

Progress Report 2

Kelompok 2

Dave Travis - 2201020008
Muhammad Noval - 2201020014
Rizsky Parsadanta R. - 2201020117
Arya Winata - 2201020001

Judul proyek : Analisis Serangan Sniffing & Mitigasinya di Wireshark

Tujuan proyek : Memahami cara kerja penyerangan *packet sniffing* dan metode pencegahannya.

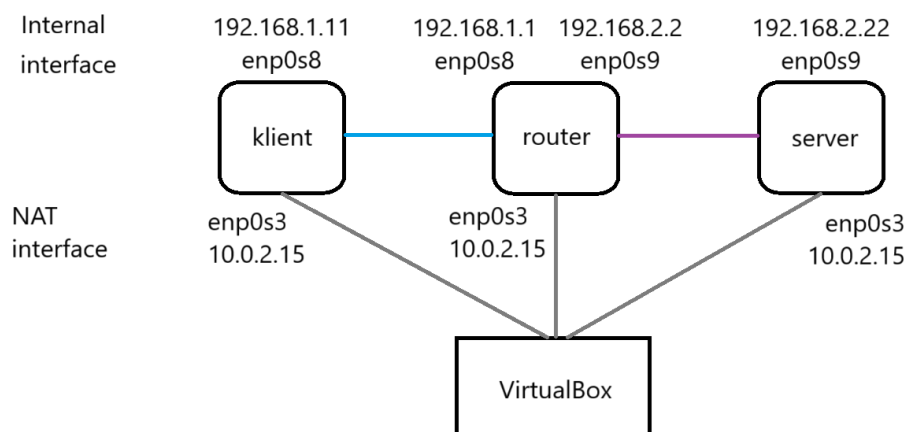
Target proyek : Setup jaringan sederhana (LAN/VirtualBox/Packet Tracer)
(Minggu 2)

Pengantar:

Pada progress minggu kedua ini, kami akan membangun lingkungan jaringan yang akan digunakan untuk simulasi dan analisis paket. Namun karena tahapan minggu ini masih progress, kami hanya akan mengatur topologi sederhana nya saja, dan memastikan kalau perangkat pada topologi tersebut dapat berkomunikasi satu sama lain.

Kami memilih menggunakan VirtualBox, dengan alasan memudahkan interaksi GUI nya agar memudahkan proses pembelajaran, baik dari sisi satu kelompok, hingga mempermudah presentasi nantinya, yang mana peragaan proses yang dilakukan dapat disampaikan dengan jelas.

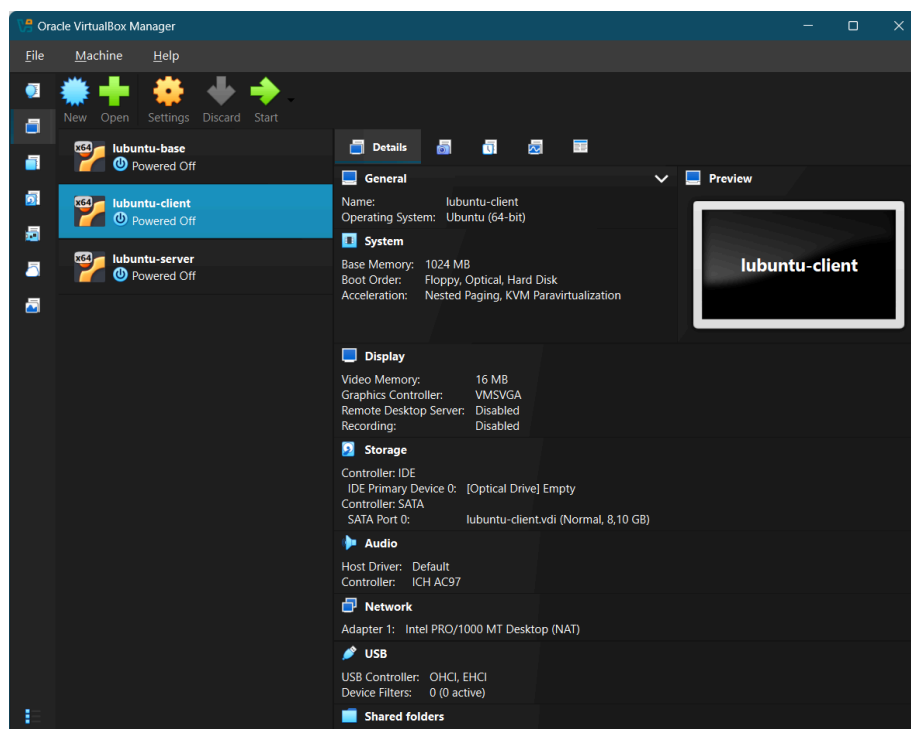
Desain Topologi:



