Assignment Name: Introduction to Information Security Concepts

Duration : 2 weeks (Starting from July 26th , 2021)

Operation system: Any

Note: Completed assignments should be submitted via http://school.wso2.com.

Assignment answer file must be named as Information_Security.pdf

Create the document that includes steps that you followed to answer each question , Ultimately someone else should be able to refer your answers as guide to provide solutions to below questions / use cases

In the following assignment, you may commit your answers to a GitHub repository and provide the relevant links as answers:

1. Use OpenSSL to encrypt the PDF document available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf with AES-256 (with sha256 message digest), using the password "wso2training" (without quotes). Provide the encrypted file and a screenshot of the command you executed as answer.

2. Use OpenSSL to encrypt the PDF document available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf with AES-256 (with sha256 message digest) using the password "wso2training" (without quotes), while setting following parameters. Provide the encrypted file and a screenshot of the command you executed as answer.

   a. IV = 4702A2949A628E975C12A0CD459E2646

   b. Key = 458354644CC9C1AFB8E6F3C6DC90B2734C5B19E5BBB839A870B81125C3208320

3. Create a RSA key pair using a 4096-bit key. Attach your public-key and a screenshot of the command you executed as answer.

4. Use the RSA public key stored at https://drive.google.com/file/d/18E4pYx8o04o0PlhC9Dmboaz68ApU3V3N/view?usp=sharing to encrypt the PDF https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf. Provide the encrypted file and a screenshot of the command you executed as answer.

5. Calculate the SHA512 hash of the file https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf. Provide the encrypted file and a screenshot of the command you executed as answer.

6. Write a simple Python program to accept a value as a command line argument and return only the PBKDF2 hash of the value. Use SHA512 hash digest algorithm for HMAC. Use 200000 as the iteration count. Salt should be the byte value of "Km5d5ivMy8iexuHcZrsD". Only use Python "hashlib" and no other third party library. Provide the source file of the script and a screenshot of the command you executed as answer.

    a. Example execution: python yourscript.py **example**

    b. Example output: 231fafc34a512dc424cd72e001d805a1a3f55b6048107dac75d8bbfdc830b452d845d7a02e67f13715ccacf1b23d1ccb1ef57a28279c5ba76e49b670b255cfc9

7. Change the program created to answer item 7 to use a secure random as the salt value of PBKDF2 hash generation. Provide the source file of the script as the answer.

8. Change the program created to answer item 7 to use a secure random as the salt value and generate a SHA512 hash. Provide the source file of the script as the answer.

9. Use https://hashcat.net/hashcat/ and the wordlist available at https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/phpbb.txt to crack the MD5 value "3c2223212b6dde34bcf86b580bdb71d4" and recover the password. Provide a screenshot of the command you executed to perform this action as the answer.

10. Use the GPG key located at https://keys.openpgp.org/search?q=ayomawdb%40gmail.com to encrypt the PDF document at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf. Provide the encrypted file and a screenshot of the command you executed as answer.

11. Create a GPG key for yourself and upload the public key to any public keyserver (such as https://keys.openpgp.org). Provide the URL to your key as the answer. (Example: https://keys.openpgp.org/vks/v1/by-fingerprint/34FB0BA2155A9D20D248BD0E7D11327265445CF2)

12. Calculate the CVSS 3.1 score for a security issue that can be exploited over the network, with the help of a person-in-the-middle attack, via an admin user of an application, without any additional user interactions and without having an impact on any other systems. Provide the CVSS 3.1 vector string as the answer (example of the format is: "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N"). Consider the CIA impact as follows:

    a. Confidentiality: Low

b. Integrity: High

c. Availability: None

13. Use https://testssl.sh/ to assess the TLS security levels of google.com domain. Provide a screenshot of the command you executed to perform this action as the answer (including "Testing protocols" section of the command output).