

# Envenenamiento ARP



## Resumen

### ❖ **Protocolo ARP ( Address Resolution Protocol) .**

(El protocolo de resolución de direcciones es responsable de convertir las dirección de protocolo de alto nivel(direcciones IP) a direcciones de red físicas. Primero, consideremos algunas cuestiones generales acerca de Ethernet.

#### **ARP Spoofing:**

Un ataque “ARP Spoofing” es una técnica donde se aprovechan debilidades del protocolo ARP (Address Resolution Protocol) mediante envío de mensajes “Spoofed” o falsos en una red LAN. La intención es asociar la dirección MAC del atacante con la dirección IP de otro host (como el gateway o pasarela por defecto), causando que cualquier tráfico destinado para esta dirección IP sea en su lugar enviada hacia el atacante. Este ataque es utilizado como un comienzo para un ataque MITM (man in the middle) o de Hombre en el Medio.

## Material y recursos

- ❖ Virtualbox.
- ❖ Router wifi ( se sugiere realizar el ejercicio en el entorno controlado de su casa).
- ❖ Máquina atacante con Kali Linux.
- ❖ Máquina víctima ( puede emplearse el equipo anfitrión).
- ❖ Ettercap.
- ❖ Wireshark.

### Objetivo:

Interiorizar las vulnerabilidades que pueden potencializar un ataque valiéndose de protocolos como ARP mediante una de las técnicas actualmente más explotadas como lo son los ataques de “hombre en el medio”.

Tiempo asignado:

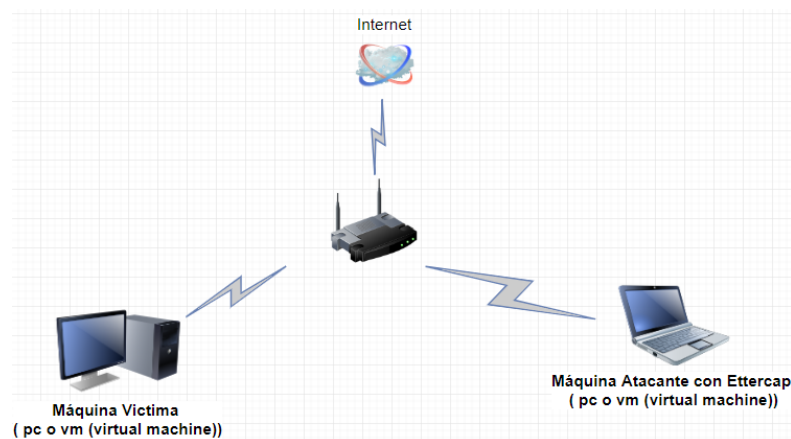
45 minutos práctica. 60 minutos informe escrito.

