**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**

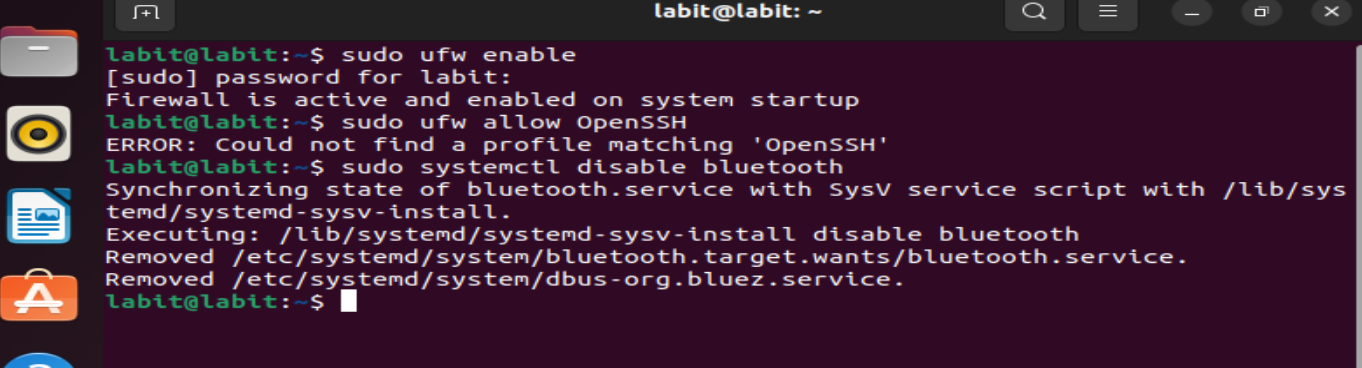
* Disable unused services.
* Enable a firewall (e.g., ufw).
* Configure SSH for key-based login only.

**Commands:**

sudo ufw enable

sudo ufw allow OpenSSH

sudo systemctl disable bluetooth

****

**Task 2: Implement Access Control Mechanisms**

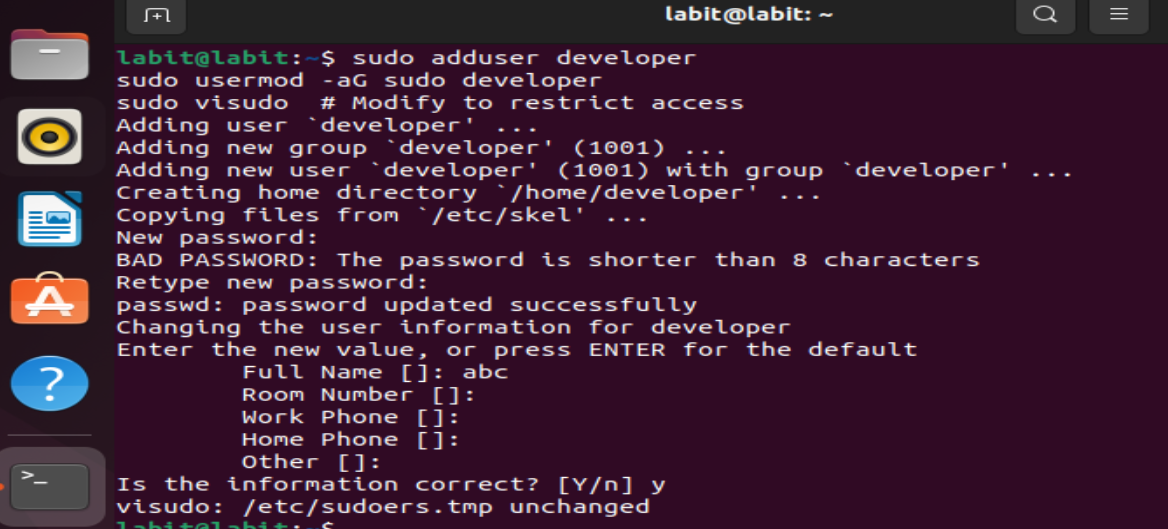
* Create users and assign roles.
* Restrict sudo access to essential users.

