COS 432 Assignment 4
Network Security

Please fill in your answers to each of the questions below, and submit this file via Gradescope. Save this file often and check that your answers are persisting; some PDF viewers do not save form data. **After the submission, please double-check that your answers are properly displayed on the Gradescope submission, and that all of the group members are included in the submission.** Should you need additional space to write your answer for a question, feel free to use the additional space on the last page.

Part 1. Exploring Network Traces

1. Multiple devices are connected to the local network. What are their MAC and IP addresses? Who manufactured these devices?

2. What type of network does this appear to be (e.g., a large corporation, an ISP backbone, etc.)? Point to evidence from the trace that supports this.

3. One of the clients connects to an FTP server during the trace

   (a) What is the DNS hostname of the server it connects to?

   (b) Is the connection using Active or Passive FTP?

   (c) Based on the packet capture, what is one major vulnerability of the FTP protocol?

   (d) Name at least two network protocols that can be used in place of FTP to provide secure file transfer.

4. The trace shows that at least one of the clients makes HTTPS connections to sites other than Facebook. Pick one of these connections and answer the following:

   (a) What is the domain name of the site the client is connecting to?

   (b) Is there any way the HTTPS server can protect against the leak of information in (a)?

   (c) During the TLS handshake, the client provides a list of supported cipher suites. List the first three cipher suites and name the crypto algorithms used in each.

   (d) Are any of these cipher suites worrisome from a security or privacy perspective? Why?

   (e) What cipher suite does the server choose for the connection?

5. One of the clients makes a number of requests to Facebook.

   (a) Even though logins are processed over HTTPS, what is insecure about the way the browser is authenticated to Facebook?

   (b) How would this let an attacker impersonate the user on Facebook?

   (c) How can users protect themselves against this type of attack?

   (d) What did the user do while on the Facebook site?

Part 2. Anomaly Detection

Please have **one** member of your group submit your detector script to the COS Dropbox. Enter the NetID of this member below.

Part 3. Penetration Testing

1. How many possible Wi-Fi passwords are there that fulfills the password format?

2. What is that actual Wi-Fi password used? How did you obtain that password?

3. There are three machines in the network, namely the employee, the firewall, and the mainframe.

   (a) What are their IP addresses, respectively? (If a machine has multiple interfaces, report all IP addresses.) How did you get these addresses?

   (b) What services are currently running on these machines respectively? On which port is each service running? How did you obtain this information?

4. There are unencrypted and encrypted conversations between Alice and Bob.

   (a) What does the unencrypted conversation say? Please paste it here and briefly explain how you obtained the contents.

   (b) *(Extra Credit)* Can you decrypt the encrypted messages? If so, what does the plaintext say? Describe how you determined the plaintext contents of the encrypted messages.

5. SketchyCorp is setting up a remote office. Where is it going to be located? How did you obtain this information?

6. List all the clients of SketchyCorp. Briefly explain how you gained access to this information.

Additional Space