Nessus Vulnerability Scan – Step-by-Step Guide (Target: 10.0.3.4 Windows PC)

Scope: Unauthenticated (basic network) vulnerability scan against a Windows host at 10.0.3.4 from a Kali Linux Nessus scanner.

1. Prerequisites and lab setup

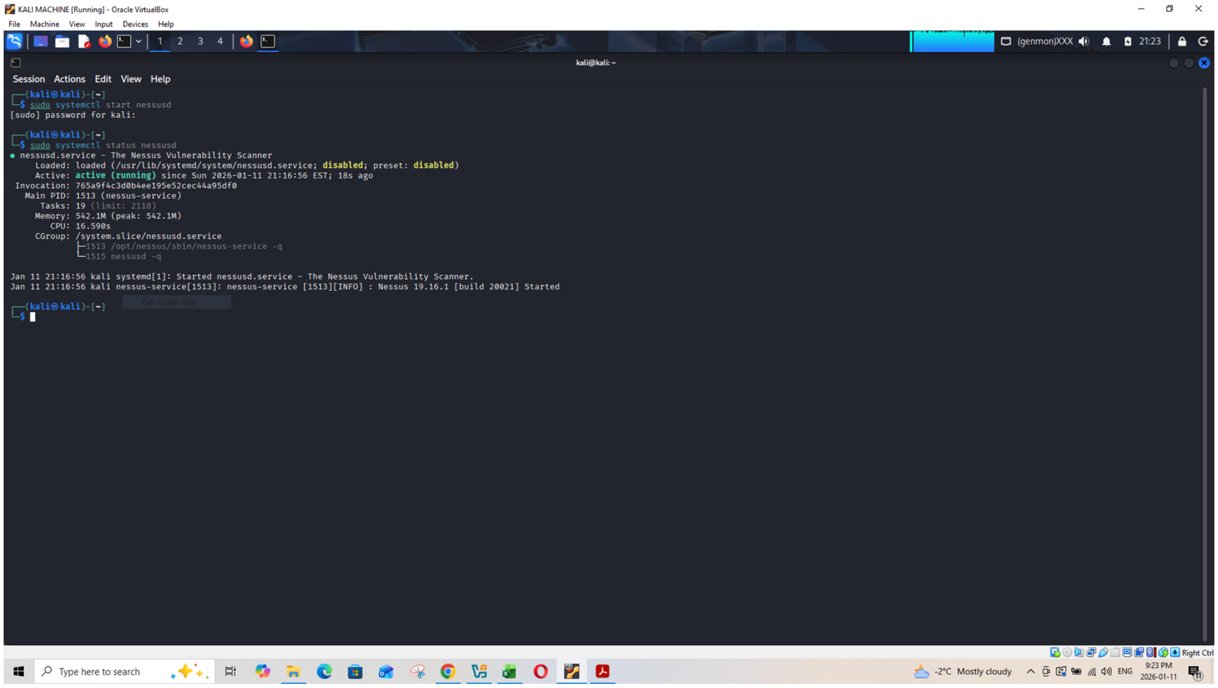
Before scanning, confirm the following:

- Nessus is installed on the scanner machine (Kali Linux VM).
- The target Windows PC is reachable on the network at 10.0.3.4 (same network segment/subnet as the scanner).
- You have permission to scan the target system.
- If you want deeper results (patch level, local checks), prepare valid Windows credentials for a credentialed scan.

2. Start and verify the Nessus service (Kali)

On Kali, start the Nessus daemon and confirm it is running:

```
sudo systemctl start nessusd
sudo systemctl status nessusd
```



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Sun 2026-01-11 21:16:56 EST; 18s ago
 Invocation: 765a9f4c3d0b4ee195e52cec44a95df0
   Main PID: 1513 (nessus-service)
      Tasks: 19 (limit: 2118)
     Memory: 542.1M (peak: 542.1M)
        CPU: 16.590s
     CGroup: /system.slice/nessusd.service
             ├─1513 /opt/nessus/sbin/nessus-service -q
             └─1515 nessusd -q

Jan 11 21:16:56 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Jan 11 21:16:56 kali nessus-service[1513]: nessus-service [1513][INFO] : Nessus 19.16.1 [build 20021] Started