Kami memutuskan untuk menggunakan 3 buah virtual machine untuk demonstrasi pembuatan jaringan LAN pada kali ini, yang mana masing-masing vm terdapat IP masing-masing yang dapat dilihat pada gambar di atas. Pada jaringan LAN ini, dikarenakan terdapat pada VirtualBox, jadinya kami pisahkan menjadi 2 jaringan, yaitu jaringan internal, yang berkomunikasi dengan saluran enp0s8 dan enp0s9 yang IP nya akan diatur secara statis, dan jaringan NAT melalui enp0s3, yang mana menghubungkan tiap-tiap vm ke perangkat utama, alias laptop kelompok, via IP DHCP.

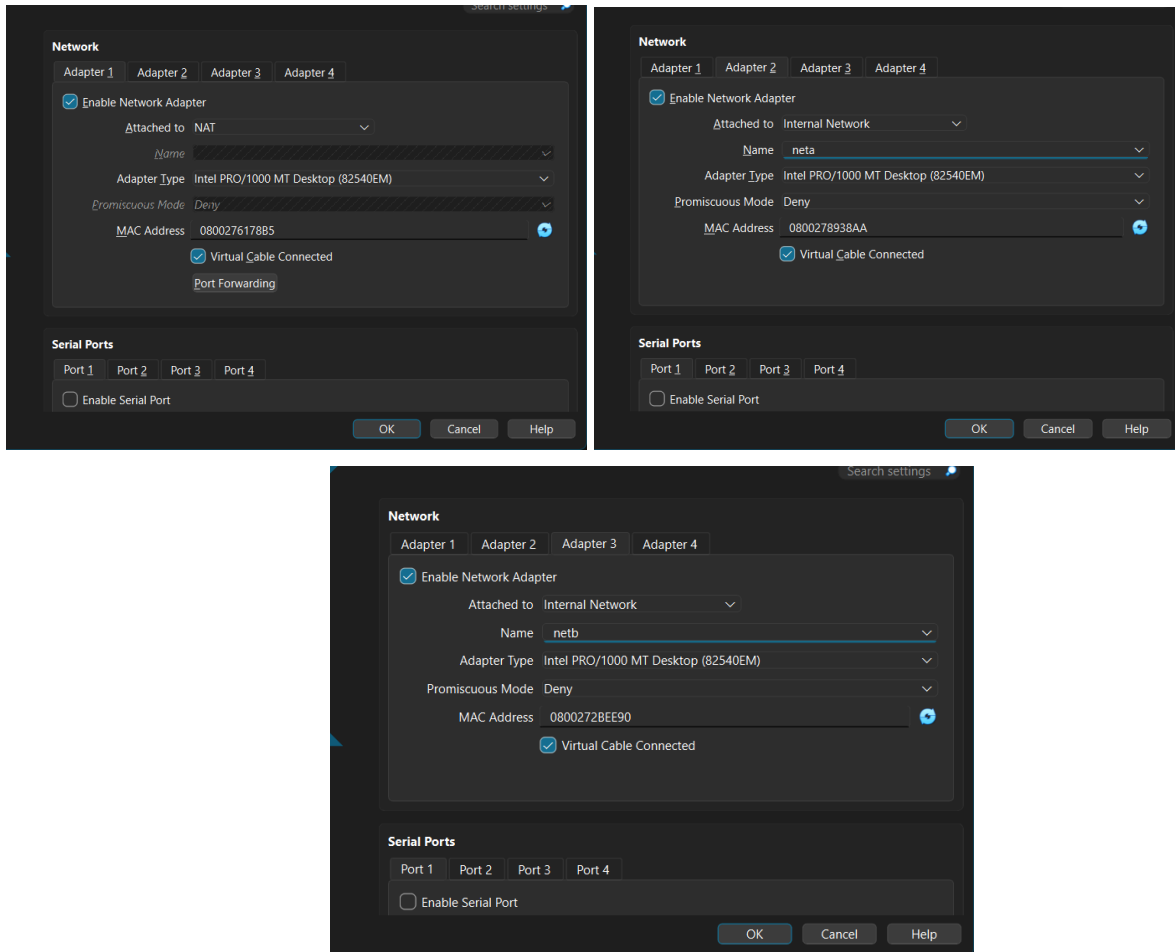
Untuk konfigurasi pada VirtualBox nya itu sendiri, dapat dilihat pada gambar di bawah beserta penjelasannya.

