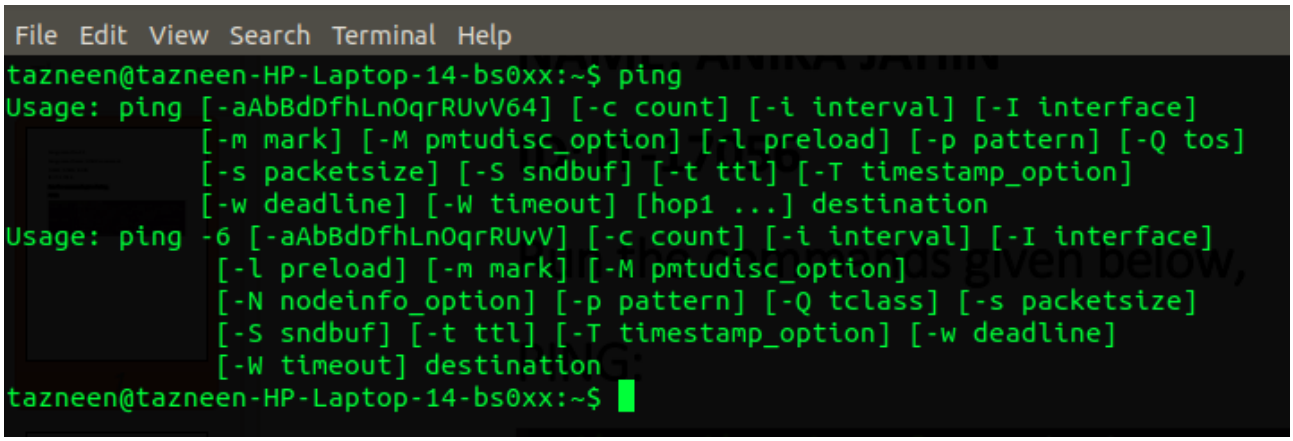
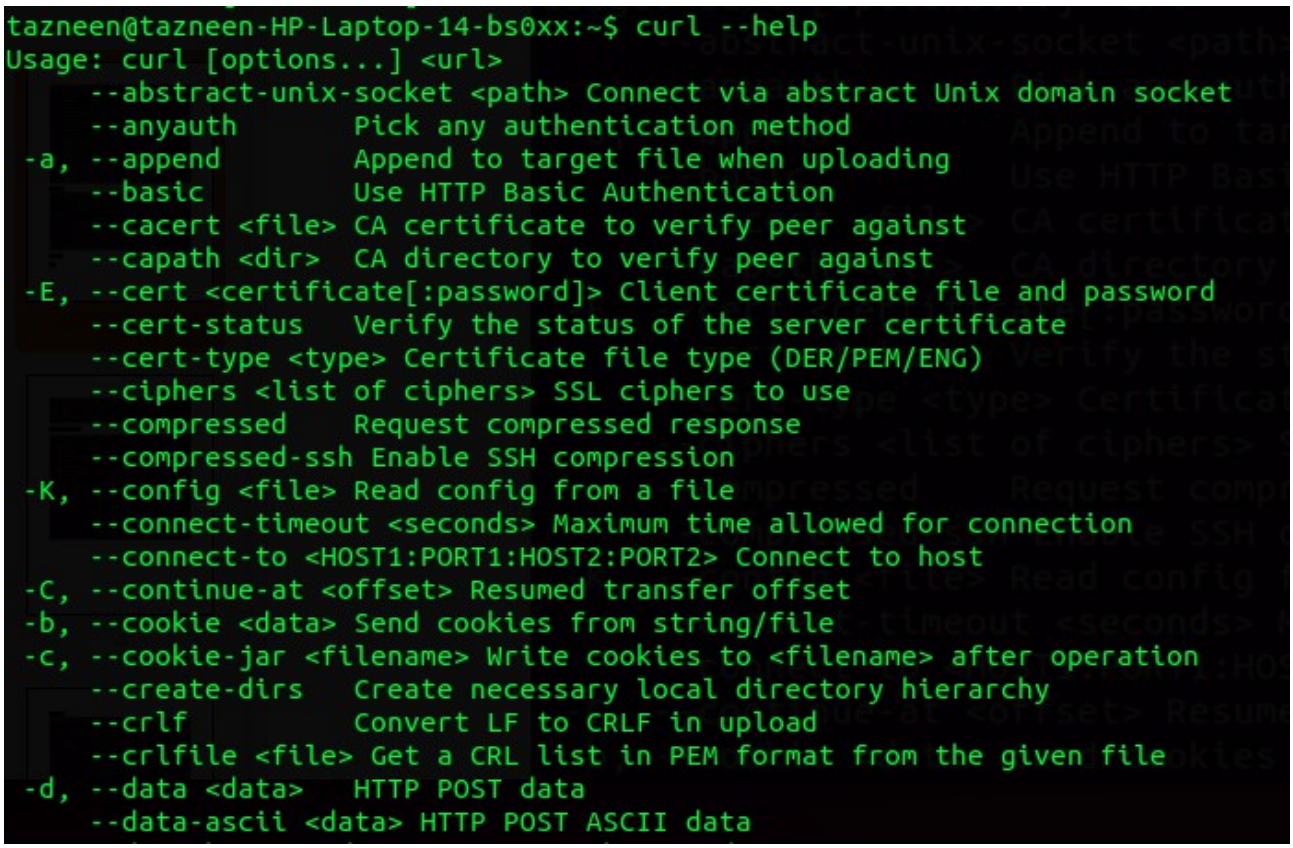
Assignment No: 01
Assignment Name: LINUX commands.
NAME: Tazneen Akter
ID: IT-18056
Run the commands given below:

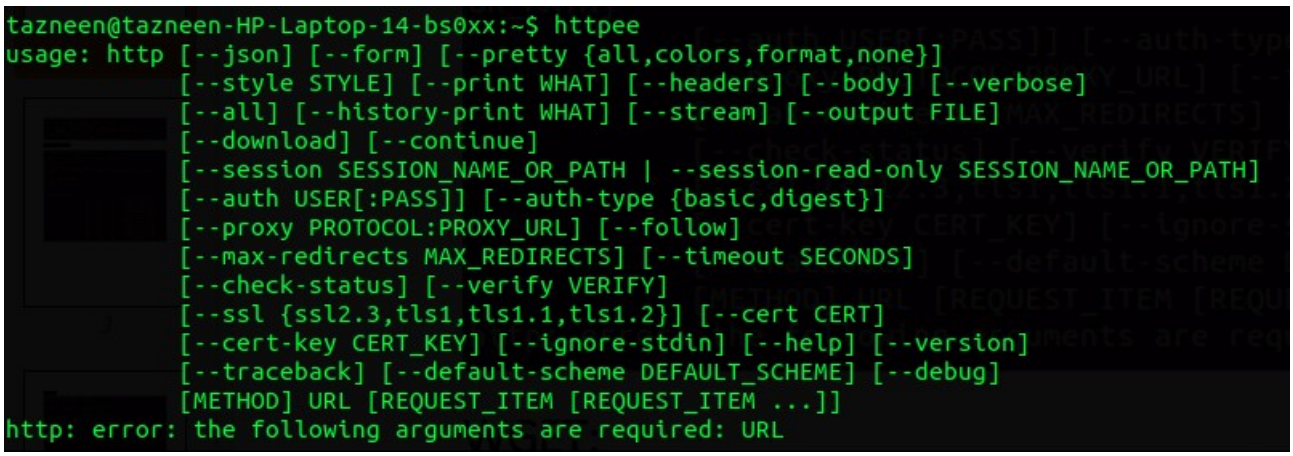
PING: The **ping** command is one of the most used tools for troubleshooting, testing, and diagnosing network connectivity issues. Ping works by sending one or more ICMP (Internet Control Message Protocol) Echo Request packages to a specified destination IP on the network and waits for a reply.



