LAPORAN PRAKTIKUM KEAMANAN SIBER TUGAS 8

KELAS PRAKTIKUM KEAMANAN SIBER C– TIK

KELOMPOK :

1. **ELSA ESTER LOKAS** **220211060213**
2. **GABRIELLA IGNATIA MANENGKEY** **220211060195**
3. **JUSTISYA INJILIA TUMBEL** **220211060229**

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS SAM RATULANGI

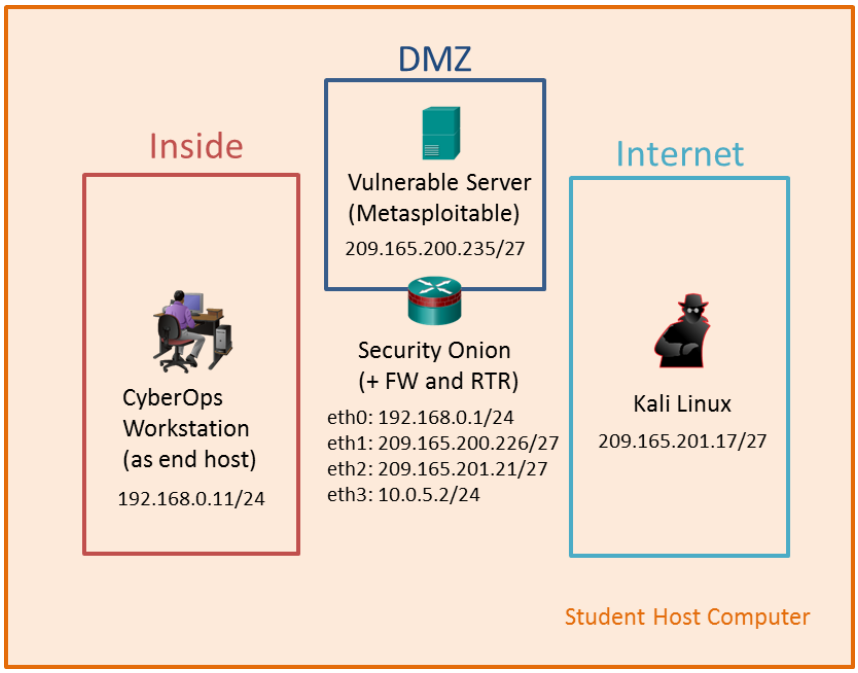
2025

Link Video :

https://www.youtube.com/playlist?list=PLi7QDVC5aN-Jb4TSNesCzCswvZvFrI7TD

Lab – Setup a Multi-VM Environment

Topology



Objectives

In this lab, you will set up a virtual network environment by connecting multiple virtual machines in Virtualbox.

Background / Scenario

A virtual network security sandbox or multi-VM lab environment is useful for security analysis and testing. This multi-VM environment is a requirement for more advanced labs in this course.

Required Resources

- The CyberOps Workstation VM (cyberops_workstation.ova).
- Internet Connection
- The following .ova files for creating additional VMs: kali_linux.ova, metasploitable.ova, and security_onion.ova. Click each link to download the files.
- Host computer with at least 8 GB of RAM and 45 GB of free disk space.

  Note: If your computer only has 8 GB of RAM, make sure you have no other applications open except for a PDF reader program to refer to this lab. VM Settings

Virtual Machine	OS	OVA Size	Disk Space	RAM	Username	Password
CyberOps Workstation VM	Arch Linux	2.23 GB	7 GB	1 GB	analyst	cyberops
Kali	Kali Linux	3.07 GB	10 GB	1 GB	root	cyberops
Metasploitable	Ubuntu Linux	851 MB	8 GB	512 MB	msfadmin	msfadmin
Security Onion	Ubuntu Linux	2.35 GB	10 GB	4 GB	analyst	cyberops
	Totals	**8.5 GB**	**45 GB**	**6.5 GB**		

