

Report di Penetration Testing — *Jangow*

Analista: Gianluca

Target: CTF-jangow

Attaccante: Kali Linux

1) – Sommario Esecutivo

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) - Ambito e Metodologia

L'attività è stata limitata esclusivamente alla macchina virtuale *jangow* fornita da VulnHub, all'interno della rete Host-Only 192.168.56.0/24.

Sono state autorizzate tutte le operazioni di enumerazione, scanning, fuzzing, exploitation e privilege escalation necessarie al raggiungimento dei privilegi di root.

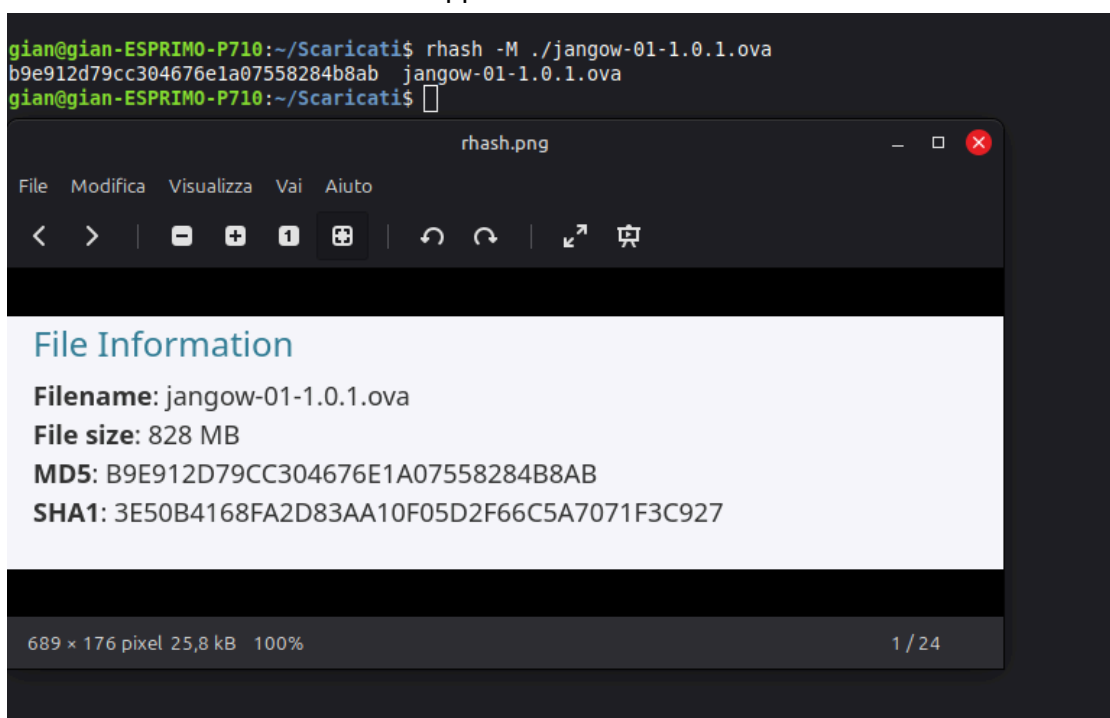
Non sono stati eseguiti attacchi verso altri host o servizi esterni alla VM.

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. Riconoscizione 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 resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.01% done
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.52% 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 86.94% done; ETC: 08:45 (0:00:14 remaining)
Nmap scan report for 192.168.56.118
Host is up (0.000025s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
MAC Address: 08:00:27:36:57:B6 (PCS Systemtechnik/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 3.13 - 4.4 (97%), 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 4.4) (91%), 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 -sC --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 50.00% 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 (0.000585s 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: 08:00:27:36:57:B6 (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

