

avvio msfconsole e utilizzo il comando use per attivare lo scanner telnet.

inserisco l'indirizzo ip della macchina bersaglio e avvio l'exploit, che ha successo e rileva la porta telnet (23)

```
kali@kali: ~  
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%$a,]%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]  
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%$$'za,]%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]  
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%?a,]%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]  
[%-----.,a$a]-----%]  
[%|_||_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|]|  
[%|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|]|  
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%..a,$$]%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]  
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%a,a,$$]%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]  
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%a,$$]%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]  
[%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%$]%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]  
  
=[ metasploit v6.3.27-dev ]  
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit tip: Writing a custom module? After editing your  
module, why not try the reload command  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use auxiliary/scanner/telnet/telnet_version  
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://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 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) > exploit  
  
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

**Provo a stabilire una  
connessione tramite il  
comando telnet, essa  
funziona correttamente e ho  
accesso alla macchina**

```
kali@kali: ~
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) > exploit

[+] 192.168.1.40:23          - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^['.

      _ _ _ _ _
     / / / / /
    / / / / /
   / / / / /
  / / / / /
 / / / / /
/ / / / /

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 Jan 16 04:07:20 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:~$
```