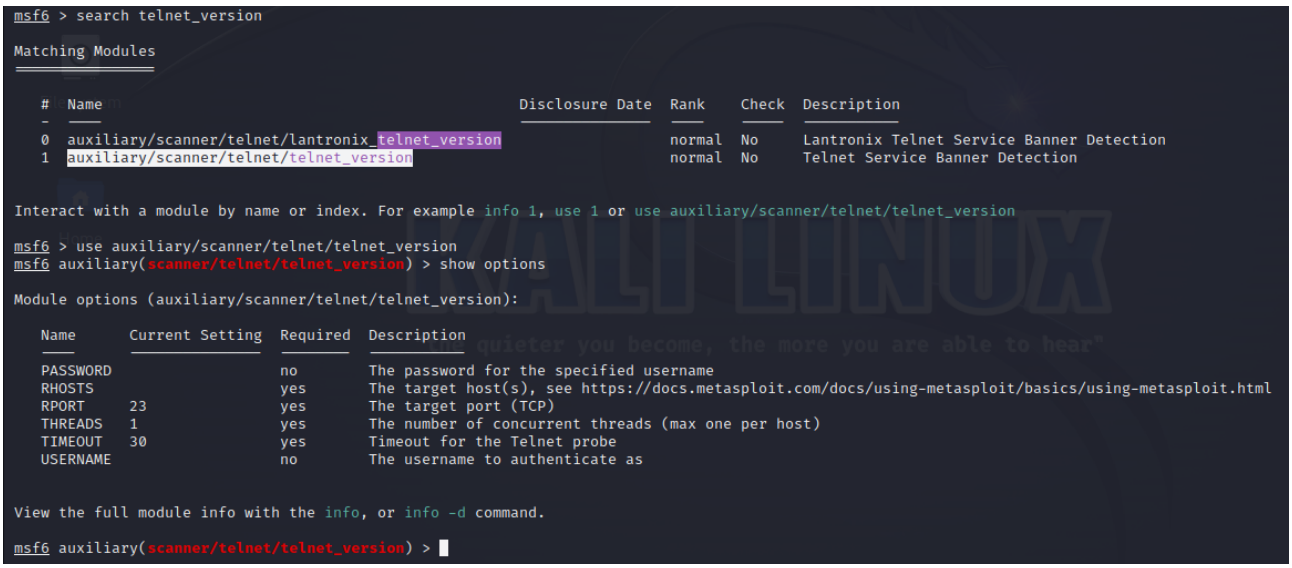
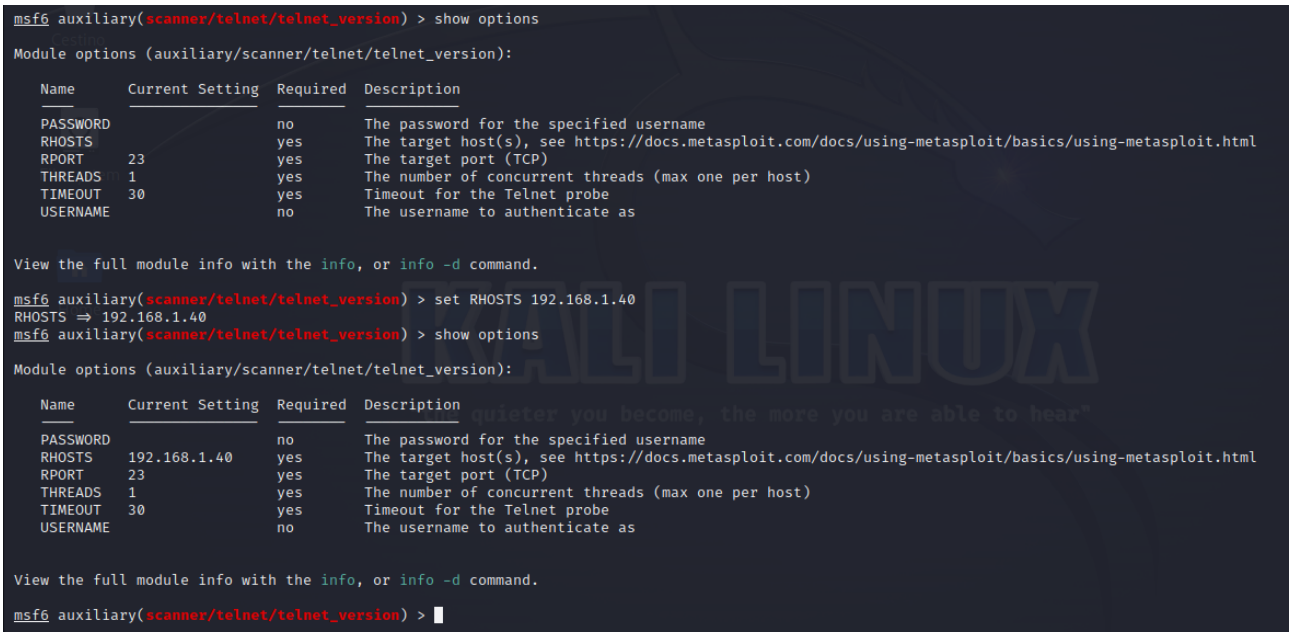
Oggi andremo a sfruttare la vulnerabilità sulla porta 23 che offre il servizio Telnet:

aperto msfconsole , cerco il modulo in questione cercano “telnet_version”:

