



Spring-2017

Information Security and Assurance  
Assignment-2

Submitted by:

Moulika Chadalavada

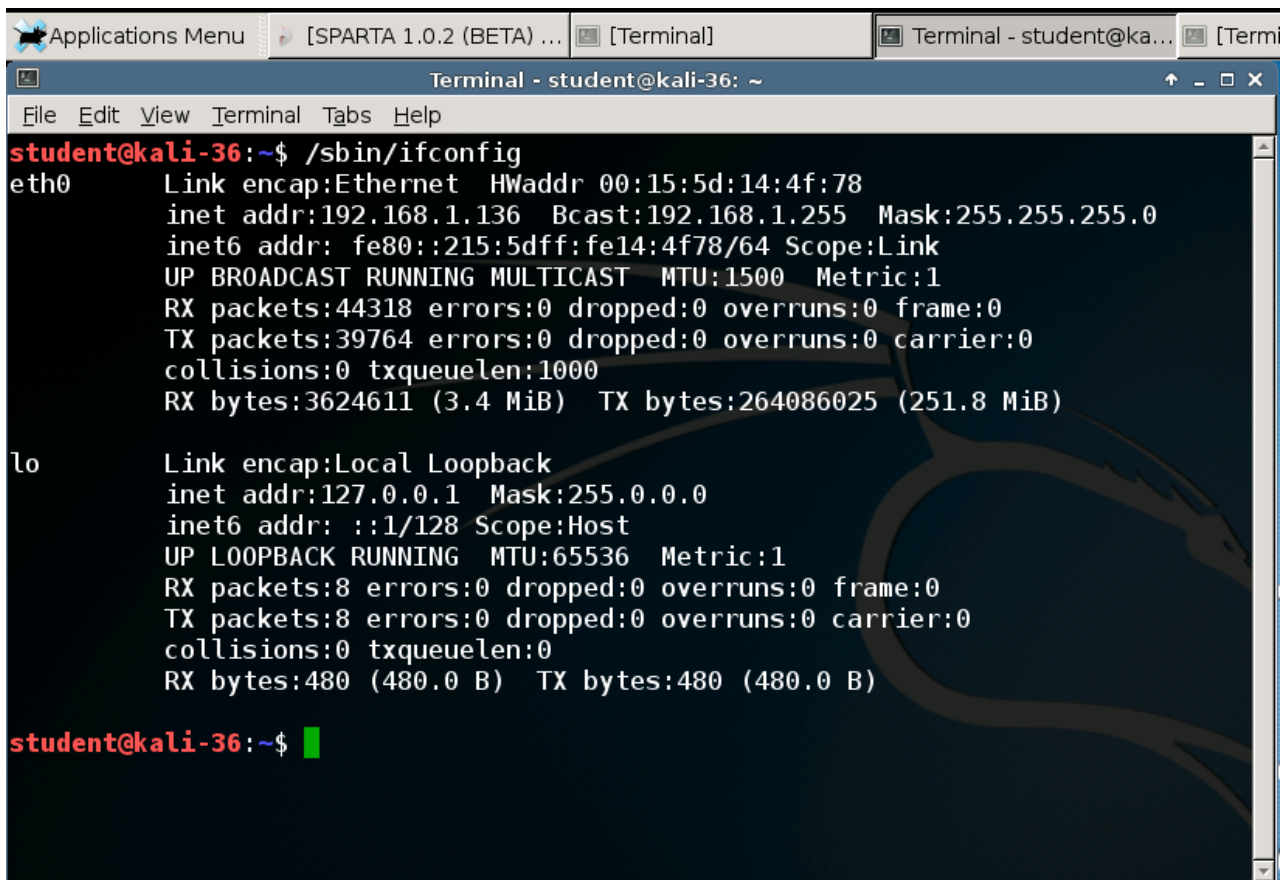
16234180

1. List the **live systems** that are reachable to your system (1 point)

Ans:

**Command:** nmap -sP 192.168.1.0/24**Output:**

- First to get IP Address of system in terminal we have to give /sbin/ifconfig. Then from this ip address and mask the subnet is calculated which is 192.168.1.0/24