┌──(kali㉿kali)-[~]
└─$ 
```

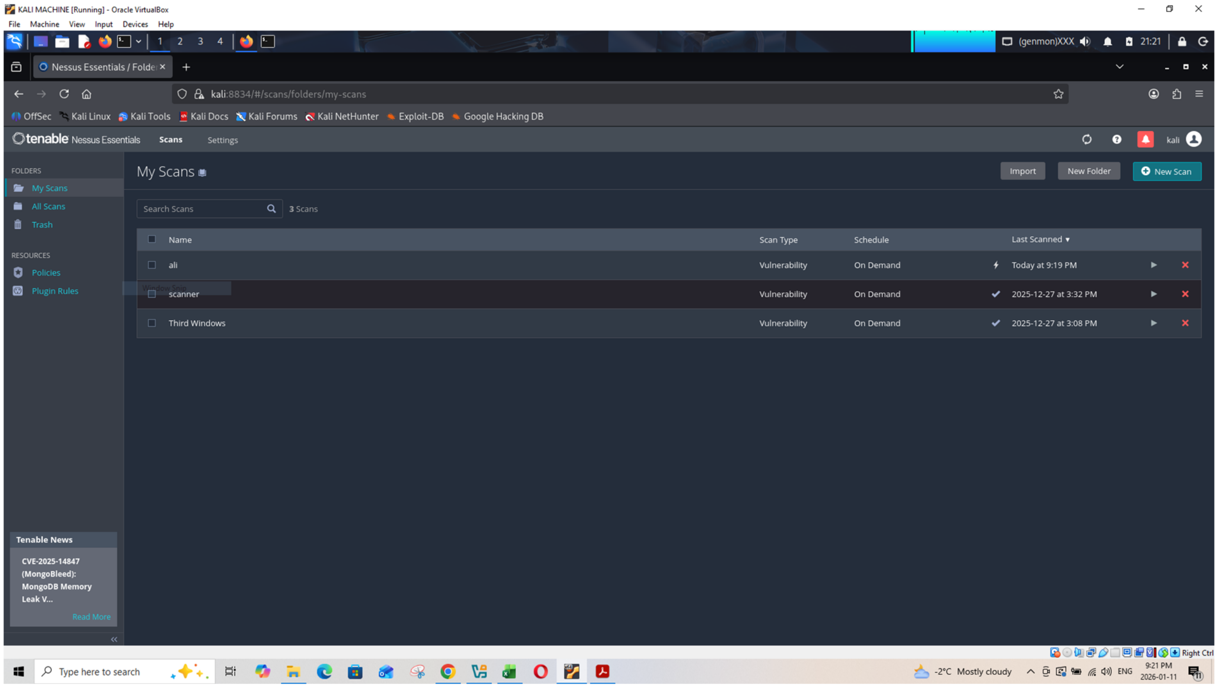
Figure 1: Starting and verifying the nessusd service on Kali (systemctl status shows active/running).

3. Open the Nessus web interface

In a browser on the Kali VM, open Nessus at:

```
https://kali:8834
```

Log in to your Nessus account to access the scanning dashboard (Scans > My Scans).



kali:8834/#/scans/folders/my-scans

My Scans

3 Scans

Name	Scan Type	Schedule	Last Scanned ▾
ali	Vulnerability	On Demand	Today at 9:19 PM
scanner	Vulnerability	On Demand	2025-12-27 at 3:32 PM
Third Windows	Vulnerability	On Demand	2025-12-27 at 3:08 PM

Tenable News

CVE-2025-14847 (MongoBleed): MongoDB Memory Leak V...

Read More

Figure 2: Nessus Essentials dashboard showing the My Scans folder and existing scans.

4. Create a new vulnerability scan

From the My Scans page:

1. Click New Scan.
2. Select a template. For a basic unauthenticated scan, choose Basic Network Scan.
3. Set the scan Name (example: scanner) and optionally a Description.
4. In Targets, enter the target IP: 10.0.3.4.
5. Leave Schedule as On Demand (or set a schedule if needed).
6. Optional: Add credentials (Windows/SMB) if you want a credentialed scan.
7. Click Save.

5. Launch the scan

To run the scan:

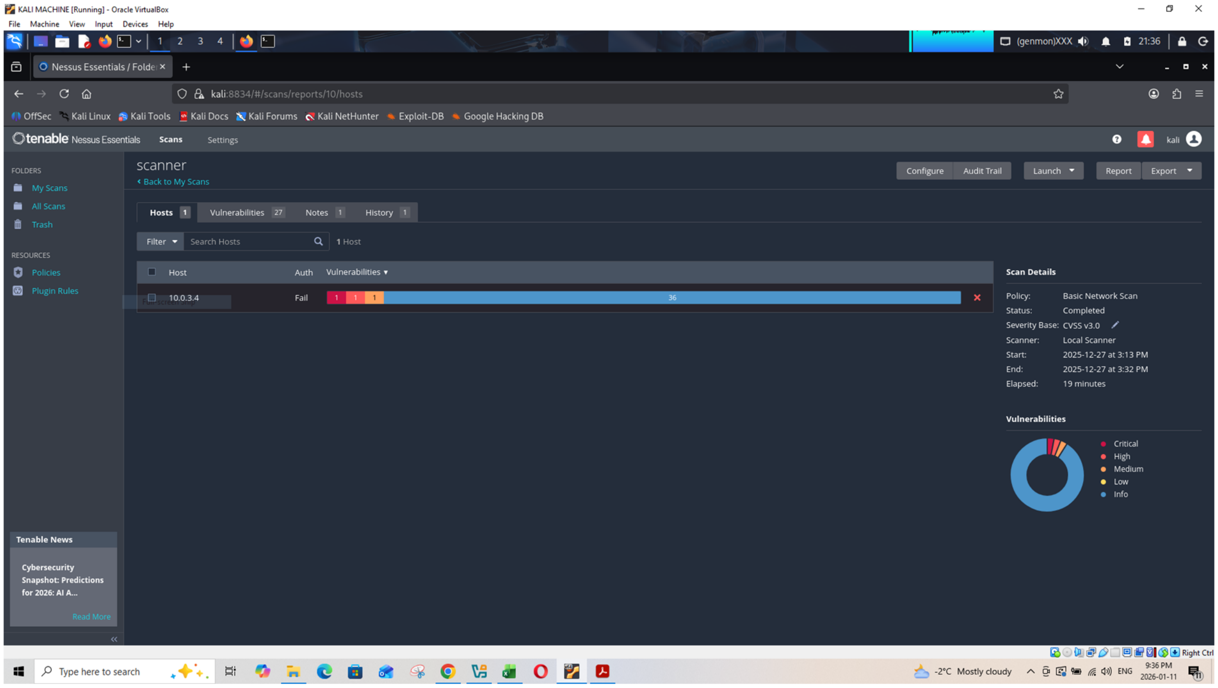
1. Open the saved scan from My Scans.
2. Click Launch (or the play icon) to start scanning.
3. Wait for the scan status to change to Completed.

6. Review results – Hosts view

After the scan completes, open the scan results and review the Hosts tab.

Key things to check on this page:

- Host discovered (10.0.3.4).
- Authentication status (Auth: Fail indicates an unauthenticated scan or credential failure).
- Vulnerability counts by severity.


KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folde
kali:8834/#/scans/reports/10/hosts
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
kali
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Cybersecurity Snapshot: Predictions for 2026: AI A...
Read More
Configure
Audit Trail
Launch
Report
Export
Filter
Search Hosts
Type here to search
