

Mata Kuliah Jaringan Komputer
Dosen : Ade Ismail, S.Kom., M.TI.

Praktikum 04
Protokol Lapisan Transport

oleh :



Nama : Muhammad Farhan Fahraby
Kelas : 2I
No Urut : 18
No HP : 082331269664
email : fahrabyf@gmail.com

MODUL PRAKTIKUM IV

PROTOKOL LAPISAN TRANSPORT

KOMPETENSI:

- ❖ Mahasiswa mampu menggunakan tool jaringan untuk mengamati cara kerja protokol lapisan Transport

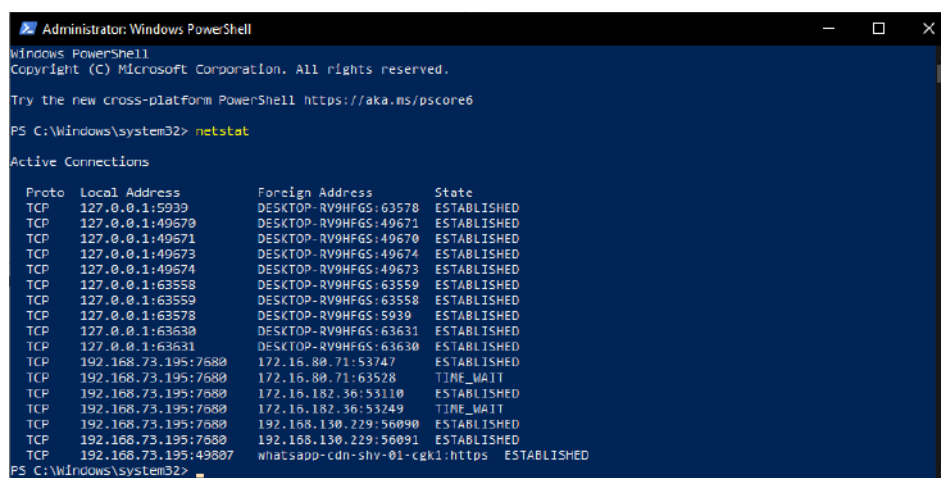
ALAT DAN BAHAN:

- Software Simulator GNS3
- Koneksi Internet Yang Stabil
- Terkoneksi ke Server VPN Jurusan TI

ULASAN TEORI:

I. NETSTAT

Netstat (Network Statistics) adalah program berbasis teks yang berfungsi untuk memantau koneksi jaringan pada suatu komputer, baik itu jaringan lokal (LAN) maupun jaringan internet. Netstat dapat digunakan jika pada suatu ketika sedang beraktivitas di internet kemudian tiba-tiba koneksi menjadi sangat lambat dan dicurigai ada program di komputer yang menjadi penyebabnya. Untuk menggunakan perintah tersebut, Anda dapat mengakses terminal pada sistem operasi yang Anda gunakan dan menjalankan perintah netstat.



```
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>
```

Pada tampilan utilitas netstat terdapat beberapa keterangan, antara lain:

- Proto. Kolom proto menunjukkan jenis protokol yang dipakai bisa TCP atau UDP.
- Local Address. Kolom ini menjelaskan alamat dan nomor port yang ada di komputer yang mana saat itu sedang aktif melakukan koneksi. Contoh diatas 192.168.88.125 adalah nama host dari komputer saya dan 50059 adalah nomor port di komputer saya yang sedang melakukan koneksi.
- Foreign Address. Kolom ini menunjukkan koneksi yang dituju oleh local address beserta nomor portnya. Contoh diatas komputer sedang koneksi ke server DEBIAN melalui ssh (port 22) yang artinya sedang koneksi ke server ssh.
- State. Kolom ini menunjukkan status dari koneksi yang sedang terjadi. ESTABLISHED artinya sudah terhubung dengan komputer lain dan siap mengirimkan data.

State yang mungkin terjadi :

- LISTENING -> siap untuk melakukan koneksi
- SYN_SENT -> mengirimkan paket SYN
- SYN_RECEIVED -> menerima paket SYN
- ESTABLISHED -> koneksi terjadi dan siap mengirimkan data
- TIME_WAIT -> sedang menunggu koneksi

a) netstat pada sistem operasi Windows

Pada sistem operasi Windows, perintah netstat memiliki beberapa opsi yang dapat digunakan. Opsi-opsi tersebut antara lain:

- netstat -a <host/ip target>, menampilkan semua koneksi baik yang listening maupun yang tidak
- netstat -e <host/ip target>, menampilkan statistik paket yang dikirim dan yang diterima
- netstat -n <host/ip target>, menampilkan alamat dan port dalam bentuk numerik
- netstat -o <host/ip target>, menampilkan PID (Process ID) untuk setiap koneksi
- netstat -s <host/ip target>, menampilkan statistik per protokol
- netstat -r <host/ip target>, menampilkan routing table
- netstat -p <host/ip target>, menampilkan statistik berdasarkan port tertentu

b) netstat pada sistem operasi Linux

Pada sistem operasi Linux, perintah netstat memiliki beberapa opsi yang dapat digunakan. Opsi-opsi tersebut antara lain:

- netstat -a <host/ip target>, menampilkan semua koneksi baik yang listening maupun yang tidak
- netstat -l <host/ip target>, menampilkan semua koneksi yang listening saja
- netstat -s <host/ip target>, menampilkan statistik per protokol
- netstat -n <host/ip target>, menampilkan dalam bentuk numerik
- netstat -o <host/ip target>, menampilkan timer
- netstat -g <host/ip target>, menampilkan berdasarkan group membership
- netstat -i <host/ip target>, menampilkan tabel network interface
- netstat -p <host/ip target>, menampilkan spesifik port pada mesin target
- netstat -O <host/ip target>, mengidentifikasi sistem operasi mesin
- netstat -sV <host/ip target>, mengidentifikasi service yang berjalan pada port

Selain opsi yang telah dijabarkan diatas, masih ada opsi-opsi lain yang dapat digunakan dalam perintah netstat. Anda dapat melihat opsi tersebut dengan membuka manual dari perintah tersebut. Caranya adalah dengan menjalankan perintah man netstat pada terminal Anda.

II. NMAP

Nmap ("Network Mapper") merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

```

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  wsddapi
8080/tcp  open  http-proxy

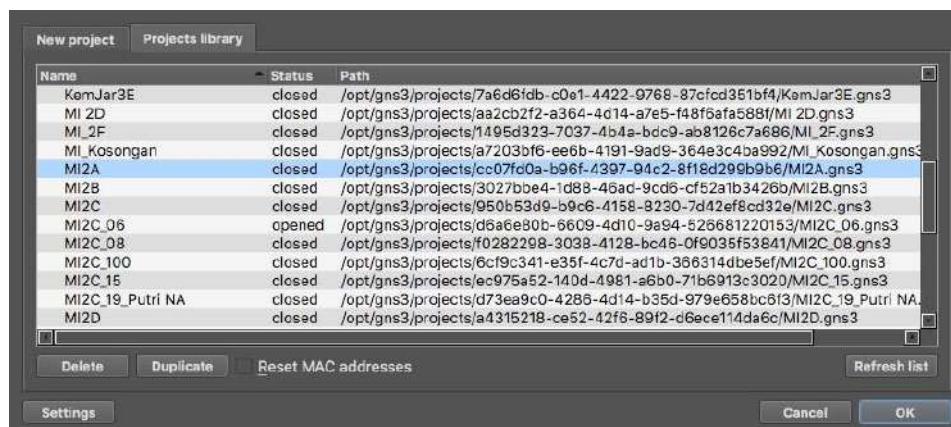
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

```

Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Informasi itu adalah “tabel port”. Tabel tersebut berisi daftar angka port dan protokol, nama layanan, dan status. Statusnya adalah terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (listening) untuk koneksi/paket pada port tersebut. Difilter berarti bahwa sebuah firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup port tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. Port digolongkan sebagai tidak difilter ketika mereka menanggapi probe Nmap, namun Nmap tidak dapat menentukan apakah mereka terbuka atau tertutup. Nmap melaporkan kombinasi status open|filtered dan closed|filtered ketika ia tidak dapat menentukan status manakah yang menggambarkan sebuah port.

PERSIAPAN PRAKTIKUM

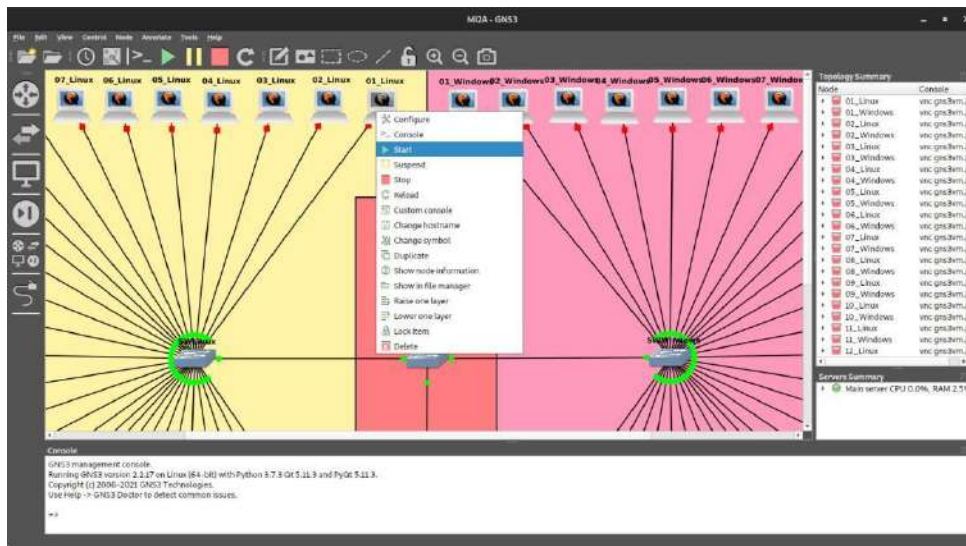
1. Koneksikan komputer Anda ke jaringan internet.
2. Koneksikan komputer Anda ke server VPN Jurusan Teknologi Informasi menggunakan aplikasi OpenVPN Connect. Gunakan profile, username dan password yang telah Anda dapatkan pada pertemuan sebelumnya.
3. Setelah terhubung dengan server OpenVPN, buka aplikasi GNS3 pada komputer Anda.
4. Pada tampilan awal jendela aplikasi GNS3, pilih tab Project library. Kemudian pilih project yang telah disiapkan untuk kelas Anda (misal MI2A). Kemudian hilangkan tanda centang pada opsi Reset MAC Address. Kemudian tekan tombol OK.



