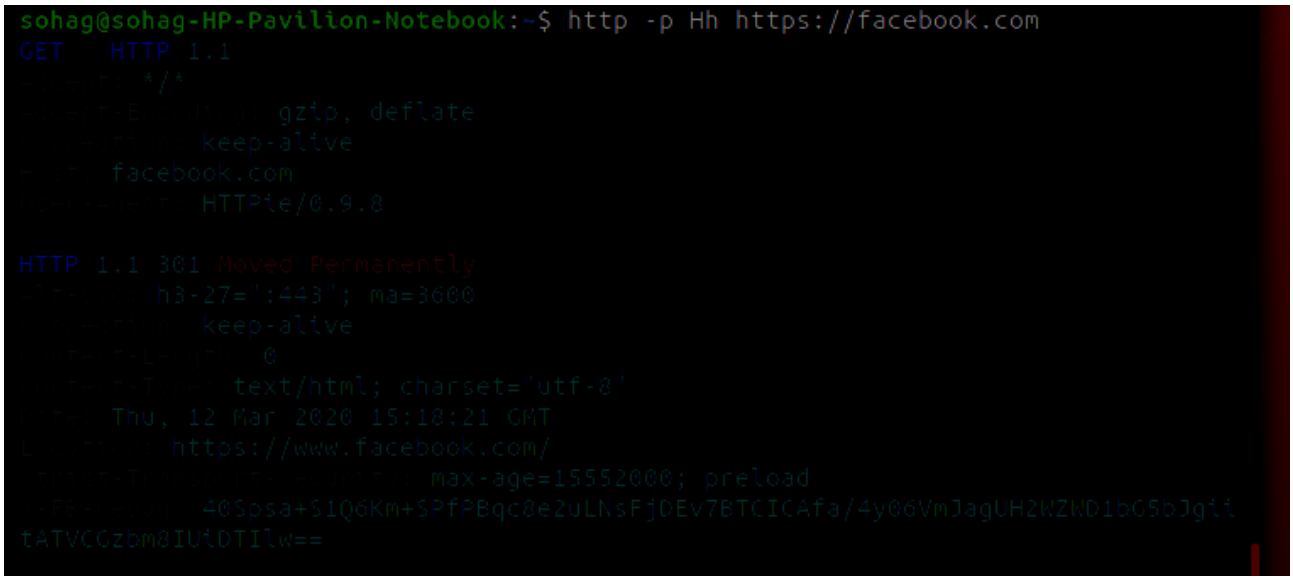
Assignment No	:	01
Name of the Assignment	:	Every networking tool (Linux exercise)
ID	:	IT-17060
Objective	:	Learn about network tool: ping ,curl,httpie,wget,tc,dig/nslookup , whois ,ssh , ngrip, tshark,tcpflow,ifconfig,route ,ip,arp,mitmproxy,nmap , iptables,nftables,hping3,traceroute/mtr,tcptraceroute , ethtool, iw/iwconfig , sysctl , openssl , stunnel , python -m SimpleHttpserver , ipcalc , nsenter

1) Ping : ping is sending out packets called echo requests that simply ask the remote host to respond we got several responses before we stop the requests.

2) curl : make any HTTP request you want . *curl* is a command line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, SMTP, TFTP, TELNET, LDAP or FILE).

```
sohag@sohag-HP-Pavilion-Notebook:~$ curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
```

3.Httpie : HTTPie (pronounced aitch-tee-tee-pie) is a command line HTTP client. Its goal is to make CLI interaction with web services as human-friendly as possible.



4) tc : show/manipulate traffic control settings . **Tc** is used to configure Traffic Control in the Linux kernel.

```
sohag@sohag-HP-Pavilion-Notebook:~$ 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]
sohag@sohag-HP-Pavilion-Notebook:~$
```

5) wget : download files . Wget command is a Linux command line utility that helps us to download the files from the web. We can download the files from web servers using HTTP, HTTPS and FTP protocols. We can use wget in scripts and cronjobs.

