

Assignment

Assignment Name: LINUX commands.

Course code: ICT-3208

Course title: Computer Network Lab

Date of

Performance: 09/11/2020

Date of

Submission: 19/11/2020

SUBMITTED BY

Name: Shakhera khanom

ID: IT-18033

3rd year 2nd semester

Session: 2017-18

Department of ICT,

MBSTU.

SUBMITTED TO

Nazrul Islam

Assistant Professor

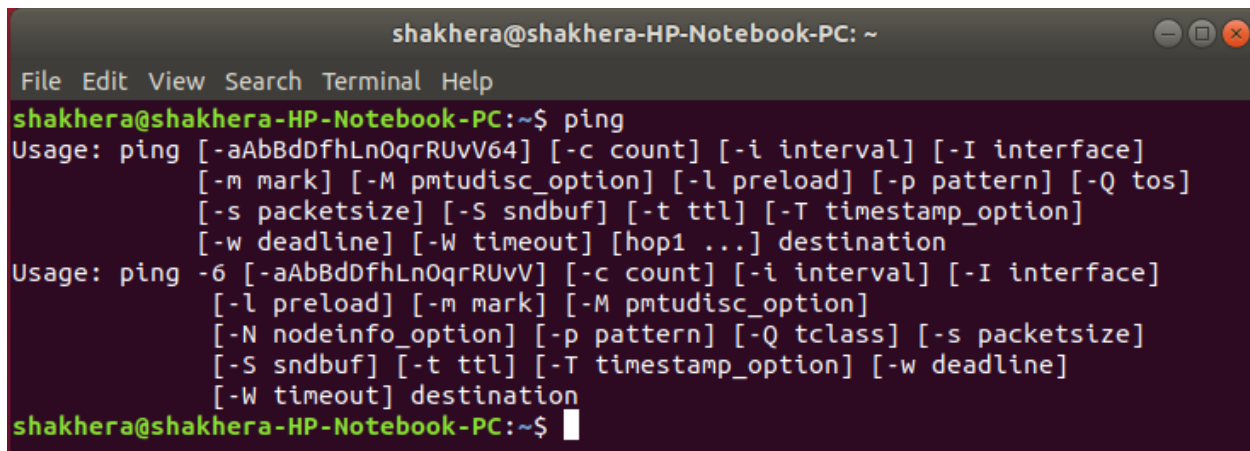
Department of ICT,

MBSTU.

Assignment No: 01

Assignment Name: LINUX commands.

PING: Linux “*ping*” command stands for (Packet Internet Groper). It checks connectivity between two nodes to see if a server is available. It sends ICMP ECHO_REQUEST packets to network hosts and displays the data on the remote server's response. It checks if a remote host is up, or that network interfaces can be reached. Further, it is used to check if a network connection is available between two devices. It is also handy tool for checking your network connection and verifying network issues.

A screenshot of a Linux terminal window titled "shakhera@shakhera-HP-Notebook-PC: ~". The terminal shows the command "ping" being entered, followed by its usage information. The usage text is displayed in two columns, showing various options like [-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, [-6], [-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. The prompt "shakhera@shakhera-HP-Notebook-PC:~\$" is visible at the bottom.

```
shakhera@shakhera-HP-Notebook-PC: ~  
File Edit View Search Terminal Help  
shakhera@shakhera-HP-Notebook-PC:~$ 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  
shakhera@shakhera-HP-Notebook-PC:~$
```

CURL: Linux “*curl*” command is used to download or upload data to a server via supported protocols such as HTTP, FTP, IMAP, SFTP, TFTP, IMAP, POP3, SCP, etc. It is a remote utility, so it works without user interaction.

```
shakhera@shakhera-HP-Notebook-PC: ~  
File Edit View Search Terminal Help  
shakhera@shakhera-HP-Notebook-PC:~$ 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
```

HTTPIE: Linux “*httpie*” aitch-tee-tee-pie is a user friendly command-line http client for the api era. It comes with JSON support, system highlighting, persistent sessions, wget-like downloads, plugins, and more.

```
shakhera@shakhera-HP-Notebook-PC: ~  
File Edit View Search Terminal Help  
shakhera@shakhera-HP-Notebook-PC:~$ httpie  
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  
shakhera@shakhera-HP-Notebook-PC:~$
```

WGET: Linux command *wget* stands for web get. The *wget* is a free non-interactive file downloader command. Non-interactive means it can work in background when user is not logged in. This allows user to get disconnected with the system while *wget* finish its work. It can even download entire website as a

local version of remote websites, fully recreating the structure of original website. In short, you can mirror an entire website with *wget*.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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
```

TC: Linux “*tc*” (traffic control) is the user-space utility program used to configure the Linux kernel packet scheduler.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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]
shakhera@shakhera-HP-Notebook-PC:~$
```

