Talleres didácticos CEU

Descubre cómo proteger tu red frente a los hackers

v 2.0 – junio 2019

Víctor M. López Millán - Teodoro Rojo Aladro

CEU
Universidad San Pablo

ESCUELA POLITÉCNICA SUPERIOR
Departamento de Tecnologías de la Información

Índice

Atacantes. Quién y por qué

- **¿Quién nos ataca?**
  - Delincuentes
  - Oponentes (empresariales, políticos, …)
  - Vándalos
  - Empleados descontentos

- **¿Por qué lo hace?**
  - Beneficio económico (robo, extorsión, …)
  - Venganza
  - Vandalismo
  - Reto intelectual, afán de protagonismo
  - …

Atacantes. Cómo

- Configuración inadecuada
  - Configuración por defecto
  - Contraseñas débiles
  - Vulnerabilidades no corregidas (parches)
  - Vulnerabilidades sin corrección o desconocidas *(zero-day attack)*
- Ejecución de malware (código malicioso)
- Errores en el software
  - Desbordamientos de *buffer*, combinaciones inesperadas de entrada, bombas lógicas, inyección de código, …
- Debilidades en los algoritmos o protocolos de seguridad
- Ingeniería social (son las debilidades “humanas”)

El triángulo de la intrusión (*fraud triangle*)

- La realización de un ataque requiere la combinación de tres elementos: medios técnicos, motivación y oportunidad (el conocido como *Triángulo de la Intrusión*).

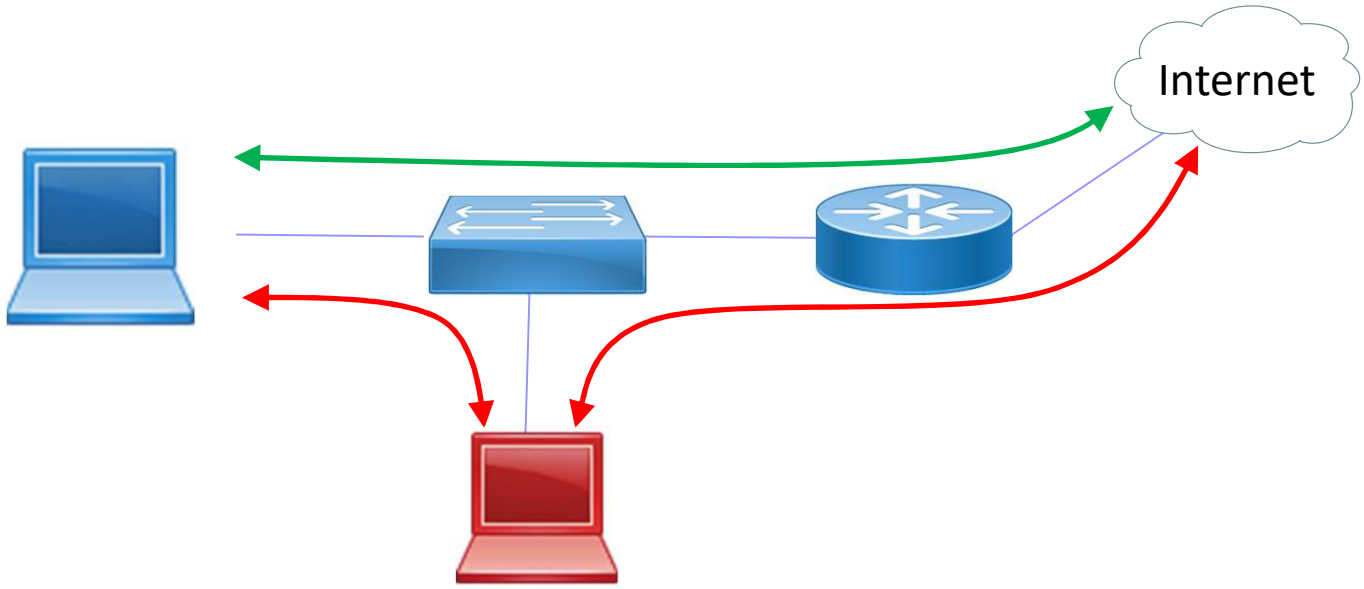
Tipos de ataques

- Análisis de tráfico (*sniffing*)
- Ataques de repetición (*replay attacks*)
- Suplantación de identidad (*spoofing*)
- Inyección de código
- *Cross-Site Scripting* (*XSS*)
- Denegación de servicio (*DoS*)
- Denegación de servicio distribuida (*DDoS*)
- Fraudes, engaños y extorsiones
- …

