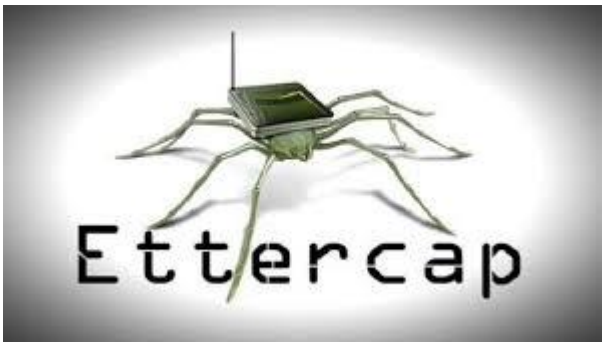
Envenenamiento ARP



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:

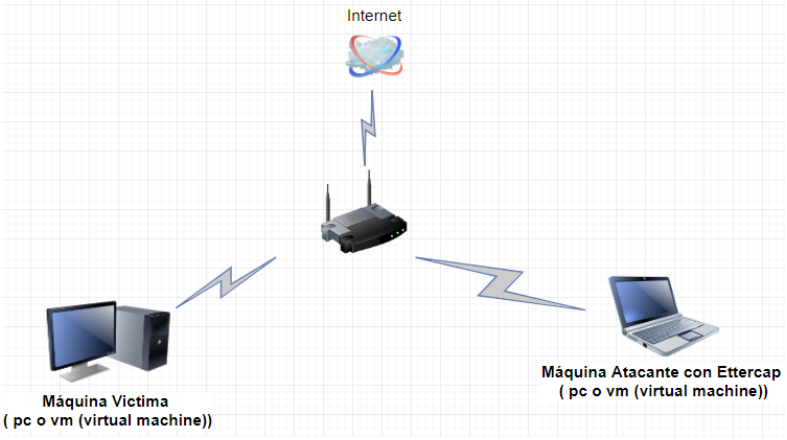
45 minutos práctica. 60 minutos informe escrito.

