eylemleri ile bilgisayara virüs bulaştırmaya çalışır.

Tuş Tutucular (Keylogger)

Tuş tutucular klavyeden basılan her tuşu kaydeden ve bu kayıtları kişisel bilgilerini çalmak isteyen kişilere göndermek için aracılık yapan programlardır. Bilgisayar korsanları sisteme sızdıktan sonra istedikleri zaman kayıtlara ulaşıp yazılan her tür bilgileri gönderebilir.

Kullanıcıların e-posta parolaları, kredi kartı numaraları, sosyal medya hesaplarının parolaları gibi önemli bilgiler çalınabilir. Tuş tutucular, yazılımla çalışanlar ve donanımla çalışan olarak iki farklı türde incelenebilir.



Şekil 2.10. Tuş tutucular

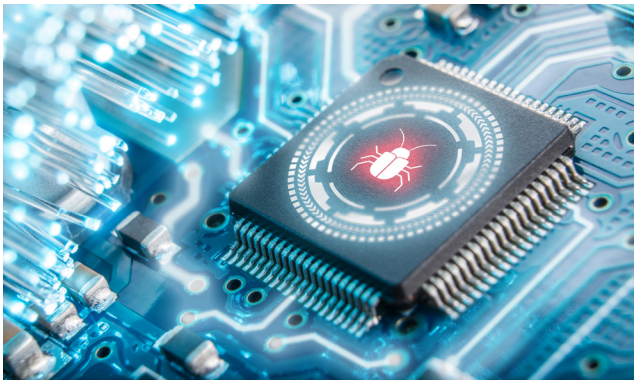
Yazılımla Çalışanlar; Sisteme yükledikten sonra işleme girilebilen ve tuşlarını takip eden programlarıdır.

Donanımla Çalışanlar: Bilgisayara dışarıdan bir donanımın eklenmesiyle işleme girilebilen ve basılan tuşları takip edip, bu takipten sonrada basılan tuşları donanıma kaydeden programlardır.

Rootkit

Rootkit'ler üçüncü kişilerin bilgisayardaki sistemleri kontrol etmesine olanak sağlar. Yüklendikten sonra, izinsiz girişini gizlemeye ve tehdit aktörüne ayrıcalıklı erişim sağlamaya devam etmektedir [13]. Amacı virüslerde olduğu gibi bilgisayarı yavaşlatmak veya bilgisayardaki özel bilgilere erişmek değildir.

En temel amaçları bilgisayarın kontrolünü ele geçirmek istemeleridir. Tüm süreç kullanıcı farkında olmadan gerçekleşir. İnternete bağlı bir bilgisayar Rootkit yazılımlarla kontrol edilebilir,

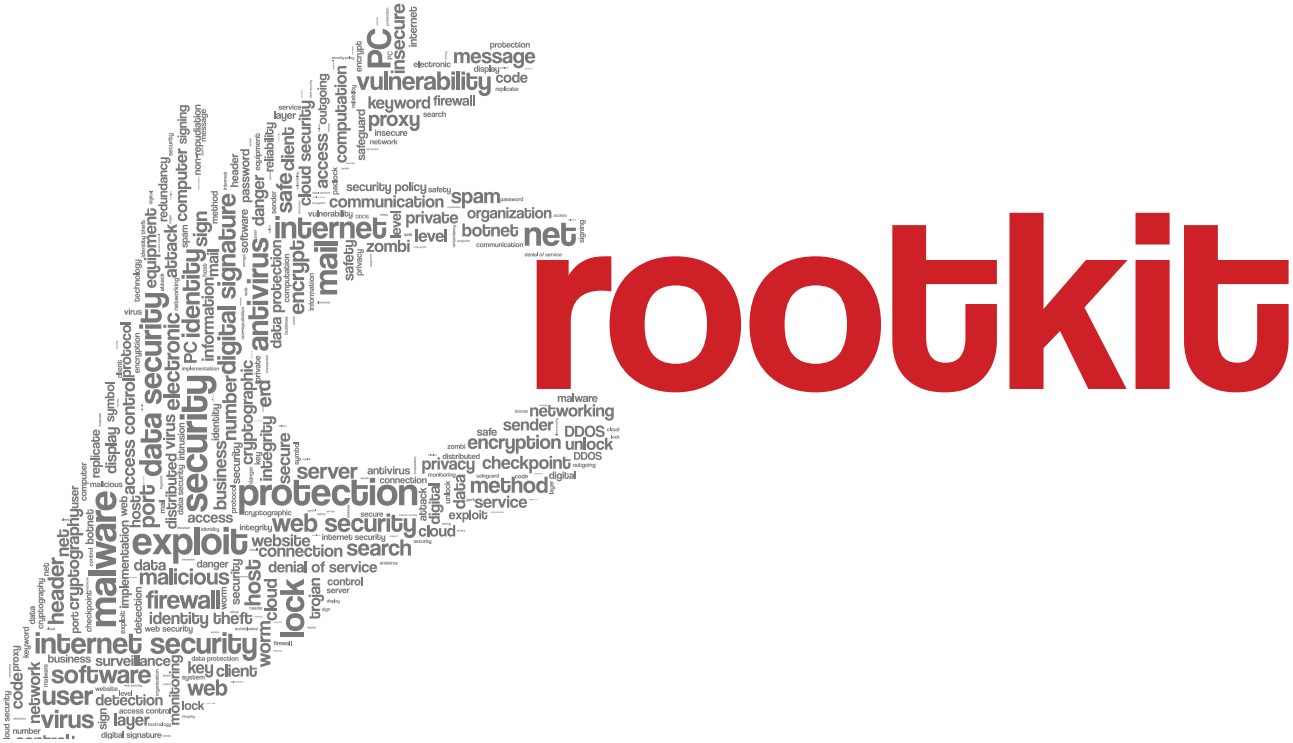


Şekil 2.11. Rootkit zararlı yazılımı bilgisayar kontrolünü ele geçirebilir.

kullanıcı farkına varmadan yasal olmayan sitelere girebilir veya siber saldırılar yapabilir. Rootkit'ler genellikle işletim sisteminin çekirdeğine yerleşir bu yüzden güvenilir antivirüs programları tarafından da tespit edilmesi zorlaşır.

2.2.5 RootKit Türleri ve Tespit Yöntemleri

Rootkit, yetkisiz bir kullanıcının (ya da tehdit aktörünün) bir sisteme girmesini ya da yazılımının kısıtlı alanlarına ayrıcalıklı erişime sahip olmasını sağlayan zararlı bir yazılımdır. Bilgisayarda gizli kalmaları için tasarlanmışlardır. Bir rootkit, tuş tutucular, bankacılık bilgilerini çalanlar, parola çalanlar, antivirüs engelleyicileri ve DDoS saldırıları için botlar gibi bir dizi zararlı araç içerebilir. Bu zararlı yazılım bilgisayarda gizli kalır ve saldırganın bilgisayara uzaktan erişmesini sağlar. Hedef cihaza yüklenebilen birçok rootkit türü vardır. Aşağıda bu zararlı yazılım türlerinden bazılarına değinilmiştir [19].



Şekil 2.12. Rootkit sistemlerden temizlenmelidir.

1- Kullanıcı Modu ya da Uygulama Rootkitleri: Kullanıcı modu rootkitleri, kullanıcı düzeyinde çalışan zararlı rootkitlerdir. Bilgisayardaki standart dosyaları rootkit dosyalarıyla değiştirirler. Bu rootkitler örneğin Windows işletim sisteminde Word, Paint veya Notepad gibi uygulamaları etkileyebilir. Bu programlar her çalıştırıldığında, bilgisayar korsanlarının bilgisayara erişimine izin verilmiş olur. Antivirüs programlarıyla aynı katmanda çalıştıkları için bunların tespit edilmesi nispeten kolaydır. Ancak enfekte olmuş programlar normal şekilde çalıştığından kullanıcıların rootkiti algılaması zor olabilir.

2- Çekirdek Modu Rootkitler: Bu rootkitler işletim sisteminin çekirdeğini (kernel) hedefleyen, işletim sisteminin çalışma şeklini değiştiren zararlı yazılımlardır. Doğrudan çekirdeğe ya da donanımı kullanan sürücülere (driver) müdahale edilebilir. Böylece tüm sisteme tam kontrol sağlanmış olduğundan tespit edilmesi çok daha zordur.

3- Önyükleyici (Bootloader) Rootkitleri: Bootloader, makina açıldığında bilgisayarın işletim sistemini yüklemeyi sağlayan önemli bir araçtır. Bu rootkitler, Ana Önyükleme Kaydına (Master Boot Record - MBR) bulaşarak hedef sistemin denetimini ele geçirir. Bir programın hedef işletim sistemi yüklenmeden önce yürütülmesini sağlayabilirler. Bu durum, bilgisayarın işletim sistemi açılmadan önce rootkitin etkinleştirildiği anlamına gelir.

4- Bellenim (Firmware) Rootkitleri: Bellenim rootkitleri, bilgisayarın anakartındaki küçük bir bellek yongasına yüklenen yazılım olan bilgisayarın sabit sürücüsüne veya sistem BIOS'una bulaşabilen zararlı yazılımlardır. Teorik olarak yönlendiriciler gibi donanımlara da bulaşabilir. Bilgisayar korsanları, diske yazılan verilere müdahale etmek için bu rootkitleri kullanabilir.

5- Hafıza Rootkitleri: Bu tür bir rootkit, bilgisayarın Rasgele Erişim Belleğinde (RAM) gizlenir ve kullanıcıdan gizli olarak arka planda zararlı faaliyetler gerçekleştirir. Rastegele erişimli bellekte yer aldıklarından kalıcı değillerdir, elektrik kesildiğinde aktiviteleri biter. Ancak sistem yeniden başladığında tekrar devreye girebilirler.

Rootkit Tespit Teknikleri

Rootkitler, siber dünyadaki belki de en tehlikeleri zararlı yazılımlardır. Her geçen gün çok daha farklı ve yeni teknikler ile daha yetenekli hâle gelen bu zararlı yazılımlara karşı, siber güvenlik uzmanının da çeşitli tespit etme teknikleri ve önleme yolları vardır. Aşağıda bu tekniklerden bazıları ve öneriler yer almaktadır:

1. **Analiz için Güvenilir Konak:** İşletim sistemlerinde çekirdeğe bulaşmış rootkitlerin olduğu dikkate alınırsa, bu yöntemde güvenilir olduğu bilinen bir konak kullanılabilir.

Özellikle CD gibi sadece okunur ortamlara yüklü olan işletim sistemlerinin bulunduğu konaklar kullanılabilir.

2. **İmza Tabanlı Teknik:** En yaygın olan tekniktir. Ancak sadece daha önceden tespit edilmiş olan rootkitlerin imzalarına dayalı bir yöntem olduğundan en zayıf tekniklerden biridir.

3. **Davranış Tabanlı Teknik:** Tüm diğer zararlı yazılımlarda olduğu gibi, rootkitler de sistemde iz bırakırlar. Bu iz genellikle sistemin doğal davranışını değiştirir. Sistemin anormal davranışının tespitinden yararlanan yöntemdir. Bu yöntem daha önceden bilimeyen rootkitlerin de tespit edilmesini sağlayabilir. Ancak "false positive" olarak adlandırılan yanlış alarma da neden olabilir.

4. **Temel Çizgi Tabanlı Teknik:** Daha önceden temiz olduğu bilinen, sistemin davranışlarının temel çizgisinin (baseline) çizildiği ve buna göre farklılıklara göre tespitin yapıldığı davranış tabanlı bir tekniktir.

5. **Bütünlük Doğrulama Tekniği:** Rootkitler genellikle sistem üzerindeki (registry) gibi kayıtları ya da sistem dosyalarını değiştirebilir. Sistemdeki kaynakların bütünlüğünün doğru bir sistemle karşılaştırıldığı yöntemdir.

Bu tekniklerin haricinde, bellek döküm tekniği, çarpraz doğrulama tekniği, sezgisel yöntemler, ağ analiz yöntemi ve sistem kaynağı izleme gibi teknikler de bulunmaktadır.

Rootkitlere karşı savunmanın belirli tek bir yöntemi bulunmamaktadır. Ancak yine de son kullanıcının savunma açısından yapabilecekleri ve dikkat etmesi gereken kuralları vardır. Aşağıda bu hususlar maddeler halinde belirtilmiştir:

- İşletim sistemi ve diğer yazılımlara ilişkin güncellemelerin yapılması gerekir.
- Oltalama e-postalarına karşı dikkatli olunması gerekir.
- USB gibi otomatik çalışan sistemleri kullanırken dikkatli olunması gerekir.
- Bilinmeyen kaynaklardan dosyaların sisteme yüklenmemesi gerekir.
- Korsan yazılımların kullanılmaması gerekir.

2.2.6 Zararlı Yazılımın Belirtileri ve Korunma Yöntemleri

Sisteme bulaşmış zararlı yazılım türü ne olursa olsun sistemde görülebilecek zararlı yazılım belirtileri;

- CPU kullanımında bir artış,
- Bilgisayar hızında bir azalma,
- Bilgisayarın sık sık donması veya çökmesi
- Web tarama hızında bir azalma,
- Ağ bağlantılarıyla açıklanamayan sorunlar,
- Değişen dosyalar,
- Silinen dosyalar.
- Bilinmeyen dosyalar, programlar veya masaüstü simgeler,
- Çalışan ve bilinmeyen süreçler,
- Kendilerini kapatan programlar veya yeniden yapılandırılan programlar,
- Kullanıcının bilgisi veya rızası olmadan gönderilen e-posta olarak sıralanabilir.

Zararlı Yazılımlardan Korunma Yöntemleri

- Gönderilen e-postaları kontrol ederken tanımadığınız kişilerce gelen e-postalar güvenliğinden emin olunmadan açmayınız. Gönderilen bağlantıları ve dosyaları indirmeden önce tarama zararlı yazılım taraması yapınız. Günümüzde zararlı yazılımların bilgisayara sızmasındaki en tehlikeli araç e-postalardaki indirilen dosyalardır.
- Sosyal Medya kullanırken kişisel bilgilerinizi paylaşmamaya özen göstermelisinz ve sadece tanıdıklarınız için profilinizi açık kullanmalısınız.
- Antivirüs programlarını düzenli güncellemelisiniz.
- Sisteminizdeki yazılımlarda otomatik seç yerine, yazılımları manuel olarak nelere erişim yapabileceği konusunda siz karar vermelisiniz.

- Resmi, bir devlet sitesinde işleminiz varsa, kişisel bilgilerinizi girerken o sitede SSL Güvenlik Sertifikası kullanıldığına dikkat ediniz.
- Korsan yazılımları kullanmak yerine güvenlik açısından o programın lisanslı halini kullanınız.
- İşletim sistemini ve programları güncel tutarak zararlı yazılımlardan korunabilirsiniz.
- Güçlü parolalar kullanmalısınız ve parolalarınızı belirli aralıkla değiştirmelisiniz.
- Güvenlik duvarı sisteminiz ve internetiniz arasında sizi koruyan bir aracıdır. Güvenlik duvarınızı açık ve güncel tutmalısınız
- Sisteminize ihtiyacınız olmayan uygulamaları indirmemelisiniz.

2.3 SİBER GÜVENLİK UNSURLARI

Şekil 2.13. Siber güvenlik unsurları

Siber güvenlik ya da daha genel olarak ilgi güvenliği, bilgilerin izinsiz ve yetkisiz erişimlerden, kullanımından, ifşa edilmesinden, ortadan kaldırılmasından, değiştirilmesinden veya hasar verilmesinden korunması işlemidir. Bilgi güvenliği üç temel bileşenden meydana gelmektedir. Bunlar; gizlilik, bütünlük ve erişebilirliktir. Bu üçlüye kısaca **CIA** (Confidentiality-Gizlilik, Integrity-Bütünlük, Avaibility-Erişilebilirlik) adı verilmektedir.

2.3.1 Gizlilik

Bilgisayarlar arası iletişimin güvenli bir şekilde yapılması çok önemlidir. Bunun için bilgisayar sistemlerini kullanan kişilere ait bilgilerin başka kişiler ile paylaşılmaması gizlilik olarak

isimlendirilir. İzin verdiğiniz kişisel bilgilerin sadece bu bilgilere erişebilecek kişilerce erişilebilmesi ve görüntüleme ile sınırlandırılması gerekmektedir. Örneğin; basit bir amaç için kullanılan bir program veya uygulamanın sadece amacı doğrultusunda sizin verilerinizi kullanması gerekmektedir. Mesaj amacı ile kullandığınız bir uygulamanın üçüncü kişiler ile paylaşılabilecek bir yapıya bürünmesi gizlilik için bir sorundur.

Bireysel verinin yanında kurumların sahip oluğu veriler çok daha büyük miktarda olabilir. Kurumların ellerinde bulunan verilerin gizliliğinin sağlanması için bilgisayar sistemleri kullanılabilmektedir. Ancak bu sistemleri kullanan kişilere veri güvenliğinin sağlanması için erişim yetkileri verilmesi gerekmektedir. Yetkisiz erişimler verilerin gizliliğini bozabilmektedir.

Gizliliğin sağlanması için farklı şifreleme sistemleri kullanılmaktadır. Bunlar arasında yaygın olarak kullanılanları biyometrik tanımlama (retina, parmak izi vb) ve e-imza gibi sitemler bulunmaktadır.

2.3.2 Bütünlük

Bilginin bütünlüğü, bilginin korunması anlamına gelmektedir. Bilgi bir kaynaktan çıktıktan sonra alıcıya ulaşana kadar geçtiği süre boyunca değiştirilmemesi güvence altına alınması gerekmektedir. Bir bilgi bilgisayar sistemleri boyunca taşındığından, yetkisiz kişilerin eline geçmemesi ve değiştirilmemesi için gerekli tedbirlerin alınması gerekmektedir.

Özellikle dosya paylaşımlarında erişimlerin kayıt altına alınması, izinsiz erişimlerin engellenmesi, yedekleme amaçlı farklı sistemlerin kullanımı bütünlük için alınması gereken önlemler arasında yer alabilir. Kurumsal olarak incelenecek olursa, özellikle yedekleme bütünlük için en önemli konulardan biridir. Verinin bütünlüğünün bozulması yani verinin bir kısmının veya tamamının kaybolması sırasında verinin yeniden geri getirilmesi için farklı noktalarda yedeklerin alınması ve/veya güvenli ve uzak bir bölgede felaket kurtarma (Disaster Recovery) merkezlerinde tutulması bütünlük açısından alınabilecek önlemlerin başında gelmektedir

2.3.3 Erişilebilirlik

Bir veriye veya bilgiye erişim yetkisi olan kişilerce erişilmesi ve erişim yetkisi olmayan kişilerce erişilmemesine denilir. Erişim yetkisi belirli sürelerde ve belirli sınırlamalar ile yapılması gerekmektedir. Buradaki amaç yeteri kadar erişim yetkisi verilmesidir. Kişilere verilecek daha fazla erişim yetkisi amacına uygun olmayabilir. Alınacak her türlü erişilebilirlik önlemi, gelebilecek tehditlere karşı bir tedbirdir.

2.3.4 Bilgi Güvenliğinde Diğer Unsurlar

Bilgi güvenliği belirtilen 3 unsur haricinde daha birçok unsurdan oluşur. Bunlar;

- **Güvenilirlik (Reliability):** İstenilen ve beklenen sonuç ile sistemin verdiği sonuç arasındaki tutarlılıktır. Sistem her çalıştırıldığında tutarlı olarak aynı sonucu üretmesidir.
- **İnkâr Edememe (Non-repudiation):** Bu unsur, iki bilgisayar sistemi arasında bir veri iletişimi yapıldığında gönderici bilgisayarın veri gönderdiğini, alıcı bilgisayarın ise veriyi aldığını inkâr etmemesidir. Bu şekilde alıcı ve gönderici arasındaki iletişim sorunları en aza indirilmesi hedeflenmiştir. Bu unsurdan önce kimlik doğrulama işleminin gerçekleşmesi gerekmektedir.
- **Kimliklendirme (Identification):** Bir kullanıcının bir bilgisayar sistemine veya kaynağına erişmek için girdiği bilgilerdir. Bu bilgiler kullanıcı adı, şifresi, parmak izi gibi bilgiler olabilir.
- **Kimlik Doğrulaması (Authentication):** Kimliklendirme (Idendity) tek başına kullanıldığında çoğu zaman yeterli ve güvenilir bir unsur değildir. Herhangi bir kişinin sadece kullanıcı ID'sini beyan ederek sisteme bağlanmak istemesi güvenlik için yeterli değildir. Kişi, erişim yapanın ya da işlemi yapacak olanın kendisi olduğunu sisteme ispatlaması gereklidir. Bu işlem "kimik doğrulaması" olarak adlandırılır. İlerki bölümlerde ele alıancak olan dijital imzalar ya da daha yaygın kullanımı olan parolalar bu amaç için kullanılır.
- **Yetkilendirme (Authorization):** Kullanıcının kimlik doğrulaması sonrası hangi yetkilerle sisteme erişmesine imkân veren bir unsurdur. Sistemi kullanan kullanıcılar için bir kullanıcı havuzu oluşturulur ve bu havuzdaki kullanıcılar belirli amaçlar doğrultusunda gruplandırılır. Her gruba erişim yetkisi tanımlanır. Kullanıcılar sadece kendisine tanımlanmış olan yetkiler çerçevesinde sistemleri kullanabilirler. Bu şekilde yetkisiz işlemlerden kaçınılmış olunur.
- **İzlenebilirlik/Kayıt Tutma (Auditing):** Bir sistemi kullanan tüm kullanıcıların yaptıkları işlemlerin izlenmesi ve kayıt altına lınması işlemidir. Normal şartlar dışında bir durum oluşturğunda sorunun tespit edilebilmesi ve giderilmesi için alınan tedbirdir. Örneğin bir kuruma ait bilgilerin kurum dışına çıkarılması işlemi için ağ trafiği izlenebilir ve sorumlu kişilerin tespiti sağlanabilir.
- **Hesap Verilebilirlik (Accountability):** Kişileri eylemlerinden dolayı sorumlu tutmak ve benzer olarak yanlış yargılamaya sebep olmamak için log kayıtları kullanılır. Bu sebeple "Auditing" ile karıştırılabilir [29].

2.4 SİBER SALDIRILAR VE SALDIRI TÜRLERİ

Tehdit aktörleri, çok çeşitli motivasyonlarla hareket etmekte ve sistemlere saldırılar yapmaktadır. Bu başlık altında saldırıların ne olduğu ve yaygın saldırılar ele alınmıştır.

2.4.1 Siber Saldırılar

Siber saldırılar (ya da siber ataklar), siber tehdit aktörleri tarafından bir veya daha fazla bilişim sistemi kullanılarak, bir ya da birçok sisteme veya ağa yapılan saldırılardır. Bir siber saldırı, kötü niyetli olarak sistemleri devre dışı bırakabilir, verileri çalabilir veya ihlal edilen bir bilgisayarı diğer saldırılar için aracı olarak kullanabilir. Siber suçlular, diğer yöntemlerin yanı sıra zararlı yazılım, kimlik avı, fidye yazılımı, hizmet reddi dâhil olmak üzere siber saldırı başlatmak için çeşitli yöntemler kullanır.

IETF RFC 2828'deki tanımlamaya göre siber saldırı, "akıllı bir tehditten kaynaklanan sistem güvenliğine yönelik bir saldırı, yani, güvenlik hizmetlerinden kaçmak ve bir sistemin güvenlik politikasını ihlal etmek için kasıtlı bir girişim (özellikle bir yöntem veya teknik) olan akıllı bir eylem" olarak ifade edilmiştir. Bu kitap boyunca ***"Bilgi sistemi kaynaklarını veya bilginin kendisini toplamaya, bozmaya, reddetmeye ya da yok etmeye çalışan her türlü kötü amaçlı etkinlik"*** tanımı esas alınacaktır.

Şekil 2.14. Siber saldırılar çeşitli kötü amaçlar doğrultusunda yapılır

Siber saldırıların sınıflandırılmasında genel kabul görmüş yaygın bir sınıflandırma yöntemi olmasa da, çeşitli kriteler kullanılarak sınıflandırmalar yapılmıştır. Ancak IETF'e göre siber ataklar, **aktif saldırılar** ve **pasif saldırılar** olmak üzere ikiye ayrılabilir (RFC 2828). Aktif saldırılar, sistem kaynaklarını değiştirmeye ya da sistemin işleyişini değiştirmeye yönelik saldırılardır. Pasif saldırılar sistem kaynaklarını etkilemeden kullanmaya ve bilgi almaya yönelik saldırılardır. Genellikle sistem tarafından farkedilmeden bilgi toplamaya ve aktif siber saldırı öncesi hazırlık olmak amacıyla bilişim sisteminin ya da ağın gözlemlenmesini içerir.

2.4.2 Ağ Saldırıları

Ağ saldırıları, keşif saldırısı, erişim saldırısı ve DoS saldırıları olmak üzere üç başlık altında incelenir. Her bir saldırı yine birden çok alt saldırı türü de içermektedir.

Keşif Saldırısı (Reconnaissance attack) : Keşif saldırısında amaç bilgi toplamaktır, genellikle yapılandırılmış profesyonel bir saldırının ilk aşamasıdır. Hedef sistem ya da ağ hakkında zayıflıklar da yine bu saldırının altında incelenir. Bu amaç doğrultusunda, çeşitli araçlar ve teknikler kullanılarak port taraması, IP taraması, zafiyet araması gibi ataklar yapılabilir. Aşağıdaki tabloda keşif saldırısında yer alan teknikler ele alınmıştır.

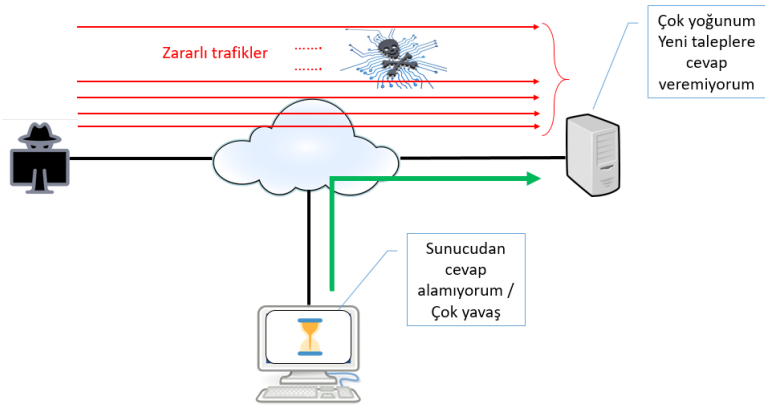
Teknik	Açıklama
Hedef hakkında bilgi sorgulaması yapma	Hedef hakkında arama motorları, whois sorguları, kurumsal web sayfalarında araştırmalar yapılabilir.
Hedef ağda ping taraması başlatma	Hedef ağda hangi IP'lerin aktif olduğunun tespit edilmesine yönelik yapılan taramadır.
Port taraması yapma	Hedef konak tespit edildikten sonra hangi portların ya da hizmetle-rin açık olduğunun tespit edilmesidir. Nmap, SuperScan, Angry IP Scanner, ve NetScanTools araçları kullanılabilir.
Zaafiyet Taraması	Hedef cihaz hakkında zayıflıkların taranmasına yönelik yapılan ta-ramalardır. Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT ve Open VAS gibi araçlar kullanılır.
İstismarın Yürütülme araçları	Tehdit aktörü savunmasız hizmetleri keşfetmeye çalışır. Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit ve Netsparker gibi çeşitli güvenlik açığı istismar araçları kullanılır.

Tablo 2.1. Keşif saldırı teknikleri

Erişim Saldırıları: Kimlik doğrulama hizmetleri, web hizmetleri gibi kullanıcı erişim bilgileri barındıran hizmetlerdeki güvenlik açıklarından yararlanarak, web hesaplarına, erişimi sınırlandırılmış veri tabanlarına ya da diğer hassas bilgilere giriş yapabilmektir. Tehdit aktörleri, verileri almak, erişim elde etmek veya erişim ayrıcalıklarını yönetici durumuna yükseltmek için ağ aygıtlarına ve bilgisayarlarına erişim saldırılarını kullanır. Bu saldırılar arasında, parola saldırısı, aldatma (spoofing) saldırıları yer almaktadır. Parola saldırısında, tehdit aktörü çeşitli yöntemler kullanarak kritik sistem parolalarını keşfetmeye çalışır. Parola saldırıları çok yaygındır ve çeşitli parola kırma araçları kullanılarak yapılır. Aldatma saldırılarında, tehdit aktör cihazı başka bir cihaz gibi davranmaya çalışır. IP aldatma, MAC aldatma ve DHCP aldatma bu kategoride yer alan saldırılardır. Bu saldırılar, kitabın sonraki kısımlarında daha ayrıntılı olarak ele alınacaktır. Diğer erişim saldırılarından bazıları şunlardır:

- **Güven istismarı (trust exploitation):** Belirli bir hedefe doğrudan erişimin yapılamadığı durumda, hedefin güvendiği bir sistem gibi davranmak, ya da hedefin güvendiği sistem üzerinden saldırı yapmayı ifade eder.
- **Ortadaki adam (Man-in-the-middle) :** Bu saldırı türünde, tehdit aktörü iletişim kuran iki sistem arasına sızmıştır. Verileri okuyup değiştirme yapabilir.
- **Arabellek taşması (buffer overflow):** Arabellek taşması saldırısında, tehdit aktörü arabelleğin kaldırabileceğinden fazla yük ile doldurup genellikle sistemi çalışmaz hale getirerek bir DoS saldırısı oluşturur

2.4.3 DoS ve DDoS Saldırıları



Şekil 2.15. DoS Saldırısı

Bilgisayar ağlarında özellikle sunuculara ve ağ ara bağlantı cihazlarına karşı yapılan saldırılardan en yaygın olanı ve en çok adı geçen, hizmet reddi **(Denial of Service - DoS)** saldırılarıdır. Diğer birçok saldırının ya da zararlı yazılımların nihai hedef işlemi de yine DoS saldırısı olabilir. Temel olarak DoS saldırılarında amaç, hizmet sunan bir cihazın işlevselliğini durdurmaktır [7],[10],[32].

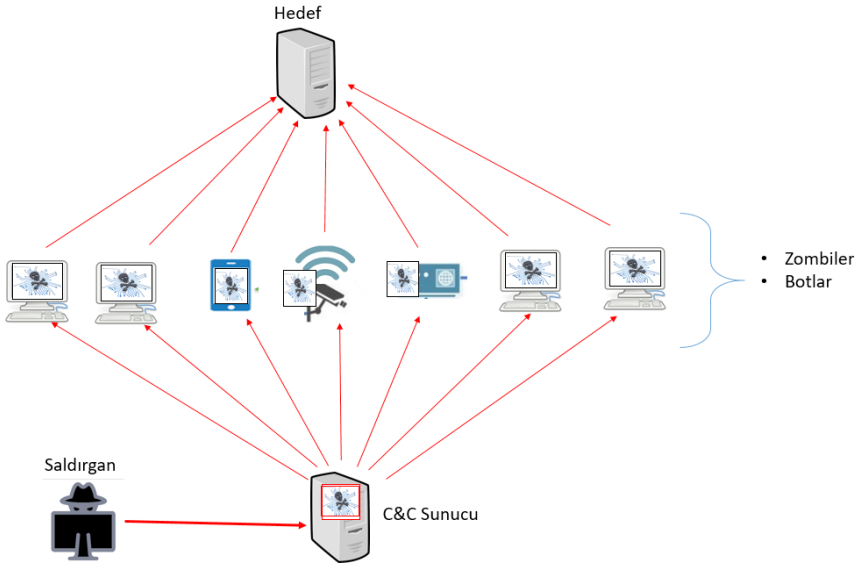
Çok farklı türde DoS saldırı türü olmasına karşın temelde olmak ***Aşırı Miktarda Trafik*** ve ***Kötü Amaçlı Yapılandırılmış Paketler*** üzere iki tür DoS saldırı türü vardır.

Aşırı Trafik Miktarı - Tehdit aktörü, hedef cihaza (veya uygulamaya) karşılayamayacağı kadar büyük miktarda ya da karşılayamayacağı hızda veri gönderir. Bu durum cevap sürelerinin yavaşlamasına neden olabildiği gibi, cihazın veya hizmetin çökmesine neden olabilir.

Kötü Amaçlı Yapılandırılmış Paketler - Tehdit aktörü, kötü niyetli olarak biçimlendirilmiş bir paketi bilgisayara veya uygulamaya gönderir. Alıcı, hatalı yapılandırılmış paketi işleyemez ya da işlerken ara bellek taşmasına neden olur.

Saldırgan açısından başarılı olan bir DoS saldırısı sonrasında, cihaz tekrar işlevselliğini kazanıncaya kadar bir süre boyunca devre dışı kalabilir. Sonuç olarak hizmetin türüne göre kurum parasal kayıplar yaşayabilir ya da itibar kaybına uğrayabilir.

DDoS Saldırıları ise, zararlı yazılım barındıran (enfekte olmuş) cihazlar tarafından yapılan dağıtılmış DoS saldırılardır.



Şekil 2.16. DDoS saldırısı

Enfekte olmuş cihazlar, botnetler olabildiği gibi zararlı yazılım barındıran ve saldırgandan bir eylem komutu bekleyen konaklar da olabilir. Saldırgan komuta kontrol (C&C) sunucusu aracılığıyla

belirlenen hedefe saldırı komutunu gönderir. C&C Sunucusu, zararlı yazılım yüklü cihazlara hedefe saldırısı başlatması komutunu gönderir. Zararlı yazılım yüklü olan enfekte cihazlar, çoğu zaman o ana kadar herhangi bir zararlı aktivite göstermemiş olan saldırı için C&C sunucusundan komut bekleyen cihazlardır. Bu nedenle genellikle **"zombi"** olarak adlandırılırlar. Truva atları ve solucanlar gibi zararlı yazılımlar, arka kapı açarak C&C sunucusundan komut bekleyebilirler. 2016 yılında ortaya çıkan Mirai botnet saldırısında olduğu gibi, cihazlar sadece bilgisayarlar değil, güvenlik açığı barındıran Nesnelerin İnterneti (IoT) cihazları da olabilir. Yani teorik olarak, internete bağlı olan ve zafiyet barındıran bir mutfak robotu ya da su ısıtıcısı DDoS saldırısının birer parçası olabilir.

2.4.4 Sosyal Mühendislik Saldırıları

Bilgisayar sistemlerine sızan kötü amaçlı kişilerin sisteme yetkisiz bir şekilde erişmek için bilgi güvenliği üçgenini bozarak gizli bilgilerin açığa çıkarılmasında gösterdikleri faaliyetler **sosyal mühendislik** olarak ifade edilir. Saldırgan ya da bilgisayar korsanı olarak ifade edilen kötü amaçlı kişiler, kullanıcıların kullandıkları sistemlerin olabilecek zafiyetlerini iyi bilirler. Sistemlerin zafiyetleri üzerinden ancak en çok da kullanıcılardan kaynaklı zaafiyetler üzerinden sistemlere erişim sağlarlar. Bilişim alanındaki bilgi ve becerileri kendi amaçlarını için kişi ve kurumlara zarar vermek için kullanan kötü amaçlı kişileri sistemleri kullanan dijital okuryazarlık düzeyi düşük, siber tehdit farkındalığı düşük kullanıcıları kendi amaçları ile yönlendirerek, çeşitli eylemler yapmaya zorlarlar. Sosyal Mühendislik saldırıları aracılığı ile en çok ulaşılmak istenilen şey kişilerin kimlik bilgileridir. Bu da kimlik avı hırsızlığı olarak ifade edilir. Kimlik avı sonucunda sonucunda kişiler için çok yüksek finansal kayıplar oluşabilir. Sosyal mühendislik, kişileri çeşitli eylemleri yapmaya veya gizli bilgileri ifşa etmeye yönlendirmeye çalışan bir saldırıdır. Bazı sosyal mühendislik teknikleri şahsen yapılırken, bazıları telefon veya interneti (özellikle sosyal medya araçlarını) kullanabilir. Sosyal mühendislik saldırısı yapan tehdit aktörleri genellikle insanların yardımcı olma isteğini ya da korkularını kullanırlar.

Ünlü bilgisayar korsanı ve sonrasında kariyerine siber güvenlik uzmanı olarak devam eden Kevin D. Mitnick de

- "Sosyal mühendislik cephanemdeki en güçlü silahlardan biriydi"
- "İnsan unsuru aslında güvenliğin en zayıf halkasıdır"
- "Sorun makinelerde değil, insan unsurunda" demektedir.

Sosyal mühendislik ile erişmek istenilen verilere daha kolay ulaşılabileceğinden bahsetmiştir.

Hemen her geçen gün çok farklı teknikler ve çoğu zaman güncel senaryolar kullanılarak bu saldırılar gerçekleştirilmektedir. Aşağıda bu yöntemlerden bazıları ele alınmıştır.

Bahane Uydurma (Pretexting): Tehdit aktörü, alıcının kimliğini doğrulamak için kişisel veya finansal verilere ihtiyaç duyduğunu belirterek, kişi hakkında özel bilgileri (parola, TC Kimlik, anne kızlık soyadı, ev adresi vb) almaya çalşır.

Oltalama (Phishing) : İnsanları kandıramak, tuzağa düşürmek ve dolandırmak anlamındadır. Kullanıcılarının kredi kartı bilgileri, kimlik numarası, kişisel bilgileri, banka hesap numaraları ve bu hesapların parolalarını elde etmek amacıyla saldırganlar tarafından yapılan sosyal mühendislik saldırılarından biridir. Bu saldırılarda kullanıcı kandırıldığı ve oltaya takılan bir balığa benzetildiği için saldırının adı "oltalama" saldırısıdır. Oltalama ile telefon dolandırıcılığı, ürün tanıtımı adı altında dolandırıcılık ve bu tarz aklınıza gelebilecek ya da gelemeyecek çok farklı senaryolar üretilerek parola gibi kritik bilgiler ele geçirilmeye çalışılır. En yaygın oltalama e-posta yoluyla yapılmaktadır.

Şekil 2.17. Oltalama saldırısı

Yemleme Kancası (Spear Phishing) : Hedef hakkında ayrıntılı araştırma yapıldıktan sonra, hedefin ilgisini çeken reklam, SMS, e-posta göndererek kimlik bilgilerinin (ya da diğer yararlı bilgilerin) ele geçirilmesini sağlayan yöntemdir. Örneğin, hedefin araba satın almak istediği öğrenildikten sonra, kişiye özgü cazip olabilecek bir e-posta gönderilerek belirli bir zararlı siteye yönlendirmek gibi…

Bir şey için bir şey (quid pro quo): *"Hediye kazandınız"* gibi mesajlarla, hedefi zararlı bir siteye yönlendirmek ya da zararlı bir yazılım yüklemek için kandırmaktır.

Tuzağa düşürmek (Baiting): Meraklı kullanıcıları hedef alan bir sosyal mühendislik yöntemidir. Zararlı yazılım yüklü bir belleği hedefe yakın bir yerde kasıtlı olarak bırakarak, hedefin bu belleği sisteme yüklenmesi beklenmesi bu saldırıya bir örnek olarak verilebilir.

Oltalama Yoluyla Gerçekleşen Örnek Bir Saldırı

Dolandırıcılar kendilerini bilinen bir banka olarak tanıtıp kullanıcılara rastgele e-posta gönderir ve e-postanın içeriğine bakıldığında ise kredi kartı ya da banka kartı güncellenmesi ile ilgili bankadan gelmiş izlenimi oluşturulur. İnandırıcılığı arttırmak için e-Postada resmi bir dil kullanılır. e-Postadaki bağlantı üzerinden kullanıcının bilgilerini girebileceği farklı bir bağlantıya yönlendirilir. Kullanıcı bağlantıya tıkladığında kullanıcının tüm kart bilgilerinin ve kişisel bilgilerinin girilmesini istenir. Kullanıcı bilgilerini girdiğinde bilgiler bankanın gerçek sistesine değil, doğrudan bilgisayar korsanına iletilir ve oltalama işlemi başarıya ulaşır.

Bu örnek otlama saldırısında kullanıcının bankadan geldiğine inandırıldığı bir posta ile dolandırılmıştır. Kullanıcının kendisine gönderilen bağlantıya tıklamadan önce kimden geldiğini kontrol etmesi ve otlama saldırılarına karşı uyanık olması onu koruyacak en güçlü savunma yöntemi olacaktır.

Sosyal mühendislik saldırıları, doğası gereği hedefe insanı koyduğundan ve senaryoları değişebileceğinden, en önemli koruma yöntemi kişilerin eğitimle bilgilendirilmesidir. Her ne kadar bu bölümde savunma konusu ele alınmasa da, önemine binaen aşağıdaki konulara dikkat edilmesi gerektiği unutulmamalıdır.

- Kullanıcı adı ve parola gibi kişisel bilgiler kimseyle paylaşılmamalıdır.
- Kullanıcı adı ve parola bilgileri erişimin açık olduğu bir yere yazılmamalıdır
- Bilinmeyen kişilerden gelen e-postalar açılmamalıdır.

2.4.5 Uygulama Atakları

SQL enjeksiyonu (injection): Etkileşimli web uygulamaların çoğunda kullanıcılardan bilgi alınır ve bu bilgi veritabanında sorgulanır. Örneğin, bir kullanıcının bir siteye erişiminin olup olmadığını belirlemek için kullanıcıdan kullanıcı adı ve parola gibi bilgiler istenebilir. İstenen bilgi veritabanında SQL sorguları ile araştırılır. SQL enjeksiyonu saldırısı bu noktada kullanılan bir saldırıdır. Yani web uygulamasında kullanılan SQL sorgularının içerisine komut ya da diğer bir SQL kodu enjekte edilmesidir [50]. Saldırgan bu sayede yetkisi dışında yer alan veri tabanındaki tablolara ya da alanlara erişebilir.

SQL enjeksiyonu saldırısının açıklanabilmesi için öncelikle kısaca veritabanında yer alan verilere ilişkin temel SQL sorguları anlaşılmalıdır. Buna göre "siber" isimli veritabanında aşağıdaki gibi tablolar olsun.

Not: Tablolarda parolaların açık bir şekilde kayıt edilmesi bir güvenlik açığıdır. Ancak bu kısımda konunun anlaşılabilmesi için bu durum göz ardı edilmiş ve parolanın açık bir şekilde veritabanına kayıt edildiği farzedilmiştir.

Kisiler Tablosu		
ID	Ad	Soyad
11	Erdal	OZDOGAN
12	Onur	DEMIRKAPI
13	Hakan	VOLKAN

Users Tablosu		
ID	userName	Password
1	erdal	123
2	onur	456
3	hakan	789

Normal bir SQL sorgusunda, Kisiler tablosunda yer alan tüm kullanıcıları listelemek için aşağıdaki gibi bir sorgu kullanılabilir:

```
SELECT * FROM Kisiler;
```

Aynı tabloda yer alan ve ID değeri 12 olan kaydın Ad bilgisini listelemek için aşağıdaki kod yazılabilir:

```
SELECT Ad,Soyad FROM Kisiler WHERE ID= '12';
>Onur, DEMIRKAPI
```

SQL yapısal sorgulama dilinde iki farklı sorgu UNION anahtarı kullanılarak birleştirilebilir.

```
SELECT Ad,Soyad FROM Kisiler WHERE ID='11' UNION SELECT UserName, Password FROM Users;
```

Yukarıdaki gibi bir sorgu satırının sonucunda aşağıdaki gibi bir sonuç listelenir.

```
Erdal, OZDOGAN,
erdal, 123
onur,  456
hakan, 789
```

Bu son sorguda ID bilgisi statik olarak SQL içerisinde doğrudan yazılmıştır. Ancak daha önce de ifade edildiği gibi, web uygulamalarında kullanıcılardan verinin alınıp sorgu satırında dinamik olarak kullanılması mümkündür. Örneğin, php ile aşağıdaki gibi kullanıcıdan gelen bilgi (gID) isimli bir değişkene atandıktan sonra sorgulanabilir.

```
$gID=$_GET['gID'];
$sorgu = "SELECT Ad, Soyad FROM Kisiler WHERE ID='$gID';";
```

Normal şartlarda kullanıcıdan gelen bilgiye göre, ID değerinin girilmesi sonucunda Ad,Soyad bilgisinin görüntülenmesi beklenir. Örneğin kullanıcı php ile tasarlanmış web sayfasında "13" değerini girerse, "Hakan, VOLKAN" kaydı görüntülenecektir. Ancak tehdit aktörü veri giriş alanına diğer bir sorguyu girebilir. Örneğin ilgili alana ' OR '5'= '5 değeri girilebilir. Bu durumda sorgu işletildiğinde aşağıdaki hâle gelecektir. $gID yerine kullanıcıdan girilen değer görüntülenir.

```
SELECT Ad, Soyad FROM Kisiler WHERE ID= '' OR '5'='5';
```

Bu sorgu cümlesine göre, ID değeri boş olduğunda ya da her zaman (çünkü 5 her zaman 5'e eşittir) Ad, Soyad bilgilerini gösterir. Ancak kullanıcı ilgili alana aşağıdaki gibi bir satır da yazabilir.

```
' UNION SELECT userName, Password FROM Users WHERE 'e'='e
```

Bu durumda sorgu aşağıdaki gibi olacaktır;

```
SELECT Ad, Soyad FROM Kisiler WHERE ID= '' UNION SELECT userName, Password FROM Users WHERE 'e'='e';
```

Bu durumda Kisiler tablosundaki ID değeri boş olanlar ve Users tablosundaki **userName** ve **Password** bilgileri alınacaktır. Her ne kadar veritabanlarında parolalar bu örnekte olduğu gibi açıkça yazılmayıp genellikle özetlenmiş (hash) olarak saklansa da, çeşitli yöntemlerle bu parolaların bulunması mümkün olabilir.

Yine SQL enjeksiyonu kullanılarak, hatalı yapılandırılmış bir web sitesinin veri tabanındaki tabloların silinmesi de sağlanabilir. Normalde şartlarda aşağıdaki SQL satırı Users isimli tabloyu silmek için kullanılır.

```
DROP TABLE Users;
```

Yine farzedelim ki kullanıcıdan, web isteği (http Request) ile kullanıcı kimliğini (ID) alıp Kisiler tablosundan sorguladığımız aşağıdaki Python kodları yazılmış olsun.

```
qID = request.args("ID");

sqlSorgu = "SELECT * FROM Kisiler WHERE ID = " + qID;
```

Normal şartlarda kullanıcıdan beklenen davranış "11" gibi bir değer yazmasıdır. Bu durumda çıktı aşağıdaki gibi olacaktır.

```
Erdal, OZDOGAN
```

Ancak saldırgan, bu alana 11 ; DROP Table Kisiler satırlarını yazar. Bu durumda (örneğin tarayıcı tarafından) web isteği yerine getirildiğinde SQL cümlesi aşağıdaki gibi olacaktır.

```
SELECT * FROM Kisiler WHERE ID = 11; DROP TABLE Kisiler;
```

Bu durumda Kişiler tablosundaki ilgili kayıt web tarayıcısında gösterildikten sonra, tablo silme işlemi gerçekleşir. SQL enjeksiyonu ile bu konuda anlatılanlara benzer birçok zararlı işlem saldırgan tarafından yapılabilir.

Not: *Bu bölümde belirtilen kodlamalar, SQL enjeksiyonu saldırısının anlaşılabilmesi için bilinçli olarak hatalı (ya da eksik) yazılmıştır. Uygulama geliştirme esnasında bu kodların zaafiyete neden olduğu unutulmamalıdır.*

xSite Scripting: Cross Site Scripting olarak adlandırılan bu saldırının amacı, zafiyet barındıran web siteler üzerinden, kullanıcının web tarayıcısına JavaScript gibi çalışan kodları ya da html kodları enjekte etmektir. Kullanıcıdan alınan bir girdinin (örneğin, adının, eposta adresinin

alınması gibi) web uygulamasında bir çıktı olarak kullanıldığında bu saldırı gerçekleştirilebilir. Böylece saldırgan içerik üzerinde kontrol sahibi olabilecek ve kullanıcılara saldırabilecektir.

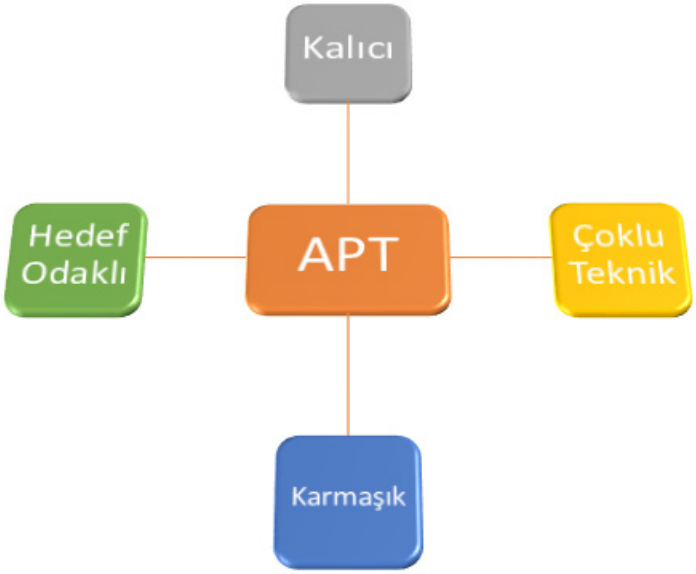
Bu saldırının sonucunda tehdit aktörü, tüm sistemin kontrolünü ele geçirebilir, tarayıcının kontrolünü ele geçirebilir, tarayıcılardan çerezleri (cookies) çalabilir ya da kullanıcının yazdıklarını ele geçirebilir (keylogger).

2.4.6 Gelişmiş Kalıcı Tehditler (APT)

Siber saldırıların içerisinde belki de en zararlı olanlardan biri, Gelişmiş Kalıcı Tehditlerdir (APT - Advanced Persistent Thread). Bu saldırıda, gelişmiş ve çoklu saldırı teknikleri kullanılarak sistemde uzun süreli kalmak ve fark edilmemek esastır. Finansal bilgileri ve fikri mülkiyetleri arayan siber suçlulardan, verileri çalmak ve altyapıyı tehlikeye atmak için tasarlanmış devlet destekli siber saldırılara kadar, günümüzün gelişmiş kalıcı tehditleri siber güvenlik önlemlerinden kaçabilir ve ciddi zararlar verebilir. Yetenekli ve kararlı bir siber suçlu, aylarca tespit edilmeden birden fazla atak vektörü kullanabilir.

Bu saldırıları önleyebilmek için öncelikle saldırı iyi analiz edilmeli ve APT saldırısının nasıl çalıştığı bilinmelidir. APT saldırılarının altı adımı asaăıda belirtilmistir [11].

1. Tehdit aktörü, keşif atakları (reconnaissance attack) yaparak saldırısını özelleştirmek için hedef ağ hakkında bilgiler toplar. Doğrudan önemli bir cihaza erişim yapması önemli değildir. Ağdaki hatalı bir güvenlik duvarı yapılandırmasından ya da herhangi bir cihazdaki zafiyetten faydalanabilir. e-posta, dosya veya uygulamalardaki güvenlik açığı yoluyla cihaza giriş yetkisi kazanır ve ağa zararlı yazılımı (malware)



Şekil 2.18. APT özellikleri

yerleştirir. Gelişmiş zararlı yazılım, olası diğer ağ erişimini ve güvenlik açıklarını bulmaya çalışır. Ayrıca C&C sunucuları ile iletişime geçerek ek talimatlar ya da zararlı kodlar alır.

2. Zararlı yazılım, kalıcılığını sağlamak amacıyla, tespit edildiği bir noktada kapatılsa dahi diğer noktalara da kendisini kurar ve etkinleştirir.
3. Tehdit aktörü, güvenilir ağ erişimi kurduğunu belirlediğinde, hesap bilgileri ve parolalar gibi verileri toplar. Parolalar şifrelenmiş olsa bile şifre çeşitli teknikler ile kırılabilir. Bu işlem gerçekleştiğinde, tehdit aktörü verileri tanımlayabilir ve verilere erişebilir.
4. Zararlı yazılım, verileri geçici bir sunucusunda toplar, ardından verileri ağın dışına ve tehdit aktörünün tam kontrolüne sunar.
5. APT saldırısının izleri sistemden kaldırılır, ancak tehdit devam etmektedir. Siber suçlu istediği zaman tekrar geri dönebilir.

Bu saldırı geleneksel güvenlik yaklaşımları ile kolaylıkla tespit edilemez. Saldırının doğasında olduğu gibi, savunmada da aynı şekilde birden çok tekniği kullanan entegre çözümler kullanmak gerekebilir.

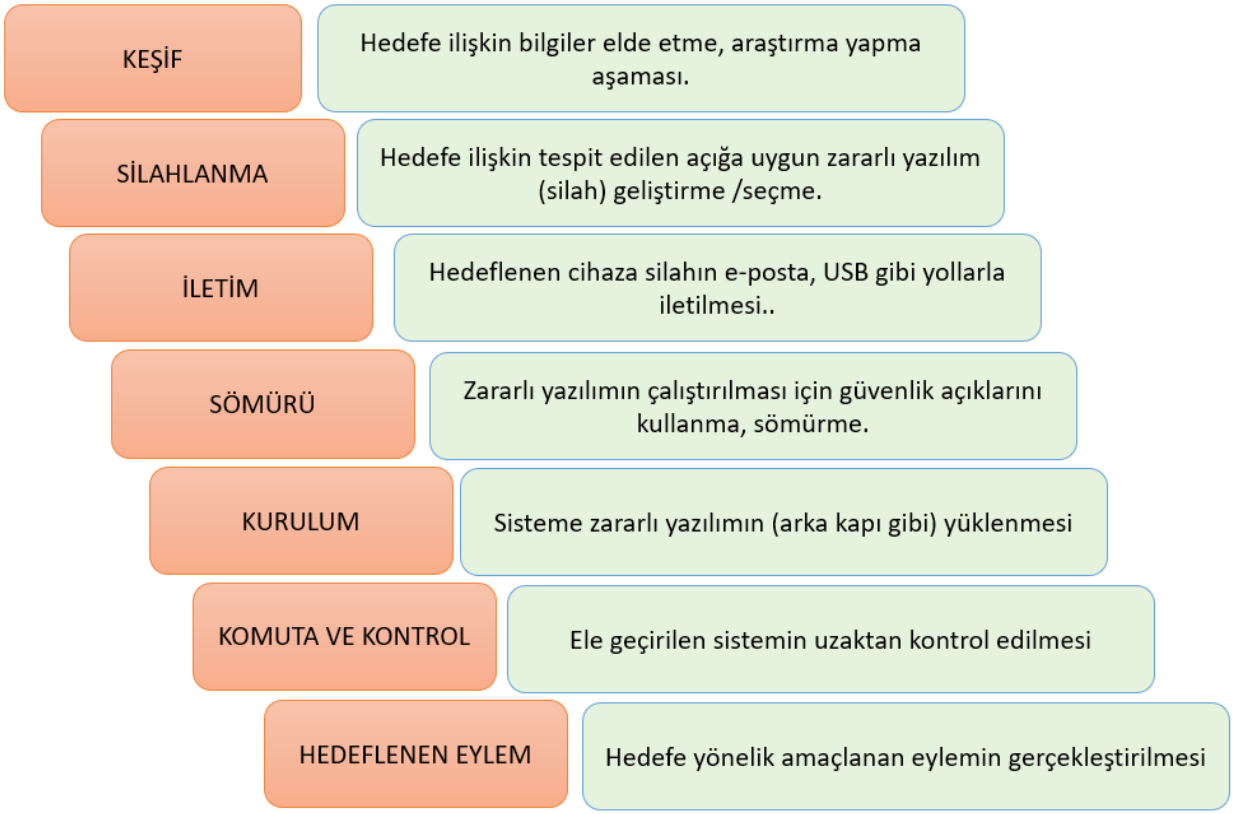
APT saldırılarının belirtileri şunlardır:

- Kullanıcı davranışlarındaki gariplikler, alışılmadık kullanıcı davranışları
- Çok miktarda veri transferi ya da veri tabanı hareketliliği
- Birden çok arka kapı ve truva atının varlığı
- Bilinmeyen, alışık olunmayan dosya ve dosya türleri

2.4.7 Siber Ölüm Zinciri (Cyber Kill Chain)

APT gibi gelişmiş saldırılar, ciddi bir hazırlık ve planlama gerektiren, aşamalı üst düzey saldırılardır. Uluslararası bir savunma şirketi olan Lockheed Martin, bu tür saldırıların tanımlanmasındaki aşamaları ve her aşamadaki işleyişi açıklayan bir model geliştirmiştir. ***Siber Ölüm Zinciri*** olarak adlandırılan yedi aşamalı bu model, saldırının doğru anlaşılmasını sağlayan ve buna bağlı olarak savunmayı aşamalı olarak ele alan bir modeldir. Bu aşamalara odaklanmak, tehdit aktörlerinin tekniklerini, araçlarını ve yöntemlerini anlamayı sağlar. Saldırının başarılı olarak gerçekleşmesi, bu aşamaların her birinin farkedilmeden tamamlanmasına bağlıdır. Her aşamanın

da kendine özgü belirtileri olacaktır. Belirtilere göre alınacak aksiyonlara göre saldırının önlenmesi, zincirin kırılması mümkündür. Saldırının erken aşamada önlenmesi, verilecek zararın daha hafif olmasını sağlayacaktır. Siber Ölüm Zincirinin aşamaları Şekil 2.9'da gösterilmiştir.



Şekil 2.19. Ölüm zinciri aşamaları

Keşif (Reconnaissance) aşaması, hedef ağa, sistemde ya da kullanıcıya ilişkin araştırmaların yapıldığı ve bilgilerin toplandığı aşamadır. Bilgi toplama için hemen her fırsat değerlendirilir. Sosyal medya, aktif ve pasif bilgi toplama araçları, sosyal mühendislik yöntemleri, kurumsal web sayfaları gibi kaynaklar kullanılabilir. Keşif aşamasında en savunmasız ya da en çok ihmal edilen sistemler

(veya kullanıcılar) hedef olarak belirlenebilir. Bu ilk hedef, daha değerli başka bir hedefe ulaşmak için aracı olarak da kullanılabilir.

Silahlanma (weaponization), keşif aşamasındaki zayıf noktası bulunduktan sonra, hangi atak vektörünün kullanılacağının belirlendiği aşamadır. Bu aşamada, oltalama, yemleme kancası, truva atı gibi araçlar veya yöntemler kullanılabilir. Silahlanmada amaç, keşiften elde edilen bilgileri, belirli sistemlere veya bireylere karşı bir silah geliştirmek üzere kullanmaktır. Bu silahı geliştirmek için tespit edilen güvenlik açıkları kullanılır. Tehdit aktörü, sistemdeki diğer zaafiyetleri ortaya çıkarmak, diğer sistemler üzerinde kontrol sağlamak ya da ek saldırılar uygulamak için ağı daha ayrıntılı olarak inceleyecektir. Her detaylı inceleme, daha özellikli bir silahın ortaya çıkmasını sağlayacaktır. Silahlanma aşamasında kullanılabilecek, çoğu önceden denenmiş birçok araç ve yöntem vardır. Ancak bu yöntemler tehdit aktörü tarafından bilindiği gibi, güvenlik uzmanı tarafından da bilinecektir. Bu nedenle, iyi yapılandırılmış bir saldırıda olduğu gibi (stuxnet örneği), tespit edilmemek amacıyla, genellikle **sıfırıncı-gün saldırıları** (zero-day attack) kullanılır. Sıfırıncı gün saldırıları (ya da güvenlik açıkları) henüz savunma unsurları tarafından tespit edilemeyen, yeni saldırılar ya da zaafiyetlerdir.

Silahlanma aşamasında geliştirilen saldırı aracının hedef sisteme iletimi, teslimat (delivery) ya da **iletim aşamasında** gerçekleşir. Bu aşamada web sayfaları, taşınabilir USB bellekler ya da e-posta ekleri kullanılarak "silah" hedef sisteme iletilir. Saldırgan, iletilen bu zararlı yükün **(payload)** güvenlik sistemleri tarafından tespitini önlemek için, şifreleme gibi mekanizmalar kullanabilir. Yine zararsız bir ağ trafiği gibi görünen (ya da meşru ağ trafiğine gizlice gömülen) sızma teknikleri de kullanılabilir.

Sömürü (veya İstismar) aşamasında, bir önceki adımda iletilen "silah" kullanılarak, hedef sistemdeki zaafiyet istismar edilerek (sömürü - **exploit)**, hedef üzerinde kontrol sağlanması amaçlanır. İşletim sistemlerindeki zaafiyetler, uygulamalardaki zaafiyetler ya da (en zayıf halka) kullanıcıdaki zaafiyetler bu aşamanın potansiyel hedefleridir.

Kurulum aşamasında, hedef sisteme uzaktan kontrol olanağı sunan arka kapılar kurulur. Bu sayede sistemde daha uzun vadeli kalınması ve doğru zaman için beklenmesi sağlanabilir.

Komut ve kontrol aşamasında, hedef sistemde komut ve kontrol (C&C ya da CnC) kanallarının kurulması amaçlanır. Bu kanallar, saldırgan tarafından hedefe yüklenen zararlı yazılımlara uzaktan komut gönderme olanağı sunar.

Siber Ölüm Zincirinin son aşaması, hedeflenen saldırının gerçekleşmesi olan **hedeflenen eylem** aşamasıdır. Bu aşamaya kadar gelen (zinciri kırılmamış) bir saldırı, hizmet reddi, veri hırsızlığı gibi hedeflenen eylemi gerçekleştirecektir.

2.4.8 Siber Saldırı Vektörleri ve Saldırı Yüzeyleri

Önceki bölümlerde görüldüğü gibi, tehdit aktörlerinin kullanabileceği birçok farklı ihlal yöntemi bulunmaktadır. **Saldırı yüzeyi**, tehdit aktörü gibi yetkisiz bir kullanıcının bir ortama veri girmeye veya bir ortamdan veri çıkarmaya çalışabileceği farklı noktaların toplamıdır. Her bir nokta, **bir atak (saldırı) vektörüdür** [8]. Bu atak yüzeyini en küçüklemek (minimize etmek), yani hedef küçültmek en temel siber güvenlik (hatta temel savunma) ilkelerindendir.

Siber güvenlik uzayında, tehdit unsurunun kullanabileceği yüzden fazla atak vektörü bulunmaktadır. En yaygın olanlar aşağıda belirtilmiştir [14].

- Güvenliği ihlal edilmiş kimlik bilgileri
- Zayıf / çalınmış parolalar
- Kötü niyetli dâhili çalışanlar (kullanıcılar)
- Zayıf ya da eksik şifreleme
- Hatalı cihaz yapılandırması
- Fidye Yazılımları
- Oltalama
- Güven ilişkileri
- Sıfırıncı-gün zafiyetleri
- Deneme-Yanılma Saldırısı
- DDoS

2.5 SİBER SAVAŞ ÖRNEKLERİ

Dünya üzerine internet teknolojisinin gelişmesine bağlı olarak siber saldırı türleri ve sayısı artmaktadır. Kişisel, kurumsal veya ülkelerin işleyişini aksatmak, bozmak ve/veya yıkıcı hasarlar vermek sebepleri ile siber saldırılar yapılmaktadır. Ülkelerin bütünlüklerine ve erişilebilirliklerine yönelik saldırılar daha organize olup bütün etkileri barındırmaktadır. Bu saldırılardan bazıları aşağıda anlatılmıştır.

Şekil 2.20. Siber savaş

Estonya'ya yapılan Siber Saldırı

Rusya'da bulunan bilgisayar korsan gruplarının Estonya'ya yapmış oldukları bir siber saldırıdır [30]. 27 Nisan 2007 tarihinde başlayan bu siber saldırı 18 Mayıs 2007 tarihine kadar devam etmiştir. Bu siber saldırıda kamu hedef alınmış ve bu süre zarfında Estonya'nın bankacılık sistemleri ile haberleşme sistemleri hizmet veremez hale getirilmiştir. Dünyada bir devletin başka bir devlete karşı yaptığı ilk siber saldırı olarak bilinmektedir.

Siber saldırının sebebi Tallinn'de bulunan "Asker Heykeli" olarak gösterilmiştir. 2. Dünya savaşı sırasında ölen Sovyet askerlerini temsil eden bu heykelin sökülmek istenmesi nedeniyle karşı karşıya gelen bürokrasi nedeniyle Estonya, Rusya tarafından hedef alınmıştır. Bu siber saldırı soruncunda Estonya'nın en büyük iki bankası ve 2 iletişim-haberleşme kurumu hizmet veremeyecek duruma gelmiştir.

Rusya'da bulunan saldırganları Distributed Denial of Service (DDos) olarak bilinen bir siber saldırı tekniğini kullanmıştır. Bu saldırı türünde önce çok fazla sayıda bilgisayarı komuta etmek isteyen saldırgan grubu, önce dünya üzerinde çok sayıda bilgisayarın kontrolünü ele geçirmiş, daha sonra bu bilgisayarları kontrol ederek (Botnet) saldırı aracı olarak kullanmıştır. Saniyede 4 milyon civarında bir veri paket gönderen bu bilgisayarlar, ülkenin bankacılık ve iletişim faaliyeti yürüten kurumlarını çalışamaz hale getirmiştir.

Estonyalı yetkililer bu saldırıları, saldırı arasında incelemiş ve çoğu saldırının Rus kamu kurumlarından yapıldığını tespit ettiklerini bildirmiştir.

Estonya dünya üzerinde e-devlet hizmetleri açısından önemli çalışmalar yürüten ve bu hizmetleri ilk uygulayan ülkelerden biridir. E-devlet hizmetlerine yönelik yapılan ilk siber saldırı ile Estonya, 2008 yılında Cooperative Cyber Defense Center of Excellence (CCD-COE) adında siber güvenlik mükemmeliyet merkezini kurmuştur.

İran'a Yapılan Siber Saldırı

İran'ın uranyum zenginleştirerek nükleer enerji üretmesinin engellenmesi amaçlanarak yapılan bir siber saldırıdır. Saldırı 2009 yılının Şubat ayında başlamasına rağmen, 2010 yılının Mayıs ayına kadar uzanan bir sürece yayılmıştır.

Saldırı Stuxnet adına bir virüsün kullanılmasıyla gerçekleştirilmiştir. Stuxnet bilgisayar virüsü olarak bilinse de, aslında uzaktaki bir bilgisayar sistemine sızması ve kontrol altına alınması için tasarlanmış bir programdır. Stuxnet, o zamana kadar bilinen bir açığı kullanmadığından dolayı "zero-day" yani sıfırıncı gün adı verilen bir saldırı türüdür. Stuxnet, sisteme yüklendiği andan itibaren, nükleer tesiste içinde uranyum zenginleştirilen santrifüjlerin dönüş hızlarını sabote etmiştir. Dönüş hızı etkilenen santrifüjlerin kullanım ömürlerini azalmış ve uranyum zenginleştirme sürecine olumsuz etki sağlamıştır. Bunu yaparken, nükleer santralde kullanılan SCADA (Supervisory Control and Data Acquisition) sistemlerinin ekranlarına, daha önceden almış olduğu 21 saniyelik ekran görüntüsünü ard arda gösterilmiş ve İranlı kontrol mühendislerini yanıltmayı başarmıştır. Bu görüntülere bakarak sorunu tespit edemeyen mühendislerden dolayı, santrifüjlerin dönüş hızlarını artırıp azaltarak santrifüjleri ömürlerini azaltmıştır [31].

Virüs üzerinde çalışan uzmanlar, saldırının hedefinin nükleer tesiste kullanılan Alman Siemens şirketi tarafından üretilmiş olan 'Simatic WinCC Step7' isimli denetleme kontrol ve veri toplama sistemi (SCADA) adlı program olduğunu tespit etmişlerdir. SCADA, enerji üretim ve dağıtımının kontrolü gibi kritik altyapıların kontrol edilmesinde kullanılan Siemens şirketinin programıdır. SCADA sisteminin internet üzerinden bir ağ bağlantısına sahip olmadığı dikkate alındığında, virüsün bir USB bellek ile bulaştırılmış olma ihtimali çok yüksek olduğunu düşünülmekte ve daha sonra yapılan araştırmalarda bu konu kesin gibi görünmektedir.

Ukrayna'ya Yapılan Siber Saldırı

Ukranya'ya yapılan siber saldırı Estonya'da olduğu gibi Rusya merkezli olduğu iddaa edilmektedir. Genel olarak hizmet sektörü hedef alınmış ve bankacılık işlemleri yapılamaz hale getirilmiştir. Bununla beraber enerji sektörünü de hedefe alınmış ve ülkenin bir bölümüne elektrik verilememiştir. Bu saldırıların altında ilk defa mobil cihazların aktif olarak kullanıldığı belirlenmiştir. Mobil cihazların bu denli etkili olarak hizmeti durdurma noktasına getirdiği ilk siber saldırı olarak nitelendirilmiştir.

Ayrıca Cernobil nükleer santrale ait radyasyon ölçümlerin internet üzerinden yapılamadığı bu sebeple gerekli ölçümlerin manuel olarak yapılmıştır. Rusya tarafından yapıldığı düşünülen siber saldırılar ile kamu kurumlarındaki bilgisayar sistemlerinin çalışmadığı, sosyal medyanın engellendiği rapor edilmiştir.

BÖLÜM 3

GÜVENLİK STRATEJİLERİ ve KORUNMA

Siber saldırılara, tehditlere ve zararlı yazılımlara karşı savunma yapabilmek ya da koruma stratejileri geliştirebilmek için, tehdit aktörlerinin yöntemlerini, tekniklerini, ağın işleyişini ve yapısını bilmeyi gerektirir. Daha önceki bölümlerde ele alındığı gibi, saldırının ilk aşaması keşif aşamasıdır. Saldırgan bu aşamada hedefe ilişkin bilgi toplamaktadır. Siber güvenlik uzmanının da bu bilgi toplama yöntemlerini bilmesi, güvenlik stratejileri oluşturmada ve korunma aşamaları tasarlamalarında yararlı olacaktır. Bu bölümde, bilgi toplama yöntemleri, bilgi toplama araçları, temel güvenlik önlemleri ve stratejileri ele alınmıştır.

3.1 SİBER GÜVENLİKTE BİLGİ TOPLAMA

Siber güvenlik dünyasında gerek saldırı için olsun, gerek savunma için olsun bilgi toplama ihtiyacı vardır. Bilgi toplama yöntemleri, Pasif Bilgi Toplama ve Aktif Bilgi Toplama olarak iki başlık altında ele alınabilir.

3.1.1 Pasif Bilgi Toplama

Pasif bilgi toplama sürecinde, bilgi alınmak istenen ağ ya da sistem ile doğrudan bir etkileşim bulunmaz. Elde edilen bilgi, doğrudan sistemden değil internet kaynaklarından elde edilir. Bu bilgi toplama yöntemlerinde şunlar yapılabilir.

- IP Adresleri Hakkında Bilgi Toplama
- Domainler Hakkında Bilgi Toplama
- Web Sayfalarında Bilgi Toplama

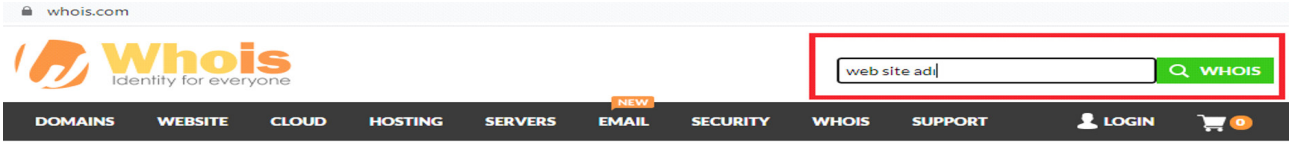
IP Adresleri Hakkında Bilgi Toplama

IP adreslerinin dünyadaki dağıtım merkezi ICANN (Internet Corporation for Assigned Names and Numbers)'dır. Bu kâr amacı gütmeyen kurum, İnternet adresi alanı tahsisi, protokol ataması ve ülke kodu (.tr, .de, .se gibi) internet alan adı yönetiminden sorumludur. Bir IP adresi sorgusunu en kısa yoldan Whois Sorgusu ile yapılmaktadır.

Whois Sorgusu

Whois sorgusu, sorgu yapılan alan adı ile bazı bilgilere ulaşmayı hedefler. Alan adı sahibi kişiye ait iletişim bilgileri ve alan adı ile ilgili teknik bilgiler yasal çerçevede (ICANN) listelenir.

Whois sorgusununu herkes yapabilir yani herkes ulaşabilir. Ancak alan adı sahibi kendisine ait bilgilerin Who is sorgusu sırasında listenmesini istemeyebilir. Bunun için Whois Gizleme servisinin aktif edilmesi gerekmektedir. Bu sayede, ICANN verileri gizleyip başka kişiler ile paylaşmayacaktır.

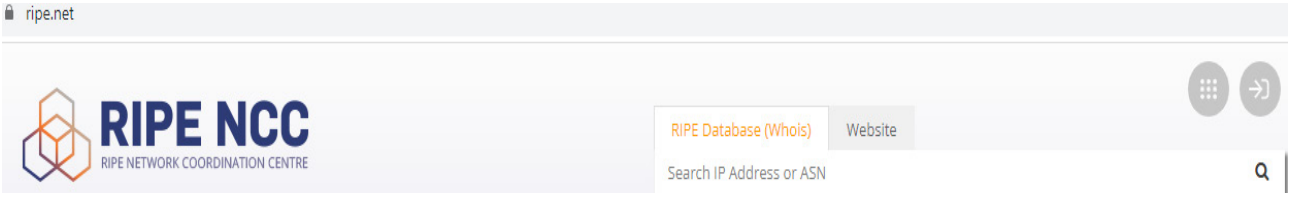


Şekil 3.1. Whois web sitesi ve arama işlemi

http://www.whois.com/ internet adresine bilgi edinmek istenilen alan adı yazıldığında (örnek: www.meb.gov.tr) Şekil 3.2'deki ekran görünmektedir [24].