-2°C Mostly cloudy
ENG
9:36 PM
2026-01-11
21:36

scanner
‹ Back to My Scans

Hosts 1 | Vulnerabilities 27 | Notes 1 | History 1

1 Host

Host	Auth	Vulnerabilities ▾
10.0.3.4	Fail	1 1 1 36

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: 2025-12-27 at 3:13 PM
End: 2025-12-27 at 3:32 PM
Elapsed: 19 minutes

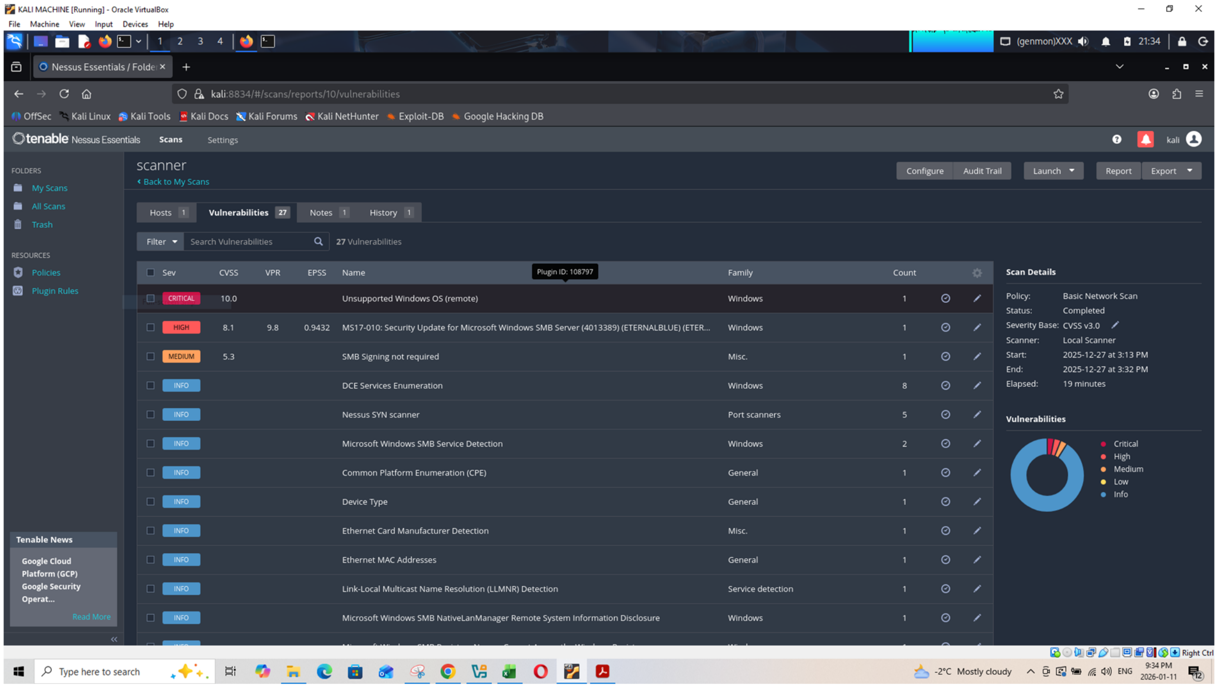
Vulnerabilities

Critical
High
Medium
Low
Info

Figure 3: Hosts tab showing the scanned host (10.0.3.4) and vulnerability distribution; Auth shows Fail (unauthenticated scan).

7. Review results – Vulnerabilities list

Go to the Vulnerabilities tab to see all findings grouped by plugin/vulnerability. Sort by Severity and focus on Critical and High findings first.


KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folde
kali:8834/#/scans/reports/10/vulnerabilities
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
kali
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Google Cloud Platform (GCP) Google Security Operat...
Read More
Configure
Audit Trail
Launch
Report
Export
Filter
Search Vulnerabilities
Plugin ID: 108797
Type here to search
-2°C Mostly cloudy
ENG
9:34 PM
2026-01-11
21:34

scanner
‹ Back to My Scans

Hosts 1 | Vulnerabilities 27 | Notes 1 | History 1

27 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Unsupported Windows OS (remote)	Windows	1
HIGH	8.1	9.8	0.9432	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETER...	Windows	1
MEDIUM	5.3			SMB Signing not required	Misc.	1
INFO				DCE Services Enumeration	Windows	8
INFO				Nessus SYN scanner	Port scanners	5
INFO				Microsoft Windows SMB Service Detection	Windows	2
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
INFO				Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows	1

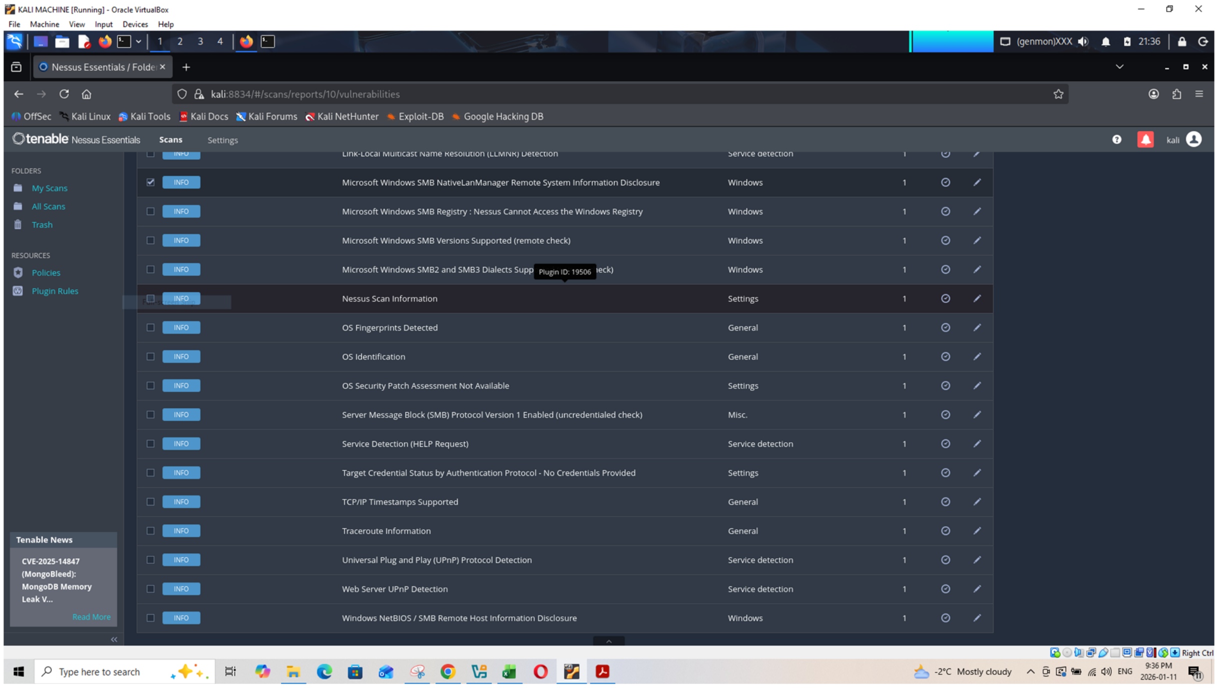
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: 2025-12-27 at 3:13 PM
