

Assignment No: 01

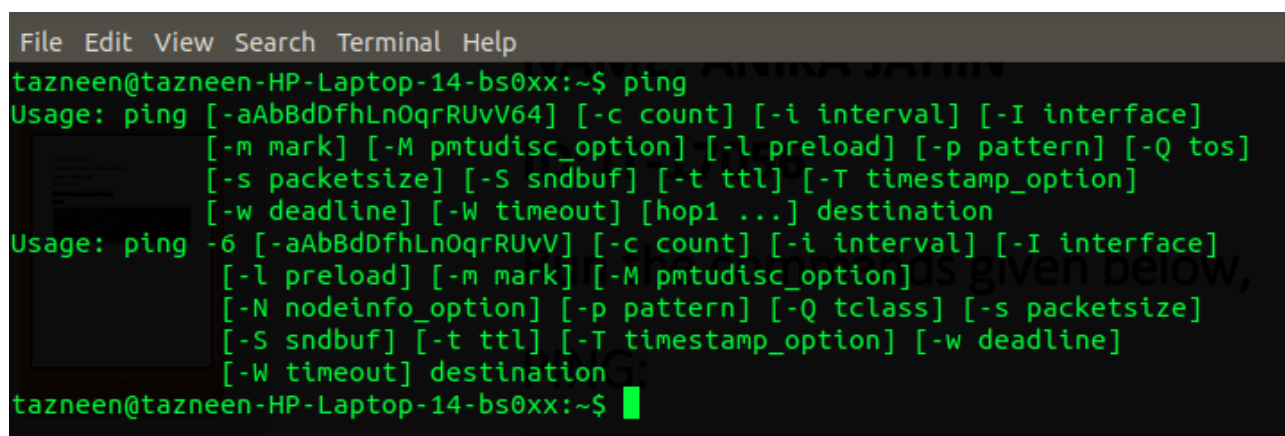
Assignment Name: LINUX commands.

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.

A screenshot of a Linux terminal window. The title bar shows 'File Edit View Search Terminal Help'. The terminal text is as follows:

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ping
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
          [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
          [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
          [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
          [-l preload] [-m mark] [-M pmtudisc_option]
          [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
          [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
          [-W timeout] destination
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

**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.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ curl --help
Usage: curl [options...] <url>
  --abstract-unix-socket <path> Connect via abstract Unix domain socket
  --anyauth             Pick any authentication method
  -a, --append          Append to target file when uploading
  --basic              Use HTTP Basic Authentication
  --cacert <file>      CA certificate to verify peer against
  --capath <dir>       CA directory to verify peer against
  -E, --cert <certificate[:password]> Client certificate file and password
  --cert-status        Verify the status of the server certificate
  --cert-type <type>   Certificate file type (DER/PEM/ENG)
  --ciphers <list of ciphers> SSL ciphers to use
  --compressed        Request compressed response
  --compressed-ssh     Enable SSH compression
  -K, --config <file>  Read config from a file
  --connect-timeout <seconds> Maximum time allowed for connection
  --connect-to <HOST1:PORT1:HOST2:PORT2> Connect to host
  -C, --continue-at <offset> Resumed transfer offset
  -b, --cookie <data>  Send cookies from string/file
  -c, --cookie-jar <filename> Write cookies to <filename> after operation
  --create-dirs        Create necessary local directory hierarchy
  --crlf              Convert LF to CRLF in upload
  --crlfile <file>    Get a CRL list in PEM format from the given file
  -d, --data <data>   HTTP POST data
  --data-ascii <data> HTTP POST ASCII data
```

**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.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ httpree
usage: http [--json] [--form] [--pretty {all,colors,format,none}]
  [--style STYLE] [--print WHAT] [--headers] [--body] [--verbose]
  [--all] [--history-print WHAT] [--stream] [--output FILE]
  [--download] [--continue]
  [--session SESSION_NAME_OR_PATH | --session-read-only SESSION_NAME_OR_PATH]
  [--auth USER[:PASS]] [--auth-type {basic,digest}]
  [--proxy PROTOCOL:PROXY_URL] [--follow]
  [--max-redirects MAX_REDIRECTS] [--timeout SECONDS]
  [--check-status] [--verify VERIFY]
  [--ssl {ssl2.3,tls1,tls1.1,tls1.2}] [--cert CERT]
  [--cert-key CERT_KEY] [--ignore-stdin] [--help] [--version]
  [--traceback] [--default-scheme DEFAULT_SCHEME] [--debug]
  [METHOD] URL [REQUEST_ITEM [REQUEST_ITEM ...]]
http: error: the following arguments are required: URL
```

