**UF5: ARP SPOOFING, MAN IN THE MIDDLE, BURP, SSL SCRIPT**

A lo largo de la UF4 hemos aprendido a forjar paquetería con SCAPY, esta herramienta soporta decenas de protocolos estándares de la red uno de ellos es el protocolo ARP.

ARP nos permite resolver direcciones MAC a partir de direcciones IP, este protocolo es imprescindible para las comunicaciones en una red lan. Su estructura de funcionamiento es muy sencillo ya que solo existen 2 tipos de paquetería el ARP REQUEST y el ARP REPLAY, cada uno de estos paquetes no tiene asociación ni identificador de pregunta respuesta por lo tanto se pueden generar muchas preguntas sin respuestas y muchas respuestas sin preguntas.

Debido a la estructura de este protocolo los hackers han aprovechado durante muchos años para realizar envenenamientos de la red. A lo largo de este capítulo nos daremos cuenta que el envenenamiento ARP o bien ARP POISONING es un ataque imprescindible para redes LAN y captura de datos.

**Envenenamiento ARP**

Como hemos visto el protocolo ARP tiene ciertas vulnerabilidades propias de su diseño y la que es fundamental es que no hay una relación entre pregunta y respuesta por lo tanto se pueden forjar muchas respuestas de tipo “replay”.

Pasos para el ataque de envenenamiento ARP:

1. El hacker utiliza una aplicación o SCAPY para forjar un paquete de tipo ARP Replay.
2. Para realizar el envenenamiento el hacker indicará que la IP de la puerta de enlace corresponde a la MAC del ordenador del hacker.
3. El mensaje encapsulado se enviará repetidamente durante todo el ataque.
4. La víctima o bien todo el Broadcast reciben el mensaje y actualiza su tabla ARP es en ese momento cuando el envenenamiento ya a tenido efecto.
5. Si la víctima consulta su tabla ARP vemos que la MAC propuesta ya no es la MAC original si no la del hacker.

Una vez realizado el ataque vamos a entender que pasa con los paquetes que salen hacia internet. Debido a que la tabla ARP del cliente contiene la MAC del hacker como puerta de enlace y la red está basada en Switch el Switch reenviara toda la paquetería al hacker, este tendrá activado un Proxy o bien una Pasarela y ese tráfico capturado será reenviado a internet de forma totalmente transparente sin que la víctima se de cuenta.

Si se quiere revertir el ataque es tan sencillo como que el hacker encapsule otra trama de tipo ARP Reply con la MAC original de la puerta de enlace, de esta forma el ataque se puede habilitar y deshabilitar tantas veces como se desee.

