

**Department of Engineering Technology**

SET-222

Software Operations & Maintenance

Experiment # 13

**Experiment Title**

Security and Compliance, encryption, audit logging.

**Assessment of CLO(s): 03**

**Performed on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name:** |  | | |
| **Roll No.** |  | **Group** |  |
| **Semester** |  | **Session** |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | **Perf. Level**  **Criteria** | **Excellent**  **(2.5)** | **Good**  **(2)** | **Satisfactory**  **(1.5)** | **Needs Improvement**  **(0 ~ 1)** | **Marks Obtained** |
| **1** | Project Execution & Implementation | Fully functional, optimized, and well-structured. | Minor errors, mostly functional. | Some errors, requires guidance. | Major errors, non-functional, or not Performed. |  |
| **2** | Results & Debugging  Or Troubleshooting | Accurate results with effective debugging  Or Troubleshooting. | Mostly correct, some debugging Or Troubleshooting needed. | Partial results, minimal debugging  Or Troubleshooting. | Incorrect results, no debugging Or Troubleshooting, or not attempted. |  |
| **3** | Problem-Solving & Adaptability  (VIVA) | Creative approach, efficiently solves challenges. | Adapts well, minor struggles. | Some adaptability, needs guidance. | Lacks innovation or no innovation, unable to solve problems. |  |
| **4** | Report Quality & Documentation | Clear, structured, with detailed visuals. | Mostly clear, minor gaps. | Some clarity issues, missing details. | Poorly structured, lacks clarity, or not submitted. |  |
| **Total Marks Obtained Out of 10** | | | | | |  |

**Experiment evaluated by**

|  |  |  |  |
| --- | --- | --- | --- |
| **Instructor’s Name** | **Ms. Shagufta Aftab** | | |
| **Date** |  | **Signature** |  |

## Copyright © Department of Engineering & Technology – UIT University Karachi

**Objective:**

1. Understand the importance of security and compliance in IT systems.
2. Implement basic encryption techniques to secure sensitive data.
3. Configure and test audit logging for user and system activities.
4. Analyze logs for potential security events and compliance verification.

**Prerequisites:**

* Basic understanding of cybersecurity principles.
* Familiarity with Linux/Windows command line.
* Basic Python scripting knowledge (optional).
* Access to a virtual machine or local environment.

**Required Tools/Software:**

* Operating System: Ubuntu/Linux or Windows (with admin rights)
* Python 3.x (optional)
* OpenSSL
* Text Editor (VS Code, Sublime, or nano)
* Auditd (for Linux)
* Event Viewer (for Windows)

**Section A: Encryption**

**1. Symmetric Encryption with OpenSSL**

**Objective:** Encrypt and decrypt files using AES.

**Steps:**

1. Create a sample file:

echo "Confidential Data" > data.txt

1. Encrypt the file using AES-256:

openssl enc -aes-256-cbc -salt -in data.txt -out data.enc

1. Decrypt the file:

openssl enc -aes-256-cbc -d -in data.enc -out decrypted.txt

1. Compare original and decrypted files:

diff data.txt decrypted.txt

**Expected Output:** Files should match.

**2. Asymmetric Encryption (Optional: RSA with Python or OpenSSL)**

* Generate keys using openssl or cryptography Python module.
* Encrypt a message with the public key and decrypt using the private key.

**Section B: Audit Logging**

**1. Linux: Using auditd**

**Objective:** Set up and monitor audit logs.

**Steps:**

1. Install auditd:

sudo apt install auditd audispd-plugins

1. Start the service:

sudo systemctl start auditd

1. Add a rule to monitor /etc/passwd:

sudo auditctl -w /etc/passwd -p wa -k passwd\_changes

1. Trigger an event:

sudo nano /etc/passwd

1. Search logs:

sudo ausearch -k passwd\_changes

**2. Windows: Viewing Logs in Event Viewer**

**Objective:** Analyze system and security logs.

**Steps:**

1. Open **Event Viewer**.
2. Navigate to **Windows Logs > Security**.
3. Identify a successful login event (ID: 4624).
4. Filter logs by event ID.
5. Document time, user, and source.

**Section C: Compliance Check (Discussion/Reflection)**

* Identify compliance standards relevant to encryption and audit logs (e.g., GDPR, HIPAA, ISO 27001).
* Discuss how encryption and audit logging help meet compliance requirements.
* Reflect on best practices for secure system administration.

**Assessment Questions:**

1. What are the advantages and limitations of symmetric vs. asymmetric encryption?
2. What information can audit logs provide in the event of a security breach?
3. Which compliance standards mandate encryption and logging?
4. How would you secure audit logs against tampering?