Vulnerability Management Lab

This report outlines the setup and execution of a vulnerability management scan using Nessus Essentials to assess the security posture of Windows 10 hosts in a sandbox network. The primary objectives were to identify, prioritize, assess, report, remediate, and verify vulnerabilities. Notable steps and activities included:

Nessus Essentials Installation and Configuration:

- Installed and configured Nessus Essentials to perform credentialed vulnerability scans on Windows 10 hosts.
- Ensured that Nessus had the necessary credentials and permissions to access the target hosts.

Vulnerability Management Implementation:

- Established a comprehensive Vulnerability Management function within the sandbox network, encompassing the full vulnerability management lifecycle.

Vulnerability Discovery:

- Conducted vulnerability assessments using Nessus to discover vulnerabilities in Windows 10 hosts.

Identified vulnerabilities related to both Windows updates and third-party software.

Prioritization and Assessment:

- Prioritized identified vulnerabilities based on severity, potential impact, and exploitability.

Conducted in-depth assessments of the vulnerabilities to understand their underlying causes and potential risks.

Reporting:

- Generated detailed vulnerability reports to document findings, including vulnerability descriptions, severity ratings, and recommendations for remediation.

Remediation:

- Initiated the remediation process to address the identified vulnerabilities promptly.
- Developed an automated remediation process to proactively handle vulnerabilities stemming from both Windows updates and third-party software.

Verification:

- Conducted post-remediation scans to verify that the vulnerabilities had been successfully addressed.
- Ensured that the security posture of the Windows 10 hosts had improved.
- By implementing Nessus Essentials and following a structured vulnerability management approach, the sandbox network successfully identified, prioritized, assessed, reported, remediated, and verified vulnerabilities in Windows 10 hosts. This proactive and

comprehensive approach to vulnerability management significantly enhanced the security of the network and reduced potential risks associated with unaddressed vulnerabilities.