NETWORK VULNERABILITY ASSESSMENT:

PROJECT :- 1

Date: 26/01/2025

Cyber Security Intership

Extion Infotech

MAHENDRA A. PATIL

mrpatil0804@gmail.com

Introduction

- 1.1 Purpose: The objective of this assessment is to evaluate the security posture of the simulated network environment and identify potential vulnerabilities that could be exploited by malicious actors. This will help to mitigate risks, protect sensitive information, and ensure the overall security of the network.

- 1.2 Scope: The scope of this assessment includes the following:

Operating System: Windows 7 operating system

- Network Services and Applications:Identify and list all network services and applications running on the system, including:
  - Web servers (e.g., IIS)
  - File sharing services (e.g., SMB)
  - Remote desktop services (e.g., RDP)
  - Email servers (if applicable)
  - Database servers (if applicable)
  - Other relevant services

- Network Configuration and Security Settings:Review the network configuration, including:
  - Firewall rules
  - Router and switch configurations
  - Network segmentation
  - Access control lists (ACLs)
- Examine security settings, such as:
  - User accounts and permissions
  - Password policies
  - Group policies
  - Security updates and patches
  - Logging and monitoring

Introduction

1.3 Methodology:

- Tools and Techniques:
  - Nessus vulnerability scanner
  - Manual checks for configuration and security settings

Assessment Process:

a. Initial Reconnaissance:Gather information about the target system, including its operating system, installed software, and network configuration.
b. Vulnerability Scanning:Use Nessus to scan the system for known vulnerabilities.
c. Analyze the scan results to identify potential security risks.
d. Manual Verification:Manually verify the identified vulnerabilities to confirm their existence and assess their potential impact.
e. Check for misconfigurations, weak passwords, and other security issues.
f. Risk Assessment:Evaluate the severity and likelihood of exploitation for each identified vulnerability.
g. Prioritize vulnerabilities based on their potential impact and the ease of exploitation.
h. Report Generation:Document the findings of the assessment, including a detailed description of each vulnerability, its potential impact, and recommended mitigation strategies.

Vulnerability

Vulnerability 1:

Description: A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account. Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

Severity: Critical

Impact: Remote code execution, leading to potential system compromise and data theft.

Recommended Mitigation Strategies:

Install the latest security updates: Microsoft has released a patch to address this vulnerability. Ensure that all affected Windows systems have the latest security updates installed.
Disable LLMNR: If LLMNR is not essential for network operations, consider disabling it to mitigate the risk of exploitation.
Implement network segmentation: Segmenting the network can limit the impact of a successful attack. Isolate critical systems and restrict network traffic to necessary flows.

Vulnerability

Vulnerability 2:

Description: Vulnerability Type: Missing Patches/End-of-Life Software

- Affected Software: Microsoft Windows (Remote)
- Affected Systems: Remote Windows systems
- CVSS v3.0 Base Score: 10.0
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- CVSS v2.0 Base Score: 10.0
- CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
- Specific Details: The remote Windows system is running an unsupported version. This means Microsoft no longer provides security updates, patches, or technical support for this operating system. As a result, the system is highly vulnerable to known and unknown security exploits, including malware infections, data breaches, and system compromise.

Severity: Critical

Vulnerability

Vulnerability 3: MS17-010: SMB Server Vulnerabilities (ETERNALBLUE**)**

Description:
Multiple critical vulnerabilities (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148) exist in Microsoft Server Message Block 1.0 (SMBv1). These vulnerabilities, collectively known as MS17-010, allow unauthenticated remote attackers to exploit weaknesses in SMBv1 to Execute arbitrary code remotely: Attackers can gain control over the affected system, install malware, steal data, or disrupt services.
Disclose sensitive information: Attackers can exploit these vulnerabilities to steal sensitive data from the affected system.
This vulnerability has been actively exploited in real-world attacks, such as WannaCry and NotPetya ransomware, causing significant global disruption. Publicly available exploits and tools (ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, ETERNALSYNERGY) make it easier for attackers to exploit these vulnerabilities.

Severity: Critical

Impact:

Remote Code Execution: Enables attackers to gain control of the affected system.
Data Theft: Allows attackers to steal sensitive data.
System Disruption: Can lead to service disruptions and system unavailability.
Widespread Impact: Due to the severity and ease of exploitation, this vulnerability has the potential for significant and widespread impact.

Vulnerability

Vulnerability 4: ICMP Timestamp Request Remote Date Disclosure

Description:

The remote host responds to ICMP timestamp requests. This allows an attacker to determine the approximate date/time set on the target machine. While this information alone may not directly compromise the system, it can be used by attackers to:

Assist in defeating time-based authentication protocols: By knowing the system time, attackers can potentially exploit timing-based security measures or synchronization mechanisms.
Gain additional information for social engineering attacks: The system time can provide clues about the target's location or activity patterns.
Note: Windows Vista, 7, 2008, and 2008 R2 systems attempt to mitigate this by returning inaccurate timestamps, but these are typically within 1000 seconds of the actual system time**.**

Severity: Low

Impact:

Limited Direct Impact: Primarily aids in social engineering or bypassing time-based security controls.
Indirect Risk: Can be used as a component in more complex attacks.\

Recommended Mitigation Strategies:

Disable ICMP Timestamp Responses: If possible, configure the system to not respond to ICMP timestamp requests. This can be achieved through firewall rules or operating system-specific configurations.
Regular Time Synchronization: Ensure accurate and frequent time synchronization with a reliable time source (e.g., NTP server) to minimize the impact of potential timing-based attacks.