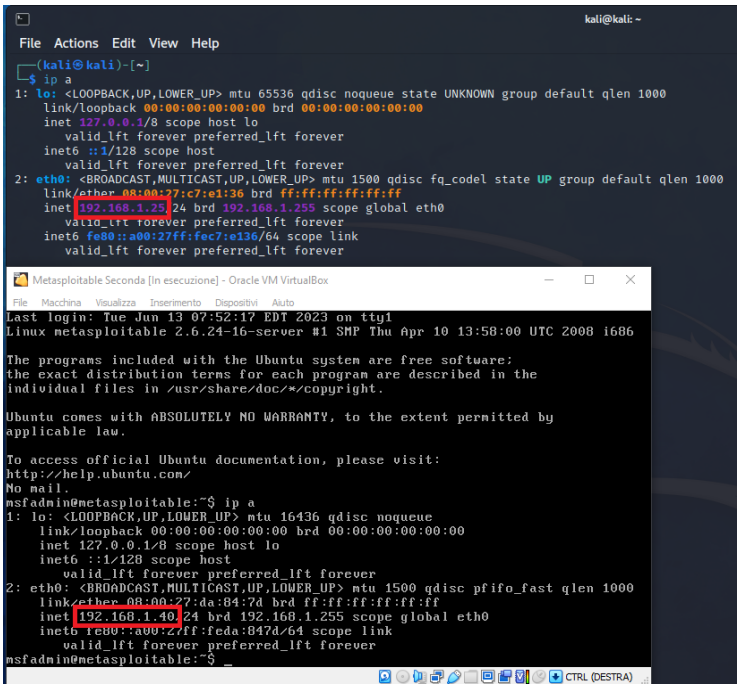
Exploit Telnet

Obiettivo: Sfruttare li servizio Telnet per hackerare la macchina Metasploitable

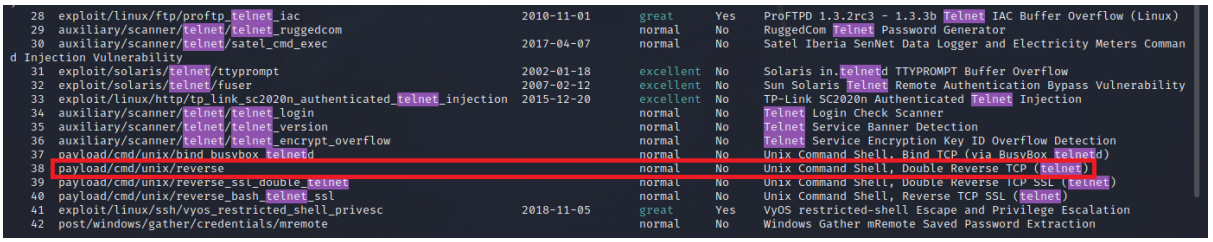
1) Configurazione IP

Per iniziare ho settato gli indirizzi IP di **Kali** (192.168.1.25) e **Metasploitable** (192.168.1.40) come da traccia.



