

Servidores Web de Altas Prestaciones

Tema: Man In The Middle (MITM)

**INTRODUCCIÓN, CONCEPTO, ATAQUES,
DETECCIÓN Y PROTECCIÓN**



ugr

Universidad
de **Granada**

Autor: Jonathan Martín Valera

TABLA DE CONTENIDOS

1. INTRODUCCIÓN	3
2. ¿QUÉ ES UN ATAQUE MAN IN THE MIDDLE?	3
3. MODALIDADES DE ATAQUE	4
3.1 Ataques basados en servidores dhcp	4
3.2 Ataques basados en cache poisoning	4
3.3 Ataques basados en servidores dns	5
3.4 Ataques basados en la simulación de un punto de acceso inalámbrico	5
3.5 Ataques basados en man in the browser	5
4. VULNERABILIDADES EN LA ACTUALIDAD	6
4.1 Aplicaciones bancarias de EE.UU y Reino Unido	6
4.2 El Bluetooth y el Internet de las Cosas (IoT)	6
4.3 Blockstack	7
4.4 Gitlab	7
4.5 Errores en Windows	8
5. SIMULACIÓN DEL ATAQUE	8
5.1 Ataque para HTTP	9
5.2 Ataque para HTTPS	11
6. MECANISMOS DE DETECCIÓN Y PROTECCIÓN	13
6.1 Detección del ataque	13
6.2 Aplicaciones para detectar sniffers	14
6.3 Técnicas de protección frente a los sniffers	15
7. CONCLUSIONES	16
8. BIBLIOGRAFÍA	17

1. INTRODUCCIÓN

Desde que la humanidad ha sido capaz de enviar mensajes a través de internet, ha habido personas que han intentado interceptarlos o manipularlos pasando desapercibidos. Si antes se acechaba a los mensajeros o se “pinchaban” los cables del teléfono, hoy Internet ofrece posibilidades de espionaje mucho más sutiles. Gran parte del tráfico mundial de datos tiene lugar por medio de redes públicas que no están lo suficientemente cifradas y a esto hay que añadir que las vías de transmisión en la red global de ordenadores resultan algo opacas para los usuarios.

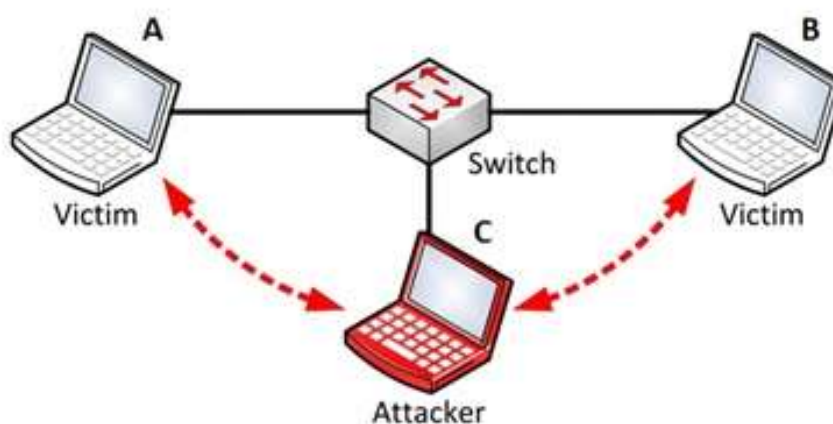
Los paquetes de datos, en el camino que va desde el remitente hasta el destinatario, pasan generalmente por una gran variedad de etapas intermedias con diferentes niveles de seguridad. Aquí es donde entran en juego los hackers y los servicios de inteligencia, cuyo objetivo es acceder a datos sensibles y usarlos en beneficio propio. Cada vez es mayor el número de usuarios que buscan opciones para que las vías de transmisión en Internet sean más seguras. Sin embargo, ¿qué ocurre cuando un atacante se hace pasar por el receptor legítimo de la información que se tiene que transmitir? Este **método de espionaje** recibe el nombre de ataque **Man in The Middle** o Man in The Middle attack.

2. ¿QUÉ ES UN ATAQUE MAN IN THE MIDDLE?

Se entiende por aquel método en el que un hacker interviene en el tráfico de datos de dos participantes en la comunicación haciéndose pasar por uno o por otro, de forma que les hace creer que se están comunicando entre ellos cuando en realidad lo hacen con el intermediario.

El **esquema básico** de un ataque Man in The Middle es el siguiente:

[1] “El sistema A intenta crear una conexión codificada con el sistema B. En su lugar, un tercer partido malintencionado desvía el flujo de datos para establecer la conexión codificada del sistema A con el sistema C. Esto tiene como consecuencia que aquel que tenga el control sobre el sistema C (el atacante generalmente) pueda examinar, grabar o manipular el tráfico de datos, a menudo incluso sin que los participantes en la comunicación sean conscientes de ello. Una vez hecha la transmisión a la world wide web, el sistema C se presentará como servidor web ante el sistema A y como navegador web ante el sistema B”.



3. MODALIDADES DE ATAQUE

Para infiltrarse en el tráfico de datos entre dos o más sistemas, los hackers recurren a diversas técnicas que se centran en las debilidades de la comunicación por Internet. [1]

El servicio **DHCP** (Dynamic Host Configuration Protocol), responsable de la concesión de direcciones IP locales, ofrece, por ejemplo, una superficie de ataque para los ataques Man in The Middle internos en la red de área local. Por otro lado, el **protocolo de resolución de direcciones**, conocido como ARP o Address Resolution Protocol, entra en juego para lo referente a la investigación de direcciones de hardware (Media Access Control, MAC). En términos generales, los ataques Man in The Middle pueden llevarse a cabo mediante la **manipulación de servidores DNS**, que son los encargados de la resolución de direcciones de Internet en IP públicas. Además, los hackers hacen uso de las **brechas de seguridad en software de navegación anticuados** o ponen a disposición de los usuarios más ingenuos accesos corruptos a redes de área local inalámbricas.