File Macchina Visualizza Inserimento Dispositivi Auto

Session Actions Edit View Help

kali@kali: ~

kali@kali: ~

kali@kali: ~

kali@kali: ~

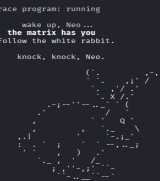
kali@kali: ~

kali@kali: ~

Exploit Title

vsftpd 3.0.3 - Remote Denial of Service

Shellcodes: No Results

---(kali@kali)~\$-
\$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and select the intended module, e.g., use kerberos/get_ticket or use kerberos_forge_silver_ticket
call trans op: received. 2-19-08 13:24:18 REC:Loc
Trace program: running
wake up, Neo ...
the matrix has you
follow the white rabbit.
knock, knock, Neo.

https://metasploit.com

---(kali@kali)~\$-
\$ searchsploit apache 2.4.18

Exploit Title	Path
Apache - PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	/php/remote/29200.c
Apache - PHP < 5.3.12 / < 5.4.2 - Remote Code Execution - Scripts	/php/remote/29126.py
Apache 2.4.17 < 2.4.18 - 'mod_ssl' (openssl) 'openssl' Local Privilege Escalation	/linux/local/04639.php
Apache < 2.2.34 / < 2.4.27 - OPENDNS Memory Leak	/linux/webapps/42175.py
Apache CXC < 2.5.0/2.5.1/2.2.4 - Denial of Service	/multiple/remote/29178.txt
Apache mod_ssl < 2.6.7 OpenSSL - 'openssl' Remote Buffer Overflow	/unix/remote/21071.c
Apache mod_ssl < 2.6.7 OpenSSL - 'openssl' Remote Buffer Overflow (1)	/unix/remote/794.c
Apache mod_ssl < 2.6.7 OpenSSL - 'openssl' Remote Buffer Overflow (2)	/unix/remote/4700.c
Apache OpnWebinars 1.0.x < 3.1.0 - 'ZIP' File Directory Traversal	/linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing	/multiple/remote/2901.txt
Apache Tomcat < 6.0.18 - 'JSP' Directory Traversal	/unix/remote/7448.c
Apache Tomcat < 6.0.18 - 'JSP' File Directory Traversal (PnC)	/multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (beta) / < 8.5.22 / < 8.0.40 / < 7.0.8 - 'ZIP' Upload Bypass / Remote Code Execution (1)	/multiple/webapps/42933.txt
Apache Tomcat < 9.0.1 (beta) / < 8.5.22 / < 8.0.40 / < 7.0.8 - 'ZIP' Upload Bypass / Remote Code Execution (2)	/multiple/webapps/42934.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PnC)	/linux/docs/36980.txt
Webroot Shoutbox < 2.12 (remote) - Local File Inclusion / Remote Code Execution	/linux/remote/34.pl

Shellcodes: No Results

---(kali@kali)~\$-
\$ searchsploit httpd 2.4.18

Exploit Title	Path
OpenBSD HTTPD < 6.0 - Memory Exhaustion Denial of Service	/openbsd/docs/41278.txt

