

Fundamentals of Information Technology Security  
CSEC 1110  
Lab 06

- Contact your instructor with your questions about the assignments.
- The student must insure all the answers are free from any malware.
- The student must ensure all answers are legal as defined by the class syllabus.
- All parts of your answers must be neat and easy to read.
- Paragraphs are at least four properly constructed English sentences.
- Embedding documents within documents does not work with the D2L Bright Space assignments.
- Plagiarism will not be tolerated.
- Unless noted, all lab sections must be done as unprivileged login.
- Labeling answers is highly recommended.

## 2. Lab06: Secret and Public Keys

- 2.1. Upload each answer to the D2L Bright Space Assignment section 6.1 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
  - 2.1.1. Provide a comprehensive list of digital certificates considered authoritative by your operating system or a browser.
  - 2.1.2. Explain how to add and delete a digital certificate to the list you provided. Remember to cite any sources of information you use. Each step, mouse click, and answer must be in a separate sentence or bullet point.
  - 2.1.3. Using at least one paragraph, explain the impact of adding or removing a digital certificate. Remember to cite any sources of information you use.
  - 2.1.4. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.
- 2.2. Upload each answer to the D2L Bright Space Assignment section 6.2 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
  - 2.2.1. Provide evidence of successfully concealing a message using steganography on host 1. Identify the host 1.
  - 2.2.2. Provide evidence of successfully extracting/viewing the steganography concealed message on a different host 2. Identify the host 2.
  - 2.2.3. Provide directions about how to use steganography to hide a message. Each step, mouse click, and answer must be in a separate sentence or bullet point.
  - 2.2.4. Provide directions about how to use steganography to unhide a message. Each step, mouse click, and answer must be in a separate sentence or bullet point.
  - 2.2.5. In paragraph, explain how steganography could be used to enhance security.
  - 2.2.6. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.
- 2.3. Upload each answer to the D2L Bright Space Assignment section 6.3 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
  - 2.3.1. Download a copy of the class permission form.
  - 2.3.2. Complete the form requesting permission to collect network traffic on the class network.
    - 2.3.2.1. Please do not send the permission form as an attachment.
  - 2.3.3. Submit a copy of the completed class permission form with your instructor's **verified** correct digital signature.
  - 2.3.4. Provide two forms of identification for your network at home.
  - 2.3.5. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.
- 2.4. Upload each answer to the D2L Bright Space Assignment section 6.4 before the due date found in the csec1110a.pdf document. Submit a Portable Document Format (PDF) or word processing file containing the following. Put your answer in a single document.
  - 2.4.1. Identify a current security breach that could happen to a system you control.
  - 2.4.2. Provide the following information about the identified security breach.
    - 2.4.2.1. How do you know the security breach has happened?
    - 2.4.2.2. How can you tell when the breach happened and how long has the breach occurred?

- 2.4.2.3. What are the log file entries that support the investigation?
  - 2.4.2.4. What is the maximum damage the security breach can cause?
  - 2.4.2.5. How quickly can the breach cause maximum damage?
  - 2.4.2.6. How quickly will you notice and respond appropriately?
  - 2.4.2.7. What are at least two things that could go wrong as a defender?
- 2.4.3. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.