Fundamentals of Information Technology Security
CSEC 1110
Lab 05

- 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.

Lab05: Encrypting Files

5.1. Each part is worth eight points for a maximum of twenty-five points. Upload each section answer D2L Bright Space Assignment section 5.1 before the due date found in the csec1110a.pdf document. You may only perform this operation on a system fully under your legal control. The text must be readable by the instructor. Submit a Windows or UNIX text file with the appropriate Windows extension.

5.1.1. Run a password-cracking program against the following passwords. Some of these passwords are from http://gizmodo.com/5954372/the-25-most-popular-passwords-of-2012

5.1.1.1. Password
5.1.1.2. 654321
5.1.1.3. 123abc
5.1.1.4. qwerty
5.1.1.5. letmein
5.1.1.6. An eight-character password of your choice
5.1.1.7. Odnltmotd5dbguaseo
5.1.1.8. “A honu dancing with Snuffy”

5.1.2. Provide a report of the password cracking program results for each password and execution time. You may stop work on a password after eight hours.

5.2. Each part is worth five points for a maximum of twenty-five points. Upload each section answer D2L Bright Space Assignment section 5.2 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.

5.2.1. Provide a list of 10 files on host1. Calculate the computer hash utilizing two different computer hash algorithm and report the result for each file. Please label your answer.
5.2.2. Copy the files from the previous section to host2. Calculate the computer hash utilizing the same algorithms and report the result for each file. Please label your answer.
5.2.3. Provide at least one sentence explanation of what you did to insure the values are the same between both operating systems. Please label your answer.
5.2.4. Select one operating system. Make the simplest modification to each file to change the hash value in both algorithms for each file. Report the result for each file. Please label your answer.
5.2.5. Provide a document identifying the algorithms and what you did to change the computer hash value.

5.3. Each part is worth five points for a maximum of twenty-five points. Upload each section answer D2L Bright Space Assignment section 5.3 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.

5.3.1. Provide directions for successfully encrypting a file. Include any necessary citations for your directions.
5.3.2. Provide evidence of successfully encrypting at least ten files.
5.3.3. Provide evidence of unsuccessful decryption of any of the encrypted files.
5.3.4. Provide evidence of successful decryption of all then encrypted files.
5.3.5. Identify the encryption algorithm and strength for this section.

5.4. Each part is worth five points for a maximum of twenty-five points. Upload each section answer D2L Bright Space Assignment section 5.4 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.

5.4.1. Send a plain text email to your instructor requesting a plain text response with your instructor's digital signature using PGP/GPG.
5.4.2. Provide evidence of correctly verifying your instructor's trusted digital signature using PGP/GPG.
5.4.3. Successfully send and encrypt an email to your instructor. In this email, request your instructor to encrypt a reply using your public key on the class key server using PGP/GPG.
5.4.4. Provide the successfully decrypted response using PGP/GPG.
5.4.5. Provide your operating systems location and permission settings for your private key. Please label your answer.