3.1 Ataques basados en servidores DHCP

Es un hacker el que coloca su propio ordenador (o uno que esté bajo su control) en una red de área local (LAN) a modo de servidor DHCP. Este es un componente esencial de una red local y se encarga de la asignación de la configuración de red a otros ordenadores de la red local. Asimismo, éste envía un mensaje de transmisión a todos los dispositivos conectados a la red de área local, aguarda a la respuesta de un servidor DHCP y acepta la primera que entre.

Con ello, los hackers tienen la posibilidad de controlar la adjudicación de direcciones IP locales mediante el servidor DHCP simulado, de registrar las puertas de acceso que se deseen y el servidor DNS en los ordenadores a los que se ha engañado y, por lo tanto, de **desviar el tráfico de datos saliente a cualquier ordenador** para interceptar y manipular contenidos.

Debido a que esta modalidad de ataque se basa en la manipulación del sistema DHCP, la terminología adoptada en este caso es la de **DHCP spoofing** (en español, manipulación). Sin embargo, la condición para realizar el ataque Man in The Middle es que el **atacante utilice la misma red de área local** que su víctima. En el caso de las LAN de los hoteles o en las redes inalámbricas públicas existe el peligro de convertirse en el blanco de un ataque basado en un servidor DHCP. Si un atacante quiere infiltrarse en una red corporativa que funciona por cable, este tendrá que conseguir primero un acceso físico a la red LAN para poder introducir un servidor DHCP falso.

3.2 Ataques basados en cache poisoning

Por **ARP** (Address Resolution Protocol) se entiende aquel protocolo de red que sirve para resolver direcciones IP de redes LAN en direcciones de hardware (direcciones MAC).

Esta asignación de direcciones MAC a IP locales se guarda en forma de **tabla en el caché ARP** del ordenador que solicita la información. Es aquí donde actúa el llamado ARP cache poisoning (envenenamiento de caché ARP).

El objetivo de este tipo de ataque **es manipular las tablas ARP** de los diversos ordenadores de la red por medio de respuestas de ARP falsas para que, por ejemplo, un ordenador que está bajo el control del atacante actúe como punto de acceso inalámbrico o puerta de entrada para Internet.

Si un ataque de ARP spoofing tiene éxito, los atacantes tienen la posibilidad de **leer** la totalidad de los **datos salientes** de los ordenadores a los que se ha engañado, pero también de registrarlos o de **manipularlos** antes de transmitirlos a la verdadera puerta de acceso. Al igual que el DHCP spoofing, el envenenamiento de caché ARP solo puede ser posible cuando el **atacante** se encuentra en la **misma red de área local** que el sistema que ha sido víctima del ataque.

3.3 Ataques basados en servidores DNS

La prioridad del envenenamiento del caché basado en servidores DNS es el **sistema de nombres de dominio** de Internet, que es el responsable de la resolución de URL en direcciones IP públicas. En este tipo de ataques, los hackers **manipulan las entradas en el caché de un servidor DNS** con el objetivo de persuadirlos para que respondan a las solicitudes con **direcciones de destino falsas**. Si el ataque Man in The Middle se ha llevado a cabo con éxito, los hackers pueden derivar a otros usuarios de Internet, sin que estos sean conscientes, a una página web de la red. Para ello, en la mayoría de los casos se emplean las **vulnerabilidades conocidas de los servidores DNS más antiguos**.

3.4 Ataques basados en la simulación de un punto de acceso inalámbrico

Un modelo de ataque dirigido sobre todo a los usuarios de dispositivos móviles se basa en la **simulación de un punto de acceso inalámbrico** en una red inalámbrica pública, como las de las cafeterías o las de los aeropuertos. En ello, un atacante configura su ordenador de tal manera que este se convierta en una **vía adicional para acceder a Internet** (probablemente una con una calidad de señal mejor que el propio punto de acceso). De esta manera, si el atacante consigue engañar a los usuarios más ingenuos, este **puede acceder y manipular la totalidad de los datos de su sistema** antes de que éstos se transmitan al verdadero access point o punto de acceso. Si este requiere autenticación, el hacker recibe para ello los nombres de usuario y contraseñas que se utilizan en el registro. El peligro de convertirse en el blanco de estos ataques Man in The Middle se da particularmente cuando los dispositivos de salida se configuran de tal manera que se pueden comunicar automáticamente con los puntos de acceso con mayor potencia de señal.

3.5 Ataques basados en man in the browser

El **ataque man in the browser** es una variante del ataque Man in The Middle. En él, el atacante instala **malware en el navegador** de los usuarios de Internet con el objetivo de **interceptar sus datos**. Los ordenadores que no están correctamente actualizados son los que, sobre todo, ofrecen brechas de seguridad que permiten a los atacantes infiltrarse en el sistema. Si se introducen programas en el navegador de un usuario de forma clandestina, estos registran en un segundo plano todos los datos que se intercambian entre el sistema de la persona que ha sido víctima del ataque y las diferentes páginas web. De esta manera, esta modalidad de ataque hace que los hackers puedan intervenir en una gran cantidad de sistemas con relativamente poco esfuerzo. En ello, el espionaje de datos suele tener lugar, por lo general, antes de que se lleve a cabo una posible codificación del transporte de datos mediante protocolos como TLS o SSL.

