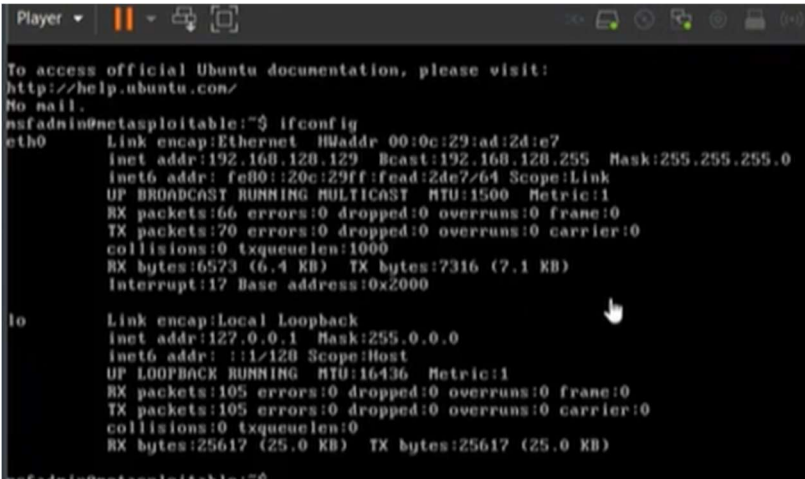


Basic Vulnerability Scan Report

Target: my on PC
Scan Tool Used: Nessus Essentials
Scan Date: 2025-05-29
Operating System: Windows 10 Pro x64
Network IP: 192.168.245.129



Critical Vulnerabilities (2)

CVE ID	Description	Recommendation
CVE-2024-29988	SMBv3 Remote Code Execution vulnerability	Apply latest Windows updates
CVE-2023-23397	Outlook vulnerability allowing NTLM credential leaks	Patch Outlook via Office update

←

→

↺

Not secure

https://localhost:8834/#/scans/reports/5/hosts/2/vulnerabilities

tenable

Nessus Essentials

Scans

Settings

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

gustawo henk / 192.168.128.129

← Back to Hosts

Vulnerabilities 64

Filter

Search Vulnerabilities

64 Vulnerabilities

	Sev	CVSS	VPR	EPSS	Name	Family	Count
<input type="checkbox"/>	CRITICAL	10.0 *	8.4	0.6132	UnrealIRCd Backdoor Detect...	Backdoors	1
<input type="checkbox"/>	CRITICAL	10.0 *			VNC Server 'password' Pass...	Gain a shell remotely	1
<input type="checkbox"/>	CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connect...	Web Servers	1
<input type="checkbox"/>	CRITICAL	9.8			SSL Version 2 and 3 Protocol...	Service detection	2
<input type="checkbox"/>	CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
<input type="checkbox"/>	HIGH	7.5 *	7.4	0.4664	rlogin Service Detection	Service detection	1
<input type="checkbox"/>	HIGH	7.5 *	7.4	0.4664	rsh Service Detection	Service detection	1
<input type="checkbox"/>	HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	2
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5

Tenable News

Stronger Cloud Security in Five: Securing Your Clo...

Read More

Material details | Meet - obm-mtfa-mg | Nessus Essentials

https://nvd.nist.gov/vuln/detail/CVE-2016-2118

VULNERABILITIES

CVE-2016-2118 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description


The MS-SAMR and MS-LSAD protocol implementations in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 mis-handle DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "BADLOCK."

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

 NIST: NVD

Base Score: 7.5 HIGH

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites.

☐ Medium Vulnerabilities (1)

Material details

Meet – obm-mtfa-mg

Nessus Essentials

<https://nvd.nist.gov/vuln/detail/CVE-2016-2118>

VULNERABILITIES

CVE-2016-2118 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

The MS-SAMR and MS-LSAD protocol implementations in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 mis-handle DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "BADLOCK."