DIG/NSLOOKUP: Linux “*dig*” command stands for Domain Information Groper. This command is used for tasks related to DNS lookup to query DNS name servers.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ dig

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33316
;; 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:
.           80801    IN      NS      m.root-servers.net.
.           80801    IN      NS      f.root-servers.net.
.           80801    IN      NS      j.root-servers.net.
.           80801    IN      NS      l.root-servers.net.
.           80801    IN      NS      e.root-servers.net.
.           80801    IN      NS      c.root-servers.net.
.           80801    IN      NS      g.root-servers.net.
```

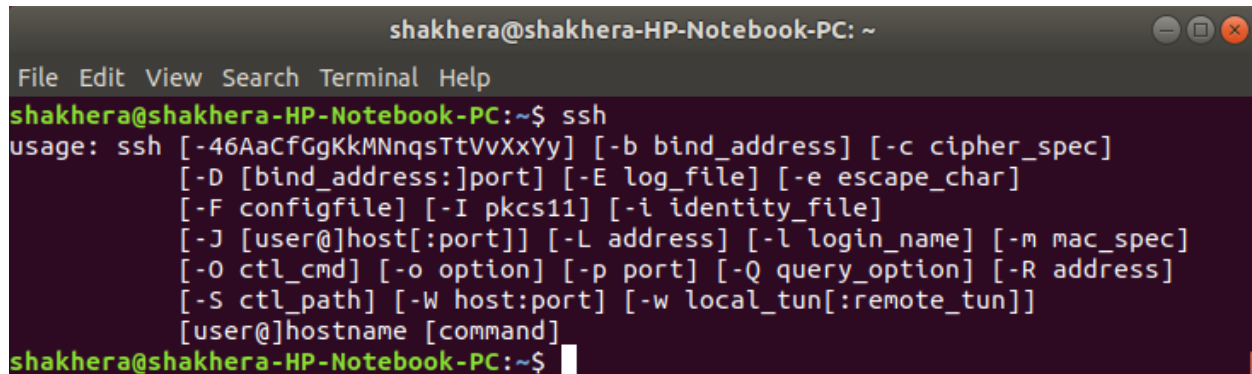
WHOIS: Linux “*whois*” command displays information about a website's record. You may get all the information about a website regarding its registration and owner's information.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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

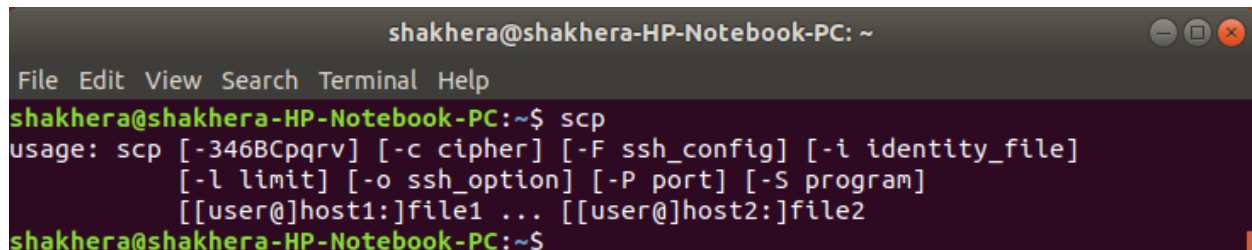
These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                    find the one level less specific match
-L                    find all levels less specific matches
-m                    find all one level more specific matches
-M                    find all levels of more 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
```

SSH: Linux “*ssh*” (Secure SHell) command is a Network protocol used for communication between two networked computer. It is different from other protocols in way that it provide security while accessing other system. Hence anyone on network will see only encrypted data and not the plain data.

A terminal window titled 'shakhera@shakhera-HP-Notebook-PC: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'shakhera@shakhera-HP-Notebook-PC:~\$' followed by the command 'ssh'. The output shows the usage for the ssh command: '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]'. The prompt returns to 'shakhera@shakhera-HP-Notebook-PC:~\$' with a cursor.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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]
shakhera@shakhera-HP-Notebook-PC:~$
```

SCP: Linux “*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. It uses the same authentication and security as it is used in the Secure Shell (SSH) protocol. SCP is known for its simplicity, security and pre-installed availability.

A terminal window titled 'shakhera@shakhera-HP-Notebook-PC: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'shakhera@shakhera-HP-Notebook-PC:~\$' followed by the command 'scp'. The output shows the usage for the scp command: '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]'. The prompt returns to 'shakhera@shakhera-HP-Notebook-PC:~\$' with a cursor.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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
shakhera@shakhera-HP-Notebook-PC:~$
```

RSYNC: The “*rsync*” or remote synchronization is a software utility for Unix-Like systems that efficiently sync files and directories between two hosts or machines. One of them being the source or the local-host from which the files will be synced, the other one being the remote-host, on which synchronization will take place.


```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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, symlinks, 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
```

NGREP: The “*ngrep*” strives to provide most of GNU *grep*'s common features, applying them to the network layer. *ngrep* is a pcap-aware tool that will allow you to specify extended regular expressions to match against data payloads of packets.

