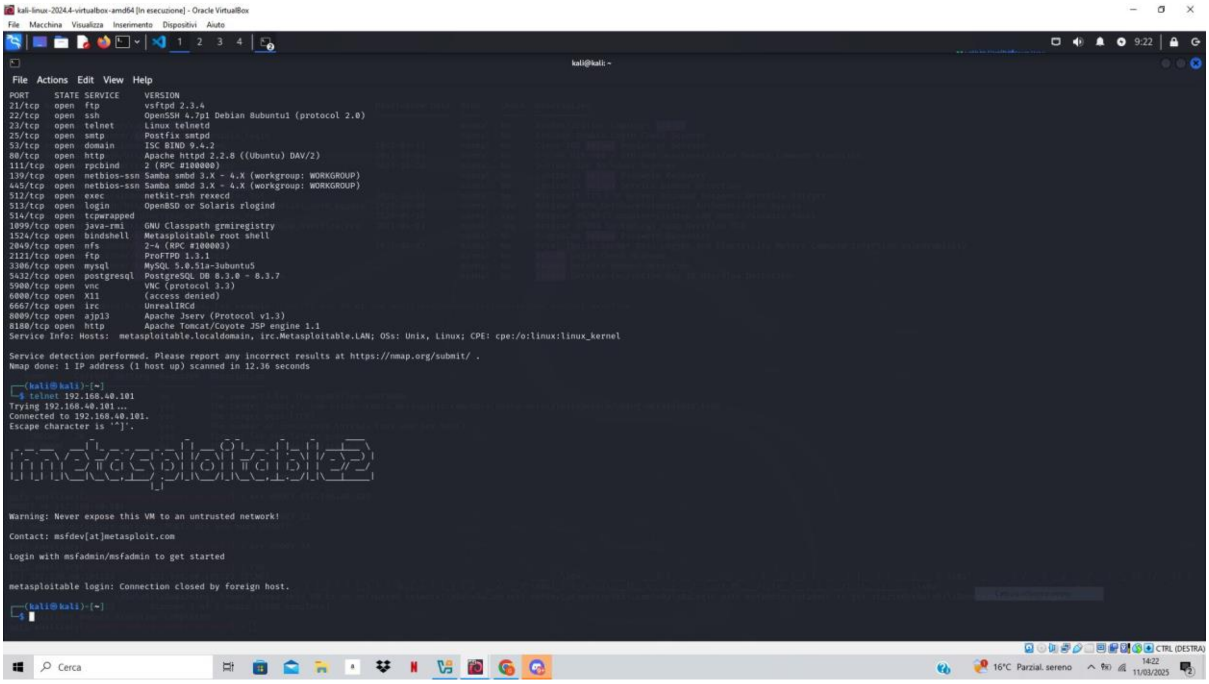
REPORT ESERCIZIO

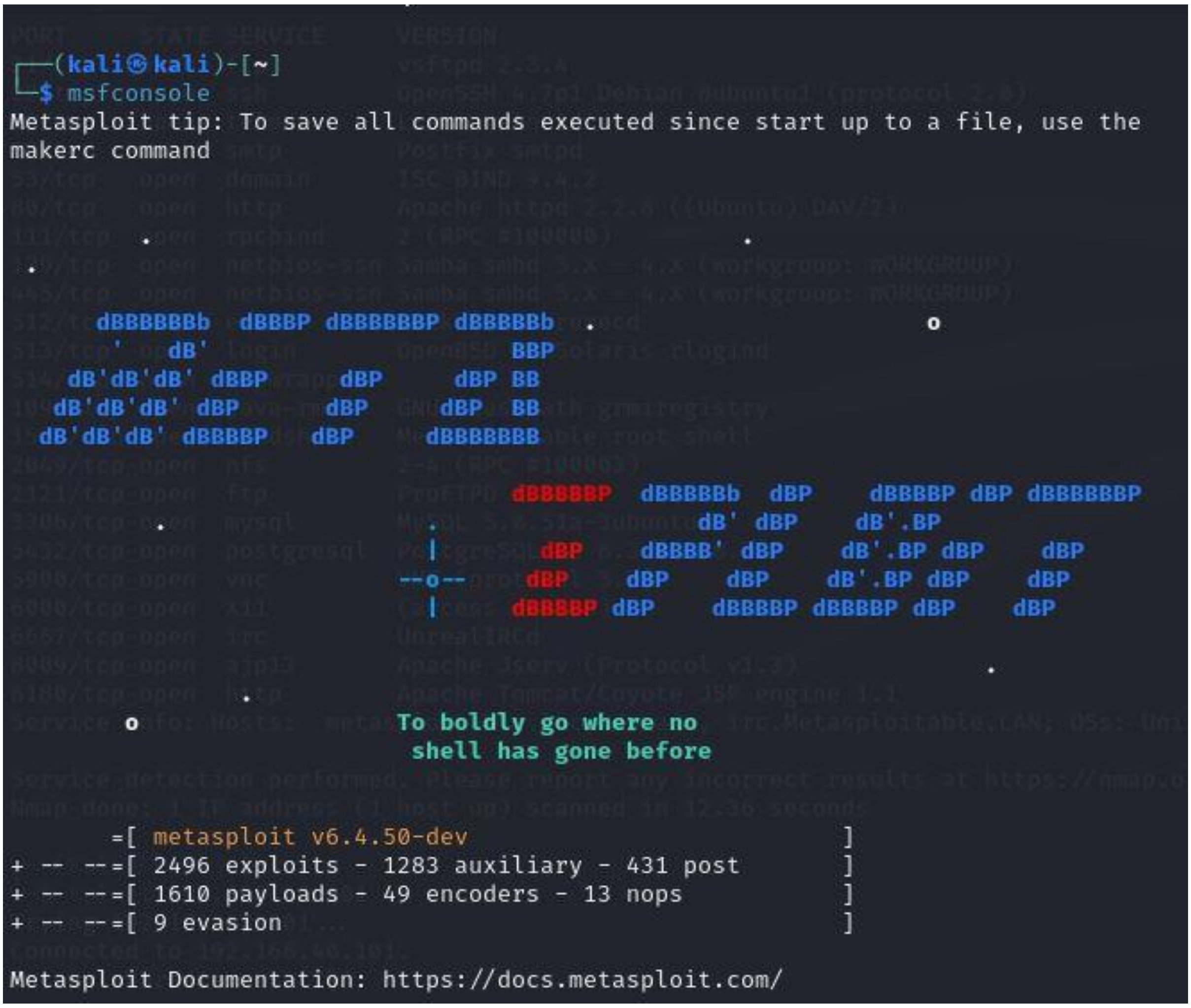
Inizialmente ultizzerò **nmap** per una scansione di porte su Metasploitable:



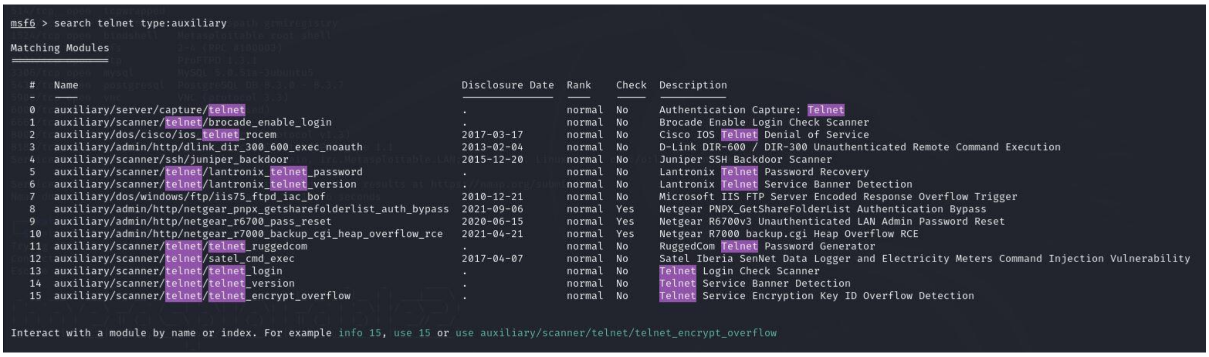
kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
Cerca

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds

┌──(kali㉿kali)-[~]
└─$ telnet 192.168.40.101
Trying 192.168.40.101...
Connected to 192.168.40.101.
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: Connection closed by foreign host.

