Hack Metasploit Telnet

Cos’è un Exploit

In sicurezza informatica, un "exploit" è un software, un codice o una sequenza di comandi che sfrutta una specifica vulnerabilità in un sistema o un'applicazione al fine di ottenere un vantaggio non autorizzato.

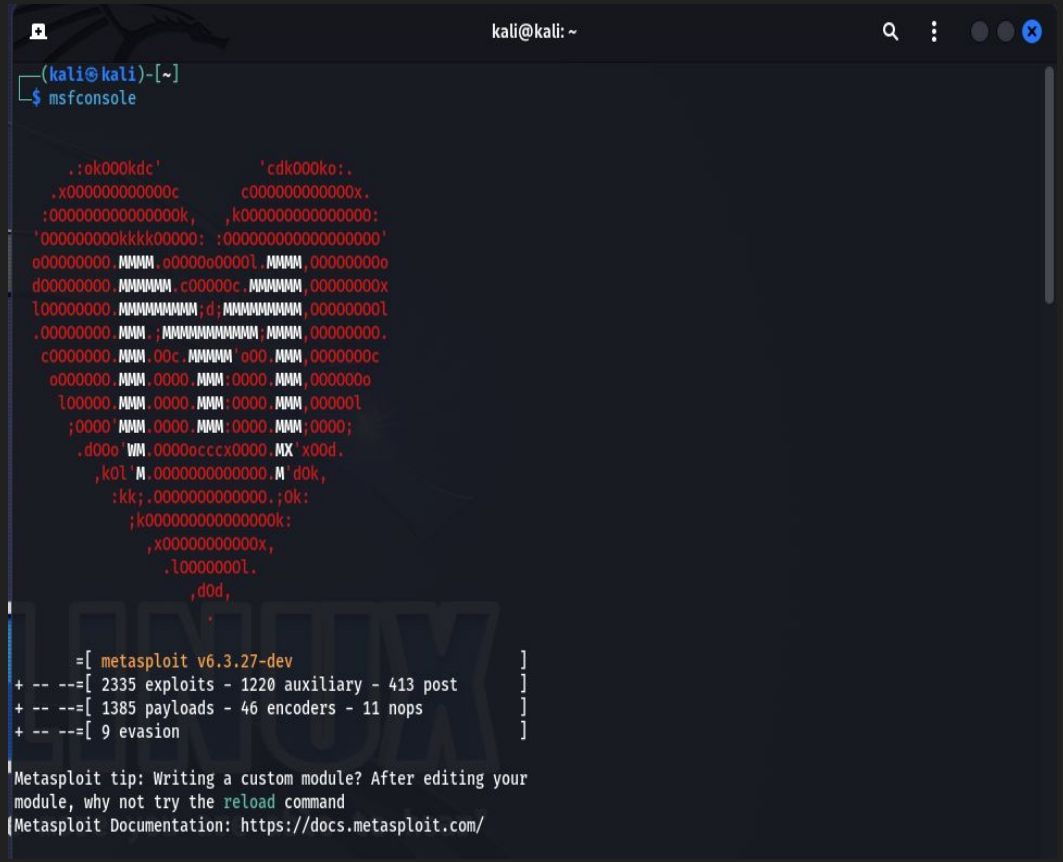
Le vulnerabilità possono essere errori di progettazione, bug di implementazione o altri problemi che possono essere sfruttati.

