

SET-222

Software Operations & Maintenance

Experiment # 08

**Experiment Title**

Security and Compliance in Software Deployments (Open Ended Lab Activity)

**Assessment of CLO(s): 04**

**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**

To understand and implement essential security and compliance practices during software deployment processes, ensuring data integrity, access control, encryption, and auditing.

**Software/Tools Required:**

* Virtual Machine or Cloud Instance (e.g., Ubuntu/Linux)
* Web Server (Apache/Nginx)
* MySQL or PostgreSQL
* SSH Key-based Authentication Setup
* Log Management Tool (e.g., rsyslog, journald)

**Lab Tasks:**

**Task 1: Secure Configuration of Deployment Environment**

* Disable unused services.
* Enable a firewall (e.g., ufw).
* Configure SSH for key-based login only.

**Commands:**

sudo ufw enable

sudo ufw allow OpenSSH

sudo systemctl disable bluetooth

**Task 2: Implement Access Control Mechanisms**

* Create users and assign roles.
* Restrict sudo access to essential users.

**Commands:**

sudo adduser developer

sudo usermod -aG sudo developer

sudo visudo # Modify to restrict access

**Task 3: Enable Encryption for Sensitive Data**

* Set up HTTPS using self-signed or Let's Encrypt certificates.
* Configure database to use encrypted connections.

**Steps:**

1. Generate SSL certificate using OpenSSL.
2. Configure Apache/Nginx to use SSL.

**Task 4: Audit Logging Configuration**

* Enable logging of system access and changes.
* Configure rsyslog to store logs securely.

**Commands:**

sudo apt install rsyslog

sudo systemctl start rsyslog

sudo journalctl -xe

**Task 5: Compliance Checklist Verification**

* Verify that the deployment complies with standards like OWASP, ISO/IEC 27001.
* Use automated tools like Lynis or OpenSCAP.

**Expected Outcome:**

* A securely configured deployment environment
* Enforced user access controls
* Encrypted communication channels
* System auditing enabled
* Compliance gaps identified and remediated

**Assessment Questions:**

1. What are the risks of not using encryption in deployment?
2. How do audit logs contribute to compliance?
3. What command is used to allow SSH in UFW?
4. Explain the importance of key-based SSH login.
5. Name one compliance framework related to deployment security.