**Commands:**

sudo adduser developer

sudo usermod -aG sudo developer

sudo visudo # Modify to restrict access

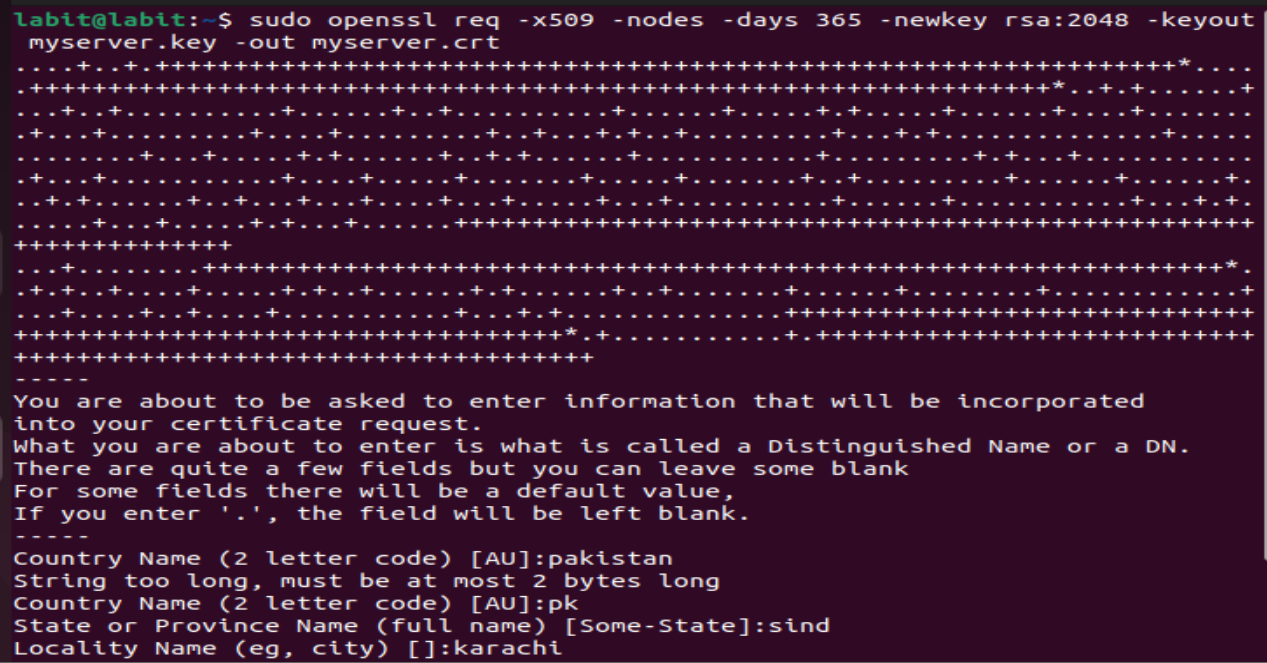


**Task 3: Enable Encryption for Sensitive