**Herramientas que se pueden utilizar:**

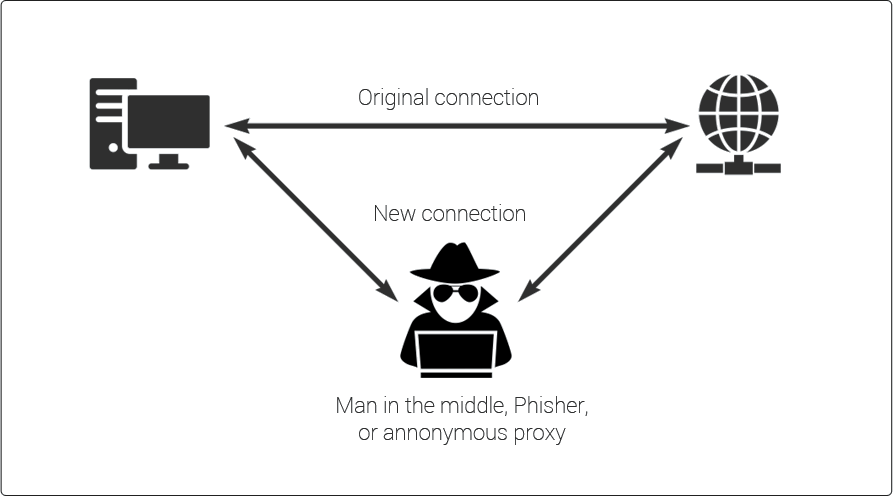
1. SCAPY
2. ARP Spoof
3. ettercap

**MAN IN THE MIDDLE (NITN)**

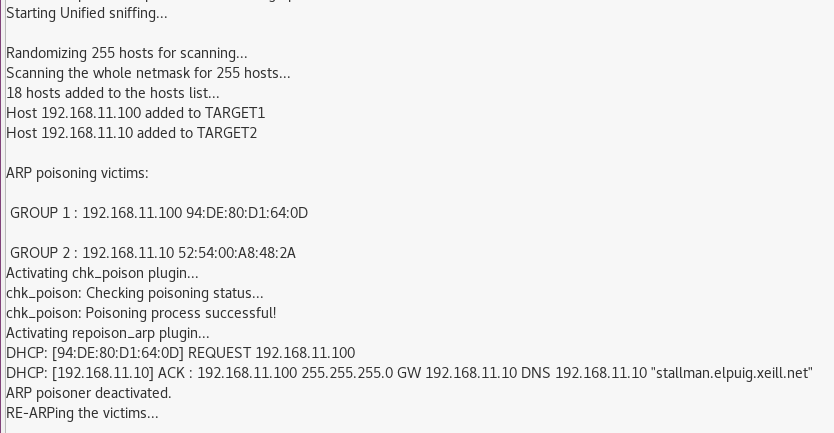
El Man in the middle es una técnica que básicamente consiste en un ARP Poison pero en las 2 direcciones, es decir el hacker envenena la tabla ARP de las víctimas pero también envenena la tabla ARP del otro por lo tanto la de la puerta de enlace, causando un efecto extremadamente peligroso para los usuarios ya que todo el tráfico tanto de ida como de vuelta puede ser capturado, manipulado y analizado. Al igual que ARP poison el Man in the middle se puede revertir fácilmente y es transparente para los usuarios.

