PRACTICUM MODULE IV

TRANSPORT LAYER PROTOCOL

COMPETENCE:

- Students are able to use network tools to observe how the Transport layer protocol works

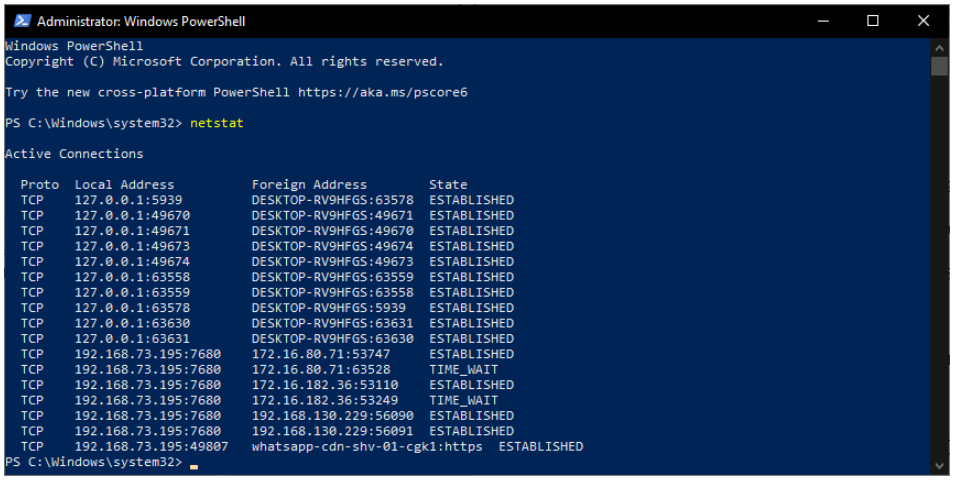
TOOLS AND MATERIALS:

- GNS3 Simulator Software
- Stable Internet Connection
- Connect to a VPN Server of the IT Department

THEORY REVIEW:

I. NETSTAT

Netstat (Network Statistics) is a text-based program to monitor network connections on a computer, to a local network (LAN) or to internet. Netstat can be used to examine connectionsof our computer when the internet connection suddenly becomes very slow and it is suspected that there are maybe some programs on the computer that become the cause. To use the command, you can access the terminal on the operating system you are using and execute the netstat command.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:5939         DESKTOP-RV9HFGS:63578  ESTABLISHED
  TCP    127.0.0.1:49670        DESKTOP-RV9HFGS:49671  ESTABLISHED
  TCP    127.0.0.1:49671        DESKTOP-RV9HFGS:49670  ESTABLISHED
  TCP    127.0.0.1:49673        DESKTOP-RV9HFGS:49674  ESTABLISHED
  TCP    127.0.0.1:49674        DESKTOP-RV9HFGS:49673  ESTABLISHED
  TCP    127.0.0.1:63558        DESKTOP-RV9HFGS:63559  ESTABLISHED
  TCP    127.0.0.1:63559        DESKTOP-RV9HFGS:63558  ESTABLISHED
  TCP    127.0.0.1:63578        DESKTOP-RV9HFGS:5939   ESTABLISHED
  TCP    127.0.0.1:63630        DESKTOP-RV9HFGS:63631  ESTABLISHED
  TCP    127.0.0.1:63631        DESKTOP-RV9HFGS:63630  ESTABLISHED
  TCP    192.168.73.195:7680    172.16.80.71:53747     ESTABLISHED
  TCP    192.168.73.195:7680    172.16.80.71:63528     TIME_WAIT
  TCP    192.168.73.195:7680    172.16.182.36:53110    ESTABLISHED
  TCP    192.168.73.195:7680    172.16.182.36:53249    TIME_WAIT
  TCP    192.168.73.195:7680    192.168.130.229:56090  ESTABLISHED
  TCP    192.168.73.195:7680    192.168.130.229:56091  ESTABLISHED
  TCP    192.168.73.195:49807   whatsapp-cdn-shv-01-cgk1:https  ESTABLISHED
PS C:\Windows\system32>
```

On the netstat utility result there are several fields :

- Proto. The proto column indicates the type of protocol used, TCP or UDP.
- Local Address. This column describes the address and port number on our computer where it was actively connecting. The above example 192.168.73.195 is the host address of my computer and 7680 is the port number used by my computer in connection.
- Foreign Address. This column shows the connection that the local address is aiming for and its port number. From the example , my computer is connecting to a DEBIAN server via ssh (port 22) which means it is connecting to an ssh server.
- State. This column shows the status of the connection that is active. ESTABLISHED means that it is connected to other computers and ready to send data.

  Possible states are :
  - LISTENING -> ready to make connections
  - SYN_SENT -> deliver SYN packets
  - SYN_RECEIVED -> receive SYN packages
  - ESTABLISHED - > connection occurs and ready to transmit data
  - TIME_WAIT -> waiting for connection

a) netstat on Windows operating system

On the Windows operating system, the netstat command has several options that can be used. These options include:

- netstat -a <host/ip target>, displaying all connections both listening and non-listening
- netstat -e <host/ip target>, displaying statistics of packets sent and received
- netstat -n <host/ip target>, displaying addresses and ports in numeric form
- netstat -o <host/ip target>, displaying PID (Process ID) for each connection
- netstat -s <host/ ip target>, displaying statistics per protocol
- netstat -r <host/ip target>, displaying routing table
- netstat -p <host/ip target>, displays statistics based on specific ports

b) netstat on Linux operating system

On Linux operating systems, the netstat command has several options that can be used. These options include:

- netstat -a <host/ip target>, displays all connections both listening and non-listening
- netstat -l <host/ip target>, displaying all listening connections only
- netstat -s <host/ ip target>, displaying statistics per protocol
- netstat -n <host/ip target>, displaying in numeric form
- netstat -o <host/ip target>, display timer
- netstat -g <host/ ip target>, displayed by group membership
- netstat -i <host/ip target>, displaying network interface table
- netstat -p <host/ip target>, displaying port specifics on the target machine
- netstat -O <host/ip target>, identifies machine operating system
- netstat -sV <host/ip target>, identifies services running on ports In addition to

the options described above, there are still other options that can be used in netstat command. You can see the option by manually opening the command. The trick is to run the “man netstat” command on your terminal.

II. NMAP

Nmap ("Network Mapper") is an open source tool for network security exploration and auditing. It is designed to quickly monitor big network, although it can also works on a single host. Nmap uses raw IP packets in a sophisticated way to determine which hosts are available on the network, what services (application names and versions) are provided, what operating system (and version) are used, what type of firewall/packet filter is used, and a number of other characteristics. Although Nmap is commonly used for security audits, many system and network administrators find it useful for routine tasks such as network inventory, scheduling service upgrade, and monitoring host or service uptime.

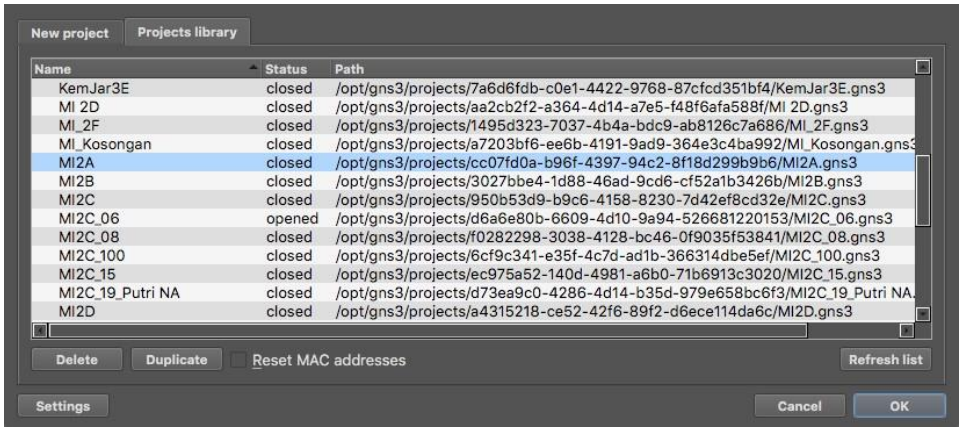
```
debian@debian:~$ nmap repolinux.jti.polinema.ac.id
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-21 10:45 WIB
Nmap scan report for repolinux.jti.polinema.ac.id (192.168.60.22)
Host is up (0.00083s latency).
rDNS record for 192.168.60.22: training.jti.polinema.ac.id
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
5357/tcp open  wsdapi
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Nmap output is a list of targets that are checked, with additional information depending on the options used. That information is a "port table". The table lists port and protocol numbers, service names, and statuses. The status is open, filtered, closed, or unfiltered. Open means that the application on the target machine is listening for the connection/packet on that port. Filtered means that a firewall, filter, or other network barrier blocks the port so that Nmap cannot tell if it is open or closed. Closed ports do not have applications that are listening, although they can open at any time. Ports are classified as unfiltered when they respond to Nmap probes, but Nmap cannot determine whether they are open or closed. Nmap reports a combination of open|filtered and closed|filtered states when it cannot determine which state describes a port.

