**VULNERABILITY ASSESMENT REPORT **

Name:Aparna Sajeevan

Cyber Security and Ethical HAcking

Project: **1**

Target: Windows 7 Professional VM
Assessment conducted from: Kali Linux VM

Date: 2025-12-02

Table of Contents

1. Introduction

This report documents a vulnerability assessment conducted on a Windows 7 Professional virtual machine using Kali Linux. The goal is to identify potential vulnerabilities that could be exploited by attackers and to provide recommendations for improving system security.

2. Scope and Objectives

Scope:

- **Target: Windows 7 Professional VM**
- **Assessment performed from Kali Linux VM**
- **Only scanning and non-intrusive vulnerability scripts used**

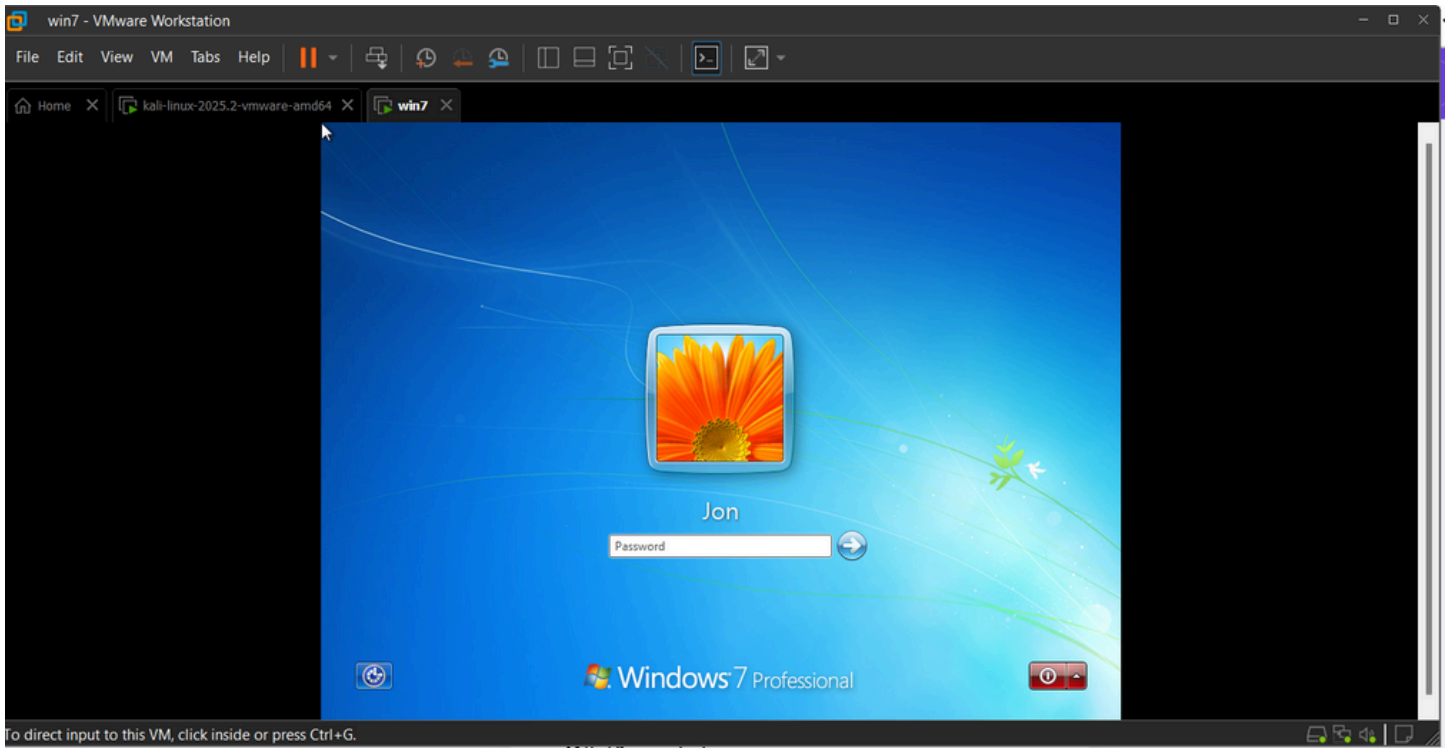
Objectives:

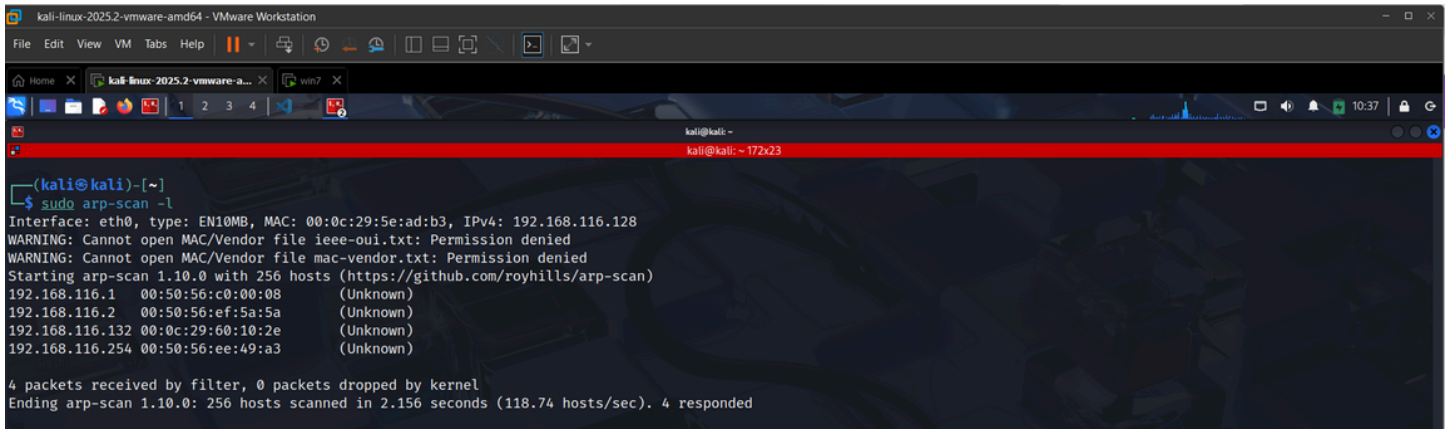
- **Identify live hosts**
- **Detect open ports and running services**
- **Determine the operating system**
- **Identify potential vulnerabilities using Nmap scripts**
- **Document findings for educational purposes**

