CSE508: Network Security, Spring 2021

Homework 1: Passive Network Monitoring

Submission deadline: 2/26/2021 11:59pm EDT
Submission through https://blackboard.stonybrook.edu

In this assignment you will get familiar with passive network traffic monitoring and analysis. Tcpdump is probably the most popular and widely used passive network monitoring tool. It is built on top of the Libpcap packet capture library and can capture and display packet headers and payloads either from a network interface or a network trace file. Your task is to analyze a network trace file and answer some questions.

0. Preparation

Download the hw1.pcap trace file from the "Resources" page of Piazza.

Use the following command to read the trace file:

```
tcpdump -n -r hw1.pcap | head
```

-n skips the DNS resolution of IP addresses (faster output)

The output is redirected to 'head' to avoid flooding the console - this is a good strategy while assembling your commands. Alternatively, you can use more(1) to scroll through the output, or you can redirect all output to a text file for further analysis.

1. Network traffic analysis using tcpdump

You can find the answers to all of the following questions using only tcpdump's man page and shell one-liners. You may find the following utilities useful: wc, grep, sed, awk, cut, head, tail, more, sort, uniq. You are free to use any other tools you might want (although the above are more than enough).

1.1 How many packets does the trace contain?

1.2 How many ARP packets and how many UDP packets?

1.3 How many packets were exchanged between 91.189.90.41 and 192.168.0.200?

1.4 Print the unique source IP addresses found in the trace.

1.5 Print the unique 'private network' (according to RFC1918) source IP addresses found in the trace.

1.6 Print the unique destination IP addresses found in the trace.

1.7 What are the top-5 TCP and top-5 UDP destination ports?

1.8 How many TCP packets have the SYN flag set?

1.9 How many TCP connection attempts were made?

1.10 Towards which ports were TCP connection attempts made? How many attempts per port?

1.11 How many HTTP GET requests were made? Print the URLs of all HTTP requests for JPG files.

1.12 When (date and time) was the first and last packet of the trace sent?

1.13 What is the brand of the device that sent most of the packets? What is its IP address?

1.14 Report the distribution of Ethernet packet sizes (how many packets of size X exist in the trace, for all values of X in the trace).

2. What to submit

An plain ASCII text file with the answers to the above questions, along with the command/script/approach used to find them.