5. Kemudian setelah project terbuka pada jendela utama aplikasi GNS3, Anda dapat menyesuaikan zoom pada tampilan project tersebut sesuai keinginan Anda dengan menekan tombol kaca pembesar positif (untuk memperbesar) atau tombol kaca pembesar negatif (untuk memperkecil) yang ada pada toolbar bagian atas jendela tersebut.



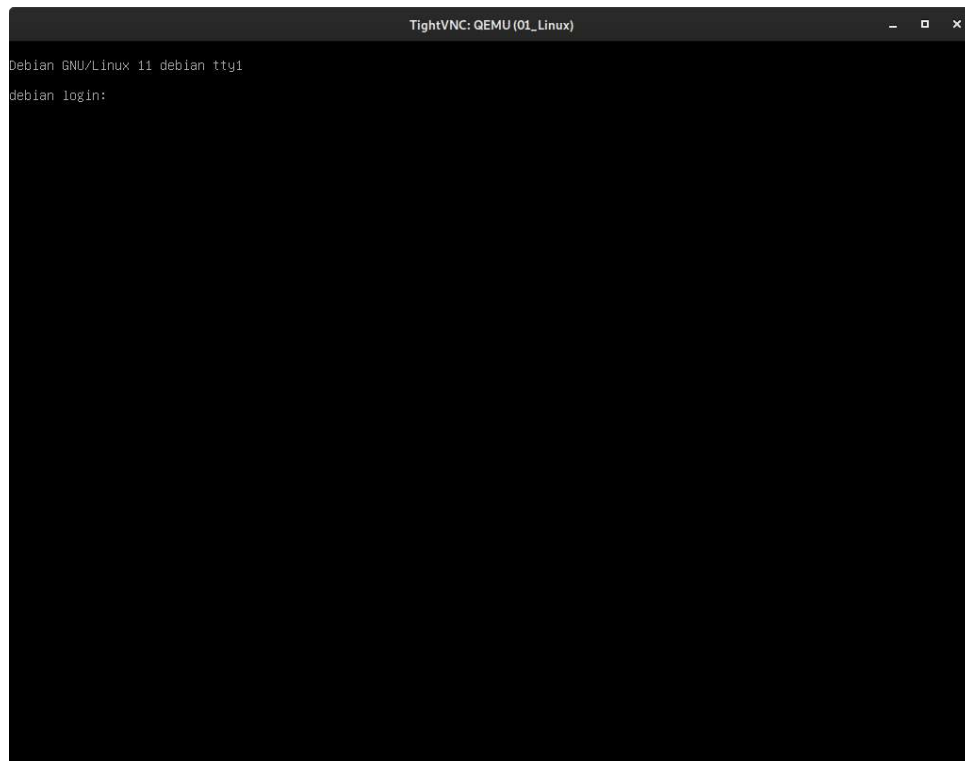
6. Kemudian Anda dapat menyalakan komputer yang akan Anda gunakan. Caranya, klik kanan pada logo komputer yang akan Anda gunakan, kemudian pilih opsi Start.



7. Tunggu beberapa saat dan Anda dapat memeriksa status menyala atau tidaknya komputer Anda pada sidebar Topology Summary sebelah kanan jendela tersebut.

Topology Summary	
Node	Console
01_Linux	vnc gns3vm.ji
01_Windows	vnc gns3vm.ji
02_Linux	vnc gns3vm.ji
02_Windows	vnc gns3vm.ji
03_Linux	vnc gns3vm.ji
03_Windows	vnc gns3vm.ji
04_Linux	vnc gns3vm.ji

8. Setelah komputer Anda menyala, akses komputer Anda dengan melakukan klik dua kali (2x) pada logo komputer Anda. Maka akan muncul jendela baru, yaitu tampilan komputer Anda seperti gambar di bawah ini.

