CIS6395: Homework 2 (Wireshark)
University of Central Florida
Cliff C. Zou
Assigned: Sept. 21st, 2016;   Due: midnight Sept. 30th, 2016

This homework is modified from the programming project 2 in Dr. Paxson/Wagner's course "CS161: computer security" in Spring 2010:
http://www-inst.eecs.berkeley.edu/~cs161/sp10/projects/proj2.pdf

I have put a trace file on Webcourse in this homework submission page: HW-2.trace. The packets within each trace are stored in the libpcap file format, which can be opened and read by Wireshark.

Questions

1. (10 pts.) HTTP Sessions
For this problem, find all web servers that were visited in the trace (that is, contacted via HTTP). Submit a list of their IP addresses as your answer, then provide the total number of webservers in the list. (Please note that you should not try to identify HTTPS traffic)

2. (15 pts.) Directory Traversal
One simple way people attempt to exploit a web server is by making requests for files outside the normal directories it serves using pathnames with sequences like "../../../". (Of course, a reasonably well-implemented web server will not fall for tricks like this.) Find a host that appears to be attempting this type of attack and submit its IP address.

3. (15 pts.) Password Guessing
If you've ever looked through the logs of an SSH server, you've likely seen attempts to login through brute force guessing of usernames and passwords. Of course, the same attack is possible for any type of protocol with password authentication. There is one host that attempted such an attack against a password protected FTP server. Find that host and submit the IP address of the attacker. Also answer: how many times the attacker has tried different passwords in login attempts in your trace?

4. (20 pts.) Unencrypted Usernames and Passwords
Next, find an unencrypted username and password. Note that we are interested in a real username and password, so failed login attempts don't count. Examples of protocols that can send usernames and passwords without encryption are Telnet, FTP in this project's traces. List all the usernames and passwords (and their protocols) as your answer.

5. (15 pts.) Service Versions
Finding hosts running specific versions of servers is an important step in exploiting them; in general, older versions will have more vulnerabilities. For this problem, find the host running the oldest version of Apache. (Apache is the most widely used web server on the Internet.) Don't count "Apache-Coyote" as "Apache"; also, ignore any servers that don't specify their version. Submit that host's IP address.

6. (15 pts.) DNS and Source Port Randomization

Most clients now select a random UDP source port when making DNS queries to help prevent the Kaminsky attack. For this problem, look for clients which do not use a random source port in your trace file. There are exactly two such DNS resolvers (using DNS UDP port 53). As your answer to this question, submit the IP addresses of the two DNS resolvers that use the same source port for all the DNS queries they make (and make more than 1 query).

7. (10 pts.) Ping Scanning
'Ping' program can be used to find out whether a remoter computer is online or not, or be used by attackers to do initial probing before real attacks. Identify the hosts that are running Ping in the traffic trace. Submit the list of IP addresses of the client computers that initiate Ping and the list of IP addresses of their targets.

Delivery

You need to submit a report file. Besides the direct answers to the above 7 questions, you MUST also explain in each question how you derive that solution, such as: what the filter term you have used? What program or command lines you have used to analyze packet text file you saved?