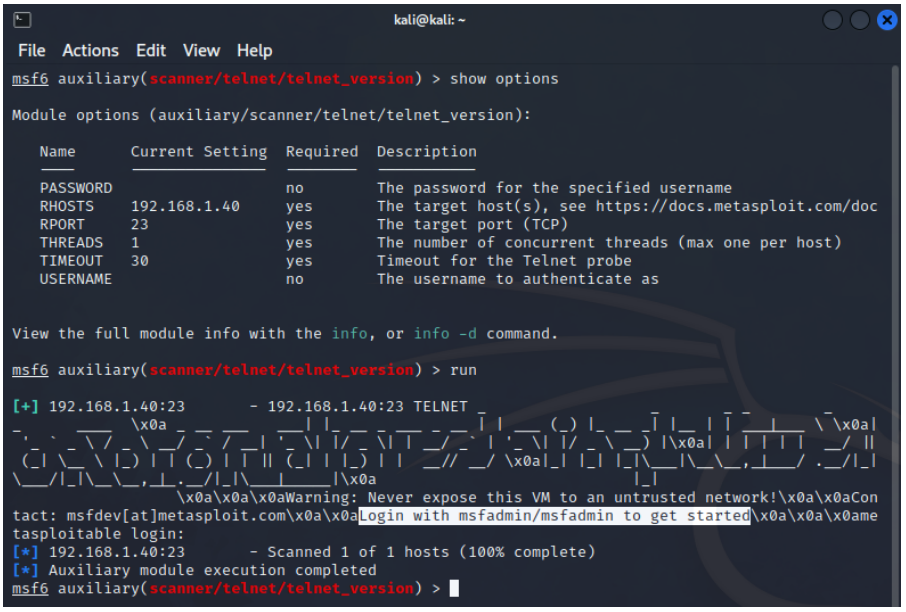
2) Modulo Telnet su Msfconsole

Una volta stabilita una connessione tra le due macchine ho avviato il tool **msfconsole** per ricercare il modulo per poter sfruttare gli exploit della **Metasploitable**, più precisamente ho ricercato i moduli inerenti al servizio *telnet*.

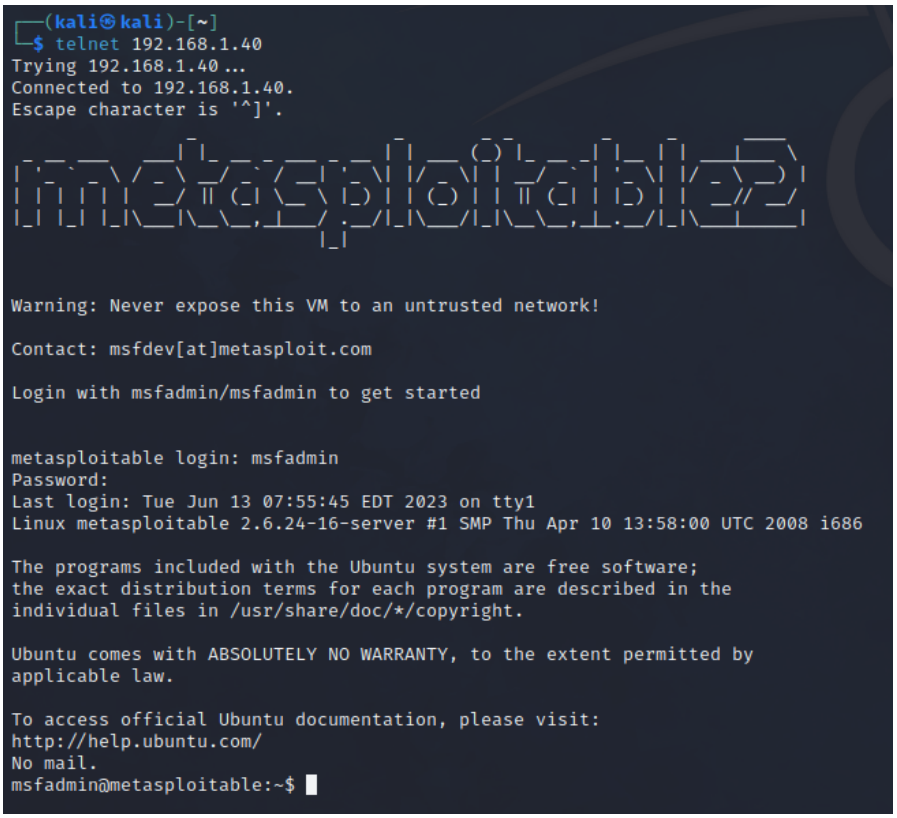


Con *search telnet* la ricerca ha portato a 42 risultati ma in questo caso a noi serve il modulo 36 (può variare perciò è meglio controllare il nome prima di tutto). Con il comando open 36 ho caricato il modulo; in questo caso non sono necessari payload perciò una volta montato basta avviare il tutto con *run* o *exploit*.

Come possiamo notare dalla figura sotto una volta avviato (ed avuto successo) il tool ci mostra la schermata iniziale della **Metasploitable** con *username* e *password*.