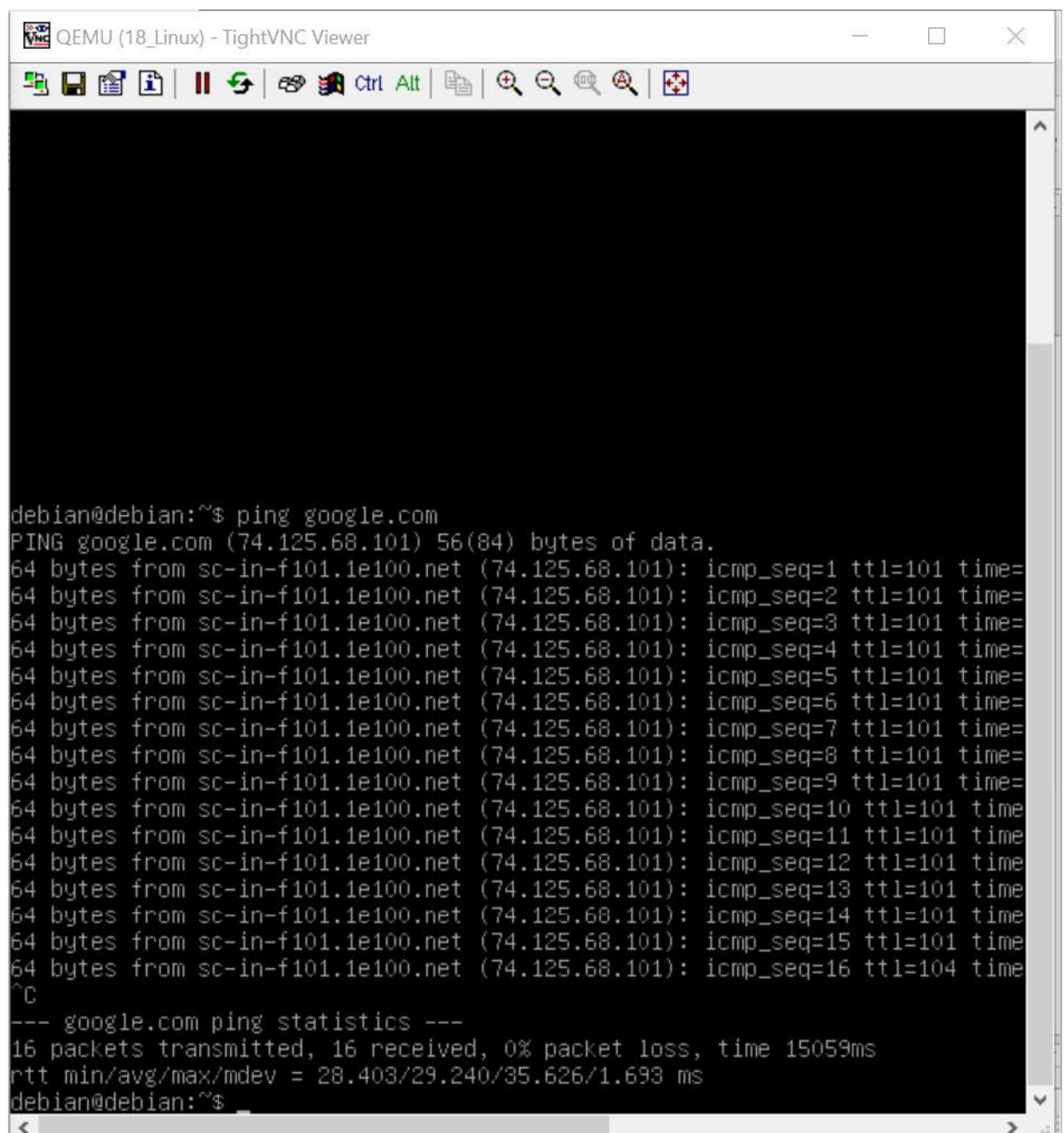


9. Anda dapat menggunakan komputer tersebut untuk praktikum sesuai dengan langkah-langkah selanjutnya.

LANGKAH PRAKTIKUM

I. Netstat Pada Sistem Operasi Linux

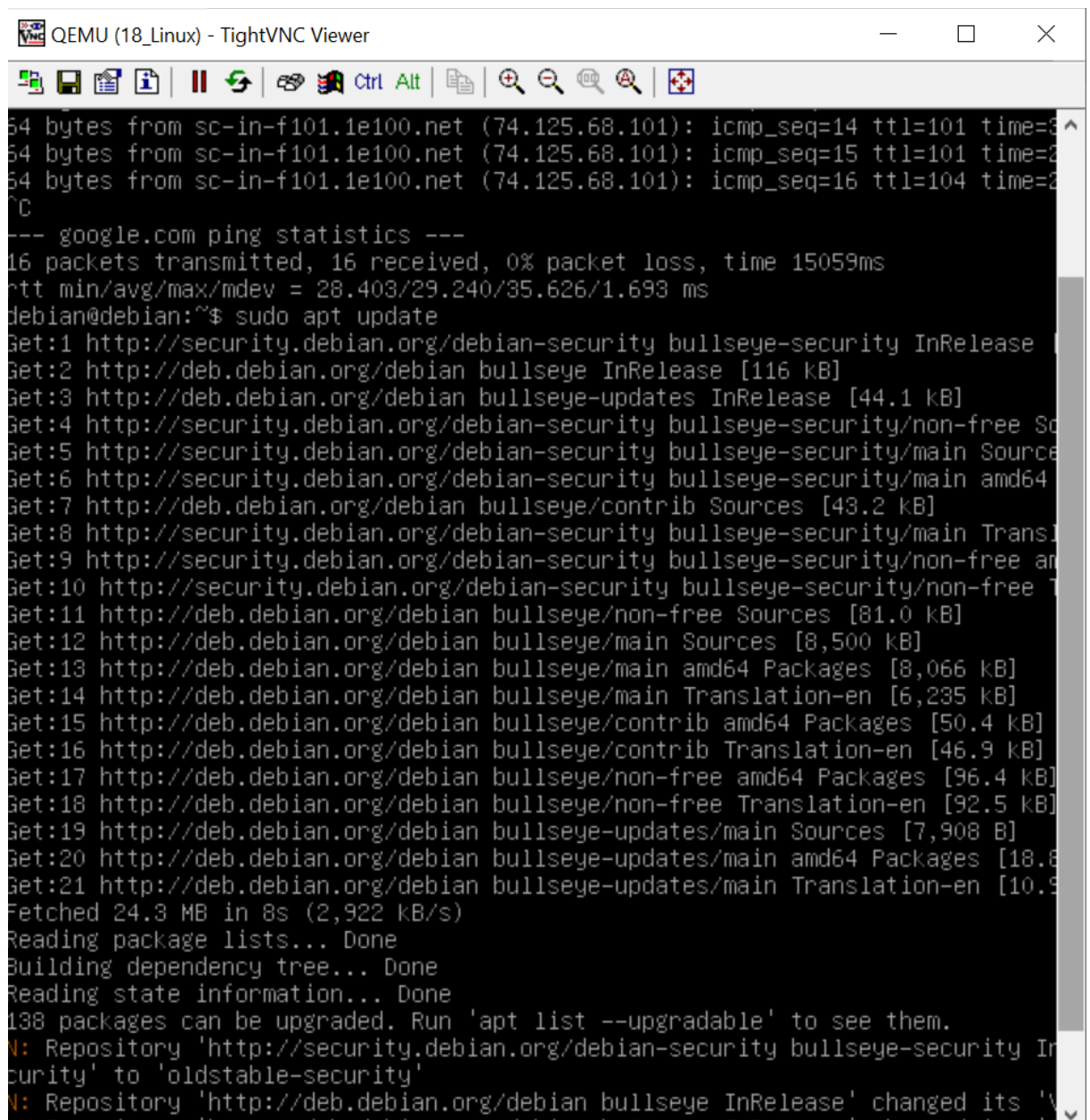
1. Akses komputer linux Anda dalam project yang telah terbuka.
2. Pastikan koneksi komputer anda sudah terhubung dengan internet, dengan menjalankan perintah ping ke www.google.com. Pastikan terdapat kata-kata replay pada output perintah tersebut. Hentikan utilitas ping dengan menekan kombinasi tombol keyboard ctrl+c.



```
QEMU (18_Linux) - TightVNC Viewer
debian@debian:~$ ping google.com
PING google.com (74.125.68.101) 56(84) bytes of data:
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=1 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=2 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=3 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=4 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=5 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=6 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=7 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=8 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=9 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=10 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=11 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=12 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=13 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=14 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=15 ttl=101 time=
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=16 ttl=104 time=
^C
--- google.com ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15059ms
rtt min/avg/max/mdev = 28.403/29.240/35.626/1.693 ms
debian@debian:~$
```

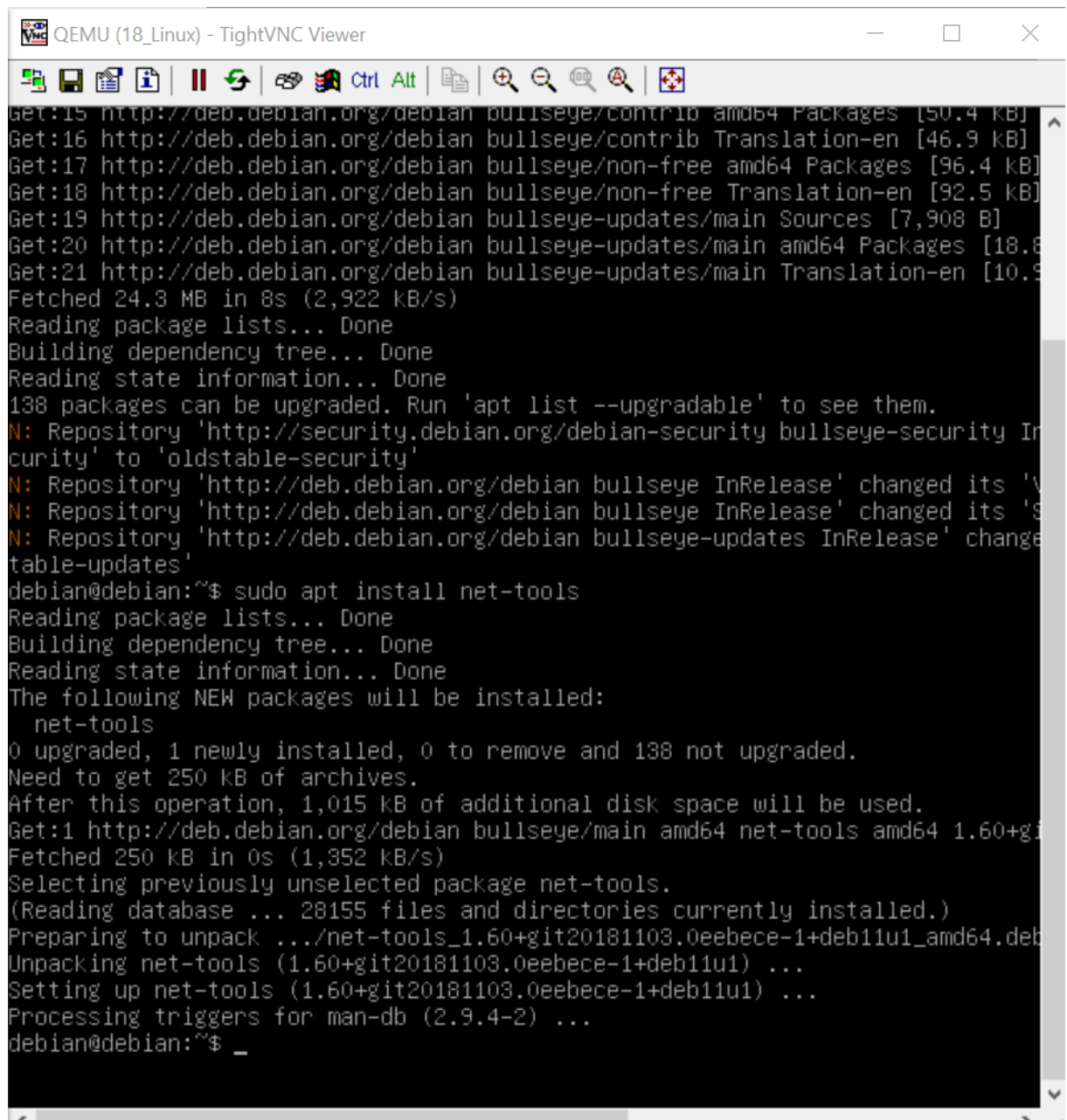
3. Jika belum, tanyakan ke dosen / instruktur agar bisa mendapatkan koneksi internet.
4. Lakukan pemutakhiran indeks repositori pada komputer linux Anda dengan menjalankan perintah “sudo apt update”, kemudian masukkan password dari user linux yang Anda gunakan. Dan pastikan tidak ada kata-kata error yang muncul pada

proses pemutakhiran tersebut.



