

ORTADAKİ ADAM SALDIRISI

Karamanoğlu Mehmetbey Üniversitesi

Bilgisayar Mühendisliği

Bilgisayar Ağları Final Raporu

**İSMET ARSLAN
191312073**

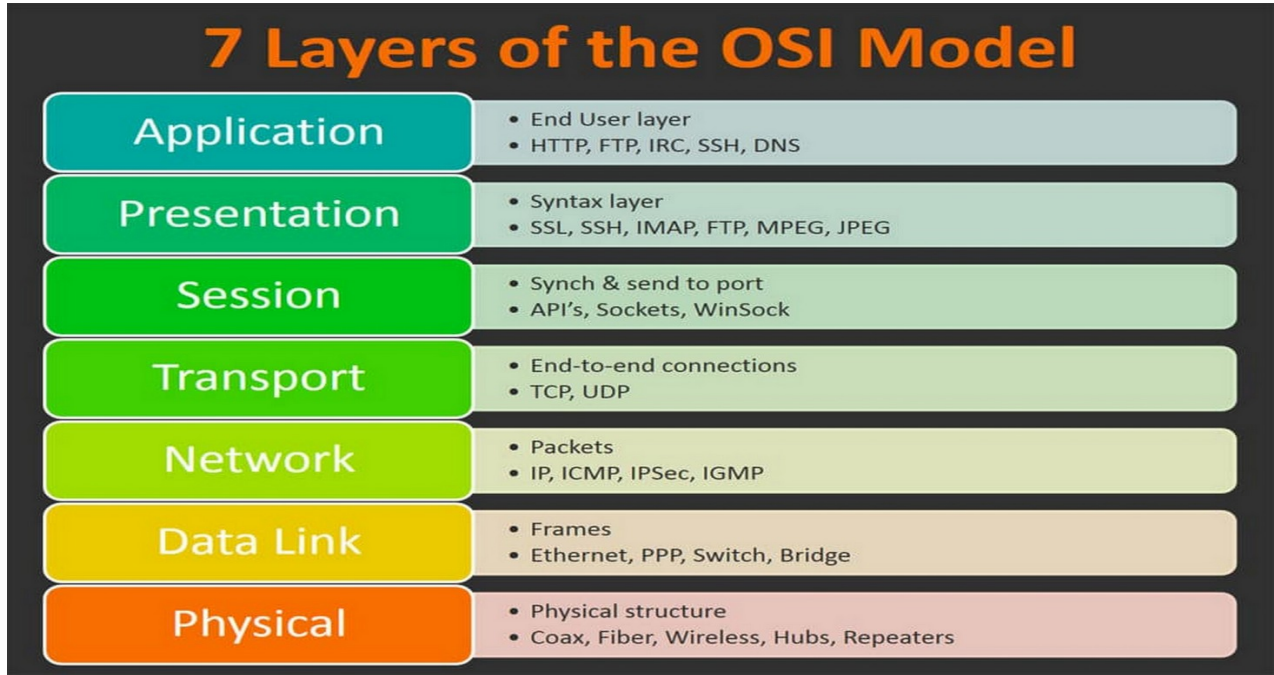
OCAK 2021

İÇİNDEKİLER

LAYER 2 (2. KATMAN) SALRIDILARI NEDEN KRİTİKTİR ?.....	3
MAN IN THE MIDDLE ATTACK (ORTADAKİ ADAM SALDIRISI).....	3
ARP POISONING (ARP ZEHİRLENMESİ).....	4
ARP POISONING İLE ORTADAKİ ADAM SALDIRISI UYGULAMASI.....	6
ARP POISONING ÖNLEMLERİ.....	14
ARP POISONING TESPİTİ YAPAN PYTHON KODU.....	15
KAYNAKÇA.....	16

LAYER 2 SALDIRILARI NEDEN KRİTİKTİR ?

OSI modelinin 2. katmanı (layer 2) veri bağlantısı katmanıdır. Data link katmanı en zayıf görünen ve güvenliği göz ardı edilen katmandır. Saldırganların genellikle dışarıdan geleceği düşünülerek çeşitli önlemler alınmaya ve güvenlik cihazları kurulmaya çalışılır. Halbuki içeriden gelebilecek saldırılar göz ardı edilir. FBI'ın 2004 yılında yaptığı bir araştırmaya göre memnun olmayan çalışanların içeriden saldırı yapabilme ihtimalini %56 olarak belirlemiştir. Tüm verinin 2. katman üzerinden aktığı düşünülürse ; saldırgan bu katmana erişim sağladığında üst katmanlarda alınan tüm güvenlik önlemleri anlamsız kalacaktır.



MAN IN THE MIDDLE ATTACK (ORTADAKİ ADAM SALDIRISI)

Türkçe karşılığı olarak Ortadaki Adam Saldırısı ya da Aradaki Adam Saldırısı, bir ağ içerisinde hedef ile ağ bileşenleri (switch, server, router) arasında geçen trafiği dinlemek, değiştirmek olarak tanımlanır. MITM'de iki taraf arasındaki iletişim kesilebilir ya da yanıltıcı bir iletişim oluşturulabilir. Bu saldırı ağ üzerindeki paketleri yakalayarak manipüle etmek olarak özetlenebilir.

Kablosuz ağlarda paketler tamamen broadcast olarak yayıldığı için herhangi bir ön işleme gerek olmaksızın tüm paketler saldırgan tarafından yakalanabilir. Bu sebeple ücretsiz Wi-Fi sağlayan alanlar, MITM saldırısının gerçekleştirilmesi için en uygun alanlardır. Şifrelenmemiş paketlerin içerikleri kolaylıkla okunabilir. Wifi alanındaki saldırganlar network trafiğini kendi üzerilerinden geçecek şekilde yönlendirirler. Böylece o ağdaki kişilerin trafiği saldırgan üzerinden akmaya başlar. Bu Trafiği ele geçiren saldırgan birçok kişisel verileri elde edebilir.

