

# **\*\*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**

## **2. Scope and Objectives**

## **3. Methodology**

- **3.1 Host Discovery (-sn)**
- **3.2 Port Scanning (-sS)**
- **3.3 Service & Version Detection (-sV)**
- **3.4 OS Detection (-O)**
- **3.5 Nmap Vulnerability Scripts (--script vuln)**

## **4. Results**

- **4.1 Host Discovery**
- **4.2 Open Ports**
- **4.3 Service Versions**
- **4.4 OS Detection**
- **4.5 Vulnerabilities Found**

## **5. Analysis**

## **6. Recommendation**

## **7. Conclusion**

## **8. References**

## **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**

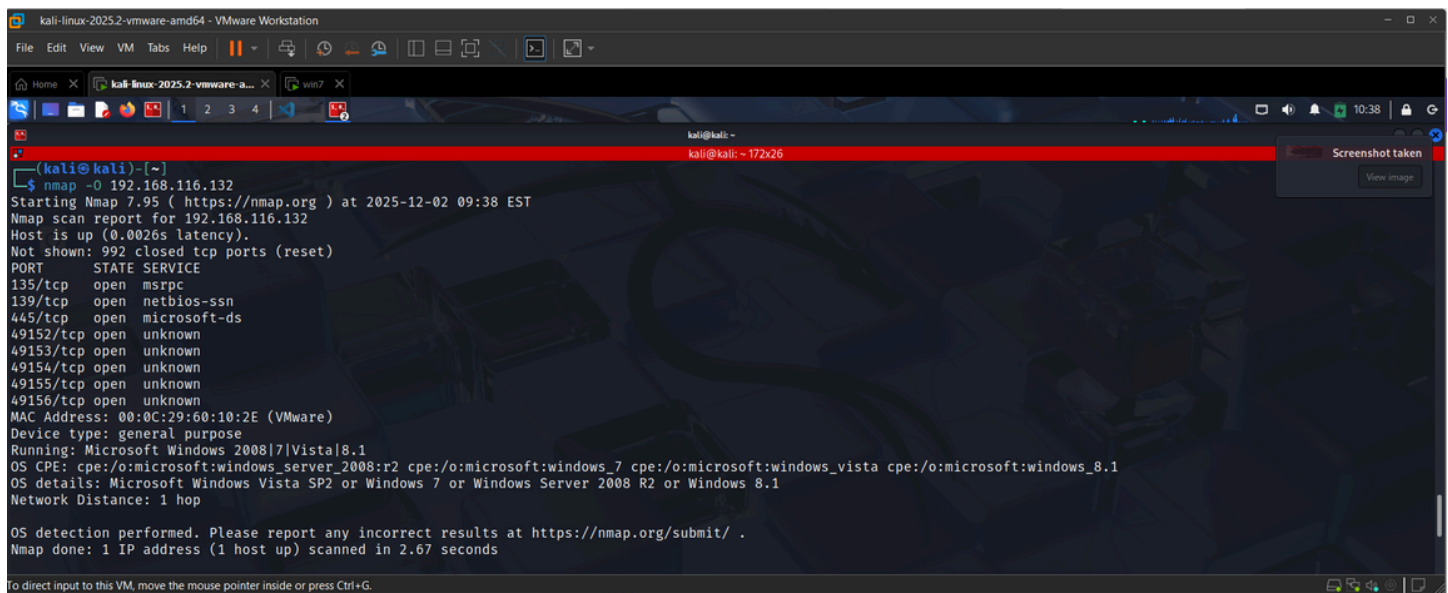
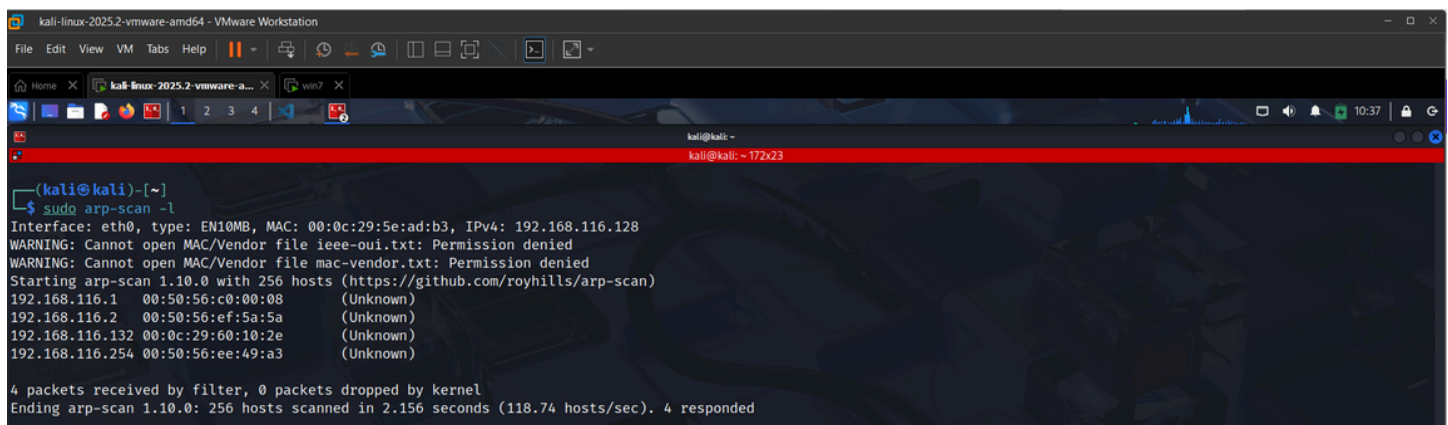
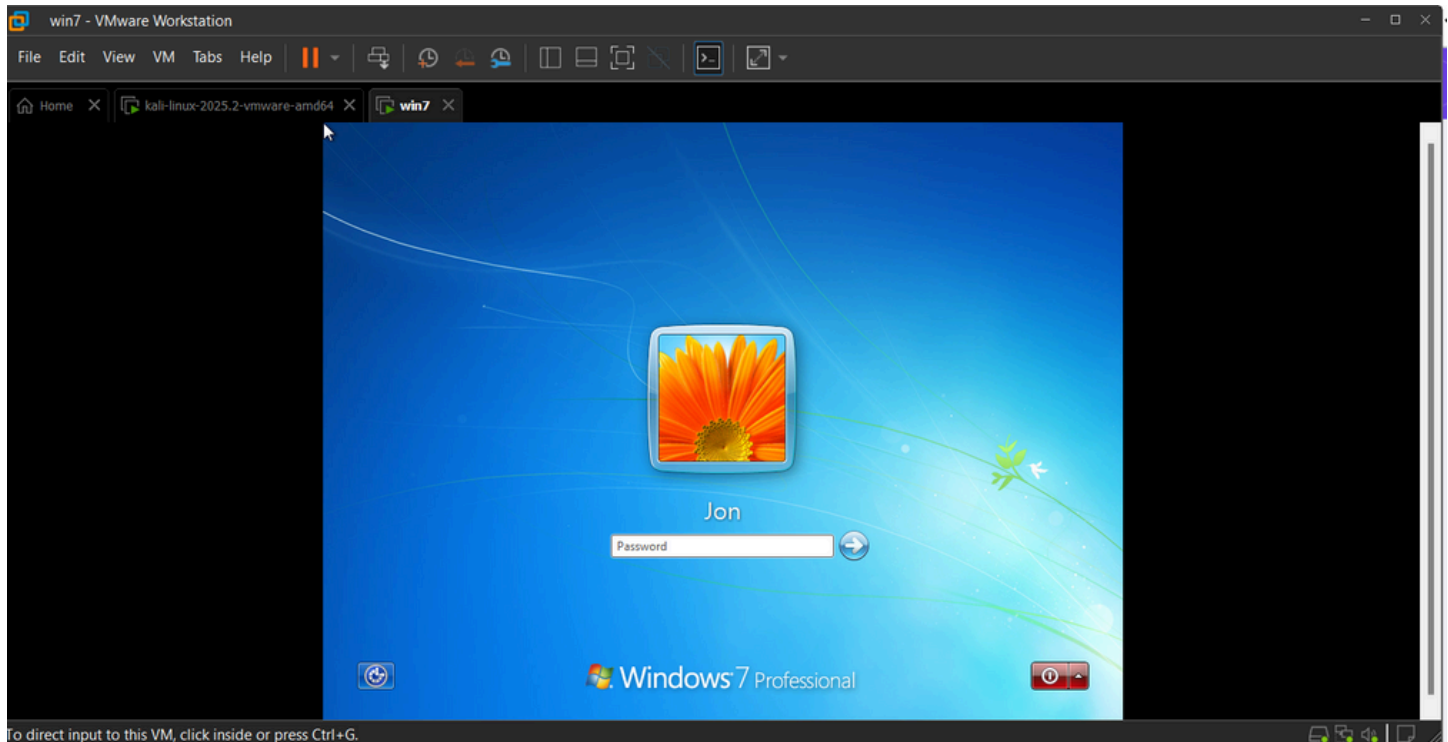
### **Objectives:**

