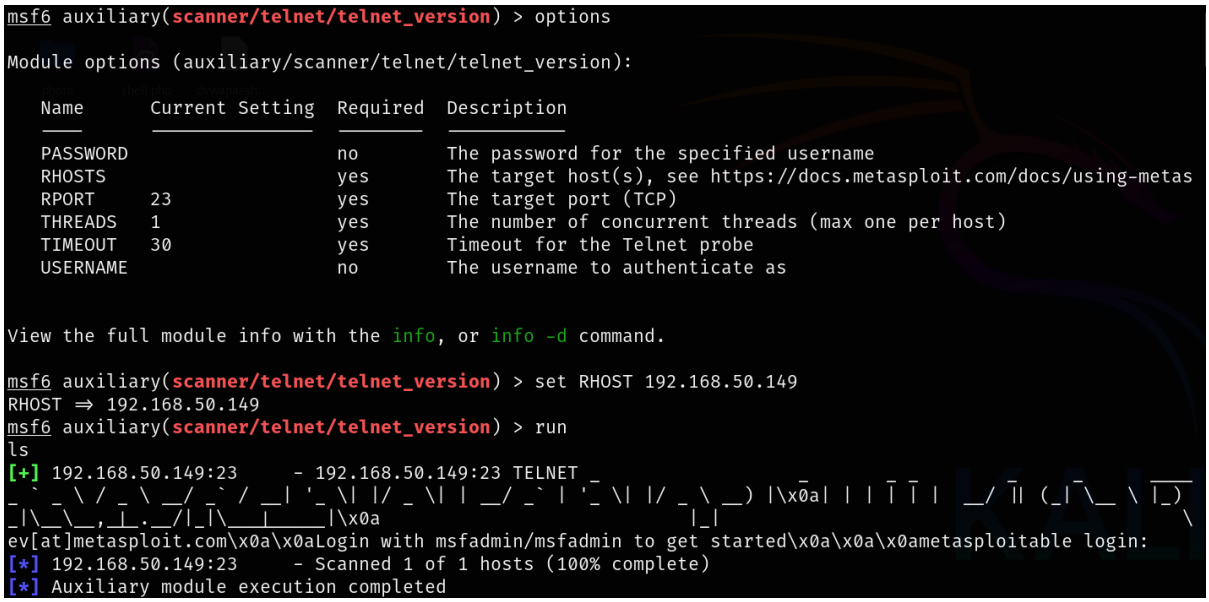
Exploit Telnet con Metasploit

Durante l'esercitazione di oggi, abbiamo esplorato l'utilizzo del framework Metasploit per identificare e sfruttare una vulnerabilità relativa al servizio Telnet sulla macchina virtuale Metasploitable . L'obiettivo principale era utilizzare il modulo **auxiliary/scanner/telnet/telnet_version** per raccogliere informazioni sul servizio Telnet in esecuzione sulla macchina target.

Per iniziare, abbiamo avviato il framework Metasploit tramite il terminale di Kali Linux e selezionato il modulo **auxiliary/scanner/telnet/telnet_version**, che consente di rilevare la versione del servizio Telnet in esecuzione su una macchina remota.