Puesta en práctica

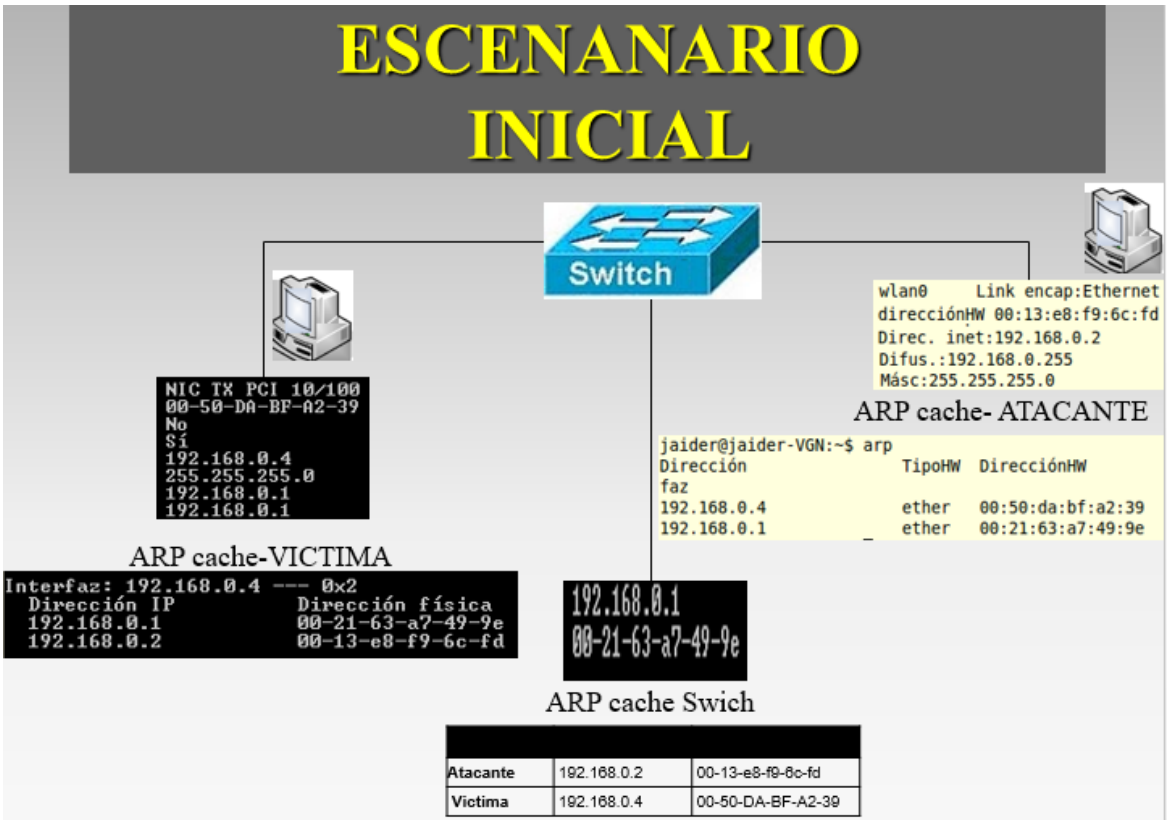
Procedimiento

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).



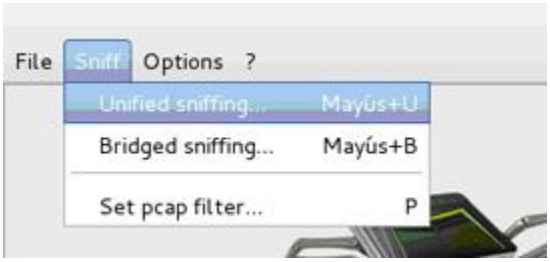
❑ Valide sus caché arp antes de iniciar el ataque mediante el comando arp -a desde consola, como se observa en la siguiente imagen



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

 # ettercap -G

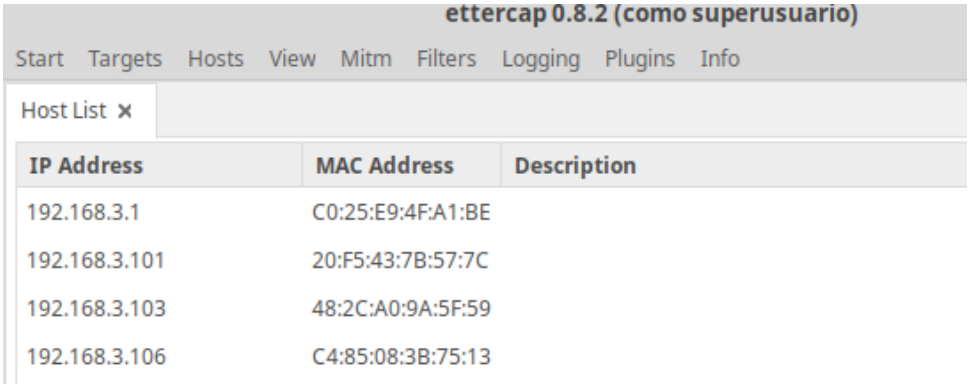
❑ De clic en la opción “Sniff -> Unified Sniffing” ubicado en el menú superior de ettercap.



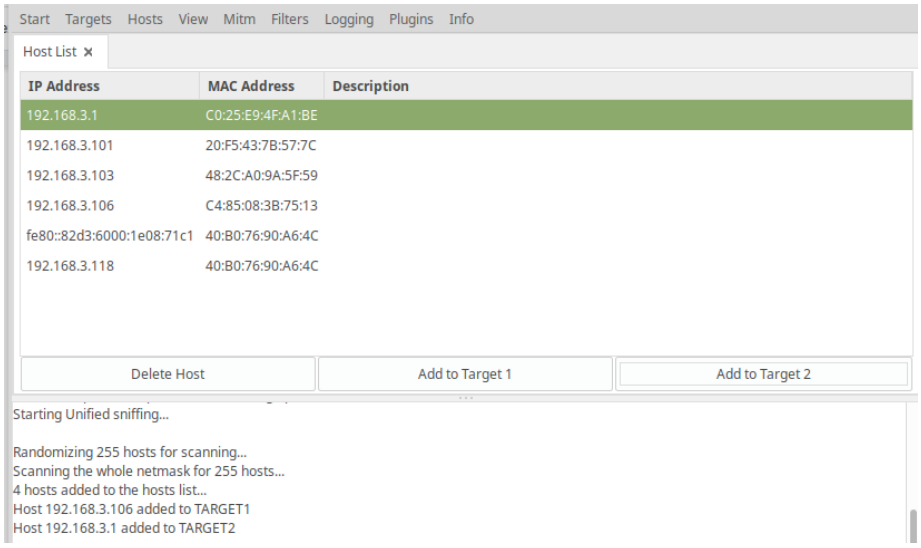
❑ Seleccionar la Interfaz, según sea su caso. Para el caso de la presente práctica corresponde a “wpl5so”.