Data**

* 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**

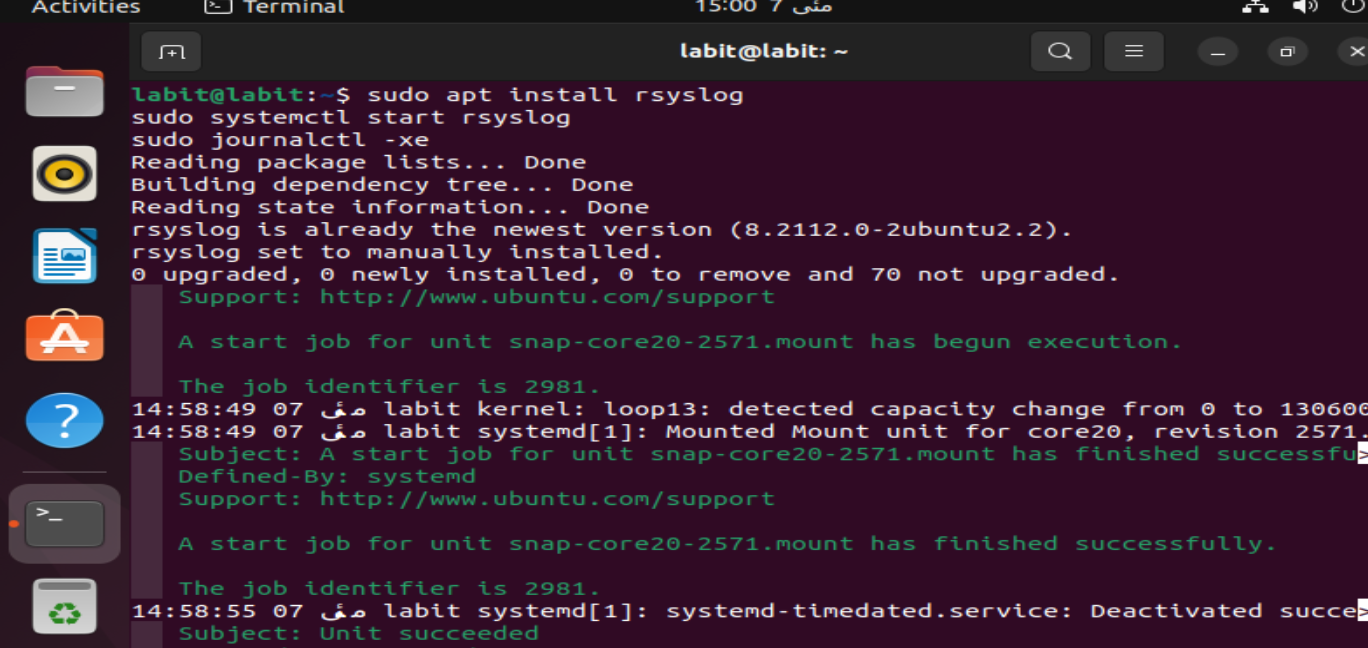
* Enable logging of system access and changes.
* Configure rsyslog to store logs securely.

