Proviamo adesso a sfruttare la vulnerabilità di metasploitable legata al servizio “telnet”. Settiamo gli indirizzi di kali (macchina attaccante) e metasploitable (macchina vittima) rispettivamente con IP 192.168.1.25 e 192.168.1.40.

Apriamo la console con il comando “msfconsole” ed avviamo l’exploit con il comando “auxiliary/scanner/telnet/telnet_version”. Si tratta di un modulo ausiliario; sebbene non sia un modulo aggressivo (infatti non attacca direttamente la macchina), ci restituisce informazioni importantissime sulla macchina bersaglio: nome utente e password per accedere alla macchina e quindi ai servizi da remoto.

Questo, come tanti altri moduli possono essere trovati con il comando “search” seguito dalla parola chiave che ci interessa (servizio, protocollo ecc…).

Per accertarci di quali parametri ha bisogno l’exploit per partire usiamo il comando “show option”.

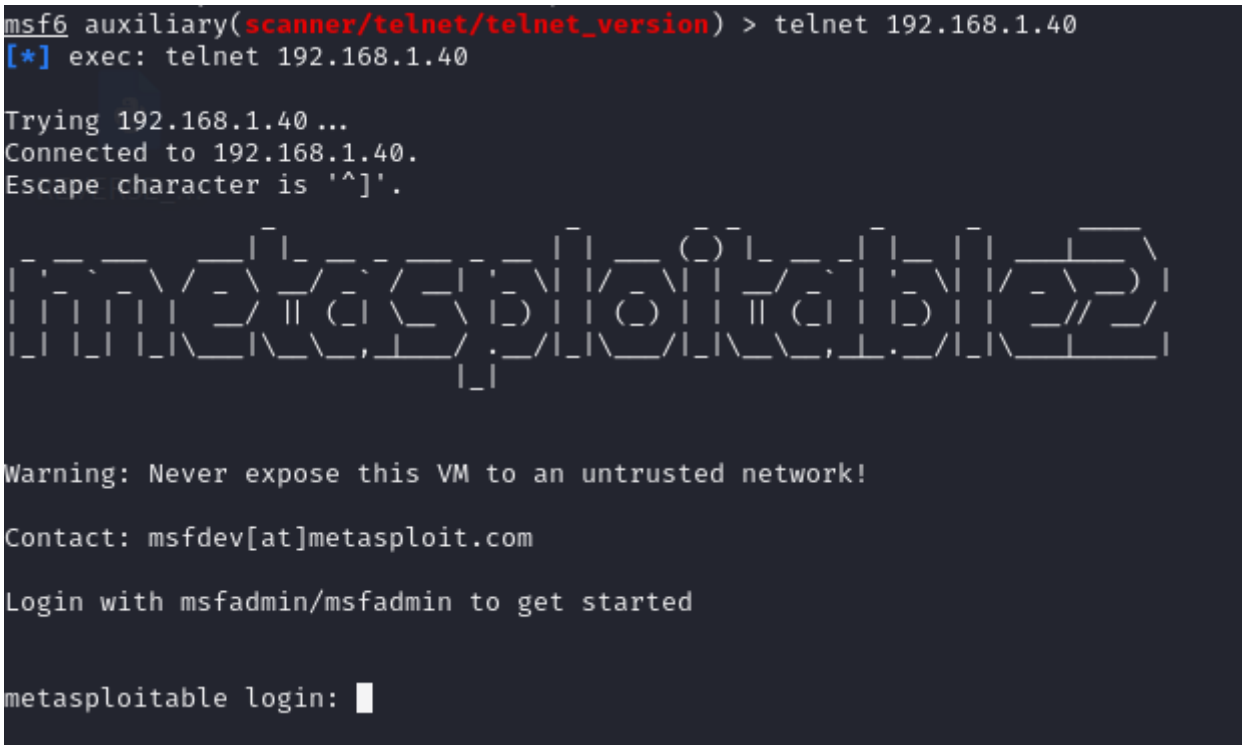
L’exploit ha bisogno solo del parametro RHOST per funzionare; gli altri già ce li ha (tipo la RPORT) oppure non sono necessari (tipo l’username).

Settiamo come RHOST l’IP di metasploitable.

L’exploit è pronto a partire (non c’è neanche bisogno di impostare il payload). Diamo quindi il comando “exploit”.

Nella foto vediamo che l’exploit ha avuto successo: ci sono state restituite le credenziali d’accesso della macchina metasploitable (cerchiato in verde).

E’ il momento di collegarci alla macchina da remoto sfruttando il protocollo telnet. Digitiamo quindi sulla console msfconsole il comando “telnet 192.168.1.40”.



Poiché il servizio è filtrato, ci chiederà nome utente e password di metasploitable. Inseriamo nome utente e password da poco recuperati e siamo connessi.

Vediamo come abbiamo preso pieno controllo della macchina metasploitable. Infatti eseguendo il comando “ifconfig”, ci troviamo sulla stessa shell di metasploitable.