Grado en Ingeniería Informática

Servidores Web de altas prestaciones
Curso 2017-2018

Universidad de Granada

ugr | Universidad de Granada

Trabajo Final
Ataques man-in-the-middle

Realizado por
Natalia María Mártir Moreno
Francisco Antonio Martinez Blanco

Índice

1. Introducción

El objetivo de la mayoría de los ciberdelincuentes es robar la información valiosa para los usuarios.
Los ataques pueden ser dirigidos a usuarios individuales, páginas web con más envergadura o bases de datos financieras. Aunque la forma de hacerlo sea diferente en cada situación, el fin siempre es el mismo.

En la mayoría de los casos, los criminales intentan, en primer lugar, insertar algún tipo de malware en el equipo de la víctima, ya que ésta es la forma más sencilla de robar los datos, pero si esto no resulta posible por cualquier motivo otra de las formas más comunes es el ataque Man-in-the-Middle.

Como sugiere su nombre en inglés, en este método se introduce un intermediario (el cibercriminal o una herramienta maliciosa) entre la víctima y la fuente: una página de banca online o una cuenta de correo electrónico. Estos ataques son realmente efectivos y, a su vez, muy difíciles de detectar por el usuario, quien no es consciente de los daños que puede llegar a sufrir.

2. ¿Qué es un ataque man-in-the-middle?

Una vez introducidos este tipo de ataques, pasaremos a definir con detalles lo que son.
El concepto de un ataque man-in-the-middle es muy sencillo. Además, no se limita únicamente al ámbito de la seguridad informática o el mundo online.
Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas.
Por ejemplo, en el mundo offline, se crearían facturas falsas, enviándolas al correo de la víctima e interceptando los cheques de pago de dichos recibos.
En el mundo online, un ataque MiTM es mucho más complejo, pero la idea es la misma. El atacante se sitúa entre el objetivo y la fuente; pasando totalmente desapercibido para poder alcanzar con éxito la meta.

En resumen el atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.
El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando éste se emplea sin autenticación.

3. ¿Qué implica un ataque Man-in-the-Middle?

Hasta el momento, hemos dado a entender que el ataque permite la lectura de la información. Sin embargo, es necesario añadir que no solo está disponible esta opción. El atacante también puede añadir información a la ya existente o modificar aquella ya existente. Esto abre un abanico bastante amplio de posibilidades para el atacante.

En la actualidad, los ciberdelincuentes utilizan este ataque para modificar la información que el usuario visualiza en una página web. Es decir, es probable que esté ante un formulario, pero que este no sea el legítimo de la página web, sino el introducido por el atacante.

4. La necesidad de una transferencia adicional por un canal seguro

Salvo en el protocolo de interbloqueo , todos los sistemas criptográficos seguros frente a ataques MitM requieren un intercambio adicional de datos o la transmisión de cierta información a través de algún tipo de canal seguro.

En ese sentido, se han desarrollado muchos métodos de negociación de claves con diferentes exigencias de seguridad respecto al canal seguro.

5. Variantes de ataque

En el ataque MiTM más habitual, se utiliza un router WiFi para interceptar las comunicaciones del usuario. Esto se puede realizar configurando el router malicioso para que parezca legítimo o atacando un error del mismo e interceptando la sesión del usuario.

En el primero de los casos, el atancante configura su ordenador u otro dispositivo para que actúe como red WiFi, nombrándolo como si fuera una red pública (de un aeropuerto o una cafetería).

Después, el usuario se conecta al “router” y busca páginas de banca o compras online, capturando el criminal las credenciales de la víctima para usarlas posteriormente.

En el segundo caso, un delincuente encuentra una vulnerabilidad en la configuración del sistema de cifrado de un WiFi legítimo y la utiliza para interceptar las comunicaciones entre el usuario y el router. Éste es el método más complejo de los dos, pero también el más efectivo; ya que el atacante tiene acceso continuo al router durante horas o días. Además, puede husmear en las sesiones de forma silenciosa sin que la víctima sea consciente de nada.

Una variante más reciente de este tipo de ataque es el ataque man-in-the-browser. En este contexto, el ciberdelincuente usa una serie de métodos para insertar un código malicioso en el equipo de la víctima, el cual funciona dentro del navegador. Este malware registra, silenciosamente, los datos enviados entre el navegador y las páginas. Estos ataques han ganado en popularidad porque permiten al delincuente atacar a un grupo mayor de víctimas sin la necesidad de estar cerca de éstas.

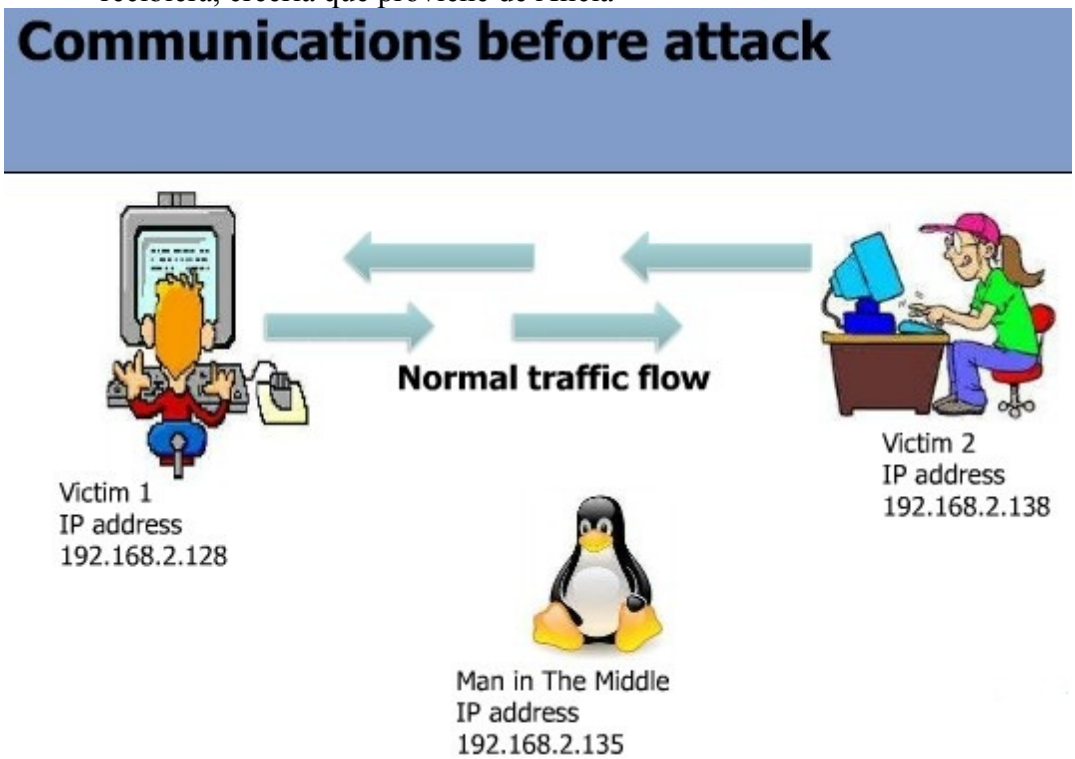
6. Comunicación

Antes del ataque :