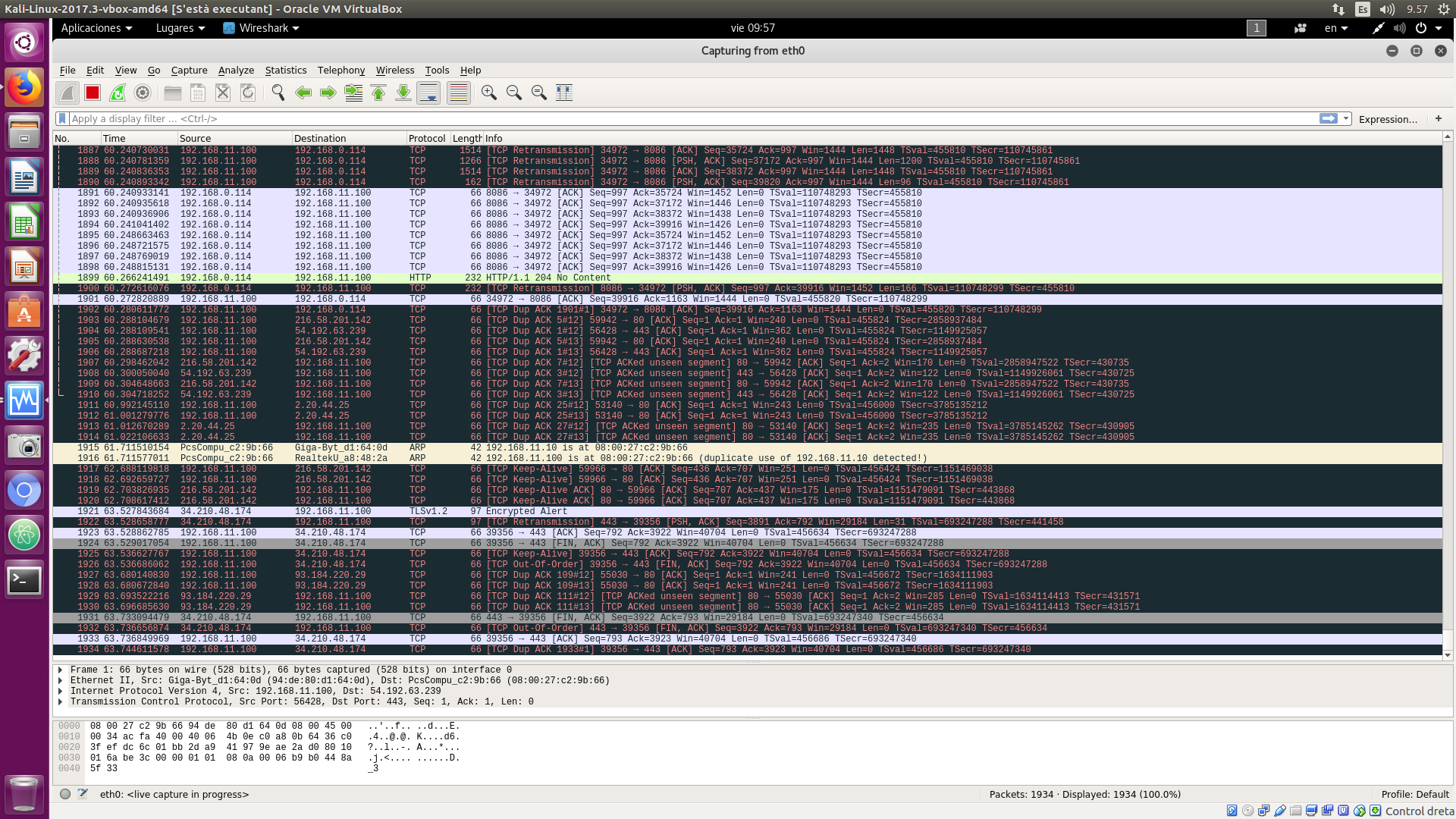
El Man in the middle es el ataque más importante en redes LAN ya que es la base para realizar otro tipo de ataques de suplantación de identidad, Paijacking, etc. Los programas que se utilizan para el Man in the middle son:

1. ARPSpoof con 2 terminales uno de ida y otro de vuelta (Uno envenena la víctima y otro el proxy)
2. Ettercap



Como hemos comprobado en clase en la siguiente imagen muestra como el programa Ettercap habilita el Man in the middle de forma muy sencilla envenenando una víctima y reenviando la paqueteria en las 2 direcciones de forma automática la captura de la pantalla no es nada más que el Wireshark capturando estos paquetes de ida y de vuelta. Esta captura podría manipulada, analizada, etc.





Como hemos observado en la práctica de Ettercap, activar y habilitar el Man in the Middle es una tarea muy fácil a partir de aquí se podrán combinar otros ataques como por ejemplo: la manipulación de protocolos de niveles superiores (HTTP), a continuación vamos a utilizar otra herramienta que aporta Ettercap, llamada Etterfilter.

**Etterfilter**

Ettercap es la herramienta que permite habilitar de forma fácil algunos ataques de base entre ellos el MINT pero también existe una aplicación del mismo paquete denominada Etterfilter, con esta herramienta se pueden crear scripts que indican las reglas de manipulación de la paqueteria que redirecciona el hacker, vamos a poner algunos ejemplos:

1. Dropea todos los paquetes de un host y de tipo UDP.
2. Desencapsula todos los paquetes de cuerpo 80 de la víctima y manipula el código HTTP existente.
3. etc.

**Manipulación HTTP en tiempo real con Etterfilter**

<http://highsec.es/2014/09/jugando-con-etterfilter/> (entra examen)

**Entra Examen:**

* **ARP**
* **Envenenamiento ARP**
* **Man in the Middle**
* **Ettercap**
* **Etterfilter**