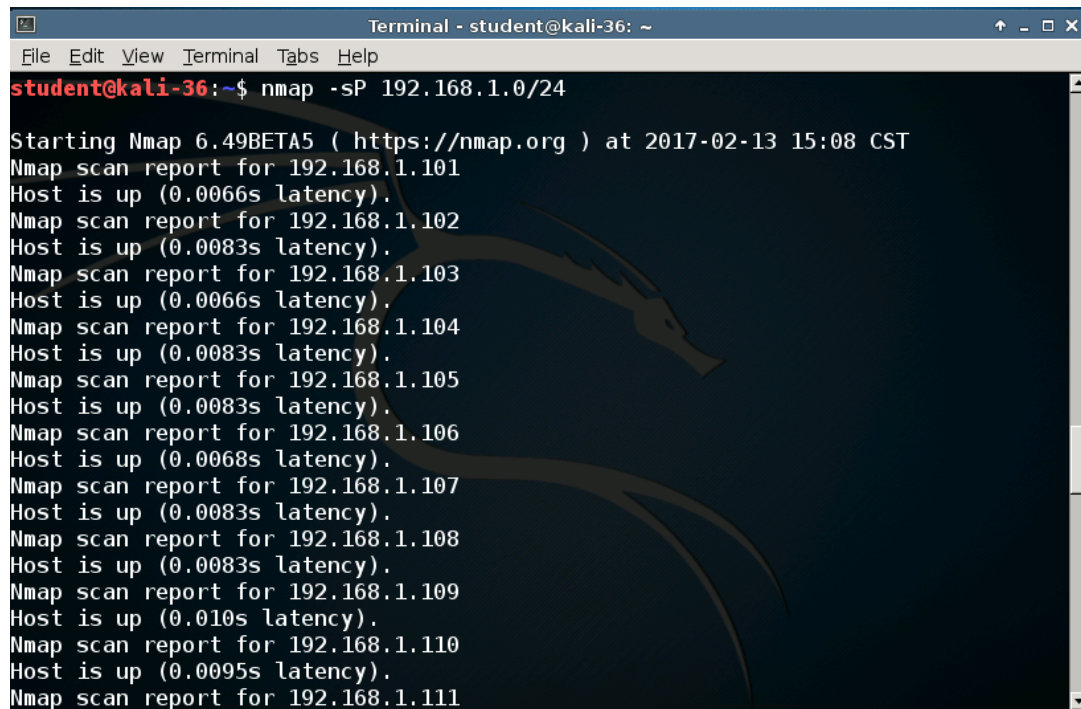


```
student@kali-36:~$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:14:4f:78
          inet addr:192.168.1.136  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe14:4f78/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44318 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39764 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3624611 (3.4 MiB)  TX bytes:264086025 (251.8 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 B)  TX bytes:480 (480.0 B)

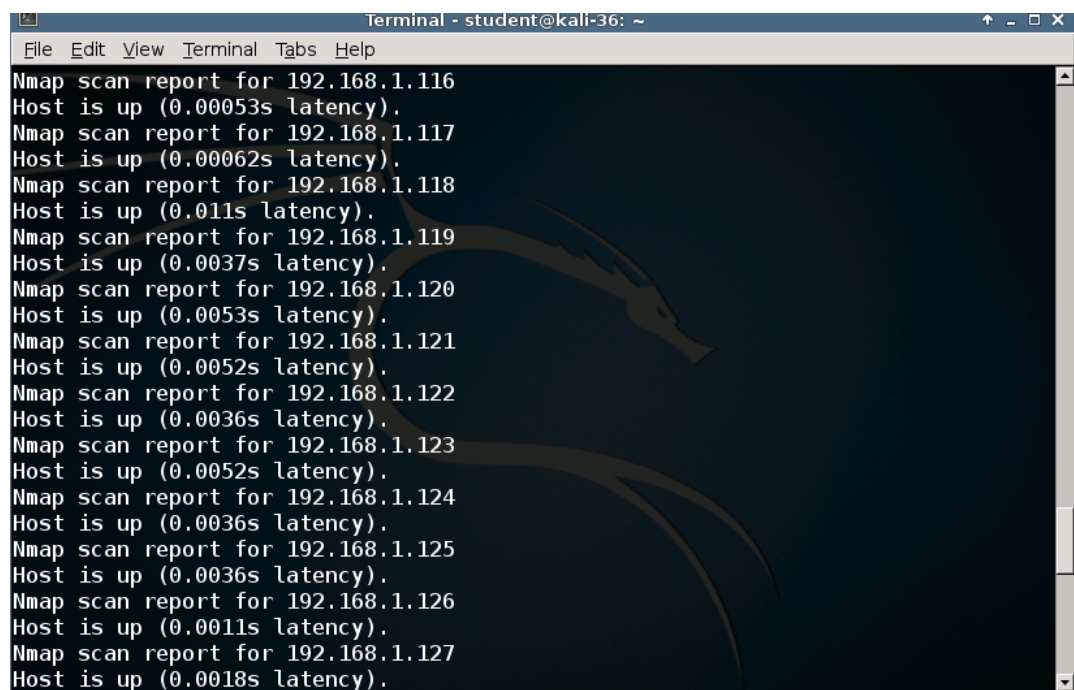
student@kali-36:~$
```

