Tcpdump Lab: Wired Network Traffic Sniffing

1 Lab Overview

This lab provides students an introduction to a powerful network packet TCP/IP sniffer, *tcpdump*, and its basic usage within a virtualized environment. Students are assumed to be comfortable using a command line interface.

Students will work on four tasks:

- Extract packet arrival time, source IP address, destination IP address and port.
- Extract source MAC address and destination MAC address.
- Get inter-arrival time while capturing packets.
- Draw a chart with inter-arrival time versus the order of sequence number.

This lab uses a virtualized environment, the modified version of Wenliang Du’s SEEDUbuntu. It is available at [http://ccf.cs.uml.edu/](http://ccf.cs.uml.edu/) Before continuing, students should have their network within the visualized environment set up and be ready to get on websites.

Please note that this lab assumes VMWare Workstation is being used. The principles are the same among other virtualization software, but terminology and features may change. Some alternatives to VMWare Workstation include Virtualbox, VMWare Player, and Microsoft Virtual PC.

2 Tcpdump Introduction

Tcpdump, like wireshark and many other sniffers, is usually used to capture packets and analyze network protocols. The network card of a computer drops packets if the packets are not addressed to the system. However in the *promiscuous mode*, the network card forwards all packets reaching the card to the operating system so that tcpdump can capture them, regardless of their (MAC) addresses. Using tcpdump in the promiscuous mode can exam all traffic through the interface, extract sensitive information and thereby sniffer the network. For example, if Computer A and a few other computers are inter-connected by a hub, which broadcasts packets it receives to all connected computers, Computer A in the promiscuous mode will be able to capture all packets going through the hub.

A computer not in the promiscuous mode is able to capture packets addressed to itself and its outgoing packets. Root privilege is required to use tcpdump for sniffer.

3 Tcpdump Installation

Tcpdump can be downloaded from [http://www.tcpdump.org/#latest-release](http://www.tcpdump.org/#latest-release) for the latest version which now is tcpdump-4.3.0, and installed using following commands:
root@seed-desktop:/home/seed# tar xvfz tcpdump-4.3.0.tar.gz
root@seed-desktop:/home/seed# cd tcpdump-4.3.0
root@seed-desktop:/home/seed/tcpdump-4.3.0# ./configure
root@seed-desktop:/home/seed/tcpdump-4.3.0# make
root@seed-desktop:/home/seed/tcpdump-4.3.0# make install

4 Switch Network to Promiscuous Mode

Turn on promiscuous mode with command:

    root@seed-desktop:/home/seed# ifconfig eth7 promisc

then use command:

    root@seed-desktop:/home/seed# ifconfig -v | grep -i promisc

to check if the network is in promiscuous mode or not. Here we use flag -v (or -a) to display information
about all surfaces. If promiscuous mode is on, the output should be like this:

    root@seed-desktop:/home/seed# ifconfig -v | grep -i promisc
    UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1

To turn off promiscuous mode, use command:

    root@seed-desktop:/home/seed# ifconfig eth7 -promisc

Please note that here eth7 is the ethernet name of the system. Students should use the ethernet names of
their own systems to replace eth7 in all commands from this lab instruction.

5 Lab Tasks

Please follow the instructions below and complete the task. Use screen shots to demonstrate the success
of every task. To gain a deep understanding of network protocols as well as the usage of tcpdump,
students must explain what each screen shot means.

5.1 Task 1: Extract Packet Arrival Time, Source IP Address, Destination IP Address and Port.

Use command:

    root@seed-desktop:/home/seed# tcpdump -n

to listen to default ethernet surface and show IP address instead of names, or use command:

    root@seed-desktop:/home/seed# tcpdump -n -i eth7

to filter to a particular ethernet surface to listen to, which here is eth7. The result shows arrival time, source
IP address, destination IP address and port in the form of

    [arrival time][source IP].[port]>[destination IP].[port].

Example:
First use command:
to show the IP address of ethernet on our machine, which here is 192.168.81.128. Then run command:

```
root@seed-desktop:/home/seed# ifconfig -v eth7 | grep 'inet addr'
inet addr:192.168.81.128 Bcast:192.168.81.255 Mask:255.255.255.0
```

Open website http://www.uml.edu/sciences/computer-science/default.html to make some network traffic, meanwhile check out the output of tcpdump:

```
20:35:52.323220 IP 192.168.81.128.56846 > 129.63.176.200.80: Flags [P.], seq 2057279542:2057...
20:35:52.323605 IP 129.63.176.200.80 > 192.168.81.128.56846: Flags [.] , ack 509, win 4096
```

above is part of the result. If flag -n is not used in command, the result will show names instead of IP address, like this:

```
root@seed-desktop:/home/seed# tcpdump
```

Please use tcpdump to extract packet arrival time, source IP address, destination IP address and port information in the student’s environment. Students can browse some website such as yahoo.com to generate network traffic so that tcpdump can capture it. Note: run tcpdump before browsing.