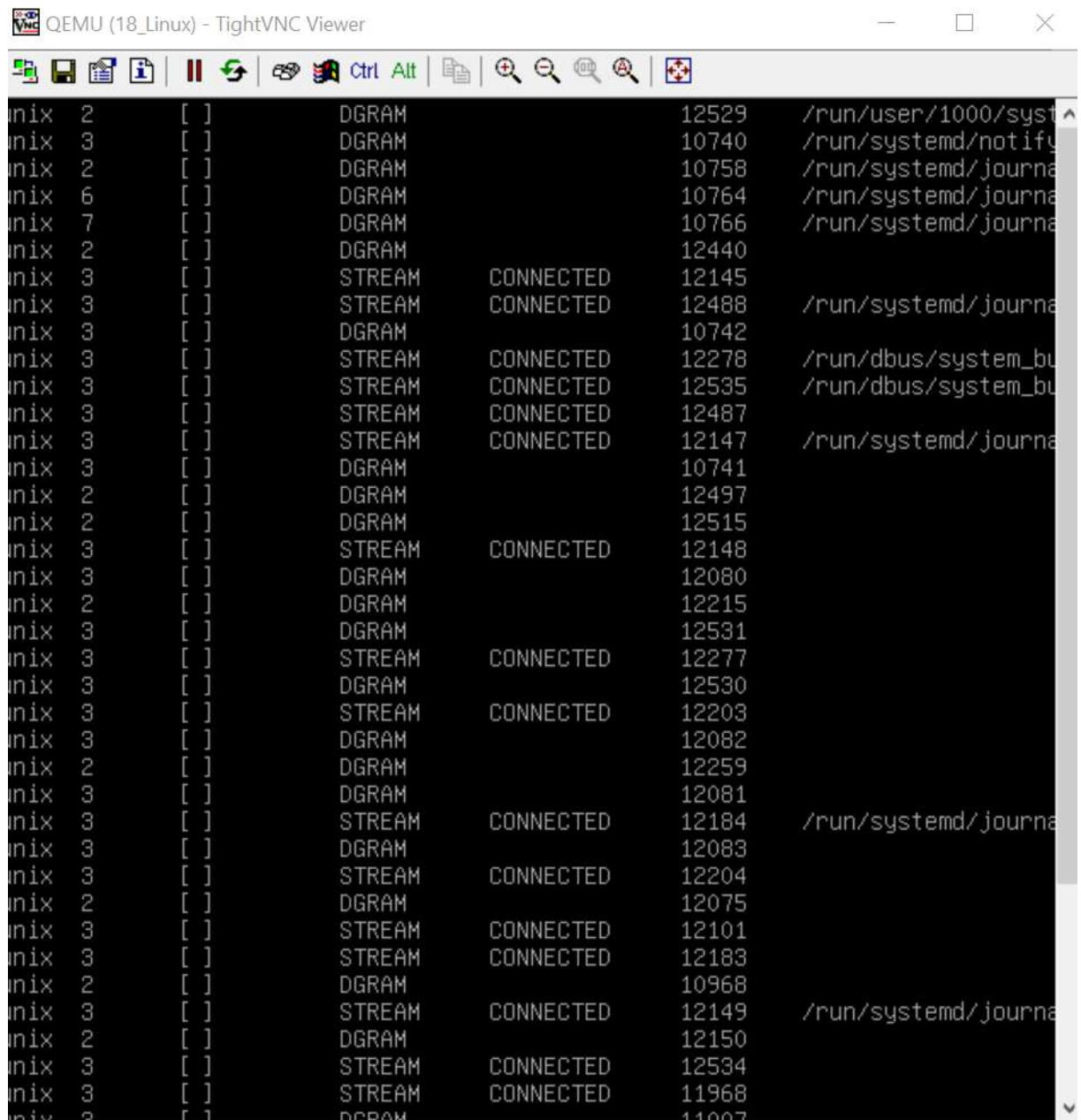
```
QEMU (18_Linux) - TightVNC Viewer
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=14 ttl=101 time=3
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=15 ttl=101 time=3
64 bytes from sc-in-f101.1e100.net (74.125.68.101): icmp_seq=16 ttl=104 time=3
^C
--- google.com ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15059ms
rtt min/avg/max/mdev = 28.403/29.240/35.626/1.693 ms
debian@debian:~$ sudo apt update
Get:1 http://security.debian.org/debian-security bullseye-security InRelease [
Get:2 http://deb.debian.org/debian bullseye InRelease [116 kB]
Get:3 http://deb.debian.org/debian bullseye-updates InRelease [44.1 kB]
Get:4 http://security.debian.org/debian-security bullseye-security/non-free So
Get:5 http://security.debian.org/debian-security bullseye-security/main Source
Get:6 http://security.debian.org/debian-security bullseye-security/main amd64
Get:7 http://deb.debian.org/debian bullseye/contrib Sources [43.2 kB]
Get:8 http://security.debian.org/debian-security bullseye-security/main Transl
Get:9 http://security.debian.org/debian-security bullseye-security/non-free an
Get:10 http://security.debian.org/debian-security bullseye-security/non-free T
Get:11 http://deb.debian.org/debian bullseye/non-free Sources [81.0 kB]
Get:12 http://deb.debian.org/debian bullseye/main Sources [8,500 kB]
Get:13 http://deb.debian.org/debian bullseye/main amd64 Packages [8,066 kB]
Get:14 http://deb.debian.org/debian bullseye/main Translation-en [6,235 kB]
Get:15 http://deb.debian.org/debian bullseye/contrib amd64 Packages [50.4 kB]
Get:16 http://deb.debian.org/debian bullseye/contrib Translation-en [46.9 kB]
Get:17 http://deb.debian.org/debian bullseye/non-free amd64 Packages [96.4 kB]
Get:18 http://deb.debian.org/debian bullseye/non-free Translation-en [92.5 kB]
Get:19 http://deb.debian.org/debian bullseye-updates/main Sources [7,908 B]
Get:20 http://deb.debian.org/debian bullseye-updates/main amd64 Packages [18.6
Get:21 http://deb.debian.org/debian bullseye-updates/main Translation-en [10.9
Fetched 24.3 MB in 8s (2,922 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
138 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Repository 'http://security.debian.org/debian-security bullseye-security In
curity' to 'oldstable-security'
N: Repository 'http://deb.debian.org/debian bullseye InRelease' changed its 'V
```

5. Pada sistem operasi linux, utilitas netstat berada pada paket aplikasi net-tools. Oleh karena itu lakukan instalasi paket net-tools untuk dapat menggunakan utilitas netstat. Jalankan perintah “sudo apt install net-tools” untuk melakukan instalasi paket tersebut.



```
Get:15 http://deb.debian.org/debian bullseye/contrib amd64 Packages [50.4 kB]
Get:16 http://deb.debian.org/debian bullseye/contrib Translation-en [46.9 kB]
Get:17 http://deb.debian.org/debian bullseye/non-free amd64 Packages [96.4 kB]
Get:18 http://deb.debian.org/debian bullseye/non-free Translation-en [92.5 kB]
Get:19 http://deb.debian.org/debian bullseye-updates/main Sources [7,908 B]
Get:20 http://deb.debian.org/debian bullseye-updates/main amd64 Packages [18.8 kB]
Get:21 http://deb.debian.org/debian bullseye-updates/main Translation-en [10.9 kB]
Fetched 24.3 MB in 8s (2,922 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
138 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Repository 'http://security.debian.org/debian-security bullseye-security InRelease' changed its 'URL' to 'oldstable-security'
N: Repository 'http://deb.debian.org/debian bullseye InRelease' changed its 'URL' to 'oldstable'
N: Repository 'http://deb.debian.org/debian bullseye InRelease' changed its 'URL' to 'oldstable'
N: Repository 'http://deb.debian.org/debian bullseye-updates InRelease' changed its 'URL' to 'oldstable-updates'
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 138 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://deb.debian.org/debian bullseye/main amd64 net-tools amd64 1.60+git20181103.0eebece-1+deb11u1 [250 kB]
Fetched 250 kB in 0s (1,352 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 28155 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1+deb11u1_amd64.deb ...
Unpacking net-tools (1.60+git20181103.0eebece-1+deb11u1) ...
Setting up net-tools (1.60+git20181103.0eebece-1+deb11u1) ...
Processing triggers for man-db (2.9.4-2) ...
debian@debian:~$ _
```

6. Kemudian setelah paket aplikasi berhasil dipasang, jalankan perintah “netstat”.



```
QEMU (18_Linux) - TightVNC Viewer
nix 2 [ ] DGRAM 12529 /run/user/1000/syst
nix 3 [ ] DGRAM 10740 /run/systemd/notifu
nix 2 [ ] DGRAM 10758 /run/systemd/journa
nix 6 [ ] DGRAM 10764 /run/systemd/journa
nix 7 [ ] DGRAM 10766 /run/systemd/journa
nix 2 [ ] DGRAM 12440
nix 3 [ ] STREAM CONNECTED 12145
nix 3 [ ] STREAM CONNECTED 12488 /run/systemd/journa
nix 3 [ ] DGRAM 10742
nix 3 [ ] STREAM CONNECTED 12278 /run/dbus/system_bu
nix 3 [ ] STREAM CONNECTED 12535 /run/dbus/system_bu
nix 3 [ ] STREAM CONNECTED 12487
nix 3 [ ] STREAM CONNECTED 12147 /run/systemd/journa
nix 3 [ ] DGRAM 10741
nix 2 [ ] DGRAM 12497
nix 2 [ ] DGRAM 12515
nix 3 [ ] STREAM CONNECTED 12148
nix 3 [ ] DGRAM 12080
nix 2 [ ] DGRAM 12215
nix 3 [ ] DGRAM 12531
nix 3 [ ] STREAM CONNECTED 12277
nix 3 [ ] DGRAM 12530
nix 3 [ ] STREAM CONNECTED 12203
nix 3 [ ] DGRAM 12082
nix 2 [ ] DGRAM 12259
nix 3 [ ] DGRAM 12081
nix 3 [ ] STREAM CONNECTED 12184 /run/systemd/journa
nix 3 [ ] DGRAM 12083
nix 3 [ ] STREAM CONNECTED 12204
nix 2 [ ] DGRAM 12075
nix 3 [ ] STREAM CONNECTED 12101
nix 3 [ ] STREAM CONNECTED 12183
nix 2 [ ] DGRAM 10968
nix 3 [ ] STREAM CONNECTED 12149 /run/systemd/journa
nix 2 [ ] DGRAM 12150
nix 3 [ ] STREAM CONNECTED 12534
nix 3 [ ] STREAM CONNECTED 11968
nix 3 [ ] DGRAM 11007
```