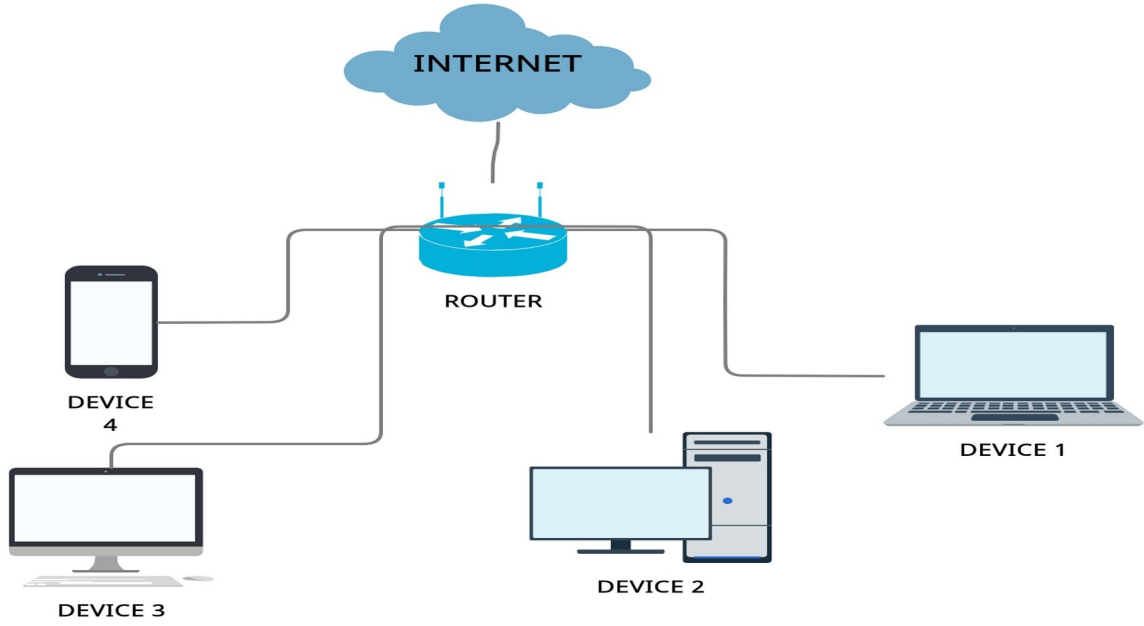
MITM saldırıları Layer 2 (OSI katmanı, Data Link) içerisinde gerçekleştiği için, saldırgan başarılı olduktan sonra tüm trafiğe hakim olabilmektedir. Bu hakimiyet şifreli olan "https" trafiğinden şifresiz trafiklere kadar sınırsızdır.

Ağ Güvenliği konusunda oldukça bilinen bir saldırı türü olmasına karşın en az tedbir alınan saldırı tipidir.

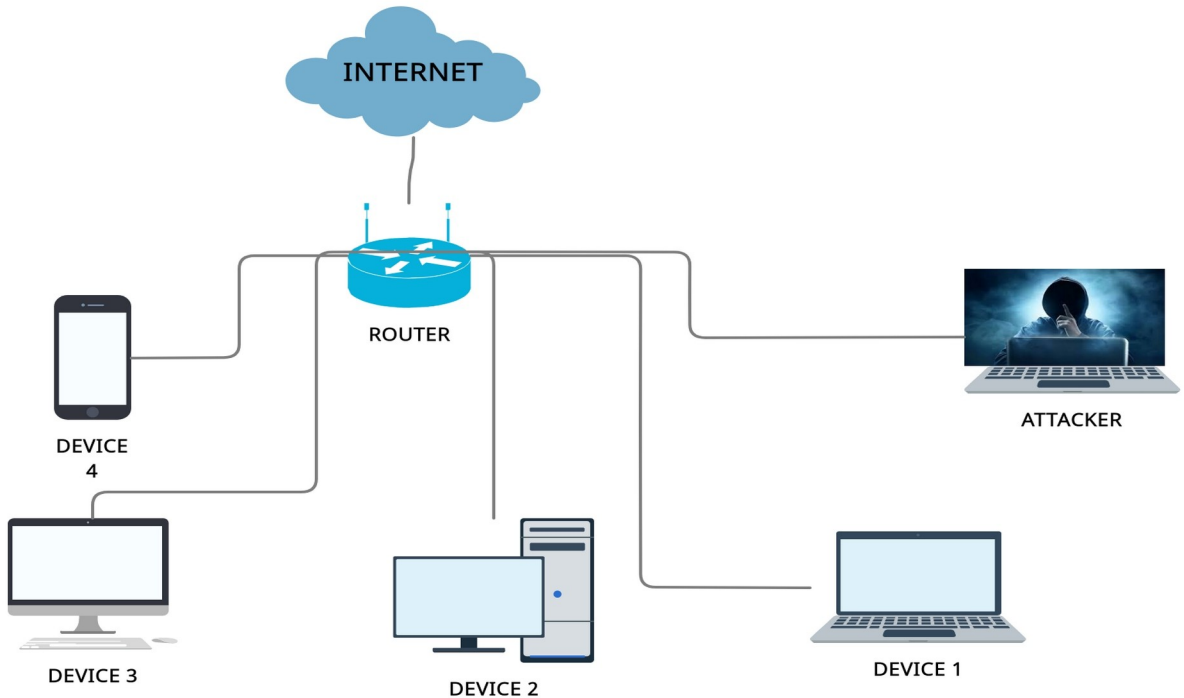
ARP POISONING (ARP ZEHİRLENMESİ)

ARP (Address Resolution Protocol) protokolü MAC adreslerinin çözülmesini sağlar. Yani IP adreslerini MAC adreslerine çevirir. Bu çevirme işlemini yapabilmek için MAC adreslerini ve IP adreslerini cahce denilen bir tabloda tutar. ARP protokolü OSI modelinin 2. katmanında (Data-Link) çalışır.

ARP Spoofing (ARP Kandırmacısı)/ARP Poisoning(ARP Zehirlenmesi) ise ARP paketlerinin kullanılarak yerel ağa bağlı olan cihazların gönderdiği paketlerin bu cihazların kandırılmasına ve kandırılmış cihazların ağ trafiğini izlemeye ve manipüle edilmesidir.



Yukarıdaki LAN'a bir saldırganın dahil olduğunu varsayalım.



Saldırgan router'a "ben device 1'im" diye broadcast paketleri gönderir. Router ARP tablosunu belirli aralıklarla bu gelen mesajlara göre düzenlediği için bir süre sonra device 1 olarak artık saldırgan cihaz tutulmaya başlar.

ARP SPOOF ÖNCESİ ROUTER ARP TABLOSU

	MAC	IP
device 1:	FF:DC:6E:5A	192.168.1.3
device 2:	DE:76:12:AC	192.168.1.5
device 3:	56:AD:CE:FF	192.168.1.4
device 4:	1F:E4:DD:AA	192.168.1.10

ARP SPOOF SONRASI ROUTER ARP TABLOSU

	MAC	IP
device 1:	AA:BB:CC:DD	192.168.1.3
device 2:	DE:76:12:AC	192.168.1.5
device 3:	56:AD:CE:FF	192.168.1.4
device 4:	1F:E4:DD:AA	192.168.1.10
attacker:	AA:BB:CC:DD	192.168.1.17

Görüldüğü gibi router artık saldırganın MAC adresini device 1'in MAC adresi olduğunu zannediyor.

Sonrasında saldırgan benzer bir işlemi device 1'e "ben router'ım" diye broadcast yapmaya başlar. Device 1'de bir süre sonra saldırganı router zannetmeye başlar.

ARP SPOOF ÖNCESİ DEVICE 1 ARP TABLOSU

	MAC	IP
router:	CC:FF:EE:BB	192.168.1.1

ARP SPOOF SONRASI DEVICE 1 ARP TABLOSU

	MAC	IP
router:	AA:BB:CC:DD	192.168.1.1
attacker:	AA:BB:CC:DD	192.168.1.17

Görüldüğü gibi device 1 artık saldırganı router olarak tanıyor. Artık device 1'in ağ trafiği saldırgan üzerinden akmaya başlayacaktır. Saldırgan gelen trafiği istediği gibi manipüle ederek router'a device 1 gibi gönderir.