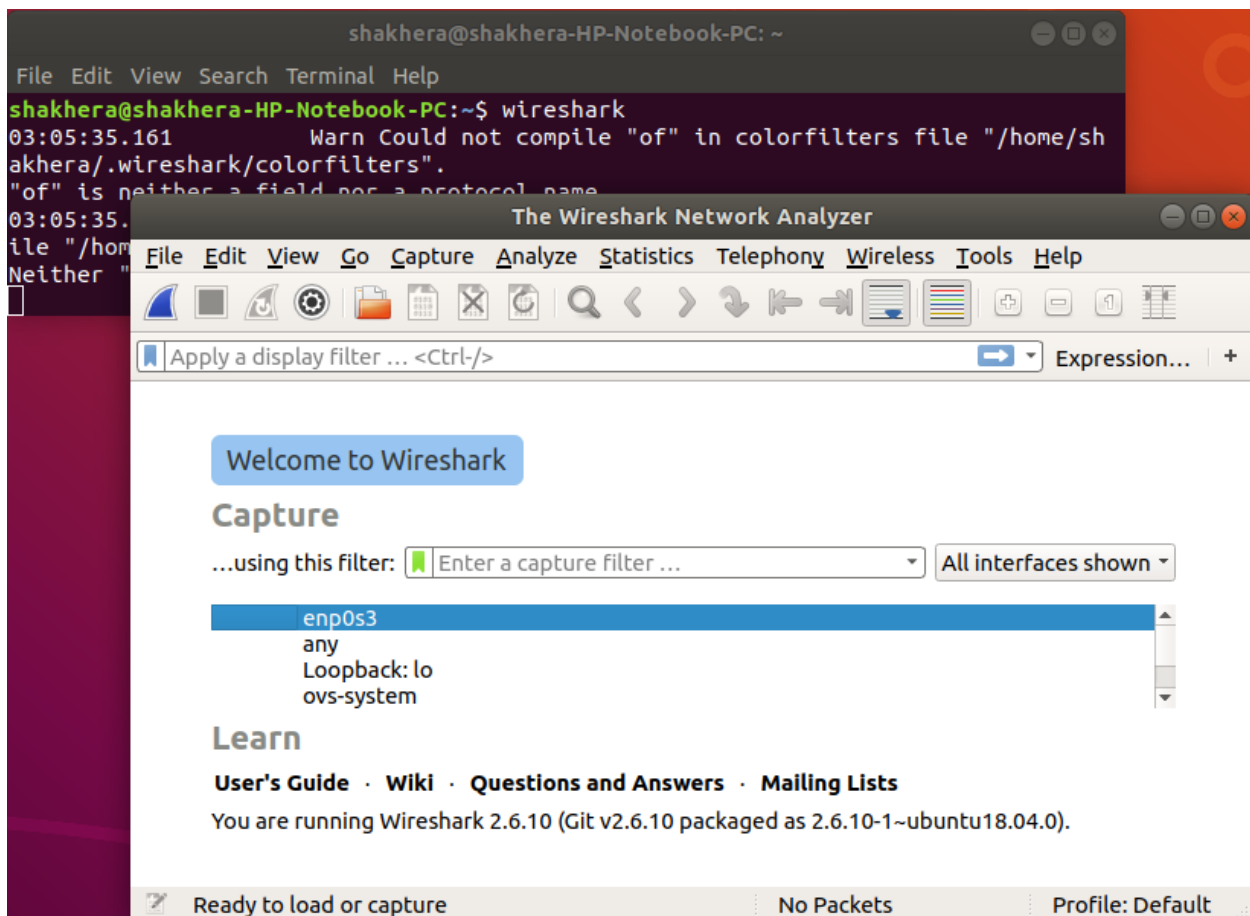
```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ ngrep
enp0s3: You don't have permission to capture on that device (socket: Operation n
ot permitted): Operation not permitted
exit
0 received, 0 matched
shakhera@shakhera-HP-Notebook-PC:~$
```

TCPDUMP: The “*tcpdump*” is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured

information in a pcap file, these pcap files can then be opened through [Wireshark](#) or through the command tool itself.