## Puesta en práctica

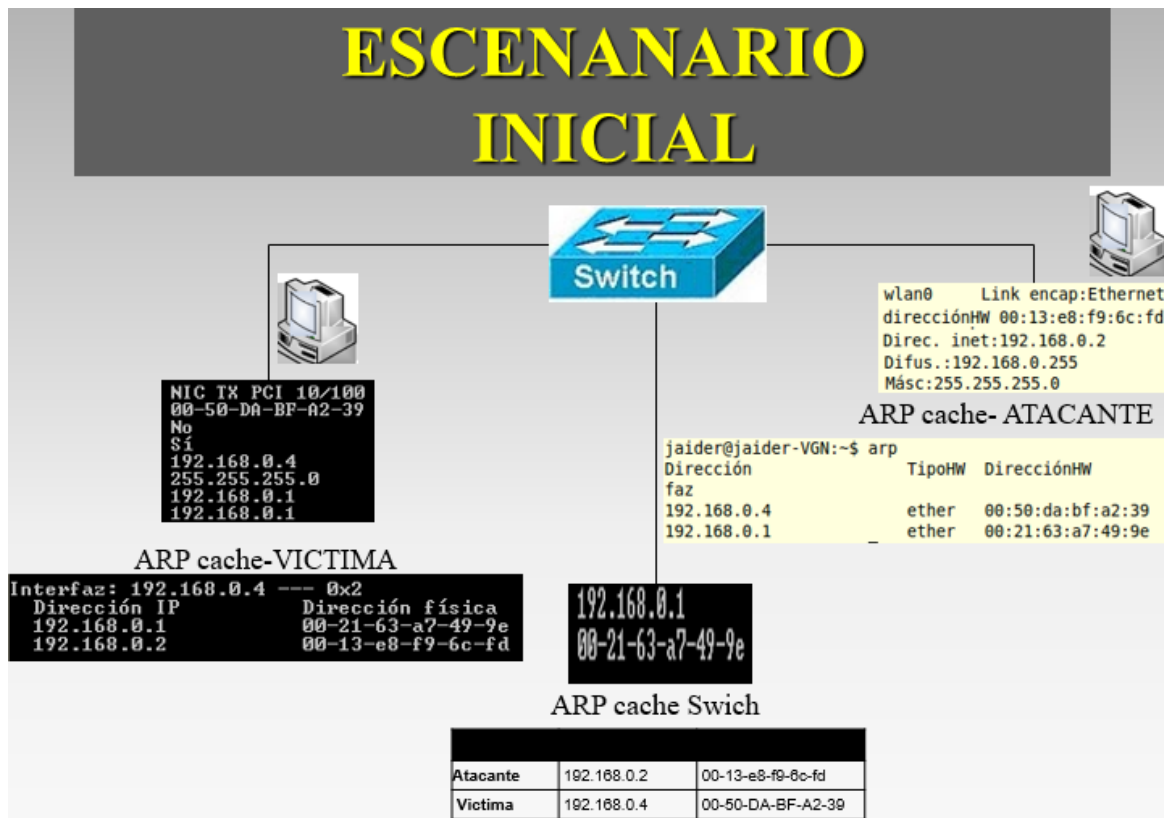
### Procedimiento

#### a. Preparación

Implemente la siguiente arquitectura, las máquinas pueden ser host físicos o virtuales siempre y cuando hagan parte de la misma red ( modo bridge).



- ❑ Valide sus caché arp antes de iniciar el ataque mediante el comando arp -a desde consola, como se observa en la siguiente imagen

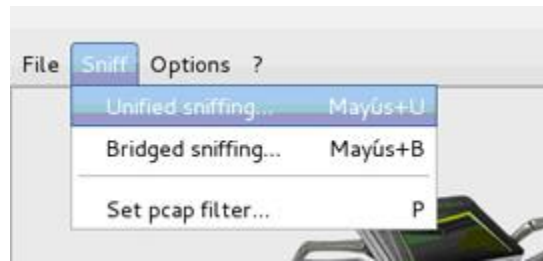


- ❑ En la máquina atacante ( Kali LINUX) inicie ettercap, bien sea mediante aplicaciones o en una terminal de línea de comandos tipeando:

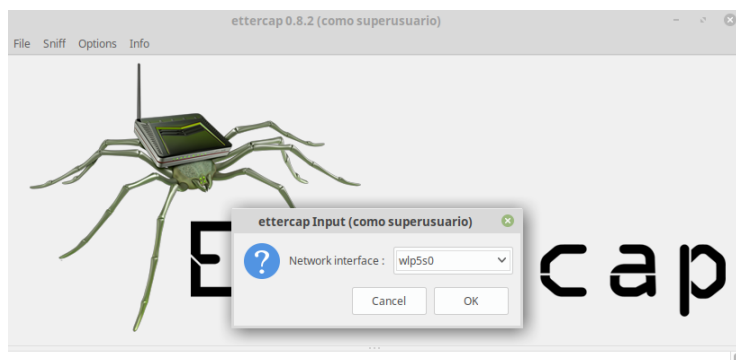
**# ettercap -G**



- ❑ De clic en la opción “Sniff -> Unified Sniffing” ubicado en el menú superior de ettercap.