ARP POISONING İLE ORTADAKİ ADAM SALDIRISI UYGULAMASI

Kablosuz ağlarda güvenlik önlemi olarak gizli SSID kullanılıyor ya da bulunduğumuz ortamda birden fazla kablosuz ağ bulunuyor olabilir. Saldırıların ilk aşaması da bilgi toplamak olduğu için etrafımızda bulunan tüm ağları tarıyoruz.

Aircrack-ng araç seti içerisinde airmon-ng aracı ile ağ kartlarımızı monitör moda alabiliriz. Öncelikle tüm işlemlerin sonlandırılmış olduğundan emin olabilmek için

airmon-ng check kill
komutunu giriyoruz.

Ardından

airmon-ng check

komutu ile arka planda airmon-ng üzerinde çalışan bir süreç olmadığından emin oluyoruz.

Eğer devam eden süreç varsa *airmon-ng check kill* komutu ile sonlandırılır.

```
try@kali: ~  
Dosya Eylemler Düzen Görünüm Yardım  
try@kali:~$ sudo airmon-ng check kill  
Killing these processes:  
PID Name  
1250 wpa_supplicant
```

Ağ kartımızı monitör moda almak için

airmon-ng start wlan 0

komutunu kullanıyoruz.

```
try@kali: ~  
Dosya Eylemler Düzen Görünüm Yardım  
try@kali:~$ sudo airmon-ng start wlan0  
  
PHY      Interface      Driver      Chipset  
phy0     wlan0          rtl8187     Realtek Semiconductor Corp. RTL81  
87  
(monitor mode enabled)
```

Ardından kismet aracı ile grafiksel olarak etrafımızda bulunan tüm kablosuz ağların bilgilerini görüntülüyoruz.

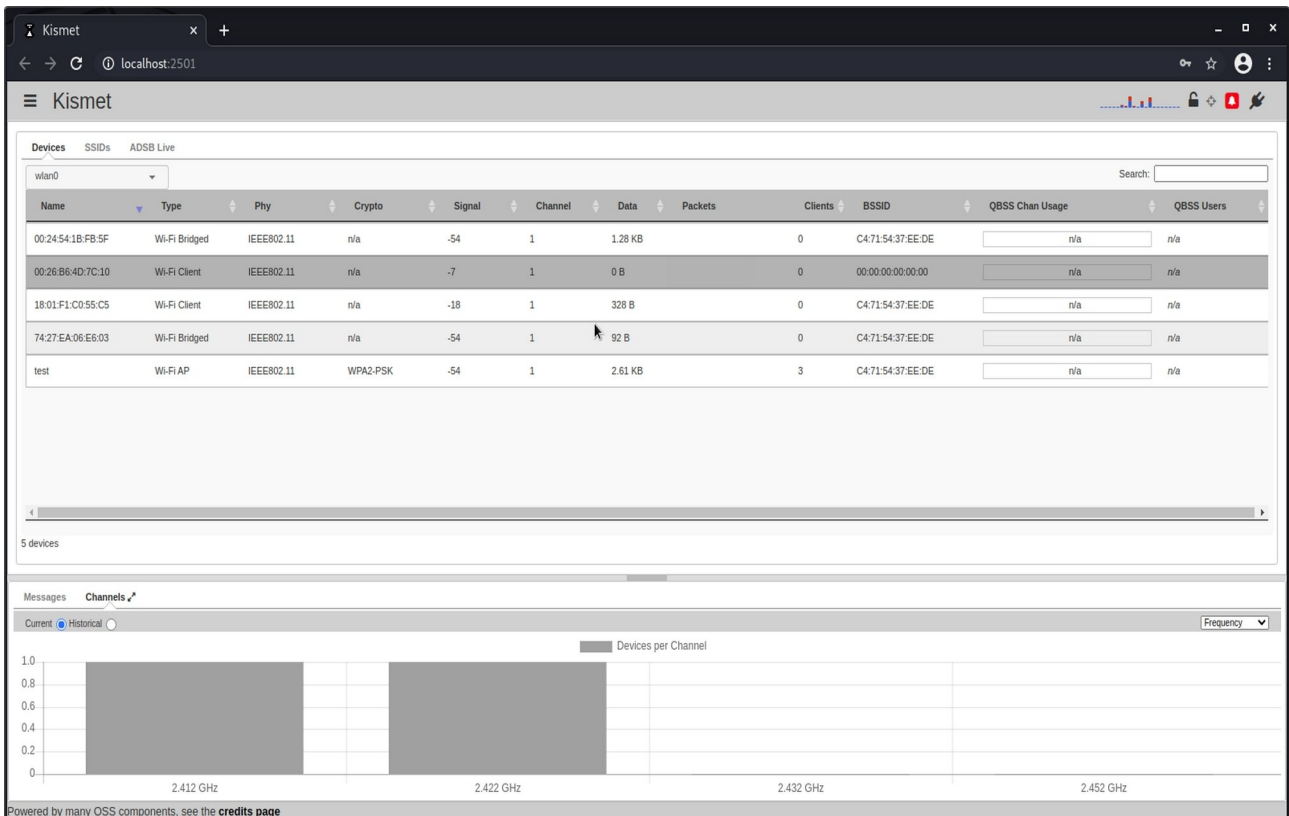
kismet -c wlan0

komutu ile kismet aracı çalıştırılır.