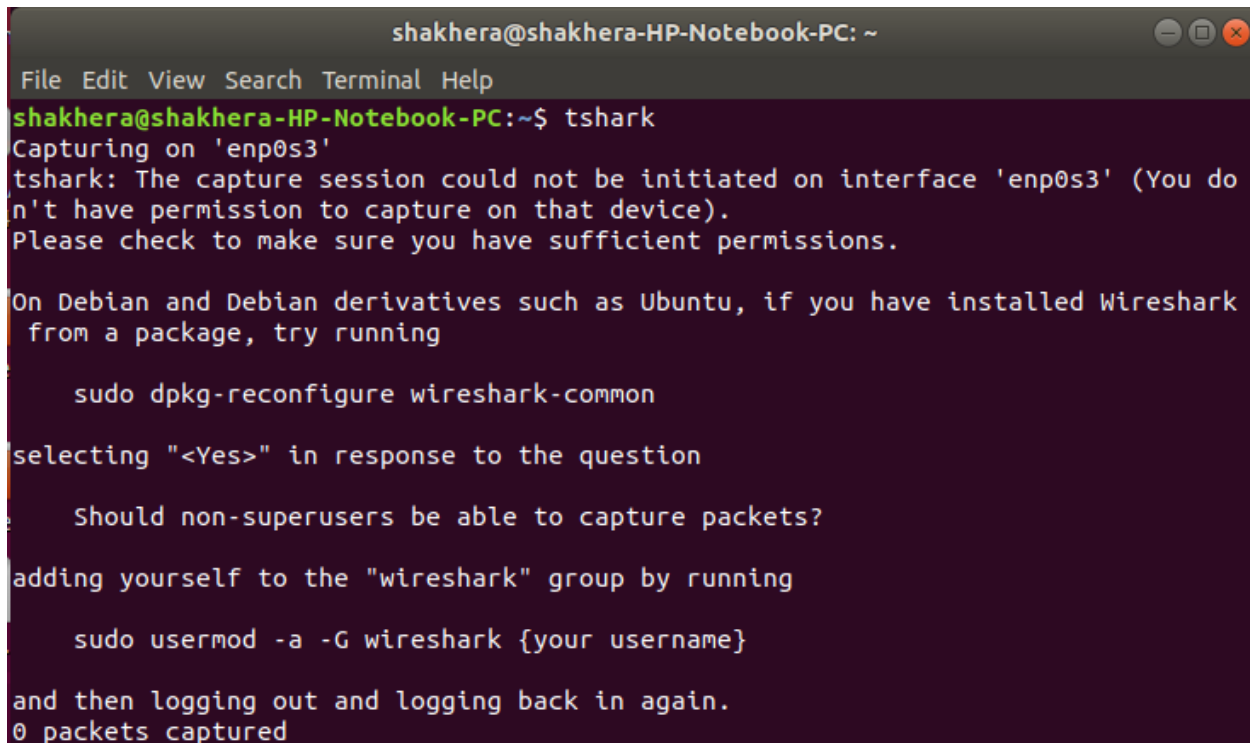
```
shakhera@shakhera-HP-Notebook-PC: ~  
File Edit View Search Terminal Help  
shakhera@shakhera-HP-Notebook-PC:~$ tcpdump  
tcpdump: enp0s3: You don't have permission to capture on that device  
(socket: Operation not permitted)
```

WIRESHARK: Linux “*wireshark*” command is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

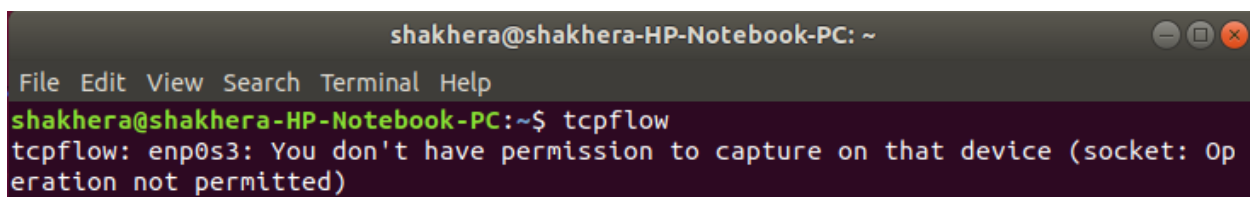


TSHARK: Linux “*tshark*” is the command-line version of wireshark. It provide many useful commands and capture filters that can be used on terminal which

provides an efficient way to analyse the incoming traffic and capture the traffic in pcap. Let me give you a brief about the terminology we use in *tshark*.

A terminal window titled 'shakhera@shakhera-HP-Notebook-PC: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'shakhera@shakhera-HP-Notebook-PC:~\$'. The command 'tshark' is entered. The output shows 'Capturing on 'enp0s3'', followed by an error: 'tshark: The capture session could not be initiated on interface 'enp0s3' (You don't have permission to capture on that device). Please check to make sure you have sufficient permissions.' Below this, instructions are provided for Debian/Ubuntu users: 'On Debian and Debian derivatives such as Ubuntu, if you have installed Wireshark from a package, try running' followed by the command 'sudo dpkg-reconfigure wireshark-common'. This leads to a configuration prompt: 'selecting "<Yes>" in response to the question' and 'Should non-superusers be able to capture packets?'. Further instructions say 'adding yourself to the "wireshark" group by running' followed by 'sudo usermod -a -G wireshark {your username}' and 'and then logging out and logging back in again.' The final line shows '0 packets captured'.