Índice

Ataque MitM – *Man in the Middle*

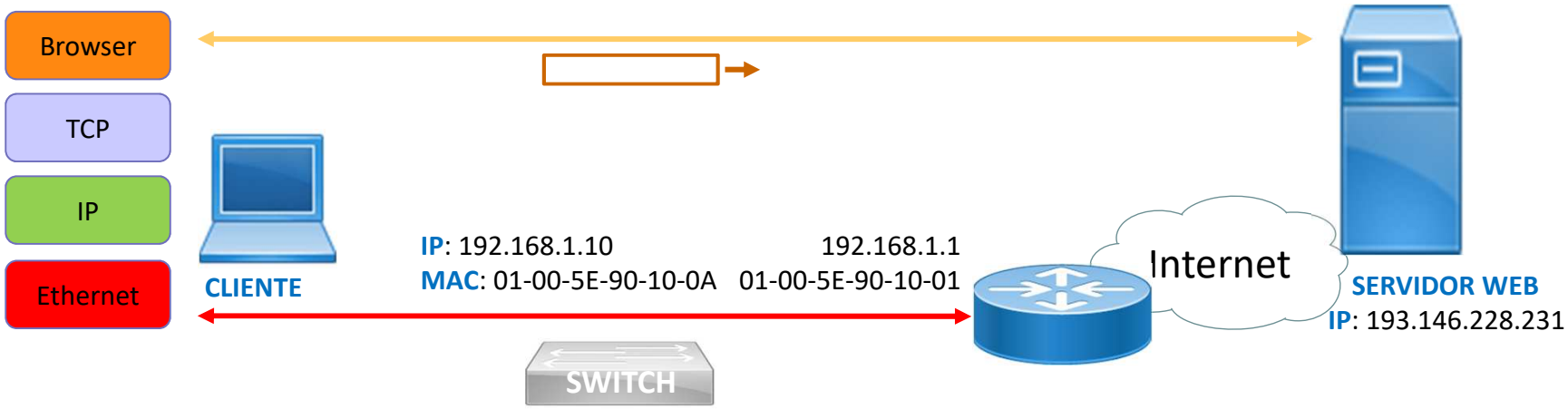
- Ataque de ámbito local: Red de área Local (LAN) o Wifi
- El tráfico legítimo se desvía hacia el atacante alterando las tablas de direcciones MAC (*ARP spoofing* / *ARP poisoning*)

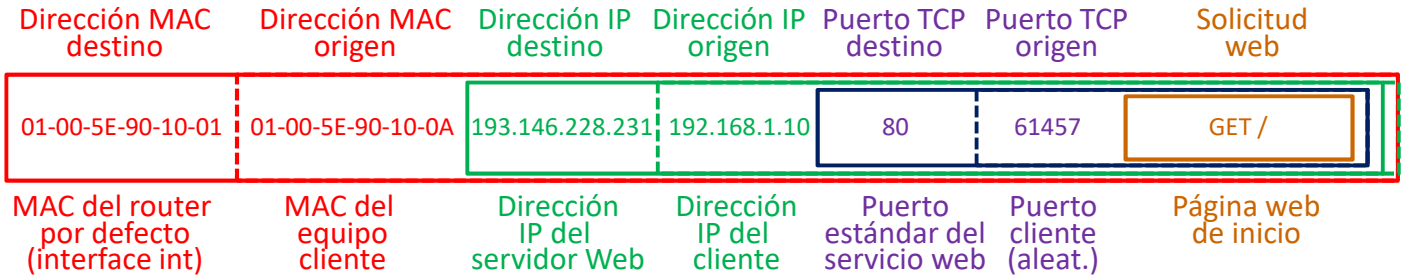


En los esquemas se han usado iconos de la librería *Cisco Network Topology Icons*