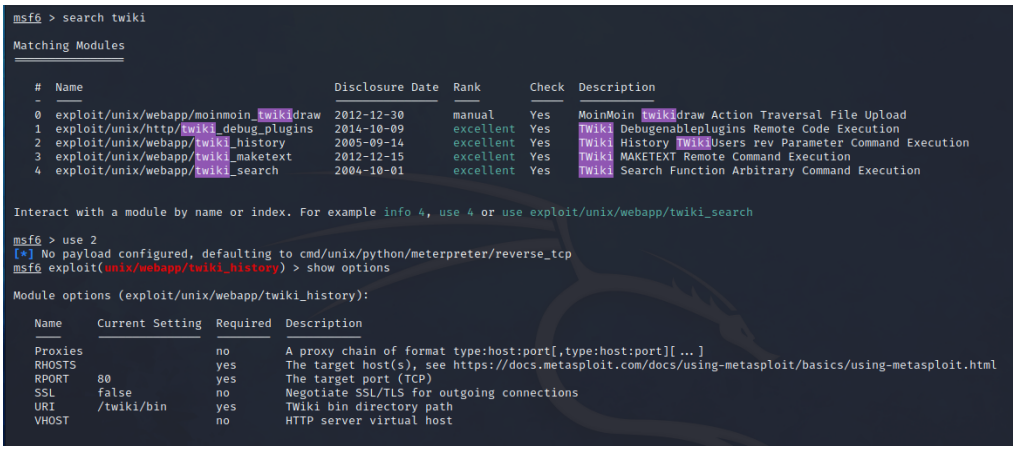
Come controprova ho avviato il servizio telnet collegandomi all'indirizzo IP della **Metasploitable** inserendo le credenziali lette ed entrando all'interno della macchina.



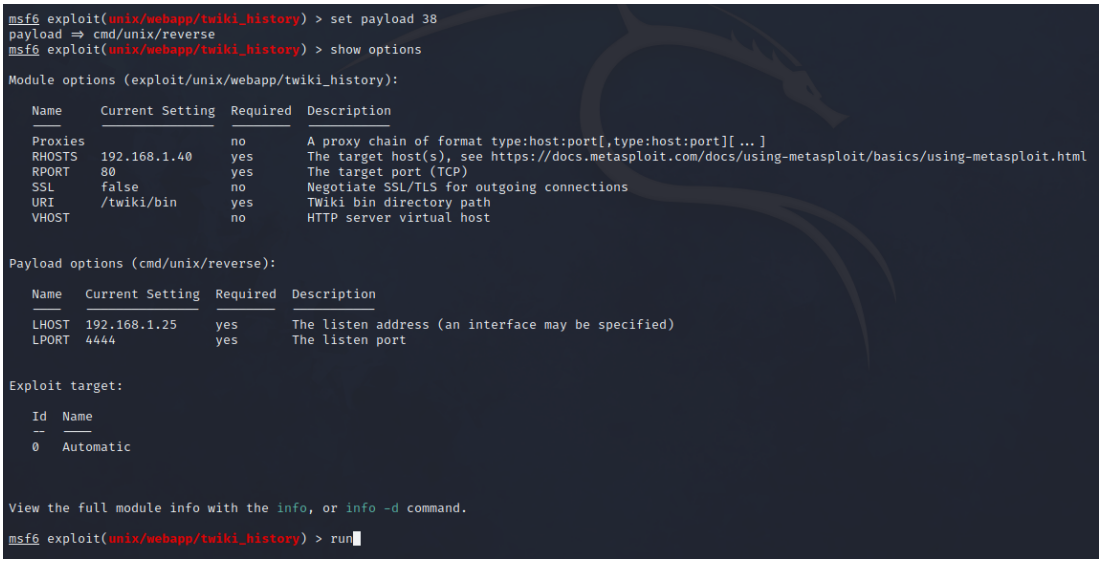
3) Twiki

Dopo aver hackerato la **Metasploitable** con il servizio *telnet* ho provato ad hackerare la porta 80 che ospita un servizio **Apache** con all'interno una piattaforma **Twiki**.

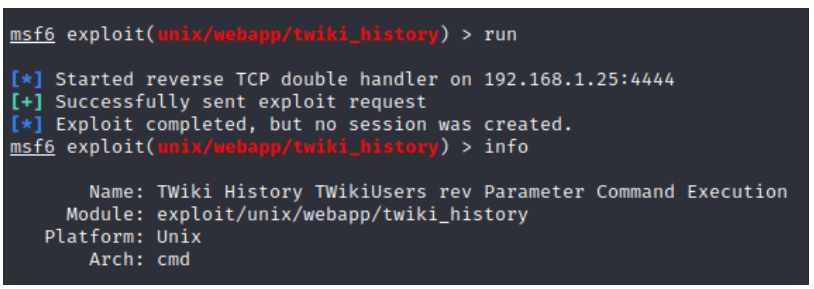
Ho avviato **msfconsole** come per la precedente prova cercando il modulo inerente alla *twiki_history*.