TCPFLOW: The “*tcpflow*” is a free, open source, powerful command line based tool for analyzing network traffic on Unix-like systems such as Linux. It captures data received or transferred over TCP connections, and stores it in a file for later analysis, in a useful format that allows for protocol analysis and debugging.

A terminal window titled 'shakhera@shakhera-HP-Notebook-PC: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'shakhera@shakhera-HP-Notebook-PC:~\$'. The command 'tcpflow' is entered. The output shows an error: 'tcpflow: enp0s3: You don't have permission to capture on that device (socket: Operation not permitted)'.

IFCONFIG: Linux “*ifconfig*” command is used for displaying current network configuration information, setting up an ip address, netmask or broadcast address to an network interface, creating an alias for network interface, setting up hardware address and enable or disable network interfaces.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::90d6:8cf8:3ad9:8238 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:25:23:01 txqueuelen 1000 (Ethernet)
    RX packets 23767 bytes 33066325 (33.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11624 bytes 752733 (752.7 KB)
    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 11151 bytes 569116 (569.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11151 bytes 569116 (569.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ROUTE: Linux “*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

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 100 0 0 enp0s3
10.0.2.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3
link-local 0.0.0.0 255.255.0.0 U 1000 0 0 enp0s3
```

IP: Linux “*ip*” command in Linux is present in the net-tools which is used for performing several network administration tasks. IP stands for Internet Protocol. This command is used to show or manipulate routing, devices, and tunnels.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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: Linux “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)

```
shakhera@shakhera-HP-Notebook-PC:~$ arp
Address                HWtype  HWaddress           Flags Mask            Iface
_gateway               ether    52:54:00:12:35:02    C                     enp0s3

```

MITMPROXY: The “mitmproxy” is a set of tools that provide an interactive, SSL/TLS-capable intercepting proxy for HTTP/1, HTTP/2, and WebSockets.

```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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-pac
kages), Requirement.parse('urwid<1.4,>=1.3.1'), {'mitmproxy'})

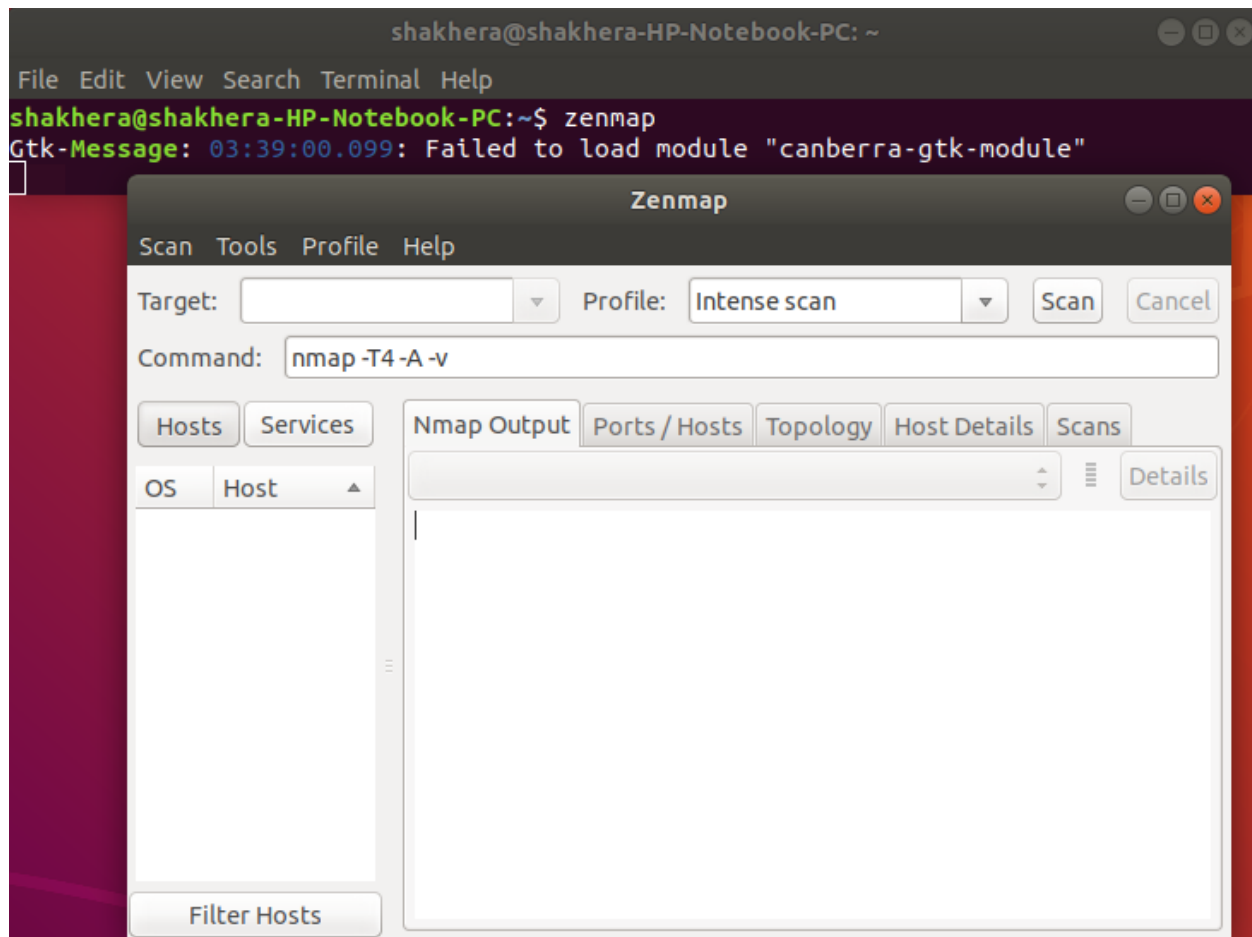
During handling of the above exception, another exception occurred:

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>
```

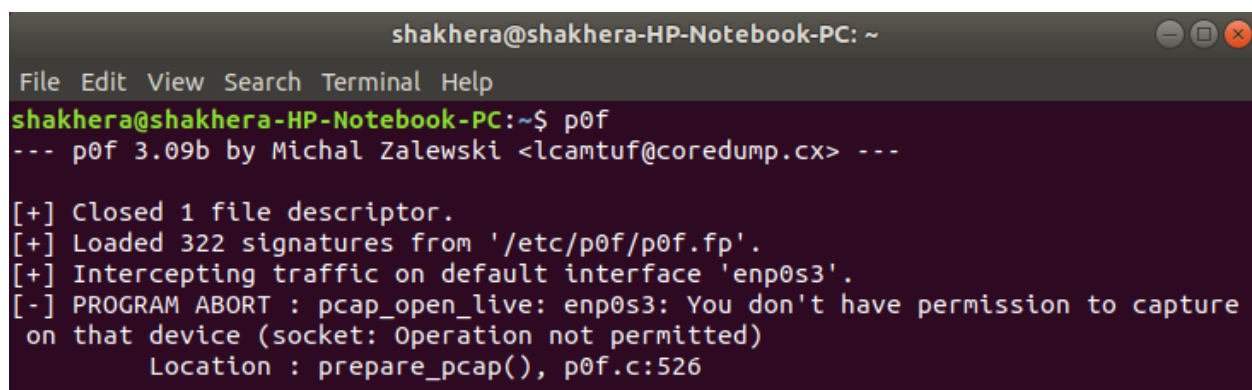
NMAP: Linux “*nmap*” is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators.

```
shakhera@shakhera-HP-Notebook-PC: ~  
File Edit View Search Terminal Help  
shakhera@shakhera-HP-Notebook-PC:~$ nmap  
Nmap 7.91 ( 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
```

ZENMAP: Linux “*zenmap*” command is a graphical user interface developed for “nmap”, a tool that we use on the command line terminal for scanning ports and networks.



P0f: The “*p0f*” is a passive TCP/IP stack fingerprinting tool. P0f can attempt to identify the system running on machines that sent 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 analyzing other aspects of the remote system.



OPENVPN: Linux “*openvpn*” command is open source *openvpn* CLI program. The open source project client program can also connect to the access server


```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
shakhera@shakhera-HP-Notebook-PC:~$ 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.
```

WIREGUARD:

NC: Linux “nc” command runs netcat, a utility for sending raw data over a network connection.

```
shakhera@shakhera-HP-Notebook-PC:~$ 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 t
imeout]
        [-X proxy_protocol] [-x proxy_address[:port]]          [destination]
[port]
```

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

```
shakhera@shakhera-HP-Notebook-PC:~$ socat
2020/11/19 03:47:15 socat[16328] E exactly 2 addresses required (there are 0); u
se option "-h" for help
```

TELNET: Linux “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.

```
shakhera@shakhera-HP-Notebook-PC:~$ telnet
telnet> |
```

FTP/SFTP: Linux “ftp” command is a standard network protocol used to transfer files to and from a remote network. FTP client to connect to the remote server and download or upload files.

