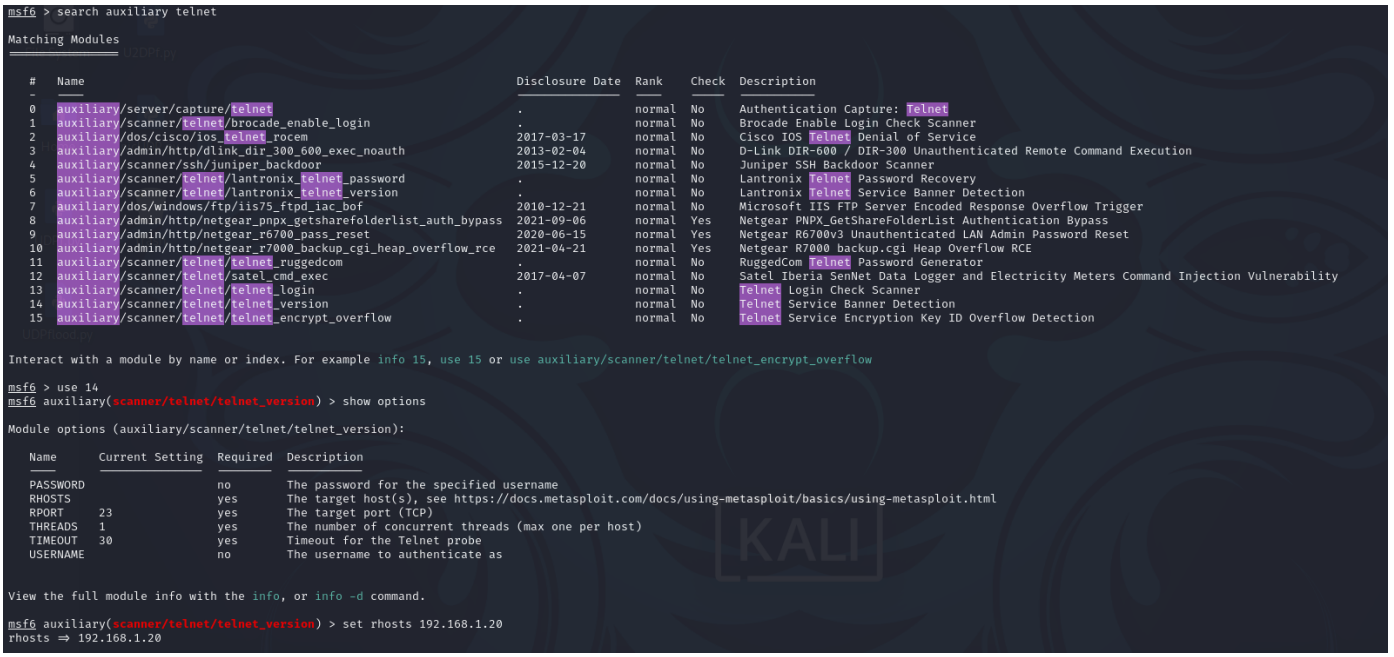
W16D2

una volta lanciato
msfconsole



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.
Spoofer: 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 _                  _       _ _        _     _      ____   \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _
\ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\__
_|______|\x0a                             |_|                                          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogi
n with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.20:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```