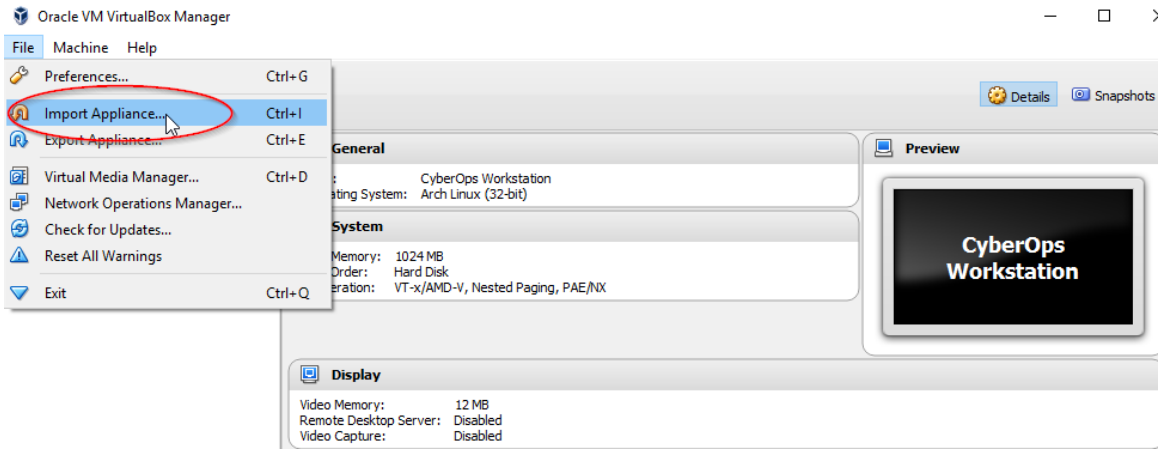
Note: If you have typed the username incorrectly for the Kali VM, click **Cancel** to input the correct username.

Step 1: Import appliance virtual machines into VirtualBox.

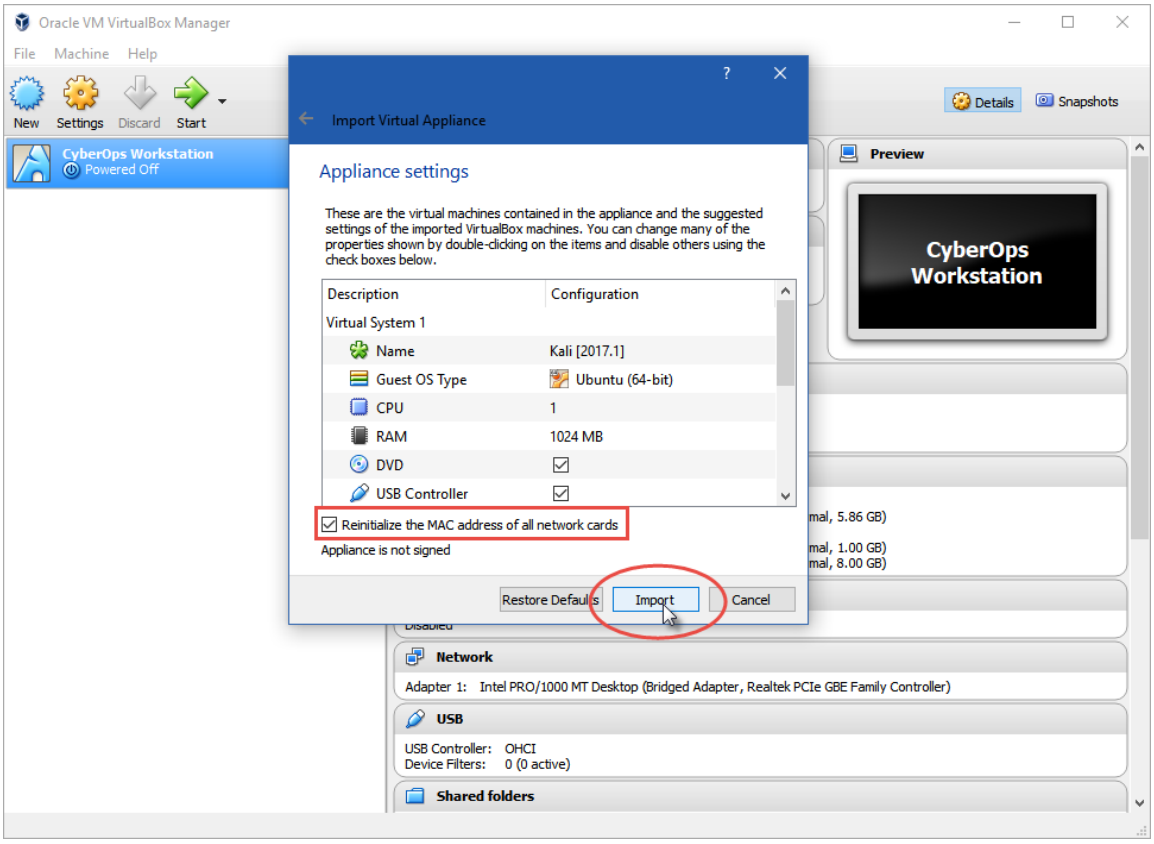
VirtualBox is able to host and run multiple virtual machines. Along with the CyberOps Workstation VM that has already been installed, you will import additional virtual machines into VirtualBox to create a virtual network.

