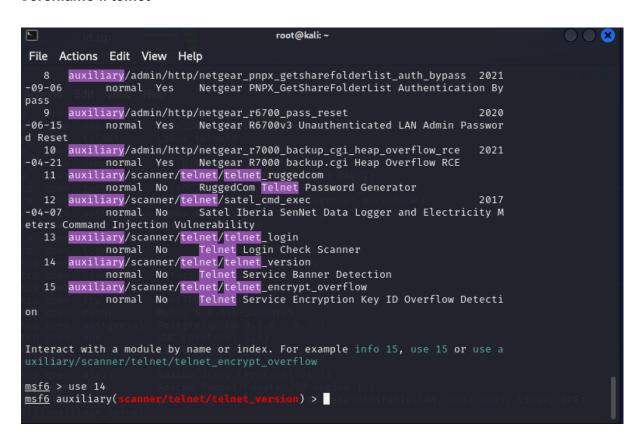
Oggi eseguiremo un attacco sulla porta del telnet di metasploitable

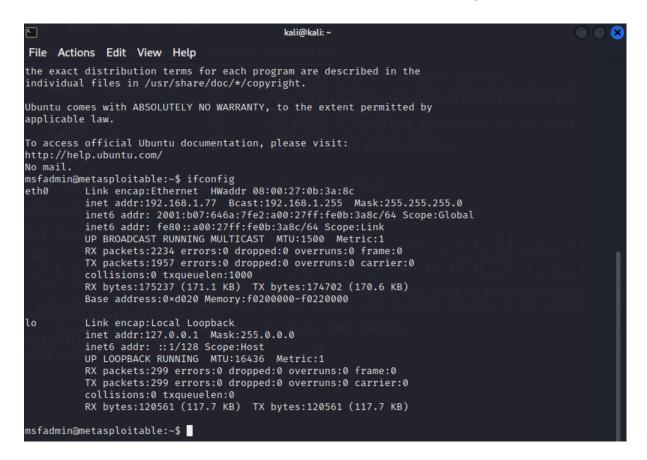
```
msf6 > search auxiliary telnet
Matching Modules
                                                                              Disc
   #
       Name
losure Date Rank
                      Check Description
       auxiliary/server/capture/telnet
   0
             normal No 4
                           (RFAuthentication Capture: Telnet
       auxiliary/scanner/telnet/brocade_enable_login
             normal No Brocade Enable Login Check Scanner
       auxiliary/dos/cisco/ios_telnet_rocem
   2
                                                                              2017
-03-17
             normal No ( Cisco IOS Telnet Denial of Service
       auxiliary/admin/http/dlink_dir_300_600_exec_noauth 2013
normal No D-Link DIR-600 / DIR-300 Unauthenticated Remote C
             normal No
-02-04
ommand Execution
       auxiliary/scanner/ssh/juniper_backdoor
                                                                              2015
             normal No
-12-20
                              Juniper SSH Backdoor Scanner
```

Cerchiamo il telnet



Usiamo quello che si addice al nostro attacco

Cambiamo rhosts mettendo l'ip di metasploitable dopodichè eseguiamo l'attacco



Facendo ifconfig notiamo di essere riusciti ad entrare nella macchina metasploitable

Telnet è un protocollo di rete utilizzato per stabilire una connessione remota a un server o a un dispositivo tramite la rete. La sua principale funzione è quella di consentire agli utenti di accedere a una shell o a una sessione di comando su un host remoto. Telnet facilita l'interazione con sistemi e dispositivi remoti, consentendo agli utenti di eseguire comandi, trasferire file e svolgere altre attività come se fossero direttamente collegati al sistema remoto. Tuttavia, è importante notare che Telnet trasmette dati, inclusi nomi utente e password, in formato di testo non crittografato, il che può costituire un rischio per la sicurezza. A causa di questa vulnerabilità, Telnet è

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