**Performed Tasks & Implementation**

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

* Disabled unused service: bluetooth
* Enabled UFW firewall and allowed only SSH:

sudo ufw enable

sudo ufw allow OpenSSH

sudo systemctl disable bluetooth

* Configured SSH for key-based login by:
  + Generating SSH keys using ssh-keygen
  + Copying public key using ssh-copy-id

**Task 2: Access Control Mechanisms**

* Added a new user developer:

sudo adduser developer

* Added user to sudo group:

sudo usermod -aG sudo developer

* Edited /etc/sudoers using visudo to restrict unnecessary access.

**Task 3: Encryption for Sensitive Data**

* Generated SSL certificate:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout myserver.key -out myserver.crt

* Configured Apache to use HTTPS:
  + Placed SSL files in /etc/ssl/
  + Edited default-ssl.conf and enabled site using:

bash

CopyEdit

sudo a2enmod ssl

sudo a2ensite default-ssl

sudo systemctl restart apache2

**Task 4: Audit Logging Configuration**

* Installed and started rsyslog:

sudo apt install rsyslog

sudo systemctl start rsyslog

* Verified logs using:

sudo journalctl -xe

**Task 5: Compliance Checklist Verification**

* Used Lynis for security auditing:

sudo apt install lynis

sudo lynis audit system

* Verified settings related to OWASP top 10 and ISO/IEC 27001 compliance points.

**Expected Outcomes Achieved**

* System access controlled via SSH keys.
* Firewall active and unnecessary services disabled.
* HTTPS enabled for secure communication.
* System auditing functional via rsyslog.
* Initial compliance audit performed using Lynis.

**Answers to Assessment Questions**

1. **What are the risks of not using encryption in deployment?**
   * Data can be intercepted (MITM attacks), credentials exposed, and confidentiality compromised.
2. **How do audit logs contribute to compliance?**
   * They track user actions, help detect anomalies, and provide traceability for audits.
3. **What command is used to allow SSH in UFW?**

sudo ufw allow OpenSSH

1. **Explain the importance of key-based SSH login.**
   * It enhances security by removing password reliance and reducing brute-force vulnerability.
2. **Name one compliance framework related to deployment security.**
   * **ISO/IEC 27001** or **OWASP ASVS**.