Esercizio M4-W4-D1 Daniele Atzori Exploit Telnet con Metasploit

Con le parole chiave auxiliary e telnet restringiamo la ricerca sui possibili auxiliary presenti che ci possano essere utili.

```
Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote

msf6 > search auxiliary telnet

Matching Modules

# Name
Check Description

0 auxiliary/server/capture/telnet
No Authentication Capture: Ednet
1 auxiliary/senumer/telnet/brocade enable_login normal
No Brocade Enable_login Check Scanner
2 auxiliary/dsni/http/dink dir, 300, 600_exec_noauth
No Cisco 105 Telnet Denial of Service
3 auxiliary/dsni/http/dink dir, 300, 600_exec_noauth
No D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
No Juniper SSH Backdoor Scanner
3 auxiliary/scanner/scheck/lantronix_telnet_password
No Juniper SSH Backdoor Scanner
5 auxiliary/scanner/telnet/lantronix_telnet_password
No Lantronix_Telnet_Service Banner Detection
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Server Encoded Response Overflow Trigger
No Microsoft IIS FTP Serv
```

In questo caso scegliamo "auxiliary/scanner/telnet/telnet_version". Con show options vediamo i requisiti necessari (segnati da yes) per far partire l'attacco, in questo caso l'unico da settare manualmente è l'IP della macchina target. Poi andiamo con "exploit" e come vediamo ci appaiono admin e password della VM Metasploitable.