❑ 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”

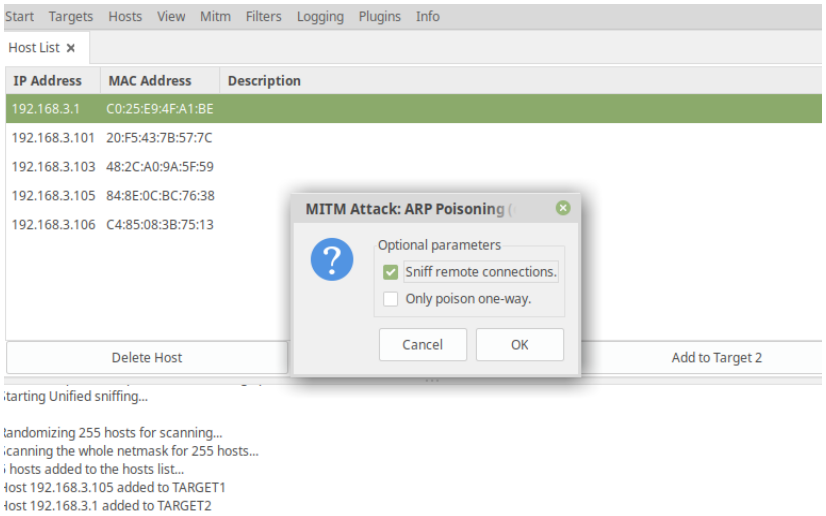
❑ Seleccionar la opción “Host -> Host List”. Ante lo cual se presentará una nueva pestaña con el listado de los Hosts.



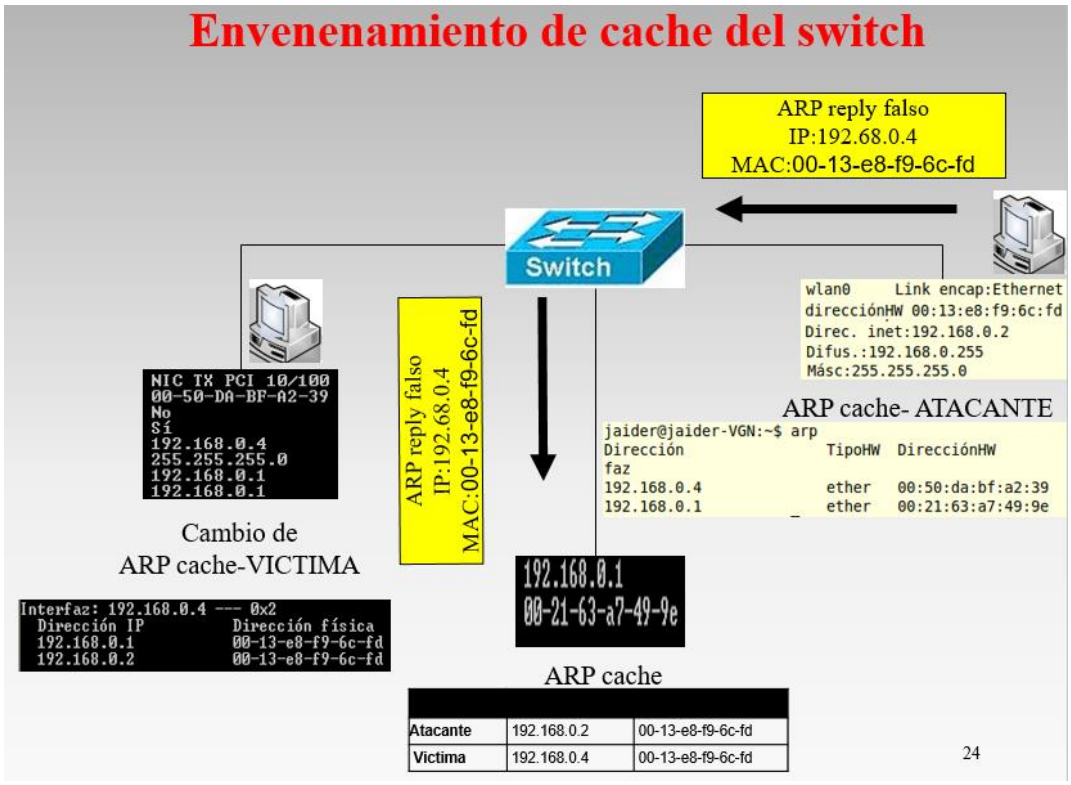
- Ahora se debe elegir los targets de nuestro ataque, para el caso de estudio el host 192.168.3.106 es nuestro pc víctima y se adiciona como target 1 mientras que la IP 192.168.3.1 que corresponde al router seríia el target 2; ubicándonos en el medio de estos dos equipos para cristalizar el ataque MITM.