01-00-5E-90-10-00

Funcionamiento de la red



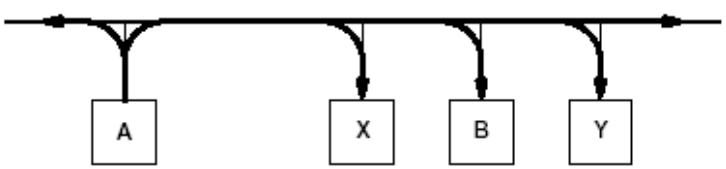


Nota: la función del *switch* es reenviar las tramas entre los equipos conectados

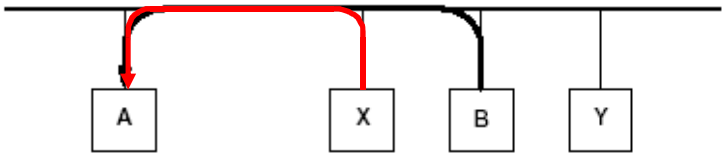
ARP. Conversión entre direcciones MAC e IP

- La dirección MAC (48 bits) es una dirección física única, asignada por el fabricante de la tarjeta de red. La dirección IP (32 o 128 bits) es una dirección lógica, asignada por el administrador de la red.
- Para poder enviar un mensaje (datagrama) a otra dirección IP es necesario obtener la dirección MAC del siguiente salto. Se realiza mediante el protocolo ARP (*Address Resolution Protocol*).
- Ejemplo: A quiere conocer la dirección MAC de B

1. A envía un **ARP Request** Con la IP de B



2. B reconoce su IP y envía a A ***ARP Response*** Con su MAC



ARP Spoofing

Un host X envía muchos *ARP Responses* al host A diciendo que la IP de B corresponde a la MAC de X (la suya): el tráfico dirigido a B se enviará a X

Ejemplo

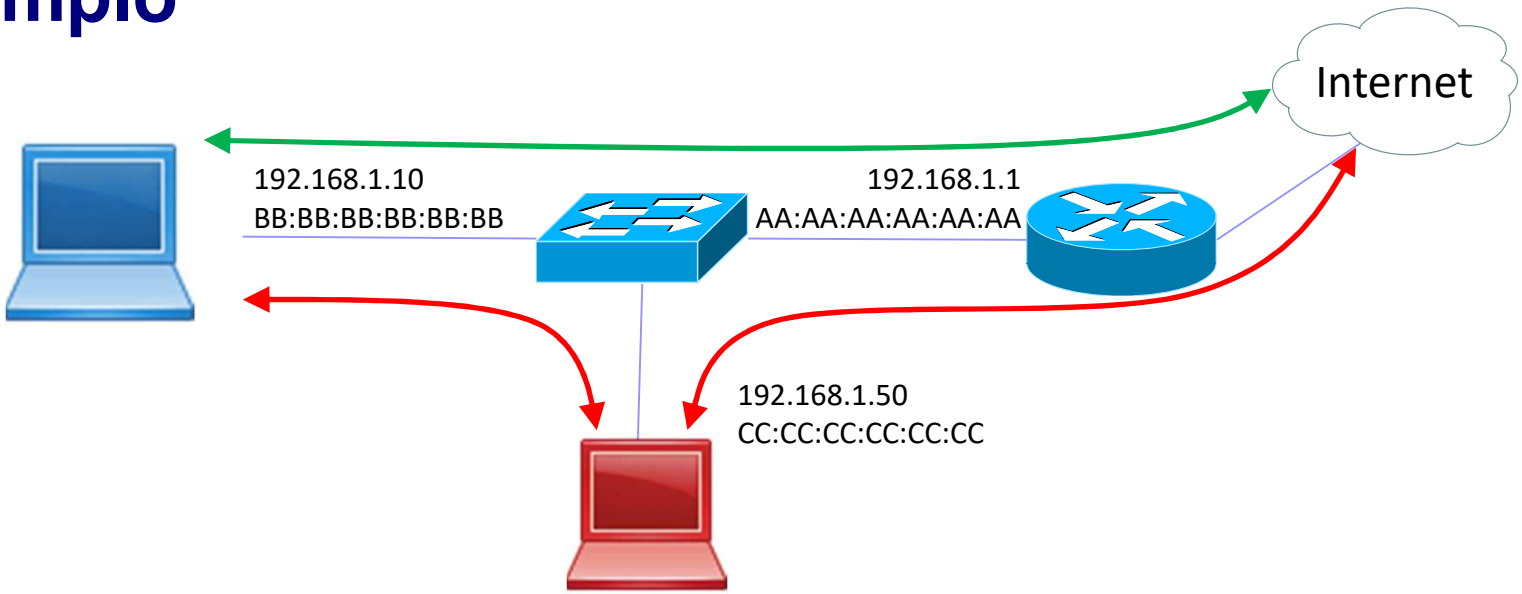


Tabla ARP del Atacante

Direcc. IP	Direcc. MAC
192.168.1.1	AA:AA:AA:AA:AA:AA
192.168.1.10	BB:BB:BB:BB:BB:BB