Esto para explicarlo mejor, lo pondremos con un ejemplo :

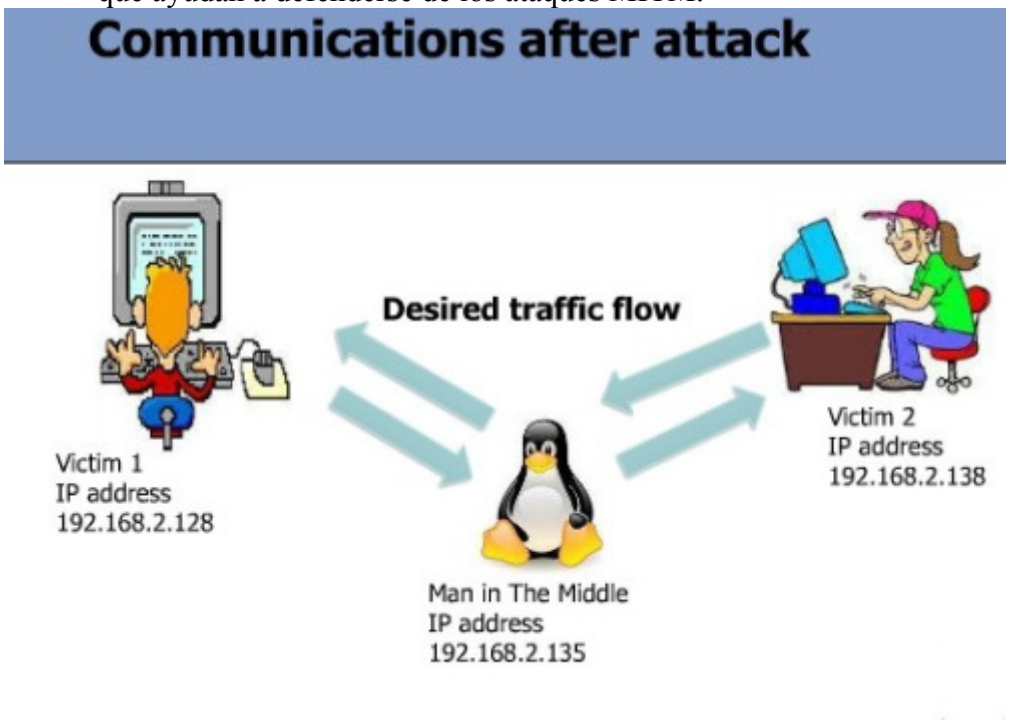
Supongamos que Alicia desea comunicarse con Roberto, y Manuel (ATACANTE) quiere interceptar esa conversación, o quizás quiera hacer llegar un mensaje falso a Roberto. Para iniciar la comunicación, Alicia debe solicitar a Roberto su clave pública. Si Roberto envía su clave a Alicia, pero Manuel es capaz de interceptarla, éste podría desplegar un ataque MITM.

Manuel podría enviar a Alicia su propia clave pública (la de Manuel, en lugar de la de Roberto). Alicia, creyendo que la clave pública recibida es de Roberto, cifraría su mensaje con la clave de Manuel y enviaría el criptograma a Roberto. Manuel interceptaría de nuevo, descifraría el mensaje con su clave privada, guardaría una copia; volvería a cifrar el mensaje con la clave de Roberto (tras una alteración, si así lo desea) y lo re-enviaría a Roberto. Cuando éste lo recibiera, creería que proviene de Alicia



Después del ataque :

Este ejemplo ilustra la necesidad de Alicia y Roberto de contar con alguna garantía de que están usando efectivamente las claves públicas correctas. En otro caso, sus comunicaciones se verían expuestas a ataques de este tipo usando la tecnología de clave pública. Afortunadamente, existe una variedad de técnicas que ayudan a defenderse de los ataques MITM.



7. Defensas contra el ataque :

La posibilidad de un ataque man-in-the-middle sigue siendo un problema potencial de seguridad muy serio, incluso para muchos cripto-sistemas basados en clave pública. Existen varios tipos de defensa contra estos ataques MITM, estas defensas emplean técnicas de autenticación basadas en:

- Infraestructura de claves públicas
- Autenticación mutua fuerte tales como:
- Claves secretas (que suelen ser información secreta de entropía alta y por lo tanto más segura)
- Contraseñas (passwords) (que son generalmente información secreta de entropía baja y por lo tanto menos segura)
- El examen de latencia, como con mucho los cálculos de la función hash criptográfica que conducen a decenas de segundos, si ambas partes toman normalmente 20 segundos y el cálculo de 60 segundos para llegar a cada parte, esto puede indicar a un tercero en la comunicación.
- Un segundo canal de verificación (seguro).
- Pads(almohadillas) de una sola vez son inmunes a los ataques MITM, en el supuesto caso de la seguridad y la confianza de la plataforma de una sola vez.
- Verificación hacia adelante

- Se están llevando a cabo pruebas sobre la eliminación de certificados comprometidos por las autoridades de emisión en las computadoras actuales y los certificados comprometidos están siendo exportados al área de sandbox antes de removerlos para analizar.

La integridad de las claves públicas en general se deben asegurarse de alguna manera, pero éstas no tienen que ser secretas. Las contraseñas (passwords) y claves secretas compartidas tienen el requerimiento de secreto adicional. Las claves públicas pueden ser verificadas por una autoridad de certificación (CA), cuya clave pública se distribuye a través de un canal seguro (por ejemplo: con un navegador web o instalación en el sistema operativo). Las claves públicas también pueden ser verificadas por una web de confianza que distribuye las claves públicas a través de un canal seguro (por ejemplo: reuniones cara a cara).

También tendremos que tener en cuenta:

Usa siempre HTTPS: muchos sitios web ofrecen desde hace tiempo comunicaciones cifradas a través de SSL, siempre que visites una página asegúrate de que la dirección muestre HTTPS en lugar de HTTP, y si no lo hace, escríbelo manualmente. Esto no te protege de vulnerabilidades del lado del cliente, y de sitios que no han aplicado el parche a Heartbleed si fueron afectados, pero al menos evita que que los ataques menos sofisticados intercepten tus comunicaciones.

Activar la verificación de dos pasos: muchos servicios han comenzado a ofrecer verificación de dos factores en sus servicios para aumentar la seguridad del acceso a las cuentas de usuario. Siempre que el mecanismo de verificación de los dos factores sea suficientemente fuerte, esta es otra linea de defensa contra atacantes.

Usar una red VPN: de esta manera la conexión se cifra entre un cliente VPN y un servidor VPN, estableciéndose a través de un túnel de comunicación seguro.