- ❑ Seleccionar la Interfaz, según sea su caso. Para el caso de la presente práctica corresponde a “wpl5so”.



- ❑ Añadir a la lista de hosts, los objetivos contra los cuales se realizará el “ARP Spoofing”. Para ello se procede a hacer clic en la opción “Hosts -> Scan for Host”



- ❑ Seleccionar la opción “Host -> Host List”. Ante lo cual se presentará una nueva pestaña con el listado de los Hosts.

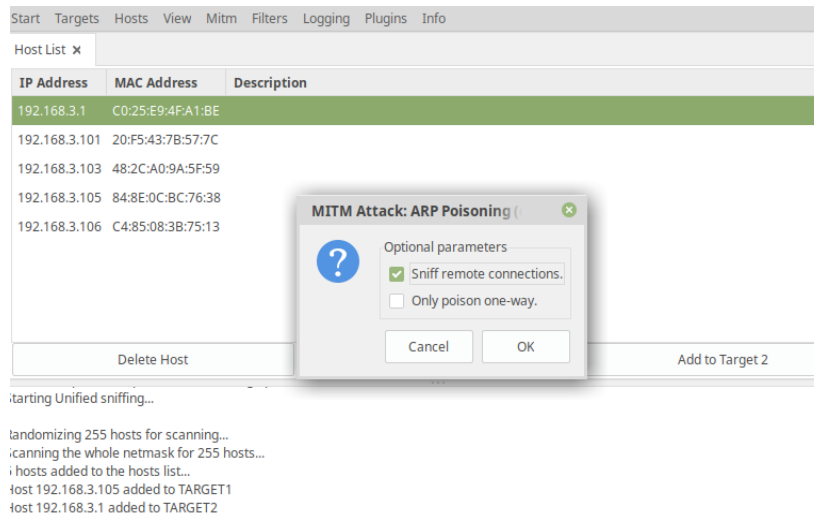
**ettercap 0.8.2 (como superusuario)**

Start Targets Hosts View Mitm Filters Logging Plugins Info		
Host List ✕		
IP Address	MAC Address	Description
192.168.3.1	C0:25:E9:4F:A1:BE	
192.168.3.101	20:F5:43:7B:57:7C	
192.168.3.103	48:2C:A0:9A:5F:59	
192.168.3.106	C4:85:08:3B:75:13	