6)dig/nslookup : Dig stands for (**Domain Information Groper**) is a network administration command-line tool for querying **Domain Name System** (**DNS**) name servers.

```
sohag@sohag-HP-Pavilion-Notebook:~$ dig google.com

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15119
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             57      IN      A       216.58.197.46

;; Query time: 5 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Mar 12 21:52:24 +06 2020
;; MSG SIZE  rcvd: 55
```

```
sohag@sohag-HP-Pavilion-Notebook:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.197.46
Name:   google.com
Address: 2404:6800:4007:807::200e
```

7) whois : You can use the *whois* command in Linux to find out information about a domain, such as the owner of the domain, the owner's contact information, and the nameservers that the domain is using.

```
sohag@sohag-HP-Pavilion-Notebook:~$ whois bbc.com
   Domain Name: BBC.COM
   Registry Domain ID: 4794897_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.tucows.com
   Registrar URL: http://www.tucows.com
   Updated Date: 2019-06-15T05:12:04Z
   Creation Date: 1989-07-15T04:00:00Z
   Registry Expiry Date: 2020-07-14T04:00:00Z
   Registrar: Tucows Domains Inc.
   Registrar IANA ID: 69
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhi
bited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhi
bited
```

8) ssh : *ssh* stands for "Secure Shell". It is a protocol used to securely connect to a remote server/system

```
sohag@sohag-HP-Pavilion-Notebook:~$ ssh 192.168.0.13
ssh: connect to host 192.168.0.13 port 22: No route to host
```

9) tshark : command line super powerful packet analysis. Dump and analyze network traffic. TShark is a network protocol analyzer

```
sohag@sohag-HP-Pavilion-Notebook:~$ tshark
Capturing on 'wlo1'
tshark: The capture session could not be initiated on interface 'wlo1' (You don'
t have permission to capture on that device).
Please check to make sure you have sufficient permissions.

On Debian and Debian derivatives such as Ubuntu, if you have installed Wireshark
 from a package, try running

    sudo dpkg-reconfigure wireshark-common

selecting "<Yes>" in response to the question

    Should non-superusers be able to capture packets?

adding yourself to the "wireshark" group by running

    sudo usermod -a -G wireshark {your username}

and then logging out and logging back in again.
0 packets captured
```

10. tcpflow: capture and assemble tcpstreams . tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like *tcpdump(4)* shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted.

```
sohag@sohag-HP-Pavilion-Notebook:~$ sudo tcpflow
tcpflow: listening on wlo1
```

11) ifconfig : 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 .

```
sohag@sohag-HP-Pavilion-Notebook:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether c8:d3:ff:d4:50:17  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 11586  bytes 1189900 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11586  bytes 1189900 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

12) route : Route command is used to show/manipulate the IP routing table. It is primarily used to setup static routes to specific host or networks via an interface.

```
sohag@sohag-HP-Pavilion-Notebook:~$ 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
```

13) ip : The ip command is used to assign an address to a network interface and/or configure network interface parameters on Linux operating systems.

```
sohag@sohag-HP-Pavilion-Notebook:~$ ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
 default qlen 1000
    inet 192.168.0.108/24 brd 192.168.0.255 scope global dynamic noprefixroute w
lo1
       valid_lft 4430sec preferred_lft 4430sec
```

14) nmap : in ur network scanning ur ports . **Nmap** is a tool used for determining the hosts that are running and what services the hosts are running . The **Nmap** aka **Network Mapper** is an open source and a very versatile tool for Linux system/network administrators.

```
sohag@sohag-HP-Pavilion-Notebook:~$ nmap -v 192.168.0.116

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-12 22:11 +06
Initiating Ping Scan at 22:11
Scanning 192.168.0.116 [2 ports]
Completed Ping Scan at 22:11, 3.00s elapsed (1 total hosts)
Nmap scan report for 192.168.0.116 [host down]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
```

15) zenmap : GUI for nmap. Graphical Nmap frontend and results viewer. Zenmap is a multi-platform graphical Nmap frontend and results viewer. Zenmap aims to make Nmap easy for beginners to use while giving experienced Nmap users advanced features.

```
sohag@sohag-HP-Pavilion-Notebook:~$ zenmap
Gtk-Message:                    : Failed to load module "canberra-gtk-module"
```

16) nc : Netcat (nc) command is a powerful tool to analyze network connections, scan for open ports, transfer data etc. It is a networking utility for reading from and writing to network connections using TCP or UDP protocols.