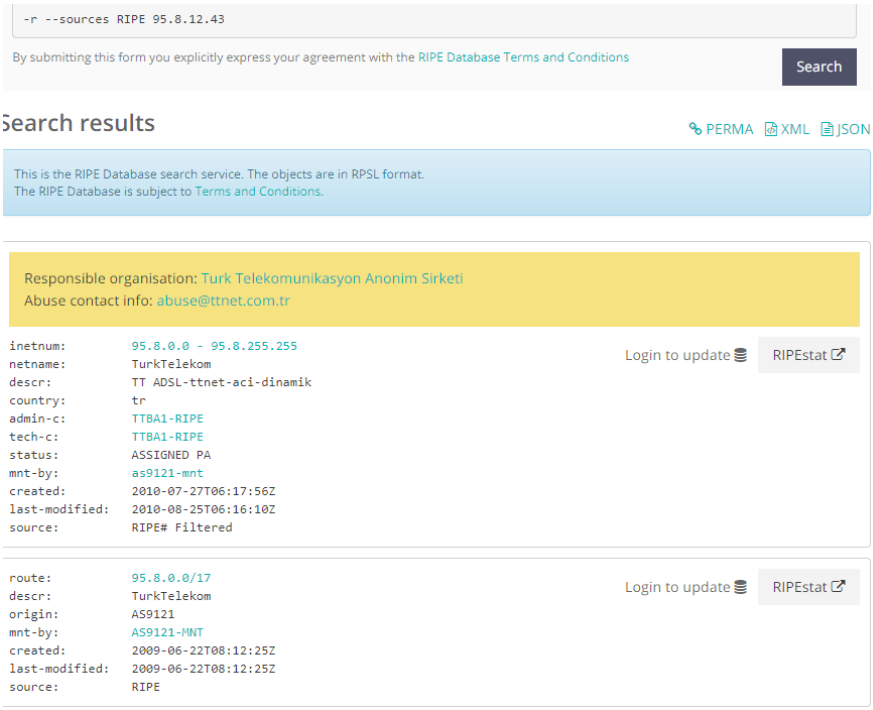
Şekil 3.2. Örnek Whois sorgusu

RIPE Üzerinden IP Sorgulama



Şekil 3.3. RIPE NCC sayfası

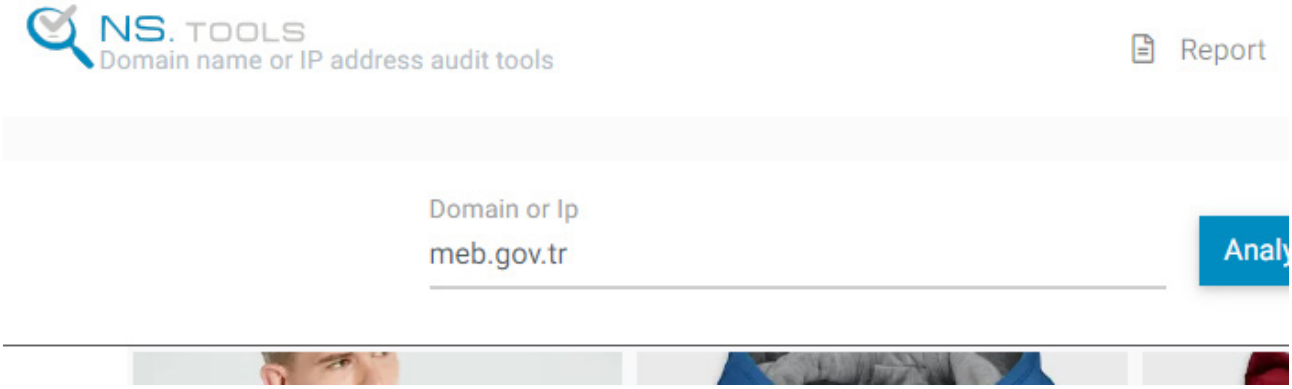
RIPE NCC, IANA kuruluşuna bağlı olan, Avrupa ve Ortadoğu bölgesi gibi bir bölgeye IP adresi dağıtımından sorumlu olan bir kuruluştur [25]. Bu kuruluşa https://www.ripe.net/ internet adresinden erişlebilir. Belirtilen bölgede yer alan IP adreslerine ilişkin pasif bilgi sorgulaması yapılabilir. İlgili web sayfasında sorgulanmak istenen IP adresi yazılarak sorgulama yapılabilir. Şekil 3.4'te yer alan ekran görüntüsünde örnek bir sorgulama yapılmıştır.



Şekil 3.4. Örnek sorgulama

Site Durumunu öğrenme

https://ns.tools/ web istesi, bir web sayfanın aktif mi yoksa pasif mi olduğunu öğrenmek için ping işlemi uygular. Bu yöntemle web sitesinin işlevsel ve aktif olup olmadığı öğrenebilir. Ayrıca bu web sitesi ile ilgili daha farklı bilgiler de toplanabilir [26].



*Şekil 3.5.*ns.tools site sorgulama

Alan Adları Hakkında Bilgi Toplama: Etki alan adları olarak da adlandırılan domain adları, genellikle web sitelerine IP numaraları yerine, hatırlaması daha kolay olan isim yazarak erişmek için kullanılan bir sistemdir. İnternet ortamında cihazların iletişiminde nümerik IP adresleri kullanılır. Ancak kullanıcılar erişmek istedikleri web sayfaları ya da herhangi bir kaynağın IP adresini akılda tutması güç olabilir. Bu nedenle belirli kurallar dâhilinde, benzersiz alan isimleri kullanılır.

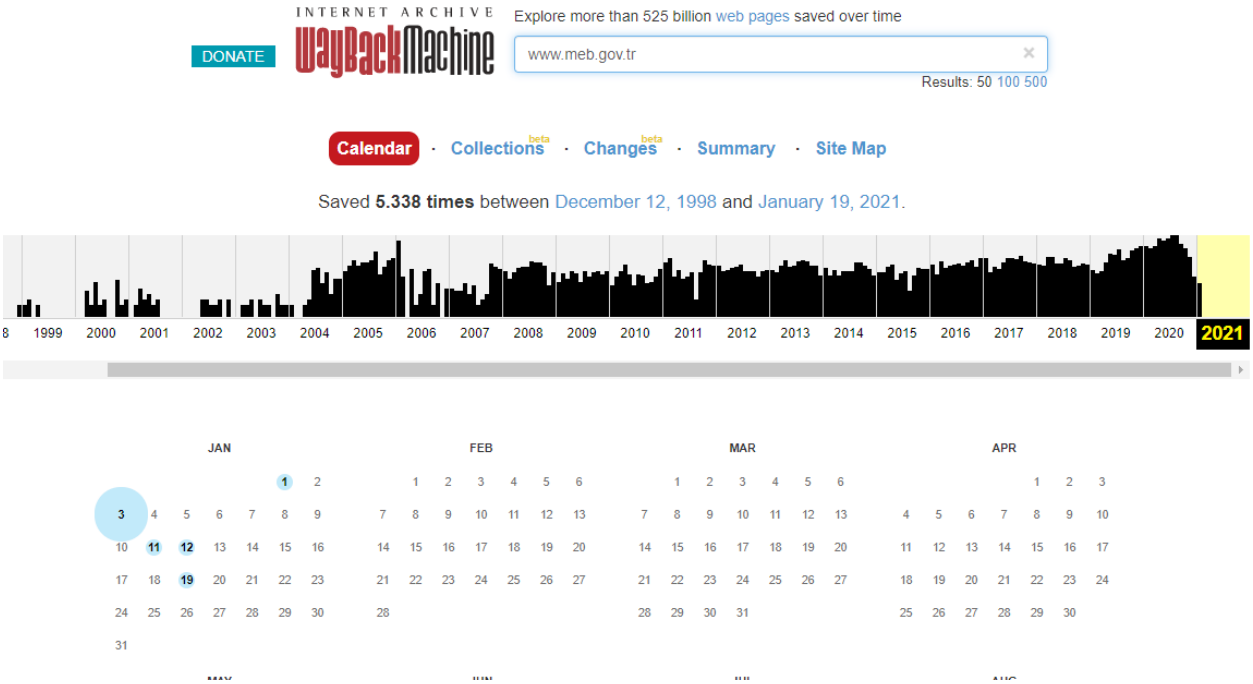
Alan adı isimlendirmesi, daha önce bahsedilen DNS sistemi ile ilişkilidir. Belirli bir web sitesine ilişkin bu benzersiz alan adları hakkında bilgi toplamak için isim sorgulaması yapılabilir. Alan adlarının kullanımda olup olmadığı ya da var olup olmadığına ilişkin bilgilere erişmek için domain sorgulama sistemleri kullanılabilir [28].

Web Sayfalarında Bilgi Toplama

- Archive.org
- Netcraft.com
- Pipl.com

Archive.org : İnternet ortamında yıllar boyunca devasa sayıda web sayfaları yayına girer ve bazen çeşitli nedenlerle kapanabilir. Archive.org sayfası, 1996 yılından itibaren web sitelerinin görüntülerini indeksleyen oldukça yararlı bir web sayfasıdır. Yayından kaldırılan ya da günümüzde var olmayanların yanı sıra, günümüzde var olan sitelerin de eski görüntülerine erişmek mümkündür.

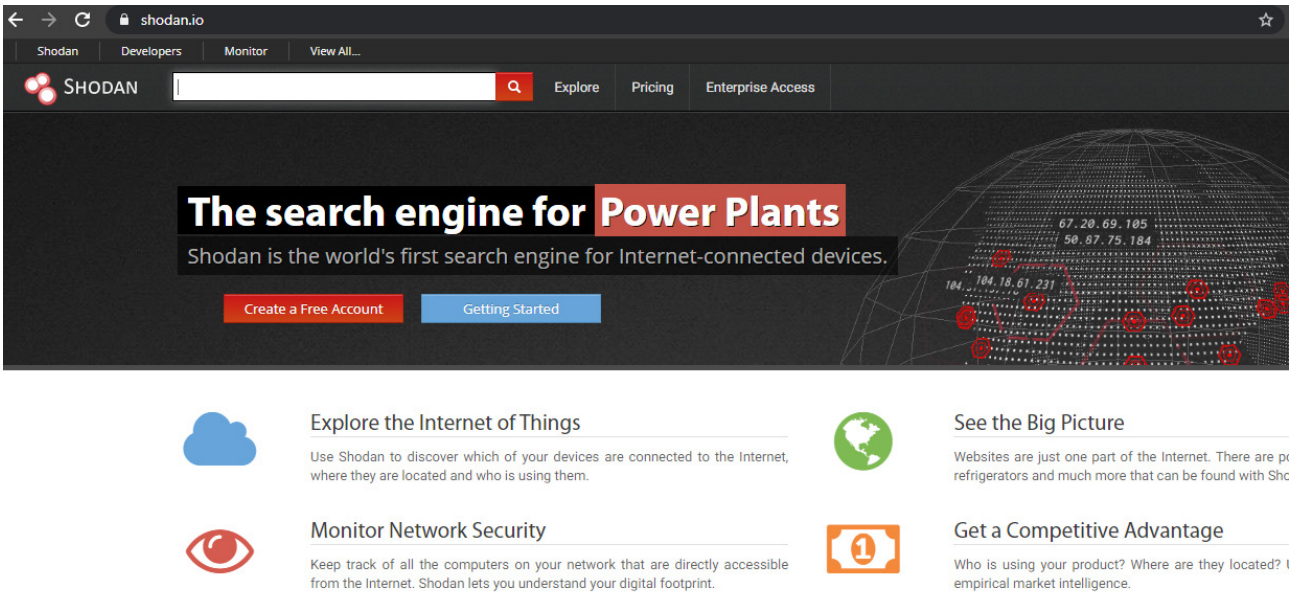
İlgili sayfada sorgulanmak istenen web sitenin adresi yazılır. Arama ("Search") alanına sorgulanmak istenen site adresi yazılır ve "Go" tuşuna basılır. Şekil 3.6'da örnek bir ekran görüntüsü yer almaktadır [27].



Şekil 3.6. Örnek web arşivleme ekranı

Açılan takvimden, (indexlenmişse) istenilen bir tarihe ait sayfanın görüntüsüne ulaşılabilir.

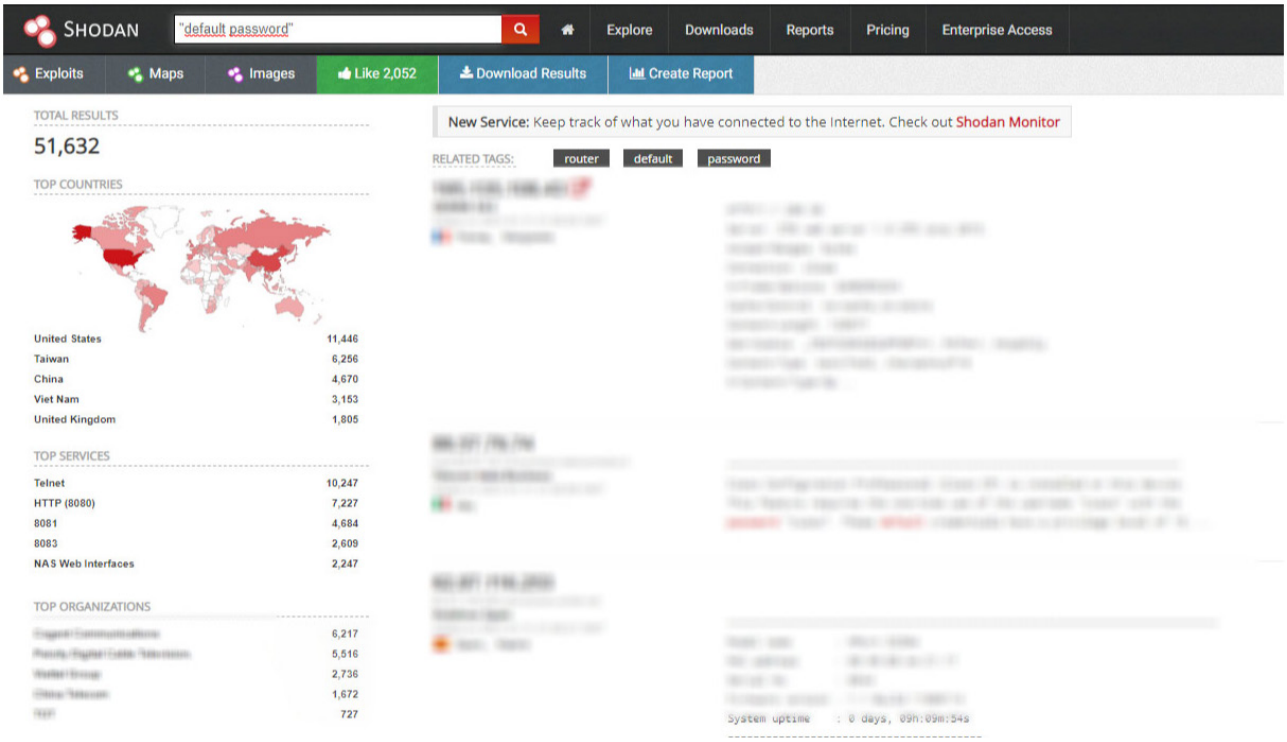
Shodan Kullanarak Bilgi Toplama: Shodan, çeşitli filtreler kullanarak internete bağlı bilgi işlem cihaz türlerini bulmayı sağlayan www.shodan.io sayfasından hizmet veren bir arama motorudur.



Şekil 3.7. Shodan ana sayfası

Shodan, internete bağlı cihazları aramak için interneti sürekli olarak tarayan dünya çapına yayılmış sunuculara sahiptir. Web kameraları, varsayılan parola kullanan cihazlar, yönlendiriciler ve IoT cihazları gibi birçok cihazın bulunmasını sağlayabilir. Hangi cihazların bağlı olduğu, nereye bağlı oldukları ve hangi servislerin güvenlik açığı içerdiği ile ilgili olarak veri madenciliği yapmak amacıyla kullanılabilir.

Shodan ekranında görüntülenen tüm cihazlar, güvenlik açığı içeren sistemler değildir. Ancak bazı güvenlik açığı barındıran sistemlerin de tespit edilebilmesi mümkün olabilir. Örneğin, varsayılan parola kullanan sistemlerin tespit edilebilmesi için arama alanına **"default password"** yazınız.



Şekil 3.8. Örnek Shodan sorgusu

Şekil 3.8'deki Shodan ekran görüntüsünde varsayılan parolayı kullanan sistemlere ilişkin bilgiler gösterilmektedir. Shodan aramasında, filtreleme parametreleri de kullanılabilir. Shodan ile kullanılabilecek bazı filtreler şunlardır:

- **city:** Belirli bir şehirde arama yapar
- **country:** Belirli bir ülkede arama yapar
- **os:** işletim sistemine göre arama yapar
- **port:** Açık olan TCP/UDP portlarına göre arama yapar
- **product:** Belirli bir ürüne göre arama yapılır.

Örneğin, Amerika Birleşik Devletlerinde SNMP hizmeti açık olan Cisco 7200 yönlendiricileri görmek için arama kutusuna;

```
country:US product:"Cisco 7200 Router" port:161
```

yazılabilir.

Siber güvenlik kapsamında yapılabilecek diğer bir Shodan araması da, ileriki bölümlerde ele alınacak olan **CVE** güvenlik zaafiyeti numarasına göre arama yapmaktır. Ancak bu tür bir arama sadece lisanslı ve akademik kullanıma açıktır.

Not: *Bu bölümde yapılan aramalar ve anlatılan konular eğitim amaçlıdır. Lütfen yasal olmayan durumlara karşı dikkatli olunuz.*

3.1.2 Aktif Bilgi Toplama

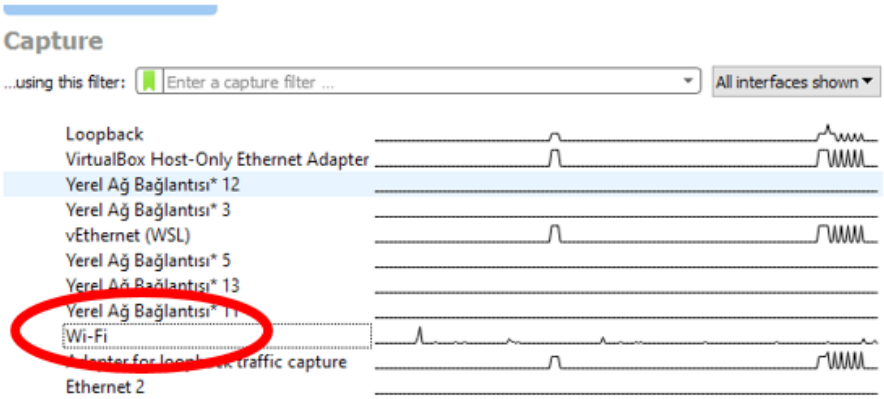
Bu bilgi toplama yönteminde hedef sistem ile doğrudan iletişime geçirilir. Saldırgan açısından riskli bilgi toplama yöntemidir ve çok dikkatli olunması gerekmektedir. Yakalanma olasılığı her zaman mevcuttur. Bir siber güvenlik uzmanının da savunma amaçlı olarak bu aktif bilgi tekniklerini bilmesi gerekmektedir.

Network Maping : Network mapper, en yaygın bilinen şekliyle bilgisayarın açık olan bağlantı noktalarını, parmak izini, kullanılan servislerin isim ve versiyon numaralarını bulmaya yarayan bir araçtır. NMAP, daha önceki konularda ele alınan çeşitli ağ protokolleri aracılığıyla veri toplamayı sağlayan yararlı bir araçtır. Ağda yer alan konaklara ICMP gibi paketler gönderilerek sorgulamalar yapılır ve cihazlardan gelen cevaplar incelenir. Gelen cevaplardaki bilgilerdeki doğrudan bilgilere ya da ipuçlarına göre ağda keşif işlemleri yapılabilir, aktif olarak bilgi alınabilir.

Nmap, ağ haritalaması üzerine odaklanmış bir araçtır. Bu sayede incelenmek istenen bir ağda bulunan cihazların, kullanılan işletim sistemlerinin ve açık bulunan servis ve bağlantı noktası bilgileri tespit edilebilir. Bu bilgilerin elde edilebilmesi için sadece hedef bilgisayar sistemine ait web adresini veya IP adresini bilmek ve Nmap'i kullanmak yeterlidir. Örneğin bir IP'nin bulnduğu ağın haritasının çıkarılması için ;

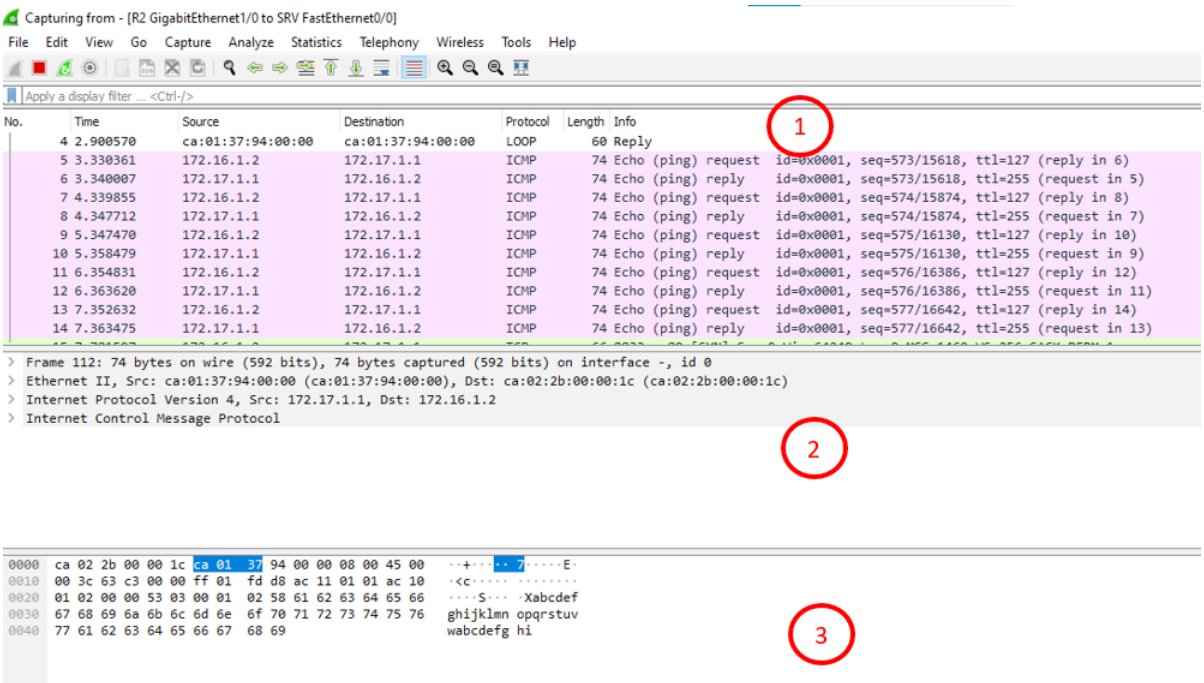
"nmap IP_adresi" yazmak yeterlidir. Bu komut ile o IP adresindeki bilgisayarın bilinen bağlantı noktalarına SYN taraması gerçekleştirir. Bağlantı noktaları, bir sistemde çalışan hizmetler ve uygulamalar ilişkili bir kavramdır. Hedefe ilişkin SYN taraması yapmak, TCP protokolünün SYN bayrağını kullanarak açık hizmetlerin bulunmasını sağlamaktadır.

WireShark ile Bilgi Toplama: WireShark, ağ ortamında paketlerin yakalanmasını ve analiz edimesini sağlayan ücretsiz ve en popüler protokol analiz ve paket yakalama aracıdır. Bu yararlı yazılım https://www.wireshark.org/ sayfasından indirilebilir [49].



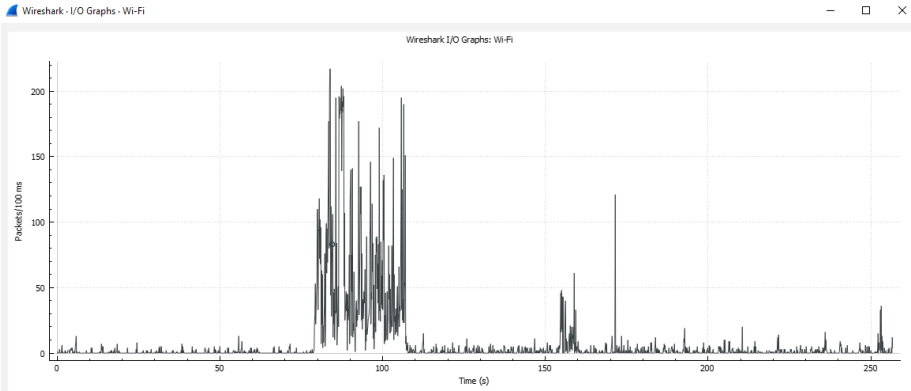
Şekil 3.9. Wireshark dinlenecek arayüz seçme

Yazılım çalıştırılırken ilk olarak paketin yakalanacağı arayüz (NIC) seçilir. Arayüz seçiminin ardından, Şekil 3.10'daki gibi bir ekran görüntüsü gelir.



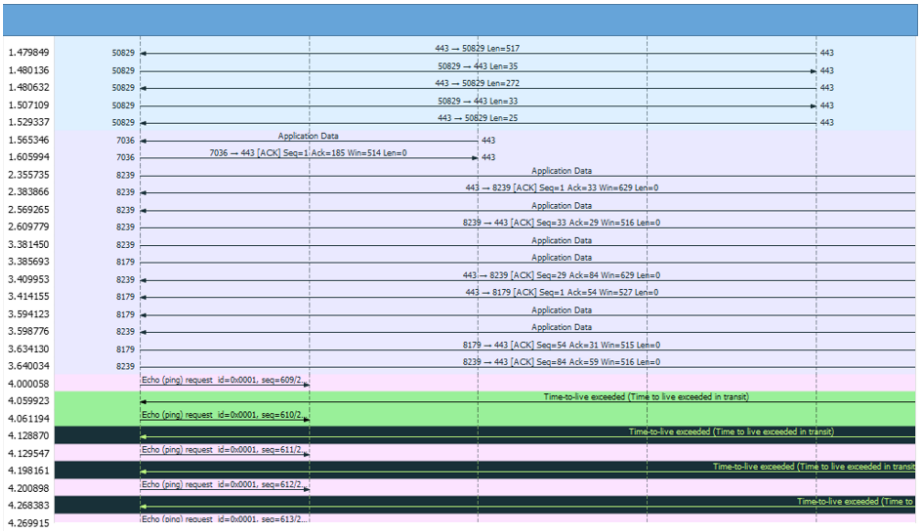
Şekil 3.10. Wireshark yazılımı

WireShark ekranı üç ana bölümden oluşur. İlk bölümde zamana göre yakalanan paketler yer almaktadır. İkinci bölümde yakalanan bu paketin katmanlı yapıdaki içerikleri, üçüncü bölümde ise paketin içerdiği veriler kodlanmış olarak görüntülenmektedir.



Şekil 3.11. Wireshark istatistiksel analiz ekranı

Yakalanan paketlerin tek tek incelenmesinin yanı sıra, ağ ortamı hakkında genel ağ kullanımı, en fazla iletişim kuran IP'ler, TCP veri akışı gibi istatistiksel ve görsel bilgiler de sunmaktadır.



Şekil 3.12. Wireshark iletişiminin görselleştirilmesi

3.1.3 Google Hack Veritabanı ile Veri Toplama

Google internette en yaygın kullanılan arama motorudur. Siber güvenlik dünyasında bilgi toplamada, Google arama motorunun sağladığı anahtar kelimeler ile detaylı bilgi toplama yapılabilir. Arama motorunun indeksleme becerisi, zararlı olabilecek birçok kritik bilginin de indekslenmesine neden olmuştur. Google Hack Veritabanı, https://www.exploit-db.com/google-hacking-database bağlantısından erişilebilen Google sorgularının listesini içeren bir indeksleme veritabanıdır.

Google Hacking Database

Filters | Reset A

Show 15 | Quick Search

Date Added	Dork	Category	Author
2021-01-15	inurl:/config/device/wcd	Web Server Detection	Javier Bernardo
2021-01-15	site:p2.*.* intitle:"login"	Pages Containing Login Portals	Reza Abasi
2021-01-15	inurl:/Jview "zoom"	Various Online Devices	Sanu Jose M
2021-01-07	intitle:Login intext:HIKVISION inurl:login.asp?	Pages Containing Login Portals	Nicholas Doropoulos
2021-01-07	inurl:"/phpmyadmin/user_password.php	Web Server Detection	Mukul Trivedi
2021-01-07	inurl:authorization.ping	Pages Containing Login Portals	Sunil Singh
2021-01-07	inurl:weblogin intitle:("USG20-VPN"|"USG20W-VPN"|USG40|USG40W|USG60|USG60W|USG110|USG210|USG310|USG1100|USG1900|USG2200|"ZyWALL110"|"ZyWALL310"|"ZyWALL1100"|ATP100|ATP100W|ATP200|ATP500|ATP700|ATP800|VPN50|VPN100|VPN300|VPN000|"FLEX")	Pages Containing Login Portals	Javier Bernardo
2021-01-07	inurl:https://trello.com AND intext:@gmail.com AND intext:password	Files Containing Juicy Info	Rushabh Doshi
2021-01-07	intitle:"index of" intext:"apikey.txt	Files Containing Juicy Info	Mohammed Saneem

Şekil 3.13. Google Hack Veritabanı

Örneğin, bir web sunucusunun parmak izi, Google üzerinden Apache çevrimiçi dokümantasyonu veya IIS tarafından web kök dizinine eklenen özel bir klasör için sorgulama yapılaması mümkündür.

```
intitle:"Apache HTTP Server" intitle:"documentation" site: hedefsite.abc
```

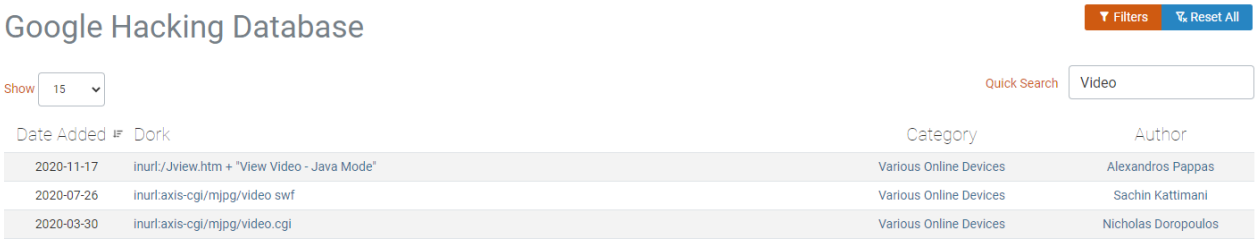
Bunun için belirli bir siteye yönelik (hedefsite.abc) yukarıdaki sorgulama cümlesi yazılarak, google'ın indekslediği verilerden özelleştirme yapılabilir.

Diğer bir örnek de, dosya türüne göre belirli bir sitede arama yapmaktır. Buna göre hedefsite için bak dosyalarının tespitine yönelik olarak aşağıdaki gibi bir sorgulama yapılabilir.

```
filetype:"bak" site:hedefsite.abc
```

Görüleceği üzere, Google hack veritabanı kullanılarak, kullanıcı adı & parolalar, kritik bilgiler içeren hata mesajları ve güvenlik zafiyetleri bulunabilir. İlgili veritabanında yer alan güncel sorgular kullanılarak bilgiler toplanabilir.

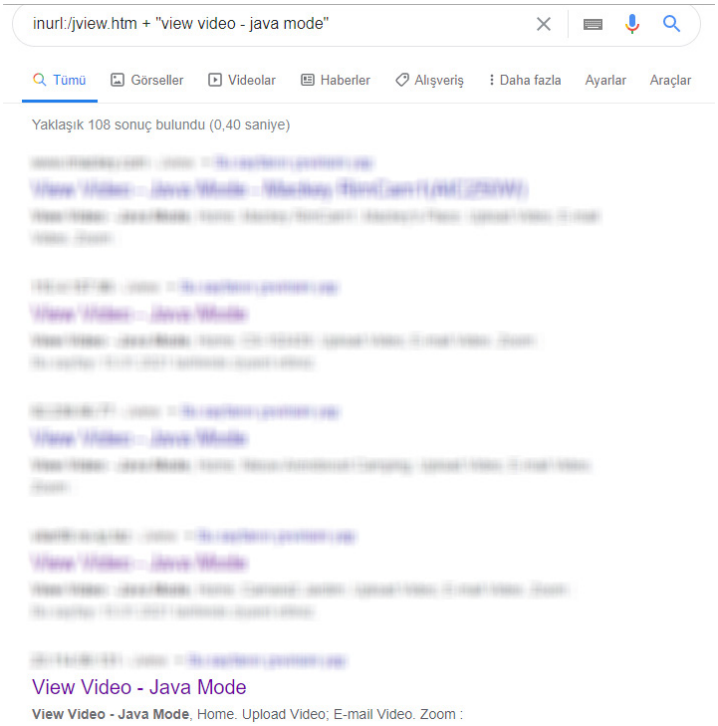
Örnek olarak, ilgili veritabanında yer alan arama kısmına "video" yazılarak, bununla ilgili sorgulara ulaşılabilir.



Şekil 3.14. Örnek sorgulama

Gelen ilk ekrandaki ilk sorgu cümlesi Google arama motorunda yazılabilir. Bu durumda Şekil 3.15'teki gibi bir liste görüntülenecektir.

Bu sorguya cevap veren herhangi bir link açıldığında kamera video akışını gösteren cihaza erişim sağlanabilecektir.



Şekil 3.15. Sorgulama sonucu

3.2 TEMEL GÜVENLİK ÖNLEMLERİ

Bir bilgisayarı güvenli hale getirmek, kişi veya kuruma göre farklı nedenlerden dolayı farklı türdeki eylemleri uygulamaya koymak amacıyla yapılması gereken işlemler ve kurallar bütünüdür. Bilgisayar güvenliği kuralları, bilgisayarı kullandığınız sürece devam eder. Bir bilgisayar sisteminin güvenliği ne kadar iyi tasarlanırsa tasarlansın, güvenlik ile ilgili işlemler kontrol edilmez ve zaman göre güncellenmezse, sisteminiz herhangi potansiyel bir bilgisayar korsanına karşı savunmasız bırakabilir.

Araştırmalara göre yeni bir bilgisayar kurulumu tamamlandıktan sonra ilk siber saldırı ortalama yedi dakika sonra gerçekleşmektedir. Bunun nedeni, bilgisayar saldırganlarının genellikle fırsat arayan ve sürekli araştıran otomatik tarama araçları kullanmasıdır. Bir istismar, genellikle bir kurulumu tamamladıktan sonra, güvenlik önlemleri alınmadan dakikalar içinde gerçekleşebilir. Bu araştırma bizlere, bilgisayar kurulumu yapıldıktan sonra internet bağlantısı kurulmadan tüm savunma ve koruma işlemlerini yerine getirmemiz gerektiği sonucunu ortaya çıkartmaktadır.

Bilgisayar kullanıcılarının sayısı arttıkça bilgisayar güvenliği konusuna yeterli önemi göstermeyen veya deneyimsiz bir kullanıcının kullandığı bilgisayar, belirlenmiş bir hedefe yönelik dağıtılmış bir hizmet reddi (DDoS) saldırısına dâhil edilebilir. Bu gibi sorunlara karşı üç konuda temel bilgisayar güvenliğini ele alabiliriz.

Şekil 3.16. Fiziksel güvenlik önemlidir

Fiziksel Güvenlik: Bilgisayar sisteminin fiziksel güvenliğidir. Bilgisayarın fiziksel olarak zarar görmemesi veya kötü niyetli kişilerce ele geçirilmemesi için gerekli önlemlerin alınmasıdır. Bununla beraber aşırı elektrik akımından korumak için kesintisiz güç kaynağı kullanmak bilgisayarın ve bilgisayar içinde saklanan verilerin güvenliği için oldukça önemlidir. Günümüzde kişisel bilgisayarlarda elektrik hatlarındaki problemler dolayısı ile veri kaybı oldukça sık

görülmektedir. Modem, sabit sürücü veya ana kart arızaları nedenleri ile bilgisayarların bir süre kullanılamaması gibi problemlere karşı fiziksel güvenlik tedbirleri alınmalıdır.

Veri Bütünlüğü: Verilerin yedeklenmesi ve bu şekilde veri kaybının önlenmesidir. Kurumlar veya kişisel kullanıcılar kendileri için değerli gördükleri verileri korumalıdır. Her yıl, bir şekilde kaybedilen değerli bilgileri yeniden üretmek için büyük bir miktarda iş gücü kaybı oluşmaktadır. Yedeklemeler flaş diskler, sürücüler, kâğıt çıktılar veya diğer bilgisayar sistemlerinde olabilir. Orijinal verinin kaybolmasını önlemek ve verileri yangın, su baskını gibi nedenlerle yedeklemek için bu yedeklemelerin kopyalarını düzenli olarak orijinal verinin tutulduğu yerden daha uzak fiziksel konumlara koymak önemlidir. Ayrıca önemli veriler için RAID sistemleri kullanılabilir çözümlerdir. RAID sistemleri bir verinin kopyasını aynı zamanda başka sürücülere de yazması anlamına gelir. Bir sürücünün arızalanması durumunda, içeriği diğer sürücülerdeki verilerden elde edilebilir.

Veri Güvenliği: Veri güvenliğine yönelik en önemli tehdit, yasa dışı bilgisayar korsanlarıdır. İçten veya dıştan gelebilecek her türlü güvenlik ihlaline karşı alınması gereken bazı önemli tedbirler bulunmaktadır. Bilgisayarlara parola koymak, önemli doya ve dizinlere erişim izinleri koymak, güvenlik duvarı gibi çözümleri kullanmak, kullanılan yazılımların güvenliğini yamalar ve güncelleştirmeler ile sağlamak, veri tabanlarını güvende tutmak, e-posta gibi güvensiz uygulamalar için gerekli önlemleri almak veri güvenliği için oldukça önemlidir.

Bilgisayarları daha güvenli hale getirmek için yapılması gereken temel işlemlerin listesi aşağıdaki gibidir.

- Bilgisayarın fiziksel güvenliği sağlanmalı
- Yedekleme alınmalı ve sisteminizin olduğundan uzak bir yerde saklanmalı
- Elektrik sorunların karşın kesintisiz güç kaynağı kullanılmalı
- Periyodik olarak virüs kontrolü yapılmalı
- Güvenlik duvarı gibi çözümler kullanılmalı
- İyi ve güvenli parola kullanılmalı
- Düzenli aralıklarla parolaların güncellenmesi
- Kullanılmayan hesapların kaldırılması
- Dosya ve dizin erişimlerinin yapılması

- Önemli dosyaların şifrelenmesi
- Şifrelenmiş e-posta yazılımları kullanılmalı
- İşletim sistemi ve yazılımlara ait yamaların ve güncelleştirmelerin yapılması
- Bilinmeyen yazılımların yüklenmemesi ve izinlerin verilmemesi
- Bilgisayarın kullanılmadığı zamanlarda kapatılması
- Bilgisayarı mümkün olduğunca yönetici (administrator) hesabı ile kullanılmaması
- E-posta adresinizi her web sitesine vermemelidir.

3.2.1 Parola Güvenliği

Parolalar günümüzde hayatımızda oldukça önemli yer tutmaktadır. Parolalar kimlik doğrulaması için kullanılan en etkili yöntemlerden birisidir. Bilişim teknolojilerinin gelişmesi ile hayatımıza gelen yeniliklerinin tamamına yakınında parolalar kullanılmaktadır. Banka kartlarımızda, internet hesaplarımızda, telefonlarımızda, ev güvenlik sistemlerinde vb. parolaları kullanmaktayız.

Not: *Parola ve şifre farklı kavramlar olsa da, çoğu zaman birbirinin yerine kullanılır.*

Parolaların kimlik doğrulamasında kullanılması beraberinde önemli bir sorunu meydana getirdiler. Bunların içinde en önemli olarak gürünler sorunlar ise; kullanıcıların zayıf veya tahmin edilmesi kolay parolaları

Şekil 3.17. Parola güvenliği son kullanıcı açısından önemli bir konudur.

seçmeye ve aynı parolaları farklı yerlerde yeniden kullanmaya devam etmeleridir. Dünya üzerinde son on yılda yapılan araştırmalar kullanıcıların en sık tercih ettiği parolaların;

- 123456
- password
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

olduğunu ortaya koymaktadır. Her yıl yapılan uyarılara rağmen bu liste pek değişmemiştir. Bunun için kullanıcılara bir takım parola belirleme kuralları tavsiye edilmektedir. Bu kurallar aşağıdaki listede belirtilmiştir.

- Minimum karakterin karşılanması gibi karmaşıklık gereksinimlerin belirlenmesi,
- Daha önceden kullanılan şifrelerin seçilmemesi,
- Parolaların periyodik olarak ve belki de sık sık değiştirilmesi,
- Kullanılan parolaların yukarıdaki listedeki gibi yaygın ve zayıf olarak kullanılan parolalardan seçilmemesi.

Parolaların belirlenmesi ve belirli standartların yakalanması için Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) parola ilkeleri sorununa çözüm getirmeyi amaçlamıştır. NIST parolalar ve bunların nasıl yönetilip saklanması gerektiği hakkında detayları ortaya koymaktadır. Buna göre, olası parolaların yaygın olarak kullanıldığı ve bilinen değerleri içeren bir listeye karşı kontrol edilmesi gerektiği belirtmiştir. Parolaların belirlenmesinde dikkat edilmesi gereken hususlar şunlardır;

- Kullanıcı tarafından sağlanan parolalar en az sekiz alfa numerik karakterden oluşmalıdır.
- Önceki ihlallerden elde edilen parolalar olmamalıdır.

- Sözlük kelimeleri olmamalıdır.
- Doğrum tarihleri gibi 1900-2020 arasındaki tarihler olmamalıdır.
- Tekrarlayan veya sıralı karakterler (örneğin aaaaaa veya 1234abcd) olmamalıdır.
- Hizmetin adı, kullanıcı adı ve bunların türevleri gibi kullanım amacına özgü kelimeler olmamalıdır.

Parolalar belirlenirken yukarıdaki kriterler dikkate alınmalı ve karmaşık yapıdaki parolaların oluşturulması sağlanmalıdır.

Parola Karmaşıklığı : Parola karmaşıklığı, parola belirleme ilklerine bağlı olarak, güçlü bir parola için biz dizi kuralı karşılaması anlamına gelmektedir. Parola karmaşıklığındaki temel kurallar şunlardır.

- Parola, hesap adını veya hesap adındaki varyasyonları içeremez.
- Parola hem büyük harf (A-Z) hem de küçük harf (a-z) içermelidir.
- Parola içinde özel karakterler (~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /) olmalıdır. (Genellikle ALT tuşu ile çıkan karakterlerdir. Ancak Euro gibi para birimi simgeleri, özel karakter olarak sayılmaz.).
- En az karakter sayısına uyulmalıdır. Bu değer sistemden sisteme, kullanıcıdan kullanıcıya değişebilir. En az parola uzunluğu 8 karakter olması gerekirken tavsiye edilen karakter sayısı 12'dir.

Parolalar yukarıda sıralanan kurallara göre en az 8 karakter ile oluşturulduğunda, tek bir parola için en az 218.340.105.584.896 farklı olasılık anlamına gelir. Oluşturulan parolanın olasılığı kaba kuvvet saldırısını oldukça zorlaştırır, ancak parolanın kırılması yine de imkânsız değildir. Kırılması neredeyse imkânsıza yakın bir parola için, parola karakter sayısını artırmak gereklidir. Minimum karakter sayısı artarsa, parolanın kırılma süresi de artar.

Parola karmaşıklığının sağladığı yararların yanı sıra bazı zorlukları da beraberinde getirmektedir. Bunların başında parolanın unutulması gelir. Daha uzun ve içinde özel karakterlerin bulunduğu bir parolayı hatırlamak zordur. Hele bir de tüm parolalar farklı farklı olduğunda hatırlamak ve diğerleri ile karıştırmamak oldukça zor bir olaydır. Bu nedenle parolalar oluşturulurken belirli bir mantık takip edilmelidir.

Örneğin;

• **B**en **D**ört **Ç**ocuklu **B**ir **A**ilenin **3**. **B**ireyiyim**!**

gibi bir cümleyi kendi gerçek yaşamınızdan yazabilirsiniz. Cümlenin ilk karakterleri ve özel karakterleri alındığında **Bdcba3.B!** gibi bir parola elde etmiş olunur.

• **B**u **W**eb **S**itesine **(e**ğitim **i**le **i**lgili**) 20 A**ralık **g**ünü **ü**ye **o**ldum**.**

gibi bir cümleyi üye olduğunuz bir web sitesinin ilgi alanına ve üyelik tarihine göre özelleştirebilir ve unutmamanızı sağlayabilirsiniz. İlk karakterleri ile özel karakterleri alındığında **BWS(eii)20Aguo.** gibi bir parola elde etmiş olunur.

Güçlü parola oluşturmak için farklı teknikleri de kullanabilirsiniz. Bunlardan bir kaçına dair örnekler aşağıda verilmiştir.

- Cümleler olduğu gibi yazılarak güçlü parola oluşturulabilir. Örneğin;
- Bu Web Sitesine 4.Nisanda Python Ogrenmek icin uye oldum.
- Siber Guvenlik dersini 13:30'a koymuşlar.
- Benzer rakam ve harfleri birbirinin yerine kullanarak güçlü parolalar oluşturulabilir. Örneğin;
- O yerine 0, L yerine 1, Z yerine 2, E yerine 3, S yerine 5, G yerine 6, B yerine 8 yazılarak;
- Leylek = 13y13k
- MorMenekşe = M0rM3n3k53
- Zonguldak = 20n6u1dak
- Bazı kelime veya karakterlerin yerine özel karakter kullanarak güçlü parolalar oluşturulabilir. Örneğin;
- Yağmur yerine "" işareti, yüz yerine %, ve yerine &, ş yerine $, ı-i yerine !, boşluk yerine * yazılarak;
- Yarın Yağmur yağacakmış = Yar!n""ya6acakm!$
- Yüzmeyi severim = %mey!*sever!m

• Parola için oluşturduğunuz cümledeki sadece sesli veya sadece sessiz harfleri kullanarak güçlü parolalar oluşturabilirsiniz. Örneğin;

• Bu vatan 1 bütündür. = Bvtn1btndr.

• Atam 30 Agustos'da zaferi ilan etti. = Aa30auo'azeiiaei.

Parola Güvenliğini Sağlama: Günümüzün çevrimiçi ortamında, güvenliğe yönelik basit "kullanıcı adı ve parola" yaklaşımı, siber suçlular için kolay bir avdır. Birçok oturum açma işlemi dakikalar içinde tehlikeye atılabilir ve özel veriler kötü niyetli kişilerin ellerine geçebilir.

Parolaların tahmin edilerek veya daha farklı yöntemler kullanılarak başkaları tarafından ele geçirilmesini engellemek için parolaların güvenliğinin sağlanması gerekmektedir. Bunlar için yapılması gereken hususlar şunlardır.

1- Gizli sorular ile güvenceye alma

2- İki aşamalı doğrulama yöntemi kullanılması

3- Biometrik kimlik doğrulama kullanılması

Gizli Soru: Güvenlik soruları, bir kullanıcının parolasını unutması veya çok faktörlü kimlik doğrulama (MFA) gerektiğinde ikincil kimlik doğrulama faktörlerini kaybetmesi durumunda hesabına yeniden erişim sağlamasına olanak sağlamak için birçok web sitesi tarafından kullanılır. Bununla birlikte, genellikle parolalardan çok daha zayıf bir kimlik doğrulama biçimidir.

Yeni bir çevrimiçi hesap oluşturulduğunda, web siteleri genellikle kullanıcıdan güvenlik sorularını yanıtlamalarını ister, böylece bir kullanıcı kendi kimliğini doğrulaması istenirse parolayı girecek, hatırlamaması durumunda kendisini kanıtlaması için güvenlik sorularını soracaktır. Bu sorular arasında "Annenizin kızlık soyadı nedir?" , "Hangi şehirde doğdunuz?" veya "Gittiğiniz ilkokulun adı nedir?" gibi sorular yer almaktadır.

Şekil 3.18. Güvenlik Soru ve Cevap Arayüzü

Maalesef web sitelerine üyelik veya hizmet alımı sırasında buna benzer çevrimiçi güvenlik sorularını doğru olarak yanıtladığınızda bu işlemin yeterli bir güvenli durum olmadığını söylemek gerekir. Bunun nedeni, hesabınıza erişmek isteyen birinin yanıtları bulmak için kolayca İnternet araştırması yapabilmesidir. Sosyal medya hesaplarınızı inceleyen saldırgan bilgisayar korsanı dayınıza yazdığınız bir mesaja ulaşabilir ve dayınızın soy isminden annenizin kızlık soyadını bulabilir.

Bir kullanıcının kimliğini doğrulamak için tek bir mekanizma olarak güvenlik sorularına güvenilmemelidir. Bir öneri olarak, "hangi şehirde doğdunuz?" gibi bir parola hatırlatma sorusuna ilk kayıt esnasında şehir adı olmayan ancak hatırda kalınabilecek bir ifade yazılabilir.

3.2.2 İki Aşamalı (Faktörlü) Doğrulama

İki faktörlü kimlik doğrulama (2FA), bir sisteme erişmek için iki farklı tanımlama biçimi gerektiren bir güvenlik sistemidir. Çevrimiçi bir hesabın, akıllı telefonun veya bir kapının güvenliğini güçlendirmek için iki faktörlü kimlik doğrulama kullanılabilir. Bu doğrula sistemi güvenli olan veriye veya sisteme erişilmeden önce kullanıcıdan iki tür bilgi talep ederek yapar. Bu bilgiler bir parola veya kişisel kimlik numarası (PIN), kullanıcının akıllı telefonuna gönderilen bir kod (SMS gibi) olabilir.

Yeni bir cihazda ilk kez oturum açılmak istenildiğinde, şifre ile telefon numaranıza gönderilen 4-8 basamaklı doğrulama kodu olmak üzere iki bilgi sağlanması gerekir. Kodu girilerek yeni cihaza güvenildiği doğrulanmış olur.

İki faktörlü kimlik doğrulama, yetkisiz kullanıcıların çalıntı bir parola kullanarak bir hesaba erişim sağlamasını önlemek için tasarlanmıştır. Kullanıcılar, özellikle aynı parolayı birden fazla web sitesinde kullanırlarsa, parolaların ele geçirilmesi konusunda büyük bir risk altında olabilirler.

İki faktörlü kimlik doğrulama, aşağıda verilen iki tekniğin birleşimidir:

- Bildiğiniz parolanız
- Sahip olduğunuz bir bilgi veya akıllı telefonunuza veya başka bir cihaza gönderilen bir kod içeren bir metin (veya bir akıllı telefon kimlik doğrulama uygulaması gibi).

2FA güvenliği artırsa da parolanın güvenliği için kusursuz değildir. Bilgisayar korsanları yine de hesaplara yetkisiz erişim elde edebilir. Bunu yapmanın yaygın yolları arasında kimlik avı saldırıları, hesap kurtarma prosedürleri ve kötü amaçlı yazılımlardır.

3.2.3 Biometrik Kimlik Doğrulama

Biyometrik kimlik doğrulama, kişinin kendisini kanıtlaması ve doğru kişi olduğunu ispatlamak için bireyin eşsiz biyolojik özelliklerine dayanan bir güvenlik sürecidir. Biyometrik doğrulama sistemleri, elde edilen biyometrik veriyi veri tabanındaki kayıtlı, depolanmış ve daha önceden onaylanmış gerçek verilerle karşılaştırır. Elde edilen biyometrik veri örneği ile kayıtlı olan biyometrik veri eşleşirse, kimlik doğrulaması onaylanır. Kişiye özgü olan bu biyometrik veriler unutulamaz veya kaybedilemez, taklit edilemez olmaları, bu kimlik doğrulamayı diğer yöntemlerden ayırır. Ancak son derece özel olan biyometrik kişisel bilgilerin kullanılıyor olması, siber güvenlik açısından önem gösterilmesini gerektirir.

Biyometrik kimlik doğrulama yöntemleri, birden fazla biyometrik deseni birleştirerek veya biyometrik doğrulamayı tamamlayan geleneksel bir şifre veya ikincil cihazla birlikte iki faktörlü kimlik doğrulama (2FA) veya çok faktörlü kimlik doğrulama (MFA) biçimi olarak da kullanılabilir.

Günümüzde yaygın olarak kullanılan biyometrik kimlik doğrulama teknolojileri şunlardır:

Parmak izi tarama: Parmak ucunda yer alan izlerin modelinde belirli özellikleri arayarak kimlik doğrulama yapar. Harici bir özelliğe sahip bir görüntüyü yakalamanın dezavantajı, bu görüntünün kodlanmış biçimde saklansa bile kopyalanabilmesidir. Parmak izleri, taklit edilebilen bir kimlik doğrulama yöntemidir. Bazı parmak izi çizgi modelleri o kadar benzerdir ki pratikte bu yüksek bir yanlış kabul oranına neden olabilir.

Retina taramaları, bireyin iç gözünü kaplayan ışığa duyarlı yüzeyde kan damarı deseninin bir görüntüsünü üretir.

İris tanıma: İnsanın göz bebeğinin etrafında yer alan benzersiz halkadaki desene göre yapılan kimlik doğrulamadır. Bir iris taraması gerçekleştirildiğinde, tarayıcı bir irisin benzersiz özelliklerini okur ve bunlar daha sonra şifrelenmiş bir koda dönüştürülür. İris taraması, özellikle kızılötesi ışık kullanılarak yapıldığında çok iyi sonuçlar vermektedir.

Parmak damar kimliği ve avuç tanıma: Bir insanın parmağında yer alan ve benzersiz olan damar desenine göre yapılan bir kimlik doğrulamadır. Damar deseni tanıma durumunda, parmaktaki damarların bitiş noktaları ve çatallanmaları bir görüntü biçiminde yakalanır, sayısallaştırılır ve şifreli bir koda dönüştürülür.

Yüz tanıma sistemleri: Bu sistemler, bir eşleşme belirlemek için yüzün farklı bölümlerinin şeklini ve konumunu analiz ederler. Bununla birlikte, yüz tanımanın bir takım önemli dezavantajları

da vardır. Örneğin bir kişinin tanımasını mümkün kılmak için genellikle doğrudan kameraya bakması gerekir.

Ses tanıma sistemleri, daha değişken koşullardan ziyade konuşmacının ağzının ve boğazının şekli tarafından oluşturulan özelliklere dayanır.

Biyometrik sahtekârlık, başka bir kişi olarak tanımlanmak amacıyla sahte bir biyometrik özelliğin sunulmasıdır. Bu, kopyalanmış bir parmak izi veya tahrif edilmiş iris modeline sahip bir kontakt lens kullanmayı içerebilir.

3.2.4 Parola Kırma Teknikleri

Parola kullanımı, kimlik doğrulama sistemlerinde en sık kullanılan yöntemdir. Kullanıcı ya da bir ağ cihazı, doğru parolayı kimlik doğrulayıcıya sunabilirse, iddia ettiği kullanıcı ya da cihaz olduğunu ispat etmiş olur. Parola, kimliğin ispatı olduğundan güvenliği ve gizliliği son derece önemlidir. Ancak tehdit aktörleri, parolayı elde etmeye yönelik oltalama saldırılarından, tersine mühendislik yöntemlerine kadar çok çeşitli yöntemler kullanırlar. Temel olarak parolayı elde etme yöntemleri "parola kırma (password cracking)" olarak adlandırılır.

Parola tahmin etme: Saldırgan açısından, uygulaması en kolay olan parola kırma tekniğidir. Hedef kullanıcı hakkında bilgi toplandıktan sonra, doğum tarihi, memleketi, tuttuğu futbol takımı gibi kişisel bilgilerden yola çıkarak parola tahmini yapılır. Bu kategorideki diğer bir yöntem de, en sık kullanılan "qwerty" veya "123qwe" parolaların denenmesidir. Yine bu kısımda ele alınabilecek diğer bir husus olarak, aynı parolanın farklı yerler için de kullanılması ile ilgilidir. Eğer kullanıcı her yerde aynı parolayı kullanıyorsa ve bu kullanım alanlarından birinde parola kırılmışsa, saldırganın ilk yapacağı aynı parolayı farklı noktalar için denemek olacaktır.

Sözlük saldırıları: Brute force (kaba kuvvet ya da deneme yanılma) saldırılarında kullanılan yöntemdir. Bir yazılım tarafından belirli bir kelime listesinde (sözlük) yer alan parolaların sıralı olarak denenmesi mantığına dayanır. Bu sözlük, en sık kullanılan gerçek kelimeleri içerdiği gibi, "Ankara06" ve "Passw0rd1" gibi yine sık kullanılan parolalardan da oluşabilir. Tehdit aktörleri, bu listelere internet ortamından rahatlıkla ulaşabilmektedir. Sözlük saldırısı kategorisinde yer alabilecek diğer bir yöntem de, karakter üreteçleri kullanarak kendi özelleştirilmiş listelerini oluşturmak ve bu oluşturulan liste üzerinden deneme yanılma saldırısı yapmaktır. Bu yöntem hem parola üretmek hem de denemek olarak iki kısımdan oluştuğu için uzun zaman alabilir. Kullanıcılar unutmamak için genellikle kısa parolalar kullandıklarından, bu saldırılar oldukça başarılı saldırılardır.

Önceden hesaplanmış parola listeleri: Daha önce ifade edildiği gibi, parolalar veritabanlarında genellikle özetlenerek (hash) saklanır. Bir şekilde bu veritabanı eğer saldırgan tarafından eşe geçirilmişse, parola açık olarak veri tabanında yer almayacaktır. MD5 ve SHA gibi özetleme fonksiyonları tek yönlü matematiksel fonksiyon olduklarından, hash değerinden parolanın ham haline ulaşmak tersine mühendislik yöntemi ile mümkün değildir. Ancak, bu durumda saldırgan önceden hesaplanan hash değerlerinin yer aldığı listelerden yola çıkarak parolanın ham haline ulaşabilir *(rainbow table attacks)*. Ancak bu yöntemin başarılı olabilmesi için, parolanın bu listede önceden yer alıp özetlenmiş olması gerekir. Sık kullanılan kelimeler (ya da parolalar) bu listede çok büyük ihtimalle yer aldığından, kırılması muhtemeldir. Bu nedenle, parolanın tek başına özetlenmiş olarak veritabanında kaydedilmesi yeterli bir güvenlik önlemi değildir, parolanın seçimi de son derece önemlidir.

Parolaların şifrelenmesi, özetlenmesi ya da veritabanına çeşitli tekniklerle kaydedilerek güvenliğinin sağlanması önemli bir konudur. Ancak tüm bu parola güvenlik çabalarını riske atabilecek bir durum vardır, kullanıcının hafızasında yer alan bu parola bilgisini *bilinçli ya da bilinçsiz* olarak saldırgana vermesidir. Saldırganlar son derece etkili sosyal mühendislik teknikleri (senaryoları) ile bu parolaları elde etmek için uğraşabilirler. Oltalama saldırıları ile bu işlem yapılabildiği gibi, yetkili bir otorite gibi görünerek parolayı kullanıcıdan isteyebilirler. Kullanıcı, parola girdiği her yere dikkat etmeli ve parolayı kesinlikle hiç kimseye vermemelidir.

3.3 GÜVENLİK ZAAFİYETİ DERECELENDİRME

Siber güvenlikte amaç, sistemleri ve kullanıcıları tehdit aktörlerinin kötü amaçlı saldırılarına karşı korumaktır. Saldırılar, teknik, mantıksal veya fiziksel olabilen güvenlik açıklarını hedefler. Risk yönetimi gereği tüm potansiyel tehditler ele alınmalı ve güvenlik açısından riskleri tehdidin önemine göre ele alınmalıdır. Zararlı yazılımların resmi bir isimlendirme kural yapısı yoktur. Zararlı yazılımların bilinen isimleri, genellikle tehdidi tanımlayan araştırmacılar tarafından verilmiş isimlerdir. Bu başlıkta güvenlik tehditleri ve zafiyetlerin tanımlanmasında kullanılan isimlendirme ve zaafiyet derecelendirmesi ele alınacaktır.

3.3.1 CVE İsimlendirmesi

Siber güvenlik dünyasında bir güvenlik açığıyla ilişkili riski derecelendirmek ve bu güvenlik açığı hakkında iletişim kurmak için bir isimlendirme ve puanlama sistemi kullanılır. Bu sayede,

siber güvenlik tarafları aynı güvenlik açığı hakkında herhangi bir kafa karışıklığı olmadan iletişim kurabileceklerdir.

CVE (Common Vulnerabilities and Exposures), Ortak Güvenlik Açıkları ve Etkilenmeler sistemi, genel olarak bilinen bilgi güvenliği açıkları ve riskleri için bir referans yöntemi sağlar. Belirli tanımlamalara göre güvenlik zafiyetlerinin tutulmasını sağlayan bir isimlendirme veri tabanıdır. Bu veri tabanına https://cve.mitre.org/ sitesinden ulaşılabilir [9].

CVE yapısında, 1999 yılından itibaren tespit edilen güvenlik açıklarını listelemek için bir isimlendirme kuralı geliştirmiştir. Buna göre tespit edilen açık, CVE-YYYY-NNNN olarak isimlendiriliyordu. YYYY tespit edilen yılı, NNNN ise güvenlik açığına verilen numarayı gösterir. Ancak daha sonra bu isimlendirme geliştirildi. Aynı web sayfasından yeni isimlendirme kuralına bakılabilir. Örneğin Şekil 3.19'daki ekran görüntüsünde, CVE-2019-3568 numaralı WhatsApp uygulamasına yönelik bir güvenlik açığı listelenmektedir.

CVE-ID

CVE-2019-3568 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number. The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:108329
- URL:http://www.securityfocus.com/bid/108329
- MISC:https://www.facebook.com/security/advisories/cve-2019-3568

Assigning CNA

Facebook

Date Record Created

20190102 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Şekil 3.19. Örnek CVE ekranı

Belirli bir CVE ile ilişkili daha fazla ayrıntılı bilgi için https://www.cvedetails.com/ sayfası ziyaret edilebilir.

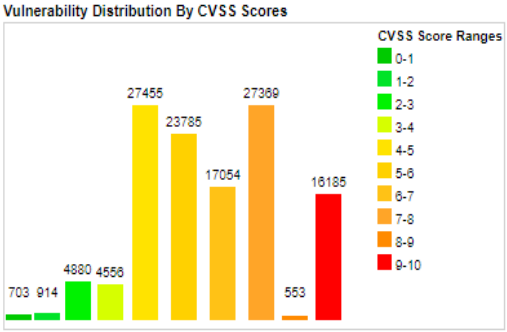
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

Weighted Average CVSS Score: **6.6**

Vulnerability Distribution By CVSS Scores



Şekil 3.20. Zaafiyete ilişkin skor belgesi

CVE-2019-3568 numaralı güvenlik açığına ilişkin detaylı incelemenin ekran görüntüsü Şekil 3.21'de gösterildiği gibidir.

Vulnerability Details : CVE-2019-3568

A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number. The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15.

Publish Date : 2019-05-14 Last Update Date : 2019-08-13

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Overflow
CWE ID	119

– Products Affected By CVE-2019-3568

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Whatsapp	Whatsapp	2.2.5		~~~iphone Os~~		Version Details Vulnerabilities
2	Application	Whatsapp	Whatsapp	2.6.4		~~~iphone Os~~		Version Details Vulnerabilities
3	Application	Whatsapp	Whatsapp	2.6.5		~~~iphone Os~~		Version Details Vulnerabilities
4	Application	Whatsapp	Whatsapp	2.6.6		~~~iphone Os~~		Version Details Vulnerabilities
5	Application	Whatsapp	Whatsapp	2.6.7		~~~iphone Os~~		Version Details Vulnerabilities

Şekil 3.21. CVE detay ekranı

Güvenlik açığına ilişkin detaylı bilgilerin sunulduğu bu sayfada, güvenlik açığının açıklaması, güvenlik açığı türü, etkilenen ürünler, zaafiyetin karmaşıklığı gibi bilgilerin yanı sıra, güvenlik açığının derecesini belirten **CVSS skoru** da yer almaktadır (Örnekte 7.5).

3.3.2 Zaafiyet Derecelendirmesi (CVSS)

CVSS, Ortak Güvenlik Açığı Puanlama Sistemi (Common Vulnerability Scoring System) olarak adlandırılan ve bir güvenlik açığının (güvenlik zafiyetinin) derecelendirilmesi için kullanılan bir sistemdir. Sistemde güvenlik açığının önem düzeyine göre, kompozit metrikler kullanılarak 0 **(en az tehlikeli)** ile 10 **(en çok tehlikeli)** arasında puanlama yapılır.

Puanlama birden fazla parametreye bakılarak hesaplanır. CVSS puanlama yapısı birkaç kez değişmiştir. Günümüzde kullanılan en güncel puanlama sürümü, 2019 yılı Haziran ayından beri kullanılan **CVSSv3.1** sürümüdür.

CVSSv2 puanının hesaplanmasında temel puanlama **(base)**, zamansal puanlama **(temporal)** ve çervesel **(environmental)** puanlama olmak üzere üç ölçüt **(metric)** kullanılmaktadır.

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Local (AV:L)	Adjacent Network (AV:A)	Network (AV:N)

Access Complexity (AC)*

High (AC:H)	Medium (AC:M)	Low (AC:L)

Authentication (Au)*

Multiple (Au:M)	Single (Au:S)	None (Au:N)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Partial (C:P)	Complete (C:C)

Integrity Impact (I)*

None (I:N)	Partial (I:P)	Complete (I:C)

Availability Impact (A)*

None (A:N)	Partial (A:P)	Complete (A:C)

Şekil 3.22. CVSS Base Score Metrikleri

Temel puanlamada, siber güvenliğin temel bileşenleri (C-I-A) bir alt grupta, saldırı vektörü, erişim karmaşıklığı ve kimlik doğrulama da diğer bir alt grupta hesaplamaya katılır.

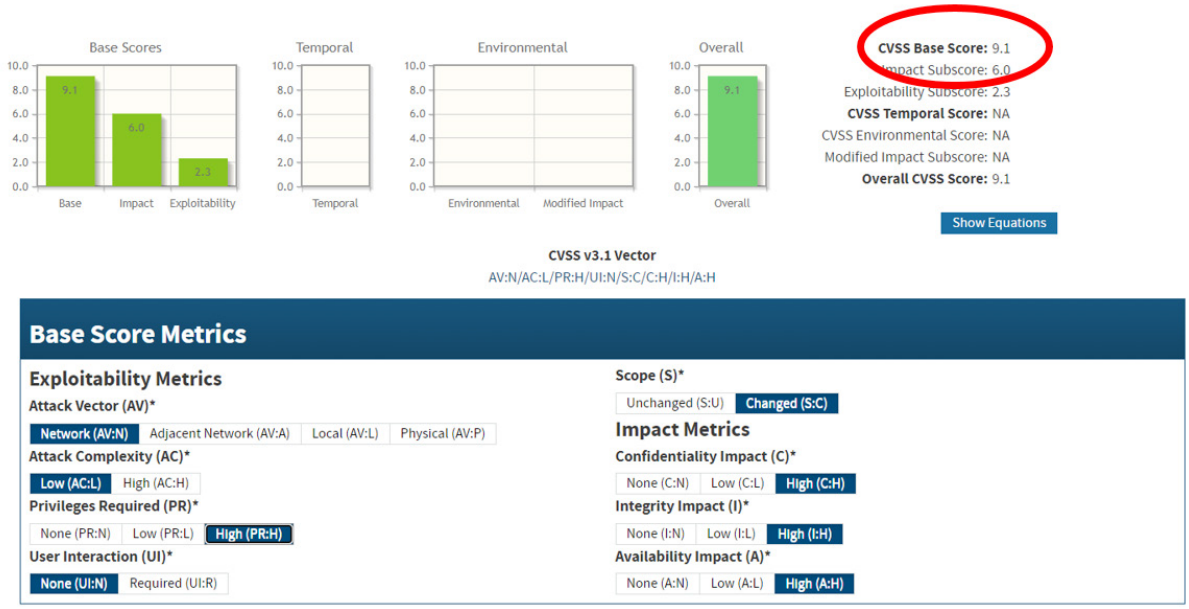
Erişim vektöründe yer alan *"Lokal Erişim (Local)"* istismarın ağ üzerinden yapılamayacağını, sadece yerel cihazdan yapılabildiğini belirtir. "Bitişik Ağ (Adjacent Network)" ifadesi saldırının aynı ortamda bulunan, aynı mantıksal ağdan yapılabildiğini belirtir. "Ağ (Network)" ifadesi ise, internet gibi farklı ağ üzerinden (ya da farklı VLAN üzerinden) yapılabildiğini belirtir. Bu durum, güvenlik açığı puanının daha yüksek olduğu anlamına gelir.

Zaafiyetin **erişim karmaşıklığı** (access complexity) için düşük, orta ve yüksek ölçekler kullanılmaktadır. Karmaşıklık düzeyinin artması, zaafiyetin puanını arttır.

Kimlik doğrulamada (Authentication) ise çoklu doğrulama (Multiple), tek doğrulama (Single) ve doğrulama yok (None) olmak üzere yine üç farklı ölçüt kullanılmaktadır. Çoklu kimlik doğrulamada, zaafiyetin birden fazla kez kimlik denetiminden geçildikten sonra gerçekleşebileceği belirtilir. Her kimlik doğrulama bir güvenlik olduğundan, çoklu kimlik doğrulamaya sahip bir zafiyet düşük puanlı olmasını sağlar. Tek kimlik doğrulama ise, zaafiyetin gerçekleşmesi için sadece bir kez kimlik doğrulamadan geçilmesinin yeterli olduğu anlamına gelir. Kimlik doğrulamanın olmaması, bu alt metrik için en tehlikeli olanıdır.

Aynı şekilde derecelendirmede **gizlilik** (confidentiality), **bütünlük** (integrity) ve **kullanılabilirlik** (availability) parametrelerinin her biri için üç düzey belirlenmiştir.

CVSSv3.1 için güncellenmiş puanlama ölçütleri https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator adresinde yer almaktadır.



Şekil 3.23. CVSS skor hesaplama

CVSSv3.1 için yukarıdaki bağlantıda yer alan hesaplama aracı kullanılarak, parametrelerin değişiminin CVSS skoruna etkisi görülebilir. Şekil 3.23'deki ekran görüntüsünde, CVSS temel metrik skoru 9,1 olarak belirlenen bir güvenlik zafiyetinin özellikleri görüntülenmektedir. Aynı araç kullanılarak, zamansal puanlama **(temporal)** ve çevresel **(environmental)** puanlama hesaplanabilir.

3.4 GÜVENLİK YAZILIMLARI

Önceki bölümlerde ele alındığı gibi ağlar siber saldırıların hedefidir. Ağları korumak için ağ düzeyinde koruma sağlayan IPS, IDS, güvenlik duvarları gibi sistemler kullanılır. Aynı şekilde son kullanıcı cihazlarında da kullanılabilcek güvenlik yazılımları vardır. Bazı güvenlik çözümleri birden fazla bileşen de içerebeilir. Örneğin hem antivirüs hem de anti-malware aynı yazılımda sunulabilir.

3.4.1 Antivirüs

Virüsleri tespit etmek ve sistemden kaldırmak için bir hoşta yüklenen programlardır. Windows Defender, Norton Security, McAfee, Trend Micro gibi birçok antivirüs yazılımı bulunmaktadır. Antivirüsler genellikle daha önceden antivirüs üreticileri tarafından tespit edilen ve zararlı yazılımın karakteristik özelliklerini (imzaları) kaydeden veri tabanı yapısını kullanırlar. İmza veri tabanının sürekli olarak güncel tutulması bu nedenle önemlidir. Birçok antivirüst programı, verileri analiz ederek gerçek zamanlı koruma da sağlayabilir. Bu programlar aynı zamanda sisteme gerçek zamanlı olarak tanınmadan önce girmiş olabilecek mevcut zararlı yazılımları da tarar.

Yazılım olarak kullanılan konak tabanlı antivirüs koruması, ajan tabanlı antivirüs olarak da bilinir. Ajan tabanlı antivirüs, korunan her makinede çalışır ve merkezi bir sistemden tarama gerçekleştirir. Aracısız sistemler, aynı anda bir bilgisayarda birden çok işletim sistemi örneğinin çalıştığı sanallaştırılmış ortamlar için popüler hale gelmiştir. Sanallaştırılmış her sistemde çalışan ajan tabanlı antivirüs, sistem kaynakları üzerinde ciddi bir yük oluşturabilir.

3.4.2 AntiMalware

Günümüzde anti-virüs yazılımları ile birlikte entegre olarak çalışan yazılımlardır. Bu programlar, üç farklı yaklaşım kullanarak virüsleri algılayabilir. İmza tabanlı yaklaşımda, bilinen zararlı yazılım dosyalarının çeşitli özelliklerini (imzalarını) tanır. Sezgisel tabanlı yaklaşımda, çeşitli zararlı yazılım türleri tarafından paylaşılan genel özellikleri tanır. Davranış temelli yaklaşımda ise şüpheli davranışların analizini kullanır.

3.4.3 Konak Tabanlı Güvenlik Duvarı

Yazılımsal güvenlik duvarı, sistemi kötü amaçlı yazılımlardan, solucanlardan, virüslerden ve e-posta eklerinden korumayı amaçlayan konak tabanlı güvenlik duvarı programlardır. Genellikle konak bilgisayardan çıkan ve konak bilgisayara giren belirli protokollerin filtrelenmesini sağlamak üzere geliştirilmişlerdir.

3.4.4 Diğer Yazılımlar

Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP) - Virüslere ve kötü amaçlı yazılımlara karşı uç nokta koruması sağlar.

E-posta Güvenlik Aracı (ESA) - SPAM ve potansiyel olarak kötü niyetli e-postaların uç noktaya ulaşmadan önce filtrelenmesini sağlar.

Web Güvenlik Aracı (WSA) - Konakların web üzerindeki tehlikeli konumlara ulaşmasını önlemek için web sitelerinin filtrelenmesini ve kara listeye alınmasını sağlar. Kullanıcıların internete nasıl eriştiğini kontrol eder ve kabul edilebilir kullanım politikalarını uygulayabilir, belirli sitelere ve hizmetlere erişimi kontrol edebilir ve zararlı yazılım taraması yapabilir.

Ağ Kabul Kontrolü (NAC) - Yalnızca yetkili ve belirli kriterlerin sağlandığı (örneği işletim sisteminin güncel olması) sistemlerin ağa bağlanmasına izin verir.

3.5 GÜVENLİK OPERASYONLARI MERKEZİ

Güvenlik operasyonları merkezi (Security Operations Center – SOC), kurumsal ve teknik düzeyde güvenlik sorunlarıyla ilgilenen merkezi bir birimdir [23]. Güvenlik Operasyon Merkezi, siber tehditleri önlerken, saldırıları tespit eder, ağı analiz eder ve olası tehditlere yanıt verir. Daha genel bir ifade ile bir kuruluşun güvenlik duruşunu sürekli olarak izlemek ve iyileştirmek için insanları, süreçleri ve teknolojiyi kullanan kuruluş içindeki merkezi bir işlevdir.