Note: The screen may look different depending on your version of VirtualBox.

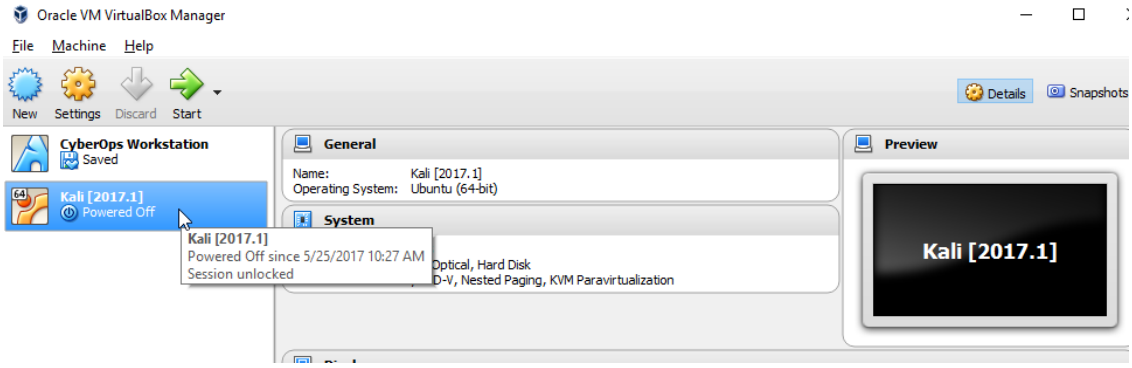
a. Use the file menu in VirtualBox to install Kali Linux: **File > Import Appliance**, then navigate to the kali_linux.ova file and click **Next**.



b. A new window will appear presenting the settings suggested in the OVA archive. Check the **"Reinitialize the MAC address of all network cards"** box at bottom of the window. Leave all other settings as default. Click **Import**.