Shellcodes: No Results

```

]=[ metasploit v6.4.95-dev ]
+ -- --=[ 2,566 exploits - 1,315 auxiliary - 1,683 payloads ]
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion ]

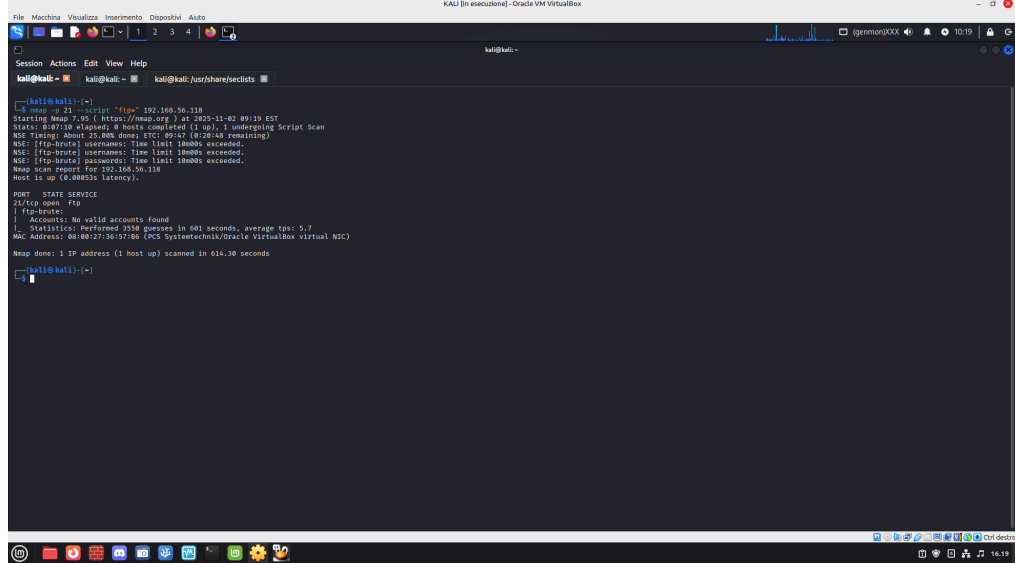
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search apache 2.4.18
[-] No results from search
msf > search httpd 2.4.18
[-] No results from search
msf >

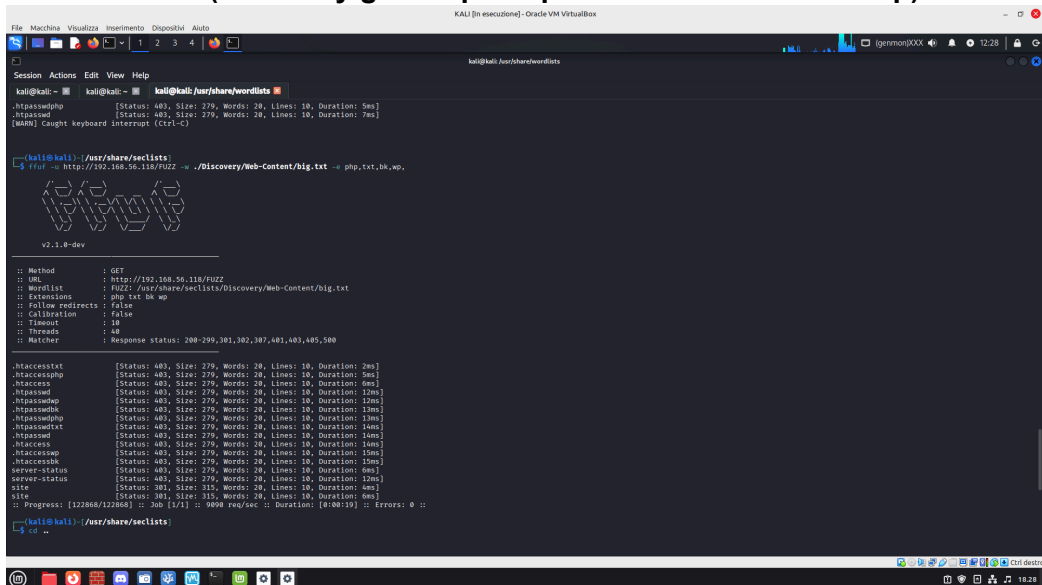
```