7. Ambil gambar hasil output perintah netstat tersebut, dan jelaskan arti dari output tampilan yang ada pada komputer linux Anda tersebut.
8. Tambahkan opsi yang cocok pada perintah netstat untuk menampilkan port-port yang sedang terbuka dan listen pada komputer linux Anda beserta nama proses atau PIDnya. Jangan lupa menggunakan akses super user (sudo) untuk dapat menampilkan detail nama proses atau PID dari aplikasi yang sedang menggunakan port tersebut.
9. Cobalah menggunakan 5 opsi yang telah dijelaskan pada dasar teori. Ambil gambar output tampilan perintah dengan opsi yang telah Anda pilih. Dan berikan penjelasan atau analisa maksud dari tampilan yang Anda dapatkan.

```

debian@debian:~$ sudo netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type        State         I-Node      Path
unix  2      [ ACC ]     STREAM     LISTENING     12532       /run/user/1000/s
unix  2      [ ACC ]     STREAM     LISTENING     10743       /run/systemd/pri
unix  2      [ ACC ]     STREAM     LISTENING     10745       /run/systemd/user
unix  2      [ ACC ]     STREAM     LISTENING     10746       /run/systemd/io.
unix  2      [ ACC ]     STREAM     LISTENING     10756       /run/lvm/lvmpoll
unix  2      [ ACC ]     STREAM     LISTENING     10760       /run/systemd/fsc
unix  2      [ ACC ]     STREAM     LISTENING     10768       /run/systemd/jou
unix  2      [ ACC ]     SEQUPACKET LISTENING     10770       /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     10966       /run/systemd/jou
unix  2      [ ACC ]     STREAM     LISTENING     12088       /run/dbus/system
debian@debian:~$

```

QEMU (18_Linux) - TightVNC Viewer

tempns:

```

    InType0: 16
    InType8: 2
    OutType0: 2
    OutType8: 16

```

Tcp:

```

    3 active connection openings
    0 passive connection openings
    0 failed connection attempts
    0 connection resets received
    0 connections established
    8123 segments received
    5250 segments sent out
    0 segments retransmitted
    0 bad segments received
    0 resets sent

```

Udp:

```

    36 packets received
    0 packets to unknown port received
    0 packet receive errors
    221 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 40

```

UdpLite:

TcpExt:

```

    3 TCP sockets finished time wait in fast timer
    1 delayed acks sent
    4066 packet headers predicted
    13 acknowledgments not containing data payload received
    Detected reordering 1 times using SACK
    TCPBacklogCoalesce: 30
    TCPSackShiftFallback: 2
    TCPRcvCoalesce: 4734
    TCP0FOQueue: 2563
    TCPOrigDataSent: 14
    TCPDelivered: 17
    TCPAckCompressed: 850

```



```

debian@debian:~$ sudo netstat -i
Kernel Interface table

```

Interface	MTU	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR
eth0	1500	17381	34	0 0	0 0	5560	0	0	0 0
lo	65536	0	0	0 0	0 0	0	0	0	0 0

```

debian@debian:~$

```

```

debian@debian:~$ sudo netstat -0
netstat: invalid option -- '0'
usage: netstat [-vWeenNcCF] [<Af>] -r          netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -i | [-cnNe] -M | -s [-6tuw] }

    -r, --route          display routing table
    -i, --interfaces    display interface table
    -g, --groups         display multicast group memberships
    -s, --statistics    display networking statistics (like SNMP)
    -M, --masquerade    display masqueraded connections

    -v, --verbose        be verbose
    -W, --wide           don't truncate IP addresses
    -n, --numeric        don't resolve names
    --numeric-hosts      don't resolve host names
    --numeric-ports      don't resolve port names
    --numeric-users      don't resolve user names
    -N, --symbolic      resolve hardware names
    -e, --extend         display other/more information
    -p, --programs       display PID/Program name for sockets
    -o, --timers         display timers
    -c, --continuous    continuous listing

    -l, --listening     display listening server sockets
    -a, --all            display all sockets (default: connected)
    -F, --fib            display Forwarding Information Base (default: disabled)

```

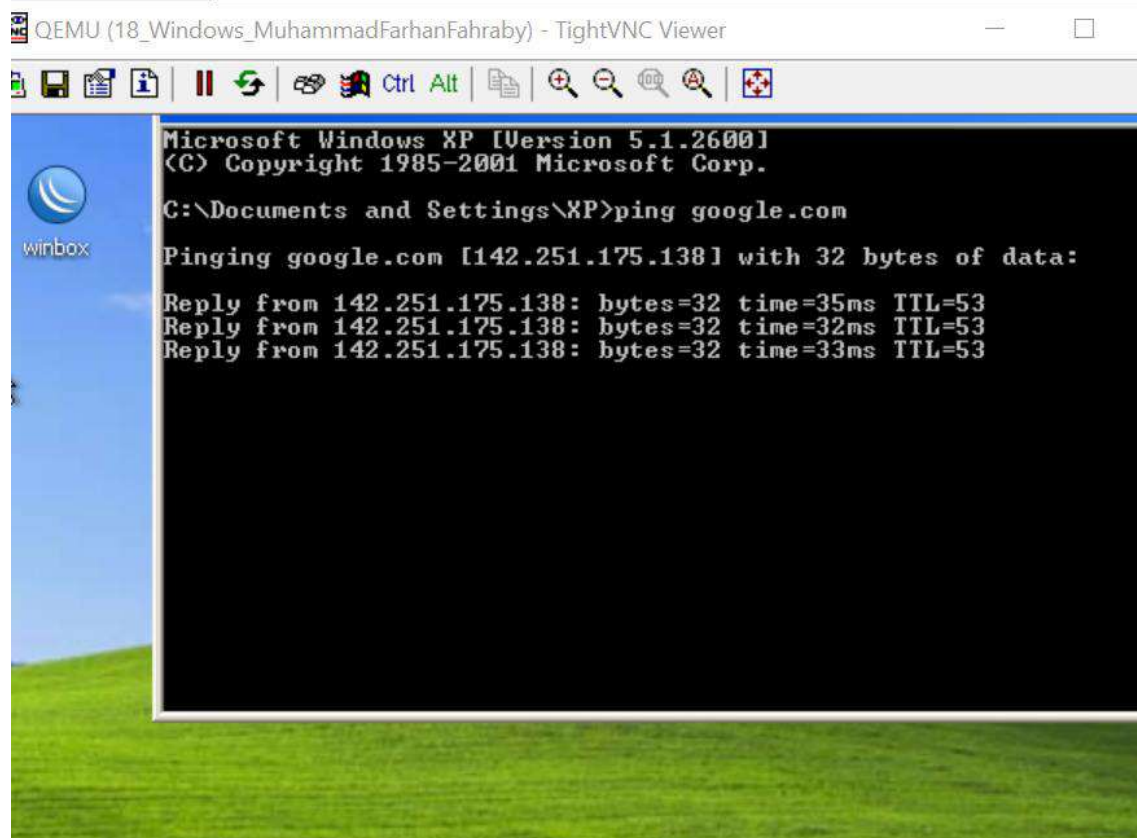
The screenshot shows a TightVNC viewer window titled "QEMU (18_Linux) - TightVNC Viewer". The main display area shows network statistics for ICMP, IcmpMsg, Tcp, Udp, UdpLite, and TcpExt. Below this, a terminal window shows the output of the command "sudo netstat -r".

```
ICMP output histogram:
  echo requests: 16
  echo replies: 2
IcmpMsg:
  InType0: 16
  InType8: 2
  OutType0: 2
  OutType8: 16
Tcp:
  3 active connection openings
  0 passive connection openings
  0 failed connection attempts
  0 connection resets received
  0 connections established
  8123 segments received
  5250 segments sent out
  0 segments retransmitted
  0 bad segments received
  0 resets sent
Udp:
  36 packets received
  0 packets to unknown port received
  0 packet receive errors
  221 packets sent
  0 receive buffer errors
  0 send buffer errors
  IgnoredMulti: 90
UdpLite:
TcpExt:
  3 TCP sockets finished time wait in fast timer
  1 delayed acks sent
  4066 packet headers predicted
  13 acknowledgments not containing data payload received
  Detected reordering 1 times using SACK
  TCPBacklogCoalesce: 30
  TCPSackShiftFallback: 2
  TCPRcvCoalesce: 4734

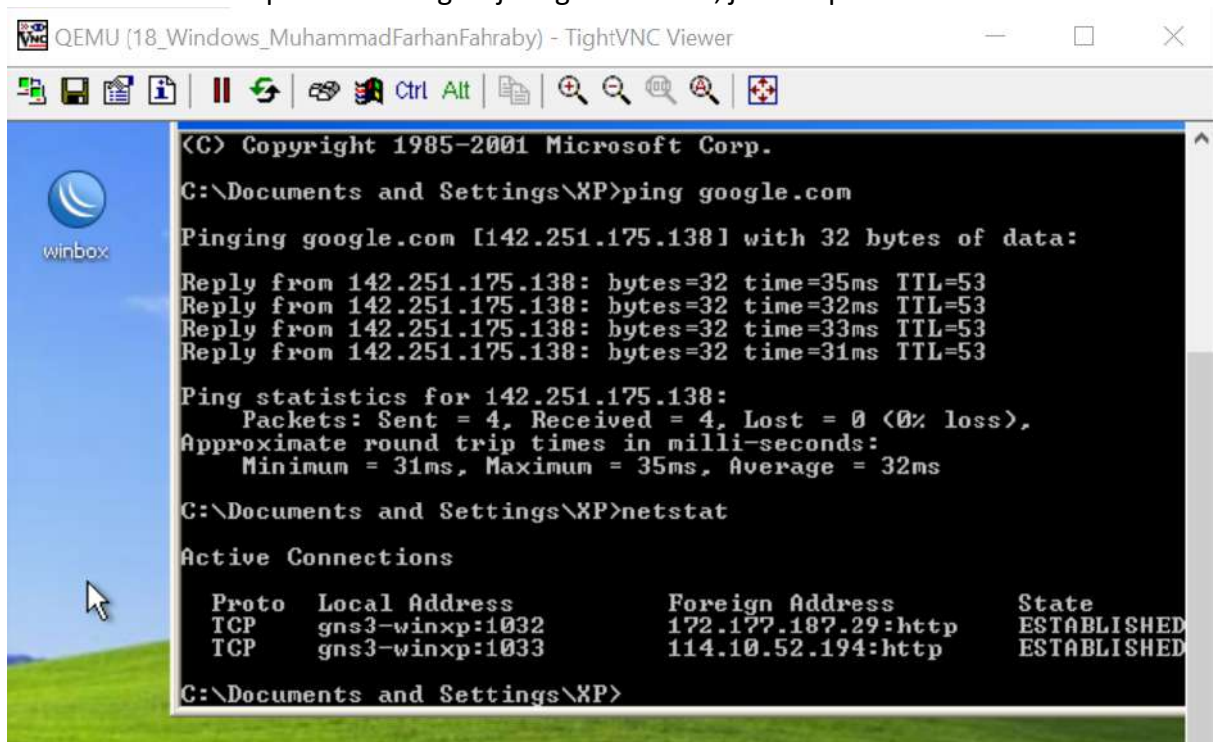
debian@debian:~$ sudo netstat -r
Kernel IP routing table
Destination        Gateway            Genmask           Flags   MSS Window  irtt Ifa
default            10.10.10.1        0.0.0.0          UG        0 0        0 ens
10.10.10.0         0.0.0.0           255.255.255.0    U        0 0        0 ens
debian@debian:~$
```