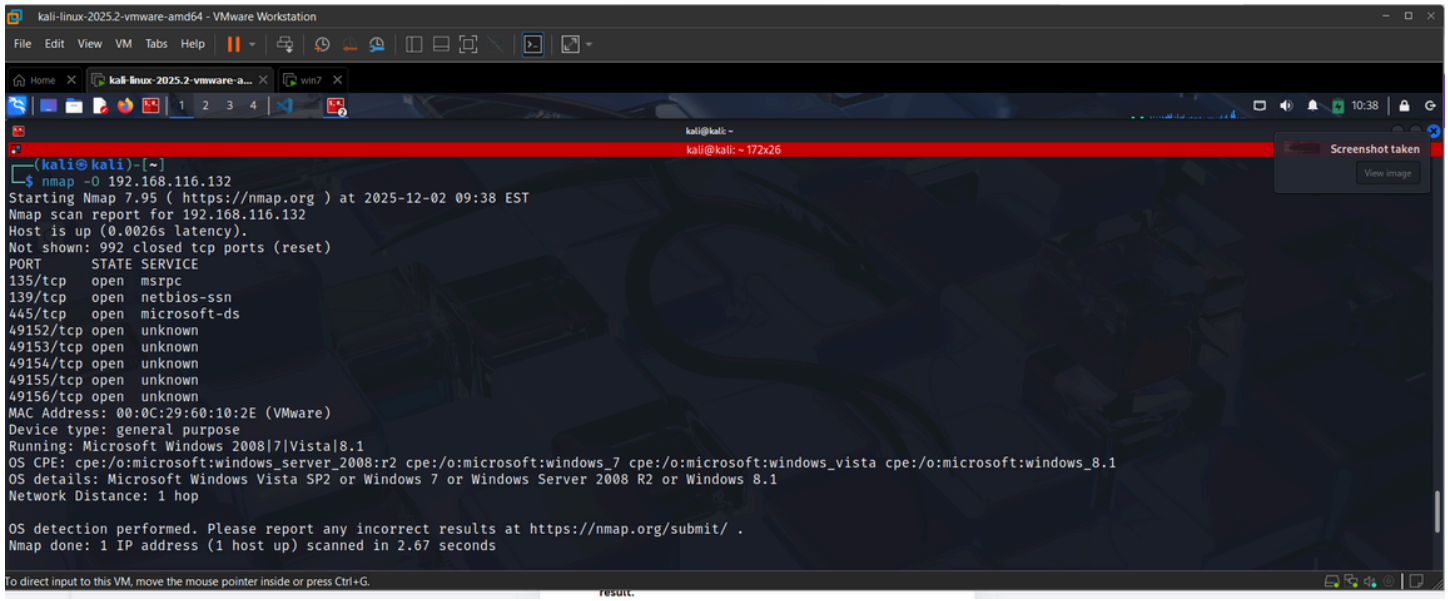
3. Lab Setup

- **Target VM: Windows 7 Professional**
- **Attacker VM: Kali Linux**

- **Network configuration: NAT network to allow VM communication**
- **Tools used: Nmap, Canva**



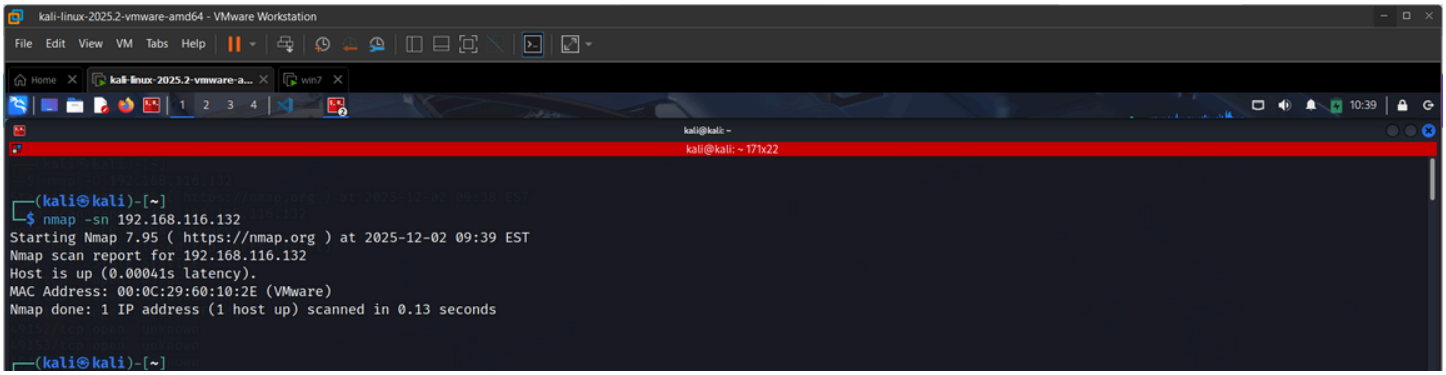




4. Methodology

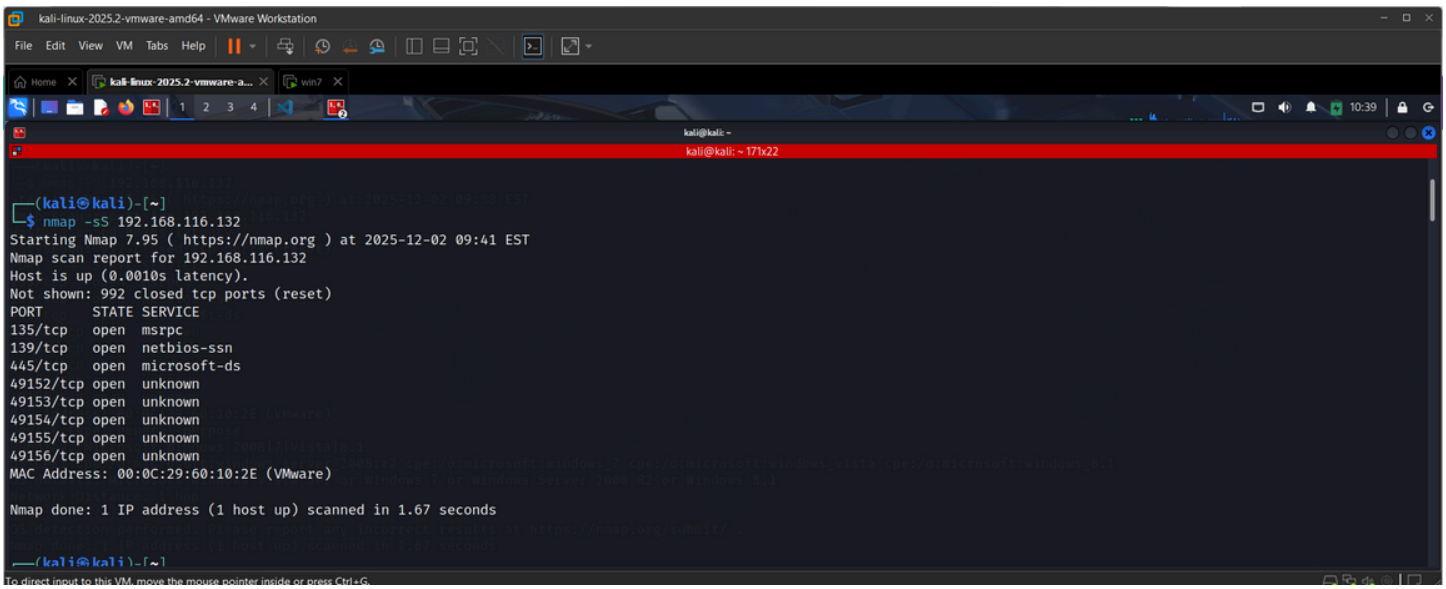
4.1 Host Discovery (-sn)