- **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**

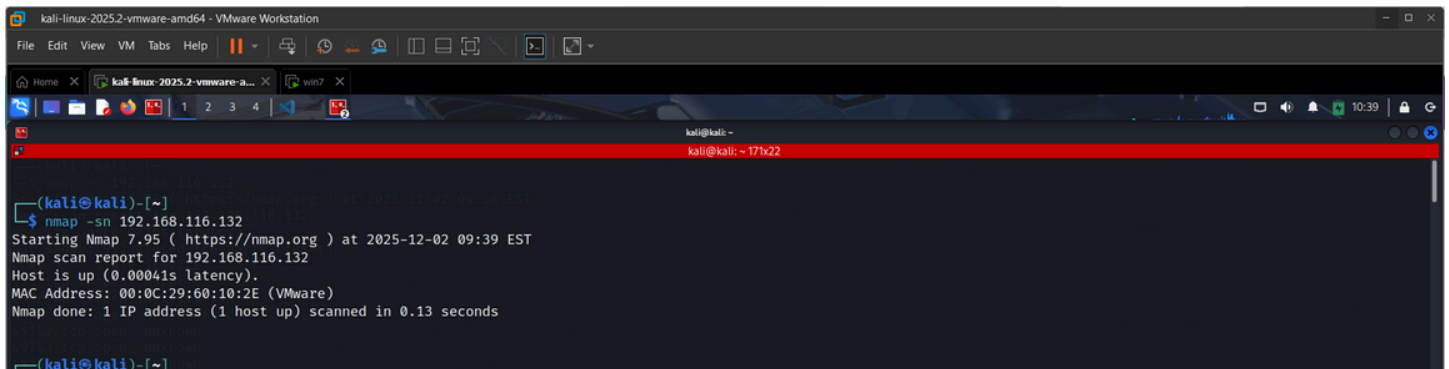
- **Network configuration: NAT network to allow VM communication**
- **Tools used: Nmap, Canva**



