Network Security
CSIS 441
Lab 02

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.

Lab02 - Malware and Social Engineering Attacks

2.1. This section is four parts. All answers must be in pdf file format. You will upload to the appropriate drop box. This section is based on the SANS Top 6 Essential Log Reports found on the D2L site.

2.1.1. Provide the complete text or XML log entry from a Windows system you control showing “Authentication and Authorization Report” issue. Windows systems will report event id 4624 or equivalent.

2.1.2. Provide the complete text or XML log entry from a Linux system you control showing “Authentication and Authorization Report” issue.

2.1.3. Provide the complete text or XML log entry from a Windows system you control showing "Systems and Data Change Report" issue. Windows systems will report event id 4741, 4742, or equivalent.

2.1.4. Provide the complete text or XML log entry from a Linux system you control showing "Systems and Data Change Report" issue.

2.2. This section is four parts. All answers must be in pdf file format. You will upload to the appropriate drop box. This section is based on the SANS organization Top 6 Essential Log Reports found on the D2L site.

2.2.1. Provide the complete text or XML log entry from a Windows system you control showing "Network Activity Report" issue. Windows systems will report event id 5031, 5140, 5142, or equivalent.

2.2.2. Provide the complete text or XML log entry from a Linux system you control showing "Network Activity Report" issue.

2.2.3. Provide the complete text or XML log entry from a Windows system you control showing "Resource Access Report" issue. Windows systems will report event id 4663, 4819, or equivalent.

2.2.4. Provide the complete text or XML log entry from a Linux system you control showing "Resource Access Report" issue.

2.3. This section is three parts. All answers must be in pdf file format. You will upload to the appropriate drop box. This section is based on the SANS organization Top 6 Essential Log Reports found on the D2L site.

2.3.1. Provide the complete text or XML log entry from a system you control showing "Malware Activity Report" issue.

2.3.2. Provide the complete text or XML log entry from a Windows system you control showing "Failure and Critical Error Report" issue. Windows systems will report event id 4875, 4881, 5025, or equivalent.

2.3.3. Provide the complete text or XML log entry from a Linux system you control showing "Failure and Critical Error Report" issue.

2.4. This section is two parts. All answers must be in pdf file format. You will upload to the appropriate drop box.

2.4.1. One section is creating a batch file or script with the following elements.

2.4.1.1. Identify the purpose of the batch file or script.

2.4.1.2. Identify the creation date, any modification dates, and primary author.

2.4.1.3. Identify any addition sources of help or information to create the batch file or script.

2.4.1.4. Provide every file’s permission setting for your home directory. Put the data in a file.

2.4.1.5. Provide the current operating version in the file.

2.4.1.6. Provide the current date in the file.

2.4.1.7. Add a copy of the source code to the file.

2.4.2. One section is providing the complete output of the batch file or script.