NETWORK VULNERABILITY ASSESSMENT: A COMPREHENSIVE VULNERABILITY ASSESSMENT USING NMAP, TO IDENTIFY AND MITIGATE NETWORK VULNERABILITIES.

Prepared by

TOMI FAKOS

Intern at

EXTION INFOTECH

June 27th, 2024

Table of Contents

Introduction

An object is considered vulnerable when a vulnerability is present, which is often a result of a weakness or disability. However, vulnerability can be seen as an access point for those who recognize it, and this access can be exploited in the digital space. While organizations may view vulnerabilities as mere weaknesses to be addressed over time, they can be exploited by attackers to cause significant damage beyond the owner's expectations. Therefore, regular vulnerability assessment and scanning should be a priority for any digital organization seeking to thrive in the digital landscape.

This report presents the findings of a vulnerability assessment conducted on the staff's System IP Address at Leverage Technologies company [an imaginary company]. The assessment sought to identify potential vulnerabilities in the staff's system and provide recommendations for remediation. By addressing these vulnerabilities proactively, Leverage Technologies can strengthen its cybersecurity defenses, safeguard sensitive data, and prevent unauthorized access or exploitation.

Vulnerability Assessment

Defined for precision, a Vulnerability Assessment is a methodical process that systematically identifies and evaluates potential vulnerabilities in an organization's systems, networks, and applications. This comprehensive examination scrutinizes various components, configurations, and security controls to uncover weaknesses that could be exploited by attackers. The primary objective is to proactively identify and prioritize vulnerabilities that pose a risk to the organization's assets, enabling timely remediation and mitigation of potential threats.

Methodology:

This vulnerability assessment employed a structured approach, leveraging Nmap methodology to gather information and perform comprehensive scanning. The process involved:

- Network reconnaissance
- Port scanning to detect potential vulnerabilities
- Configured vulnerability scanning with Nmap, an industry-leading tool

This systematic approach enabled the identification of potential vulnerabilities and informed recommendations for remediation.

Vulnerability Scanning and Results

The vulnerability scanning phase utilized advanced scanning techniques to identify vulnerabilities within the staff's systems. The scan was performed to gain a comprehensive understanding of the security landscape. The vulnerability assessment identified several vulnerabilities within the staff's systems, categorized by severity level (high to low).

To conduct the vulnerability assessment using Nmap on Kali Linux, I followed these steps:

1. Open a Terminal: Launched the Terminal application on my Kali Linux system (shortcut: Ctrl+Alt+T or find it in the applications menu).

2. Run Nmap with vulnerability scanning options: In the Terminal, I used the following command to conduct a vulnerability assessment on the target IP address using Nmap: "sudo nmap -p- --script=vuln <target address"

Important Note: Running Nmap with `sudo` is necessary to ensure required privileges for sending and receiving network packets.

Nmap scanned all ports on the target IP address for vulnerabilities using its built-in scripts. The scan duration depends on the target network's size, as observed in my research. Mine took a little while.

Vulnerability Scanning and Results

Based on the scan report, the following five critical vulnerabilities were identified:

- CVE-2007-6750 (Slowloris DOS attack)
- SMB (Server Message Block) vulnerability
- Unknown open ports (5040, 8089, 8191, 49665, 49666, 49667, 49668, 49670)
- Open ports for common services (135, 139, 445, 8000)
- Lack of response on filtered TCP ports

1. CVE-2007-6750 (Slowloris DOS attack): This vulnerability allows an attacker to keep multiple connections open to a target web server, starving its resources and causing a denial of service.

2. SMB vulnerability: The scan results indicate that there are issues with negotiating a connection and receiving bytes related to SMB (Server Message Block) services. This could potentially indicate vulnerabilities such as MS10-054 and MS10-061.