**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 verbosity, 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 unlimited)

```

**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:~$

```

**DIG/NSLOOKUP:** Dig (**D**omain **I**nformation **G**roper) 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.



```

tazneen@tazneen-HP-Laptop-14-bs0xx:~$ dig
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36307 batch fll
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 65494
;; QUESTION SECTION:
;
; IN NS

;; ANSWER SECTION:
87097 IN NS a.root-servers.net.
87097 IN NS b.root-servers.net.
87097 IN NS c.root-servers.net.
87097 IN NS d.root-servers.net.
87097 IN NS e.root-servers.net.
87097 IN NS f.root-servers.net.
87097 IN NS g.root-servers.net.
87097 IN NS h.root-servers.net.
87097 IN NS i.root-servers.net.
87097 IN NS j.root-servers.net.
87097 IN NS k.root-servers.net.
87097 IN NS l.root-servers.net.
87097 IN NS m.root-servers.net.

;; Query time: 33 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Nov 22 18:24:49 +06 2020
;; MSG SIZE rcvd: 239

```

**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 [-46AaCfGgKkMnqsTtVvXxYy] [-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:~$
```

Welcome to Wireshark

### Capture


...using this filter:  All interfaces shown ▾

<input checked="" type="checkbox"/>	wlo1	—
<input type="checkbox"/>	any	—
<input type="checkbox"/>	Loopback: lo	—
<input type="checkbox"/>	eno1	—
<input type="checkbox"/>	bluetooth0	—
<input type="checkbox"/>	nflog	—
<input type="checkbox"/>	nfqueue	—
<input type="checkbox"/>	usbmon1	—
<input type="checkbox"/>	usbmon2	—
<input checked="" type="checkbox"/>	Cisco remote capture: ciscodump	—

### Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

 Ready to load or capture No Packets Profile: Default

**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
```

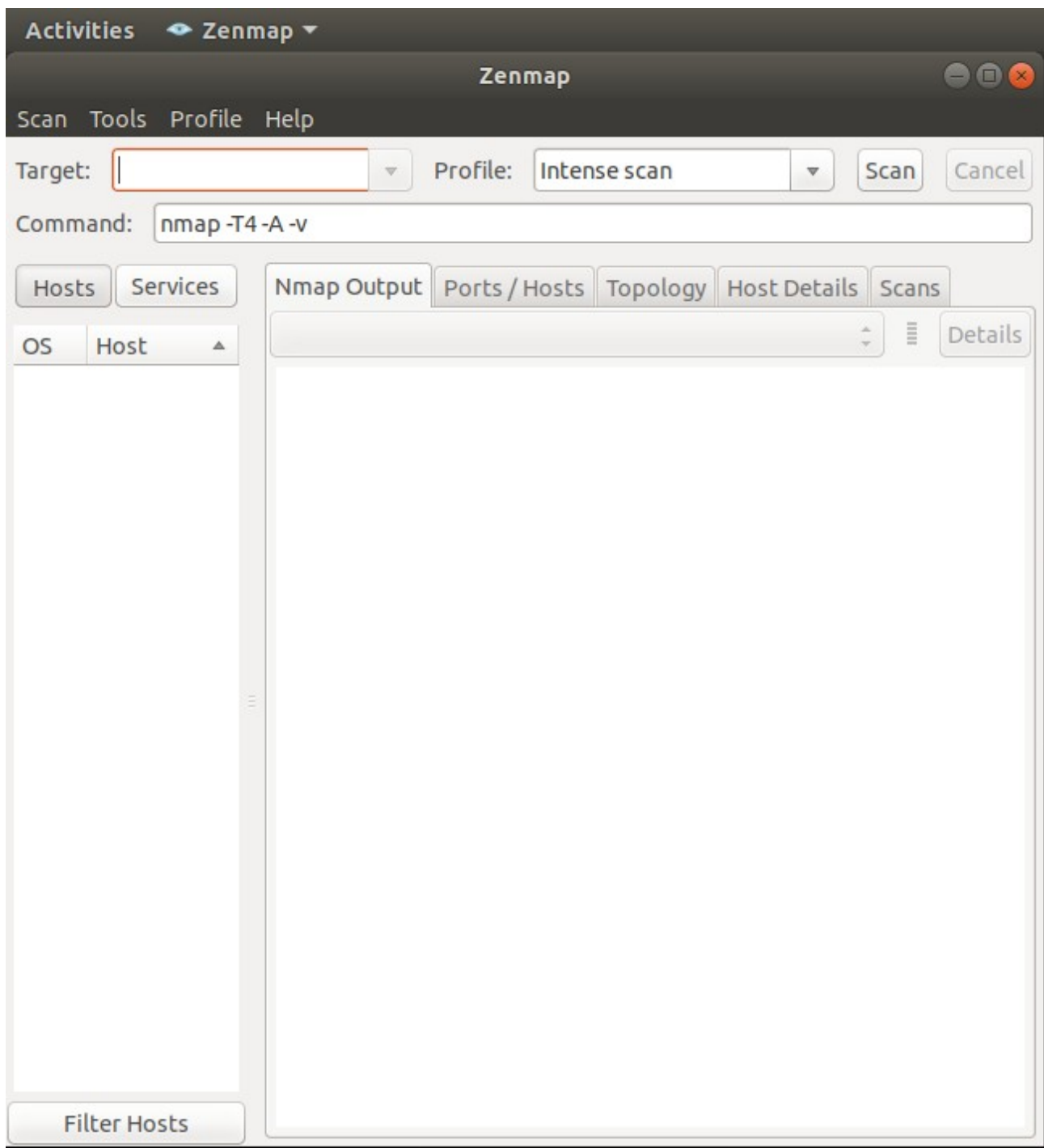
**NMAP:** **Nmap** is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators.

```

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
  -t: Scan ports consecutively... don't randomize