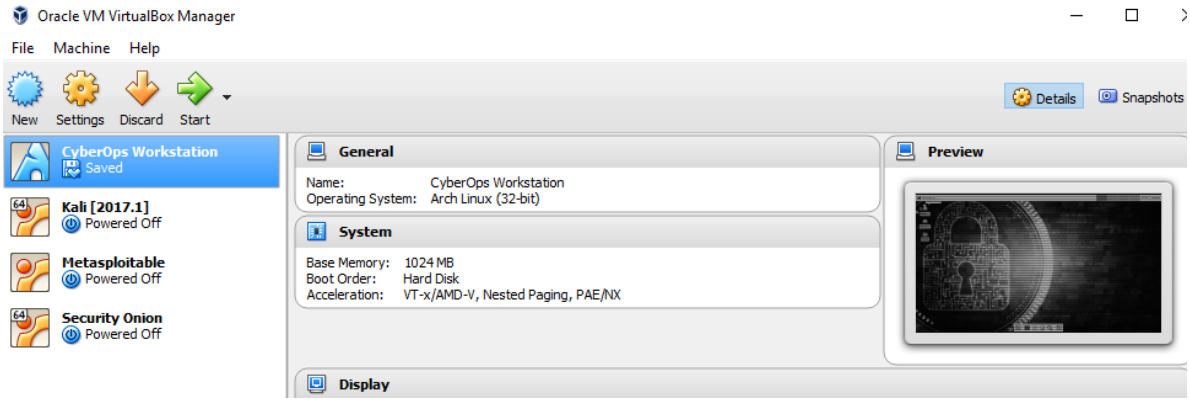


c. After the import is complete, VirtualBox will show the new Kali VM. Your Kali Linux VM file name might be different than the graphic shown below.



d. Now import the Metasploitable and the Security Onion VMs using the same method.

e. All four VMs are now shown in VirtualBox.

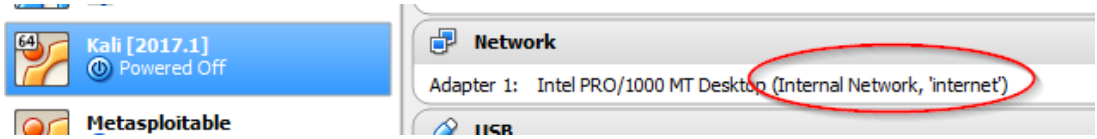


Step 2: Network the Virtual Machines to create a virtual lab.

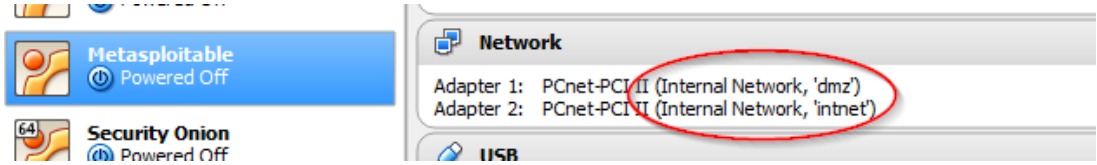
In this part, you will ensure that networking is configured between the VMs. In VirtualBox, a VM's network adapter can be in bridged mode (visible on the network like any other physical device), NAT mode (visible on the network but in a separate IP address space), or internal mode (only visible to other virtual machines with the same internal name or virtual local area network [VLAN]).

Examine the network settings for each virtual machine and take note of how the network adapter modes and names place the VMs in different VLANs.

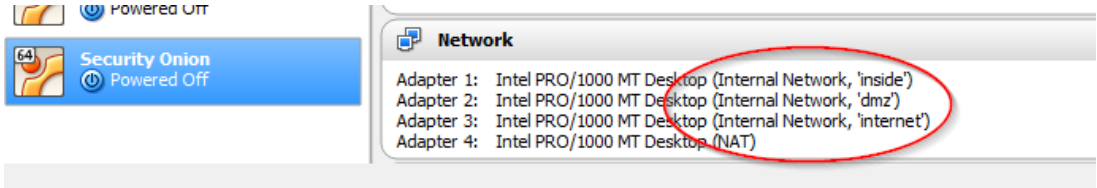
a. Kali has one network adaptor using **internal network** mode in the **internet** VLAN. Notice how this corresponds to the network diagram on page 1.