CURL: curl is a *command* line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE). *curl* is powered by Libcurl. This tool is preferred for automation, since it is designed to work without user interaction.



HTTPIE: HTTPie – A Modern HTTP Client Similar to Curl and Wget commands. HTTPie (pronounced aitch-tee-tee-pie) is a cURL-like, modern, user-friendly, and cross-platform command line HTTP client written in Python. It is designed to make CLI interaction with web services easy and as user-friendly as possible.



WGET: wget is a free utility for non-interactive download of files from the web.It
supports HTTP,HTTPS, and FTP protocols.

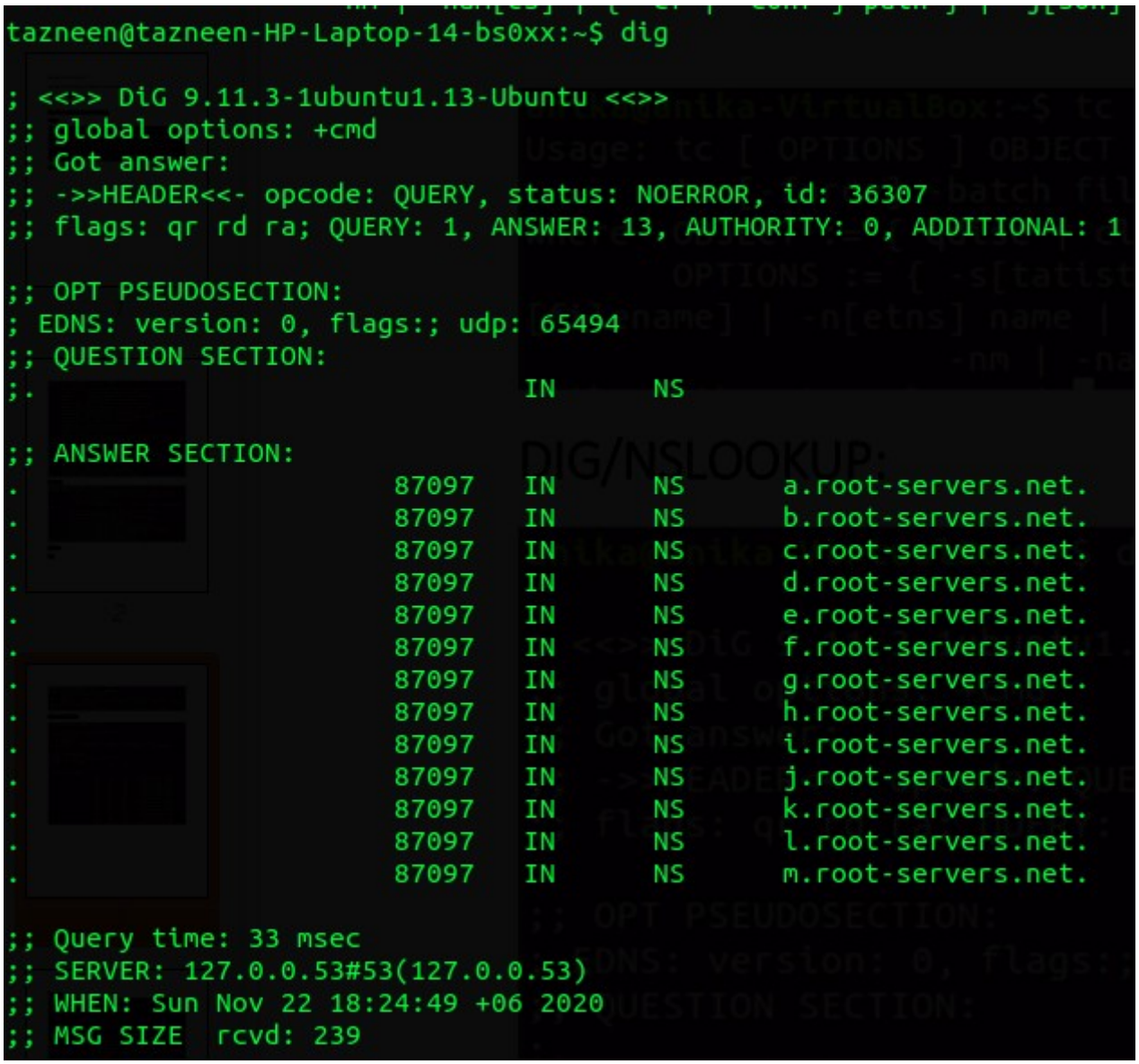
```
File  Edit  View  Search  Terminal  Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ wget
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try `wget --help' for more options.
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ wget --help
GNU Wget 1.19.4, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version                   display the version of Wget and exit
  -h,  --help                      print this help
  -b,  --background                go to background after startup
  -e,  --execute=COMMAND           execute a `.wgetrc'-style command

Logging and input file:
  -o,  --output-file=FILE          log messages to FILE
  -a,  --append-output=FILE        append messages to FILE
  -d,  --debug                     print lots of debugging information
  -q,  --quiet                     quiet (no output)
  -v,  --verbose                   be verbose (this is the default)
  -nv, --no-verbose                turn off verboseness, without being quiet
       --report-speed=TYPE         output bandwidth as TYPE.  TYPE can be bits
  -i,  --input-file=FILE           download URLs found in local or external FILE
  -F,  --force-html                treat input file as HTML
  -B,  --base=URL                  resolves HTML input-file links (-i -F)
                                     relative to URL
       --config=FILE               specify config file to use
       --no-config                 do not read any config file
       --rejected-log=FILE         log reasons for URL rejection to FILE

Download:
  -t,  --tries=NUMBER              set number of retries to NUMBER (0 unlimits)
```

TC: Tc is used to configure Traffic Control in the Linux kernel. Traffic Control consists of the following: SHAPING When traffic is shaped, its rate of transmission is under control. Shaping may be more than lowering the available bandwidth - it is also used to smooth out bursts in traffic for better network behaviour.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ tc
Usage: tc [ OPTIONS ] OBJECT { COMMAND | help }
       tc [-force] -batch filename
where  OBJECT := { qdisc | class | filter | action | monitor | exec }
       OPTIONS := { -s[tatistics] | -d[etails] | -r[aw] | -p[retty] | -b[atch] [filename] | -n[etns] name |
                    -nm | -nam[es] | { -cf | -conf } path } | -j[son]
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

Terminal

DIG/NSLOOKUP: Dig (Domain Information Groper) is a command line utility that performs DNS lookup by querying name servers and displaying the result to you. In this tutorial, you'll find all the basic uses of the command you should know in the Linux operating system.