8. Análisis de un ataque :

Trafico capturado de una red que se sospecha esta bajo un ataque MITM puede ser analizado con el fin de determinar si realmente fue un ataque MITM o no. Una prueba importante para analizar al hacer el análisis forense de la red de un sospechoso ataque MITM SSL incluye:

- Dirección IP del servidor
- DNS del servidor
- Certificado del servidor X.509
    - Es el mismo certificado firmado?
    - Es el certificado firmado por una CA de confianza?
    - Ha sido revocado el certificado?
    - Ha sido certificado recientemente?

Otros clientes, en otros lugares de internet, también obtuvieron el mismo certificado?

9. Posibles subataques

El ataque MitM puede incluir algunos de los siguientes subataques:

- Interceptación de la comunicación, incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos conocidos.
- Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.
- Ataques de sustitución.
- Ataques de repetición.
- Ataque por denegación de servicio. El atacante podría, por ejemplo, bloquear las comunicaciones antes de atacar una de las partes. La defensa en ese caso pasa por el envío periódico de mensajes de *status* autenticados.

MitM se emplea típicamente para referirse a manipulaciones activas de los mensajes, más que para denotar interceptación pasiva de la comunicación.

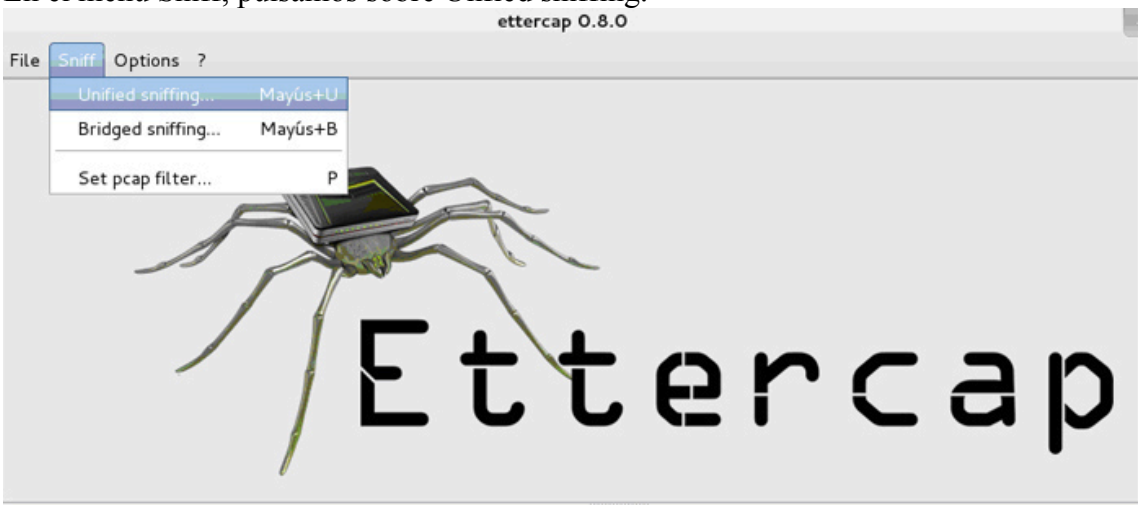
10. Ejemplo de cómo producir un ataque:

Lo primero que vamos a hacer es abrir el Ettercap-graphical en Kali y el WireShark. Este último programa es un potente sniffer de red, muy útil para los que trabajamos administrando redes informáticas, ya sea para ver posibles ataques, o simplemente para tener un mayor control del tráfico de red, e incluso diagnosticar problemas de red por exceso de tráfico.

Para abrirlo vamos a Aplicaciones, Kali Linux, Husmeando, Envenenamiento de redes y ettercal-graphical. El WireShark dispone de una guía de uso en la sección Manuales.

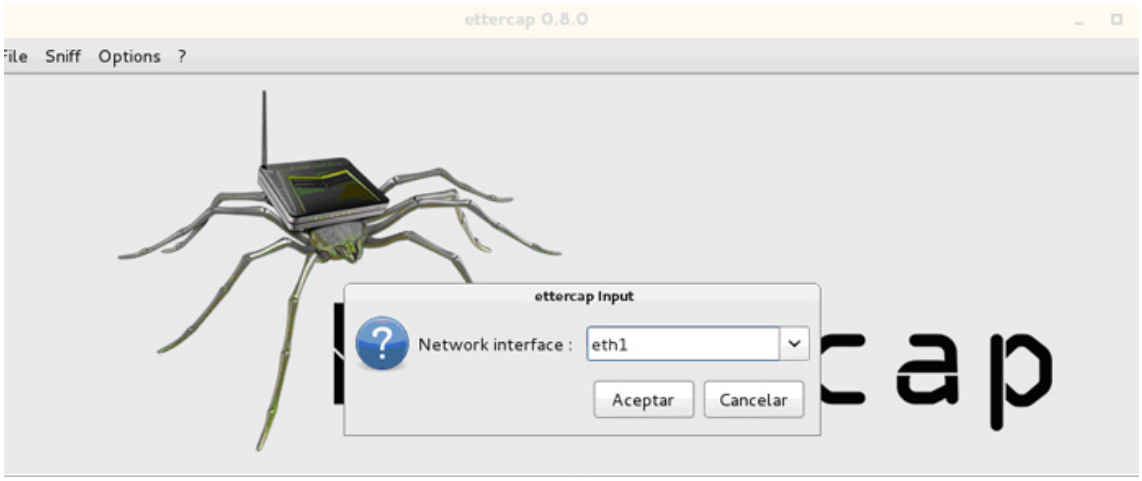
Se abrirá la siguiente pantalla.

En el menú Sniff, pulsamos sobre Unfied sniffing.