```
shakhera@shakhera-HP-Notebook-PC: ~  
File Edit View Search Terminal Help  
shakhera@shakhera-HP-Notebook-PC:~$ ftp  
ftp>
```

NETSTAT/SS/LSOF/FUSER: Linux “*netstat*” command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

```
shakhera@shakhera-HP-Notebook-PC: ~  
File Edit View Search Terminal Help  
shakhera@shakhera-HP-Notebook-PC:~$ netstat -r  
Kernel IP routing table  
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface  
default          _gateway        0.0.0.0         UG      0 0       0 enp0s3  
10.0.2.0         0.0.0.0         255.255.255.0   U       0 0       0 enp0s3  
link-local       0.0.0.0         255.255.0.0     U       0 0       0 enp0s3
```

IPTABLES: Linux “*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.

```
shakhera@shakhera-HP-Notebook-PC:~$ iptables  
iptables v1.6.1: no command specified  
Try 'iptables -h' or 'iptables --help' for more information.
```

NFTABLES:

HPING3: Linux “*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.

```
shakhera@shakhera-HP-Notebook-PC:~$ hping3  
hping3>
```

TRACEROUTE/MTR: Linux “*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.

```
shakhera@shakhera-HP-Notebook-PC:~$ traceroute --help
Usage: traceroute [OPTION...] HOST
Print the route packets trace to network host.

-f, --first-hop=NUM      set initial hop distance, i.e., time-to-live
-g, --gateways=GATES     list of gateways for loose source routing
-I, --icmp               use ICMP ECHO as probe
-m, --max-hop=NUM        set maximal hop count (default: 64)
-M, --type=METHOD       use METHOD ('icmp' or 'udp') for traceroute
                           operations, defaulting to 'udp'
-p, --port=PORT          use destination PORT port (default: 33434)
-q, --tries=NUM          send NUM probe packets per hop (default: 3)
    --resolve-hostnames   resolve hostnames
-t, --tos=NUM            set type of service (TOS) to NUM
-w, --wait=NUM           wait NUM seconds for response (default: 3)
-?, --help               give this help list
    --usage               give a short usage message
-V, --version             print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.
```

ETHTOOL: Linux “*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.

```
shakhera@shakhera-HP-Notebook-PC:~$ ethtool
ethtool: bad command line argument(s)
For more information run ethtool -h
```

IW/IWCONFIG: Linux *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. *iwconfig* may also be used to display the parameters, and the wireless statistics which are extracted from */proc/net/wireless*.

```
shakhera@shakhera-HP-Notebook-PC:~$ iwconfig
enp0s3    no wireless extensions.

lo        no wireless extensions.

s1        no wireless extensions.

ovs-system no wireless extensions.
```

SYSCTL: Linux “*sysctl*” command is used to modify kernel parameters at runtime. The parameters available are those listed under `/proc/sys/`.

```
shakhera@shakhera-HP-Notebook-PC:~$ 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>
```

OPENSSL: The “*openssl*” is a cryptography software library or toolkit that makes communication over computer networks more secure. The *openssl* program is a command-line tool for using the various cryptography functions of *openssl*’s crypto library from the shell. It is generally used for Transport Layer Security(TLS) or Secure Socket Layer(SSL) protocols.