Tabla ARP del equipo ⟷ **Tabla ARP del router**

Direcc. IP	Direcc. MAC
192.168.1.1	AA:AA:AA:AA:AA:AA

Direcc. IP	Direcc. MAC
192.168.1.10	BB:BB:BB:BB:BB:BB

1. Funcionamiento normal

Tabla ARP del Atacante

Direcc. IP	Direcc. MAC
192.168.1.1	AA:AA:AA:AA:AA:AA
192.168.1.10	BB:BB:BB:BB:BB:BB

Tabla ARP del equipo **Tabla ARP del router**

Direcc. IP	Direcc. MAC
192.168.1.1	CC:CC:CC:CC:CC:CC

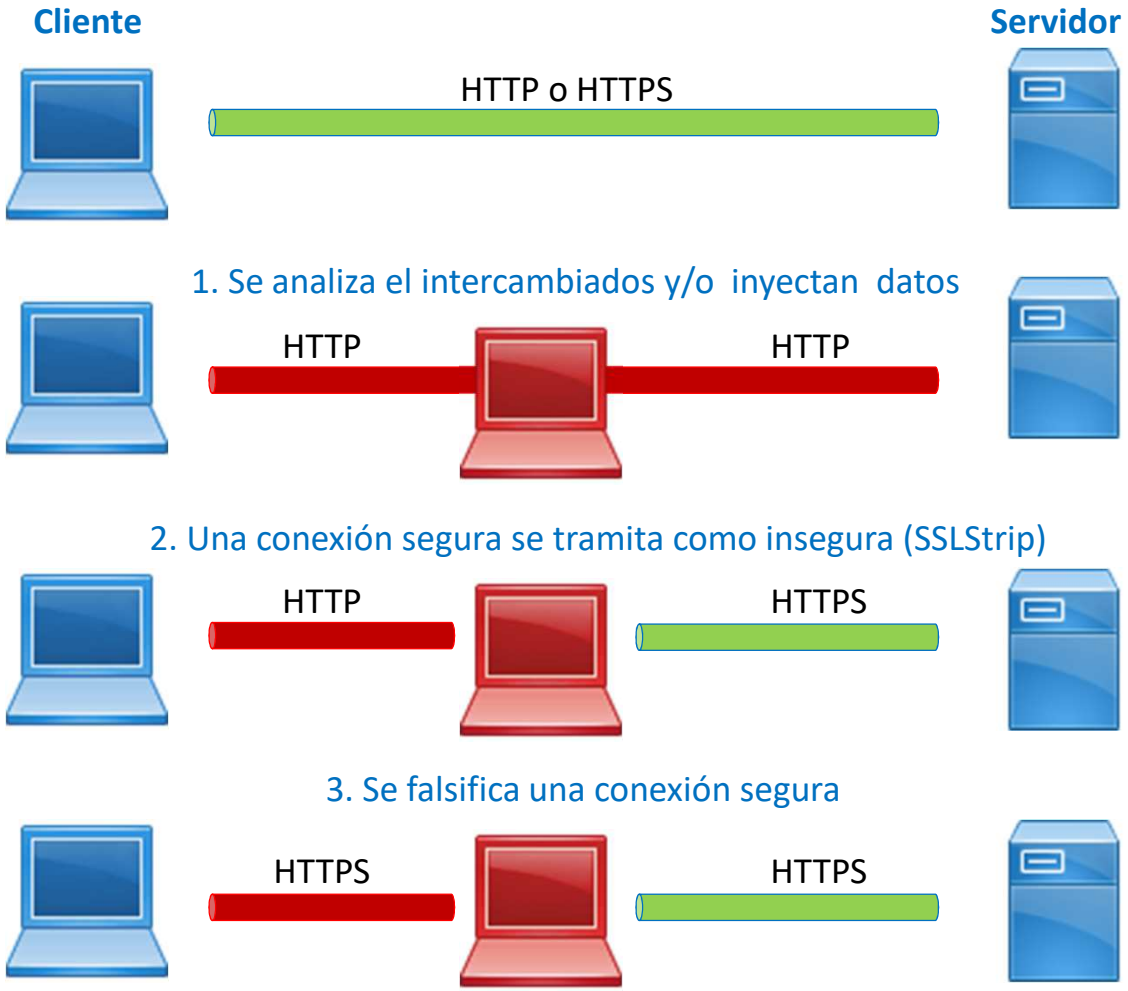
Direcc. IP	Direcc. MAC
192.168.1.10	CC:CC:CC:CC:CC:CC

