Penetration Test Report

Blackbox Jangow01 – CTF FACILE

INTRODUZIONE

Questo report documenta le attività svolte durante un penetration test su un target designato come 'blackbox'. L'obiettivo è quello di identificare vulnerabilità sfruttabili per ottenere l'accesso iniziale e successivamente eseguire una privilege escalation fino a ottenere i privilegi di root sul sistema.

1. Fase di Ricognizione

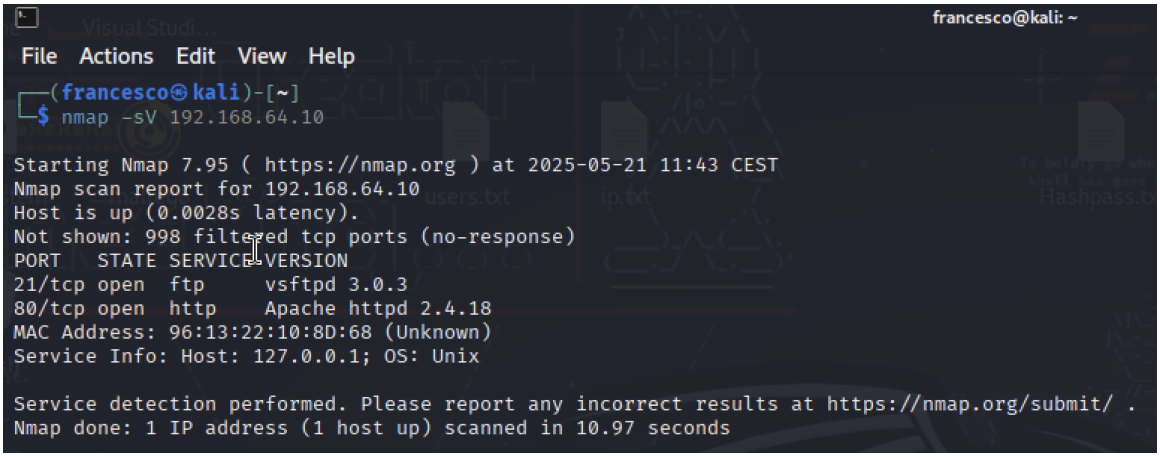
La prima attività svolta è stata una scansione delle porte del sistema target utilizzando Nmap:

Comando eseguito:

nmap -sV 192.168.64.10

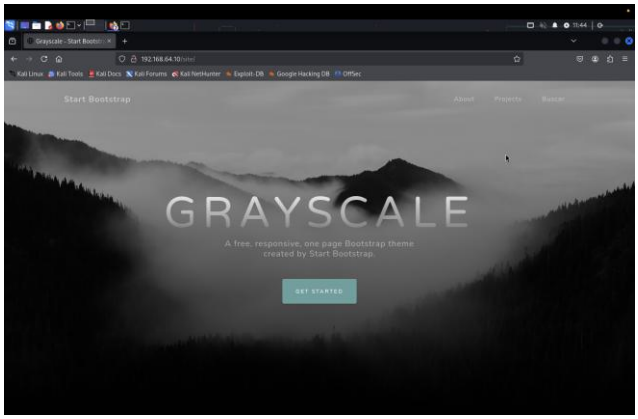
Risultati: - Porta 21: FTP aperto
- Porta 80: HTTP aperto

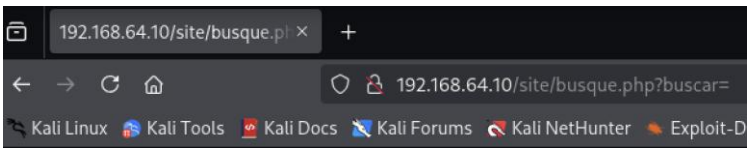
L'attenzione si è quindi concentrata sul servizio HTTP per investigare ulteriormente eventuali punti d'ingresso.



2. Analisi del Servizio Web

Navigando al sito web presente sulla porta 80, è stata individuata una funzionalità sospetta denominata 'buscar'. Tramite analisi delle richieste HTTP è stato osservato che il tasto invia parametri tramite il metodo GET. Questo ha indicato una potenziale superficie d'attacco per iniezioni.