WHOIS: In Linux, the **whois command** line utility is a **WHOIS** client for communicating with the **WHOIS** server (or database host) which listen to requests on the well-known port number 43, which stores and delivers database content in a human-readable format.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-H                     hide legal disclaimers
     --verbose         explain what is being done
     --help            display this help and exit
     --version         output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                     only primary keys are returned
-r                     turn off recursive look-ups for contact information
-R                     force to show local copy of the domain object even
                       if it contains referral
-a                     also search all the mirrored databases
-s SOURCE[,SOURCE]...  search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

SSH: ssh command provides a secure encrypted connection between two hosts over an insecure network. This connection can also be used for terminal access, file transfers, and for tunneling other applications. Graphical X11 applications can also be run securely over **SSH** from a remote location.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file]
           [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           [user@]hostname [command]
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

SCP: scp (secure copy) command in Linux system is used to copy file(s) between servers in a secure way. The SCP command or secure copy allows secure transferring of files in between the local host and the remote host or between two remote hosts.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ scp
usage: scp [-346BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-l limit] [-o ssh_option] [-P port] [-S program]
           [[user@]host1:]file1 ... [[user@]host2:]file2
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

RSYNC: rsync is a fast and versatile command-line utility for synchronizing files and directories between two locations over a remote shell, or from/to a remote **Rsync** daemon. It provides fast incremental file transfer by transferring only the differences between the source and the destination.

```
File  Edit  View  Search  Terminal  Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ rsync
rsync  version 3.1.2  protocol version 31
Copyright (C) 1996-2015 by Andrew Tridgell, Wayne Davison, and others.
Web site: http://rsync.samba.org/
Capabilities:
    64-bit files, 64-bit inums, 64-bit timestamps, 64-bit long ints,
    socketpairs, hardlinks, symlinks, IPv6, batchfiles, inplace,
    append, ACLs, xattrs, iconv, symtimes, prealloc

rsync comes with ABSOLUTELY NO WARRANTY.  This is free software, and you
are welcome to redistribute it under certain conditions.  See the GNU
General Public Licence for details.

rsync is a file transfer program capable of efficient remote update
via a fast differencing algorithm.

Usage: rsync [OPTION]... SRC [SRC]... DEST
  or   rsync [OPTION]... SRC [SRC]... [USER@]HOST:DEST
  or   rsync [OPTION]... SRC [SRC]... [USER@]HOST::DEST
  or   rsync [OPTION]... SRC [SRC]... rsync://[USER@]HOST[:PORT]/DEST
  or   rsync [OPTION]... [USER@]HOST:SRC [DEST]
  or   rsync [OPTION]... [USER@]HOST::SRC [DEST]
  or   rsync [OPTION]... rsync://[USER@]HOST[:PORT]/SRC [DEST]
The ':' usages connect via remote shell, while '::' & 'rsync://' usages connect
to an rsync daemon, and require SRC or DEST to start with a module name.

Options
 -v, --verbose               increase verbosity
     --info=FLAGS            fine-grained informational verbosity
     --debug=FLAGS           fine-grained debug verbosity
     --msgs2stderr           special output handling for debugging
 -q, --quiet                 suppress non-error messages
     --no-motd               suppress daemon-mode MOTD (see manpage caveat)
 -c, --checksum              skip based on checksum, not mod-time & size
 -a, --archive               archive mode; equals -rlptgoD (no -H,-A,-X)
```

NGREP: *ngrep* (network grep) is a network packet analyzer written by Jordan Ritter. It has a *command*-line interface, and relies upon the pcap library and the ... it works in many UNIX-like operating systems: *Linux*, Solaris, illumos, BSD, AIX.

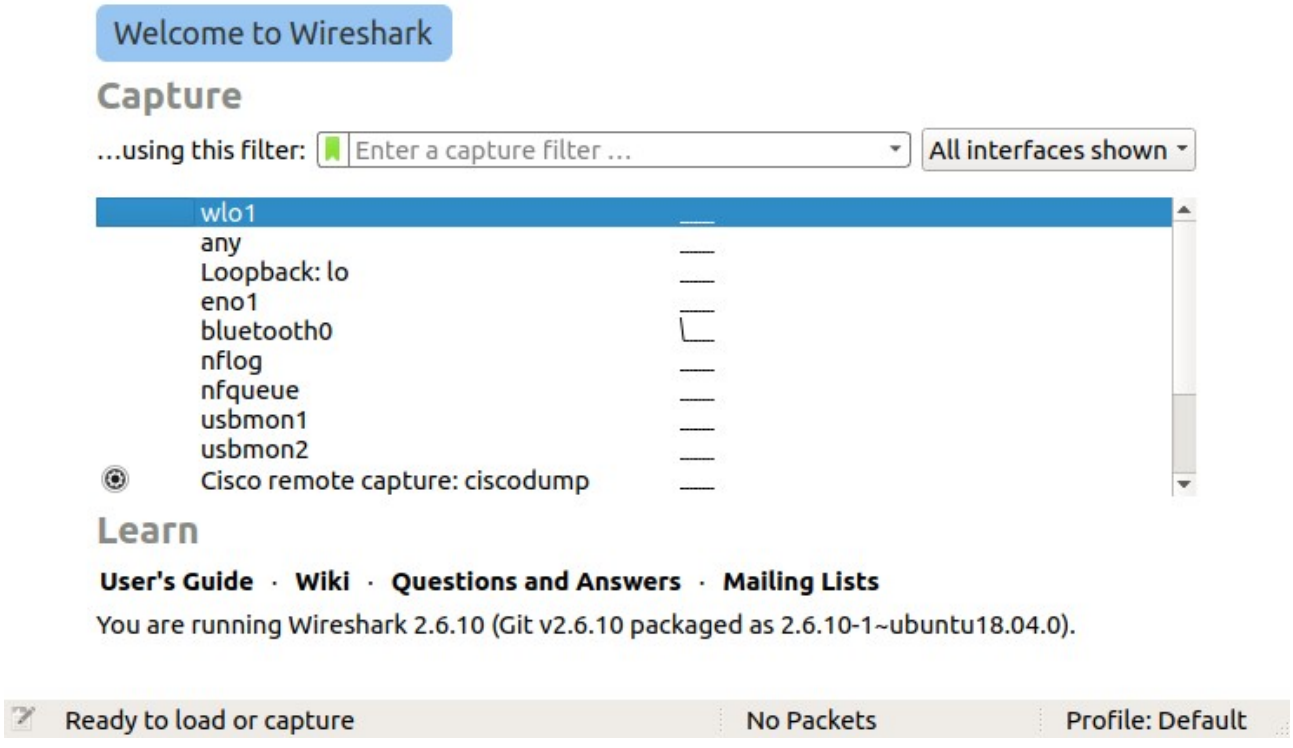
```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ngrep
wlo1: You don't have permission to capture on that device (socket: Operation not permitted): Operation not permitted
exit
0 received, 0 matched
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

TCPDUMP: tcpdump is a most powerful and widely used command-line packets sniffer or package analyzer tool which is used to capture or filter TCP/IP packets that received or transferred over a network on a specific *interface*. It is available under most of the *Linux*/*Unix* based operating systems.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ tcpdump
tcpdump: wlo1: You don't have permission to capture on that device
(socket: Operation not permitted)
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

WIRESHARK:

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlo1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
192.168.0.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```



IFCONFIG: stands for "interface configuration." It is used to view and change the configuration of the network interfaces on your system.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 48:ba:4e:5a:67:dd  txqueuelen 1000  (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

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 2740  bytes 257887 (257.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2740  bytes 257887 (257.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.103  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::e326:748:8c28:e207  prefixlen 64  scopeid 0x20<link>
        ether 28:c6:3f:25:b7:19  txqueuelen 1000  (Ethernet)
        RX packets 114735  bytes 122694773 (122.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86326  bytes 9721514 (9.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ROUTE: route command in Linux is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlo1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
192.168.0.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

IP: The **ip** command is a Linux net-tool for system and network administrators. IP stands for Internet Protocol and as the name suggests, the tool is used for configuring network interfaces. Older Linux distributions used the **ifconfig** command, which operates similarly.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
                   netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila |
                   vrf | sr }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -iec |
                    -f[amily] { inet | inet6 | ipx | dnet | mpls | bridge | link } |
                    -4 | -6 | -I | -D | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                    -rc[vbuf] [size] | -n[etns] name | -a[ll] | -c[olor]}
```