4. VULNERABILIDADES EN LA ACTUALIDAD

Man in The Middle sigue muy presente en nuestros días, prueba de ellos son las siguientes vulnerabilidades actualmente detectadas en las que un ataque Man in The Middle sería totalmente útil.

A continuación se presenta una serie de vulnerabilidades que se han encontrado recientemente, que el ataque Man in The Middle podrían explotar.

4.1 Aplicaciones bancarias de EE.UU y Reino Unido

Hace tan solo unos días saltaban las alarmas [2] debido a que ocho aplicaciones bancarias contenían una vulnerabilidad oculta en sus protecciones TLS, que podrían haberse explotado para realizar ataques Man in The Middle y robar diversos datos de usuarios. Esto se debe a que un error de fijación del certificado dejó a los clientes de las aplicaciones susceptibles a los ataques Man in The Middle que a su vez ponían sus credenciales (nombre de usuario, contraseñas, información personal, información bancaria) en riesgo de robo.

Esto es precisamente el tipo de cosa que se supone que un certificado de este tipo previene. Una serie de investigadores descubrieron que en la implementación de certificados y verificación de éstos (utilizados para crear la conexión de seguridad en la capa de transporte), **el certificado tenía un fallo en la correcta verificación en el nombre del host**, lo que permitía el ataque Man in The Middle.

Actualmente la mayoría de navegadores web y plataformas móviles como Android e iOS confían en un almacén que contiene una gran cantidad de certificados de CA. Si uno de ellos actúa de forma maliciosa o ha sido comprometido, pueden generarse certificados para cualquier dominio permitiendo así a un atacante realizar un Man in The Middle a cualquier aplicación que confíe en dicho certificado de CA.

Para evitar esto ya se implementó una medida de seguridad adicional, **denominada certificado Pinning** [3]. Así los desarrolladores podían elegir aceptar sólo certificados firmados por un único certificado raíz CA. A pesar de esto, analizando las aplicaciones bancarias se descubrió que aunque las aplicaciones enlazaban correctamente con el certificado raíz de CA, éstas no verificaban el nombre del host, dejando así la puerta abierta a un ataque Man in The Middle.

4.2 El Bluetooth y el Internet de las Cosas (IoT)

Recientemente se hacía público [4] que un nuevo vector de ataque ponía en peligro los principales sistemas operativos móviles, de escritorio y del Internet de las Cosas, incluidos Android, iOS, Windows y Linux y cualquier otro dispositivo que los utilice, corriendo el riesgo de sufrir tanto de ataques de malware como de man in the middle que pueden llevarse a cabo de forma remota para controlar tu dispositivo sin requerir ninguna interacción de la parte de la víctima.

Utilizando estas vulnerabilidades, los investigadores de seguridad de la empresa de IoT Armis han ideado un ataque, **BlueBorne** [5], que podría permitir a cualquier atacante hacerse por completo de los dispositivos habilitados para bluetooth, propagar malware, o incluso establecer una conexión Man in The Middle para obtener acceso a los datos y redes críticas de los dispositivos, incluso propagarse por dispositivos adyacentes.

Tal y como especifica la plataforma de seguridad que ha tratado la vulnerabilidad [6], uno de los puntos fuertes de este ataque es que se propaga por el aire (airborne), incluso aunque el dispositivo no se encuentre en modo detectable. Al propagarse por el aire, BlueBorne apunta al punto más débil de la defensa de las redes, y el único que no protege ninguna medida de seguridad, siendo así **altamente infeccioso**. Además, dado que el proceso de Bluetooth tiene altos privilegios en todos los sistemas operativos, explotarlo proporciona prácticamente un **control total sobre el dispositivo**, capacidades extremadamente deseables para todo hacker.

Esto ha llegado a generar hasta ocho vulnerabilidades de día cero, siendo cuatro clasificadas como **críticas**. Destacamos aquellas dos en las que se puede realizar un ataque Man in The Middle:

The Bluetooth Pineapple – Man in The Middle attack (CVE-2017-0783) → Android

Con una severidad media [6], esta vulnerabilidad permite al atacante **interceptar e intervenir todos los datos que van o vienen del dispositivo objetivo**. Para crear un ataque MITM usando WIFI, el atacante requiere de un equipo especial y una solicitud de conexión del dispositivo objetivo a una red WIFI abierta. La vulnerabilidad reside en un perfil de la pila Bluetooth y permite al atacante crear una interfaz de red maliciosa en el dispositivo de la víctima, reconfigurar el enrutamiento IP y formar al dispositivo para transmitir todas las comunicaciones a través de la interfaz de red maliciosa. Este ataque no requiere ninguna interacción del usuario, por lo que es prácticamente invisible.

The Bluetooth Pineapple – Man in The Middle attack (CVE-2017-8628) → Windows

Idéntica a la anterior y de igual severidad, pero para la plataforma Windows [7].

4.3 Blockstack

Si bien los ataques de Man in The Middle normalmente suelen ser con fines malintencionados, este reciente caso nos muestra el lado contrario. Concretamente ocurrió cuando un grupo de hackers intentaron engañar a los inversores durante una oferta inicial de monedas (ICO-TOKENS) a la startup Blockstack [8].

Blockstack [9] es una startup que intenta establecer un nuevo Internet para aplicaciones descentralizadas desde su propio navegador, ofrece aplicaciones que permiten mantener una privacidad, seguridad y libertad. Aprovechando esta posición, unos estafadores aprovecharon la oportunidad de crear sitios web de **phishing** que eran réplicas de blockstack.com. Estos sitios web falsificados realmente estaban en contacto con un servidor regulado por Blockstack, en concreto, éste alimentaba el banner superior del sitio legítimo con tweets de la cuenta de Twitter de la compañía.