End: 2025-12-27 at 3:32 PM
Elapsed: 19 minutes

Vulnerabilities

Figure 4: Vulnerabilities tab listing findings with severity, CVSS score, and plugin names.

Scroll to review informational findings (fingerprinting, service detection, protocol support) that help with asset inventory and attack-surface mapping.



☐	INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
☑	INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows	1
☐	INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Windows	1
☐	INFO	Microsoft Windows SMB Versions Supported (remote check)	Windows	1
☐	INFO	Microsoft Windows SMB2 and SMB3 Dialects Supp Plugin ID: 19506 eck)	Windows	1
☐	INFO	Nessus Scan Information	Settings	1
☐	INFO	OS Fingerprints Detected	General	1
☐	INFO	OS Identification	General	1
☐	INFO	OS Security Patch Assessment Not Available	Settings	1
☐	INFO	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	Misc.	1
☐	INFO	Service Detection (HELP Request)	Service detection	1
☐	INFO	Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
☐	INFO	TCP/IP Timestamps Supported	General	1
☐	INFO	Traceroute Information	General	1
☐	INFO	Universal Plug and Play (UPnP) Protocol Detection	Service detection	1
☐	INFO	Web Server UPnP Detection	Service detection	1
☐	INFO	Windows NetBIOS / SMB Remote Host Information Disclosure	Windows	1

Figure 5: Additional INFO-level findings (e.g., OS identification, SMB protocol checks, service detection).

8. Investigate key findings (drill-down into plugin details)

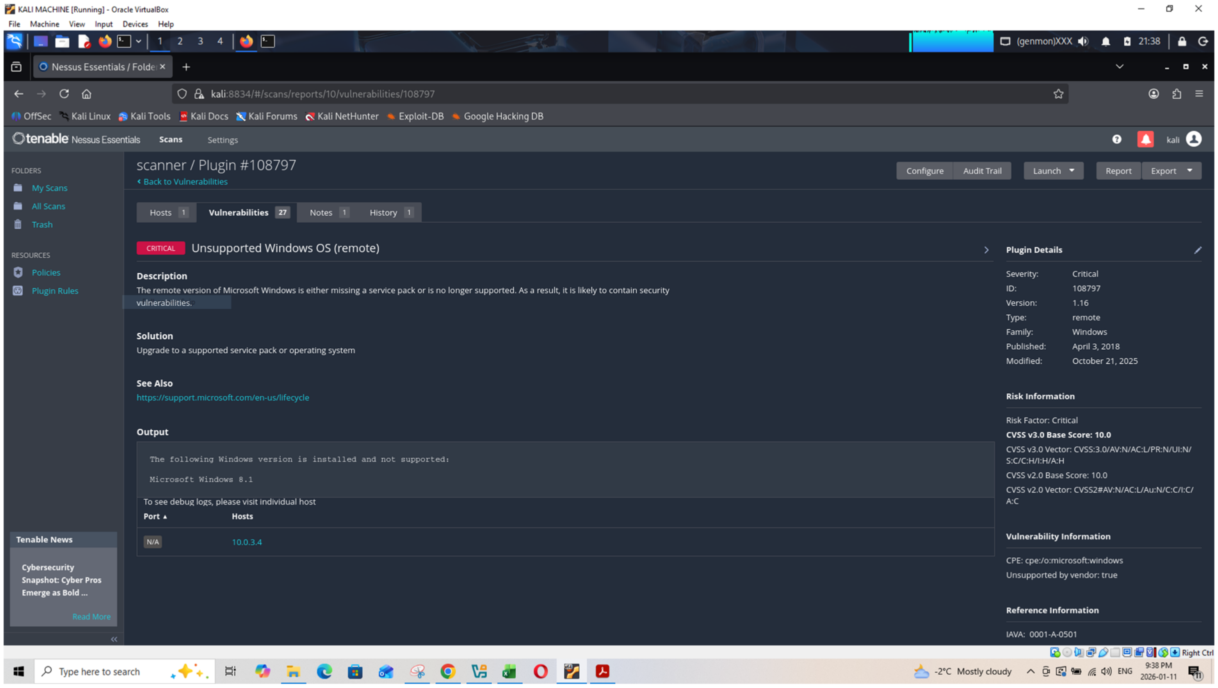
Click any vulnerability name to open its plugin page. This page provides Description, Impact, Evidence/Output, and Remediation guidance.

8.1 Critical: Unsupported Windows OS (remote)

This finding often means the host is running an OS version that is out of support (no longer receives security updates), which increases risk across the system.