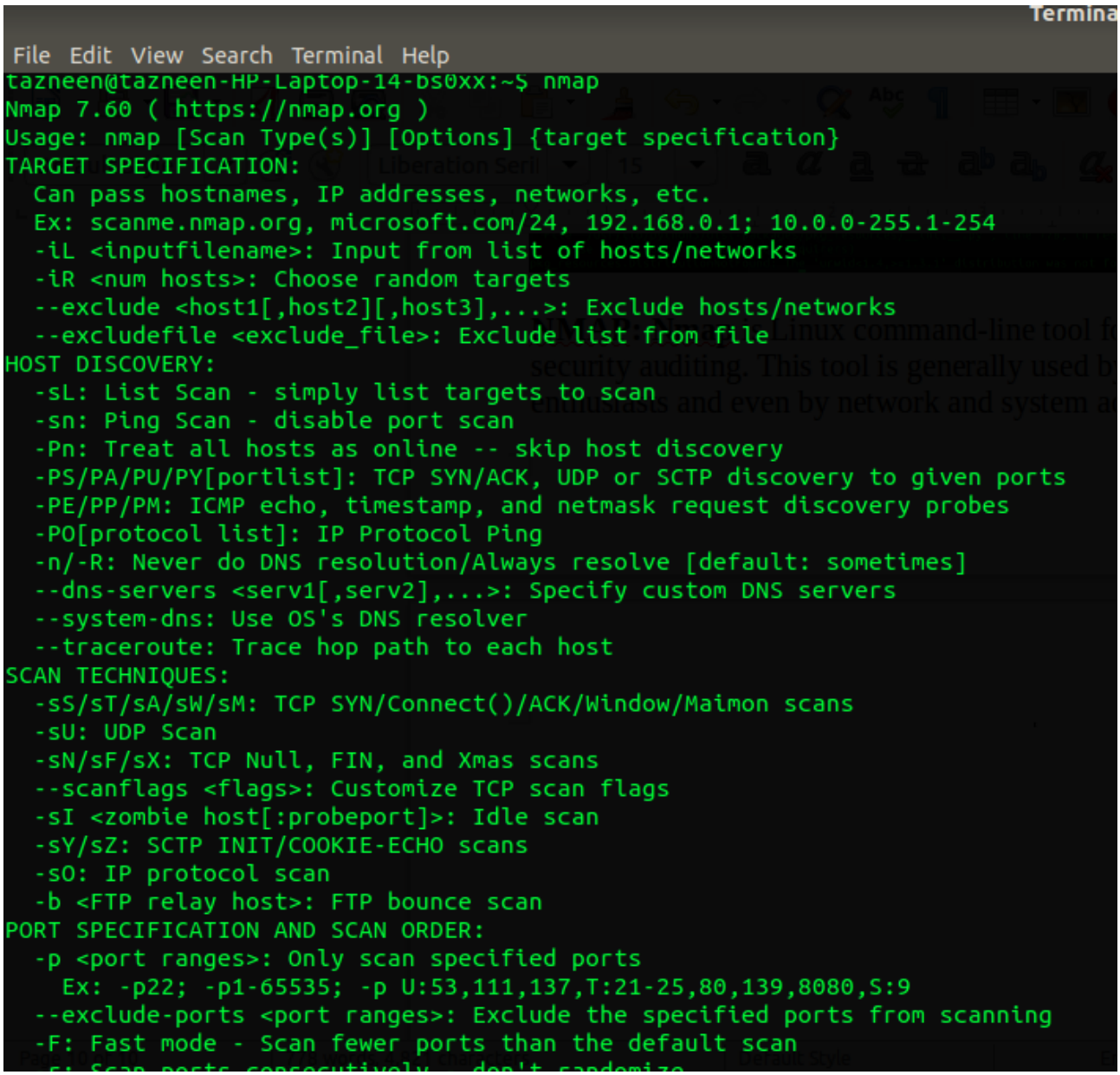
ARP: arp command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   50:d4:f7:0b:6e:50   C                     wlo1
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

