

Oggi eseguiremo un attacco sulla porta del telnet di metasploitable

```
msf6 > search auxiliary telnet
Matching Modules
=====
#  Name
--  ---
0  auxiliary/server/capture/telnet
1  auxiliary/scanner/telnet/brocade_enable_login
2  auxiliary/dos/cisco/ios_telnet_rocem
3  auxiliary/admin/http/dlink_dir_300_600_exec_noauth
4  auxiliary/scanner/ssh/juniper_backdoor

Disclosure Date  Rank  Check  Description  Disc
-----
0  normal  No  Authentication Capture: Telnet
1  normal  No  Brocade Enable Login Check Scanner
2  normal  No  Cisco IOS Telnet Denial of Service 2017
3  normal  No  D-Link DIR-600 / DIR-300 Unauthenticated Remote C
ommand Execution 2013
4  normal  No  Juniper SSH Backdoor Scanner 2015
```

Cerchiamo il telnet

```
File Actions Edit View Help
8  auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass 2021
-09-06 normal Yes Netgear PNPX_GetShareFolderList Authentication By
pass
9  auxiliary/admin/http/netgear_r6700_pass_reset 2020
-06-15 normal Yes Netgear R6700v3 Unauthenticated LAN Admin Passwor
d 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/telnet_satel_cmd_exec 2017
-04-07 normal No Satel Iberia SenNet Data Logger and Electricity M
eters 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 Detecti
on

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

msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Usiamo quello che si addice al nostro attacco

stato in larga parte sostituito da protocolli più sicuri come SSH (Secure Shell) per le connessioni remote.