PTES REPORT

1. Engagement Scope

This penetration test focused on evaluating the security posture of the designated target environment. The assessment included network-level scanning, service enumeration, vulnerability identification, exploitation attempts, and post-exploitation validation. Only approved hosts and services were tested, and all activities were performed within controlled and authorized boundaries to avoid service disruption.

2. Methodology

The assessment followed the PTES phases:

1. **Reconnaissance:** Gathered publicly available information and enumerated network assets.
2. **Threat Modeling:** Prioritized high-risk exposure points.
3. **Vulnerability Analysis:** Performed automated and manual testing to identify weaknesses.
4. **Exploitation:** Attempted safe exploitation to validate real impact.
5. **Post-Exploitation:** Checked privilege escalation and access depth.
6. **Reporting:** Documented findings and recommended fixes.

3. Recon Findings

Recon identified active hosts, open ports, and exposed services. Several technologies and versions were fingerprinted, revealing outdated services, default configurations, and accessible directories. Web enumeration showed publicly accessible admin panels, directory listings, and potential entry points. No rate limiting or access restrictions were observed in some endpoints, increasing exposure risk.

4. Vulnerability Summary

Multiple medium-to-high severity issues were discovered, including outdated software versions, weak authentication mechanisms, default credentials, misconfigured services, and missing input validation. Web scanning revealed directory traversal risks, missing security headers, and potential injection points. These vulnerabilities increase opportunities for unauthorized access and data exposure.

5. Exploitation Details

Controlled exploitation confirmed several issues. Weak credentials allowed access to restricted portals. Directory traversal enabled viewing sensitive files. Outdated services were successfully probed for known vulnerabilities, demonstrating potential remote code execution or privilege escalation if exploited in real-world scenarios. No destructive actions were performed during testing.

6. Remediation

- Apply all pending software and service updates.
- Enforce strong authentication and disable default accounts.
- Restrict access to administrative panels and sensitive endpoints.
- Implement security headers and proper input validation.
- Harden configurations, disable unused ports/services, and apply least-privilege principles.
- Continuously monitor logs and perform routine vulnerability scanning.

SUMMARIES

Recon Summary

Recon revealed active hosts, open ports, and exposed services with outdated versions and weak configurations. Web enumeration identified admin panels, directory listings, and endpoints lacking access controls. These findings provided clear attack paths and formed the basis for deeper vulnerability testing and exploitation attempts.

Non-Technical Summary

A security assessment was performed to understand how well the system can withstand cyberattacks. First, publicly visible information and system exposures were identified. Then, the system was scanned for weaknesses such as outdated software, misconfigurations, and weak login protections. Safe exploitation attempts confirmed how these weaknesses could be misused by an attacker to access sensitive areas. The assessment highlights where the system is vulnerable and provides clear, practical recommendations to improve security, reduce risk, and protect data more effectively.