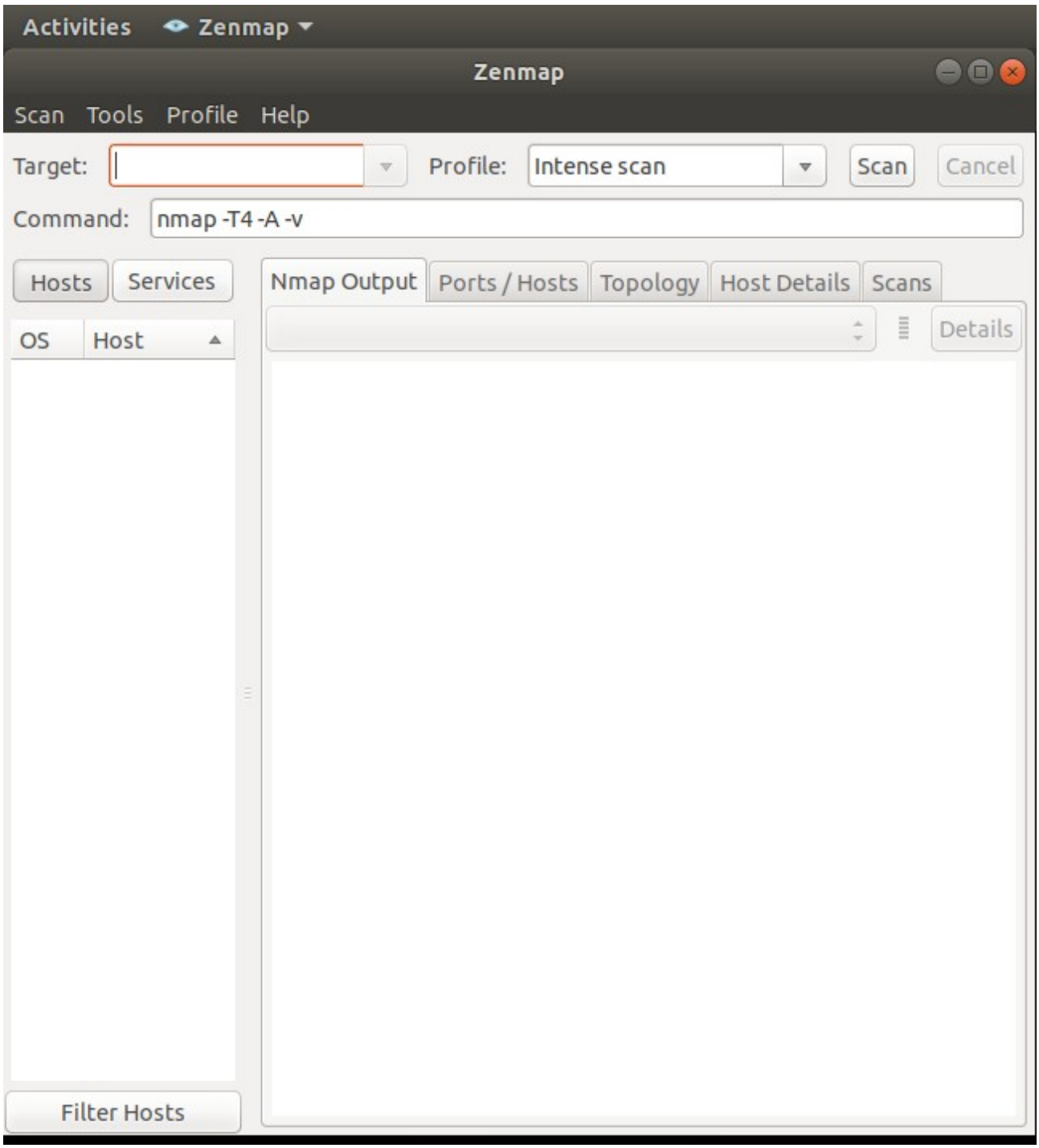
MITMPROXY: mitmproxy is an SSL-capable man-in-the-middle HTTP proxy. It provides a console interface that allows traffic flows to be inspected and edited on the fly. Also shipped is mitmdump, the command-line version of **mitmproxy**, with the same functionality but without the frills. Think tcpdump for HTTP.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ mitmproxy
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 574, in _build_master
    ws.require(__requires__)
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 892, in require
    needed = self.resolve(parse_requirements(requirements))
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 783, in resolve
    raise VersionConflict(dist, req).with_context(dependent_req)
pkg_resources.ContextualVersionConflict: (urwid 2.0.1 (/usr/lib/python3/dist-packages), Requirement.parse('urwid<1.4,>=1.3.1'), {'mitmproxy'})

