Student Name: Oluwabukunmi Olumide Fakowajo

Student ID: K2455760

Title: Vulnerability Assessment Report

Module: CI7130 – Network and Information Security

School: Faculty of Engineering and Computing Environment

Date of Submission: 24th April 2025

1. Executive Summary

This vulnerability Assessment was carried out to examine the security Posture of a windows 7 machine inside an internal network using Industry specified tools and techniques. The main goal of this objective was to find critical vulnerabilities, evaluate their exploitability and suggest mitigation techniques suitable for business continuity.

The following are the main conclusions:

- Critical Vulnerability: Unauthorized Remote Access.
- Other vulnerabilities include: Unsupported windows software.
- Exploitation Technique: Metasploit is a tool which can be used to exploit the vulnerability.
- Impact: Denial of service, Possible system takeover.
- Network Reachability: Target system was reachable over the internal network Risk Level: **Critical**

Required resources, budget and quantities:

Resources	Detail	Estimated Cost (£)
Hardware	Windows 7 test machine, Kali Linux machine	Nil
Software	Nessus scanner, Firewall	1500
Labor	CISO, Security analyst, Penetration Tester	45-90/hr
OS Upgrade	Windows 10 licenses	120 per device

Table 1: Required resources, budget and quantities

The following include suggested effective mitigation strategies against such vulnerabilities:

1. **Regular upgrades**: Switch to a compatible operating system (like Windows 10) from Windows 7.
2. **Patch Management**: Ensure all updates and fixes for the DNS service are installed promptly. This helps close security gaps and keeps the system protected from known threats.
3. **Firewall Hardening**: Make sure that only reliable systems and devices are permitted to transmit DNS queries by adjusting the firewall's settings.

2. Vulnerability Assessment

2.1 Introduction

This section outlines the objective of the vulnerability assessment, which was to evaluate the internal network security posture of a legacy Windows 7 system. The aim was to identify potential weaknesses that could compromise system performance or availability. The assessment was conducted using industry-standard tools within a controlled and virtualized environment.

Assessment Environment: The Table 2.1 below outlines the key components of the security assessment, including the systems, tools, and network setup used during the evaluation.

Category	Details
Vulnerable system	Unpatched Windows 7 (**192.168.10.251**)
Potential Attacker System	Kali Linux (**192.168.10.3**)
Assessment Tools	**Tenable's Nessus (10.8.3)**: Performs risk-based vulnerability scanning, identifies misconfigurations, and checks compliance issues. Based on Common Vulnerabilities and Exposures (CVEs). Nessus was selected because of its CVE correlation capabilities and enterprisegrade database of more than 130,000 vulnerabilities.
Assessment Duration	2 days
Network Topology	A single subnet where the target system is accessible over the local network as shown in (Figure 2.1).

Table 2.1: Assessment Environment

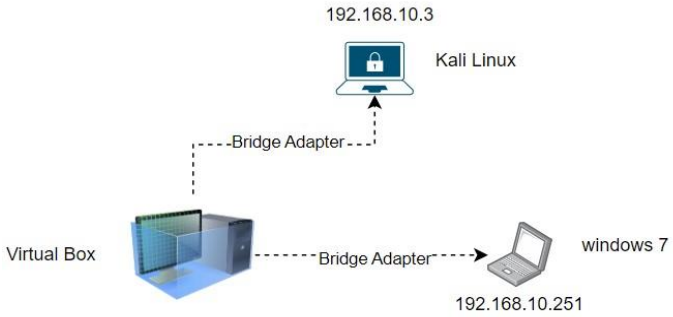

Figure 2.1: Network Topology

2.2 Vulnerability Assessment Report

2.2.1 Network Reachability Phase (Pre- Assessment check)

Prior to conducting a vulnerability scan on the target host, a ping command was initiated from the scanning system to test the connectivity between the scanning machine (Kali Linux) and the target host (Windows 7), as shown in Figure 2.2.1.

