Sample Report

NCTU CN2018 Lab. 1 – Packet Manipulation via Scapy

Student name: Yung-Sheng Lu   Student ID: XXXXXXX   Department: CS

Part A. Questions

1. What is your command to filter the packet with customized header on Wireshark?
2. Show the screenshot of filtering the packet with customized header.
3. What is your command to filter the packet with “secret” payload on Wireshark?
4. Show the screenshot of filtering the packet with “secret” payload.
5. Show the result after decoding the “secret” payload.

Part B. Description

Task 1 – Environment setup

- Configure Dockerfile
  - How to configure Dockerfile?
    https://docs.docker.com/engine/reference/builder/
  - First, download base image from yungshenglu/ubuntu-env:16.04

    ```
    # Download base image from yungshenglu/ubuntu-env:16.04
    FROM yungshenglu/ubuntu-env:16.04
    ```
  - Second, update all software repository

    ```
    # Update software repository
    FROM apt-get update
    ```
  - …
- Build the container with Dockerfile
  - …
- …

Task 7 – Load PCAP via Wireshark

- Download the code from GitHub

  ```
  $ git clone https://github.com/nctucn/lab1-yungshenglu.git
  ```
- Open the PCAP file using Wireshark
  (Screenshots)
- …

Task 8 – Filter the target packet

- Filter the packets of our defined protocol
  - Filter rule: ……
  - (Screenshot)
- Filter the packets with the “secret” bits
  - Filter rule: ……
  - (Screenshots)
- What is my secret key? How to find it?

Task 9 – Decode the secret key

- Input the secret key into ./src/decoder.py on local machine
  - My result is?