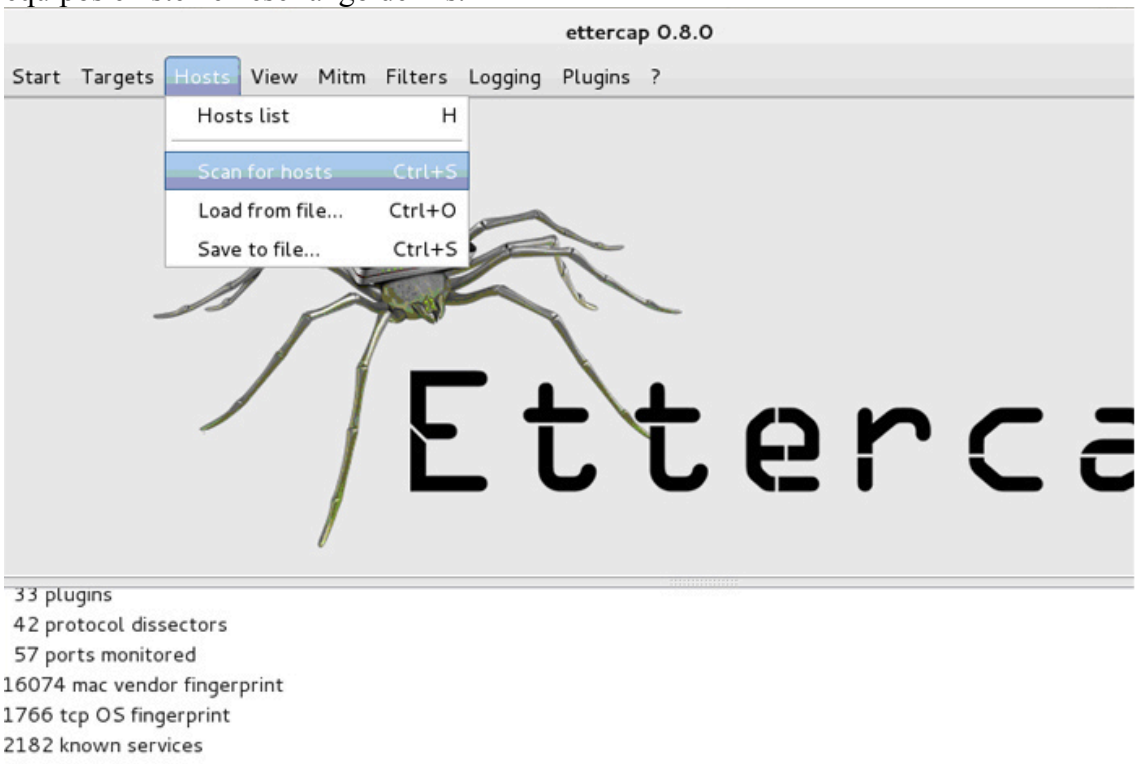


Ahora si disponemos de más de una tarjeta de red, o interface de red virtuales, seleccionamos la correspondiente, en mi caso eth1. Debe ser el interface de red que esté configurado con una IP dentro del rango de la víctima, que lógicamente conoceremos o será imposible atacar.

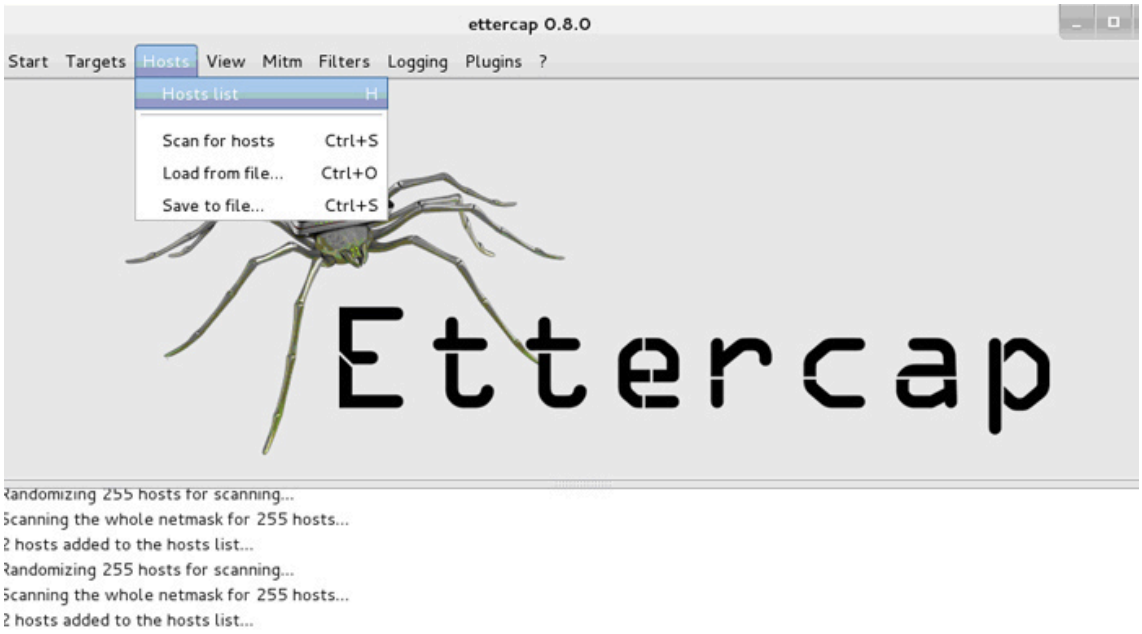
Para saberlo existen miles de aplicaciones, de dispositivos móviles o de ordenador, cualquiera nois servirá, sino podéis acudir a la guía de hackear wifi, donde se muestran los comandos paso a paso para obtener esas IP.



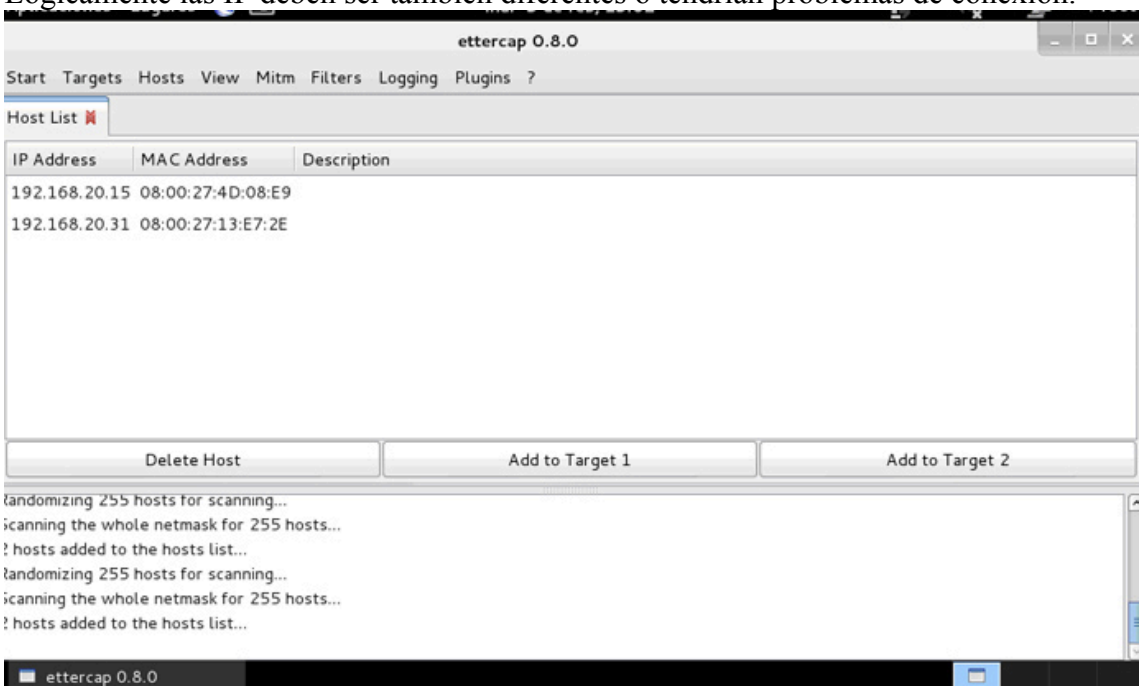
Ahora nos aparecerán nuevos menús. Le damos a Hosts y Scan for hosts para ver que equipos existen en ese rango de IPs.