┌──(kali㉿kali)-[~]
└─$ 
```

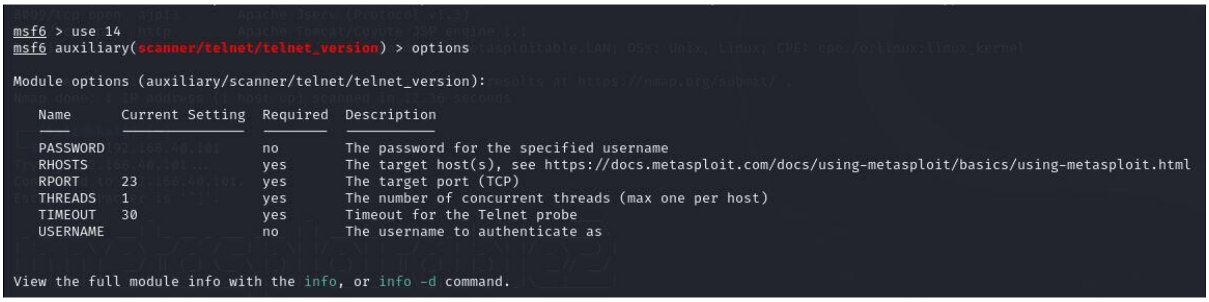
Ora utilizzerò **Metasploit** per sfruttare la vulnerabilità relativa a **Telnet** con il modulo **auxiliary telnet_version** sulla macchina Metasploitable;



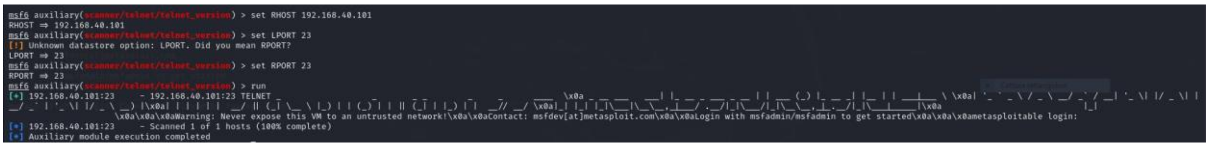
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

          .                                        .
 .

     dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP     dBP     dBP  BB
  dB'dB'dB' dBBBBP  dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .         dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before

       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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



```
msf6 > search telnet type:auxiliary

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

   #   Name                                                     Disclosure Date  Rank    Check  Description
   -   ----                                                     ---------------  ----    -----  -----------
   0   auxiliary/server/capture/telnet                          .                normal  No     Authentication Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login            .                normal  No     Brocade Enable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                     2017-03-17       normal  No     Cisco IOS Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth       2013-02-04       normal  No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                   2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password       .                normal  No     Lantronix Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version        .                normal  No     Lantronix Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof             2010-12-21       normal  No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes  Netgear PNPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset            2020-06-15       normal  Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21  normal  Yes  Netgear R7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom                .                normal  No     RuggedCom Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                  2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   13  auxiliary/scanner/telnet/telnet_login                    .                normal  No     Telnet Login Check Scanner
   14  auxiliary/scanner/telnet/telnet_version                  .                normal  No     Telnet Service Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow         .                normal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow
```



```
msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > 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 RHOST 192.168.40.101
RHOST ⇒ 192.168.40.101
msf6 auxiliary(scanner/telnet/telnet_version) > set LPORT 23
[!] Unknown datastore option: LPORT. Did you mean RPORT?
LPORT ⇒ 23
msf6 auxiliary(scanner/telnet/telnet_version) > set RPORT 23
RPORT ⇒ 23
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.40.101:23     - 192.168.40.101:23 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 with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.40.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```