

JOB SHEET PRACTICE

LEARNING ACTIVITIES:1

Nama : Andry Saputra

Sekolah : SMKN 1 Kota Bekasi

Software :

Virtual Machine: **VirtualBox**

OS : Linux Debian 9, KaliLinux, Windows 7

all applications can be downloaded at : 119.235.16.190

Hardware Minimal :

Processor : Laptop (AMD Athlon Silver 3050u with Integrated Graphics) or Intel Core Processor i5 2520M later / above.

RAM : 8 GB

HOST OS : Windows 10

Internet

Work Steps

1. Install Virtual Machine
2. Create PC host, scheme :

INFORMATION OF ADAPTERS

Tools

Kali Linux
Running

Server Debian
Running

Windows 10
Powered Off

New Settings Discard Show

General

Name: Kali Linux
Operating System: Other Linux (64-bit)

System

Base Memory: 1500 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 119 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Primary Device 0: Kali Linux.vdi (Normal, 180.00 GB)
IDE Secondary Device 0: [Optical Drive] kali-linux-2019.3-amd64.iso (2.83 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Server (Bridged Adapter, Intel(R) Ethernet Connection I217-LM)
Adapter 2: Intel PRO/1000 MT Server (Host-only Adapter, VirtualBox Host-Only Ethernet Adapter)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

Tools

Kali Linux
Running

Server Debian
Running

Windows 10
Running

New Settings Discard Show

General

Name: Server Debian
Operating System: Debian (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Server Debian.vdi (Normal, 80.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Server (Bridged Adapter, Intel(R) Ethernet Connection I217-LM)
Adapter 2: Intel PRO/1000 MT Server (Host-only Adapter, VirtualBox Host-Only Ethernet Adapter)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

Tools

Kali Linux

Running

Server Debian

Running

Windows 10

Running

New

Settings

Discard

Show

General

Name: Windows 10

Operating System: Windows 10 (64-bit)

System

Base Memory: 2048 MB

Processors: 2

Boot Order: Floppy, Optical, Hard Disk

Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB

Graphics Controller: VBoxSVGA

Remote Desktop Server: Disabled

Recording: Disabled

Storage

Controller: SATA

SATA Port 0: Windows 10.vdi (Normal, 50.00 GB)

SATA Port 1: [Optical Drive] Win10_MAI_2019_UPDATE_English_x64.iso (4.60 GB)

Audio

Host Driver: Windows DirectSound

Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Server (Bridged Adapter, Intel(R) Ethernet Connection I217-LM)

USB

USB Controller: xHCI

Device Filters: 0 (0 active)

