S7 – L1
HACKING CON METASPLOIT

Introduzione: Il presente esercizio ha lo scopo di applicare in modo pratico le tecniche di penetration testing ttraverso 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.

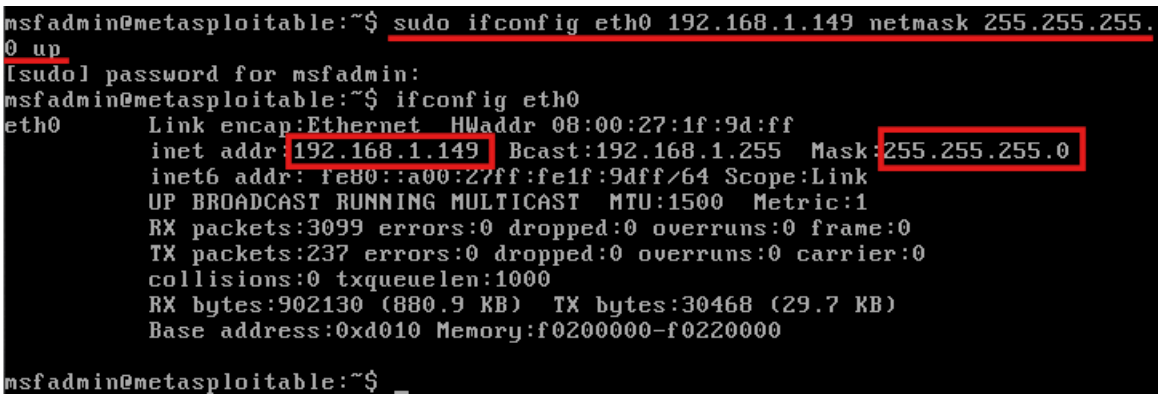
L'attività si concentra sulle fasi fondamentali di un attacco offensivo: configurazione dell'ambiente, verifica della connettività, individuazione di un servizio vulnerabile e sfruttamento dell'exploit tramite Metasploit.
L'esercizio evidenzia come **servizi non aggiornati o mal configurati possano condurre 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**



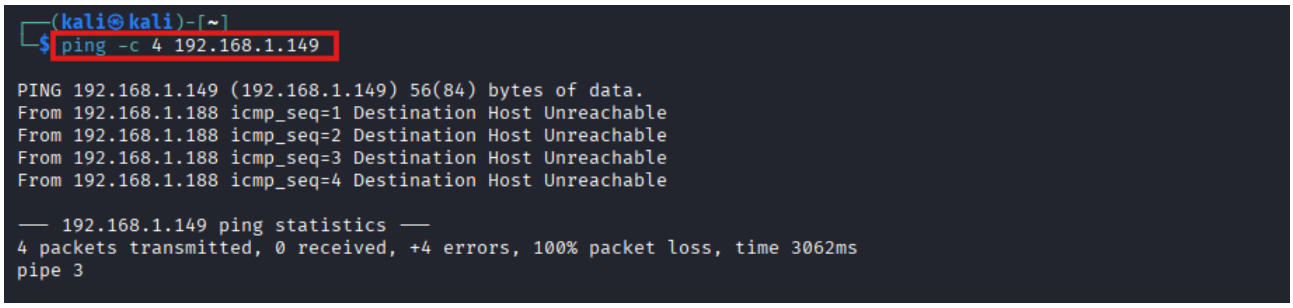
- **Impostazioni di rete/output che dimostra l'IP di Metasploitable**

---

2) Verifica connettività da Kali verso Metasploitable

Su Kali:

```
ping -c 4 192.168.1.149
```



- 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:

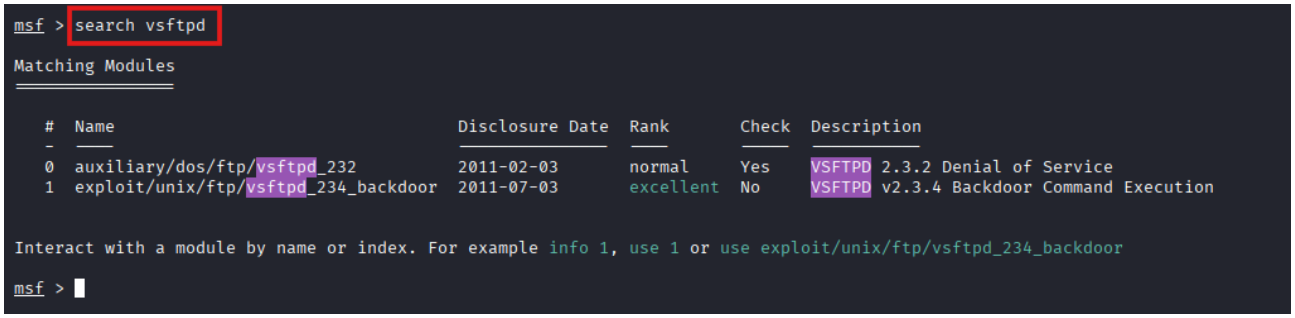
```
msfconsole
```

- Console avviata (banner + prompt).