Este detalle ayudó de manera muy importante en la resolución del conflicto, ya que esta conexión permitió al equipo de Blockstack socavar los sitios de phishing realizando un contraataque basado en Man in The Middle.

En un ataque Man in The Middle como este, consiguieron colocarse entre su propio feed de Twitter y los sitios web de estafa (phishing), advirtiendo así con diferentes mensajes a aquellos que potencialmente podrían haber perdido fondos por los sitios que no eran legítimos.

4.4 Gitlab

Gitlab, el popular gestor de repositorios Git basados en la web, ha estado afectado por una vulnerabilidad que podría haber expuesto a sus usuarios a ataques de secuestro de sesión.

Tras un test de penetración, un investigador descubrió [10] que era posible realizar un **secuestro de sesiones** en Gitlab. Este tipo de ataque involucra la interceptación de tokens de sesión, que identifican a usuarios individuales conectados a un sitio web. Un atacante puede usar un token secuestrado para acceder a la cuenta de un usuario, hacer compras ilegales, cambiar las credenciales de inicio de sesión y acceder a datos de la tarjeta de crédito por nombrar algunas posibilidades.

Además, dichos **tokens de sesión** eran **persistentes**, una vez emitidos nunca caducan sin importar cuanto tiempo ha estado inactivo un usuario, o incluso si ha cerrado sesión en su cuenta. Dentro de este método se incluye el ataque Man in The Middle, con el que se podría robar los tokens de sesión y utilizarlos para transmitir una conexión como segura, obteniendo así un método para recoger los datos.

Ésta no es la única vulnerabilidad que disfruta Gitlab, si quisiéramos ejecutar **compilaciones en una máquina remota** haciendo uso del SSH, nuevamente estaríamos expuestos a un posible Man in The Middle, concretamente debido a una opción que falta en su configuración, la StrictHostKeyChecking [11].

4.5 Errores en Windows

Sistemas operativos como Windows tampoco están exentos de posibles vulnerabilidades que se puedan aprovechar mediante Man in The Middle.

Concretamente, podemos encontrar dos que afectan al **protocolo de seguridad NT Lan Manager**. Dado este problema, un atacante podría ejecutar un ataque Man in The Middle anulando el funcionamiento de LDAP, es decir, se podrían **secuestrar las credenciales** aprovechando el protocolo de seguridad propio de sistemas Windows. No sólo esto, sino que además un atacante podría crearse una cuenta de administrador para **tomar el control sobre la red atacada**, siempre y cuando el sistema tenga registrado un administrador.

Uno de ellos, el registrado como **CVE-2017-8563** [12] y de estado crítico, ha sido solucionado recientemente.

5. SIMULACIÓN DEL ATAQUE

Una vez conocido en qué consiste el ataque, sus tipos y algunos casos reales, vamos a proceder a realizar una simulación de ataque.

En este caso vamos a realizar el ataque Man in The Middle entre dos entidades, **una entidad atacante** (Ubuntu 16.04 virtualizado), y una **entidad atacada** la cual ha sido Ubuntu (Ubuntu 16.04 virtualizado) [13].

Vamos a realizar varios ataques Man in The Middle. En un primer caso para **HTTP** y después para **HTTPS**. Vamos a utilizar varias herramientas, principalmente ettercap, SSLstrip y wireshark.

5.1 Ataque para HTTP

HTTP es un **protocolo de comunicación** que permite las transferencias de información en la World Wide Web, que **no utiliza cifrado** en el proceso de comunicación, por lo tanto, es **vulnerable a recibir ataques** como el de Man in The Middle.

Para realizar el ataque, se va a utilizar la herramienta **ettercap** [14]. Con ella, realizaremos un envenenamiento en el protocolo ARP, y con ello intentaremos obtener los datos de usuario y password de la entidad atacada.

Procedemos a realizar el ataque. En primer lugar iniciamos la máquina atacante con privilegios de administrador, abrimos la herramienta ettercap, y una vez dentro, seguimos los siguientes pasos:

1. Seleccionamos la tarjeta de red para proceder a realizar el esnifado de la red (registrar el tráfico de la red y procesarlo). En este caso hemos seleccionado la tarjeta de red eth0.

```
Listening on:
enp0s3 -> 08:00:27:D0:57:DE
      192.168.1.200/255.255.255.0
      fe80::ba13:53d8:e318:c865/64

Listening on:
lo -> 00:00:00:00:00:00
      127.0.0.1/255.0.0.0
      ::1/128

Privileges dropped to EUID 65534 EGID 65534...

33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Bridged sniffing...
```

2. Realizamos un análisis de los hosts conectados a esa red, utilizando una máscara /255. A continuación se nos muestra una lista de los hosts que se encuentran conectados a la red, incluyendo el router.

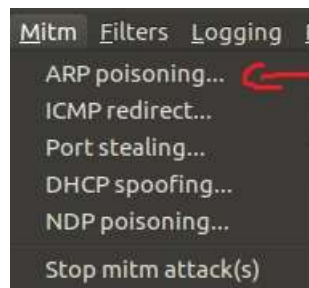
En este ejemplo se nos muestran 5 dispositivos conectados. Podemos deducir que el router es el dispositivo con IP= 192.168.1.1, ya que los routers siempre suelen tener las primeras direcciones de la red.