```

## 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.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ p0f
--- p0f 3.09b by Michal Zalewski <lcantuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'wlo1'.
[-] PROGRAM ABORT : pcap_open_live: wlo1: You don't have permission to capture on that device (socket: Operation not permitted)
    Location : prepare_pcap(), p0f.c:526
```



## OPENVPN:

```
File Edit View Search Terminal Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ openvpn
OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2019

General Options:
--config file      : Read configuration options from file.
--help            : Show options.
--version         : Show copyright and version information.

Tunnel Options:
--local host      : Local host name or ip address. Implies --bind.
--remote host [port] : Remote host name or ip address.
--remote-random   : If multiple --remote options specified, choose one randomly.
--remote-random-hostname : Add a random string to remote DNS name.
--mode m         : Major mode, m = 'p2p' (default, point-to-point) or 'server'.
--proto p        : Use protocol p for communicating with peer.
                  p = udp (default), tcp-server, or tcp-client
--proto-force p   : only consider protocol p in list of connection profiles.
                  p = udp6, tcp6-server, or tcp6-client (ipv6)
--connect-retry n [m] : For client, number of seconds to wait between
                  connection retries (default=5). On repeated retries
                  the wait time is exponentially increased to a maximum of m
                  (default=300).
--connect-retry-max n : Maximum connection attempt retries, default infinite.
--http-proxy s p [up] [auth] : Connect to remote host
                  through an HTTP proxy at address s and port p.
                  If proxy authentication is required,
                  up is a file containing username/password on 2 lines, or
                  'stdin' to prompt from console. Add auth='ntlm' if
                  the proxy requires NTLM authentication.
--http-proxy s p 'auto[nct]' : Like the above directive, but automatically
                  determine auth method and query for username/password
                  if needed. auto-nct disables weak proxy auth methods.
--http-proxy-option type [parm] : Set extended HTTP proxy options.
                  Repeat to set multiple options.
VERSION version (default=1.0)
```

## 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.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ nc
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl] [-m minttl]
          [-O length] [-P proxy_username] [-p source_port] [-q seconds] [-s source]
          [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]] [destination] [port]
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

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

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ socat
2020/11/22 18:54:35 socat[29060] E exactly 2 addresses required (there are 0); use option "-h" for help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$
```

**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.

```

tazneen@tazneen-HP-Laptop-14-bs0xx:~$ iptables -h
iptables v1.6.1

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)

Commands:
Either long or short options are allowed.
--append -A chain          Append to chain
--check  -C chain          Check for the existence of a rule
--delete -D chain          Delete matching rule from chain
--delete -D chain rulenum  Delete rule rulenum (1 = first) from chain
--insert -I chain [rulenum] Insert in chain as rulenum (default 1=first)
--replace -R chain rulenum Replace rule rulenum (1 = first) in chain
--list   -L [chain [rulenum]]

