Fundamentals of Information Technology Security
CSEC 1110
Lab 03

- Contact your instructor with your questions about the assignments.
- The student must insure all the answers are free from any malware.
- The student must insure 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.

Lab 03: Sharing Files

3.1. Upload you answer to the D2L Bright Space Assignment section 3.1 before the due date found in the csec1110a.pdf document. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. The text must be readable by the instructor. Submit a Portable Document Format (PDF) or word processing file containing your answers.

3.1.1. Provide the complete text or XML log entry from a system you control showing "Systems and Data Change Report" issue. Windows systems will report event id 4741, 4742, or equivalent. Please label your answer. [8 points]

3.1.2. Provide the source code appropriate to the host with the following attributes. [8 points]

3.1.2.1. The code purpose is clearly identified.

3.1.2.2. All sources of help are identified. This includes people, web sites, and AI program(s).

3.1.2.3. The author name and date

3.1.2.4. The code will extract the log entries for this section into a csv or similar type of file.

3.1.3. Provide the output of the source code showing at least five entries. [8 points]

3.1.4. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used. [1 point]

3.2. Upload you answer to the D2L Bright Space Assignment section 3.2 before the due date found in the csec1110a.pdf document. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. The text must be readable by the instructor. Submit a Portable Document Format (PDF) or word processing file containing your answers.

3.2.1. Provide the complete text or XML log entry from a system you control showing "Network Activity Report" issue. Windows systems will report event id 5031, 5140, 5142, or equivalent. Please label your answer. [8 points]

3.2.2. Provide the source code appropriate to the host with the following attributes. [8 points]

3.2.2.1. The code purpose is clearly identified.

3.2.2.2. All sources of help are identified. This includes people, web sites, and AI program(s).

3.2.2.3. The author name and date

3.2.2.4. The code will extract the log entries for this section into a csv or similar type of file.

3.2.3. Provide the output of the source code showing at least five entries. [8 points]

3.2.4. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used. [1 point]

3.3. Upload each section answer to D2L Bright Space Assignment section 3.3 before the due date found in the csec1110a.pdf document. This requires two hosts under your full control. The text must be readable by the instructor. Submit a Portable Document Format (PDF) or word processing file containing your answers.

3.3.1. Provide the complete text or XML log entry from a system you control showing "Resource Access Report" issue. Windows systems will report event id 4663, 4819, or equivalent. Please label your answer. [8 points]

3.3.2. Provide the source code appropriate to the host with the following attributes. [8 points]

3.3.2.1. The code purpose is clearly identified.

3.3.2.2. All sources of help are identified. This includes people, web sites, and AI program(s).

3.3.2.3. The author name and date

3.3.2.4. The code will extract the log entries for this section into a csv or similar type of file.

3.3.3. Provide the output of the source code showing at least five entries. [8 points]

3.3.4. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used. [1 point]

3.4. Upload each section answer D2L Bright Space Assignment section 3.4 before the due date found in the csec1110a.pdf document. The text must be readable by the instructor. Submit a Portable Document Format (PDF) or word processing file containing your answers.

3.4.1. Provide the complete text or XML log entry from a system you control showing "Malware Activity Report" issue. Please label your answer. [8 points]

3.4.2. Provide the source code appropriate to the host with the following attributes. [8 points]

3.4.2.1. The code purpose is clearly identified.

3.4.2.2. All sources of help are identified. This includes people, web sites, and AI program(s).

3.4.2.3. The author name and date

3.4.2.4. The code will extract the log entries for this section into a csv or similar type of file.

3.4.3. Provide the output of the source code showing at least five entries. [8 points]

3.4.4. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used. [1 point]