SOC, birbiri ile uyum içinde çalışan birimlerden ve teknolojilerden oluşan bir merkezi nokta olarak ele alınabilir. Bir kurumda SOC yapısının bulunması, ağın daha geniş bir ifade ile kurumdaki varlıkların sürekli izlenmesini sağlayarak, saldırı öncesi,

Şekil 3.24. SOC bileşenleri

saldırı anı ve saldırı sonrası eylemlerin gerçekleştirilerek potansiyel (veya devam eden) tehditlerin ortadan kaldırılmasını sağlar. SOC yapısının varlığı sadece kurumun fiziksel varlıklarını değil, iş döngüsünü, süreci ve yapıyı da korur.

3.5.1 SOC Fonksiyonları

Güvenlik Operasyonları Merkezi, birbiri son derece önemli olan ile ilişkili birçok fonksiyonlardan oluşur. Bu fonksiyonların yürütülmesi, ağın daha fazla güvenli olmasını sağlayacaktır. Aşağıda bu fonksiyonlardan bazıları ele alınmıştır [22].

1- **Mevcut Kaynakların Listesini Alma**: SOC, farkında olmadığı ya da varlığından habersiz olduğu kaynakları koruyamaz. Bu nedenle kurumda korunması gereken kaynakları ve varlıkların belirlenmesi ile bu kaynakların nasıl korunacağının belirlenmesi gerekir. Bu aşama aynı zamanda saldırı yüzeyinin ve saldırı vektörlerinin de tanımlanmasını sağlar. Savunma esasında kullanılabilecek donanımların, yazılımların ve araçların varlığının tespiti bu fonksiyon içerisinde ele alınır.

2- **Hazırlık ve Önleyici Bakım**: Ağlar için en tehlikeli saldırılardan birisi, sıfırıncı gün olarak bilinen saldırılardır. Bu tür saldırılardan korunmanın en önemli yöntemlerinden biri, hazırlık yapma ve önleyici bakım yapmaktır. SOC ekibinin, güncel saldırıları takip etmesi gerektiği gibi en güncel güvenlik gelişmelerini de takip etmesi gerekir. Ancak yine de saldırı gerçekleşebilir. Bu nedenle olası bir saldırı durumunda, felaket kurtarma planının bulunması gerekir. Önleyici bakım olarak, tüm sistemlerin güncel olduğu sağlanmalıdır. Yine sistemdeki beyaz liste (kabul edilebilir) ya da kara listenin de (kabul edilemez) bu doğrultuda güncellenmesi gerekebilir. Aynı şekilde personelin de periyodik olarak eğitimler ile bilgilendirilmesi gerekir.

3- **Sürekli Proaktif İzleme**: Saldırının ne zaman gerçekleşeceği bilinmez. Bu nedenle anormal bir durum oluşup oluşmadığının belirlenmesi için varlıkların sürekli olarak izlenmesi gerekir. Ağdaki günlük dosyalarının, mesajların ve olayların izlenmesini sağlayan SIEM yazılımları bu amaç doğrultusunda kullanılır.

4- **Uyarı Sıralaması ve Yönetimi**: Ağın izlenmesi sırasında çok farklı düzeyde ve önemde tehditler yakalanabilir. SOC analistinin görevi, uyarılara göre tehditleri önem sırasına dizmek ve acil eylem gerekenler ile diğerlerini birbirinden ayırt edebilmektir.

5- **Olay Müdahale**: Tehditin ya da saldırının gerçekleştiği anlaşıldığı anda yapılması gerekenleri ifade eder. Genellikle ilk verilen tepki, saldırının yayılmasını önlemek

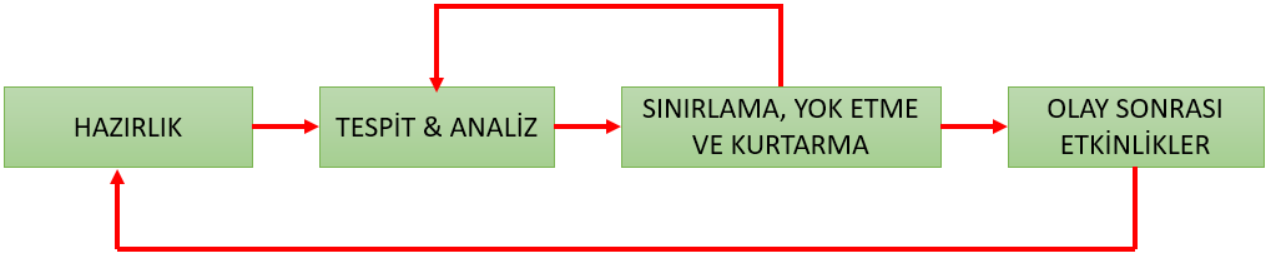
amacıyla izolasyon sağlamaktır. Zararlı yazılımın tespit edilip silinmesi, zararlı işlemin durdurulması ve zararlı dosyanın silinmesi bu aşamada gerçekleşir. Hedef izole edildikte sonra tüm ağ tekrar analiz edilir.

6- **Kurtarma ve İyileştirme:** Saldırı gerçekleştikten sonrsa mümkün olan en kısa sürede sistemin tekrar devreye alınması gerekir. Geciken her süre, itibar ve parasal kayıp olarak yorumlanabilir. Sistem yapılandırmalarının düzenlenmesi, yedeklerin yüklenmesi gibi işlemler bu fonksiyonun sorumluluğundadır.

7- **Log Yönetimi:** SOC için belki de en önemli işlemlerdendir. Sistemdeli tüm kaynaklardan gelen loğların ve olayların SIEM yazılımları ile yönetimini ifade eder. Hem saldırı öncesi hem de saldırı sonrası ayrı ayrı incelenmesi gereken bir durumdur. Saldırı öncesinde anomali tespiti yapılması bir örnek olarak verilebilir. Aynı şekilde saldırı sonrasında, saldırının nasıl gerçekleştiğinin ve etkisinin analizi de yine bu fonksiyonun sorumluluğundadır.

3.5.2 Olay Müdahale Yaşam Döngüsü

Bir saldırıya hazırlıklı ve planlı olmak önemlidir. Olay müdahalesi bir kez gerçekleşen bir durum değil, her zaman gelişen bir döngüdür. Bu yöntemlerden biri de Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından belirlenen, olay müdahale yaşam döngüsüdür.



Şekil 3.25. Olay Müdahale Yaşam Döngüsü

Hazırlık, olay müdahale ekibinin bir olaya nasıl müdahale edecekleri konusunda eğitimi aşamasıdır.

Tespit ve Analiz - Sürekli izleme yaparak, bir olayı hızla tanımlar, analiz eder ve doğrular.

Sınırlama, Yok Etme ve Kurtarma - Tehdidi kontrol altına almak, kurumsal varlıklar üzerindeki etkiyi ortadan kaldırmak, verileri ve yazılımı geri yüklemek için yedekleri kullanmak gibi işlemleri uygular. Daha fazla bilgi toplamak veya araştırmanın kapsamını genişletmek için tespit ve analize geri dönebilir.

Olay Sonrası Aktiviteler - Daha sonra olayın nasıl ele alındığının belgelenmesidir. Gelecekteki müdahale için güncellemeler önerir ve bir tekrar oluşmasının nasıl önleneceğini belirtir.

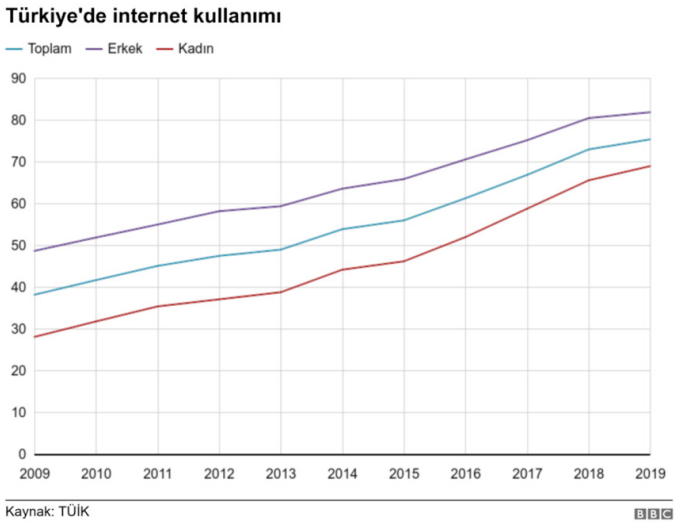
Siber Güvenlik

Siber Güvenlik

BÖLÜM 4

İNTERNET ve SOSYAL MEDYA GÜVENLİĞİ

Bugün yaşamımızda ekmek gibi su gibi temel bir gereksinim haline gelen, küresel iletişimimizi sağlayan internetin de ilk ortaya çıkışı, birçok teknoloji gibi askeri amaçlı olarak ortaya çıkmıştır. Internet, bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağı olarak tanımlanmaktadır. Amerikan İleri Araştırma Projeleri Birimi (ARPA) tarafından 1969 yılında oluşturulan ARPANET internetin başlangıç noktası olarak kabul edilmektedir. 1970'li yılların ortalarında ağ iletişimde kullanılan TCP/IP protokolü oluşturulmuştur. TCP/IP protokolünün de işlevselliği ile kurulan internet ağı ile hızlı bir şekilde üniversitelerden hükümet birimlerine ve düşünce kuruluşlarına kadar genişlemesinin önü açılmıştır. 1989 yılında Avrupa CERN'de Tim Barners-Lee tarafından geliştirilen 'world wide web' (www) internete farklı bir boyut ve işlevsellik kazandırmıştır. Bilgisayarlar sahip oldukları içeriklerini küresel anlamda erişimin sağlanmasını mümkün kılmıştır. İnternet küresel bir boyut kazanmıştır. Artık dünyanın farklı noktalarından insanların birbirine bağlanabildiği, alışveriş yapabildiği, iletişim kurabildiği bir ortam sunmaya başlamıştır.



Şekil 4.1. Türkiye'de İnternet kullanımı

Yaşamımızın büyük bir parçası haline gelen, teknoloji devrimi olarak da nitelendirilen internet içinde fırsatlar bulundurduğu kadar tehditleri içermektedir. İnternette bize sunulan dijital ortamda bu tehditlere karşı korunmamız için en temel yaklaşımlardan biri farkındalıktır. İnternet ortamındaki dijital ayak izimizi her platforma kaydetmemek ve güvenli sitelerle iletişim bulunmak ilk farkındalıklarımız olmalıdır.

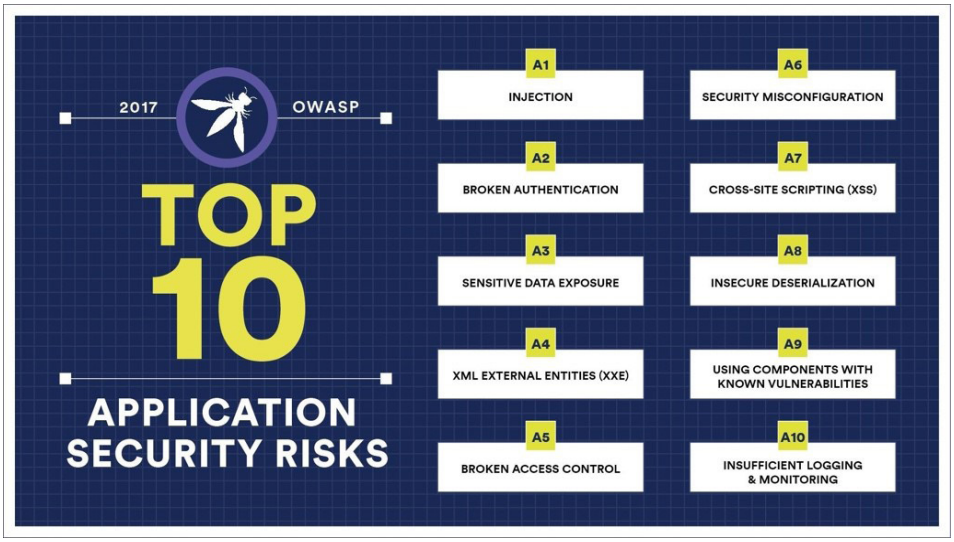
Eriştiğimiz bir sitenin güvenli olup olmadığını nasıl anlayabiliriz? Güvenli siteler ***SSL olarak ifade ettiğimiz güvenlik sertifikasına sahiptir.*** Tarayıcıdaki adres çubuğuna erişmek istenilen adres girildiğinde **"https"** etiketinin olması sitenin SSL sertifikasına sahip, güvenli bir site olduğunu göstermektedir. Tarayıcının adres çubuğundaki kilit sembolü de sitenin güvenli olduğunu göstermektedir. İnternetten güvenli olmayan siteler üzerinden eriştiğimizde kullandığımız cihazlara cihazlarımıza zararlı yazılımların bulaşma ihtimali vardır. İnternette karşılaşacağımız riskleri düşürmek için kullanıcıya düşen temel sorumluluk interneti bilinçli ve güvenli kullanmak konusunda farkındalığının yüksek olmasıdır.

İnternet ortamındaki tehlikeleri sınıflandırmak istersek;

1. Kullanıcıların dijital okuryazarlıklarının düşük olması ile birlikte karşımıza çıkan internette yer alan doğru ve güvenli olmayan içerikler,
2. İnternetin kullanım alışkanlıklarının bedensel ve ruhsal anlamda insan yaşamını olumsuz etkileme durumları,
3. İnternet istismarı ile internet bağlantısı olan cihazlara yapılacak saldırılar olarak sınıflandırabiliriz.

4.1 İNTERNET ORTAMINDAKİ SİBER TEHDİTLER VE TEHLİKELER

İnternet ortamındaki tehdit, bilgi güvenliği üçgenin ihlal edilmesidir. Siber ortamda verilerimiz gizlilik, erişebilirlik ve bütünlük çerçevesinde tutulmalıdır. Verilerin izinsiz alınması, sistemlerin verdiği hizmetleri veremeyecek şekilde hizmet dışı bırakılması, zararlı yazılımların cihazlara bulaşması, tehdit ve şantaj maksatlı verilerin kullanılması ve sosyal medyanın istismarı en fazla karşılaştığımız tehlikeler olarak gösterilebilir. Web tabanlı uygulamaların güvenliği için çalışmalar yapan Açık Web Uygulamaları Güvenlik Projesine **(OWASP)** göre, en önemli 10 web açıkları aşağıda gösterilmiştir [21].



Şekil 4.2. OWASP uygulama güvenlik riskleri

4.1.1 İnternetteki Tehlikeler ve Tehditlerin Sınıflandırması

Siber ortamda paylaşmak istemediğimiz özel yazışmalarımız, fotoğraflarımız ve mahrem bilgilerimize izinsiz erişim sağlanması, siber ortamın kişiler üzerinde bağımlılık oluşturması, insan sağlığını tehdit etmesi ve kullanıcıların siber ortamda işlenen suçlara farkına varmadan hedef haline gelmesi gibi sorunları beraberinde getirmektedir. Bu bağlamda internetteki tehlikeleri şu şekilde sınıflandırabiliriz;

İnternette yer alan içerikten kaynaklanan tehlikeler; terör propagandaları, cinsel istismar küfür ve kötü söz gibi siber zorbalık olarak da ifade edilen bilinçli olarak erişilen veya başka amaçla siber ortamda dolaşırken karşılaşan içerikler bu sınıfa dâhil edilir. YouTube gibi sık kullanılan sosyal medya ortamlarında videoların altına yazılan hakaret, kötü söz veya küfürler bulunmaktadır. Özellikle çocukların bu zararlı içeriklere erişmesi duygusal gelişimlerine zarar vermektedir.

İnternetin kullanım tarzının insan hayatını etkilemesinden doğan tehlikeler; İnternet üzerinden kumar oynamak ya da arkadaşlık sitelerinin olumsuz etkileri internet bağımlılığı olarak kişilerin hayatların olumsuz etkilemektedir. Özellikle internet ortamında oluşan bağımlılıklar kişileri ölüme kadar götürebilen zararlı sonuçlara ulaşabilmektedir. Siber Suçlarla Mücadele Derneği Başkanlığı tarafından oluşturulan **Siberay** programının temel amacı da güvenli internet kullanımı için kullanıcılara ve vatandaşlara yol göstermektir.

İnternetin istismar edilmesi ve internete bağlı bilgisayarlara yapılan saldırılardan kaynaklanan tehlikeler; Siber ortamda yapılan dolandırıcılık, bilgi çalınması, zararlı yazılımlar üzerinden saldırı yapılması ve internet hizmetinin engellenmesi gibi durumlardan kaynaklanan tehlikeler olarak ifade edilir.

4.2 İNTERNETİN İSTİSMARI, SİBER TEHDİT VE TEHLİKELER

4.2.1 Veri Çalınması

İnternet ortamında paylaşılan özel bilgiler, e-postalarla gönderilen içerikler ve forumlarda ya da sosyal medyada paylaşılan bilgiler, bilgisayarlardaki güvenlik zaafiyetleri, zararlı yazılımlar ya da sosyal mühendislik saldırıları ile çalınabilmektedir.

Kişilerin kimlik bilgilerini, fotoğraflarını, ticari sırlarını, kredi kartı bilgilerini içeren mali önemdeki veriler, şifreler ve daha birçok bilgi kontrolümüz dışında çalınabilmektdir. Çalınan verilern farklı amaçlar için kullanılabilmekte ya da siber ortamda satılabilmektedir.

Saldırganların verilerin çalışmasına ortam hazırlayan durum ve faaliyetler;

- Siber ortama erişim yapılan cihazlarda bulunan donanım veya yazılımlarda bulunan güvenlik açıklıklarının kullanılması,
- Sosyal medya veya forum sitelerinde paylaşılan bilgilerin kullanılması,
- Gerçek olmayan tuzak olarak adlandırdığımız internet siteleri üzerine kullanıcıların farkında olmadan bağlantı yapması ile kredi kartı bilgilerini, kişisel bilgilerini ve diğer mahrem bilgilerini bu sitelere oltalama yöntemi ile girilmesi,
- Sosyal mühendislik yoluyla, karşıdaki kişilere inanarak veya onları başka birileri sanarak (arkadaş, akraba, güvenlik birimleri, fima temsilcileri vb.) istenilen bilgilerin verilmesi,
- Sunucu ve kullanıcı bilgisayarlarında yeterli güvenlik tedbirlerinin alınmaması ya da uygun güvenlik sistemlerinin oluşturulmaması ile saldırılara açık duruma gelinmesi,
- Kablosuz iletişim cihazlarında yeterli güvenlik önlemi alınmaması ile iletişim ağından şifresiz olarak geçen verilerin ele geçirilmesi,
- İnternet ağında kablolu ağ üzerinde veya aktif ağ cihazlarında (yönlendirici, anahtar vb. cihazları) yetkisiz dinleme yapılması,
- Bilgisayarlara casus yazılım olarak ifade edilen truva atları, tuş kaydedici yazımlar, arka kapı yazılımlar veya zombi bilgisayar yazılımların kurulması.

4.2.2 Sistemlerin Hizmet Dışı Bırakılması

İnternete bağlı olan sunucu sistemleri, internet siteleri, e-devlet siteleri, paylaşım siteleri, firma sunucuları, askeri sistemler gibi sistemler, kullanıcıların hizmet almasını engellemek için saldırıya uğrayabilir ve hizmet dışı kalabilir. Sistemleri hizmet dışı bırakmak için kullanılan yöntemler;

- Kullanılan yazılımlara yerleştirilen arka kapılar,
- Tuzak donanımların kullanılması ve bu tuzakların zamanı geldiğinde aktif duruma getirilmesi,

- Sistemlerde bulunan yazılım ve güvenlik zafiyetlerinin kullanılması,
- Zararlı yazılımların farklı yöntemlerle bilgisayarlara yüklenmesinin sağlanması ile sistemlerin devre dışı bırakılması,
- Zombi bilgisayarlar üzerinden dağıtık hizmet dışı bırakma (DDOS) saldırıların gerçekleştirilmesi.

4.2.3 Zararlı Yazılım Yüklenmesi

Virüs, Truva atı, tuş kaydedici, arka kapı, solucan gibi zararlı yazılımlar farklı yöntemlerle bilgisayarlara bulaşarak sistemleri yavaşlatabilir, bozabilir ya da hizmet dışı kalmasına veya veri çalışmasına neden olabilir. Zararlı yazılımların bilgisayarlara bulaşma yöntemleri;

- Zararlı içerik sunan internet sitelerine erişim,
- Saldırganlar tarafından ele geçirilen ve güvenlik açıklıklarını kullanan kodların bulunduğu internet sitelerine bağlanılması,
- Oltalama saldırıları ile beraber zararlı internet sitelerine bağlanılması,
- CD, DVD ve USB bellek gibi harici donanımlara virüs taraması yapılmadan bilgisayara takılması,
- İnternetten indirilen dosyaların virüs kontrolünden geçirilmemesi,
- Herkesin kullanımına açık, amacı dışında içine zararlı kod yerleştirilmiş ücretsiz yazılımların kullanılması,
- Lisanslı yazılımların kırılmış (crack) sürümlerinin kullanılması ile güvenlik zafiyetlerine açık olunması,
- Bağlanılan sitelerde, açılan pencerelerdeki her soruya okumadan "evet" denilmesi ile bilgisayara yüklenen farklı amaçlı programların olması,
- E-posta ile gönderilen içinde zararlı yazılım içeren programların bilgisayara yüklenmesidir.

4.2.4 Tehdit ve Şantaj Maksatlı Kullanım

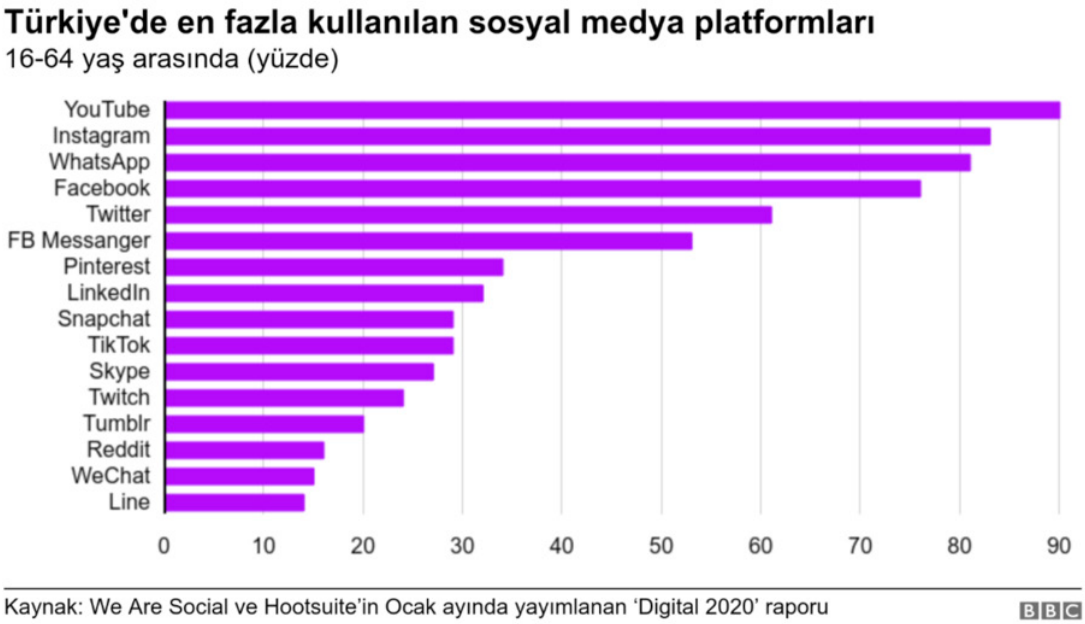
Farklı yöntemlerle elde edilen kişisel ve kurumsal veriler ile kişi ve kurumların verilerini ifşa ederek gerçek ya da gereçek dışı haberler yapılabilmektedir. Gerçek dışı haber ve yayınlar dijital

ortamda geleneksel medya ortamlarından daha hızlı yayılmaktadır. Hızla yayılan bu ifşalar kişi ve kurumlar için tehdit ve şantaj unsuru olarak kullanılabilmektedir. Siber dünyada kullanılan farklı İnternetin sağladığı imkânlar sayesinde, özel teknikler kullanılarak başka adresler hedef gösterilebilmekte, yakalanmadan kurum veya kişiler tehdit edilebilmektedir.

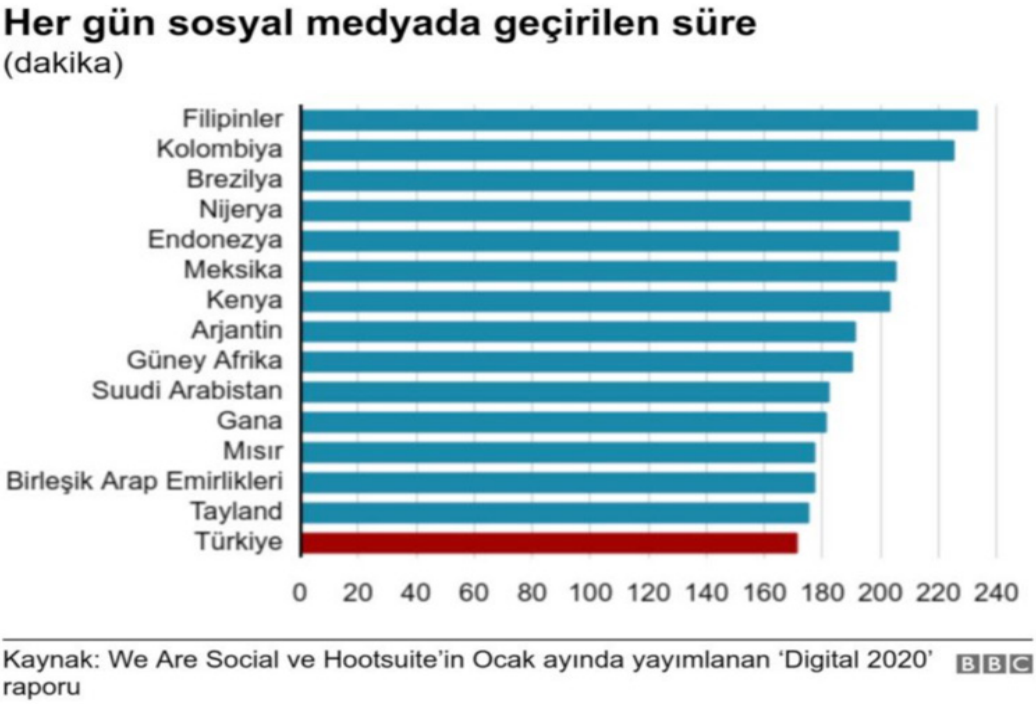
4.3 SOSYAL MEDYANIN İSTİSMARI

Sosyal medya, kurumlar topluluklar ve bireyler arasında etkileşimli bir iletişim imkânı sağlayan, kullanıcı veya müşterilerin ürettiği içeriğin yer aldığı web tabanlı uygulamalara verilen genel isimdir. İnternet forumları, internet günlükleri, video resim ve dosya paylaşım siteleri, kişisel sayfalar, bilgi paylaşım, arkadaşlık ve haber paylaşım siteleri gibi internet hizmetleri bu gruba girmektedir.

Facebook, Twitter, YouTube, Instagram sosyal medya platformlarına örnek olarak gösterilebilir. Sosyal medya, kişiler arasında yaygın oldugu kadar devlet kurumları ve firmalar arasında da resmi hesaplar açıklarak yaygın olarak kullanılmaktadır.



Şekil 4.3. Türkiye'de kullanılan sosyal medya platformları



Şekil 4.4. Sosyal medyada geçirilen süre

Sosyal medyanın istismarına yol açan davranışlar;

- Tanınmayan kişilerle arkadaşlık kurmak,
- Mahrem bilgi ve fotoğrafları paylaşmak,
- Arkadaşlar listesinde gereksiz ayrıntıların verilmemesi,
- Yasa dışı veya çalışılan kurumun ilkelerine aykırı görüş ve düşüncelerin dile getirmek,
- Gündelik hayata yönelik tehlikeli ayrıntıların verilmesidir. Özellikle sosyal medya üzerinden yapılan açık konum belirtmeler hırsızlar için değerli bir bilgi olarak kullanılmaktadır.
- Kullanıcılar, sosyal medyayı kişisel kullanımdan kaynaklanan tehditlerin yanında, sosyal medya platformlarının güvenlik açıklıklarından kaynaklanan tehditlere de maruz kalabilmektedir.

4.3.1 Sosyal Medyada Güvenli İletişim

Sosyal Medya kullanımındada tıpkı internet kullanımındaki gibi tedbiri elden bırakmamak ve gerekmedikçe kişisel bilgi paylaşımından kaçınmak gerekir. Tanımadığınız kişilerle bağlantı kurmak son derece güvensiz ve tehlikelidir. Konum bilgileride kişisel bilgilerimizden biri olduğu için sosyal medyanın güvenli kullanımında gerekmedikçe paylaşılmamalı gizli tutulmalıdır. Gizlilik ayarları da bir dereceye kadar açılmalı ve sadece tanıdığınız kişilerle irtibat halinde kalmak istiyorsanız hesap gizliliğini onaylamanız gerekir. Sosyal medya için en önemlisi güçlü parola oluşturulmalıdır. Herkes tarafından kullanılan, tahmin edilmesi kolay sayılabilecek (içerisinde doğum tarihi, adınız, soyadınız, yaşınız, varsa evcil hayvanınızın ismi vb.) gibi sizi tanıyan insanların aklına gelebilecek bilgileri içeren parolaları kullanmaktan kaçınılmalıdır. Parolalar en az 8 karakter olmalıdır. Karakter sayısının arttırılması da parolanın güçlü olmasına katkı sağlar. Parola içinde büyük harf, küçük harf, rakam ve en az bir özel karakter içermelidir.

4.3.2 Sosyal Medyada ve Güvenlik Ayarları

Sosyal medyada güvenliğinizi sağlamak için ilk ve en önemli aşama kullandığınız sosyal medyanın güvenlik ayarlarını öğrenmek olmalıdır. Sosyal medya hesaplarınızda bulunan güvenlik ayarları ile profilinizi gizli hesaba geçirebilirsiniz. Profilinizin herkese açık olarak tutulmasına dikkat ediniz. Paylaşımlarınıza yapılan yorumlarınızı filtreleyebilir ve rahatsız edici hatta siber zorbalık anlamında yer alabilecek yorumları kaldırabilirsiniz. Yorumları yapanları da engelleyip, platformların yöneticilerine şikâyet edebilirsiniz. Sosyal medya üzerinden yapılan siber zorbalık ile ilgili ekran görüntüleri alınıp hukuki yollara başvuru yapabiliriniz.

Sosyal medyada güvenlik ayarlarını kullanarak, şifrenizi sık aralıklarla değiştirebilir, hesaplarınıza yapılan giriş çıkış hareket kayıtlarını kontrol edebilirsiniz. Sosyal medya hesaplarınız için güvenlik seviyenizi arttırmak için iki faktörlü kimlik (2FA) doğrulamasını aktif edebilirsiniz.

Profilinizi güvenli duruma getirmek için sosyal medya platformlarında kişisel bilgilerinizi paylaşmamalısınız.

Profilinizi ve paylaşımlarınızı tanıdığınız kişilerle sınırlandırmalısınız. Sosyal medya hesapları üzerinden size ulaşan mesajların tehlikeli olabileceğini düşünüp, tanımadığınız kişilerden gelen mesajlara karşı dikkatli ve temkinli olmalısınız.

Şekil 4.5. Sosyal medya ve güvenlik

Sosyal medya üzerinden yapılan e-alışverişler konusunda da dikkatli olunmalıdır. Satışı yapan hesapların ve ödeme sistemlerinin güvenli olup olmadığı araştırılmalıdır. Yaş kısıtlaması olarak 13 yaşının altındaki çocukların sosyal medyayı kullanmaması gerekmektedir. 13 yaşındaki çocukların ise 18 yaşına kadar ebeveyn gözetiminde kullanması daha güvenlidir.

4.4 İNTERNET TARAYICILAR

İnternet tarayıcıları veritabanında sundukları bilgilere ulaşmamızı sağlamaktadır. İstediğiniz bir ürüne ulaşmak için sitenin adını veya adresini adres çubuğuna yazarak ilgili sayfaya ulaşılabilir.

Şekil 4.6. İnternet tarayıcılar

Sık tercih edilen İnternet Tarayıcıları;

- Chrome
- İnternet Explorer
- Mozilla Firefox
- Safari
- Opera en sık tercih edilen internet tarayıcılarından bazılarıdır.

4.4.1 E-posta ve Web Tarayıcı Gizliliği

E-posta, mektup göndermeye benzemektedir. E-postanın kopyaları erişimi olan herkes tarafından okunabilmektedir. E-postalar farklı sunucular arasında aktarılır. E-postanızın saldırganlar tarafından kullanılıp, kullanılmadığı ile ilgili https://haveibeenpwned.com/ sitesini ziyaret edebilirsiniz.

Web tarayıcının gizli modunu kullanmak, başkalarının çevrimiçi etkinlikleriniz hakkında bilgi toplaması engelleyebilir.

Gizli Mod desteği olan popüler tarayıcılar;

- Microsoft Internet Explorer: InPrivate
- Google Chrome: Incognito
- Mozilla Firefox: Private tab / private window
- Safari: Private: Private browsing

4.4.2 Tarayıcı Eklentileri

Tarayıcı eklentisi web sitesine sayısız özellik ve işlev eklemektedir. Bu eklentiler web sitesinin arayüzünü değiştirebilme gibi bir sürü özelliği de beraberinde getirmektedir. Tarayıcı eklentileri genellikle API'ler kullanılarak oluşturulur. API'ler bir uygulamaya ait yeteneklerin, başka bir uygulamada da kullanılabilmesi için, yeteneklerini paylaşan uygulamanın sağladığı arayüzdür. Arka planda çalışan küçük programlardır. Küçük olmasının yanı sıra çok büyük işlevleri vardır. Örnek olarak Mozilla Firefox tarayıcısında desteklenen aşağıdaki gibi eklentiler sayesinde;

- Bir web sitesini geliştirip tamamlayabilmek,
- Kullanıcıların kişiselleştirmesine izin vermek,
- Web sayfasına içerik eklemek ve silmek,
- Araçlar ve yeni gözatma özellikleri eklemek,
- Oyunlar eklemek ve oynayabilmek,
- Geliştirici araçları eklemek ve web sitesinde istenilen düzenlemeyi yapabilmek,

- Reklamları engelleyebilmektir.
- Google Chrome tarayıcısının eklentilerine göz atmak istenirse yapılması gereken eklentiyi Chrome Web Mağazasından bulup Chrome'a ekle butonuna basmaktır.
- Chrome'da en çok kullanılan 3 Eklenti;
- Hover Zoom+ : Görselleri üstüne tıklamadan açmaya ve sadece klavyede ki "s" tuşuna basarak kaydetme imkânı sağlamaktadır.
- Adblock: Web sitesindeki reklamların %95'i engelleyen bir eklentidir.
- Print Friendly & PDF : Sitedeki gereksiz resimler ve sözcükler kaldırılabilir ve pdf formatına dönüştürülme, gmailden gönderme gibi seçenekler sunulmaktadır.

Tarayıcı Eklentileri Güvenliği:

Tarayıcı Eklentilerinin bu kadar çok özelliği olması ve bize bir sürü kolaylıklar sağlamasının yanı sıra güvenliğimizi ve gizliliğimizi tehdit de edebilir mi? Tamamen kötü amaç için eklenmiş, bilgilerimizi ele geçirmek için eklentiler olabilir. Bu eklentilere izin verme durumunda çünkü o eklenti izin vermediğimiz zaman eklenmemektedir. İstenilen izinde için *"ziyaret ettiğiniz tüm web sitelerindeki tüm verilerinizi okuma ve değiştirme"* şeklinde bir ifade karşımıza çıkmaktadır. En basit eklenti için bile izin süreci bulunmaktadır. Bu izin verildiği durumda eklentiler verilerinize erişim hakkı kazanıyor. Tarayıcı eklentileri suçlular için ilgi çekicidir. Çünkü birçok eklenti oldukça kapsamlı bir kullanıcı veritabanı bilgisini içermektedir. Tarayıcı eklentilerinin güvenlik açısından risk oluşturabilecek bir yönü de eklentilerin kullanıcıların kontrolünden bağımsız, otomatik olarak güncellenebiliyor olmasıdır. Güvenliğinden emin olduğunuz bir eklenti sonrasında kötü amaçlı kişilerce kötü amaçlı bir eklenti olacak şekilde güncellenebilmektedir. Bu uzantının güncellemesini farketmeden indirebilirsiniz. Çoğu eklenti kötü amaçlı kullanılmıyor. İstedikleri verileri para elde etmek amaçlı üçüncü taraflı kişilere satabilmek oluyor.

Web of Trust eklentisi kullanıcıların tüm tarama geçmişini kayıt altına tutuyordu. Bir web sitesinin iddiasına göre de, Web of Trust kaydettiği verileri güvenli bir biçimde anonim haline getirmeden üçüncü taraflarca satmasıydı. Mozilla Firefox bu yüzden uzantıyı mağazasından kaldırdı. Sonrada ise eklentinin geliştiricileri, eklentiyi diğer tarayıcıların web mağazalarından da kaldırmıştır. Fakat birkaç ay sonra eklenti mağazalara geri yüklenmiştir. Web of Trust kötü amaçlı

bir eklenti olarak düşünülmemiştir. Ancakd kullanıcıların bilgilerini güvenli bir biçimde anonim hale getirmeden üçüncü taraflarca satılması Kişisel Verileri Koruma Kanunu kapsamından da yasal olarak suç teşkil etmektedir. Bu durum kullanıcıların bilgi güvenliğini, mahremiyetini ihlal etmek anlamına gelmektedir.

Eklentiler Nasıl Güvenli Bir Biçimde Kullanılabilir?

Güvenlik açısından kullanılmaması önerilmektedir. Ya da güvenlik problemini en aza indirgemek için şu adımları izlemeniz önerilebilir;

- Sadece ihtiyacınızın olduğunu düşündüğünüzün eklentiyi indirmek,
- Eklentiyi indirirken istenilen izinleri kontrol etmek, anlayamadığınız bir izin maddesi varsa o eklentiyi indirmemek,
- Eklentiyi kurulum yapılıp kullanılmaya başlandıktan sonra bir güncelleme istiyorsa eklentiyi silmek,
- Eklentileri resmi siteler üzerinden indirmek de riski azaltabilir. Şunu da biliyoruz ki; kullandığımız hiçbir sistem için yüzde yüz güvenlik bulunmamaktadır.

4.4.3 Çerez (Cookie) Yönetimi

Kullanıcının ziyaret ettiği web sayfaları tarafından bilgisayarlarda saklanan dosyalar çerezler olarak adlandırılır. Çerezler, kullanıcı ile ilgili tercih edilen dil ayarları, parolalar gibi çeşitli bilgileri barındırırlar. Bu sayede web sayfasına tekrar girildiğinde kullanıcının tercihlerine göre özelleştirilmiş özellikler görüntülenmektedir. Ancak burada tutulan veriler, güvenlik riski barındırabilirler. Bilgisayarda tutacakları çerezler ile ilgili Kişisel Verileri Koruma Kanunu kapsamında bilgilendirme yapılmak zorundadır. Sitelerin için onaylanan çerez politikasını iptal etmek için tarayıcınızın ***"gizlilik ve güvenlik"*** seçeneğinden çerez ayarlarına gidilip düzeneleme yapılabilir.

4.4.4 Parola Yönetimi

Tarayıcının üzerindeki kayıtlı parolaları kontrol etmek istiyorsanız kullandığınız tarayıcının parola yöneticisini kullanabilirsiniz. Güvenlik ve gizlilik açısından güvenli olmayan sitelere parolanızı ve kişisel bilgilerinizi kaydetmemelisiniz. Oluşturduğunuz parolalarınızı hiçbir elektronik

ortamda ya da bulutta saklamamalısınız. Sakladığınız ortamın hacklenmesi ile parolalarınız da ele geçirilebilir. Bazı firmalar şifre yönetimine o kadar önem vermektedir ki çalışanları için parola politikası oluşturmaktadır. Google üzerinden Şifre Yöneticisi ayarlarında "Şifre Güvenliği'ne git" butonuna basarak kayıtlı parolalarınızı kontrol edebilirsiniz.

Şekil 4.7. Şifre yöneticisi

4.5 İNTERNETTE GÜVENLİ İLETİŞİM

Öncelikle Antivirüs Yazılımları Güvenli Bir İnternet İçin Yeterli midir? Klasik antivirüs yazılımları imza tabanlı olduğu için virüsün yakalanması için o virüsün imzasına ihtiyaç duyulur. Her geçen gün farklı özellikle virüs yazılımı siber ortama sunulmaktadır. Antivürüs firmalarınında yazmak zorunda kaldığı virüs imzalarının sayısı hızla artmaktadır. Çok sayıda zararlı yazılımın ortaya çıktığı bir ortamda imza tabanlı antivürüs yazılımlarının üretimi yetersiz kalmakta bu yazılımların tek başına sistemi tehditlerden koruması mümkün olamamaktadır.

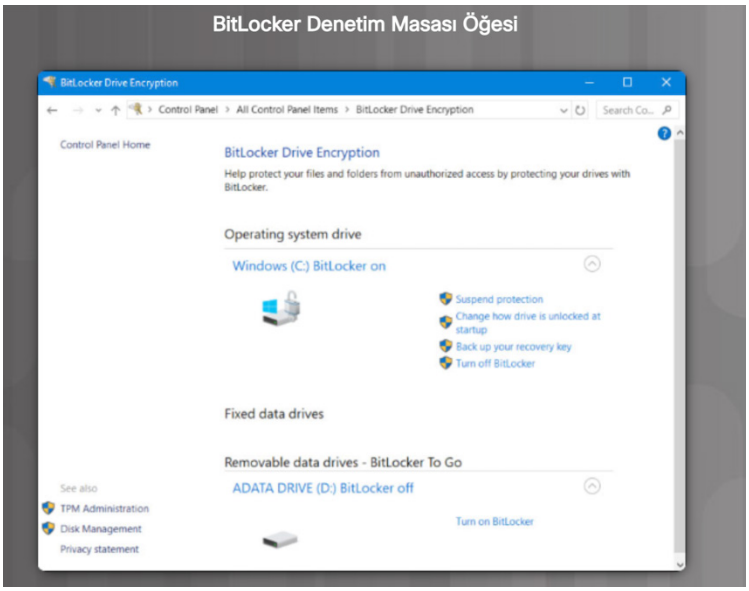
4.5.1 İnternette Tehlikelerden Korunma ve Güvenli İletişim Kurma

İşletim sistemi bilgisayar donanımını etkin olarak kullandığımız yazılımdır. İşletim sisteminin güncel olması önemlidir. Güncelliğini yitirip, üretici firmanın desteğini bıraktığı işletim sistemleri kullanılmamalıdır. İşletim sisteminin otomatik güncelleme seçeneği de aktif tutulmalıdır.

Lisanslı bir antivirüs programı kullanılmaldır. Virüs programının da güncellemeleri düzenli yapılmalıdır. Bilgisayardaki kullanıcı hesaplarının, kullanılan e-posta hesaplarının veya diğer

sosyal medya platformlarının parolaları tahmin edilmesi zor ve güvenli parolalar olmalıdır. Tüm sistemler üzerinde aynı parolalar kullanılmamalıdır. Parolalar düzenli aralıklarla değiştirilmelidir. Güvenli olmayan internet sitelerinden yazılıp indirilmemelidir.

Kaynağı bilinmeyen e-postalar da açılmadan önce dikkatli olunmalıdır. Özellikle e-posta içerisinde gelen bağlantılara tıklamadan önce bağlantının kontrol edilmesi gerekir. Bilgisayarda sabit diski veya diskin bir kısmını şifreleyen BitLocker gibi programlar kullanılabilir. Verilerin şifrelenmesi verilerin okunmasını zorlaştıracaktır. Böylece veriler güvenli saklamak mümkün olacaktır.



Şekil 4.8. Bitlocker

Bilgisayarda dosya ve dizinler paylaşıma açılırken dikkatli olunmalıdır. Gerekli dosya ve dizinler paylaşıma açık tutulmalıdır. Özellikle evlerde internete bağlanmak için kullanılan kablosuz modemlerin işletim sistemleri de güncellenmelidir. Ayrıca; modemler ile birlikte kullanılan varsayılan parolar da değiştirilmelidir. İnternet tarayıcılarının da güvenlik güncellemeleri yapılmalıdır. Tarayıcı güvenlik ayarları da yapılmalıdır.

İnternet ortamında gezinti yaptığınız siteler, sosyal medya platformları aracılığı ile büyük veriye yaptığınız katkınız siber dünyada bıraktığınız izler ile izlenebilir. Bu anlamda siber dünyada ürettiğiniz veri ve yaptığınız hareketler için sorumlu olduğunuzu unutmayınız.

4.6 HTTP ve WEB GÜVENLİĞİ

Kitabın ilk bölümünde özetle ifade edildiği gibi, http en yaygın kullanılan uygulama protokolüdür. Uygulama protokolü olması, OSI modelinin 7.katmanında çalıştığını ve kullanıcı ile en yakın etkileşimde olması nedeniyledir. Bu alt bölümde, http protokolünün nasıl çalıştığı ayrıntılı olarak ele alınmıştır.

4.6.1 http Protokolünün Temelleri

Son kullanıcıların en çok yaptığı işlemlerden biri web sayfalarında gezinmektir. Bu durumda http protokolü çalışır ve web tarayıcı kullanarak iletişimi başlatan (istemci) ile web hizmetini veren (sunucu) arasında istemci-sunucu mimarisinde bir takım kurallar çerçevesinde iletişim gerçekleşir.

Şekil 4.9. http İstemci Sunucu haberleşmesi

İstemci tarafından gönderilen http isteğine (http request) sunucu tarafından yanıtlar (http response) verilir ve veri takası gerçekleşir. Yukarıdaki örnekte, google.com adresine varsayılan port (80) ile http isteği gönderilmesi gösterilmiştir. İstemci tarafından gönderilen http request mesajının başlık yapısı (header) şekildeki gibidir.

```
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:36.0) Gecko/20100101 Firefox/36.0
Accept: text/html,application/xhtml+xml
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Örnekte yer alan başlık bilgisindeki alanların açıklamaları aşağıda maddeler halinde verilmiştir.

- **GET**: http istek mesajının metodunu belirttir. Bir veri talebini belirten GET dışında, POST, PUT, DELETE gibi mesaj türleri de vardır.
- **PATH (/)** : Sunucudan hangi sayfanın istediğini, yolu (path) belirtir. "/" ifadesi, ana sayfanın istemci tarafından istendiğini ifade eder. Eğer sunucuda bir dizin altındaki bir dosya isteniyorsa, yol olarak da belirtilebilir. Bu durumda ifade "/sayfalar/dosyalar.php" gibi görünür.
- **HTTP/1.1**: Kullanılan http protokolünün sürümünü belirtir.

http isteğinin başlık bilgisinde yer alan diğer alanlar **başlık_adı:değer** şeklinde ifade edilmiştir. Bir sonraki satırda;

- **Host:** www.google.com , isteğin bir IP adresinde barındırılan hangi konak ile iletişime geçilmesi istendiğini ifade eder. Host değeri ile path değerinin birleşimi URL adresini verir. Bu örnekte URL adresi, www.google.com/ olacaktır.
- **User-Agent:** İstemci hakkında, kullanılan tarayıcı, işletim sistemi gibi bilgileri barındırır. Bu değer sayesinde web sayfaları, istemcinin hangi tarayıcıyı kullandıklarını öğrenebilir.
- **Accept:** İstemcinin cevap olarak hangi dosya türlerini kabul edeceğini belirten alandır.
- **Accept-Encoding:** Yine kabul edilen dosya türlerine ilişkin kodlayıcı bilgileri barındırır. Örneğin sıkıştırılmış dosyalar gibi.
- **Connection:** Sunucu ile iletişimin şeklini belirtir. "Keep-Alive" olması, her isteğin bağımsız olarak ele alınmaması gerektiğini ve iletişimin devam ettirilmesi gerektiğini belirtir.

http Request mesajına sunucu tarafından **http Response** ile cevap verilir. Aşağıda örnek bir cevap paketi gösterilmektedir.

```
HTTP/1.1 200 OK
Date: Fri, 13 Mar 2015 11:26:05 GMT
Cache-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 258

