Packet Sniffing Lab

1 Overview

Packet sniffing and spoofing are two important concepts in network security; they are two major threats in network communication. Being able to understand these two threats is essential for understanding security measures in networking. There are many packet sniffing and spoofing tools, such as `Wireshark`, `Tcpdump`, `Networx`, etc, and some of these tools are widely used by security experts, as well as by attackers.

2 Lab Setup

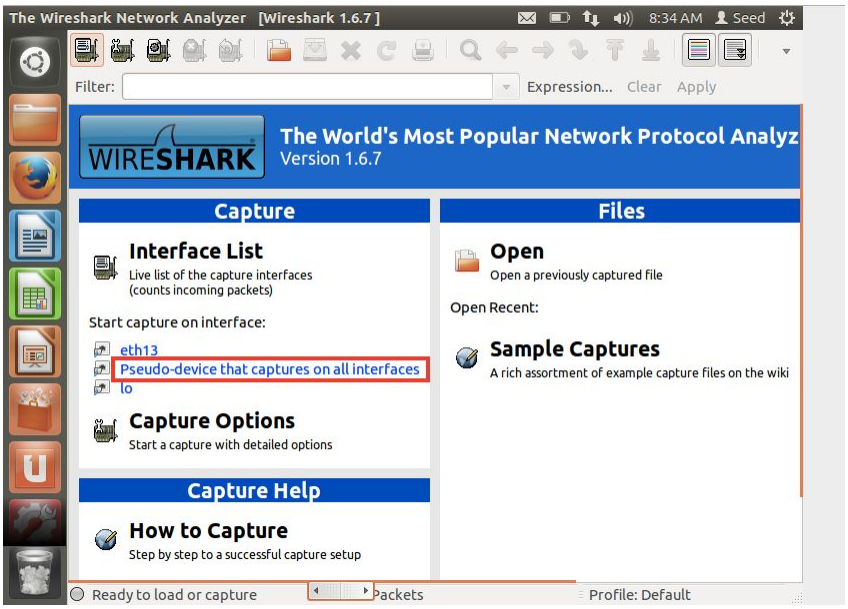
For this lab, we will need to create a VM. First, download the hard disk image of the VM here.

On VirtualBox, select the "Tools" button on the top menu bar, and then select "Import". Choose the VM you downloaded from the link above, and follow default settings to import the VM.

3 Lab Tasks

3.1 Task 1: Using a Packet Sniffing Program g

Start up and log into the VM (password: dees). Open a terminal, and find the "myonyen.txt" file in the home directory. Edit this file, replacing the onyen there with your own. Then, close the VM, and restart it. Open the program on your home directory called Wireshark, and start a live capture:



The program will now be capturing any packets going to or from your network. The packet we are looking for will have the protocol “TCP”. Inspect these TCP packets until you find one with a 32-character string inside of its data - this is your “secret”. Once you find your secret, create a text file with the following format:

```
your_onyen
secret
```

Name your file “secret.txt” for submission.

4 Submission

On Gradescope, please submit your `secret.txt` file. Similar to the A3, this should be a text file with your Onyen on the first line, and the secret you found on the second.