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 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.

3. Lab 03: Sharing Files

3.1. Upload each answer to the D2L Bright Space Assignment section 3.1 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.

3.1.1. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. 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.

3.1.2. In at least one sentence, explain how the log entry fits with the requested log report category.

3.1.3. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. Provide the complete text or XML log entry from a system you control showing "Systems and Data Change Report" issue for a Linux system.

3.1.4. In at least one sentence, explain how the log entry fits with the requested log report category.

3.1.5. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.

3.2. Upload each answer to the D2L Bright Space Assignment section 3.2 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.

3.2.1. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. 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.

3.2.2. In at least one sentence, explain how the log entry fits with the requested log report category.

3.2.3. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. Provide the complete text or XML log entry from a system you control showing "Network Activity Report" issue for a Linux system.

3.2.4. In at least one sentence, explain how the log entry fits with the requested log report category.

3.2.5. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.

3.3. Upload each answer to the D2L Bright Space Assignment section 3.3 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.

3.3.1. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. 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.

3.3.2. In at least one sentence, explain how the log entry fits with the requested log report category.

3.3.3. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. Provide the complete text or XML log entry from a system you control showing "Resource Access Report" issue for a Linux system.

3.3.4. In at least one sentence, explain how the log entry fits with the requested log report category.

3.3.5. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.

3.4. Upload each answer to the D2L Bright Space Assignment section 3.4 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.

3.4.1. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. Provide the complete text or XML log entry from a system you control showing "Malware Activity Report" issue for a

Windows system

3.4.2. In at least one sentence, explain how the log entry fits with the requested log report category.
3.4.3. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site. Provide the complete text or XML log entry from a system you control showing "Malware Activity Report" issue for a Linux system.
3.4.4. In at least one sentence, explain how the log entry fits with the requested log report category.
3.4.5. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used.