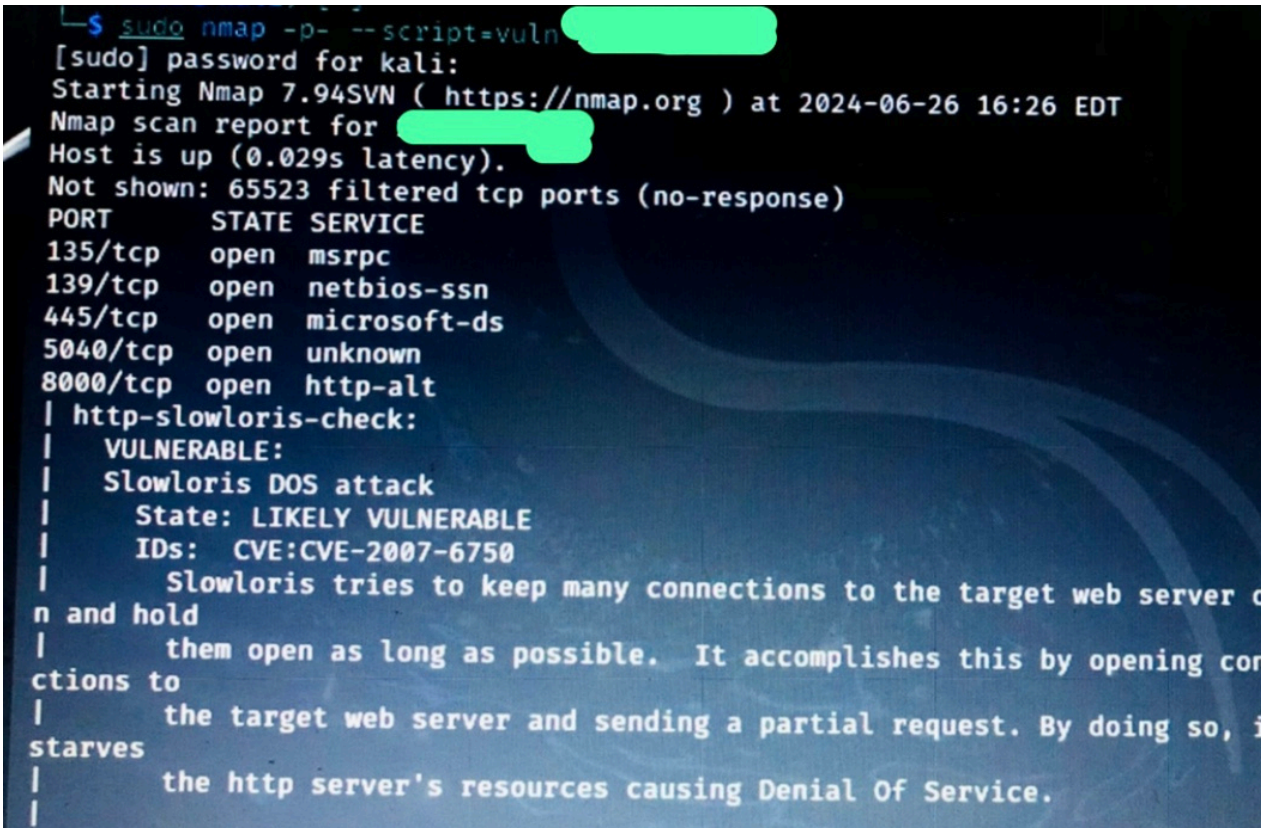
3. Unknown open ports (5040, 8089, 8191, 49665, 49666, 49667, 49668, 49670): The fact that these ports are open and their service is unknown poses a potential security risk.