2. Después del *ARP spoofing*

Secuencia de un ataque MitM

- Identificar a la pareja de víctimas a atacar (*targets*). También pueden seleccionarse múltiples targets.
- Iniciar un proceso de suplantación de identidad (*ARP spoofing, ICMP redirect, …*) en uno o ambos sentidos de la comunicación.
- Analizar el tráfico capturado en busca de información sensible.
- Opcionalmente, es posible interrumpir la comunicación en un momento de la misma y suplantar a un interlocutor, redirigir el tráfico HTTPS a HTTP (*SSLStrip*), falsear una conexión HTTPS, inyectar código malicioso dentro de una secuencia intercambiada, etc.

Los peligros del MitM

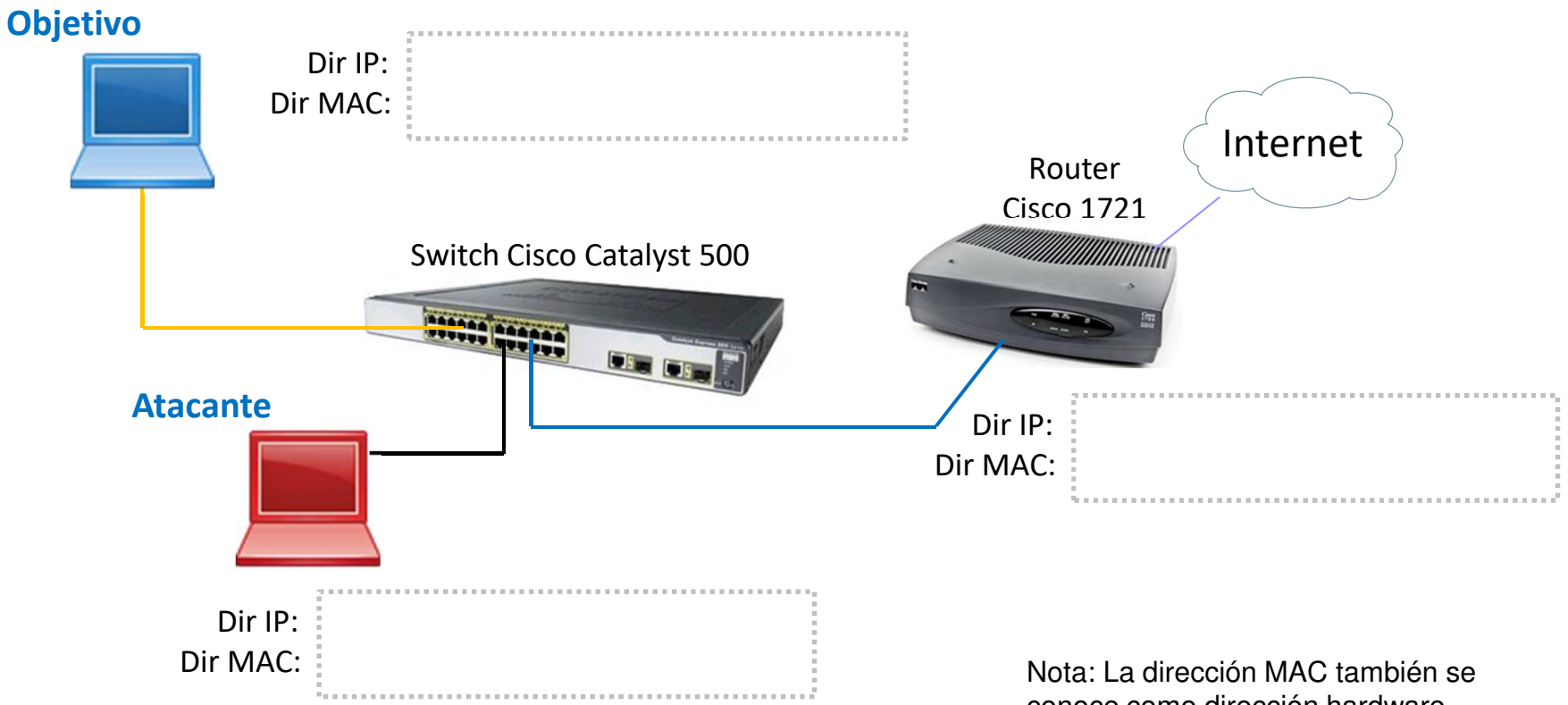


Bettercap

- **Bettercap**[1] es un conjunto de herramientas *open source* para interceptar y analizar tráfico en una red cableada o Wifi.
- Automatiza tareas como la detección de equipos en la LAN, el ataque MitM contra uno o varios objetivos, la captura de tráfico y recolección de información sensible (contraseñas, números de cuenta,…), el filtrado y la sustitución de tráfico, la sustitución de conexiones seguras (*SSLStrip*), etc.
- Usa distintas técnicas para conseguir la suplantación o desvío del tráfico:
  - *ARP spoofing*
  - *ICMP redirect*
  - *DNS spoofing*

[1] https://www.bettercap.org/

Bettercap. Escenario de pruebas



Nota: La dirección MAC también se conoce como dirección hardware
Es una secuencia de 12 dígitos hexadecimales (0..9 y a..f)

Tareas a realizar (I)

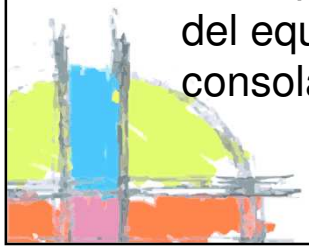
1. Abrir sesiones en los equipos (atacante, objetivo y *router*). En el laboratorio tenemos los siguientes usuarios y contraseñas:

	Windows	Linux		Cisco IOS
usuario	alumno	**alumno**	root	cisco
password	[sin pw]	**ceu**	root	cisco

2. Identificar las direcciones IP y MAC de los tres equipos y anotarlas sobre el esquema anterior. Comandos necesarios:

Windows	Linux	Cisco IOS
ipconfig	ifconfig eth0	show interface fa0
arp -a	arp -n	show arp

Nota: para acceder al *router* puede usar el comando `sudo minicom` en una ventana del equipo Objetivo (este equipo está conectado al *router* a través de un cable de consola de color azul). Para finalizar la sesión de consola: Ctrl + A, q



Tareas a realizar (II)

3. Abrir un terminal como *root* en la máquina atacante (`sudo su –`). A continuación, lanzar una primera ejecución de bettercap. No se realizará ARP *spoofing* (MitM) ni visualización (*sniffing*), sólo se identificarán los equipos presentes:

```
bettercap --no-spoofing
```

4. Ver las máquinas detectadas y también los indicadores de las funciones activadas en el programa (aparecen en verde y rojo en la parte superior). Finalizar la ejecución pulsando la combinación ***Ctrl+C***.

5. Lanzar un ataque MitM con *ARP spoofing* sobre toda la red y en ambos sentidos:

```
bettercap -X --full-duplex
```

Para comprobar que se está interceptando el tráfico abra un navegador en el equipo Objetivo y navegue por Internet.

Tareas a realizar (III)

6. Comprobar el efecto del ataque sobre las tablas ARP del objetivo y del *router*. En ambas tablas debería aparece la dirección MAC del atacante asociada a la dirección IP del otro extremo.