- **Command used: nmap -sn <192.168.116.132 >**
- **Purpose: Verify that the target host is reachable on the network.**



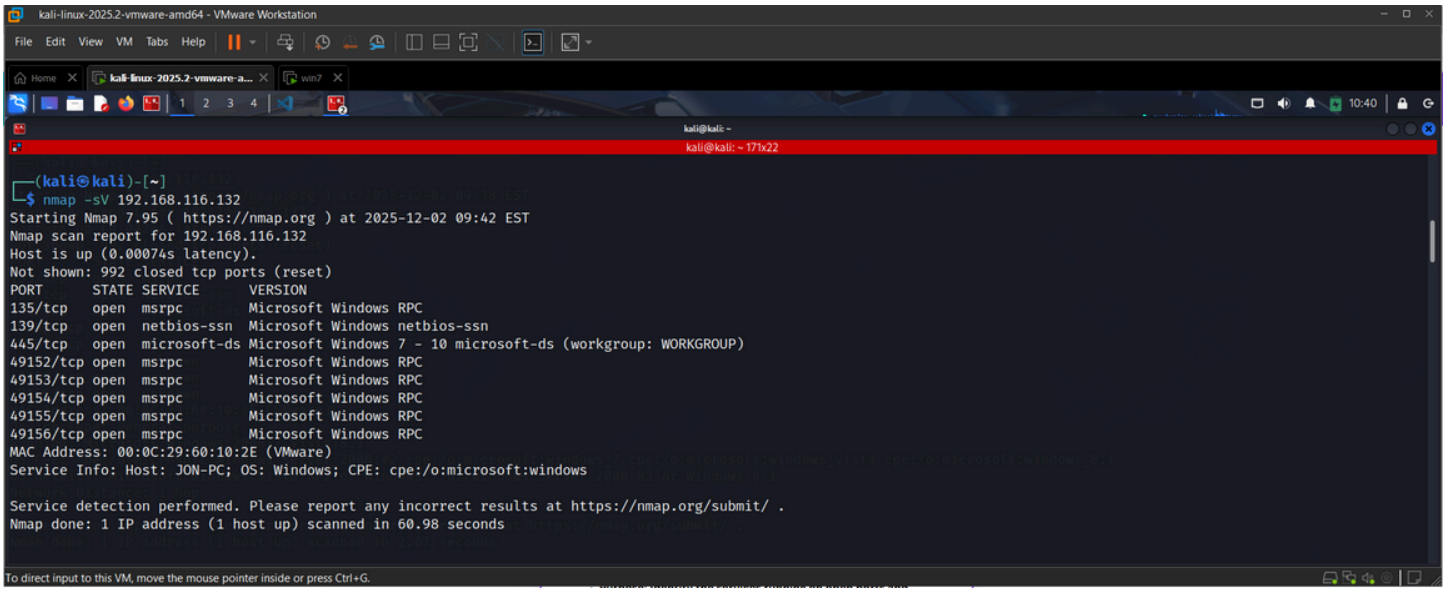
4.2 Port Scanning (-sS)

- **Command used: nmap -sS <192.168.116.132 >**
- **Purpose: Identify open TCP ports that may expose services to attackers.**



