



# Siber Güvenlik Temelleri

## Murat ÖZALP

# İÇİNDEKİLER

## TEORİK

- Siber güvenlik temelleri
- Tehdit türleri
- Parola güvenliği
- Zafiyetli test ortamları
- Siber güvenlikte kariyer
- Son kullanıcı için tedbirler
- Faydalı linkler

## UYGULAMA

- Ortalama postası analizi
- Wireshark ile trafik analizi
- Kali Linux kurulum ve kullanımı
- Hydra ile parola kırma
- Metasploit
- GVM ile zafiyet tarama

# ÖNEMLİ !

- Etik kurallar
- Yasal mevzuat (TCK 243):
  - Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye **bir yıla kadar hapis veya adli para cezası** verilir.
  - Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, **altı aydan iki yıla kadar hapis** cezasına hükmolunur.” hükmüne amirdir.

# Siber Güvenlik – *Kime Göre?*

- Son kullanıcı (anne, baba, teyze, amca, dede, nine, ...)
- İş yerinde bilgisayar kullanmak zorunda olanlar
- Teknolojiyi etkin kullanan -*özellikle*- gençler
- Bilgisayar tutkunları
- Yazılımcılar
- Karanlık tarafta takılanlar
- Mesleği “siber güvenlik” olanlar



# CIA Üçgeni



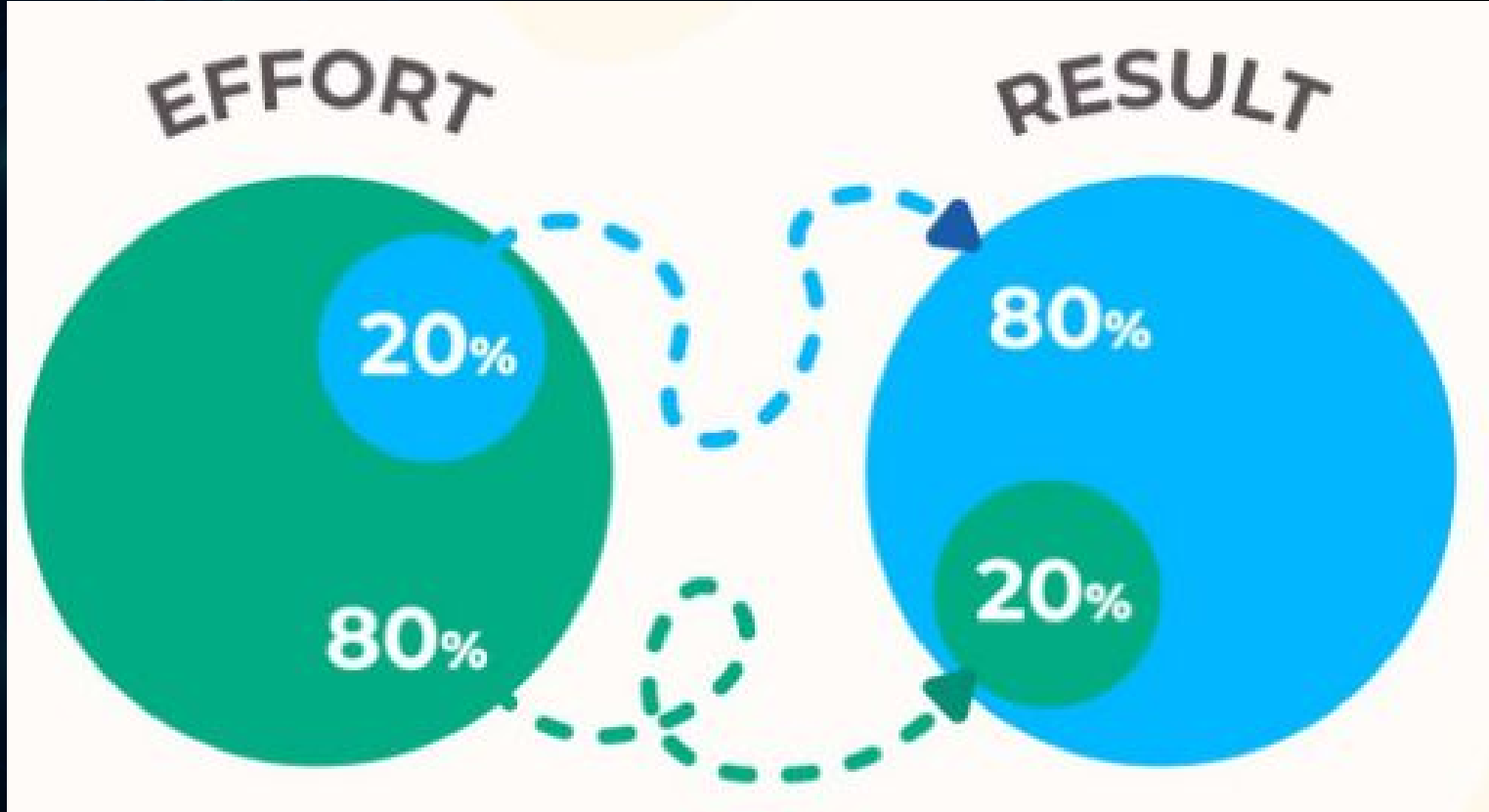
- Erişilebilirlik
- Bütünlük
- Gizlilik

Görsel kaynağı:

<https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important>



# Pareto İlkesi



Görsel kaynağı: <https://www.linkedin.com/pulse/pareto-principle-101-boost-your-productivity-pedro-pinto-mba-mcc/>

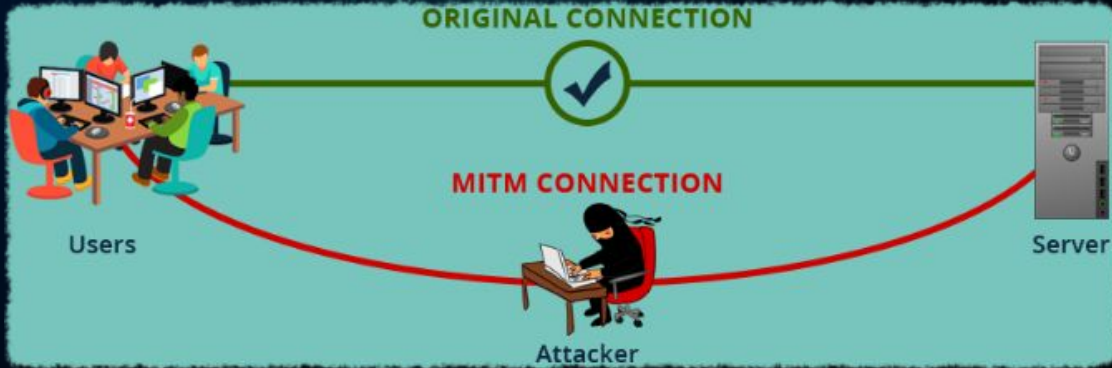
# Yaygın Tehdit Türleri - 1

- Oltalama (phishing)
- Kötü yazılımlar (malware)
- Fidye yazılımları (ransomware)

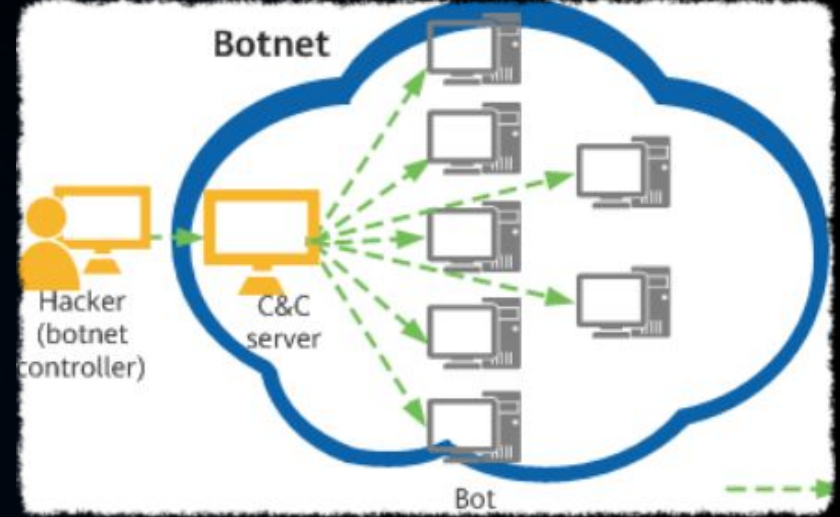


# Yaygın Tehdit Türleri - 2

- Araya girme (MITM)
- Hizmet dışı bırakma (DoS/DDoS)
- Botnet (zombi bilgisayarlar)
- Sosyal mühendislik



