UNIVERSIDAD
DE GRANADA

SERVIDORES WEB DE ALTAS PRESTACIONES

GRADO EN INGENIERÍA INFORMÁTICA

Ataques Man-In-The-Middle

Autores
Elena María Gómez Ríos
Nazaret Román Guerrero
Guillermo Sandoval Schmidt

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

CURSO 2018-2019

Índice

1. ¿Qué es?

Un ataque ***Man-In-The-Middle*** es un ataque en el que se consigue la capacidad de leer, modificar y reenviar datos a voluntad. De esta forma se puede acceder al contenido privado como, por ejemplo, datos confidenciales y contraseñas.

La sutileza del ataque se basa en que todo tiene que suceder sin que el cliente y el servidor o el cliente y el cliente entre los que se realiza la conexión se den cuenta de que hay un infiltrado entre ellos. Este tipo de ataques criptográficos tienen especial interés cuando se lleva a cabo el intercambio de *Diffie-Hellman* sin autenticación.

2. Software para realizar un ataque MITM

Hemos utilizado una máquina virtual con Kali Linux para realizar el ataque ya que tiene instaladas las aplicaciones necesarias para este tipo de ataques, como por ejemplo Ettercap, que es la aplicación que nosotros hemos utilizado.

Actualmente existen una gran cantidad de programas para realizar ataques *Man-In-The-Middle*. Por ejemplo, se podría utilizar WireShark que es un potente sniffer de red con el que se pueden ver posibles ataques. Otro programa es mitmAP que está escrito en python e incorpora otras herramientas para realizar este tipo de ataque. Otros ejemplos son: Bettercap, MITMProxy, Evilgrade, Hamster o Ferret.

3. ¿Cómo defenderse ante un ataque MITM?

A pesar de ser un ataque básico y ser conocido por todos en el ámbito, sigue siendo uno de los principales ataques de seguridad que se pueden llevar a cabo. Para poder defenderse de este, se pueden utilizar mecanismos como los siguientes:

- **Claves públicas.** En este caso, se cifran los mensajes con la clave privada del primer sujeto y el sujeto B lo descifra con la clave pública. De esta forma, el sujeto intermedio no conoce la clave pública que comparten ni tampoco tiene una clave privada que descifre el mensaje, de forma que la conexión es asimétrica y segura.
- **Claves secretas (con alta entropía).** Similar al caso anterior pero teniendo en cuenta la entropía de las claves, es decir, la información que muestran los símbolos que forman la llave. En el caso de, por ejemplo, una clave de texto, las palabras más “raras” son las que tienen mayor entropía y las que ofrecen mayor información.
- **Técnicas biométricas.** Difíciles de suplantar para poder actuar como un intermediario de las conexiones, como por ejemplo reconocimiento de voz, escáner de huellas dactilares o de retina...

- **HTTPS.** Asegurarse de que la conexión se realiza a través de un canal seguro para evitar accesos indeseados a los datos.
- **Conexiones VPN.** Conectarse a una red WIFI pública conlleva peligros como una exposición directa a ataques de este tipo. Utilizar una conexión privada es mucho más segura que utilizar una conexión pública asegurada con métodos anteriores.
- **Malware.** A la hora de descargar software, hay que hacerlo de sitios seguros y de confianza, para evitar que el software descargado contenga malware que pueda afectar a nuestras conexiones.
- **Actualizaciones.** Mantener el software utilizado actualizado, ya que, cuanto más antiguo es el software, más fácil es que se hayan encontrado debilidades expongan la seguridad.