VirtualBox:



Karena adanya 3 perangkat yang kami ingin buat pada jaringan LAN ini, maka kami menyiapkan 3 vm pada VirtualBox, menggunakan Linux dengan distro Lubuntu. Agar dapat membuat jaringan internal dan NAT seperti yang dibicarakan di atas, maka untuk masing-masing konfigurasi network vm ialah seperti ini.

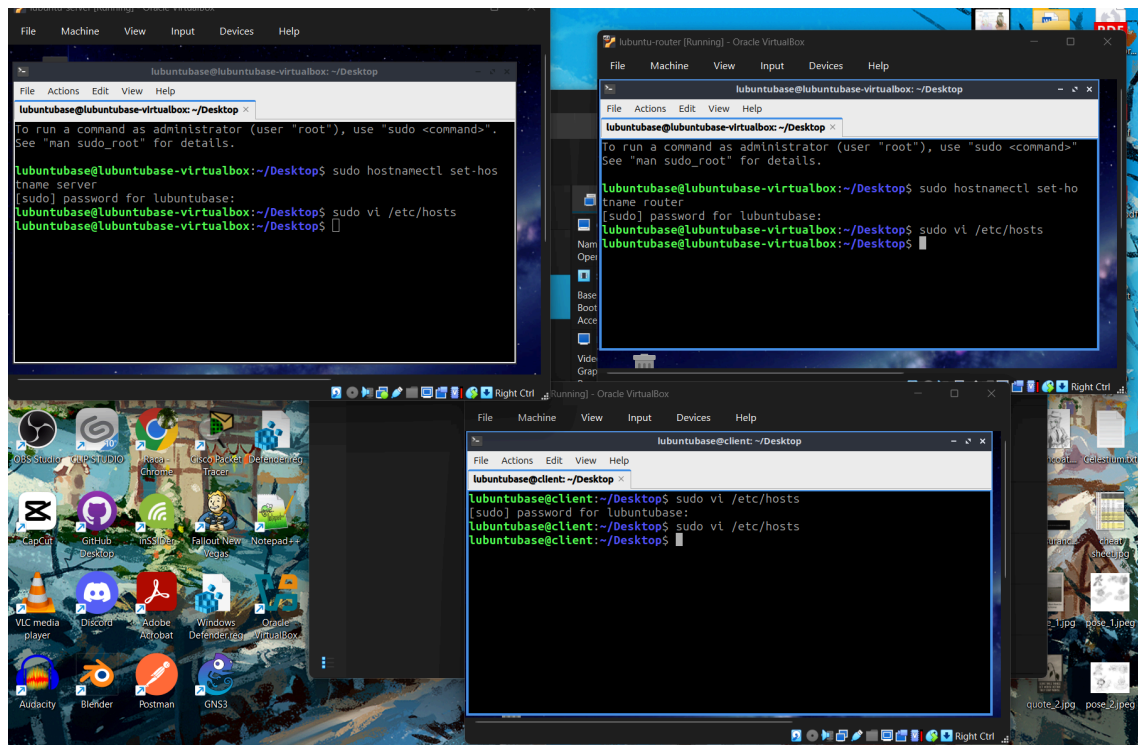
Kita mulai untuk vm klient, yang mana akan menggunakan 2 slot adapter.