Una vez finalizado, que no tarda apenas, damos de nuevo al menú Hosts y a Hosts list para que nos muestre que equipos a encontrado.

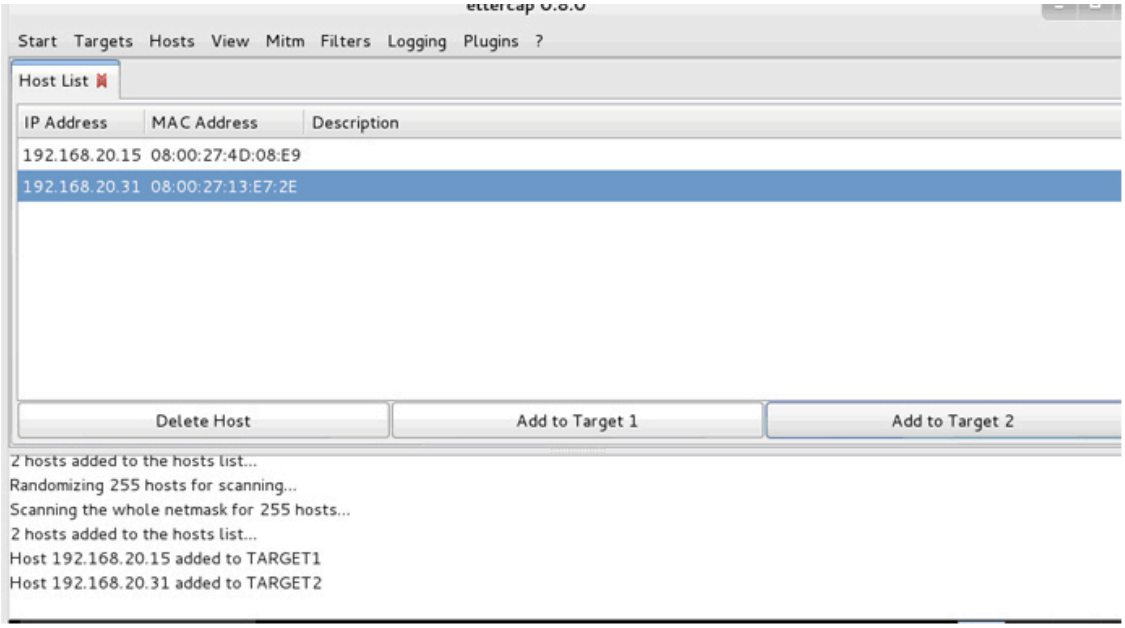


Encuentra los equipos de la red, mostrando sus IP y sus direcciones MAC de las tarjetas de red de cada equipo. Como véis, la MAC siempre es diferente, no existen dos iguales salvo que cambiemos una virtualizando esa dirección para falsearla. Lógicamente las IP deben ser también diferentes o tendrían problemas de conexión.

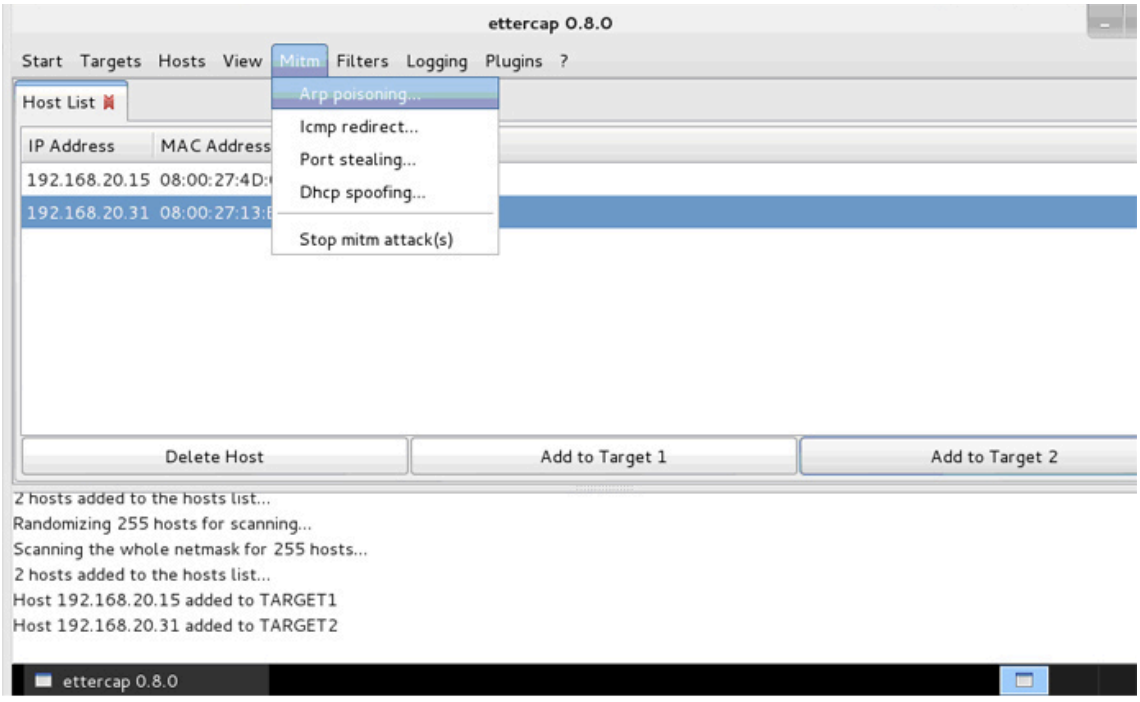


En mi caso la IP acabada en 31 es el Servidor y la 15 el Windows.

