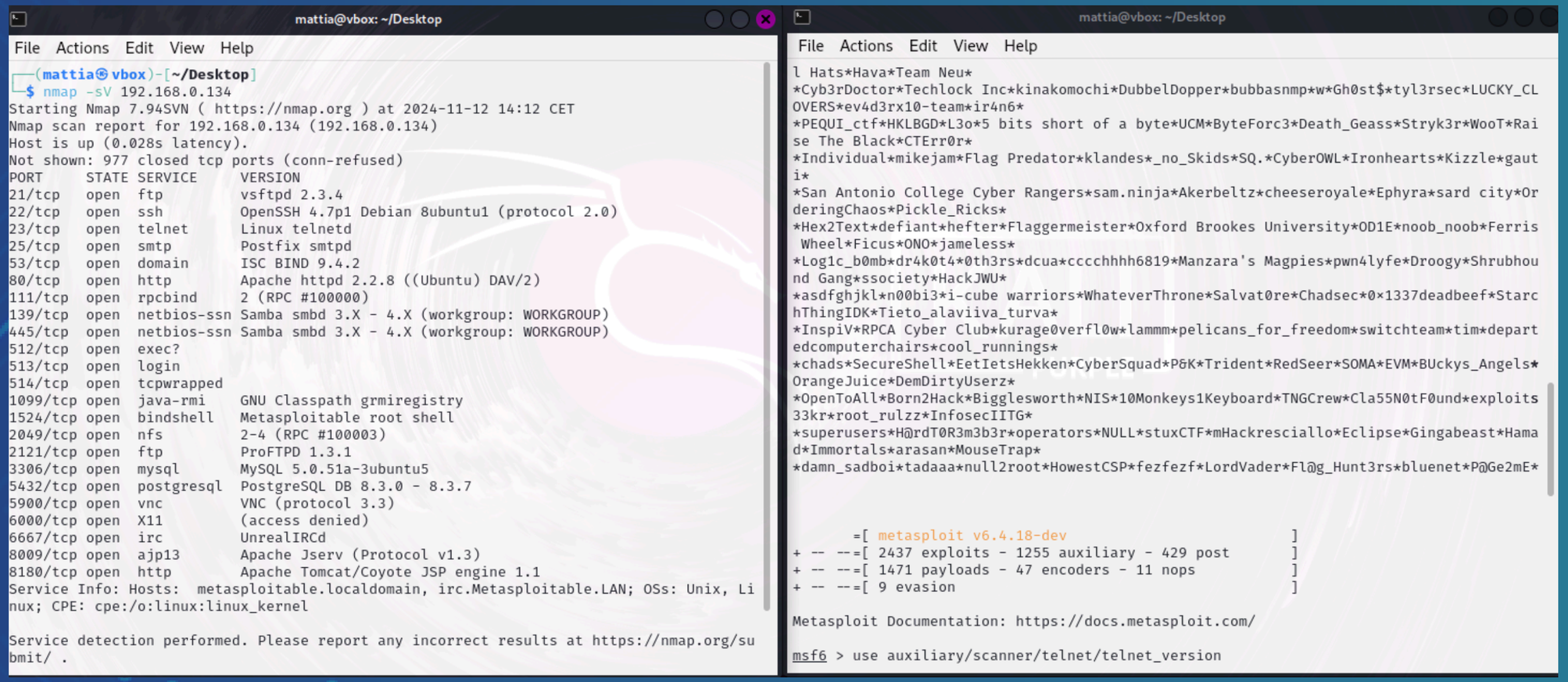
S7-L2

EXPLOIT TELNET

TRACCIA

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version con Kali linux sulla macchina metasploitable2

RICERCA NMAP + MSFCONSOLE



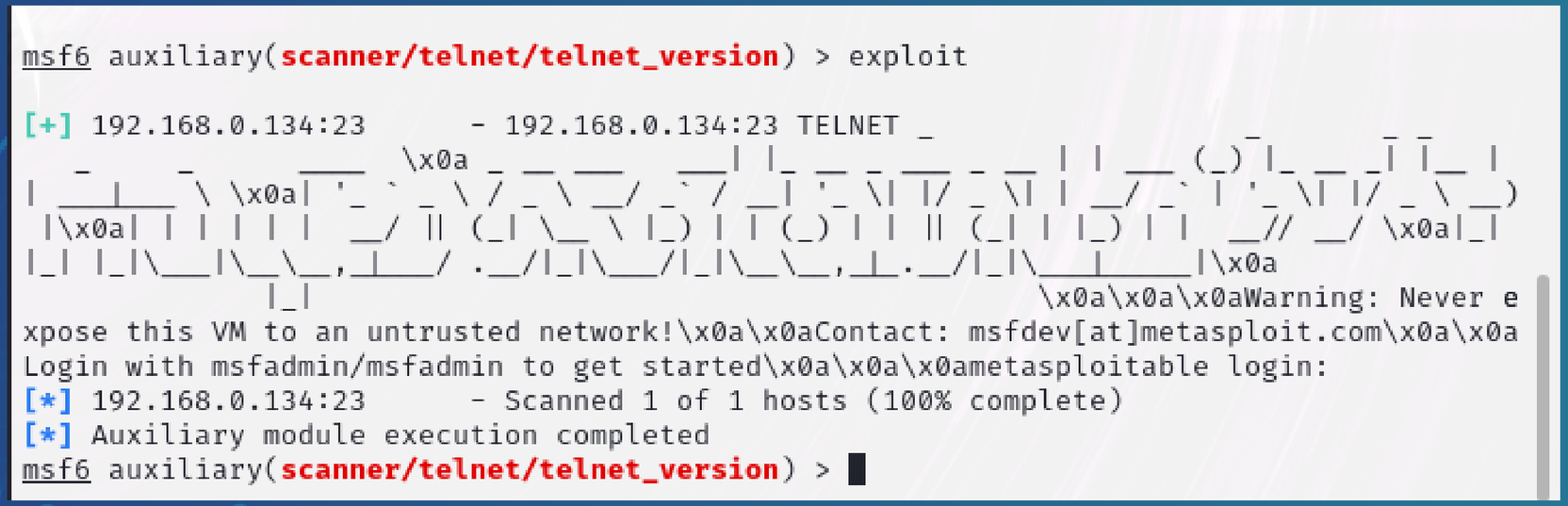
SET RHOSTS

Una volta effettuata ricerca su nmap e avviato msfconsole, procediamo a configurare il nostro target hosts manualmente con il comando “set RHOSTS ip di metasploit”.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.0.134
RHOSTS ⇒ 192.168.0.134
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    192.168.0.134    yes       The target host(s), see https://docs.metasplo
                                        it.com/docs/using-metasploit/basics/using-met
                                        asploit.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.
```

EXPLOIT

Una volta settato l’ip target, si procede all’exploit. Quest’ultimo ha avuto successo come si può vedere dallo screen in basso.
La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Questo significa che un potenziale attaccante potrebbe intercettare la comunicazione e rubare informazioni sensibili come username, password e i comandi scambiati tra client e server.



THANKS

MATTIA DI DONATO