Recommended remediation:

- Upgrade the system to a supported Windows version (or apply the required service pack/feature update).
- Ensure Windows Update (or centralized patching) is enabled and regularly applied.
- If the system cannot be upgraded, isolate it (network segmentation) and restrict inbound access.


KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folde
kali:8834/#/scans/reports/10/vulnerabilities/108797
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Cybersecurity Snapshot: Cyber Pros Emerge as Bold ...
Read More
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 27
Notes 1
History 1

scanner / Plugin #108797

‹ Back to Vulnerabilities

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 8.1
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	10.0.3.4

Plugin Details

Severity:	Critical
ID:	108797
Version:	1.16
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	October 21, 2025

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score: 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Unsupported by vendor: true

Reference Information

IAVA: 0001-A-0501

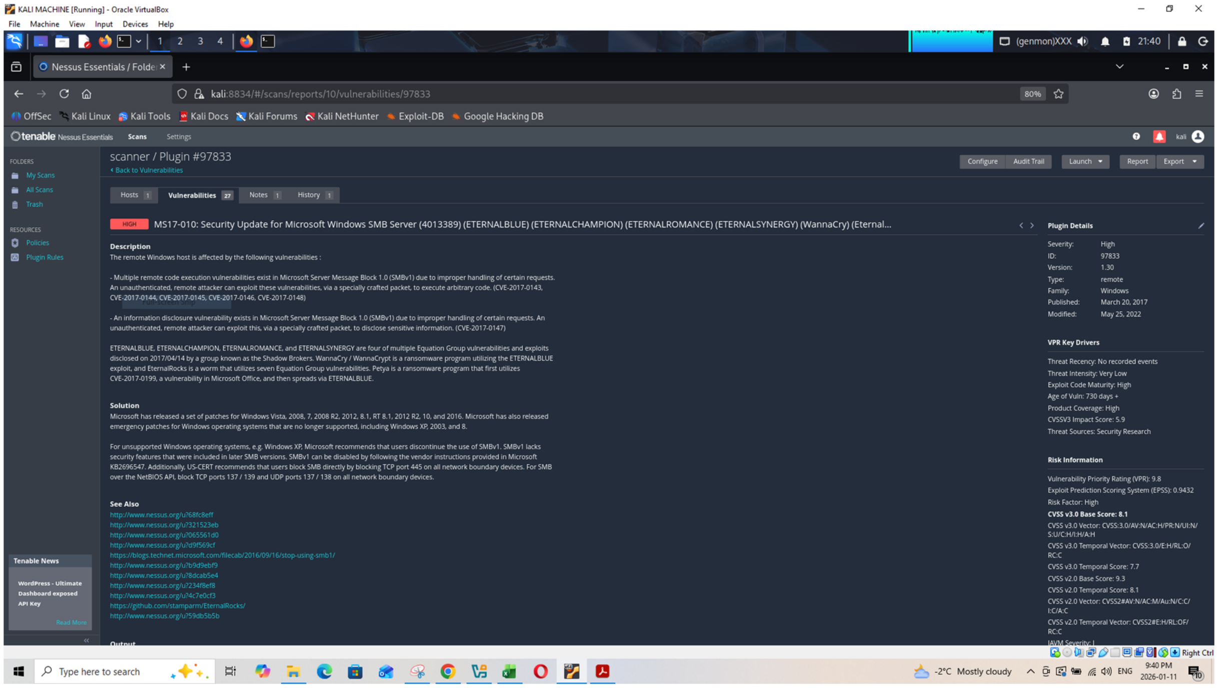
Figure 6: Plugin details for Unsupported Windows OS (remote), including description and recommended solution.

8.2 High: MS17-010 (SMB) – EternalBlue-related risk

MS17-010 is a Microsoft security update addressing critical SMB vulnerabilities that have been widely exploited. If the host is missing the patch (or has SMBv1 exposed), it may be vulnerable to remote compromise.

Recommended remediation (defensive):

- Apply the MS17-010 patches through Windows Update/WSUS/endpoint management.
- Disable SMBv1 where possible and prefer SMBv2/SMBv3.
- Restrict SMB exposure: block/limit TCP 445 at the host firewall and network boundaries where it is not required.