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/bin/mitmproxy", line 6, in <module>
    from pkg_resources import load_entry_point
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 3088, in <module>
    @_call_aside
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 3072, in _call_aside
    f(*args, **kwargs)
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 3101, in _initialize_master_working_set
    working_set = WorkingSet._build_master()
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 576, in _build_master
    return cls._build_from_requirements(__requires__)
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 589, in _build_from_requirements
    dists = ws.resolve(reqs, Environment())
  File "/usr/lib/python3/dist-packages/pkg_resources/__init__.py", line 778, in resolve
    raise DistributionNotFound(req, requirers)
pkg_resources.DistributionNotFound: The 'urwid<1.4,>=1.3.1' distribution was not found and is required by mitmproxy
```

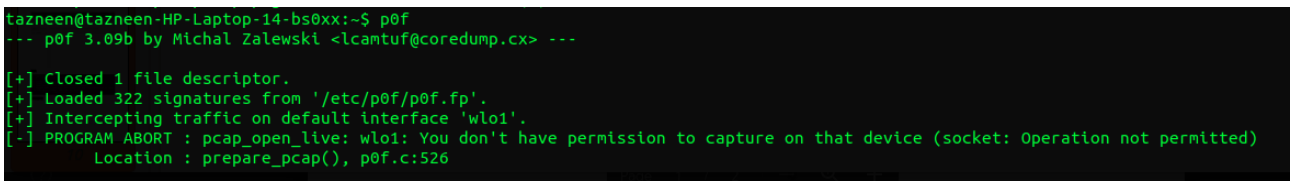
NMAP: Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators.


Termina
File Edit View Search Terminal Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ nmap
Nmap 7.60 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan

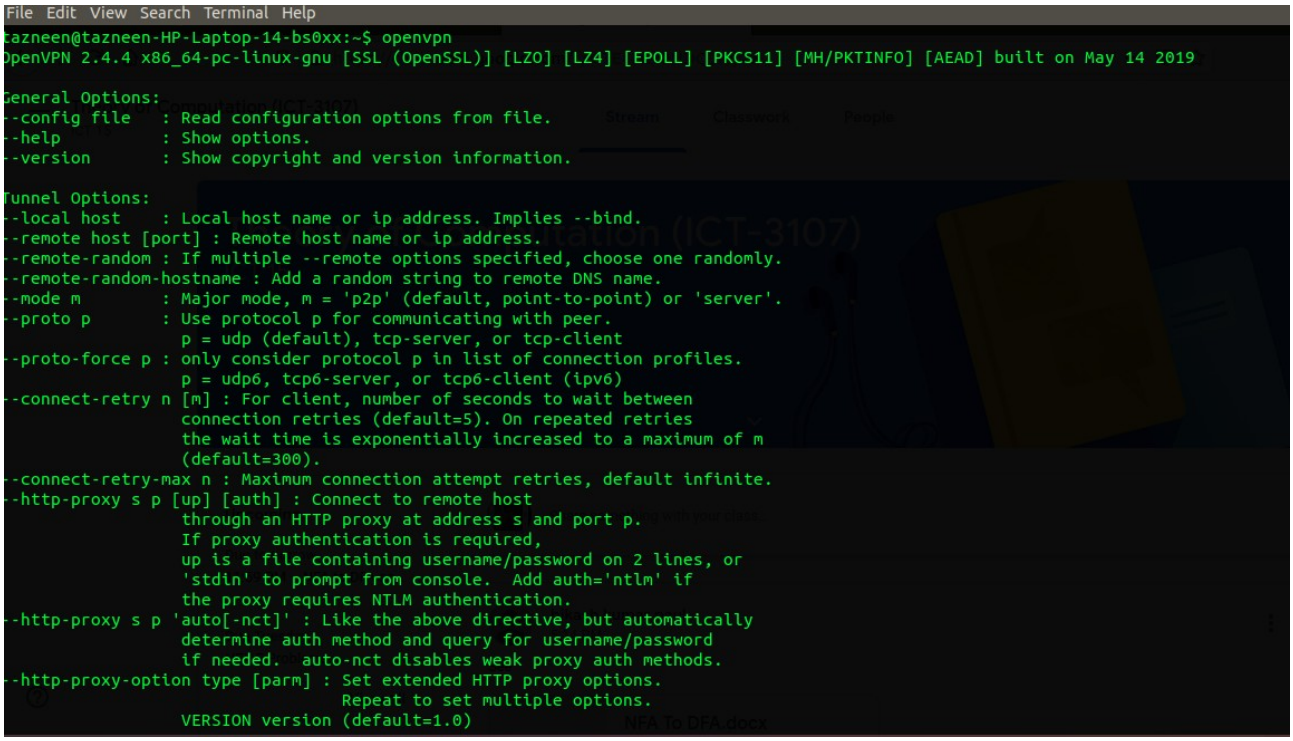
ZENMAP:



P0F: p0f is a passive TCP/IP stack fingerprinting tool. p0f can attempt to identify the system running on machines that send network traffic to the box it is running on, or to a machine that shares a medium with the machine it is running on. p0f can also assist in analysing other aspects of the remote system.

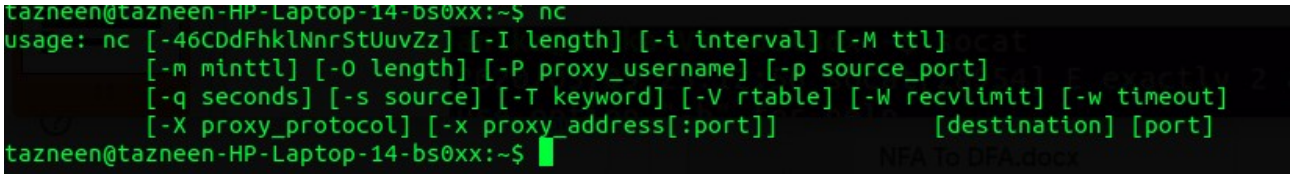


OPENVPN:

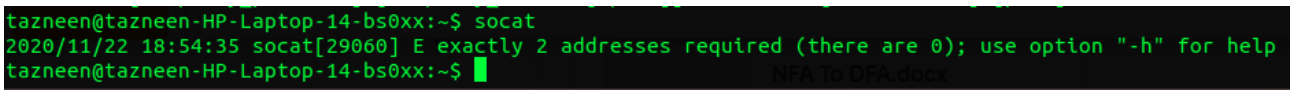


WIREGUARD:

NC: ncat or **nc** is networking utility with functionality similar to cat command but for network. It is a general purpose CLI tool for reading, writing, redirecting data across a network. It is designed to be a reliable back-end tool that can be used with scripts or other programs.



SOCAT: Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them.



TELNET: In Linux, the **telnet command** is used to create a remote connection with a system over a TCP/IP network. It allows us to administrate other systems by the terminal. We can run a program to conduct administration. It uses a **TELNET** protocol.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ telnet
telnet>
```

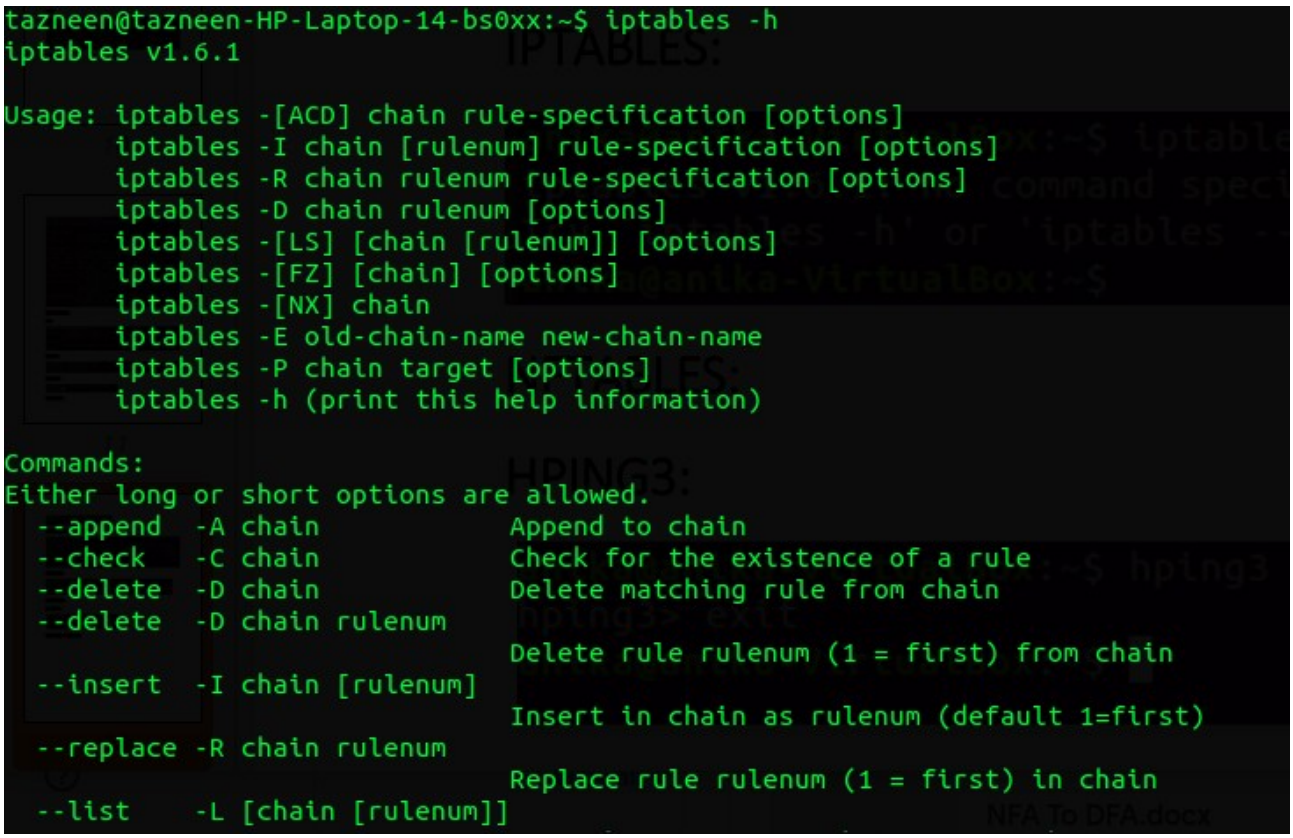
FTP/SFTP: FTP (File Transfer Protocol) is a standard network protocol used to transfer files to and from a remote network. ... However, the **ftp** command is useful when you work on a server without GUI and you want to transfer files over **FTP** to or from a remote server.

```
File  Edit  View  Search  Terminal  Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ftp
ftp>
```

