Student Name: Oluwabukunmi Olumide Fakowajo

Student ID: K2455760

Title: Vulnerability Assessment Report

Module: CI7130 – Network and Information Security

School: Faculty of Engineering, Computing and The Environment

Date of Submission: 24thApril 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: **LLMNR DNS Remote Code Execution (RCE) vulnerability**
- Other vulnerabilities include**: Unsupported windows OS**, **Outdated Microsoft windows SMB Server**
- Exploitation Technique: Metasploit is a tool which ca n be used to exploit the vulnerability
- Impact: Denial of service, Possible remote code execution
- 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 attacker machine	1200
Software	Nessus scanner, Metasploit Framework, Firewall, IDS	2500
Labor	CISO, Security analyst, Penetration Tester	45-90/hr
OS Upgrade	Windows 10 licenses	120 per device

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

The purpose of this vulnerability assessment was to find vulnerabilities in a Windows 7 system's internal network security posture. **Nessus** for vulnerability scanning was used to evaluate the system and **Metasploit** for exploitation. The vulnerabilities resulting in a Denial of service (DOS), due to repeated attacks on the systems DNS service.

Assessment Environment: The table 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. **Metasploit Framework**: Automates the exploitation of known 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)

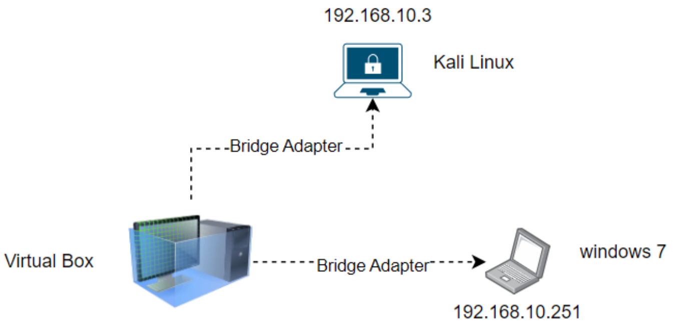


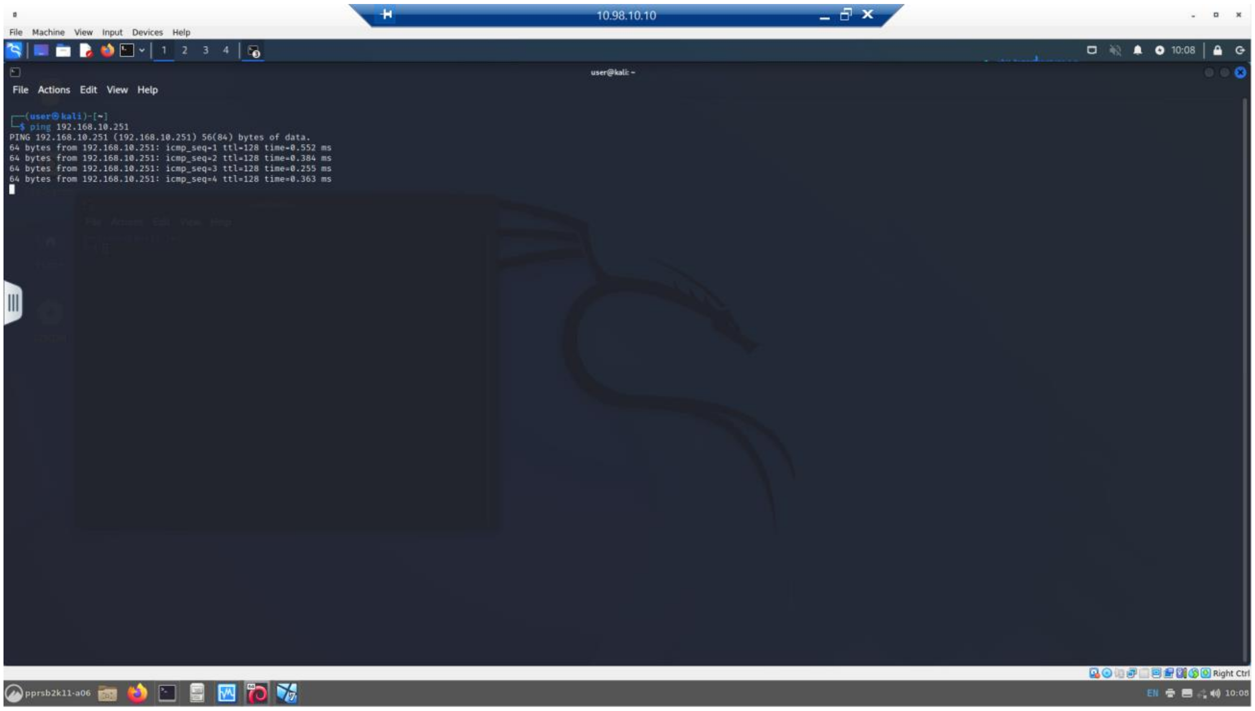
Figure 2.1: Network Topology

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 attacker system to test the connectivity between the attacker machine (Kali Linux) and the target host (Windows 7) (As shown in Figure 2.2.1).