4. Ataques famosos

- En 2015, 49 personas fueron detenidas en Europa tras una operación organizada por la Europol. Los hackers, mediante una técnica de "phising" se quedaban con datos de los clientes de varios bancos, engañandolos utilizando un página prácticamente idéntica a la original de dichos bancos. De este modo, las transferencias en lugar de llegar al destino intencionado, llegaban a los estafadores, llegando a conseguir de manera fraudulenta cerca de 6.000.000€.
- Sin irnos más lejos, en 2016, en España, una joven de 19 años fue detenida tras realizar un ataque MITM a una empresa, suplantando la identidad de esta y estafando 6.500€ de la misma, ya que modificó el número de cuenta original al que iba dirigida la transferencia.
- Quizás uno de los casos más conocidos de ataque MITM y que fue destapado por Edward Snowden, fue el perpetrado por la Agencia Nacional de Seguridad Estadounidense, que simulaba los servicios de búsqueda de Google para recolectar datos de los usuarios.

5. Actuando como intermediario

Ahora es nuestro turno de llevar a cabo un ataque. Para ello, y utilizando el software descrito anteriormente, descubriremos el usuario y la contraseña de un cliente que se conectará a una página web sin seguridad.

5.1. Configuración del cortafuegos de la máquina atacante

Para configurar el cortafuegos al iniciar la máquina, hemos utilizado un script de bash que ejecute los comandos necesarios para configurar *iptables.* El script es el que sigue:

```
#!/bin/bash
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -i eth1 -p tcp --destination-port 80
         -j REDIRECT --to-port 10000

iptables-save > /etc/iptables.up.rules
```

Listing 1: bash version

Con esto hemos conseguido infiltrarnos en la conexión y enmascarar nuestra presencia, fingiendo que somos el cliente cuando los paquetes provengan del servidor, y el servidor cuando los paquetes provengan del cliente.

5.2. Situándonos entre las víctimas

Para este paso es necesario utilizar el software *Ettercap*.

1. Comenzamos a esnifar la conexión con SNIFF→UNIFIED SNIFFING.
2. Detectamos los hosts que hay en nuestra red y a los que vamos a atacar.