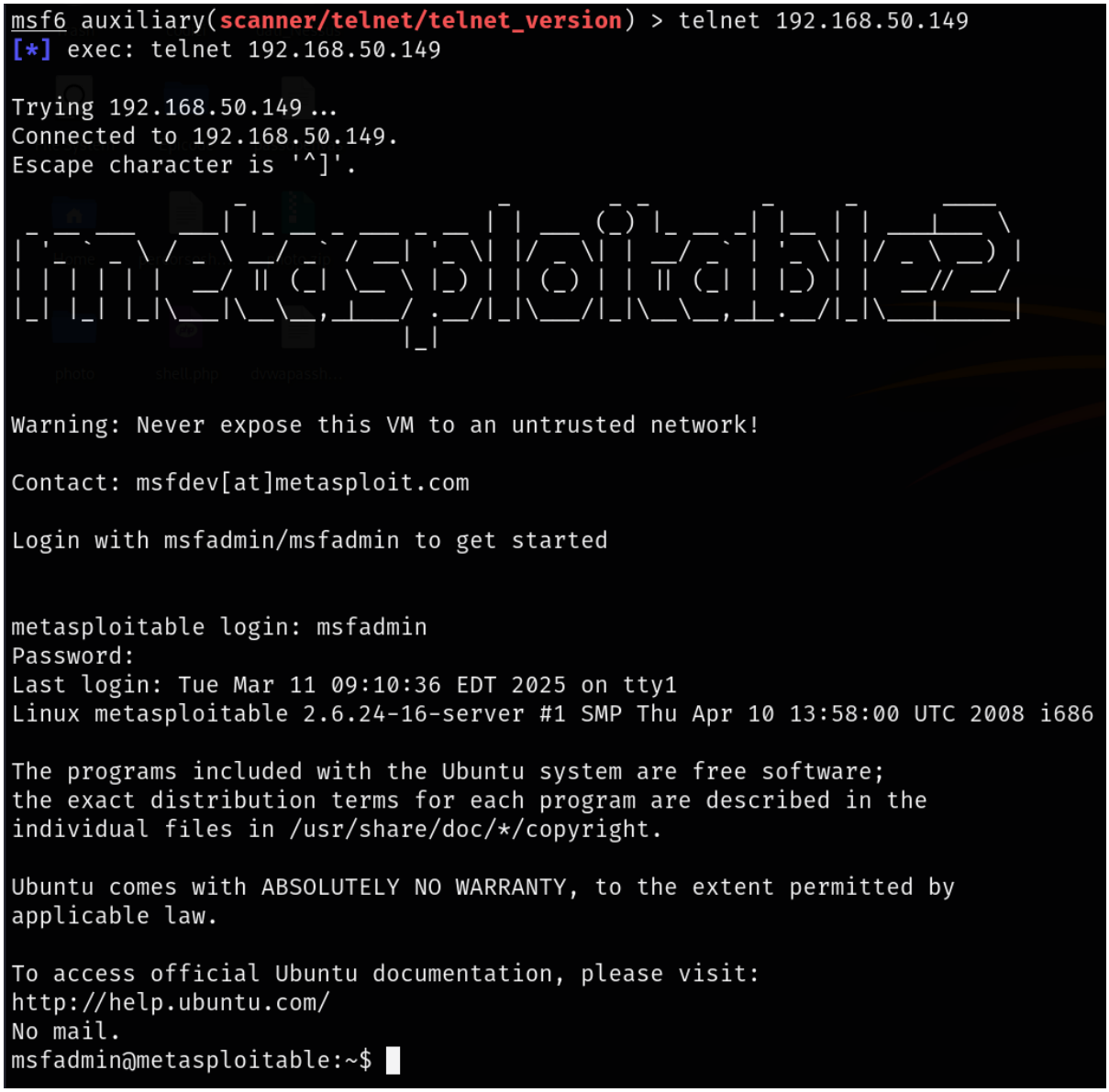
Inseriamo l'indirizzo IP della macchina target e avviamo il modulo con il comando **run**.



Dopo aver eseguito il modulo **auxiliary/scanner/telnet/telnet_version**, abbiamo scoperto che lo scan ha rivelato le seguenti credenziali predefinite:

- Username : **msfadmin**
- Password : **msfadmin**

Eseguiamo da Metasploit il comando «telnet» seguito dall'ip della macchina Metasploitable. Nel nostro lab la Metasploitable ha IP 192.168.1.149, quindi eseguiremo il comando «telnet 192.168.1.149»



Dopo aver inserito le credenziali, siamo stati autenticati con successo e abbiamo ottenuto un prompt della shell della metasploitable.