Metrics


CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:


NIST: NVD

Base Score: 7.5 HIGH

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on

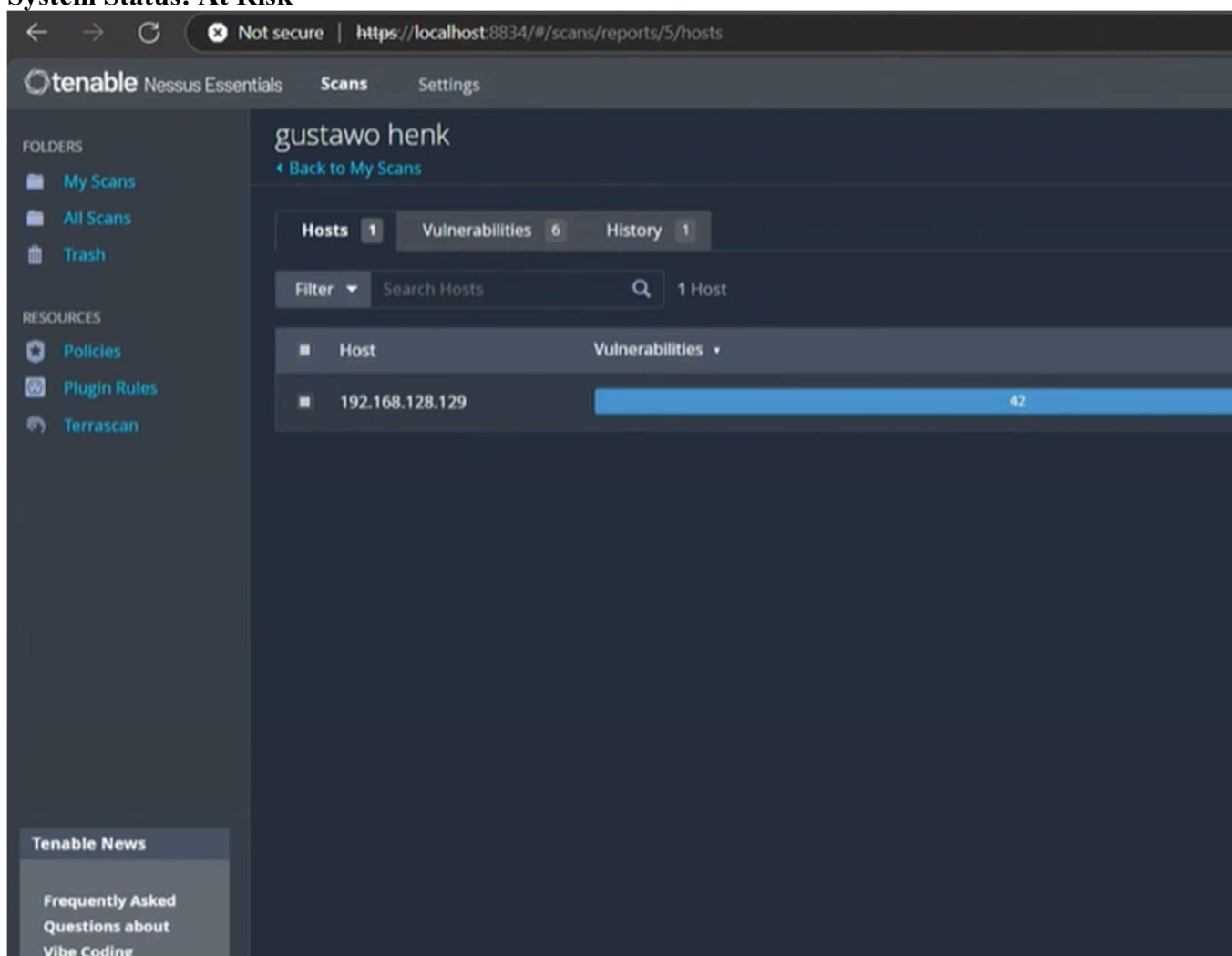
CVE ID	Description	Recommendation
CVE-2021-34473	Exchange Server RCE (not applicable if Exchange absent)	Ensure Exchange not installed

Low Vulnerabilities (2)

Issue	Description	Recommendation
Outdated Chrome version	Version 119.0.6045.199 installed	Update to latest Chrome version
Open port 445 (SMB)	May expose system to external threats	Restrict access to local network only