Görsel kaynağı: <https://www.clickssl.net/blog/how-to-stay-safe-against-the-man-in-the-middle-attack>



Görsel Kaynağı:

<https://info.support.huawei.com/info-finder/encyclopedia/en/Botnet.html>



# Parola != Şifre

- **Parola** (password) kelimesi yerine **şifre** kelimesinin kullanıldığını sıkça duyabiliriz. Şifre (cipher) terimi, şifreleme algoritmalarını ifade eder ve parola kavramının şifreleme ile doğrudan bir ilgisi yoktur.

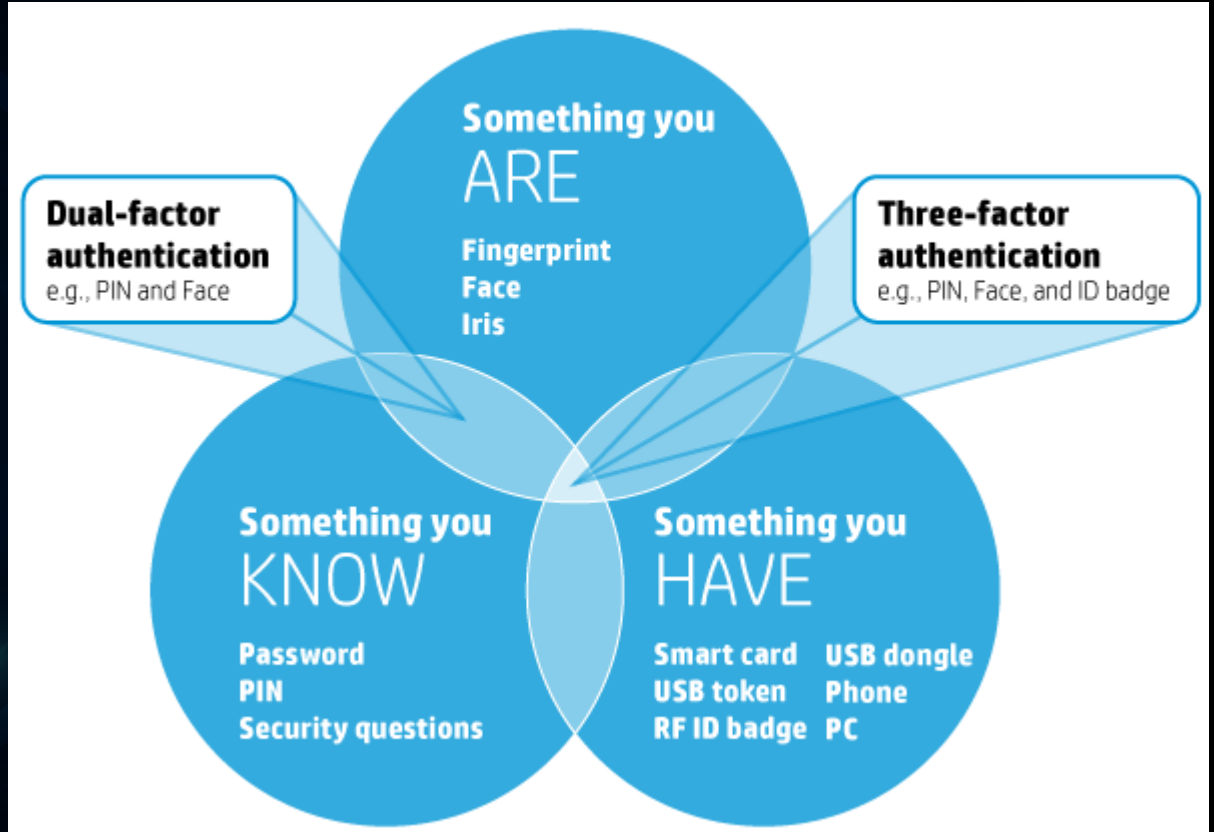


# Parola Güvenliği

- Uzun, karmaşık, tahmin edilemeyecek, sözlüklerde olmayan parolalar
- Parola yöneticileri. Proton pass, Keepass, vb.
- Parolam ne kadar güçlü? Gerçek parolanızı bu sitelere girmeyin.
  - <https://password.kaspersky.com/tr/>
- Kendinize özel parola algoritmaları oluşturabilirsiniz.
  - <https://chatgpt.com/share/c0ea769e-f363-4e8d-b78f-1e3f24f2130e>
- Çok katmanlı doğrulama (MFA) kullanın.