Shared folders

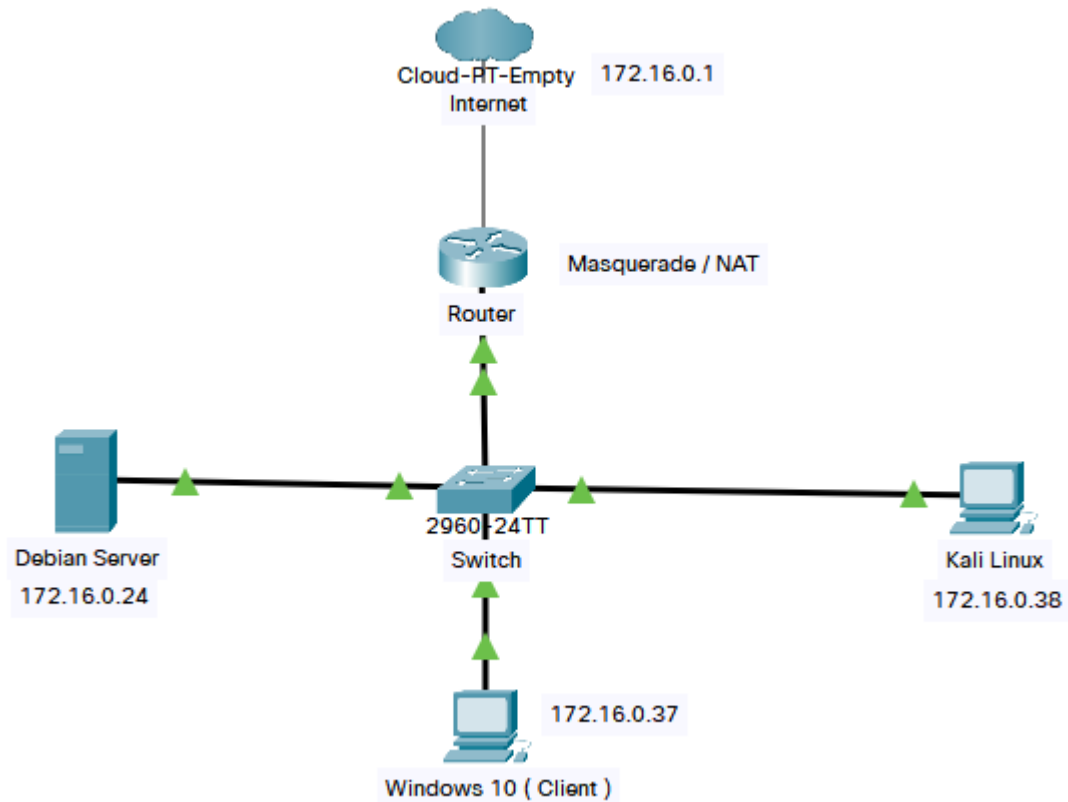
None

Description

None

JOB SHEET PRACTICE

LEARNING ACTIVITIES:1



Gambar Topology

No	Steps	Information
1.	Install Debian	Version: 9.7 Amd x64 Codename : Debian Stretch
	Boot :	<i>DVD/CD : ISO</i>
	Type installation	<i>GUI (Graphical User Interface)</i>
	Instalasi language	<i>English</i>
	your location	<i>Other > Asia > Indonesia</i>
	keyboard	<i>American English.</i>
	Network	<i>Automatically Network Configure with DHCP (enp0s17)</i>
	Hostname	<i>andry</i>
	Root password	<i>123 * case sensitive</i>
	Full name for new user	<i>andry * case sensitive</i>
	Username for your account	<i>andry * case sensitive</i>

	Password new user	123 * case sensitive
	Time Zone	based on your location exp : western / Jakarta
	Partisi hardisk (partisi hardisk)	Guide Partition. Separate /home partition (recommend new users)
	Configuration Packet manager. Scan Another CD or DVD	No Survey : no
	Software Selection	1. Standar System Utility 2. ssh server

	install GRUB boot loader on Hardisk :	Yes, /dev/sda
	Success For Debian Client Installation?	Yes

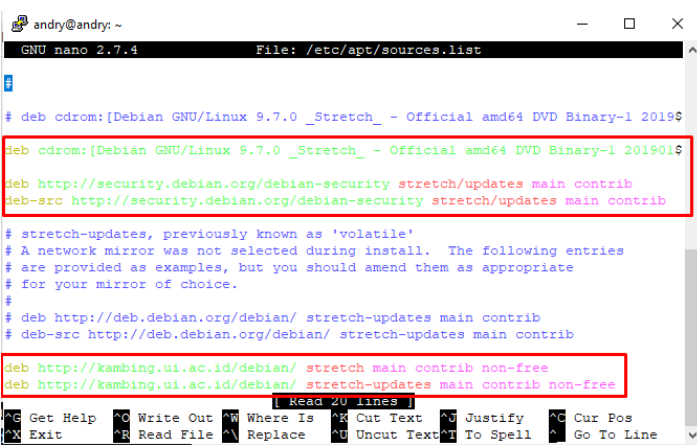
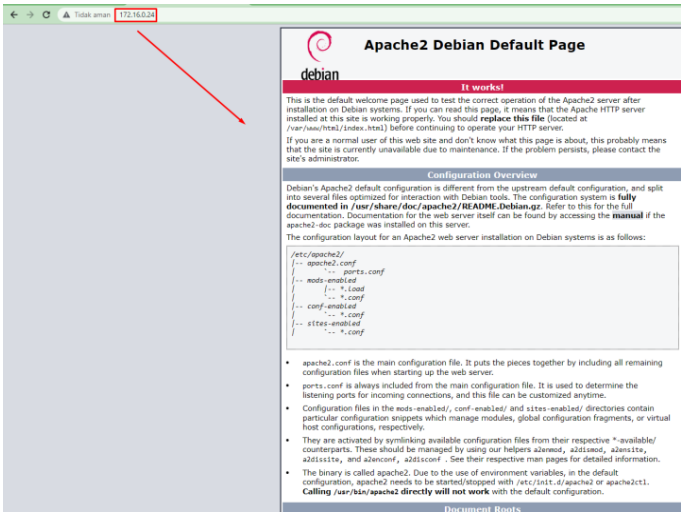
Server configuration