```

## 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.

```

tazneen@tazneen-HP-Laptop-14-bs0xx:~$ hping3
hping3>

```

**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.



```

File Edit View Search Terminal Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ traceroute
Usage:
traceroute [ -4dFItnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ]
[ -w MAX,HERE,NEAR ] [ -q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]
Options:
-4                      Use IPv4
-6                      Use IPv6
-d --debug              Enable socket level debugging
-F --dont-fragment      Do not fragment packets
-f first_ttl --first=first_ttl
                        Start from the first_ttl hop (instead from 1)
-g gate,... --gateway=gate,...
                        Route packets through the specified gateway
                        (Maximum 8 for IPv4 and 127 for IPv6)
-I --icmp               Use ICMP ECHO for tracerouting
-T --tcp               Use TCP SYN for tracerouting (default port is 80)
-i device --interface=device
                        Specify a network interface to operate with
-m max_ttl --max-hops=max_ttl
                        Set the max number of hops (max TTL to be
                        reached). Default is 30
-N squeries --sim-queries=squeries
                        Set the number of probes to be tried
                        simultaneously (default is 16)
-n                      Do not resolve IP addresses to their domain names
-p port --port=port     Set the destination port to use. It is either
                        initial udp port value for "default" method
                        (incremented by each probe, default is 33434), or
                        initial seq for "icmp" (incremented as well,
                        default from 1), or some constant destination
                        port for other methods (with default of 80 for
                        "tcp", 53 for "udp", etc.)
-t tos --tos=tos        Set the TOS (IPv4 type of service) or TC (IPv6
                        traffic class) value for outgoing packets
-l flow_label --flowlabel=flow_label

```

**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.

```
File Edit View Search Terminal Help
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ ethtool -h
ethtool version 4.15
Usage:
  ethtool DEVNAME Display standard information about device
  ethtool -s|--change DEVNAME [ options ] Change generic options
    [ speed %d ]
    [ duplex half|full ]
    [ port tp|aui|bnc|mii|fibre ]
    [ mdix auto|on|off ]
    [ autoneg on|off ]
    [ advertise %x ]
    [ phyad %d ]
    [ xcvr internal|external ]
    [ wol p|u|m|b|a|g|s|d... ]
    [ sopass %x:%x:%x:%x:%x:%x ]
    [ msglvl %d | msglvl type on|off ... ]
  ethtool -a|--show-pause DEVNAME Show pause options
  ethtool -A|--pause DEVNAME [ options ] Set pause options
    [ autoneg on|off ]
    [ rx on|off ]
    [ tx on|off ]
  ethtool -c|--show-coalesce DEVNAME Show coalesce options
  ethtool -C|--coalesce DEVNAME [ options ] Set coalesce options
    [ adaptive-rx on|off ]
    [ adaptive-tx on|off ]
    [ rx-usecs N ]
    [ rx-frames N ]
    [ rx-usecs-irq N ]
    [ rx-frames-irq N ]
    [ tx-usecs N ]
    [ tx-frames N ]
    [ tx-usecs-irq N ]
    [ tx-frames-irq N ]
    [ stats-block-usecs N ]
    [ pkt-rate-low N ]
```

**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 names
Usage:
  sysctl [options] [variable[=value] ...] --load[=<file>]

Options:
  -a, --all                display all variables system
  -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.

```
tazneen@tazneen-HP-Laptop-14-bs0xx:~$ stunnel4
[ ] Clients allowed=500
[!] Invalid configuration file name "/etc/stun
[.] stunnel 5.44 on x86_64-pc-linux-gnu platform
[.] Compiled with OpenSSL 1.1.0g  2 Nov 2017
[.] Running with OpenSSL 1.1.1  11 Sep 2018
[.] Update OpenSSL shared libraries or rebuild stunnel
[.] Threading:PTHREAD Sockets:POLL,IPv6,SYSTEMD TLS:ENGINE,FIPS,OCSP,PSK,SNI Auth:LIBWRAP
[ ] errno: (*__errno_location ())
[!] Invalid configuration file name "/etc/stunnel/stunnel.conf"
[!] realpath: No such file or directory (2)
```

**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.