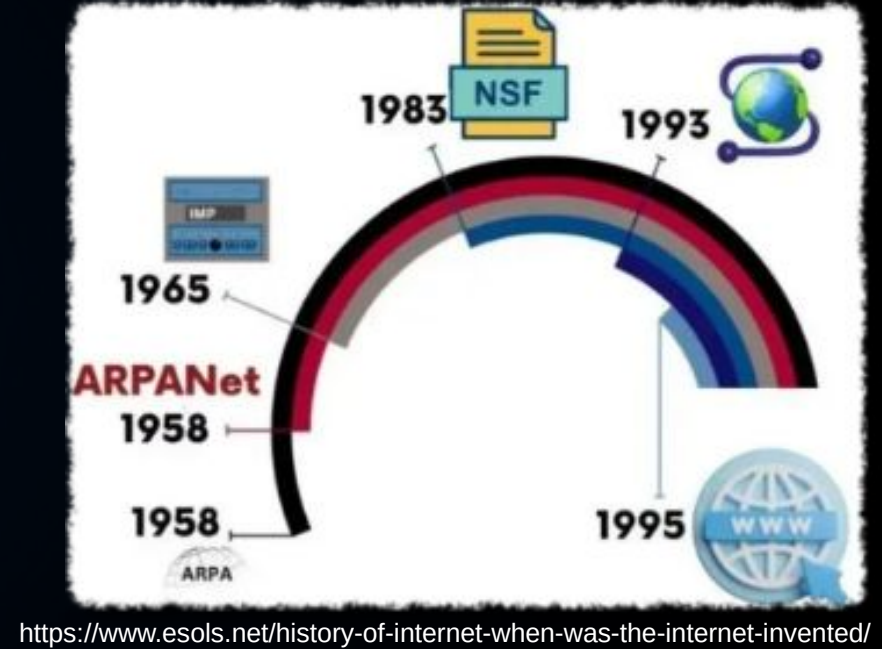
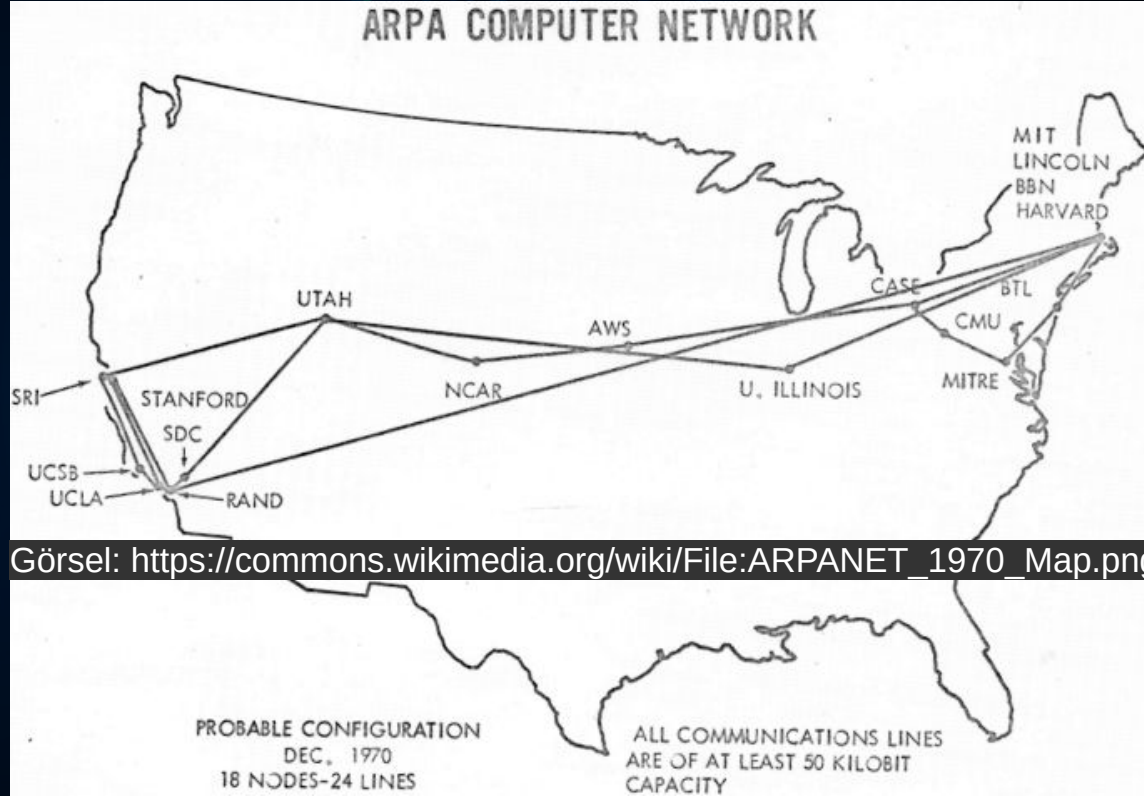
# Kimlik Doğrulama Ana Faktörleri

