Assignment 4[1]

1 Overview

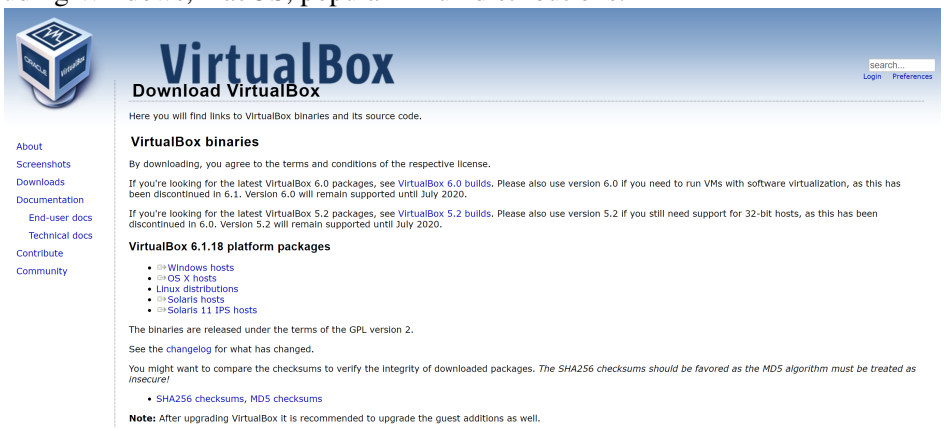
The goal of this assignment is to let students gain experiences on implementing a customized network topology using Mininet. With Mininet, we can conduct network experiments on a single machine without having to purchase real network devices and user computers. In this assignment, you are expected to setup a Mininet instance in a virtual machine. The instance will contain several users. Different hosts have different roles, and can communicate with one another. At last, a very simple SYN flooding attack experiment will be conducted in the instance.

2 Preparation

Take the following steps to setup the Mininet in your machine:

2.1 Install *Oracle VM Virtualbox*

You can download, install and run *Oracle VM Virtualbox* from here. Virtualbox supports different OSs, including Windows, macOS, popular Linux distributions.



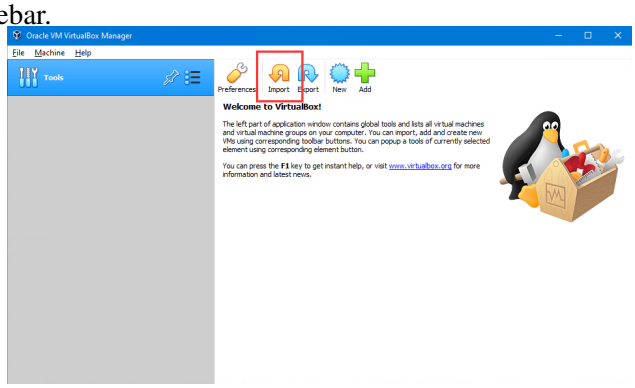
2.2 Download Virtual Appliance File

A virtual appliance file (*.ova) is a packaging file which can be imported into VirtualBox. It contains a operating system with customized applications and files. You can download the virtual appliance file from here.

[1] This assignment is a modified version of:
[Wenliang, Du. "TCP Attack Lab", SEED Labs, Syracuse University]