NETSTAT/SS/LSOF/FUSER: The **netstat** command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information. The most frequently used options for determining network status are: s , r , and i .

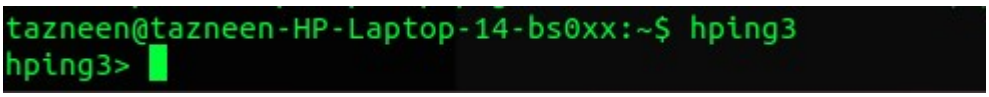
```
File  Edit  View  Search  Terminal  Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlo1
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlo1
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 wlo1
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

IPTABLES: iptables is a command line interface used to set up and maintain tables for the Netfilter firewall for IPv4, included in the Linux kernel. The firewall matches packets with rules defined in these tables and then takes the specified action on a possible match. Tables is the name for a set of chains.

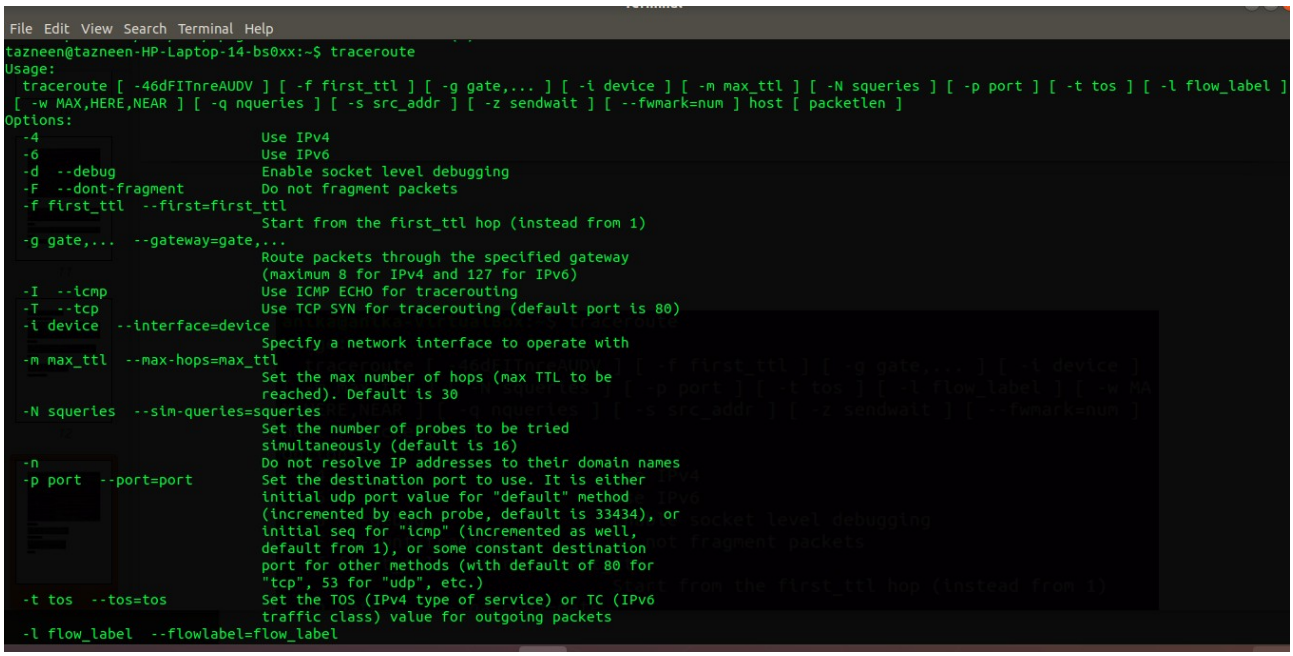


NFTABLES:

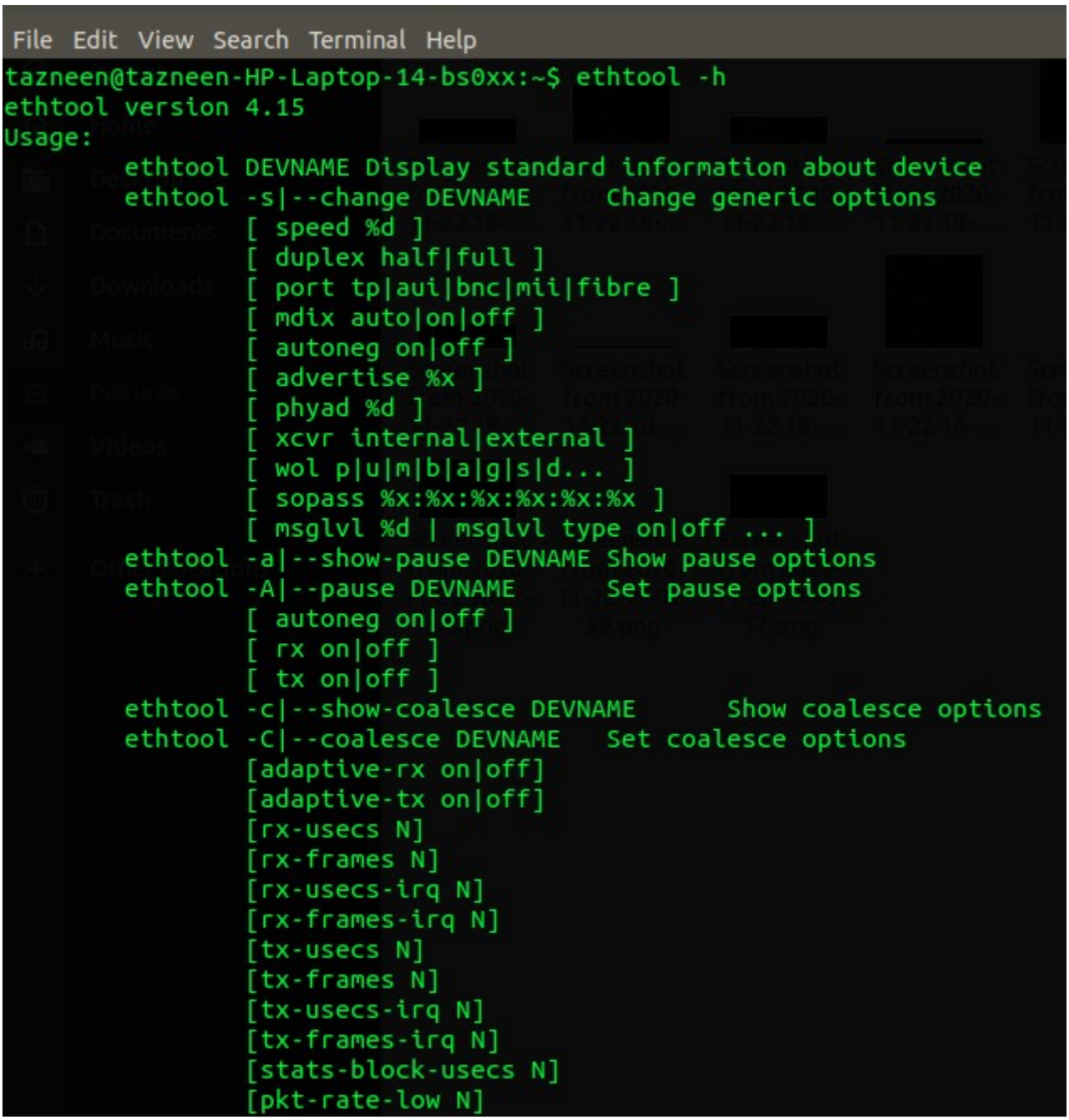
HPING3: hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.



TRACEROUTE/MTR: traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.



ETHTOOL: The **ethtool** command is used to display/change Ethernet adapter settings. You can change network card speed, auto-negotiation, wake on LAN setting, duplex mode using this tool in Linux.



IW/IWCONFIG: iwconfig command in Linux is like ifconfig command, in the sense it works with kernel-resident network interface but it is dedicated to wireless networking interfaces only. It is used to set the parameters of the network interface that are particular to the wireless operation like SSID, frequency etc.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ iwconfig
lo        no wireless extensions.

wlo1      IEEE 802.11  ESSID:"Raisa"
          Mode:Managed  Frequency:2.417 GHz  Access Point: 50:D4:F7:0B:6E:50
          Bit Rate=60 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=30/70  Signal level=-80 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:202   Missed beacon:0

eno1      no wireless extensions.
```

