

VULNERABILITY ASSESSMENT

ASSIGNMENT REPORT



**Peter Kinyumu,
cs-sa07-24067,
June 10th, 2024.**

1. INTRODUCTION

This module guided me through understanding Vulnerability Assessment, which is about identifying and categorizing risks for security weaknesses related to assets within an environment. It explains the steps of performing a network vulnerability assessment, the various ways to calculate the severity ratings of vulnerabilities, how to conduct vulnerability assessment with tools like Nessus and OpenVAS and how to clearly report findings.

2. ANSWERS TO QUESTIONS

Nessus

- a. What is the name of one of the accessible SMB shares from the authenticated Windows scan? (One word)

From the Vulnerabilities section of the Windows Authenticated scan, we can search for “SMB Shares” to filter the results.

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules). The main area is titled 'Windows_basic_authed' and shows a list of 'Vulnerabilities' (349 total). A filter bar at the top says 'Filter: SMB Share'. Below it, a table lists several vulnerabilities, with the first one highlighted by a red box:

Sev	Score	Name	Family	Count	Action
INFO		Microsoft Windows SMB Share Host	Windows	1	○ /
INFO		Microsoft Windows SMB Share Permissio...	Windows	1	○ /
INFO		Microsoft Windows SMB Shares Access	Windows	1	○ /
INFO		Microsoft Windows SMB Shares Enumera...	Windows	1	○ /

A red arrow points from the text 'We can click to view accessible shares' to the highlighted row. To the right of the table, there's a 'Scan Details' section and a 'Vulnerabilities' pie chart. The pie chart has segments for Critical (dark blue), High (red), Medium (orange), Low (yellow), and Info (light blue).

We can then click the “Windows SMB Shares Access” to view the accessible SMB shares.

b. What was the target for the authenticated scan?

c. What is the plugin ID of the highest criticality vulnerability for the Windows authenticated scan?

The first listed vulnerability is the one with the highest criticality. If we hover over it, we see the plugin ID used.

Plugin ID can be viewed by hovering over the vulnerability or opening the vulnerability

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: 2022-02-13 at 2:54 AM
- End: 2022-02-13 at 3:17 AM
- Elapsed: 23 minutes

Vulnerabilities

Severity	Count
Critical	9
High	1
Medium	1
Low	1
Info	9

d. What is the name of the vulnerability with plugin ID 26925 from the Windows authenticated scan? (Case sensitive)

Filters

Match All of the following:

Plugin ID	is equal to	26925
-----------	-------------	-------

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: 2022-02-13 at 2:54 AM
- End: 2022-02-13 at 3:17 AM
- Elapsed: 23 minutes

Vulnerabilities

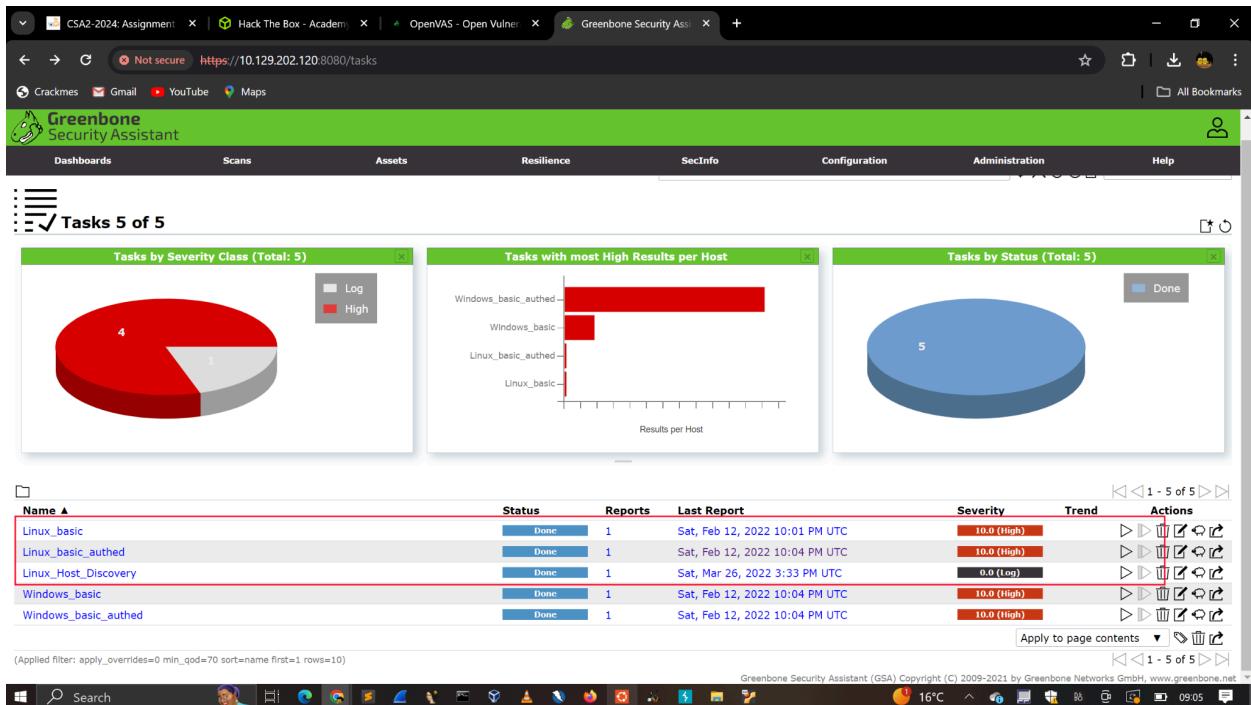
Severity	Count
Critical	9
High	1
Medium	1
Low	1
Info	9

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Scans' selected. The main area displays a scan titled 'Windows_basic_authed'. A red arrow points from the text 'Vulnerability Name' to the 'Name' column of the table, which lists 'VNC Server Unauthenticated Access'. The table also includes columns for 'Sev', 'Score', 'Family', and 'Count'. To the right, there's a 'Scan Details' section with information like Policy: Basic Network Scan, Status: Completed, and Severity Base: CVSS v3.0. Below that is a 'Vulnerabilities' section with a pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light green), and Info (blue).

