

Fundamentals of Information Technology Security
CSEC 1110
Lab 08

- 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 08: Network of Networks

- 8.1. Each part is worth six points for a maximum of twenty-five points. Upload your answer to D2L Bright Space Assignment section 8.1 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.
 - 8.1.1. Provide the grant of permission to port scan on the network. All tests must occur during the permission time. A properly signed permission statement is required for any lab section credit.
 - 8.1.2. Report the scanner system IP addresses and scanner version. The scanner host and target systems may not be the same system. Please label your answer.
 - 8.1.3. Report all the findings of an external base port scanner similar to NMAP against a Windows host utilizing "Intense Scan, all TCP ports". The timestamps must be in Central Time or UTC time. Please label your answer.
 - 8.1.4. For each open port found, explain why it should or should not be open.

- 8.2. Each part is worth six points for a maximum of twenty-five points. Each part is worth four points for a maximum of twenty-five points. Upload each section answer D2L Bright Space Assignment section 8.2 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
 - 8.2.1. Provide the grant of permission to port scan on the network. All tests must occur during the permission time. A properly signed permission statement is required for any lab section credit.
 - 8.2.2. Report the scanner system IP addresses and scanner version. The scanner host and target systems may not be the same system. Please label your answer.
 - 8.2.3. Report all the findings of an external base port scanner similar to NMAP against a Linux host utilizing "Intense Scan, all TCP ports". The timestamps must be in Central Time or UTC time. Please label your answer.
 - 8.2.4. For each open port found, explain why it should or should not be open.

- 8.3. Each part is worth six points for a maximum of twenty-five points. Each part is worth four points for a maximum of twenty-five points. Upload each section answer D2L Bright Space Assignment section 8.3 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.
 - 8.3.1. Provide the grant of permission to port scan on the network. All tests must occur during the permission time. A properly signed permission statement is required for any lab section credit.
 - 8.3.2. Report the scanner system IP addresses and scanner version. The scanner host and target systems may not be the same system. Please label your answer.
 - 8.3.3. Report all the findings of an external base port scanner similar to NMAP against a game or similar host utilizing "Intense Scan, all TCP ports". The timestamps must be in Central Time or UTC time. Please label your answer.
 - 8.3.4. For each open port found, explain why it should or should not be open.

- 8.4. Each part is worth five points for a maximum of twenty-five points. Each part is worth four points for a maximum of twenty-five points. Upload each section answer D2L Bright Space Assignment section 8.4 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.
 - 8.4.1. Provide evidence of installing OSSEC on a host.
 - 8.4.2. Provide a copy of the OSSEC configuration file.
 - 8.4.3. Provide a copy of the OSSEC log file after performing a NMAP "Intense Scan, all TCP ports" scan.
 - 8.4.4. Provide a copy of the OSSEC active response log file after performing a NMAP "Intense Scan, all TCP ports" scan.
 - 8.4.5. In a paragraph, explain how OSSEC enhances the security of the host and the network.