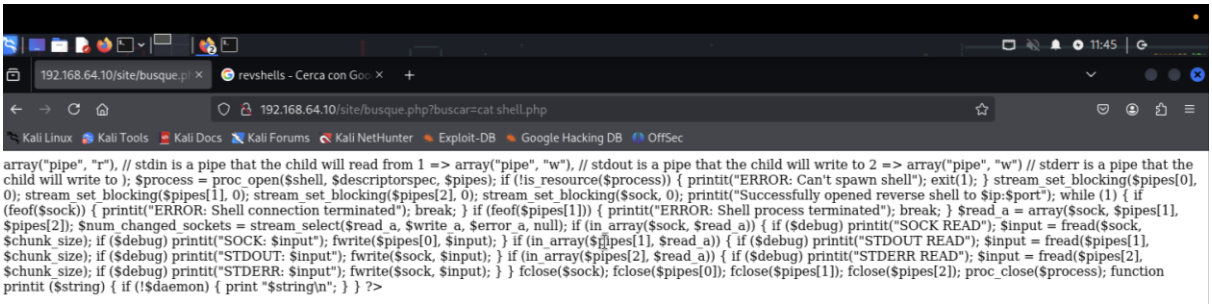


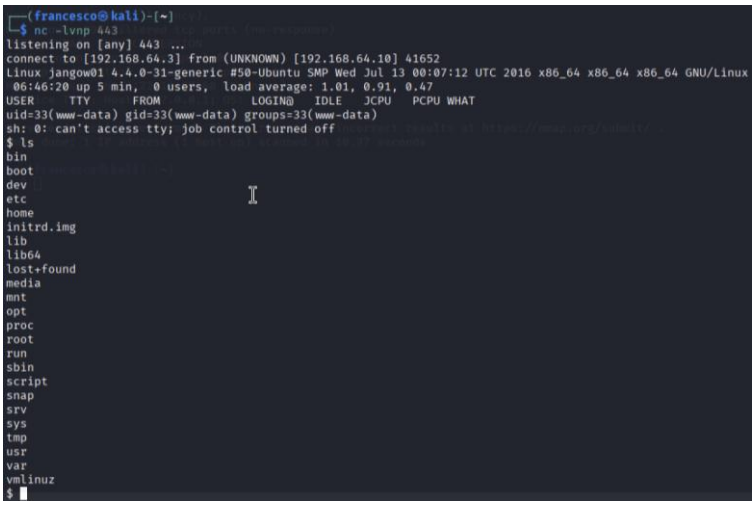
3. Accesso Iniziale – Reverse Shell

A seguito di test, è stata iniettata una reverse shell scritta in PHP attraverso il parametro GET vulnerabile. La shell utilizzata è stata la *php pentest monkey* fornita dal sito Revshell.com.
Dal terminale di Kali è stata poi eseguita la connessione alla shell tramite comando netcat:

```
nc -lvnp 443
```

L'attacco ha avuto successo, consentendo l'ottenimento di una shell interattiva sul sistema remoto con i privilegi dell'utente web.