II. Netstat Pada Sistem Operasi Windows

1. Akses komputer windows Anda dalam project yang telah terbuka.
2. Pastikan koneksi komputer anda sudah terhubung dengan internet, dengan menjalankan perintah ping ke www.google.com pada terminal command prompt. Pastikan terdapat kata-kata replay pada output perintah tersebut. Hentikan utilitas ping dengan menekan kombinasi tombol keyboard ctrl+c.



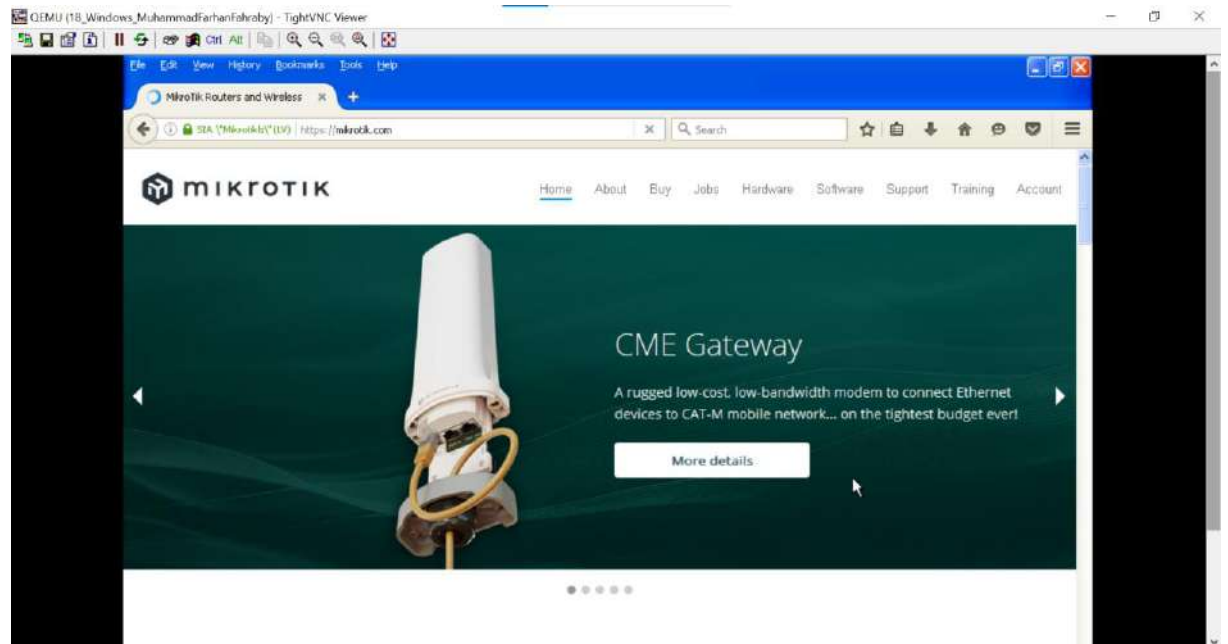
3. Jika belum, tanyakan ke dosen / instruktur agar bisa mendapatkan koneksi internet.
4. Jika telah dapat terhubung ke jaringan internet, jalankan perintah “netstat”.



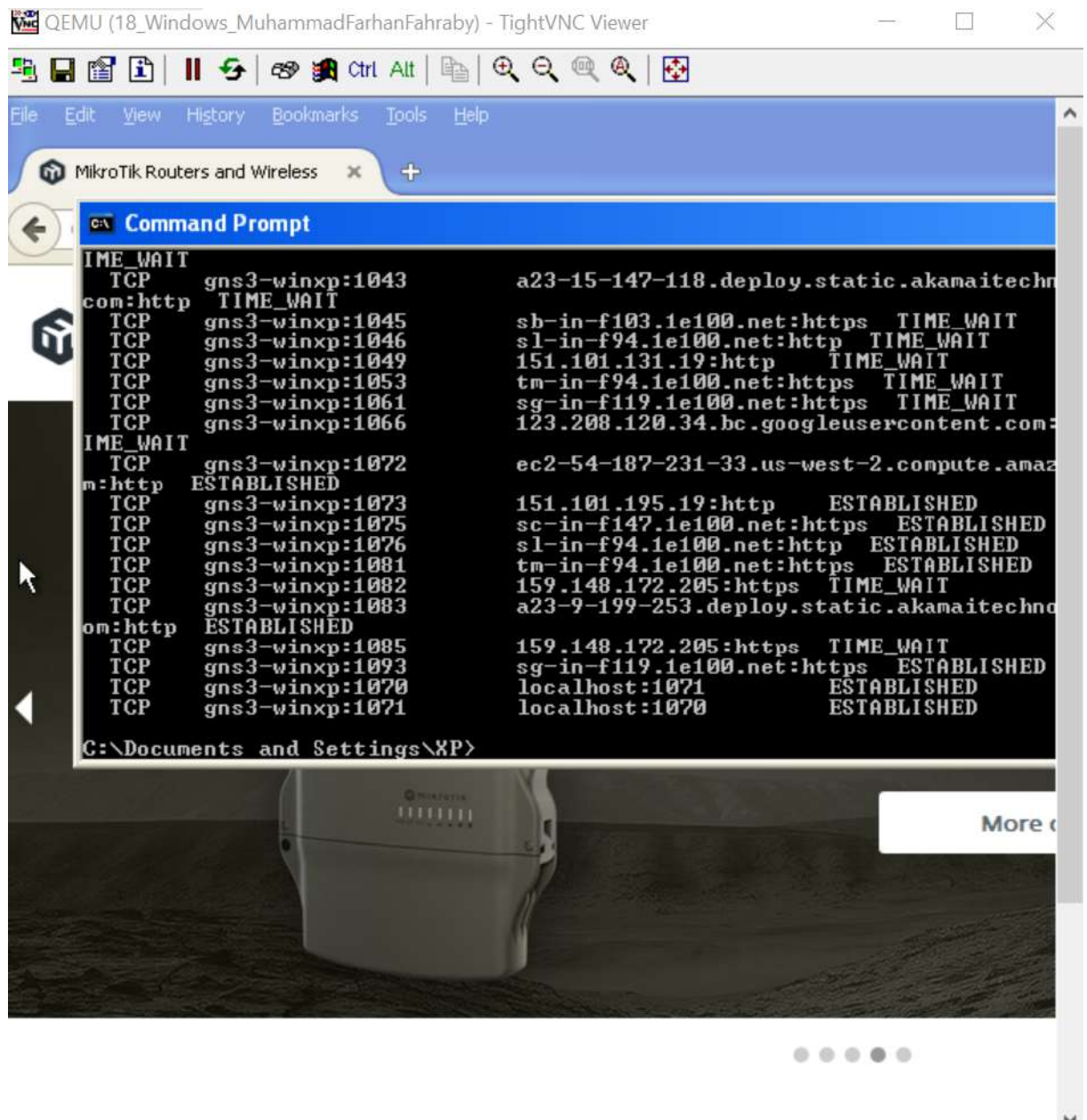
5. Ambil gambar hasil output perintah netstat tersebut, dan jelaskan arti dari output tampilan yang ada pada komputer linux Anda tersebut.

Komputer gns3-winxp memiliki dua koneksi TCP aktif ke server eksternal melalui port HTTP (kemungkinan browsing atau akses web), dengan status ESTABLISHED (aktif).

6. Cobalah untuk membuka sebuah laman web menggunakan aplikasi peramban yang ada pada komputer windows Anda tersebut.



7. Jalankan kembali perintah "netstat" pada command prompt Anda.



8. Ambil gambar hasil output perintah netstat tersebut, dan jelaskan arti dari output tampilan yang ada pada komputer linux Anda tersebut.

Penjelasan Singkat: Koneksi Aktif (ESTABLISHED): Komputer terhubung ke beberapa server, termasuk Google, Amazon AWS, dan Akamai melalui protokol HTTP (port 80) dan HTTPS (port 443). Contoh: 151.101.195.19:http → Koneksi aktif ke server IP tersebut. sc-in-f94.1e100.net:https → Koneksi HTTPS ke server Google. Koneksi yang Berakhir (TIME_WAIT): Beberapa koneksi dalam status TIME_WAIT, artinya sesi telah ditutup dan menunggu untuk dilepaskan oleh sistem.