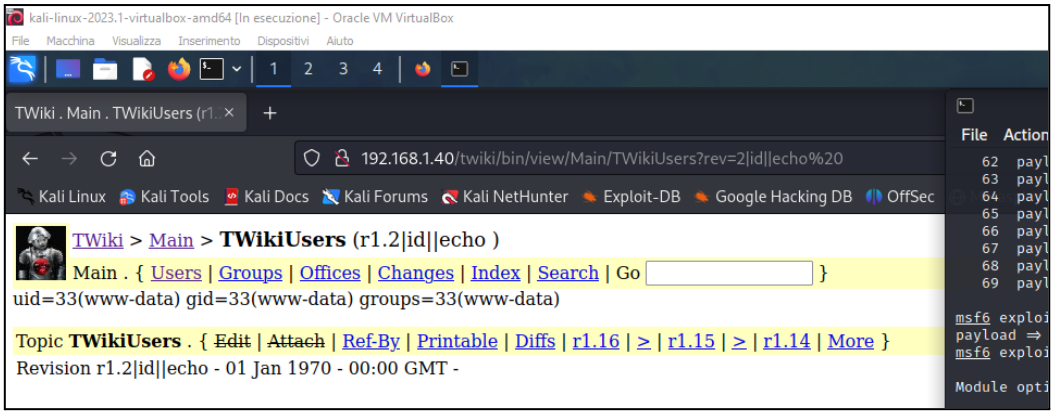


Il modulo che cerchiamo è il numero 2 ma serve anche caricare un payload che possiamo ricercare con il comando *show payloads*. La lista è molto lunga (69 risultati), ma a noi interessa il payload *cmd/unix/reverse* (numero 38 in questo caso) e montandolo con *set payload* 38 bisogna soltanto configurare con *set RHOST* l'indirizzo IP del bersaglio.

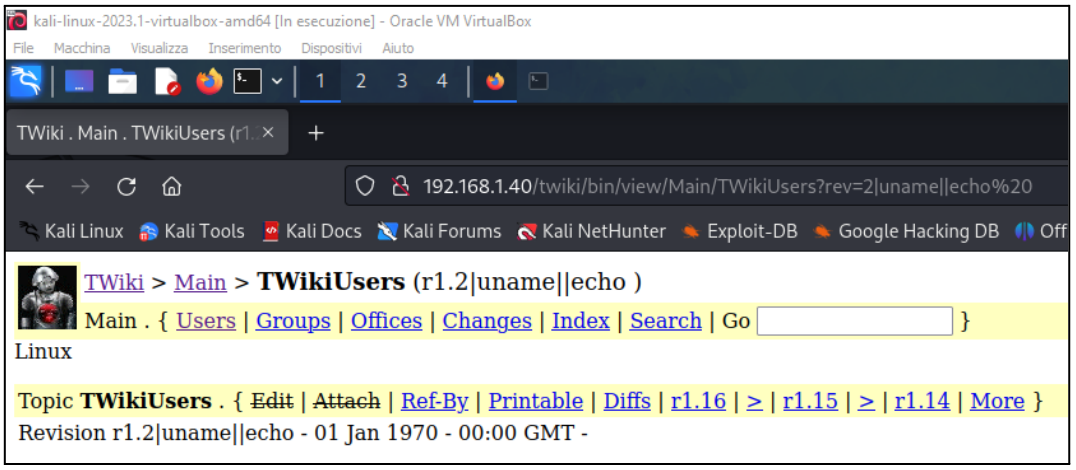


Ho avviato il modulo e dopo aver ricevuto un messaggio positivo sono andato da browser sulla piattaforma **Twiki** per testare l'exploit. Ho usato il codice suggerito dalla slide di teoria per elencare gli *id utente* e *gruppo* attraverso la pagina degli **Utenti** di **Twiki**.





Ho provato anche a cambiare il comando *id* con *uname* per visualizzare il sistema operativo.



4) Armitage

La prima prova sul servizio *telnet* l'ho riprodotta anche attraverso il tool **Armitage**, ovvero una sorta di **GUI** di **msfconsole**. Andando sull'opzione *Hosts* dalla barra in alto del tool ho avviato una scansione totale sulla **Metasploitable**. Una volta completata la scansione dalla colonna di sinistra ho ricercato l'exploit riguardante telnet avviandolo con doppio click.