Green University of Bangladesh
Department of Computer Science and Engineering (CSE)

Faculty of Sciences and Engineering
Semester: (Spring, Year: 2022), B.Sc. in CSE (Day/Eve)

Course Title: Computer Networking
Course Code: 311 Section:EA

Topic Name: Network Security

Student Details

Name		ID
1.	Mohtamim Islam Nayeem	193015047

Submission Date : 10-05-2022
Course Teacher's Name : Mohammad Ehsan Shahmi Chowdhury

[For Teachers use only: Don't Write Anything inside this box]

Assignment Status

Marks: ………………………………… Signature: ....

Comments: .... Date: ....

GENERAL INSTRUCTIONS

1. Introduction

   This project will introduce you to common network protocols, to network packet trace analysis, and to the basics of network penetration testing.

2. Motivation

   - Gain exposure to core network protocols and concepts.
   - Learn to apply manual and automated traffic analysis to detect security problems.
   - Understand offensive techniques used to attack local network traffic.
   - Practice network penetration testing.

3. Topic in details

   - This project asks you to perform attacks, with our permission, against a target network that we are providing for this purpose. Attempting the same kinds of attacks against other networks without authorization is prohibited by law and university policies and may result in fines, expulsion, and jail time. You must not attack any network without authorization! Per course policy, you are required to respect the privacy and property rights of others at all times, or else you will fail the course. See “Right, Rules, and Responsibilities” on the Princeton University website for more details.
   - Security analysts and attackers both frequently study network traffic to search for vulnerabilities and to characterize network behavior. In this section, you will examine a network packet trace (commonly called a “pcap”) that we recorded on a sample network we set up for this assignment. You will search for specific vulnerable behaviors and extract relevant details using the Wireshark network analyzer, which is available at https://www.wireshark.org. Download the pcap from https://goo.gl/GorPRU using the NetID of the user in your group with the highest lexical rank, and examine it using Wireshark. Familiarize yourself with Wireshark’s features. and try exploring the various options for filtering and for reconstructing data streams.
   - you manually explored a network trace. Now, you will programmatically analyze a pcap file to detect suspicious behavior. Specifically, you will be attempting to identify port scanning. Port scanning is a technique used to find network hosts that have services listening on one or more target ports. It can be used offensively to locate vulnerable systems in preparation for an attack, or defensively for research or network administration. In one kind of port scan technique, known as a SYN scan, the scanner sends TCP SYN packets (the first packet in the TCP handshake) and watches for hosts that respond with SYN+ACK packets (the second handshake step). Since most hosts are not prepared to receive connections on any given port, typically, during a port scan, a much smaller number of hosts will respond with SYN+ACK packets than originally received SYN packets. By observing this effect in a packet trace, you can identify source addresses that may be attempting a port scan. Your task is to develop a Python program that analyzes a pcap file in order to detect possible SYN scans. To do this, you will use dpkt, a library for packet manipulation and dissection. It is available in most package repositories. You can find more information about dpkt at https://github.com/kbandla/dpkt and view documentation by running pydoc dpkt, pydoc dpkt.ip, etc.; there’s also a helpful tutorial here: https://jon.oberheide.org/blog/2008/10/15/dpkt-tutorial-2-parsing-a-pcapfile/.

Your program will take the path of the pcap file to be analyzed as a command-line parameter, e.g.: python2.7 detector.py capture.pcap The output should be the set of IP addresses (one per line) that sent more than 3 times as many SYN packets as the number of SYN+ACK packets they received. Your program should silently ignore packets that are malformed or that are not using Ethernet, IP, and TCP. A large sample pcap file captured from a real network can be downloaded at ftp://ftp.bro-ids.org/ enterprise-traces/hdr-traces05/lbl-internal.20041004-1305.port002.dump.anon. (You can examine the packets manually by opening this file in Wireshark.) For this input, your program's output should be these lines, in any order: 128.3.23.2 128.3.23.5 128.3.23.117 128.3.23.158 128.3.164.248 128.3.164.249

- The fictional company SketchyCorp has contracted with COS 432 to provide penetration testing services to it in exchange for free hugs and awesome memes. Each project team will conduct a thorough penetration test of the company's networks and exposed systems. Before you begin This part of the project spec serves as a Pen Test Engagement Agreement, covering the goals, scope, compensation, and authorization to begin the penetration test. You must agree to these terms in writing (as explained below) before you begin your work. Contact information General questions should be posted to Piazza as private unless they are related to logistics only. We encourage giving each other help, but do not post spoilers (hints that give away the "Aha!" moments) or detailed instructions. Questions about potential rule-breaking should be emailed to cos432-a5@lists.cs.princeton.edu. Introduction SketchyCorp recently set up a remote office on the 3rd floor of the Sherrerd Hall building for its employees to work in. SketchyCorp is concerned that its remote office may be more vulnerable than its headquarters since it uses a wireless network to provide access to its remote employees. From there, they can access the SketchyCorp server, which allows company employees to log in and gain access to company proprietary information. It just so happens that there is an employee at SketchyCorp with your NetID. This employee's password will provided to you. Your objective is to test the security of SketchyCorp's networks and systems. In this engagement you will be authorized to break in to SketchyCorp's systems and explore any vulnerabilities you find, subject to the Rules of Engagement below. As in a real-world penetration test, you will be expected to use your ingenuity and technical skills to discover clues and techniques for meeting your objectives.

4. Special critical analysis of the topic –
   - A description of any findings you may have made. Specifically, include details about the following: • Hostnames of any machines you gain access to during the pen test. • Any encryption keys for networks you gain access to. • Any credentials you are able to obtain (not including your own). • Other company secrets you accessed (briefly list each one). • [Extra credit] What is Bob hiding? (If you encounter a file or folder with "bonus" in its name, it pertains entirely to this optional question.)
5. Conclusion

   - A good network security system helps business reduce the risk of falling victim of data theft and sabotage. Network security helps protect your workstations from harmful spyware. It also ensures that shared data is kept secure.

-

6. References

- https://www.cs.princeton.edu/