< SAYFA İÇERİĞİ >
```

Cevap içerisinde yer alan HTTP/1.1 ifadesi kullanılan protokolün sürümünü ifade eder. 200 ve OK ifadeleri de sırasıyla cevabın durum kodunu (status code) ve bu kodun anlamını gösterir. Cevap kodları IANA tarafından sağlanır ve temelde beş grup altında toplanır.

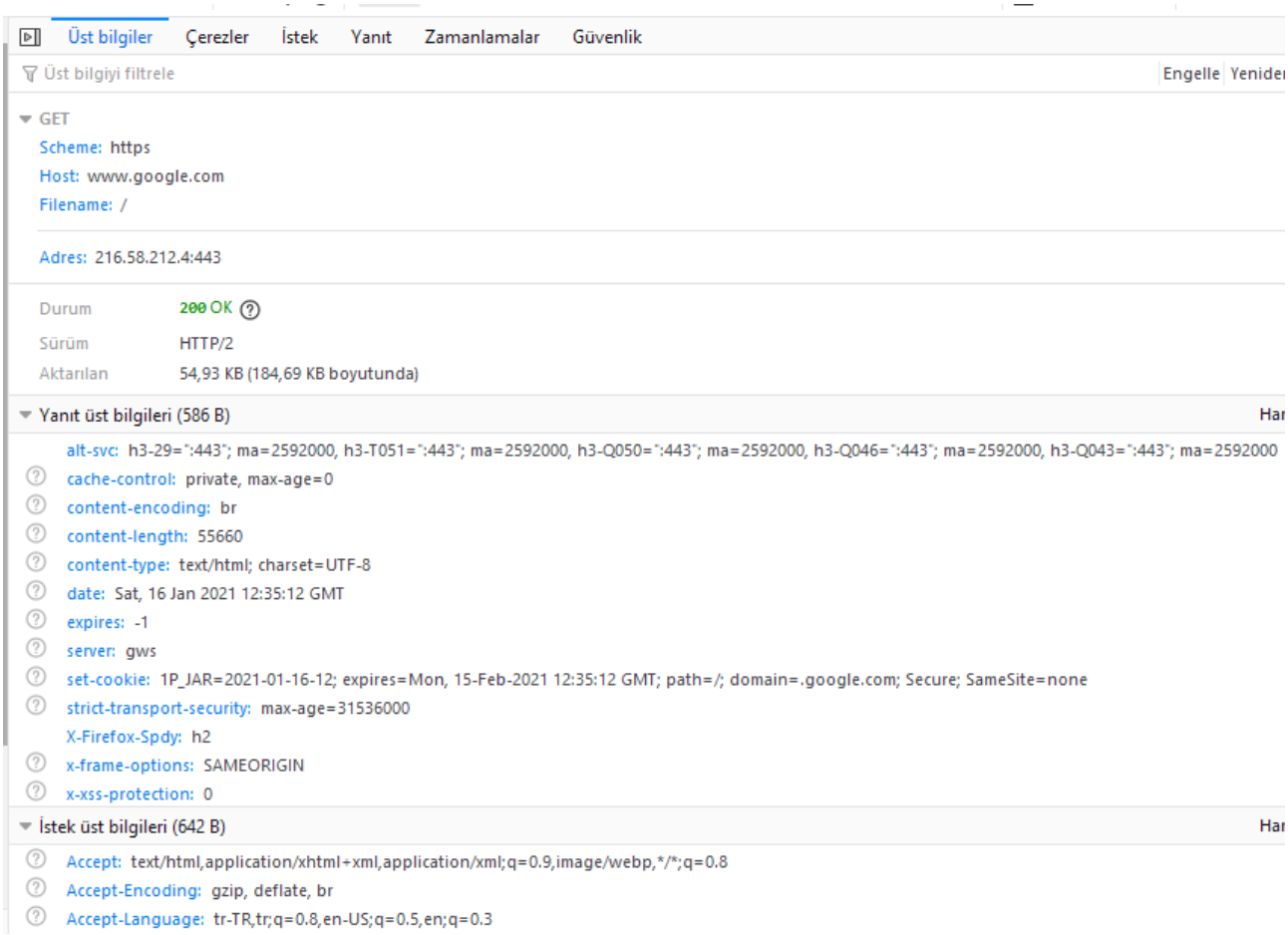
Cevaba ilişkin bilgileri barındıran durum kodlarının bazıları tabloda gösterilmiştir.

Türü	Durum Kodu	Açıklama
Bilgilendirme 1xx	100	"Continue"... İstemcinin isteğine devam etmesi ya da bitmişse bu bilgiyi yoksayması gerektiğini gösterir.
	102	İşleniyor... Alınan bilginin işleniyor olduğunu belirtir.
Başarılı Yanıtlar 2xx	200	"OK"... Kaynak alındı ve mesaj gövdesinde gösterildi.
	201	İstek başarılı ve sonuç olara yeni bir kaynak oluşturuldu. Genellikle POST veya PUT isteklerinden sonra gönderilir.
Yönlendirmeler 3xx	301	"Moved Permanently". İstenen URI kaynağı değiştirildi. Kaynağın yeni adresi cevapta gönderilebilir.
İstemci Hataları 4xx	400	"Bad Request". Sunucu isteği hatalı sözdizimi gibi nedenlerle anlayamadığını belirtir.
	401	"Unathorized". İstemcinin kimlik doğrulamadan geçemediğini belirtir.
	403	"Forbidden". İstemcinin kimliği biliniyor. Ancak erişim izni yok.
	404	"Not found". Sunucu istenen kaynağı bulamıyor. Bazen sunucular kaynağın var olduğunu gizlemek için "403" hatası yerine bu hatayı da gönderebilir.
Sunucu hataları 5xx	500	"Internal Server Error". Sunucu nasıl ele alacağını bilemediği bir hata ile karşılaştı.
	503	"Service Unavaliable". Sunucu bu isteği işlemeye hazır değil.

Başlık bilgisindeki durum kodlar, sunucu ya da durum ile ilgili birçok bilgiyi barındırır.

http Response alanındaki diğer bir veri, **"Date"** alanıdır ve cevabın üretildiği zamana ilişkin bilgileri verir. Bant genişliğinden tasarruf ve hız için kullanılan başlık alanı, **"Cache-Control"** alanıdır. İstemci tarafından alınan verilerin önbellekte ve tutulması her defasında ile ilgili anlaşmayı ve bu süreyi içerir. **"Content-Type"** alanı, cevapta gelen içeriğin nasıl yorumlanacağını ve nasıl

kodlandığını belirtir. Bu örnekte mesajın html mesajı olduğu belirtilmiştir. "Content-Encoding" alanı, bir önceki type alanının genişlemesi olarak düşünülebilir. Bu örnekte, gzip ile sıkıştırıldığı ifade edilmiştir. "Server" alanı, sunucunun başlığını (bu örnekte gws-Google Web Server), "length" alanı ise mesajın boyutunu byte olarak belirtir.



Şekil 4.10. http İstemci Sunucu haberleşmesi

Şekil 4.10'daki ekran görüntüsünde www.google.com adresine yapılan http requeste verilen http Response mesajı Firefox web tarayıcı geliştirici seçenekleri ile görüntülenmektedir. http, doğası gereği açık metin (clear-text) bir protokoldür, yani paketlerin yetkisiz kişiler tarafından

yakalanması durumunda içeriği okunabilir. Aynı şekilde güçlü bir kimlik doğrulama mekanizması sunmamaktadır. http'nin güvenli olmasını sağlamak için SSL/TLS denilen kriptolojik protokol ile birlikte kullanılır **(https).** Bu sayede şifreleme ile güvenlik daha doğrusu gizlilik sağlanmış olur.

4.6.2 Web Güvenliği

Günlük hayatımızda mobil uygulamalar kadar çok kullandığımız web sitelerinin güvenliği bizler için çok önemlidir. Yapılan birçok çalışmada kullanıcıların zafiyet yaratacak şekilde üyelik oluşturdukları ve bunu neredeyse tüm sitelerde tekrar ettikleri tespit edilmiştir. Örneğin bir kullanıcı A sitesine üye olurken kullandığı e-posta adresi ve kullanıcı şifresi ile B sitesine de üye olmaktadır Hatta kullandığı e-posta adresinin şifresinin de aynı olması muhtemeldir. Dolayısı ile teknik nedenlerden kaynaklanan sorunların yanı sıra, kullanıcı hatalarından kaynaklı sorunlar da web sitelerinde yaşanabilecek siber güvenlik zafiyetlerini oluşturmaktadır.

SQL Enjeksiyon Zafiyeti

En sık karşılaşılan ve kitabın önceki bölümlerinde açıklaması yapılan bir zaafiyet türüdür. Birçok kurum bu saldırıdan nasibini almıştır. Web siteleri kayıtlarını veritabanı üzerinde tutmaktadır. Kullanıcı adı ve şifre kullanılarak giriş sağlayan formlar gibi kullanıcı arayüzleri ile veritabanı üzerinde işlem yapılmasını sağlayan sistemler eğer form üzerinden gelen verilerin kontrolü doğru bir şekilde yapmaz ise bu zafiyetin kurbanı olmaktadır. Bu açık bulunan web sitesinde, örneğin site içerisinde arama yapabileceğiniz basit bir arama kutusu kullanılarak site yöneticisine ait kullanıcı adı ve şifre elde edilebildiği gibi tüm veritabanının indirilmesi de sağlanabilir. Kullanıcı kaynaklı bir hata olmamakla birlikte yazılımcı kaynaklıdır.

XSS (Cross Site Script) Zafiyeti

SQL Injection zafiyetinden sonra en çok rastlanan zafiyet türü XSS zafiyetidir. Kelime anlamı olarak çapraz kod olan XSS, en basit anlatım olarak kullanıcının girdiği verilerin kontrol edilmemesinden kaynaklı olarak yetkisiz bir kullanıcının zararlı kod çalıştırabilmesidir. Örneğin üyelik sistemi olan bir sitede kullanıcı adı ve şifre girilebilecek alanın XSS zafiyeti varsa herkese açık bu arayüzün saldırgan tarafından da kullanılabileceği demektir. Bu zafiyet kullanıcı hatası kaynaklı olmamakla birlikte kullandığımız web sitesinin kodları ile ilgilidir.

iFrame Zafiyeti (iFrame Injection)

Bir bankanın web sitesinde keşfedilen bu açık farklı bir tür XSS atağıdır. iFrame web sitesi içerisinde başka bir web sitesini veya aynı sitenin başka bir sayfasını göstermemize yarayan yapıdır.

iFrame zafiyetinin keşfedildiği banka sitesinde kullanıcıların çevrimiçi bankacılığa giriş ekranı bir iframe içerisinde yer almakta ve burada uygulanan atak ile giriş yapan kullanıcıların başka bir web sitesine yönlendirilmesi sağlanmaktadır. Bankaya yapılan bu saldırı örneğinde, müşteri bilgilerinin farklı bir yere aktarılabileceğini düşününce konunun ciddiyeti kat kat önem kazanmaktadır.

Oturum Yönetimi Zafiyeti

Oturum, bir web uygulamasına giriş yapıldığına sunucuda ve kullanıcı bilgisayarında oluşturulan bilgidir. Bu bilgi HTTP başlık bilgisi ile iletilir. SessionID ile ifade edilen kullanıcıya ait oturum bilgisi uygulamayı geliştirenler tarafından mümkün olduğunda karmaşık şekilde oluşturulmalıdır. Eğer tahmin edilebilir bir SessionID değeri bulunur ise bundan yola çıkarak birçok kullanıcıya ait oturum bilgileri elde edilmiş olur. Kullanıcı tarafında yapılacak bir XSS atak ile de bu bilgiler elde edilebilmektedir. Dolayısı ile kullanıcının güvenliği için web sitelerinin de güvenliğinin sağlanması bunun gibi zafiyetlerin önüne geçmek için gerekli bir zorunluluktur.

Kaba Kuvvet Saldırı

Kaba Kuvvet ya da deneme yanılma saldırıları (brüte force) yıllardır kullanılan bir yöntemdir. Kısaca bahsetmek gerekirse web sitesi, e-posta adresi gibi bir uygulamaya girmek istediğinde ihtiyaç duyulan iki şey vardır; kullanıcı adı ve şifre. Bir siber korsanın birçok kullanıcı adı ve paroladan oluşan liste ile denemeler yaptığında doğru kombinasyonu bulması sadece biraz zaman gerektirecektir. Hatta bu işlemi yapan programlar ile gerekli olan zamanı kısaltmak da mümkün olmaktadır.

Günümüzde web uygulamaları belirli sayıdaki denemeden sonra yeni bir deneme için belirli bir zaman geçmesini bekleyerek kaba kuvvet saldırılarını engellemeye çalışmaktadır. Ayrıca hatalı bir denemeden sonra giriş yapmaya çalışanın bilgisayar mı insan mı olduğunu ayırt eden uygulamalar kullanılmaktadır.

Oltalama ve Sosyal Mühendislik

Oltalama ve Sosyal Mühendislikte hedef sistem değil kullanıcıdır. Kullanıcıların zafiyetlerinden faydalanıp onları kandırarak çeşitli bilgiler elde edip daha önce anlattığımız yöntemlerle birlikte sisteme yetkisiz girmeyi hedeflemektedir. Geçtiğimiz yıllarda Sosyal Mühendislik kullanılarak çok büyük bir veri zafiyeti yaşanmıştır. 270bin Facebook üyesine gelen anketi doldurdukları takdirde 5$ kazanacakları mesajına inanıp birçok bilgiye erişim izni vermeleri ile yaklaşık 50milyon kişinin çeşitli bilgilerine izinsiz olarak erişilmiştir. Bu olay Cambridge Analytica olayı olarak medyada çok yankı bulmuştur. Her gün birçok oltalama ve sosyal mühendislik olayı yaşanmakta, çoğunda

benzer senaryolar ile kullanıcı verilerine erişilmektedir. Neredeyse hiçbir uygulama kullanmadan sadece hedef kişiden çeşitli bilgiler edinerek zafiyet yaratılması siber güvenlikte en zayıf noktanın kullanıcı olduğunu ortaya koymaktadır.

HTTPS Önemi

HTTPS, veri aktarım yöntemi olarak bildiğimiz HTTP metodunun güvenli halidir. Farklı bir bağlantı portundan SSL ile şifrelenmiş olarak veri alış-verişini sağlayan bu protokol ile web uygulamalarında veri akışının güvenli bir şekilde sürdürülmesi sağlanmaktadır. Günümüzde özellikle bankacılık, eticaret gibi kredi kartı ve özel bilgilerimizi paylaştığımız web sitelerinde kullanılması çok önemlidir. Https kullanılan web sitelerinde iletişim 2048bit şifreli olarak sağlandığından veri kaybı, değiştirilmesi veya kullanıcı kimliği zafiyeti önlenmiş olacaktır.

Kullanıcıların yapması gereken kredi kartı bilgilerini girecekleri web sitelerinde mutlaka https kullanıldığını kontrol etmeleri gerekmektedir. Ayrıca kullanılan sitenin sahte bir site olmadığını, doğru site olduğunu anlamak için adres satırındaki kilit simgesine tıklandığında web sitesine ait çeşitli bilgiler ekrana gelecektir.

Parola ve E-posta Güvenliği

Kullanıcıların en sık yaptığı hata basit parola belirlemeleri ve aynı e-posta adresini tüm üye oldukları sitelerde kullanmaları. Aynı e-posta adresini kullanmaları oltalama saldırılarına daha fazla maruz kalmalarına neden olacaktır.

Diğer önemli nokta parolanın güvenli olması olacaktır. Genelde kullanıcılar doğum tarihi, telefon numarası gibi hatırlaması kolay numaraları parola olarak tercih etmektedirler. Ancak bunlar kullanıcıyı tanıyan birinin kolay tahmin edilebileceği bilgiler olacaktır. Parolaların sadece kişinin kendisinin bildiği formatta yeterince uzun ve farklı karakterlerden oluşan bir parola olması daha güvenilir olacaktır. Örneğin sadece sayılardan oluşan altı haneli bir parolanın brute force saldırısı ile tespit edilmesi birkaç dakika sürecektir. Bu süre güvenliğimizi sağlayan en önemli unsur olan şifre için çok çok kısa bir süre. Aynı parolanın içerisine büyük-küçük harfler eklersek parolanın tespit edilme süresi birkaç yıla kadar uzayabilir. Daha da güvenli hale getirmek için aynı parola içerisine *#!? gibi özel karakter eklendiğinde tespit süresi yüzyıllara ulaşacaktır.

Web Sitesinin Güvenilirliği

Bir mağazaya girip alışveriş yapmak istediğimizde markanın güvenilirliği, sunduğu hizmetin kalitesi, herhangi bir sorunda irtibat kurabileceğimiz muhatap bulunması gibi kriterler önemlidir. Benzer kriterlerin internette üye olunan veya alış-veriş yapılan web siteleri için de önemli olduğu

unutulmamalıdır. Web sitesinin kaç yıldır faal olduğu, kullanıcı sözleşmesi, https kullanması, iletişim kanallarının bulunması o siteye ne kadar güveneceğimizi belirleyecek en temel unsurlar olacaktır. Tabi ki bazen tüm bunların sağlanması da yeterli olmayabilir, bu durumda o site ile ilgili şikayet olup olmadığı basit bir arama ile tespit edilebilir.

Bazı web siteleri üyelik sözleşmelerine farklı maddeler yerleştirerek kullanıcılardan çeşitli imtiyazlar talep etmektedir. Özellikle kullanıcı verilerinin reklam ve pazarlama amaçlı olarak satılması en çok karşılaşılan durumdur. Mesela bir sosyal medya platformu üye olan kullanıcılarının o platformdaki bilgileri üzerinde sonsuza dek geri alınamaz hak sahibi olacağını sözleşmelerinde belirtmektedir. Dolayısı ile bir siteye üye olurken tüm bunları göz önüne almak güvenlik açısından faydalı olacaktır. Bu konudaki klasikleşmiş ama güncelliğini yitirmeyen en önemli sözü unutmamak önemlidir; "Ürün bedavaysa ürün sizsiniz".

Oltalama ve Sosyal Mühendisliğe Karşı Tedbirler

Birkaç başlık altında bahsettiğimiz oltalama ve sosyal mühendislik güvenlik halkasının en zayıf zincirinin kullanıcı olması nedeni ile tekrar karşımıza çıkmaktadır. Aslında bu tür saldırılardan korunmak tamamen kullanıcının dikkatli olması ile mümkündür. Eposta adreslerine gelen veya internette herkesin karşısına çıkabilecek linklere tıklandığında adres satırındaki bilginin doğruluğu en önemli unsurdur. Bu nedenle bir web sitesine ulaşmaya çalışırken Google'da arama yaparak erişmek yerine adres satırına web sitesinin tam adresini yazarak erişmek güvenliği önemli ölçüde arttıracaktır. Çünkü arama motorları sadece doğru sonuçları gösteren uygulamalar değildir, manipüle edilebilir ve kullanıcıların en çok tıkladıkları sonuçları en başta göstermektedir. Dolayısı ile adres bilgisini kontrol etmeden arama sonuçlarına tıklamak bazen oltanın üzerine atlamak gibi olacaktır.

2FA Doğrulama Önemi

Kullanıcılar birçok yerde telefon, e-posta gibi bilgilerini kolayca verebilirken, kullandıkları e-posta ve sosyal ağlarda bu bilgileri vermekten çekinmektedirler. Kullanıcıların akıllı telefonlarına kurdukları yazılımlar ile zaten bu bilgileri kolayca elde edebilirken, bunları güvenlik amacı ile kullanmak daha faydalı olacaktır. Tüm e-posta hizmeti sağlayıcılarında ve sosyal medya platformlarında İki Aşamalı Doğrulama (2FA) ayarlar bölümünde yer almaktadır. 2FA ile yeni bir cihazdan erişim yapmaya sağlandığında SMS ile doğrulama kodu talep edilmektedir. Tek yapılması gereken cep telefonu numarasının ve kurtarma e-posta adresinin güncel olmasını sağlamaktır. Ayrıca bazı platformlarda hesabınızın çalınma durumuna karşı güvendiğiniz kişilerden oluşan bir liste oluşturarak olumsuz bir durumda bu kişiler üzerinden irtibat kurabilmeniz sağlanmaktadır.

4.7 DİJİTAL OYUNLAR VE TEHDİTLER

4.7.1 Dijital Oyunlar

Oyunlar insanoğlunun varoluşundan itibaren her kültürde kendine yer bulmayı başarmıştır. Çocukların sosyal ilişkilerini ve zihinsel becerilerini geliştiren geleneksel oyunlar (Saklambaç, Körebe, Seksek, İp Atlama, Beş Taş vb.) kültürel miras olarak nesilden nesile aktarılmıştır. Bazı oyunlar ortaya çıktığı ilk günkü değeri koruyarak bugünlere değişmeden gelmeyi başarmışken bazıları ise günün şartlarına göre dönüşerek var olmaya devam etmektedir.

Sonucu düşünülmeden, eğlenmek amacıyla yapılan hareketler olarak tanımlanan oyunlar; kişilerin gelişimine katkı sunan bir faaliyet olarak her dönem değer görmüştür. Oyunlar her yaştan bireyin eğitiminde, etkili olan bir öğrenme aracı olarak da kabul görmektedir. Özellikle çocuklar için ilgi uyandıracak içerikli dersler oluşturmak için sıklıkla kullanılmaktadır. Çocuğun oyunla ilişkisi bir eğlence aracı olmasının yanı sıra oyunun, çocukların oyunlar ile çevrelerini anlamlı hale getirebilme ve bu çevre içinde nasıl yer alacaklarını öğrendiklerine ilişkin tanımlar vardır. Oyun sayesinde çocuğa hiç kimsenin öğretemeyeceği konuların, çocuğun kendi deneyimleriyle öğrenmesinin sağladığı vurgulanmaktadır.

Internet teknolojisinin sunduğu kolaylıklar ve fırsatlar için her geçen gün daha çok dijital dünyanın parçası oluyoruz. Salgın nedeniyle de bireyler iş, eğitim, alışveriş, finans ve eğlence gibi hemen hemen her alanda birçok faaliyeti salgın öncesine göre daha fazla dijital dünyada gerçekleştiriyoruz. Siber güvenlik farkındalığı düşük olan kişiler ise dijital faaliyetlerini gerçekleştirirken siber dünyadaki saldırganlar tarafından kolay ve hızlı kandırılabilmektedir.

90'lı yıllardan sonra farklı türlerde internet teknolojisinin de gelişimi ile farklı türde dijital oyunlar da üretilmeye başlanmıştır. Yaşadığımız dönemde oyuncuların ihtiyaç ve tercihleri doğrultusunda üretilmiş ya da değişime uğramış çok sayıda ve farklı türde dijital oyun bulunmaktadır. Bu oyunları genel olarak taktik, yap boz, macera, aksiyon, spor, rol yapma ve simülasyon olmak üzere sınıflandırabiliriz. Günümüzde taktik oyunları ve aksiyon oyunları yoğun olarak tercih edilen oyun türlerindendir.

Sosyalleşme ve oyun ihtiyaçlarımızı gidermek için sıklıkla kullandığımız dijital oyunlar çeşitli riskleri de beraberinde getirmektedir [15 – 18]. Özellikle çocuk kullanıcılar bu risklerden en fazla etkilenen kitleyi oluşturmaktadır.

4.7.2 Dijital Oyunlardaki Tehditler

Dijital oyunlar kontrollü kullanıldığında çocukların ve gençlerin zihinsel gelişimlerine olumlu katkı yapabilmektedir. Ancak kontrol edilemeyen oyun isteği, hem sosyal, hem psikolojik hem de fiziksel bağımlılıklara neden olabilir. Dijital oyun bağımlılığı; kişiler üzerinde sosyal veya duygusal sorunlara neden olduğu halde, kişileri bilgisayar ya da video oyunlarını aşırı şekilde kullanmayı bırakamayarak, kişilerin aşırı kullanmasını kontrol edememesi olarak tanımlanmaktadır. Kişinin otokontrolünü yitirmesi, oyunun kişiyi etkisi ve kontrolü altına alması olarak da ifade edilebilir. Dijital oyun bağımlılığı kavramı, dijital oyunların kişilerde ortaya çıkardığı olumsuz durumları ifade etmektedir.

Dijital oyunlar kişilerin ruh sağlıklarını da bozarak, kişileri intihara kadar götürebilme gücüne sahiptir. Özellikle Mavi Balina gibi dijital oyunlarda çocuklar gerçek dünya ile dijital dünya arasında sıkışmaktadır. Çocuklar oyundaki senaryoları gerçekleştirmek için gece uyanmakta ve gündelik yaşamları da buna bağlı olarak düzensizleşmektedir. Çocukların korku duygusu ile gerçekte var olmayan içerikli video ve görüntüler izlemeleri sağlanmaktadır. Çocukların kontrol edemediği ve günlerce süren bu süreçte, yanlış değer yargıları uyandırılarak, çocuklarda değersizlik hissi de oluşturulmaktadır.

Oyun senaryoları üzerinden kişisel bilgileri oltalama oluyla alınan kişiler tehdit, şantaj veya siber zorbalık yöntemleri ile tuzağa düşürülerek intihara kadar sürüklenebilmektedir. Yapılan araştırmalarda özellikle şiddet içeren dijital oyunların;

- Olumlu sosyal davranışların azalması,
- Yaşam doyumunun düşmesi,
- Düşmanca duygularda artış görülmesi,
- Şiddete karşı duyarsızlaşmanın başlaması,
- Dikkat sorunlarının ortaya çıkması,
- Depresyon,
- Saldırganlık,

- Anksiyete,
- Şiddet eğilimi
- Yalnızlık

gibi psikososyal problemlere yol açtığı belirlenmiştir.

4.7.3 Dijital Oyunlardaki Tehditlerden Korunma

Çocuklar için büyük bir tehdit olan Mavi Balina ve riskli diğer dijital oyunlardaki tehditlerden korunmak için;

1. Ebeveynlerin çocukların oynadıkları oyunlarlar ile ilgili bilgi sahibi olması ve çocukları dijital oyunlardaki tehditler ile ilgili bilgilendirmesi önemlidir.

2. Ebeveynler çocuklarının girdikleri internet sitelerini takip etmelidir. Etik olmayan davranışları ya da şiddeti özendiren site ve oyunların olumsuz etkisini çocuklarla paylaşmalıdır.

3. Çocukların internete erişiminin ailenin izleyebileceği, kontrol edebileceği ortak alandaki bir dijital ortam üzerinden yapılması sağlanmalıdır.

4. Ebeveynler çocukları ile internet ve dijital dünyadeki tehditler için sık sık bilgi paylaşımı yapmalıdır. Ayrıca; ebeveynler çocukların internet dünyasını keşfinde birlikte olup ve uygun davranışların sergilendiği aktiviteleri çocukları ile birlikte yapmalıdır.

5. Çocukların dijital ortamda geçirdikleri zamanlar ve faaliyetler gözlemlenmelidir.

   Çocukların kullandığı bütün dijital cihazlar için ebeveyn koruma sisteminin açık olduğundan emin olunmalıdır.

6. Bilinçli ve siber güvenlik farkındalığı yüksek ebeveynler internet aracılığıyla yaptıkları aktivitelerin farkında olmalı ve dijital ortamın kullanımı anlamında çocuklarına rol model olmalıdır.

7. Ebeveynler farklı ebeveynlerle konuşarak, bilgi paylaşımı yaparak çocukları için en iyi yöntemi bulmak için bilgi alışverişi yapmalıdır.

8. Ebeveynler internette yayılan yeni akımların içeriği ile ilgili güncel bilgileri takip etmelidir.
9. Ebeveynler çocuklarının davranışlarını yakından gözlemlemelidir. Çocukların ruh halinde değişiklik, iletişimde azalma, çalışma isteksizliği veya notlarındaki düşüş gibi beklenmedik değişimler konusunda her an uyanık ve hazır bulunmalıdır. Değişimler fark edilirse, çocukların internet üzerindeki faaliyetleri yakından izlenmeli ve okul yetkilileriyle, okul rehber öğretmeni ile temasa geçilmelidir. Çocuğun durumu ile ilgili psikoloğa da danışılmalıdır.
10. Çocuğun Mavi Balina oyununu oynadığının fark edilmesi durumunda, hemen tüm dijital ortamlardan internet erişimi kesilmelidir. Polis yetkilileri durumdan haberdar edilerek, alınacak önlemler için yetkililerin tavsiyeleri uygulanmalıdır.

BÖLÜM 5

AĞ GÜVENLİĞİ

Bilgisayar ağları ve internet, siber güvenlik dünyasının önemli bir kısmını oluşturmaktadır. Milyarlarca cihazın (veya nesnenin) çeşitli teknolojiler ile birbirine bağlı olduğu bir ortam siber saldırganlar için de cazip bir ortamdır. Çoğu saldırgan hedeflerini İnternet aracılığıyla bulmakta, zararlı yazılımlar bilgisayar ağları aracılığıyla yayılmakta ve yine internet ve bilgisayar ağları sosyal mühendisliğin de ilgi alanı olmuştur. Bu bölümde, bilgisayar ağlarının çalışma şeklini belirleyen protokoller ve bilgisayar ağları siber güvenlik açısından ele alınacaktır.

Protokoller temel amaç itibariyle, iletişimin doğru bir şekilde çalışmasını sağlayan kurallar olsa da çeşitli zafiyetler barındırmaktadır. Bu protokolleri analiz tehdit aktörleri, zafiyetleri kullanarak zararlı yazılımlar ya da saldırılar yapabilmektedir. Bu nedenle siber güvenlik uzmanının da protokollerin çalışma prensiplerini iyi analiz edebilmesi ve protokollerdeki zayıflıkları bilip, saldırı (veya tehdit) öncesinde güvenlik adımlarını atması gerekmektedir.

5.1 TCP/IP PROTOKOLLERİNDEKİ ZAYIFLIKLAR

Kitabın önceki bölümlerinde ele alındığı gibi, TCP/IP protokol kümesi birçok protokolden oluşmaktadır. Bunların en yaygınları TCP ve IP olduklarından, protokol kümesine ismini vermiştir. IP (özellikle sürüm 4), temel amacı itibariyle verinin taşınması olduğundan, güvenlik özelliklerini içinde barındırmaz. IP'nin güvenilirliği (reliabilitiy) ve güvenliği (security) ek protokollere ve mimarilere (IPSec gibi) dayanır. Siber güvenlik uzmanının bu alanlara en az tehdit aktörleri kadar hâkim olması gerekmektedir. Örneğin, IP başlık yapısını ve fragmantasyon işlemini doğru analiz eden saldırganlar, eski sistemlerde DoS saldırısına neden olan Ping of Death atağını geliştirmişlerdir. Aşağıda **Ping of Death** saldırının arkasındaki mantık anlatılmaktadır.

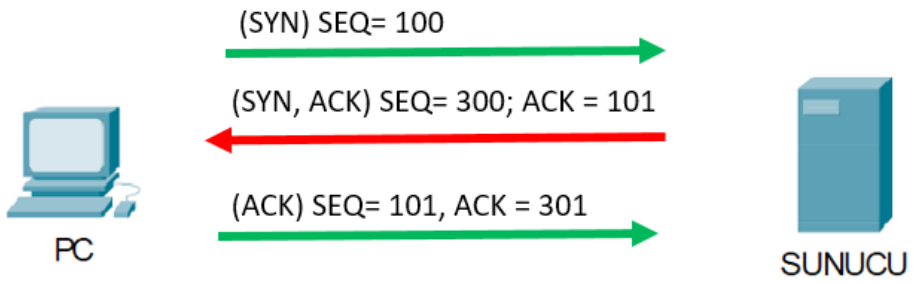
IP paketi verinin doğru adrese gitmesi için, taşınan verinin yanında başlık bilgisini de içerir (OSI modeli ve kapsülleme konusuna bakınız). Bir IP paketinin boyutu, başlık bilgisindeki (header) alana göre (Toplam Uzunluk alanı 16 bittir) en fazla 65.535 değerini alabilir. Ancak iletişim esnasında bu paketler kullanılan teknolojiye göre parçalanıp gönderilmektedir (fragmantasyon). Örneğin Ethernet teknolojisinde 1500 Byte 'lar şeklinde paketlere bölünür. Parçalanan paketlerin alıcı tarafta tekrar birleştirilmesi gerektiğinden, paketlerde hangi parça olduğu paket başlığındaki 13-bitlik parça ofseti (fragment offset) alanında belirtilir. Bu alanın, toplam paket uzunluğu alanından 3-bit eksik olması nedeniyle, parça ofseti alanında bu kısım 8'in katları şeklinde ifade edilir (2^3=8). Bu nedenle ofset alanındaki en büyük değer, 65528 değerine işaret edebilir (2^13-1)*8. 20 baytlık paket başlık bilgisi eklendiğinde, toplam 65548 bayt olacaktır. Alıcı cihazda paketlerin birleştirilmesi esnasında IP paketi için belirlenen (ve gerçekten de olması

gereken) 65535 bayttan daha fazla bir alanı işgal edecektir. Bu beklenmedik boyut, alıcı cihaz için bellek taşmasına (buffer overflow) neden olmaktadır. Eski sistemlerde bu saldırı birçok cihazın devre dışı kalmasına neden olduğu için bir DoS saldırısı olarak kullanılmaktaydı.

Ping of Death örneğinde görüldüğü gibi, tehdit aktörleri analiz yapmakta ve her fırsatı değerlendirmektedir. Bu nedenle siber güvenlik uzmandan da aynı yeteneğe sahip olması beklenmektedir.

5.1.1 TCP Zayıflıkları

OSI modelinin 4.katmanında çalışan TCP protokolünün amacı, veriyi uygulamalar arasında taşımaktır. Yani uygulamaların haberleşmesini sağlamaktır. TCP yapısı ve çalışma prensibi gereği güvenilir bir protokoldür. TCP'nin güvenilir olması, gönderilen verinin karşı uygulamaya gidip gitmediğinin bilinmesinden ve olası paket kayıpları durumunda tekrar gönderiminden kaynaklanır. TCP iletişiminde veri gönderiminden önce, 3-yollu el sıkışma (3-way handshake) olarak adlandırılan bir ön anlaşma işlemi gerçekleşir. Bu işlemin ardından oturum kurulur (establish) ve ardından veri iletişimi başlar.



Şekil 5.1. TCP üç yollu el sıkışması

Şekil 5.1'de gösterildiği gibi, trafiği baslatan taraf olarak PC, TCP başlık bilgisinde yer alan SYN isimli bayrağı işaretler (SYN=1) ve rastgele bir değer içeren sıra numarasını (sequence number) gönderir. Şekilde bu değer 100 olarak belirtilmiştir. Senkronize olma talebini (SYN) alan sunucu, senkronizasyonu onaylamak için ACK bayrağını işaretler ve kendisinin de senkronize olma talebini iletir. Böylece, hem SYN hem de ACK bayrakları işaretlenir. PC'nin gönderdiği sıra numarasını aldığını belirtmek üzere, 100 sıra nolu TCP segmentini aldığını ve bir sonraki sıra numaralı segmenti talep ettiğini belirtmek üzere ACK numarasını 101 yapar. Aynı şekilde sunucu rastgele bir değer belirleyip (örnekte 300) kendi sıra numarası olarak gönderir. PC, sunucudan

gelen SYN mesajını kabul eder (ACK=1) ve paketi aldığını belirtmek üzere ACK numarasını 301 olarak belirler. Ayrıca sunucunun beklediği değeri olan 101'i de sıra numarası olarak gönderir. Bu işlemin başarılı bir şekilde gerçekleşmesinin ardından TCP oturumu kurulur. Ancak bu yapı ve çalışma prensibi güvenlik yönünden bazı zayıflıklar içermektedir.

Kötü amaçlı tehdit aktörü, sunucuya **SYN** bayrağı işaretlenmiş bir istek gönderir. Bu iletiyi alan sunucu, olması gerektiği gibi SYN ve **ACK** bayraklarını işaretleyerek mesaja cevap verir. Beklenen şey, PC'nin ACK bayrağı işaretlenmiş 3.adımı gerçekleştirmesidir. Ancak saldırgan bu 3. Mesajı göndermez. Böylece sunucu 3.mesajı beklemeye başlar. Saldırgan sahte IP adresleri ile bu işlemi tekrar eder. Böylece sunucuda birden çok tamamlanmamış oturum oluşur. Bu yarım açık kalan oturumlar nedeniyle sunucu yeni oturum alamayacaktır. Bu saldırı, TCP "Syn Flood Attack" olarak adlandırılan bir DoS saldırısıdır.

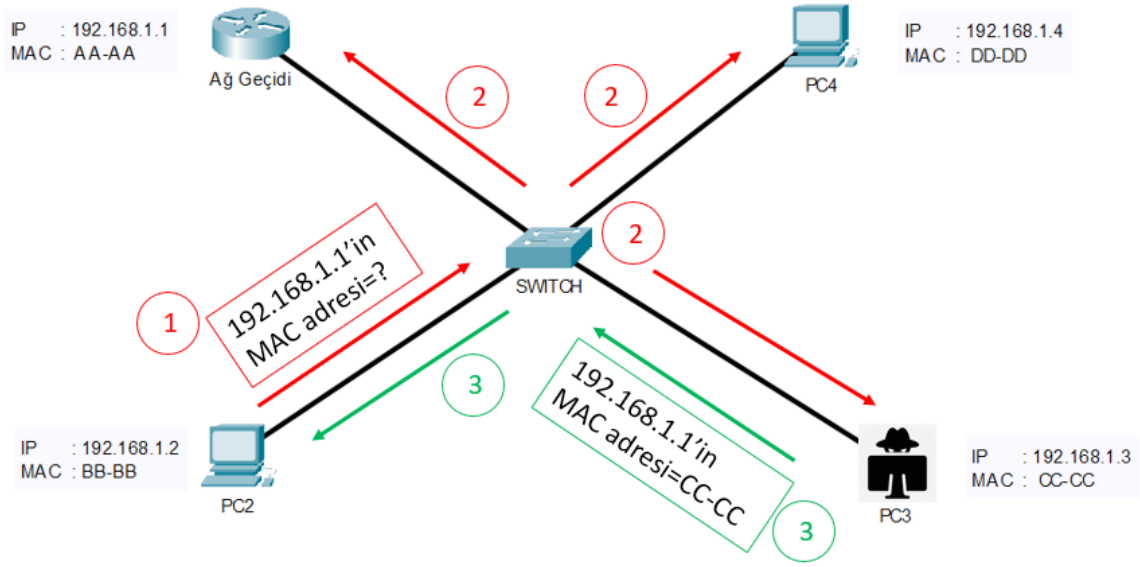
TCP'ye yönelik yapılan saldırılardan biri de, sıra numarasının (Sequence number) tahmin edilmesine yönelik yapılan saldırılardır. Doğru bir algoritma kullanarak TCP'nin bir veri paketi akışına atadığı sıra numarası tahmin edilebilir. Bir sonraki sayıyı bilen bir saldırgan, potansiyel olarak devam eden bir iletişime dâhil olabilir ve mesajı gönderen kaynak cihaz olarak görünebilir. TCP sıra numaraları genellikle her saniye sabit bir değerde artar. İlk sıra numarası için rastgele bir artış oluşturmakla başlayan saldırgan, bu değeri yakalayabilir. Bu durum yine TCP'nin zayıflıklarından biridir.

Diğer bir TCP saldırısı da, *"TCP reset attack"* olarak adlandırılan saldırıdır. TCP başlık bilgisinde, SYN ve ACK gibi toplamda 6 adet bayrak bulunmaktadır. Bunlardan biri de **RST** bayrağıdır. Normal TCP veri akışında bu bayrağın değeri sıfırdır. TCP bağlantısının acil olarak durdurulması gerektiği durumlarda kullanılır. Tasarımı itibariyle faydalı olan bu özellik, saldırgan tarafından legal olan iletişimi sonlandırmak için kullanılabilir. İki cihaz arasındaki trafiği dinleyen bir saldırgan, port numaralarını yakalayarak trafiği sonlandırmak üzere uç noktalardan birine bu sahte TCP paketini gönderir.

5.1.2 ARP Zayıflıkları

Daha önceki bölümlerde değinildiği gibi, Ethernet iletişiminde fiziksel adres olarak MAC adresler kullanılmaktadır. Aynı ağda yer alan iletişimde, kaynak cihaz iletişim kuracağı cihazın IP adresinin yanı sıra, MAC adresini de bilmesi gerekir. Farklı ağ ile yapılan iletişimde ise Ağ Geçidi cihazın MAC adresi bilinmelidir. ARP protokolü, IP adresi bilinen bir cihazın MAC adresini bulmayı sağlayan bir protokoldür.

Protokolde, yayın olarak yapılan MAC adresi öğrenme isteğine (ARP isteği) verilen cevabın (ARP cevabı), doğru IP tarafından yanıtlandığı protokolde kontrol edilmez. Bu nedenle potansiyel olarak herhangi bir IP (dolayısıyla saldırgan) ARP isteğine cevap verebilir. Bu durum, Şekil 5.2'de gösterilmiştir. Şekilde MAC adresler anlaşılabilirliği sağlamak amacıyla AA-AA, BB-BB gibi kısaltılarak gösterilmiştir, gerçek MAC adreslerin gösterimi dikkate alınmamıştır. MAC adresin gerçek gösterimi için kitabın birinci bölümüne bakınız.



Şekil 5.2. ARP saldırısı

Şekil 5.2'de, ARP zehirlenmesi olarak adlandırılan saldırı şöyle gerçekleşmektedir.

1. PC2, kendi ağının dışındaki bir IP ile (örneğin internetteki herhangi bir yer) iletişime geçecektir. Bu nedenle kendi ağ geçidi adresinin (192.168.1.1) MAC adresini öğrenmesi gerekir. Bu amaçla yayın olarak **ARP isteği** yapar.
2. Anahtar yayın olarak gelen bu iletiyi ağdaki herkese gönderecektir.
3. Saldırgan (PC3), bu isteğe **ARP cevabı** ile yanıt verir. Ancak verdiği cevapta ağ geçidinin değil, kendi MAC adresini (CC-CC) gönderecektir.

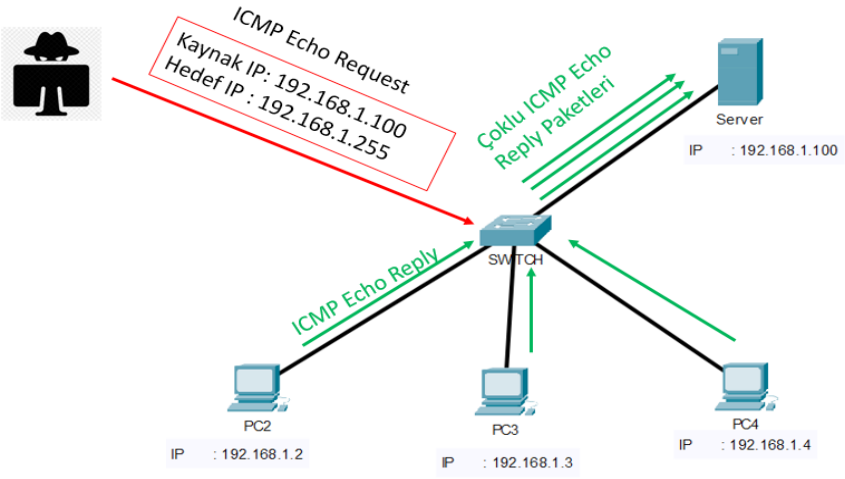
Bu durumda PC2, ağ geçidine göndereceği paketleri MAC adresi CC-CC olan cihaza (saldırgana) gönderecektir. Veri paketleri saldırgan tarafından okunup doğru hedefe gönderilebilir, değiştirilip gönderilebilir ya da iletişimin tümden kesilmesi sağlanabilir.

ARP kullanılarak yapılan diğer bir saldırı da, yine sahte ARP cevabına dayanır. Buna göre saldırgan, ağda yapılan tüm ARP isteklerine kendi MAC adresi yerine ağdaki işlevselliği yüksek bir cihazın (örneğin bir sunucunun) MAC adresini cevap olarak gönderir. Bu durumda, ağdaki tüm iletişimleri sunucuya gidecek ve sunucunun ağ performansı düşürülerek DoS saldırısı gerçekleştirilmiş olur.

Görüldüğü üzere ARP yapısındaki zayıflıklar, saldırganlar tarafından DoS (hizmet reddi), MITM (ortadaki adam) gibi ataklar için kullanılabilmektedir.

5.1.3 ICMP Zayıflıkları

ICMP, ağda erişilebilirlik sorunlarının teşhisi için sorun giderme sürecinde en yaygın kullanılan protokollerden biridir. Windows güvenliği kısmında anlatıldığı gibi, **tracert ve ping** komutları ICMP protokolünü kullanır. 3.katman düzeyinde ağdaki cihazların erişilebilir olup olmadıklarını, erişilemez olması durumunda bunun olası nedenlerini (zaman aşımı, hedef ağ bilinmiyor gibi) sunan oldukça yararlı bir protokoldür. Ancak yine bu protokol de çeşitli saldırılarda ya da ağdan gizli bilgi göndermede kullanılabilir. Örneğin, **smurf attack** olarak adlandırılan bir saldırıda, saldırgan ICMP paketinin kaynak adresini taklit eder ve o ağdaki tüm bilgisayarlara bir yayın gönderecektir.



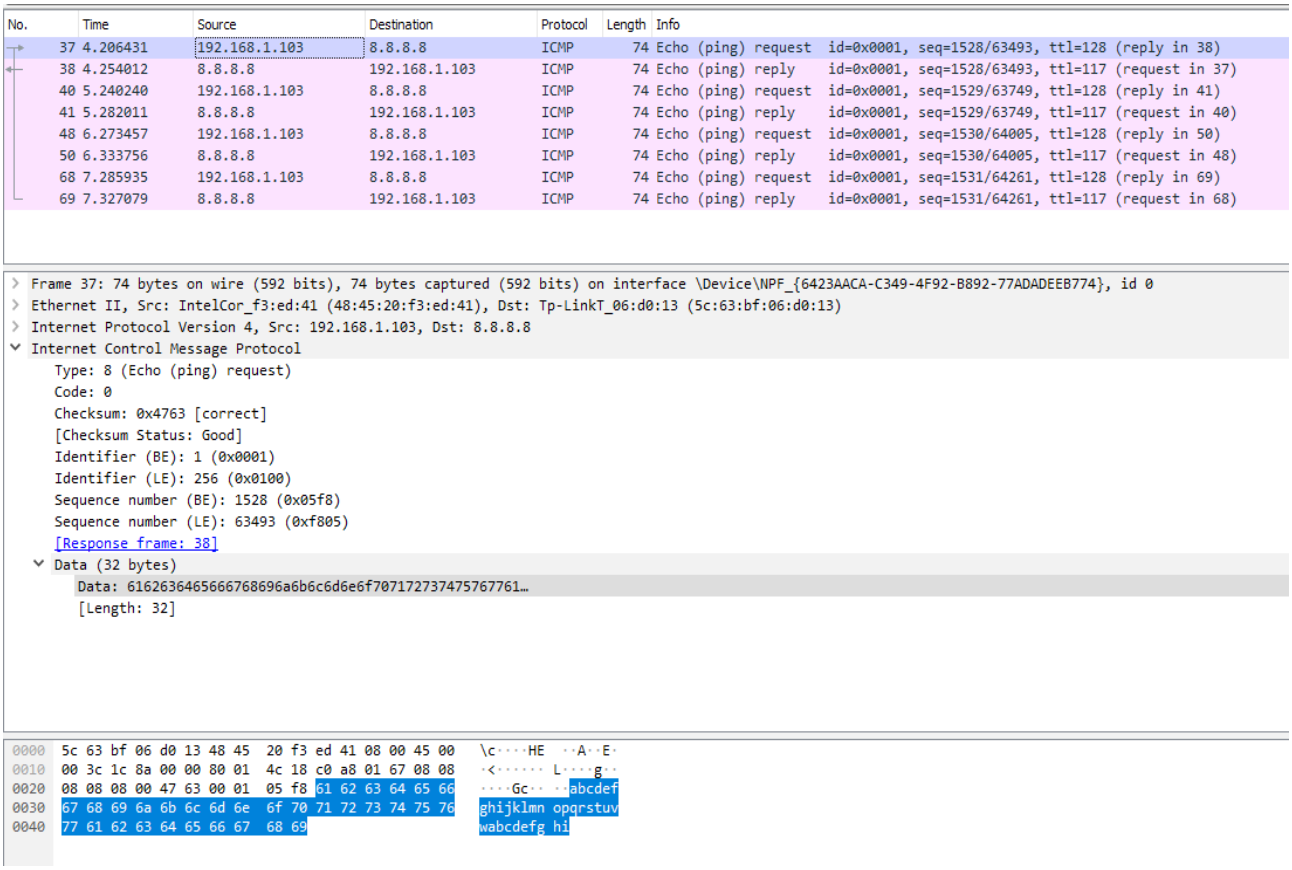
Şekil 5.3. ICMP temelli bir saldırı

Ağ cihazları bu trafiği filtrelemezse, ağdaki tüm bilgisayarlara yayınlanır. Hedef ağ trafiğinde tıkanıklıklar yaşanır ve ağın verimliliği düşer.

ICMP protokolü sağladığı bilgiler faydalı olsa da, yanlış ellerde bu bilgiler keşif ataklarında **(reconnaissance attack)** veri toplama için de kullanılabilir. Örneğin, gönderilen ICMP echo isteklerine verilen cevaptan hedef cihazın işletim sisteminin tespit edilmesi mümkündür. TTL

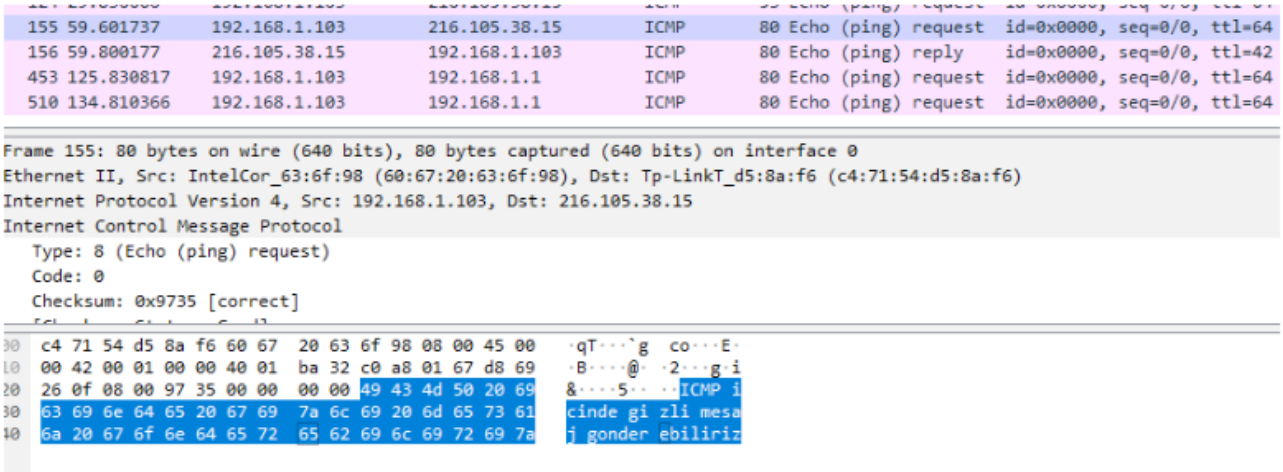
alanındaki başlangıç değer 128 ise Windows işletim sistemi, 64 ise Linux işletim sistemi olduğu söylenebilir. Aynı şekilde, tracert ile paketlerin geçtiği yoldaki cihazların IP adresleri öğrenilerek ağ haritası hakkında da bilgi toplamak mümkündür.

ICMP protokolü ile uygulanabilecek diğer bir güvenlik zaafiyeti de, ağda meşru bir trafik gibi görünen ICMP protokolü aracılığıyla gizli bilgi göndermektir. Bu sayede ağ güvenlik cihazları atlatılarak veri hırsızlığı yapılabilir. Aşağıdaki örnekte, 8.8.8.8 IP adresine ping atılarak ICMP yankı isteği gönderilmiştir. Windows işletim sistemlerinde gönderilen ICMP paketlerinde varsayılan olarak **"abcd...."** şeklinde sabit 32 baytlık bir veri gönderildiği WireShark ekran görüntüsünden görüntülenmektedir.



Şekil 5.4. ICMP'nin Wireshark ekran görüntüsü

Ancak çeşitli araçlar kullanılarak bu 32 baytlık kısım değiştirilebilir. Gizli bilginin gönderilme işleminin WireShark ekran görüntüsü aşağıda verilmiştir.



Şekil 5.5. ICMP içinde küçük mesaj gönderme

5.1.4 DHCP Zayıflıkları

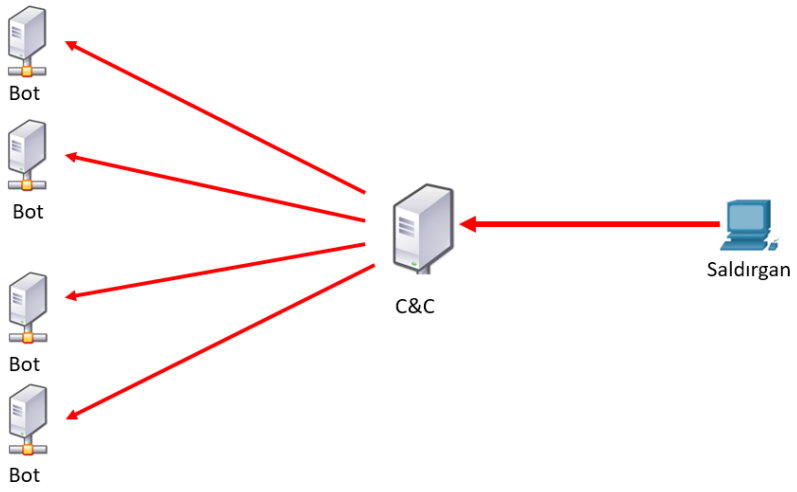
DHCP, konak cihazlara IP adresleme bilgilerini sağlayan UDP tabanlı bir uygulama protokolüdür. Konak cihazın ihtiyaç duyduğu bilgiler, DHCP sunucusu tarafından istemci cihaza kiralanır. Ancak bu protokol, çeşitli yönlerden güvenlik zafiyetleri barındırmaktadır. DHCP açlık saldırısı **(DHCP starvation)** olarak bilinen saldırıda, DHCP sunucusunun mevcut IP adresleri tükeninceye kadar saldırgan tarafından IP talep edilir. Sunucuda IP adresi tükendiğinde, ağdaki meşru kullanıcılar IP talep ettiklerinde DHCP sunucusu tarafından IP verilemez ve ağda işlem yapmaları engellenir.

Diğer bir DHCP saldırısında ise, saldırgan cihazların ihtiyaç duydukları IP, DNS, Ağ Geçidi gibi bilgileri dağıtır. Ancak bu bilgiler hatalıdır. Örneğin ağ geçidi yerine saldırgan kendi IP adresini, ya da DNS sunucu adresi yerine yine zararlı bir adrese yönlendirme yapabilir.

5.1.5 DNS Zayıflıkları

DNS protokolü, www.meb.gov.tr gibi alan adlarını IPv4 veya IPv6 adresi gibi gerekli sayısal ağ adresiyle eşleştiren otomatik bir hizmeti tanımlar. Açık DNS sunucular (örneğin 8.8.8.8 Google DNS) yaygın olarak kurumsal ya da bireysel olarak kullanılır. DNS bir ağın çalışması için çok

önemlidir ve güvenliğinin sağlanması gerekir. Özellikle herkese açık DNS'lere yönelik yapılan birçok saldırı vardır. **DNS Yükseltme ve Yansıtma saldırılarında,** tehdit aktörleri, saldırıların miktarını artırmak ve bir saldırının gerçek kaynağını gizlemek için DNS açık çözümleyicilerine yönelik DoS veya DDoS saldırılarını kullanır. Tehdit aktörleri, bir hedef bilgisayarın IP adresini kullanarak açık çözümleyicilere DNS mesajları gönderir. Açık çözümleyici, sorguyu yapan herkesin sorgularını yanıtlayacağından, hedef sisteme çoklu paketlerin ulaştığı saldırının gerçekleşmesi mümkündür.



Şekil 5.6. DNS tabanlı bir saldırı

DNS Tünelleme saldırısında, botnetler yaygın olarak kullanılır. Bu saldırıda, DNS tünellemesini kullanan tehdit aktörleri, DNS olmayan trafiği DNS trafiğine yerleştirir. Bu yöntem genellikle güvenlik çözümlerini atlatır.

- Bu saldırıda, veriler, birden çok kodlanmış parçaya bölünür.
- Her parça, DNS sorgusunun daha düşük düzey bir etki alanı adı etiketine yerleştirilir.
- Sorgu için yerel veya ağa bağlı DNS'den yanıt olmadığından, istek ISS'nin özyinelemeli DNS sunucularına gönderilir.
- Özyinelemeli DNS hizmeti, sorguyu saldırganın yetkili ad sunucusuna iletir.
- İşlem, parçaları içeren tüm sorgular gönderilinceye kadar tekrarlanır.
- Saldırganın yetkili ad sunucusu, virüslü cihazlardan DNS sorgularını aldığında, kapsüllenmiş, kodlanmış komutları içeren her DNS sorgusu için yanıtlar gönderir.
- Güvenliği ihlal edilen bilgisayardaki zararlı yazılım, parçaları yeniden birleştirir ve içinde gizli olan komutları çalıştırır.

5.1.6 Diğer Protokollerdeki Zayıflıklar

Bu bölüm altında TCP/IP takımında yer alan diğer protokollerin zayıflıklar özetle ele alınmıştır. Örneğin ağdaki bir cihazın uzaktan yönetilmesini sağlayan **Telnet** protokolünde, veriler şifrelenmeden gönderildiği için güvensiz bir protokoldür. Bu nedenle, güvenliği şüpheli ağlarda (ya da genele açık ağlarda) kullanılmamalıdır. Aynı şekilde http protokolü ile transfer edilen verilerin şifrelenmediği unutulmamalıdır. Bilgisayar ağlarında güvenlik açısından dikkate alınması gereken diğer protokol de SNMP protokolüdür. Özellikle anahtar ve yönlendirici gibi aracı cihazların uzaktan yönetilmesinde, izlenmesinde yararlı olan bu protokolün 3.sürümü öncesindeki tüm sürümlerde güvenlik sadece "community string" olarak ifade edilen ve varsayılan olarak birçok cihazda "public" ve "private" olan kelimeler kullanılmaktadır. Bu nedenle eski sürüm SNMP kullanan cihazların güvenliği kolaylıkla ihlal edilebilir.

5.2 KABLOSUZ AĞLARDA GÜVENLİK

5.2.1 Kablosuz Ağlar

Kablosuz ağlar, kablolu ağlara alternatif olarak oluşturulmuş temelde RF(Radyo Frekans) teknolojisini kullanan verileri kablo üzerinden değil de radyo sinyalleri ile gönderilmesini sağlayan iletişim protokolüdür. Günümüzde maliyetler, kullanım kolaylığı ve özellikle mobil cihazların kablolu bağlantıyı desteklememesi nedeni ile tercih edilmektedir.

1997 yılında WLAN standartlarını IEEE geliştirilmesinden sonra günümüze kadar IEEE 802.11 başlığı altında geliştirilmeye devam etmektedir. Bu başlık altında 802.11a, 802.11b, 802.11g, 802.11n ve daha yeni geliştirilen 802.11ac ile 802.11ax kablosuz ağ standartları geliştirilmiştir.

Kablosuz erişim cihazınızın (kablosuz modem veya access point) hangi standartta çalıştığını bilmek yaşanabilecek tehditler konusunda bilgi sahibi olunmasını sağlayacaktır. Örneğin 802.11a, 802.11b, 802.11g ve 802.11n standartlarından birini kullanan kablosuz erişim cihazı hem hız, hem verimlilik hem de güvenlik açısından sorun yaşanmasına neden olabilir. Eğer birkaç yıl önce alınan kablosuz erişim cihazı varsa muhtemelen yeni standartlar olan 802.11ac ve 802.11ax protokollerini desteklemektedir.

802.11ac (WiFi 5) standardının en önemli özelliklerinden biri Dual-Band teknolojisi ile önceki standartlardan farklı olarak hem 2.4GHz hem de 5GHz eş zamanlı bağlantı desteğini sağlamaktadır. Dual-Band desteği ile frekans yoğunluğuna göre farklı band aralığı seçilerek iletişim verimliliği arttırılabilmektedir. Ayrıca 2.4GHZ bandında 450Mbps hızına erişirken, 5GHZ

bandında 1300Mbps gibi yüksek hızlara erişebilmektedir. Aynı zamanda 802.11 b/g/n destekli cihazların erişimine imkan vermektedir.

802.11ac ile Beamforming ve MU-MIMO (Multi User Multiple Input Multiple Output) teknolojileri hayatımıza girmiştir. Beamforming ile WiFi sinyali dağıtılmadan cihazların konumu tespit edilip sinyalin odaklanmasıyla iletişim sağlamaktadır. Bu sadece sinyal kirliliği önlenerek, maksimum hız ve kararlılık korunmaya çalışılmaktadır. MU-MIMO teknolojisi ile birden fazla sayıda cihaz eş zamanlı olarak ağa bağlandığında hizmetlerde kayıp olmadan iletişimin devam etmesini sağlamaktadır.

802.11ax (WiFi 6) en yeni kablosuz iletişim teknolojisidir. 802.11ac standardına göre %37 daha hızlı veri transferini mümkün kılmaktadır. Aynı zamanda güç verimliliği ile cihazların batarya sürelerini arttırmaktadır. Diğer standartlardan farklı olarak aynı anda 8 cihazın iletişimine imkân sağlamaktadır. Özellikle AVM, havaalanı, oteller, kampüsler gibi çok kullanıcı olan alanlarda performans kaybı yaşamaksızın erişim sağlanabilmektedir.

Kablosuz ağlar için önemli olan diğer bir terim SSID (Service Set Identifer) ifadesidir. Kısaca kablosuz ağın ismine SSID denmektedir. İsimsiz bir kablosuz ağ tanımlanamamaktadır, bu nedenle her kablosuz ağın bir SSID ismi bulunması gerekmektedir.

5.2.2 Kablosuz Ağ Şifreleme Modelleri

Kablosuz ağların güvenliğini sağlamak her yöne ve en az 100 metre gibi bir mesafeye yayın yapan iletişim sistemleri için önem arz etmektedir. Kablosuz ağ şifreleme modelleri, kablosuz ağ cihazı (modem, access point) ile kullanıcının cihazı (dizüstü bilgisayar, akıllı cep telefonu, tablet vb) arasındaki iletişimin güvenliğini sağlayan en önemli araçtır. Zamanla bazı modellerin güvenliğinin aşılabilir olduğu tespit edilmiş bu nedenle yeni modeller ortaya çıkmıştır. Dolayısı ile kullanılacak şifreleme modelinin en günceli olduğundan emin olunması gerekmektedir. Kablosuz ağ şifreleme modelleri şunlardır;

a-WEP: Kablosuz ağ standartları geliştirilmeye başladığında 1999 ilk ortaya çıkan şifreleme modelidir. WEP şifreleme modelinde kimlik doğrulaması yoktur bu nedenle kullanımı risklidir. Bruteforce saldırıları ile kolayca WEP şifresini kırmak mümkündür. Günümüzde kullanılan modemlerin çoğunda WEP şifreleme modelinin kullanımına izin verilmemektedir.

b-WPA: WEP modelinin güvensizliği tespit edildikten sonra 2003 yılında WPA modeli geliştirildi. Aslında temelde WEP şifreleme modeli tabanlı olup WEP şifreleme modelinde yer alan

açıkların giderilmiştir halidir. Geçici anahtar bütünlüğü protokolü (TKIP) WEP modelindeki sorunun giderilmesi için geçici bir çözüm olarak tasarlanmıştır.

c-WPA2: Günümüzde en çok kullanılan şifreleme standardıdır. 2004 yılında duyurulmuş ve 2006 yılında tüm modemlerde standart hale getirilmiştir. Fakat yapılan güvenlik çalışmalarında WPA2 modelinin de çeşitli yazılımlar ile kırılabilir olduğunu ortaya koymuştur. Şuan en az güvenlik zafiyetine sahip olan olan WPA2 yavaş yavaş yerini WPA3 standardına bırakacaktır. WPA2 ile AES şifreleme standardı dâhil edilmiş ve TKIP standardından daha güvenilirdir. AES şifreleme ve şifre çözmede kullanılan simetrik anahtarlamalı bir algoritmadır.

d-WPA3: WPA2 şifreleme modelinin kırılabilir olduğu ortaya çıktıktan sonra WPA3 modeli 2018 yılında duyurulmuş ve yeni cihazlarda WPA2 modelinin yerini almaya başlamıştır. Cihaz üreticileri yayınladıkları güncellemeler ile WPA3 desteği kullanılmaya başlanmaktadır. WPA3 modeli daha güçlü şifreleme sağlarken bruteforce (kaba kuvvet) saldırılarına karşı daha fazla koruma sağlamaktadır. Bazı kaynaklarda WPA3'ün kırılabilir olduğu açıklansa da hâlihazırda en güvenilir şifreleme modelidir.

WPS : Kablosuz ağların güvenliği şifre ile sağlanır ve ağa dahil olmak isteyen kullanıcı normal süreçte bu şifre ile kayıt olmalıdır. Ancak özellikle ev kullanıcıları için bu süreci hızlandırmak adına farklı yöntemler geliştirilmektedir. Birçok modemde standart haline gelen WPS özelliği kullanıcıların bir tuş ile şifre girmeden kablosuz ağa dâhil olmasını sağlamaktadır. Kullanıcı modem üzerindeki WPS tuşuna bastığında birkaç dakikalığına erişime açık hale gelecek ve kablosuz cihazları ağa dâhil olma talebi iletildiğinde gerekli güvenlik adımları tamamlanmış olacaktır. Bu özelliği kullanabilmek için modeme fiziksel erişim olması gerekmektedir ancak çeşitli şekillerde uzaktan WPS özelliği aktif hale getirilerek izinsiz kullanıcılar da ağa dâhil olabilmektedir. Dolayısı ile kullanım kolaylığı sağlayan bu özellik aynı zamanda ciddi bir risk oluşturmaktadır.

5.2.3 Kablosuz Ağlara Yönelik Yapılan Saldırılar

Kaba Kuvvet (Brute-Force) Saldırısı : Modem ile bağlantı sağlarken kablosuz ağlardan ilgili ağı seçildikten sonra ağ şifresinin girilmesi gerekmektedir. Bu kimlik doğrulama protokolüne tokalaşma (handshake) denmektedir. Tokalaşma işlemi başladığında bu süreci sağlayacak iletişim paketleri ağa katılmak isteyen cihaza ulaştığında ağ parolası beklenmekte ve parola doğru ise bağlantı sağlanmaktadır. Eğer kullanıcı hatalı giriş yapar ve bunu tekrarlar ise tokalaşma işlemi gerçekleşmediği gibi modem cihazı bir süreliğine engellemektedir. Dolayısı ile kaba kuvvet saldırı yöntemi bu aşamada modeme sürekli farklı parolalar ile giriş yapmayı deneyerek yetkisiz bir kablosuz ağa bağlanmak mümkün olmayacaktır.

Bu aşamada yapılan asıl işlem tokalaşma paketlerini yakalamak ve kaba kuvvet işlemini bu paketler üzerinde gerçekleştirmektir. Kablosuz ağ mimarisi gereği bunu engellemek mümkün değildir. Dolayısı ile güvenli parolalar kablosuz ağa yetkisiz erişimi, birkaç dakikadan yıllar sürecek bir süreye çıkartabilir.

WPS Saldırısı : WPS kullanıcılar açısından kullanım kolaylığı sağlamakta ancak eski ve güncellenmemiş modemlerde aynı zamanda bir risk yaratmaktadır. Bu açığın bulunduğu modemlere çeşitli yazılımlar ile saldırı gerçekleştirildiğinde kablosuz ağ parolasına gerek olmadan yetkisiz olarak ağa dahil olmak mümkündür.

Şeytani İkiz Saldırısı: Bu saldırı türü aslında oltalama saldırısı olarak da kabul edilebilir. Ağ şifresini ele geçirmeye çalışan veya ağ trafiğini kontrol etmek isteyen biri kablosuz ağ ismi aynı olan sahte bir ağ hazırlayarak kullanıcıların bağlanmasını beklemektedir. Ağa katılmak isteyen kullanıcının internet bağlantısı kesilmekte sonrasında oluşturulan sahte ağa bağlanmaktadır. Sahte ağ üzerinden WiFi bilgileri ele geçirildikten sonra sahte ağ kaybolup kullanıcının gerçek ağa bağlanması sağlanmaktadır. Bu tarz bir saldırıda, saldırgan ile kurbanın fiziken yakın olması gerekmektedir. Uzaktan gerçekleştirmesi çok kolay olmayan bir saldırı türüdür.

Diğer Saldırılar: Kablosuz ağlar, kablolu ağlara göre saldırıya daha açık ağlardır. Fiziksel erişime gerek olmadığından saldırı yapmak isteyenlerin veya bedava internet erişimi isteyenlerin iştahını kabartmaktadır. Bahsettiğimiz erişime izin veren yöntemler gibi mevcut kablosuz bağlantıyı kullanılmaz hale getirebilecek saldırı yöntemleri mevcuttur. Temelde diğer saldırı yöntemleri ile benzerlik göstersede SSID verisi ile oluşturulacak kablosuz ağ ile mevcut bağlantı sinyalini karıştırarak, ağ ve internet erişim cihazı açık olduğu sürece yavaşlatmak veya kullanılmaz hale getirmek mümkündür. Veri hırsızlığı veya yetkisiz erişim içermese de sinir bozucu olacağı kesindir.

5.2.4 Kablosuz Ağlarda Güvenlik Uygulamaları

Kablosuz ağlarda güvenliği sağlamak için yapılması gereken tedbirlerin bazılarını birkaç madde olarak sıralamak, alınabilecek tedbirleri hatırlatması açısından faydalı olacaktır.

Cihaz Yönetim Parolasını Değiştirmek: Modemler veta kablosuz erişim noktaları marka, model veya servis sağlayıcıya bağlı olarak erişim ve yapılandırma için belirli parolaları kullanmaktadır. Genellikle bu parola kısa bir internet araması veya modemin altındaki etiketten tespit edilebilir. Dolayısı ile yeni bir modem veya erişim noktası alındığında yapılması gereken ilk iş modem parolasını değiştirmek olmalıdır.

SSID Değiştirmek: Yeni alınan kablosuz cihazın parolası gibi SSID adı da varsayılan bir

değerde olabilir. Bu isim modemin marka modeli veya servis sağlayıcısı ile ilgili bilgi içereceğinden parolasının tahmin edilmesini de kolaylaştıracaktır. Cihazın marka ve modeline göre arayüzünden birkaç adımda ilgili değişikliği yapılabilmektedir.

WiFi Parolasını Değiştirmek: Diğer iki maddede olduğu gibi çoğu modemde kablosuz ağ parolası hazır olarak gelmektedir. Bu parola standart olmayabilir ancak çoğunlukla cihazın altındaki bilgi etiketinde yer alır. Dolayısı ile cihaza fiziksel erişimi olan birinin parolayı öğrenmesi çok kolay olacaktır. İlk yapılması gereken işlemlerden biri de kablosuz ağ parolasının değiştirilmesi olmalıdır. Seçilecek parolanın güvenilir olması önemli diğer bir noktadır. Doğum günü veya telefon numarası gibi kolay tahmin edilebilir parolalar yerine, güvenli ve tahmin edilmesi zor parolalar belirlenmesi çok önemlidir. Özellikle büyük/küçük harf, sayı ve özel karakterleri bir arada içermesi parola güvenliğini arttıran en önemli ayrıntılardandır.

- WPS Seçeneğini Kapatmak: WPS atak işlemi ile modeme yetkisiz erişim sağlanabileceği önceki bölümlerde açıklanmıştı. Dolayısı ile yeni veya güncel bir modem olsa bile WPS risk teşkil eden bir özelliktir. Modemi kurup WPS ile kullanılacak tüm cihazlar tanımlandıktan sonra bu özelliği kapatmak faydalı olacaktır.

- MAC Filtreleme: Bilindiği gibi her cihazın her bir bağlantı noktasının MAC adresi bulunmaktadır. Cihazın kablosuz bağlantı adaptörünün MAC adresi modeme kayıt edildiğinde ve MAC filtreleme aktif hale getirildiğinde sadece kayıtlı olan cihazlar bağlantı sağlayabileceklerdir. Bu kablosuz ağ güvenliğini arttıran önemli bir özelliktir. Ancak yeni bir cihaz kablosuz ağa bağlanmak istediğinde modeme erişim yetkisi olan birinin mutlaka kayıt etmesi gerekmektedir.

Misafir Oturumu: Bazı kablosuz cihazlarda misafir oturumu olarak geçen günlük veya saatlik kablosuz ağ erişim parolası tanımlayabileceğiniz özellikler bulunmaktadır. Bu özellik, misafir olarak ziyaret eden kişilere asıl parolayı vermekten daha güvenilir bir seçenek olacaktır.

5.3 DİĞER KABLOSUZ TEKNOLOJİLERDE GÜVENLİK

5.3.1 Bluetooth

Bluetooth akıllı cihaz teknolojisi ile artık günlük hayatımızın bir parçasıdır. Akıllı cihazlarımıza kulaklık veya saat gibi cihazları bağlamak için daha çok kullansak da birçok cihazda bulunan bir özelliktir. Dizüstü bilgisayarlardan, akıllı televizyona kadar yeni nesil teknolojik cihazlarda kullanabilmekte ancak birçoğumuz farkında bile olmayabiliriz.