- After getting the subnet mask the command `nmap -sP 192.168.1.0/24` is used to get the live system that are reachable to the system.



```
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
student@kali-36:~$ nmap -sP 192.168.1.0/24

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2017-02-13 15:08 CST
Nmap scan report for 192.168.1.101
Host is up (0.0066s latency).
Nmap scan report for 192.168.1.102
Host is up (0.0083s latency).
Nmap scan report for 192.168.1.103
Host is up (0.0066s latency).
Nmap scan report for 192.168.1.104
Host is up (0.0083s latency).
Nmap scan report for 192.168.1.105
Host is up (0.0083s latency).
Nmap scan report for 192.168.1.106
Host is up (0.0068s latency).
Nmap scan report for 192.168.1.107
Host is up (0.0083s latency).
Nmap scan report for 192.168.1.108
Host is up (0.0083s latency).
Nmap scan report for 192.168.1.109
Host is up (0.010s latency).
Nmap scan report for 192.168.1.110
Host is up (0.0095s latency).
Nmap scan report for 192.168.1.111
```



```
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
Nmap scan report for 192.168.1.116
Host is up (0.00053s latency).
Nmap scan report for 192.168.1.117
Host is up (0.00062s latency).
Nmap scan report for 192.168.1.118
Host is up (0.011s latency).
Nmap scan report for 192.168.1.119
Host is up (0.0037s latency).
Nmap scan report for 192.168.1.120
Host is up (0.0053s latency).
Nmap scan report for 192.168.1.121
Host is up (0.0052s latency).
Nmap scan report for 192.168.1.122
Host is up (0.0036s latency).
Nmap scan report for 192.168.1.123
Host is up (0.0052s latency).
Nmap scan report for 192.168.1.124
Host is up (0.0036s latency).
Nmap scan report for 192.168.1.125
Host is up (0.0036s latency).
Nmap scan report for 192.168.1.126
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.127
Host is up (0.0018s latency).
```



```
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
Nmap scan report for 192.168.1.127
Host is up (0.0018s latency).
Nmap scan report for 192.168.1.128
Host is up (0.0034s latency).
Nmap scan report for 192.168.1.129
Host is up (0.0050s latency).
Nmap scan report for 192.168.1.130
Host is up (0.0050s latency).
Nmap scan report for 192.168.1.131
Host is up (0.0030s latency).
Nmap scan report for 192.168.1.132
Host is up (0.0050s latency).
Nmap scan report for 192.168.1.133
Host is up (0.0033s latency).
Nmap scan report for 192.168.1.134
Host is up (0.0016s latency).
Nmap scan report for 192.168.1.135
Host is up (0.0016s latency).
Nmap scan report for 192.168.1.136
Host is up (0.00041s latency).
Nmap scan report for 192.168.1.137
Host is up (0.0047s latency).
Nmap scan report for 192.168.1.138
Host is up (0.0047s latency).
```

```
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
Nmap scan report for 192.168.1.133
Host is up (0.0033s latency).
Nmap scan report for 192.168.1.134
Host is up (0.0016s latency).
Nmap scan report for 192.168.1.135
Host is up (0.0016s latency).
Nmap scan report for 192.168.1.136
Host is up (0.00041s latency).
Nmap scan report for 192.168.1.137
Host is up (0.0047s latency).
Nmap scan report for 192.168.1.138
Host is up (0.0047s latency).
Nmap scan report for 192.168.1.139
Host is up (0.0046s latency).
Nmap scan report for 192.168.1.140
Host is up (0.0046s latency).
Nmap scan report for 192.168.1.141
Host is up (0.0046s latency).
Nmap scan report for 192.168.1.142
Host is up (0.0030s latency).
Nmap scan report for 192.168.1.143
Host is up (0.0030s latency).
Nmap done: 256 IP addresses (43 hosts up) scanned in 2.02 seconds
student@kali-36:~$
```