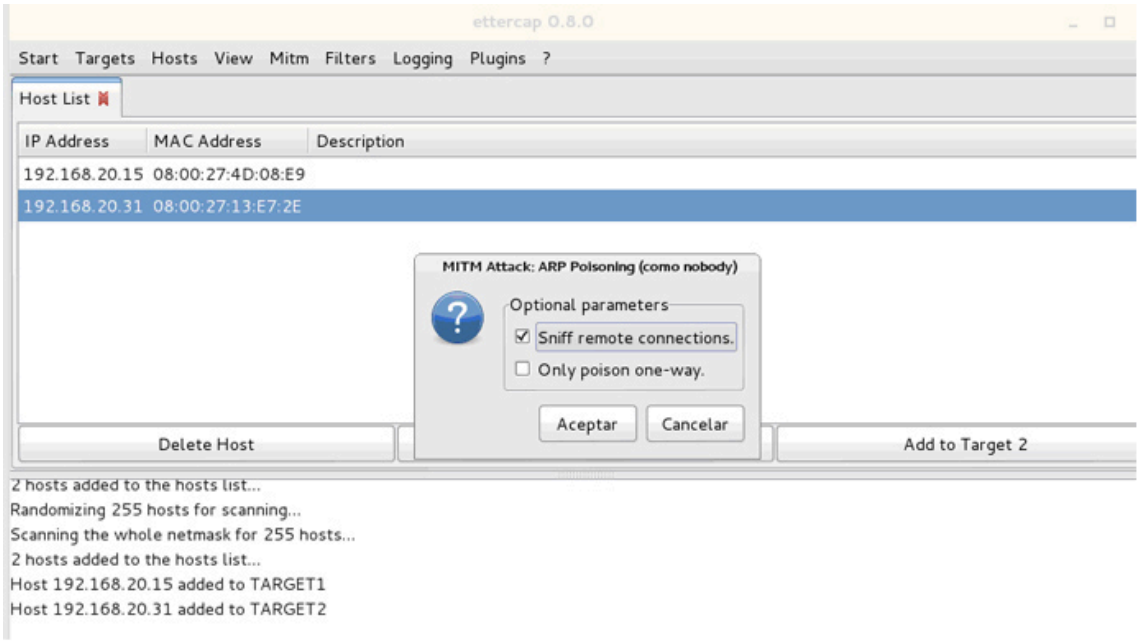
Ahora debemos añadir objetivos, en este caso es muy simple, ya que sólo he levantado dos máquinas virtuales a parte de la atacante. Simplemente marcamos una de las dos víctimas y le damos al botón Add to Target1. Después marcamos la otra víctima y damos al botón Add to target 2.



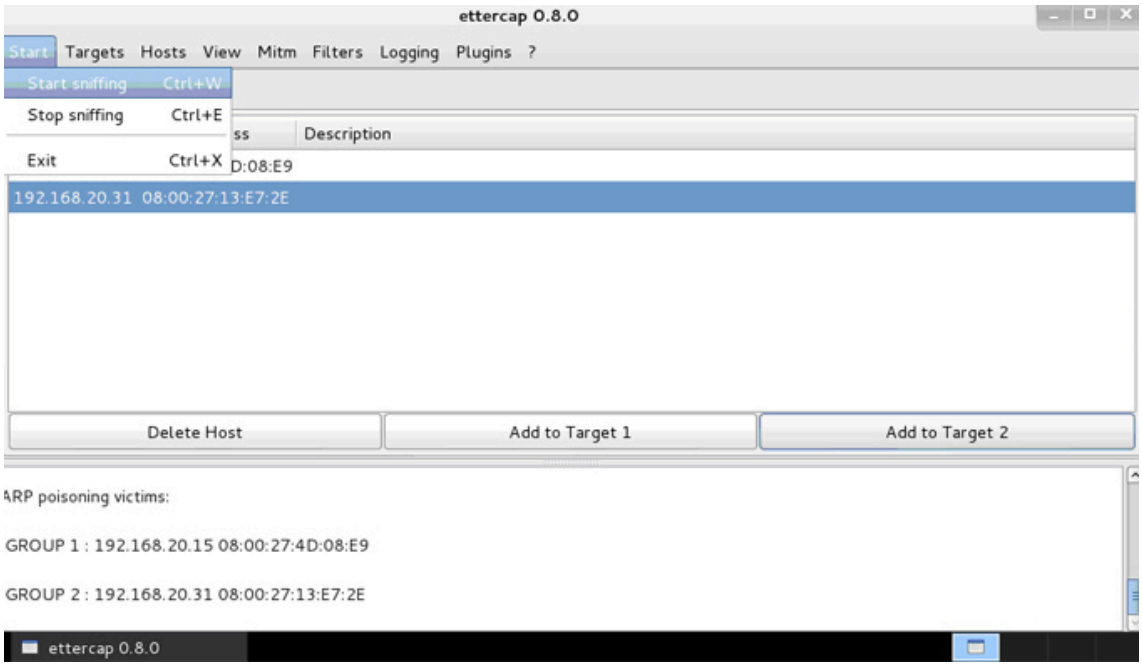
Ahora vamos a realizar un envenenamiento del protocolo ARP para que las víctimas se crean que soy la otra máquina de su red y me manden a mí su tráfico. Damos al manú Mitm y a Arp poisoning.



Nos saldrá la siguiente pantalla, marcamos la opción Sniff remote connections y aceptamos.



Ahora dejamos nuestro sniffer esnifando el tráfico. Damos a Start y a Start sniffing.



Vamos a Windows y ejecutamos el comando arp –a para ver que esté corecto.

La dirección IP acabada en 21 es la atacante, en este caso la Kali Linux. En la primera ejecución vemos que el Kali y el Windows Server tienen diferentes IP y diferentes direcciones MAC. Tras la ejecución del mismo comando tras el envenenamiento ARP, vemos que el Windows XP cree que el Windows Server tiene la dirección MAC del Kali
Con esto hacemos que el tráfico dirigido al servidor, o router si fuese el caso, pase por nosotros.

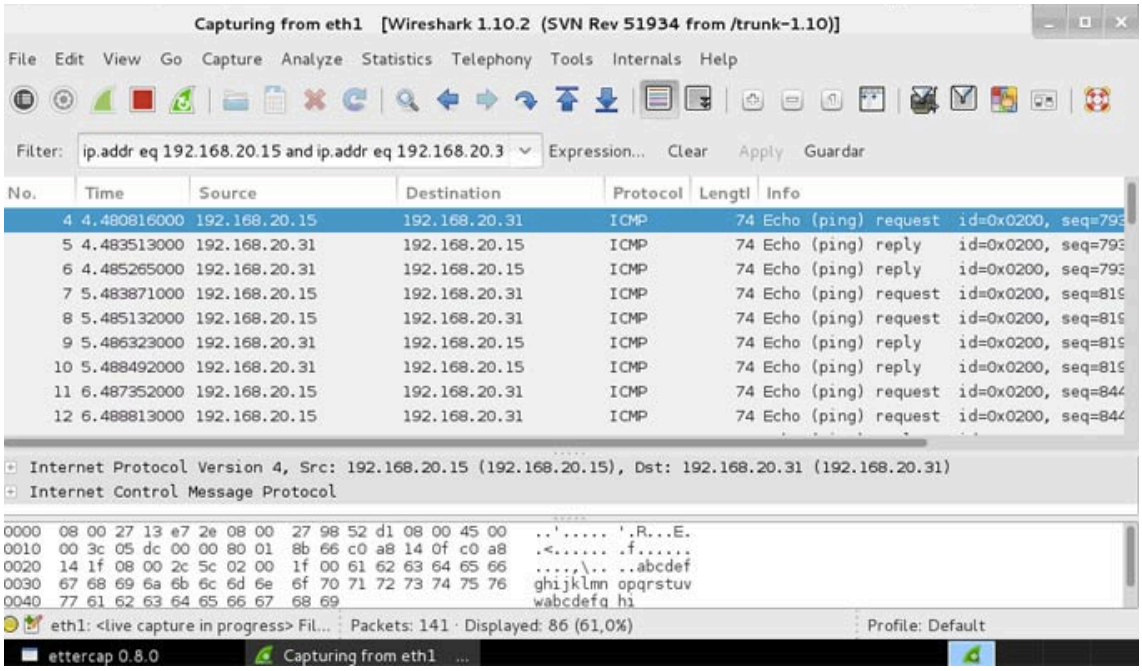
```
Interfaz: 192.168.20.15 --- 0x10003
  Dirección IP          Dirección física      Tipo
  192.168.20.21         08-00-27-98-52-d1     dinámico
  192.168.20.31         08-00-27-13-e7-2e     dinámico

C:\Documents and Settings\Administrador>arp -a

Interfaz: 192.168.20.15 --- 0x10003
  Dirección IP          Dirección física      Tipo
  192.168.20.21         08-00-27-98-52-d1     dinámico
  192.168.20.31         08-00-27-98-52-d1     dinámico

C:\Documents and Settings\Administrador>
```