Command Executed: “**Ping 192.168.10.251**”


10.98.10.10
File Machine View Input Devices Help
user@kali: ~
File Actions Edit View Help
pprsb2k11-a06
Right Ctrl
EN
10:08

```
┌──(user㉿kali)-[~]
└─$ ping 192.168.10.251
PING 192.168.10.251 (192.168.10.251) 56(84) bytes of data.
64 bytes from 192.168.10.251: icmp_seq=1 ttl=128 time=0.552 ms
64 bytes from 192.168.10.251: icmp_seq=2 ttl=128 time=0.384 ms
64 bytes from 192.168.10.251: icmp_seq=3 ttl=128 time=0.255 ms
64 bytes from 192.168.10.251: icmp_seq=4 ttl=128 time=0.363 ms
```

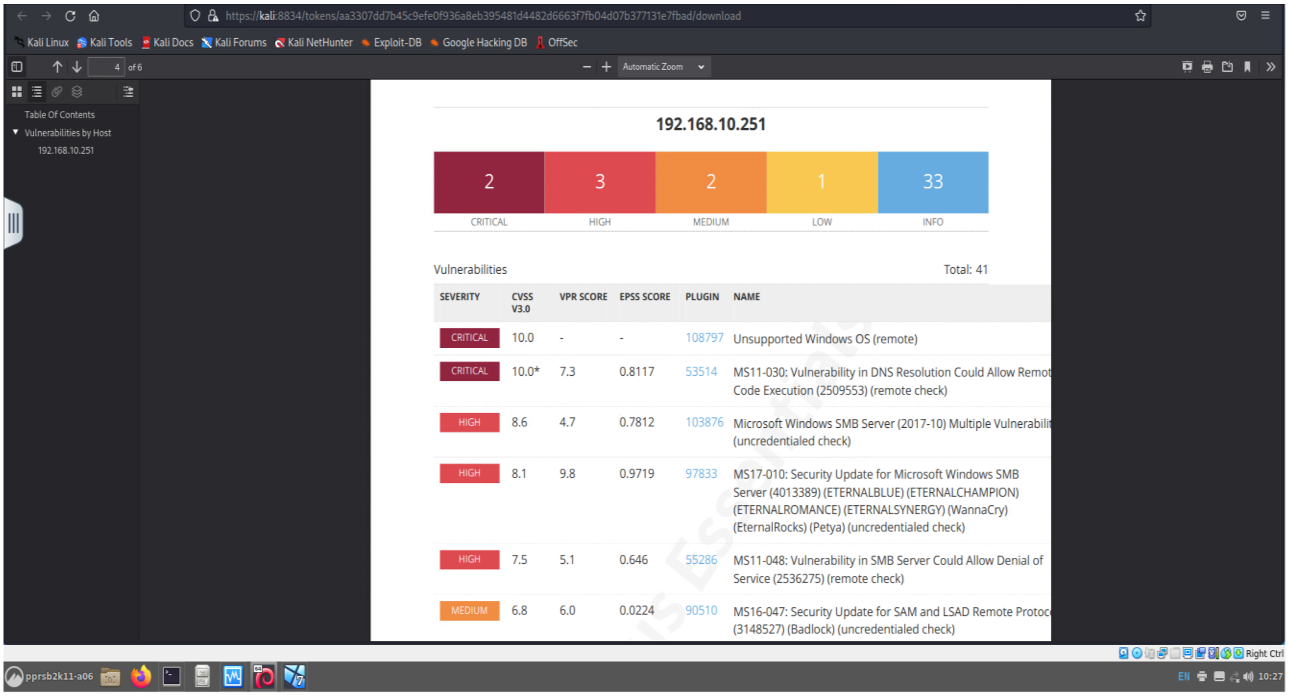
Figure 2.2.1: Host reachability via ping

2.2.2 Vulnerability scanning Phase

Tool used: Tenable Nessus scanner (10.8.3)

Findings:

- **Critical**: LLMNR DNS Remote Code Execution vulnerability using udp port 5355
- High: Multiple old application components found
- Medium: Inadequate access control mechanisms identified



192.168.10.251

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	3	2	1	33

Vulnerabilities Total: 41

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.3	0.8117	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remot Code Execution (2509553) (remote check)
HIGH	8.6	4.7	0.7812	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilit (uncredentialed check)
HIGH	8.1	9.8	0.9719	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	5.1	0.646	55286	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275) (remote check)
MEDIUM	6.8	6.0	0.0224	90510	MS16-047: Security Update for SAM and LSAD Remote Protoc (3148527) (Badlock) (uncredentialed check)

Figure 2.2.2: Vulnerability report 1

2.3 Evaluation

The scan on **192.168.10.251** using nessus uncovered 41 vulnerabilities, including **2 Critical** and **3 High** severity risks**.** The LLMNR RCE vulnerability (MS11-030) on UDP port 5355 is a significant concern because it can be easily exploited through spoofing attacks, allowing attackers to execute remote code. Focusing on LLMNR is crucial as it can bypass DNS security measures and provide a pathway for malicious activities within a network.