### 5.2 Task 2: Extract Source MAC Address and Destination MAC Address.

Use command:

```bash
root@seed-desktop:/home/seed# tcpdump -e
```

Example: First run command:

```
root@seed-desktop:/home/seed# tcpdump -e -i eth7
```

Then open website http://www.uml.edu/sciences/computer-science/default.html to make some network traffic, meanwhile check out the output of tcpdump:

```
03:07:38.143512 00:50:56:e7:00:28 (oui Unknown) > 192.168.81.2.domain: 9979+ PTR? 200.176.63.129
```

Please use tcpdump to extract packet arrival time, source IP address, destination IP address and port information in the student’s environment. Students can browse some website such as yahoo.com to generate network traffic so that tcpdump can capture it. Note: run tcpdump before browsing.
In the result, source MAC address and destination MAC address is shown in following form:

[source MAC address] > [destination MAC address]

Please use tcpdump to extract source MAC address and destination MAC address information in the student’s environment. Students can browse some website such as yahoo.com to generate network traffic so that tcpdump can capture it. Note: run tcpdump before browsing.

5.3 Task 3: Get Inter-Arrival Time While Capturing Packets.

Command:

root@seed-desktop:/home/seed# tcpdump -ttt

allows you to capture packets and show inter-arrival time instead of arrival time in result.

Example: First run command:

root@seed-desktop:/home/seed# tcpdump -ttt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth7, link-type EN10MB (Ethernet), capture size 65535 bytes

Then open website http://www.uml.edu/sciences/computer-science/default.html The output of tcpdump should be similar to the following:

00:00:00.000000 IP seed-desktop.local.33720 > umlweb.uml.edu.www: Flags [P.], seq 3343073954:334
00:00:00.000371 IP umlweb.uml.edu.www > seed-desktop.local.33720: Flags [.] , ack 50
00:00:00.001412 IP umlweb.uml.edu.www > seed-desktop.local.33720: Flags [P.], seq 1:246,
00:00:00.000018 IP seed-desktop.local.33720 > umlweb.uml.edu.www: Flags [.] , ack 246,

Please use tcpdump to get inter-arrival time while capturing packets information in the student’s environment. Students can browse some website such as yahoo.com to generate network traffic so that tcpdump can capture it. Note: run tcpdump before browsing.

5.4 Task 4: Draw A Chart with Inter-Arrival Time and Order of Sequence Number.

This task can be easily done within following steps:

1. Capture packets which shows inter-arrival time and save the output to a table.

2. Save rows that have the same port number from the previous table to new a new table.

3. Sort rows in the new table according to sequence number.

4. Draw a chart with order of sequence numbers as the horizontal axis and inter-arrival times in microseconds as the vertical axis.

Example: First run command:

root@seed-desktop:/home/seed# tcpdump -ttt > tcprecord.csv
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth7, link-type EN10MB (Ethernet), capture size 65535 bytes
to capture packets, show inter-arrival time in result and save result to file tcprecord.csv. Here the result is saved as a csv file so that it can be opened and manipulated by Microsoft Excel later. Watch a video on youtube to make some network traffic. use Ctrl+c to finish capturing packets and save result. Then run command:
root@seed-desktop:/home/seed# less tcprecord.csv

to view result, which in this case is the following:

00:00:00.000000 IP seed-desktop.local.38498 > iad23s05-in-f7.1e100.net.www: Flags [P.],
00:00:00.000329 IP iad23s05-in-f7.1e100.net.www > seed-desktop.local.38498: Flags [P.]
00:00:00.031206 IP seed-desktop.local.44043 > 192.168.81.2.domain: 16048+ PTR? 7.228.125.74.in
00:00:00.002229 IP 192.168.81.2.domain > seed-desktop.local.44043: 16048 1/0/0 PTR
00:00:00.000188 IP seed-desktop.local.46731 > 192.168.81.2.domain: 13589+ PTR? 128.81.168.192.
00:00:00.003589 IP 192.168.81.2.domain > seed-desktop.local.46731: 13589 NXDomain 0/1/0
00:00:00.137418 IP seed-desktop.local.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 128.81.168.192.
00:00:00.000924 IP seed-desktop.local.mdns > 224.0.0.251.mdns: 0*-[0q] 1/0/0 (Cache
00:00:00.001035 IP iad23s05-in-f7.1e100.net.www > seed-desktop.local.38498: Flags [P.]
00:00:00.0001256 IP seed-desktop.local.57732 > 192.168.81.2.domain: 12594+ PTR? 2.81.168.192.
00:00:00.002379 IP 192.168.81.2.domain > seed-desktop.local.57732: 12594 NXDomain 0/1/0
00:00:00.070966 IP iad23s05-in-f7.1e100.net.www > seed-desktop.local.38498: Flags [P.]
00:00:00.000022 IP seed-desktop.local.38498 > iad23s05-in-f7.1e100.net.www: Flags [P.]
00:00:00.001035 IP iad23s05-in-f7.1e100.net.www > seed-desktop.local.38498: Flags [P.]

The record contains traffic through difficult ports, then let us draw a chart from a random port, like 38498.
Run command:

root@seed-desktop:/home/seed# grep 38498 tcprecord.csv | grep seq > 38498.csv

Please use the introduced commands above and import the data into excel. Draw a curve of inter-arrival time versus packet sequence number. Calculate the mean and standard deviation of the inter-arrival time samples that the student collected.