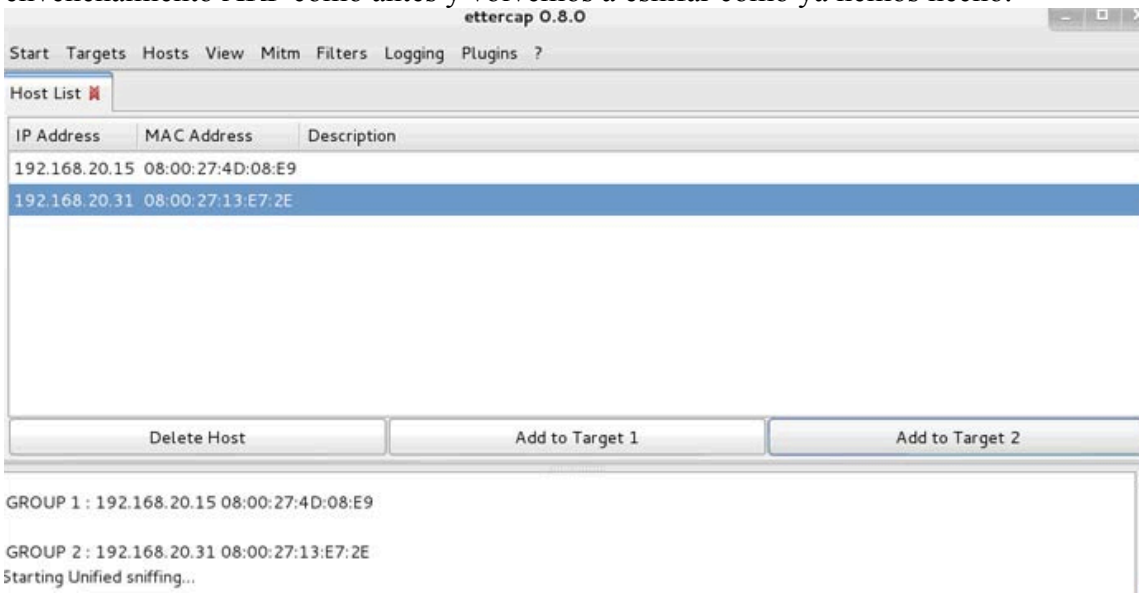
Vamos ahora al Wireshark y lo ponemos a esnifar.



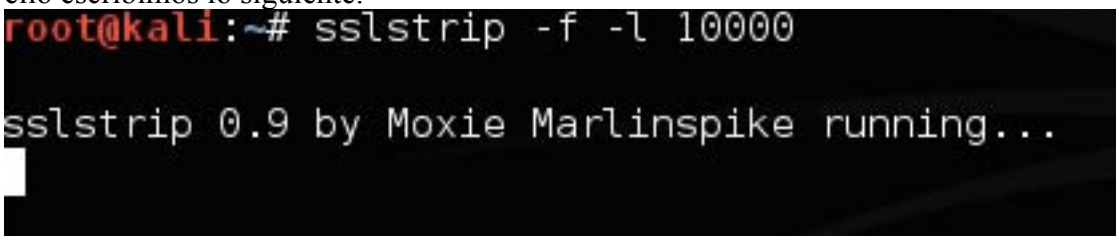
Lanzamos un ping desde la terminal del Windows XP al Servidor de Windows (comando: ping 192.168.20.31). Vemos como las IP que aparecen sólo son del XP y el Servidor, no aparece el atacante por ningún lado.

Ahora creamos un archivo iptables.sh

En el Ethercat añadimos las dos direcciones como target 1 y 2 y hacemos el envenenamiento ARP como antes y volvemos a esnifar como ya hemos hecho.



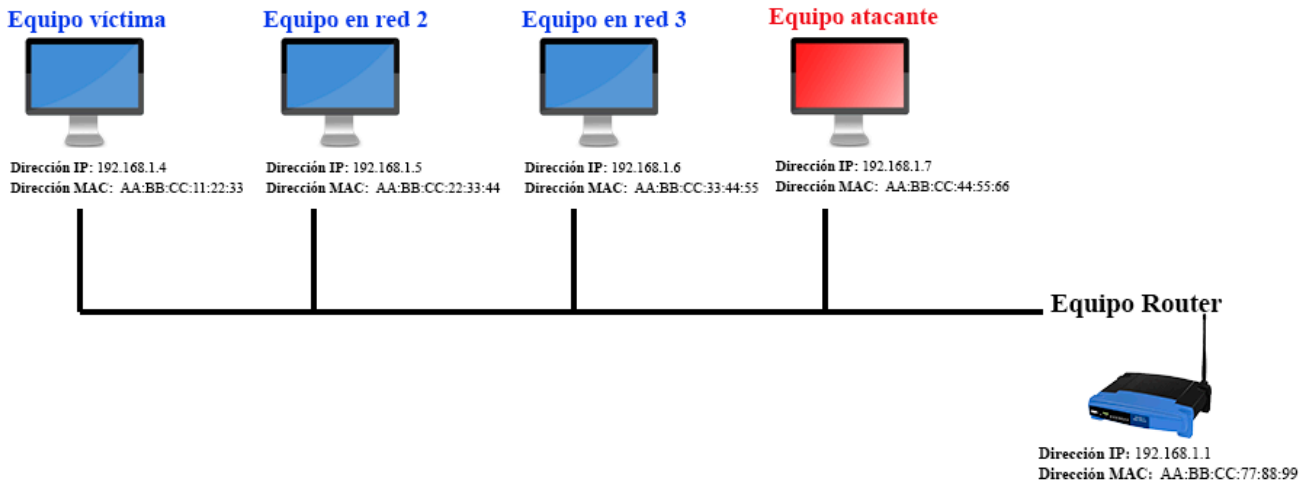
Hacemos un sslstrip desde la consola de comandos del Kali para que las webs SSL (https) se conviertan en simples http y el Ettercap pueda obtener las contraseñas. Para ello escribimos lo siguiente.