9. Tambahkan opsi yang cocok pada perintah netstat untuk menampilkan semua port-port yang sedang menggunakan oleh protokol tcp.

```

C:\ Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 25ms, Average = 25ms

C:\Documents and Settings\XP>netstat -a

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:nethios-ssn gns3-winxp:0           LISTENING
    TCP    gns3-winxp:1029        gns3-winxp:0           LISTENING
    UDP    gns3-winxp:microsoft-ds *:.*
    UDP    gns3-winxp:isakmp      *:.*
    UDP    gns3-winxp:1043        *:.*
    UDP    gns3-winxp:4500        *:.*
    UDP    gns3-winxp:ntp         *:.*
    UDP    gns3-winxp:nethios-ns  *:.*
    UDP    gns3-winxp:nethios-dgm *:.*
    UDP    gns3-winxp:1900        *:.*
    UDP    gns3-winxp:ntp         *:.*
    UDP    gns3-winxp:1025        *:.*
    UDP    gns3-winxp:1900        *:.*

C:\Documents and Settings\XP>

```

10. Cobalah menggunakan 3 opsi yang telah dijelaskan pada dasar teori. Ambil gambar output tampilan perintah dengan opsi yang telah Anda pilih. Dan berikan penjelasan atau analisa maksud dari tampilan yang Anda dapatkan.

```

C:\Documents and Settings\XP>netstat -e
Interface Statistics

    Received Sent
Bytes 47041 12717
Unicast packets 21 19
Non-unicast packets 369 85
Discards 0 0
Errors 0 0
Unknown protocols 0 0

C:\Documents and Settings\XP>

```

```

C:\Documents and Settings\XP>netstat -o
Active Connections

    Proto Local Address          Foreign Address         State      PID
C:\Documents and Settings\XP>

```

```
C:\Documents and Settings\XP>netstat -e  
Interface Statistics
```

	Received	Sent
Bytes	51151	12717
Unicast packets	21	19
Non-unicast packets	405	85
Discards	0	0
Errors	0	0
Unknown protocols	0	0

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

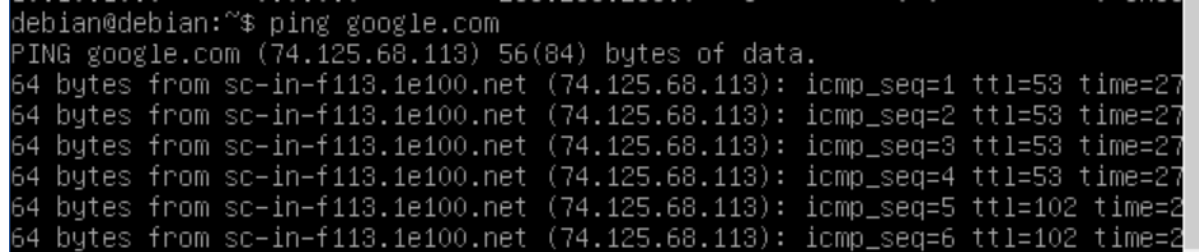
```
Active Connections
```

Proto	Local Address	Foreign Address	State
-------	---------------	-----------------	-------

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

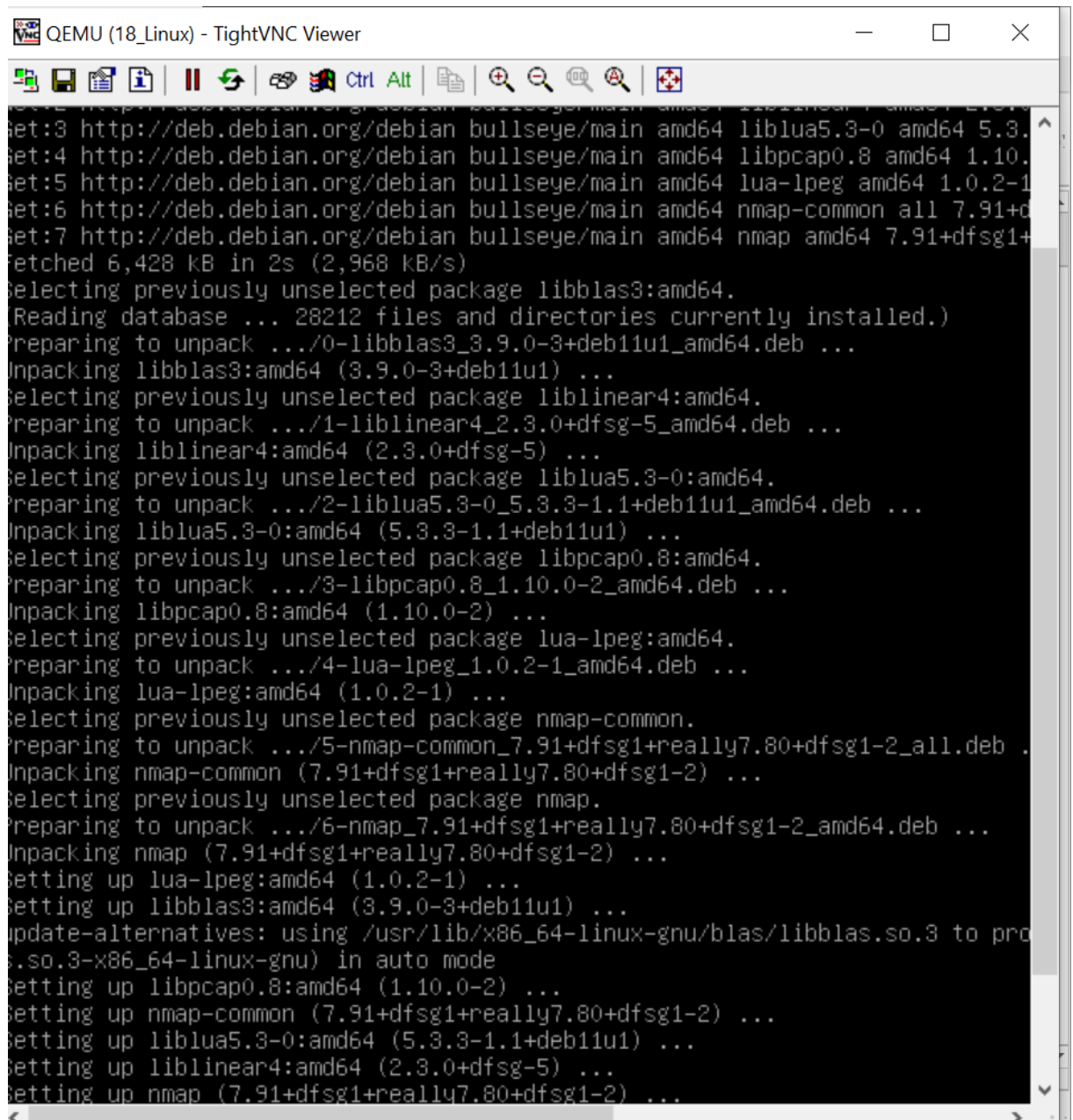
III. NMAP

1. Akses kembali komputer linux Anda dalam project yang telah terbuka.
2. Pastikan koneksi komputer anda masih dapat terhubung dengan internet, dengan menjalankan perintah ping ke www.google.com. Pastikan terdapat kata-kata replay pada output perintah tersebut. Hentikan utilitas ping dengan menekan kombinasi tombol keyboard ctrl+c.

A terminal window showing the execution of the 'ping google.com' command. The output displays six successful replies from 'sc-in-f113.1e100.net' (74.125.68.113) with varying TTL and time values. The terminal text is as follows:

```
debian@debian:~$ ping google.com
PING google.com (74.125.68.113) 56(84) bytes of data:
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=1 ttl=53 time=27.4 ms
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=2 ttl=53 time=27.4 ms
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=3 ttl=53 time=27.4 ms
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=4 ttl=53 time=27.4 ms
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=5 ttl=102 time=27.4 ms
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=6 ttl=102 time=27.4 ms
```

3. Jika tidak terkoneksi, tanyakan ke dosen / instruktur agar bisa mendapatkan koneksi internet kembali.
4. Lakukan instalasi paket aplikasi nmap untuk dapat menggunakan utilitas nmap. Jalankan perintah “sudo apt install nmap” untuk melakukan instalasi paket tersebut. Masukkan password dari user debian Anda jika diminta. Kemudian ketikkan huruf “Y” dan tekan tombol enter untuk menyetujui instalasi.