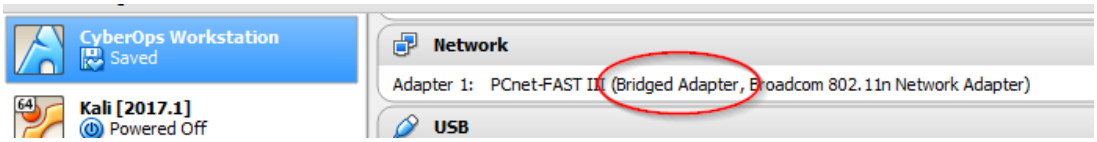
b. Metasploitable has two network adaptors using **internal network** mode, Adapter 1 corresponds to this lab and is in the **dmz** VLAN. While Adapter 2 is displayed by VirtualBox, it is not used in this topology and it can be ignored.



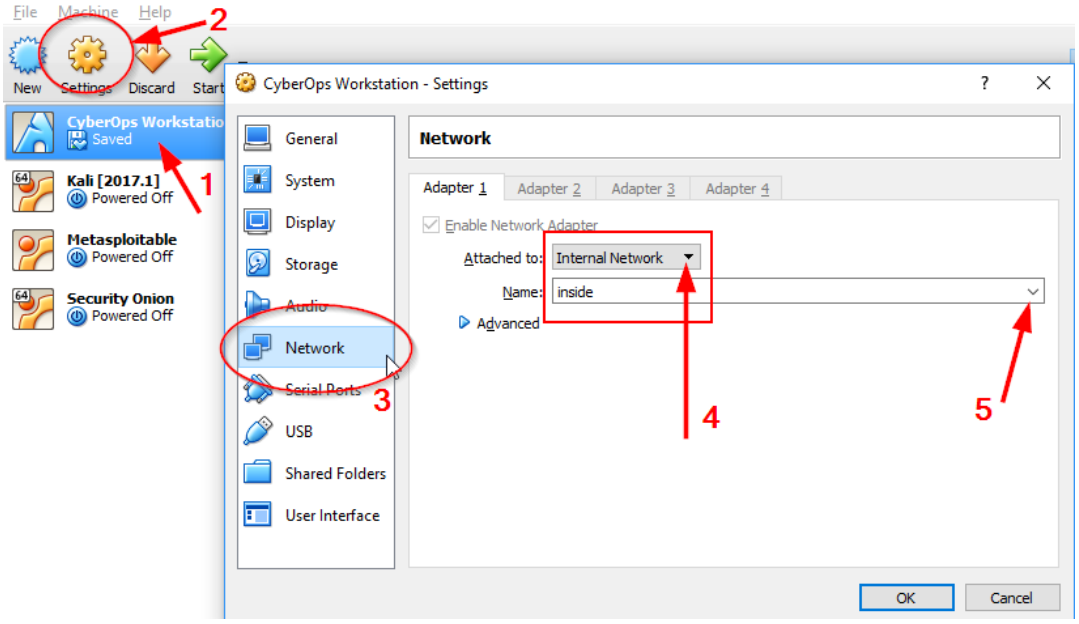
c. Security Onion has four network adaptors, three using **internal network** mode and one using **NAT** mode which could be used to reach the internet. Security Onion connects all of the VMs in the virtual network, with a network adapter in each of the VLANs (**inside**, **dmz**, and **internet**).



d. CyberOps Workstation VM is in **bridged** mode. It is not in an internal network with the other VMs. You will need to change the network adapter next.



e. Select the CyberOps Workstation VM in VirtualBox and click Settings. Select **Network** and change Adapter 1 to **internal network**, with the name **inside**. Click **OK**.



f. Now that the network adapter is in the right internal network or VLAN, launch the CyberOps Workstation VM and log in. You will need to change the IP address settings to communicate on the virtual network.