- Kimsin?
- Ne biliyorsun?
- Neye sahipsin?



Görsel kaynağı: <https://www.isysl.net/are-multi-factor-authentication-mfa-solutions-equally-secure>

# İnternet Neden Bu Kadar Güvensiz?





# Gelecekte Göreceklerimiz

İsviçre'de bir hacker grubu, internet bağlantısı bulunan milyonlarca elektronik diş fırçasını hackledi.

[Translate post](#)



8:58 PM · Feb 7, 2024 · 116.3K Views

12 Reposts 21 Quotes 854 Likes 27 Bookmarks

Bu haber doğru değil ama yakın gelecekte buna benzer haberler göreceğiz.

<https://teyit.org/analiz/isvicredeki-siber-saldirida-milyonlarca-dis-fircasi-hacklendi-mi>

# Zafiyetli Test Ortamları

- <https://www.hackthebox.com/machines>
- <https://www.vulnhub.com/>
- <https://tryhackme.com/>
- <https://www.root-me.org/>
- <https://picoctf.org/>
- İsterseniz, DVWA gibi uygulamaları kendi bilgisayarınıza da kurabilirsiniz



Sağa sola saldırmayın :)

Görsel:  
<https://blog.korayspor.com/kum-torbasiyla-yapilabilecek-antrenmanlar/>

# Kariyer Planlama

- Sertifikalar (CEH, OSCP, CISSP, vb.)
- Yol haritaları (<https://Roadmap.sh> gibi)
- İş ilanları analizi
  - Bir terimi yazıp, komşu terimlerini tespit ederek yol haritası çıkarma.
  - Bir iş dalını yazarak gereklilikleri tespit etme
- Özgeçmiş hazırlamaktan daha önemli: İnternet paylaşımları
  - Youtube, Github, blog, vb.
  - Google'da isminiz aranınca ne çıksın?

# Oltalama E-posta Analizi

- Gönderen e-posta adresi
- Konu inceleme
- E-posta içerik metni
- Linklerin gerçek adresi. <https://checkshorturl.com/>
- Ek dosya incelemesi
- Kurumun resmi web sitesi
- Kaynak incelemesi
  - <https://mxtoolbox.com/EmailHeaders.aspx>
- Link güvenilirliği sorgulama
  - <https://transparencyreport.google.com/safe-browsing/search>
  - <https://www.virustotal.com/gui/home/url>