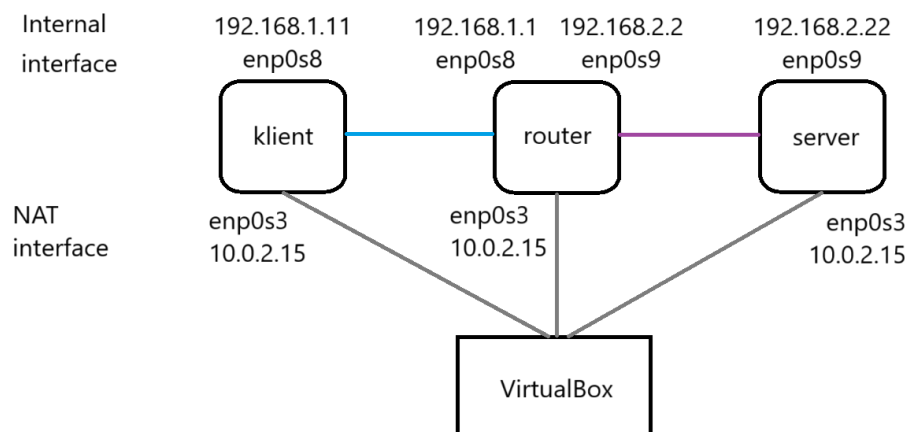
Pada adapter 1, kami membiarkan settingan default NAT, agar vm bisa tetap terhubung dengan perangkat utama, alias laptop, dan juga akan diatur sebagai default adapter bagi tiap-tiap vm nantinya, baik vm router dan vm server. Untuk adapter 2, kami mengaturnya sebagai Internal Network bernama 'neta', sehingga adanya jembatan antara vm klient dan vm router. Untuk Internal Network pada adapter 2 bernama 'neta' ini juga kami tambahkan pada vm router.

Untuk vm server, kami menambahkan adapter 3, yang mana juga Internal Network dengan nama 'netb' sebagai jembatan antara vm server dengan vm router. Hal yang sama juga kami tambahkan pada vm router.

Setelah selesai konfigurasi network pada halaman awal, kami boot up semua vm dan setup sederhana nama bagi masing-masing vm.



Setelah sudah di setup nama bagi masing-masing vm, maka akan kita bagi IP static untuk masing-masing vm, yang mana berdasarkan gambar di atas, kami tampilkan lagi.