Command Executed: "**Ping 192.168.10.251**"

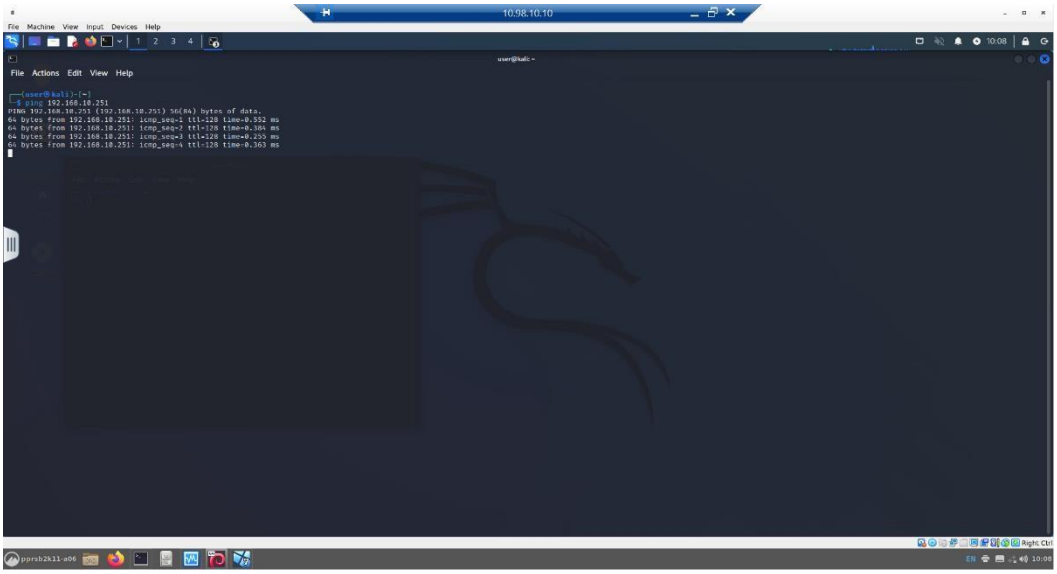

Figure 2.2.1: Host reachability via ping

2.2.2 Vulnerability scanning Phase

After confirming that the target machine was reachable, the next step involved scanning the target system for potential security flaws and misconfigurations that could expose it to threats.

Tool utilized: Tenable Nessus scanner (10.8.3), a strong vulnerability assessment tool that can find known CVEs, obsolete software components, unsafe setups, and noncompliance with regulations.

Scan Configuration:

- Scan type: Advanced Scan
- Target: IP address of the windows 7 host (192.168.10.251)
- Port Range: Full port scan (1-65535)
- Credential Access: Enabled with windows SMB Username and Password, which helps uncover deeper Vulnerabilities
- Post-scan Action: Export results to PDF.

Key Findings: The list of vulnerabilities found during the Nessus scan on the Windows 7 host system (192.168.10.251) is summarized in Figure 2.2.2 below. The graphic breakdown includes information about the most important results as well as the quantity of vulnerabilities grouped by severity levels.