Cos’è il modulo auxiliary telnet_version

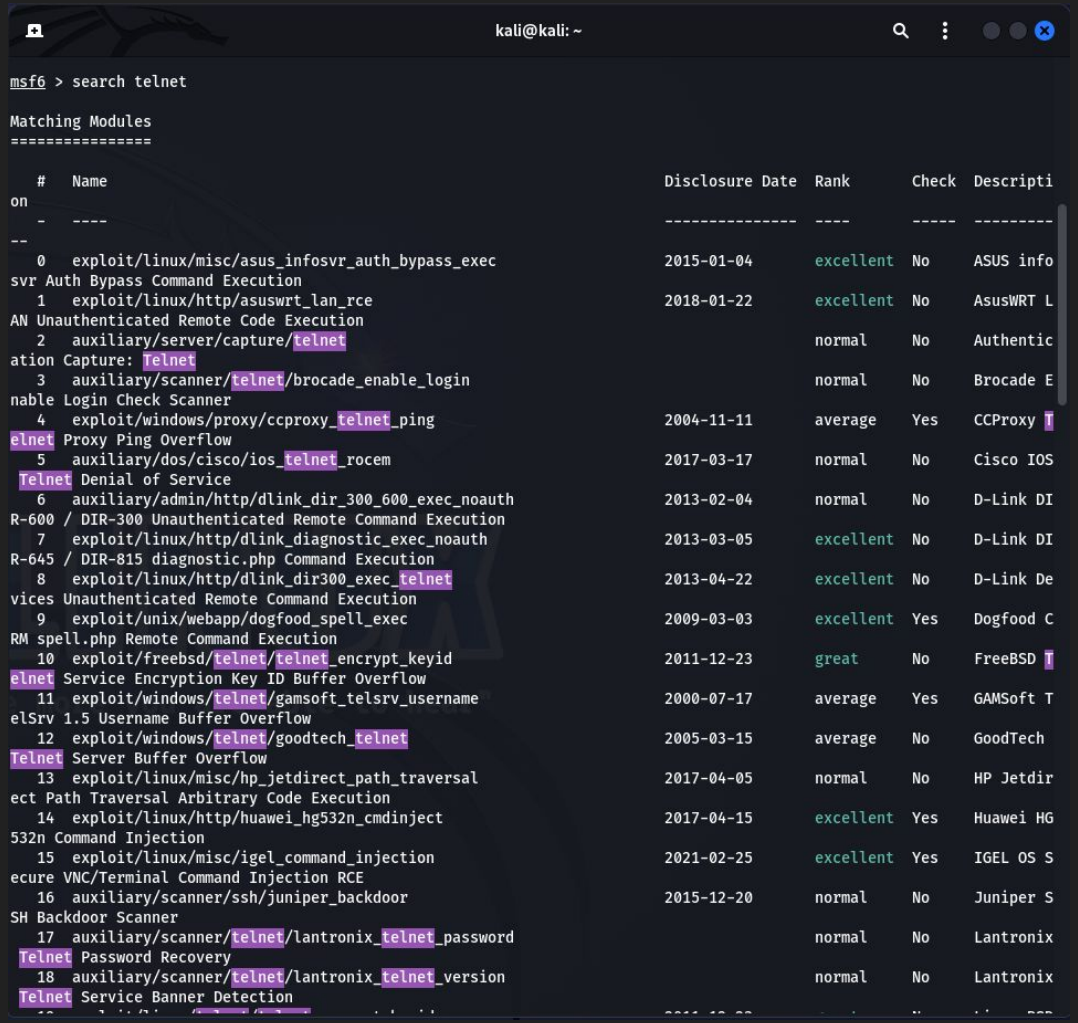
Il modulo "auxiliary/telnet/telnet_version" in Metasploit è progettato per eseguire una scansione di versione Telnet su un host di destinazione per identificare la versione specifica del servizio Telnet in esecuzione. Questo modulo rientra nella categoria "auxiliary" di Metasploit, che comprende moduli non necessariamente finalizzati all'esecuzione di exploit, ma piuttosto a fornire informazioni o eseguire attività ausiliarie.