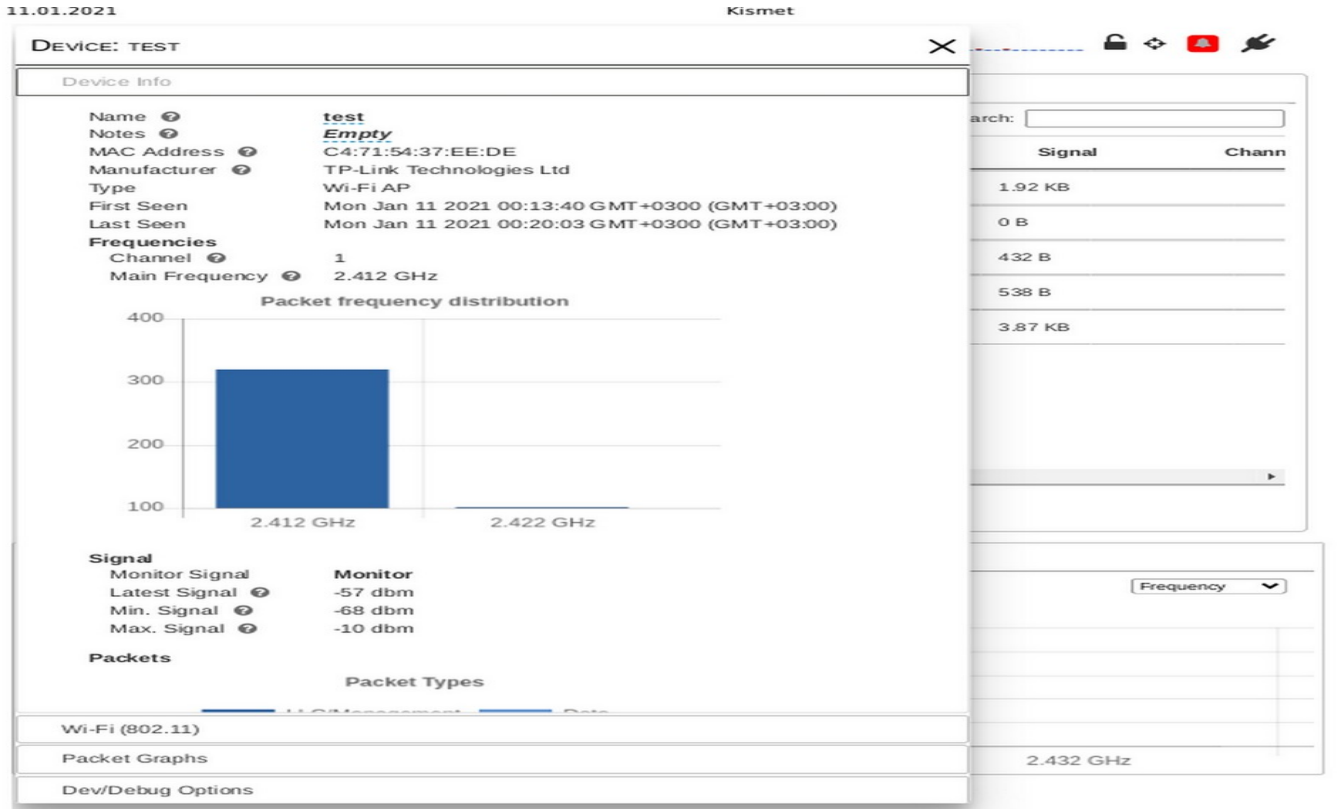
```
try@kali: ~  
Dosya Eylemler Düzen Görünüm Yardım  
try@kali:~$ sudo kismet -c wlan0
```

```
try@kali: ~  
Dosya Eylemler Düzen Görünüm Yardım  
KISMET - Point your browser to http://localhost:2501 (or the address of this system) for  
INFO: Opened kismetdb log file './Kismet-20210110-21-22-37-1.kismet'  
INFO: Saving packets to the Kismet database log.  
ALERT: rootuser Kismet is running as root; this is less secure. If you  
        are running Kismet at boot via systemd, make sure to use `systemctl  
        edit kismet.service` to change the user. For more information, see  
        the Kismet README for setting up Kismet with minimal privileges.  
INFO: Starting Kismet web server...  
INFO: (HTTPD) Started http server on port 2501  
INFO: Found type 'linuxwifi' for 'wlan0'  
INFO: wlan0 interface 'wlan0' is already in monitor mode  
INFO: wlan0 finished configuring wlan0, ready to capture  
INFO: Data source 'wlan0' launched successfully  
INFO: Detected new 802.11 Wi-Fi access point C4:71:54:37:EE:DE  
INFO: 802.11 Wi-Fi device C4:71:54:37:EE:DE advertising SSID 'test'
```

Kismet aracı local host üzerinde çalışan bir grafik arayüzü sunuyor. <http://localhost:2501> adresinden erişilebilir.



Detaylı görünüm için çift tıklayınca çeşitli kategoriler ile bilgileri görüntüleyebiliyoruz.



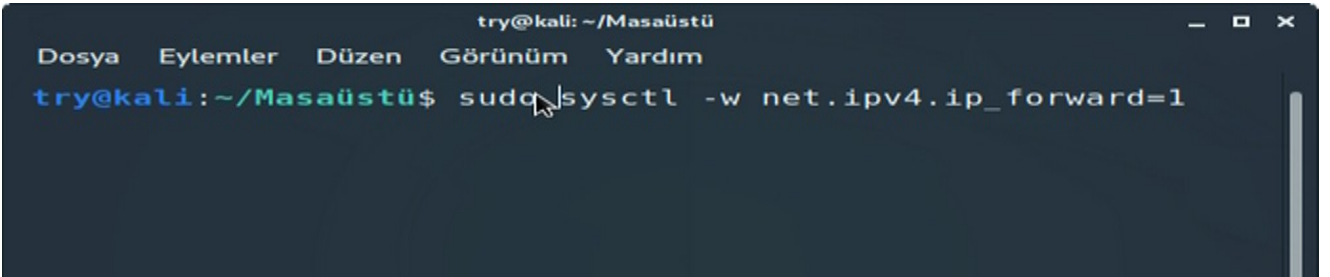
ARP Poisoning Saldırısı:

ARP Poisoning Saldırısı için kullanılabilircek birçok araç olsa da biz Kali-Linux üzerinde gelen Ettercap'ı kullanacağız.

Ip yönlendirmeyi aktif hale getirmek için /proc/sys/net/ipv4 dizinin içerisinde bulunan ip_forward dosyasının içeriğini 1 olarak değiştirmemiz gerekiyor.

```
sudo /proc/sys/net/proc/sys/net/ipv4/ip_forward=1
```

Komutu ile IP yönlendirmesini etkinleştiriyoruz.

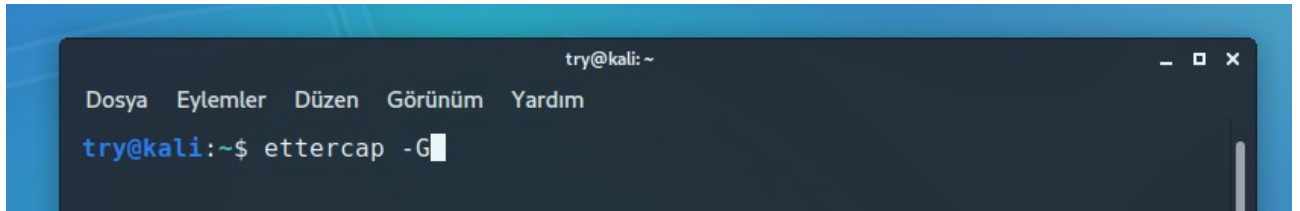


```
try@kali: ~/Masaüstü
Dosya Eylemler Düzen Görünüm Yardım
try@kali:~/Masaüstü$ sudo sysctl -w net.ipv4.ip_forward=1
```