```
root@sohag-HP-Pavilion-Notebook:~# nc -vn 192.168.0.116
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]
```

17) dir: **dir** command differs from ls command in the format of listing contents that is in default listing options. By default, **dir** command lists the files and folders in columns, sorted vertically and special characters are represented by backslash escape sequences.

```
root@sohag-HP-Pavilion-Notebook:~# dir
052.072.018.087.00443-192.168.000.108.37136    examples.desktop
052.072.018.087.00443-192.168.000.108.37138    index.html
142.250.004.189.00443-192.168.000.108.39394    index.html.1
142.250.004.189.00443-192.168.000.108.39394c1  Music
172.217.031.206.00443-192.168.000.108.36850    Pictures
192.168.000.108.36850-172.217.031.206.00443    Public
192.168.000.108.37136-052.072.018.087.00443    report.xml
192.168.000.108.37138-052.072.018.087.00443    snap
Desktop                                        Templates
Documents                                      Videos
Downloads
```

18) traceroute : Traceroute is a simple tool to show the pathway to a remote server. This can be anything from a website that you are attempting to visit, to a printer on your local network.

```
root@sohag-HP-Pavilion-Notebook:~# traceroute google.com
traceroute to google.com (216.58.197.46), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  5.118 ms  5.025 ms  4.981 ms
 2  103.83.15.166 (103.83.15.166)  5.665 ms  6.372 ms  7.637 ms
 3  103.83.15.165 (103.83.15.165)  10.884 ms  11.977 ms  11.614 ms
 4  103.244.185.129 (103.244.185.129)  15.472 ms  15.644 ms  15.586 ms
 5  103.7.248.109 (103.7.248.109)  24.251 ms  25.112 ms  26.291 ms
 6  hu-cig2-0700-cag2-0000.pico.net.bd (103.7.251.121)  67.333 ms  61.815 ms  61
.736 ms
 7  be-google-chn-tata-cig1-100.pico.net.bd (103.7.248.142)  44.519 ms  38.682 m
s  39.958 ms
 8  * * *
 9  74.125.242.129 (74.125.242.129)  40.925 ms 74.125.252.90 (74.125.252.90)  47
.024 ms 216.239.54.158 (216.239.54.158)  39.509 ms
10  74.125.242.131 (74.125.242.131)  47.473 ms 74.125.242.146 (74.125.242.146)
38.812 ms 74.125.242.155 (74.125.242.155)  47.143 ms
```

```
sohag@sohag-HP-Pavilion-Notebook:~$ tcptraceroute webserver
Running:
        traceroute -T -O info webserver
webserver: Name or service not known
Cannot handle "host" cmdline arg `webserver' on position 1 (argc 4)
```

19) iwconfig : manage wireless network settings.(see speed/frequency) . **Iwconfig** is similar to ***ifconfig***, but is dedicated to the wireless interfaces. It is used to set the parameters of the network interface which are specific to the wireless operation

```
sohag@sohag-HP-Pavilion-Notebook:~$ iwconfig
wlo1      IEEE 802.11  ESSID:"404notFound"
          Mode:Managed  Frequency:2.432 GHz  Access Point: 84:16:F9:58:1A:82
          Bit Rate=90 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=40/70  Signal level=-70 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:61  Invalid misc:13307   Missed beacon:0

eno1      no wireless extensions.