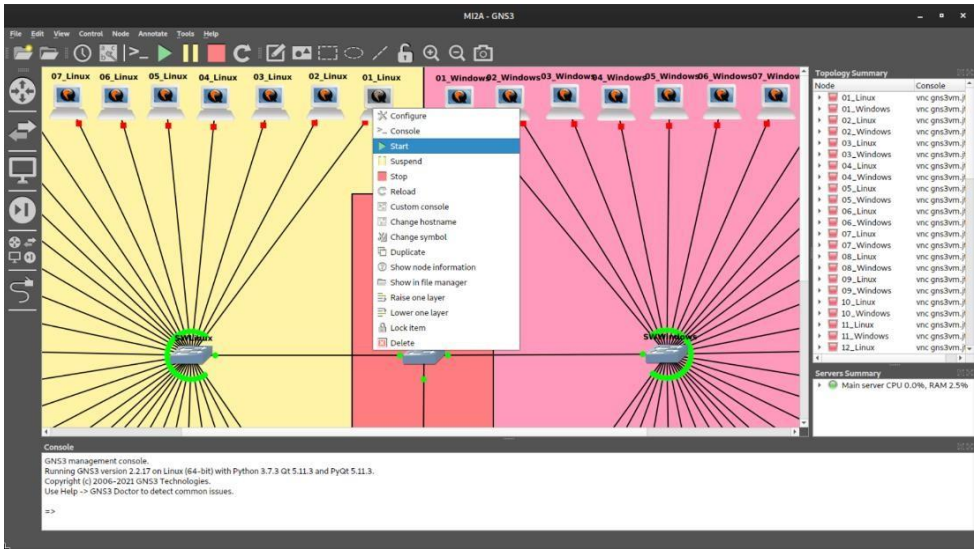
PRACTICUM PREPARATION

1. Connect your computer to the internet network.
2. Connect your computer to an Information Technology Department VPN server using the OpenVPN Connect app. Use the profile, username and password you have obtained at previous meetings.
3. Once connected to an OpenVPN server, open the GNS3 app on your computer.
4. In the initial view of the GNS3 application window, select the Project library tab. Then select the project that has been set up for your class (e.g. TI2I). Then remove the check mark on the Reset MAC Address option. Then press the OK button.

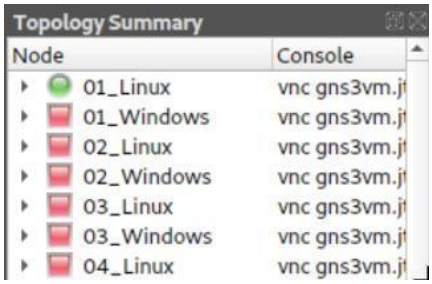


5. Then after the project opens in the main window of the GNS3 application, you can adjust the zoom on the appearance of the project to your liking by pressing the positive magnifying glass button (to enlarge) or the negative magnifying glass button (to minimize) on the toolbar at the top of the window.