Sonrasında Ettercap aracını grafiksel olarak kullanabilmek için

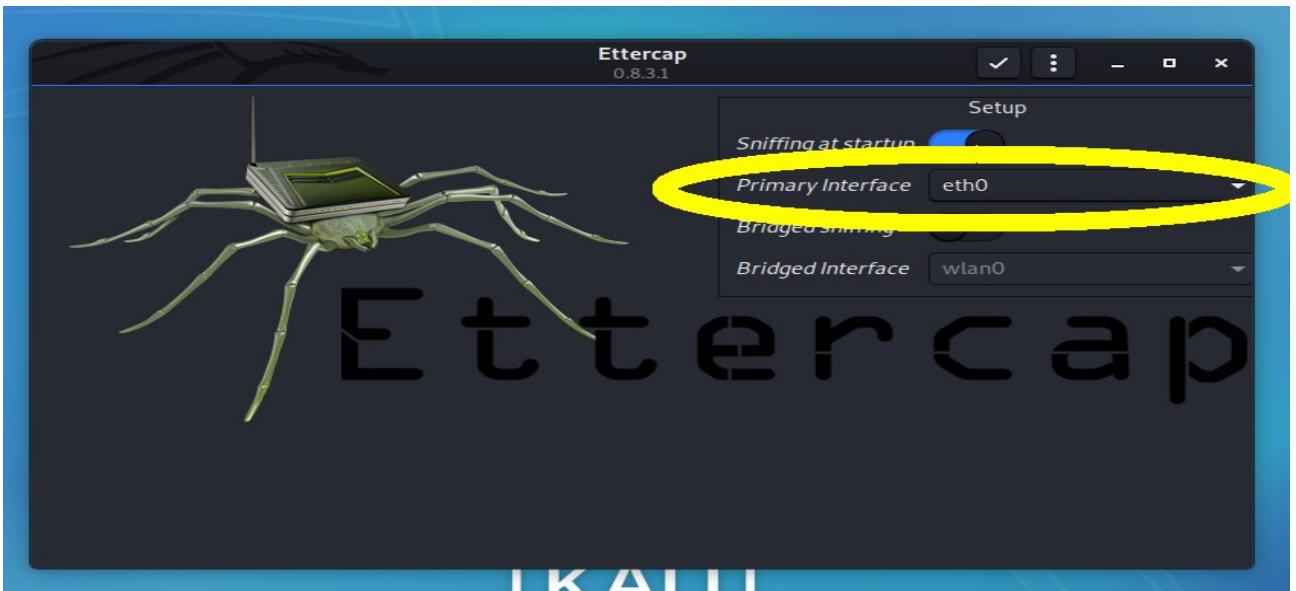
```
ettercap -G
```

komutunu çalıştırıyoruz.



```
try@kali: ~
Dosya Eylemler Düzen Görünüm Yardım
try@kali:~$ ettercap -G
```

Ardından sniff etmek istediğimiz ağ arayüzünü seçiyoruz.

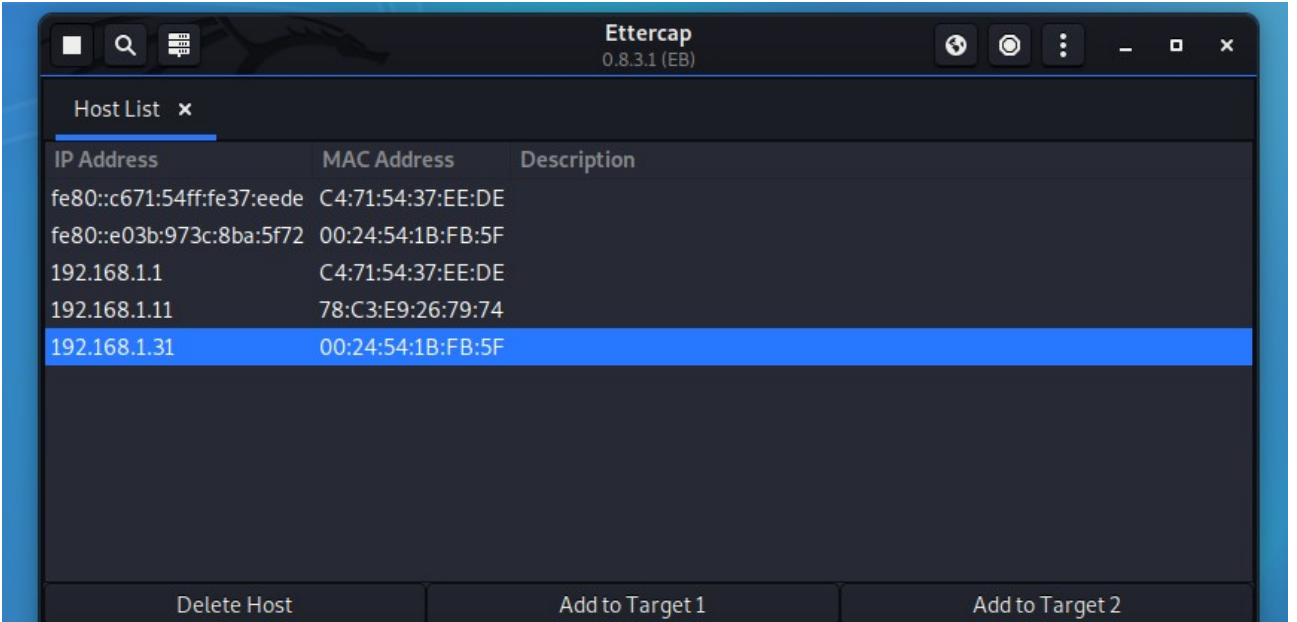


Ağ kartımız wlan0 üzerinde çalıştığı için wlan0 interface'ini seçiyor ve tik işaretine tıklıyoruz.

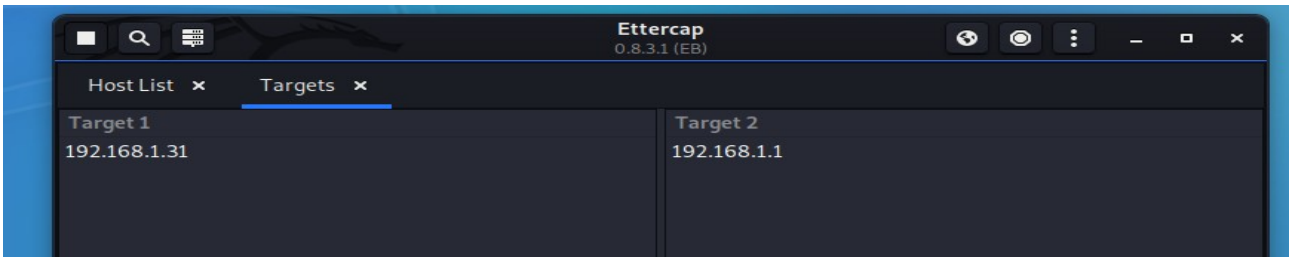


Daha sonrasında “Host” ve “Scan For Host” srasını takip ederek ağ üzerinde bulunan istemcileri tarıyoruz.

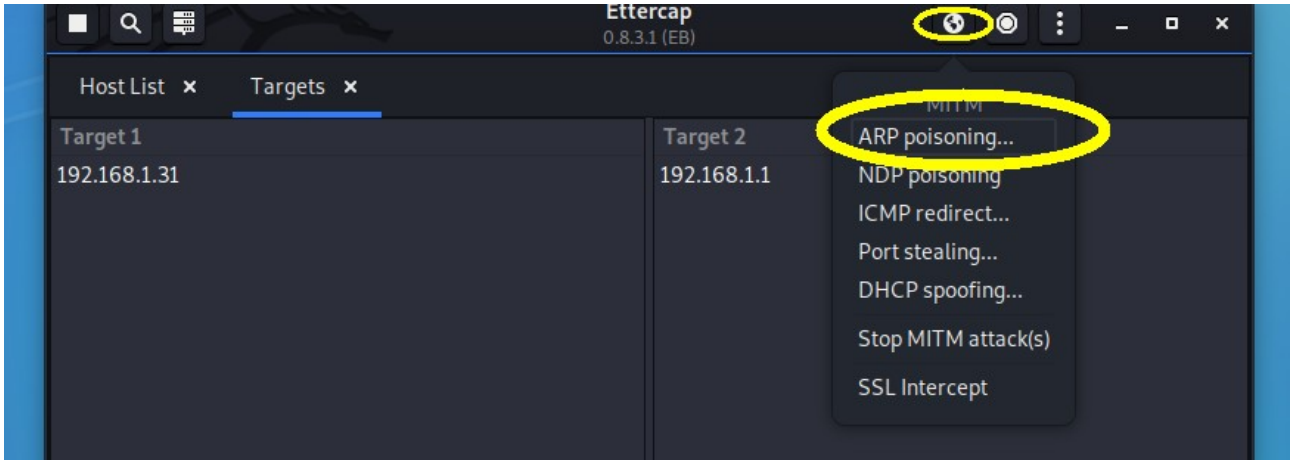
Sonrasında hedef aldığımız cihazı Target 1, router cihazını ise Target 2 olarak ekliyoruz.