Esercizio

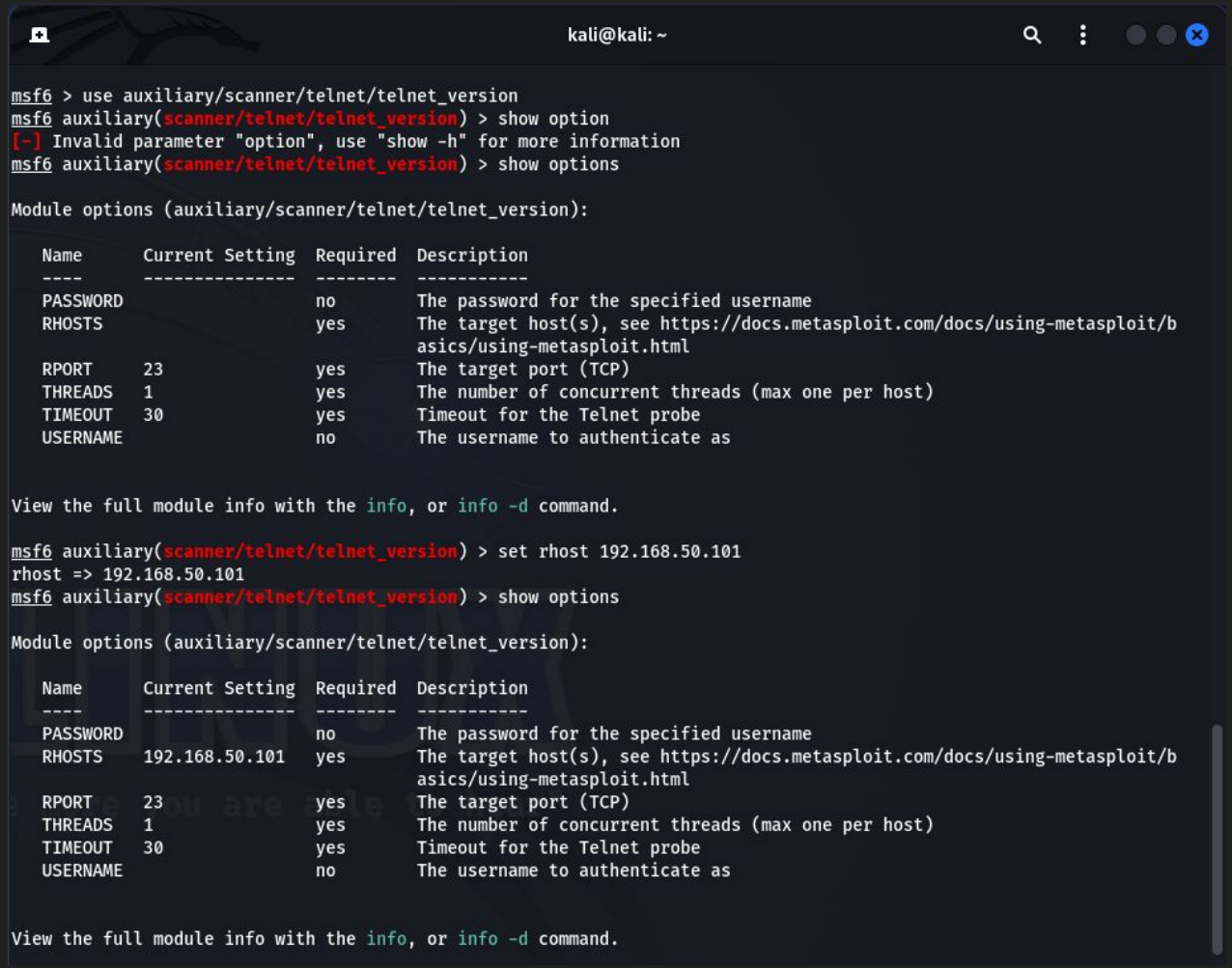
Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.



Con il comando msfconsole, avviamo l'interfaccia a riga di comando di Metasploit, fornendo un ambiente interattivo per l'utilizzo del framework e l'esecuzione di attività di penetration testing.

