Mawlana Bhashani Science and Technology University

Santosh, Tangail-1902.

Lab Report

Department of Information and Communication Technology

Report No: 02
Report Name: Linux Exercise (Linux Networking Tools) .
Course Title: Network Planning and designing Lab.

Course Code: ICT-3208

Submitted By	Submitted To
Name: **Zafrul Hasan Khan** ID: **IT-18003** Session: 2017-18 3rd Year 2nd Semester Dept. of Information & Communication Technology, MBSTU.	**Nazrul Islam** **Assistant Professor,** Dept. of Information & Communication Technology, MBSTU.

Submission Date: 25-11-2020

Objectives : Install , use and understand how to Linux networking tools. To Learn how to use the tools ping, netstat, whois, nslookup, and finger etc for Linux administration and troubleshooting.

Explanation :

Linux Networking tools : One can use a variety of network tools to perform tasks such as obtaining information about other systems on your network, accessing other systems, and communicating directly with other users. Network information can be obtained using utilities such as ping, finger, traceroute, host, dig, nslookup etc

Details of Linux Networking tools :

Ping: PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ ping google.com
PING google.com (172.217.163.78) 56(84) bytes of data.
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=1 ttl=112 t
me=214 ms
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=3 ttl=112 t
me=174 ms
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=4 ttl=112 t
me=804 ms
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=7 ttl=112 t
me=339 ms
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=8 ttl=112 t
me=466 ms
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=9 ttl=112 t
me=624 ms
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=10 ttl=112
ime=175 ms
64 bytes from maa05s02-in-f14.1e100.net (172.217.163.78): icmp_seq=11 ttl=112
```

Curl : curl is a command line tool to transfer data to or from a server, using any of the supported protocols .

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ curl https://lucid
-franklin-20947c.netlify.app
<!DOCTYPE html>
<html>
<head>
  <link rel="stylesheet" href=
"https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css">
    <script src=
"https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js">
    </script>
    <script src=
"https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js">
    </script>
    <script src=
"https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js">
    </script>

    <!-- CDN link used below is compatible with this example -->
    <link rel="stylesheet" href=
"https://cdnjs.cloudflare.com/ajax/libs/bootstrap-select/1.13.1/css/bootstrap-s
elect.min.css">
    <script src=
"https://cdnjs.cloudflare.com/ajax/libs/bootstrap-select/1.13.1/js/bootstrap-se
lect.min.js">
    </script>

    <link rel="stylesheet" href="style.css">
</head>
<body>
```

HTTP : HTTP clients are utility software that enables you to download files over the Internet. Apart from being able to download files remotely, these command line tools can be used for

other tasks such as debugging and interacting with web servers.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ http  https://luci
d-franklin-20947c.netlify.app
HTTP/1.1 200 OK
Age: 576
Cache-Control: public, max-age=0, must-revalidate
Connection: keep-alive
Content-Encoding: gzip
Content-Length: 2111
Content-Type: text/html; charset=UTF-8
Date: Tue, 24 Nov 2020 13:37:32 GMT
Etag: "874a053a27a5d398ed45d578dd03ce5a-ssl-df"
Server: Netlify
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Vary: Accept-Encoding
X-NF-Request-ID: d29f3b0d-4b74-46a6-a4fa-41601d18f0ac-20712300

<!DOCTYPE html>
<html>
<head>
  <link rel="stylesheet" href=
"https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css">
    <script src=
"https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js">
    </script>
    <script src=
"https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js">
    </script>
```

Wget : Wget is the non-interactive network downloader which is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ wget  https://luci
d-franklin-20947c.netlify.app
--2020-11-24 20:15:47--  https://lucid-franklin-20947c.netlify.app/
Resolving lucid-franklin-20947c.netlify.app (lucid-franklin-20947c.netlify.app)
... 178.128.17.49, 157.230.37.202, 2400:6180:0:d1::360:1001, ...
Connecting to lucid-franklin-20947c.netlify.app (lucid-franklin-20947c.netlify.
app)|178.128.17.49|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10772 (11K) [text/html]
Saving to: ‘index.html’

index.html          100%[==================>]  10.52K  37.6KB/s    in 0.3s

2020-11-24 20:15:48 (37.6 KB/s) - ‘index.html’ saved [10772/10772]
```