Host List 🚪		
IP Address	MAC Address	Description
192.168.1.1	00:4A:77:E2:52:7D	
192.168.1.7	16:88:11:C3:75:1A	
192.168.1.131	F8:94:C2:B7:84:37	
192.168.1.132	D4:61:2E:69:F5:6D	
192.168.1.150	08:00:27:99:C1:0C	

3. Por ejemplo, **vamos a atacar** a la IP 192.168.150, por tanto, lo que se hace es añadir esta IP como **objetivo 1** y el **gateway(router)** como **objetivo 2**. La idea es ser intermediario entre la comunicación del equipo con IP 192.168.1.150 y el router(192.168.1.1). El resultado debe ser el siguiente:

```
Host 192.168.1.150 added to TARGET1  
Host 192.168.1.1 added to TARGET2
```

4. Ahora realizamos un envenenamiento del protocolo ARP para recibir el tráfico entre el objetivo 1 y el objetivo 2. La idea es vincular la dirección MAC del atacante con la dirección IP del equipo. Si esto se realiza con éxito, podremos interceptar el tráfico entre los dos objetivos seleccionados.



5. Tras realizar los pasos anteriores ahora debemos esperar a que empiece a generarse tráfico entre el objetivo 1 y el objetivo 2.

Por ejemplo, observamos lo siguiente:

```
GROUP 1 : 192.168.1.150 08:00:27:99:C1:0C  
GROUP 2 : 192.168.1.1 00:4A:77:E2:52:7D  
HTTP : 46.245.181.141:80 -> USER: swap PASS: pwdswap INFO: http://www.comunio.es/login.phtml  
CONTENT: login=swap&pass=pwdswap&action=login&%3E%3E+Login_x=33&tzOffset=2
```

Observamos que se ha enviado tráfico a la dirección IP 46.245.181.141:80, y nos muestra la información que se ha enviado durante ese tráfico. En esa información podemos ver las credenciales de acceso de la víctima para acceder a dicho sitio web (user: swap, password: pwdswap).

Veamos otro ejemplo:

```
HTTP : 192.168.1.1:80 -> USER: admin PASS: admin INFO: http://192.168.1.1/  
CONTENT: frashnum=&action=login&Frm_Logintoken=0&port=&Username=admin&Password=admin
```

En este caso, se ha producido tráfico hacia la dirección 192.168.1.1, dirección para acceder a la configuración del router. Como podemos comprobar, también se ha capturado las credenciales de acceso de la víctima para acceder a dicha configuración.

5.2 Ataque para HTTPS

En este caso, vamos a utilizar la herramienta **ettercap** y **SSLstrip**. Respecto a ettercap, el procedimiento es el mismo que se ha descrito para el ataque HTTP. Lo que hace SSLstrip es engañar al servidor y **convertir todo el HTTPS de una web en HTTP** (sin cifrar).

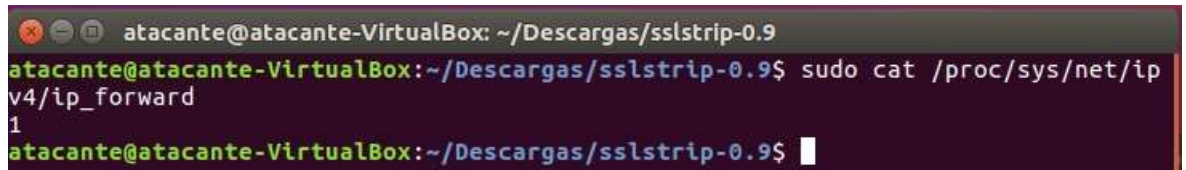
La definición de SSLStrip[14] es variada, intentemos acercarnos a la realidad práctica que es lo que más nos puede interesar. SSLStrip consiste en hacer creer al usuario que está bajo una conexión segura, ya sea porque el usuario ve un candadito que indica seguridad, SSLstrip puede falsificarlo, o por que el usuario no se fija si está bajo tráfico cifrado o no.

Cuando un atacante lanza SSL Strip sobre una víctima, ésta sigue navegando felizmente por la red. El problema viene cuando se conecta a una página bajo HTTPS, la víctima puede observar como el HTTPS ha desaparecido de su navegador, si no se fija en ese pequeño detalle y se autentifique en algún sitio, sus credenciales irán en texto plano hacia la víctima.

Vamos a proceder a realizar el ataque [14]:

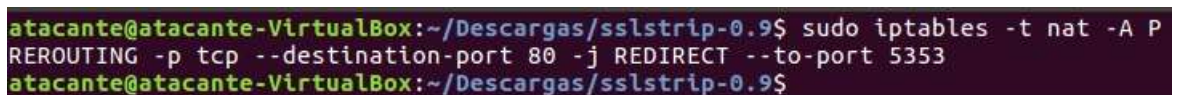
1. En primer lugar, introducimos los siguientes comandos en la terminal:

- Configura la interceptación en modo de reenvío.