Bluetooth WiFi veya ethernet gibi MAC adresine sahip bir bağlantı arayüzüdür. Bu da dışarıdan gelecek olan müdahalelere açık bir kapı olması demektir. Örneğin akıllı cep telefonunun bluetooth bağlantılar için açık olduğunda, bu yetkisiz bir kişinin telefonunuzdan bilgi çalması veya takip edebileceği bir program yükleyebilmesi anlamına gelmektedir. Aynı durum dizüstü bilgisayarınız için geçerlidir. Tabi ki bunu yapacak kişinin 10 metre kadar yakınınızda olmasından başka bir ihtiyacı bulunmuyor.

Bluetooth güvenliğini arttırmak için bazı öneriler vermek gerekirse;

- Eğer kullanılmıyorsa mutlaka Bluetooth devre dışı bırakılmalıdır.
- Bağlantı için şifre belirlenebiliyorsa standart olarak belirlenen 1234 veya 0000 gibi şifreler yerine karmaşık ve en az 5 haneli şifre belirlenmelidir.
- Akıllı cihazınızda Bluetooth kullanan programları ara ara kontrol edilmeli, erişim izni olmaması gerekenlerin iznini kapatılmalıdır.
- "X aygıtından gönderilen veriyi kabul etmek istiyor musunuz?" sorusuna eğer kullanıcının bilgisi dışında bir talep ise "Hayır" cevabı verilmelidir.
- Bluetooth Kimliğe Bürünme Saldırıları (BIAS - Bluetooth Impersonation Attacks) gibi saldırılardan korunmak için daha önce veri paylaşımı için bağlanılan başkalarına ait cihazlar var ise mutlaka eşleşmeyi sonlandırılmalıdır.
- Akıllı saatler, bileklikler, kulaklıklar güvenli bağlantı olarak nitelendirildiğinden pek çok cihazda bu bluetooth aygıtlara yakın olduğunda şifre sorulmadan ekran açılabilir. Yani şifre güvenilir olabilir ama gözden kaçabilecek basit nedenlerle şifre gerekmeden cihazınıza erişim sağlanabilir.

5.3.2 NFC (Yakın Alan İletişimi - Near Field Communication)

NFC genellikle üst düzey akıllı cihazlarda bulunan bir teknolojidir. Yakın mesafeden ödeme ve veri aktarımı yapmak için geliştirilmiş bu sistem en güncel şifreleme algoritmalarını kullanmaktadır. Ancak her veri arayüzünde olduğu gibi NFC de bir güvenlik ihlaline neden olabilmektedir. NFC teknolojisine alternatif olabilecek olan QR kod neredeyse tüm cihazları desteklemesinden dolayı NFC ihtiyacı ve popüleritesini bir nebze etkilemiştir.

NFC ile ilgili en önemli ayrıntı veri aktarımı veya ödeme yapılabilmesi için 1-2 cm yakınlaşması gerekmektedir. Dolayısı ile NFC arayüzünden bir veri ihlali olabilmesi için cihaza epeyce yaklaşmak

aynı zamanda da veri aktarımını ya da ödemenin yapılacağı programın açık olması gerekmektedir. NFC arayüzünün güvenliğini sağlayabilmek için;

- Öncelikle cihazda NCF olduğundan emin olunması gerekmektedir.
- Eğer cihazda NFC desteği var ise *Ayarlar > Diğer Bağlantılar* (bu cihaza ve işletim sistemine göre değişebilir) bölümünden kullanılmıyorsa kapatılmalıdır.
- NFC ile ödeme ve veri aktarımı yapılıyorsa işlem tamamlandığında ilgili program mutlaka kapatılmalıdır.
- Cihaz ekranı kapatıldığında NFC de kapalı konuma geçmektedir ancak Bluetooth aygıtlar aracılığı ile ekran aktif olabileceğinden kontrol etmek faydalı olacaktır.

5.3.3 RFID

Aslında çok yeni bir teknoloji olmayan RFID (Radyo Frekanslı Kimlik) ucuzlaması ile günlük hayatımıza daha fazla girmiştir. Özellikle 2020 yılında yaşadığımız pandemi ile fiziksel pos cihazları ile yapılan ödemelerin büyük bir kısmı temassız ödeme özellikli kredi kartları ile yapılmıştır. NFC ile benzer şekilde kullanılan RFID için mesafe okuyucu cihaz tarafından belirlenmektedir. RFID ile ilgili en kritik durum kredi kartlarının verileri ile temassız belirli bir limite kadar ödeme yapılabilmesidir. Hatta Youtube'da farkında olmadan cebindeki kredi kartından ödeme alınan müşteri videolarını izleyebilirsiniz.

RFID ile kullanıcıları tehdit eden birkaç konu bulunmaktadır;

- Kullanıcının kredi kartı, ödeme araçları veya araç tanımlama kartları için kullanılan RFID kartlarda izinsiz okuma yapılması
- Kullanıcıya ait RFID kart verisinin kopyalanması
- RFID kart üzerindeki verinin kullanılmaz hale getirilmesi

RFID güvenliği ile ilgili en temel nokta diğer bağlantı türlerinde olduğu gibi basit bir kurala dayanıyor "Kullanmıyorsan kapat". Eğer kredi kartındaki temassız ödeme seçeneği kullanılmıyorsa çevrimiçi bankacılık hizmetinizden veya müşteri hizmetlerinden kullanıma kapatabilir ya da limiti düşürülebilir. Kart verisinin kopyalanmasına karşı ödemelerinizi takip edilmesi ve RFID kart verilerinin çıkarılmadan okunmasını engelleyen cüzdan kullanılması faydalı olacaktır.

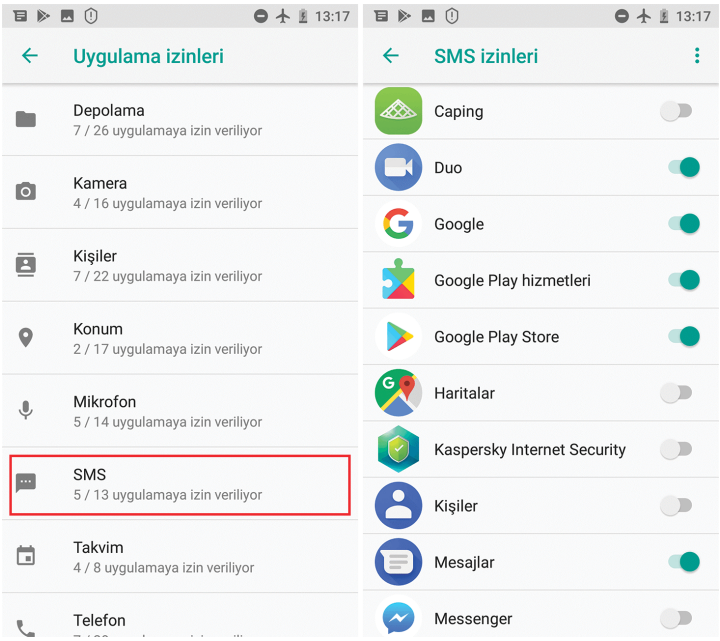
5.4 MOBİL CİHAZ GÜVENLİĞİ

5.4.1 Mobil Cihazlara Yönelik Tehditler

Akıllı cep telefonu ve tablet kullanımı, dizüstü bilgisayar kullanımına göre çok daha fazladır. Özellikle akıllı cep telefonlarının WiFi veya hücresel veri ile sürekli internet erişiminin olması bu cihazları hedef haline getirmektedir. Kullanıcıların bilgisayarlarda güvenlik yazılımları kullanırken akıllı cep telefonu ve tabletlerde güvenlik yazılımlarına ihtiyaç olmadığı gibi bir düşünce hâkimdir. Hâlbuki bu cihazlar siber korsanlar için birer hazine niteliğindedir. Bu cihazlara yönelik tehditlerden bazıları aşağıda belirtilmiştir.

a.Veri Sızıntısı: Kullanıcılar zaafiyetlere neden olabilecek çok fazla davranışa sahiptir ve kendi verilerinin öneminin farkında değildir. Uygun yönlendirme ile şifrelerini kolaylıkla verebilir veya verilerinin ele geçirilmesine neden olabilecek programları kolaylıkla kurabilir. Örneğin önceki yıllarda Google Play'de bir milyon üzerinde kullanıcıya sahip basit bir el feneri uygulamasının kullanıcıya ait birçok veriyi farklı sunuculara sızdırmıştır. Android ve IOS yeni sürümlerinde program ile ilgili izinleri kontrol edebilme imkânı gelmiş olsada suistimale çok açık bir durumdur. Benzer durum WiFi veya hücresel veri ile iletişim sağlarken şahsi birçok bilginizi aktarmak mümkün olabilir. Dolayısı ile sürekli zaman geçirdiğimiz ve yanımızda olan mobil cihazlar aynı zamanda birer açık kapı olabilir.

Mobil cihazların bunun gibi veri zaafiyetlerine neden olmaması için yapılması gereken işlem basittir. Mobil cihaza bir program kurulduğunda mutlaka izinlerinin kontrol edilmesi gerekmektedir. Bu işlem Android sürümüne göre değişmekle birlikte, ***Ayarlar> Uygulamalar ve bildirimler -> Uygulama izinleri*** yoluyla yapılmaktadır. Şekil 5.7'deki ekran görüntüsünde SMS uygulaması için için bu işlem örnek olarak gösterilmiştir [12].



Şekil 5.7. Android uygulama izinleri

Bir programın talep ettiği izinler ve kullanıcı sözleşmesi için web sitesi kontrol edilebilir. Ayrıca bilgisayarlarda kullanıldığı gibi güvenlik yazılımlarının mobil cihazlarında da kullanılması güvenlik açısından çok önemlidir.

b. Sosyal Mühendislik: Sosyal mühendislik kavramı yetkisiz erişim ve bilgi ele geçirmek için hedef olan kişinin psikolojik olarak manipüle edilmesine denir. Sosyal mühendislik yapmayı planlayan siber korsan hedef hakkında az da olsa bilgi sahibi olmalıdır. Sosyal mühendislik yapacak olan siber korsan yavaş yavaş hedefin güvenini kazanır ve ardından talep ettiği bilgiye ulaşır. Sosyal mühendislik altı temel ilkeye dayanmaktadır;

- Karşılıklılık: İnsanlar kendilerine yapılan iyiliğe karşılık verme eğilimindedir.
- Bağlılık ve Tutarlılık: İnsanlar bir fikre yazılı veya sözlü taahhüt verirse bunu yerine getirme olasılığı yüksektir.
- Sosyal Kanıt: İnsanlar diğer insanların yaptıklarını yapma eğilimindedir.
- Otorite: İnsanlar kanuna aykırı bile olsa otorite figürüne itaat etme eğiliminden dolayı söylenileni yapmaktadır.
- Sempati: İnsanlar sempati duydukları insanlar tarafından daha kolay ikna edilmektedir.
- Kıtlık: Bir fırsat için zaman veya talep sınırı bulunması teşvik edicidir.

Ülkemizde de sık sık rastlanan telefon aramaları ile dolandırıcılık yöntemi bu stratejilere dayanmaktadır. Bu tarz tehditlerin amacı maddi kazanç veya güvenlik zaafiyeti gerçekleştirmek içindir. Bu yönteme karşı yapılabilecek en iyi ve tek savunma uyanık davranmak olacaktır.

c. Güvenli Olmayan Kablosuz Ağlar: Kullanıcılar bağlanabilecekleri ücretsiz bir kablosuz ağ varken hücresel veri limitini kullanmak istemez. Ücretsiz görünen kablosuz ağ, kullanıcıya bir fırsat gibi. Şifresinin olması güvenli olduğu anlamına gelmemektedir. Müşteri bir cafede çayını söylediğinde bağlandığı kablosuz ağda bulunan ve diğer bir masada çalışıyor görünen kişi belki de diğer müşterilerin verilerini ele geçirmekle meşgul olabilir. Müşteri ile aynı ağ içerisinde bulunduğundan "Man in the middle" saldırısı yapması çok kolay olacaktır. Bu tür durumlarda şüpheci olunması ve hassas olabilecek işlemlerin bu ağ üzerinde yapılmaması önemlidir. Özellikle kredi kartı ve bankacılık işlemi gibi işlemler için hücresel verinin kullanılması çok daha güvenilir olacaktır.

d. Güncel veya Güvenli Olmayan Cihazlar ve Uygulamalar: Kullanıcıların pek önemsemediği diğer bir konu cihazın işletim sisteminin veya uygulamaların güncelliğidir. Ancak

bu güncellemeler sadece yeni özellikler kazandırmak için değil ortaya çıkan güvenlik açıklarını kapatmak için yapılmış düzeltmeler içermektedir. Kullanıcılar güncellemeler ile cihazların yavaşladığını düşünmektedir ve bu nedenle güncellemeleri uygulamaktan çekinmektedir. Hâlbuki cihazın güvenliği için işletim sisteminin ve programların güncel olması güvenlik açısından çok önemlidir.

Önemli olan diğer konu uygulamaların kurulduğu adrestir. Mobil uygulamaların bir kısmı ücretli olabilmektedir. Kullanıcılar bu programlara para vermemek için illegal kaynaklardan programları bulup kurma yolunu seçmektedir. Bunun yapılabilmesi için cihazda önemli izinler verilmesi gerekmektedir. Dolayısı ile bu izinlerin verilmesi güvenlik zaafiyeti oluşturacak bir kapının aralanması demektir.

Cihazın yazılımsal olarak güvenliğini sağlamak için yapılabilecek iki önemli nokta bulunmaktadır. Bunlardan ilki işletim sisteminin ve kullanılan uygulamaların güncel olmasının sağlanması, diğeri ise kurulacak uygulamaların güvenilir uygulama marketlerinden indirilmesidir.

e. Hırsızlık: Mobil cihazlara yönelik diğer bir tehdit boyutlarının küçük olması ve taşınabilir olması nedeni ile hırsızlıktır. Eğer bu cihazlarda güçlü bir şifre koruması, biyometrik koruma, uzaktan erişim, cihaz şifrelemesi yok ise en başta kişisel verilerin ele geçirilmesi olmak üzere birçok konuda güvenlik zaafiyeti meydana getirebilir. Böyle bir durumda kullanıcının hatası çok olmakla birlikte alınabilecek bazı tedbirler ile en az zarar yaşanması sağlanabilir.

Öncelikle cihazın ilk kullanmaya başladığında mutlaka güçlü şifreler ve mümkünse biyometrik veri ile cihazın açılmasını sağlanmalıdır. Çok fazla tedbir gibi görünsede bilgiler çalındığında onlarla ne yapılacağı tamamen çalan kişinin insafına kalmış bir durum olacaktır. Cihazın işletim sistemi veya markasına göre uzaktan erişim/yönetim seçeneklerinin aktif olmasının kaybolma veya hırsızlık durumlarında cihazı kilitleme, yerini tespit etme, uzaktan verileri temizleme gibi imkânlar sunduğunu unutulmamalıdır. Son olarak akıllı saat veya bileklik gibi giyilebilir teknolojiler kullanılıyorsa mutlaka cihazınızdan uzaklaşıldığında uyarı verecek şekilde ayarlanmalıdır. Böyle bir durum yaşandığında geç olmadan fark etmenizi sağlayacaktır.

Bulut Sistemlerden Erişim: Günümüzde Android ve IOS olarak düşünürsek mobil cihazlarda kullanılan her iki işletim sisteminin birlikte çalıştığı bulut (cloud) veri saklama sistemleri mevcut. Hatta bazı markaların kendi bulut sistemini entegre etmeye çalışması olayın ciddiyetini bir nebze arttırır niteliktedir. Çünkü kişi listesinden, fotoğraflara kadar otomatik olarak buraya yedeklemek mümkündür. Risk oluşturan boyutu korsanların iştahını kabartan bu verilerin bir yedeğinin de cihazın dışında bir yerde bulunuyor olması demektir. Son yıllarda yaşanan kişisel

veri sızıntılarını incelediğinizde çoğunun aslında direk olarak cihazı değil cihazın bağlı bulunduğu bulut sistemi hedef aldığını görebilirsiniz. Çoğu kullanıcı cihazın güvenliğini parola, biyometrik koruma ile sağlarken bulut sistemini pek düşünmemekte hatta iki aşamalı doğrulama (2FA) için cep telefonu numarası istendiğinde bunu bir tehdit olarak görmektedir. Yani bulut sistemi aslında cihaza göre tehditlere daha açık konumdadır ancak kullanmamak da başka sorunları beraberinde getirmektedir. Dolayısı ile bulut sistemin güvenliğinin sağlanması da çok önemli olacaktır.

Mobil cihaz ile entegre olarak kullanılan bulut sisteminin güvenliğini sağlamak bir kaç adımda mümkündür. İlk olarak tıpkı e-posta ve diğer çevrimiçi hizmetlerde olduğu gibi güvenilir bir şifre kullanmak çok önemlidir. İlk adımı sağladıktan sonra mutlaka yapılması gereken iki aşamalı doğrulama sistemini (2FA) aktif hale getirmektir. Hesap ayarları bölümünde bulabilecek iki aşamalı doğrulamayı birkaç farklı şekilde yapmak mümkündür. Cep telefonuna gelecek SMS mesajı veya Google Authenticator gibi zaman damgalı geçici şifreler üreten bir araçta kullanılabilir. Kullanılan bulut sistemi her ikisinin aktive edilme sürecinde yardımcı olacak adımlar içermektedir. Ayrıca cep telefonuna erişim olmaması durumuna karşı kurtarma e-posta adresi veya kurtarma şifresi seçeneklerini de mutlaka değerlendirmek yararlı olacaktır.

g. Cryptojacking ve Mobil Bankacılık: Cryptojacking coin cüzdanlarını ele geçirerek kazanç sağlama yöntemidir. Aslında ağırlıklı olarak bilgisayarları ilgilendiren bir durum olsa da son yıllarda coin borsalarının mobil uygulamalarının artmış olması akıllı cihazları için de bir tehdit oluşturmaktadır. Mobil bankacılık ise günümüzde akıllı cep telefonlarını bir kimlik teyidi aracı olarak kullanan yapı oluşturmaktadır. Cihaz kimliğini kaydederek 2FA giriş şifrelerini ilgili bankanın mobil uygulaması üzerinden direk cihazınıza göndermektedir. Şuan aşılması zor olsa da mümkün olma ihtimali bulunan bir tehdittir. Bu konudaki güvenliğin sağlanması için önceki maddelerde belirtilen güvenlik önlemlerinin alınmış olması gerekmektedir. Cihaz ve şifre güvenliği sağlandığı takdirde dikkat edilmesi gereken sosyal mühendislik olacaktır. Bankanın çevrimiçi ve telefon ile iletişim kanallarının işletişi hakkında az da olsa bilgi sahibi olmak önemli bir noktadır. Mesela bankanın müşterisini arayarak belirli bilgileri söyledikten sonra kredi kartı bilgisini veya şifresini sorması, annenizin evlenmeden önceki soyadının tüm karakterlerini öğrenmek istemesi pek de olası bir durum değildir.

5.4.2 Mobil Platformlara Yönelik Tehditler

Akıllı cihazlar sahibinin kara kutusu gibidir. Kullanıcıların elinden düşürmediği bu cihazlar muhtemelen ailelerinden daha iyi tanımaktadır kullanıcılarını... Bir yıl önce şu an neredeydiniz, üç ay önce öğlen yemeğini nerede yediniz, geçen ay en fazla kiminle sohbet ettiniz (sadece internet

ortamında da değil) bu ve bunun gibi birçok bilgiyi kayıt altına almaktadır. Bir şehir efsanesi gibi bahsedilen sohbet programlarındaki konuşmalarınızda veya bir arkadaşınız ile çay içerken bahsettiğiniz bir ürünün reklamının sürekli karşınıza çıkması akıllı cep telefonlarının pazarlama sektörüne kazandırdığı reklam modellerinden bir tanesidir.

Android: Dünyada en çok kullanılan mobil işletim sistemi olan Android, açık kaynak kodlu olması nedeni ile cihaz üreticileri tarafından en çok tercih edilen işletim sistemidir. Bir yazılımın açık kaynak kodlu olması hem bir avantaj hem de dezavantajdır. İşletim sistemindeki açıklar sürekli olarak Android geliştirme ekibi tarafından rapor edilmekte ve güvenlik güncellemeleri yayınlanmaktadır. Android için en önemli tehdit tam burada başlamaktadır çünkü güvenlik açıkları rapor edilip Android ekibi tarafından güvenlik güncellemeleri hızlı bir şekilde paylaşılırken, cihaz üreticileri bu güncellemeleri aynı hızda cihazlara uygulayamamaktadır. Hatta bazı cihaz üreticilerin bu güvenlik güncellemelerini 12 ay boyunca cihazlarına yüklemediği tespit edilmiştir. Aradaki zaman cihazların tespit edilen açıklara karşı savunmasız olduğu bir dönemdir. Bu da korsanlar için bulunmaz bir nimet olabilir.

Android işletim sistemi için diğer bir problem uygulama marketi olan Google Play'e alternatif market uygulamaları olmasıdır. Bir uygulamanın Google Play'de yer alabilmesi için kodlarının uzman ekipçe incelenmesi ve onaylanması gerekmektedir. Ama alternatif uygulama marketlerinde bu şekilde bir kontrol bulunmamaktadır. . Dolayısı ile yüklenilen uygulamanın ne içerdiği konusunda bilgi sahibi olunması çok mümkün değildir. Herkesin kullandığı sıradan bir uygulama indirildiğinde beraberinde casus yazılımların da kurulması da sağlanabilir.

IOS: Apple tarafından geliştirilen Unix işletim sistemi tabanlı IOS işletim sistemi sadece Apple cihazlarına yüklendiğinden rakiplerine göre daha avantajlıdır. Çok daha katı uygulama marketi politikasına sahiptir. Farklı uygulama marketlerinin kurulmasına normal şartlarda izin vermemektedir. IOS cihazlarınıza farklı uygulama marketi kurmak isterseniz mutlaka cihazınızı jailbreak etmeniz gerekmektedir. Jailbreak işlemi uzmanlık gerektirse de yaptığınızda Apple sistemi güvencesinden vazgeçmeniz demektir.

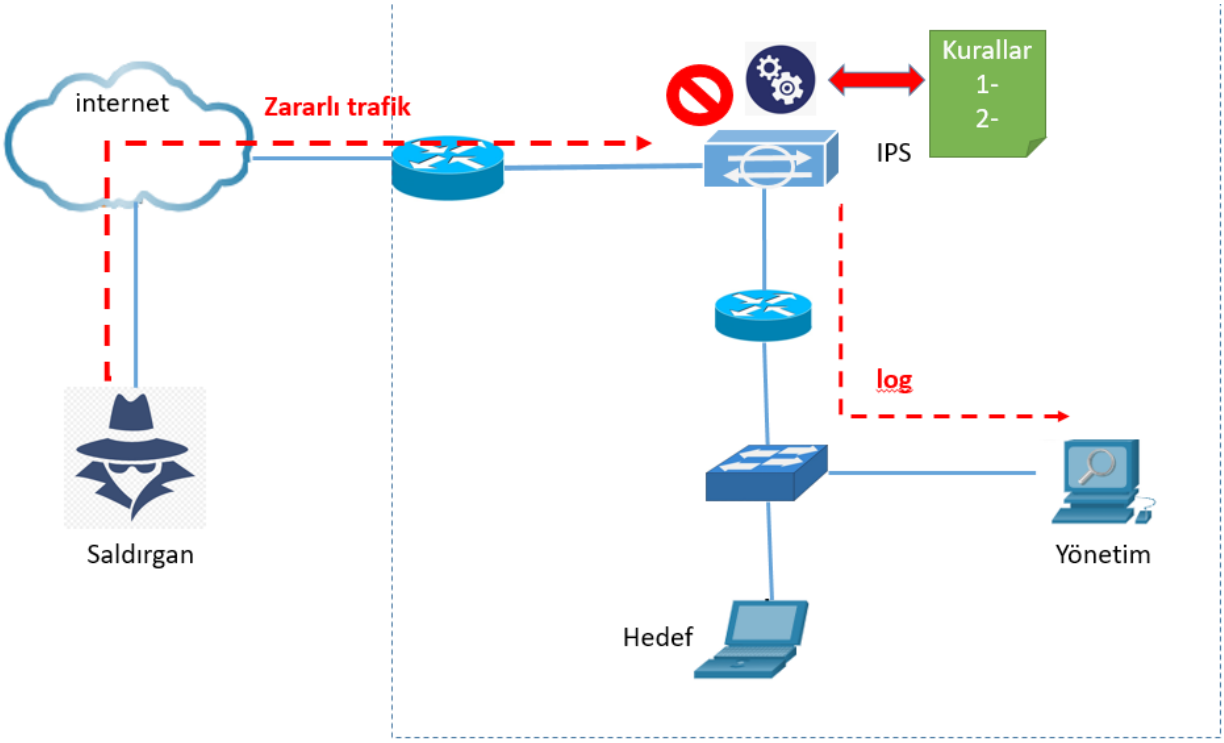
IOS ile Android siber saldırı açısından mukayese edildiğinde gerek kullanıcı sayısı gerekse sistemin yapısı nedeni ile daha az saldırıya maruz kalmaktadır. Ancak son yıllarda özellikle iCloud bulut sistemi üzerinden gerçekleştirilen veri sızıntıları kullanıcılar açısından risk oluşturmaktadır. Aynı zamanda IOS sistemine saldırı ne kadar zor olsa da sonuçlarının daha ciddi olacağı düşünülmektedir.

5.5 AĞ GÜVENLİK CİHAZLARI

"Tüm ağlar potansiyel bir hedeftir" cümlesi, ağ güvenliğinin mevcut yapısını tanımlamak için kullanılan yaygın bir sözdür. Tehditleri azaltmak için tüm ağlar güvenli hale getirilmeli ve korunmalıdır. Siber tehditlerin çeşitliliği, hedeflerin son kullanıcı cihazlarından aracı cihazlara kadar geniş bir yelpazede olması, çok katmanlı derinlemesine savunma yaklaşımını gerektirir. Bu savunma yaklaşımında, IPS, IDS, Güvenlik Duvarı gibi ağ güvenlik cihazlarının rolü büyüktür.

5.5.1 Saldırı Önleme (IPS) ve Saldırı Tespit (IDS) Sistemleri

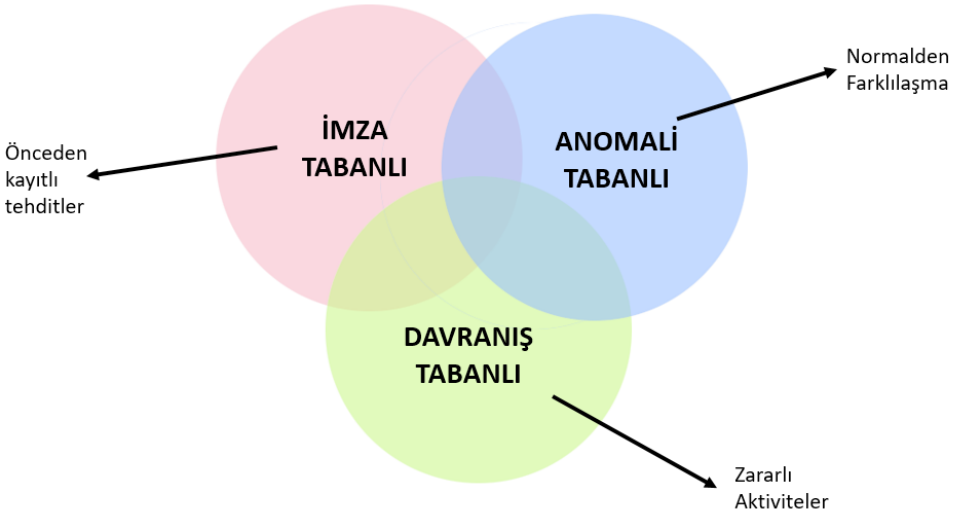
Saldırı Tespit Sistemleri (IDS), ağa offline olarak dâhil edilen ve daha önceden tanımlanan kurallara ya da ağdaki beklenmedik anomalilere göre ağ trafiklerinin saldırı olup olmadıklarını belirleyen donanımlardır.



Şekil 5.8. Bir ağda örnek IPS kullanımı

IPS gibi cihazlar ağa hat üzerinde (inline) bağlanır. Yani trafik IPS cihazından geçer. IPS, kurumsal ağa giren ağ trafiğini izler ve yapılandırılmış kurallarla karşılaştırırlar. Bir eşleşme varsa, trafik kurala göre ele alınır (engeller ya da geçişine izin verir). Durum bir yönetim konsoluna günlük (log) olarak kaydedilir. Saldırı tespit yapısında ise, trafiğin bir kopyası incelenmek üzere **IDS** cihazına gönderilir. Zararlı bir trafik varsa bu durum tespit edilebilir ancak önlenemez.

İmza tabanlı çalışan IDS ve IPS teknolojileri, ağ trafiğindeki desenleri algılamak için, tıpkı antivitüs yazılımlarında olduğu gibi imzaları kullanır. İmzalar, zararlı ağ etkinliğini tespit etmek için kullandığı bir dizi kuraldır. İmzalar, güvenlik ihlallerini ve ağ saldırılarını tespit etmek için kullanılabilir. IDS ve IPS teknolojileri, atomik imza modellerini (tek pakete bakarak saldırıyı algılayabilme) veya bileşik imza modellerini (çoklu paketlere bakarak) algılayabilir.



Şekil 5.9. Farklı mantıklarla çalışan IPS sistemleri

Ağdaki istatistiksel anomalilere göre de zararlı trafikleri analiz eden IPS sistemleri bulunmaktadır. **Davranışsal IPS** olarak adlandırılan bu sistemlerde, ağın normal davranışını belirleyen temel çizgisi (baseline) belirlenir. Bu temel çizgiye göre istatistiksel sapmalar, potansiyel zararlı ağ trafiği olarak adlandırılabilir. Ancak bu yöntemde, zararlı olmayan trafikler de zararlı olarak işaretlenebilir (***false positive alarm*** denir).

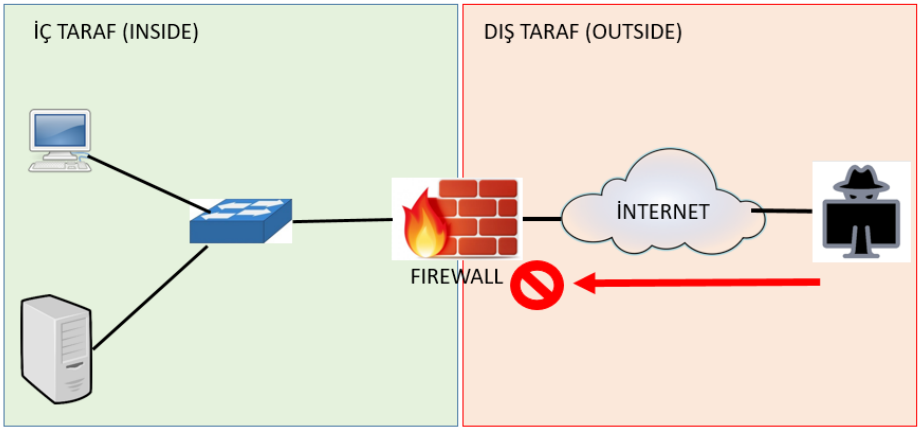
İmza tabanlı ve davranışsal analiz tabanlı IPS çözümlerinin yanı sıra, **politika tabanlı** olarak çalışan diğer bir IPS çalışma prensibi daha vardır. Bu yönteme göre, önceden ağ ile ilgili kabul

edilebilir ya da kabul edilemez trafikler politikalar olarak belirlenir. Bu politikalar ile eşleşen trafiklere ilgili politikanın belirlediği kural uygulanır.

Her ne kadar bu kısımda bahsedilen IPS cihazları, **donanımsal IPS** cihazları olsa da, kişisel bilgisayarlar için geliştirilmiş **yazılımsal IPS** güvenlik çözümleri de bulunmaktadır. Donanımsal cihazlarda genellikle ağ koruması amaçlandığından ağ **(network) tabanlı IPS**; yazılımsal IPS cihazlarında da konak **(host) tabanlı IPS** denmektedir.

5.5.2 Güvenlik Duvarı (Firewall)

Güvenlik duvarı (Firewall) teriminin kökeni, bir yangını bitişik binaların içinde sınırlandırmayı, yani bir taraftaki yangının diğer tarafa geçmesini önlemeyi amaçlayan bir duvardan gelmektedir. Aynı mantık ağ yapısında da kullanılır yani ağın bir tarafındaki istenmeyen trafik diğer tarafına geçirilmez. Şekil 5.10'daki ekran görüntüsünde, DIŞ-TARAFTAN gelen istenmeyen trafiğin İÇ-TARAF olarak belirlenen bölgeye geçişi engellenir.



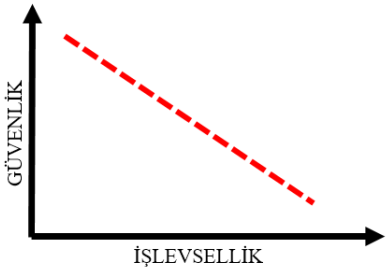
Şekil 5.10. Ağda güvenlik duvarı kullanımı

Ağ güvenlik duvarları, ağlar arasındaki trafik akışını izleyen bir dizi kurala göre çalışan ağ cihazlarıdır. Kurala göre bazı paketler (ya da trafikler) yasaklanırken bazılarına izin verilir. Güvenlik duvarları genellikle aşağıda belirlenen iki yönteme göre trafik incelemesi (veya filtrelemesi) yaparlar [20]:

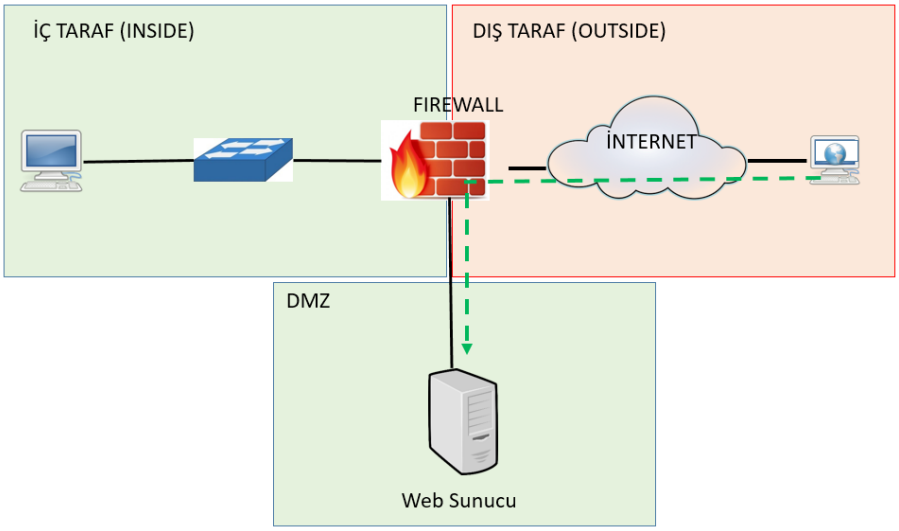
- Güvenlik duvarı, yasaklı olarak belirlenenler dışındaki tüm trafiğe izin verebilir (kara liste yöntemi).
- Güvenlik duvarı, güvenlik duvarının üzerinde çalıştığı ağ katmanına bağlı olarak belirli kriterleri karşılamayan herhangi bir trafiği reddedebilir.

Güvenlik duvarlarında trafikleri belirlemek için en temel yapıda, OSI modelinin üçüncü katmanındaki kaynak/hedef IP adresleri ve dördüncü katmanındaki bağlantı noktası numaralarını kullanır. Her ne kadar trafiği sadece bu bilgilere göre belirlemeye (analiz etmeye) çalışmak yeterli olmasa da, temel olarak bu yöntem kullanılmaktadır. Hemen her güvenlik cihazında olduğu gibi, güvenlik duvarlarının da çeşitli avantajları ve dezavantajları bulunmaktadır. Öncelikle daha önceki bölümlerde de belirtildiği gibi, güvenlik ile işlevsellik arasında ters bir korelasyon vardır.

Ağı güvenlik tehdidinden ve ihlalden korumak için sıkı savunma mekanizmaları uygulanırsa, meşru iletişimin de arızalanmasına ve performans düşüklüğüne neden olabilir. Daha hafif güvenlik uygulamak ise, ağın saldırıya maruz kalmasına neden olabilir. Bu nedenle bir siber güvenlik uzmanının ağını iyi tanıması ve bu korelasyonu doğru dengede tutması gerekir.



DMZ: Güvenlik duvarları ile bir ağı sadece iç ve dış olarak ayırmak bazı durumlarda yetersiz olacaktır. Dış ağ her zaman iç ağa göre güvensiz bir ağ olduğu göz önüne alınmalı ve iç ağa trafik girişleri incelenmelidir. Ancak bazı durumlarda, ağda yer alan web sunucusu gibi kaynaklara dışardan güvenli erişim sağlamak gerekebilir. Bu tür ağ dışından erişimin iç ağa göre daha kolay olması gereken bölgelere silahsızlandırılmış bölge (Demilitarized Zone – **DMZ**) denir.



Şekil 5.11. Güvenlik duvarı arkasında farklı bölgeler

Güvenlik duvarlarından bahsedilirken birçok teknoloji ve kavram kullanılmaktadır. Bazı kavramlar güvenlik duvarı türü iken bazıları ise kullanılan teknolojiyi tanımlamaktadır. Bu tanımlamalar ve kavramlar şunlardır:

Donanımsal güvenlik duvarı: Bir ağı korumak için tasarlanmış, ağa ek güvenlik katmanı sunan cihazlarıdır. Donanımsal güvenlik duvarları daha yüksek bant genişliğinde çalışabilir, bu da saniyede daha fazla paket işleyebileceği anlamına gelir. Ancak tek bir hata noktasının (SPoF – Single Point of Failure) oluşması dezavantajıdır.

Yazılımsal güvenlik duvarı: Yazılımsal güvenlik duvarı, sistemi kötü amaçlı yazılımlardan, solucanlardan, virüslerden ve e-posta eklerinden korumayı amaçlayan programlardır. Windows işletim sisteminde çalışan Defender, Linux işletim sistemlerindeki *IPTables* yazılımsal birer güvenlik duvarıdır. Yazılımsal güvenlik duvarları, antivirüs programlarını da içerecek şekilde özelleştirilebilir.

Paket filtrelemeli güvenlik duvarı: Bu tür güvenlik duvarları, OSI modelinin ağ katmanındaki IP başlık bilgisini ve taşıma katmanındaki, örneğin TCP'nin başlık bilgilerini kullanır. Önceden tanımlanmış kurallara göre, paketin geçmesi ya da filtrelenmesi sağlanabilir.

Durumlu Paket İncelemesi: Durumlu paket incelemesi (SPI – Stateful Packet Inspection) bir dizi kurala dayalı olarak paketlere izin verir veya engeller. TCP başlık bilgisinde yer alan SYN ve ACK bayraklarına ve sıra numarasına göre dış ağdan iç ağa paketin geçip geçmeyeceğini belirler. Diğer bir ifade ile dışarıdan gelen paketler, sadece içerden başlatılan trafiklerin cevapları ise geçiş yapabilir. Bu durum temel düzeyde basit bir koruma sağlar.

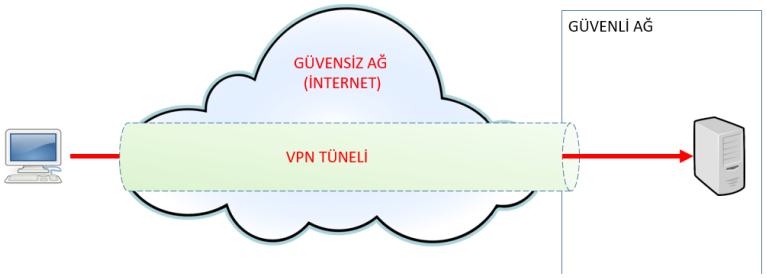
5.6 VPN TEKNOLOJİLERİ

Ağ iletişiminde veri paketlerinin taşınmasını sağlayan IP protokolünün yapısında güvenlik yoktur. Dolayısıyla salt IP paketi içerisinde taşınan veriler güvensizdir. IP içerisinde taşınan verinin güvenliği IPsec olarak adlandırılan çerçeve kullanılarak sağlanır. IPsec mimarisi, bu kitabın kriptoloji bölümünde açıklanmaktadır. Bu bölümde, IPsec mimarisini kullanan ve güvenli iletişimi sağlayan Sanal Özel Ağ (Virtual Private Network – VPN) kavramı ele alınacaktır.

5.6.1 VPN Nedir

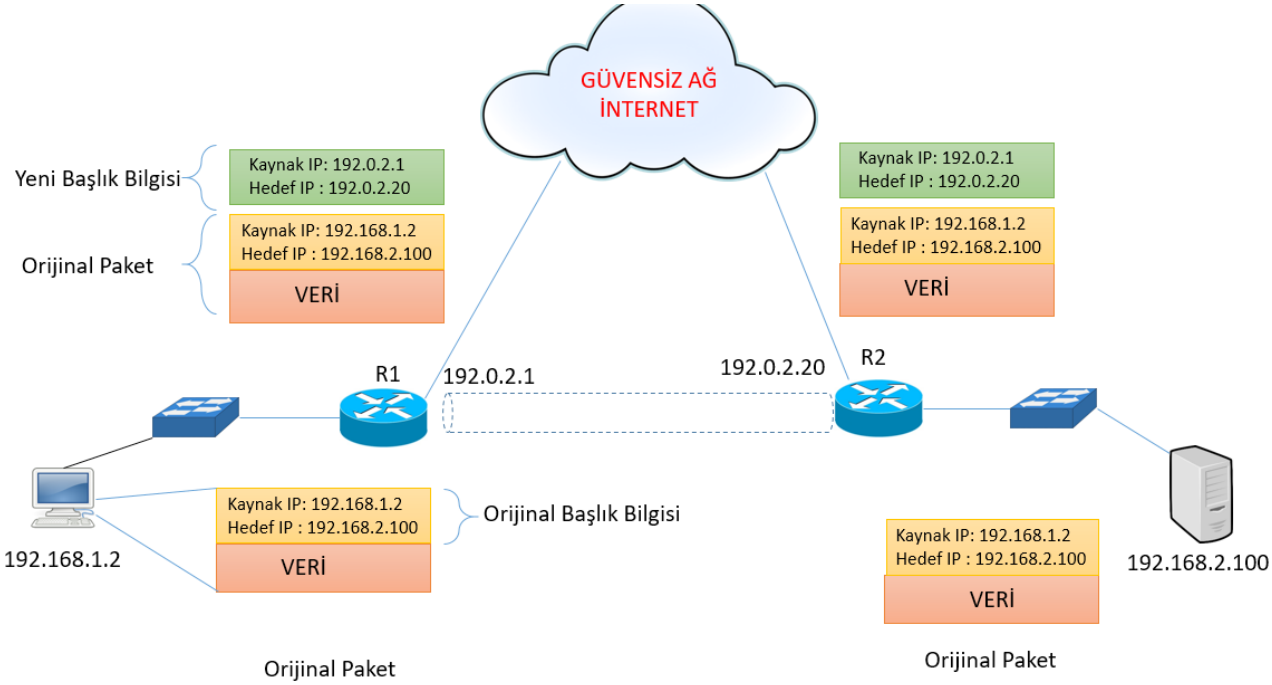
Sanal Özel Ağ (VPN), gelişmiş kriptolama teknikleri ve tünel kullanarak internet ya da extranet gibi güvenli olmayan bir ağdan güvenli, noktadan noktaya, özel (private) ağ bağlantıları kurmalarını sağlar.

VPN, gönderici kimlik denetimi (authentication), mesaj bütünlüğü (integrity) ve paketlerin yetkisiz kişiler tarafından okunmasına karşı mahremiyet (confidentiality) sağlamak için kriptografik tünel protokolleri kullanır.



Şekil 5.12. VPN tüneli

İlk VPN örneği, şifreleme ve veri bütünlüğü olmayan genel yönlendirme kapsüllemesi (GRE) ile sadece tünelleme sağlayan yapılardı. Tünel kavramı, genel olarak paketin başlığına yeni bir başlık bilgisinin eklenerek ek bir kapsülleme sunmasıdır. Bu durumda genel internet ortamında gerçek gönderici ile alıcı değil, yeni başlık bilgisindeki gönderici ve alıcı adresleri kullanılır.



Şekil 5.13. Örnek VPN tünel iletişimi

Şekil 5.13'te tünel yapısı özetle gösterilmiştir. Buna göre, normalde 192.168.1.2 adresine sahip cihaz, 192.168.2.100 adresine sahip bir sunucuya veri göndermek istediğinde, göndereceği verinin başına başlık bilgisi ekler (detaylı bilgi için kitabın ilk bölümündeki kapsülleme konusuna bakınız). Bu orijinal başlık bilgisinde gönderici ve alıcı sırasıyla 192.168.1.2 ve 192.168.2.100 olacaktır. R1 ile R2 yönlendiricileri arasında tünelleme yapılandırıldığında, gelen bu orijinal pakete yeni GRE başlık bilgisi eklenir. Bu yeni GRE başlık bilgisine göre gönderici 192.0.2.1 alıcı ise 192.0.2.20 olacaktır. Örnekte bu yeni başlık bilgisi yeşil renk ile gösterilmiştir. Bu yeni paket yapısı güvensiz olan internete gönderilir. İnternette yer alan yönlendiriciler bu paketi, 192.0.2.1 ile 192.0.2.20 arasında bir transfer olarak ele alır. Bu durum GRE tüneli olarak ifade edilir. Ancak, paketin içeriği internette yer alan yetkisiz cihazlar ya da kullanıcılar tarafından incelenirse, orijinal paket ve dolayısıyla gerçek gönderici ve alıcı tespit edilebilir. Çünkü bu yapıdaki bir tünellemede şifreleme yoktur. Bu nedenle daha önce bahsedildiği gibi, tünelin güvenilir olması için IPsec gibi şifreleme ve veri bütünlüğü iletişime eklenmelidir.

Güvenli bir VPN bağlantısı, Kimlik denetimi, Mesaj bütünlüğü ve Veri Gizliliği özelliklerini barındırmalıdır.

Kimlik Denetimi (Authentication): Mesajın güvenilir bir kaynaktan gelip yine güvenilir bir kaynağa gitmesini sağlar. VPN teknolojisi bunun için parola, dijital sertifika, smart kart veya biyometrik yapı kullanabilir.

Veri Gizliliği (Data confidentiality) : Geleneksel güvenliğin bir diğer konusu da verinin yetkisiz kişilerce okunmasını önlemektir. VPN bu durumu kapsülleme ve kriptolama (şifreleme) ile sağlar.

Veri Bütünlüğü (Data integrity): Genel erişime açık bir ağ üzerinden gelen verinin değiştirilme ya da bozulma olasılığı bulunmaktadır. Bütünlük, verinin kaynaktan hedefe gelinceye kadar yol üzerinde herhangi bir değişikliğe uğramadığının garantisidir. VPN genel olarak tek-yönlü özetleme (hash) fonksiyonu, Message Authentication Codes (MAC) ve Dijital imzalar olmak üzere üç tür veri bütünlüğü yapısı kullanır.

5.6.2 VPN Türleri

VPN teknolojisinde amaç iletişimde gizlilik ve bütünlük sağlamaktır. Bu genel amaç doğrultusunda, kullanım senaryosuna bağlı olarak değişen çok çeşitli VPN türleri bulunmaktadır. Aşağıda bu türlerden yaygın olanlar ele alınmıştır.

Siteden Siteye VPN (Site to Site VPN): Merkez bir ağ ile uzak konumda bulunan şube bir ağ gibi, farklı iki ağı internet gibi genele açık bir güvensiz ortamdan birbirine bağlayan VPN türüdür. Şube ağındakilerin merkez ağa erişimin güvenliği sağlandığından, merkez ile şube arasındaki iletişim aynı ağ yapısında gibi görünür.

Uzaktan Erişim VPN (Remote Access VPN) : Bu VPN türünde, özellikle konumu sabit olmayan uzaktan çalışanların güvenli bir ağa bağlanmasını sağlar. Bir önceki VPN türünde merkez ile şubenin konumu sabittir. Oysa uzaktan çalışan ya da mobil erişim sağlayan kullanıcıların konumu değişkenlik gösterecektir. Bu tür erişimler için, bir VPN istemci yazılımına ihtiyaç duyulan VPN bağlantısı ya da web üzerinden SSL ile bağlantının sağlandığı istemcisiz VPN türleri bulunmaktadır.

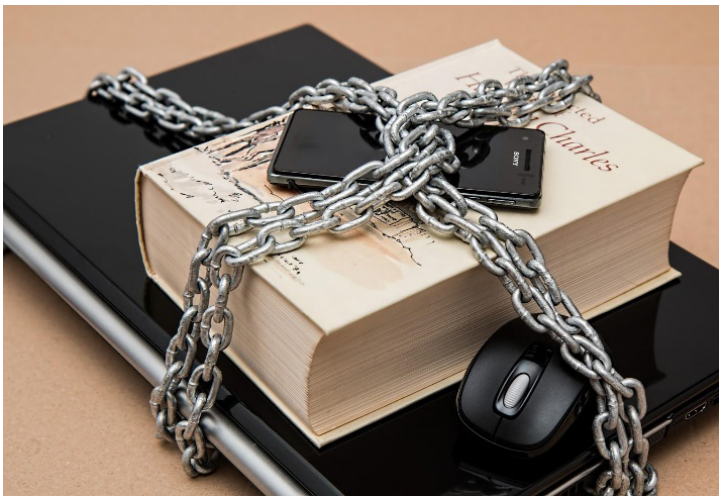
Bu türlerin haricinde PPTP VPN, L2TP VPN, MPLS VPN ve DMVPN gibi türler de bulunmaktadır.

Siber Güvenlik

BÖLÜM 6

İŞLETİM SİSTEMİ GÜVENLİĞİ

İŞLETİM SİSTEMİ GÜVENLİĞİ



İşletim sistemi; bilgisayarda çalışan, donanım kaynaklarını yöneten ve çeşitli uygulama yazılımları için alt yapı sağlayan bir yazılımlar bütünüdür. İşletim Sistemi aslında bizim uygulama yazılımlarını kullanmamıza olanak sağlayan donanım ile haberleşen bir aracıdır. Biz onun sayesinde işimize yarayan programları kullanır ve onun üzerinden programlar çalıştırılır. Yani işletim sistemi, donanım ile uygulama yazılımları arasında bir köprü görevi görür. Bilgisayar sistemlerinin temel yapısını oluşturan işletim sistemleri, üzerinde çalışan uygulamalara da güvenlik alt yapısını sağladığı için işletim sisteminin güvenliği bütün sistemin güvenliği için büyük bir rolü üstlenmiştir. İşletim sistemi açıkları ve zaafiyetlerine karşı gerekli önlemler alınmadığı sürece sistem risk altına girebilir ve büyük zararlara uğrayabilir. İşletim sisteminin risk altına girmesi aynı zamanda bilgisayardaki tüm uygulamaların da tehlikede olduğu anlamına gelmektedir.

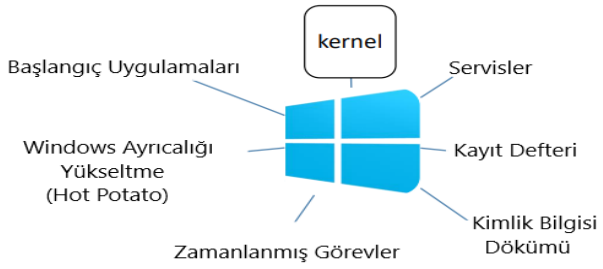
İşletim sistemlerinde hali hazırda bulunan güvenlik yazılımları kullanıyor olsalar bile, sistem yöneticileri ve kullanıcıların güvenlik konularına hâkim olmaları ve olası bir tehdite karşı da uyanık olmaları gerekmektedir. Aynı zamanda işletim sisteminin vadettiği güvenlik yazılımlarının da sınanması ve bu fonksiyonları yerine getirip getirmediğinin onaylanması güvenilirlik açısından çok önemlidir. Sistemin sıkılaştırarak en güvenli hale getirilmesi gerekmektedir.

Windows, Linux ve Mobil İşletim Sistemlerinde güvenliğin, yani sistem sıkılaştırmanın en üst seviyeye çıkarılması için yapılması gerekenlerden bahsedilecektir.

6.1 WİNDOWS İŞLETİM SİSTEMİ GÜVENLİĞİ

Windows işletim sistemi Microsoft tarafından geliştirilen kapalı kaynak kodlu ve genellikle ücret ödeyerek sahip olduğumuz bir işletim sistemidir. Bunun iyi yanları ve kötü yanları elbette vardır. İyi yanı güvenlik için birileri sizin adınıza bir sürü uygulama geliştirmiş ve bunu size sunmuştur. Sizin tek yapmanız gereken o araçları kullanmak ve gerektiğinde olaya müdahale etmektir. Kötü yanı ise arka planda ne tür uygulamaların çalıştıklarını bilmemektir.

Windows'un çıktığı günden itibaren değişik isimlerde sürümleri piyasaya sürülmüştür. Bunlardan en güncel olan işletim sistemi Windows 10'dur. Bu bölümde Windows 10 işletim sistemi ele alınmıştır [39].



Şekil 6.1. Windows temel özellikleri

Windows 10, Microsoft tarafından geliştirilen, Windows NT ailesinden olan bir işletim sistemidir. Windows NT ailesinin çıkan en son sürümüdür. Temmuz 2015 de piyasaya sürülmüştür.

Windows 10, ek ücret ödemeden kapsamlı ve yerleşik bir koruma hizmetini verir. En son virüsten koruma özelliğini sağlayan Windows Güvenliği'ni sunar. Windows 10 çalışmaya başladıktan sonra bu araç devreye girer ve bizi kötü amaçlı yazılımlardan, diğer tehdit aktörlerinden etkili bir şekilde gerçek zamanlı olarak bilgisayarımızı korur. Buraya ulaşmak için;

Başlat > Ayarlar > Güncelleştirme ve Güvenlik > Windows Güvenliği i seçiniz.

Virüs ve Tehdit Koruması: Cihazımıza karşı gelebilecek tehditleri takip edebilir, tarama yapabilir ve en son tehditleri belirlemeye yardımcı olacak güncellemeleri yapabilir.

Hesap Koruması: Oturum açma seçeneklerini ve hesap ayarlarına erişilen menüdür.

Windows da 6 farklı oturum açma seçeneği vardır.

1- Windows Hello Yüz Tanıma

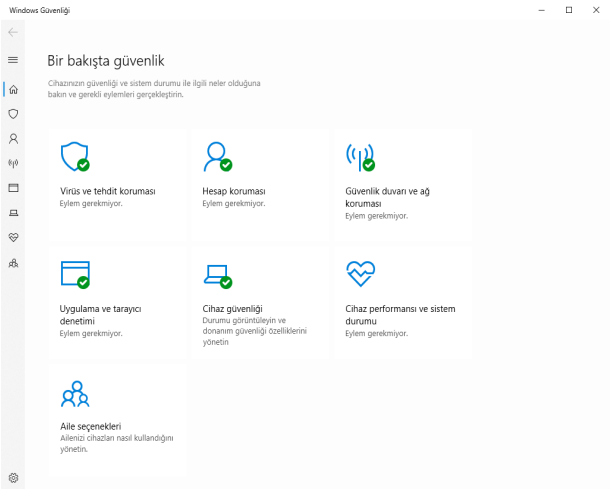
2- Windows Hello Parmak İzi Tanıma

3- Windows Hello Pin

4- Güvenlik Anahtarı

5- Parola

6- Resimli Parola



Şekil 6.2. Windows güvenliği ekran görüntüsü

Güvenlik Duvarı ve Ağ Koruması: Güvenlik duvarı ayarlarını yönetip ağ ve internet bağlantılarında neler olup bittiğini takip edebilecek bölümdür.

Uygulama ve Tarayıcı Denetimi: Cihazlara zarar verebilecek uygulama, dosya, site ve indirmelere karşı korur. Exploit Protection özelliği ile cihazın sistem ve uygulama tabanlı olarak saldırılara karşı korunabilir. Koruma ayarlarını özelleştirerek daha sıkı bir sistem haline gelebilir.

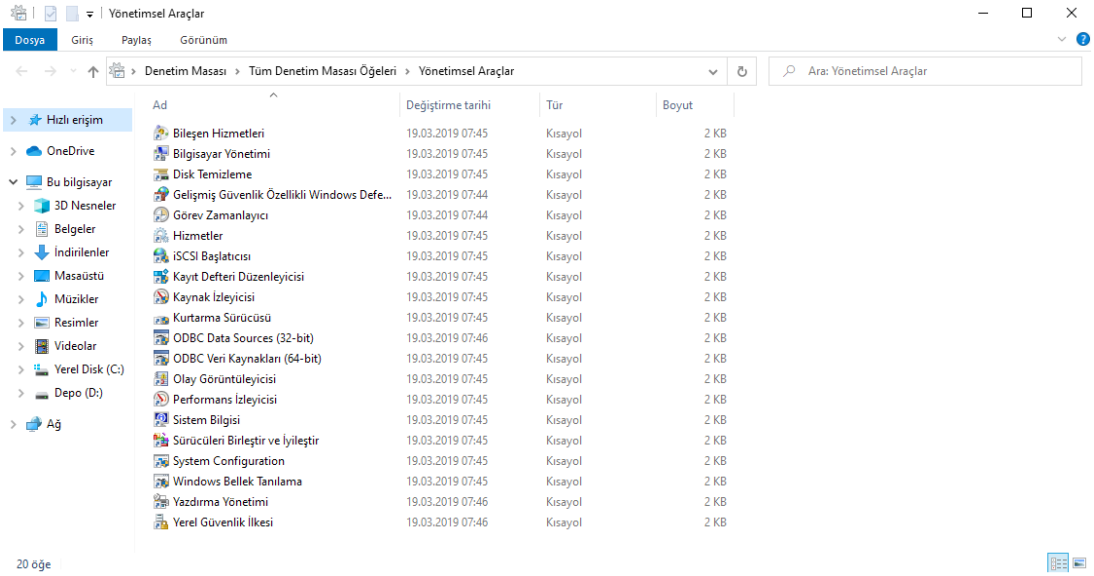
Cihaz Güvenliği: Cihazın kötü amaçlı yazılımların saldırılarına karşı korumaya yardımcı olmak için kullanılan güvenlik seçeneğidir.

Cihaz performansı ve sistem durumu; Cihazın performans durumu hakkındaki bilgileri görüntüler ve cihazın sistem durumu hakkında rapor veren kısımdır.

Aile seçenekleri: Ailenizin dijital yaşamını basitleştirmek ve Ebeveyn denetimi sağlayan, cihazlarımızı görüntüleyip, güvenlikleri durumunda raporlar alabileceğimiz kısımdır.

6.1.1 Windows Yönetimsel Araçlar

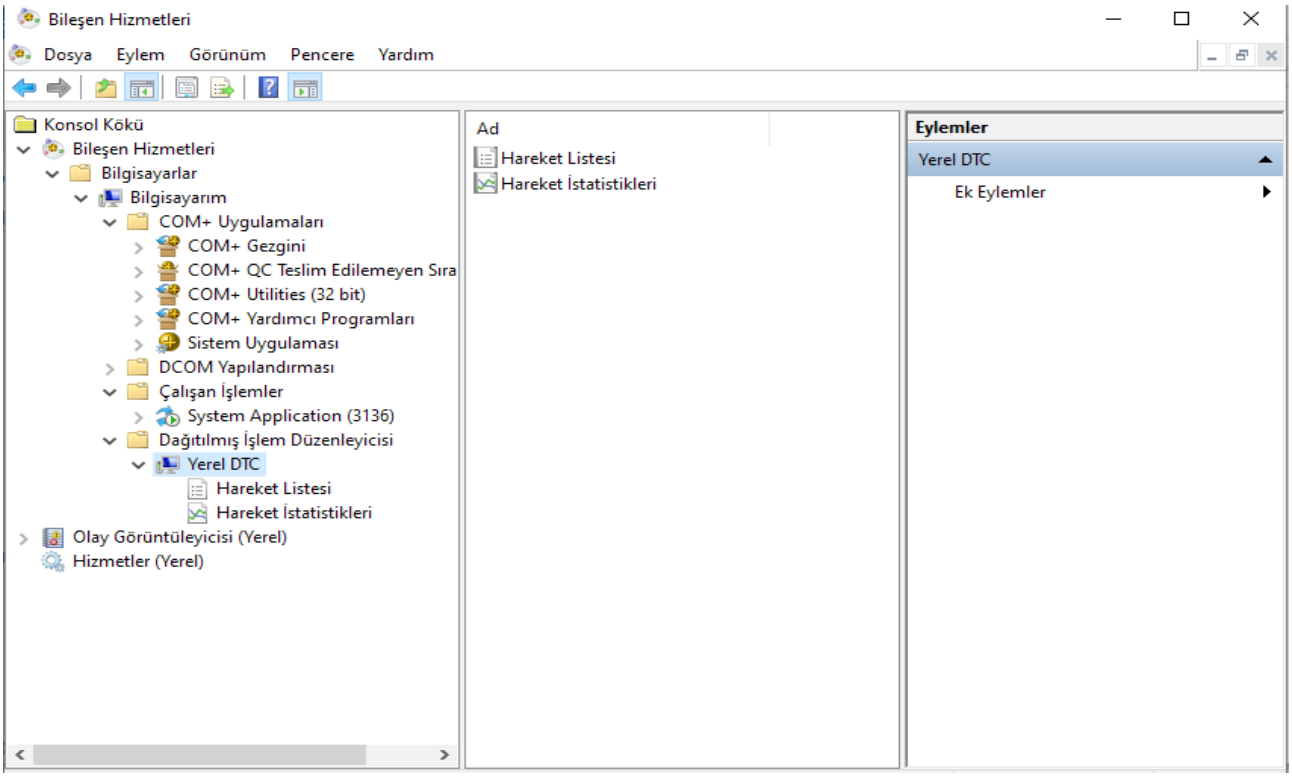
İşletim sisteminin iyi bir performansı için çalışan pek çok şeyle birlikte, ileri düzey kullanıcılar arasında en çok tercih edilen bir yönetim aracı vardır. Windows 10'un üzerinde hali hazırda gelen **Yönetimsel araçlar** içerdiği bilgiler ile kullanıcıların işine yaramaktadır.



Şekil 6.3. Windows yönetimsel araçlar ekranı

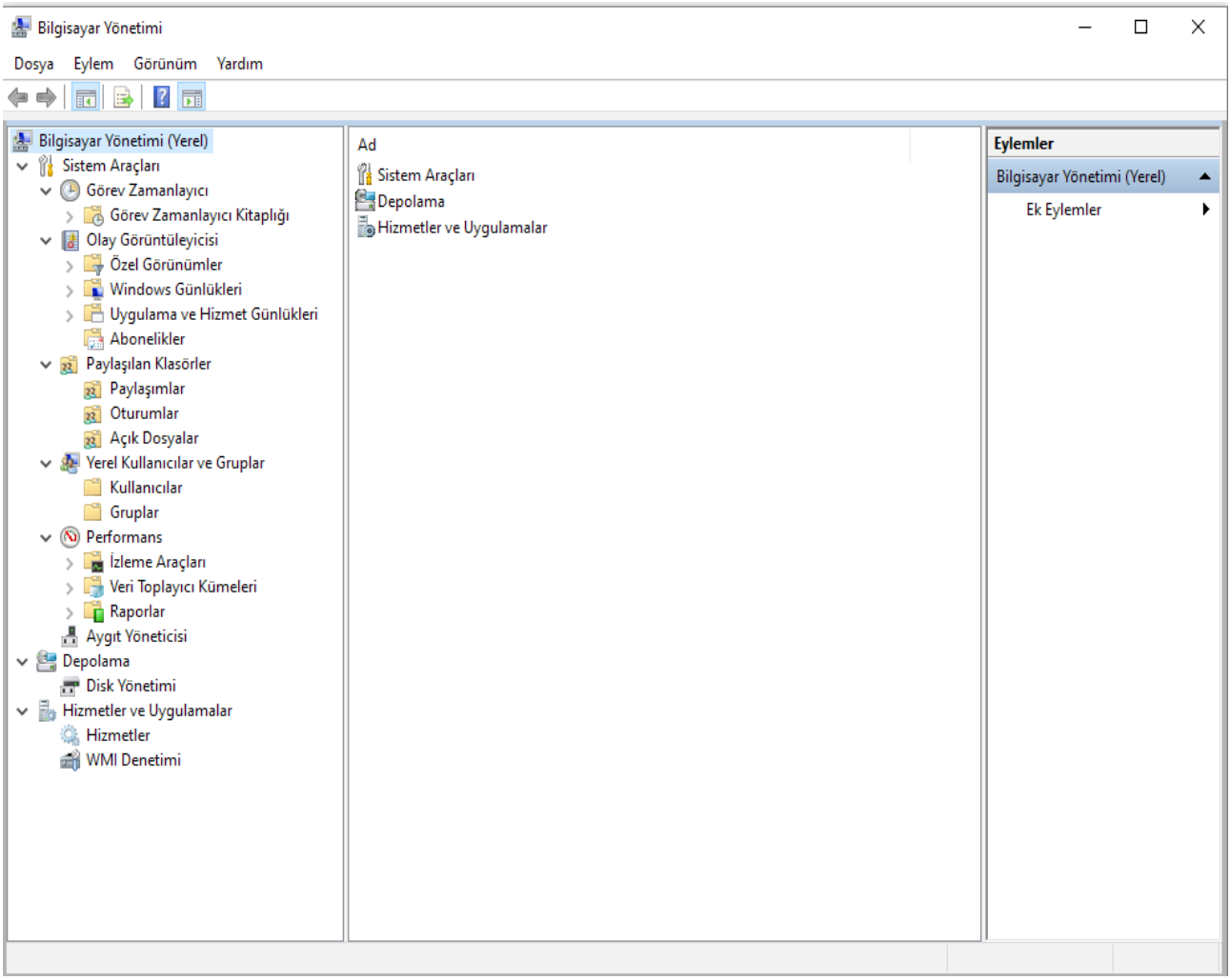
Bileşen Hizmetleri : Bileşen Hizmetleri, Microsoft Yönetim Konsolunun bir parçası olan ek bir bileşendir. COM bileşenlerini ve COM+ uygulamaları yapılandırmaya ve yönetmeye olanak tanır. Bileşen Hizmetleri Gezgini aracılığıyla yönetilir.

COM nedir ? : COM, programlama dilinden bağımsız, yazılım program parçacıklarını (component) geliştirmek için belirlenen standartlar topluluğudur.



Şekil 6.4. Windows bileşin hizmetleri ekranı

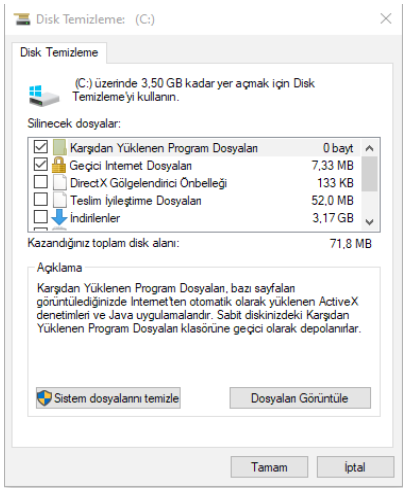
Bilgisayar Yönetimi : Bilgisayar Yönetimi, bir pencerede çeşitli yönetim araçlarından oluşan bir konsol ekranıdır. Yerel ve Uzak bilgisayarı yönetmeye yardımcı olur. Tüm yönetim araçlarının bir konsola dâhil edilmesi, kullanıcılar için kolay hale getirir.



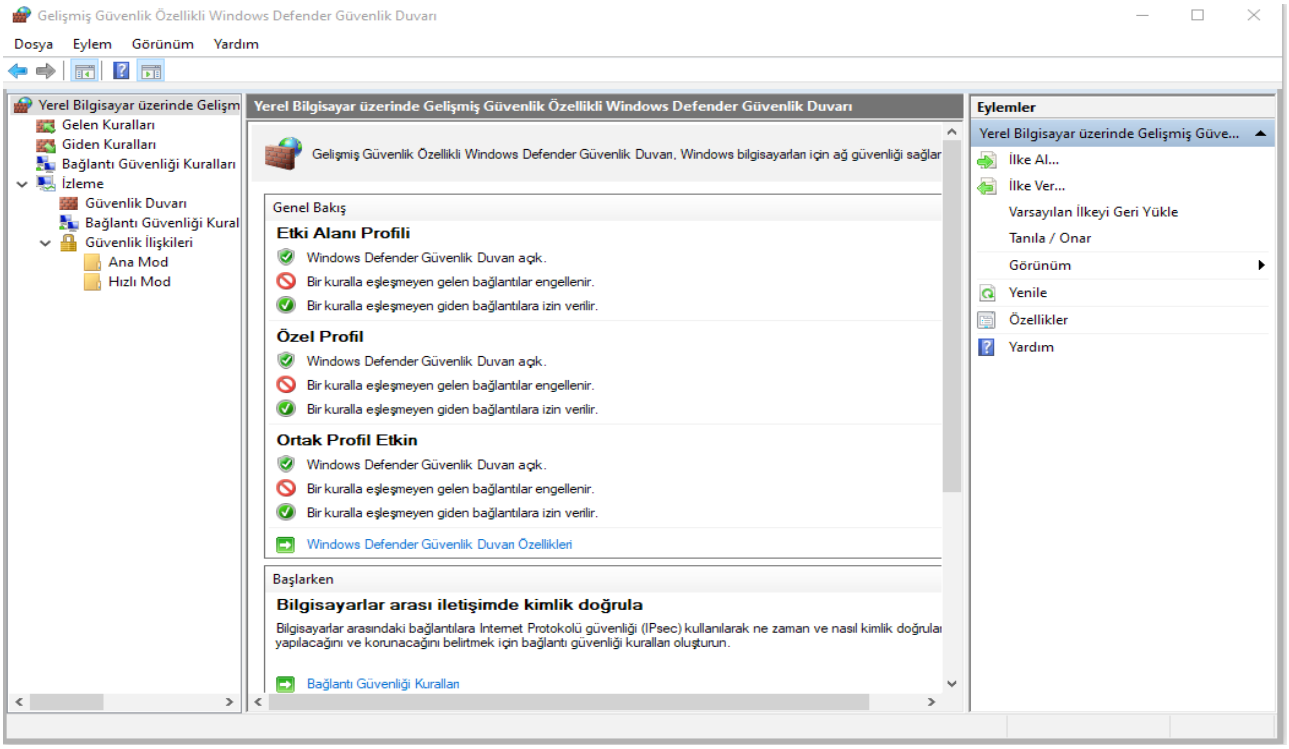
Şekil 6.5. Windows bilgisayar yönetimi

Disk Temizleme : Diski gereksiz dosyalardan temizlememizi sağlar. Geçici dosyalar, kurulum günlükleri, güncelleme günlükleri, Windows güncelleme önbelleği ve diğer alanlar gibi istenmeyen dosyaları belirlemeye yardımcı olur ve diskin anında temizlenmesini kolaylaştırır.

Gelişmiş Güvenlik Özellikli Windows Defender Güvenlik Duvarı : Güvenlik söz konusu olduğunda bu araç en önemlisidir. Herhangi bir uygulama için sisteme eklemek isteyebileceğimiz tüm kuralları ve istisnaları içinde bulundurur. Güvenlik duvarı, işletim sistemi güvenliğinde savunma hattının en önünde yer alır. Sistemdeki herhangi bir uygulamayı engellemek ve izin vermek isteyip istemediğimizi belirlememize yardımcı olur.

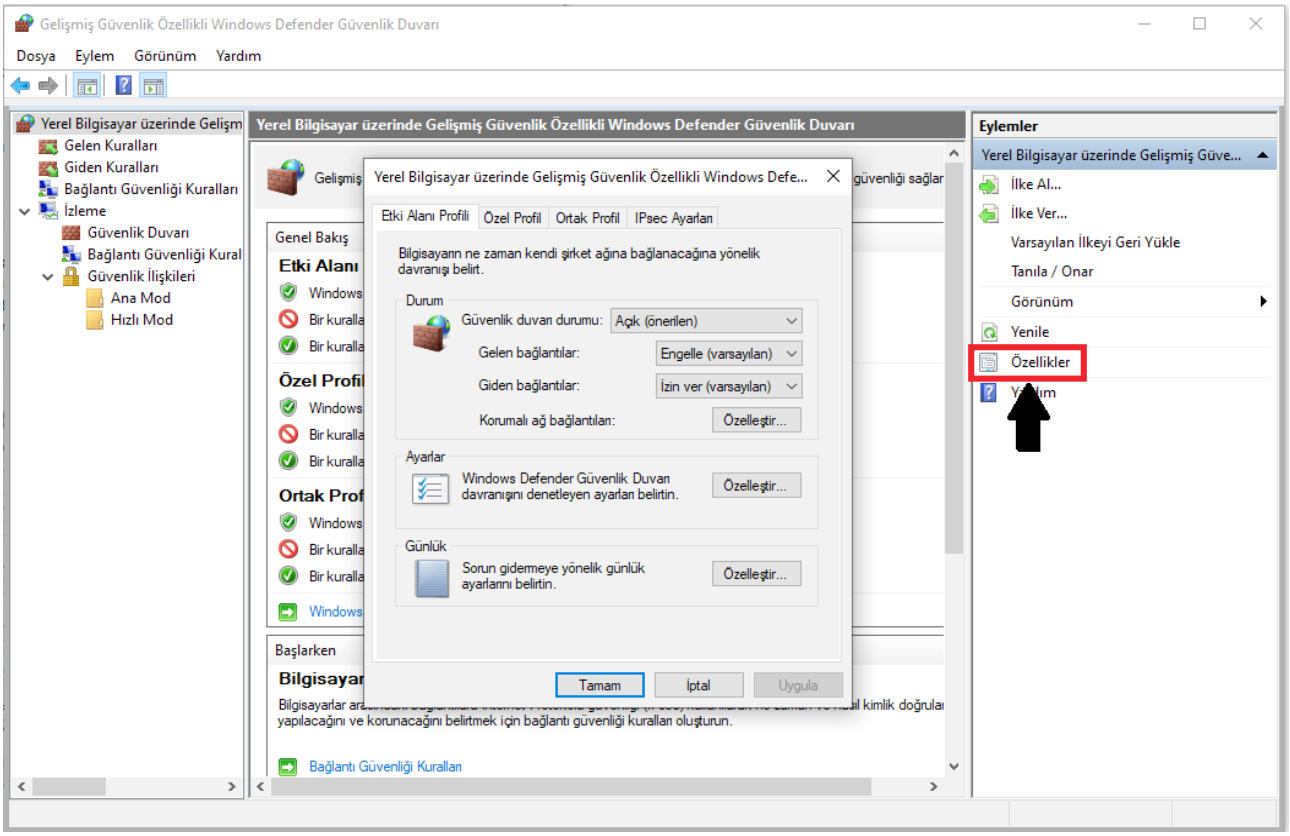


Şekil 6.6. Windows disk temizleme



Şekil 6.7. Windows güvenlik duvarı

Eylemler bölümünde yer alan Özellikler seçeneğine tıklandığı zaman aşağıdaki ekran karşımıza gelmektedir. Bu ekranda sırasıyla, Etkin Alanı Profili, Özel Profil, Ortak Profil ve IPsec Ayarları bulunmaktadır.



Şekil 6.8. Windows güvenlik duvarında gelişmiş ayarlar

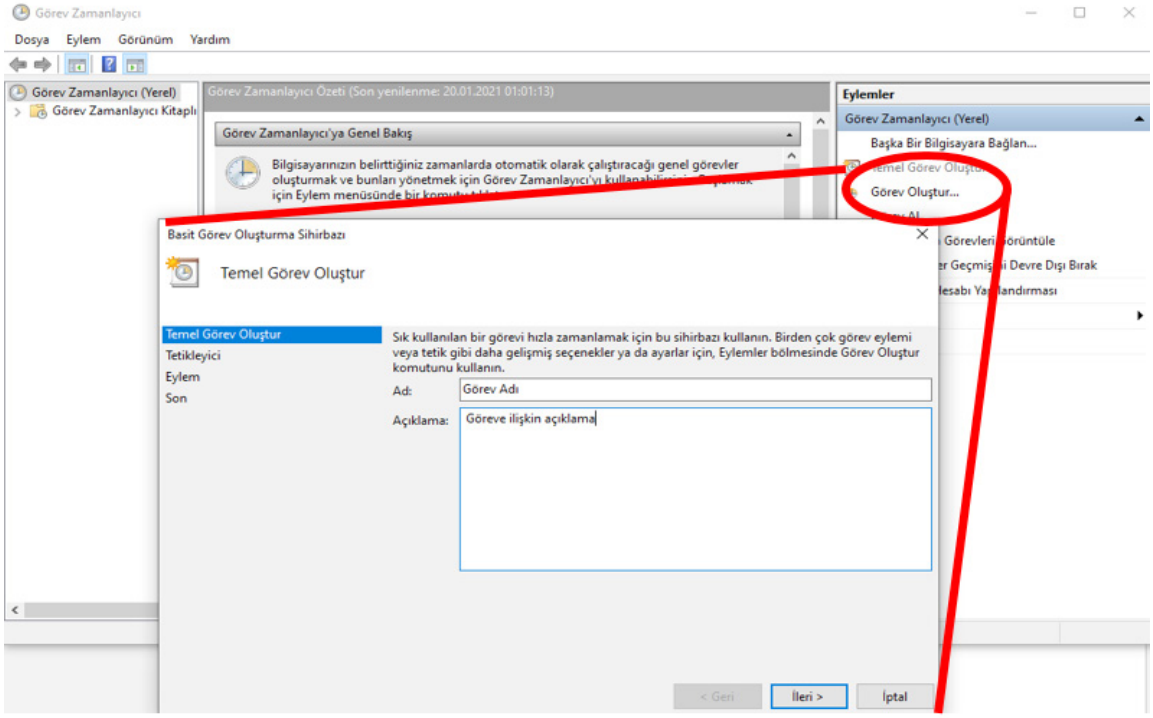
Etki Alanı Profili, Özel Profil ve Ortak Profil: Bu sekme ile Güvenlik Duvarını kapatıp açabilir, Gelen ve Giden bağlantılara İzin verip, Engelleyebilir, Korumalı Ağ Bağlantıları bölümünden etki alanı profili için korumalı ağ bağlantılarını aktif ya da pasif edilebilir. Ayarlar bölümünden Güvenlik Duvarı Davranışını Özelleştirilebilir, Günlük bölümünden de günlük dosyalarının konumunu, boyutunu, bırakılan paket günlüğü ve başarılı bağlantılar günlüğü ayarları yapılır.

IPsec (Internet Protokolü Güvenliği) Ayarları :

IPsec: İnternet Protokolü kullanılarak sağlanan iletişimlerde her paket için doğrulama ve şifreleme kullanarak koruma sağlayan bir protokol paketidir. İçinde bulundurduğu protokoller sayesinde oturum başlarken karşılıklı doğrulama ve oturum sırasında anahtar değişimlerini gerçekleştirme hakkına sahiptir.

Bu sekme ile IPsec varsayılan bölümünden ayarlarını (Anahtar değişimi, Veri koruması, Kimlik doğrulama yöntemini ayarlanır. Etkin bağlantı güvenliği kuralları olduğunda, IPsec güvenli bağlantılar kurmak için bu ayarları kullanır.) özelleştirebilir. IPsec muafiyetleri bölümünden, ICMP paketini IPsec ten muaf tutulabilir. IPsec tüneli yetkilendirmesi bölümünden ise IPsec tüneli kurmakla yetkilendirilen kullanıcıları ve bilgisayarları belirlenir.

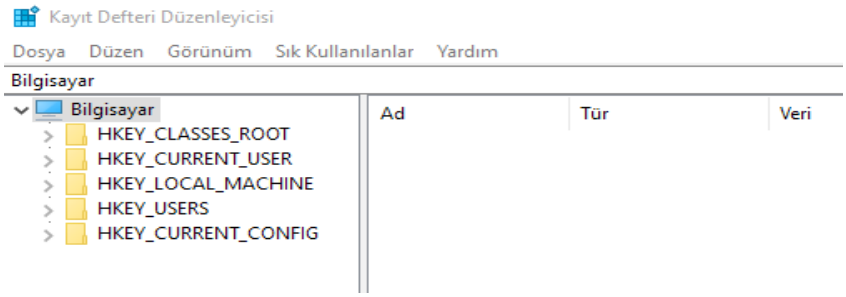
Görev Zamanlayıcısı : Günlük, haftalık, aylık, sadece bir kez vb gibi belirlenen zamanlarda otomatik olarak çalıştıracağı görevler oluşturmak ve bu tanımlı görevleri yönetmek için kullanılır.



Şekil 6.9. Windows görev zamanlayıcısı

Hizmetler : İşletim sistemi çalışmaya başladıktan sonra arka planda çalışan tüm hizmetleri görüntülemek için kullanılan araçtır. Bu araç işletim sistemindeki tüm hizmetleri yönetmeyi ve ayrıca sistem kaynaklarını tüketen hizmetleri öğrenmeyi sağlar. Herhangi bir hizmeti Başlatabilir, Durdurabilir, Durdaklatabilir, Devam Ettirebilir, Yeniden Başlatılabilir.

Kayıt Defteri Düzenleyicisi : Windows ve çoğu program, birçok yapılandırma ayarını bu bölümde saklar. Programlar, ayarlarını yapılandırma dosyalarında da saklayabilirler ancak çoğunlukla Kayıt Defterini kullanırlar [40]. Kayıt Defteri, işletim sisteminin içerisinde yer alan kayıtlarını, ayarlarını, tercihlerini ve diğer verileri barındıran bir ana veri tabanıdır. Bilgisayara yeni bir program yüklendiğinde bu programa ait ayarlar, hangi dizinde yer aldığı, programın sürümü gibi birçok anahtar kayıt defterine işlenir. Kayıt Defteri aşağıdaki ana bölümlere ayrılmıştır. Kayıt defteri düzenleyicisine ulaşmak için arama çubuğuna yada çalıştır bölümüne **regedit.exe** de yazılabilir.



Şekil 6.10. Windows kayıt defteri (regedit) ekranı

HKEY_CLASSES_ROOT	Temel sistem bilgilerini içeren dosyaların olduğu bölümdür. Kısayol bilgileri, dosya ilişkilendirmeleri bulunur. Eğer silinirse sistem açılır fakat hiçbir dosya açılamaz.
HKEY_CURRENT_USER	O anda oturum açmış kullanıcıyla ilgili bilgileri tutar.
HKEY_LOCAL_MACHINE	Sistemle ilgili bilgileri tutar. Donanım ayarları ve bazı yazılım ayarlarının bulunduğu yerdir.
HKEY_USERS	Bilgisayardaki kullanıcı hesaplarıyla ilgili bilgileri tutar. (Örneğin; Masaüstü arkaplanı, denetim masası ayarları vb.)
HKEY_CURRENT_CONFIG	Mevcut donanım profiliyle ilgili bilgileri tutar.

Tablo 6.1. Windows regedit ana bölümler tablosu

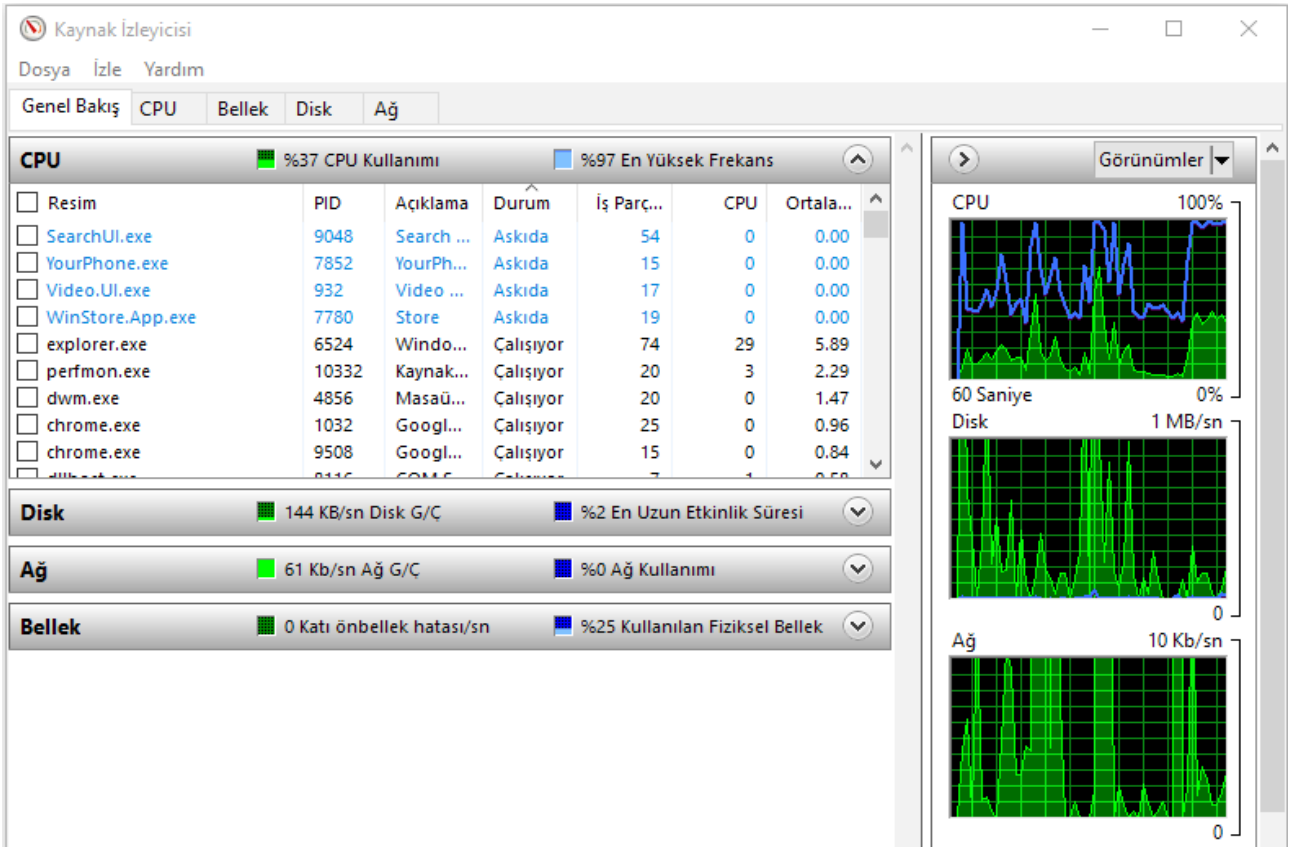
Kayıt defterine istersek kendi elimizle de kayıtlar girebilir veya girilen bir kaydın değerini değiştirebiliriz. Fakat bu iş çok riskli bir işlem olacaktır. Yapılan yanlış bir giriş sisteminizin çalışmamasına veya çalışan programlarınızın çalışmamasına neden olabilir. Aşağıdaki tabloda kayıt defterine yazabileceğimiz sık kullanılan veri türleri yer almaktadır.

Veri Türü	.reg Dosyasındaki Veri Türü
REG_BINARY	Ham ikili veriler. Çoğu donanım bileşeni bilgisi ikili veri olarak depolanır ve Kayıt Defteri Düzenleyicisi'nde onaltılık biçimde görüntülenir.
REG_DWORD	4 bayt uzunluğunda bir sayıyla temsil edilen veriler (32 bitlik bir tam sayı). Aygıt sürücüleri ve hizmetleri için birçok parametre bu türdendir ve Kayıt Defteri Düzenleyicisi'nde ikili, onaltılık veya ondalık biçimde görüntülenir. İlgili değerler, DWORD_LITTLE_ENDIAN (en önemsiz bayt en düşük adrestedir) ve REG_DWORD_BIG_ENDIAN'dır (en az anlamlı bayt en yüksek adrestedir).
REG_EXPAND_SZ	Değişken uzunluklu veri dizesi. Bu veri türü, bir program veya hizmet verileri kullandığında çözülen değişkenleri içerir.
REG_MULTI_SZ	Çoklu dizge. İnsanların okuyabileceği bir biçimde listeler veya birden çok değer içeren değerler genellikle bu türdendir. Girişler boşluk, virgül veya diğer işaretlerle ayrılır.
REG_SZ	Sabit uzunlukta bir metin dizesi.
REG_QWORD	64 bitlik bir tam sayı olan bir sayıyla temsil edilen veriler. Bu veriler, Kayıt Defteri Düzenleyicisi'nde İkili Değer olarak görüntülenir ve Windows 2000'de kullanıma sunulmuştur.

Tablo 6.2. Windows regedit veri türleri

Kaynak İzleyicisi

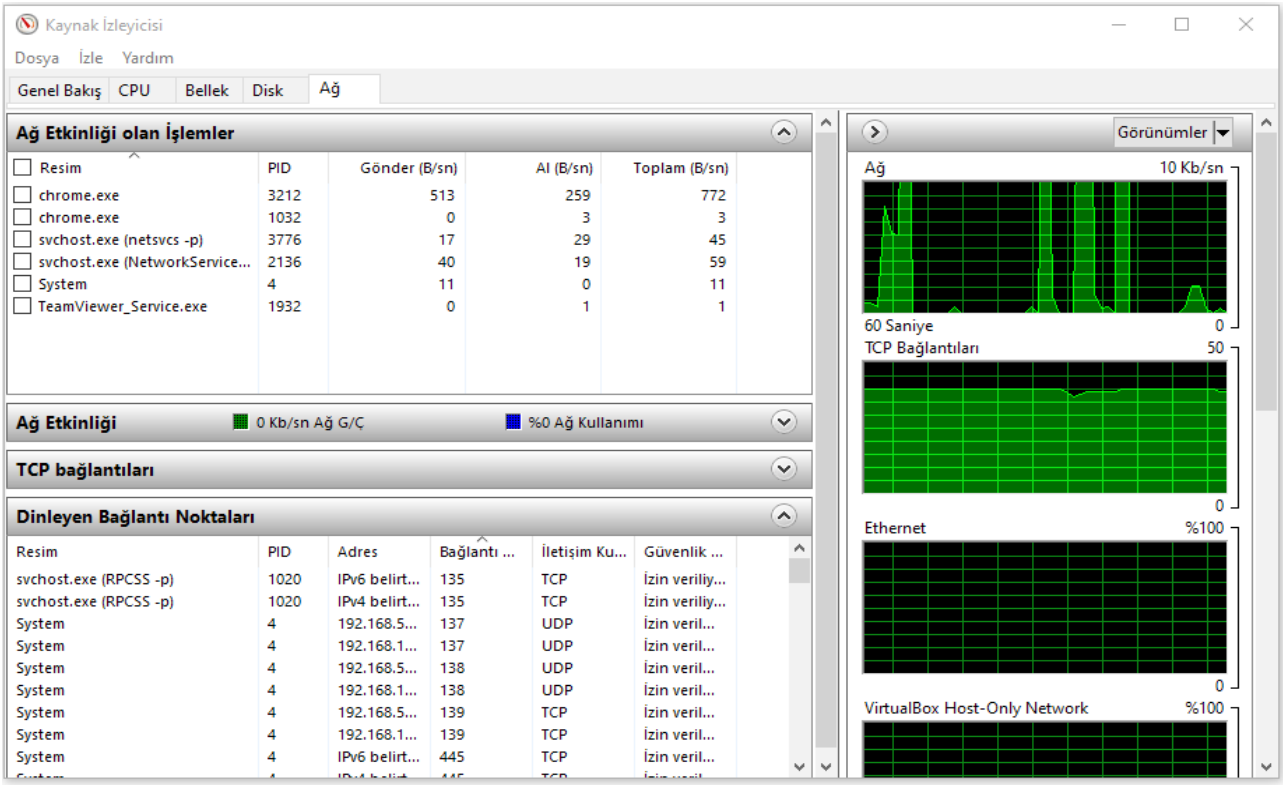
CPU, disk, ağ ve bellek kaynaklarının gerçek zamanlı kullanımı ve performanslarını izlemek için kullanılır.



Şekil 6.11. Windows kaynak izleyicisi

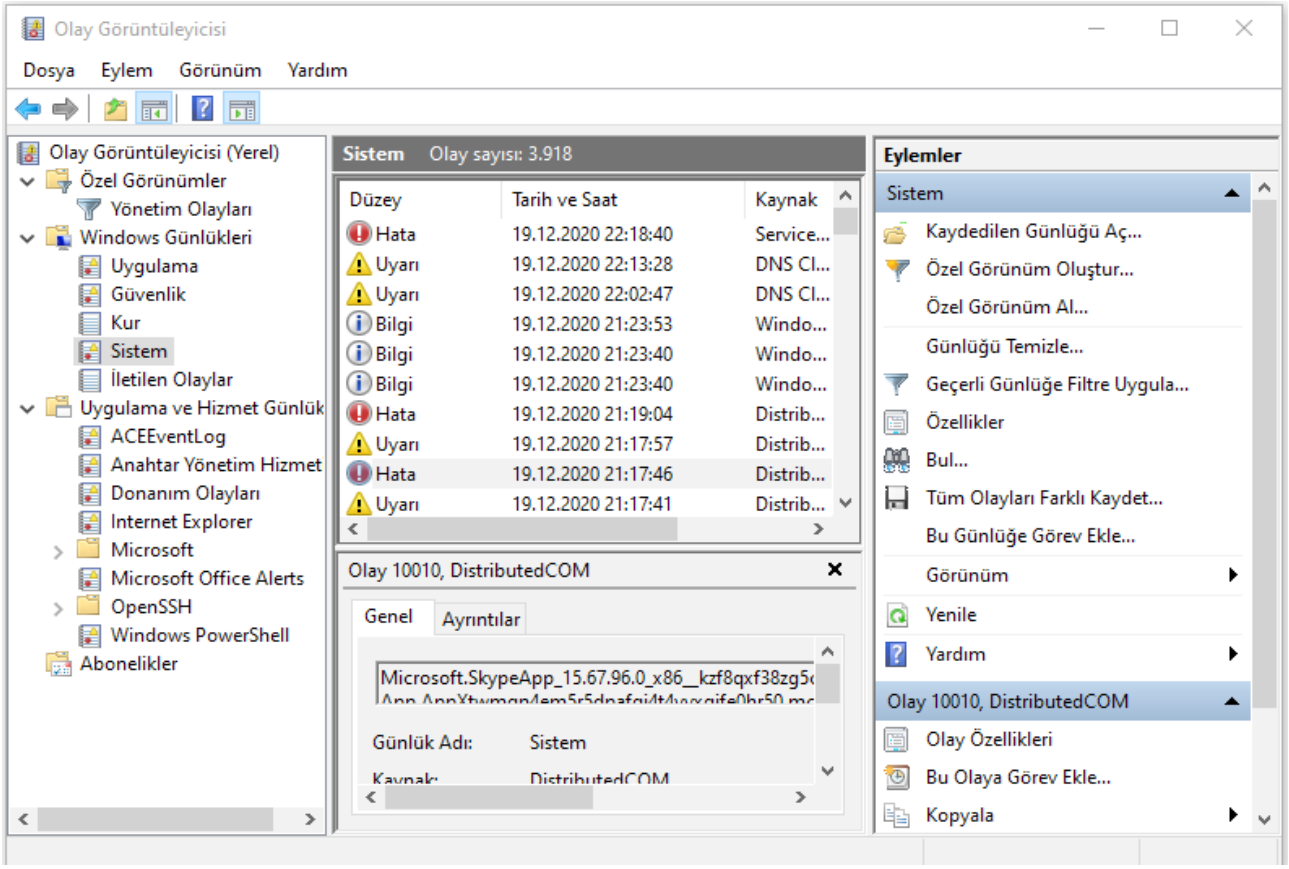
CPU sekmesinde işlemcinin o anda çalışan işlemleri (process), PID değerlerini, açıklamalarını, durumunu, iş parçacıklarını (thread), ortalama CPU gibi bilgiler görüntülenir. Bellek sekmesinde belleği programları, PID değerini, Katı önbellek hatasını, ayrılan kb değerini, çalışma kümesini kb cinsinden, paylaşılabilir kb bilgisini ve özel kb değerleri görülebilir. Disk sekmesinde diski kullanan programları, PID değerlerini, o anda Okunan, yazılan ve toplam veri miktarını B/sn cinsinden

izlenebilir. Ağ sekmesinde ise ağı kullanan programları, PID değerlerini, o anda gönderilen, alınan ve toplam veri miktarını B/sn cinsinden izlenebilir. Ayrıca Ağ sekmesinin altında Ağ Etkinliğini izlenebilir, TCP bağlantılarını görülebilir ve Dinleyen Bağlantılar izlenebilir.



Şekil 6.12. Windows kaynak izleyicisinde birçok özellik izlenebilir

Olay Görüntüleyicisi: Olay Görüntüleyicisi, yöneticilerin ve kullanıcıların yerel veya uzak bir makinede olay günlüklerini (Log) görüntülenmesine olanak tanıyan Microsoft işletim sisteminin bir bileşenidir.



Şekil 6.13. Windows olay görüntüleyicisi

Olay görüntüleyicisi Windows Günlükleri (Log) aşağıdaki kategorilere ayrılmıştır;

- Uygulama
- Güvenlik
- Kur
- Sistem
- İletilen Olaylar

Yukarıdaki şekilden de görüleceği gibi olaylar **Hata, Uyarı ve Bilgi** olarak 3 farklı seviyede çalışır.

Hata; önemli bir sorundur, örneğin çalışan bir uygulamanın zorla sonlandırılması, veri kaybı vb.

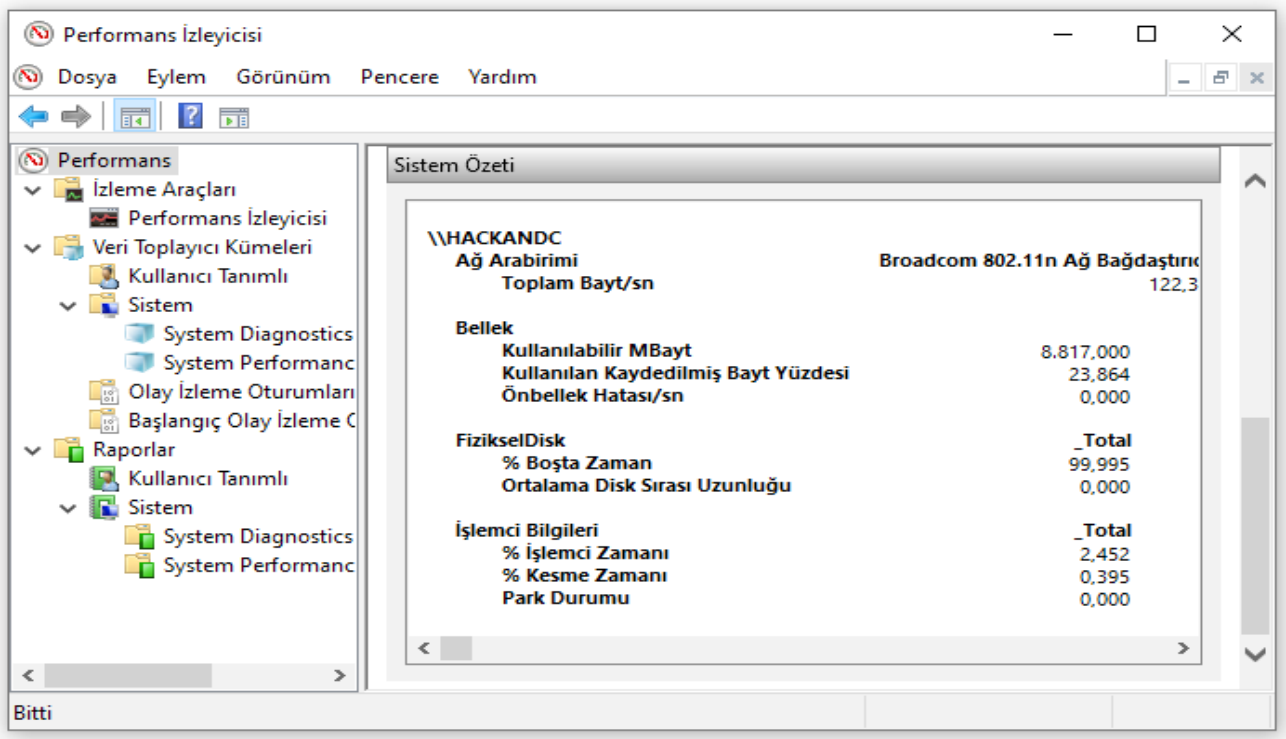
Uyarı; çok önemli olmayan ancak ileride sorun oluşmasına neden olabilecek bir olaydır,

Bilgi; ise bir programın, sürücünün veya hizmetin başarılı bir şekilde çalıştığını belirtir.

İşletim sistemi güvenliği için önemli bir araçtır. Sistemin günlüklerini sağ taraftaki Eylemler sekmesinden filtreleyerek de izlemeyi sağlar.

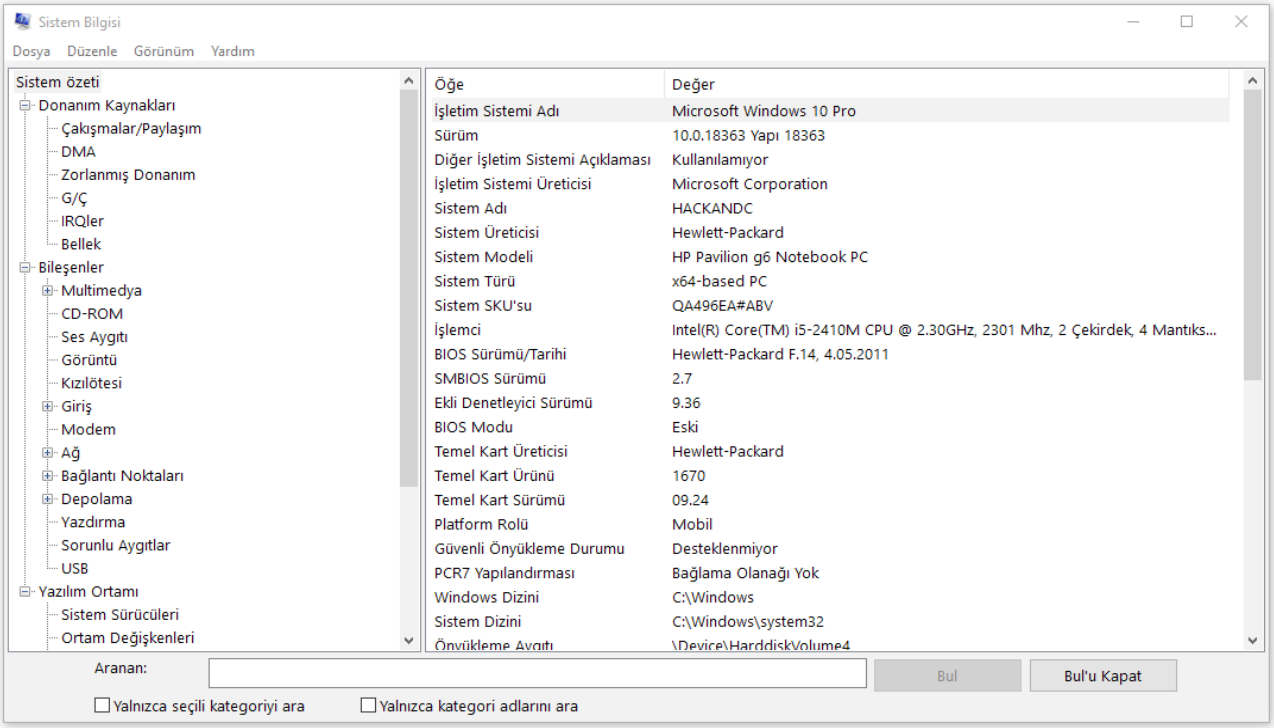
Performans İzleyicisi : Performans izleyicisini, performans verilerini gerçek zamanlı olarak veya bir günlük dosyasından görmek için kullanılır.

İzleme Araçları ile detaylı bir performans monitörü kişiselleştirebilir ve izleyebilir, sonuçları çözümlemek ve raporları görmek üzere performansın sayacını, olay izlemeyi, yapılandırma veri koleksiyonunu yapılandırmak ve zamanlamak için Veri Toplayıcı Kümeleri oluşturabilir.



Şekil 6.14. Windows performans izleyicisi

Sistem Bilgisi: Bilgisayarın hakkında çok detaylı bilgi gösterir. Bu bilgiler arasında, Sistem Üreticisi, İşletim Sistemi, Sistem Adı gibi birçok faydalı bilgileri göstermektedir.

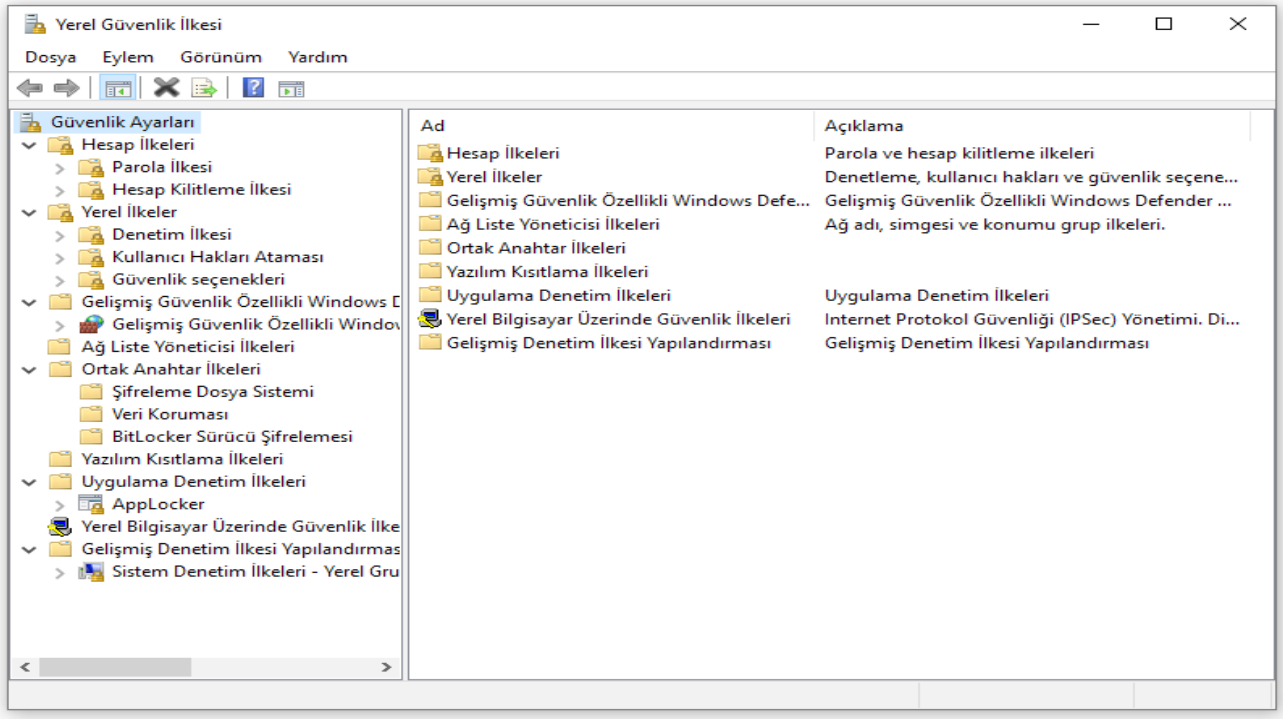


Şekil 6.15. Windows sistem bilgisi

Yerel Güvenlik İlkesi : Yerel Güvenlik ilkesi, bir kuruluştaki bir ağın, verilerin ve bilgisayar sistemlerinin güvenliğini sağlayan bir dizi yapılandırma içerir. Windows bilgisayarları kullanan çoğu ağda, Active Directory bir Windows Sunucusundaki Etki Alanları ile yapılandırılır. Windows bilgisayarlar etki alanına katılır. Windows Yerel Güvenlik İlkesi, bir Active Directory etki alanının parçası olmayan bağımsız bilgisayarlar için kullanılır. Parola yönergeleri, bir güvenlik politikasının önemli bir bileşenidir. Yerel Güvenlik Politikasında, Parola İlkesi Hesap İlkeleri altında bulunur ve yerel bilgisayardaki tüm kullanıcılar için parola kriterlerini tanımlar. Kaba kuvvet (Brute force) oturum açma girişimlerini önlemek için Hesap Politikalarındaki Hesap Kilitleme Politikası kullanılır. Kullanıcılar uzaktayken bilgisayarların güvende olmasını sağlamak önemlidir. Bir güvenlik politikası, ekran koruyucu başladığında bilgisayarın kilitlenmesini zorunlu kılan bir kural içermelidir.

Her bağımsız bilgisayardaki Yerel Güvenlik İlkesi aynıysa, Dışa Aktarma İlkesi özelliğini kullanarak diğer bilgisayarlara da bu ilke uygulanabilir. Bu, özellikle yöneticinin kullanıcı hakları ve güvenlik seçenekleri için kapsamlı yerel ilkeler yapılandırması gerektiğinde faydalıdır. Yerel Güvenlik İlkesi uygulaması, özellikle yerel bilgisayara uygulanan güvenlik ayarlarını içerir. Kullanıcı, Kullanıcı Haklarını, Güvenlik Duvarı Kurallarını ve kullanıcıların veya grupların AppLocker ile çalışmasına izin verilen dosyaları kısıtlama yeteneğini yapılandırabilir. Yerel Güvenlik İlkesi ile aşağıdaki ilkeler ve özellikleri kısıtlayabilir veya yapılandırılır;

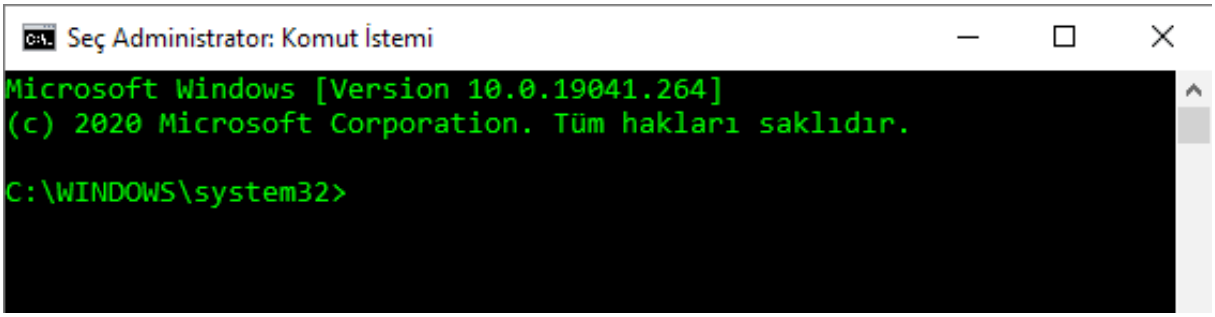
- Hesap ilkeleri
- Yerel İlkeler
- Windows Güvenlik Duvarı
- Ağ listesi Yöneticisi ilkeleri
- Ortak Anahtar İlkeleri
- Yazılım Kısıtlama İlkeleri
- Uygulama denetim ilkeleri
- Yerel bilgisayarda IP güvenlik ilkeleri
- Gelişmiş denetim ilkesi yapılandırması



Şekil 6.16. Windows güvenlik ilkesi

Komut Satırı (CMD) Nedir?

Cmd, komut satırı olarak bilinen ve Windows işletim Sistemlerinde bulunan Ms-Dos tabanlı bir komut yazma konsol ekranıdır [53]. CMD ekranına girmek için ise iki yolu vardır. Bunlardan ilki Windows arama çubuğuna çalıştır yazdıktan sonra CMD yazılır. İkinci yol ise klavyedeki Windows ve R tuşlarına aynı anda basıp (Windows+R) çıkan ekrana CMD yazılır. Bazı komutların yazılması, yönetimsel ayrıcalık gerektirebilir. Bu durumda "Yönetici Olarak Çalıştır" ile programı başlatmak gerekmektedir.

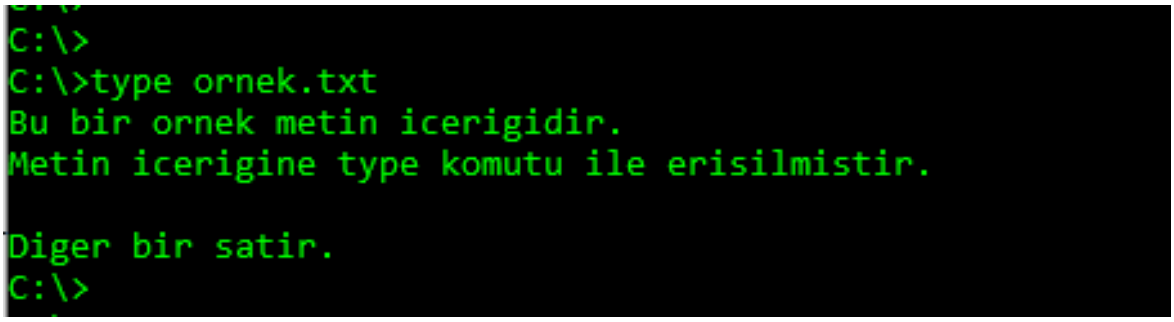


Şekil 6.17. Windows komut satırı ekranı

Bu konsol ekranı ile yapılabilecekler sınırlı olsa da, bir kullanıcının ihtiyaç duyduğu temel görevler için yeterince gelişmiştir. CMD konsolunda temel işlemlerin (dosya açma, kopyalama silme vb) yanı sıra uygulanabilecek bazı ileri düzey komutlar şunlardır;

Type Komutu

type komutu ile dosyaların içi görüntülenir. Kullanımı: **type "dosyaismi"** şeklindedir.



Şekil 6.18. type komutu kullanımı

Pipe (|) operatörü

Pipe operatörü ile bir komutun çıktısı diğer komutun girdisi yapılabilir. Böylelikle aynı anda iki veya daha fazla işlem birleştirilebilir.

Komut	Açıklaması
type agaclar.txt | more	Bu komut ile agaclar.txt dosyasının içindekiler more komutu sayesinde sayfa sayfa gösterilecektir. Pipe operatörü ve more komutu kullanılmasaydı tek seferde ekrana tüm dosya içeriğini yazacaktı.

Büyüktür Operatörü (>)

Bu operatörün solundaki bilgiler ile sağındaki ad ile bir dosya oluşturulur ve tüm bilgiler içine kaydedilir.