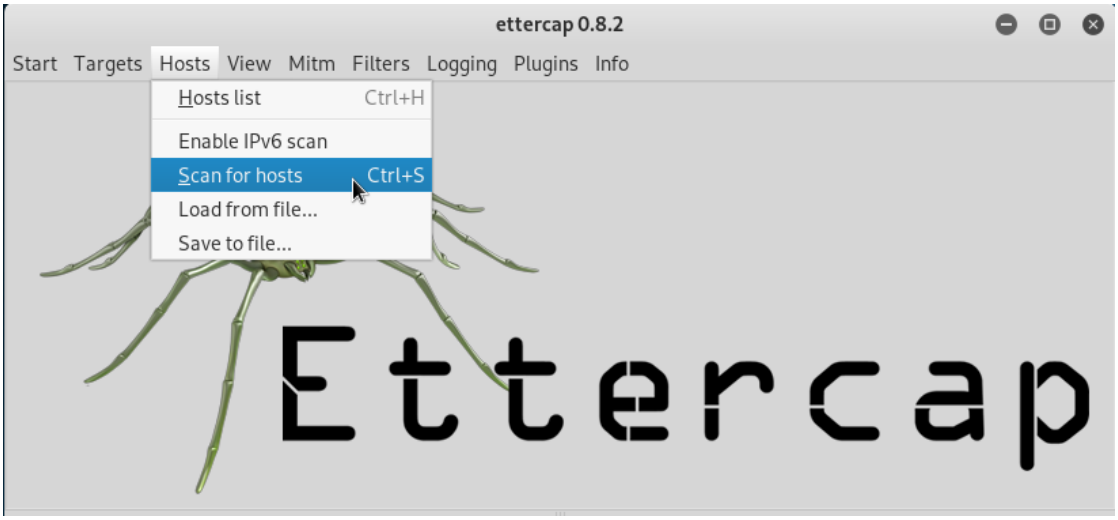

Figura 1: Escaneado de hosts

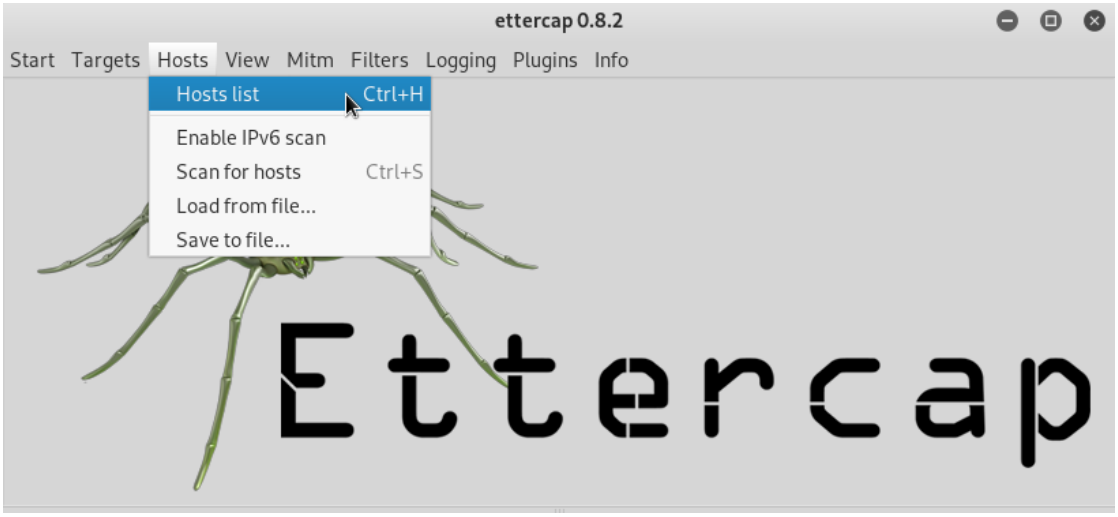

Figura 2: Lista de máquinas

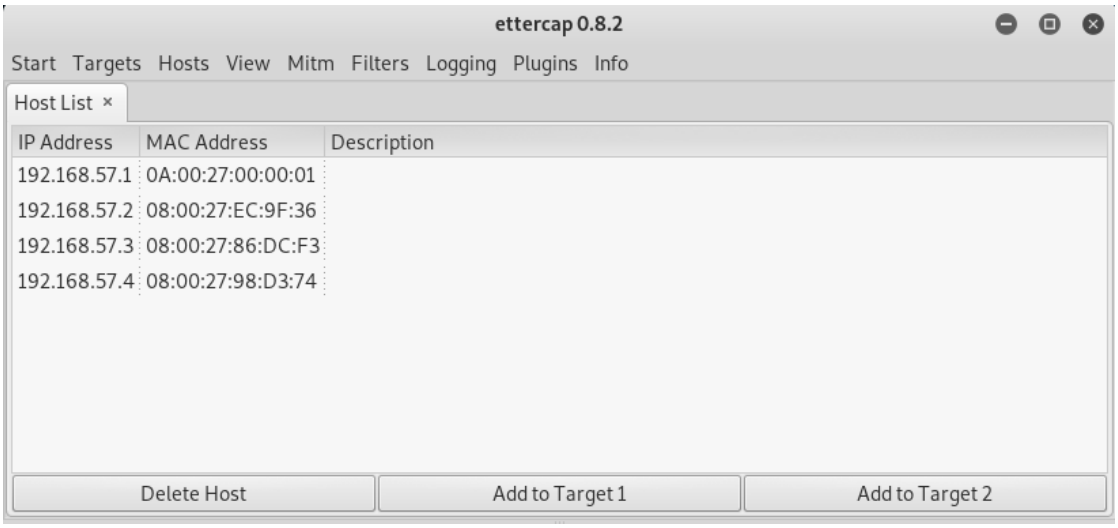

Figura 3: Hosts disponibles

3. Paramos el sniffing con SNIFF→STOP SNIFFING.

4. Añadimos cada host a un TARGET, seleccionando el host y clickando en ADD TO TARGET1. Nuestros host son el 192.168.57.3 (como servidor) y el 192.168.57.4 (como cliente).

5. Ahora hay que hacer un envenenamiento del protocolo ARP para que, en la ruta, entremos nosotros como punto intermedio al que pasarle los datos.