```
shakhera@shakhera-HP-Notebook-PC:~$ openssl
OpenSSL> quit
shakhera@shakhera-HP-Notebook-PC:~$
```

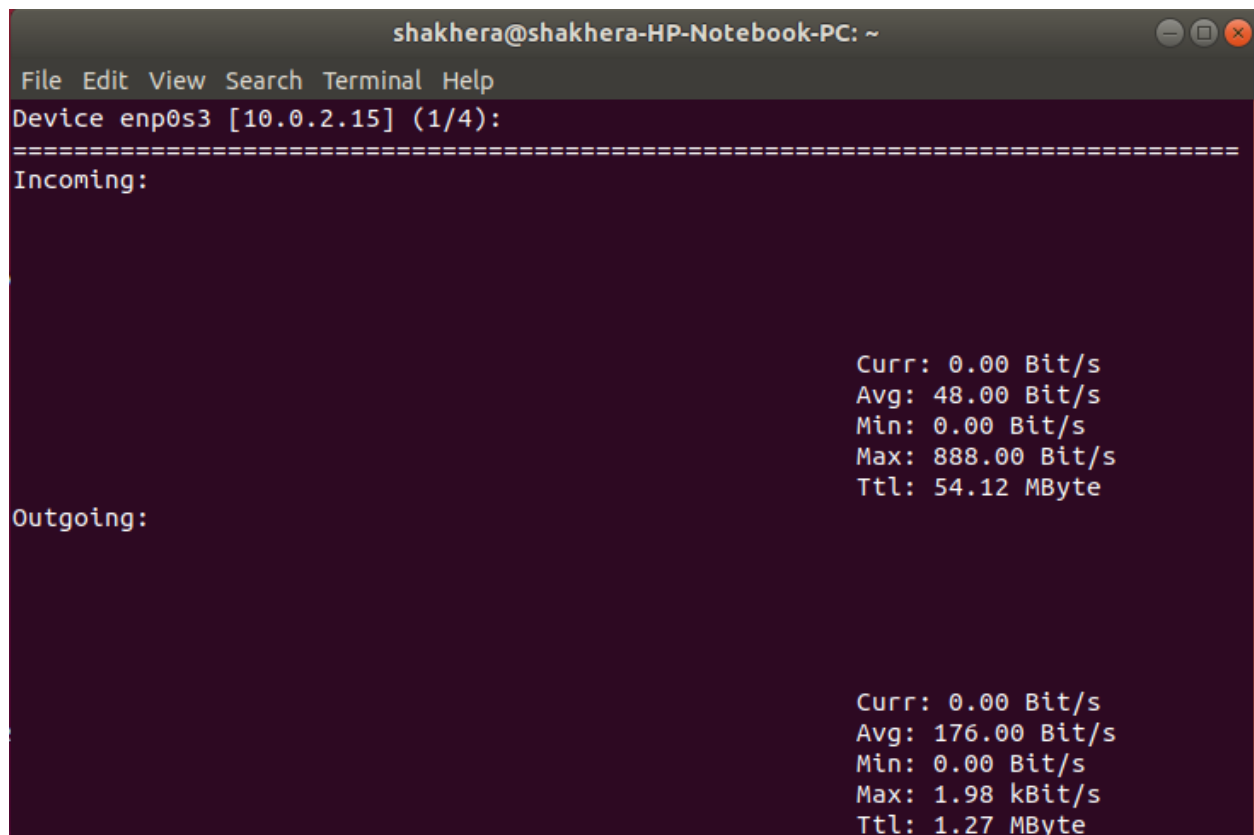
STUNNEL: The “*stunnel*” program is designed to work as *SSL* encryption wrapper between remote clients and local (*inetd*-startable) or remote servers. The concept is that having non-SSL aware daemons running on your system you can easily set them up to communicate with clients over secure *SSL* channels.

```
shakhera@shakhera-HP-Notebook-PC:~$ stunnel
[ ] Clients allowed=500
[.] 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: Linux “*iftop*” command is a network analyzing tool used by system administrators to view the bandwidth related stats. It shows a quick overview of the networking activities on an interface. It stands from Interface TOP and the top is derived from op command in Linux. It even acts as a diagnostics to diagnose which program is causing the problem to the network.

```
shakhera@shakhera-HP-Notebook-PC:~$ iftop
interface: enp0s3
IP address is: 10.0.2.15
MAC address is: 08:00:27:25:23:01
pcap_open_live(enp0s3): enp0s3: You don't have permission to capture on that dev
ice (socket: Operation not permitted)
```

AB/NLOAD/IPERF: Linux “*nload*” is a Linux command-line tool used to monitor network traffic and bandwidth usage in real time, using insightful graphs and traffic statistics.



```
shakhera@shakhera-HP-Notebook-PC: ~
File Edit View Search Terminal Help
Device enp0s3 [10.0.2.15] (1/4):
=====
Incoming:

                                Curr: 0.00 Bit/s
                                Avg: 48.00 Bit/s
                                Min: 0.00 Bit/s
                                Max: 888.00 Bit/s
                                Ttl: 54.12 MByte

Outgoing:

                                Curr: 0.00 Bit/s
                                Avg: 176.00 Bit/s
                                Min: 0.00 Bit/s
                                Max: 1.98 kBit/s
                                Ttl: 1.27 MByte
```

PYTHON-M:

```
shakhera@shakhera-HP-Notebook-PC:~$ python3m
Python 3.6.9 (default, Jul 17 2020, 12:50:27)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> █
```

IPCALC: The “*ipcalc*” provides a simple way to calculate IP information for a host. The various options specify what information *ipcalc* should display on standard out. Multiple options may be specified. An IP address to operate on must always be specified. Most operations also require a netmask or a CIDR prefix as well.

```
shakhera@shakhera-HP-Notebook-PC:~$ 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.
```

NSENTER: The “*nsenter*” command executes program in the namespace(s) that are specified in the command-line options.

```
shakhera@shakhera-HP-Notebook-PC:~$ nsenter
shakhera@shakhera-HP-Notebook-PC:~$
```

Discussion: Every computer is connected to some other computer through a network whether internally or externally to exchange some information. This network can be small as some computers connected in your home or office, or can be large or complicated as in large University or the entire Internet. Maintaining a system's network we use some task. This task includes configuration and troubleshooting commands, that some command run above. So, we can say that, from assignment, we learn about Linux Networking commands.

