# COMP3355 Cyber Security

# Lab 2

**(Due on Nov. 14, 23:55)**

## Disclaimer

"All lecture notes, handouts and discussions relating to technological means of hacking, virus attacks, denial of services or any other means of attacking a computer system are for the sole educational purpose of teaching COMP3355 (Cyber Security). Those are not intended to be adopted or applied to launch any attack on or to cause any damage to any computer system, and do not in any way encourage anyone to engage in such acts. By taking this course, you also agree not to adopt or apply any of the technological means discussed or otherwise disclosed in this course to engage in such acts."

## Overview

**Wireshark** is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. It is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets.

**Nmap (Network Mapper)** is a security scanner used to discover hosts and services on a computer network. It sends specially crafted packets to the target host(s) and then analyses the responses. It provides a number of features for probing computer networks, including host discovery and service and operating-system detection.

## 1. Wireshark

**(a)** In this section, you are going to use Wireshark to capture packets under an insecurity transfer protocol.

Open Wireshark.

Select **eth0** at the Welcome page. (according to ipconfig output)

Click on the  button on the top left corner to start package capturing.

Open Browser. Go to the webpage http://www.techpanda.org/.

Type in email **admin@google.com** and password **Password2010**, then submit.

Several packets will be captured. Click on the  button on the top left corner to stop package capturing.

Q1. (10%) What kind of protocols are the website using?

Q2. (10%) What web server is the website using?

Q3. (10%) What is the length of the packet (in bytes) containing the login information (i.e. email and password)?

Q4. (5%) What kind of request method is used in the packet containing the login information (i.e. email and password)?

**(b)** In this section, you are going to use Wireshark to capture packets under a security transfer protocol.

Open Wireshark.

Select **eth0** at the Welcome page. (according to ipconfig output)

(1) Click on the  button on the top left corner to start package capturing.

Open Browser. Go to the webpage https://aavtrain.com.

Type in email **admin@google.com** and password **Password2010**, then submit.

Several packets will be captured. Click on the  button on the top left corner to stop package capturing.

Q5. (10%) Can you display the raw html? Why or why not?

Q6. (10%) Which kind of protocol can protect your login information? Please explain how it can protect login information compared with the original (vulnerable) protocol.

(2) Click on the  button on the top left corner to start package capturing.

Open the terminal and ping google.com.

Several packets will be captured. Click on the  button on the top left corner to stop package capturing.

Q7. (10%) Can you find the ping record? Screenshot your results.

## 2. Nmap

**(a)** Ping Scan. (Which hosts are up now?)

Use ipconfig/ifconfig to find out your ip address, then do a ping sweep over the 256 ip addresses within the range your ip is located. (i.e., if your ip is 10.68.35.180, perform the ping sweep over 10.68.35.* using wild cards.)

Q8. (5%) What hosts are up now? Screenshot your results.

**(b)** Port Scan. (Any vulnerable services available?)

(1) TCP Scan.

Q9. (5%) Perform TCP scan to find out port conditions for google.com and hku.hk. Screenshot what you found.

(2) UDP Scan.

Q10. (5%) Perform UDP scan to find out port conditions for google.com and hku.hk. Screenshot what you found.

**(c)** OS Fingerprinting. (Which OS is running on the host?)

Q11. (5%) Predict the OS for google.com & hku.hk. Screenshot what you get.

Q12. (5%) Select whatever ip address that you are interested and predict the OS of it. Screenshot what you get.

**(d)** CVE Detection using Nmap

Q13. (5%) Scan your localhost and see if there are any vulnerability detected and any CVE items raised up. Screenshot your result.

Q14. (5%) Perform CVE Detection for google.com and hku.hk and see what you could find. Screenshot your result.