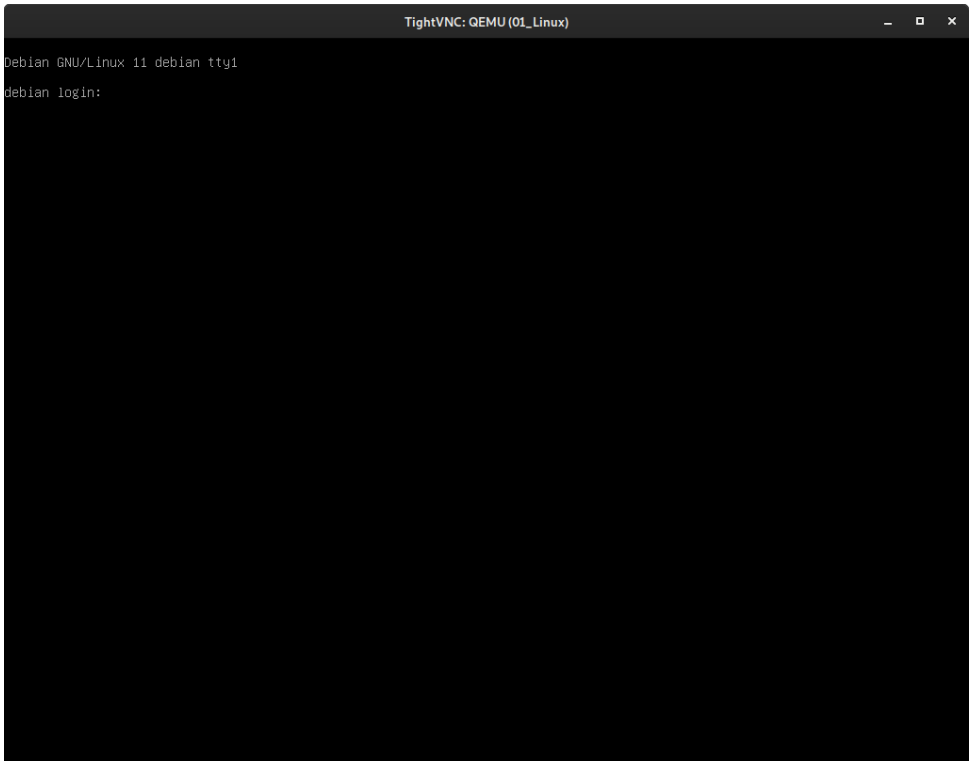
6. Then you can turn on the computer you are going to use. To do this, right-click on the logo of the computer you are going to use, and then select the Start option.



7. Wait for a while and you can check the status of whether or not your computer is on in the Topology Summary sidebar to the right of the window.



8. Once your computer is on, access your computer by double-clicking (2x) on your computer logo. Then a new window will appear, which is the appearance of your computer as shown below .



9. You can use the computer for practicum according to the next steps.

PRACTICUM STEPS

I. Netstat On Linux Operating System

1. Access your linux computer in an open project .
2. Make sure your computer connection is connected to the internet, by running ping commands to the www.google.com. Make sure there are “reply” words on the output of the command. Stop the ping utility by pressing the keyboard key combination **ctrl+c**.

```
debian@debian:~$ ping google.com
PING google.com (216.239.38.120) 56(84) bytes of data.
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=1 ttl=113 time=31.4 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=2 ttl=113 time=28.6 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=3 ttl=113 time=28.5 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=4 ttl=113 time=28.5 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=5 ttl=113 time=28.8 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 28.468/29.157/31.357/1.106 ms
```