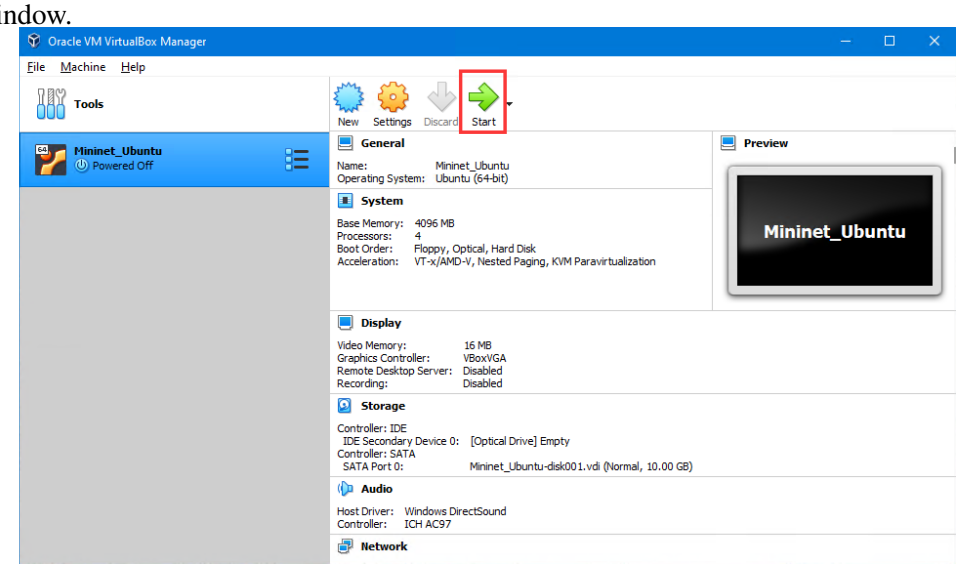
2.3 Import Virtual Appliance File

Run VirtualBox, click the "Import" button to import the appliance downloaded in the previous step. Keep default settings. Then, a new machine called *Mininet Ubuntu* should be added into the list of VMs in the left sidebar.



2.4 Start Virtual Machine

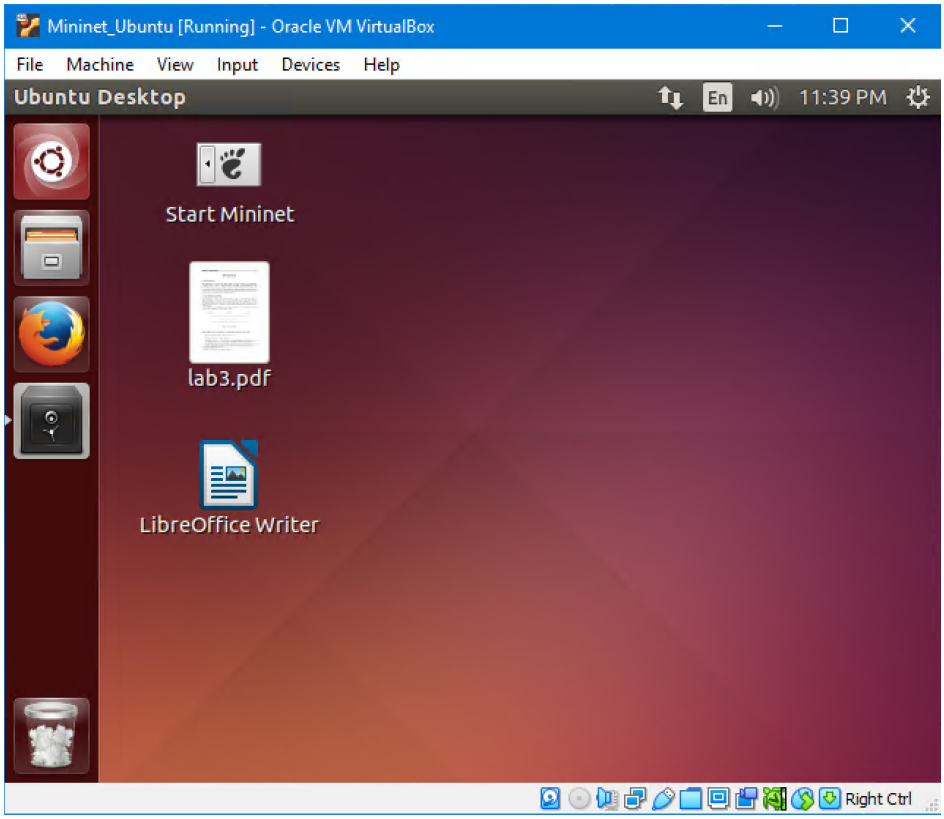
Power ON *Mininet Ubuntu* by clicking "Start" button and wait for Ubuntu to boot up. This machine has only one root user named *student* whose password is *lab3*. It is recommended to maximize the virtual machine window.