lo        no wireless extensions.
```

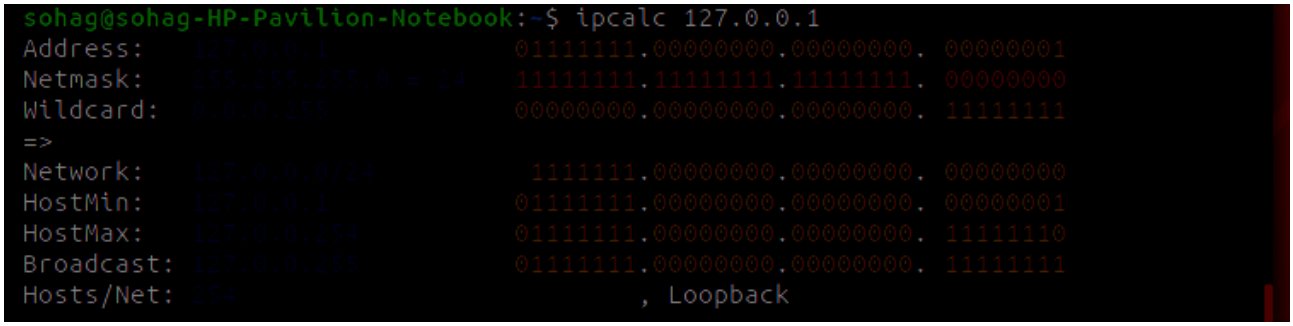
20) openssl : do literally anything with SSL certificates. OpenSSL is an open-source command line tool that is commonly used to generate private keys, create CSRs, install your SSL/TLS certificate, and identify certificate information.

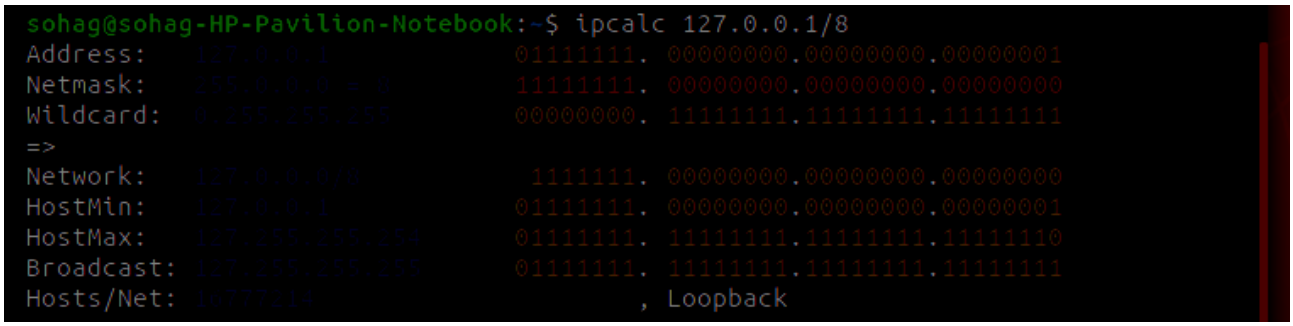
```
sohag@sohag-HP-Pavilion-Notebook:~$ openssl version
OpenSSL 1.1.1  11 Sep 2018
```

21) stunnel : make a SSL proxy for an insecure server . 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.

```
sohag@sohag-HP-Pavilion-Notebook:~$ 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 Aut
h:LIBWRAP
[ ] errno: (*__errno_location ())
[!] Invalid configuration file name "/etc/stunnel/stunnel.conf"
[!] realpath: No such file or directory (2)
```

22) ipcalc : The math behind IP addresses is convoluted. Our nice IPv4 addresses start out as 32-bit binary numbers, which are then converted to base 10 numbers in four 8-bit fields. Decimal numbers are easier to manage than long binary strings; still, calculating address ranges, netmasks, and subnets is a bit difficult and error-prone, except for the brainiacs who can do binary conversions in their heads. For the rest of us, meet `ipcalc` and `ipv6calc`.


sohag@sohag-HP-Pavilion-Notebook:~$ ipcalc 127.0.0.1
Address: 127.0.0.1 01111111.00000000.00000000. 00000001
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255 00000000.00000000.00000000. 11111111
=>
Network: 127.0.0.0/24 1111111.00000000.00000000. 00000000
HostMin: 127.0.0.1 01111111.00000000.00000000. 00000001
HostMax: 127.0.0.254 01111111.00000000.00000000. 11111110
Broadcast: 127.0.0.255 01111111.00000000.00000000. 11111111
Hosts/Net: 254 , Loopback


sohag@sohag-HP-Pavilion-Notebook:~$ ipcalc 127.0.0.1/8
Address: 127.0.0.1 01111111. 00000000.00000000.00000001
Netmask: 255.0.0.0 = 8 11111111. 00000000.00000000.00000000
Wildcard: 0.255.255.255 00000000. 11111111.11111111.11111111
=>
Network: 127.0.0.0/8 1111111. 00000000.00000000.00000000
HostMin: 127.0.0.1 01111111. 00000000.00000000.00000001
HostMax: 127.255.255.254 01111111. 11111111.11111111.11111110
Broadcast: 127.255.255.255 01111111. 11111111.11111111.11111111
Hosts/Net: 16777214 , Loopback