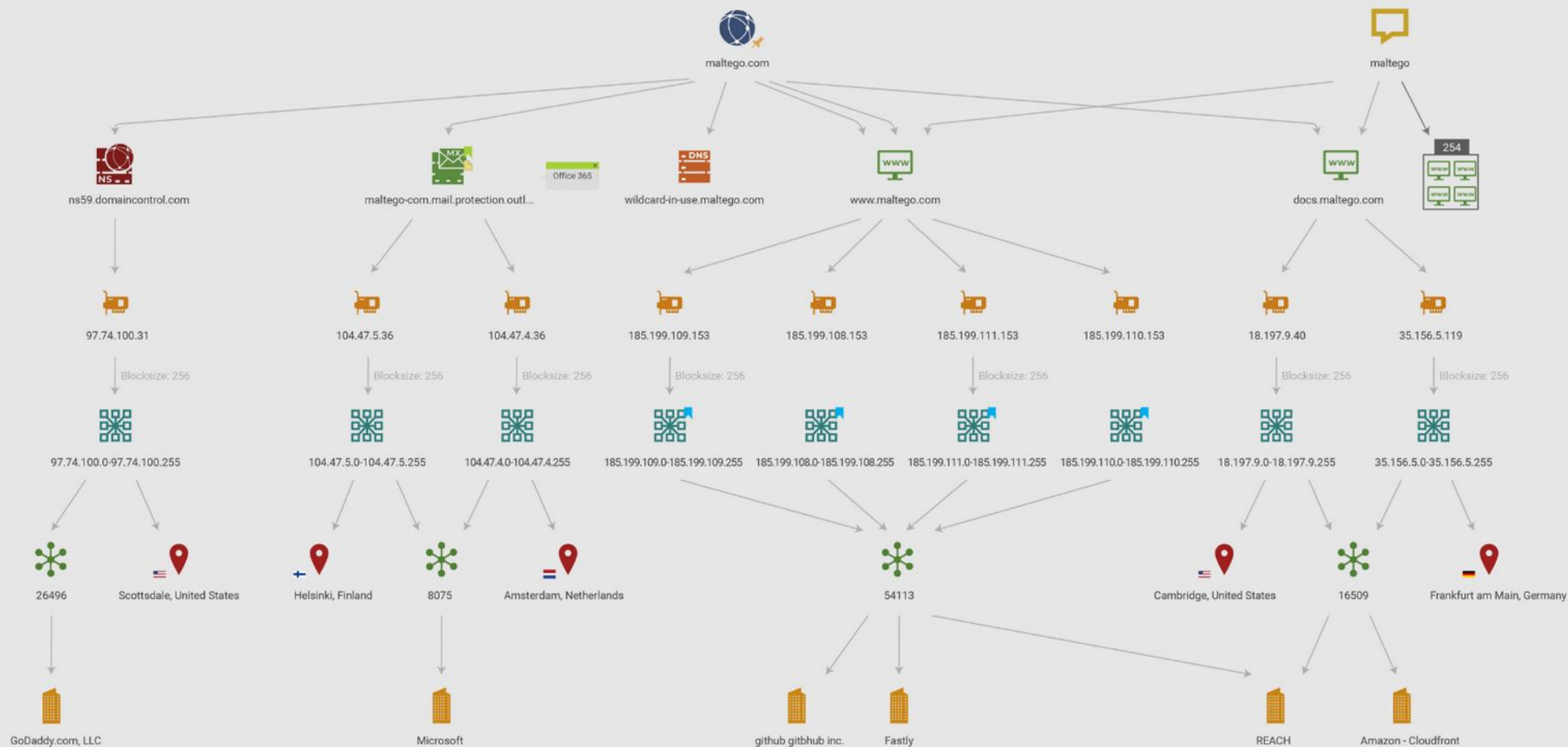
# OSINT (Açık Kaynak İstihbaratı)

Senaryo: Bir şirketin çevrimiçi varlığını analiz etmek.

- Domain Analizi
  - [Whois Lookup](#) ile domain sahibi bilgilerini öğrenme
  - Alt domain taraması ([sublist3r](#)).
- Web Sitesi Analizi
  - [Wayback Machine](#) (web sitesinin eski sürümleri)
  - [Google Dorking](#) (hassas -gizli, özel- dosyalar)
- Sosyal Medya Analizi
  - Şirketin LinkedIn, Twitter ve Facebook hesapları incelemesi
  - Çalışanların sosyal medya profilleri ([Sherlock](#))
- Teknik Analiz
  - Şirketin sunucularının incelenmesi ([Shodan](#))
  - SSL Checker ile SSL sertifikaları inceleme

```
root@kali /h/h/t/Sublist3r (master)# python sublist3r.py -  
  
Sublist3r  
  
# Coded By Ahmed Aboul-Ela - @aboul3la  
  
[-] Enumerating subdomains now for tesla.com  
[-] Searching now in Baidu..  
[-] Searching now in Yahoo..  
[-] Searching now in Google..  
[-] Searching now in Bing..  
[-] Searching now in Ask..  
[-] Searching now in Netcraft..  
[-] Searching now in DNSdumpster..  
[-] Searching now in Virustotal..  
[-] Searching now in ThreatCrowd..  
[-] Searching now in SSL Certificates..  
[-] Searching now in PassiveDNS..
```