- 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.

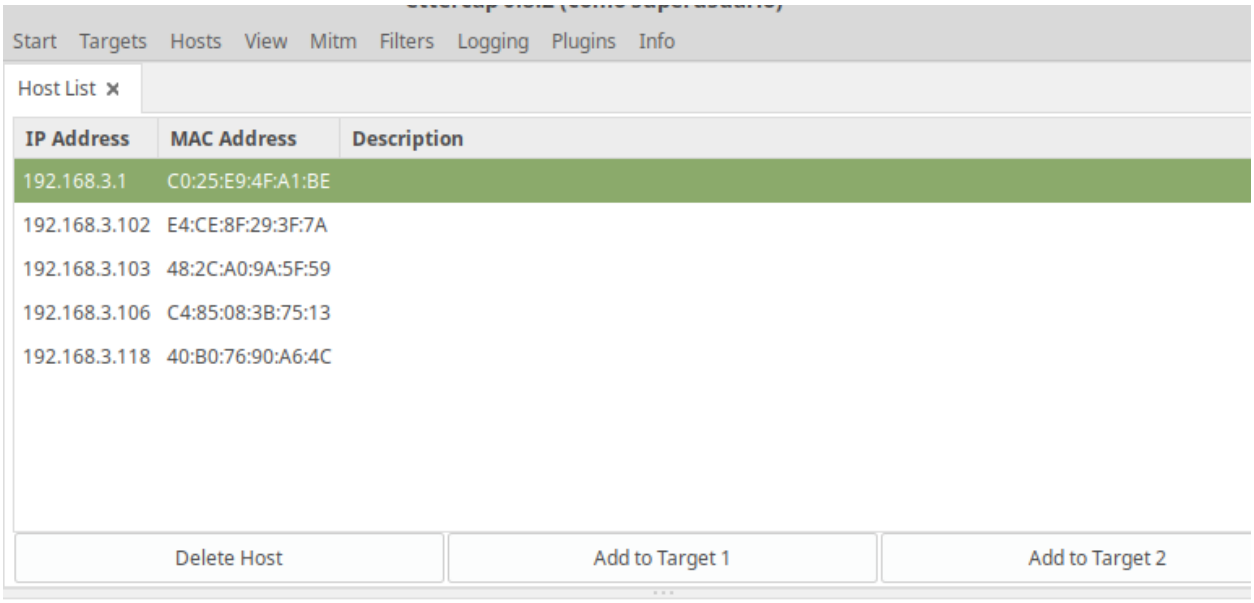


Para validar el ataque consulte las tablas ARP validando el envenenamiento en ejecución.