## 4. Methodology

### 4.1 Host Discovery (-sn)

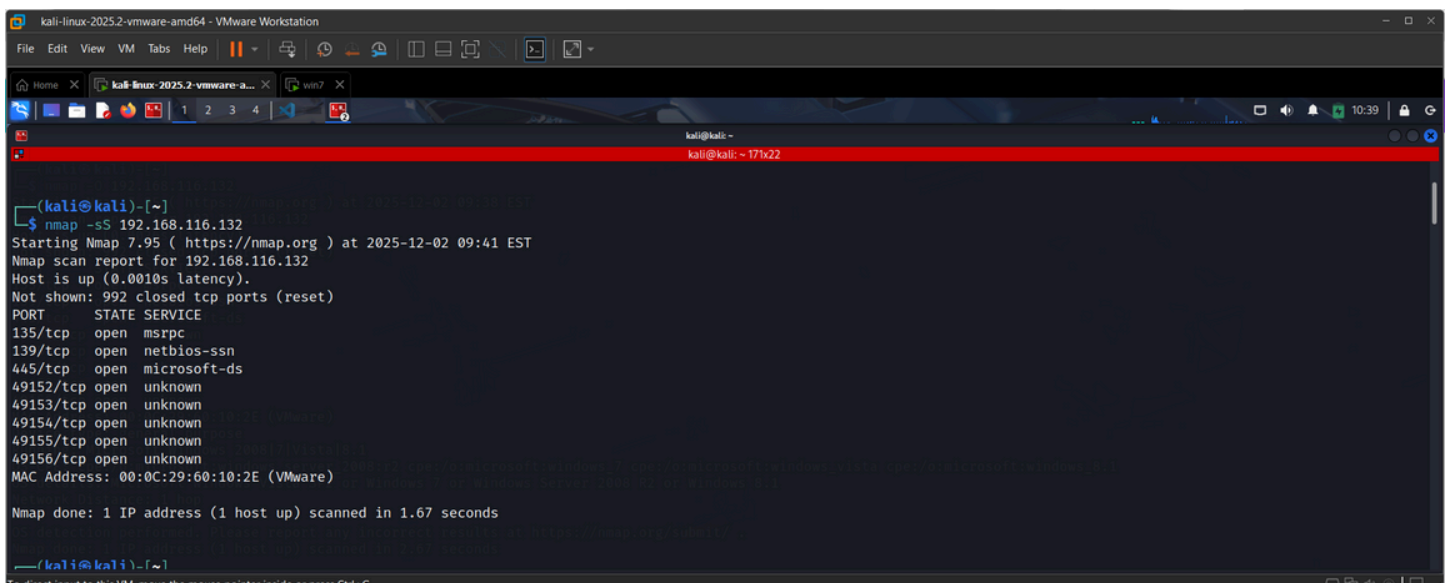
- **Command used:** `nmap -sn <192.168.116.132 >`
- **Purpose:** Verify that the target host is reachable on the network.



```
kali@kali: ~  
$ nmap -sn 192.168.116.132  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 09:39 EST  
Nmap scan report for 192.168.116.132  
Host is up (0.00041s latency).  
MAC Address: 00:0C:29:60:10:2E (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

### 4.2 Port Scanning (-sS)

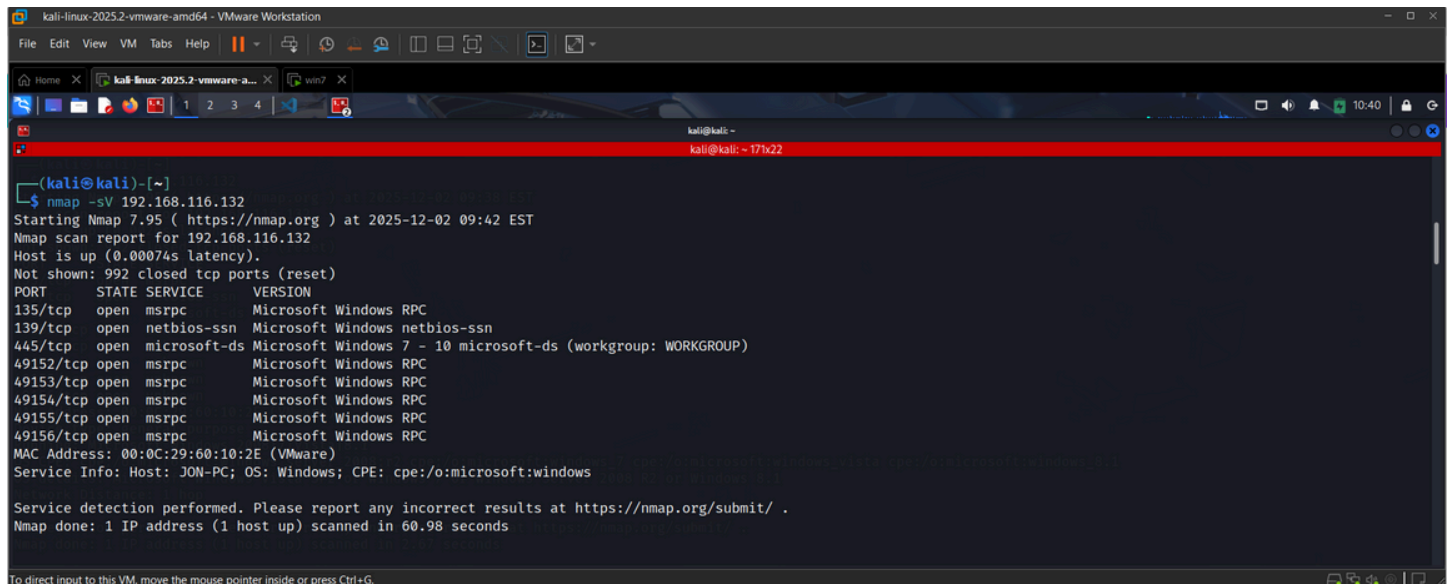
- **Command used:** `nmap -sS <192.168.116.132 >`
- **Purpose:** Identify open TCP ports that may expose services to attackers.