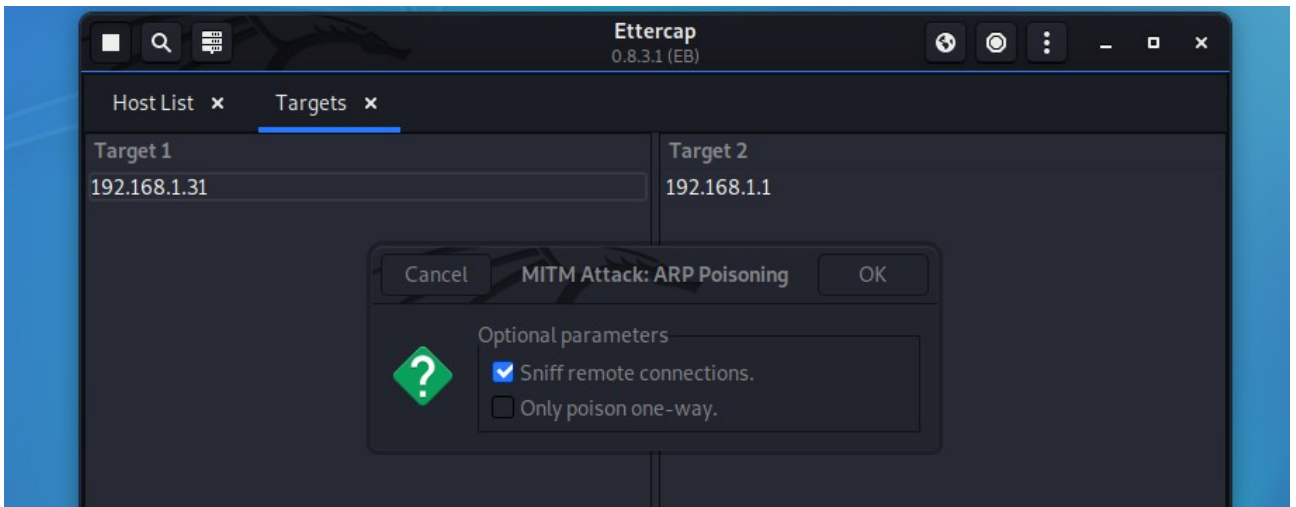
Target current seçeneği ile seçmiş olduğumuz hedeflerin IP adreslerini görüntüleyebiliriz.



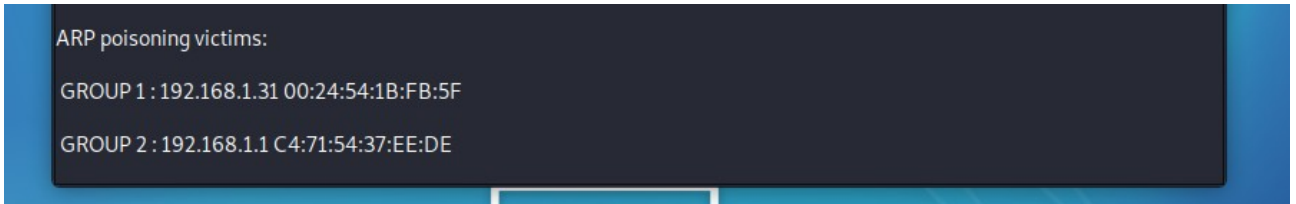
Bu adımdan sonra ARP Poisoning yaparak Man In The Middle saldırısını başlatabiliriz.



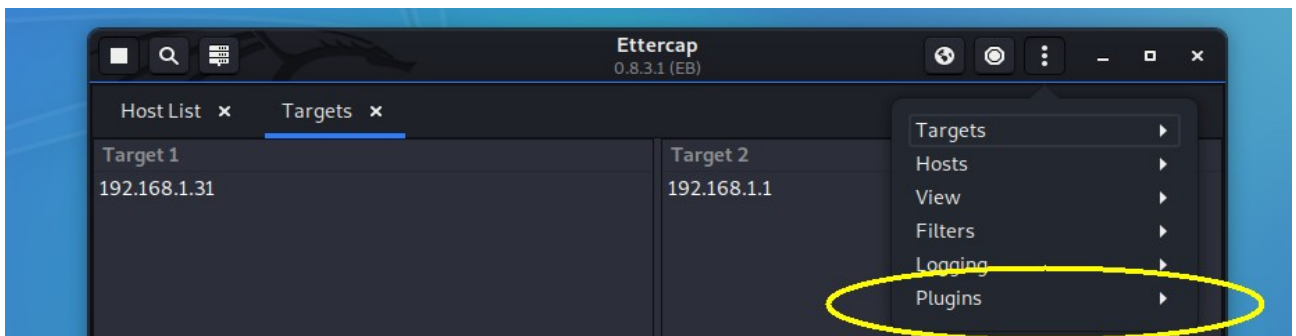
Default olarak uzaktan sniffing için işaretli gelen parametre seçeneğini onaylayalım.

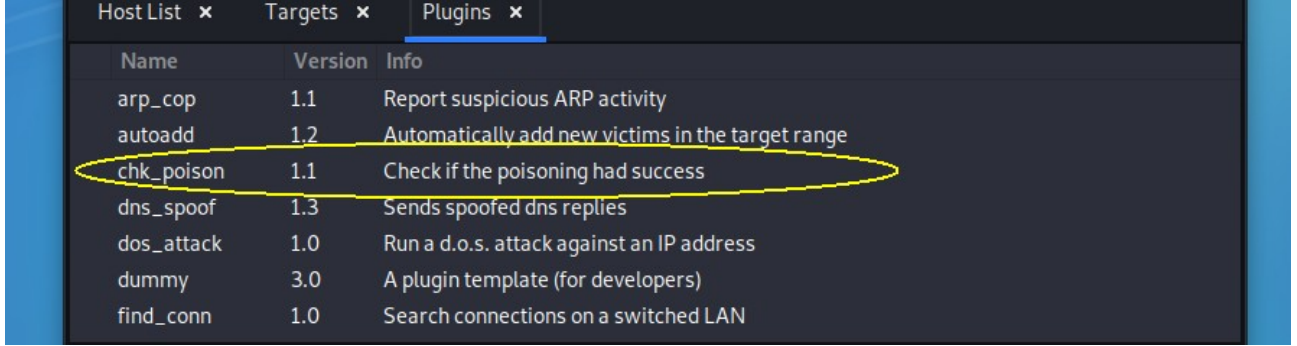
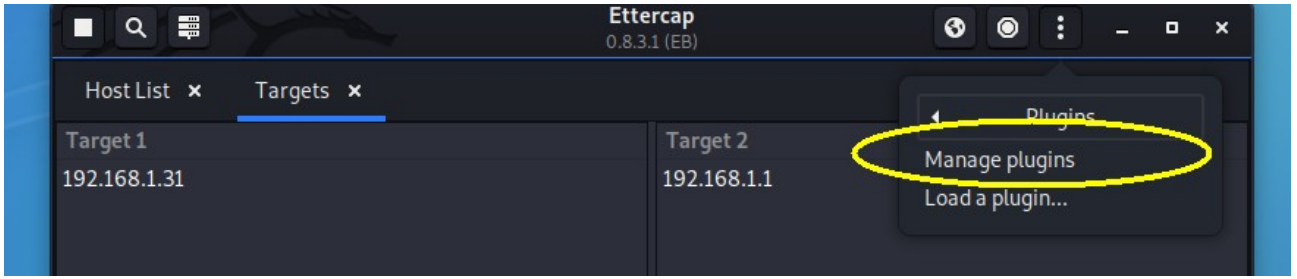