**Commands:**

sudo apt install rsyslog

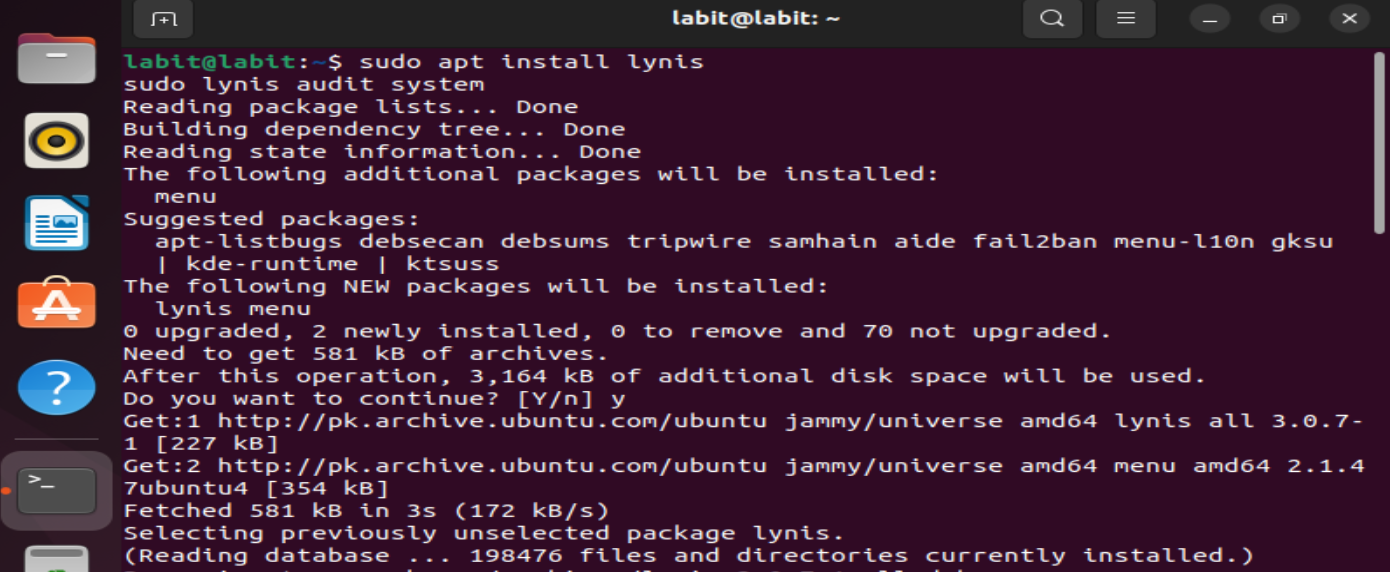
sudo systemctl start rsyslog

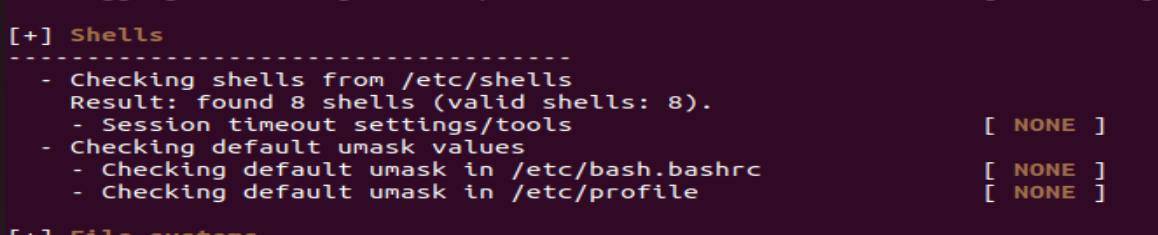
sudo journalctl –xe

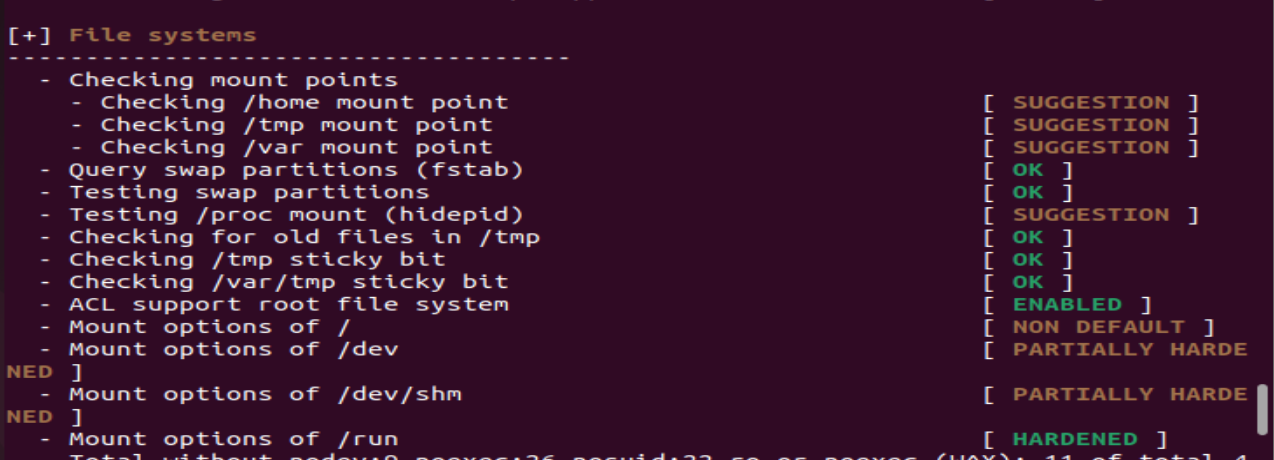


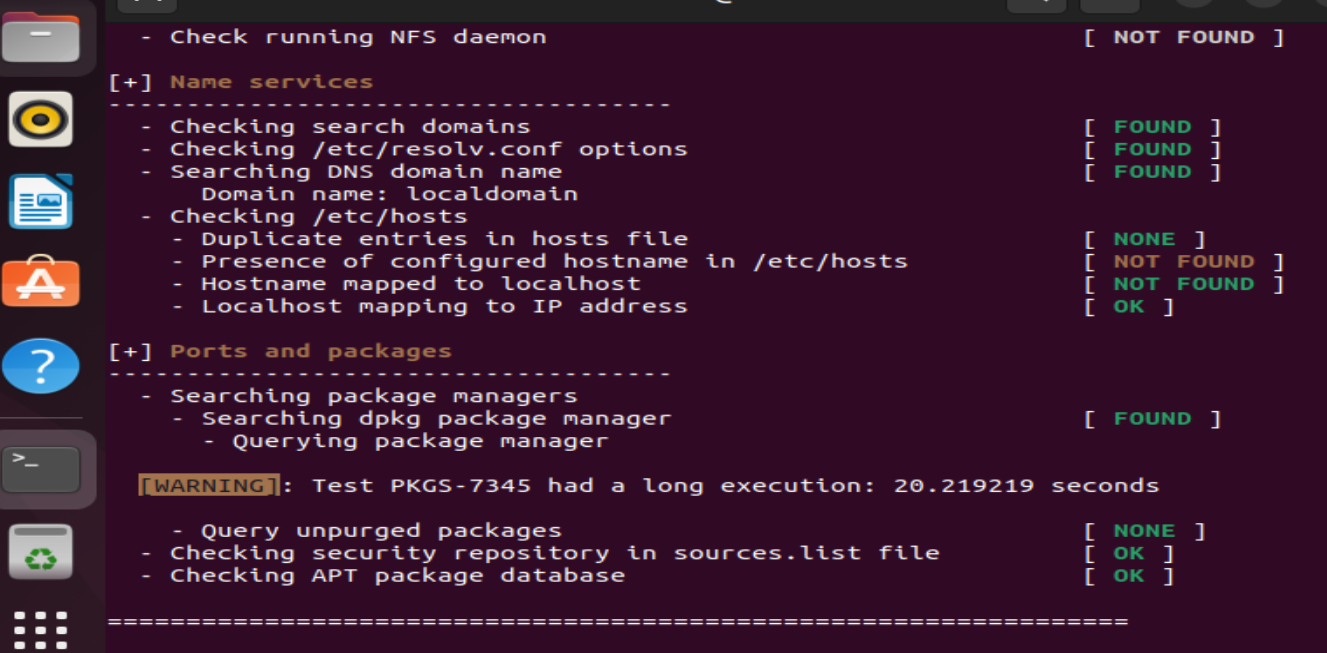
**Task 5: Compliance Checklist Verification**

* 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?**

Ans:Data can be intercepted (MITM attacks), credentials exposed, and confidentiality compromised.

**2.How do audit logs contribute to compliance?**

Ans:They track user actions, help detect anomalies, and provide traceability for audits.

**3.What command is used to allow SSH in UFW?**

Ans: sudo ufw allow OpenSSH

**4.Explain the importance of key-based SSH login.**

Ans:It enhances security by removing password reliance and reducing brute-force vulnerability.

**5.Name one compliance framework related to deployment security.**

Ans: ISO/IEC 27001 or OWASP ASVS.