- Use network segmentation to reduce lateral movement risk.


KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folde
kali:8834/#/scans/reports/10/vulnerabilities/97833
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials Scans Settings
Configure Audit Trail Launch Report Export
Hosts 1 Vulnerabilities 27 Notes 1 History 1

scanner / Plugin #97833

‹ Back to Vulnerabilities

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (Eternal...

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

http://www.nessus.org/u?68fc8eff
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?065561d0
http://www.nessus.org/u?d9f569cf
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
http://www.nessus.org/u?b9d9ebf9
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Output

Plugin Details

Severity:	High
ID:	97833
Version:	1.30
Type:	remote
Family:	Windows
Published:	March 20, 2017
Modified:	May 25, 2022

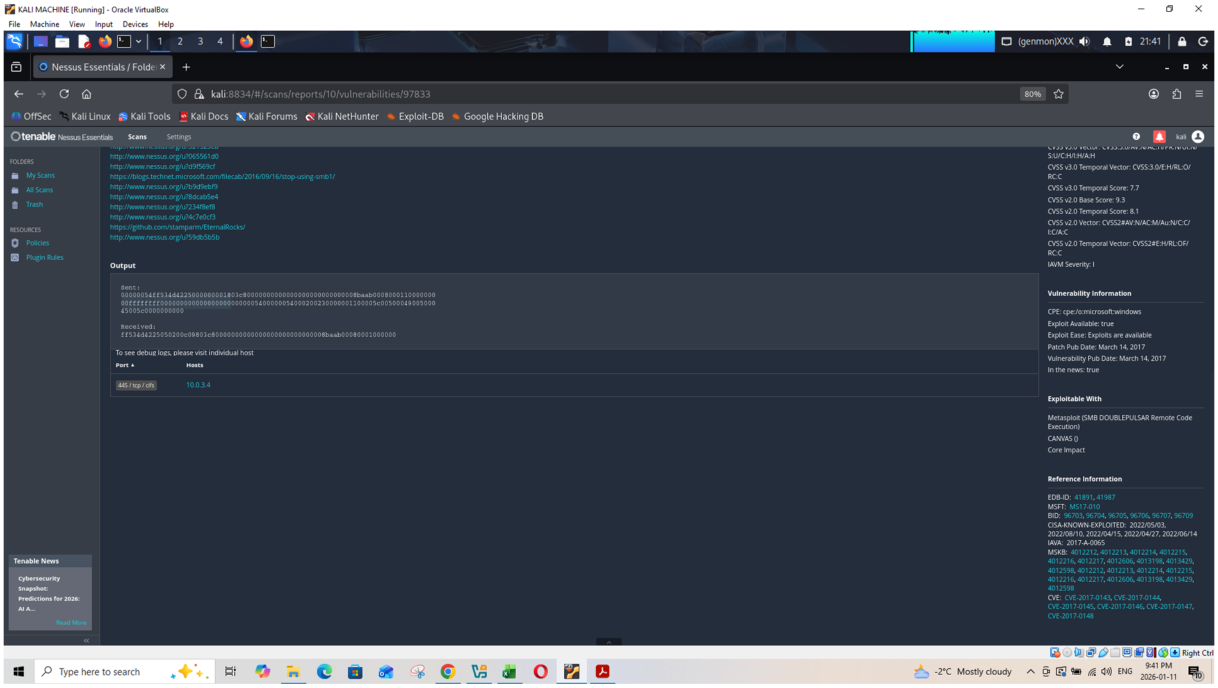
VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 5.9
Threat Sources: Security Research

Risk Information

Vulnerability Priority Rating (VPR): 9.8
Exploit Prediction Scoring System (EPSS): 0.9432
Risk Factor: High
CVSS v3.0 Base Score: 8.1
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 7.7
CVSS v2.0 Base Score: 9.3
CVSS v2.0 Temporal Score: 8.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
IAVM Severity: I

Figure 7: Plugin details for MS17-010 (SMB) showing description, risk information, and references.


KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folde
kali:8834/#/scans/reports/10/vulnerabilities/97833
tenable Nessus Essentials Scans Settings

http://www.nessus.org/u?065561d0
http://www.nessus.org/u?d9f569cf
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
http://www.nessus.org/u?b9d9ebf9
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Output