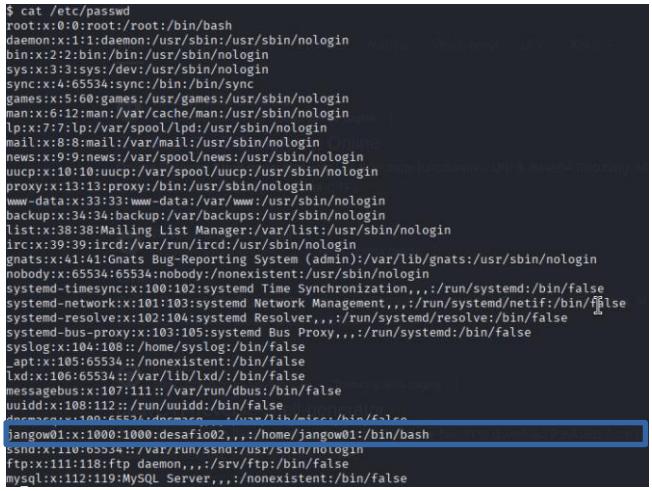


4. Enumerazione e Accesso FTP

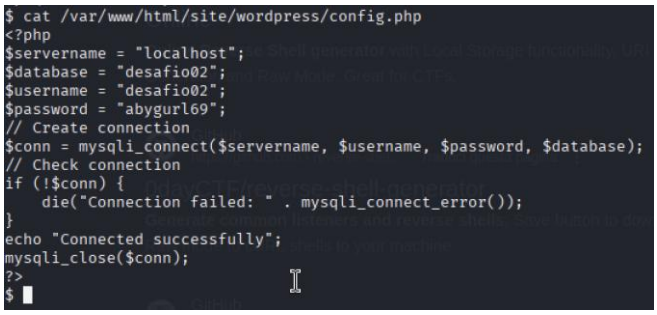
Esplorando il sistema, è stato individuato l'utente `jangow01` e, all'interno di una directory Wordpress, il file `wp-config.php`. Utilizzando il comando `cat`, è stata estratta la password MySQL che corrispondeva anche alla password dell'utente di sistema.

A questo punto è stato possibile autenticarsi con successo tramite FTP e caricare file direttamente sul server.

UTENTE

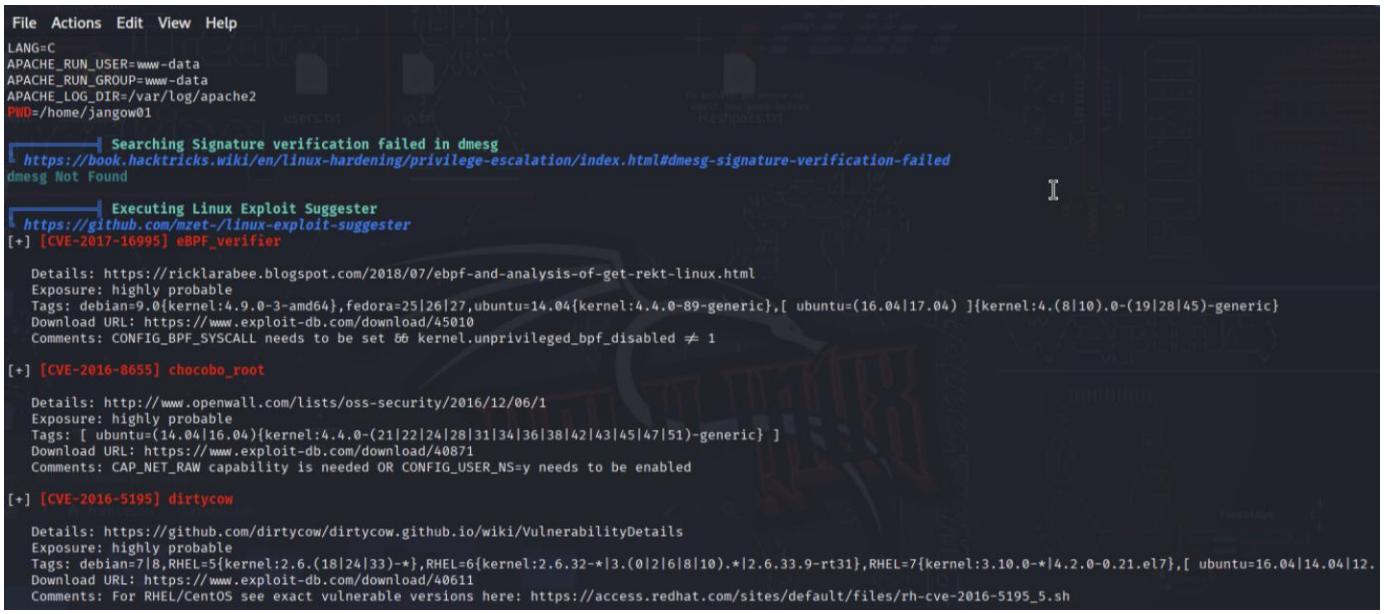


PASSWORD



5. Caricamento di linPEAS e Scansione

Utilizzando la sessione FTP, è stato caricato lo script di enumerazione `linpeas.sh`. Dopo averlo trasferito sul sistema target, lo script è stato eseguito per identificare possibili vulnerabilità locali. Il report generato ha evidenziato varie vulnerabilità note, tra cui una potenzialmente sfruttabile per ottenere l'accesso root.