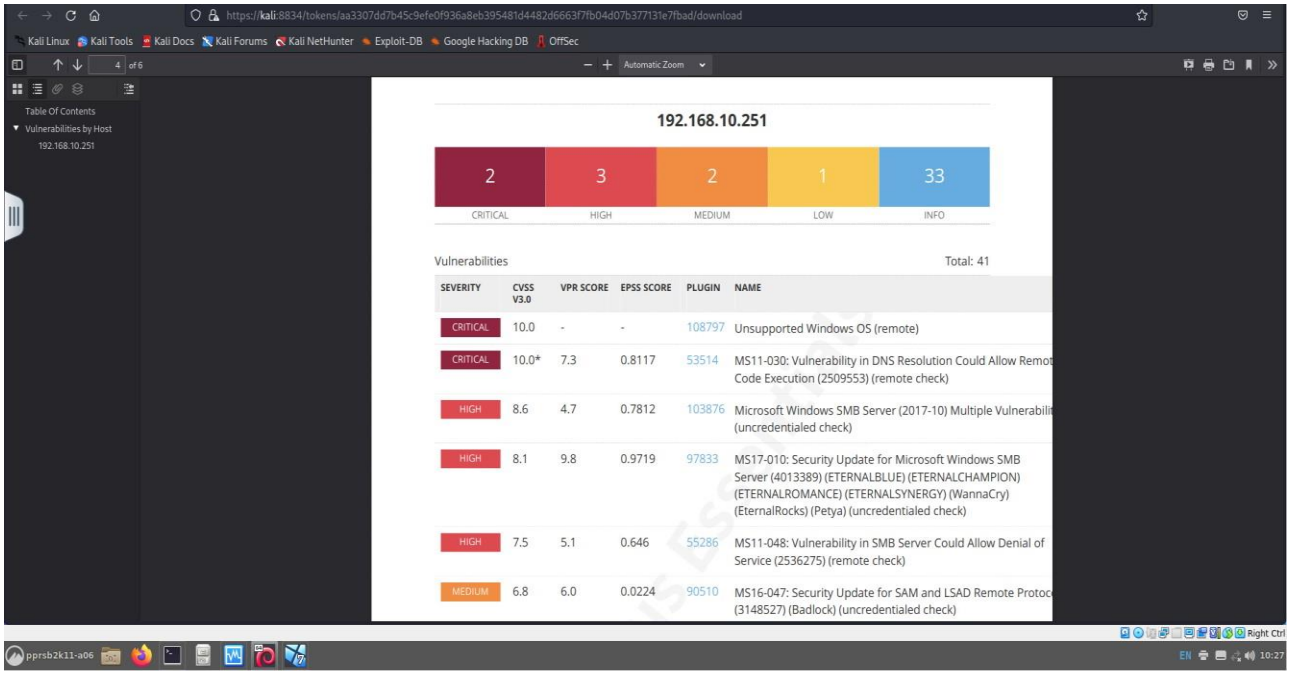

Figure 2.2.2: Vulnerability report 1

2.3 Evaluation

The vulnerability assessment of the Windows 7 host (IP: 192.168.10.251) using Nessus revealed **41 vulnerabilities** in total, categorized by severity as **2 Critical**, **3 High**, **2 Medium**, and **1 Low**. These were rated based on the CVSS v3.0 scoring system and evaluated for their potential risk and exploitability. Due of the narrow scope, I concentrated on the vulnerabilities that were most important to the operation of the core system, ranging from V1-V3; others were left out because they posed far lower risks.

- **V1**: MS11-030 – DNS RCE (CVE-2011-0658) CVSS: 10.0* (**Critical**) – Exposes windows systems to man-in-the-middle & spoofing attacks where by name resolutions may be answered by unauthorized devices listening on port 5355 leading to remote code execution (1).
- **V2**: Unsupported Windows OS CVSS: 10.0 (**Critical**) - No longer receives security patches, leaving the system open to many public exploits (Microsoft, 2020).
- **V3**: MS17-010 – SMBv1 RCE (CVE-2017-0144) CVSS: 8.6 (**High**) - Exploited in the WannaCry ransomware outbreak, this SMBv1 vulnerability enabled remote code execution, impacting over 150 countries and causing over $1 billion in damages within a week, including severe disruption to organizations like the NHS (2).

3. Results and Mitigation Recommendations

3.1 Vulnerability Severity and Impact Assessment

The Windows 7 vulnerability assesment exposed key security flaws, summarized in Table 3.1 below.

Vulnerability ID	Name/Description	Severity	Potential Impact
V1	DNS RCE	Critical	Remote code Execution
V2	Unsupported Windows OS	Critical	Unpatched exploit exposure & total system takeover
V3	SMBv1 RCE	High	Ransomware infection

Table 3.1:Vulnerability severity and impact analysis

3.2 Mitigation and Recommendations

1. **Apply All High-Risk Security Patches** – Severity: **High**

This measure directly addresses vulnerabilities like: **V1** and **V3**

Patching the OS and core services (e.g., DNS, SMB) needs to be done quickly to close up high-risk vulnerabilities Microsoft released patches that are available to eliminate such vulnerabilities.

Impact: Low if updates are scheduled; mandatory for threat prevention.

2. **Upgrade Windows 7 to Windows 10/11** – Severity: **Critical**

This measure directly addresses vulnerabilities like: **V1 and V2**

Platforms that are not supported are inherently insecure. Continuous patching and compatibility with contemporary protections like Credential Guard are guaranteed by upgrading.

Impact: Major security advantage; little resource use during changeover.

3. Firewall Hardening: Restrict DNS Traffic – Severity: High

This measure directly addresses vulnerabilities like: **V1** and **V3.**

Blocking certain open ports like 5355 from external sources and limiting search to just reliable internal DNS servers using firewall DNS filters. This reduces spoofing or redirection attacks and inhibits illegal resolution pathways.

Impact: Boosts DNS trust; maintains devices utilizing only reliable name servers, helps prevent phony replies, and protects the network from deception attacks.

References

1. O'Leary M. Attacking the Windows Domain. Cyber Operations. 2019. 347–417 p.
2. Askarifar S, Abd Rahman NA, Osman H. A review of latest wannacry ransomware: Actions and preventions. J Eng Sci Technol. 2018;13(Special Issue on ICCSIT 2018):24–33.

Microsoft (2017). CVE-2017-0144*:* Microsoft SMB Remote Code Execution Vulnerability*.* [online] Available at: Microsoft Security Bulletin MS17-010 - Critical | Microsoft Learn

Microsoft (2011). CVE-2011-0658: DNS remote code execution vulnerability.[online] Available at: Microsoft Security Bulletin MS11-030 - Critical | Microsoft Learn