```
C:\>
C:\>tree Test > agacOrnek.txt

C:\>type agacOrnek.txt
Folder PATH listing
Volume serial number is A4F7-43E8
C:\TEST
├───AltKlasor1
└───AltKlasor2
    └───IcKlasor

C:\>_
```

Şekil 6.19. > operatörü kullanımı

Komut	Açıklaması
tree /F > "agaclar.txt"	tree /F komutu ile bir sürücünün her klasördeki dosya adlarını grafiksel olarak görüntüler ve sonrasında agaclar.txt dosyasını oluşturup içinde ne olduğuna bakmadan tüm çıktıyı buraya yazar.

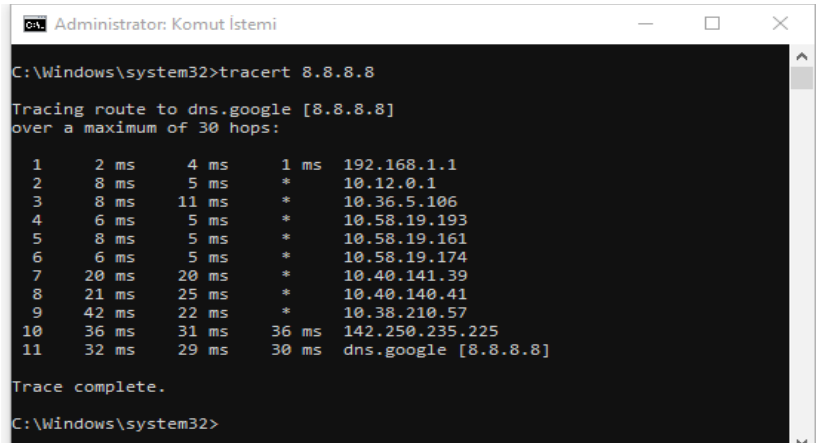
Çift Büyüktür Operatörü (>>)

Bu operatör > operatörünün bir başka halidir. >> operatöründe dosya yoksa baştan oluşturulur ve bilgiler yazılır, varsa da dosyanın sonuna eklenir içindekiler silinmez.

Komut	Açıklaması
tree /F >> "agaclar.txt"	tree /F komutu ile bir sürücünün her klasördeki dosya adlarını grafiksel olarak görüntüler ve sonrasında agaclar.txt dosyası yoksa oluşturulup içine yazılır varsa da sonuna eklenir.

Tracert Komutu

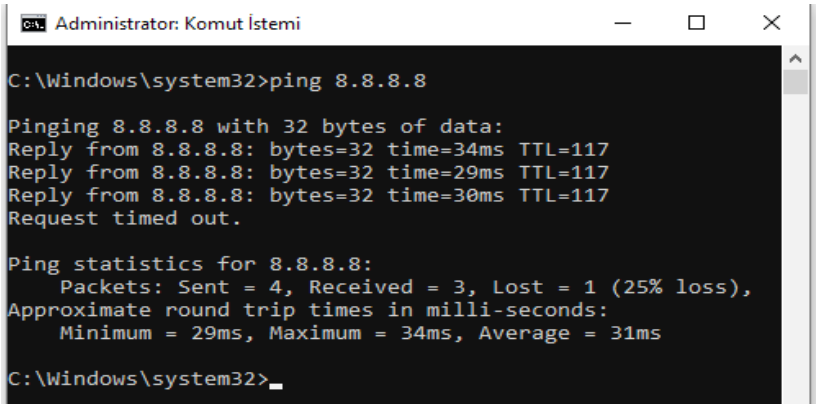
Tracert komutu, bir paketin bir hedefe gitmesi için kullandığı yolu izler ve kullanıcılara bu yol hakkında bir rapor görüntüler.



*Şekil 6.20.*trecert komutu kullanımı

Ping komutu

Ping komutu ile karşıdaki bilgisayara 32 baytlık bir ICMP (Internet Control Message Protocol-İnternet Kontrol Mesaj Protokolü) paketleri gönderir ve aynı paketin geri gelmesini bekler. Bu basit kod ile karşıdaki bilgisayar veya sunucunun gerçekten var olup olmadığını ve ne kadar uzakta olduğunu öğrenebileceğimiz çok kullanışlı bir komuttur.



*Şekil 6.21.*ping komutu kullanımı

PathPing Komutu

Ping ve Tracert komutlarının özelliklerinin, bu iki araçta bulunmayan ek özellikler ile birleştiren bir yol izleme komutudur.

```
Administrator: Komut İstemi

C:\Windows\system32>pathping 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:
  0  HackanDC.home [192.168.1.26]
  1  192.168.1.1
  2  10.12.0.1
  3  10.36.5.106
  4  10.58.19.193
  5  10.58.19.161
  6  10.58.19.174
  7  10.40.141.39
  8  10.40.140.41
  9  10.38.210.57
 10  142.250.235.225
 11  dns.google [8.8.8.8]

Computing statistics for 275 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           HackanDC.home [192.168.1.26]
                                     0/ 100 =  0%   |
  1   42ms     0/ 100 =  0%          0/ 100 =  0%  192.168.1.1
                                     0/ 100 =  0%   |
  2   46ms     0/ 100 =  0%          0/ 100 =  0%  10.12.0.1
                                     0/ 100 =  0%   |
  3   46ms     0/ 100 =  0%          0/ 100 =  0%  10.36.5.106
                                     0/ 100 =  0%   |
  4   48ms     0/ 100 =  0%          0/ 100 =  0%  10.58.19.193
                                     0/ 100 =  0%   |
  5   52ms     0/ 100 =  0%          0/ 100 =  0%  10.58.19.161
                                     0/ 100 =  0%   |
  6   44ms     0/ 100 =  0%          0/ 100 =  0%  10.58.19.174
                                     0/ 100 =  0%   |
  7  ---     100/ 100 =100%        100/ 100 =100%  10.40.141.39
                                     0/ 100 =  0%   |
  8  ---     100/ 100 =100%        100/ 100 =100%  10.40.140.41
                                     0/ 100 =  0%   |
  9  ---     100/ 100 =100%        100/ 100 =100%  10.38.210.57
                                     0/ 100 =  0%   |
 10   75ms     1/ 100 =  1%          1/ 100 =  1%  142.250.235.225
                                     0/ 100 =  0%   |
 11   68ms     0/ 100 =  0%          0/ 100 =  0%  dns.google [8.8.8.8]

Trace complete.

C:\Windows\system32>
```

Şekil 6.22. patping komutu kullanımı

TaskList Komutu

Bu komut ile çalışan işlemlerin (prosess) isimlerini, PID (Process IDentifier) değerlerini, Oturum (Session) adını, otururum numarasını ve kullandığı bellek miktarını gösterir.

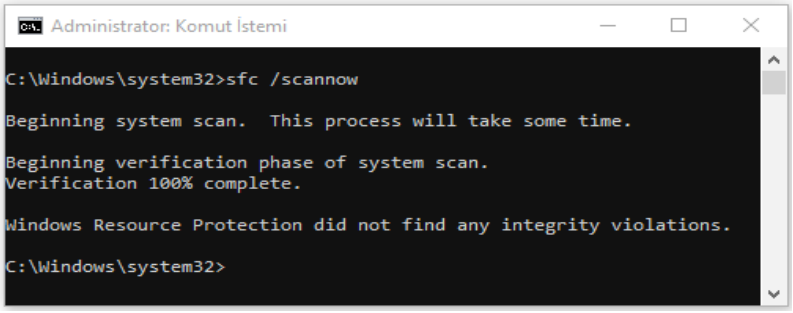
```
C:\>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      6.796 K
Registry                       100 Services                   0     37.324 K
smss.exe                       568 Services                   0        332 K
csrss.exe                      988 Services                   0      2.872 K
wininit.exe                    640 Services                   0      1.824 K
services.exe                   824 Services                   0      7.168 K
lsass.exe                      812 Services                   0     87.928 K
svchost.exe                   1124 Services                   0        896 K
WUDFHost.exe                  1144 Services                   0      2.792 K
svchost.exe                   1156 Services                   0     20.416 K
```

Şekil 6.23. tasklist komutu kullanımı

taskkill -pid "pid numarası" komutu ile sonlandırılmak istenilen işlemi numarası yazılarak ilgili işlem sonlandırılır. **taskkill -im "işlem adı"** yazarak da işlemin adını (Image Name) kullanarak işleme son verilebilir.

sfc Komutu

sfc /scannow komutu korunan tüm sistem dosyalarını tarar ve bozuk dosyaları %WinDir%\System32\dllcache dizinindeki bir sıkıştırılmış klasörde bulunan önbelleğe alınmış kopyası ile değiştirir. %WinDir% yer tutucu, Windows işletim sistemi klasörünü gösterir.



Şekil 6.24. sfc komutu kullanımı

Not: *Doğrulama %100 tamamlanana kadar bu Komut İstemi penceresi kapatılmamalıdır. Bu işlem tamamlandıktan sonra tarama sonuçları gösterilir.*

6.1.2 PowerShell

Powershell Microsort firması tarafından cmd.exe (Windows Komut Satırı) alternatifi ve daha güçlü olarak geliştirilen bir komut satırı yorumlayıcısıdır. 2016 yılında Core versiyonu ile açık kaynak ve çapraz (cross platform) platformu da desteklemektedir. PowerShell'de komutlar genellikle belirli bir işlemi uygulayan özel .NET sınıfları olan cmdlet'ler kullanılarak gerçekleştirilmektedir. Hem yerel hem de uzak sunuculardan erişilebilir ve yönetilirdir [52]. Arama satırına PowerShell yazılarak erişilir.

PowerShell'in bazı özellikleri şunlardır:

- Ağ soketlerine hızlı ve kolay erişim
- Win32 Uygulama Programlama Arayüzüne (API) direk erişim
- Windows Yönetim Araçları (WMI) iledaha kullanılabilir bir arayüz
- Güçlü komut dosyası işletimi ve yönetimi
- Kripto kiütüphanelerine kolay erişim,
- Bileşen Nesne Modeli'ne (COM) kolaylıkla bağlantı kurma

PowerShell Etkinliğini Günlüğe Kaydetme

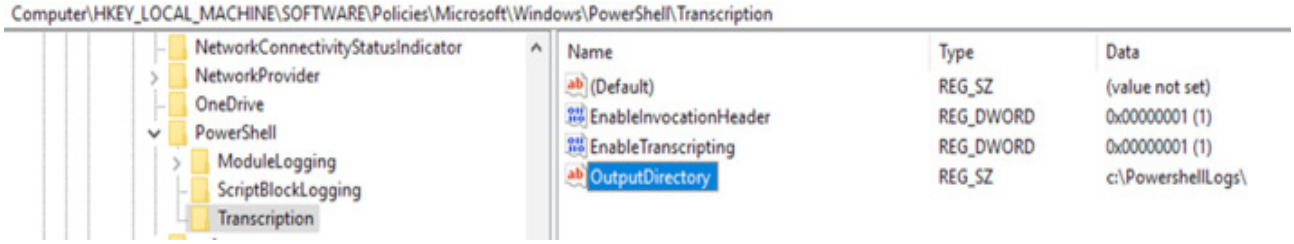
Oluşan şüpheli bir olayı saptamak için PowerShell etkinliğini günlüğe kaydetmek önemli bir güvenlik kontrolüdür. Bunlar, PowerShell için ana günlüğe kaydetme bileşenleridir:

a. Transkript Günlüğü

Transkript günlükleri, tam olarak oturumda göründüğü gibi tüm giriş ve çıkışlar dâhil olmak üzere her PowerShell oturumunun benzersiz bir kaydını oluşturur. Transkriptler, kullanıcı ve oturuma göre ayrılmış olarak metin dosyalarına yazılır ve analize yardımcı olmak için her komut için zaman damgaları (tarih, saat bilgisi) ve meta verileri de içerir. Ancak, transkript sadece PowerShell terminalinde görünenleri kaydeder ve bu, yürütülen komut dosyalarının içeriğini veya dosya sistemi gibi diğer hedeflere yazılan sonuçları içermez.

i. PowerShell Transkripsiyon Grup İlkesini Aç ayarını etkinleştirin

ii. HKEY_LOCAL_MACHINE \ Software \ Policies \ Microsoft \ Windows \ PowerShell \ Transcription



Şekil 6.25. Powershell günlüğünü regeditte açmak

b. Komut Dosyası Blog Günlüğü (Scriptblock Logging)

Komut dosyası bloğu günlüğü, PowerShell tarafından yürütülürken kod bloklarını kaydeder, böylece komut dosyaları ve komutlar dâhil olmak üzere bir saldırgan tarafından yürütülen kodun tüm içeriğini yakalar.

i. PowerShell Komut Dosyası Engelleme Günlüğünü Grup İlkesi ayarını kullanarak etkinleştirilir.

ii. HKEY_LOCAL_MACHINE \ Software \ Policies \ Microsoft \ Windows \ PowerShell \ ScriptBlockLogging

c. Korumalı Olay Günlüğü

Korumalı Olay Günlüğü, eklenen uygulamaların dikkat edilmesi gereken ve önemli verileri olay günlüğüne yazarken şifrelemesini sağlamaktadır.

i. Korumalı Olay Günlüğü Kaydetmeyi Etkinleştir Grup İlkesi ayarını etkinleştirilir.

d. Modül Günlüğü

Modül günlüğü, değişken başlatma ve komut çağrıları dâhil olmak üzere PowerShell yürütürken ardışık düzen yürütme ayrıntılarını kaydeder. Modül günlüğü, komut dosyalarının bölümlerini, bazı karmaşık olmayan kodları ve çıktı için biçimlendirilmiş bazı verileri kaydeder.

i. Modül Günlüğü PowerShell Grup İlkesi ayarını kullanarak etkinleştirilir.

Windows yöneticilerinin PowerShell üzerinde (Admin/Administrator) bilmesi gereken komutlar şunlardır:

Get-Help : Her yöneticinin öğrenmesi gereken ilk PowerShell komutu Get-Help'dir. Başka herhangi bir komutla ilgili yardım almak için bu komutu kullanılır. Örneğin, Get-Process komutunun nasıl çalıştığını bilmek istiyorsak, şunu yazılır:

```
Get-Help -Name Get-Process
```

Komutun ardından Windows tam komut sözdizimini gösterecektir.

Set-ExecutionPolicy : PowerShell betikleri oluşturup çalıştırabilmenize rağmen, Microsoft, kötü niyetli kodun bir PowerShell ortamında yürütülmesini önlemek için varsayılan olarak komut dosyalarını devre dışı bırakmıştır. PowerShell komut dosyalarını çevreleyen güvenlik düzeyini kontrol etmek için Set-ExecutionPolicy komutunu kullanabilirsiniz. Sizin için dört güvenlik seviyesi mevcuttur:

- **Kısıtlı (Redistricted) -** Kısıtlı, varsayılan yürütme ilkesidir ve PowerShell'i kilitler, böylece komutlar yalnızca etkileşimli olarak girilebilir. PowerShell betiklerinin çalışmasına izin verilmez.
- **Tümü İmzalandı (All Signed) -** Yürütme politikası Tümü İmzalandı olarak ayarlanırsa, komut dosyalarının çalışmasına izin verilir, ancak bu yalnızca güvenilir bir yayıncı tarafından imzalanmışsa çalışmasına izin verilir.
- **Uzaktan İmzalı (Remote Signed) -** Yürütme ilkesi Uzaktan İmzalı olarak ayarlanırsa, yerel olarak oluşturulan tüm PowerShell komut dosyalarının çalışmasına izin verilir. Uzaktan oluşturulan komut dosyalarının, yalnızca güvenilir bir yayıncı tarafından imzalanmış olmaları durumunda çalışmasına izin verilir.
- **Sınırsız (Unrestricted) -** Adından da anlaşılacağı gibi Sınırsız, yürütme politikasındaki tüm kısıtlamaları kaldırır.

Set-ExecutionPolicy komutunu ve ardından ilkenin adını girerek bir yürütme ilkesi belirleyebilirsiniz. Örneğin, komut dosyalarının sınırsız bir şekilde çalışmasına izin vermek isteniyorsa aşağıdaki komut yazılır;

```
Set-ExecutionPolicy Unrestricted
```

Get-ExecutionPolicy: Bilinmeyen bir sunucu üzerinde çalışılıyorsa, bir komut dosyasını çalıştırmadan önce hangi yürütme politikasının kullanımda olduğunu bilmek gerekir. Get-ExecutionPolicy komutu kullanılarak bu politikalar öğrenilir.

Get-Service: Get-Service komutu, sistemde yüklü olan tüm hizmetlerin bir listesini sağlar. Belirli bir hizmet için, -name anahtarı ve hizmetin adı eklenir. Windows hizmetin durumunu gösterecektir.

```
PS C:\Users> Get-Service -name power

Status   Name               DisplayName
------   ----               -----------
Running  power              Güç
```

Şekil 6.26. Get-Service komutunun örnek kullanımı

ConvertTo-HTML: PowerShell, sistem hakkında çok sayıda bilgi sağlayabilir, ancak bazen yalnızca ekrandaki bilgileri görüntülemekten daha fazlasını yapmanız gerekir. Bazen birine gönderebileceğiniz bir rapor oluşturmak faydalı olabilir. Bunu başarmanın bir yolu, ConvertTo-HTML komutunu kullanmaktır.

Bu komutu kullanmak için, çıktıyı başka bir komuttan ConvertTo-HTML komutuna aktarmanız yeterlidir. HTML dosyasına hangi çıktı özelliklerinin dâhil edileceğini kontrol etmek için -Property anahtarını kullanmanız ve bir dosya adı sağlamanız gerekir.

Bu komutun nasıl kullanılabileceğini görmek için, sistemde yüklü olan her hizmetin bir listesini oluşturmak için Get-Service yazdığımız önceki bölümü düşünün. Şimdi, her hizmetin adını durumuyla birlikte (hizmetin çalışıp çalışmadığına bakılmaksızın) listeleyen bir HTML raporu oluşturmak istediğinizi hayal edin. Bunu yapmak için aşağıdaki komutu kullanabilirsiniz:

```
Get-Service | ConvertTo-HTML -Property Name, Status > C:\services.htm
```

Export-CSV: PowerShell verilerine dayalı bir HTML raporu oluşturabildiğiniz gibi, verileri PowerShell'den Microsoft Excel kullanarak açabileceğiniz bir CSV dosyasına da aktarabilirsiniz. Sözdizimi, bir komutun çıktısını HTML'ye dönüştürmeye benzer. En azından bir çıktı dosya adı sağlamalısınız. Örneğin, sistem hizmetleri listesini bir CSV dosyasına vermek için aşağıdaki komutu kullanabilirsiniz:

```
Get-Service | Export-CSV c:\service.csv
```

Select-Object : Yukarıdaki komut uygulandığında CSV dosyasında çok sayıda özellik olduğu görülür. Yalnızca gerçekten ilgilendiğiniz özellikleri dâhil ederek işleri daraltmak genellikle yararlıdır. Select-Object komutu burada devreye girer. Select-Object komutu, dâhil edilecek belirli özellikleri belirlemenize olanak tanır. Örneğin, her bir sistem hizmetinin adını ve durumunu içeren bir CSV dosyası oluşturmak için aşağıdaki komut kullanılabilir:

```
Get-Service | Select-Object Name, Status | Export-CSV c:\service.csv
```

Get-EventLog: Bilgisayarınızın olay günlüklerini ayrıştırmak için aslında PowerShell kullanılabilir. Kullanılabilen birkaç parametre vardır, ancak yalnızca -Log anahtarını ve ardından günlük dosyasının adını sağlayarak komutu deneyebilirsiniz. Örneğin, Uygulama günlüğünü görmek için aşağıdaki komut kullanılır:

```
Get-EventLog -Log "Uygulama"
```

Tabii ki, bu komut gerçek dünyada nadiren kullanılır. Çıktıyı filtrelemek ve bir CSV veya HTML dosyasına dökmek için diğer komutları kullanma olasılığı daha yüksektir.

Get-Process: Tüm sistem hizmetlerinin bir listesini görüntülemek için Get-Service komutunu kullanabildiğiniz gibi, şu anda sistemde çalışan tüm işlemlerin bir listesini görüntülemek için Get-Process komutu da kullanılabilir.

Stop-Process İşlemi: Bazen bir süreç donar. Bu olduğunda, yanıt vermeyi durduran işlemin adını veya işlem kimliğini almak için Get-Process komutu kullanılır. Daha sonra İşlemi Durdur komutunu kullanarak işlem sonlandırılır. Bir işlemi adına veya işlem kimliğine göre sonlarmak mümkündür. Örneğin, aşağıdaki komutlardan birini kullanarak Not Defteri'ni sonlandırılabilir:

```
Stop-Process -Name notepad<br> Stop-Process -ID 2668
```

İşlem kimliğinin oturumdan oturuma değişebileceğini unutmamak gerekir.

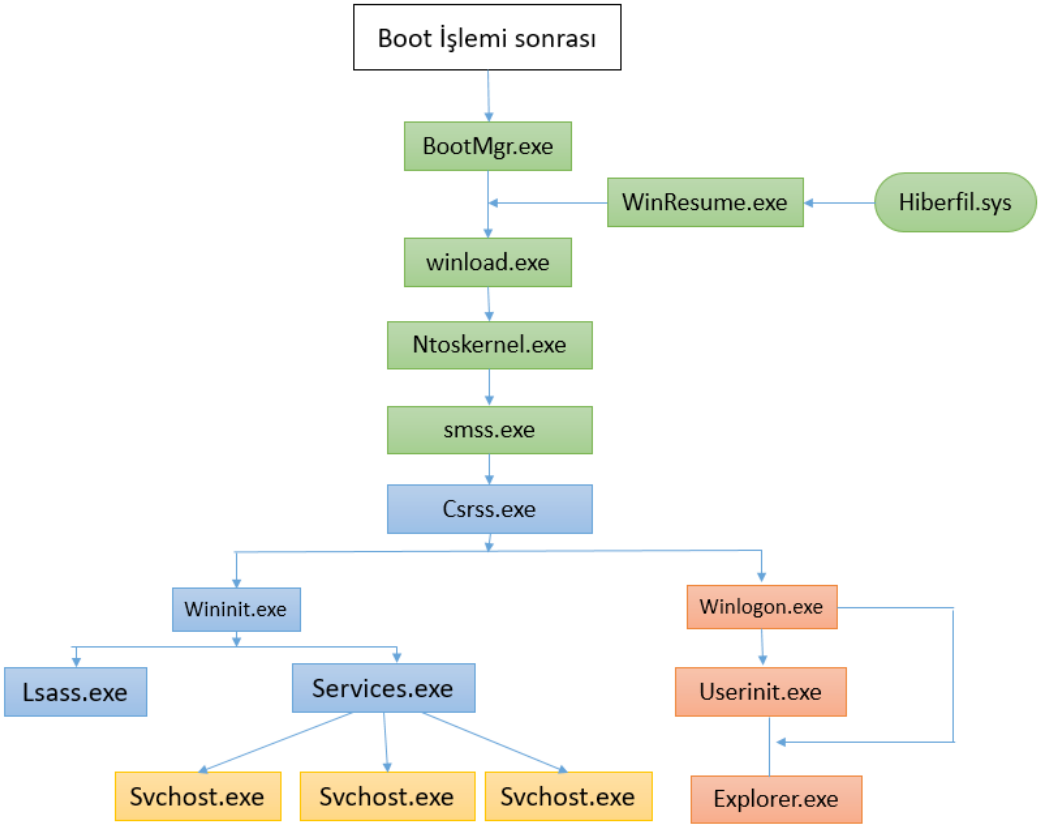
6.1.3 Windows İşletim Sisteminde Zararlı Yazılım Analizi

Bu bölümdeki konular, kısa ipuçları şeklinde yer almaktadır. Ekran görüntüleri ve kullanılan araçlar Windows 10 işletim sistemi temel alınarak hazırlanmıştır. Windows zararlı yazılım analizinde Microsoft tarafından sunulan ***SysInternalsSuite*** araçları kullanılacaktır. Bu araç takımına aşağıdaki bağlantıdan ulaşılabilir:

https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

SysInternalsSuite araç takımı, Microsoft işletim sistemini izlemek, yönetmek ve sorunları gidermek için kullanılan birçok aracı barındıran yararlı bir yardımcı yazılım setidir. Araçlardaki yazılımlar kurulum gerektirmeyen dosyalardır.

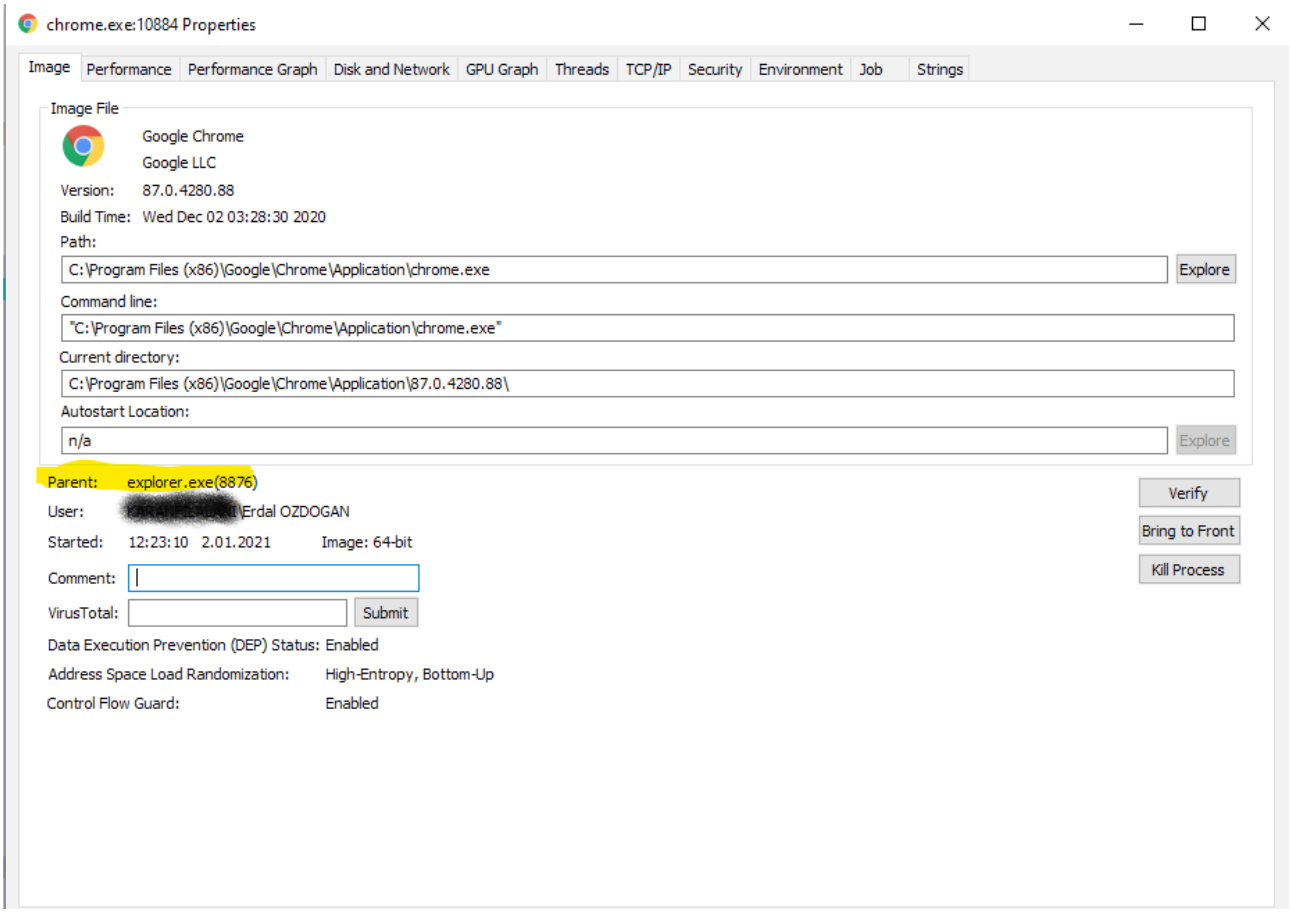
Windows İşletim Sisteminde zararlı yazılım analizinin yapılabilmesi, bu işletim sistemindeki işlemler **(process)** hakkında derinlemesine bilgi sahibi olmayı gerektirir. Sistemde çalışan yasal işlemlerin, bu işlemlerin davranışlarının ve süreçlerinin bilinmesi, yasal olmayan (ya da zararlı) yazılımların tespitini kolaylaştırır.



Şekil 6.27. Windows açılış süreci şeması

Şekilden de görüleceği üzere, önemli işlemlerden biri, işletim sisteminin kabuğunu (Shell) temsil eden Explorer.exe işlemidir. **Explorer.exe**, Userinit.exe tarafından başlatılan ancak herhangi

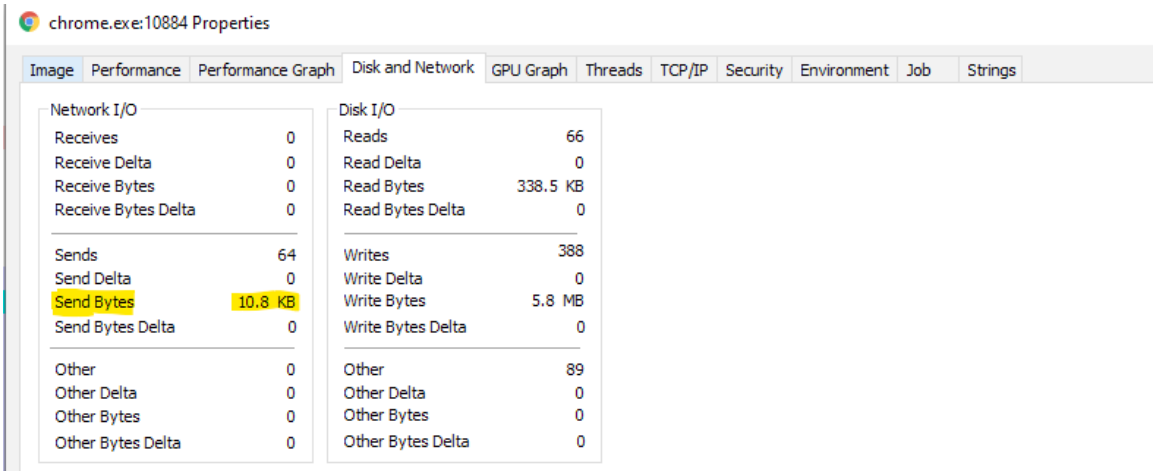
parent işlemi olmayan bir işlemdir. Bu işleminin ardından userinit.exe sona erer. Bunun anlamı, Explorer.exe'nin parent bir işlemi yoktur. Ancak, Explorer.exe tarafından başlatılan bir sürecin parent bir işlemi ve dolayısıyla PPID değeri (Parent Process ID) vardır. Şekil 6.28'deki ekran görüntüsünde, *chrome.exe* çalıştırılmış ve **SysInternalsSuit** araç takımı içinde yer alan **Process Explorer** aracı ile bir örnek gösterilmiştir.



Şekil 6.28. Windows Process Explorer aracı ile işlem kontrolü

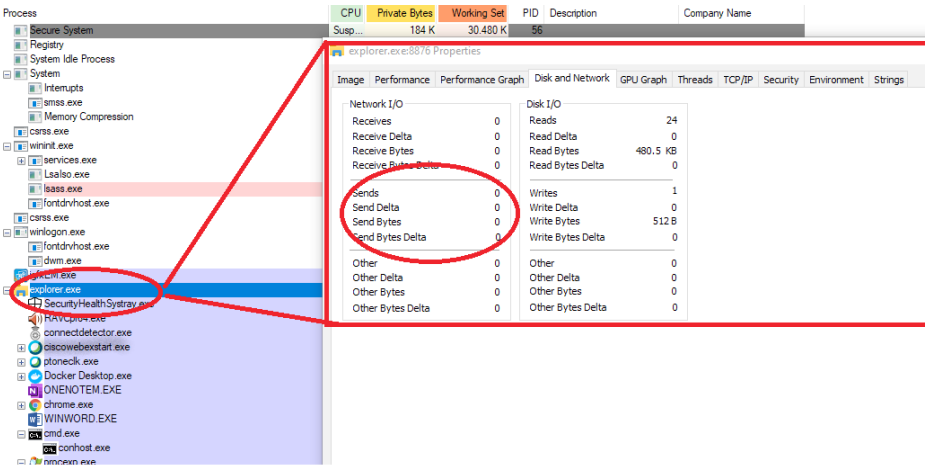
Zararlı yazılımların önemli karakteristiklerinden biri, ağ trafiği oluşturmaktır (bir konuma veri gönderme gibi). Burada dikkat edilmesi gereken bir konu, Explorer.exe'nin kesinlikle ağ trafiği

oluşturmadığıdır. Ancak Explorer.exe'nin alt işlemleri (Explorer.exe tarafından başlatılan işlemler) ağ trafiği oluşturabilir. Şekil 6.29'daki ekran görüntüsünde, chrome.exe için bu örnek gösterilmiştir.



Şekil 6.29. Process Explorer aracı ile chrome.exe işleminin özellikleri

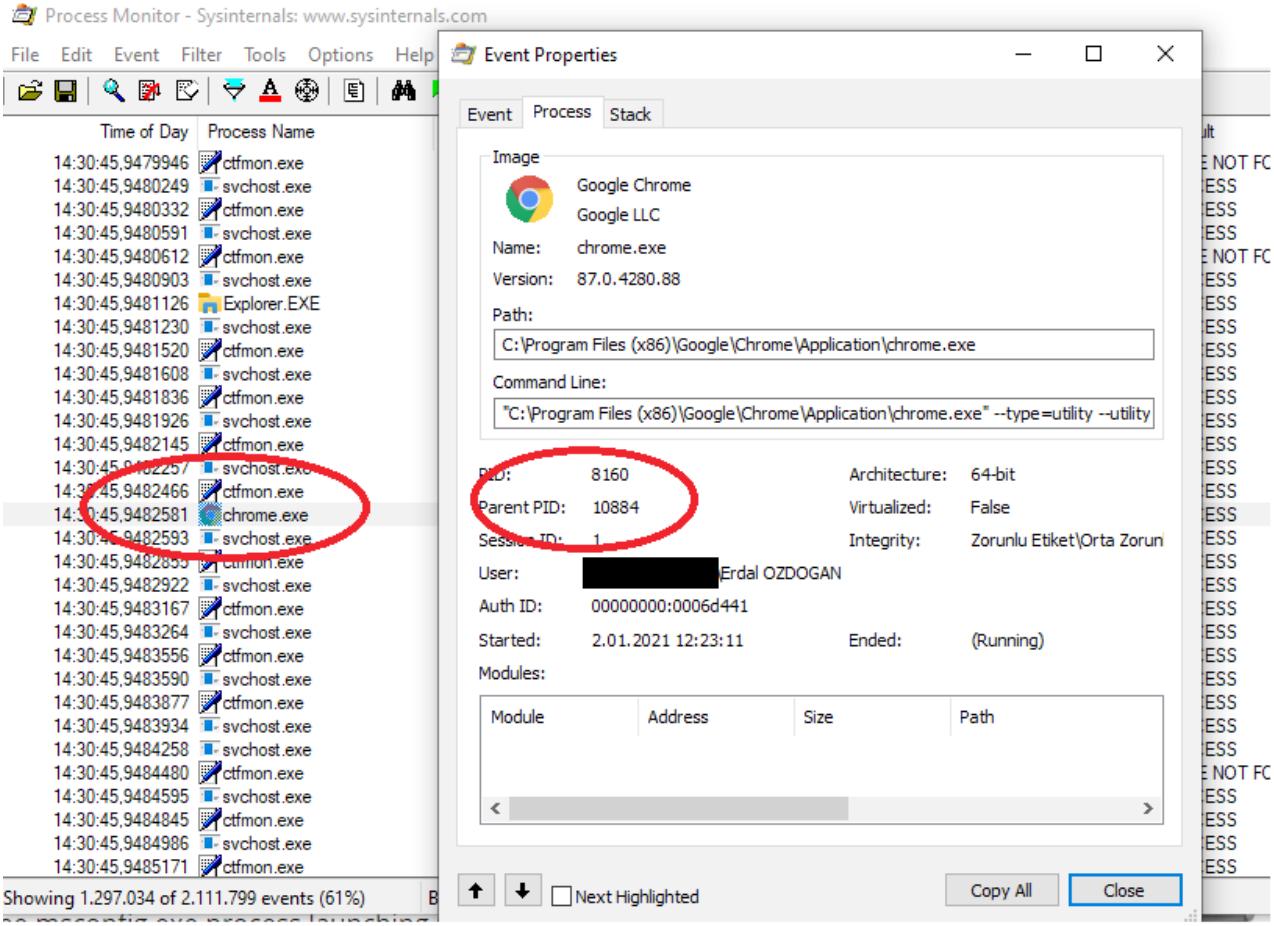
Şekil 6.20'da yer alan ekran görüntüsünde gösterildiği gibi Explorer.exe işleminin ağda veri göndermemesi gerekmektedir.



Şekil 6.30. Process Explorer aracı ile chrome.exe işlemin kontrolü

Explorer.exe için gönderilen byte (send byte) kısmının sıfırdan farklı bir değerde olması, bu işlemin değiştirilmiş olduğunu ve zararlı yazılımın olduğunu göstermektedir.

Parent işlemini görmenin diğer bir yolu da, Şekil 6.31'deki ekran görüntüsünde yer alan ***Process Monitor*** aracını kullanmaktır.



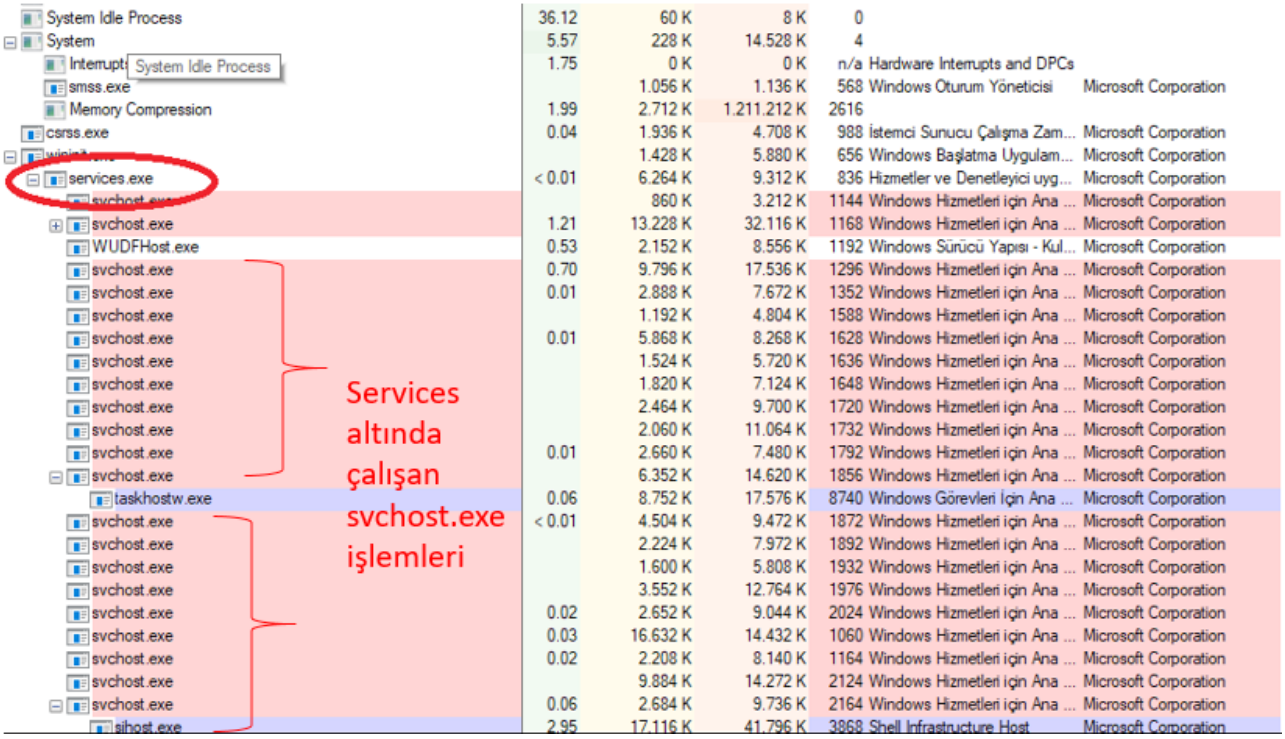
Şekil 6.31. Process Monitör aracı ile chrome.exe işlem kontrolü

Bu ekranda, yine chrome.exe için Parent PID değeri gösterilmektedir. Bu araç, bilinmeyen bir işlemin çok kısa bir süre (1 – 2 saniye) çalışıp durduğu durumlarda, işlemin yakalanması ve analizi için oldukça yararlıdır. Önceki araçta ***(Process Explorer)*** görüntülenemeyen işlemler, Process

Monitor'de her şey yakalama süresi boyunca zaten kaydedildiğinden, işlemin halen çalışıyor veya sonlandırılmış olması önemli değildir.

Windows işletim sistemlerinde çalışan önemli işlemlerden biri de **svchost.exe** işlemidir. Bu işlem, DLL içindeki hizmetleri başlatmak için kullanılır ve saldırganların (zararlı yazılımların) sıklıkla kullandığı (ya da taklit ettiği) bir işlemdir.

Windows işletim sistemi başlatıldığında, birçok svchost hizmeti çalışır. Ancak bunların tamamı, **services.exe** hizmeti tarafından yürütülmüştür. Process Explorer aracına bu durum Şekil 6.32'deki ekran görüntüsünde yer almaktadır.



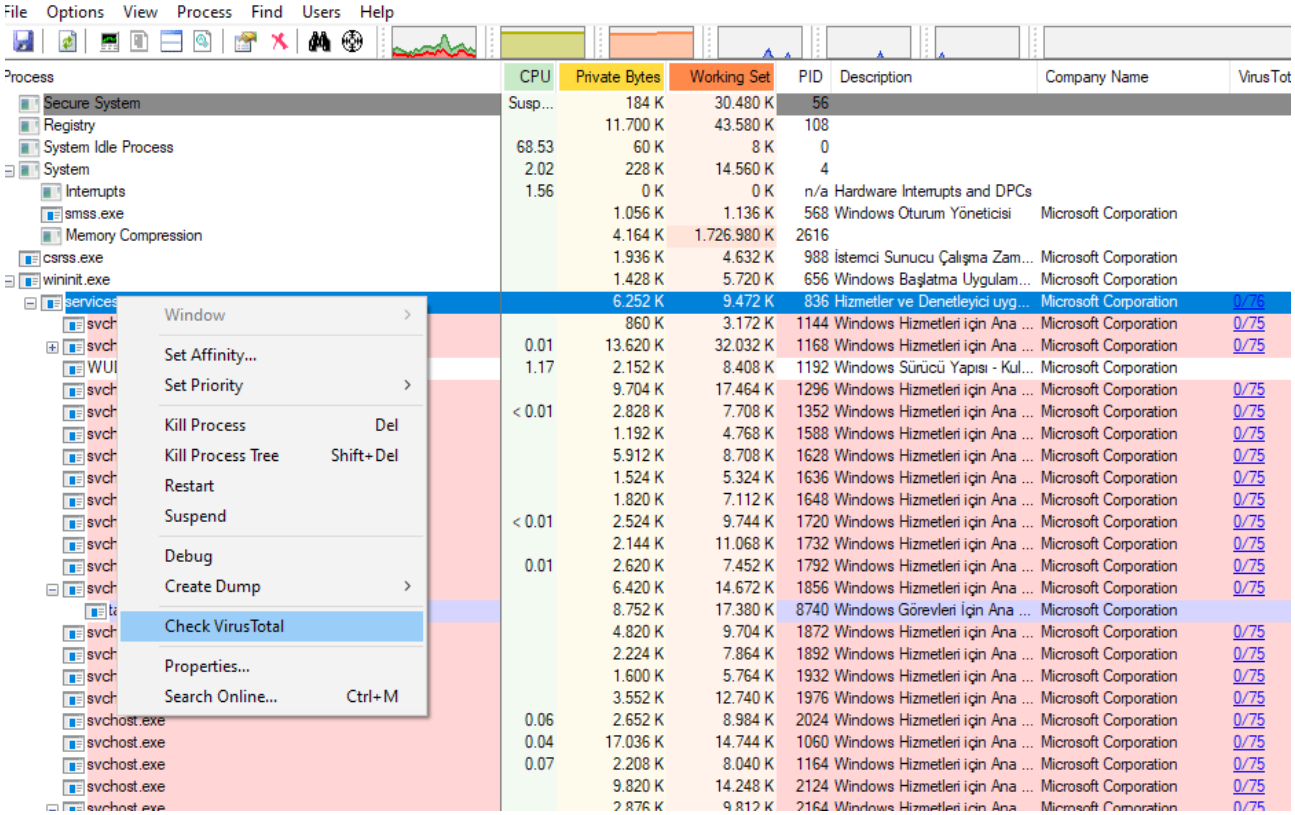
System Idle Process	36.12	60 K	8 K	0		
System	5.57	228 K	14.528 K	4		
Interrupts	1.75	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1.056 K	1.136 K	568	Windows Oturum Yöneticisi	Microsoft Corporation
Memory Compression	1.99	2.712 K	1.211.212 K	2616		
csrss.exe	0.04	1.936 K	4.708 K	988	İstemci Sunucu Çalışma Zam...	Microsoft Corporation
wininit.exe		1.428 K	5.880 K	656	Windows Başlatma Uygulam...	Microsoft Corporation
services.exe	< 0.01	6.264 K	9.312 K	836	Hizmetler ve Denetleyici uyg...	Microsoft Corporation
svchost.exe		860 K	3.212 K	1144	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	1.21	13.228 K	32.116 K	1168	Windows Hizmetleri için Ana ...	Microsoft Corporation
WUDFHost.exe	0.53	2.152 K	8.556 K	1192	Windows Sürücü Yapısı - Kul...	Microsoft Corporation
svchost.exe	0.70	9.796 K	17.536 K	1296	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	0.01	2.888 K	7.672 K	1352	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		1.192 K	4.804 K	1588	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	0.01	5.868 K	8.268 K	1628	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		1.524 K	5.720 K	1636	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		1.820 K	7.124 K	1648	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		2.464 K	9.700 K	1720	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		2.060 K	11.064 K	1732	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	0.01	2.660 K	7.480 K	1792	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		6.352 K	14.620 K	1856	Windows Hizmetleri için Ana ...	Microsoft Corporation
taskhostw.exe	0.06	8.752 K	17.576 K	8740	Windows Görevleri Için Ana ...	Microsoft Corporation
svchost.exe	< 0.01	4.504 K	9.472 K	1872	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		2.224 K	7.972 K	1892	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		1.600 K	5.808 K	1932	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		3.552 K	12.764 K	1976	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	0.02	2.652 K	9.044 K	2024	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	0.03	16.632 K	14.432 K	1060	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	0.02	2.208 K	8.140 K	1164	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe		9.884 K	14.272 K	2124	Windows Hizmetleri için Ana ...	Microsoft Corporation
svchost.exe	0.06	2.684 K	9.736 K	2164	Windows Hizmetleri için Ana ...	Microsoft Corporation
sihost.exe	2.95	17.116 K	41.796 K	3868	Shell Infrastructure Host	Microsoft Corporation

Şekil 6.32. Services altında çalışan svchost işlemleri

Services.exe işlemi altında yer almayan her svchost işlemi, bir zararlı yazılımın göstergesidir.

Zararlı yazılım analizlerinden biri de, çalışan bir işlemi virustotal.com aracılığıyla kontrol etmektir. VirusTotal.com, elliden fazla farklı antivirüs ürününe sahip çok motorlu bir tarayıcı

hizmetidir. Virustotal, web sayfası üzerinden çalışabildiği gibi Process Explorer'a entegre olarak da çalışmaktadır. Bu entegrasyon sayesinde dosyaların hash değerleri gönderilir. Şekil 6.33'de yer alan ekran görüntüsünde, Process Explorer aracı ile bu işlemin nasıl yapılacağı gösterilmektedir.



Şekil 6.33. Process Explorer ile bir işlemin zararlı olup olmadığı virustotal ile sorgulanabilir

Şekil 6.33'deki ekranda, 0/75 VirusTotal sonucu, 75 antivirüs motorunun dosyayı kontrol ettiği ve hiçbirinin bir virüs imzası tespit etmediği anlamına gelir. Ayrıntılı raporu bir web tarayıcısında açmak için bağlantıya tıklanır. Bu raporda taramanın ne zaman yapıldığı, hangi antivirüs ürününün neyi tespit ettiği ve ne tür olası zararlı yazılım olduğu gibi bilgiler yer almaktadır. Zararlı yazılımın tespit edilmesi durumunda sağda görünen değer sıfırdan farklı olacaktır.

6.2 LİNUX İŞLETİM SİSTEMİ VE GÜVENLİĞİ

Linux, 1991 yılında Finlandiyalı bir üniversite öğrencisi olan Linus Torvalds tarafından, daha eski işletim sistemlerinden birisi olan UNIX'in mimarisine ve POSIX standartlarıyla uygun şekilde sıfırdan yazılmaya başlanmıştır. Geliştirilmesinde Unix mimarisinden esinlenilmiş olmakla birlikte Linux içinde Unix'ten alınmış herhangi bir kod bulunmamaktadır [41].

Linux açık kaynak kodlu, hızlı, güvenilir ve küçüktür. Çalıştırmak için çok az donanım kaynağı gerektirir ve oldukça özelleştirilebilir bır işletim sistemidir. Linux, ağa bağlanmak üzere tasarlanmıştır, bu da ağ tabanlı uygulamaları yazmayı ve kullanmayı çok daha basit hale getirir.

Linux gelişen yapısı ile aşağıdaki platformlarda kullanılmaktadır;

- İnternet sunucuları (Linux, Apache, MySQL, PHP),
- Ev ve ofis (Ubuntu, Debian, Fedora, openSUSE, Linux Mint, Mageia),
- Süper bilgisayarlar (IBM Sequoia),
- Bulut bilişim (OpenStack projesi),
- Mini bilgisayarlar (Raspberry Pi),
- Mobil cihazlar (Android, Tizen, WebOs),
- Gömülü cihazlar (Akıllı TV ler, Yönlendiriciler),
- Nesnelerin interneti (Akıllı Buzdolabı, Çevrim içi kilitler),.
- Oyun ve eğlence,
- Otomotiv (Büyük otomotiv üreticilerinin dijital sistemlerinde)

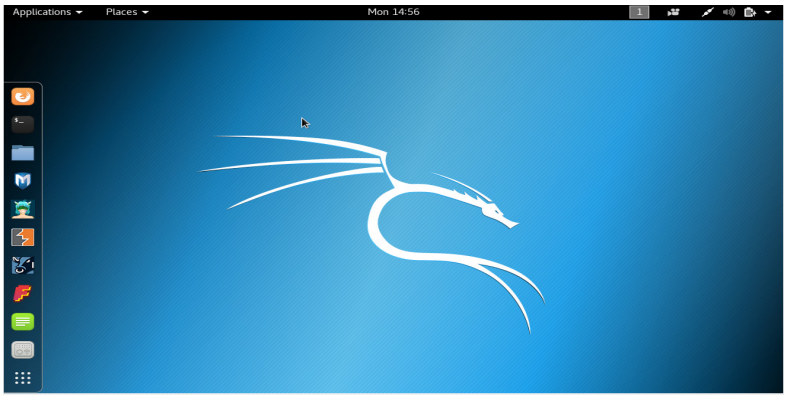
Linux de her sey bir dosyadır, tüm yapılandırmalar, sabit diskiniz, raminiz, hepsine tek bir komut ile ulaşabilmek mümkündür.

Linux Dağıtımları

GNU/Linux dağıtımı (kısaca **dağıtım**); Linux dağıtımı, farklı kuruluşlar tarafından oluşturulan paketleri tanımlamak için kullanılan terimdir ve Linux çekirdeğini özelleştirilmiş araçlar ve yazılım paketleri ile birlikte içerir. GNU/Linux dünyasına katkıları ile öne çıkan bazı dağıtımlar vardır: Debian, Ubuntu, Red Hat, Fedora, Linux Mint, openSUSE bunlardan birkaçıdır [42]. Kali Linux, bağlantı noktası tarayıcıları, paket analiz programları, şifre kırıcıları, metinsel ve grafiksel siber

saldırı yönetim araçları, gibi 300'ün üzerinde ağ testi programı ile donatılmış, çeşitli araçlardan, web uygulama güvenlik tarayıcıları ve kablosuz ağ testi tespit programlardan oluşan ve Penetrasyon testi için özelleştirilmiş bir işletim sistemidir [47].

Linux'ün öne çıkan özellikleri;



Linux, genellikle Güvenlik Operasyon Merkezi'nde tercih edilen işletim sistemidir. Linux'u tercih etmeniz için bazı nedenler şunlardır:

Linux açık kaynaklıdır - Herhangi bir kişi Linux'u ücretsiz olarak edinebilir ve belirli ihtiyaçlara uyacak şekilde değiştirebilir.

Linux CLI çok güçlüdür - Linux Komut Satırı Arabirimi (CLI) son derece güçlüdür ve analistlerin görevleri yalnızca doğrudan bir terminalde değil, aynı zamanda uzaktan gerçekleştirmelerini sağlar.

Kullanıcı işletim sistemi üzerinde daha fazla kontrole sahiptir - Root kullanıcı veya süper kullanıcı olarak bilinen Linux'taki yönetici kullanıcı, bilgisayarın herhangi bir özelliğini birkaç tuşa basarak değiştirebilir.

Daha iyi ağ iletişim kontrolüne izin verir - Kontrol Linux'un doğal bir parçasıdır.

Bir işletim sistemi ne isimle ve ne özellikle olursa olsun mutlaka bakım isteyen bir yazılımdır. Yapılacak küçük hatalar veya oluşan bir hatanını göz ardı edilmesi, değerli olan zamanını boşa gitmesine ve daha büyük problemler ile karşı karşıya kalmamıza neden olur. Linux gibi açık kaynak kodlu bir işletim sisteminde ise kapalı kaynak kodlu işletim sistemlerine nazaran sistem yöneticisinin en ufak hatası geri dönülemez sorunlara neden olabilir.

6.2.1 Linux İşletim Sisteminde Güvenlik

Bilgisayar yazılımları geliştirilirken genellikle çok kapsamlı olarak geliştirme yapıldı. Ama bunlardan kullanım kolaylığı ve güvenlik daha ön plana çıkmıştır. Kullanıcılar ve üreticiler ise seçimlerini kullanım kolaylığı tarafından kullandığından, güvenlik arka planda kalmıştır. Ama

artık kullanım kolaylığı kadar güvenliğin de vazgeçilmez olduğunu sistemlerimizin çöktüğünde ya da işlevlerini yerine getirmediğinde çok daha iyi anlıyoruz. Bu bölümde Linux İşletim Sistemi yöneticilerine güvenlik ile ilgili yapabilecekleri konusunda bilgiler verilecektir.

Kali Linux Güvenlik Araçları	Açıklama
Ağ paketi yakalama yazılımları	• Bir ağ işleminin her ayrıntısını gözlemlemeyi ve anlamayı mümkün kıldığı için bir Linux Sistem yöneticileri için çok önemli bir araçtır. • Wireshark, popüler bir paket yakalama aracıdır.
Kötü amaçlı yazılım analiz araçları	• Bu araçlar, analistlerin, altta yatan sistemi tehlikeye atma riski olmadan, kötü amaçlı yazılım yürütmesini güvenli bir şekilde çalıştırmasına ve gözlemlenmesine olanak tanır.
Saldırı tespit sistemleri (IDS'ler)	• Bu araçlar, gerçek zamanlı trafik izleme ve inceleme için kullanılır. • Halihazırda akan trafiğin herhangi bir yönü belirlenmiş kurallardan herhangi biriyle eşleşirse, önceden tanımlanmış bir eylem gerçekleştirilir.
Firewalls	• Bu yazılım, önceden tanımlanmış kurallara göre trafiğin bir ağa veya aygıta girmesine veya çıkmasına izin verilip verilmeyeceğini belirtmek için kullanılır.
Log managers	• Olayları kaydetmek için günlük dosyaları kullanılır. • Bir ağ çok fazla sayıda günlük girişi oluşturabildiğinden, günlük izlemeyi kolaylaştırmak için günlük yöneticisi yazılımı kullanılır.

Linux Kabuğu (Linux Shell)

Linux'ta kullanıcı, CLI veya GUI'yi kullanarak işletim sistemi ile iletişim kurar. Linux genellikle varsayılan olarak GUI'de başlar. Bu, CLI'yi kullanıcıdan gizler. CLI'ye GUI'den erişmenin bir yolu, bir terminal emülatör uygulamasıdır. Bu uygulamalar, CLI'ye kullanıcı erişimi sağlar ve kelime terminalinin bir varyasyonu olarak adlandırılır. Linux'ta, popüler terminal emülatörleri Terminator, eterm, xterm, console ve gnome-terminal dir.

Not: *Kabuk, konsol, konsol penceresi, CLI terminali ve terminal penceresi terimleri genellikle birbirinin yerine kullanılır. Biz de terminal kelimesini kullanacağız. En sık kullanılan komutlar aşağıdaki tabloda verilmiştir.*

Komut	Açıklama
mv	Dosyaları ve dizinleri taşır veya yeniden adlandırır.
chmod	Dosya izinlerini değiştirir.
chown	Bir dosyanın sahipliğini değiştirir.
dd	Bir girdiden çıktıya verileri kopyalar.
pwd	Geçerli dizinin adını görüntüler.
ps	Sistemde şu anda çalışan işlemleri listeler.
su	Girişi başka bir kullanıcı olarak veya süper kullanıcı olarak simüle eder.
sudo	Varsayılan olarak bir komutu süper kullanıcı olarak veya başka bir adlandırılmış kullanıcı olarak çalıştırın.
grep	Bir dosya veya diğer komut çıktıları içindeki belirli karakter dizelerini aramak için kullanılır.
ifconfig	Ağ kartıyla ilgili bilgileri görüntülemek veya yapılandırmak için kullanılır
apt-get	Debian ve türevlerine paketleri yüklemek, yapılandırmak ve kaldırmak için kullanılır.
iwconfig	Kablosuz ağ kartıyla ilgili bilgileri görüntülemek veya yapılandırmak için kullanılır.
shutdown	Sistemi kapatır ve yeniden başlatma, durdurma, uykumoduna alma veya şu anda bağlı olan tüm kullanıcıları kovma gibi ilgili görevleri kapatır.
passwd	Parolayı değiştirmek için kullanılır.
cat	Bir dosyanın içeriğini listelemek için kullanılır ve parametre olarak dosya adını bekler.
man	Belirli bir komut için belgeleri görüntülemek için kullanılır.
ls	Dosyaları bir dizinin içinde görüntüler.
cd	Geçerli dizini değiştirir.
mkdir	Geçerli dizin altında bir dizin oluşturur.
cp	Dosyaları kaynaktan hedefe kopyalar.
mv	Dosyaları farklı bir dizine taşır.
rm	Dosyaları kaldırır.
grep	Bir dosya veya diğer komut çıktıları içindeki belirli karakter dizelerini arar.
cat	Bir dosyanın içeriğini listeler ve parametre olarak dosya adını bekler.

Linux Dosya Sistemi: Hız, esneklik, güvenlik, boyut, yapı, mantık ve daha fazla özellikleri değişen birçok farklı dosya sistemleri türü vardır. Yönetici, işletim sistemi için uygun olan dosya sistemi türünü karar verir. Aşağıdaki tabloda, Linux tarafından yaygın olarak bulunan ve desteklenen birkaç dosya sistemi türü listelenir.

Linux Dosya Sistemi	Açıklama
ext2 (second extended file system)	• ext2, ext3 tarafından yerini alana kadar birçok büyük Linux dağıtımında varsayılan dosya sistemiydi. • ext2 hala flash tabanlı depolama ortamı için tercih edilen dosya sistemidir, çünkü bir günlük olmaması, performansı artırır ve yazma sayısını en aza indirir. • Flash bellek aygıtlarının sınırlı sayıda yazma işlemi olduğu için, yazma işlemlerini en aza indirmek cihazın ömrünü artırır.
ext3 (third extended file system)	• ext3, varolan ext2 dosya sistemini geliştirmek için tasarlanmış günlük bir dosya sistemidir. • Ext3'e eklenen ana özellik olan günlük, ani güç kaybı durumunda dosya sistemi bozulması riskini en aza indirmek için kullanılan bir tekniktir. • Dosya sistemleri yapılacak tüm değişikliklerin bir günlük tutar. Değişiklik tamamlanmadan önce bilgisayar çöküyorsa, günlük kilitlenme tarafından oluşturulan sorunları geri yüklemek veya düzeltmek için kullanılabilir. • Ext3 dosya sistemlerinde maksimum dosya boyutu 32 TB'dir.
ext4 (fourth extended file system)	• ext4 uzantıları ext3 performansını artırmak ve desteklenen dosya boyutlarını artırmak için ortaya çıktı. Fakat geliştiriciler den bazıları ext4 ün istikrar sorunları hakkında endişe duyması nedeniyle kararlı ext3 uzantıları destekledi. • Ext3 projesi ikiye bölündü; biri ext3 ü devam ettirdi, diğerleri ise ext4 isimli uzantıyı kullanmaya karar verdi.
HFS Plus or HFS+ (Hierarchical File System Plus)	• Apple'ın Macintosh bilgisayarlarında kullandığı bir dosya sistemi. Linux çekirdeği, okuma yazma işlemleri için HFS+ montajı için bir modül içerir.
APFS (Apple File System)	• Apple aygıtları tarafından kullanılan güncelleştirilmiş bir dosya sistemi. • Güçlü şifreleme sağlar ve flash ve katı hal sürücüleri için optimize edilmiştir.

Servis Konfigürasyon Dosyaları: Her bilgisayar tarafından bilinen servislerin isimleri ve hangi portları kullandıkları /etc/services dosyasında tutulur.

```
root@kali: /
File  Edit  View  Search  Terminal  Help
root@kali:/# cat /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
```

- **rsyslog.d ve /etc/rsyslog.conf**

  rsyslog.d programı Linux'taki çeşitli olayların kayıtlarını tutar. Bunlar genellikle hata mesajları veya çekirdek mesajları gibi kayıtlardır. rsyslog.d sistem açılırken arkaplanda işlemeye bırakılır [54].

  /etc/rsyslog.conf, rsyslog.d programının konfigürasyonu için kullanılır.

Örnek bir rsyslog.conf dosyası aşağıda yer almaktadır.