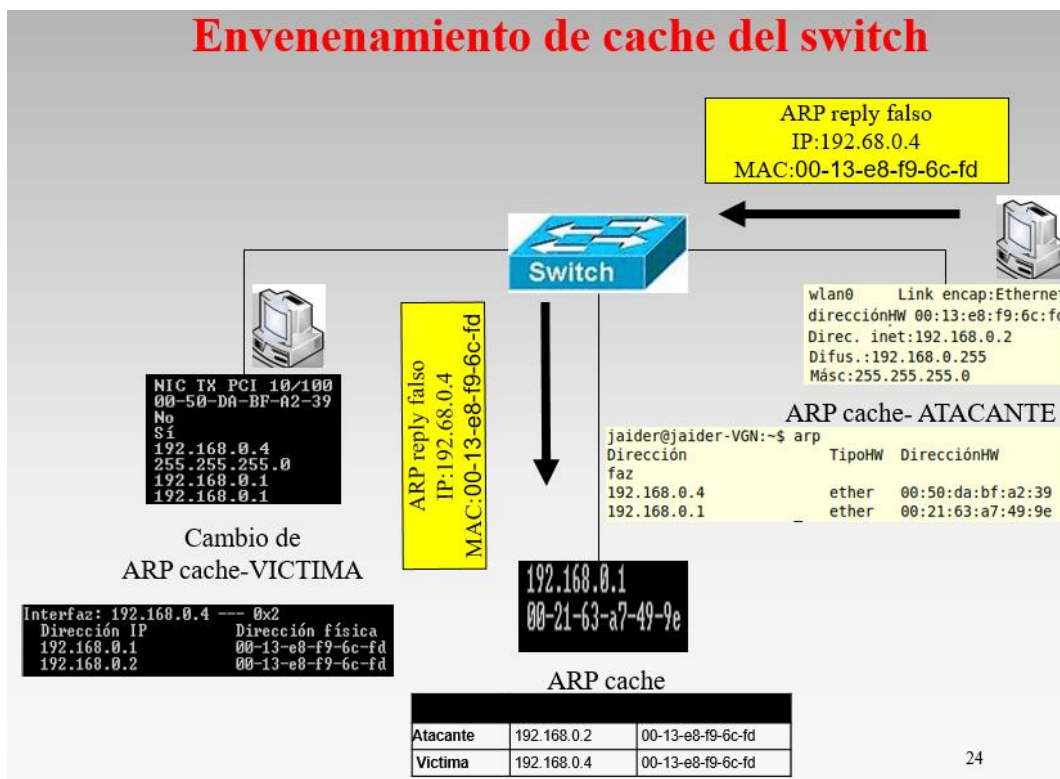
- ❑ Ahora se debe elegir los targets de nuestro ataque, para el caso de estudio el host 192.168.3.106 es nuestro pc víctima y se adiciona como target 1 mientras que la IP 192.168.3.1 que corresponde al router sería el target 2; ubicándonos en el medio de estos dos equipos para cristalizar el ataque MITM.

Start Targets Hosts View Mitm Filters Logging Plugins Info		
Host List ✕		
IP Address	MAC Address	Description
192.168.3.1	C0:25:E9:4F:A1:BE	
192.168.3.101	20:F5:43:7B:57:7C	
192.168.3.103	48:2C:A0:9A:5F:59	
192.168.3.106	C4:85:08:3B:75:13	
fe80::82d3:6000:1e08:71c1	40:B0:76:90:A6:4C	
192.168.3.118	40:B0:76:90:A6:4C	
<div> Delete Host Add to Target 1 Add to Target 2 </div>		
Starting Unified sniffing... Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 4 hosts added to the hosts list... Host 192.168.3.106 added to TARGET1 Host 192.168.3.1 added to TARGET2		

- ❑ Acto seguido queda seleccionar el tipo de ataque para lo cual desde donde se debe seleccionar “Mitm -> Arp poisoning...” y la opción “Sniff remote connections.” o husmear conexiones remotas.



Para validar el ataque consulte las tablas ARP validando el envenenamiento en ejecución.



- ❑ Diríjase al navegador de la víctima y realice una búsqueda de sitios vulnerables ingresando in inurl /login.php

Para el ejercicio se ingresó a <http://testphp.vulnweb.com/login.php> y desde ettercap se puede observa la captura en texto plano del login efectuado!!!.

Host List ✕		
IP Address	MAC Address	Description
192.168.3.1	C0:25:E9:4F:A1:BE	
192.168.3.102	E4:CE:8F:29:3F:7A	
192.168.3.103	48:2C:A0:9A:5F:59	
192.168.3.106	C4:85:08:3B:75:13	
192.168.3.118	40:B0:76:90:A6:4C	
<div> Delete Host Add to Target 1 Add to Target 2 </div>		

Unified sniffing already started...

HTTP : 176.28.50.165:80 -> USER: jaider PASS: navas10014 INFO: http://testphp.vulnweb.com/login.php  
CONTENT: uname=jaider&pass=navas10014

HTTP : 204.15.135.77:80 -> USER: jaider PASS: test INFO: http://www.fomendoza.com.ar/sistema/login.php  
CONTENT: login=jaider&password=test&Button\_DoLogin=Login

Finalmente, para detener el ataque se debe hacer click en el menú "mitm", y luego stop "mitm", y observar que el tráfico deja de pasar a través del Kali.

