EC605: Computer Engineering Fundamentals — Fall 2016
Lab 7: Networking

Goals

- Gain understanding of network layers and packet types and data
- Use the Wireshark packet analyzer and network information to analyze network trace

Overview

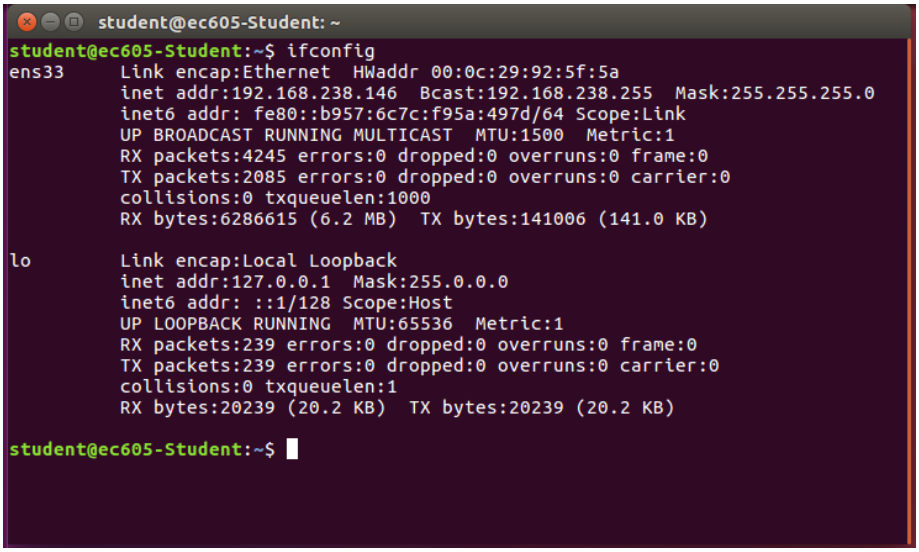
This lab aims to give a better understanding of the different layers that make up network packets. Network packets will be explored via some unique features of the Wireshark open source packet analyzer.

Tasks

Task 1: Introduction to Wireshark

Capture a live trace using Wireshark. Start by opening the Wireshark application on your Ubuntu Virtual Machine. Wireshark can be found by searching for the application through the launcher, or by typing *wireshark* into a terminal session.

In a terminal window, run *ifconfig* to get a list of devices. In the example below, refer to *ens33* as the Ethernet device, and ignore the *lo* device:



```
student@ec605-Student: ~
student@ec605-Student:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:92:5f:5a
          inet addr:192.168.238.146  Bcast:192.168.238.255  Mask:255.255.255.0
          inet6 addr: fe80::b957:6c7c:f95a:497d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2085 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6286615 (6.2 MB)  TX bytes:141006 (141.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:239 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:20239 (20.2 KB)  TX bytes:20239 (20.2 KB)

student@ec605-Student:~$
```

In Wireshark, start a capture on the ethernet device. In another terminal window, run the command *ping www.bu.edu* to get a simple trace. More information about *ifconfig* and *ping* can be found at the bottom of the document in the reference section.

Provide a screenshot of the Wireshark trace and answer the following questions:

1. What kind of protocol is used when performing a ping command?
2. What information is transferred in this protocol?

Task 2: Unsecure Packets

Run the command *wget www.google.com* in a terminal session and get a simple trace of network packets. Find the *HTTP GET* command packet to answer questions below.

Provide a screenshot of the Wireshark trace and answer the following questions:

1. Specify the destination IP address
2. Specify the destination IP MAC address
3. Specify the Internet Protocol version
4. Specify the Source and Destination Port
5. Specify the version of wget
6. Specify the TCP Flags

Task 3: Secure vs. Unsecure Packets

Capture a trace for the secure website *https://www.google.com* and compare the information captured with the previous unsecure packet.

Provide a screenshot of the Wireshark trace. List the packets sent between two machines and the purpose of each packet. (Example: Client Hello).

Task 4: Find an Image File in the Trace

On Blackboard, there is a mystery packet trace, which was taken during a file/image capture, named *ptrace.pcap*. Load this trace into Wireshark and answer the following questions:

1. List out as much information you can about the trace, including:
   Which IP addresses are in the trace?
   Which IP is the host?
   What websites/hostnames are being accessed? (You may find the website *https://www.whois.com/whois* useful)
2. Using Wireshark, get a copy of the image file and include it in the write-up.

Deliverables

- Submit a single file with the traces and answers to all the questions.

Reference

ifconfig – Program used to display all interfaces which are currently available (usage: ifconfig)

ping – Send ECHO_REQUEST to network hosts (usage: ping <hostname>)

wget – Program to download a network file through Linux terminal (usage: wget <web address>)