5) Cercare l’exploit per vsftpd

Dentro **`msfconsole`**:

Comando: `search vsftpd`



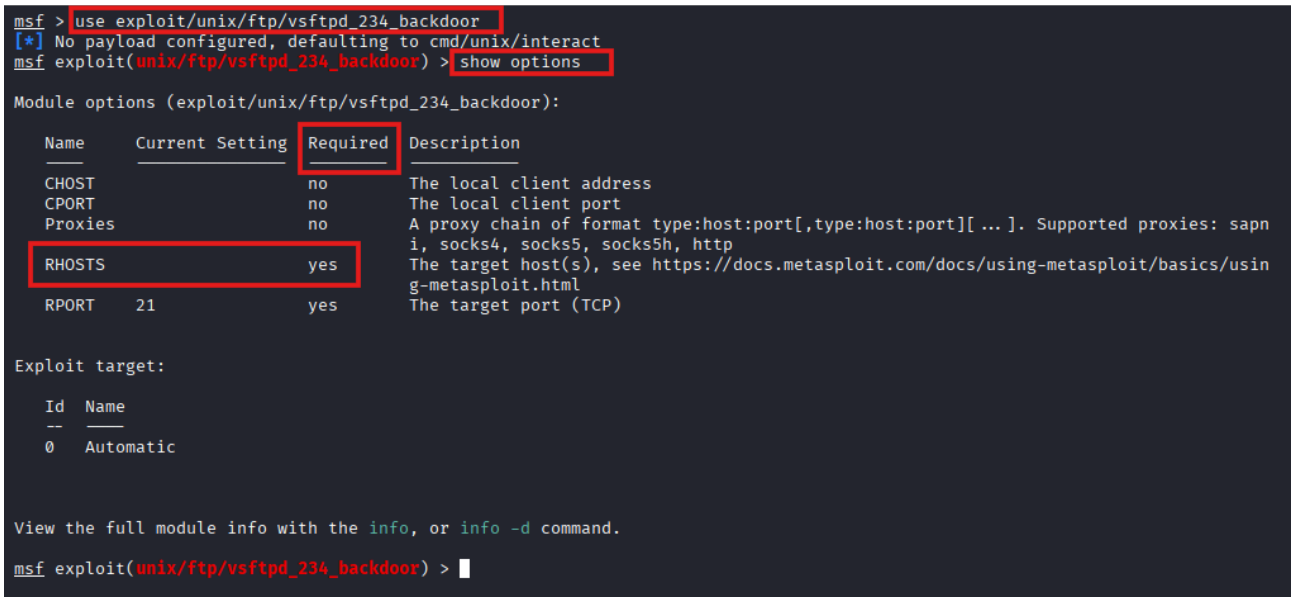
- Modulo exploit relativo a **vsftpd backdoor**
- Risultato della ricerca con la riga del modulo.