2.5 Start Mininet

Inside the Ubuntu virtual machine, run *Start Mininet* on the Desktop, which sets up all you need: a Mininet network, a terminal for each of the nodes `att`, `vic`, and `leg`, along with Wireshark with a proper filter on node `att`. [2]

[2] Note that the terminals may cover each other and Wireshark may be opened in a too large window. Drag the top terminals and resize the Wireshark window to reveal the the hidden ones if needed.



Note. Several tricks while using virtual machine:

1. To return your mouse to your native OS from the VM, you need to press "host key" shown in right bottom corner of VirtualBox window. e.g., "Right Ctrl" for Windows.

2. There are several ways to transfer files between the VM and your native OS. First, since you can access Internet directly from the virtual machine, you can upload files to any network drive using a browser. Second, you can use shared folder, a feature provided by *Oracle VM Virtualbox*. On the menu bar, click "Devices", "Shared Folders", "Shared Folder Settings", and select a folder in your real native OS.

3. To taking screenshots in Ubuntu is, use `shift + PrintScrn` and select the desired area.

3 Network Topology

To do this assignment, a network with 3 virtual hosts is needed in Mininet: One host is used for attacking, the second one is used as the victim, and the third one as a legitimate user. All these three hosts should be setup on the same LAN, and should be able to capture each other's packets. To do so, they are connected via a *hub*, a network device that broadcasts the Ethernet frames on all ports regardless of their destination.

We will use Mininet to emulate the topology in a virtual network. A hub can be modeled with a controller in Mininet. The configuration is summarized in the Figure 1.

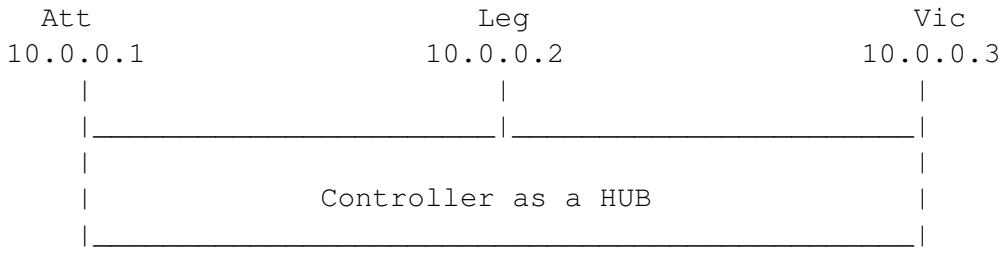


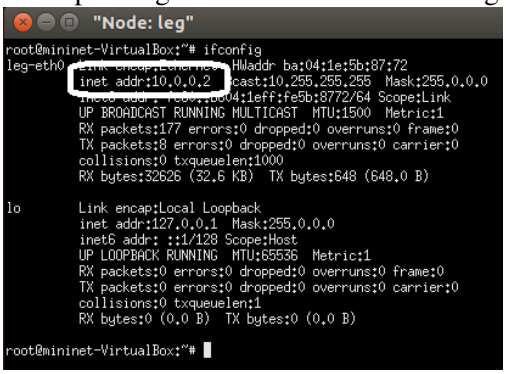
Figure 1: Network topology

4 Tasks

4.1 Task 1 : Mininet Test (15 Marks)

1. Verify if the controller act as a HUB and broadcast the Ethernet frames. To do so, ping the node `vic` from the node `leg` by typing "ping ip_address_of_node_vic" in node `leg`'s terminal (ip_address_of_node_vic is to be replaced by the IP address of node `vic`), check if the ICMP packet can be sniffed by the Wireshark running on the node `att`. Save a screenshot of the output of the ping command in the node `leg`'s terminal and a screenshot of Wireshark of the above ICMP packet. (5 marks)

   Note that you can find out the IP address of each nodes by running the command `ifconfig` on the corresponding terminal as shown in the figure below.