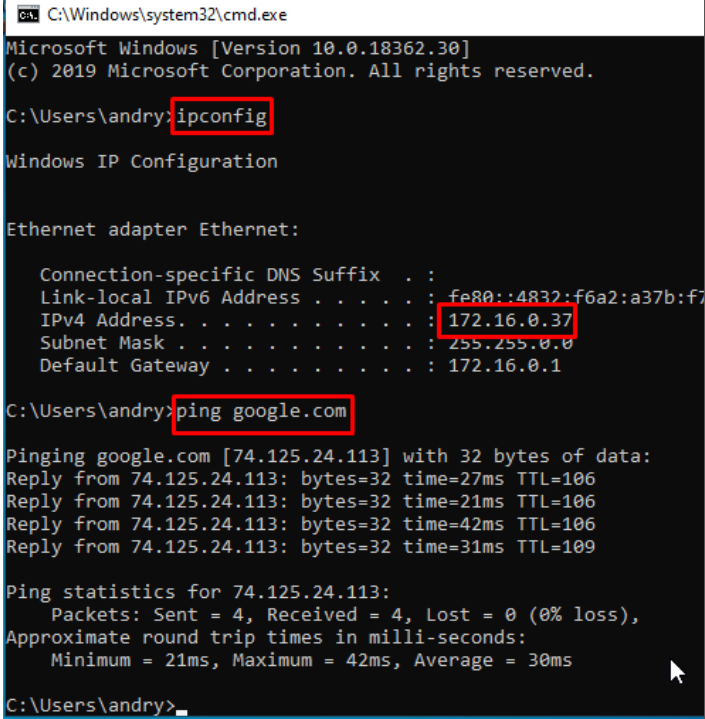
2.	Login	username : andry, password: 123
3.	show interfaces	ls /sys/class/net
4.	Configure network fil.	nano /etc/network/interfaces <pre># Th WAN network interface allow-hotplug enp0s17 iface enp0s17 inet dhcp</pre> ----- <pre> 2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdis group default qlen 1000 link/ether 08:00:27:c8:f8:ec brd ff:ff:ff:ff:ff:ff 3: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdi group default qlen 1000 link/ether 08:00:27:f5:31:62 brd ff:ff:ff:ff:ff:ff inet 172.16.0.24/16 brd 172.16.255.255 scope global dy valid lft 421sec preferred lft 421sec inet6 fe80::a00:27ff:fef5:3162/64 scope link valid lft forever preferred_lft forever root@andry:/home/andry# █ </pre> Note: all ip address adapted with your condition network. The configuration above is just an example Ctrl x Save : Y Then Reboot

5.	Check	<i>Ip addr</i>
6.	Repository file	<i>nano /etc/apt/sources.list</i>
		<i>Deactive all repository with #</i>
		# deb cdrom:[Debian GNU/Linux 9.5.0 _Stretch_ -Official i386 DVD Binary-1 2018\$ deb cdrom:[Debian GNU/Linux 9.5.0 _Stretch_ -Official i386 DVD Binary-1 201807\$ deb http://security.debian.org/debian-security stretch/updates main contrib deb-src http://security.debian.org/debian-security stretch/updates main contrib # stretch-updates, previously known as 'volatile' # A network mirror was not selected during install. The following entries # are provided as examples, but you should amend them as appropriate # for your mirror of choice. # # deb http://deb.debian.org/debian/ stretch-updates main contrib

		# deb-src http://deb.debian.org/debian/ stretch-updates main contrib
7.	Update Debian	<i>apt-get update</i>
8.	Install ifconfig	<i>apt-get install net-tools</i>
9.	Install iptables	<i>apt-get install iptables-persistent</i> <i>apt-get install netfilter-persistent</i>
10.	Router Configuration	<i>nano /etc/sysctl.conf</i>
11.		<i>Change line :</i> <i>net.ipv4.ip_forward=0</i> <i>to</i> <i>net.ipv4.ip_forward=1</i>
12.		<i>nano /proc/sys/net/ipv4/ip_forward</i>