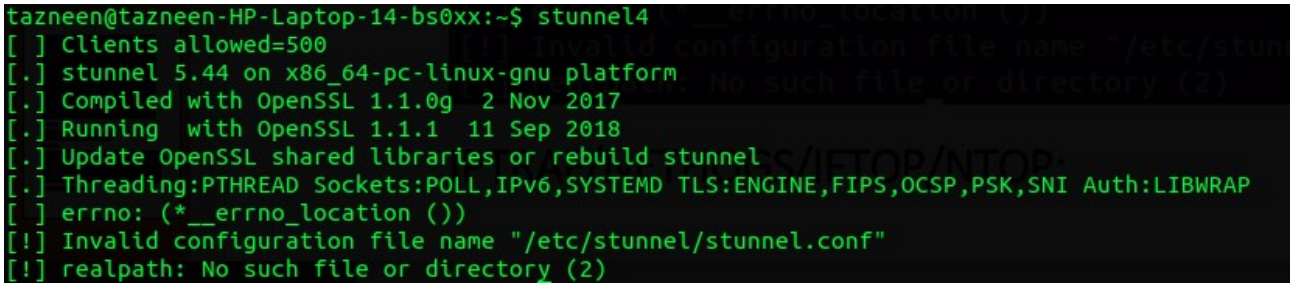
SYSCTL: The **sysctl command** reads the information from the /proc/sys directory. /proc/sys is a virtual directory that contains file objects that can be used to view and set the current kernel parameters. You can also view a parameter value by displaying the content of the appropriate file.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ sysctl

Usage:
 sysctl [options] [variable[=value] ...]

Options:
  -a, --all            display all variables
  -A                   alias of -a
  -X                   alias of -a
      --deprecated     include deprecated parameters to listing
  -b, --binary         print value without new line
  -e, --ignore         ignore unknown variables errors
  -N, --names          print variable names without values
  -n, --values         print only values of a variables
  -p, --load[=<file>]  read values from file
  -f                   alias of -p
      --system         read values from all system directories
  -r, --pattern <expression>
                       select setting that match expression
  -q, --quiet          do not echo variable set
  -w, --write          enable writing a value to variable
  -o                   does nothing
  -x                   does nothing
  -d                   alias of -h

 -h, --help     display this help and exit
 -V, --version  output version information and exit
```

OPENSSL: OpenSSL is a versatile *command* line tool that can be used for a large variety of tasks ... This includes OpenSSL examples of generating private keys, certificate signing requests, and certificate *format* conversion.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ openssl
OpenSSL>
```

STUNNEL: Stunnel is an open-source multi-platform application used to provide a universal TLS/SSL tunneling service. **Stunnel** can be used to provide secure encrypted connections for clients or servers that do not speak TLS or SSL natively.



IPTRAF/NETHOGS/IFTOP/NTOP: The **iftop** command listens to network traffic on a named network interface, or on the first interface, it can find which looks like an external interface if none is specified, and displays a table of current bandwidth usage by pairs of hosts. The iftop is a perfect tool for remote Linux server over an ssh based session.

IPCALC:

```
File  Edit  View  Search  Terminal  Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ipcalc
Usage: ipcalc [options] <ADDRESS>[[/]<NETMASK>] [NETMASK]

ipcalc takes an IP address and netmask and calculates the resulting
broadcast, network, Cisco wildcard mask, and host range. By giving a
second netmask, you can design sub- and supernetworks. It is also
intended to be a teaching tool and presents the results as
easy-to-understand binary values.

 -n --nocolor  Don't display ANSI color codes.
 -c --color    Display ANSI color codes (default).
 -b --nobinary Suppress the bitwise output.
 -c --class    Just print bit-count-mask of given address.
 -h --html     Display results as HTML (not finished in this version).
 -v --version  Print Version.
 -s --split n1 n2 n3
               Split into networks of size n1, n2, n3.
 -r --range    Deaggregate address range.
    --help     Longer help text.

Examples:

ipcalc 192.168.0.1/24
ipcalc 192.168.0.1/255.255.128.0
ipcalc 192.168.0.1 255.255.128.0 255.255.192.0
ipcalc 192.168.0.1 0.0.63.255


ipcalc <ADDRESS1> - <ADDRESS2>  deaggregate address range

ipcalc <ADDRESS>/<NETMASK> --s a b c
                               split network to subnets
                               where a b c fits in.
```