Penetration Testing Report

Task#1

Assessment of Windows Systems SecurityDate: 6 August 2024 Performed by Rayyan Alam

Executive Summary

Purpose: To evaluate the security posture of Windows-based systems.

Scope: Included Windows servers, workstations, and Active Directory.

Key Findings: Several critical and high-risk vulnerabilities were discovered.

Conclusion: Immediate remediation is recommended to mitigate identified risks.

Objectives and Scope

Objectives:

•Identify and prioritize vulnerabilities.

•Assess compliance with security best practices.

•Test the organization's incident response capabilities.

Scope:

•In-Scope: Windows servers, workstations, Active Directory.

•Out-of-Scope: Excluded systems or components specified by the organization.

Methodology

- Testing Approach: Grey-box testing.

Phases:

  - Reconnaissance
  - Vulnerability
  - Identification
  - Exploitation
  - Post-Exploitation
  - Reporting

Key Findings - Critical Vulnerabilities

•**SMBv1 Enabled**

Description: Outdated protocol with known vulnerabilities**.**

Impact: Susceptible to exploits such as WannaCry.

Recommendation: Disable SMBv1 and upgrade to SMBv3.

•**Weak Password Policy**

Description: Allows simple passwords**.**

Impact: Increases risk of unauthorized access.

Recommendation: Enforce complex password policies and regular changes.

(Tools Used: Nmap, Nessus, Metasploit, Burp Suite.)

Key Findings - High-Risk Vulnerabilities

- **Unpatched Systems**

Description: Systems lacking critical updates.

Impact: Vulnerable to known exploits.

Recommendation: Implement a robust patch management process.

- **Insecure Configurations**

Description: Misconfigurations in firewall and Group Policies**.**

Impact: Potential unauthorized access and data leakage**.**

Recommendation: Review and update configurations**.**

Medium and Low-Risk Vulnerabilities

- **Medium-Risk**:
  - Outdated Antivirus Software
  - Lack of Logging and Monitoring

- **Low-Risk:**
  - Minor Misconfigurations
- Outdated Software Versions

Vulnerability Distribution

- **Vulnerability Severity Distribution:**

Bar chart illustrating the count of vulnerabilities by severity level.

- **Vulnerability Distribution by Severity:**

Pie chart showing the percentage of critical, high, medium, and low-risk vulnerabilities.

Recommendations

- **Immediate Actions**:
- Disable SMBv1, update firewall rules, and apply critical patches.
- **Short-Term Actions**:
- Implement strong password policies and correct insecure configurations.
- **Long-Term Actions**:
- Conduct regular security assessments and improve staff training.

Conclusion

- **Overall Security Posture:**

The Windows systems have several vulnerabilities that need prompt attention.

- **Next Steps**:

Address identified issues, improve security controls, and schedule follow-up assessments.

Thank You