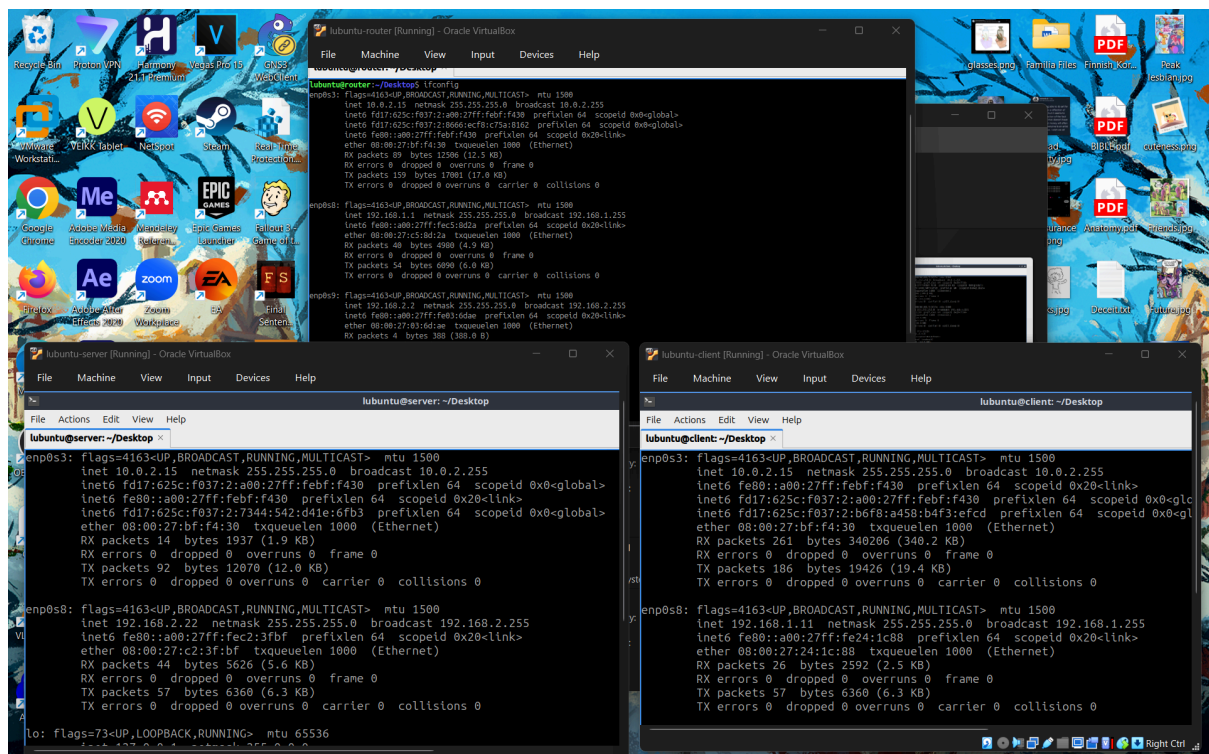
Setelah IP sudah didapat, maka saatnya kita menginput IP untuk masing-masing vm.

```
lubuntu@client: ~/Desktop
GNU nano 7.2 /etc/netplan/01-network-manager-all.yaml
# This file was written by calamares.
# Let NetworkManager manage all devices on this system.
# For more information, see netplan(5).
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true

    enp0s8:
      dhcp4: false
      addresses:
        - 192.168.1.11/24
      routes:
        - to: 192.168.0.0/16
          via: 192.168.1.1

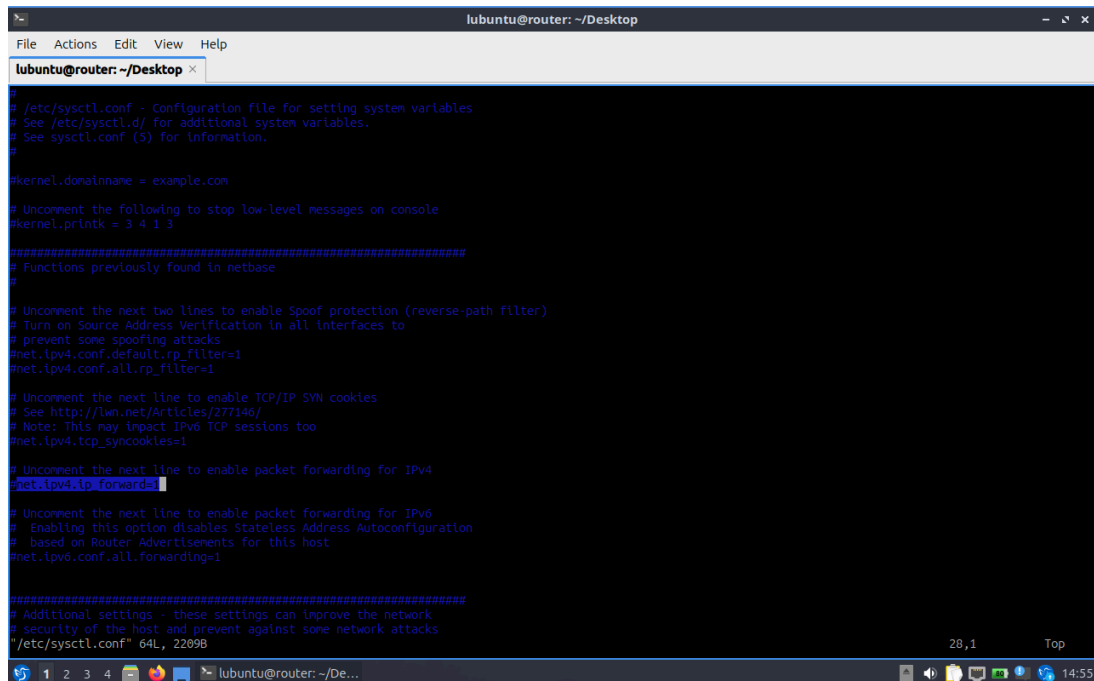
  nameservers:
    addresses: [8.8.8.8, 1.1.1.1]
```

Gambar di atas ialah ilustrasi input IP statis pada vm klien, yang mana kurang lebih sama juga penulisannya untuk vm lainnya. Dan jika sudah siap, maka hasilnya akan seperti ini.