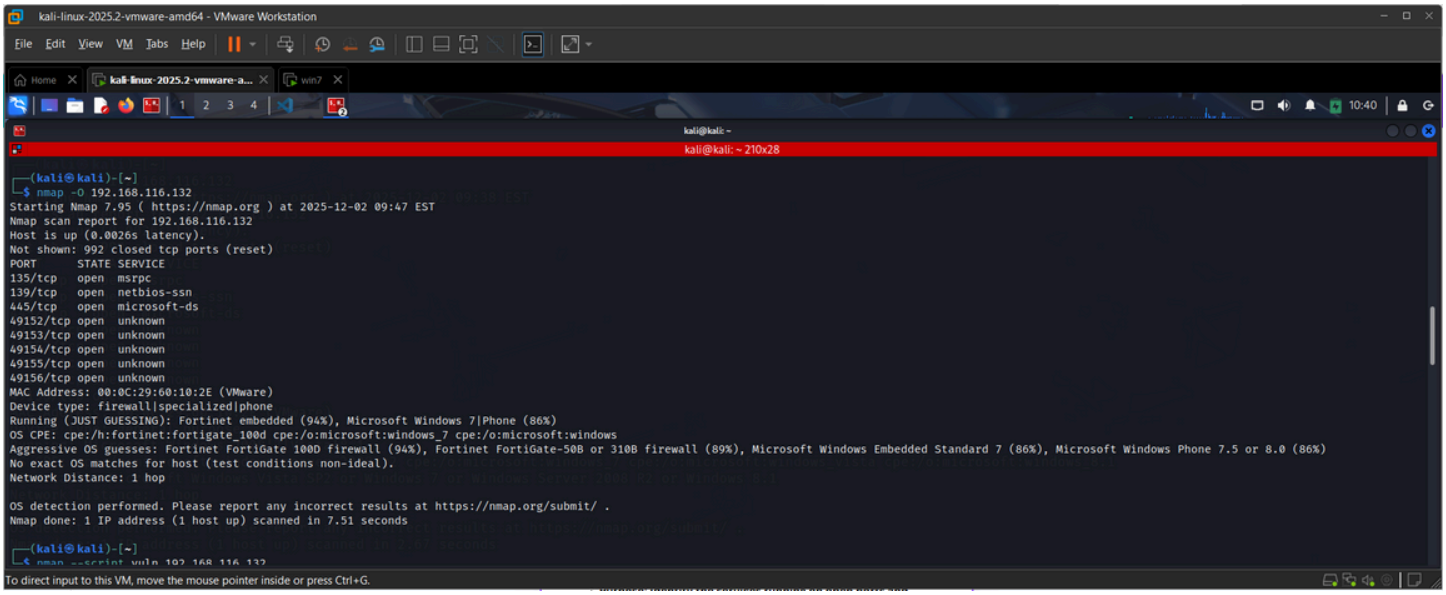
4.3 Service & Version Detection (-sV)

- **Command used: nmap -sV <192.168.116.132 >**
- **Purpose: Identify the services running on open ports and their versions.**