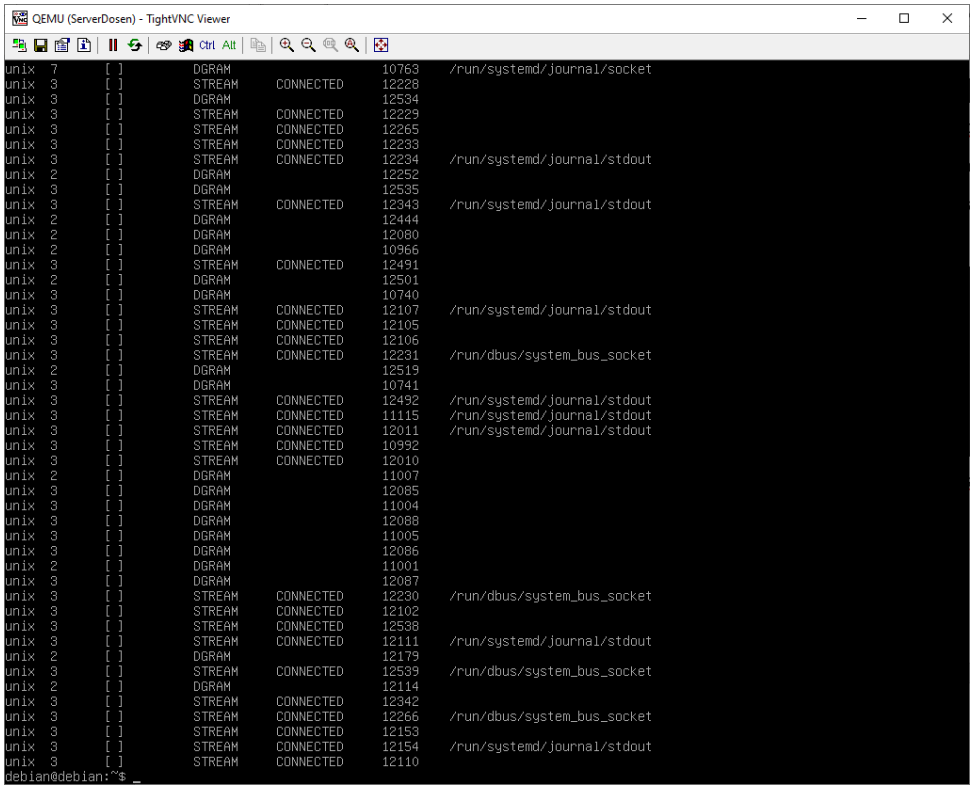
3. If there are not “reply” in the result, ask the lecturer / instructor to get an internet connection.
4. Then update the repository index on your linux computer by running the "sudo apt update" command, then entering the password of the linux user you are using. And make sure no error words appear in the upgrade process.

```
debian@debian:~$ sudo apt update
Hit:1 http://repolinux.jti.polinema.ac.id/debian bullseye InRelease
Hit:2 http://repolinux.jti.polinema.ac.id/debian bullseye-updates InRelease
Hit:3 http://security.debian.org/debian-security bullseye-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
```

5. On linux operating systems, the netstat utility resides in the **net-tools** application package. Therefore , install a **net-tools package** to be able to use the netstat utility. Run the command "**sudo apt install net-tools**" to perform the installation of the package.

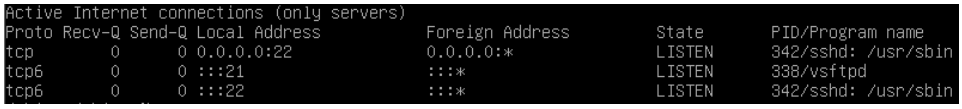
```
debian@debian:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 250 kB of archives.
After this operation, 1,015 kB of additional disk space will be used.
Get:1 http://repolinux.jti.polinema.ac.id/debian bullseye/main amd64 net-tools amd64 1.60+git20181103.0eebece-1 [250 kB]
Fetched 250 kB in 0s (676 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 28288 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1_amd64.deb ...
Unpacking net-tools (1.60+git20181103.0eebece-1) ...
Setting up net-tools (1.60+git20181103.0eebece-1) ...
Processing triggers for man-db (2.9.4-2) ...
debian@debian:~$
```

6. Then after the application package is successfully installed, run the "netstat" command.



```
QEMU (ServerDosen) - TightVNC Viewer
unix  7      [ ]         DGRAM                    10763    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     12228
unix  3      [ ]         DGRAM                    12534
unix  3      [ ]         STREAM     CONNECTED     12229
unix  3      [ ]         STREAM     CONNECTED     12265
unix  3      [ ]         STREAM     CONNECTED     12233
unix  3      [ ]         STREAM     CONNECTED     12234    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    12252
unix  3      [ ]         DGRAM                    12535
unix  3      [ ]         STREAM     CONNECTED     12343    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    12444
unix  2      [ ]         DGRAM                    12080
unix  2      [ ]         DGRAM                    10966
unix  3      [ ]         STREAM     CONNECTED     12491
unix  2      [ ]         DGRAM                    12501
unix  3      [ ]         DGRAM                    10740
unix  3      [ ]         STREAM     CONNECTED     12107    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12105
unix  3      [ ]         STREAM     CONNECTED     12106
unix  3      [ ]         STREAM     CONNECTED     12231    /run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    12519
unix  3      [ ]         DGRAM                    10741
unix  3      [ ]         STREAM     CONNECTED     12492    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11115    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12011    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     10992
unix  3      [ ]         STREAM     CONNECTED     12010
unix  2      [ ]         DGRAM                    11007
unix  3      [ ]         DGRAM                    12085
unix  3      [ ]         DGRAM                    11004
unix  3      [ ]         DGRAM                    12088
unix  3      [ ]         DGRAM                    11005
unix  3      [ ]         DGRAM                    12086
unix  2      [ ]         DGRAM                    11001
unix  3      [ ]         DGRAM                    12087
unix  3      [ ]         STREAM     CONNECTED     12230    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     12102
unix  3      [ ]         STREAM     CONNECTED     12538
unix  3      [ ]         STREAM     CONNECTED     12111    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    12179
unix  3      [ ]         STREAM     CONNECTED     12539    /run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    12114
unix  3      [ ]         STREAM     CONNECTED     12342
unix  3      [ ]         STREAM     CONNECTED     12266    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     12153
unix  3      [ ]         STREAM     CONNECTED     12154    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12110
debian@debian:~$ _
```