13.		Change 0 To 1
14.	Iptables command	<i>iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE</i>
15.	Save iptable	<i>iptables-save > /etc/iptables/rules.v4</i> or <i>netfilter-persistent save</i>
16.	Show location iptables save	<i>nano /etc/iptables/rules.v4</i>
17.	Debian Server	PC Guest 2 : server, do as steps 1
	Configuration	
18.	Login	<i>username : andry , password: 123</i>
19.	show interfaces	<i>ls /sys/class/net</i>
20.	Configure network file	<i>nano /etc/network/interfaces</i>
		<i>Allow-hotplug enp0s3</i> <i>Iface enp0s3 inet dhcp</i>
		Ctr x Save : Y <i>Then Reboot</i> ----- Note: all ip address adapted with your condition network. The configuration above is just an example
21.	Check	<i>Ip addr</i>
22.	Repository file	<i>nano /etc/apt/sources.list</i>
		<i>Deactive all repository with #</i>
		<i>Remote using putty</i>

		 if kambing ui after apt update get error, use another repository Recommend Use Kartolo sby. Get now from linuxsec
23.	Update debian	<i>apt-get update</i>
24.	Install ifconfig	<i>apt-get install net-tools</i>
25.	Install http	<i>apt-get install apache2</i> * configuration and testing later
26.	Install FTP - Testing Server address with one client to access one feature have been installed	<i>apt-get install proftpd</i> * configuration and testing later Choose Web Server Options : 
27.	Install Windows 10	<i>PC Guest 3 : client,</i>
28.	Boot	<i>DVD/CD : ISO</i>
	Computer Name	<i>andry</i>
	Partition	<i>NTFS single partition, drive C:</i>

	Username	andry
	Password	123
	Ip address	 ----- Note: all ip address adapted with your condition network. The configuration above is just an example
29.	Install Kali Linux 2019.3	PC Guest 3 : testing NMAP, do as steps 1
30.	Configuration	
	Login	username : kali , password: kali
	show interfaces	ls /sys/class/net
	Configure network file	nano /etc/network/interfaces

	Note: all ip address adapted with your condition network. The configuration above is just an example	<pre> root@kali:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo up default qlen 1000 link/ether 08:00:27:8d:bb:82 brd ff:ff:ff:ff:ff:ff inet 192.168.56.101/24 brd 192.168.56.255 scope global dynar eth0 valid_lft 533sec preferred_lft 533sec inet6 fe80::a1db:f412:9190:a08e/64 scope link noprefixroute valid_lft forever preferred_lft forever 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo up default qlen 1000 link/ether 08:00:27:f9:f4:c1 brd ff:ff:ff:ff:ff:ff inet 172.16.0.38/16 brd 172.16.255.255 scope global dynamic 1 valid_lft 509sec preferred_lft 509sec inet6 fe80::c955:5f36:2f03:987c/64 scope link noprefixroute valid_lft forever preferred_lft forever root@kali:~# root@kali:~# ping google.com PING google.com (142.251.10.100) 56(84) bytes of data. 64 bytes from sd-in-f100.1e100.net (142.251.10.100): icmp_seq=1 ttl= ms 64 bytes from sd-in-f100.1e100.net (142.251.10.100): icmp_seq=2 ttl= ms ^C --- google.com ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1002ms rtt min/avg/max/mdev = 23.539/30.537/37.536/6.998 ms </pre>
31.	Testing NMAP and capture screen your results	<i>nmap -sP 172.16.0.24 -sP</i> <i>nmap 172.16.0.37 -sP & nmap 172.16.0.38 -sP</i>

	All testing adapted with your ip address condition	<i>nmap 172.16.0.24 -sT</i> <i>nmap 172.16.0.37 -sT</i>
		<i>nmap 172.16.0.24 -sS</i> <i>nmap 172.16.0.37 -sS</i> <i>nmap 172.16.0.38 -sS</i>
		<i>nmap 172.16.0.24 -sF</i> <i>nmap 172.16.0.37 -sF</i> <i>nmap 172.16.0.38 -sF</i>
		<i>nmap -O nmap 172.16.0.24</i> <i>nmap -O nmap 172.16.0.37</i>
32.	Paste capture screen in tables belows	Table 2
33.	Upload this file	LMS your account