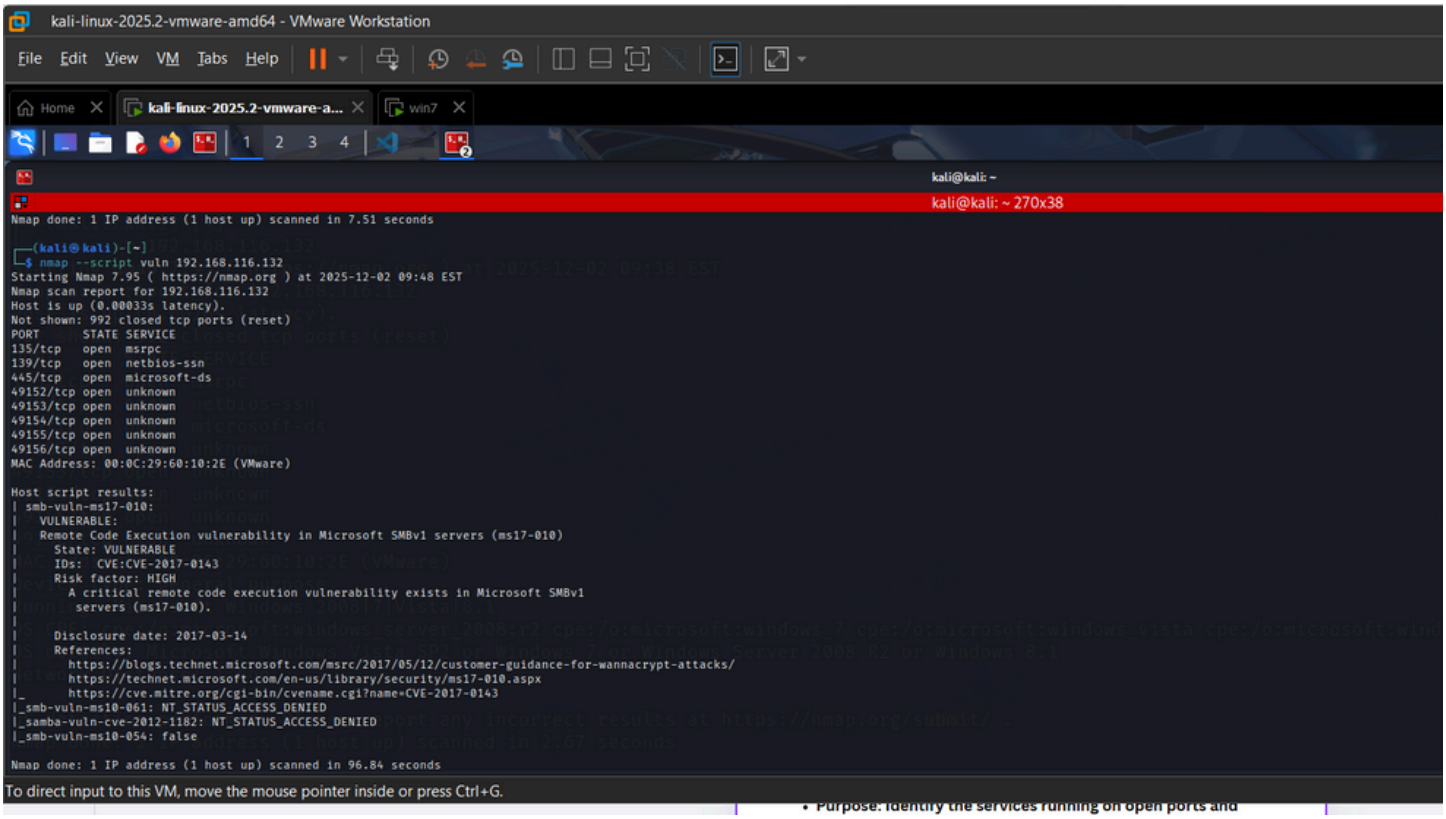
4.4 OS Detection (-O)

- **Command used: nmap -O <192.168.116.132 >**
- **Purpose: Determine the operating system of the target, useful for OS-specific vulnerability assessment.**



4.5 Nmap Vulnerability Scripts (--script vuln)

- **Command used: nmap --script vuln <192.168.116.132 >**
- **Purpose: Automatically detect known vulnerabilities and misconfigurations.**



5. Results

5.1 Host Discovery

- **Target IP: 192.168.116.132**
- **Host is online**

5.2 Open Ports

Port	Service	State	Notes
135	MSRPC	Open	Windows RPC
139	NetBIOS	Open	File and printer sharing
445	SMB	Open	Microsoft-DS, vulnerable service
49152–49156	MSRPC	Open	Dynamic RPC ports

5.3 Service Versions

Port	Service	Version	Notes
135	MSRPC	Microsoft Windows RPC	-
139	NetBIOS	Microsoft Windows netbios-ssn	-
445	SMB	Windows 7 Professional microsoft-ds	Vulnerable to MS17-010

5.4 OS Detection

- **Detected OS: Windows 7 Professional SP1**
- **Device type: firewall/specialized/Windows**

5.5 Vulnerabilities Found

- **MS17-010 (EternalBlue) — HIGH RISK**
  - **SMBv1 vulnerability allowing remote code execution**
  - **CVE: CVE-2017-0143**
- **SMB signing disabled (dangerous default)**
- **Guest account enabled**

6. Analysis

- **Windows 7 is unsupported, increasing security risk**
- **SMBv1 enabled is highly vulnerable**
- **Open RPC ports expand the attack surface**
- **Safe scanning confirms critical vulnerabilities without performing attacks**

7. Recommendations

1. **Patch system: Apply MS17-010 patch or upgrade OS**
2. **Disable SMBv1**
3. **Enable SMB signing**
4. **Restrict RPC/NetBIOS ports via firewall**
5. **Limit guest account access**
6. **Consider upgrading to a supported OS (Windows 10 or 11)**

8. Conclusion

The vulnerability assessment successfully identified critical vulnerabilities on Windows 7 VM. MS17-010 represents a severe risk and illustrates why outdated OS and services must be patched. Applying recommended measures will significantly reduce potential exposure.