

# **Vulnerability Assessment Scan Report on a windows machine Using **Nmap and Nessus.****

**IP Address: 10.0.2.5**

**Prepared by: Temilola Babalola**

**Date: 19<sup>th</sup> June, 2025**

## Table of Contents

Executive summary .....	3
Objective .....	4
Nmap Scan Report .....	5
Findings from Nmap scan on 10.0.2.5 .....	6
Nessus findings .....	8
Analysis & Recommendations: .....	11
Conclusion.....	12

## Executive summary

This report presents the findings of a penetration testing scan performed on a Kali machine with the IP address **10.0.2.5**. The assessment was conducted using **Nmap** and **Nessus**, which were leveraged to gather a wide range of security-related information about the target system.

The objective of the scan was to identify **open ports, running services, known vulnerabilities**, and other potential security risks that could be exploited by malicious actors.

The results indicate that the target system is **highly vulnerable**, with multiple outdated services running — some of which have publicly known exploits. These weaknesses pose a significant risk and could be used as entry points for attacks.

## Objective

The goal of this assessment is to evaluate the security exposure of a **Windows 7 machine** (IP: 10.0.2.5) using **Nmap** and **Nessus**.

- **Nmap** was used to detect open ports, running services, OS type, and run basic vulnerability scripts.
- **Nessus** was used to identify known vulnerabilities, misconfigurations, and assign severity ratings.

Together, the tools simulate attacker behavior to uncover risks and support proactive system hardening.

# Nmap Scan Report

Scan Command Used

**Nmap -A -p- 10.0.2.5**

This is a **powerful Nmap scan** that provides **detailed information** about a target machine (10.0.2.5). Here's what each flag does:

## Breaking it Down:

1. **Nmap** → Calls the **Nmap** tool, which is used for network scanning and security auditing.
2. **-A (Aggressive Scan)** → Enables multiple advanced features, including:
  - OS detection
  - Version detection
  - Script scanning
  - Traceroute
3. **-p- (Scan All Ports)** → Scans **all 65,535 TCP ports** instead of just the default 1,000.
4. **10.0.2.5** → The target IP address being scanned.

## How It Helps in a Vulnerability Scan:

- **Identifies Open Ports** → Shows which services are running and where vulnerabilities might exist.
- **Detects Running Services & Versions** → Helps find outdated or misconfigured services.
- **Finds OS & System Info** → Useful for fingerprinting a system to tailor attacks or defenses.
- **Performs Traceroute** → Helps map out the network for possible attack paths.

## Findings from Nmap Scan on 10.0.2.5

### General Information:

- **Target IP:** 10.0.2.5
- **Host is up:** 0.00053s latency.
- **Operating System:** Microsoft windows 7
- **Network Distance:** 1 hop
- **MAC Address:** MAC Address: 08:00:27: 5D:4F:BD
- **Hostname:** SecOps

```
(kali㉿kali)-[~]  
$ nmap -A -p- 10.0.2.5  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 08:16 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.00072s latency).  
Not shown: 65534 filtered tcp ports (no-response)
```

Scan indicate that 65534 filtered tcp ports has no response and only 445/tcp is open

```
Not shown: 65534 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: SECOPS)  
MAC Address: 08:00:27:5D:4F:BD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

### Open Ports and Services:

#### SMB (Port 445)

- Service: Microsoft-ds (Windows SMB)
- Notes: Running on a VirtualBox VM NIC
- Vulnerability Scan Results:
  - MS10-054: Not vulnerable
  - Other SMB vulnerabilities: Could not test due to lack of valid SMB credentials
- Recommendation: Use valid credentials for deeper scans; ensure SMB is patched and secured

```
(kali㉿kali)-[~]  
$ nmap --script vuln -p445 10.0.2.5  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 08:39 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.0084s latency).  
  
PORT      STATE SERVICE  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:5D:4F:BD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Host script results:  
|_samba-vuln-cve-2012-1182: No accounts left to try  
|_smb-vuln-ms10-054: false  
|_smb-vuln-ms10-061: No accounts left to try  
  
Nmap done: 1 IP address (1 host up) scanned in 15.52 seconds
```

# Findings from Nessus

8ate / Plugin #88561

[Back to Vulnerabilities](#)

Vulnerabilities16

CRITICAL

Microsoft Windows 8 Unsupported Installation Detection

Description

The remote host is running Microsoft Windows 8. Support for this operating system by Microsoft ended January 12th, 2016.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

Solution

Upgrade to a version of Microsoft Windows that is currently supported.

See Also

<https://support.microsoft.com/en-us/help/18581/lifecycle-faq-windows-products>

Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	10.0.2.5

8ate / 10.0.2.5 / Microsoft Windows (Multiple Issues)

[Back to Vulnerabilities](#)

Vulnerabilities16

Search Vulnerabilities

2 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲
<input type="checkbox"/>	CRITICAL	10.0			Unsupported Windows OS (remote)	Windows
<input type="checkbox"/>	INFO				WMI Not Available	Windows



ans  
ns  
  
s  
Rules  
can  
  
  
ews

8ate / Plugin #108797

[← Back to Vulnerability Group](#)

Vulnerabilities16

CRITICAL

Unsupported Windows OS (remote)

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a supported service pack or operating system

See Also

<https://support.microsoft.com/en-us/lifecycle>

Output

The following Windows version is installed and not supported:

Microsoft Windows 8 Pro

To see debug logs, please visit individual host

Port ▲

Hosts

N/A

10.0.2.5

## 8ate / Plugin #57608

[← Back to Vulnerability Group](#)

Vulnerabilities **16**

### MEDIUM SMB Signing not required

#### Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

#### Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

#### See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>


<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

#### Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	10.0.2.5 

# Analysis & Recommendations

## Analysis

- The target system has minimal open ports, which reduces the attack surface. However, the presence of an open SMB port (445) poses a significant risk due to its historical exploitation in Windows systems.
- The OS detection as Windows 7 is important because Microsoft officially ended mainstream support for Windows 7, meaning no security updates are issued, exposing the system to unpatched vulnerabilities.
- The scan results indicate most ports are filtered, which could be due to a firewall or security appliance, but further validation is recommended.
- Lack of credentials for SMB limits the depth of vulnerability scanning; credentials would enable authenticated scans revealing additional risks.

## Recommendations

1. **Patch Management:**
  - Upgrade the operating system to a supported version such as Windows 10 or 11.
  - Ensure all Windows updates and security patches are applied regularly.
2. **SMB Security:**
  - Restrict SMB access to trusted internal networks only.
  - Use strong credentials and enable SMB signing to prevent man-in-the-middle attacks.
  - Consider disabling SMBv1 if it is still enabled, as it is deprecated and vulnerable.
3. **Network Hardening:**
  - Implement firewall rules to block unnecessary inbound and outbound traffic.
  - Use network segmentation to isolate critical assets.
4. **Credentialed Scanning:**
  - Use valid credentials during vulnerability scans to uncover deeper security issues on SMB and other services.
5. **Use Additional Tools:**
  - Employ Nessus to complement findings from Nmap and Nikto by performing detailed vulnerability and compliance checks.
  - Run Nikto scans on hosted web servers to detect web application vulnerabilities (not covered here as the machine is Windows desktop).

## **Conclusion**

The vulnerability assessment shows the target Windows 7 machine running with limited open ports but exposing SMB on port 445, which presents a security risk if left unpatched or unsecured. Upgrading the OS, applying patches, restricting SMB, and conducting credentialed scans are critical next steps to improve the security posture.

Continuous monitoring and regular vulnerability assessments using multiple tools such as Nmap, and Nessus are recommended to maintain system security over time.