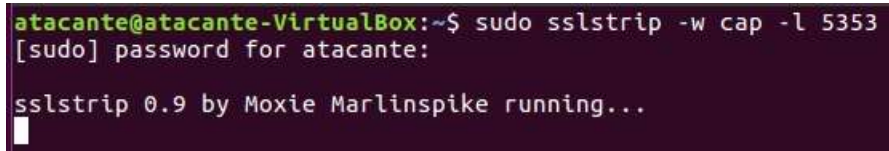
```
atacante@atacante-VirtualBox: ~/Descargas/sslstrip-0.9
atacante@atacante-VirtualBox:~/Descargas/sslstrip-0.9$ sudo cat /proc/sys/net/ipv4/ip_forward
1
atacante@atacante-VirtualBox:~/Descargas/sslstrip-0.9$
```

- Indicamos al firewall que redirija el tráfico del puerto 80 a SSLstrip(indicamos puerto 5353).



```
atacante@atacante-VirtualBox:~/Descargas/sslstrip-0.9$ sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 5353
atacante@atacante-VirtualBox:~/Descargas/sslstrip-0.9$
```

- Iniciamos SSLstrip para convertir el tráfico HTTPS a HTTP.



```
atacante@atacante-VirtualBox:~$ sudo sslstrip -w cap -l 5353
[sudo] password for atacante:
sslstrip 0.9 by Moxie Marlinspike running...
```

2. Seleccionamos la tarjeta de red para proceder a realizar el esnifado de la red (registrar el tráfico de la red y procesarlo). En este caso hemos seleccionado la tarjeta de red eth0 (mismo proceso que para el ataque a HTTP).

3. Realizamos un análisis de los hosts conectados a esa red, utilizando una máscara /255. A continuación se nos muestra una lista de los hosts que se encuentran conectados a la red, incluyendo el router (mismo proceso que para el ataque a HTTP).

4. Por ejemplo, **vamos a atacar** a la IP 192.168.1.150, por tanto, lo que se hace es añadir esta IP como **objetivo 1** y el **gateway(router)** como **objetivo 2**. La idea es ser intermediario entre la comunicación del equipo con IP 192.168.1.150 y el router(192.168.1.1) (mismo proceso que para el ataque a HTTP).

5. Ahora realizamos un envenenamiento del protocolo ARP para recibir el tráfico entre el objetivo 1 y el objetivo 2. La idea es vincular la dirección MAC del atacante con la dirección IP del equipo. Si esto se realiza con éxito y SSLstrip funciona, podremos interceptar el tráfico entre los dos objetivos seleccionados (mismo proceso que para el ataque a HTTP).

6. Tras realizar los pasos anteriores ahora debemos esperar a que empiece a generarse tráfico entre el objetivo 1 y el objetivo 2.

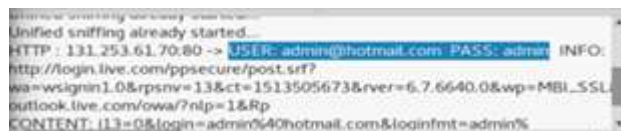
Por ejemplo, vamos a observar un ejemplo:

La víctima ha entrado en la página de la universidad de Granada: www.prado.ugr.es



Como podemos observar, ettercap nos muestra las credenciales que ha usado la víctima para hacer login en la página de la universidad de Granada (se ha ocultado la contraseña por motivos de seguridad).

Si esperamos un poco más, podemos esperar a que la víctima inserte las credenciales en diferentes sitios. En este ejemplo nos muestra las credenciales que se han utilizado para acceder al servidor de correo Hotmail.



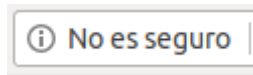
Como podemos observar, ettercap nos muestra toda la información que puede desear el atacante, ya sean las credenciales usadas por la víctima, o la dirección IP de destino donde poder utilizar dichas credenciales.

¿Cómo ha funcionado esto si tanto la plataforma de Prado, como la de Hotmail utilizan el protocolo HTTPS?

Lo que ha hecho la herramienta SSLstrip ha sido forzar a que la navegación de la víctima sea mediante el protocolo HTTP, y éste no utiliza cifrado (como se ha visto anteriormente).

¿Cómo podemos darnos cuenta si navegamos por HTTP o HTTPS?

Podemos comprobar si nuestra navegación es segura o no observando la barra de direcciones del navegador. Por ejemplo, en el ejemplo mostrado anteriormente, cuando la víctima ha entrado en la página de la universidad de Granada, en la barra de direcciones le mostraba lo siguiente:



Este mensaje nos muestra que estamos navegando de forma no segura, por lo que podríamos ser vulnerables a recibir un ataque de este tipo.

Mencionar que también hay que tener en cuenta el nivel de seguridad del navegador, ya que hay navegadores que permiten la navegación en modo no seguro, y otros que no la permiten. Por ejemplo, en el ataque que se ha mostrado, la víctima utilizó el navegador **chromium**, mientras que si hubiera utilizado otro como por ejemplo Firefox, que consta de un nivel mayor de seguridad, el ataque no hubiera tenido éxito.

6. MECANISMOS DE DETECCIÓN Y PROTECCIÓN

Una vez se ha conocido como funciona el ataque Man in The Middle, ¿cómo podemos **detectar** si alguien nos está intentando realizar este tipo de ataque?, ¿cómo podemos **protegernos** ante este tipo de ataque?, a continuación se van a proporcionar ciertos métodos y actitudes para responder a estas preguntas.

6.1 Detección del ataque

Es complicado detectar un Man in The Middle (que suelen utilizar aplicaciones de tipo Wireshark o Cain) porque trabajan de manera pasiva con programas que no dejan huellas. Un ordenador mediante un simple sniffer conectado a una misma red puede acceder a mucha de la información que circula por la red ya que esa información suele circular en texto plano.

Algunas de las técnicas para detectar un ataque Man in The Middle son:

Acceso físico: Si tenemos acceso físico a todos los ordenadores de la red podemos ver para cada uno los procesos activos y así detectar si existe algún proceso de tipo sniffer. Si estos programas **no están ejecutados** en ese momento podemos **comprobar la lista de aplicaciones instaladas**.