# Maltego



# Wireshark ile Trafik İnceleme

The image shows the Wireshark network traffic analysis interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. A display filter bar shows "Apply a display filter ... <Ctrl-/>". The main packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 12) is highlighted in blue. Below the packet list, the packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
10	9.041865	192.168.200.21	192.168.200.135	TCP	66	cisco-sccp(2000) → 7876 [SYN, ACK] Seq=
11	9.047489	192.168.200.135	192.168.200.21	TCP	60	7876 → cisco-sccp(2000) [ACK] Seq=1 Ac
12	9.047526	192.168.200.135	192.168.200.21	TCP	15...	7876 → cisco-sccp(2000) [ACK] Seq=1 Ac
13	9.047543	192.168.200.21	192.168.200.135	TCP	54	cisco-sccp(2000) → 7876 [ACK] Seq=1 Ac
14	9.047559	192.168.200.135	192.168.200.21	TCP	15...	7876 → cisco-sccp(2000) [ACK] Seq=1461
15	9.047567	192.168.200.21	192.168.200.135	TCP	54	cisco-sccp(2000) → 7876 [ACK] Seq=1 Ac
16	9.047570	192.168.200.135	192.168.200.21	TCP	15...	7876 → cisco-sccp(2000) [ACK] Seq=2921
17	9.047574	192.168.200.21	192.168.200.135	TCP	54	cisco-sccp(2000) → 7876 [ACK] Seq=1 Ac
18	9.047577	192.168.200.135	192.168.200.21	TCP	15	7876 → cisco-sccp(2000) [ACK] Seq=4381

Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0  
• Ethernet II, Src: Dell\_96:12:0e (ec:f4:bb:96:12:0e), Dst: Vmware\_b4:90:14 (00:0c:29:b4:90:14)  
• Destination: Vmware\_b4:90:14 (00:0c:29:b4:90:14)  
• Source: Dell\_96:12:0e (ec:f4:bb:96:12:0e)  
Type: IPv4 (0x0800)  
• Internet Protocol Version 4, Src: 192.168.200.135 (192.168.200.135), Dst: 192.168.200.21 (192.168.200.21)  
• Transmission Control Protocol, Src Port: 7876 (7876), Dst Port: cisco-sccp (2000), Seq: 1, Ack: 1, Len: 1460  
• Data (1460 bytes)

0000 00 0c 29 b4 90 14 ec f4 bb 96 12 0e 08 00 45 00 ..)....E  
0010 05 dc 1d 1f 40 00 80 06 c6 0e c0 a8 c8 87 c0 a8 .....@.....  
0020 c8 15 1e c4 07 d0 6a f0 7c f6 6f 9b 26 e0 50 10 .....j. |.o.&P  
0030 04 02 af 99 00 00 0a 0a 0a 0a 0a 0a 4e 65 74 77 .....Netw  
0040 6f 72 6b 20 57 6f 72 6b 69 6e 67 20 47 72 6f 75 ork Work ing Grou  
0050 70 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 p  
0060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  
0070 20 20 20 20 20 20 44 2e 20 57 61 69 74 7a 6d 61 6e D. Waitzman

Source Hardware Address (eth.src), 6 bytes  
Packets: 35 - Displayed: 35 (100.0%)  
Profile: Default

# Metasploit

```
└─(kali㉿kali)-[/var/lib]
```

```
$ msfconsole
```

```
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```