Pengujian

Tabel 2 your result

No	Nmap	explanation	capture screen
1	<code>nmap -sP 172.16.0.24-38</code>	Dari percobaan tersebut dapat dilihat bahwa nmap akan mencari discovery host yang aktif dan akan mencetak host yang tersedia.	<pre>root@kali:~# nmap -sP 172.16.0.24 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:41 UTC Nmap scan report for 172.16.0.24 Host is up (0.00042s latency) MAC Address: 08:00:27:F5:31:62 (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds root@kali:~#</pre> <pre>root@kali:~# nmap -sP 172.16.0.37 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:41 UTC Nmap scan report for 172.16.0.37 Host is up (0.00030s latency) MAC Address: 08:00:27:CD:8E:67 (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds root@kali:~#</pre> <pre>root@kali:~# nmap -sP 172.16.0.38 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:57 UTC Nmap scan report for 172.16.0.38 Host is up. Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds root@kali:~#</pre>

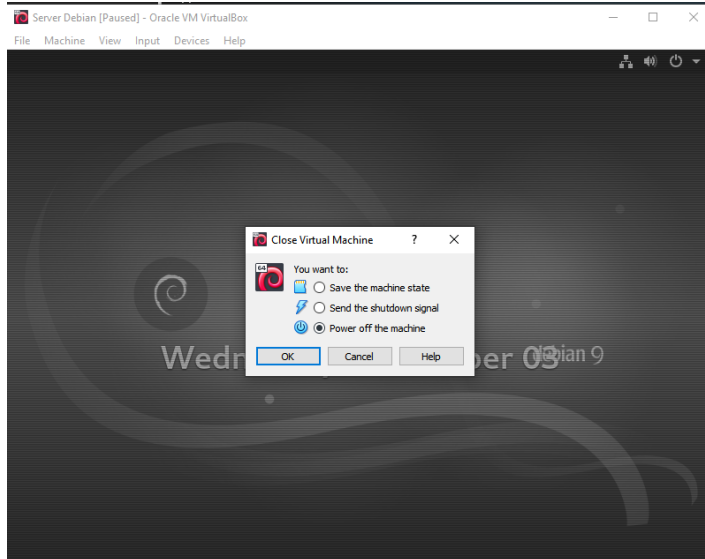
2

nmap
172.16.0.24 -sT
nmap
172.16.0.37 -sT
nmap
172.16.0.38 -sT

Dari gambar tersebut dapat dilihat bahwa nmap akan mencari port yang sudah terbuka pada setiap system operasi.

Dan ip **172.16.0.24** adalah ip dari debian server terlihat disitu "Host seems Down (0 host up)" dikarenakan saya mencoba shutdown mesin apakah hasil scan debian server adalah down dari kali linux.

```
root@kali:~# nmap -sT 172.16.0.24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 04:10 UTC
Note: Host seems down. If it is really up, but blocking our ping probes,
Nmap done: 1 IP address (0 hosts up) scanned in 0.65 seconds
root@kali:~#
```



```
root@kali:~# nmap -sT 172.16.0.37
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 04:10 UTC
Nmap scan report for 172.16.0.37
Host is up (0.00068s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
5357/tcp  open  wsddapi
MAC Address: 08:00:27:CD:8E:67 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.86 seconds
root@kali:~#
```

```
root@kali:~# nmap -sT 172.16.0.38
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 04:10 UTC
Nmap scan report for 172.16.0.38
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
root@kali:~#
```

3	<pre>nmap 172.16.0.24 -sS nmap 172.16.0.37 -sS nmap 172.16.0.38 -sS</pre>	Dari percobaan diatas dapat dilihat bahwa membuka koneksi TCP secara utuh dan tersembunyi.	<pre>root@kali:~# nmap -sS 172.16.0.24 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:5 Nmap scan report for 172.16.0.24 Host is up (0.00015s latency). Not shown: 999 closed ports PORT STATE SERVICE 80/tcp open http MAC Address: 08:00:27:F5:31:62 (Oracle VirtualBox virtual Nmap done: 1 IP address (1 host up) scanned in 0.35 second root@kali:~# root@kali:~# nmap -sS 172.16.0.37 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:59 UT Nmap scan report for 172.16.0.37 Host is up (0.00038s latency). Not shown: 999 filtered ports PORT STATE SERVICE 5357/tcp open wsdaoi MAC Address: 08:00:27:CD:8E:67 (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 14.52 seconds root@kali:~#</pre>
---	---	---	--