2. To verify if necessary services are started properly, use the `netstat -a` command, and among the outputs from the command, check for TCP sockets that listen to `ssh` and `telnet` ports. Save a screenshot of the output in the terminal. (5 marks)
   More information on "netstat" can be found by typing "man netstat" in the terminal.

3. Test the availability of a web service through the node `leg` by `wget`:

```
Test the HTTP server
#  wget 10.0.0.3
```

   Save a screenshot of the output in the terminal. (5 marks)

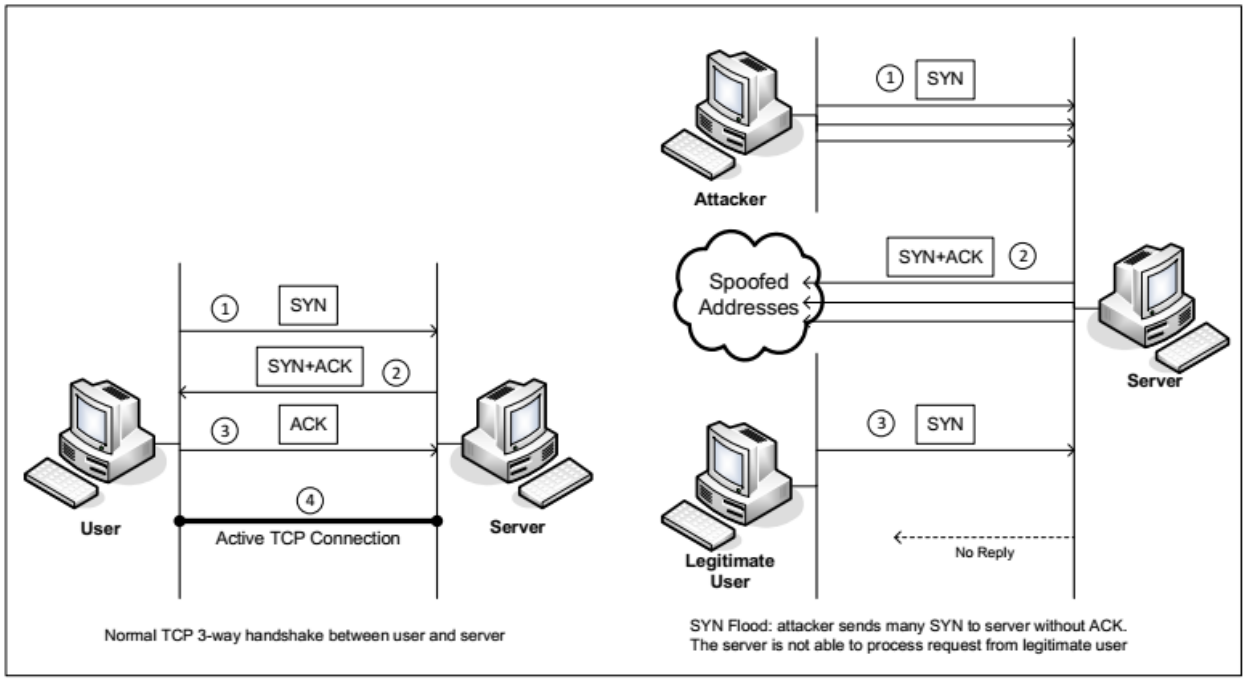


Figure 2: SYN Flood

4.2 Task 2 : SYN Flooding Attack (20 Marks)

SYN flood is a form of DoS attack in which attackers send many SYN requests to a victim's TCP port, but the attackers have no intention to finish the 3-way handshake procedure. Attackers either use spoofed IP address or do not continue the procedure. Through this attack, attackers can flood the victim's queue that is used for half-opened connections, i.e. the connections that has finished SYN, SYN-ACK, but has not yet got a final ACK back. When this queue is full, the victim cannot take any more connection. Figure 2 illustrates the attack.