```

Home
      . ' ##### ; "
. _ , . ;  0  0  ;  _ , .
" 00000 ' , ' 00  00000 ' , ' 00000 "
' - 0000000000000000  0000000000000000 0 ;
  . 000000000000000  0000000000000000 '
    "-- ' 0000  - 0  0  , ' - ' -- "
      " 0 ' ;  0  0  . ' ; '
        | 00000 0000  0  .
          ' 0000 00  00  ,
            . 00000  000  .
              ' , 00  0  ;
                ( 3 C )  / | _ _ / Metasploit! \
              ; 0 ' . _ * _ , "  \ _ _ \
                '( , , , , , " /

```

```

+ -- ==[ metasploit v6.4.45-dev ]
+ -- ==[ 2490 exploits - 1281 auxiliary - 431 post ]
+ -- ==[ 1466 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

```

Metasploit Documentation: <https://docs.metasploit.com/>


nsf6 &gt;



# Zafiyet Tarama (GVM)





← → ↻ 🏠 <https://127.0.0.1:9392/feedstatus>

[Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#)

 **Greenbone**  
Security Assistant

[Dashboards](#) [Scans](#) [Assets](#) [Resilience](#) [SecInfo](#) [Con](#)

🔍 **Feed Status**

Type	Content	Origin	Version	Status
NVT	 <a href="#">NVTs</a>	Greenbone Community Feed	20250205T0643	<b>Current</b>
SCAP	 <a href="#">CVEs</a> <a href="#">CPE</a> <a href="#">CPEs</a>	Greenbone SCAP Data Feed	20250205T0506	<b>Update in progress...</b>
CERT	 <a href="#">CERT-Bund Advisories</a>  <a href="#">DFN-CERT Advisories</a>	Greenbone CERT Data Feed	20250205T0822	<b>Update in progress...</b>

# Son Kullanıcı İçin Tedbirler - 1

- Güncellemeler (Windows, tarayıcı, Java, vb.)
- Antivirüs ve firewall (Defender iyidir)
- İSS Aile filtresi. DNS tabanlı filtreler.
- Korsan yazılım kullanma. Yaygın olmayan program (veya eklenti) kullanma. Yazılımları, orijinal kaynağı dışında bir yerden indirme.
- İnternet'te şüpheli ol. Yayılmasını istemediğin verilerini kimse ile paylaşma. İnternet'te gerçek anlamda "silme" yok.
- Emin olmadığın kablosuz ağlara bağlanma.
- Bir şey bedava ise orada ürün sen olabilirsiniz!

# Son Kullanıcı İçin Tedbirler - 2

- Oltalamaya dikkat et. "Hediye kazandın", "faturan 3 bin lira oldu", vb.
- MFA kimlik doğrulaması. Güçlü parola kullan. Parola yöneticisi kullan. Kuantum bilgisayar çıkarsa bugünkü parolalar da güçlü olamayabilir.
- Yedeklemeyi ihmal etme. Veriler çok önemli ise: 3-2-1 kuralı
- Tarayıcıda oturumu açık bırakma. Ortak kullanılan bilgisayarlarda veya halka açık cihazlarda (kütüphane, internet kafe) oturum açtıktan sonra çıkış yapmayı unutmayın.
- İzinleri kontrol et: Telefon ve bilgisayardaki uygulamaların gereksiz izinler istemediğinden emin olun. Örneğin, bir el feneri uygulamasının rehberinize erişmesi gereksizdir.

# Güncel Popüler Tehditler

- Ransomware (fidye yazılımı)
- Trojan (RAT) gibi kötü yazılımlar
- Ortalama. Sosyal medya hesaplarının ele geçirilmesinde en önemlilerden birisi bu. Akrabalarımız, adresimiz ve telefon numaramız gibi bilgiler kötü kişilerin elinde. Şantaj ve tehditler olabiliyor.
- Botnet (zombi bilgisayarlar).
- Açık kablosuz ağlar (MITM).
- Hedefli saldırılar (APT)
- Deepfake ve Yapay Zeka Destekli Dolandırıcılıklar: Gerçekçi sahte videolar ve ses kayıtları kullanılarak kimlik avı ve dolandırıcılık girişimleri artıyor.
- QR Kod Dolandırıcılığı: Sahte QR kodlar, sizi kötü amaçlı sitelere yönlendirebilir. Tanımadığınız yerlerde QR kod tararken dikkatli olun.





# SON