7. También puede verse cómo el atacante realiza el envenenamiento enviando continuamente respuestas ARP. Abrir un nuevo terminal en el equipo atacante nuevamente como *root* y ejecutar el siguiente comando:

```
tcpdump -i eth0 arp
```

8. Lanzar un nuevo ataque MitM pero más específico, dirigido sólo al Objetivo (opción –T seguida de la dirección IP del Objetivo). Al no indicar el modo full-dúplex sólo se intercepta un sentido de la comunicación, desde el Objetivo al *router*.

```
bettercap -X -T <IP del objetivo>
```

Tareas a realizar (IV)

9. Verificar que bettercap obtiene las credenciales de usuario intercambiadas a través de las conexiones en abierto. Puede probar los siguientes enlaces desde el equipo Objetivo:

   http:// (taller / Segurid4D)

   http:// (taller@ / Segurid4D)

10. Alteración de los datos intercambiados en una conexión en abierto. Ejecutar bettercap con los siguientes parámetros:

```
bettercap --proxy --proxy-module flip-image --no-sslstrip
```

   Probar a visualizar una página web desde el objetivo ¿qué ocurre?

   Nota: también puede usar el módulo HackGif ¿qué función realiza?

Tareas a realizar (y V)

11. Análisis de tráfico HTTPS por ataque *SSLStrip*: La conexión que debería ser segura (por HTTPS) se tramita como insegura (por HTTP). Todo el intercambio será visible para el atacante.

```
bettercap --proxy -P POST
```

Conecte a algún dominio seguro y vea el resultado.

12. Análisis de tráfico HTTPS por falsificado de conexión (*proxy https*). Nota: En el navegador del objetivo saltará una alerta al no reconocer el certificado digital que envía el atacante.

```
bettercap --proxy-https
```

Conecte a algún dominio seguro y vea el resultado.

Cómo protegernos frente al MitM

- En el *switch*
  - Dynamic ARP Inspection (DAI). El switch verifica la autenticidad de todos los mensajes ARP entregados, bloqueando los inválidos.
  - DHCP Snooping. El *switch* analiza los mensajes DHCP y aprende la MAC de cada usuario, para evitar que se entreguen tramas hacia puertos no asociados a las MAC. También evita la suplantación de los mensajes DHCP.
- **En el servidor**
  - Empleo de **HSTS** (*HTTP Strict Transport Security*) para informar al cliente de que requiere conexión cifrada. Ya hay muchos navegadores que tienen sitios HTTPS precargados.
- **En el host**
  - Uso de conexiones cifradas. No aceptar certificados digitales no reconocidos por nuestro sistema.
- En la red
  - Usar sistemas de detección de intrusiones (IDS/IPS), que analizan el tráfico intercambiado en la red y detectan patrones de ataque.

Índice

Consejos para fortalecer nuestro host

- Objetivo: mantener la seguridad y dificultar el trabajo al atacante.
  - Aplicar parches de seguridad en el sistema y las aplicaciones (y reiniciar…).
  - Instalar una suite de seguridad (cortafuegos, antivirus, …).
  - Cambiar las contraseñas por defecto.
  - Usar contraseñas robustas.
  - Instalar software sólo de fuentes fiables.
  - Usar siempre conexiones seguras. Desconfiar si no se reconoce el certificado del servidor o si el navegador indica que no es fiable
  - No abrir correo sospechoso. No pinchar sobre sus adjuntos.
  - Mantener copias de seguridad en almacenamiento *off-line* y/o con versionado.
  - Activar el bloqueo automático del sistema.
  - Tener presente los ataques de ingeniería social.

Seguridad en entornos wifi

- Cambiar la contraseña por defecto de acceso al *Access Point (AP)*. Debe ser robusta frente a ataques. Limitar el acceso de administración al AP (ej: sólo por SSH o HTTPS, y desde el interface cableado).
- Usar WPA2, con 802.11x/EAP (*Enterprise*) si es posible. En modo personal, configurar una PSK (*Pre Shared Key*) compleja para evitar ataques por fuerza bruta o diccionario, y cambiarla periódicamente.
- Aislar las estaciones *wireless* (si es posible).
- Deshabilitar WPS (*Wi-fi Protected Setup*). Tiene varias debilidades.
- Ubicar los AP en lugares seguros.
- Si se trabaja con usuarios estables, habilitar el filtrado de MAC. ¿Ocultar el SSID?
- No conectar a redes wifi en las que no se confía.

Índice

Bibliografía y referencias

- *Fundamentals of Information Systems Security*.
  David Kim and Michael G. Solomon
  Jones & Bartlett Learning, LLC. 2012

- Proyecto bettercap
  https://www.bettercap.org/
- Documentación bettercap
  https://www.bettercap.org/legacy/