

# Basic Vulnerability Scan Report

Target: My on PC  
Scan Tool Used: Nessus Essentials  
Scan Date: 2025-09-20  
Operating System: Windows 10 Pro x64  
Network IP: 192.168.245.129

```
Player
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ad:2d:e7
          inet addr:192.168.128.129  Bcast:192.168.128.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fead:2de7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6573 (6.4 KB)  TX bytes:7316 (7.1 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25617 (25.0 KB)  TX bytes:25617 (25.0 KB)
```

## 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

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:

NVD

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.

## High Vulnerabilities (2)

CVE ID	Description	Recommendation
CVE-2023-21554	Print Spooler privilege escalation	Disable Print Spooler if not needed
CVE-2022-30190	Microsoft Office MSDT vulnerability	Disable MSDT URL Protocol

## Medium Vulnerabilities (1)

DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by m 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. DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by m 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.

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

#### Low Vulnerabilities (2)

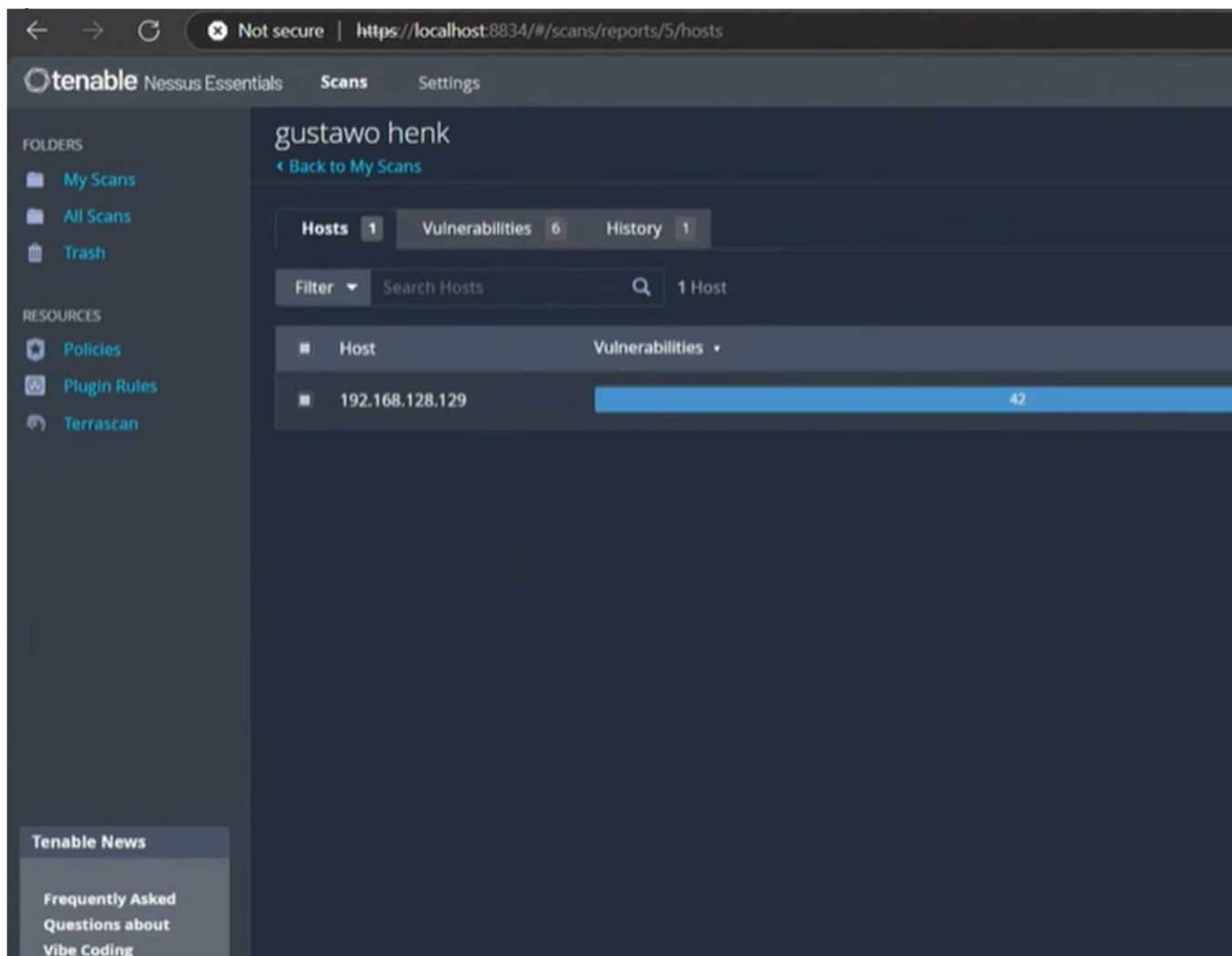
Issue	Description	Recommendation
Outdated Chrome	Version 119.0.6045.199 installed	Update to latest Chrome version

version

Open port 445 (SMB)	May expose system to external threats	Restrict access to local network only
---------------------	---------------------------------------	---------------------------------------