OK butonuna tıkladığımızda ARP Poisoning başlatılmış olur.



Saldırının başarılı olup olmadığını denetlemek için “Plugins” sekmesinden “Manage Plugins” sekmesini seçip “chk_poison” isimli eklenti ile Poisoning saldırısının başarılı olup olmadığını test edebiliriz.

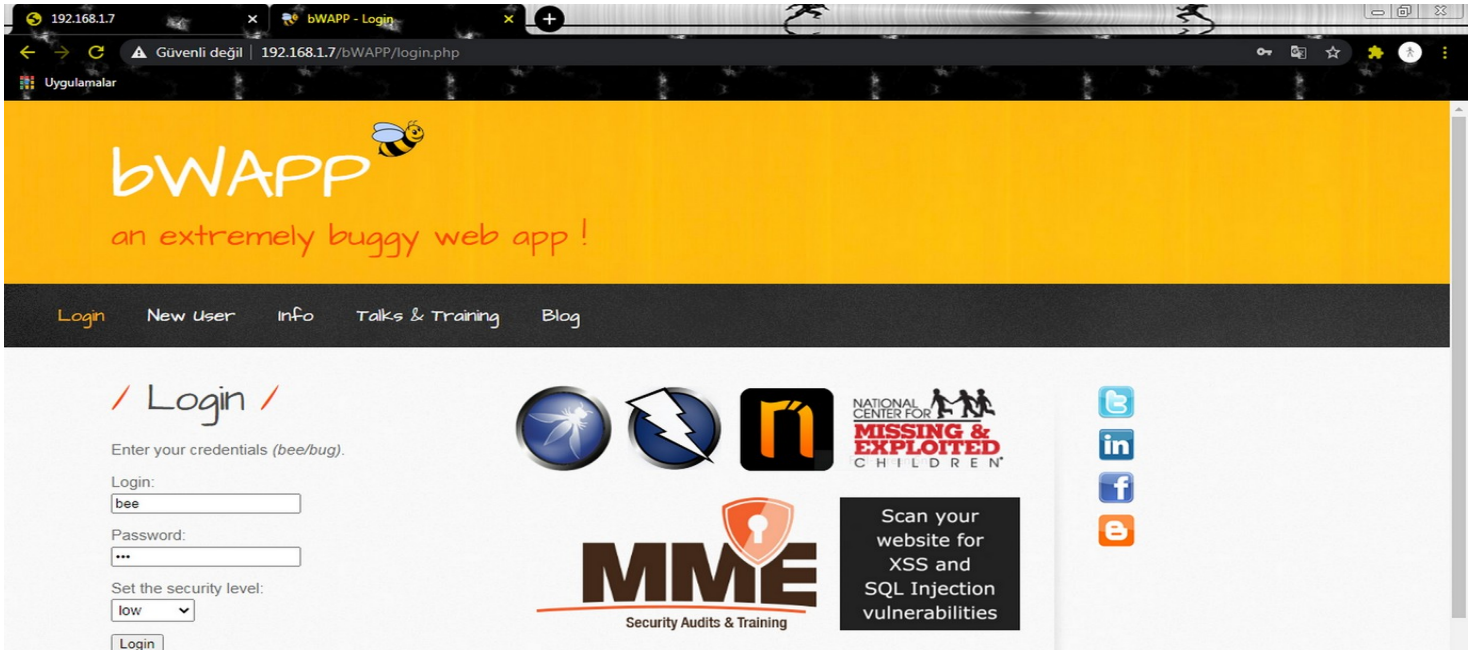




Eğer Poisoning başarılı ise şöyle bir çıktı alırsınız:

```
chk_poison: Checking poisoning status...  
chk_poison: Poisoning process successful!
```

Şimdi hedefimizin ağ üzerinde yaptığı UDP trafiği izlemek için WireShark aracını kullanalım. Hedef makinemizden local ağda oluşturduğumuz bir laboratuvar ortamına giriş yapmaya çalışalım. Eğer tüm adımlar başarılı ise hedefimizin ağ trafiği saldırgan cihaz üzerinden akacak ve böylece giriş bilgilerini elde edebileceğiz.



Sayfaya geldiğimizi saldırgan cihazdan görebiliriz.

No.	Time	Source	Destination	Protocol	Length	Info
520	48.523126956	192.168.1.31	192.168.1.7	HTTP	677	GET /bwAPP/login.php HTTP/1.1
526	48.527177920	192.168.1.7	192.168.1.31	HTTP	194	HTTP/1.1 200 OK (text/html)
529	49.248849724	192.168.1.31	192.168.1.7	HTTP	583	GET /bwAPP/images/favicon.ico HTTP/1.1
531	49.249454737	192.168.1.7	192.168.1.31	HTTP	153	HTTP/1.1 200 OK (image/x-icon)

Frame 520: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface eth0, id 0

Ethernet II, Src: SamsungE_1b:fb:5f (00:24:54:1b:fb:5f), Dst: PcsCompu_76:22:7d (08:00:27:76:22:7d)

Internet Protocol Version 4, Src: 192.168.1.31, Dst: 192.168.1.7

Transmission Control Protocol, Src Port: 1159, Dst Port: 80, Seq: 1, Ack: 1, Len: 611

Hypertext Transfer Protocol

0000	08 00 27 76 22 7d 00 24 54 1b fb 5f 08 00 45 00	..v"}.\$ T _ _ E
0010	02 97 2a 14 40 00 40 06 8a d6 c0 a8 01 1f c0 a8	..*.@ _ _ _ _
0020	01 07 04 87 00 50 c5 4a 46 01 9b 85 1c e4 80 18	..P.J F _ _ _ _
0030	41 0c fa 79 00 00 01 01 08 0a 00 01 9e 65 00 30	A..y.. _ _ _ _ e.0
0040	b2 dd 47 45 54 20 2f 62 57 41 50 50 2f 6c 6f 67	..GET /b WAPP/log
0050	69 6e 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d	in.php H TTP/1.1
0060	0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 31	..Host: 1 92.168.1
0070	2e 37 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20	..7..Conn ection:
0080	6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68	keep-alive..Cach
0090	65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61	e-Contro l: max-a
00a0	67 65 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e	ge=0..Up grade-In
00b0	73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a	secure-R equests:
00c0	20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20	1..User -Agent:

Hypertext Transfer Protocol: Protocol

Packets: 1399 · Displayed: 4 (0.3%)

Profile: Default

Görüldüğü gibi hedef makinemiz 192.168.1.7 adresine http ile bağlantı isteği göndermiş ve geriye yanıt almıştır.

