Assessment 1:

Assessing and Securing Systems on a Wide Area Network (WAN)

Leo Newton

IT-FPX4071 - Cyber Attack & Ethical Hacking

Capella University

Professor Kuhlman

03/18/2024

**Table of Contents**

Scan Type….…..……………………………………………………………………..3

MS08-067…………………...………………………………………………………..4

Vulnerabilities……………………..…………………………………………………4

Securing the WAN…….……………………………………………………..………6

References.…………………………………...……………………………………... 7

**Scan Type**

Performing vulnerability scans using tools like Nmap with exploit scripts is important for organizations to identify and remediate potential security vulnerabilities in their networks and systems, by helping to identify known vulnerabilities, prioritize remediation efforts, provide a baseline for security, meet compliance requirements, and reduce the attack surface.

Scripted scan: Nmap has a built-in library of scripts that can be used to automate vulnerability testing and other tasks. These scripts can be used to test for specific vulnerabilities or perform other security-related tasks.

OS detection: Nmap can perform operating system detection to determine the version of the operating system running on the target system.

TCP SYN scan: This is a stealth scan that sends a SYN packet to the target port and waits for a response. This type of scan does not complete the full TCP handshake, making it difficult to detect.

Port scan: Nmap can perform a port scan to identify the open ports on a target system. This information can be used to determine the types of services and applications that are running on the target system.

**MS08-067**

MS08-067 is a vulnerability in the implementation of the Server service in Microsoft Windows. This service is used to provide remote access to shared resources on a network, and it listens on TCP port 139 and 445.

The vulnerability is caused by a flaw in the way the Server service handles certain requests, allowing an attacker to send a specially crafted request to a vulnerable system, which would result in the execution of arbitrary code with elevated privileges. This means that an attacker could take control of a vulnerable system remotely, and potentially use it to compromise other systems on the same network.

**Vulnerabilities**

1. Port scanning: Nmap can be used to perform a port scan to identify the systems on the network that are running the Server service and listening on TCP port 139 and 445, which are the ports used by the Server service (Usage and examples, 2024).
2. OS detection: Nmap can also be used to perform operating system detection to determine the version of Windows running on the target systems. This information can be used to identify which versions of Windows are affected by the MS08-067 vulnerability (Usage and examples, 2024).
3. Exploit scripts: Nmap has a built-in library of exploit scripts that can be used to test for the presence of known vulnerabilities. One such script, called "ms08\_067\_netapi," can be used to test for the MS08-067 vulnerability. When run against a vulnerable system, this script will trigger the vulnerability and confirm its presence (Usage and examples, 2024).
4. Vulnerability assessment: By combining the results of the port scan, OS detection, and exploit scripts, an organization can assess the vulnerability of its systems to the MS08-067 vulnerability. This information can be used to prioritize remediation efforts and reduce the risk of a successful attack (Usage and examples, 2024).

In summary, performing the steps of the scan with Nmap and exploit scripts helped to identify the vulnerability by first identifying systems that have the Server service running and then checking if those systems are vulnerable to MS08-067 by using the ms08\_067\_netapi script. The scan provided information that can be used to assess the vulnerability of the systems, prioritize remediation efforts, and reduce the risk of a successful attack.

**Securing the WAN**

Wide Area Networks (WANs) are commonly used by organizations to connect multiple locations, including remote offices, partner networks, and cloud services, thereby leading to a distribution of assets which makes it difficult to manage and secure them. To ensure proper protection of all assets, it is critical for organizations to assess and secure systems on the WAN.

WANs increase the attack surface of an organization, as they provide more opportunities for attackers to gain access to the network (Waters, 2023). By assessing and securing systems on the WAN, an organization can reduce its attack surface and discourage attackers, as it becomes more difficult for them to gain access. This proactive approach to security can significantly reduce the risk of a successful attack, thereby protecting the organization's assets and minimizing the potential impact of any breaches that do occur.

Assessing and securing systems on a WAN is important for organizations to meet compliance requirements, protect sensitive data, and ensure business continuity. WANs are often used to transfer sensitive data between locations and are an attractive target for attackers. By assessing and securing systems on the WAN, an organization can protect sensitive data from unauthorized access, meet compliance requirements and avoid penalties, and ensure the confidentiality, integrity, and availability of its systems, thereby guaranteeing business continuity. By taking these measures, organizations can demonstrate that they are taking appropriate steps to protect their systems and data and mitigate any potential risks.

**References**

*Usage and examples: NMAP network scanning*. Usage and Examples | Nmap Network Scanning. (2024). <https://nmap.org/book/nse-usage.html>

Waters, R. (2023, December 19). *Attack surface reduction - 8 best practices*. Ivanti. <https://www.ivanti.com/blog/the-8-best-practices-for-reducing-your-organization-s-attack-surface>

**DELETE REFERENCE BELOW IN REVIEW. THANKS.**

Andrews, J., Dark, J., & West, J. (2018)*CompTIA A+ Guide to IT Technical Support Ninth Edition.*Massachusetts: Cengage Learning.