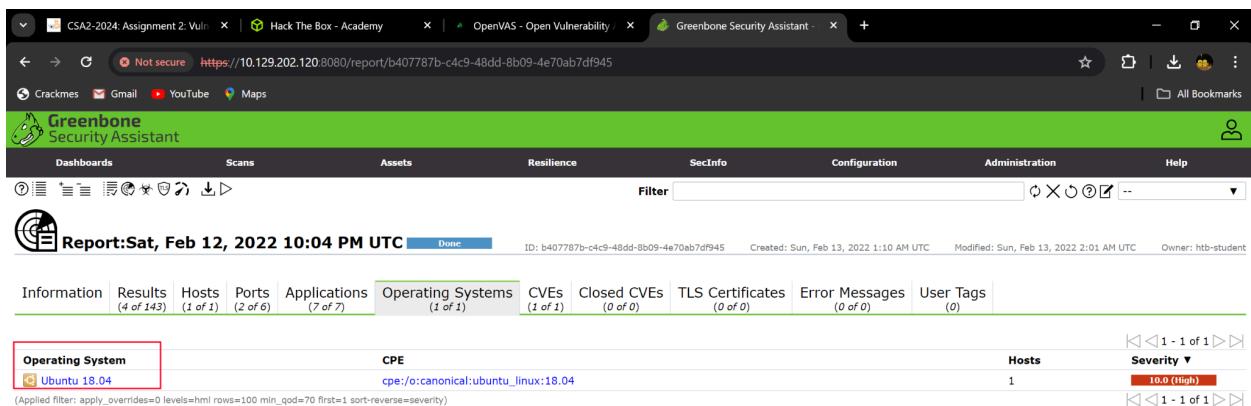
e. What port is the VNC server running on in the authenticated Windows scan?

The screenshot shows the Nessus Essentials interface. It's displaying the details of a vulnerability named 'VNC Server Unauthenticated Access'. A red arrow points from the text 'VNC Port' to the 'Hosts' field in the 'Output' section, which shows '172.16.16.100'. The 'Output' section also includes a note: 'No output recorded.' In the 'Description' section, it says: '** The VNC server installed on the remote host allows an attacker to connect to the remote host as no authentication is required to access this service.' The 'Solution' section suggests: 'Disable the No Authentication security type.' The 'Plugin Details' section provides technical details about the vulnerability, including Severity: High, ID: 26925, Version: \$Revision: 1.12 \$, Type: remote, Family: Misc., Published: October 5, 2007, and Modified: January 25, 2013.

OpenVAS



a. What type of operating system is the Linux host running? (one word)



b. What type of FTP vulnerability is on the Linux host? (Case Sensitive, four words)

The screenshot shows a browser window with the Greenbone Security Assistant interface. The title bar indicates the report was generated on Sat, Feb 12, 2022, at 10:04 PM UTC. The main content area displays a table of vulnerabilities. One specific row is highlighted with a red border:

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.16.160		general/tcp	Sun, Feb 13, 2022 1:16 AM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.16.16.160		21/tcp	Sun, Feb 13, 2022 1:26 AM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	172.16.16.160		80/tcp	Sun, Feb 13, 2022 1:43 AM UTC
TCP timestamps	2.6 (Low)	80 %	172.16.16.160		general/tcp	Sun, Feb 13, 2022 1:32 AM UTC

c. What is the IP of the Linux host targeted for the scan?

The screenshot shows a browser window with the Greenbone Security Assistant interface. The title bar indicates the report was generated on Sat, Feb 12, 2022, at 10:04 PM UTC. The main content area displays a table of hosts. One specific row is highlighted with a red border:

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity
172.16.16.160		2	9				Sun, Feb 13, 2022 1:16 AM UTC	Sun, Feb 13, 2022 2:01 AM UTC	1	2	1	0	0	4	10.0 (High)

d. What vulnerability is associated with the HTTP server? (Case-sensitive)

Report: Sat, Feb 12, 2022 10:04 PM UTC

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.16.160		general/tcp	Sun, Feb 13, 2022 1:16 AM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.16.16.160		21/tcp	Sun, Feb 13, 2022 1:26 AM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	172.16.16.160		80/tcp	Sun, Feb 13, 2022 1:43 AM UTC
TCP timestamps	2.6 (Low)	80 %	172.16.16.160		general/tcp	Sun, Feb 13, 2022 1:32 AM UTC

3. MODULE COMPLETION

<https://academy.hackthebox.com/achievement/144829/108>

To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

Great job c1ph3rbnuk!

Vulnerability Assessment

Congratulations c1ph3rbnuk!
You have just completed the Vulnerability Assessment module!

Let's share your success with everyone!

Share on LinkedIn Share on X Share on Facebook

Get a shareable link

Completed / Congrats!

4. CONCLUSION

This assignment has taught me a lot about Vulnerability Assessment. Through it, I have learned the methodology to follow when performing a vulnerability assessment. I have also learned of various assessment standards that ensure thorough assessment. Additionally, I have learned how to use vulnerability scanners like Nessus and OpenVAS to conduct vulnerability assessments. Lastly, I have learned how to clearly report the findings of the vulnerability assessment in a way that is concise, clear and easy to read and understand.