Dig : The dig command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data about Domain Name Servers.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ dig -v
DiG 9.11.3-1ubuntu1.13-Ubuntu
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ dig google.com

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36293
;; 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.             167     IN      A       172.217.31.78

;; Query time: 5 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Nov 24 20:20:39 +06 2020
;; MSG SIZE  rcvd: 55
```

Whois : Whois is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProh
ibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransfer
Prohibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProh
ibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProh
ibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransfer
Prohibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProh
ibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
```

ssh : The ssh command provides a secure encrypted connection between two hosts over an insecure network.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ sudo service ssh s
tatus
[sudo] password for zafrul_hasan_nasim:
Sorry, try again.
[sudo] password for zafrul_hasan_nasim:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
```

Ngrep : . ngrep or network grep is a command line program that can be used to analyze and search network packets for a given regex pattern.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~$ sudo ngrep -q '.' 'host goo
gle.com'
interface: enp0s3 (10.0.2.0/255.255.255.0)
filter: ( host google.com ) and ((ip || ip6) || (vlan && (ip || ip6)))
match: .
```

Wireshark : Wireshark is a popular open source graphical user interface (GUI) tool for analyzing packets. However, it also provides a powerful command-line utility called TShark for people who prefer to work on the Linux command line.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~$ wireshark
21:50:52.093          Warn Could not compile "of" in colorfilters file "/home/z
afrul_hasan_nasim/.wireshark/colorfilters".
"of" is neither a field nor a protocol name.
21:50:52.093          Warn Could not compile "Checksum Errors" in colorfilters
file "/home/zafrul_hasan_nasim/.wireshark/colorfilters".
Neither "cdp.checksum_bad" nor "1" are field or protocol names.
```

TCPflow : 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.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~$ sudo tcpflow
tcpflow: listening on enp0s3
```

ifconfig : ifconfig is used to configure the system's kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ 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::153b:cca1:e7bc:dd1c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:44:19:2e  txqueuelen 1000  (Ethernet)
        RX packets 1551  bytes 1493460 (1.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1808  bytes 144811 (144.8 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 959  bytes 74606 (74.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 959  bytes 74606 (74.6 KB)
        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

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ 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: The ip command is used to assign an address to a network interface and/or configure network interface parameters on Linux operating systems.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:44:19:2e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 81443sec preferred_lft 81443sec
    inet6 fe80::153b:cca1:e7bc:dd1c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Arp: The arp command manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one, or display the current content.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ arp
Address                  HWtype  HWaddress           Flags Mask            Ifac
e
_gateway                 ether   52:54:00:12:35:02   C                     enp0
s3
```

Nmap : Nmap is an open source Linux command line tool for network exploration and security auditing. With Nmap, server administrators can quickly reveal hosts and services, search for security issues, and scan for open ports.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ nmap subdomain.ser
ver.com

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-24 22:35 +06
Failed to resolve "subdomain.server.com".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.42 seconds
```

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ nmap 192.168.56.1

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-24 22:36 +06
Note: Host seems down. If it is really up, but blocking our ping probes, try -P
n
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds
```

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

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ socat
2020/11/24 22:38:11 socat[22518] E exactly 2 addresses required (there are 0);
use option "-h" for help
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ socat - TCP4:www.e
xample.com:80
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ socat - TCP4:www.e
xample.com:80
```

Telnet : The telnet command is used for interactive communication with another host using the TELNET protocol **.**