7. Take a picture of the output of the netstat command, and explain the meaning of some ot the display output on your linux computer.
8. Add the appropriate options/parameters to the netstat command to display the ports that are open and listen on your linux computer along with its process name or PID. Don't forget to use super user (sudo) access to be able to display the details of the process name or PID of the application that is using the port.



```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      342/sshd: /usr/sbin
tcp6       0      0 :::21                   :::*                    LISTEN      338/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      342/sshd: /usr/sbin
```

9. Try to use the 5 options that have been described on the theory. Take a picture of the command view output with the option you have selected. And give an explanation or analysis of the meaning of the display you get.

II. Netstat On Windows Operating System

1. Access your windows computer in an open project.
2. Make sure your computer connection is connected to the internet, by running ping commands to www.google.com on the command prompt terminal. Make sure there are “reply” words on the output of the command.

```
C:\Documents and Settings\XP>ping google.com

Pinging google.com [172.217.194.101] with 32 bytes of data:

Reply from 172.217.194.101: bytes=32 time=29ms TTL=103
Reply from 172.217.194.101: bytes=32 time=28ms TTL=103
Reply from 172.217.194.101: bytes=32 time=28ms TTL=103
Reply from 172.217.194.101: bytes=32 time=28ms TTL=103

Ping statistics for 172.217.194.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 29ms, Average = 28ms
```

3. If there are no **reply** words, ask the lecturer / instructor to get an internet connection.

4. If you have been able to connect to the internet network, run the command "netstat".

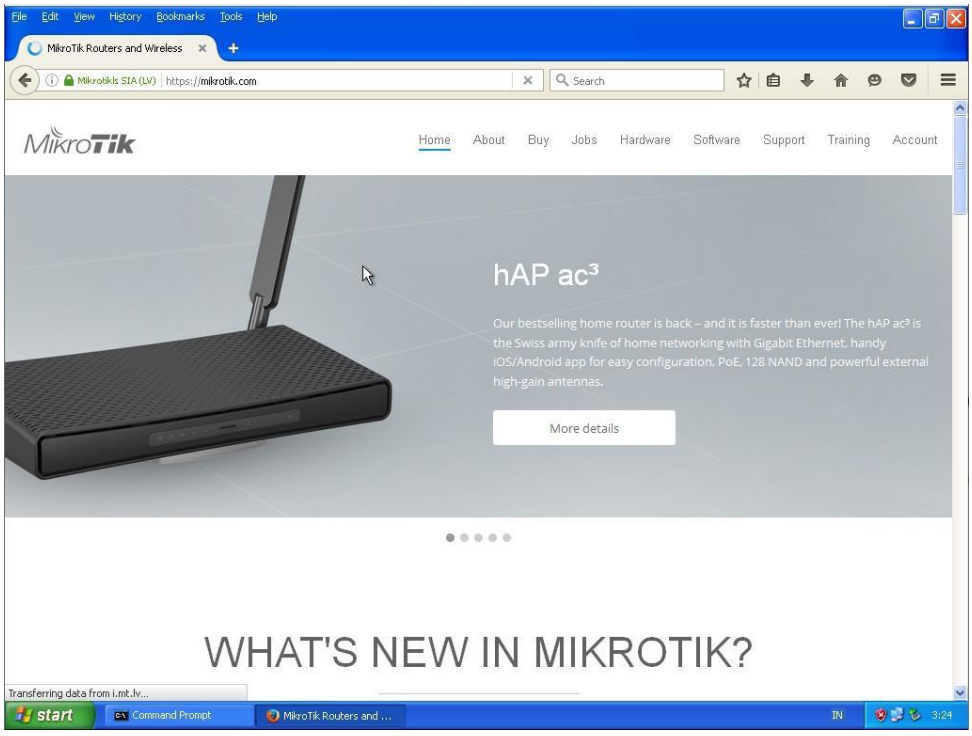
```
C:\Documents and Settings\XP>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    gns3-winxp:1032        51.143.49.66:http      ESTABLISHED
```