`Netwox` **Tools.** Netwox is a useful tool to send out network packets of different types and with different contents.

It consists of a suite of tools, each having a specific number. You can run the command like the following (the parameters depend on which tool you are using). For some of the tools, you have to run it with the root privilege:

```
# netwox number [parameters ... ]
```

If you are not sure how to set the parameters, you can look at the manual by issuing "`netwox number --help2`".

Use `netwox` tool with appropriate parameters to conduct this attack from `att` to `vic` on HTTP (port 80). The corresponding Netwox tool for this task is numbered 76. Here is a simple help screen for this tool. You can also type "`netwox 76 --help2`" to get the help information.

Listing 1: The usage of the Netwox Tool 76

```
Title: Synflood
   Usage: netwox 76 -i ip -p port [-s spoofip]
   Parameters:
   -i|--dst-ip ip       destination IP address
   -p|--dst-port port   destination port number
   -s|--spoofip spoofip IP spoof initialzation type
```

Note. It is better to run `netwox 76` command for a short time and stop it by `Ctrl+C` quickly, otherwise the disk will be full for very short time. The other option is to disable Wireshark capturing at the beginning.

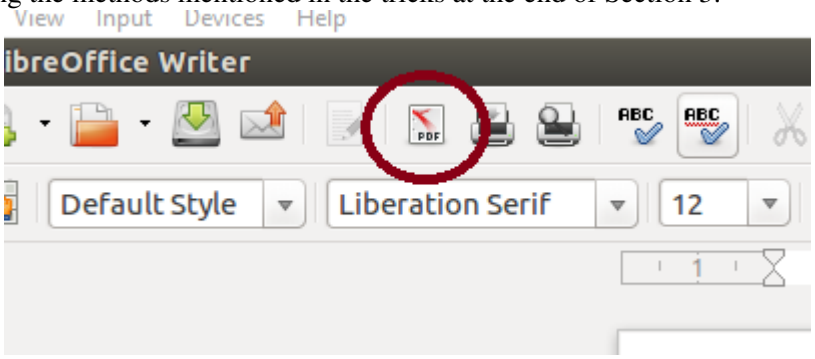
Run this attack and report the following items:

1. The `netwox` command and its arguments used for this attack (5 marks)
2. Output of command `"netstat -na"` on node `vic`, which checks the usage of the queue, i.e., the number of half-opened connections associated with a listening port. The state for such connections are `SYN-RECV`. If the 3-way handshake was finished, the state of the connections would be `ESTABLISHED`. (5 marks)
3. Include a snapshot of SYN packets sniffed by Wireshark. What can be seen about their source IP addresses? (5 marks)
4. Send a HTTP request (e.g., `wget` command) from `leg` to `vic` and trace the request via Wireshark. Could the node `leg` get any HTTP response from the server node `vic` during the attack? If yes, how long does it take? (5 marks)

5 Report (5 Marks)

Additionally, you should describe how you determine whether the attack is successful or not, e.g., by providing evidences from command outputs and your observations in ONE paragraph. (5 marks)

Hint: You can prepare your report inside the virtual machine using `libreOffice Writer` and export it directly to pdf by the following icon. Alternatively, you can transfer all screenshots to your native OS using the methods mentioned in the tricks at the end of Section 3.



Also an easy way for taking screenshots in Ubuntu is to use `shift + PrintScrn` and select the desired area.

Submit your report as a single pdf file to the "Assignment 4" folder on the Avenue.

DO NOT RUN NETWOX TO HOSTS OUTSIDE YOUR VM!