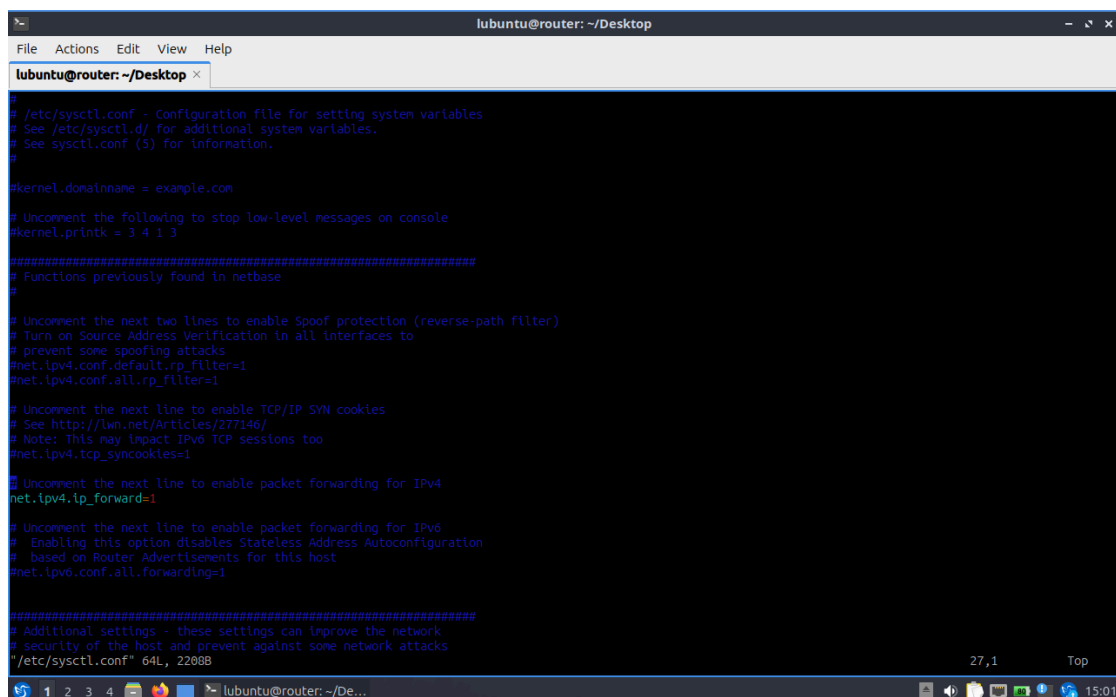
IP address untuk masing-masing vm sudah diatur sesuai dengan rancangan.

Sebelum kita testing ping untuk menguji apakah ketiga perangkat bisa berkomunikasi satu sama lain, kita perlu membuka file `/etc/sysctl.conf` terlebih dahulu pada vm router, dikarenakan vm router ialah jembatan dari kedua perangkat, maka vm router perlu mengizinkan forward packet.



