VM & Mininet demo[1]

1 Lab Overview

The learning objective of this lab is for students to gain the first-hand experience on the vulnerabilities of the TCP protocol, as well as on attacks against these vulnerabilities. The vulnerabilities in the TCP protocol represent a special genre of vulnerabilities in protocol designs and implementations; they provide an invaluable lesson as to why security should be designed in from the beginning, rather than being added as an afterthought. Moreover, studying these vulnerabilities help students understand the challenges of network security and why many network security measures are needed.

2 Lab Environment Setup

Network Topology. To conduct this lab, a network with 3 machines is needed: One machine is used for attacking, the second one is used as the victim, and the third one is used as a legitimate user. All these three machines should be setup on the same LAN, and should be able to sniff each other's packets. So the machines are connected via a *hub*, a network device that broadcast the Ethernet frames on all ports regardless of their destination.

We have used Mininet to emulate the lab in a virtual network. A hub can be modeled with a controller in Mininet. The configuration is summarized in the Figure 1.

```
  Att                     Leg                     Vic
10.0.0.1                10.0.0.2                10.0.0.3
    |                       |                       |
    |_______________________|_______________________|
    |                                               |
    |             Controller as a HUB               |
    |_______________________________________________|
```

Figure 1: Network topology

Network Setup. Take the following steps to setup the security lab network in your machine:

1. Download, install and run *Oracle VM Virtualbox* from here.
2. Download the lab 3 virtual appliance file from here.
3. In *Virtualbox* goto $Files \longrightarrow ImportAppliance$ and import the appliance downloaded in step 2. A new machine called *Mininet Ubuntu* should be added into the list of VMs in the left sidebar.
4. Power ON *Mininet Ubuntu* an 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.

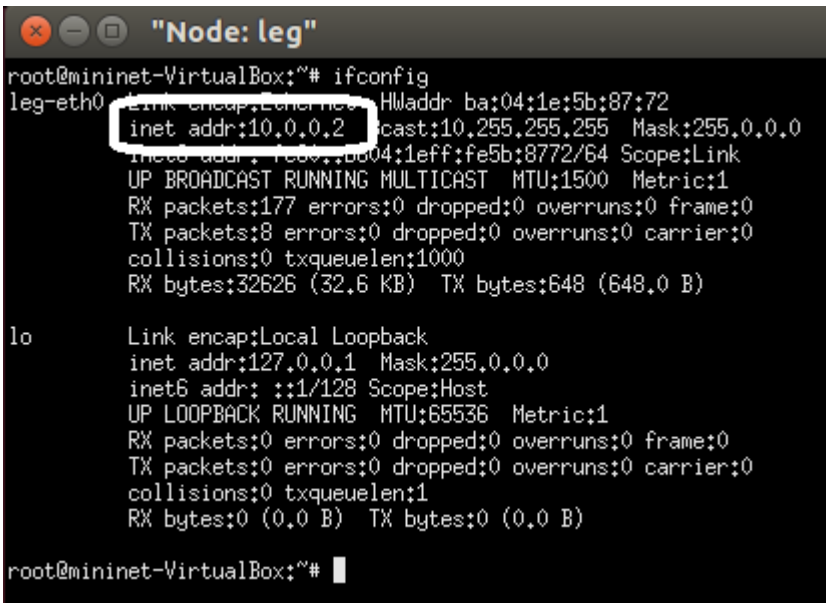
[1]This lab is a modified version of:
[Wenliang, Du. "TCP Attack Lab", SEED Labs, Syracuse University]

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

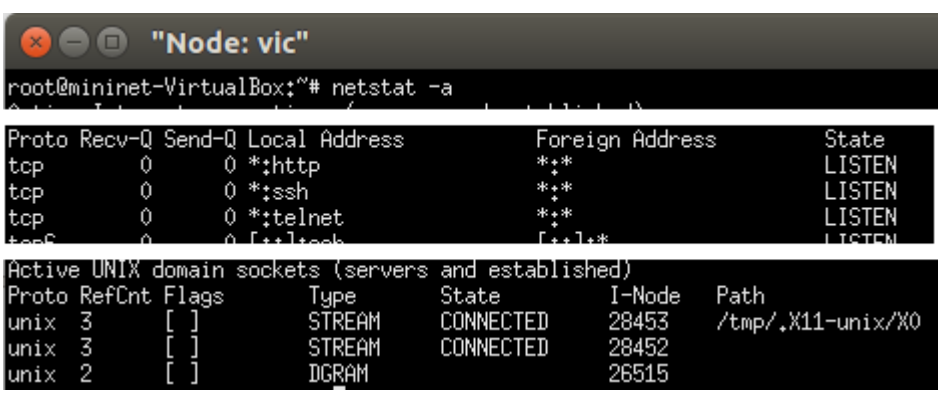
Verify the Network Setup. To check if the the network is setup correctly, do the following tests:

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`, check if the ICMP packet can be sniffed by the Wireshark running on the node `att`.

   Note that you can find out the IP address of each nodes by running the command `ifconfig` on the corresponding terminal:



2. verify if the services are started properly, use the `netstat -a` command, and in the resulted list check for the tcp sockets listening on `ssh` and `telnet` ports:

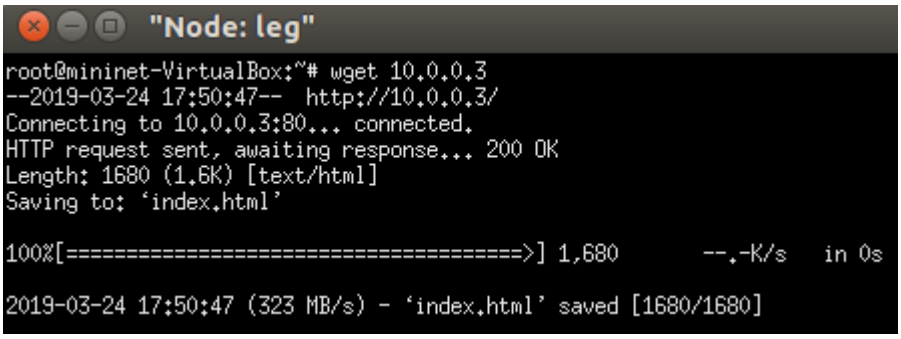


[2] Note that the terminals may cover each other and Wireshark may be opened in a too large window. Drag the top terminals and resize the Wireshark window to reveal the the hidden ones if needed.

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

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

Ensure that you get the proper response from the server as shown below:



If the above checks are passed, your network setup is complete.

`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`".