## 2. List all the **open** ports available on the system 192.168.2.77 (1 point)

Ans:

**Command:** nmap -v -sT 192.168.2.77

**Output:**

```
Applications Menu [Terminal - student@k... Terminal - student@kal... 15:19 Student
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
student@kali-36:~$ nmap -v -sT 192.168.2.77

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2017-02-13 15:15 CST
Initiating Ping Scan at 15:15
Scanning 192.168.2.77 [2 ports]
Completed Ping Scan at 15:15, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:15
Completed Parallel DNS resolution of 1 host. at 15:15, 0.02s elapsed
Initiating Connect Scan at 15:15
Scanning 192.168.2.77 [1000 ports]
Discovered open port 5900/tcp on 192.168.2.77
Discovered open port 139/tcp on 192.168.2.77
Discovered open port 80/tcp on 192.168.2.77
Discovered open port 3306/tcp on 192.168.2.77
Discovered open port 22/tcp on 192.168.2.77
Discovered open port 111/tcp on 192.168.2.77
Discovered open port 445/tcp on 192.168.2.77
Discovered open port 25/tcp on 192.168.2.77
Discovered open port 53/tcp on 192.168.2.77
Discovered open port 21/tcp on 192.168.2.77
Discovered open port 23/tcp on 192.168.2.77
Discovered open port 8180/tcp on 192.168.2.77