5. Take a picture of the output of the netstat command, and explain the meaning of the display output on your linux computer.

6. Try to open a web page using the browser application on your windows computer.



7. Rerun the "netstat" command on your command prompt.

```
C:\Documents and Settings\XP>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    gns3-winxp:1041        ec2-54-71-191-188.us-west-2.compute.amazonaws.co
m:http  ESTABLISHED
  TCP    gns3-winxp:1043        ec2-44-238-161-76.us-west-2.compute.amazonaws.co
m:https  ESTABLISHED
  TCP    gns3-winxp:1045        server-52-222-158-62.cdg52.r.cloudfront.net:http
s  ESTABLISHED
  TCP    gns3-winxp:1046        117.18.237.29:http     ESTABLISHED
  TCP    gns3-winxp:1047        si-in-f106.1e100.net:https  ESTABLISHED
  TCP    gns3-winxp:1048        sm-in-f94.1e100.net:http  ESTABLISHED
  TCP    gns3-winxp:1049        ec2-52-37-141-62.us-west-2.compute.amazonaws.com
:https  ESTABLISHED
  TCP    gns3-winxp:1050        server-54-230-151-60.sin2.r.cloudfront.net:http
 ESTABLISHED
  TCP    gns3-winxp:1051        server-54-230-151-60.sin2.r.cloudfront.net:http
 TIME_WAIT
  TCP    gns3-winxp:1053        server-52-84-228-121.sin2.r.cloudfront.net:https
  ESTABLISHED
  TCP    gns3-winxp:1056        server-52-84-228-36.sin2.r.cloudfront.net:https
 ESTABLISHED
  TCP    gns3-winxp:1058        117.18.237.29:http     ESTABLISHED
  TCP    gns3-winxp:1059        117.18.237.29:http     TIME_WAIT
  TCP    gns3-winxp:1060        117.18.237.29:http     TIME_WAIT
  TCP    gns3-winxp:1061        117.18.237.29:http     TIME_WAIT
  TCP    gns3-winxp:1062        117.18.237.29:http     TIME_WAIT
  TCP    gns3-winxp:1063        117.18.237.29:http     TIME_WAIT
  TCP    gns3-winxp:1064        sb-in-f113.1e100.net:https  ESTABLISHED
  TCP    gns3-winxp:1065        159.148.172.206:https  ESTABLISHED
  TCP    gns3-winxp:1066        159.148.172.206:https  ESTABLISHED
  TCP    gns3-winxp:1067        159.148.172.206:https  ESTABLISHED
  TCP    gns3-winxp:1069        sa-in-f154.1e100.net:https  ESTABLISHED
  TCP    gns3-winxp:1070        159.148.172.206:https  ESTABLISHED
  TCP    gns3-winxp:1071        159.148.172.206:https  ESTABLISHED
  TCP    gns3-winxp:1072        159.148.172.206:https  TIME_WAIT
  TCP    gns3-winxp:1039        localhost:1040         ESTABLISHED
  TCP    gns3-winxp:1040        localhost:1039         ESTABLISHED
```

8. Take a picture of the output of the netstat command, and explain the meaning of the display output on your linux computer.
9. Add the appropriate option to the netstat command to display all ports that are being used by the tcp protocol.