```
Applications  Places  Terminal        Sat 15:56                tr
                          root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# cat /etc/rsyslog.conf
#  /etc/rsyslog.conf    Configuration file for rsyslog.
#
#               For more information see
#               /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")


###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

#
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
```

Not: *Diğer Linux dağıtımlarında görülebilecek syslog daemon'ları: sysklogd, rsyslogd, syslog-ng'dir.*

1. Nolu Bölgelerde: Bu dosyanın en solunda yer alan ve nokta ile ayrılmış olan iki kelimeden ilki, kaydı yapılan program grubudur. Bu kısma kern (çekirdek mesajları), mail (sendmail mesajları), login (sisteme giriş veya sistemden çıkış mesajları), auth, authpriv veya security (güvenlik mesajları), cron (cron mesajları), daemon (deamon'lardan gelen mesajlar),lpr (yazıcı mesajları), news (haber grubu mesajları), user (kullanıcı mesajları) veya uucp (uucp mesajları) yazılabilir. Noktanın sağındaki kelime ise kaydı yapılan program grubunun mesaj önem sırasını belirler.

```
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf


###############
#### RULES ####
###############

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err

#
# Some "catch-all" log files.
#
*.=debug;\
     auth,authpriv.none;\
     news.none;mail.none        -/var/log/debug
*.=info;*.=notice;*.=warn;\
     auth,authpriv.none;\
     cron,daemon.none;\
     mail,news.none             -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*
root@kali:~#
```

1

2

3

2. Nolu Bölgede: Önem sırasına göre debug, info, notice, warning, err, crit, alert ve emerg bulunur. Dosyanın sağında yer alan kısımda ise bu mesajların hangi dosyaya yazılacağı vardır.

Yukarıda verilen örnekte, rsyslogd'den gelen mesajlar sanal konsollardan kullanılmayanlara yönlendirilmiştir. Böylece sistem yöneticisi F8, F9 ve F10 tuşlarını kullanarak sistem kayıtlarına anında ulaşabilir.

Başka bir makinaya kayıt tutturmak da mümkündür. Uzak makinenin ismi rsyslog.conf dosyasının sağ bölümüne yazılır. Böylece diğer makina yerel olarak sistem kayıtlarını tutacaktır.

init ve /etc/inittab

init, sistemde ilk çalışan programdır. Neredeyse sistemin tüm açılış yükünü elinde tutar. init sayesinde açılış anında hangi programların çalıştığı belirlenir. Bu programları da /etc/inittab dosyasından öğrenir.

Burada /etc/inittab dosyasından alınan birkaç örnek satır yer alıyor. Her satırın sonunda çalıştırılacak olan dosyalar vardır.

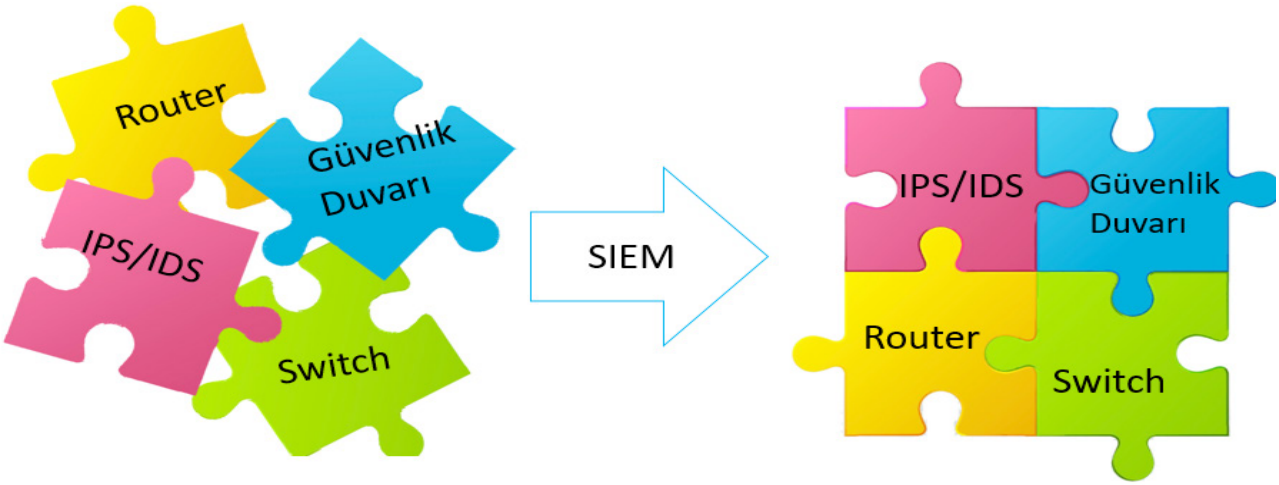
BÖLÜM 7

GÜNLÜK DOSYALARI ve OLAY YÖNETİMİ

Bilişim sistemlerine ya da ağ sistemlerine yapılan saldırılar, çok nadir olarak gerçek birer saldırı olarak görünür. Saldırgan açısından başarılı bir saldırının ardından geriye dönüp incelendiğinde, saldırıların sistemlerde çeşitli izler ya da etkiler bıraktığı görülür. Çünkü yapılan her aktif saldırı, sistemde bir değişikliği amaçlar. Doğru gözlemlendiğinde, saldırı keşif aşamasında ya da saldırı anında tehditler tespit edilebilir. Ancak her saldırı ya da zararlı yazılım, sadece bir cihazın sürekli olarak anlık izlenmesi ile tespit edilemez. Bu nedenle ağın farklı konumlarındaki tepkilerin (loglar ya da olaylar) korelasyonunun sağlanması ile bu zararlı aktiviteler tespit edilebilir. Başlangıçta güvenlik log yönetimi sunan yazılımlar ile loglar arasında korelasyon sağlayan birbirinden bağımsız olan yazılımlar, günümüzde bir bütün olarak karşımıza çıkmaktadır.

7.1 SIEM (Security Information Event Management)

Siber güvenlik söz konusu olduğunda, ağ izlemek ve analiz etmek güvenlik açısından son derece önemlidir. Ağa yönelik saldırıları ve saldırganları tespit etmek, tehditler ile mücadele etmede önemli yollardan biridir. Oysa kurumsal ağlardda izlenmesi gereken IPS/IDS, güvenlik duvarı, sunucu, yönlendirici, anahtar ve hatta konak cihazlar gibi birçok kaynak bulunmaktadır. Bu kaynakların herbiri bağımsız olarak günlük dosyası **(log)** üretmektedir. Kitabın altıncı bölümünde konak için bu günlük dosyalara ve olaylara **(event)** değinilmiştir.



Şekil 7.1. SIEM çeşitli kaynaklardan gelen günlükleri, olayları toplar ve yorumlar

Yaygın ağ izleme programlarının çoğu, kullanıcının görüntülenen ham verileri yorumlayabilmesini gerektirdiğinden genellikle teknik uzmanlık gerektirir. Bu günlük dosyalarının her birinin ayrı ayrı ele alınması ve zaman açısından zor hem de log dosyaları arasında ilişkinin manuel yollarla tespit edilip analizini zorlaştırmaktadır. SIEM yazılımı bilgisayardaki tüm çeşitli sistemlerden ve programlardan günlük **(log)** ve olay **(event)** verilerini toplar ve yorumlar [6]. Böylece teknik olmayan kullanıcının da verileri ham haliyle anlamasına gerek kalmaz. Aynı zamanda otomasyon sağlanarak, ağın gerçek zamanlı izlenmesi, olası tehdit anında alaram üretilmesi ve ağ yöneticisine saldırıya tepki **(response)** vermesi için bilgiler sunar.

Genel olarak ifade etmek gerekirse SIEM yazılımları aşağıda belirtilen özelliklere sahip olması beklenir.

- Gelişmiş tehdit tespiti
- Alarm üretimi
- Anomali tespiti
- Big Data analizi
- Raporlama

SIEM yazılımları, günlükleri toplayıp analiz etmenin ve gerçek zamanlı aksiyon sağlamanın haricinde, kullanıcılara uzun vadeli depolama ve zamana bağlı güvenlik analizi gibi avantajlar da sunabilir. Ayrıca;

- Felaket kurtarma
- Kimlik doğrulama
- Sanallaştırma hizmetleri
- Zararlı yazılım ve saldırı önleme
- Sızma testleri

gibi özellikler de yine SIEM yazılımları tarafından sağlanabilir.

7.1.1 Yaygın SIEM Yazılımları

Siber Güvenlik Dünyasında, güvenlik loglarının ve olaylarının yönetimini birleştiren çeşitli SIEM yazılımları bulunmaktadır. Bu başlık altında bu yazılımlardan yaygın olarak kullanılanlar listelenmektedir.

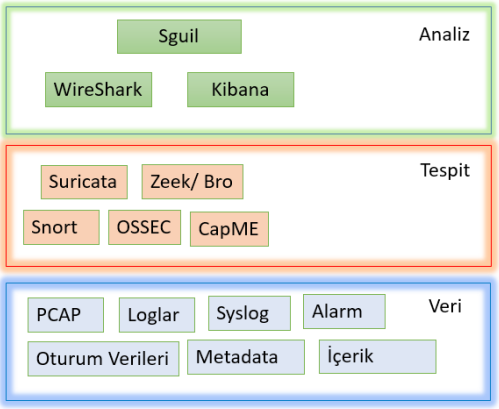
- OSSEC
- OSSIM
- SNORT
- SIEMonster
- IBMQ Radar
- SolarWinds Security Event Manager

7.2 SECURITY ONION YAZILIMI

Bilgisayar ağları ve ağ donanımları saldırganların hedefidir ve sürekli olarak izlenmesi gerekmektedir. Önceki bölümde bu yazılımlardan bazıları ele alınmıştı. Bu bölümde, açık kaynak Ağ Güvenlik İzleme araçlarını içeren ve Linux Ubunutu dağıtımında çalışan Security Onion (SO) ele alınacaktır. Security Onion, tehdit algılama, kurumsal güvenliği izleme ve günlük yönetimi sunan ücretsiz ve açık kaynaklı bir Linux dağıtımıdır [48]. Yazılım hakkında daha fazla bilgi ve indirme için aşağıdaki bağlantı kullanılabilir:

https://docs.securityonion.net/en/2.3/about.html

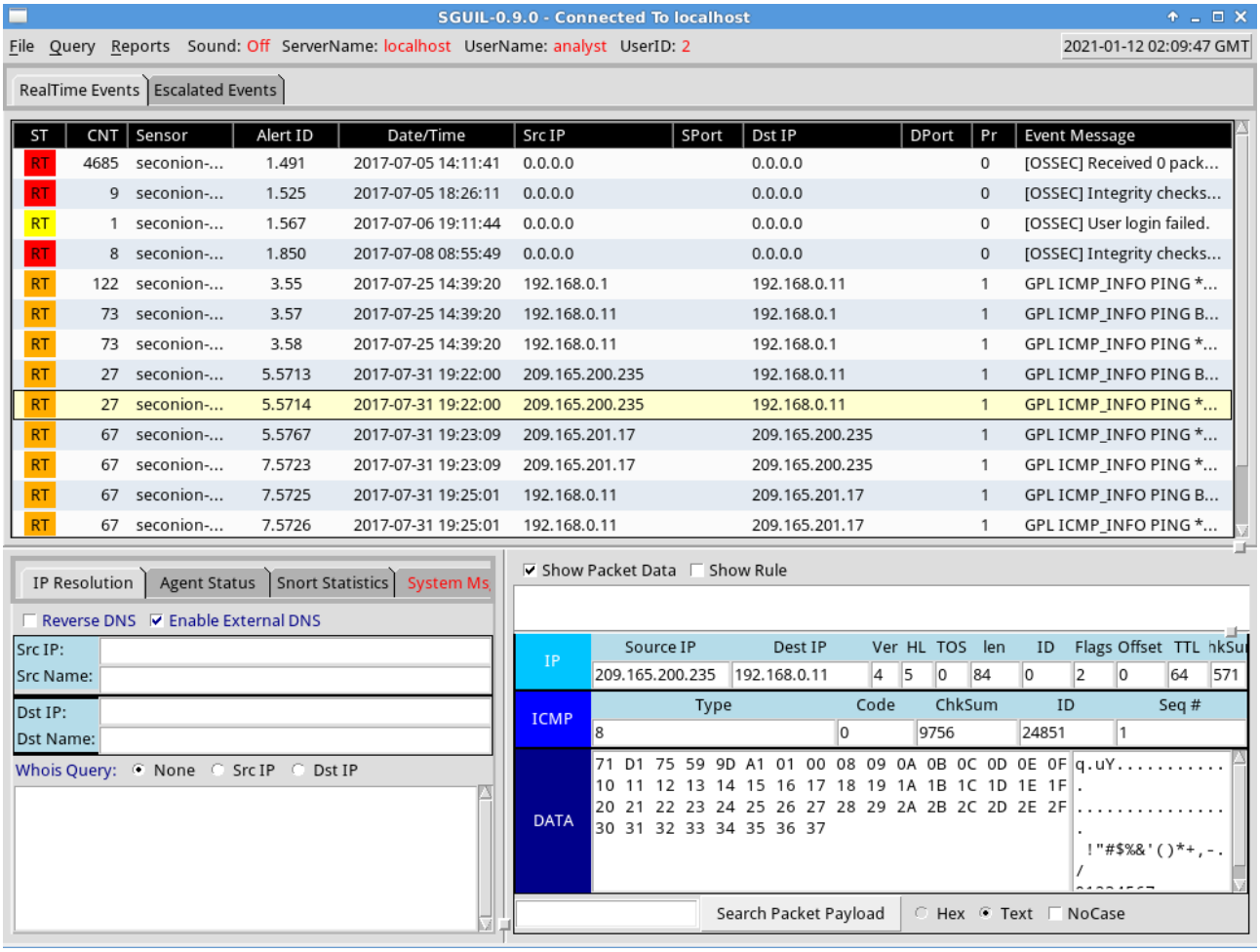
Security Onion'da yer alan araçlar, siber güvenlik analistleri için, **ağ paketlerini yakalama, Ağ ve Konak Tabanlı Saldırı Algılama Sistemi (IDS) ve ağ analisti için uyarı sistemi** olmak üzere üç temel işlev sunar. SO'nun temel mimarisi Şekil 7.2'deki gibidir [46];



Şekil 7.2. Security Onion'un temel mimarisi

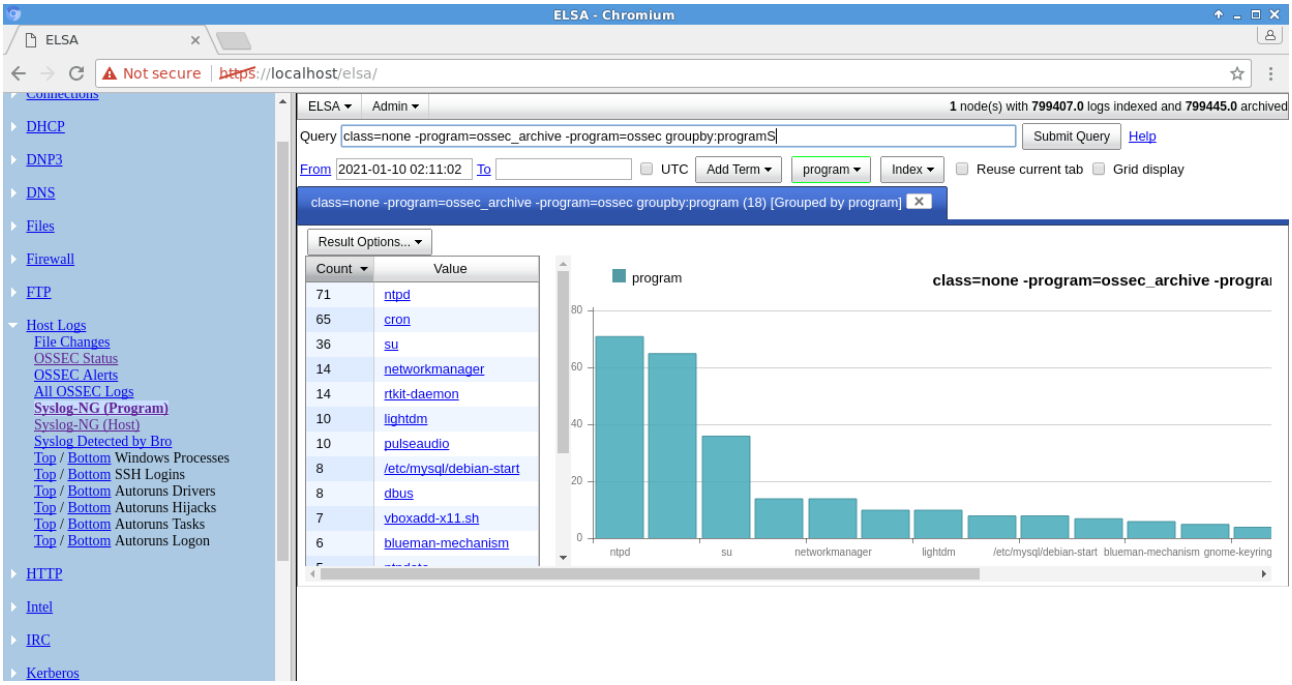
7.2.1 Security Onion Araçları

SGUIL: Çok çeşitli kaynaklardan gelen ya da yakalanan verilerin analizini ve araştırılmasını sağlayan üst düzey bir konsoldur. GUI, Snort, Suricata ve Wazuh'dan gelen verileri bir araya getirir. Sguil, güvenlik uyarılarının araştırılmasında bir başlangıç noktası olarak görülebilir [43-44].



Şekil 7.3. Security Onion'da yer alan Sguil aracı.

ELSA: ELSA, Kurumsal Günlük Arama ve Arşiv (Enterprise Log Search and Archive) anlamına gelir. Adından da anlaşılacağı üzere, birden çok kaynaktan gelen verilerinin aranmasını ve arşivlenmesini sağlayan kurumsal bir araçtır [45].



Şekil 7.4. Security Onion'da yer alan ELSA aracı.

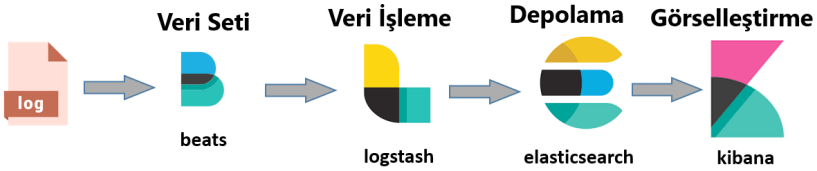
ELSA, günlük dosyası girişlerini daha sonra ELSA web arayüzünde görüntülenebilen ortak bir şemaya normalleştirebilir. Arama, basit bir sözdizimini ve ayrıca gerekirse arama ve filtreleme için daha karmaşık düzenli ifadeye dayalı kalıpları izler. ELSA, büyük miktarlarda veriyi indeksleme, arşivleme ve arama yeteneğine sahiptir.

WireShark: Daha önceki bölümlerde anlatılan önemli Security Onion paket yakalama araçlarından biridir [49].

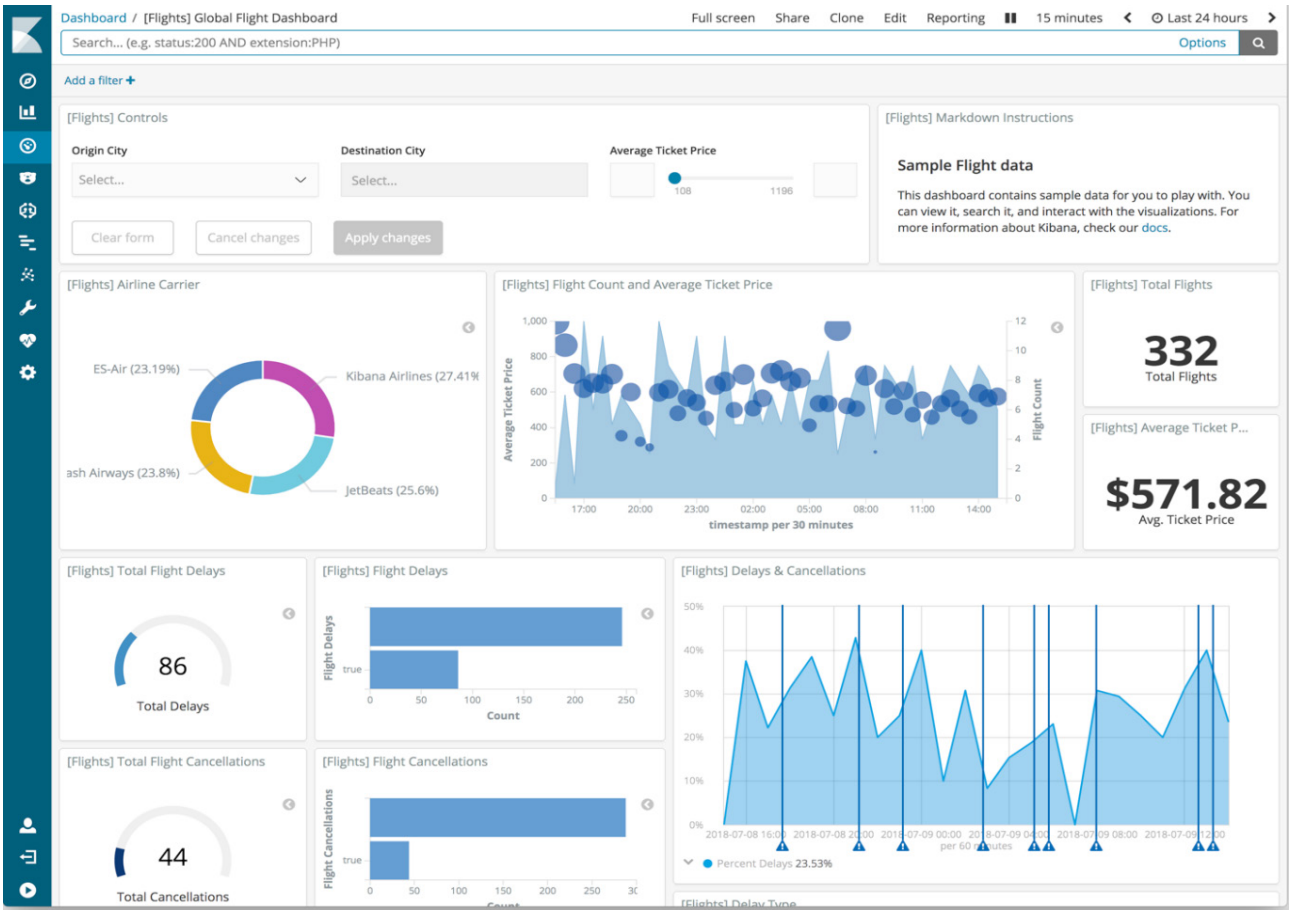
Alexa Ip Lookup: Alexa bir trafik analiz aracıdır. İnternet sitelerinin trafiğini ve ziyaretçi davranışları inceleyerek sunum yapar. Alexa'nın popüler olmasını sağlayan en başlıca özelliği sıralama özelliğidir. İnternet sitelerinin aldığı trafiğe göre dünya sıralaması oluşturur. Bu araç kullanılarak, belirlenen IP hakkında, zararlı bir site (ya da IP) olup olmadığı hakkında fikir sahibi olunabilir.

CentralOps Ip Lookup: Tarayıcı üzerinden sorgu yapılabilen diğer bir servistir.

Kibana Ip Lookup: Kibana, Elasticsearch için açık kaynaklı bir veri görselleştirme panosudur. Bir Elasticsearch kümesinde indekslenen içeriğin üstünde görselleştirme yetenekleri sağlar. Kullanıcılar, büyük hacimli verilerin üstünde çubuk, çizgi ve dağılım grafikleri veya pasta grafikler ve haritalar oluşturabilir [51].

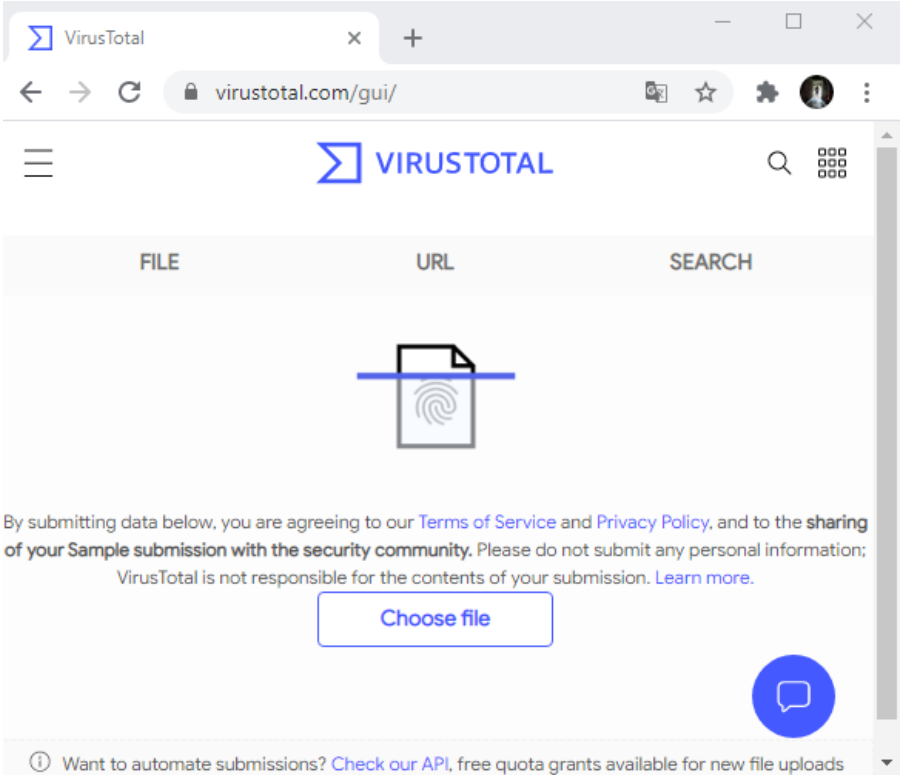


Şekil 7.5. Security Onion'da log yönetimi



Şekil 7.6. Kibana ekranı

Virus Total Ip Lookup : Virustotal sitesine bağlanarak tespit edilen zararlı yazılım ile ilgili detaylı bilgiler edinilebilir. Hangi antivirüs programlarının zararlı olarak işaretlendiğini hangi IP adreslerinden bu zararlı yazılımın dağıtımının yapıldığı gibi bilgilere ulaşılabilir. Dosyaya, URL adresine ve Md5/SHA1/SHA2 hash değerine göre arama yapılabilir.



*Şekil 7.7.*Virus Total Aracı

BÖLÜM 8

KRİPTOLOJİ

8.1 KRİPTOLOJİYE GİRİŞ

Bilgisayar ağları ve özellikle internet, doğası gereği herkese açık (public) ortamdan verilerin transfer edilmesini gerektirir. Bu nedenle, yetkisiz kişilerin hassas verilere erişim ihtimaline karşı ağ teknolojilerinde kriptoloji oldukça yararlı ve gelişen bir alandır. Kriptoloji, modüler aritmetik, olasılık kuramları, üslü sayılar gibi birçok matematiksel temellere dayanmaktadır. Ancak bu bölümde metematiksel temellerden ziyade, ağ ortamındaki kullanımın ve temel mantığına değinilecektir.

Bilgisayar ağlarında güvenlik söz konusu olduğunda iletişimin güvenli olması için Kimlik Doğrulama (Authentication), Yetkilendirme (Authorization) ve Hesap Denetimi (Accounting) özelliklerinin dikkate alınması gerekir. Bu üç özellik AAA olarak adlandırılır.

Siber güvenliğin üçlü bileşenlerinden gizlilik ve bütünlük, kriptolojik algoritmalar kullanılarak sağlanmaktadır. Yine yapısı gereği güvensiz olan IP'nin güvenliğini sağlayan IPSec mimarisi de kriptolojik temellere dayanmaktadır.

Verilerin sadece ilgili kişileri tarafından okunmasını ve anlaşılması oldukça eski tarihlere dayanan bir geçmişe sahiptir. Özellikle askeri alanda haberleşmenin gizliliğinin sağlanması için şifreleme algoritmaları kullanılmıştır. Tarihsel olarak incelendiğinde, Sezar'a atfedilen bir şifreleme türünde **(Sezar şifrelemesi)**, mesajın gizliliğini sağlamak için harf kaydırma yöntemi kullanılmıştır. Buna göre, esas mesajı şifrelemek için her harf, alfabedeki belirli bir sayı sonraki harf ile yer değiştirilir. (Örnekte Türkçe alfabe dikkate alınmış ve 2 harf kaydırma yapılmıştır).

Orijinal Mesaj (Plain Text) : "yarın şafakta doğudan giriş yapın"

Şifreli Mesaj (Cipher Text) : "acşjö ucğcmüc fpıvfcö hkşk acsjö"

Burada gizli tutulması gereken anahtar bilgi, kaç harf kaydırıdılığını belirten "2" bilgisidir. Gönderici ile alıcı arasında bu anahtar bilginin güvenli bir şekilde önceden paylaşılmış olması önemlidir. Alıcı, şifreli mesajı aldıktan sonra tersi işlemi yaparak (her harf iki önceki harf ile değişir) orijinal mesajı elde eder. Burada kullanılan şifreleme yöntemi, yerine koyma, yer değiştirme **(substitution)** yöntemidir.

Açıkça belli ki, Sezar şifrelemesi oldukça basit bir şifreleme türüdür. Ancak kullanılan "yer değiştirme" yöntemi günümüz şifrelemelerinde kullanılan yöntemlerin de temelinde kullanılmaktadır.

Şifrelemede kullanılan diğer bir algoritma da, harf matrisinin kullanıldığı **Vigenére Algoritmasıdır.**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Şekil 8.1. Vigenere tablosu

Bu algoritmada, orijinal mesaj, kaynak ile hedef arasında önceden belirlenen (ve gizli olması beklenen) bir anahtara göre yapılır.

Örnek:

Orijinal Mesaj (Plain Text) : "MERHABALAR"

Anahtar (Key) : "ERDAL"

Buna göre, anahtar kelime orijinal mesaj boyutuna eşit olacak şekilde uzatılır ve her harf sırasıyla anahtar ile karşılaştırılır ve tablodaki karşılığı bulunur.

Orijinal Mesaj	M	E	R	H	A	B	A	L	A	R
Anahtar	E	R	D	A	L	E	R	D	A	L
Şifreli Mesaj	Q	V	U	H	L	F	R	O	A	C

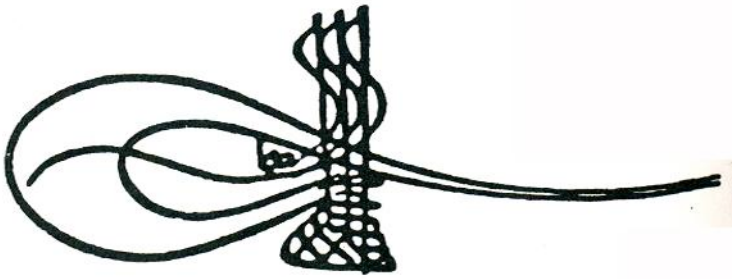
Buna göre şifreli mesaj (cipher text) "QVUHLFROAC" olacaktır. Ancak Vigenére, Sezar ya da Rail-Fence gibi algoritmalar, bilişim sistemlerinde kullanılamayacak kadar basit algoritmalardır. Alfabede kullanılan harflerin sıklıkları, dil kuralları ve deneme yanılma sayılarının nisbeten az olması nedeniyle kolaylıkla kırılabilecektir.

İletişimin güvenliğinin sağlanması sadece şifreleme ile sağlanmamaktadır. Aynı zamanda verinin başkası tarafından okunmadığının da garanti altına alınması gerekir.

Şekil 8.2. Verinin değiştirilmediğinin garantisi bütünlük (intergrity) olarak ifade edilir.

Diğer taraftan gelen mesajın başkası tarafından değiştirilmemiş olduğu da yine önemli bir kavramdır. Eskiden mektuplarda (mesajlarda) açılıp açılmadığının anlaşılabilmesi için kullanılan balmumunun amacı, veri bütünlüğünü **(integrity)** sağlamaktır. Açılmış bir mesaj artık gizli değildir, verinin doğruluğu şüphelidir. Aynı mantık bilişim sistemlerinde ve bilgisayar ağlarında da özetleme **(hashing)** algoritmaları ile sağlanmaktadır.

Son olarak bu kapsamda ele alınması gereken konulardan biri de, gelen mesajın gerçekten iddia edilen kaynaktan gelip gelmediğidir.



Şekil 8.3. Kimlik doğrulama için tarihte çeşitli yöntemler kullanılmıştır.

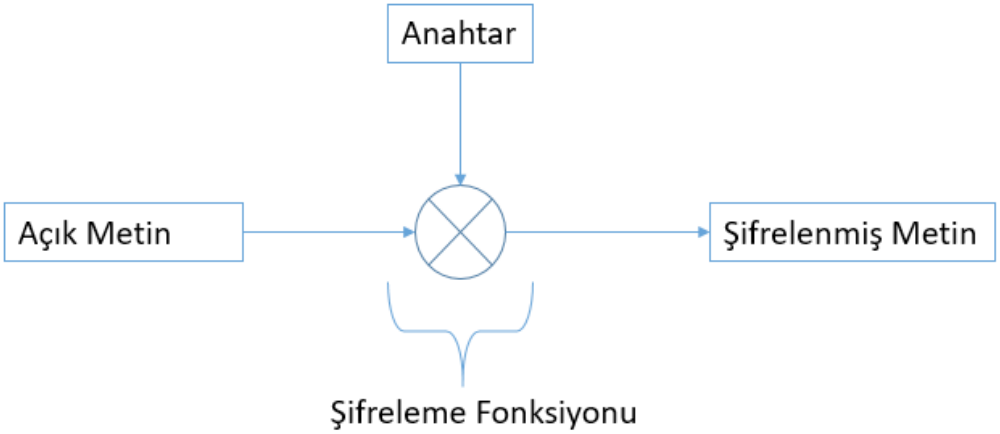
Bu durum alıcı için de geçerlidir. Yani tarafların her ikisinin de kimliğinin doğrulanması gerekir. Bu işlem kimlik doğrulama (authentication) olarak adlandırılır. Kimlik doğrulama için, ön paylaşımlı anahtar, parola ya da dijital imzalar kullanılabilir.

8.2. ŞİFRELEME ALGORİTMALARI

C-I-A siber güvenlik üçlü bileşenlerden biri mahremiyet ve gizlilik anlamına gelen **"confidentiality"** bileşenidir. Gizlilik bilgisayar genelinde verilerin yetkisiz kullanıcılar tarafından okunmasını önlemek için kullanılır. Bir sistemde yer alan (ya da depolanan) dosyaların başkası tarafından okunmaması gizlilik ilkesi gereğidir. Aynı şekilde bilgisayar ağlarında verinin hareket halinde iken de yetkisiz kişiler tarafından anlaşılamaz olması gerekir.

Bilgisayar ağlarında iletişim genele açık internet ortamından olması ve potansiyel olarak herkesin internette olabilir olması, gizliliği internet iletişiminde önemli bir unsur kılar. Gönderilen mesaj, yalnızca alıcı tarafından anlaşılabilmelidir. Bu işlem şifreleme **(encryption)** olarak adlandırılır. Açık metin olan mesaj **(plain text)** belirli bir anahtar ile şifrelenir **(ciphertext)** ve

genele açık internet ortamından gönderilir. Mesaj, internet ortamında yetkisiz kişiler tarafından yakalansa dahi, anlaşılamaz bir formda olması beklenir. Doğru alıcı (doğru anahtara sahip kişidir) şifreli mesajı aldığında anahtarı kullanarak mesajı çözer, deşifre (decryption) eder. Sonuç olarak göndericinin ilk başta ifade ettiği açık metine ulaşır.



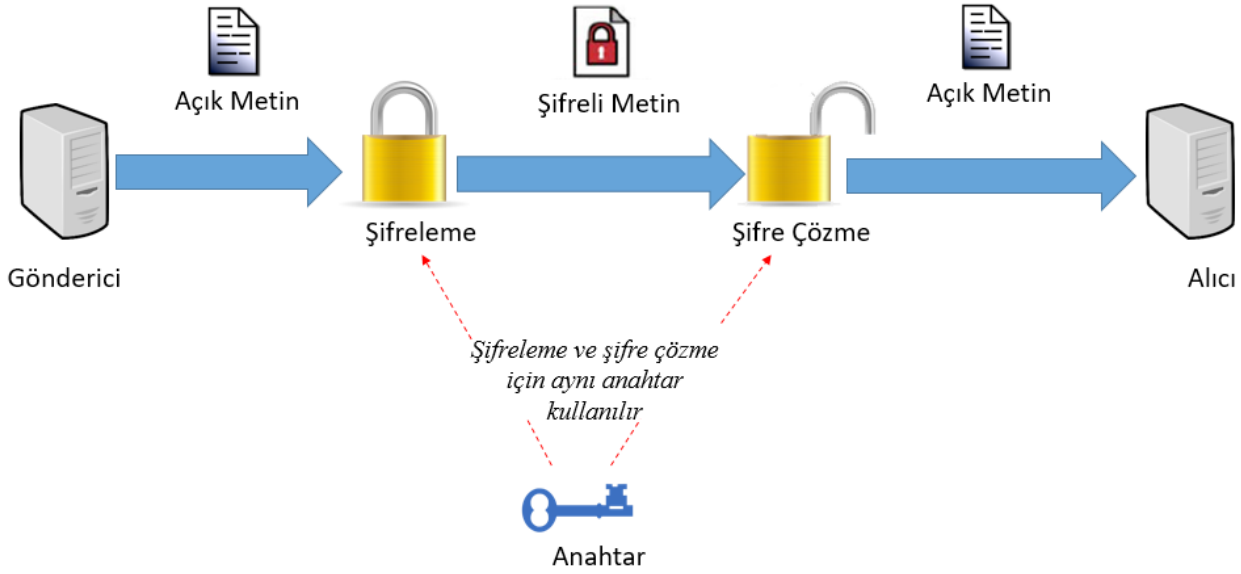
Şekil 8.4. Temel şifreleme prensibi

Bu amaç için bir önceki bölümde Sezar ve Vigenere örneklerinde olduğu gibi matematiksel algoritmalar ve fonksiyonlar kullanılır. Sezar algoritmasında, Türkçe dili için en fazla 28 denemeden sonra şifreli bir mesaj çözülebilir. Bu işlem yazılımsal olarak sırayla deneme yapıp, her olası sonucu ekrana dökerek yapılabilir. Dikkat edilirse burada önemli olan anahtarın bulunmasıdır. Sezar algoritmasında anahtar bir sayıdır ve yazılımsal sırayla tüm ihtimaller denenerek anahtar bulunabilir. Bu tür sırayla her ihtimalin denenmesine deneme-yanılma ya da kaba kuvvet (bruteforce) atağı denmektedir. Oysa Vigenere algoritmasında ise anahtar bir sayı değil, bir metin olabilir. Aynı durum bu anahtar için de geçerlidir, yani deneme yanılma yoluyla bu anahtar da sonuçta yine bulunabilir. Ancak burada önemli olan konu, anahtarın ne zaman bulunacağıdır. Bu süre, anahtarın uzunluğu ile üstel orantılıdır. Anahtar ne kadar uzunsa bulmak o kadar uzun zaman alır, ancak her ihtimal denendiği için teorik olarak bulunur. Bu durum her anahtarın bir kırılabilirlik ömrü olduğunu gösterir ve kriptolojide bu sürenin yarısına ulaşıldığında anahtarın kırıldığı farzedilir. Bu nedenle bu süre dolmadan anahtarın değiştirilmesi önerilir. Bazı sistemlerde belirli periyotlarla parola (anahtar) değiştirilmesinin nedeni budur. Günümüzde sürekli olarak daha güçlü şifreleme algoritmaları bulma çabası vardır. Daha güçlü şifreleme, kırılma süresinin daha uzun olması sonucunu doğurur.

Bilişim sistemlerinde, simetrik şifreleme ve asimetrik şifreleme olmak üzere iki tür şifreleme yöntemi vardır.

8.2.1 Simetrik Şifreleme

Tıpkı bir kapıyı kilitlemek ve açmak için aynı anahtarı kullanmak gerektiği gibi, bu yöntemde de şifreleme ve şifre çözmek için aynı anahtar kullanılır. Bu yönteme gizli anahtar yöntemi de denmektedir.



Şekil 8.5. Simetrik şifreleme.

Şekil 8.5'den de görüleceği üzere, gönderici açık metini Anahtar ile şifreler ve şifreli metni elde eder. Elde edilen bu metin ağdan transfer edilir. Alıcı taraf, aynı anahtar ile çoğu zaman algoritmanın tersini kullanarak şifreli metinden açık metni elde eder *(Aynı algoritma kullanım örneği: şifreleme için XOR işlemi kullanıldıysa çözmek için de yine XOR kullanılabilir)*.

Bu işlemde kritik nokta, anahtarın gizliliğidir. İnternet gibi genele açık ve bu anlamda güvensiz bir ortamdan bu gizli anahtarın taraflara iletilmesi önemli bir konudur ve kitabın ileriki bölümlerinde bu işlemin nasıl yapıldığı anlatılacaktır.

Simetrik şifrelemede blok şifreleme ve stream (akış) şifreleme olarak iki farklı yöntem kullanılmaktadır. Blok şifreler, sabit uzunlukta bir düz metin bloğu 64 veya 128 bitlik ortak bir şifreli metin bloğuna dönüştürür. Bloğun boyutu bir defada şifrelenecek metnin boyutunu ifade eder. Akış şifrelerinde ise düz metin her seferinde bir bayt veya bir bit olarak şifrelenir.

Simetrik şifrelemenin kendisine göre avantajları bulunmaktadır. Başlıca avantajları şu şekildedir:

- Şifreleme ve şifreyi çözme işlemleri daha hızlıdır.
- Alıcı ve verici arasındaki iletişimin gizliliği sağlanır.
- Şifreli metin çözülmedikçe orijinal metin değiştirilemeyecektir.

Simetrik Şifreleme DES, 3DES, AES, SEAL ve RC gibi birçok standart kullanılmaktadır.

DES (Data Encryption Standard): 1976 yılında standartlaşmıştır. 1997'de resmi bilgi şifreleme standardı olarak başlamış ancak zayıflıkları nedeniyle 2000 yılında AES'e yerini bırakan blok tabanlı bir şifreleme standardıdır. DES algoritması şifrelenmek istenen bir yazıyı bloklara bölerek her bloğu birbirinden bağımsız olarak şifreler. Şifrenin çözümü de aynı şekilde blokların tek tek çözümü ile gerçekleştirilir. 56-bit uzunluğunda anahtar kullanılır. Aslında 64-bit anahtar kullanır ancak 8-bit integrity için kullanıldığından şifreleme için sadece 56-bit kullanılabilir. Saniyede 255 anahtar deneyen özelleştirilmiş bir şifre kırma makinası ile 6,4 günde kırılabilmiştir. Günümüz ağlarında kullanımı yeterince güvenli değildir.

3DES : DES algoritmasının yetersizliği nedeniyle geliştirilmiştir. Üç farklı anahtarla DES'in şifreleme, deşifreleme ve tekrar şifrelenmesi ile elde edilmiş bir standarttır. 112 ve 168-bit anahtar uzunluğu kullanılmaktadır. Saniyede 255 anahtar deneyen bir makine ile 4,6 milyar yılda kırılabilir. Ancak algoritmasının zayıflığı nedeniyle yeterince güvenli kabul edilmemektedir.

AES (Advanced Encryption Standard) : 1997 yılında NIST tarafından yapılan bir yarışma sonrasında geliştirilmiş güvenli bir şifreleme standardıdır. 128, 192 ve 256-bit uzunluğunda anahtarlar kullanır. Saniyede 255 anahtar deneyen bir makine ile 149 trilyon yılda kırılabilir.

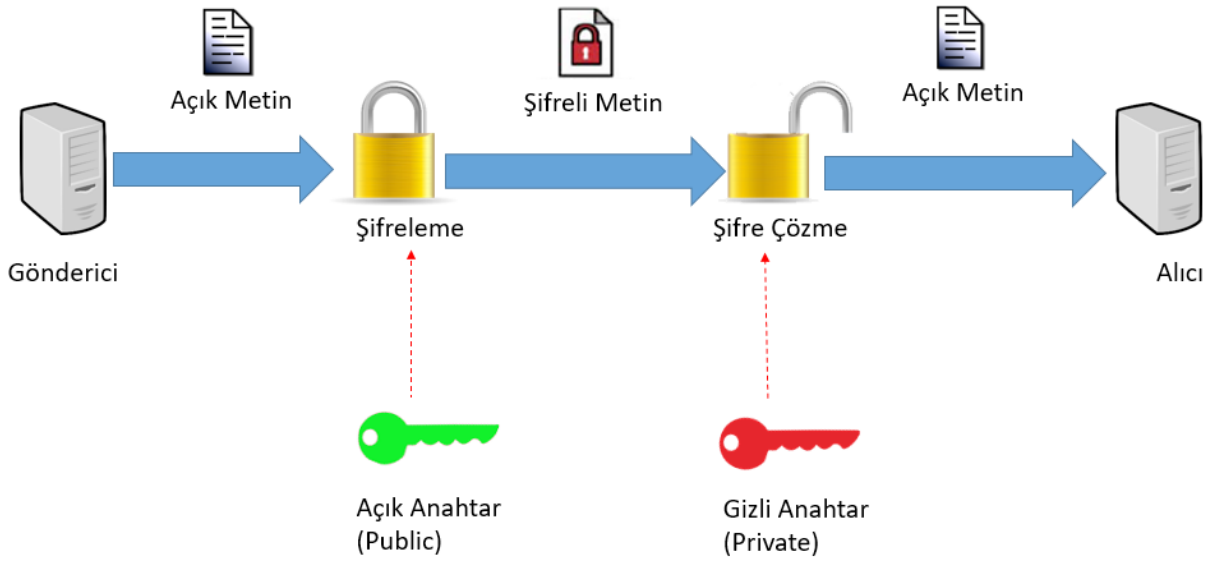
SEAL (Software-Optimized Encryption Algorithm) :1994 yılında çıkan akış tabanlı bir şifreleme türüdür. 160-bit uzunluğunda anahtar kullanır. Kırılabilirlik süresi hesaplanmamıştır ancak oldukça güvenilir olduğu düşünülmektedir. En önemli avantajı kaynak tüketiminin düşük olmasıdır.

RC Algoritmaları : Bu algoritmalar MD5 algoritmasını da tasarlayan Ronald Rivest tarafından geliştirilmiştir. 1994 yılında RC2, 1994 yılında RC5, 1998 yılında da RC6 geliştirilmiştir. En yaygın bilineni RC4 algoritmasıdır. Kablosuz ağlarda güvensiz olarak görülen WEP şifrelemede kullanılan yöntem yine RC4'tür. Genel olarak zayıf algoritmalar olarak bilinir. RC5 modern şifreleme algoritmaları sınıfında yer alan bir algoritmadır. 16, 32 ve 64 bit kelime uzunlukları ile çalışabilmektedir. Algoritma içinde "Anahtar Boyutu" ve "Döngü Sayısı" olmak üzere iki değişken bulunmaktadır. Kullanılan değişkenlere göre (yüksek anahtar boyutu ve fazla döngü sayısı) daha güçlü şifreler üretilebilir. Ancak bu şifrelerin üretilmesi daha uzun zaman alabilir.

Bu algoritmaların ve standartların haricinde de birçok simetrik şifreleme algoritmaları bulunmaktadır.

8.2.2 Asimetrik Şifreleme

Asimetrik şifreleme algoritmalarda, verileri şifrelemek ve şifreyi çözmek için farklı anahtarlar kullanır. Önceden paylaşılan bir anahtara sahip olmak zorunda kalmadan güvenli mesajlaşma sağlanabilir. Çok uzun anahtarlar kullanıldığından sistem kaynaklarını yoğun olarak harcarlar ve bu nedenle simetrik anahtarlamaya göre yavaştırlar.



Şekil 8.6. Asimetrik şifreleme.

Asimetrik anahtarlamada şifreleme ve şifre çözme için iki farklı anahtar kullanılır. Public (Açık ya da Genel) anahtar şifreleme için kullanıldıysa, şifre çözmek için Private (Gizli ya da Özel) anahtar kullanılır. Bu durumun tersi de geçerlidir. Yani şifreleme için Private anahtar kullanıldıysa, şifre çözmek için Public anahtar kullanılabilir.

Gönderici ve alıcının birbirlerini tanımadığı durumlarda kullanılan bir şifreleme türüdür. İki farklı anahtar kullanılır. Yukarıdaki örnekte alıcı cihaz, açık anahtarını isteyen herkes ile paylaşır. Ancak gizli anahtarını sadece kendisinde güvenli olarak saklar. Veriyi göndermek isteyen sistemler bu açık anahtarı kullanarak mesajı şifreler. Açık anahtar şifreleme için kullanılabildiği, şifreyi çözmek için kullanılamadığı için açık anahtara sahip diğer kullanıcılar göndericinin şifreli mesajınız çözemez. Gizli anahtara sahip alıcı cihaz kendisine gelen mesajı bu anahtarı kullanarak çözer.

VPN yapısında kullanılan IKE, güvenli cihaz bağlantısı için kullanılan SSH, güvenli web iletişiminde kullanılan SSL ve gizli anahtar paylaşımı için kullanılan Diffie-Hellmann asimetrik anahtarlama (asimetrik şifreleme) kullanır.

Asimetrik anahtarlama türünde kullanılan anahtarlar (genelde 512 ile 2048 bit arasında) uzundur. Güvenli olarak farzedilebilmesi için en az 1024-bit olması önerilir.

Asimetrik anahtarlama, simetrik olana göre daha fazla kaynak tükettiği ve yavaş olduğu için genellikle ağ iletişiminde hareket halindeki veriyi şifreleme için kullanılmazlar. Daha çok kimlik doğrulama işlemlerinde ve anahtar paylaşımında kullanılırlar. Aşağıda asimetrik anahtarlama kullanan bazı standartlar gösterilmiştir.

Dijital İmza Algoritması (DSA) : Açık ve Özel anahtar çiftleri oluşturmak, dijital imzalar oluşturmak ve doğrulamak için geliştirilen orijinal standarttır.

Rivest-Shamir Adelman Algoritması (RSA) : RSA, dijital imzaları oluşturmak ve doğrulamak için yaygın olarak kullanılan asimetrik bir algoritmadır.

Eliptik Eğri Dijital İmza Algoritması (ECDSA) - ECDSA, DSA'nın daha yeni bir çeşididir ve hesaplama verimliliği, küçük imza boyutları ve minimum bant genişliği avantajlarıyla dijital imza kimlik doğrulaması ve inkâr edememe sağlar.

8.3 ÖZETLEME ALGORİTMALARI

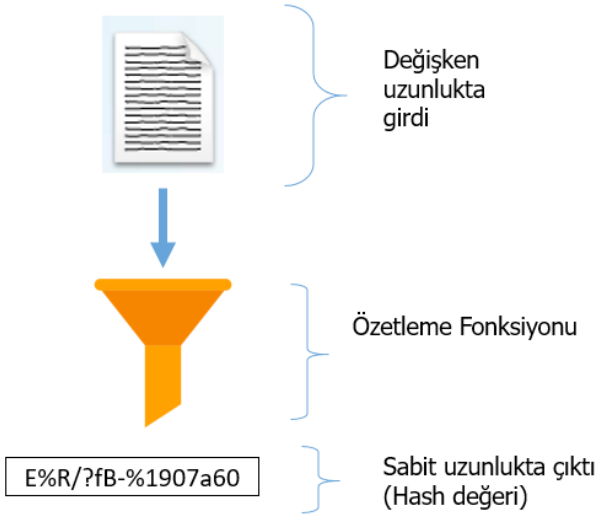
Daha önce ele alındığı gibi, iletişimin güvenliğinin sağlanmasında şifrelemenin yanı sıra veri bütünlüğünün de dikkate alınması gerekir. Bu amaçla kullanılan algoritmalara özetleme (hashing) algoritmaları denir. Hashing ifadesi için bazı kaynaklarda sağlama ya da karma ifadesi de kullanılır.

Özetleme algoritmalar tek yönlü matematiksel fonksiyonlar kullanılarak geliştirilmiştir. Bunun anlamı fonksiyonun tersinin olmamasıdır. Yani özetlenmiş bir veriden tekrar orijinal veri elde edilemez. En basit haliyle ve basitleştirilmiş olarak tek yönlü fonksiyon için şu örnek verilebilir:

Özetlenecek Veri : 1453

Özetleme Fonksiyonu : Rakamları tek basamak elde edinceye kadar toplama işlemi olsun.

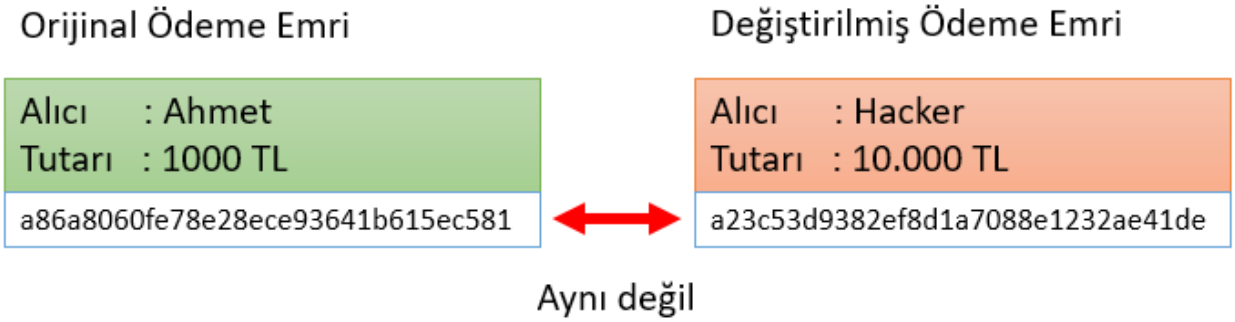
Bu durumda 1453 sayısı fonksiyona girdiğinde 1+4+5+3 → 13 →1+3 → 4 elde edilecektir. Bu basit fonksiyon için "4" sayısı özet (hash) değeridir. 1453 sayısından 4 özet değeri elde edilebilir ancak tersi geçerli değildir.



Şekil 8.7. Özetleme (hash) fonksiyonları

Özetleme fonksiyonlarında girdi olarak herhangi uzunlukta veriler kullanılabilir ancak çıktı her zaman sabit uzunluğuktadır. Bu durum, girdinin sonsuz ihtimalli olduğu, çıktının da sınırlı olduğu anlamına gelir. Boyutu ne olursa solun her girdi için sabit uzunlukta bir çıktı var olduğundan, teorik olarak aynı çıktıyı veren iki farklı girdi bulunabilir. Bu durum matematiksel olarak birebir ve örten bir fonksiyon olmadığı, dolayısıyla tersinin olmadığı ve hâliyle şifreleme / şifre çözmede kullanılamayacağı anlamını taşır. Özetleme algoritmasının gücü, aynı çıktıyı veren iki farklı girdinin oluşma olasılığının düşük olması ile ilgilidir.

VPN gibi güvenli iletişimlerde, verinin değiştirilmediğini yani veri bütünlüğü için özetleme algoritması kullanılır. Şekil 8.8'de gösterildiği gibi, veri transferi sırasında yetkisiz kişiler tarafından değiştirilmiş bir verinin özet değeri de farklı olacaktır.



Şekil 8.8. Özetleme değerleri karşılaştırılarak bütünlük control edilir.

Gönderilen mesaja özet bilgisi eklenerek, veri bütünlüğü sağlanabilir. Şekil 8.8'deki örnekte, orijinal mesaj metninin şifrelenmesi (confidentiality) ve özet bilgisinin de eklenmesi (integrity) iletişimi daha güvenli kılacaktır.

Veri iletişiminde, Ethernet çerçevelerinde kullanılan CRC algoritması bir özetleme fonksiyonudur. Bunun haricinde MD5 ve SHA en yaygın kullanılan iki özetleme fonksiyonudur.

8.3.1 MD5

Ron Rivest tarafından geliştirilen ve günümüzde çeşitli İnternet uygulamalarında kullanılan bir özetleme algoritmasıdır. MD5, giriş verileri üzerinde gerçekleştirilen ve her zaman 128-bitlik sabit bir hash mesaj özeti üreten, XOR işlemi ve çeşitli dönüşümler uygulayan ikili işlemler dizisidir.

MD5 algoritması verilen aynı girdi için her zaman aynı çıktıyı ürettiğinden, kullanıcılar kaynak dosyanın bir karmasını hedef dosyanın yeni oluşturulmuş bir karması ile karşılaştırarak sağlam ve değiştirilmemiş olduğunu kontrol edebilir. Genellikle veritabanına erişmek için kullanılan parolaları şifrelemek için kullanılır.

Web tarayıcı üzerinde http://www.md5.cz/ sitesi ile MD5 özetleme yapılabilir. Bu işlem için birçok web sistesi bulunmaktadır [34-36].

- https://passwordsgenerator.net/
- https://emn178.github.io/online-tools/sha256.html

siteleri de yine bu amaç için kullanılabilir.

8.3.2 SHA

MD5'e göre daha güvenli olan SHA'nın birkaç sürümü vardır. SHA-1 algoritması, uzunluğu 264 bitten az olan bir mesajı girdi olarak alır ve 160-bitlik bir mesaj özeti üretir. Algoritma, MD5'ten biraz daha yavaştır, ancak daha büyük mesaj özeti sayesinde kaba kuvvet saldırılarına ve ters çevirme saldırılarına karşı daha güvenlidir [37-38].

Özetleme fonksiyonları birçok farklı alanda kullanılabilir. Özellikle parola gibi hassas verilerin veritabanlarında kaydedilirken özetlenerek kaydedilmesi gerekir. Bu sayede olası bir veritabanı ihlalinde, kullanıcıların parola bilgilerinin açığa çıkması önlenmiş olur. Özetleme fonksiyonları her ne kadar tersine bir işlem ile çalışmasa da, çeşitli yöntemler kullanılarak özet değerinden orijinal verinin elde edilmesi mümkündür. Bunun en bariz örneği, veritabanına her iki değerin kaydedilmesi ile sağlanabilir.

Password	MD5Hash
Parolam	dff5ac25d959cf728db0501b2b7a8e8b
Ankara06	6953d5f4e68e7668554cb036995e1591
GizliParolam	246774bda931d479355ed5d35d2a0439
Qwerty	d8578edf8458ce06fbc5bb76a58c5ca4

Örnek olarak şekildeki gibi bir tablo daha önce oluşturulmuş olsun. Açıkça belli ki, bu tabloda yer alan parolaların deneme yanılma yoluyla üretilmesi zaman alıcıdır. Bu nedenle saldırganlar, sözlükler ya da yaygın kullanılan parola listeleri ile böyle bir tablo oluşturabilirler. Bu nedenle parola kullanımında sözlükte geçen kelimeleri ve yaygın kullanılan parolaları kullanmamak gerekir. Bu kısımda dikkat edilecek diğer bir husus da, böyle bir veritabanına sözlükte yer almayan kendi parolamızı dikkatsizce kaydetmememizdir. Bazı güvenilir olmayan web sayfalarında *"parolanızın ne kadar güçlü olduğunu ölçün"* uygulamaları bu konuda kötü amaçlı olarak, özet toplamak amacıyla kullanılabilir.

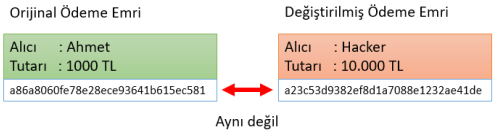
Özetleme algoritmalarının diğer bir kullanım yeri de, indirilen bir dosyanın ya da bir programın orijinal olup olmadığının teyididir. Yine çalışan bir uygulamanın zararlı yazılım barındırıp barındırmadığına (daha doğrusu değiştirilip değiştirilmediğine) bakılabilir. Örnek uygulama alanı için kitabın 6.bölümündeki uygulamaya göz atınız.

8.3.3 Salting İşlemi

Önceki kısımlarda ele alındığı üzere, parolalar veritabanına kaydedilirken genellikle özetlenerek kaydedilir. Ancak ister md5 olsun ister sha olsun, özetleme fonksiyonlarının algoritmaları bilindiğinden, veritabanı ele geçirilmişse *rainbow table* attack saldırıları ile parolaların ham haline ulaşılabilir. Ayrıca farklı kullanıcı aynı parolayı kullanmışsa, hash değerleri de aynı olacağından birden fazla kullanıcının da bilgisi bu sayede ele geçirilebilir. Bu nedenle hem standart özet fonksiyonunu manipüle etmek hem de raibnow saldırılarından korunmak için, özetleme fonksiyonlarına *"salt"* olarak ifade edilen karakterlerin eklenmesi yararlı bir uygulamadır [33].

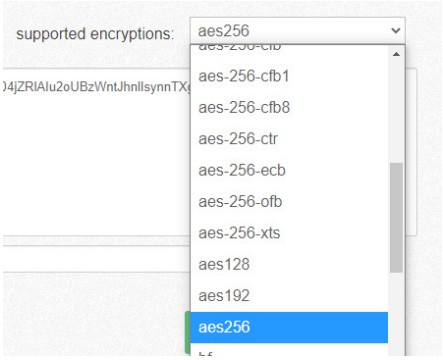
8.4 ÖRNEK UYGULAMALAR

Online ortamda birçok özetleme hesaplama aracı bulunmaktadır. Aşağıdaki ekran görüntülerinde "Siber Güvenlik" cümlesinin sırasıyla md5 ve sha özetleri için ekran görüntüleri yer almaktadır.



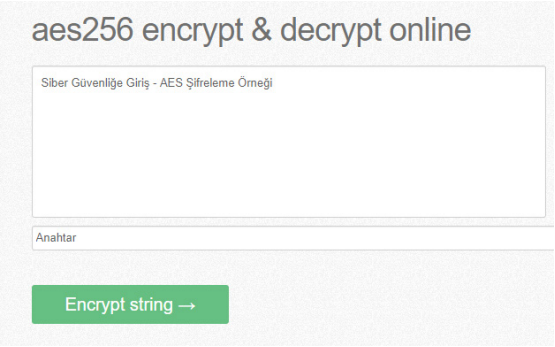
Şifreleme algoritmaları üzerinde online uygulama yapmak için https://encode-decode.com/aes256-encrypt-online/ web sayfası kullanılabilir. Sayfada sağ üstte yer alan şifreleme türü alanında birçok algoritma görüntülenmektedir.

Şekil 8.9. md5 ve sha değerleri için online karşılaştırma



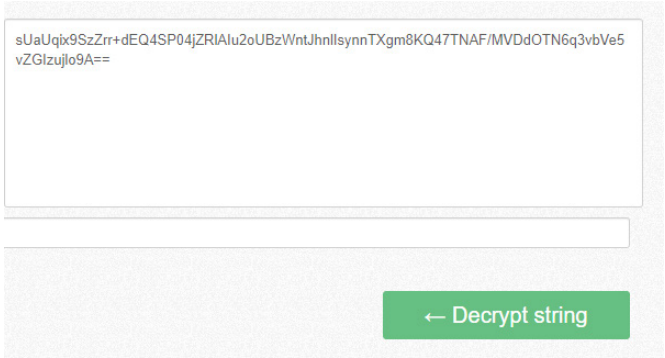
Şekil 8.10. Çeşitli online sayfalarda farklı şifrelemeler yer alır

Şekil 8.11'de yer alan ekran görüntüsünde "Siber Güvenliğe Giriş – AES Şifreleme Örneği" cümlesi "Anahtar" kelimesi kullanılarak şifrelenmiştir.



Şekil 8.11. AES şifreleme örneği

Şifreleme sonunudaki elde edilen şifreli mesaj (ciphertext) Şekil 8.12'de gösterilmiştir.



Şekil 8.12. Şifreli metnin çözümlenmesi

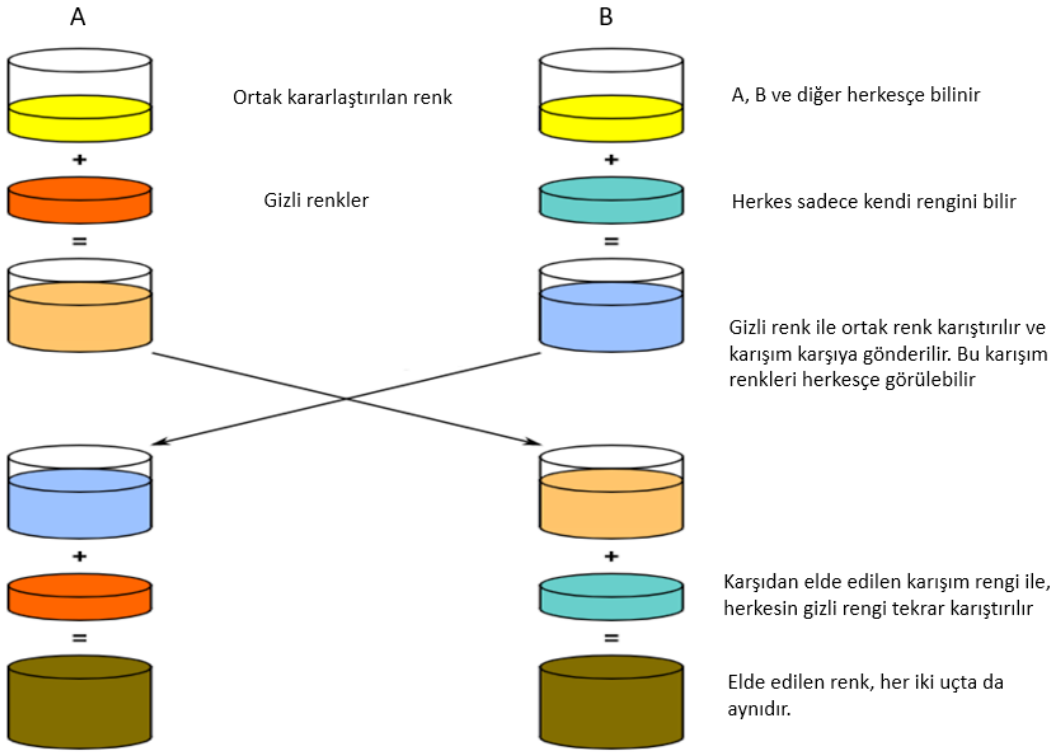
Şifreleme yaparaken kullanılan aynı anahtarı kullanmak kaydıyla "Decrypt string" düğmesine basılarak şifre çözme işlemi yapılabilir. Kitabın 10.bölümünde yer alan python kodları kullanılarak da şifreleme ve şifre çözme örneklerini yapabilirsiniz.

8.5 DİĞER ALGORİTMALAR VE TEKNİKLER

Siber güvenlik kapsamında ele alınacak birçok protokol ve teknik bulunmaktadır. Bu tekniklerde biri Diffie-Hellman Anahtar değişimi diğeri de IPSec mimarisidir.

Diffie-Hellman (DH) Anahtar Değişimi: İnternet ortamında verilerin şifrelenmesinde ve şifrenin çözülmesinde ortak (gizli) anahtarın varlığı gereklidir. Ancak en büyük sorunlardan biri, herkese açık güvensiz bir ortamdan bu anahtarın güvenli bir şekilde nasıl paylaşılacağıdır. DH, bu işlem için geliştirilmiş asimetrik anahtarlama kullanan bir tekniktir.

A ve B ortak gizli anahtar oluşturmak üzere iletişim kuran iki cihaz olsun. *Kriptoloji üzerinde yazılan makalelerde bu kişiler genellikle Alice ve Bob olarak adlandırılır.* Bu durumda A ve B için ortak anahtar oluşturma, aşağıdaki analoji ile ifade edilmiştir.



Şekil 8.13. Diffie-Hellmann anahtar değişim adımlarının renklerle ifadesi

DH işlemini matematiksel olarak basitleştirilmiş bir şekilde ifade etmek gerekirse :

1- **Ali ve Beyza** ortak bir asal sayı **(P)** ve ortak bir kök sayı **(g)** üzerinde anlaşırlar. Her iki değer de açıkça bilinir.

2- Ali ve Beyza birer gizli sayı belirlerler.

- Ali'nin gizli sayısı **a**
- Beyza'nın gizli sayısı **b** olsun

3- Ali ve Beyza, gizli sayılarını, ortak asal sayıyı (P) ve kök sayı (g) kullanarak yeni bir sayı hesaplar. Hesaplanan sayı Ali için **"A"**; Beyza için **"B"** olsun.

$$A = g^a \bmod P$$

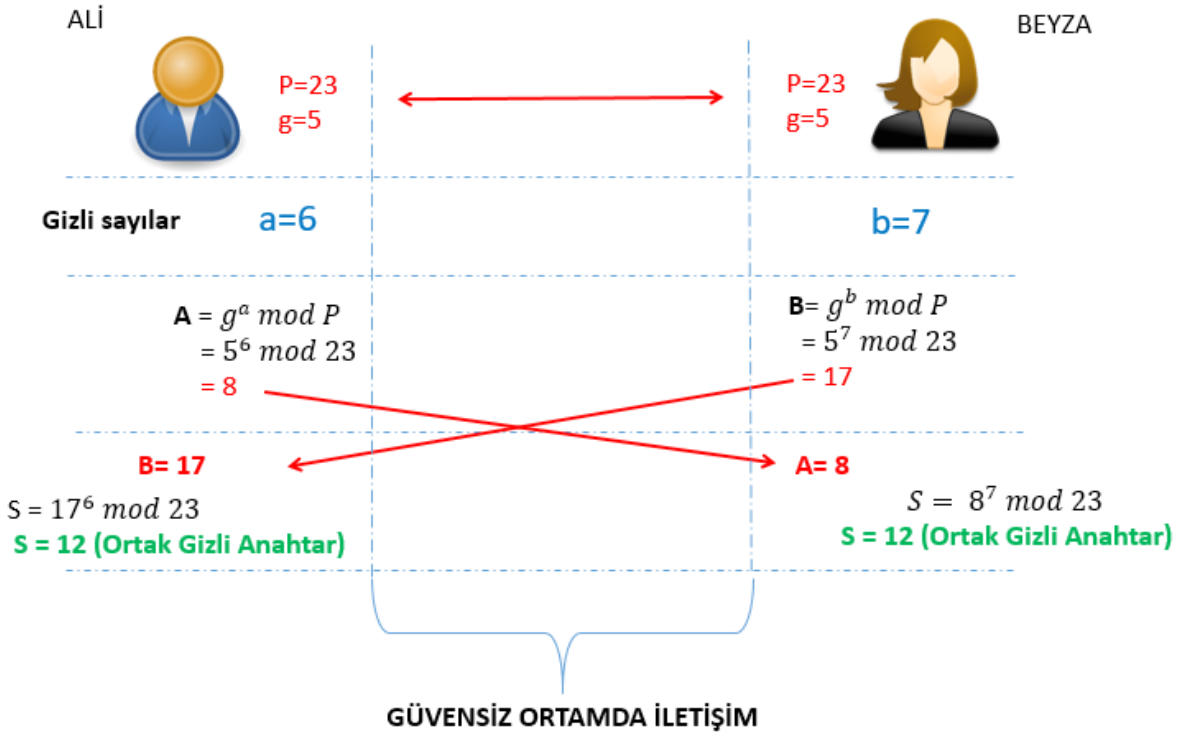
$$B = g^b \bmod P$$

4- Ali hesaplanan A değerini Beyza'ya; Beyza da hesaplanan B değerini Ali'ye gönderir.

5- Ali'nin elinde gizli sayısı "a", "B", g ve P vardır. Beyza'da gizli sayı "b", "A", g ve P vardır. Her iki tarafta elindeki bilgilere göre Sx sayısını hesaplar.

- Ali $S_a = B^a \bmod P$ hesaplar
- Beyza $S_b = A^b \bmod P$ hesaplar

6- Hesaplanan değerler Sa ve Sb birbirine eşittir ve ortak anahtardır.

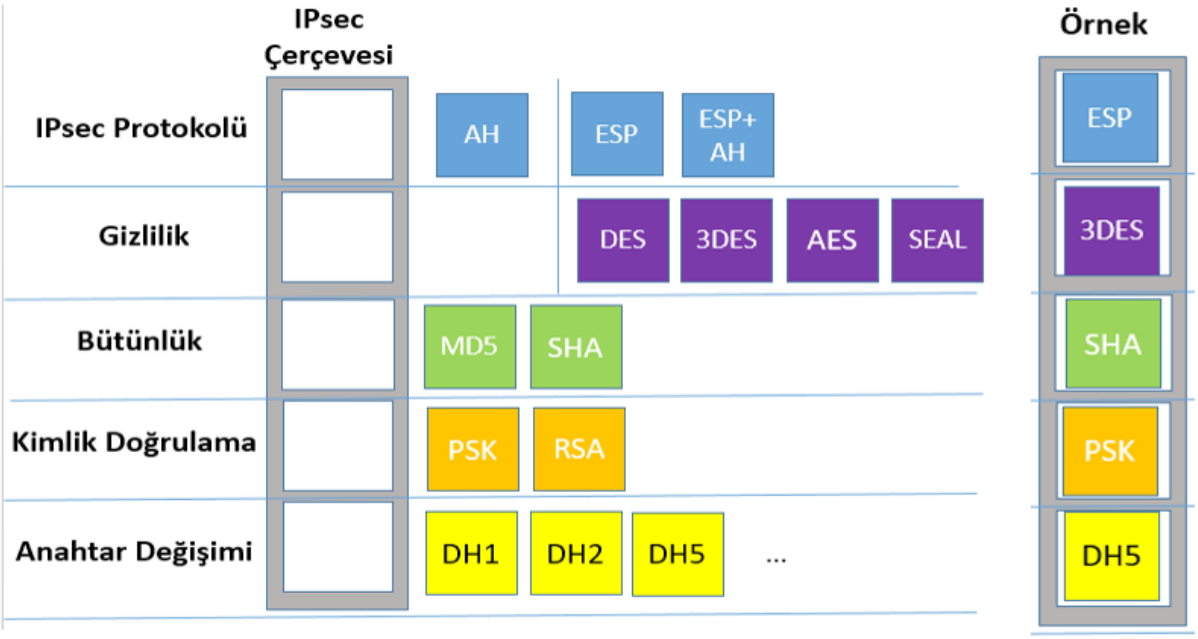


Şekil 8.14. Diffie-Hellmann anahtar değişim adımları.

Yukarıdaki şekilde, Ali ve Beyza için adımlar sayılar ile ifade edilmiştir. Şekilde kırmızı renkle görünen bilgiler, güvensiz ortamda hareket eden, dolayısıyla herkesçe bilinmesi mümkün olabilen değerlerdir. Mavi renkle ifade edilen bilgiler ise, ağda transfer edilmeyen gizli bilgilerdir. Görüleceği üzere, güvensiz ortamda DH algoritması kullanılarak ortak anahtarın güvenli olarak belirlenmesi mümkün olabilmektedir.

IPSec: Internet Protokolü doğası gereği güvenli bir protokol değildir. Yani şifreleme ve veri bütünlüğü gibi özellikleri barındırmaz. IPSec, IP'nin güvenliğini sağlayan bir çerçevedir. Bu sayede kaynak ile hedef arasında 4.katman – 7.katman arasındaki protokollerin gizliliği ve bütünlüğü sağlanabilir. IPsec aşağıdaki temel güvenlik fonksiyonlarını sağlar:

- Şifreleme kullanarak Gizlilik
- Hash (özet) algoritmaları kullanarak Bütünlük
- İnternet Anahtar Değişimi (IKE) kullanarak Kimlik Doğrulama
- Diffie-Hellman (DH) algoritmasını kullanarak güvenli Anahtar Değişimi



Şekil 8.15. IPsec mimarisi ve teknolojileri

IPsec çerçevesi esnek bir yapıdadır. Yani mevcut IPsec standartlarını güncellemeden yeni güvenlik teknolojilerini kolayca entegre edilebilmesini sağlar. IPsec, sanal özel bağlantı (VPN) yapısında kullanılır.

Siber Güvenlik

Siber Güvenlik

BÖLÜM 9

SİBER GÜVENLİK ve BİLİŞİM HUKUKU

9.1 BİLİŞİM HUKUKU TANIMI

Bilişim Hukuku, teknolojik gelişmeler çerçevesinde teknik, ekonomik ve toplumsal alanlarda kullanılan bilginin elektronik cihazlar aracılığı ile toplanması, işlenmesi, saklanması ve korunması ile bunlardan doğan ihtilafların çözümü ile ilgilenen hukuk dalıdır.

Bilgi teknolojileri ve iletişim alanındaki yaşanan sürekli gelişmeler "bilişim" kavramını ortaya çıkarmıştır. Bilişim kullanılarak; terör faaliyetleri, fikri mülkiyet sorunları, dolandırıcılık, çocuk istismarı, siber zorbalık gibi birçok yasal sorun nedeni ile bu alanın doğmasına neden olmuştur. Ülkemizde bilişim sektörü ile ilgili hukuki zemin yeni doğan ihtiyaçlar doğrultusunda düzenlenmeye devam etmektedir.

9.2 KİŞİSEL VERİLERİ KORUMA KANUNU

Ülkemizde anayasada öngörülen özel hayatın gizliliği ile ilgili temel hak ve özgürlüklerin korunması kapsamında, kişisel verilerin korunmasını sağlamak, farkındalık yaratmak, veri temelli ekonomide rekabet ortamını korumak, bunlara ilişkin vatandaşlık bilincinin oluşmasını sağlamak adına Türkiye Büyük Millet Meclisinde 24 Mart 2016 tarihinde 6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK) kabul edilmiştir.

Kimliği belli veya belirlenebilir gerçek kişi ile ilişkili her türlü veriye kişisel veri denmektedir. En basit hali ile ad, soyad, eposta, telefon, TC Kimlik numarası gibi veriler tek bir kişi ile ilişkili olduğundan kişisel veri olarak nitelendirilmektedir. Bir şirkete ait ünvan ya da adres gibi bilgiler tüzel kişiliğe ait olduğundan kişisel veri kapsamında girmemektedir. Kişisel Verileri Koruma Kurulu; kişisel verilerin elde edilme yöntemleri, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleşebilecek her türlü işlemin denetiminden sorumludur.

KVKK kapsamında herhangi bir kurumca toplanan kişisel verilerin işlenmesi, paylaşılması veya benzeri durumlar için aydınlatma yükümlülüğü maddesi uyarınca bilgi verilmesini zorunlu kılmaktadır.

Bu kapsamda kişisel veri içeren tüm bilgi teknolojisi sistemlerinin internet üzerinden oluşabilecek her türlü izinsiz erişim tehdidine karşı korunmasını zorunlu hale getirilmiştir. Bu verileri

korumak için alınacak tedbirler arasında en önemlilerinden biri güvenlik duvarı kullanılmasıdır. Ayrıca bu tür bilgi sistemlerine erişim kayıt altına alınmalı, sınırlandırılmalı ve yetkilerle belirlenmiş olmalıdır.

Aynı zamanda son dönemde sıkça bahsedilen sosyal medya platformlarının veri sorumlusu olarak ülkemizde yerleşik olan bir tüzel kişi veya Türk vatandaşı bir gerçek kişi atama zorunluluğu KVKK kapsamında ortaya çıkmıştır. Ayrıca kişisel bilgilerin saklandığı sunucuların fiziki olarak da ülkemizde bulundurulması eğer bu bilgiler yurtdışına çıkarılacaksa bilgi sahibi olan kişilerin açık rızasının bulunması zorunluluğu vardır.

KVKK uyarınca kişisel veri ihlali bulunuyorsa http://www.kvkk.gov.tr adresinde bulunan Kişisel Veri İhlal Bildirimi bölümünden şikâyet ve ihbar başvuruları yapılmaktadır.

9.3 YASAL MEVZUAT

Bilişim güvenliği süreçlerinin halen yürürlükte olan yasal mevzuatlar ile uyumlu olması gerekmektedir. Internet'in ülkemizde ilk kullanılmaya başlandığı dönemde bilişim süreçleri ile yasal süreçlerin uyumu geç bir zaman aralığında sağlanırken günümüzde bu süre epey kısaldı. Şu an yürürlükte olan yasal mevzuatlardan en önemlilere bir göz atabiliriz;

- Türkiye Cumhuriyeti Anayasası: Ülkemizde bütün yasal düzenlemeler için olduğu gibi Bilişim Hukuku'da Türkiye Cumhuriyeti Anayasasına dayanmaktadır. Özellikle anayasadaki 19. maddede tanımlanan kişi hürriyeti ve güvenliği, 20. maddede belirtilen özel hayatın gizliliği, 22. maddede belirtilen haberleşme hürriyeti konuları bilişim güvenliği ve bununla ilgili suçlarda dikkate alınması gereken yükümlülükleri tanımlamaktadır.
- 5237 Sayılı Türk Ceza Kanunu: Ceza hukukundaki yeni ve demokratik gelişmelere yer vermek ve toplumsal ihtiyaçları gidermek amacı ile 26 Eylül 2004 tarihinde TBMM'ce kabul edilen 5237 sayılı Türk Ceza Kanunu, 12 Ekim 2004 tarihli 25611 sayılı Resmi Gazete'de yayınlanmıştır. Bilişim Suçları, TCK'nın Topluma Karşı Suçlar'a ilişkin üçüncü kısmının Bilişim Alanında Suçlar başlığında yer almaktadır. Ayrıca TCK'nın Kişilere Karşı Suçlar kısmının dokuzuncu bölümünde Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar bölümünde de yer almaktadır. TCK'da yer alan başlıklar şöyledir;

- Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalmaya devam etme (md.243)
- Bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme (md.244)
- Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama (md.244)
- Banka veya kredi kartlarının kötüye kullanılması (md.245)
- Haberleşmenin engellenmesi (md.124)
- Haberleşmenin gizliliğini ihlal (md.132)
- Kişiler arasındaki konuşmanın dinlenmesi ve kayda alınması (md.133)
- Özel hayatın gizliliğini ihlal (md.134)
- Kişisel verilerin kaydedilmesi (md.135)
- Kişisel verileri hukuka aykırı olarak verme veya ele geçirme (md.136)
- Kişisel verilerin yok edilmemesi (md.138)
- Göreve ilişkin sırrın açıklanması (md.258)

Ayrıca bunlar dışında bilişim ve iletişim araçları ile işlenmiş dolandırıcılık, hırsızlık, hakaret, suç işlemek için örgüt kurma gibi suçlar da TCK kapsamında değerlendirilir.

- 5809 Sayılı Elektronik Haberleşme Kanunu: Bu kanun ile elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin sağlanması, tüketici haklarının korunması, bu hizmetlerin ülke geneline yaygınlaştırılması, haberleşme alanındaki teknolojik gelişmenin sağlanması ve bu alanlarda yatırımların teşvik edilmesi ile ilgili usul ve esasları belirler.
- 5651 Sayılı Kanun: Internet yer alan web sitesi ve benzeri hizmetler için içerik ve yer sağlayıcı, İnternet erişimi sağlayıcı ve iş yeri gibi toplu internet kullanımının olduğu toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarını ile internet ortamında belirli suçlara yönelik içerik, yer ve erişim sağlayıcıları ilişkin usul ve esasları düzenler. Buna göre Türk Ceza Kanununda yer alan intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde

temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama ve Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar bu kapsamda değerlendirilir. Bunlar gibi suçlar için www.ihbarweb.org.tr adresinden şikâyet gerçekleştirilebilmektedir.

- 5846 Sayılı Fikir ve Sanat Eserleri Kanunu: 5 Aralık 1951 tarihinde yürürlüğe giren Fikir ve Sanat Eserleri Kanunu ile estetik değere sahip olan güzel sanatlar eserleri kapsamaktadır. Bilişim alanına girmesi, bu sanat eserlerinin İnternet üzerinden dijital olarak paylaşımının, çoğaltılmasının, yayılmasının, türevlerinin üretilmesinin kolaylaşmış olmasıdır. Bu nedenle FSEK kapsamındaki problemler yaygınlaşmaktadır. Kullanıcılar olarak içerik üretebilir, paylaşabiliriz ancak bunlarla ilgili hak ve sorumluluklarımızın bilincinde olmak yasal zorunluluktur. Konu ile ilgili daha ayrıntılı bilgi almak için www.telifhaklari.gov.tr adresine göz atabilirsiniz.

  Bunlar dışında birçok kanun ve yönetmelikler bilişim alanındaki hak, sorumluluk ve suçları düzenlemektedir. Ancak unutulmaması gereken önemli noktalardan biri bilişim suçları hukuken çok yeni ve sürekli gelişmekte olsa da bilişim suçluları bazen bir adım önde olabilmektedir. Ama bir suçun bilişim araçları ile işlenmiş olması suç olmadığı anlamına gelmez.

Kullandığımız dijital platformlar, bilişim araçları, iletişim sistemleri ve hukuk alanlarında güvenliğimizin sağlanması için her gün geliştirilmeye devam edilmektedir. Bizlerin ödevi temel güvenliğimizi sağlamak, hak ve sorumluluklarımız hakkında bilgi sahibi olmaktır.

9.4 SİBER GÜVENLİK KURULU

Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri, bununla ilgili plan, program, rapor, usul, esas ve standartları belirlemek için kurulmuştur. Siber güvenlik kurulunun görevleri;

- Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik kararlar almak,
- Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak,
- Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek,
- Kanunlarla verilen diğer görevleri yapmak.

Siber Güvenlik Kurulu; Ulaştırma, Denizcilik ve Haberleşme Bakanı başkanlığında, Dışişleri Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Milli Savunma Bakanlığı Müsteşarı, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Mali Suçlar Araştırma Kurulu Başkanı ve Telekomünikasyon iletişim Başkanı yöneticilerinden oluşmaktadır.

9.5 ULUSAL SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANI

29 Aralık 2020 tarih ve 31349 sayılı Resmi Gazetede Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) yayımlandı. Daha önce 2013-2014 ve 2016-2019 dönemlerini kapsayan eylem planları çerçevesinde yürütülen çalışmalarının kapsamının genişletilerek devam edeceği belirtilmiştir. 2013-2014 eylem planında Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) kurulmuş olup siber ortamlarda ortaya çıkacak tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi hedeflenmektedir.

Eylem Planı kapsamında siber tehditlerin etkilerinin azaltılması öncelikli hedeftir. Ulusal seviyede gerekli önlemlerin alınması ve güvenli bir siber ortamın oluşturulmasının amaçlandığı planda, ülkenin siber güvenlik alanında mevcut durumunu daha da ileriye taşıyarak uluslararası

9.6 ISO 27001

ISO 27001 Bilgi Güvenliği Yönetim Sistemi, kurumsal bilgi güvenliğinin sağlanmasında insanları, süreçleri ve bilgi sistemlerini içine alan bir yönetim sistemidir. Bilgi bir kurumun en önemli varlıkları arasında yer almakta ve korunması ile ilgili standartların oluşması, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, işlemleri ve kaynakları planlamakta önem arz etmektedir.

Bilgi güvenliğinin teknik önlemlerle ve iş sürekliliğinin sağlanması ile mümkün olmadığı günümüzde açıkça görülmektedir. Kişisel anlamda yaşanan kayıpların bile insanları zor durumda bıraktığını düşünürsek bunun kurumsal bir firma için felaket olabileceği ortadadır. Bu nedenle ISO 27001 ile bilgi yönetim ve koruma süreçleri bir standart haline getirilmektedir. Kurumda görevli en alt kademe çalışandan üst düzey yöneticiye kadar herkesin içinde bulunacağı bu standart ile bilgi güvenliği en üst düzeyde sağlanmaya çalışılmaktadır.

9.6.1 ISO 27001 Faydaları

- Doğru, güvenilir ve geçerli bilgiler sağlar
- Zaman kaybını önler
- Kurumun bilgiden kaynaklı risklerini en aza indirir
- Sürekliliği sağlar
- Bilgi varlıklarının gizliliğini sağlar
- Bilgi zafiyetleri ile ilgili farkındalık sağlar
- Bilgiye erişim metotlarını belirler
- Yasal zorunluluğu sağlar
- Kurumsal saygınlık sağlar

9.7 SİBER GÜVENLİKTE KARİYER

Günümüzde Internet'e bağlı cihaz sayısı 50 milyar civarındadır. Bunların tümü bilgisayar değil tabi ki; akıllı telefonlardan, tabletlere, akıllı ev sistemlerinden, güvenlik sistemlerine birçok elektronik cihaz internete bağlanmaktadır. 2025 yılında bu sayının 80 milyar civarında olması beklenmektedir. Bu cihazların yönetilmesi ve güvenliğinin sağlanması çok önemlidir. Bu nedenle siber güvenlik ve ağ uzmanlıkları çok daha önemli hale gelmiştir.

Geçtiğimiz yıllarda gerçekleştirilen büyük bir DDoS saldırısının belirli bir marka akıllı ev sistemindeki açıktan dolayı bu sistemler üzerinden gerçekleşmesi konunun sadece kurumsal anlamda değil herkesi ilgilendiren bir konu olduğunu ortaya koymaktadır. Çok yeni bir alan olmasa da internetin hayatımıza daha fazla girdiği şu dönemlerde Siber Güvenlik Uzmanlığı büyük önem taşımaktadır. Ülkemizde elli bin üzerinde siber güvenlik uzmanına ihtiyaç bulunmaktadır. Bu rakama ağ uzmanlığını da eklediğimizde sayı yüzbinin üzerine çıkmaktadır. En küçük işletmelerde tutun kurumsal yapıdaki büyük firmalara veya kamu kurumlarına kadar her işletmede ve her sektörde siber güvenlik uzmanı ihtiyacı bulunmaktadır. Bankalar, telekomünikasyon firmaları, e-ticaret platformları, sosyal ağlar gibi günlük hayatta çok sık kullandığımız araçların güvenliğini sağlamak için siber güvenlik uzmanı ihtiyacı her geçen gün artmaktadır.

Ülkemizde üniversiteler bünyesinde eğitim ve araştırma merkezleri kurulmakta aynı zamanda birçok özel kurumda Siber Güvenlik Uzmanlığı eğitimleri verilmektedir. Ancak unutulmamalıdır ki günümüzde alışverişten, iletişime, eğitime birçok alanda kullandığımız internet konusunda güvenliğimizi sağlamak için temel siber güvenlik bilgisine tüm kullanıcıların sahip olması gerekmektedir.

BÖLÜM 10

PYTHON ile SİBER GÜVENLİK UYGULAMALARI

Python programlama dili okunması ve algılanması kolay, açık kaynak kod etkisiyle oldukça geniş kütüphane zenginliğine sahip bir programlama dilidir. Python bu geniş kütüphane zenginliği sayesinde siber güvenlik alanındaki uygulamalarda da yer edinmiştir.

Geçtiğimiz on yıl içerisinde artan bir ivmeyle programlamaya yeni başlamış kişilerden profesyonel yazılımcılara kadar geniş bir kitlenin ilgisini çekmiş ve en popüler programlama dilleri arasında yerini almıştır. Siber güvenlik alanıyla ilgili olan ya da bu alanda çalışan birisi için programlama ile ilgili yeteneğini arttırabilmek için böylesine kolay anlaşılır bir programlama diline olan ilginin artmasının kaçınılmaz olduğu düşünülebilir. Bunun yanında siber güvenlik alanında kullanılan cihazların ve yazılımların program geliştirme ara yüzlerinde tercih ettikleri programlama dili de Python'dır.

Birden fazla siber güvenlik yazılım ve hizmet sağlayıcılarının yayımladıkları raporlar incelendiğinde web sitelerine yapılan atakların %70 - % 80 arasında Python tabanlı yazılmış araçlar aracılığıyla yapıldığı belirtilmektedir.

Bu bölümde kitap içerisinde ele alınan, veri toplama, IP tabanlı sorgulama, şifreleme gibi konulara ilişkin Python kod örnekleri verilmiştir.

10.1 SOKET PROGRAMLAMA

Soket programlama bir ağdaki iki düğümün birbiriyle iletişim kurmasını sağlamanın bir yoludur. Bir soket IP'deki belirli bir bağlantı noktasını dinlerken diğer soket bağlantı oluşturmak için diğerine ulaşır. Örneğin herhangi bir istemci sunucuya erişirken dinleyici soketini oluşturur. Web omurgasının temelinde soketler bulunmaktadır.