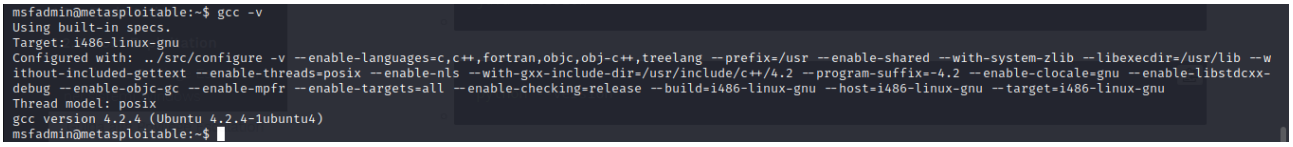


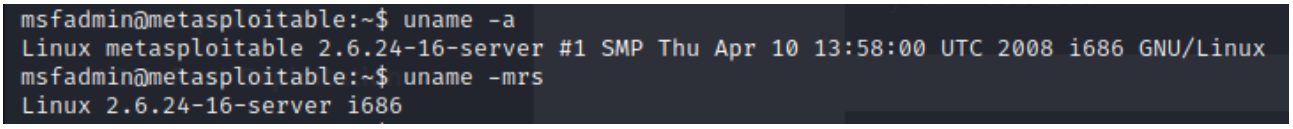
Una volta trovato il modulo, lo lancio con il comando “use” e compilo i parametri richiesti visti con il comando show options:

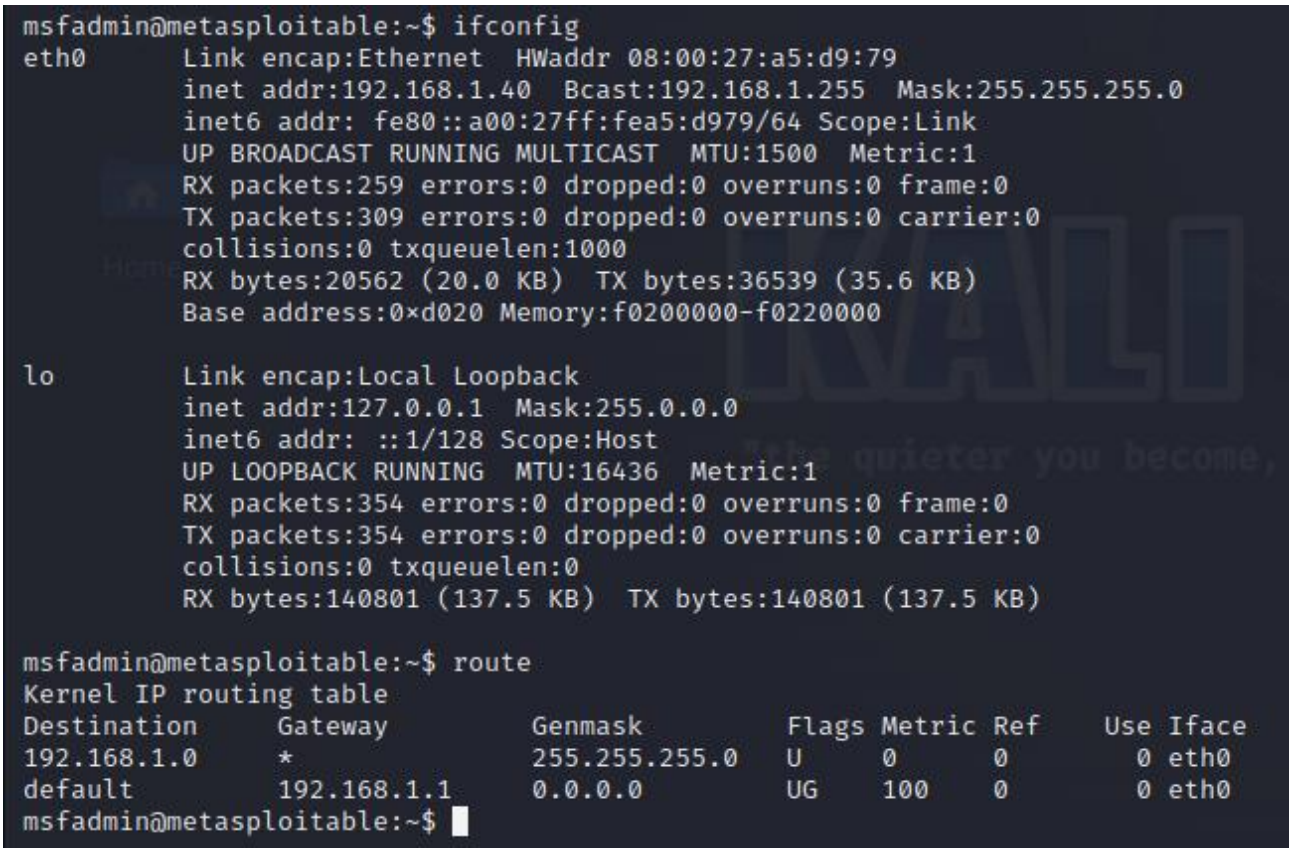


Una volta rimepiti i parametri con l’ip della macchina target (metasploitable), ed una volta settato il payload (di default), lancio l’attacco con il comando “exploit”:

Per vedere se l'attacco e andato a buon, eseguo il comando telnet seguito dall'ip della macchina attaccata ed il servizio mi chiede password e utente, che ho recuperato nel passaggio prima (msfadmin e msfadmin).







Vediamo che dopo esser loggati con le credenziali “rubate”, abbiamo accesso al terminale vero e proprio della macchina attaccata e, con diversi comandi, recupero informazioni preziosi della macchina attaccata.