Ettercap ofrece una serie de plugins para diferentes tipos de ataque que pueden ser ubicados en el menú "Plugin".

**ettercap 0.8.2 (como superusuario)**

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List x Plugins x

	Name	Version	Info
	pptp_pap	1.0	PPTP: Forces PAP authentication
	pptp_reneg	1.0	PPTP: Forces tunnel re-negotiation
	rand_flood	1.0	Flood the LAN with random MAC addresses
*	remote_browser	1.2	Sends visited URLs to the browser
	reply_arp	1.0	Simple arp responder
	repoison_arp	1.0	Repoison after broadcast ARP
	scan_poisoner	1.0	Actively search other poisoners
	search_promisc	1.2	Search promisc NICs in the LAN
	smb_clear	1.0	Tries to force SMB cleartext auth
	smb_down	1.0	Tries to force SMB to not use NTLM2 key auth

GROUP 1 : 192.168.3.106 C4:85:08:3B:75:13

GROUP 2 : 192.168.3.1 C0:25:E9:4F:A1:BE

Unified sniffing already started...

Activating remote\_browser plugin...

REMOTE COMMAND: xdg-open <http://www.aulasuniminuto.edu.co/inicio/>

REMOTE COMMAND: xdg-open <http://201910.aulasuniminuto.edu.co/>

## Evaluación

Esta actividad se puede realizar en grupos de dos personas y se socializará en clase para su calificación.

■ ■ ■

Realice una investigación sobre cómo protegerse de ataques derivados de las debilidades del protocolo ARP. Entre otras relacione escenarios, pros y contras de medidas como IPSEC, port security , plugins de navegador (HTTPS Everywhere , ForceTLS, SSLSniff ) en una tabla comparativa ( hoja de cálculo).



Identifique la captura de los paquetes ARP generados (reply, request, gratuitos) desde wireshak; tal y com, se presenta en los slides de clase; validando además la advertencia dada por este sobre la duplicación de IP.

2727	1545.946128	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2728	1545.946230	IntelCor_f9:6c:fd	3com bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2729	1555.956658	IntelCor_f9:6c:fd	3com bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2730	1555.956749	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2731	1555.966930	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2732	1555.967000	IntelCor_f9:6c:fd	3com bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2766	1565.977444	IntelCor_f9:6c:fd	3com bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd
2767	1565.977500	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2768	1565.987660	IntelCor_f9:6c:fd	AskeyCom_a7:49:9e	ARP	192.168.0.4 is at 00:13:e8:f9:6c:fd
2769	1565.987690	IntelCor_f9:6c:fd	3com bf:a2:39	ARP	192.168.0.1 is at 00:13:e8:f9:6c:fd

▶ Frame 2728 (42 bytes on wire, 42 bytes captured)  
 ▶ Ethernet II, Src: IntelCor f9:6c:fd (00:13:e8:f9:6c:fd), Dst: 3com bf:a2:39 (00:50:da:bf:a2:39)  
 ▶ [Duplicate IP address detected for 192.168.0.1 (00:13:e8:f9:6c:fd) - also in use by 00:21:63:a7:49:9e (frame 2727)]  
 ▶ Address Resolution Protocol (reply)

## Referencias:

- Presentación (slides) realizada en clase.
- <https://geekytheory.com/redes-el-protocolo-arp/>
- [http://profesores.elo.utfsm.cl/~agv/elo323/2s14/projects/reports/MoraMorales/mitm\\_kali.html](http://profesores.elo.utfsm.cl/~agv/elo323/2s14/projects/reports/MoraMorales/mitm_kali.html)
- <https://www.youtube.com/watch?v=Mac5PO21I7I>
- <https://www.youtube.com/watch?v=C2CWZ7tCM5I>