ECEN 5013/CSCI 7000-0009

Assignment 2: Analyzing Network traces

Due: Wed 9/21, 11:59pm. 25% off for each day late.

Credit: Original traces and problems from Dan Boneh (Stanford).

We've seen various ways in which a malicious party can get access to the communication between two entities – sometimes maliciously (e.g., through techniques such as spoofing), sometimes through broadcast channels (e.g., open Wi-Fi networks), and sometimes they are a network provider and have full access to the traffic legitimately (e.g., a company can exam traffic of its employees).

Here we'll explore some of the information you can get from this. I would suggest using Wireshark (http://www.wireshark.org/) and learn about Wireshark's filtering, but you are welcome to use any tool. And to answer the questions, you may need to look up the details of a given protocol. Please let me know what tool you used and the answers to the following questions. On the website is a tarball with four packet traces in PCAP format. Each trace is associated with one set of questions.

Trace 1: HTTP

1. Give three websites visited from source IP address 128.12.173.14
2. Give three search queries made from source IP address 128.12.173.14
3. Determine the organization that 128.12.173.14 is associated to

Trace 2: FTP

1. What is the user name and password 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 connections
4. Give the packet number ranges across which there were passive connections
5. List any files that were downloaded

Trace 3: Traceroute

1. Identify the source IP address that issued a traceroute command
2. Identify the destination of the traceroute command
3. List the IP addresses on the route between the source and destination
4. Determine the organizations associated with all the IP addresses along the route

Trace 4: POP

1. What is the POP username and password
2. How many emails are in the users mailbox
3. Give the contents of from, two, subject, and date for each email