g. Open a command prompt and examine the contents of the scripts folder inside the **lab.support.files/scripts** folder.

```
[analyst@secOs~]$ ls lab.support.files/scripts
configure_as_dhcp.sh              cyops.mn                  start_ELK.sh
configure_as_static.sh            fw_rules                  start_miniedit.sh
cyberops_extended_topo_no_fw.py   mal_server_start.sh       start_pox.sh
cyberops_extended_topo.py         net_configuration_files   start_snort.sh
cyberops_topo.py                  reg_server_start.sh       start_tftpd.sh
[analyst@secOps ~]$
```

h. The script **configure_as_dhcp.sh** is used to configure the network interface to request an IP address from a DHCP server. This is the default setting for the CyberOps Workstation VM. To configure it for a multi-VM environment, you will need to run the **configure_as_static.sh** script. This will configure the network interface with the static IP address 192.168.0.11 and a default gateway of 192.168.0.1, which is the Security Onion VM. The Security Onion VM is responsible for routing between the Inside, DMZ, and Internet networks. Run the **configure_as_static.sh** script and enter the password (if prompted) to set the IP address to 192.168.0.11 in the virtual network.

```
[analyst@secOs~]$ sudo ./lab.support.files/scripts/configure_as_static.sh
[sudo] password for analyst:
Configuring the NIC as:
IP: 192.168.0.11/24
GW: 192.168.0.1

IP Configuration successful.

[analyst@secOps ~]$
```

Note: If you need to use CyberOps Workstation VM as a stand-alone environment with access to the Internet, change the network adapter back to bridged mode and run the **configure_as_dhcp.sh** script.

i. Return to VirtualBox and power on the other VMs: Kali Linux, Metasploitable, and Security Onion. Refer to the **VM Settings** table for username and password information.

Note: If necessary, use the right control key to unlock the cursor to navigate between windows.

j. When all of the VMs are running, ping from the CyberOps Workstation VM to the Metasploitable and Kali Linux VMs. Use **Ctrl+C** to stop the ping.

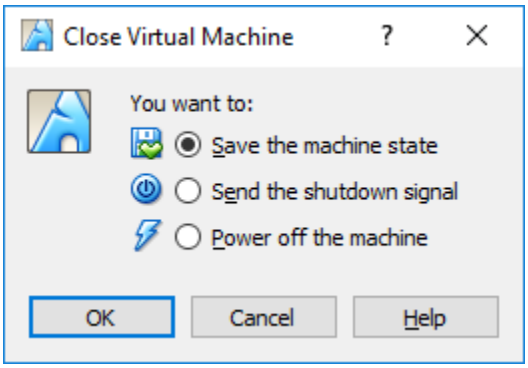
```
[analyst@secOps ~]$ ping 209.165.200.235
PING 209.165.200.235 (209.165.200.235) 56(84) bytes of data.
64 bytes from 209.165.200.235: icmp_seq=1 ttl=63 time=1.16 ms
64 bytes from 209.165.200.235: icmp_seq=2 ttl=63 time=0.399 ms
64 bytes from 209.165.200.235: icmp_seq=3 ttl=63 time=0.379 ms
^C
--- 209.165.200.235 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.379/0.646/1.162/0.365 ms
[analyst@secOps ~]$ ping 209.165.201.17
PING 209.165.201.17 (209.165.201.17) 56(84) bytes of data.
64 bytes from 209.165.201.17: icmp_seq=1 ttl=63 time=0.539 ms
64 bytes from 209.165.201.17: icmp_seq=2 ttl=63 time=0.531 ms
64 bytes from 209.165.201.17: icmp_seq=3 ttl=63 time=0.567 ms
64 bytes from 209.165.201.17: icmp_seq=4 ttl=63 time=0.408 ms
64 bytes from 209.165.201.17: icmp_seq=5 ttl=63 time=0.431 ms
^C
--- 209.165.201.17 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4065ms
rtt min/avg/max/mdev = 0.408/0.495/0.567/0.064 ms
[analyst@secOps ~]$
```

k. Close the terminal window when finished.

Step 3: Shut down the VMs.

a. For each VM, click **File > Close**.

b. Click the **Save the machine state** radio button and click **OK**. The next time you start the virtual machine, you will be able to resume working in the operating system in its current state.



The other two options are:

Send the shutdown signal: simulates pressing the power button on a physical computer

Power off the machine: simulates pulling the plug on a physical computer