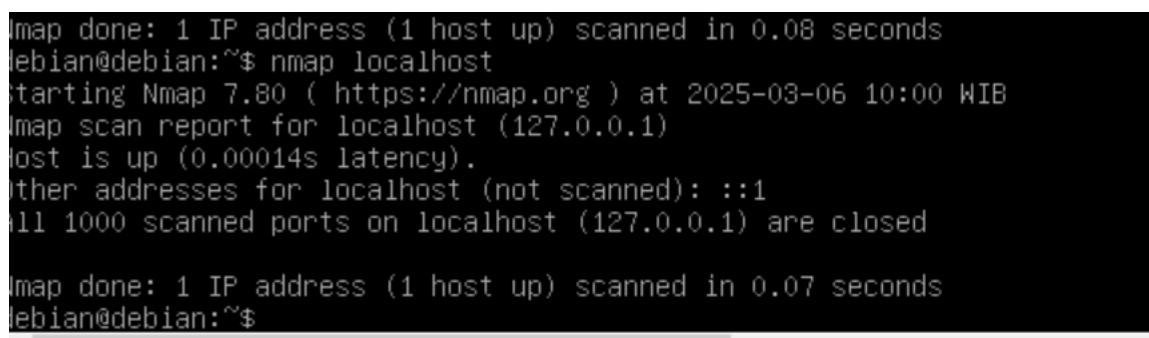


```
Get:3 http://deb.debian.org/debian bullseye/main amd64 liblua5.3-0 amd64 5.3.3-1.1+deb11u1 [108 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 libpcap0.8 amd64 1.10.0-2 [28.9 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 lua-lpeg amd64 1.0.2-1 [14.5 kB]
Get:6 http://deb.debian.org/debian bullseye/main amd64 nmap-common all 7.91+dfsg1-2 [1,104 kB]
Get:7 http://deb.debian.org/debian bullseye/main amd64 nmap amd64 7.91+dfsg1-2 [1,104 kB]
Fetched 6,428 kB in 2s (2,968 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 28212 files and directories currently installed.)
Preparing to unpack .../0-libblas3_3.9.0-3+deb11u1_amd64.deb ...
Unpacking libblas3:amd64 (3.9.0-3+deb11u1) ...
Selecting previously unselected package liblinear4:amd64.
Preparing to unpack .../1-liblinear4_2.3.0+dfsg-5_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-5) ...
Selecting previously unselected package liblua5.3-0:amd64.
Preparing to unpack .../2-liblua5.3-0_5.3.3-1.1+deb11u1_amd64.deb ...
Unpacking liblua5.3-0:amd64 (5.3.3-1.1+deb11u1) ...
Selecting previously unselected package libpcap0.8:amd64.
Preparing to unpack .../3-libpcap0.8_1.10.0-2_amd64.deb ...
Unpacking libpcap0.8:amd64 (1.10.0-2) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../4-lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../5-nmap-common_7.91+dfsg1+really7.80+dfsg1-2_all.deb ...
Unpacking nmap-common (7.91+dfsg1+really7.80+dfsg1-2) ...
Selecting previously unselected package nmap.
Preparing to unpack .../6-nmap_7.91+dfsg1+really7.80+dfsg1-2_amd64.deb ...
Unpacking nmap (7.91+dfsg1+really7.80+dfsg1-2) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up libblas3:amd64 (3.9.0-3+deb11u1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (x86_64-linux-gnu) in auto mode
Setting up libpcap0.8:amd64 (1.10.0-2) ...
Setting up nmap-common (7.91+dfsg1+really7.80+dfsg1-2) ...
Setting up liblua5.3-0:amd64 (5.3.3-1.1+deb11u1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up nmap (7.91+dfsg1+really7.80+dfsg1-2) ...

nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
debian@debian:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 10:00 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
debian@debian:~$
```

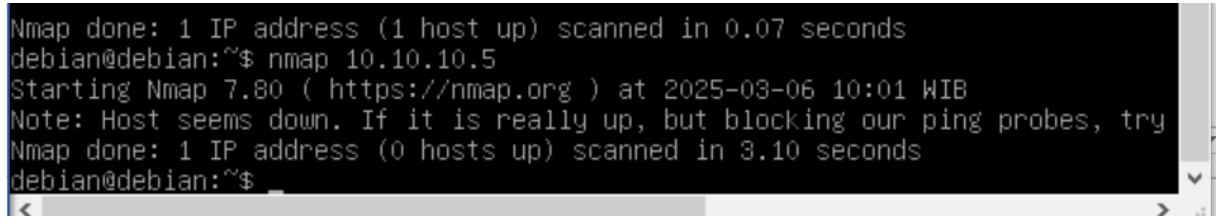
5. Kemudian setelah paket aplikasi berhasil dipasang, jalankan perintah “nmap localhost”.



```
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
debian@debian:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 10:00 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are closed

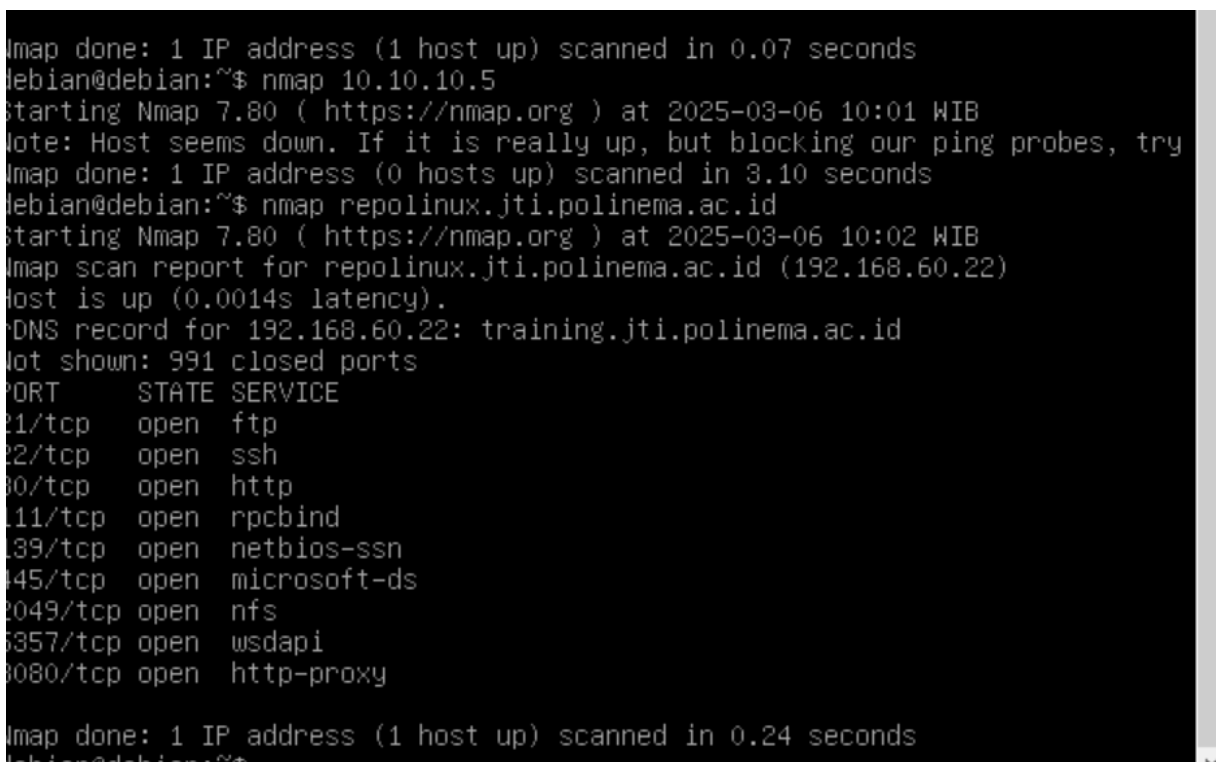
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
debian@debian:~$
```

6. Perintah di atas digunakan untuk melihat port-port mana saja yang terbuka pada komputer linux Anda.
7. Cobalah untuk melihat port-port yang terbuka pada komputer server dosen dengan alamat IP 10.10.10.5. Caranya, ganti kata “localhost” dengan alamat IP “10.10.10.5”. Ambil gambar output dari perintah tersebut. Jelaskan port-port apa saja yang terbuka dan servis apa yang berjalan pada port tersebut.

A terminal window showing the output of an nmap scan on the IP address 10.10.10.5. The output indicates that the host is down, as it blocked ping probes.

```
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
debian@debian:~$ nmap 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 10:01 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
debian@debian:~$
```

8. Cobalah untuk melihat port-port yang terbuka pada komputer server repositori lokal Jurusan Teknologi Informasi yang mempunyai alamat repolinux.jti.polinema.ac.id. Ambil gambar output dari perintah tersebut. Jelaskan port-port apa saja yang terbuka dan servis apa yang berjalan pada port tersebut.

A terminal window showing the output of an nmap scan on the domain repolinux.jti.polinema.ac.id. The output shows that the host is up and lists several open ports with their corresponding services.

```
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
debian@debian:~$ nmap 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 10:01 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
debian@debian:~$ nmap repolinux.jti.polinema.ac.id
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 10:02 WIB
Nmap scan report for repolinux.jti.polinema.ac.id (192.168.60.22)
Host is up (0.0014s latency).
DNS 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
145/tcp   open  microsoft-ds
2049/tcp  open  nfs
3357/tcp  open  wsddapi
8080/tcp  open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
debian@debian:~$
```

9. Cobalah untuk menambahkan opsi “Pn” pada perintah nmap yang Anda jalankan pada langkah 7 dan 8. Ambil gambar output dari perintah tersebut. Jelaskan port-port apa saja yang terbuka, servis apa yang berjalan pada port tersebut, dan perbedaan dari tampilan perintah yang Anda lakukan sebelumnya pada langkah 8 dan 9.

```
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
debian@debian:~$ nmap Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-06 10:02 WIB
Failed to resolve "Pn".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
debian@debian:~$
```


TUGAS

1. Buatlah laporan yang berisi *screenshot* dan penjelasan *step-by-step* dari ketiga langkah praktikum yang telah anda lakukan.
2. Kumpulkan laporan yang anda buat dalam bentuk file pdf dengan mengunggahnya ke server lms seperti pada praktikum-praktikum sebelumnya.
3. Lakukan praktikum semaksimal mungkin pada jam praktikum. Diluar jam praktikum, akan ada kemungkinan permasalahan kecepatan dari masing-masing komputer yang ada pada project tersebut.
4. Selamat mengerjakan.