❖ 3. Enumerazione web e discovery della vulnerabilità

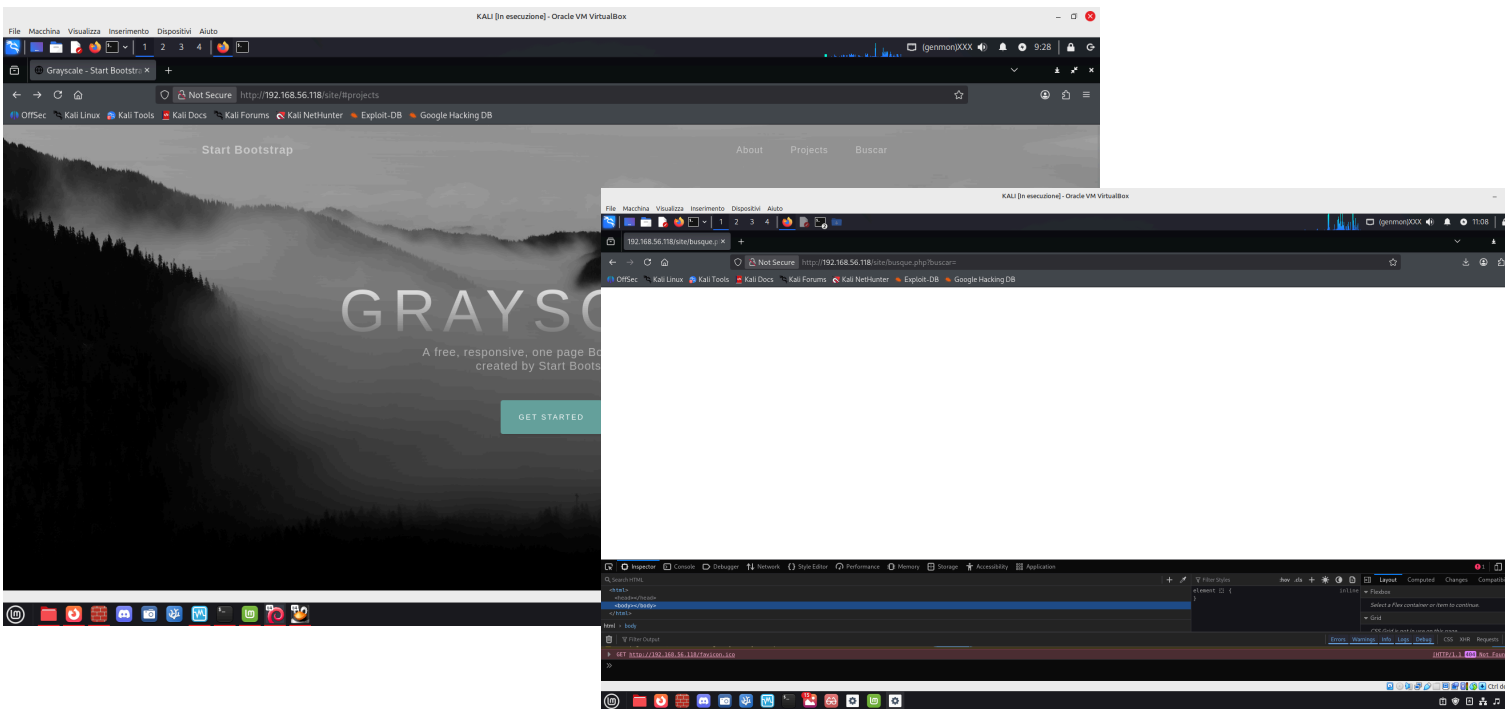
➤ **3.1. Enumerazione ftp:** ho usato un comando **di nmap** che prova tutte le sue **sonde** per enumerare il servizio alla ricerca di dati, il risultato di nmap è stato di **nessun account** molto strano ma ho conseguito nel penetration testing in quel momento etichettando forse FTP come inutilizzabile.