```
kali@kali: ~  
$ nmap -sS 192.168.116.132  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 09:41 EST  
Nmap scan report for 192.168.116.132  
Host is up (0.0010s latency).  
Not shown: 992 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
MAC Address: 00:0C:29:60:10:2E (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

## 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.

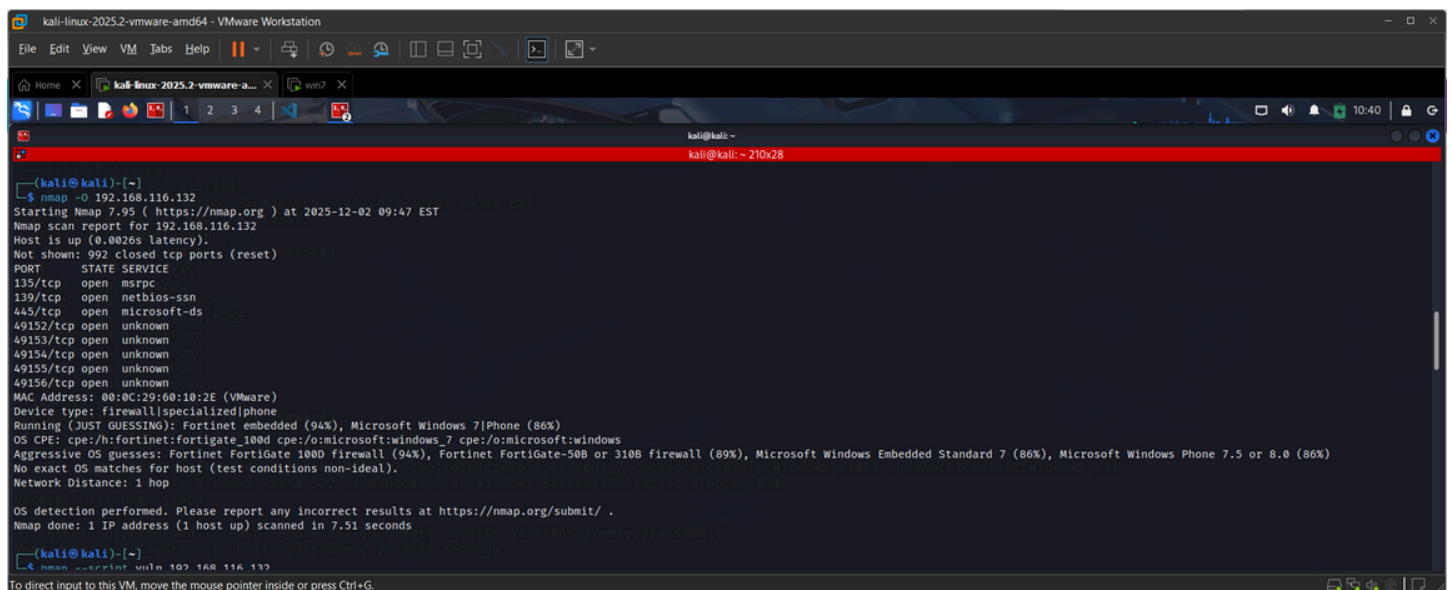


```
(kali@kali)-[~]
$ nmap -sV 192.168.116.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 09:42 EST
Nmap scan report for 192.168.116.132
Host is up (0.00074s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49156/tcp open  msrpc            Microsoft Windows RPC
MAC Address: 00:0C:29:60:10:2E (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.98 seconds
```

## 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.



```
(kali@kali)-[~]
$ nmap -O 192.168.116.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 09:47 EST
Nmap scan report for 192.168.116.132
Host is up (0.0026s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:60:10:2E (VMware)
Device type: firewall|specialized phone
Running (JUST GUESSING): Fortinet embedded (94%), Microsoft Windows 7/Phone (86%)
OS CPE: cpe:/h:fortinet:fortigate_1000 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
Aggressive OS guesses: Fortinet FortiGate 1000 firewall (94%), Fortinet FortiGate-50B or 310B firewall (89%), Microsoft Windows Embedded Standard 7 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds

(kali@kali)-[~]
$ nmap --script vuln 192.168.116.132
```

## 4.5 Nmap Vulnerability Scripts (--script vuln)

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

```

kali@kali: ~
kali@kali: ~ 270x38

Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds

(kali@kali)-[~]
$ nmap --script vuln 192.168.116.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 09:48 EST
Nmap scan report for 192.168.116.132
Host is up (0.00033s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 00:0C:29:60:10:2E (VMware)

Host script results:
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
Nmap done: 1 IP address (1 host up) scanned in 96.84 seconds

```

• Purpose: Identify the services running on open ports and

## 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.**