

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.

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.
 - 3.1.2. In a paragraph, explain how examining this type of entry helps you find potential security breaches.
- 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.
 - 3.2.2. In a paragraph, explain how examining this type of entry helps you find potential security breaches.
- 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.
 - 3.3.2. In a paragraph, explain how examining this type of entry helps you find potential security breaches.
- 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.
 - 3.4.2. In a paragraph, explain how examining this type of entry helps you find potential security breaches.