Lab 3: Background Traffic

Feng Wei

February 17, 2020

1 Introduction

In this lab we are going to learn how to collect background network traffic by *Wireshark*[2]. And use *Tcpreplay*[1] to replay the collected traffic data. Below is the experiment enviorment for this lab.

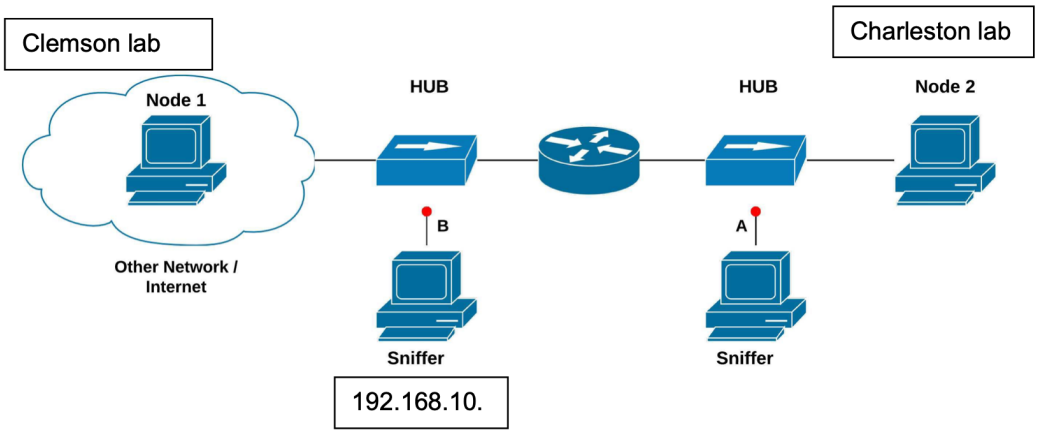


Figure 1: Lab Enviroment

The purpose of this lab is as below:

- Learn how to replay captured network traffics.
- Observe and understand the difference between operational network background traffic and a simulated background traffic.

Necessary Equipment

- One host machine on the Clemson campus to capture campus traffic.
- A pre-configured VM
- Wireshark / Tshark
- Tcpreplay

2 Methods

I followed the instructions in the lab1 to finish the experiment step by step.

2.1 Start VM.

- Copy VM from TA's node to my node. *"scp wei8@192.168.10.10:tmpDDoS_Lab6.ova"*
- vboxmanage *"import Kali_DDoS_Lab6.ova"*
- Change the network configuration of the newly created VM. Generate a new mac address by click the icon to the right of the MAC address input box. Then start the VM
- Log in with *"username: root password: private123"*

2.2 Capture and replay the campus background traffic

Follow the instructions to finish capture and tcpreplay.

- log in to host machine: *"ssh -X wei8@192.168.10.9"*
- Capture 1000 packets: *"tshark -i enp3s1 -c 1000 -w Thousand.pcap -F libpcap"*
- Capture packets arriving in 130 seconds: *"tshark -i enp3s1 -a "duration:130" -w campustraffic1.pcap -F libpcap"*
- Copy scripts from NAS: *"scp wei8@192.168.10.10:/tmp/ECE8930_lab3_spring_2018_scripts.tgz ECE8930_lab3_spring_2018_scripts.tgz"*
- Copy the captured file back to your VM: *scp wei8@192.168.10.x: /campustraffic1.pcap*
- Replay the captured traffic file: *sudo tcpreplay –intf1=lo campustraffic1.pcap*

Compare the real time series versus the generated time series:

- Use the python script to draw time series figures. *"python plot_time_series_example.py"*

3 Results

The experiment results are as below:

3.1 Capture packets

```
[wei8@clemson9 ~]$ tshark -i enp3s1 -a "duration:130" -w  campus_traffic1.pcap -
F libpcap
Capturing on 'enp3s1'
67407
[wei8@clemson9 ~]$
```

Figure 2: Capture Packets

3.2 Copy packets to VM

```
root@cnc:~# scp wei8@192.168.10.9:/home/wei8/campus*  ./
wei8@192.168.10.9's password:
campus_traffic1.pcap                          100%   17MB  17.4MB/s   00:01
root@cnc:~#
```

Figure 3: Copy packets to VM

3.3 Copy python scripts

```
root@cnc:~/plot# tar xzvf ECE8930_lab3_spring_2018_scripts.tgz
plot_time_series_example.py
rand_arr_time.py
read_pcap.py
scapy_example.py
time_series.py
bittwist.sh
python_setup.sh
setup_bittwist.sh
README
root@cnc:~/plot#
```

Figure 4: Plot Scripts

3.4 Replay the campustraffic.pacp

```
root@cnc:~# sudo tcpreplay --intf1=lo campus_traffic1.pcap
Warning in sendpacket.c:sendpacket_open_pf() line 669:
Unsupported physical layer type 0x0304 on lo.  Maybe it works, maybe it wont.  S
ee tickets #123/318
sending out lo
processing file: campus_traffic1.pcap
Actual: 67407 packets (17133446 bytes) sent in 132.79 seconds.          Rated: 1
29026.6 bps, 0.98 Mbps, 507.62 pps
Statistics for network device: lo
        Attempted packets:         67407
        Successful packets:        67407
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
root@cnc:~#
```

Figure 5: Tcprelapy

3.5 Compare the real time series versus the generated time series:

- Capture packets arriving in 130 seconds:

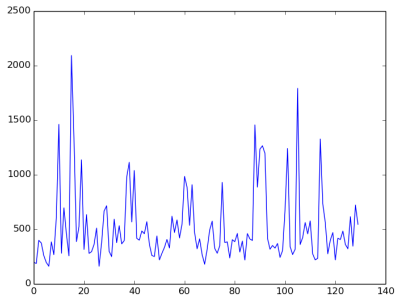


Figure 6: Capture packets arriving in 130 seconds

- Capture 1000 packets:

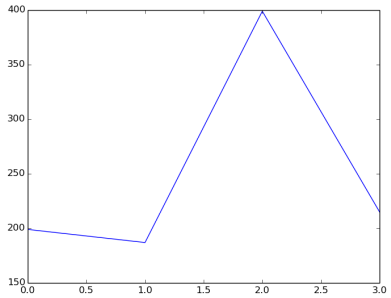


Figure 7: Capture 1000 packets

- Replay the traffic packets:

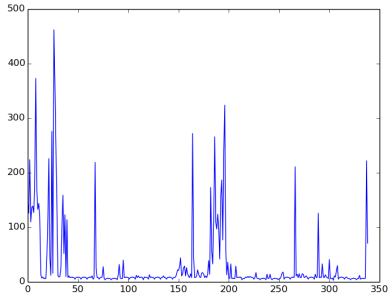


Figure 8: Replay the traffic packets

- Simulate background traffics:

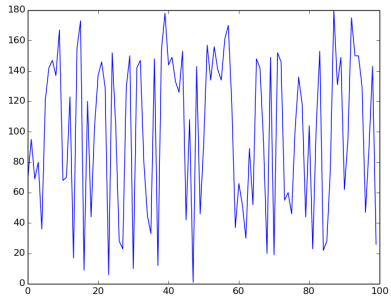
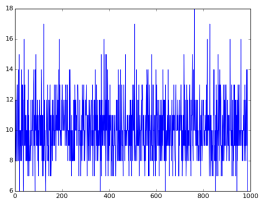
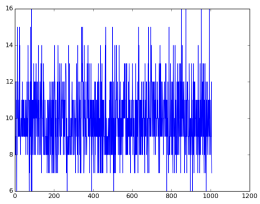


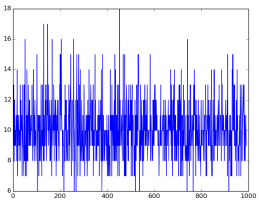
Figure 9: Simulation with option 6



(a) Simulate 0

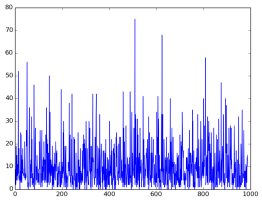


(b) Simulate 1

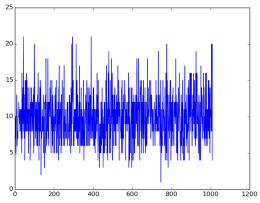


(c) Simulate 2

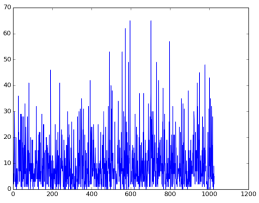
Figure 10: Simulation 0 1 2



(a) Simulate 3



(b) Simulate 4



(c) Simulate 5

Figure 11: Simulation 3 4 5

4 Question Answers

- Plot the background traffic datasets generated/used in three scenarios where x-axis shows time, and the y-axis shows the number of packets received. Compare the figures and discuss their difference.
  Answer: As show in the above figs. To capture 1000 packets it only takes 3 seconds, so it is hard to get any useful information from that fig. We can only see the packets/second rate is nearly 300. For the replay and the capture 130 seconds scenario, we can see the packets rates are different. For the replay scenario the highest is about 500, but for the capture scenario the highest rate is about 2000 and the average rate is about 500.

- Network background traffic statistic generation script (plot_time_series_example.py) generates datasets using different probability distribution functions (PDF). Compare datasets generated using different PDFs. Discuss the difference between datasets and the data-set converted from operational network data.
  Answer: I checked the source codes and the distributions functions corresponding to the options are as below: 0 Random, 1 Uniform, 2 Tnorm, 3 Poisson, 4 Exponential, 5 Poisson with random expectation of interval, 6 Randomly pick one of above functions. So the differences between them are all the mathematics features of each distribution functions. When compared with the real traffics I think the Poisson and Poisson with random interval look more real than others.

- What kind of traffic did you run between hosts in the second scenario (Replay a pcap file with tcpreplay). Justify why you think it can represent operational network traffic.
  Answer: I used *ssh and scp* commands during the scenario. Those two commands are secure and normal, so I think they can represent operational network traffics.

- You can replay and forward captured pcap files on a link in a controlled network environment to use as background traffic. If you perform a DDoS attack on this link, you can observe the effects of the DDoS attack without jeopardizing the operational network. However, some of the effects

cannot be observed with replayed/forwarded background traffic. List some of these effects and explain the reason why they can not be observed.
Answer: Although we can simulate the DDoS attacks on a controlled network with replaying the pcap traffics. But it's hard to simulate the real actions of the victims host, sometimes the DDoS attacks will totally shutdown the victim hosts that means all those packets from the victim host will not be sent after the attacks.

- Number of packets received by a node on the network is one of the popular metric used in DDoS detection applications. In this assignment, we focused on packet count statistic. Discuss what other metrics that can be used for DDoS detection.
Answer: Metrics can be used to detect DDoS attacks: *packets size*, *host numbers*, *flow information*, *flags* etc.

5 Discussion

- We can try to use the advanced features of *tcpreplay*[1] to replay traffics.

References

[1] tcpreplay. *https://tcpreplay.appneta.com/*.
[2] Wireshark. *https://www.wireshark.org/*.