6) Selezionare l’exploit

`use exploit/unix/ftp/vsftpd_234_backdoor`

`Poi:`

`show options`

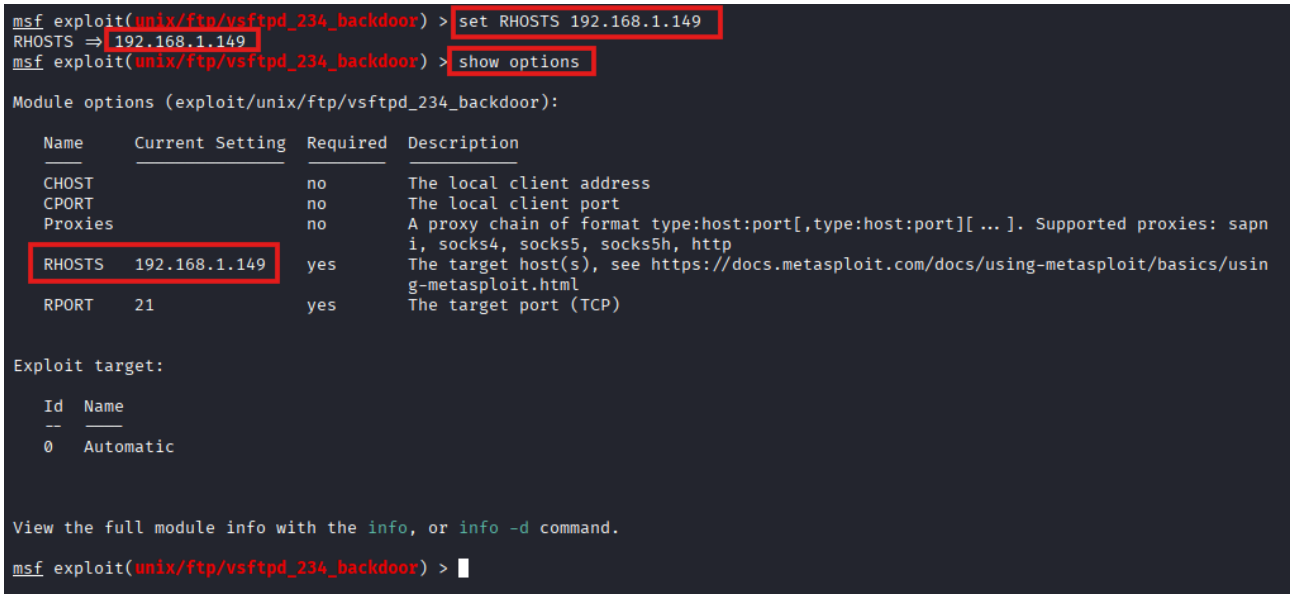


- `show options` dove si vede che **RHOSTS** è required.

7) Configura il target (RHOSTS) e verifica opzioni

`set RHOSTS 192.168.1.149`

`show options`



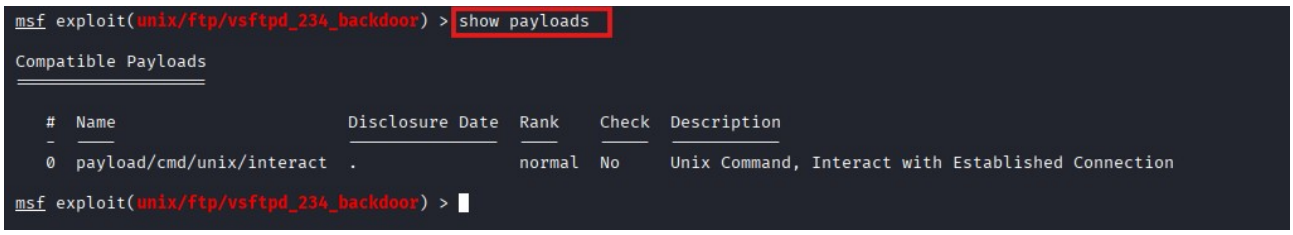
- RHOSTS valorizzato correttamente.
- `show options` con RHOSTS impostato.

---

8) Verificare payload disponibili

Spesso è già predefinito/compatibile:

`show payloads`



- 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…”).

- 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.

---

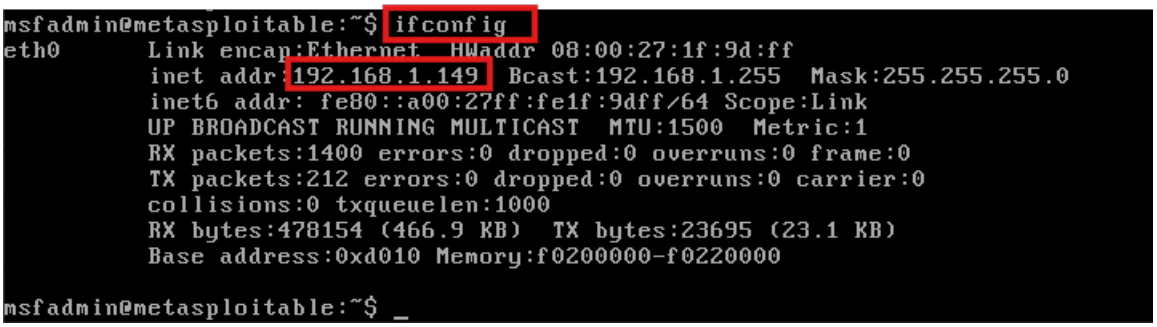
10) Verificare di essere davvero su Metasploitable (check IP)

Eseguire:

`ifconfig`

Cosa si vede:

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

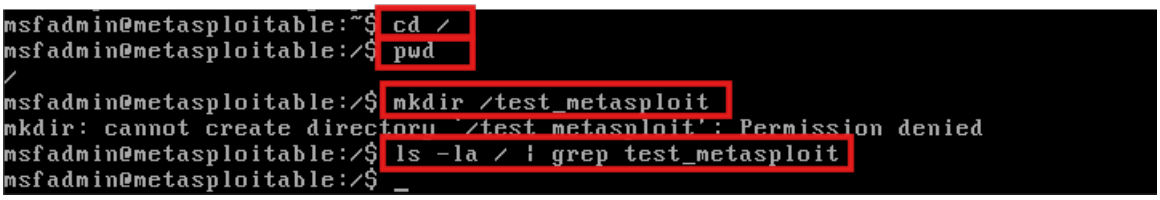


- Output `ifconfig` dove si vede l’IP.

11) Su Metaspotable 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
```



- `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.