```
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

Yukarıdaki örnekte Python kurulumu ile gömülü (built-in) olarak gelen soket modülü ve bu modül üzerinden bir nesne üretimi görülmektedir. Bu program kodu içerisinde gönderilen iki parametreden AF_INET adresin IPv4 tabanlı olduğunu SOCK_STREAM ise TCP protokolünden bir bağlantı gerçekleşeceğini ifade etmektedir.

```
# istenilen web sitesine socket ile bağlanılması örneği
def SoketIleBaglan(webURL="www.meb.gov.tr"):
    import socket
    import sys
    try:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        print("Başarıyla Soket Nesnesi Oluşturuldu.")
    except socket.error as err:
        print(f"Soket oluşturulması sırasında bir hata oluştu.Hata M
esajı :{err}")
    port = 80 # varsayılan port numarası
    try:
        host_ip = socket.gethostbyname(webURL)
    except socket.gaierror as err:
        print(f"Hata oluştu: {err}")
        sys.exit()
    s.connect((host_ip, port))
    print("soket başarıyla belirlenen adrese bağlandı.")

SoketIleBaglan("www.meb.gov.tr")
```

Yukarıdaki kodu incelediğimizde; soket nesnesinin oluşumu sırasında bir hata olması durumunda socket.error hatasına yönlendirme yapılmaktadır. Fonksiyon içerisinde bağlantı noktası 80 olarak belirlenmiştir.

Konunun daha da pekişmesi açısından bir bilgisayarda sunucu ve istemci rollerini üstlenen iki farklı fonksiyon yazılmıştır. Bir sunucu onu bir IP ve bağlantı noktası numarasıyla bağlı **bind** metoduna sahiptir. Böylece bu IP ve bağlantı noktası üzerinden gelen istekleri dinleyebilir. listen metodu ile bu dinleme işlemlerini gerçekleştirir. **accept** ve **close** metotları ile gelen isteğin kabulü ve gerektiğinde bu istemci üzerinden gelen bu bağlantının kapanma işlemini gerçekleştirir.

```
import socket
s = socket.socket()
port = 3679
s.bind(('', port))
print (f"Soket {port} numaralı portla açıldı")
s.listen(6) # en fazla 6 bağlantı
print ("Soket istemci bekliyor")
while True:
    c, addr = s.accept()
    print (f"{addr} adresinden gelen bağlantı" )
    c.send('Bağlandığın teşekkür ederiz.')
    c.close()
```

Yukarıdaki kod incelendiğinde;

- Soket nesnesi oluşturulmaktadır.
- Ardından mevcut bilgisayarda bir port rezerve edilir. bind metodunun ilk parametresini boş olması sadece bu bilgisayardan değil diğer bilgisayarlardan gelecek isteklerinde kabul edilmesini sağlamaktadır.
- listen fonksiyonu ile gelecek bağlantılar dinlenirken, fonksiyon içerisine yazılmış olan parametre kaç bağlantı kabul edileceğini belirmektedir. Bağlantı sayısının aşılması durumunda fazladan gelen bağlantılar reddedilecektir.
- Tüm işlemlerinde ardından gelen belirlenen sayı doğrultusunda gelen tüm talepleri kabul eden sunucu bir teşekkür mesajının ardından bağlantı kapatılmaktadır.

```
import socket
s = socket.socket()
port = 3679
s.connect(('127.0.0.1', port))
print(s.recv(1024))
s.close()
```

İstemci tarafında yazılan kod incelendiğinde;

- Soket nesnesi oluşturulur.
- Sunucu için IP ve belirlenen bağlantı noktası üzerinden bağlantı gerçekleştirilir.
- Sunucu tarafından gönderilen veriyi almak için recv fonksiyonu ile gelen veri ekrana yazdırılmakta ve bağlantı kapatılmaktadır.

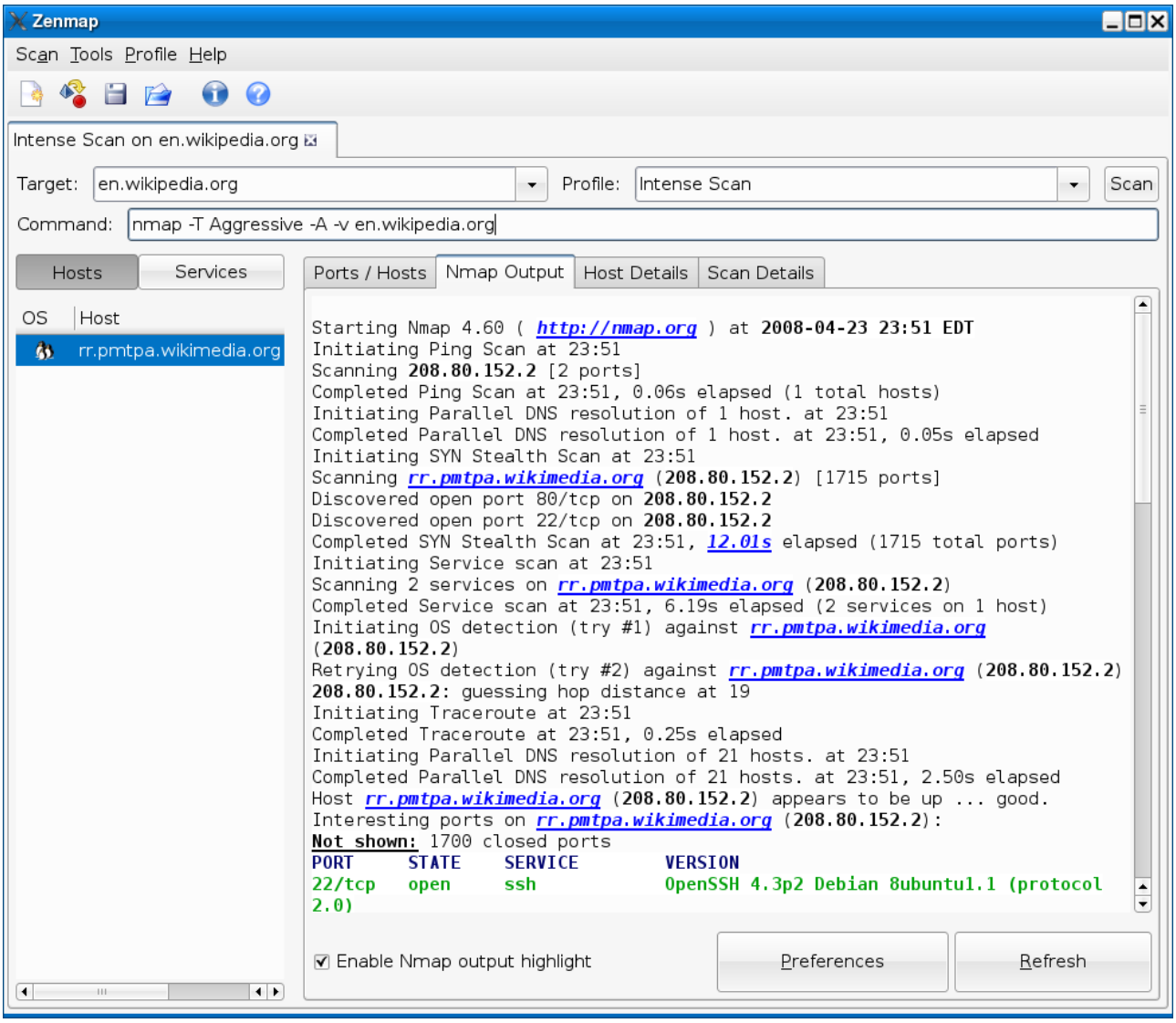
10.2 PYTHON İLE NMAP KULLANIMI

NMap bir bilgisayarın bağlı olduğu ağdaki konakları ve hizmetleri keşfederek bir harita oluşturmak için kullanılan bir güvenlik tarayıcısıdır. Nmap özel tasarlanmış paketleri göndererek aldığı yanıtların analizi sonucunda bu görevi gerçekleştirmektedir.

İster komut satırından ister bir programlama dilini kullanarak nmap ile gönderilen paketlerden alınabilecek cevaplar aşağıda listelenmektedir.

- Ağ üzerindeki ana bilgisayarların tespit edilmesini sağlar, örneğin web sitesi yayımı vb. hizmet veren ve belirli bir portu açık olan konakların listelenmesini sağlamaktadır.
- Sunucuda açık olan bağlantı noktalarını tek tek tarayarak tespit etmekte ve kullanılan işletim sistemini ve yazılım ya da servislerin sürümlerini de tespit etmektedir.
- Kendi içerisinde Lua programlama diliyle NSE (Nmap Scripting Engine) kullanarak ağ cihazları üzerinde çeşitli işlemleri gerçekleştirilebilir.
- C ve Lua programlama diliyle yazılmış olan nmap için komut satırı üzerinde gerçekleştirilebilir. Bu amaçla geliştirilmiş olan zenmap olarak bilinen bir ara yüzde mevcuttur.

Nmap üzerinden tarama yapabilmek için Python kütüphane kurulumundan bağımsız olarak bilgisayara nmap kurulumu gerçekleştirilmelidir. Linux için **"sudo apt-get install nmap"**, Windows ve Mac OS X işletim sistemleri için https://nmap.org/download.html güncel sürüm indirilerek kurulum gerçekleştirilebilir.



Zenmap Ekran Görüntüsü Kaynak: https://en.wikipedia.org/wiki/Nmap#/media/File:Zenmap.png (Erişim Tarihi:11/12/2020)

Nmap kullanarak Python programlama dilini kullanabilmek için ilgili kütüphanenin kurulması gereklidir. Bu Python kurumunun olduğu ve sistem değişkenlerine tanımlanmış bir bilgisayarda

komut satırını açarak **"pip install python-nmap"** yazarak nmap kütüphanesi mevcut Python kurulumuna eklenmektedir.

```
C:\>pip install python-nmap
```

Kurulum gerçekleştikten sonra alınan sonuç aşağıdaki gibidir. Python kurulumu üzerinden kod yazımına geçilebilir.

```
C:\>pip install python-nmap
Collecting python-nmap
  Downloading python-nmap-0.6.1.tar.gz (41 kB)
     |████████████████████████████████| 41 kB 225 kB/s
Using legacy 'setup.py install' for python-
nmap, since package 'wheel' is not installed.
Installing collected packages: python-nmap
    Running setup.py install for python-nmap ... done
Successfully installed python-nmap-0.6.1
C:\>
```

Nmap kütüphanesi Python koduna **"import nmap"** ile dâhil edilmiştir. Bir portscanner nesnesi oluşturulmuş ve bu nesne üzerinden IP ve port aralığı verilerek scan fonksiyonu ile tarama gerçekleştirilmiştir.

```
import nmap
nmTarama = nmap.PortScanner()
print(nmTarama.scan('127.0.0.1','21-443'))
```

Aşağıdaki kod incelendiğinde yapılan tarama sonuçlarının JSON (Javascript Object Notation) formatında veri üretildiği görülebilir. Bu veri Python üzerinde kullanılan sözlük (dict) veri tipinde tutulabilir.

```
{'nmap': {'command_line': 'nmap -oX - -p 21-443 -sV 127.0.0.1',
'scaninfo': {'tcp': {'method': 'syn', 'services': '21-443'}},
'scanstats': {'timestr': 'Thu Jan 21 13:06:52 2021', 'elapsed':
'8.09', 'uphosts': '1', 'downhosts': '0', 'totalhosts': '1'}},
'scan': {'127.0.0.1': {'hostnames': [{'name':
'activation.cloud.techsmith.com', 'type': 'PTR'}], 'addresses':
{'ipv4': '127.0.0.1'}, 'vendor': {}, 'status': {'state': 'up',
'reason': 'localhost-response'},

'tcp': {135: {'state': 'open', 'reason': 'syn-ack', 'name': 'msrpc',
'product': 'Microsoft Windows RPC', 'version': '', 'extrainfo': '',
'conf': '10', 'cpe': 'cpe:/o:microsoft:windows'}, 137: {'state':
'filtered', 'reason': 'no-response', 'name': 'netbios-ns',
'product': '', 'version': '', 'extrainfo': '', 'conf': '3', 'cpe':
''}}}}}
```

Bu çerçevede sözlük veri tipinin elemanlarına erişim yöntemleri tercih edilebilir. Aynı zamanda anahtar verileri fonksiyon olarak çağırılması yoluyla da aynı verilere erişilebilmektedir.

```
print(nmTarama.scaninfo())
# {'tcp': {'method': 'syn', 'services': '21-443'}}
print(nmTarama.all_hosts())
# ['127.0.0.1']
print(nmTarama["127.0.0.1"].hostname())
# localhost
print(nmTarama["127.0.0.1"]['tcp'].keys())
# dict_keys([135, 137])
print(nmTarama['127.0.0.1'].has_tcp(135))
# True
print(nmTarama['127.0.0.1'].tcp(137))
# {'state': 'filtered', 'reason': 'no-response', 'name': 'netbios-
ns',
# 'product': '', 'version': '', 'extrainfo': '', 'conf': '3', 'cpe':
 ''}
```

Buraya kadar ifade edilmiş olan kod blokları tek bir döngü içerisinde toplanmıştır.

```
import nmap
nmTarama = nmap.PortScanner()
nmTarama.scan('127.0.0.1', '21-443')
for host in nmTarama.all_hosts():
     print('Host : %s (%s)' % (host, nmTarama[host].hostname()))
     print('State : %s' % nmTarama[host].state())
     for protokol in nmTarama[host].all_protocols():
         print('----------')
         print('Protokol : %s' % protokol)
         lport = nmTarama[host][protokol].keys()
         for port in lport:
             print ('port : %s\tstate : %s' % (port, nmTarama[host][
protokol][port]['state']))
```

Açık bağlantı noktalarının yer aldığı sonuç, aşağıdaki ekran çıktısında gösterilmektedir.

```
Host : 127.0.0.1 (localhost)
State : up
----------
Protocol : tcp
port : 135      state : open
port : 137      state : filtered
```

10.3 SHODAN İLE BİLGİ TOPLAMA

Shodan özünde arama motorlarından bir farkı olmayan bir uygulamadır. Bir arama motorunda arama yaptığımızda ulaşmakta güçlük çekilen farklı sorulara cevap vermek adına yardımcı olmaktadır. Örneğin: Hangi ülkeden daha çok ziyaret edildi? Ya da mevcut bir açıktan en çok hangi sunucular etkilenebilir? Sorularının cevabını arama motorlarında bulamazken shodan bu bilgileri elde etmede yardımcı olacaktır.

İnternete bağlı olan her cihaz shodan odağındadır. Elbette açık olan paylaşılan veriler shodan tarafından alınabilmektedir.2023 te internete bağlı cihaz sayınısın 49 Milyarı bulacağı tahmini düşünüldüğünde ne kadar büyük bir topluluktan bahsettiğimiz ortaya çıkacaktır. Peki, shodan bu cihazlardaki veriyi nereden elde etmektedir? Bu sorunun cevabı hoş geldin mesajlarında banner yapılarında bulunmaktadır.

Shodan ağ güvenliği, market araştırması, Nesnelerin İnterneti, fidye yazılımı izleme gibi birçok alanda kullanılmaktadır. Arama motorları WWW (Word Wide Web) verileri üzerinden tarama yaparken, Shodan bunun ötesinden tüm interneti taramak ve resmi tamamlamak üzerine çalışmaktadır.

Arama Sonuçları

Shodan cihazlar üzerinde çalışan servisler üzerinde bilgi toplamaktadır. Örneğin bir web barındırma hizmeti veren sunucuda çalışan web servis üzerinden onunla iletişim kurarak veri toplamaktadır. Bu noktada web servislere ait bilgilerin saklandığı başlık yapısı içerisinde değerler aşağıdaki görüntüde örnek olarak verilmiştir.

Örneğin bir http başlık üzerinden elde edilen veriler

Web sitesi üzerinden arama gerçekleştirebileceğiniz gibi yukarıdaki örnekler çerçevesinde sağlanan uygulama geliştirme ara yüzü aracığıyla da sonuç alabilmeniz mümkündür. Yazının devamında ortak kullanım dikkate alınarak uygulama geliştirme arayüzü (Application Program Interface) yerine API ifadesi kullanılacaktır.

```
{
    "data": "Sample Device
            Status: Authentication disabled
            Name: NP99999_9999
            MAC: 00:90:90:90:90:90",
    "ip_str": "44.25.2.1",
    "port": 4800,
    "org": "Sample Mobile",
    "location": {
        "country_code": "TR"
    }
}
```

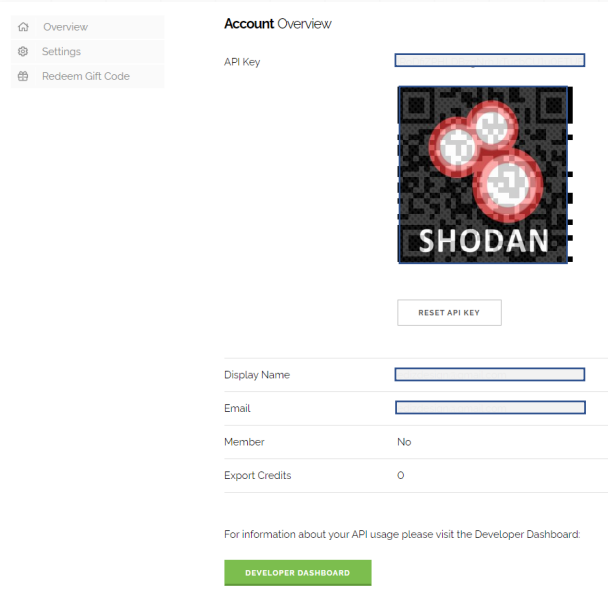
```
HTTP/1.1 200 OK
Server: nginx/1.1.17
Date: Sat, 17 Dec 2020 07:10:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive
```

Birçok programlama dili ile bu ara yüzden faydalanıp elde edilen veriler üzerinden işlemler gerçekleştirilebilmektedir. Örneğimizde Python programlama dilinde shodan için yazılmış kütüphanenin kurulumu kod içerisinde nasıl kullanılacağını açıklanmaktadır.

```
1 (shodan) C:\>pip install shodan 2
Collecting shodan
  Using cached shodan-1.24.0-py3-none-any.whl
Collecting requests>=2.2.1
  Using cached requests-2.25.1-py2.py3-none-any.whl (61 kB)
Collecting certifi>=2017.4.17
  Using cached certifi-2020.12.5-py2.py3-none-any.whl (147 kB)
Collecting chardet<5,>=3.0.2
  Using cached chardet-4.0.0-py2.py3-none-any.whl (178 kB)
Collecting idna<3,>=2.5
  Using cached idna-2.10-py2.py3-none-any.whl (58 kB)
Collecting urllib3<1.27,>=1.21.1
  Using cached urllib3-1.26.2-py2.py3-none-any.whl (136 kB)
Collecting click
  Using cached click-7.1.2-py2.py3-none-any.whl (82 kB)
Collecting click-plugins
  Using cached click_plugins-1.1.1-py2.py3-none-any.whl (7.5 kB)
Collecting colorama
  Using cached colorama-0.4.4-py2.py3-none-any.whl (16 kB)
Collecting XlsxWriter
  Using cached XlsxWriter-1.3.7-py2.py3-none-any.whl (144 kB)
```

1 numaralı shodan yazan ifade kütüphanenin kurulacağı python ortamını ifade etmektedir. Shodan kütüphanesini bu ortama ekleyebilmek için ***"pip install shodan"*** ifadesi komut satırına yazılmalıdır. Kütüphane ihtiyacı olan diğer kütüphanelerle birlikte ortama eklenecektir. Farklı olarak ***"easy_install shodan"*** komutu kullanarak kurulum yapılabilir.

Shodan'ın sağladığı servisten faydalanmak için www.shodan.io adresinde üye olunmalı ve bir API Key sağlanmalıdır.



Ücretsiz elde edilen anahtar sayesinde belirli oranda sorgulama yapılabilmektedir. Limit ve kullanım bilgilerine Developer Dashboard bağlantısına tıklanarak ulaşılabilir.

```
import shodan
SHODAN_API_KEY = "ANAHTAR BURAYA YAZILMALIDIR"
api = shodan.Shodan(SHODAN_API_KEY)
```

Python programlama dili kullanarak shodan kütüphanesi aracılığıyla arama yapılabilmektedir. API'ye bağlanmak için kullanılan program kodu aşağıdaki gibidir.

Aşağıdaki kod bloğu incelendiğinde olası hataları durdurmak ve düzeltmek adında kodun tümü bir try-except bloğu içerisinde alınmıştır. Örnekte mongodb hizmeti veren sunucular üzerine bir arama gerçekleştirilmiş. Gelen verinin python içerisinde yer alan dict veri tipine (aynı zamanda JSON veri formatına) uygun olarak ekrana yazdırılmıştır.

```
try:
    # Arama İşlemi
    sonuclar = api.search('mongodb')
    # Sonuçları Listeleme
    print(f"{sonuclar['total']} sonuç bulundu")
    for sonuc in sonuclar["matches"]:
        print(f"IP:{sonuc['ip_str']}")
        print(sonuc['data'])
except shodan.APIError as  e:
        print(f'Hata Mesajı: {e}')
```

Program çalıştırıldığında alınan terminal sonucunun bir bölümü aşağıdadır.

```
IP:54.169.116.160
MongoDB Server Information
Authentication partially enabled
{
    "storageEngines": [
        "biggie",
        "devnull",
        "ephemeralForTest",
        "wiredTiger"
    ],
    "maxBsonObjectSize": 16777216,
    "ok": 1.0,
    "bits": 64,
    "modules": [],
    "openssl": {
        "compiled": "OpenSSL 1.1.1  11 Sep 2018",
        "running": "OpenSSL 1.1.1  11 Sep 2018"
    },
    "javascriptEngine": "mozjs",
    "version": "4.2.9",
    "gitVersion": "06402114114ffc5146fd4b55402c96f1dc9ec4b5",
    "versionArray": [
        4,
        2,
        9,
        0
    ],
    "debug": false,
    "buildEnvironment": {
        "cxxflags": "-Woverloaded-virtual -Wno-maybe-uninitialized -fsized-deallocation -std=c++17",
        "cc": "/opt/mongodbtoolchain/v3/bin/gcc: gcc (GCC) 8.2.0",
        "linkflags": "-pthread -Wl,-z,now -rdynamic -Wl,--fatal-warnings -fstack-protector-strong -fuse-ld=gold -Wl,--build-id -Wl,--hash-style=gnu -Wl,-
z,noexecstack -Wl,--warn-execstack -Wl,-z,relro",
        "distarch": "x86_64",
        "cxx": "/opt/mongodbtoolchain/v3/bin/g++: g++ (GCC) 8.2.0",
        "ccflags": "-fno-omit-frame-pointer -fno-strict-aliasing -ggdb -pthread -Wall -Wsign-compare -Wno-unknown-pragmas -Winvalid-pch -Werror -O2 -Wno-
unused-local-typedefs -Wno-unused-function -Wno-deprecated-declarations -Wno-unused-const-variable -Wno-unused-but-set-variable -Wno-missing-braces -fsta
ck-protector-strong -fno-builtin-memcmp",
        "target_arch": "x86_64",
```

Üyelik doğrultusunda API üzerinden yapılacak sorgulamalar için shodan 10000 kredi sağlamaktadır. api.info() yazarak ya da https://api.shodan.io/api-info?key={API_ANAHTARI} adresine giderek üyelik planında sunulan hizmetler hakkında bilgi alınabilmektedir.

```
api.info()
SONUC:
{'scan_credits': 0, 'usage_limits': {'scan_credits': 0,
'query_credits': 0, 'monitored_ips': 0}, 'plan': 'oss',
'https': False, 'unlocked': False, 'query_credits': 0,
'monitored_ips': 0, 'unlocked_left': 0, 'telnet': False}
```

10.4 VİGENÈRE ŞİFRELEME UYGULAMASI

İsmini Fransız diplomat Blaise de Vigenère'den alan şifreleme tekniği Giovan Battista Bellaso tarafından oluşturulmuştur. İç içe geçmiş sezar şifrelemelerinden oluştuğu için sezar şifrelemeye nispeten daha zor kırılabilmektedir. Elbette günümüz bilgisayarlarının işlem hızı dikkate alındığında bu şifrenin çözülmesi hiçte zor değildir. Ancak şifreleme yöntemlerini anlamak açısından ele alınmaktadır. 1553'te ortaya atılan şifreleme yöntemi 1863 yılında Charles Babbage tarafından kırılmıştır.

Vigenère Şifreleme yöntemi çok alfabeli bir şifreleme yöntemidir. Sezar şifrelemenin aksine numara yerine alfabedeki harflerden oluşan bir anahtar ifade kullanılır. Bu ifadenin uzunluğu şifrelemenin kırılma güçlüğü ile doğru orantılıdır. Vigenère Şifrelemede şifrelenecek metin ve Vigenère anahtarı yer almalıdır.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Program kodu içerisinde yer alacak olan fonksiyonlar aşağıda listelenmiştir.

1. **anahtarUret(metin,anahtar)** : Bu fonksiyonun amacı şifrelenecek metin ile anahtarın karakter uzunluğunun aynı olmaması durumunda metin ve anahtarın karakter uzunluğu aynı olana kadar anahtar içerisindeki karakterleri terkarlı olarak sonuna eklemek ve kullanılacak nihai anahtarı üretmektir.

```
def anahtarUret(metin, anahtar):
    anahtar = list(anahtar)
    if len(metin) == len(anahtar):
        return(anahtar)
    else:
        for i in range(len(metin) -
                        len(anahtar)):
            anahtar.append(anahtar[i % len(anahtar)])
    return("" . join(anahtar))
```

2. **sifreliMetin(metin,anahtar)**: Bu fonksiyonun amacı python içerisinde yer alan "ord " fonksiyonunda faydalanarak metin içerisindeki karakterlerin ASCII karakter tablosundaki karşılıklarını

sayı olarak (Örn:ord("A")=>65) almaktadır. Program kodunda 26 sayısı İngilizce karakterler dikkate alındığında kullanılabilecek bir sayıdır. Türkçe karakter desteğiyle şifreleme yapabilmek için farklı bir algoritma düşünülebilir.

```
def sifreliMetin(metin, anahtar):
    sifreli_metin = []
    for i in range(len(metin)):
        x = (ord(metin[i]) +
             ord(anahtar[i])) % 26
        x += ord('A')
        sifreli_metin.append(chr(x))
    return("" . join(sifreli_metin))
```

3. **orijinalMetin(metin,anahtar):** Bu fonksiyon şifreli metni alarak deşifre etmektedir. sifreliMetin fonksiyonunda şifrelenmiş olan metni anahtar ile birlikte parametre olarak alıp ters işlem yaparak orijinal metni döndürmektedir.

```
def orijinalMetin(sifreli_metin, anahtar):
    asil_metin = []
    for i in range(len(sifreli_metin)):
        x = (ord(sifreli_metin[i]) -
             ord(anahtar[i]) + 26) % 26
        x += ord('A')
        asil_metin.append(chr(x))
    return("" . join(asil_metin))
```

Aşağıdaki program kodu incelendiğinde "**__name__**" değeri programın kayıtlı dosyasından çalışması sonucunda "**__main__**" değeri ile doldurulmaktadır. Bir başka ifadeyle tüm fonksiyonların kayıtlı olduğu tek bir dosyadan çalıştırılması durumunda bu koşul doğru olacaktır. Kullanıcıdan input fonksiyonları ile alınan orijinal metin ve anahtar ile şifreleme ve deşifre işlemi gerçekleştirilip ekrana yazılmaktadır.

```
if __name__ == "__main__":
    metin = input("Şifrelenecek Metni Giriniz:")
    anahtarkelime = input("Anahtar Kelimeyi Giriniz:")
    anahtar = anahtarUret(metin, anahtarkelime)
    sifreli_metin = sifreliMetin(metin,anahtar)
    print("Şifrelenmiş Metin :", sifreli_metin)
    print("Orijinal Deşifre Metin:",
          orjinalMetin(sifreli_metin, anahtar))
```

Örnek Program Çıktısı; metin için MILLIEGITIMBAKANLIGI ve anahtar veri için PYTHON girildiğinde aşağıdaki gibidir.

```
Şifrelenecek Metni Giriniz:MILLIEGITIMBAKANLIGI
Anahtar Kelimeyi Giriniz:PYTHON
Şifrelenmiş Metin : BGESWRVGMPAOPITUZVVG
Orijinal Deşifre Metin: MILLIEGITIMBAKANLIGI
```

10.5 SCAPY ile PAKET MANİPLASYONU

Scapy, kullanıcının ağ paketlerini göndermesini, koklamasını (sniff), parçalamasını, değiştirilmesini ve oluşturmasını sağlayan bir Python kütüphanesidir. Bu kütüphane kullanılarak, ağlarda bilgi toplama için tarama yapabilen ve izleme yapabilen araçlar geliştirilenbilir. Aynı şekilde saldırı araçlarının da geliştirlmesi mümkündür. Farklı programlama dillerinde bir paketi tanımlama için çok daha fazla satır kod yazmak gerekirken, scapy sayesinde paketler birkaç satırda tanımlanabilir.

Bu bölümde yer alan uygulamalarda ağ protokolleri kullanılacaktır. Örneklerin anlaşılabilmesi için IP, TCP, UDP ve ICMP gibi protokollerin yapısı ile ilgili kitabın ilk bölümlerinde yer alan açıklamaların ve temel iletişimin incelenmesi faydalı olacaktır.

Scapy aşağıdaki komut kullanılarak kurulur.

```
pip install --pre scapy[basic]
```

Scapy kurulduktan sonra interaktif olarak kullanmak için aşağıdaki komut kullanılır.

```
C:\> scapy
```

```
C:\>scapy
INFO: Can't import matplotlib. Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: No route found for IPv6 destination :: (no default route?)
INFO: Can't import python-cryptography v1.7+. Disabled WEP decryption/encryption. (Dot11)
INFO: Can't import python-cryptography v1.7+. Disabled IPsec encryption/authentication.

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.4.3
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Wanna support scapy? Rate it on
       scccccp///pSP///p          p//Y   | sectools!
      sY/////////y  caa           S//P   | http://sectools.org/tool/scapy/
       cayCyayP//Ya              pY/Ya   |              -- Satoshi Nakamoto
        sY/PsY////YCc           aC//Yp   |
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs
                                       using IPython 7.9.0
>>>
```

Tıpkı Python'da olduğu gibi bu kısımda da etkileşimli bir ekran yer almaktadır. Bu ekranda interaktif olarak paket oluşturmak, göndermek mümkündür.

Örneğin aşağıdaki ekranda, IP paketinin başlık bilgisi içerisinde yer alan TTL değeri 10 olan bir paket oluşturulmuş ve a isimli değişkene atanmıştır.

```
>>> a=IP()
>>> a.ttl=10
>>> a
<IP  ttl=10 |>
```

Bu durumda varsayılan özelliklerle beraber TTL değeri 10 olan bir paket oluşturulmuştur. Paket başlığında yer alan alanlar, a isimli değişkenin (IP paketinin) özellikleri gibi kullanılabilir. Örneğin aşağıdaki ekranda, paketin içerisindeki kaynak IP adresi ve hedef IP adresi alanları değiştirilmiş ve paket başlığı gösterilmiştir.

```
>>> a.src="192.168.1.103"
>>> a.dst="192.168.1.101"
>>> a
<IP  ttl=10 src=192.168.1.103 dst=192.168.1.101 |>
```

Paket içerisinde yer alan özellikler "del" fonksiyonu ile silinebilir. Aşağıdaki örnekte TTL alanı için önceki atama silinmiştir.

```
>>> del(a.ttl)
>>> a
<IP  src=192.168.1.103 dst=192.168.1.101 |>
>>>
>>>
```

Oluşturulan ve bir değişkene atanan paketler, kolaylıkla yeni bir değişkene de atanabilir. Aşağıdaki örnekte a ile tanımlanan paket b isimli değişkene atanmıştır. Ardından paketin tüm yapısı **show** metodu ile gösterilmiştir.

```
>>> b = a
>>> b.show()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 192.168.1.103
  dst= 192.168.1.101
  \options\
```

Dikkat edilirse, paket başlık bilgisinde yer alan bazı alanların varsayılan değerleri bulunmaktadır.

Oluşturulan paketlerin ham yapısını görmek için **raw** komutu kullanılır.

```
>>> raw(a)
b'E\x00\x00\x14\x00\x01\x00\x00@\x00\xf6\xcc\xc0\xa8\x01g\xc0\xa8\x01e'
>>>
```

Katmanlı mimarilerdeki (OSI modeli) yapıyla uyumlu olarak IP paket içerisinde TCP ya da UDP gibi 4.katman protokolleri de eklenebilir. Bu durumda her katman birbirinden "/" ifadesi ile ayrılır. Aşağıdaki örnekte, IP paketinin içerisine TCP protokolü eklenmiştir.

```
>>> IP()/TCP()
<IP  frag=0 proto=tcp |<TCP  |>>
>>>
>>> a/TCP()
<IP  frag=0 proto=tcp src=192.168.1.103 dst=192.168.1.101 |<TCP  |>>
>>>
```

Oluşturulan paketin, Ethernet (2.katman) çerçevesine konulması için aynı "/" ifadesi kullanılabilir.

```
>>> Ether()/IP()/TCP()
<Ether  type=IPv4 |<IP  frag=0 proto=tcp |<TCP  |>>>
>>>
>>>
>>> c=TCP()
>>> Ether()/a/c
<Ether  type=IPv4 |<IP  frag=0 proto=tcp src=192.168.1.103 dst=192.168.1.101 |<TCP
 |>>>
>>>
```

Yukarıdaki ekran görüntüsünde "c" isimli bir değişkene TCP başlık bilgisi atanmıştır. Daha sonra c değişkeni a isimli IP paketinin içerisine ve sonra da tümü Ethernet çerçevesine alınmıştır.

Oluşturulan bir paketin WireShark yazılımında olduğu gibi görüntülenmesi için hexdump komutu kullanılabilir.

```
>>> a=IP()
>>> a.src="192.168.1.103"
>>> a.dst="192.168.1.1"
>>> a.ttl=24
>>>
>>> hexdump(a)
0000  45 00 00 14 00 01 00 00 18 00 1F 31 C0 A8 01 67  E..........1...g
0010  C0 A8 01 01                                      ....
>>>
```

10.5.1 Scapy Örnekleri

Aşağıdaki örnekte www.meb.gov.tr adresinden index.html sayfası http protokolü kullanılarak istenmesi için paket oluşturulmuş ve hexdump ile paketin son hali görüntülenmiştir.

```
>>> a=Ether()/IP(a=Ether()/IP(dst="www.meb.gov.tr")/TCP()/"GET /index.html HTTP/1.0 \n\n"
>>>
>>> hexdump(a)
WARNING: getmacbyip failed on [Errno 1] Operation not permitted
WARNING: Mac address to reach destination not found. Using broadcast.
0000  FF FF FF FF FF FF 08 00 27 E9 3D E6 08 00 45 00  ........'.=...E.
0010  00 43 00 01 00 00 40 06 DC 7E 0A 00 02 0F D4 AE  .C....@..~......
0020  BD 78 00 14 00 50 00 00 00 00 00 00 00 00 50 02  .x...P........P.
0030  20 00 1F 7C 00 00 47 45 54 20 2F 69 6E 64 65 78   ..|..GET /index
0040  2E 68 74 6D 6C 20 48 54 54 50 2F 31 2E 30 20 0A  .html HTTP/1.0 .
0050  0A                                               .
```

Oluşturulan paketin varsayılan değerler ile son halinin görüntülenmesi için ls komutu kullanılabilir. Aşağıdaki örnekte Ethernet mac adresleri tanımlanmadığı için buna ilişkin uyarıları ve "a" paketinin yapısı görüntülenmektedir.

```
>>> ls(a)
WARNING: getmacbyip failed on [Errno 1] Operation not permitted
WARNING: Mac address to reach destination not found. Using broadcast.
dst        : DestMACField                    = 'ff:ff:ff:ff:ff:ff' (None)
src        : SourceMACField                  = '08:00:27:e9:3d:e6' (None)
type       : XShortEnumField                 = 2048            (36864)
--
version    : BitField  (4 bits)              = 4               (4)
ihl        : BitField  (4 bits)              = None            (None)
tos        : XByteField                      = 0               (0)
len        : ShortField                      = None            (None)
id         : ShortField                      = 1               (1)
flags      : FlagsField  (3 bits)            = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField  (13 bits)             = 0               (0)
ttl        : ByteField                       = 64              (64)
proto      : ByteEnumField                   = 6               (0)
chksum     : XShortField                     = None            (None)
src        : SourceIPField                   = '10.0.2.15'     (None)
dst        : DestIPField                     = Net('www.meb.gov.tr') (None)
options    : PacketListField                 = []              ([])
--
sport      : ShortEnumField                  = 20              (20)
dport      : ShortEnumField                  = 80              (80)
seq        : IntField                        = 0               (0)
ack        : IntField                        = 0               (0)
dataofs    : BitField  (4 bits)              = None            (None)
reserved   : BitField  (3 bits)              = 0               (0)
flags      : FlagsField  (9 bits)            = <Flag 2 (S)>    (<Flag 2 (S)>)
window     : ShortField                      = 8192            (8192)
chksum     : XShortField                     = None            (None)
urgptr     : ShortField                      = 0               (0)
options    : TCPOptionsField                 = []              (b'')
--
load       : StrField                        = b'GET /index.html HTTP/1.0 \n\n' (b'')
>>>
```

Not: *Bu aşamaya kadar sadece tanımlama yapılmıştır, paketler hedefe gönderilmemiştir.*

Oluşturulan bir paketin gönderilmesi için **send(packet)** komutu kullanılır. Aşağıdaki örnekte "8.8.8.8" IP adresine varsayılan değerler ile bir paket gönderilmiştir.

```
>>> pkt=IP(dst="8.8.8.8")
>>>
>>> send(pkt)
.
Sent 1 packets.
>>>
>>> _
```

Paket gönderimi çarpan ile de kullanılabilir Şekildeki örnekte 192.168.1.1 adresine 10 adet paket gönderilmiştir.

```
>>>
>>> pkt=IP(dst="192.168.1.1")
>>> send(pkt*10)
..........
Sent 10 packets.
>>>
```

Gönderilen paketler arasında süre tanımlanabilir. Aşağıdaki örnekte **0,1** sn aralıklarla sürekli olarak (loop=1) paket gönderilmiştir.

```
>>> send(pkt, inter=0.1, loop=1)
.......................................................
Sent 58 packets.
>>>
```

ICMP, 3.katman düzeyinde erişebilirlik için kullanılan bir protokoldür. Aşağıdaki ekran görüntüsünde 8.8.8.8 IP adresine bir adet ICMP paketi gönderilmiştir.

```
>>>
>>> send(IP(dst="8.8.8.8")/ICMP())
.
Sent 1 packets.
>>>
```

Aşağıdaki ilk örnekte ise TCP taşıyan, ikinci örnekte ise UDP taşıyan bir IP paketinin gönderilmesi yer almaktadır.

```
>>> erd=IP()/TCP(dport=1453,sport=1079,seq=1234567,flags=18)
>>> send(erd)

Sent 1 packets.
```

```
>>> eUDP=UDP(dport=67,sport=68)
>>> send(IP()/eUDP)
.
Sent 1 packets.
>>>
```

Paket gönderip cevabını almak için **sr** (Send & Receive) fonksiyonu kullanılır. Aşağıdaki örnekte 8.8.8.8 IP adresine 20 ICMP Yankı isteği mesajı gönderilmiş ve cevap alınmıştır. ICMP mesajının içerisine de istenen bir mesaj konmuştur.

```
from scapy.all import *
packet=IP(src="192.168.1.1",version=3, dst="8.8.8.8")/ICMP()/"ICMP icinde gizli mesaj"

p=sr1(packet*20)
```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2699	588.718134	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
2700	588.719672	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
2701	588.721581	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
2702	588.724326	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
2703	588.726623	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
2704	588.729059	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
2705	588.730361	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 2706)
2706	588.735548	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113 (request in 2705)
2707	588.736166	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113
2708	588.736166	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113
2709	588.736971	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
2710	588.738483	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 2711)
2711	588.739833	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113 (request in 2710)
2712	588.740385	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113
2713	588.741287	192.168.1.103	8.8.8.8	ICMP	65	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 2714)
2714	588.741414	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113 (request in 2713)
2715	588.743715	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113
2716	588.750549	8.8.8.8	192.168.1.103	ICMP	65	Echo (ping) reply id=0x0000, seq=0/0, ttl=113

```
> Frame 2714: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface \Device\NPF_{6423AACA-C349-4F92-B892-77ADADEEB774}, id 0
> Ethernet II, Src: Tp-LinkT_06:d0:13 (5c:63:bf:06:d0:13), Dst: IntelCor_f3:ed:41 (48:45:20:f3:ed:41)
v Internet Protocol Version 4, Src: 8.8.8.8, Src: 192.168.1.103
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000  48 45 20 f3 ed 41 5c 63  bf 06 d0 13 08 00 45 00   HE ··A\c ····· E·
0010  00 33 00 00 00 00 71 01  77 ab 08 08 08 08 c0 a8   ·3····q· w·····
0020  01 67 00 00 7c 57 00 00  00 00 49 43 4d 50 20 69   ·g··|W·· ··ICMP i
0030  63 69 6e 64 65 20 67 69  7a 6c 69 20 6d 65 73 61   cinde gi zli mesa
0040  6a                                                  j
```

Aşağıdaki ekran görüntüsünde olduğu gibi **sniff()** komutu ile paket dinlemesi yapılabilir.

```
>>> sniff()
<Sniffed: TCP:30 UDP:4 ICMP:0 Other:6>
>>> a=_
>>> a.summary()
Ether / IP / TCP 192.168.1.106:3398 > 52.114.74.39:https PA / Raw
Ether / IP / TCP 52.114.74.39:https > 192.168.1.106:3398 PA / Raw
Ether / IP / TCP 192.168.1.106:3398 > 52.114.74.39:https A
Ether / ARP who has 192.168.1.1 says 192.168.1.103 / Padding
Ether / ARP who has 192.168.1.1 says 192.168.1.103 / Padding
Ether / ARP who has 192.168.1.102 says 192.168.1.1 / Padding
Ether / ARP who has 192.168.1.103 says 192.168.1.1 / Padding
Ether / ARP who has 192.168.1.107 says 192.168.1.1 / Padding
Ether / IP / UDP / DNS Qry "b'presence.teams.microsoft.com.'"
```

Yakalanan paketler indeks numarasına göre görüntülenebilir.

```
>>> a[9]
<Ether  dst=c4:71:54:d5:8a:f6 src=60:67:20:63:6f:98 type=IPv4 |<IP  version=4 ihl=5 tos=0x0 len=74 i
106 dst=8.8.4.4 |<UDP  sport=56263 dport=domain len=54 chksum=0x3406 |<DNS  id=8629 qr=0 opcode=QUER
ount=0 arcount=0 qd=<DNSQR  qname='presence.teams.microsoft.com.' qtype=A qclass=IN |> an=None ns=No
>>> hexdump(a[9])
0000  C4 71 54 D5 8A F6 60 67 20 63 6F 98 08 00 45 00  .qT...`g co...E.
0010  00 4A CA DD 00 00 80 11 A1 A7 C0 A8 01 6A 08 08  .J..........j..
0020  04 04 DB C7 00 35 00 36 34 06 21 B5 01 00 00 01  .....5.64.!.....
0030  00 00 00 00 00 00 08 70 72 65 73 65 6E 63 65 05  .......presence.
0040  74 65 61 6D 73 09 6D 69 63 72 6F 73 6F 66 74 03  teams.microsoft.
0050  63 6F 6D 00 00 01 00 01                          com.....
>>>
>>>
```

Tüm paketler yerine filtreleme de yapılabilir. Aşağıdaki örnekte ARP mesajları veya 192.168.1.1 IP adresli paketler filtrelenmiştir.

```
>>>  sniff(filter="arp or host 192.168.1.1", count=2)
<Sniffed: TCP:0 UDP:2 ICMP:0 Other:0>
>>> a=_
>>> a.summary()
Ether / IP / UDP 192.168.1.1:ssdp > 239.255.255.250:ssdp / Raw
Ether / IP / UDP 192.168.1.1:ssdp > 239.255.255.250:ssdp / Raw
>>> hexdump(a[0])
0000  01 00 5E 7F FF FA C4 71 54 D5 8A F6 08 00 45 00  ..^....qT.....E.
0010  01 2B 00 00 40 00 04 11 C4 1E C0 A8 01 01 EF FF  .+..@...........
0020  FF FA 07 6C 07 6C 01 17 C5 3B 4E 4F 54 49 46 59  ...l.l...;NOTIFY
0030  20 2A 20 48 54 54 50 2F 31 2E 31 20 0D 0A 48 4F   * HTTP/1.1 ..HO
0040  53 54 3A 20 32 33 39 2E 32 35 35 2E 32 35 35 2E  ST: 239.255.255.
0050  32 35 30 3A 31 39 30 30 0D 0A 43 41 43 48 45 2D  250:1900..CACHE-
0060  43 4F 4E 54 52 4F 4C 3A 20 6D 61 78 2D 61 67 65  CONTROL: max-age
0070  3D 35 30 30 0D 0A 4C 6F 63 61 74 69 6F 6E 3A 20  =500..Location:
0080  68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38 2E 31  http://192.168.1
0090  2E 31 3A 34 39 34 33 31 2F 64 65 76 69 63 65 64  .1:49431/deviced
00a0  65 73 63 2E 78 6D 6C 0D 0A 4E 54 3A 20 75 70 6E  esc.xml..NT: upn
00b0  70 3A 72 6F 6F 74 64 65 76 69 63 65 0D 0A 4E 54  p:rootdevice..NT
00c0  53 3A 20 73 73 64 70 3A 61 6C 69 76 65 0D 0A 53  S: ssdp:alive..S
00d0  45 52 56 45 52 3A 4C 49 4E 55 58 2F 32 2E 36 20  ERVER:LINUX/2.6
00e0  55 50 6E 50 2F 31 2E 30 20 54 50 2D 4C 49 4E 4B  UPnP/1.0 TP-LINK
00f0  2F 31 2E 30 0D 0A 55 53 4E 3A 20 75 75 69 64 3A  /1.0..USN: uuid:
0100  33 31 37 61 33 34 39 61 2D 31 64 64 32 2D 31 31  317a349a-1dd2-11
0110  62 32 2D 62 35 36 36 2D 63 34 37 31 35 34 64 35  b2-b566-c47154d5
0120  38 61 66 36 3A 3A 75 70 6E 70 3A 72 6F 6F 74 64  8af6::upnp:rootd
0130  65 76 69 63 65 0D 0A 0D 0A                       evice....
>>>
```

Scapy kullanılarak aşağıdaki örnekteki gibi bağlantı noktası taraması da yapılabilir.

```
from scapy.all import *


portlar = [80,21,22,23,25,143,161,67,68,53]
ipler=['192.168.1.1','192.168.1.103','192.168.1.101']

for ip in ipler:
    for port in portlar:
        cevap = sr1(IP(dst=ip)/TCP(dport=port, flags="S"),verbose=False, timeout=0.2)
        if cevap :
                if cevap[TCP].flags == 18 :
                    print (ip, ":",port)
        else:
                print(ip," erişilebilir değil")
```

Yukarıdaki örnekte, taranmak istenen IP adresleri ipler isimli bir liste olarak, taranmak istenen bağlantı noktaları da portlar isimli liste olarak tanımlanmıştır. Kodlar yazılıp çalıştırıldığında aşağıdaki gibi listede yer alan IP'lere ilişkin belirtilen bağlantı noktalarının durumları çıktı olarak gösterilecektir.

```
192.168.1.1 : 80
192.168.1.1 : 21
192.168.1.1 : 53
192.168.1.101 : 80
>>>
>>>
```

Tracert, hedefe giden yolda yer alan yönlendiricilerin listesini gösteren bir komuttur ve ICMP protokolünü kullanır. Aşağıdaki uygulamada, 8.8.8.8 IP adresine giden yolda yer alan ilk 8 yönlendiricinin IP adresi gösterilmektedir.

```
from scapy.all import *


for ttl in range(8):
    pkt = IP(dst="8.8.8.8", ttl=ttl) / UDP()
    cvp = sr1(pkt, verbose=0, timeout=1)
    if cvp is not None:
        print (cvp.src)
```

Python kodu çalıştırıldığında aşağıdaki çıktı gösterilecektir.

```
192.168.1.1
192.168.1.1
212.156.201.28
81.212.105.39
195.175.175.49
81.212.207.29
81.212.217.5
212.156.104.150
```

Aşağıdaki örnekte, kaynak IP adresi değiştirilerek 8.8.8.8 IP adresine ICMP Yankı isteği (type =8) oluşturulmuştur.

```
from scapy.all import *

paket=IP(dst="8.8.8.8", src="192.168.1.177", ttl=10)/ICMP(type=8)
paket.show()
```

Oluşturulan paketin yapısı show metodu ile gösterilmiştir.

```
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 10
  proto     = icmp
  chksum    = None
  src       = 192.168.1.177
  dst       = 8.8.8.8
  \options   \
###[ ICMP ]###
     type      = echo-request
     code      = 0
     chksum    = None
     id        = 0x0
     seq       = 0x0
```

Aşağıdaki örnekte 192.168.1.103 IP adresine gelen paketler yakalanmış ve ilk paketin içeriği hexdump ile gösterilmiştir.

```
from scapy.all import *


a=sniff(filter="host=192.168.1.103",iface="Wi-Fi",timeout=100,count=10)
hexdump(a[0])

0000  5C 63 BF 06 D0 13 48 45 20 F3 ED 41 08 00 45 00  \c....HE ..A..E.
0010  04 DE 72 51 40 00 80 06 E9 5E C0 A8 01 67 12 CB  ..rQ@....^...g..
0020  C5 8F 06 26 01 BB C1 38 D4 B4 9B EF B5 43 50 18  ...&...8.....CP.
0030  02 01 80 D9 00 00 17 03 03 04 B1 83 A5 93 91 51  ................Q
0040  FC E2 B3 CF 7D 2D 55 44 6F BD 16 BD 26 43 80 A6  ....}-UDo...&C..
0050  1C A0 77 C6 FD E3 E9 FF BD 3F 4D 84 9D 5D 16 9F  ..w......?M..]..
0060  44 4D F4 B0 12 7E 8B D8 60 2F 8B 84 2A DF B8 E0  DM...~..`/..*...
0070  2E 53 AB 4F 3F 39 14 61 43 07 C4 17 89 7D EB AA  .S.O?9.aC....}..
0080  EB 2A E1 72 55 F7 22 A8 C3 92 84 36 31 88 EF A0  .*.rU."....61...
0090  A7 7B E1 60 80 13 2C 6B 6F AE 1D 1B DF 10 91 0E  .{.`..,ko.......
00a0  A1 8D 3F 0E 6C 8C 37 FB FC EA BA 47 E8 1B D7 4E  ..?.l.7....G...N
00b0  D7 4C E9 E6 05 CD 51 E1 23 46 9C 16 CF 6B 57 57  .L....Q.#F...kWW
00c0  D4 41 86 58 B2 93 4C D3 97 FA 0F 78 2A B4 BF EF  .A.X..L....x*...
00d0  E0 56 9D 52 0E 20 C9 8C A7 46 81 47 1C B8 E0 03  .V.R. ...F.G....
00e0  45 C5 D1 89 7E EC 34 DD C7 AD BB 79 E5 9E 54 A4  E     4     y  T
```

KAYNAKLAR

1 H. Hekim, O.BAŞIBÜYÜK, *"Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları"*,Uluslararası Güvenlik ve Terörizm Dergisi. 2013.

2 F. ASLAY, *"Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi"* International Journal of Multidisciplinary Studies and Innovative Technologies, 2017.

3 S. Çelik, *"Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım"*, Academic Review of Humanities and Social Sciences, 2018.

4 UDHB 2012. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ankara, s. 9-47.

5 Internet, URL: https://felsefeakademisi.tr.gg/ (Son erişim: 01.12.2020)

6 Internet, URL: https://www.dnsstuff.com/siem-tools#IBM (Son erişim: 01.12.2020)

7 Internet, URL, https://en.wikipedia.org/wiki/Denial-of-service_attack (Son erişim: 01.12.2020)

8 Internet, URL, https://en.wikipedia.org/wiki/Attack_surface (Son erişim: 01.12.2020)

9 Internet, URL, https://cve.mitre.org/ (Son erişim: 01.12.2020)

10 Internet, URL, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (Son erişim: 01.12.2020)

11 Internet, URL, https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html (Son erişim: 01.12.2020)

12 Internet, URL: https://www.kaspersky.com.tr/blog/android-8-permissions-guide/5356/ (Son erişim: 01.12.2020)

13 Internet, URL: https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html (Son erişim: 01.12.2020)

14 Internet, URL: https://www.balbix.com/insights/attack-vectors-and-breach-methods/ (Son erişim: 01.12.2020)

15 Internet, URL: https://www.guvenlioyna.org.tr/blog-detay/dijital-oyunlarda-guvenlik (Son erişim: 01.12.2020)

16 Internet, URL: https://www.guvenliweb.org.tr/blog-detay/dijital-oyun-oynarken-ne-kadar-guvendeyiz (Son erişim: 01.12.2020)

KAYNAKLAR

17 Internet, URL: https://dijitalmedyavecocuk.bilgi.edu.tr/tag/dijital-oyunlarda-guvenlik/ (Son erişim: 01.12.2020)

18 Internet, URL: https://dijitalmedyavecocuk.bilgi.edu.tr/2020/02/28/dijital-oyunlar-ve-kisisel-veriler/ (Son erişim: 01.12.2020)

19 Internet, URL: https://cybersecurity.att.com/blogs/security-essentials/rootkit-detection-techniques-and-best-practices (Son erişim: 01.12.2020)

20 Internet, URL: https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/ (Son erişim: 01.12.2020)

21 Internet, URL: https://owasp.org/www-project-top-ten/ (Son erişim: 01.12.2020)

22 Internet, URL: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/ what-is-soc.html (Son erişim: 01.12.2020)

23 Internet, URL: https://digitalguardian.com/blog/what-security-operations-center-soc (Son erişim: 01.12.2020)

24 Internet, URL: http://www.whois.com/, (Son erişim: 01.12.2020)

25 Internet, URL: https://www.ripe.net/, (Son erişim: 01.12.2020)

26 Internet, URL: https://ns.tools/, (Son erişim: 01.12.2020)

27 Internet, URL: http://www.archive.org, (Son erişim: 01.12.2020)

28 Internet, URL: http://www.netcraft.com, (Son erişim: 01.12.2020)

29 Internet, URL: www.bilgiguvenligi.gov.tr, (Son erişim: 03.12.2020)

30 https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/ (Son erişim : 25.12.2020)

31 Internet, URL: https://hukuk.deu.edu.tr/dosyalar/dergiler/dergimiz-15-1/senercelik.pdf, (Son Erişim : 25.12.2020)

32 Internet, URL: https://www.siberportal.org/). (Son Erişim : 27.12.2020)

33 Internet, URL: https://crackstation.net/hashing-security.htm, (Son Erişim: 10.12.2020

34 Internet, URL: http://www.md5.cz/ (Son Erişim : 10.12.2020)

35 Internet, URL: https://passwordsgenerator.net/, Son Erişim 11.12.2020

36 Internet, URL: https://emn178.github.io/online-tools/sha256.html, Son Erişim 11.12.2020

37 Internet, URL: https://www.cmd5.org/, Son Erişim 11.12.2020

38 Internet, URL: https://md5decrypt.net/en/Sha256/ Son Erişim 11.12.2020

39 Internet, URL: https://support.microsoft.com/tr-tr/windows/ Son Erişim: 19.01.2021

40 Internet, URL: https://forum.shiftdelete.net/konular/regedit-nedir-ve-ne-ise-yarar.462675/ Son Erişim: 19.01.2021

41 Internet, URL: https://tr.wikipedia.org/wiki/Linux Son Erişim: 19.01.2021

42 Internet, URL: https://tr.wikipedia.org/wiki/Linux_da%C4%9F%C4%B1t%C4%B1mlar_%C4%B1 Son Erişim: 19.01.2021

43 Internet, URL: https://tr.wikipedia.org/wiki/Snort Son Erişim: 19.01.2021

44 Internet, URL: https://en.wikipedia.org/wiki/Sguil Son Erişim: 19.01.2021

45 Internet, URL: https://github.com/Security-Onion-Solutions/security-onion/wiki/ELSA Son Erişim: 19.01.2021

46 Internet, URL: https://www.netacad.com/courses/cybersecurity/cyberops-associate Son Erişim: 19.01.2021

47 Internet, URL: https://www.kali.org/ Son Erişim: 19.01.2021

48 Internet, URL: https://docs.securityonion.net/en/16.04/index.html Son Erişim: 19.01.2021

49 Internet, URL: https://www.wireshark.org/docs/wsug_html_chunked/ Son Erişim: 19.01.2021

50 Internet, URL: https://tr.wikipedia.org/wiki/SQL_Injection Son Erişim: 19.01.2021

51 Internet, URL: https://docs.securityonion.net/en/16.04/kibana.html Son Erişim: 19.01.2021

52 Internet, URL: https://docs.microsoft.com/en-us/powershell/scripting/learn/ps101/00-introduction?view=powershell-7.1 Son Erişim: 19.01.2021

53 Internet, URL: https://docs.microsoft.com/en-us/windows-server/administration / windows-commands/windows-commands Son Erişim: 19.01.2021

54 Internet, URL: http://www.belgeler.org/lis/archive-tlkg-lis-5.9.html Son Erişim 19.01.2021

SİBER GÜVENLİK EĞİTİMİ