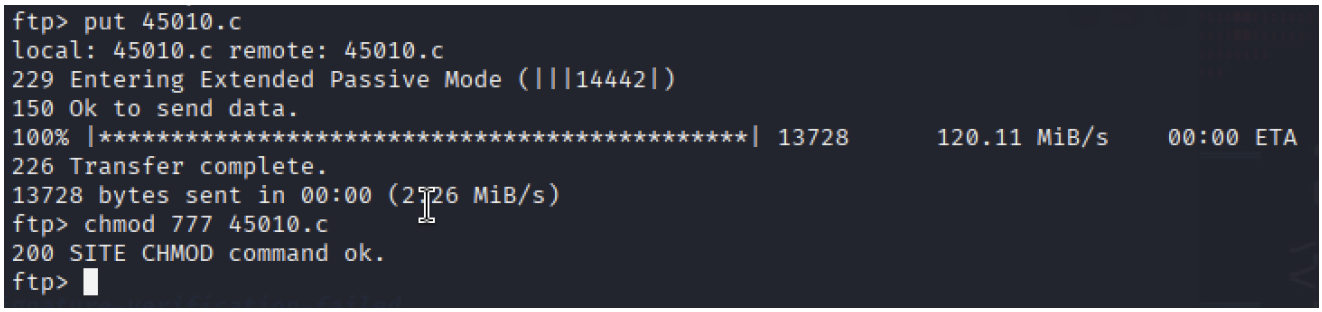
6. Privilege Escalation tramite Exploit C

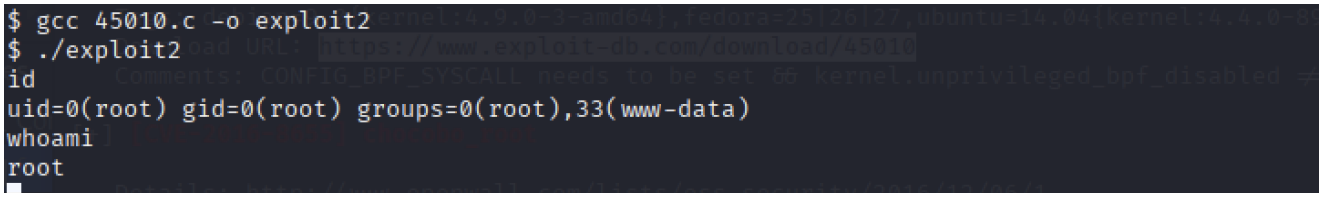
È stato scaricato dal sito Exploit-DB il codice sorgente C di un exploit corrispondente a una delle vulnerabilità individuate (CVE-2017-16995 eBPF_verifier). Il file è stato trasferito sul sistema target utilizzando FTP e posizionato nella directory `/tmp`, l'unica con permessi di scrittura ed esecuzione.

Per assicurare l'esecuzione, sono stati modificati i permessi con:
`chmod 777 /tmp`

Successivamente, l'exploit è stato compilato con:
`gcc exploit.c -o exploit -lpthread`

Infine, l'exploit è stato eseguito e ha restituito una shell con privilegi root.





CONCLUSIONI

Il test ha dimostrato che, partendo da una semplice vulnerabilità GET in un'applicazione web, è stato possibile ottenere una shell remota, accedere via FTP, caricare strumenti di enumerazione, identificare vulnerabilità kernel e infine eseguire un exploit locale per ottenere privilegi root.

Questo dimostra una catena di compromissione realistica che evidenzia la criticità di configurazioni errate, mancati aggiornamenti e la presenza di file sensibili accessibili all'utente web.