Network Security
CSIS 441
Lab 09

Name _____

- Please upload your answers to the appropriate D2L folder.
- All the requirements for a section must be satisfactory completed for credit.
- The lab must be completed before the due date and time.
- 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.

Lab09 – Administering a Secure Network

9.1. This section is four parts. All answers must be in pdf file format. You will upload to the appropriate drop box.
- 9.1.1. One section is providing the grant of permission to run a vulnerability scan on the network.
- 9.1.2. Create a diagram of the network that identifies each network device packets will cross or use.
- 9.1.3. Report all the findings of an external base vulnerability scanner similar to OpenVAS against a Windows host. The report must include all found high, medium, low, log, and false positive threats.
- 9.1.4. Report Windows host version.

9.2. This section is four parts. All answers must be in pdf file format. You will upload to the appropriate drop box.
- 9.2.1. One section is providing the grant of permission to run a vulnerability scan on the network.
- 9.2.2. Create a diagram of the network that identifies each network device packets will cross or use.
- 9.2.3. Report all the findings of an external base vulnerability scanner similar to OpenVAS against a Linux/Unix host. The report must include all found high, medium, low, log, and false positive threats.
- 9.2.4. Report Linux/Unix host version.

9.3. This section is four parts. All answers must be in pdf file format. You will upload to the appropriate drop box.
- 9.3.1. One section is providing the grant of permission to run a vulnerability scan on the network.
- 9.3.2. Create a diagram of the network that identifies each network device packets will cross or use.
- 9.3.3. Report all the findings of an external base vulnerability scanner similar to OpenVAS against a non-Windows or non-Linux host. The report must include all found high, medium, low, log, and false positive threats.
- 9.3.4. Report the device manufacturer, model, and version.

9.4. This section is four parts. All answers must be in pdf file format. You will upload to the appropriate drop box.
- 9.4.1. One section is providing the grant of permission to capture packets on the network.
- 9.4.2. Create a diagram of the network that identifies each network device packets will cross or use.
- 9.4.3. Provide a copy of the OSSEC Active Response log showing your system reacted to at least two attacks.
- 9.4.4. Your logon/login name must be visible in your answer.