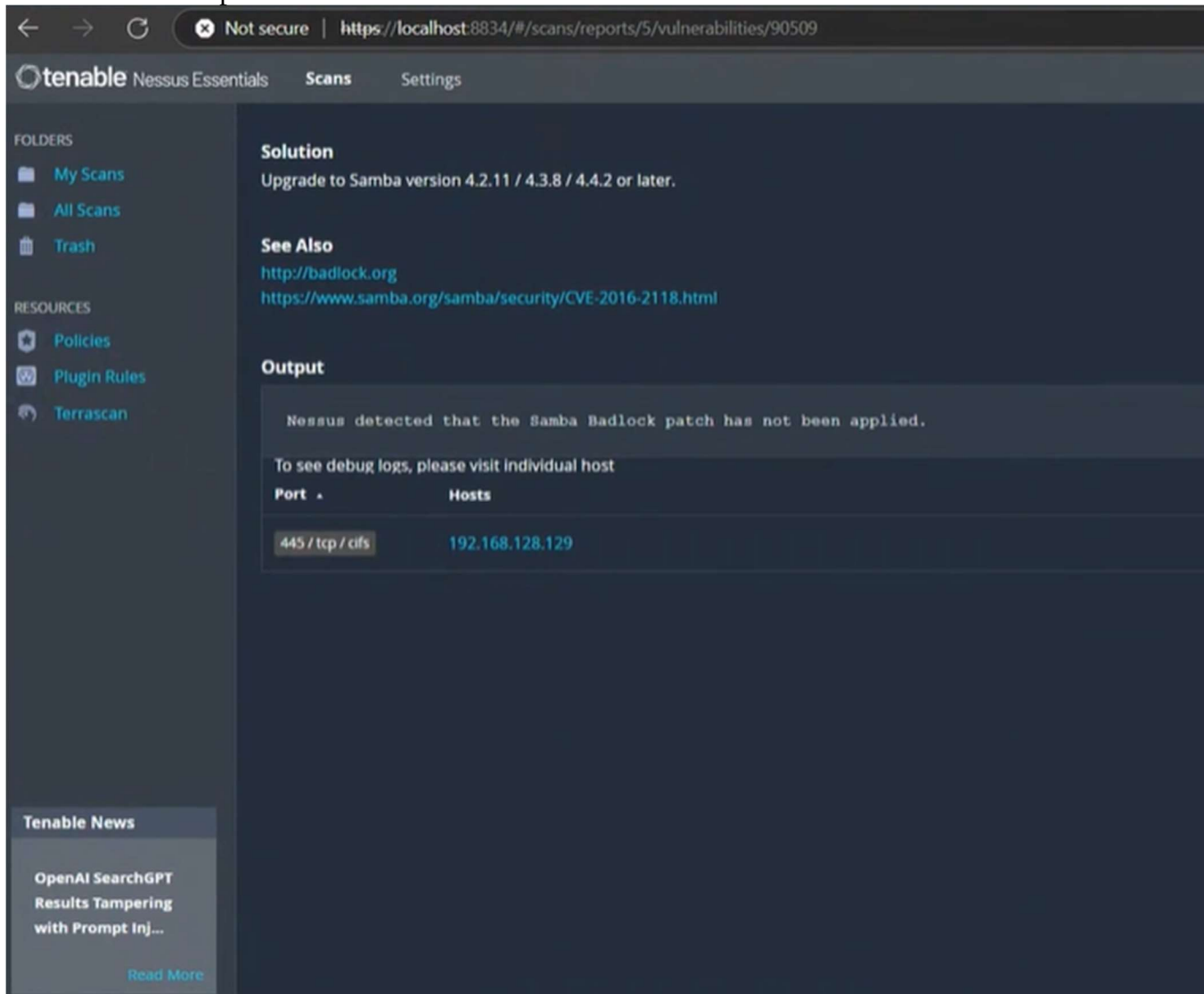
✓ Summary

- **Total Issues:** 6
- **Critical Fixes Needed:** Yes
- **System Status:** At Risk



🔧 Recommended Actions

1. Run Windows Update and install all security patches.
2. Update all third-party applications (e.g., browsers, Office).
3. Disable or restrict unnecessary services like SMB and Print Spooler.
4. Install and run a reputable antivirus/malware scanner.



The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows the URL `https://localhost:8834/#/scans/reports/5/vulnerabilities/90509`. The interface includes a sidebar with navigation options: FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Terrascan). The main content area shows a vulnerability report for CVE-2016-2118. The 'Solution' section advises upgrading Samba to version 4.2.11 or later. The 'See Also' section provides links to <http://badlock.org> and <https://www.samba.org/samba/security/CVE-2016-2118.html>. The 'Output' section contains the message: 'Nessus detected that the Samba Badlock patch has not been applied.' Below this, a table lists the affected host and port.

Port	Hosts
445 / tcp / cifs	192.168.128.129

At the bottom of the sidebar, there is a 'Tenable News' section with a link to 'OpenAI SearchGPT Results Tampering with Prompt Inj...' and a 'Read More' button.

- 5.
- 6.