```
Sent:
00000054ff534d4225000000001803c80000000000000000000000008baab0008000110000000
00ffffffff000000000000000000000054000000540002002300000001100005c005000490050000
45005c0000000000

Received:
ff534d4225050200c09803c80000000000000000000000008baab00080001000000
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	10.0.3.4

S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 7.7
CVSS v2.0 Base Score: 9.3
CVSS v2.0 Temporal Score: 8.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 14, 2017
Vulnerability Pub Date: March 14, 2017
In the news: true

Exploitable With

Metasploit (SMB DOUBLEPULSAR Remote Code Execution)
CANVAS ()
Core Impact

Reference Information

EDB-ID: 41891, 41987
MSFT: MS17-010
BID: 96703, 96704, 96705, 96706, 96707, 96709
CISA-KNOWN-EXPLOITED: 2022/05/03, 2022/08/10, 2022/04/15, 2022/04/27, 2022/06/14
IAVA: 2017-A-0065
MSKB: 4012212, 4012213, 4012214, 4012215, 4012216, 4012217, 4012606, 4013198, 4013429, 4012598, 4012212, 4012213, 4012214, 4012215, 4012216, 4012217, 4012606, 4013198, 4013429, 4012598
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

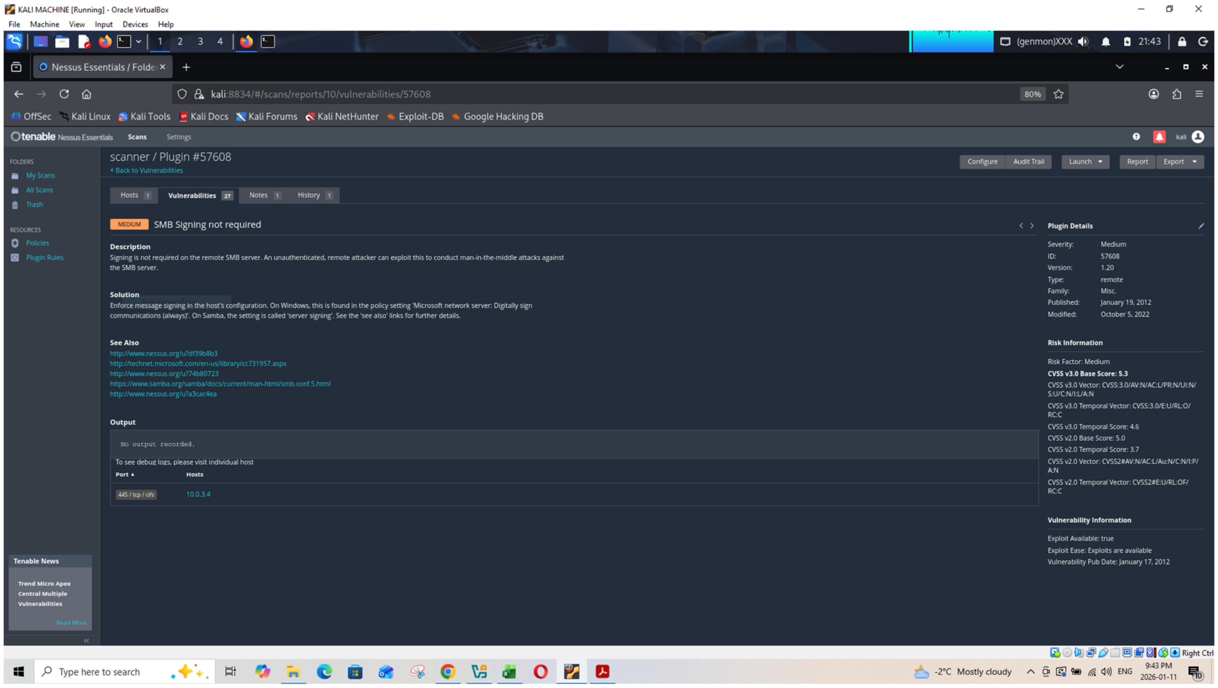
Figure 8: Evidence/output for MS17-010 showing the affected host and SMB port (445/tcp) context.

8.3 Medium: SMB Signing not required

If SMB signing is not required, an attacker on the network may be able to perform man-in-the-middle attacks against SMB traffic in some scenarios.

Recommended remediation:

- Enable and require SMB signing via Group Policy/Local Security Policy on Windows (Microsoft network server: Digitally sign communications).
- Prefer modern SMB configurations and ensure secure authentication.
- Reduce SMB usage and keep SMB traffic on trusted/segmented networks.


KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folder
kali:8834/#/scans/reports/10/vulnerabilities/57608
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials Scans Settings
FOLDERS My Scans All Scans Trash
RESOURCES Policies Plugin Rules
Configure Audit Trail Launch Report Export
kali

scanner / Plugin #57608

‹ Back to Vulnerabilities

Hosts 1 | Vulnerabilities 27 | Notes 1 | History 1

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	10.0.3.4

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 17, 2012

Figure 9: Plugin details for SMB Signing not required, including remediation guidance.

9. Export or document the scan report

To generate a deliverable:

- Click Report or Export on the scan results page.
- Choose your format (PDF is common for sharing; CSV is useful for spreadsheets).
- Include at least: scan policy, target scope, timestamp, and top findings with remediation.

10. Quick remediation checklist for this target (10.0.3.4)

Based on the findings shown in the screenshots, prioritize:

- Upgrade/patch the Windows OS (critical).
- Apply MS17-010 (or confirm it is applied) and disable SMBv1; restrict TCP 445 if not required (high).
- Require SMB signing (medium).
- Re-run the scan after remediation to confirm risk reduction.