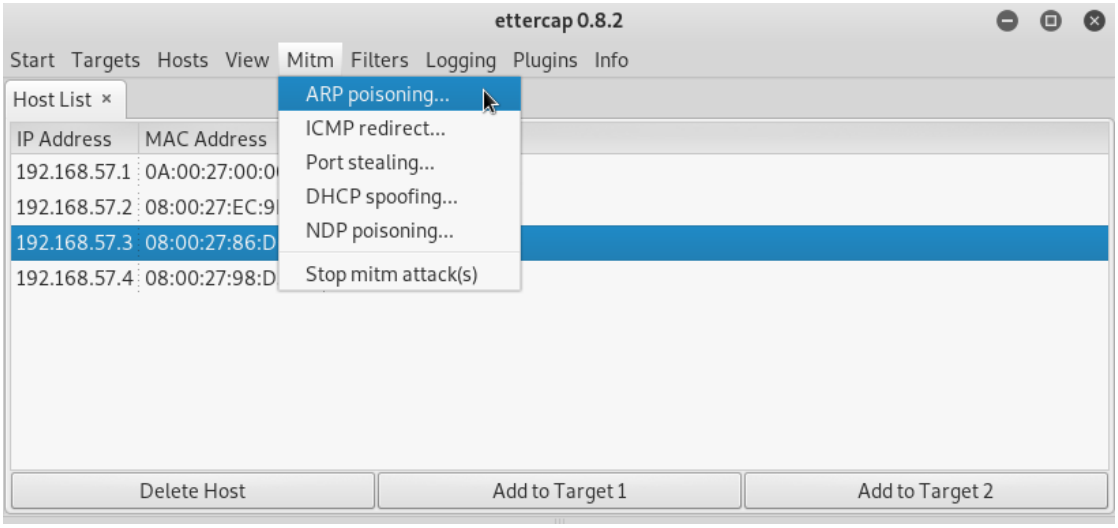

Figura 4: Envenamiento de ARP

6. Comenzamos con el proceso de sniffing de nuevo con la conexión envenenada.
7. Accedemos desde el cliente a la página.

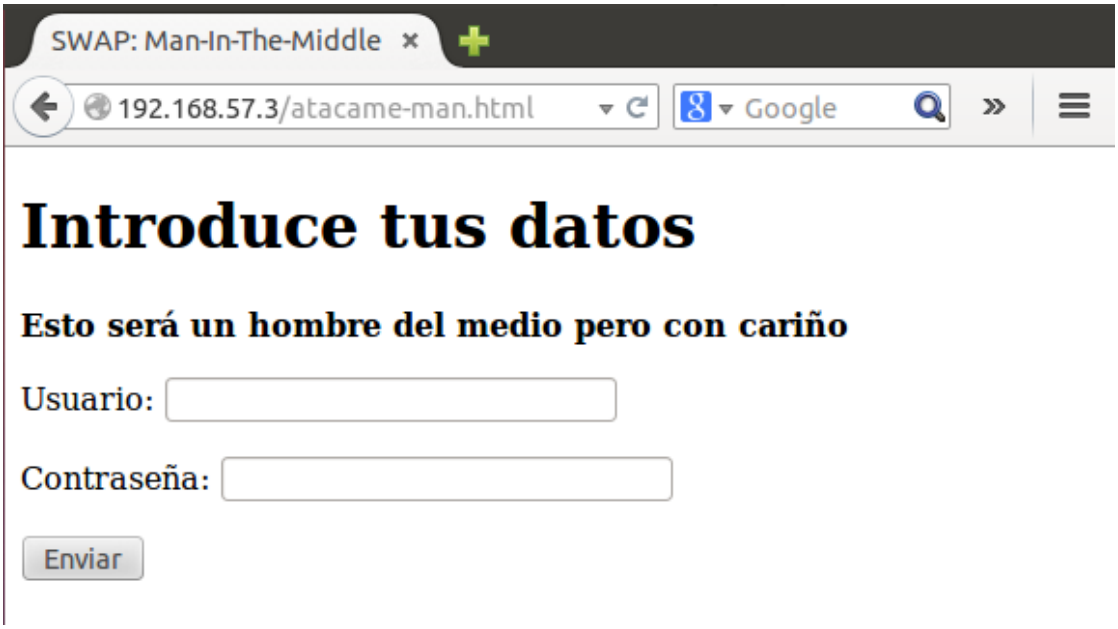

Figura 5: Formulario

8. Eliminamos la desencriptación de las peticiones.

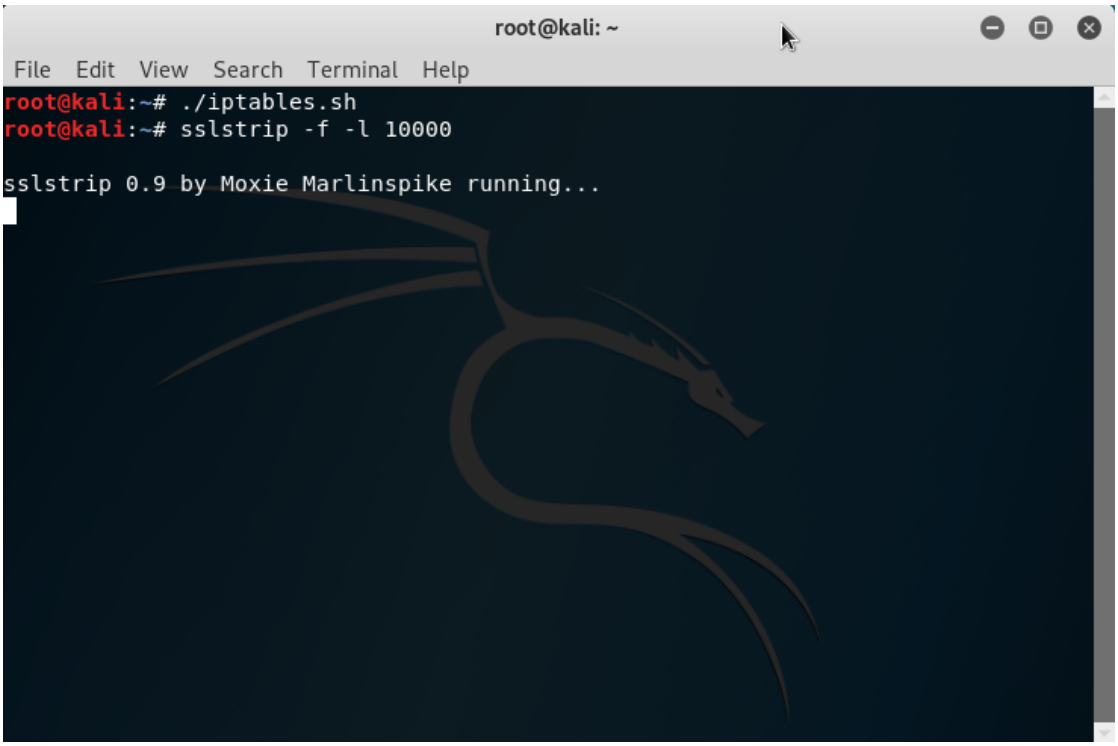

Figura 6: SSLstrip

9. Finalmente, hemos conseguido el usuario y la contraseña.

```
HTTP : 192.168.57.3:80 -> USER: hola  PASS:   INFO: http://192.168.57.3/atacame-man.html
CONTENT: user=hola&pssw=adios
```

Figura 7: MITM

6. Bibliografía

- https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- https://en.wikipedia.org/wiki/Entropy_(information_theory)
- http://www.cursodehackers.com/ManInTheMiddle.html
- https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

- https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/
- https://nakedsecurity.sophos.com/es/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/
- https://navarra.elespanol.com/articulo/sucesos/detenida-pamplona-joven-19-anos-estafar-6-500-euros-empresa/20160513113625041253.html