

W16D2

una volta lanciato

msfconsole

```
msf6 > search auxiliary telnet

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/server/capture/telnet          .               normal No    Authentication Capture: Telnet
1  auxiliary/scanner/telnet/brocade_enable_login .             normal No    Brocade Enable Login Check Scanner
2  auxiliary/dos/cisco/ios_telnet_rocm      2017-03-17      normal No    Cisco IOS Telnet Denial of Service
3  auxiliary/admin/http/dlink_dir_300_600_exec_noauth 2013-02-04      normal No    D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
4  auxiliary/scanner/ssh/juniper_backdoor   2015-12-20      normal No    Juniper SSH Backdoor Scanner
5  auxiliary/scanner/telnet/lantronix_telnet_password .             normal No    Lantronix Telnet Password Recovery
6  auxiliary/scanner/telnet/lantronix_telnet_version .             normal No    Lantronix Telnet Service Banner Detection
7  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof 2010-12-21      normal No    Microsoft IIS FTP Server Encoded Response Overflow Trigger
8  auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass 2021-09-06      normal Yes   Netgear PNPX_GetShareFolderList Authentication Bypass
9  auxiliary/admin/http/netgear_r6700v3_pass_reset 2020-06-15      normal Yes   Netgear R6700v3 Unauthenticated LAN Admin Password Reset
10 auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce 2021-04-21      normal Yes   Netgear R7000 backup.cgi Heap Overflow RCE
11 auxiliary/scanner/telnet/telnet_ruggedcom .             normal No    RuggedCom Telnet Password Generator
12 auxiliary/scanner/telnet/satel_cmd_exec  2017-04-07      normal No    Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
13 auxiliary/scanner/telnet/telnet_login    .             normal No    Telnet Login Check Scanner
14 auxiliary/scanner/telnet/telnet_version  .             normal No    Telnet Service Banner Detection
15 auxiliary/scanner/telnet/telnet_encrypt_overflow .             normal No    Telnet Service Encryption Key ID Overflow Detection

Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
-  -  -  -  -
PASSWORD  no              yes       The password for the specified username
RHOSTS    no              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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.20
rhosts => 192.168.1.20
```

come richiesto andremo a utilizzare un auxiliary su telnet

In Metasploit Framework, i moduli auxiliary sono moduli non exploit che forniscono una varietà di funzionalità utili per il penetration testing e la valutazione delle vulnerabilità. A differenza dei moduli exploit, progettati per sfruttare vulnerabilità e ottenere accesso non autorizzato, i moduli ausiliari vengono utilizzati per una gamma di altri compiti come scansioni, fingerprinting, sniffing e brute-forcing delle password.

Punti chiave sui moduli ausiliari in Metasploit

Tipi di Moduli Ausiliari:

Scanner: Utilizzati per la scoperta di rete, scansione delle porte, rilevamento dei servizi e scansione delle vulnerabilità. Ad esempio, auxiliary/scanner/portscan/tcp esegue la scansione delle porte TCP.

Fuzzer: Aiutano a trovare vulnerabilità inviando dati inaspettati o malformati a un'applicazione target.

Dos: Moduli progettati per attacchi di Denial of Service.

Sniffer: Catturano il traffico di rete.

Spoofers: Moduli che falsificano vari protocolli di rete.

Server: Avviano vari servizi server per scopi di test, come HTTP, FTP, ecc.

Client: Moduli che agiscono come client per interagire con i servizi in modi specifici, come il client SMTP per inviare email.

Brute Force: Moduli che tentano di eseguire brute-force delle credenziali di autenticazione per vari servizi.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.20
rhosts => 192.168.1.20
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.20:23 - 192.168.1.20:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
n with msfadmin/msfadmin to get started
[*] 192.168.1.20:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```