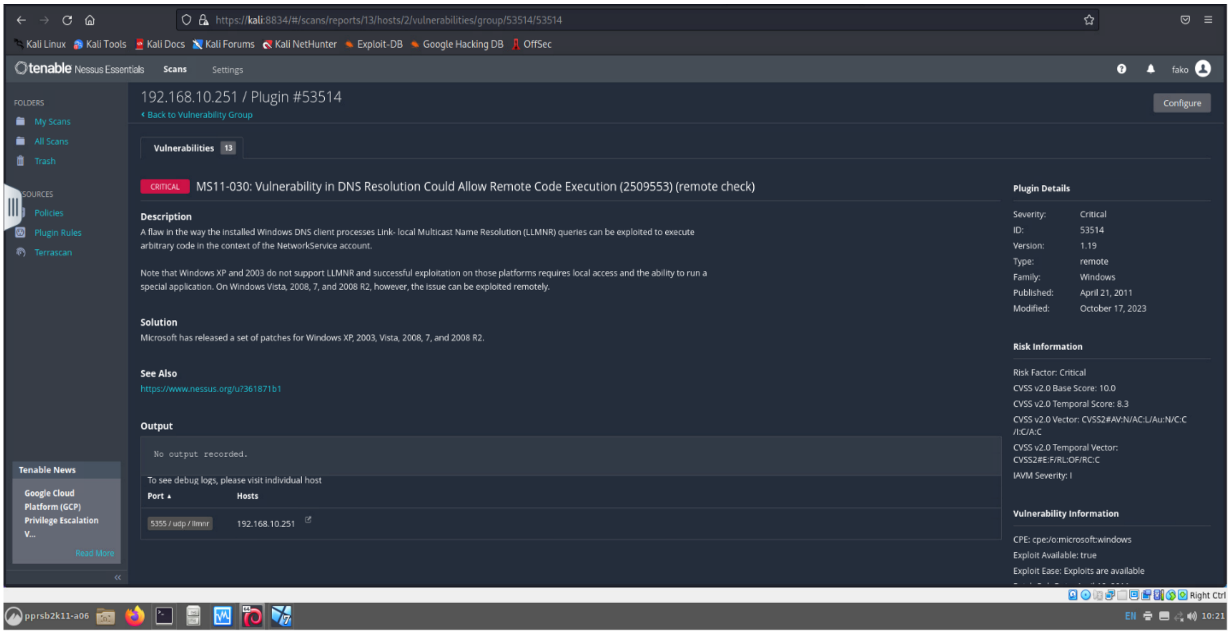
In this scenario, a malicious actor can intercept **LLMNR** requests and respond as if they are the intended destination. This allows them to capture NTLMv2 hashes, which can be cracked offline or used in relay attacks to gain unauthorized access to systems. Attackers commonly use this method for credential theft and privilege escalation within a network.

To mitigate this risk, it is essential to disable LLMNR, NetBIOS Name Service (NBT-NS) and upgrade to a higher windows version. If left unaddressed, this vulnerability leaves the network open to man-in-the-middle attacks and potential lateral movement by threat actors.

3. Results and Mitigation Recommendations

3.1 Vulnerability Severity and Impact Assessment

The most important discovery in this evaluation is the **LLMNR DNS RCE** vulnerability, which might enable remote execution of arbitrary code by attackers, because the system may be accessed over open UDP Port 53 and 5355, this vulnerability is very easily exploited (See Figure 3.1). The system's attack surface is further expanded by other flaws including out-of-date software and lax access controls.



192.168.10.251 / Plugin #53514

‹ Back to Vulnerability Group

CRITICAL MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

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.

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

See Also

https://www.nessus.org/u?361871b1

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
5355 / udp / llmnr	192.168.10.251

Plugin Details

Severity:	Critical
ID:	53514
Version:	1.19
Type:	remote
Family:	Windows
Published:	April 21, 2011
Modified:	October 17, 2023

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available

Figure 3.1: Vulnerability report 2

3.2 Mitigation and Recommendations

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

Patching the OS and core services (e.g., DNS, SMB) needs to be done quickly to close up high-risk vulnerabilities. MS11-030 and others like it that are vulnerable to remote execution are examples. Microsoft has 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: High

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

Using firewall filters, it sends DNS queries to approved internal servers. This stops spoofing/redirection attacks and makes unapproved name resolution routes inaccessible.

Impact: Minimal; enhances visibility and management of the network.