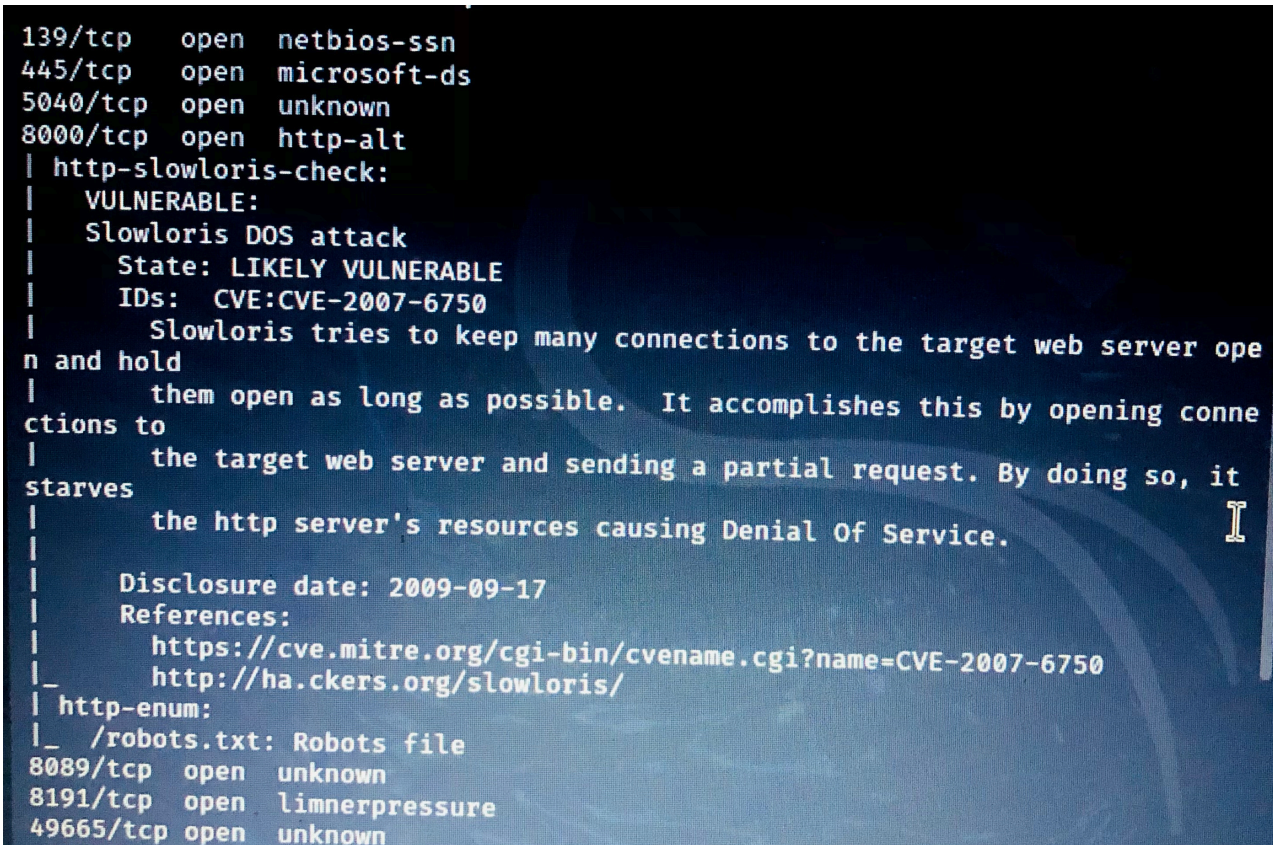
4. Open ports for common services (135, 139, 445, 8000): These ports are commonly associated with services like MSRPC, NetBIOS-SSN, Microsoft-DS, and HTTP-ALT.

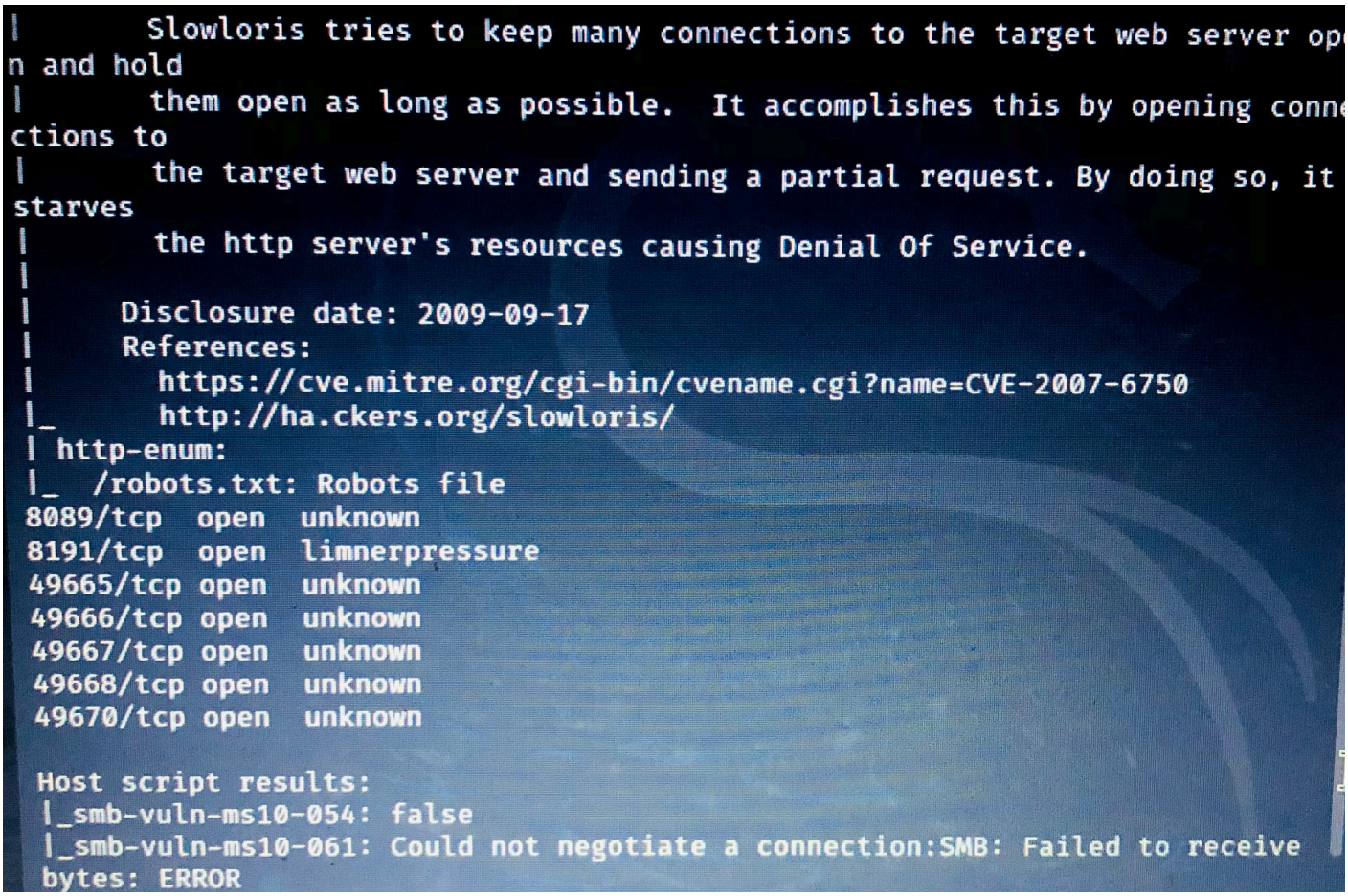
5. Lack of response on filtered TCP ports: The scan report mentions that there are 65523 filtered TCP ports that do not provide a response.