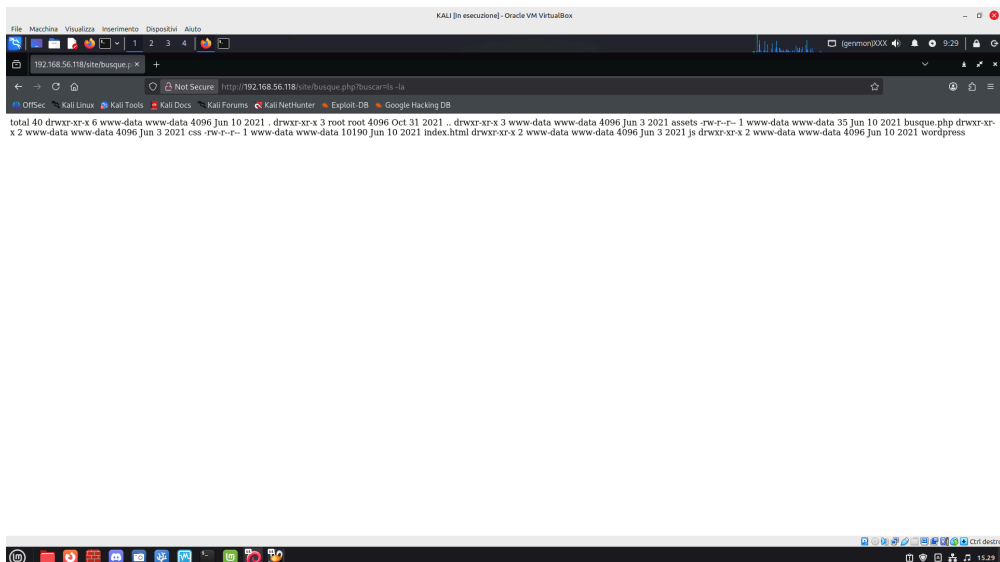
➤ **3.2. Fuzzing / Directory discovery:** ho eseguito **scan** e **fuzzing** dell'HTTP (Nikto, ffuf con seclist) e ho trovato una directory accessibile chiamata **"site"**. (directory già scoperta prima dalle sonde di nmap)



- **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”** 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: **busque.php, js,wordpress, file.php**

❖ 4. Sfruttamento iniziale — accesso FTP

- 4.1. Uso delle credenziali trovate: dal file file.PHP sensibile dentro il file il creatore ha lasciato apposta in forma di commento delle credenziali sensibili.
 - 4.2. 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)
 - 4.3. Esplorazione FTP: nella home FTP è presente **user.txt** (file contenente hash). Ho scaricato **user.txt** su Kali per analisi offline.
-

❖ 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**.
- 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.
- 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 la password trovata nel file **.php**.
- 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 tra di loro ma non sono riuscito ad elevare i privilegi neanche con la frase **decodificata** e le 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
-

❖ 6. Pivoting via FTP

- **6.1. Upload / trasferimento tool:** sfruttando **FTP** come “**trampolino**”, ho caricato [linpeas.sh](#) nella cartella **/tmp** per eseguire enumeration locale.
 - **6.2. Esecuzione LinPEAS:** ho lanciato **linpeas** e salvato l'output su file redirectato ([linpeas_out.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**)
 - **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** l'**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 dopo eseguito. dopo qualche istante mi ha dato la **shell di root**
 - **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**
-

4) – Impatto e gravità

- **Accesso utente (jangow01)** — *ALTO* per la macchina target (consente movimento laterale e raccolta info).
 - **Privilege escalation possibile tramite cron write** — *CRITICO* se confermata: permette esecuzione arbitraria come root su schedule.
 - **Kernel exploit** (se sfruttabile) — *CRITICO/ALTISSIMO*, ma non confermato in ambiente stabile.
-

5) – 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 azienda più di quel che si pensa. se fosse stato un report aziendale avrei consigliato di sanitizzare input, non esporre porte che non servono, cambiare username e password per accesso alla pagina di login di jangow e per FTP, cambiare i permessi della directory perché linpeas oltre a trovare quelle vulnerabilità ha trovato vulnerabilità riguardo alla cartella etc,cron job e molte altre, aggiornare il kernel e la versione di ubuntu SEMPRE fondamentale, e implementare un firewall anche uno basico come stateful con accept or drop, e fare un backup periodico con la rimozione dell'OS per pulizia del disco e installazione dell'OS per una maggiore sicurezza.