

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.
- Plagiarism will not be tolerated.
- Unless noted, all lab sections must be done as unprivileged login.

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 information for a virtual machine router. [4 points]
 - 2.1.2. Provide the NAT configuration to allow local network segment traffic through to the Internet. [5 points]
 - 2.1.3. Provide DHCPv4 configuration information. [5 points]
 - 2.1.4. Provide DHCPv6 configuration information. [5 points]
 - 2.1.5. Provide evidence of hardening at least five parameters according to standards. Identify the standard used. [5 points]
 - 2.1.6. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used. [1 point]

- 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 host1. [4 points]
 - 2.2.2. Provide the IPv4 address, IPv6 address, hostname, and MAC address. The host must be connected to local network segment served by the virtual machine router. [5 points]
 - 2.2.3. Provide evidence the operating system is current with updates. [5 points]
 - 2.2.4. Provide a complete list of all install application programs. [5 points]
 - 2.2.5. Provide evidence of hardening at least five parameters according to standards. Identify the standard used. [5 points]
 - 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. [1 point]

- 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 operating system version information for host1. [4 points]
 - 2.3.2. Provide the IPv4 address, IPv6 address, hostname, and MAC address. The host must be connected to local network segment served by the virtual machine router. [5 points]
 - 2.3.3. Provide evidence the operating system is current with updates. [5 points]
 - 2.3.4. Provide a complete list of all install application programs. [5 points]
 - 2.3.5. Provide evidence of hardening at least five parameters according to standards. Identify the standard used. [5 points]
 - 2.3.6. Identify if an AI type program was used to complete this lab section. If an AI program is used, identify the AI system used. [1 point]

- 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. [8 points]

- 2.4.2. Provide the source code appropriate to the host with the following attributes. [8 points]
- 2.4.2.1. The code purpose is clearly identified.
 - 2.4.2.2. All sources of help are identified. This includes people, web sites, and AI program(s).
 - 2.4.2.3. The author name and date
 - 2.4.2.4. The code will extract the log entries for this section into a csv or similar type of file.
- 2.4.3. Provide the output of the source code showing at least five entries. [8 points]
- 2.4.4. 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]