1.1 Proposed Solution :

Testing and Findings

1. Testing Approach :

To identify vulnerabilities and assess security risks, a Nessus vulnerability scan was conducted on selected systems. The testing process included:

- Defining Scope: Selecting target systems for vulnerability assessment.
- Running Nessus Scan: Conducting network, application, and compliance scans.
- Analysing Results: Reviewing detected vulnerabilities and their severity levels.

2. Findings from Nessus Scan :

The results from the scan highlighted several security weaknesses:
Critical Vulnerabilities :

- Unpatched software with remote code execution risks.
- Weak authentication mechanisms allowing unauthorized access.

High-Risk Vulnerabilities :

- Misconfigured firewall rules exposing unnecessary ports.
- Outdated SSL/TLS protocols leading to encryption weaknesses.

Medium to Low-Risk Issues :

- Open services that could be exploited (e.g., FTP, Telnet).
- Default or weak passwords increasing brute-force attack risks.

3. Proposed Solutions :

- Based on the findings, security measures were recommended: Patching and Updates: Regular software and OS updates to mitigate exploits.
- Firewall and Access Control: Restricting open ports and applying least privilege access.
- Encryption & Authentication: Enforcing multi-factor authentication (MFA) and strong encryption standard.
- Continuous Monitoring: Implementing an Intrusion Detection System (IDS) for real-time threat monitoring.