| **Task** | **Description** |
| --- | --- |
| Scenario | - You are logged in as user "analyst." - Current working directory is "/home/analyst." - Two files, "Q1.encrypted" and "README.txt," and a subdirectory "caesar" are present. - Instructions in "README.txt" direct you to find a hidden file in the "caesar" subdirectory. |
| Task 1 | - Use the "ls" command to list files in the current directory. - "README.txt" contains instructions about a hidden file in the "caesar" subdirectory. |
| Task 2 | - Use "cd" to navigate to the "caesar" subdirectory. - Use "ls -a" to list all files, including hidden ones. - Locate the hidden file ".leftShift3" and use "cat" to reveal a Caesar cipher message. - Decrypt the Caesar cipher with a "tr" command. |
| Task 3 | - Use the command revealed in ".leftShift3" to decrypt "Q1.encrypted" and recover the data. - Use "ls" to list files in the current directory. - Use "cat" to reveal the decrypted message in "Q1.recovered." Let's break down the command:openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute   * openssl: The OpenSSL command-line tool. * aes-256-cbc: The symmetric encryption algorithm to use. * -pbkdf2: Specifies the use of PBKDF2 for key derivation. * -a: Indicates that the input and output data should be base64-encoded (ASCII). * -d: Instructs OpenSSL to decrypt the input file. * -in Q1.encrypted: Specifies the input file as "Q1.encrypted." * -out Q1.recovered: Specifies the output file where the decrypted data will be saved as "Q1.recovered." * -k ettubrute: Specifies the password or key used for decryption, which is "ettubrute" in this case. |