Vamos a Instagram y nos logeamos con nuestro usuario y contraseña:
Nos vamos al Ettercap y vemos el enlace del Instagram, usuario y contraseña

11 . Ejemplo de ataque:

Imaginemos la siguiente red con los 4 equipos conectados al router.



El "Equipo atacante" quiere interceptar la conexión de "Equipo víctima" para ello el atacante tiene que hacer creer al equipo víctima que él es el router, esto se consigue creando un paquete ARP Request modificado en el cual se pone como dirección IP origen 192.168.1.4, como dirección IP destino 192.168.1.1 que es la que corresponde con el router y en la dirección MAC destino pone la del equipo atacante, es decir la AA:BB:CC:44:55:66, con todo el paquete ya montado lo enviamos por la red para que lo capte el equipo víctima y guarde en su tabla caché los datos falsificados que le hemos mandado quedando así:

Dirección de Internet	Dirección física
192.168.1.1	aa:bb:cc:44:55:66

Con lo cual ahora todos los paquetes que el equipo víctima mande hacia el router, en realidad serán enviados al equipo atacante pudiendo ser capturados con programas como Wireshark.

12 . Modalidades de ataque:

Para infiltrase 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. 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 man in the middle attacks 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.

En general, este tipo de modalidades de ataque puede automatizarse por medio de software. Si la supervisión en tiempo real se realiza mediante la intervención humana, entonces se puede hablar de human assisted attacks.

12.1 Otros tipos de ataque:

12.1.1 Ataques basados en servidores DHCP:

En el caso de los ataques basados en un servidor 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. Esta tiene lugar, por lo general, de manera automática: en cuanto un ordenador establece la conexión con una red de área local, el cliente DHCP del sistema operativo reclama datos como la dirección IP local, la máscara de red, la dirección de la puerta de acceso predeterminada, o la dirección del servidor DNS competente. Asimismo, este 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.

Las medidas que los usuarios de Internet pueden tomar para prevenir los ataques de DHCP spoofing se reducen, en general, a ser precavidos en lo relativo al uso de redes desconocidas. Grosso modo, se recomienda la utilización de aplicaciones web de bancos online y plataformas de compra que pongan en peligro la seguridad tan solo en redes locales conocidas y fidedignas, como la red doméstica privada o las redes corporativas.

12.1.2 ARP 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). Para que un ordenador pueda enviar paquetes de datos en una red, tiene que conocer las direcciones de hardware del sistema del destinatario. Para ello, se envía una petición de ARP en calidad de transmisión de direcciones MAC a todos los sistemas de la red de área local. Dicha petición contiene tanto las direcciones MAC e IP del ordenador que solicita la información, como la dirección IP del sistema solicitado. Si un ordenador de la red recibe una petición ARP de tales características, el paso siguiente es que este compruebe si el paquete contiene la dirección IP propia en calidad de dirección IP del destinatario. Si es así, se le enviará una respuesta ARP con la dirección MAC al sistema solicitante.

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. Un man in the middle attack puede llevarse a cabo por medio de sencillos programas como la herramienta gratuita **Cain & Abel**, originariamente desarrollada para recuperar contraseñas, o por medio del software Ettercap.

Al igual que en los ataques basados en servidores DHCP, que se realizan en una red de área local corrupta, en este caso los usuarios tienen muy pocas posibilidades para hacer frente al ataque de ARP spoofing. Una de las medidas preventivas consiste en evitar redes desconocidas o en utilizarlas con prudencia.

12.1.3 Ataques basados en servidores DNS:

Mientras que el ARP cache poisoning fija su atención en las debilidades de la resolución de direcciones en Ethernet, 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 persuadirlas 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**.

En principio, los datos del sistema de nombres de dominio no se depositan en un único servidor DNS, sino que se distribuyen por diferentes ordenadores de la red. Cuando un usuario quiere acceder a una página web, este usa, por lo general, un nombre de dominio. Para poder dirigirse al servidor correspondiente, es necesario contar con una dirección IP. Esta es determinada por el router del usuario, que enviará una solicitud de sistema de nombre de dominio al servidor DNS estándar indicado en la configuración. Por regla general, se trata del servidor DNS del proveedor de servicios de Internet (ISP). En caso de encontrar entradas, los llamados registros de recurso o **resource records**, para los URL solicitados, el servidor DNS emite la respuesta a la solicitud con la correspondiente dirección IP. De no ser así, el servidor DNS determinará cuál es la IP buscada con la ayuda de otros servidores con tareas relativas al sistema de nombres de dominio. Para ello, enviará una consulta a otro servidor DNS y guardará la respuesta temporalmente en el caché.

Uno de los puntos de partida para los ataques de los hackers se produce en los servidores que utilizan una versión muy antigua del software de DNS, los cuales, en general, aceptan y guardan aquellos datos solicitados de manera explícita, pero también los que se suministran de manera adicional. Si los hackers consiguen acceder a un único servidor DNS, resulta sencillo entregar registros falsos con cada dirección IP correcta y, por lo tanto, “envenenar” el caché del servidor DNS que realiza la solicitud.

La efectividad de los man in the middle attacks se muestra en algunos acontecimientos que tuvieron lugar en el pasado, en los que se desviaron rangos de nombres completos. A los usuarios les resulta prácticamente imposible protegerse frente a un ataque de este tipo, ya que estos tienen lugar directamente en la infraestructura de Internet. De ello se deduce que la principal tarea de los administradores es ocuparse de que los servidores DNS que estos facilitan utilicen un software actual y que este esté protegido como es debido. De esta manera es como se desarrollaron diversos estándares de Internet bajo el nombre de DNSSEC(Domain Name System Security Extensions), que amplía el sistema de nombres de dominio para que los diferentes mecanismos de seguridad garanticen la autenticidad e integridad de los datos. La difusión de estos estándares sigue siendo un proceso lento.

12.1.4 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 estos 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.

Para protegerse de este tipo de ataques se recomienda que los usuarios de Internet se conecten principalmente con las redes inalámbricas que les sean conocidas y que se aseguren que están utilizando el punto de acceso oficial del proveedor de la conexión.

12.1.5 Ataque 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.

La manera más efectiva de prevenir los ataques man in the browser es asegurarse que todos los componentes de software del sistema en uso están actualizados y que se reducen las vulnerabilidades por medio de actualizaciones de seguridad.

12.1.6 Human assisted attack:

Se puede hablar de human assisted attack cuando una de las modalidades de ataque anteriores no se realiza de manera automática, sino de la mano de uno o varios atacantes en tiempo real. En la práctica, uno de estos man in the middle attacks tendría lugar del siguiente modo: en cuanto un usuario de Internet inicia sesión en la página web de su banco, el hacker, que se ha colocado entre el navegador del usuario y el servidor del banco, recibe una señal. Esto le da la posibilidad de robar las cookies de sesión y la información de la autenticación en tiempo real y de conseguir, así, los nombres de usuario, las contraseñas y los códigos TAN.