# Lab #13 – Solved

## Objective:

- Understand the importance of security and compliance in IT systems.

- Implement basic encryption techniques to secure sensitive data.

- Configure and test audit logging for user and system activities.

- 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.

- Created sample file: `echo "Confidential Data" > data.txt`

- Encrypted using AES-256: `openssl enc -aes-256-cbc -salt -in data.txt -out data.enc`

- Decrypted file: `openssl enc -aes-256-cbc -d -in data.enc -out decrypted.txt`

- Compared files using `diff data.txt decrypted.txt` – Output: No differences (files matched).

### 2. Asymmetric Encryption (Optional)

Generated RSA keys using OpenSSL and encrypted a sample message with the public key, then decrypted using the private key using OpenSSL/Python's `cryptography` module.

## Section B: Audit Logging

### 1. Linux: Using auditd

- Installed auditd: `sudo apt install auditd audispd-plugins`

- Started auditd service: `sudo systemctl start auditd`

- Added rule: `sudo auditctl -w /etc/passwd -p wa -k passwd\_changes`

- Edited /etc/passwd to trigger an event: `sudo nano /etc/passwd`

- Searched logs: `sudo ausearch -k passwd\_changes` – Log showed change entry with timestamp.

### 2. Windows: Event Viewer

- Opened Event Viewer > Windows Logs > Security.

- Filtered by Event ID 4624 (successful logins).

- Noted login event details: time, user, source IP (if remote).

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

- Relevant standards: GDPR, HIPAA, ISO 27001 all mandate encryption and audit logging for sensitive data.

- Encryption ensures confidentiality and integrity; audit logs help with incident investigation and accountability.

- Best practices: use encryption at rest and in transit, regularly review logs, restrict access to logs, and use tamper-evident logging systems.

## Assessment Questions – Sample Answers

* Q: What are the advantages and limitations of symmetric vs. asymmetric encryption?

A: Symmetric is faster and suitable for large data but requires secure key sharing; asymmetric is secure for key exchange but slower.

* Q: What information can audit logs provide in the event of a security breach?

A: They show who accessed what, when, from where, and what actions were taken, helping trace unauthorized activity.

* Q: Which compliance standards mandate encryption and logging?

A: GDPR, HIPAA, PCI DSS, and ISO 27001 are examples.

* Q: How would you secure audit logs against tampering?

A: By using write-once storage, access controls, log encryption, and centralized logging servers.