Prueba de ICMP: Se realiza un 'ping' a la dirección IP que deseemos para **analizar el retardo de los paquetes**. En esa misma red creamos conexiones TCP falsas durante un periodo de tiempo esperando a que el sniffer procese estos paquetes, de esta manera incrementa el tiempo de latencia. Una vez que volvamos a analizar el retardo del 'ping' se puede observar que el tiempo en milisegundos aumenta, esto probaría que tenemos un sniffer en nuestra red.

Prueba de ARP: Se basa en un test que realiza una petición de tipo ICMP echo (ping) a la dirección IP que queramos, pero con una MAC errónea. Para esto, **agregamos una nueva entrada a la tabla ARP** mediante el comando 'arp -s [IP][MAC]' (comando que nos ofrece ARP), se puede comprobar que se ha añadido correctamente con el comando 'arp -a', que muestra el contenido de la tabla. Al ser la dirección MAC incorrecta el paquete enviado no debería llegar a su destino, en caso contrario, es decir, si el paquete llega a su destino es debido a que la tarjeta de red está en modo promiscuo dando lugar a un posible sniffer en la red.

6.2 Aplicaciones para detectar sniffers

Existen algunas aplicaciones que realizan pruebas para detectar posibles sniffers en nuestra red, muchas de ellas comprobando si la máquina está en modo promiscuo o haciendo uso de las técnicas anteriormente comentadas.

¿Qué es el modo promiscuo?

Si una máquina pone su interfaz de red en modo promiscuo, significa que la interfaz podrá **leer todo el tráfico que circula por la red**. Una máquina en modo promiscuo puede leer un paquete que circula por la red, aunque no sea suyo.

Algunas de las aplicaciones para detectar posibles sniffers son:

CPM: Aplicación encargada de ver si la interfaz de la máquina está en modo promiscuo, creada por la universidad de Carnegie Mellon.

SniffDet: Realiza pruebas de posibles protocolos que nos pueden llevar a la detección de un sniffer (prueba de ARP, test de ping de latencia, test de ICMP y test de DNS).

NEDEP: Es un programa muy sencillo que realiza peticiones de ARP para cada dirección IP de la red, destinando los paquetes a una dirección inexistente (ojo, no al broadcast), las interfaces que estén en modo promiscuo contestarán a esas peticiones, con un ARP Replay mostrando un mensaje.

Promiscan, Promisdetec y proDETECT: Creados para sistemas Windows y tratan de detectar los host que se encuentran en modo promiscuo en redes LAN.

Sentinel: hace uso de las librerías Libcap y Libnet. Parecido a Antisnif, también se encarga de detectar las técnicas en modo promiscuo, y usa test de ICMP, ping de latencia, test de DNS y test de ARP.

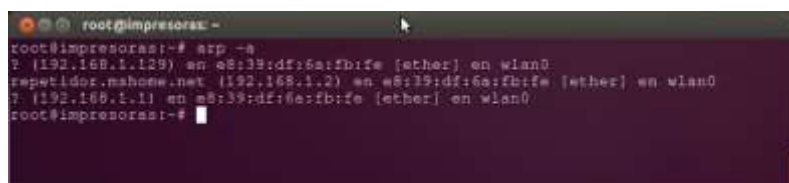
NAST (Network Analyzer Sniffer Tool): dispone de la capacidad de descubrir máquinas en modo promiscuo.

Snort: Es un Sistema de prevención y detección de intrusos en la red (IDS/IPS) de código abierto, desarrollado por Sourcefire. Snort [16] es uno de los más poderosos y ligeros IDS, posee análisis de tráfico a tiempo real, registro de paquetes, y puede detectar gran variedad de ataques y enviar alertas a tiempo real. El principal problema con los IDS es que tienden a generar una gran cantidad de falsos positivos, lo que requiere personal especializado para atender dichos eventos.

A continuación, vamos a mostrar un método sencillo para detectar posibles intrusos con la llamada prueba de ARP.

La prueba de ARP consiste en comprobar si ha habido alguna alteración en nuestra tabla ARP.

Veamos un ejemplo.

A terminal window with a dark background and light text. The prompt is 'root@impresoras:~'. The user has entered the command 'arp -a'. The output shows three entries in the ARP table, all with the MAC address 'e8:39:df:6a:fb:fe' and interface 'wlan0'. The first entry is for IP '192.168.1.129', the second for '192.168.1.2' (labeled as 'repetidor.mahone.net'), and the third for '192.168.1.1'.

```
root@impresoras:~  
root@impresoras:~# arp -a  
? (192.168.1.129) en e8:39:df:6a:fb:fe [ether] en wlan0  
repetidor.mahone.net (192.168.1.2) en e8:39:df:6a:fb:fe [ether] en wlan0  
? (192.168.1.1) en e8:39:df:6a:fb:fe [ether] en wlan0  
root@impresoras:~#
```

En esta red hay un repetidor (192.168.1.2) de un equipo router (192.168.1.1). Se pudo observar que hay una IP (192.168.1.129) que tiene la misma MAC que el repetidor. Por lo que podemos deducir que la IP (192.168.1.129) es un posible intruso.

6.3 Técnicas de protección frente a los sniffers

La mejor protección frente a los sniffers es protegiendo la información que enviamos mediante algún tipo de **cifrado**. Para hacer posible el intercambio de mensajes de manera segura para que sólo pueda identificar la información el receptor de la misma se puede hacer uso de las **técnicas de encriptación** que cifran y descifran la información. Algunas de las técnicas que se podría utilizar para la protección son:

- **SSL** (Secure Socket Layer): Proporciona autenticación privada en páginas web mediante el protocolo https.
- **SSH** (Secure Shell): Conexión remota a terminales de manera segura.
- **PGP** (Pretty Good Privacy): Uso de clave pública y clave privada.