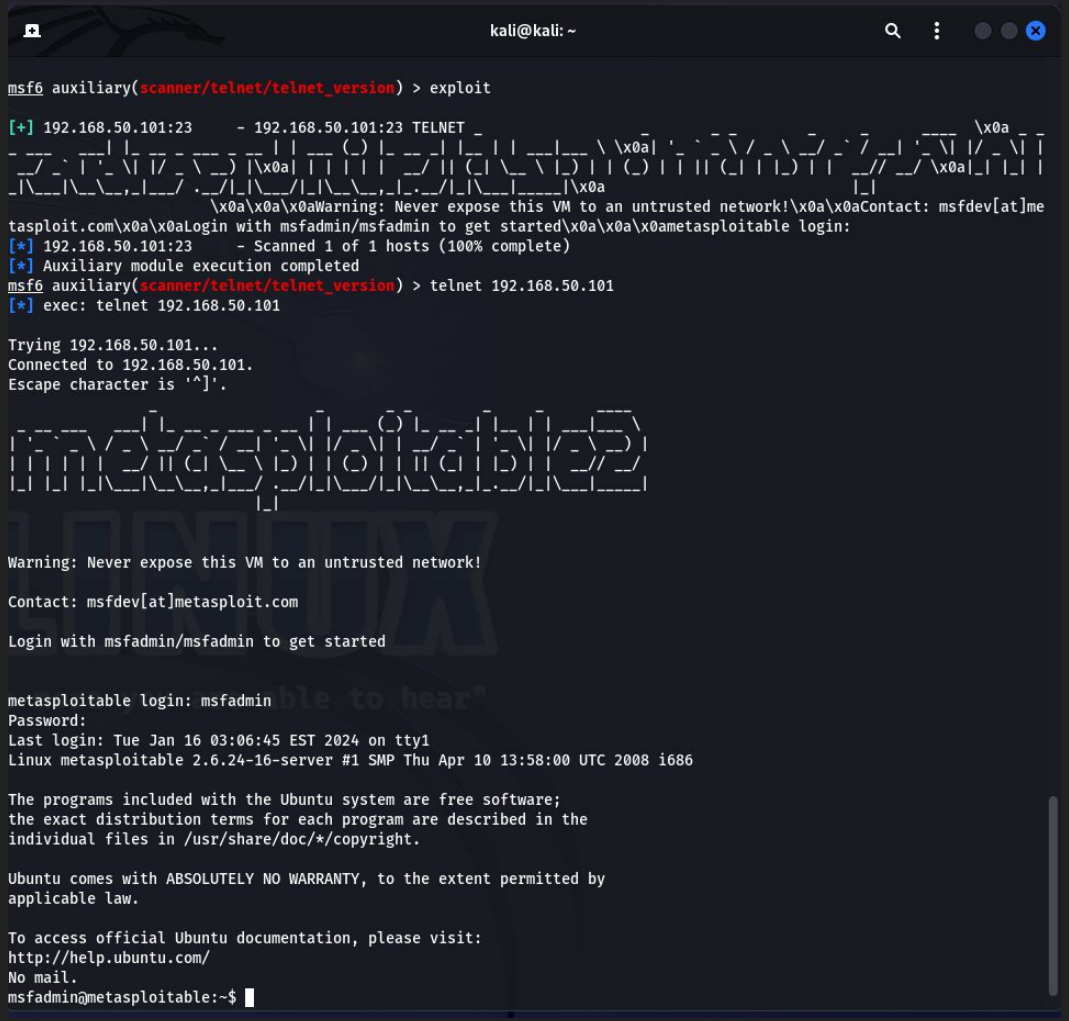


Con il comando search cerchiamo tutti moduli in cui è presente la dicitura Telnet



Con il comando use, scegliamo il modulo da utilizzare e con il comando show options vediamo le opzioni da modificare

Settiamo l'host con l'ip della macchina da attaccare con il comando rhost



Con il comando exploit facciamo partire il modulo

Con il comando telnet 192.168.50.101 ci connettiamo alla macchina vittima

Ora abbiamo il controllo della macchina vittima