

Fundamentals of Information Technology Security  
CSEC 1110  
Lab 02

- 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 02: Controlling Files**

- 2.1. Each part is worth four points for a maximum of twenty-five points. Upload you answer to the D2L Bright Space Assignment section 2.1 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.
  - 2.1.1. Provide the hostname and operating system version information for host1. This must be a Debian Linux VM installation.
  - 2.1.2. Provide the IPv4 address, IPv6 address, and MAC address.
  - 2.1.3. Provide evidence the operating system is current with updates.
  - 2.1.4. Provide a complete list of all install applications.
  - 2.1.5. Provide a complete CIS report on the listed system.
  - 2.1.6. Identify ten items from the report you changed based on the report.
  
- 2.2. Each part is worth four points for a maximum of twenty-five points. Upload you answer to the D2L Bright Space Assignment section 2.2 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.
  - 2.2.1. Provide the hostname and operating system version information for host2. This must be a Debian Linux VM installation.
  - 2.2.2. Provide the IPv4 address, IPv6 address, and MAC address.
  - 2.2.3. Provide evidence the operating system is current with updates.
  - 2.2.4. Provide a complete list of all install applications.
  - 2.2.5. Provide a complete CIS report on the listed system.
  - 2.2.6. Identify ten items from the report you changed based on the report.
  
- 2.3. Each part is worth six points for a maximum of twenty-five points. Upload you answer to the D2L Bright Space Assignment section 2.3 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.
  - 2.3.1. Provide the hostname and version information for router1.
  - 2.3.2. Provide the hard coded IPv4 and IPv6 addresses for host1 connected to a LAN segment.
  - 2.3.3. Provide the hard coded IPv4 and IPv6 addresses for host2 connected to a LAN segment.
  - 2.3.4. Provide evidence host1 accesses the Internet through router1.
  - 2.3.5. Provide evidence host2 accesses the Internet through router1.
  
- 2.4. Upload you answer to the D2L Bright Space Assignment section 2.4 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.
  - 2.4.1. Provide the complete text or XML log entry from a system you control showing "Authentication and Authorization Report" issue. Windows systems will report event id 4624 or equivalent. Please label your answer.
  - 2.4.2. In a paragraph, explain how examining this type of entry helps you find potential security breaches.