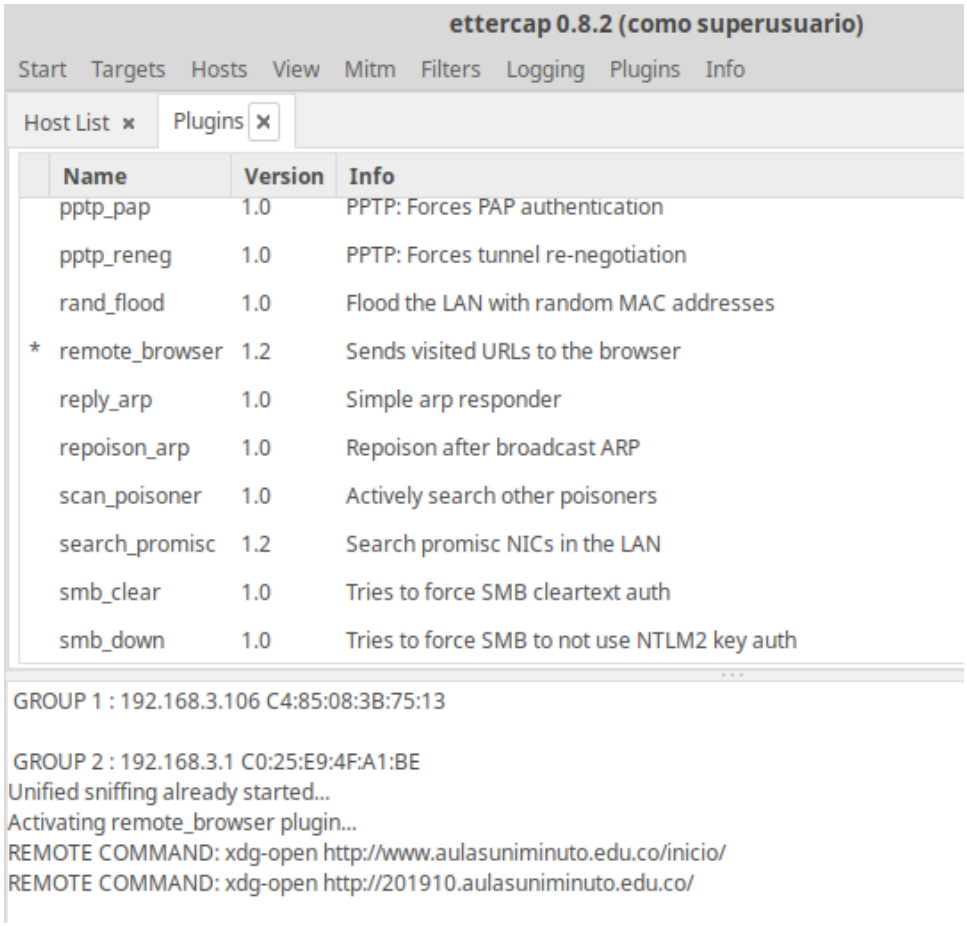
- ❏ Diríjase al navegador de la víctima y realice una búsqueda de sitios vulnerables ingresando in inurl /login.php

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!!!.



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 unas serie de plugins para diferentes tipos de ataque que pueden ser ubicados en el menú “Pluggin”.

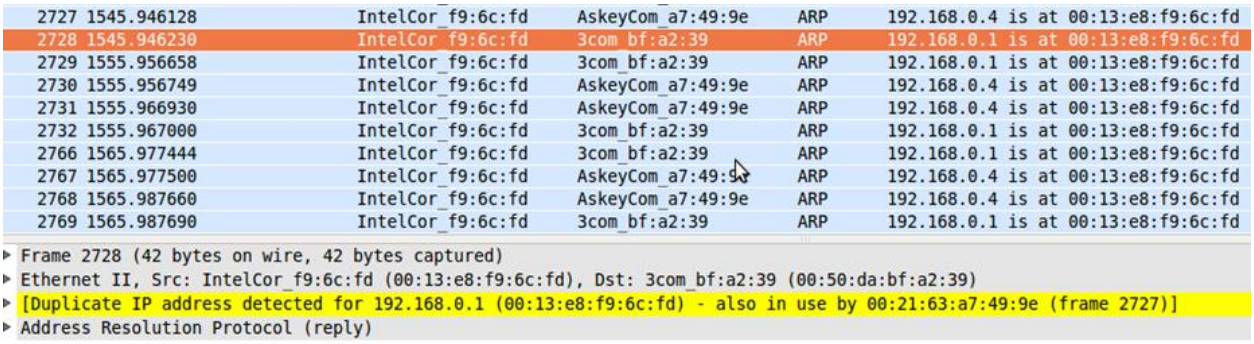


Evaluación

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, gratuituos) desde wireshak; tal y com, se presenta en los slides de clase; validando además la advertencia dada por este sobre la duplicación de IP.



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
- https://www.youtube.com/watch?v=Mac5PO21l7I
- https://www.youtube.com/watch?v=C2CWZ7tCM5I