			<pre>root@kali:~# nmap -sS 172.16.0.38 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:24 UT Nmap scan report for 172.16.0.38 Host is up (0.00014s latency). Not shown: 999 closed ports PORT STATE SERVICE 111/tcp open rpcbind Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds root@kali:~#</pre>
--	--	--	--

4	<pre> nmap 172.16.0.24 -sF nmap 172.16.0.37 -sF nmap 172.16.0.38 -sF </pre>	Dari percobaan diatas dapat dilihat status scan dari nmap akan mengecek state dari pada layanan. Dan ip 172.16.0.37 adalah ip dari windows 10 terlihat disitu "Host seems Down (0 host up)" dikarenakan saya mencoba shutdown mesin apakah hasil scan windows adalah down dari kali linux.	<pre> root@kali:~# nmap 172.16.0.24 -sF Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:46 Nmap scan report for 172.16.0.24 Host is up (0.00037s latency). Not shown: 999 closed ports PORT STATE SERVICE 80/tcp open http MAC Address: 08:00:27:F5:31:62 (Oracle VirtualBox virtual N Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds root@kali:~# nmap 172.16.0.37 -sF Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:43 Nmap scan report for 172.16.0.37 Host is up (0.00031s latency). All 1000 scanned ports on 172.16.0.37 are open filtered MAC Address: 08:00:27:CD:8E:67 (Oracle VirtualBox virtual N Nmap done: 1 IP address (1 host up) scanned in 22.01 second root@kali:~# nmap 172.16.0.37 -sF Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 03:44 Note: Host seems down. If it is really up, but blocking our Nmap done: 1 IP address (0 hosts up) scanned in 0.57 second root@kali:~# root@kali:~# nmap 172.16.0.38 -sF Starting Nmap 7.80 (https://nmap.org) at 2021-11-0 Nmap scan report for 172.16.0.38 Host is up (0.00012s latency). Not shown: 999 closed ports PORT STATE SERVICE 111/tcp open rpcbind Nmap done: 1 IP address (1 host up) scanned in 1.43 root@kali:~# </pre>
5	<pre> nmap -O nmap 172.16.0.24 nmap -O nmap 172.16.0.37 </pre>	Dari percobaan scanning nmap tersebut akan menscan sistem operasi yang digunakan setiap host.	<pre> root@kali:~# nmap -O 172.16.0.24 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 02:52 UT Nmap scan report for 172.16.0.24 Host is up (0.00034s latency). Not shown: 999 closed ports PORT STATE SERVICE 80/tcp open http MAC Address: 08:00:27:F5:31:62 (Oracle VirtualBox virtual NIC) Device type: general purpose Running: Linux 3.X 4.X OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel: OS details: Linux 3.2 - 4.9 Network Distance: 1 hop OS detection performed. Please report any incorrect results at ubmit/ . Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds root@kali:~# </pre>

			<pre> root@kali:~# nmap -O 172.16.0.37 Starting Nmap 7.80 (https://nmap.org) at 2021-11-03 04:05 UT Nmap scan report for 172.16.0.37 Host is up (0.00075s latency). Not shown: 999 filtered ports PORT STATE SERVICE 5357/tcp open wsdapi MAC Address: 08:00:27:CD:8E:67 (Oracle VirtualBox virtual NIC) Warning: OSScan results may be unreliable because we could not en and 1 closed port Device type: specialized general purpose Running (JUST GUESSING): AVtech embedded (87%), Microsoft Wind SD 6.X 10.X (86%) OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:freebsd:freebs d:freebsd:10.3 Aggressive OS guesses: AVtech Room Alert 26W environmental mon ft Windows XP SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10 No exact OS matches for host (test conditions non-ideal). Network Distance: 1 hop OS detection performed. Please report any incorrect results at ubmit/ . Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds root@kali:~# </pre>
--	--	--	---

****Note change with your ip address condition**