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ telnet localhost
Trying 127.0.0.1...
```

FTP : FTP is the simplest file transfer protocol to exchange files to and from a remote computer or network.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~$ ftp ftp.cesca.es
Connected to verdaguer-ftp.cesca.cat.
220 Welcome to Anella Cientifica FTP service.
Name (ftp.cesca.es:zafrul_hasan_nasim): exit
331 This FTP server is anonymous only.
Password:
503 Login with USER first.
Login failed.
ftp> exit
221 Goodbye.
```

Netsta : Netstat is a command line utility that can be used to list out all the network (socket) connections on a system.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 zafrul-hasan-nasi:56910 5.85.222.35.bc.goo:http FIN_WAIT2
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:55877           0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:50109              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    13208    /run/systemd/journal
/syslog
unix  2      [ ACC ]     STREAM     LISTENING     13212    /run/systemd/journal
/stdout
unix  8      [ ]         DGRAM                    13214    /run/systemd/journal
/socket
unix  2      [ ]         DGRAM                    22936    /run/user/1000/syste
md/notify
unix  3      [ ACC ]     SEQPACKET  LISTENING     13210    /run/udev/control
```

Iptables : Iptables is a Linux command line firewall that allows system administrators to manage incoming and outgoing traffic via a set of configurable table rules.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ sudo iptables -L --line-number
[sudo] password for zafrul_hasan_nasim:
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

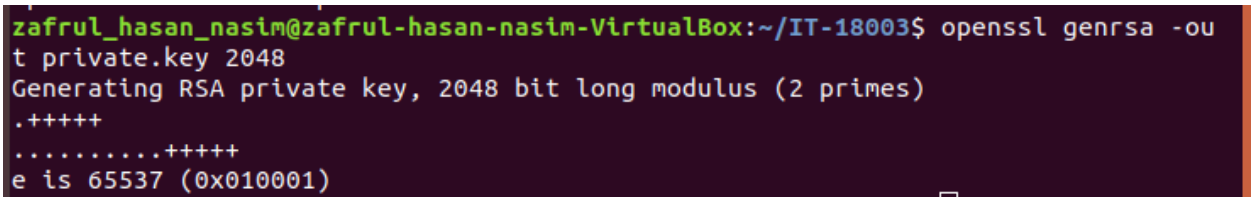
sysctl : sysctl is used to modify kernel parameters at runtime. The parameters available are those listed under /proc/sys/.

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ sysctl -a
abi.vsyscall32 = 1
debug.exception-trace = 1
debug.kprobes-optimization = 1
dev.cdrom.autoclose = 1
dev.cdrom.autoeject = 0
dev.cdrom.check_media = 0
dev.cdrom.debug = 0
dev.cdrom.info = CD-ROM information, Id: cdrom.c 3.20 2003/12/17
dev.cdrom.info =
dev.cdrom.info = drive name:            sr0
dev.cdrom.info = drive speed:           32
dev.cdrom.info = drive # of slots:      1
dev.cdrom.info = Can close tray:                1
dev.cdrom.info = Can open tray:         1
dev.cdrom.info = Can lock tray:         1
dev.cdrom.info = Can change speed:      1
dev.cdrom.info = Can select disk:       0
dev.cdrom.info = Can read multisession: 1
dev.cdrom.info = Can read MCN:          1
dev.cdrom.info = Reports media changed: 1
dev.cdrom.info = Can play audio:                1
dev.cdrom.info = Can write CD-R:                0
```

Nsenter : The **nsenter command** executes program in the namespace(s) that are specified in the **command**-line options (described below). If program is not given, then ``${SHELL}" is run (default: /bin/sh).

```
zafrul_hasan_nasim@zafrul-hasan-nasim-VirtualBox:~/IT-18003$ nsenter --v
nsenter from util-linux 2.31.1
```

OpenSSL : 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.



Conclusion : From this lab , I have known that how to install linux networking tools. I have tested to all networking tools via command line in linux terminal . I am able to efficiently collect information needed to do network design, verify routing. In this Lab, I have discussed some commonly used commands which hopefully, will help me in managing and securing my network.