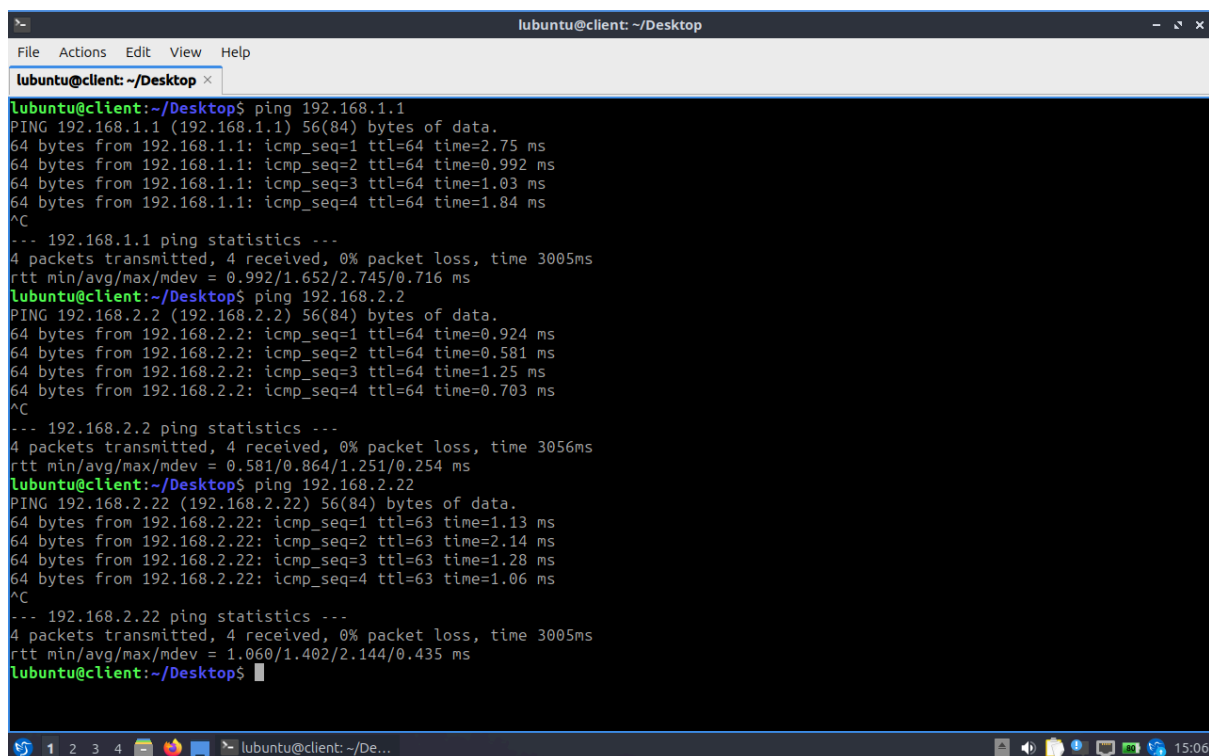
```
lubuntu@router: ~/Desktop
File Actions Edit View Help
lubuntu@router: ~/Desktop x
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
#
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
#
#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
"/etc/sysctl.conf" 64L, 2209B
28,1 Top
```

Tinggal dihapus simbol hastag nya, agar tidak dianggap sebagai komentar.



```
lubuntu@router: ~/Desktop
File Actions Edit View Help
lubuntu@router: ~/Desktop x
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
#
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
#
#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
"/etc/sysctl.conf" 64L, 2208B
27,1 Top
```

Oke, tinggal di simpan, dan kita coba ping dari vm klien ke vm lainnya.



```
lubuntu@client: ~/Desktop
File Actions Edit View Help
lubuntu@client: ~/Desktop x
lubuntu@client:~/Desktop$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.75 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.992 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.03 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.84 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.992/1.652/2.745/0.716 ms
lubuntu@client:~/Desktop$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=0.924 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=0.581 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=64 time=1.25 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=64 time=0.703 ms
^C
--- 192.168.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.581/0.864/1.251/0.254 ms
lubuntu@client:~/Desktop$ ping 192.168.2.22
PING 192.168.2.22 (192.168.2.22) 56(84) bytes of data.
64 bytes from 192.168.2.22: icmp_seq=1 ttl=63 time=1.13 ms
64 bytes from 192.168.2.22: icmp_seq=2 ttl=63 time=2.14 ms
64 bytes from 192.168.2.22: icmp_seq=3 ttl=63 time=1.28 ms
64 bytes from 192.168.2.22: icmp_seq=4 ttl=63 time=1.06 ms
^C
--- 192.168.2.22 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.060/1.402/2.144/0.435 ms
lubuntu@client:~/Desktop$
```

Seperti yang terlihat pada gambar di atas, bahwa dari client, ping ke router dan ke server terbukti berhasil, dan menandakan bahwa jaringan LAN pada VirtualBox ini berhasil.

Mungkin itu saja yang dapat kami sampaikan, kita ketemu lagi pada minggu depan saat kami membahas progress minggu ke tiga: **Capture dan analisis HTTP paket login**. *See ya there, amigos, peace!*

- Kelompok 2