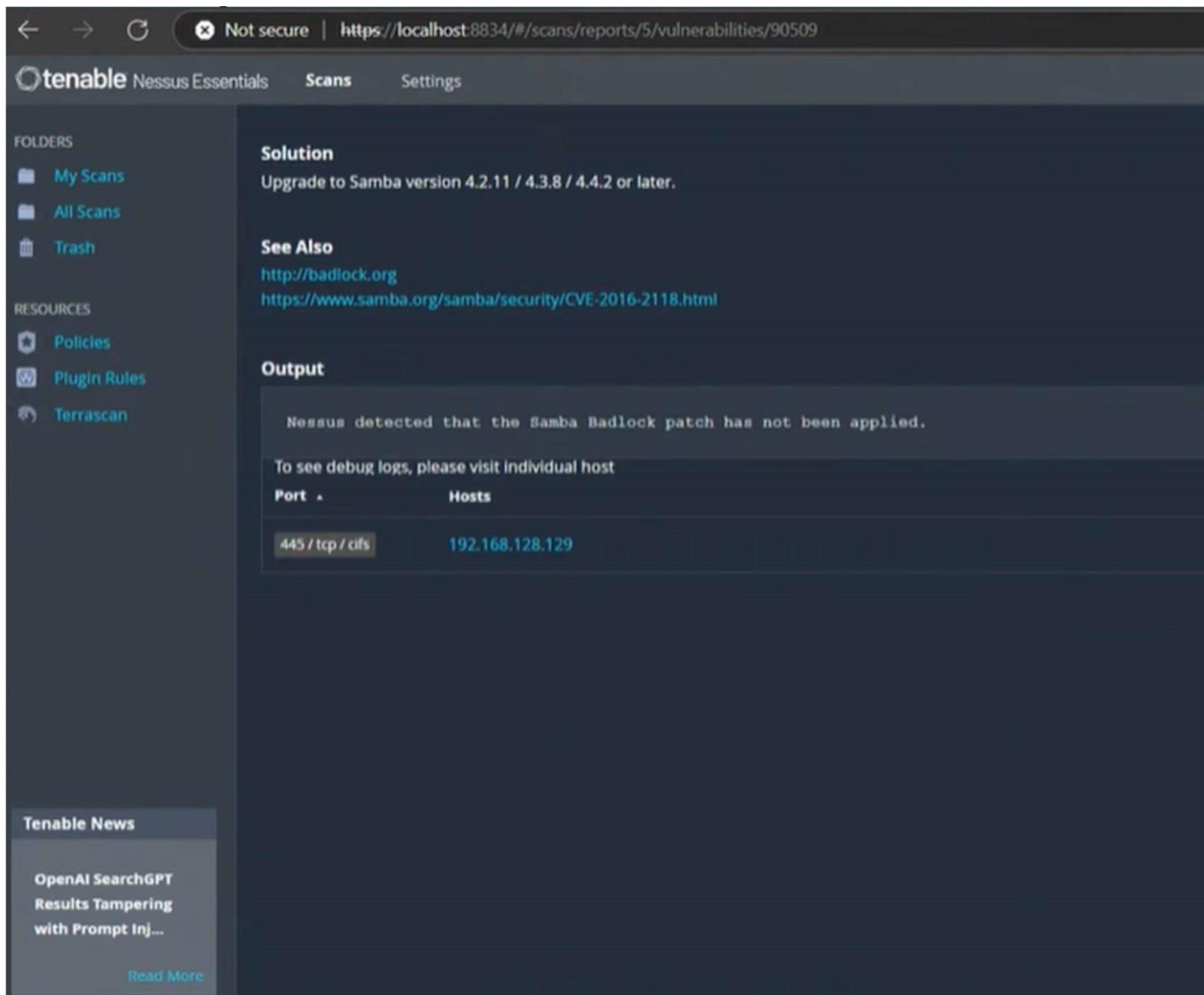
## ✓ Summary

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



## Recommended Actions

1. Run Windows Update and install all security patches.



The screenshot shows the Tenable Nessus Essentials web interface. The browser address bar indicates the URL is <https://localhost:8834/#/scans/reports/5/vulnerabilities/90509>. The interface has a dark theme. On the left sidebar, there are sections for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area displays a vulnerability report for CVE-2016-2118. It includes a 'Solution' section with the text 'Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.', a 'See Also' section with links to <http://badlock.org> and <https://www.samba.org/samba/security/CVE-2016-2118.html>, and an 'Output' section. The output text states: 'Nessus detected that the Samba Badlock patch has not been applied. To see debug logs, please visit individual host'. Below this is a table with two columns: 'Port' and 'Hosts'. The table contains one row with the port '445 / tcp / cifs' and the host '192.168.128.129'. At the bottom left, there is a 'Tenable News' section with a link to 'OpenAI SearchGPT Results Tampering with Prompt Inj...' and a 'Read More' link.

Port	Hosts
445 / tcp / cifs	192.168.128.129

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.