Supporting Evidence of Results

Detailed vulnerability reports and relevant screenshots are included in the appendix, providing additional context and evidence for each identified vulnerability, ensuring transparency and facilitating further analysis.







These supporting evidences provides a comprehensive analysis of each identified vulnerability. A brief description of each vulnerability is provided, along with its potential impact on the staff's system and data. The potential risks associated with each vulnerability, such as unauthorized access, data breaches, or service disruptions, are highlighted to emphasize the importance of mitigation.

Mitigation Strategies

For each vulnerability, specific mitigation strategies are recommended. These strategies may include applying patches or updates, configuring systems securely, implementing additional security controls, or conducting user awareness training.

The mitigation strategies are prioritized based on the severity and potential impact of each vulnerability. They are:

1. CVE-2007-6750 (Slowloris DOS attack):
   - Apply the latest patches and updates for the affected web server software.
   - Implement rate limiting or connection timeout mechanisms to prevent resource exhaustion.
   - Utilize intrusion detection and prevention systems to detect and block Slowloris attacks.
   - Regularly monitor server logs for suspicious activity.

2. SMB vulnerability:
   - Apply the necessary security patches and updates for the SMB services.
   - Configure SMB services to use secure authentication protocols.
   - Implement network segmentation and access controls to limit exposure of SMB services.
   - Utilize intrusion detection and prevention systems to detect and block SMB-related attacks.
   - Regularly monitor SMB service logs for any signs of compromise.

Mitigation Strategies Cont'd

3. Unknown open ports:
- Identify the services running on these ports and assess their necessity for business operations.
- If any unnecessary services are identified, disable or close the corresponding ports.
- Ensure that the services running on these ports are properly secured and up to date.

4. Open ports for common services:
- Ensure that the configurations of these services are secure and follow best practices.
- Implement strong authentication mechanisms and access controls for these services.
- Regularly update and patch the software associated with these services.
- Monitor the logs of these services for any suspicious activity.

5. Lack of response on filtered TCP ports:
- Review and update the filtering rules to ensure that only necessary ports are open.
- Regularly review and update the firewall configurations to align with the organization's security policies.
- Implement intrusion detection and prevention systems to detect and block potential threats.

By implementing these mitigation strategies, you can significantly reduce the risk of exploitation and enhance the security posture of your network.

Conclusion

This vulnerability assessment has yielded invaluable insights into the system's security posture, revealing critical areas that demand prompt attention. Through meticulous identification and evaluation, key findings have emerged that necessitate swift action to bolster cybersecurity measures. By implementing the recommended mitigation strategies, the organization can significantly strengthen its security posture, remediate identified vulnerabilities, and safeguard its critical assets against emerging threats. To stay ahead of evolving threats, regular reassessments, effective incident response planning, and a culture of cybersecurity awareness are crucial. By embracing a proactive approach, the organization can ensure ongoing protection and resilience in the face of ever-evolving risks.