Fundamentals of Information Technology Security
CSEC 1110
Lab 09

- 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 09: End to End Networking

9.1. Each part is worth five points for a maximum of twenty-five points. Upload each D2L Bright Space Assignment section 9.1 before the due date found in the 2236a.pdf document. The text must be readable by the instructor. Submit a Portable Document Format (PDF) or word processing file(s) containing your answers.

9.1.1. One section is providing 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.

9.1.2. 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.

9.1.3. Report all the finding of an external base vulnerability scanner similar to OpenVAS against a Windows host. This report must be a “Discovery” report including all found high, medium, low, log and false positive threats. Please label your answer. Insure the scanner has at least one valid login/password for the system(s) being scanned.

9.1.4. Report all the finding of an external base vulnerability scanner similar to OpenVAS against a Windows host. This report must be a “Full and very deep ultimate” report including all found high, medium, low, log and false positive threats. Please label your answer. Please label your answer. Insure the scanner has at least one valid login/password for the system(s) being scanned.

9.2. Each part is worth five points for a maximum of twenty-five points. Upload each D2L Bright Space Assignment section 9.2 before the due date found in the 2236a.pdf document. The text must be readable by the instructor. Submit a Portable Document Format (PDF) or word processing file(s) containing your answers.

9.2.1. One section is providing 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.

9.2.2. Create a diagram of the network that identifies each network device packets will cross or use. Please label your answer. Please submit Visio documents as PDF file.

9.2.3. 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.

9.2.4. Report all the finding of an external base vulnerability scanner similar to OpenVAS against a Linux/Unix host. This report must be a “Discovery” report including all found high, medium, low, log and false positive threats. Please label your answer. Please label your answer. Insure the scanner has at least one valid login/password for the system(s) being scanned.

9.2.5. Report all the finding of an external base vulnerability scanner similar to OpenVAS against a Linux/Unix host. This report must be a “Full and very deep ultimate” report including all found high, medium, low, log and false positive threats. Please label your answer. Please label your answer. Insure the scanner has at least one valid login/password for the system(s) being scanned.

9.3. Each part is worth five points for a maximum of twenty-five points. Upload D2L Bright Space Assignment section 9.3 before the due date found in the 2236a.pdf document. The text must be readable by the instructor. Submit a Portable Document Format (PDF) or word processing file(s) containing your answers.

9.3.1. One section is providing 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.

9.3.2. Create a diagram of the network that identifies each network device packets will cross or use. Please label your answer. Please submit Visio documents as PDF file.

9.3.3. 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.

9.3.4. Report all the finding of an external base vulnerability scanner similar to OpenVAS against a non-Windows or non-Linux host. This report must be a “Discovery” report including all found high, medium, low, log and false positive threats. Please label your answer. Please label your answer.

9.3.5. Report all the finding of an external base vulnerability scanner similar to OpenVAS against a non-Windows or non-Linux host. This report must be a “Full and very deep ultimate” report including all found high, medium, low, log and false positive threats. Please label your answer.

9.4. 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 7.4 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.

9.4.1. Provide evidence of installing OSSEC on a host.

9.4.2. Provide a copy of the OSSEC configuration file.

9.4.3. Provide a copy of the OSSEC log file after performing an OpenVAS “Full and very deep ultimate” or similar scan.

9.4.4. Provide a copy of the OSSEC active response log file after performing an OpenVAS “Full and very deep ultimate” or similar scan.

9.4.5. In a paragraph, explain how OSSEC enhances the security of the host and the network.\