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    gns3-winxp:epmap       gns3-winxp:0           LISTENING
  TCP    gns3-winxp:microsoft-ds  gns3-winxp:0           LISTENING
  TCP    gns3-winxp:netbios-ssn  gns3-winxp:0           LISTENING
  TCP    gns3-winxp:1045        server-52-222-158-62.cdg52.r.cloudfront.net:http
s  TIME_WAIT
  TCP    gns3-winxp:1046        117.18.237.29:http     TIME_WAIT
  TCP    gns3-winxp:1047        si-in-f106.1e100.net:https  TIME_WAIT
  TCP    gns3-winxp:1048        sm-in-f94.1e100.net:http  TIME_WAIT
  TCP    gns3-winxp:1050        server-54-230-151-60.sin2.r.cloudfront.net:http
 ESTABLISHED
  TCP    gns3-winxp:1053        server-52-84-228-121.sin2.r.cloudfront.net:https
  TIME_WAIT
  TCP    gns3-winxp:1056        server-52-84-228-36.sin2.r.cloudfront.net:https
 TIME_WAIT
  TCP    gns3-winxp:1058        117.18.237.29:http     TIME_WAIT
  TCP    gns3-winxp:1064        sb-in-f113.1e100.net:https  TIME_WAIT
  TCP    gns3-winxp:1069        sa-in-f154.1e100.net:https  TIME_WAIT
  TCP    gns3-winxp:1073        sd-in-f93.1e100.net:https  ESTABLISHED
  TCP    gns3-winxp:1074        ec2-54-148-159-250.us-west-2.compute.amazonaws.c
om:https  TIME_WAIT
  TCP    gns3-winxp:1075        201.181.244.35.bc.googleusercontent.com:https  E
STABLISHED
  TCP    gns3-winxp:1028        gns3-winxp:0           LISTENING
  TCP    gns3-winxp:1039        localhost:1040         ESTABLISHED
  TCP    gns3-winxp:1040        localhost:1039         ESTABLISHED
```

10. Try using the 3 options that have been described on the basis of theory. Take a picture of the command view output with the option you have selected. And give an explanation or analysis of the meaning of the display you get.

III. NMAP

1. Access your linux computer in the project .
2. Make sure your computer connection can still connect to the internet, by running ping commands to the www.google.com. Make sure there are replay words on the output of the command. Stop the ping utility by pressing the keyboard key combination ctrl+c.

```
debian@debian:~$ ping google.com
PING google.com (216.239.38.120) 56(84) bytes of data.
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=1 ttl=113 time=31.4 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=2 ttl=113 time=28.6 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=3 ttl=113 time=28.5 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=4 ttl=113 time=28.5 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=5 ttl=113 time=28.8 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 28.468/29.157/31.357/1.106 ms
```

3. If you are not connected, ask the lecturer / instructor to get an internet connection back.
4. Perform nmap application package inventory to be able to use the nmap utility. Run the command "sudo apt install nmap" to perform the installation of the package. Enter the password of your debian user if requested. Then type the letter "Y" and press the enter key to approve the installation.

```
debian@debian:~$ sudo apt install nmap
[sudo] password for debian:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.3-0 libpcap0.8 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.3-0 libpcap0.8 lua-lpeg nmap nmap-common
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 6,425 kB of archives.
After this operation, 27.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

5. Then after the application package is successfully installed, run the command "nmap localhost".

```
debian@debian:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-21 10:36 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

6. The above command is used to see which ports are open on your linux computer .
7. Try to see the ports that are open on the lecturer's server computer with ip address 10.10.10.5. The trick, replace the word "localhost" with the IP address "10.10.10.5". Take a picture of the output of the command. Describe what ports are open and what services are running on those ports.
8. Try to see the ports that open on the server computer of the local repository of the Information Technology Department that has an address repolinux.jti.polinema.ac.id. Take a picture of the output of the command. Describe what ports are open and what services are running on those ports.
9. Try to add the "Pn" option to the nmap command that you run in steps 7 and 8. Take a picture of the output of the command. Describe what ports are open, what services are running on those ports, and the difference from the appearance of commands you did earlier in steps 8 and 9.

ASSIGNMENT

1. Make a report containing *screeshots* and *step-by-step* explanations of the three practicum steps you have done.
2. Collect the reports you create in pdf file form by uploading them to the lms server as in previous practicums.
3. Do practicum as much as possible during practicum hours. Outside of practicum hours, there will be possible speed problems from each computer in the project .
4. Happy work.