CS-628A: Computer Systems Security

10th November, 2019

Jeevan Kumar

Nirjhar Roy

ASSIGNMENT 5

Please see piazza for due dates

This homework is to be done individually. You can discuss homework problems with your friends, but the write up be your own.

The goal of this homework is to get you familiar with some commonly-used tools in network security, such packet analysis tools and libraries. This homework is based in part on Stanford CS155 taught by Dan Boneh, UW-Madison CS642 taught by Thomas Ristenpar and IISC E0256 taught by Vinod Ganapathy.

The following deliverables are expected:

A txt file containing solutions(Write the answers in the given file "answers.txt" and NOT IIN ANY OTHER FILE).

You will be working with some tools and libraries commonly used by network security analysis.

Network Packet Analysis

As part of this homework, you are given packet traces in pcap format. For this question, you will learn how to read and analyze such packet capture traces. You are free to use any open-source tool for this analysis, such as tcpdump, tcpdump produces its output in textual format, and has a number of arguments that you can use to configure how the output looks. Use man tcpdump to learn about the arguments that tcpdump uses.

You are not bound to use tcpdump for this question. A number of other packet scanning tools, such as WireShark, or other GUI-based interfaces for packet trace analysis. You are free to download, install and use such tools.

Part (a) Trace 1: HTTP trace.

1. Give three websites visited from source IP address "192.168.0.100"(websites that begin with "www" and end with ".com" and NOT any other website(s)).
2. Give three search queries made from source IP address "192.168.0.100".

Part (b) Trace 2: FTP trace. FTP is the file transport protocol. There is a lot of information about it on the Internet, which you should read up to answer the questions below.

1. What is the user name and password used to connect to the FTP server?
2. Explain the difference between a passive FTP connection and an active FTP connection.
3. Give the packet number ranges across which there were active connection(s).
4. Give the packet number ranges across which there were passive connection(s).
5. List the names of any files that were downloaded.

Part (c) Trace 3: Traceroute. Traceroute is a tool used to determine the route between two IP addresses.

1. Identify the source IP address that issued a traceroute command.
2. Identify the destination IP address of the traceroute command.
3. List the IP addresses on the route between the source and destination.

Part (d) Trace 4: POP. The POP protocol is used for Email.

1. What is the POP username and password?
2. How many emails are in the user's mailbox?
3. Give the contents of from, to, subject, and date for each email.

(2 points for each of the 13 sub-questions, and 4 points for learning to use a packet trace analysis tool such as tcpdump).

See http://yuba.stanford.edu/~casado/pcap/section1.html and http://www.tcpdump.org/pcap.html for good overviews of the libpcap library.