Cybersecurity Scans and Audit Implementation

Prepared by: Leo D. Dorsey

Objective

To assess the organizations IT environment through comprehensive vulnerability scans and audit procedures in order to identify, evaluate, and mitigate security risks.

Tools & Methods

Tools Used: Nessus, Nmap, OpenVAS, Microsoft Baseline Security Analyzer

Audit Frameworks: NIST Cybersecurity Framework, CIS Controls

Methodology:

- Scheduled internal and external vulnerability scans
- System configuration reviews
- Access control policy assessments
- Log file analysis and event correlation

Implementation Steps

1. Initial Planning: Defined scope of systems and networks to be assessed.
2. Vulnerability Scanning: Conducted regular scans to detect outdated software, misconfigurations, and open ports.
3. Audit Execution: Evaluated user access rights, patch compliance, and endpoint protection settings.
4. Risk Categorization: Prioritized issues based on severity, exploitability, and business impact.
5. Remediation Guidance: Collaborated with IT teams to implement fixes and policy improvements.

Results / Findings

- Discovered multiple high-severity vulnerabilities due to outdated software and exposed services.
- Identified inconsistent access control configurations across departments.

- Detected several legacy systems lacking endpoint protection or monitoring.

- Delivered a prioritized action plan with recommended patches, configuration changes, and policy updates.

Conclusion

The scans and audits conducted significantly improved the organizations visibility into its cyber risk posture. By addressing the key issues identified, the organization reduced its exposure to threats and strengthened its compliance with industry standards.

Screenshot Section

Example Vulnerability Scan Output – OpenVAS

Vulnerability ID	Severity	Description
CVE-2021-41773	Critical	Apache HTTP Server Path Traversal
CVE-2017-0144	High	SMB Remote Code Execution (EternalBlue)
CVE-2020-0796	High	Windows SMBv3 Compression Buffer Overflow
CVE-2019-0708	Medium	Remote Desktop Services RCE (BlueKeep)
CVE-2018-8174	Medium	VBScript Engine Memory Corruption

Audit Checklist Summary

- [x] Firewall rules reviewed and documented
- [x] Endpoint protection verified on all hosts
- [x] Patch management process reviewed and tested
- [ ] Multi-factor authentication enforced for all admins
- [x] Backup and restore process validated
- [ ] Encryption standards aligned with policy
- [x] Logging and monitoring policies implemented
- [x] User access control reviewed and updated
- [ ] Third-party integrations reviewed for risk exposure