También se aconseja lo siguiente [15]:

-**Instalar VLANs**, que mejoran notablemente la seguridad. Es necesario tener en cuenta que algunos tipo de políticas / configuración VLANs, pueden ser aprovechadas para ser atacadas mediante ARP Spoofing.

-Algunos **routers / switch implantan medidas de seguridad adicionales** anti spoofing mediante reglas...

7. CONCLUSIONES

Hoy en día, utilizamos los dispositivos tecnológicos a diario, ya sea por motivos laborales, personales, de entretenimiento... Estos servicios utilizan las redes como medio de comunicación, y muchas veces no somos conscientes del riesgo que existe al hacer determinadas acciones, ni de las posibles consecuencias que conllevan.

Como hemos podido observar, con unos básicos conocimientos de redes y aplicaciones, se puede comprometer la información personal hasta el grado de poder espiar a una persona o a una organización.

¿Qué se quiere decir con esto? Pues que hay que tomarse la seguridad en redes mucho más en serio, tanto los usuarios como los administradores, tomando conciencia del riesgo, y aplicando mecanismos de prevención y protección para intentar defenderse de posibles ataques.

La seguridad nunca es efectiva al 100%, y si algo aprendemos observando, tanto el atrás como el presente, es que cada poco tiempo surgen nuevas vulnerabilidades, que posibles atacantes pueden explotar, aunque al poco tiempo se intente lanzar un parche para arreglar este posible error. Esto es un ciclo continuo, ya que el desarrollo de software siempre es propenso a poder tener algún error que no se ha previsto o detectado, y ya sea ahora o en el futuro ese error puede dar lugar a graves consecuencias.

Es responsabilidad de los administradores asegurarse de que la información se mantiene segura, pero el concentrarse en proteger el sistema sólo de los ataques externos es un error muy común de éstos, ya que la implantación de políticas de seguridad debe de tener en cuenta que los ataques que busquen comprometer a nuestros sistemas no solamente pueden venir desde fuera de nuestra red, sino también desde dentro.

“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los computadores” – Kevin Mitnick.

8. BIBLIOGRAFÍA

- [1] 1&1, Ataque Man in The Middle: modalidades y contramedidas [en línea], 6 Junio 2017, disponible en: <https://www.1and1.es/digitalguide/servidores/seguridad/ataques-man-in-the-middle-un-vistazo-general/>
- [2] Bradley Barth, Newly created tool spots TLS vulnerability in major banking and VPN apps [en línea], 6 Diciembre 2017, disponible en: <https://www.scmagazine.com/newly-created-tool-spots-tls-vulnerability-in-major-banking-and-vpn-apps/article/712371/>
- [3] Eleven Paths, Certificate pinning. El qué, el cómo y por qué (I) [en línea], 26 Agosto 2013, disponible en: <http://blog.elevenpaths.com/2013/08/certificate-pinning-el-que-el-como-y-el.html>
- [4] Swati Khandelwal, Blueborne: Critical Bluetooth Attack Puts Billions of Devices at Risk of Hacking [en línea], disponible en: <https://thehackernews.com/2017/09/blueborne-bluetooth-hacking.html>
- [5] Más información en:
The Attack Vector “BlueBorne” Exposes Almost Every Connected Device [en línea], disponible en: <https://www.armis.com/blueborne/>
- [6] Más información en:
NATIONAL VULNERABILITY DATABASE CVE-2017-0783 Detail [en línea], 14 Septiembre 2017, disponible en el siguiente enlace: <https://nvd.nist.gov/vuln/detail/CVE-2017-0783>
- [7] Más información en:
NATIONAL VULNERABILITY DATABASE CVE-2017-8628 Detail [en línea], 12 Septiembre 2017, disponible en el siguiente enlace: <https://nvd.nist.gov/vuln/detail/CVE-2017-8628>
- [8] CoinDesk, How Blockstack Counterattacked a Phishing Attempt on Its ICO [en línea], 30 Noviembre 2017, disponible en: <https://quantco.in/cms/p089lh>
- [9] Más información en:
Blockstack [en línea], disponible en: <https://blockstack.org/about>
- [10] Daniel Svartman, Discovering a Session Hijacking Vulnerability in GitLab [en línea], 30 Agosto 2017, disponible en: <https://www.incapsula.com/blog/blocking-session-hijacking-on-gitlab.html>
- [11] Más información en:
GitLab Documentation [en línea], disponible en: <https://docs.gitlab.com/runner/executors/ssh.html>
- [12] NATIONAL VULNERABILITY DATABASE CVE-2017-8563 Detail [en línea], 14 Julio 2017, disponible en: <https://nvd.nist.gov/vuln/detail/CVE-2017-8563>
- [13] Vivek Ramachandran, Cameron Buchanan, Kali linux wireless penetration testing beginner's guide, 2ª edición, Packt Publishing, edición 2015.
- [14] Robert W. Beggs, Mastering Kali linux for advanced penetration testing, 1ª edición, Packt Publishing, edición 2014

- [15] Ariel Sepulveda, Sniffers: ¿cómo detectarlos dentro de nuestra red?, [en línea], 19 Enero 2015, <https://es.safeandsavvy.f-secure.com/2015/01/19/sniffers-como-detectarlos-dentro-de-nuestra-red/>
- [16] Hou Xiangning, et al. The detection and prevention for ARP spoofing based on Snort, International Conference on Computer Application and System Modeling, IEEE, 2010