3-2 Activity: Network Assessment Approach

Joshua Merren

Southern New Hampshire University

CYB-400-13637-M01 Security Assessment & Auditing

Professor Jillian Seabrook

11 November 2024

When initiating a network assessment, it is crucial to have a well-defined strategy. This involves mapping out the network to understand its architecture and pinpointing critical assets that need protection. The assessment should start with a broad scan using tools that can detect various vulnerabilities across the system. To proactively address security, regularly update and scan systems to catch new vulnerabilities. Combining various tools enhances the check's effectiveness, allowing for a broad evaluation of the network's security posture. OpenVAS tools perform deep scans to identify known vulnerabilities and potential security risks, providing a foundation for these assessments (Narula, 2020).

A successful network assessment must consider people, processes, and technology. The people aspect involves effectively training staff to recognize and respond to security threats. Processes need to be in place to guide the assessment and response strategies. Technology, particularly the tools used for scanning and monitoring, plays a crucial role in identifying and mitigating threats. These components must work together seamlessly to defend against cyber threats. Integrating these elements facilitates a thorough understanding of the network's vulnerabilities, making it possible to develop more effective security protocols (Linnovate, 2024).

Choosing the right tools is critical for an effective network assessment, and OpenVAS stands out. This open-source vulnerability scanner offers comprehensive capabilities for unauthenticated and authenticated testing across different internet and industrial protocols. Well-suited for large-scale scanning, OpenVAS utilizes a potent internal programming language to develop extensive vulnerability tests, making it a valuable resource for systematic network assessments to identify and manage network vulnerabilities. The tool is continuously updated and supported by a passionate community of developers, ensuring its effectiveness against new threats. Additionally, integrating tools like Nmap and Wireshark with OpenVAS can improve the assessment process, providing deeper insights into network traffic and potential security breaches. This combination of tools allows for a detailed and dynamic approach to network security, ensuring all aspects of the network are scrutinized and protected (Vyas, 2023).

The combination of OpenVAS, Wireshark, and Nmap provides a thorough toolkit for network assessment. OpenVAS scans for vulnerabilities, Wireshark analyzes packet data, and Nmap maps the network environment, identifying active hosts and services. This suite of tools offers a layered method of security, allowing for detailed analysis and quicker response to identified risks. By using these tools together, security teams can obtain a holistic view of the network's security level, enabling them to make informed decisions about where to focus their remediation measures. Integrating these tools into regular security practices enhances the ability to detect and respond to threats more effectively, strengthening the organization's overall security posture (Narula, 2020).

References

Linnovate. (2024, April 17). *OpenVAS Community Edition Guide: Fortifying Cybersecurity with Open-Source Software - Proactive Insights and Support For Open-Source Applications*. Proactive Insights and Support for Open-Source Applications. https://hossted.com/knowledge-base/osspedia/infrastructure-and-network/security/openvas-community-edition-guide-fortifying-cybersecurity-with-open-source-software/

Narula, J. (2020, December 19). *How to configure, run and automate OpenVAS: Free Vulnerability Scanner*. Information Security Newspaper | Hacking News. https://www.securitynewspaper.com/2020/12/19/how-to-configure-run-and-automate-openvas-free-vulnerability-scanner/

Vyas, K. (2023, March 22). *OpenVAS vs Nessus Vulnerability Scanners: Comparison Guide*. Enterprise Storage Forum. https://www.enterprisestorageforum.com/security/openvas-vs-nessus/