Şimdi kullanıcı adı olarak “bee” ve parola olarak “bug” verilerini girip, saldırgan makineden yakalamaya çalışalım.

FileEditViewCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

http

<

Görüldüğü gibi bir login yakaladık. Detaylara bakmak için paketi inceleyelim.

```
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si...
Referer: http://192.168.1.7/bWAPP/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
Cookie: PHPSESSID=070bf0ea406c8605d8be8058c20c54d2; security_level=0\r\n
sec-gpc: 1\r\n
\r\n
[Full request URI: http://192.168.1.7/bWAPP/login.php]
[HTTP request 1/2]
[Response in frame: 1444]
[Next request in frame: 1445]
File Data: 51 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "login" = "bee"
    Key: login
    Value: bee
  Form item: "password" = "bug"
  Form item: "security_level" = "0"
  Form item: "form" = "submit"
01d0 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 l;q=0.9, image/av
01e0 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d if,image /webp,im
01f0 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 age/apng , /*;q=0
0200 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 .8,appli cation/s
0210 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 igned-ex change;v
0220 3d 62 33 3b 71 3d 30 2e 39 0d 0a 52 65 66 65 72 =b3;q=0. 9..Refer
0230 65 72 3a 20 68 74 74 70 3a 2f 2f 31 39 32 2e 31 er: http ://192.1
0240 36 38 2e 31 2e 37 2f 62 57 41 50 50 2f 6c 6f 67 68.1.7/b WAPP/log
0250 69 6e 2e 70 68 70 0d 0a 41 63 63 65 70 74 2d 45 in.php.. Accept-E
0260 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d
0270 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c eflate.. Accept-L
0280 61 6e 67 75 61 67 65 3a 20 74 72 2d 54 52 2c 74 anguage: tr-TR,t
0290 72 3b 71 3d 30 2e 39 2c 65 6e 2d 55 53 3b 71 3d r;q=0.9, en-US;q=
02a0 30 2e 38 2c 65 6e 3b 71 3d 30 2e 37 0d 0a 43 6f 0.8,en;q =0.7..Co
02b0 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d okie: PH PSESSID=
02c0 30 37 30 62 66 30 65 61 34 30 36 63 38 36 30 35 070bf0ea 406c8605
02d0 64 38 62 65 38 30 35 38 63 32 30 63 35 34 64 32 d8be8058 c20c54d2
02e0 3b 20 73 65 63 75 72 69 74 79 5f 6c 65 76 65 6c ; securi ty_level
02f0 3d 30 0d 0a 73 65 63 2d 67 70 63 3a 20 31 0d 0a =0..sec- gpc: 1..
0300 0d 0a 6c 6f 67 69 6e 3d 62 65 65 26 70 61 73 73 login= bee&pass
0310 77 6f 72 64 3d 62 75 67 26 73 65 63 75 72 69 74 word=bug &securit
0320 79 5f 6c 65 76 65 6c 3d 30 26 66 6f 72 6d 3d 73 y_level= 0&form=s
0330 75 62 6d 69 74 ubmit
```

Kullanıcı adı ve parolası http isteği içerisinde şifrelenmeden gittiği için elde edilmiş oldu.

ARP POISONING ÖNLEMLERİ

- 1- Static ARP: Arp tablosunun statik olarak doldurulması arp anonslarına ihtiyacı ortadan kaldıracak için bu saldırı önlenmiş olur. Ancak büyük networklerde için uygulanabilir bir yöntem değildir.
- 2- Encryption: Network üzerinde akan trafik şifrelenirse paketler ele geçirilse dahi okunamayacağı için işe yaramaz olacaktır. Aynı zamanda şifrenin kırılması için uzun zaman kaybına neden olacağı için saldırganın dikkatinin dağılması da olasıdır.
- 3- Subnetting: Networkü küçük Vlan(Virtual Local Area Network)'lere bölmek ve yetkili kullanıcıları dış ortamdan soyutlamak ARP poisoning saldırısının yüzeyini azaltmaktadır.
- 4- Network ürünlerinde varsa ARP security veya Dynamic ARP Inspection özellikleri aktif hale getirilerek saldırı önenebilir.
- 5- İç networkte ARP Watcher kullanarak sistemi gözlemlemek. ArpON ve Arpalert gibi açık kaynak kodlu araçlar kullanılarak ARP protokolünün güvenli bir şekilde çalışması sağlanmış olur.

ARP POISONING TESPİTİ YAPAN PYTHON KODU

```
import os
from Tkinter import *

def Alert ():
    root=Tk()
    root.title('Saldırı Var')
    w=500
    h=100
    ws=root.winfo_screenwidth()
    hs=root.winfo_screenheight()
    x=(ws/2)-(500/2)
    y=(hs/2)-(100/2)
    root.geometry('%dx%d+%d+%d' % (w,h,x,y))
    Message(root,text="Gatewat degisti.", background='red', width=300,
            fg='ivory', relief=(GROOVE).pack(padx=100,pady=10)
    root.mainloop()

gateway=(os.popen("route -n| grep 'UG[\t]' | awk '{print $2}'").read()
while 1:

    gateway=(os.popen("route -n| grep 'UG[\t]' | awk '{print $2}'").read()
    if gateway !=gateway2:

        Alert()
        break
```

Bu script ile ağ üzerinde default gateway değiştiği anda bir uyarı oluşturarak ARP Poisoning saldırısının tespit edilmesine olanak sağlar.



KAYNAKÇA

1. https://owasp.org/www-community/attacks/Man-in-the-middle_attack
2. <https://www.siberguvenlik.web.tr/index.php/2020/02/06/ikinci-katman-layer2-ataklari-ve-onlenmesi/>
3. <https://fatihurgutegitim.medium.com/layer2-sald%C4%B1r%C4%B1-t%C3%BCrleri-69748387ab53>
4. <https://app.creately.com/diagram/1L6BdS4LfFu/edit>
5. <https://www.pythondersleri.com/2014/06/python-ile-arp-zehirlemesi-tespiti.html>
6. <https://www.mshowto.org/arp-zehirlemesi-ve-alinabilecek-onlemler.html#close>
7. <http://blog.btrisk.com/2016/01/arp-poisoning-nedir-nasil-yapilir.html>
8. <https://www.irongeek.com/i.php?page=security/arpspoof>
9. <https://www.ettercap-project.org/>
10. <https://www.wireshark.org/>
11. <https://www.bilgiguvenligi.gov.tr/aktif-cihaz-guvenligi/ikinci-katman-saldirilari-1-3.html>
12. <http://www.belgeci.com/arp-spoofing.html>