Discovered open port 8009/tcp on 192.168.2.77
Discovered open port 2049/tcp on 192.168.2.77
Discovered open port 1524/tcp on 192.168.2.77
Discovered open port 5432/tcp on 192.168.2.77
Discovered open port 514/tcp on 192.168.2.77
Discovered open port 512/tcp on 192.168.2.77
Discovered open port 513/tcp on 192.168.2.77
Discovered open port 6667/tcp on 192.168.2.77
Discovered open port 6000/tcp on 192.168.2.77
Discovered open port 1099/tcp on 192.168.2.77
Discovered open port 2121/tcp on 192.168.2.77
Completed Connect Scan at 15:15, 0.10s elapsed (1000 total ports)
```

```
Applications Menu [Terminal - student@k... Terminal - student@kal... 15:19 Student
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
Discovered open port 1099/tcp on 192.168.2.77
Discovered open port 2121/tcp on 192.168.2.77
Completed Connect Scan at 15:15, 0.10s elapsed (1000 total ports)
Nmap scan report for 192.168.2.77
Host is up (0.0039s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

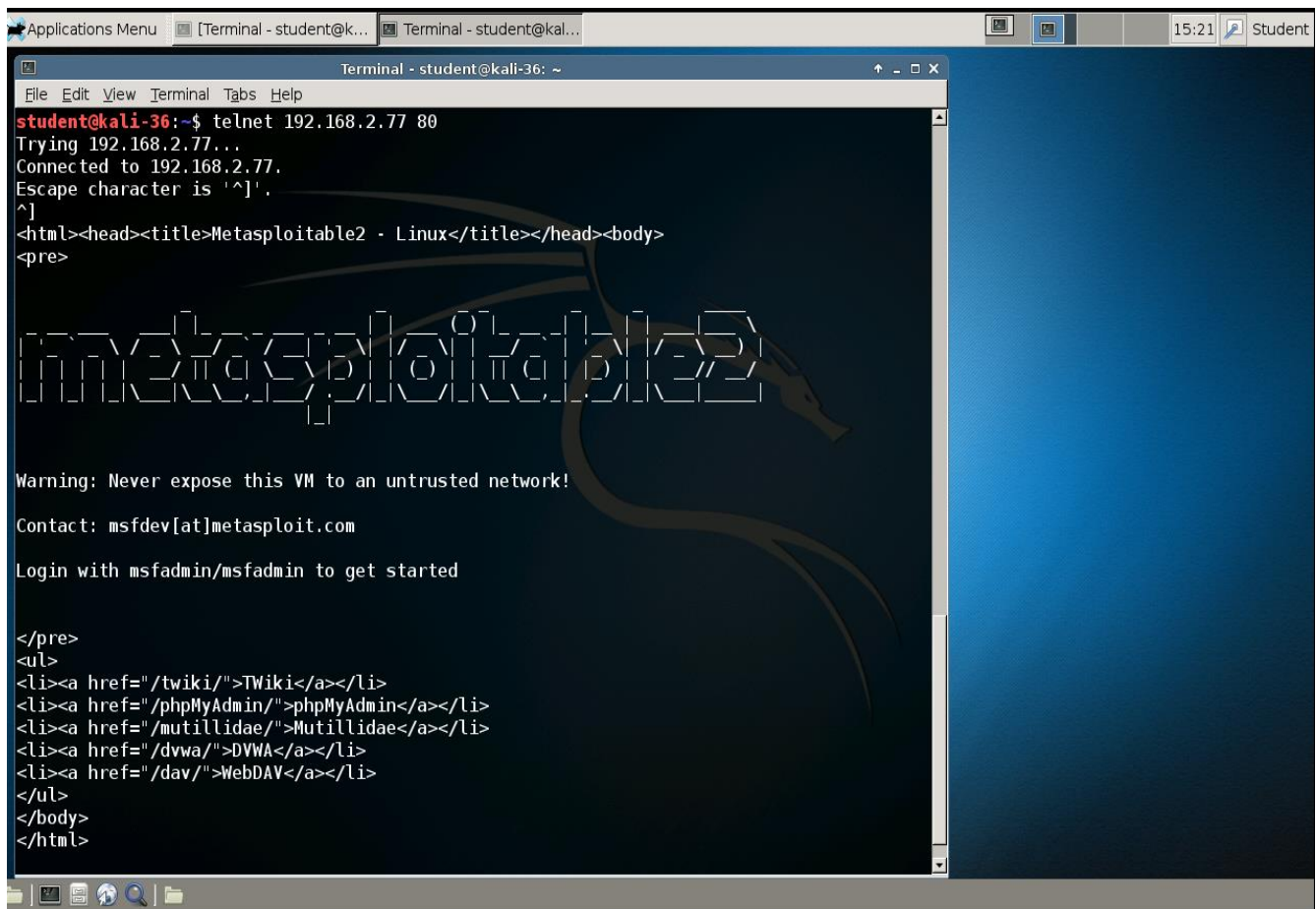
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
student@kali-36:~$
```

3. What is the **Operating System name** on the system **192.168.2.77**? (Use banner grabbing method – telnet with port 80) (1 point)

Ans:

**Command:** telnet 192.168.2.77 80

**Output:** OS Name is **metasploitable2**



```
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
student@kali-36:~$ telnet 192.168.2.77 80
Trying 192.168.2.77...
Connected to 192.168.2.77.
Escape character is '^]'.
^]
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

  _____
 |  _   _  |
 | | | | | |
 | |_| | | |
 |  _  | | |
 | | | | | |
 |_|_|_|_|_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```



4. What is the FTP **server version** on the **system 192.168.2.77**? ( Use banner grabbing method – telnet with port 21) (1 point)

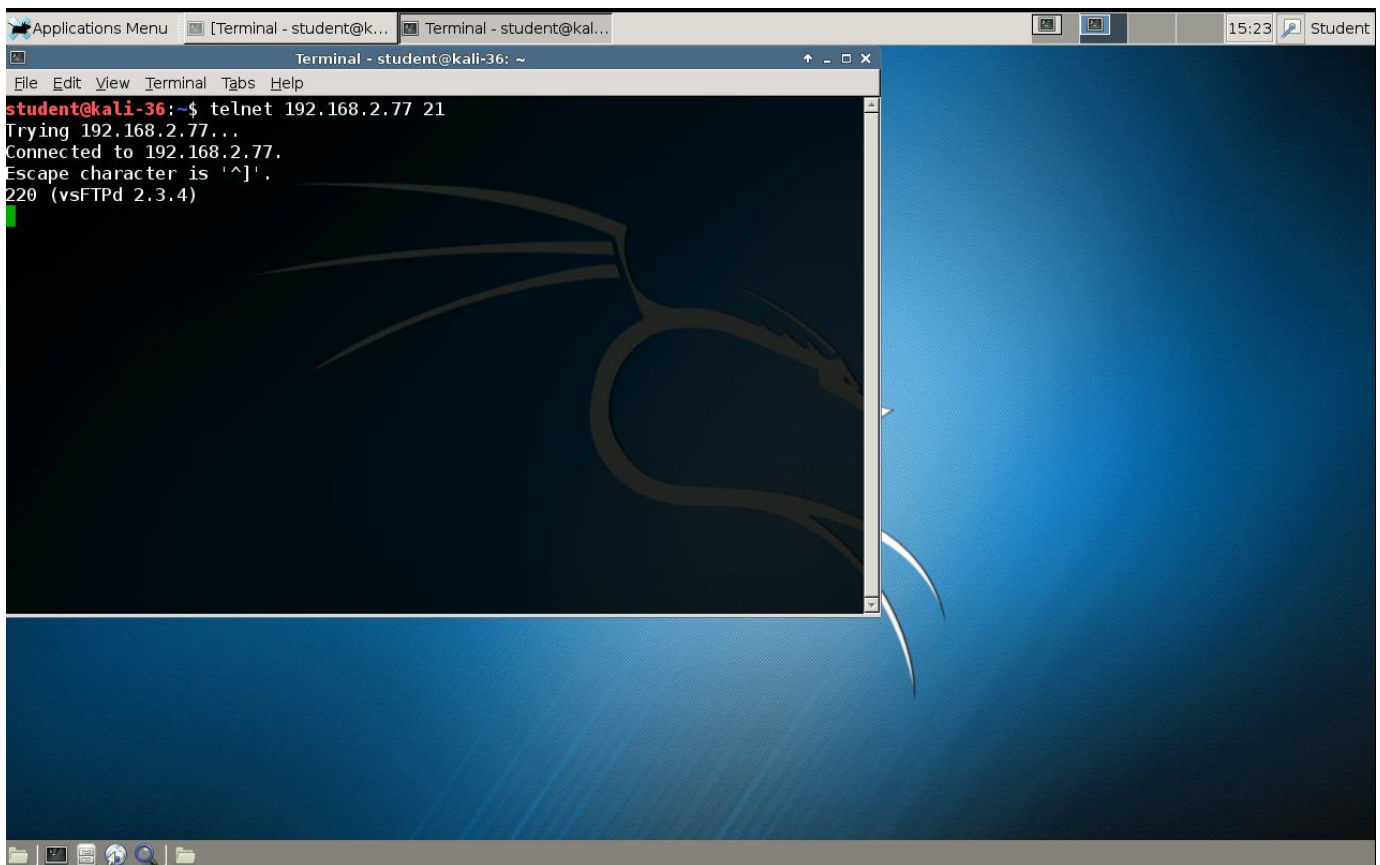
Ans:

**Command:** telnet 192.168.2.77 21

**Output:**

**Service Name:** vsFTPD

**Version:** 2.3.4



```
Applications Menu [Terminal - student@k... Terminal - student@kal... 15:23 Student
Terminal - student@kali-36: ~
File Edit View Terminal Tabs Help
student@kali-36:~$ telnet 192.168.2.77 21
Trying 192.168.2.77...
Connected to 192.168.2.77.
Escape character is '^]'.
220 (vsFTPD 2.3.4)
```