Introduction
https://academy.hackthebox.com/achievement/949661/108

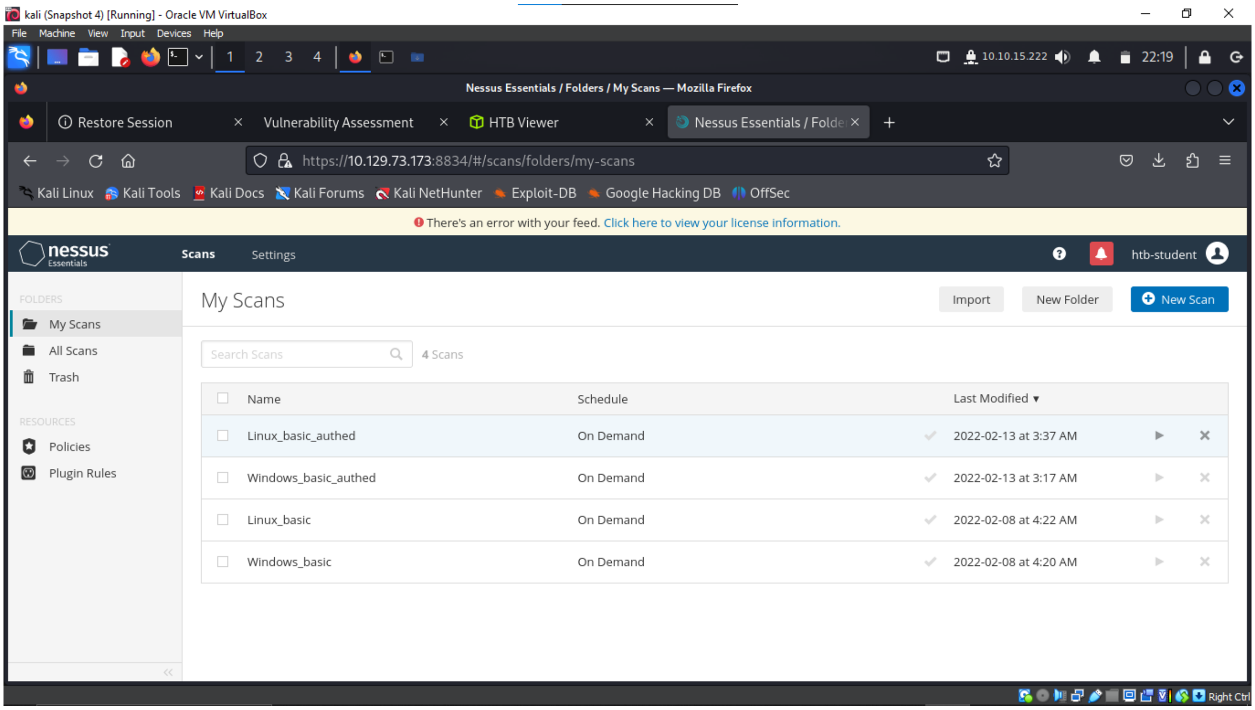
Vulnerability assessments are critical in identifying and mitigating security risks in IT environments. This report summarizes key aspects of conducting such assessments using Nessus and OpenVAS, two leading tools in the cybersecurity domain. It provides insights into their functionalities, methodologies, and reporting mechanisms.

1 . **Security Assessments**

- Purpose: Identifying and mitigating vulnerabilities in systems and networks.
- *Types*: Methods include vulnerability scanning, penetration testing, etc.
- *Compliance and Risk*: Tailored to organizational needs.
- *Security Posture Maturity*: Ranges from basic to advanced setups.
- *Continuous Monitoring*: Essential for ongoing security.

2. Nessus Vulnerability Scanner

- *Functionality*: Scans for various vulnerabilities and misconfigurations.
- *Types of Scans*: Includes both unauthenticated and authenticated scans.
- *Components*: Server component and client interface.
- *Reports and Analysis*: Detailed vulnerability reporting.


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folders / My Scans — Mozilla Firefox
Restore Session
Vulnerability Assessment
HTB Viewer
Nessus Essentials / Folde
https://10.129.73.173:8834/#/scans/folders/my-scans
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus Essentials
Scans
Settings
htb-student
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Import
New Folder
New Scan
Search Scans

There's an error with your feed. Click here to view your license information.

My Scans

4 Scans

Name	Schedule	Last Modified ▾
Linux_basic_authed	On Demand	2022-02-13 at 3:37 AM
Windows_basic_authed	On Demand	2022-02-13 at 3:17 AM
Linux_basic	On Demand	2022-02-08 at 4:22 AM
Windows_basic	On Demand	2022-02-08 at 4:20 AM

3. Windows Authenticated Scan with Nessus

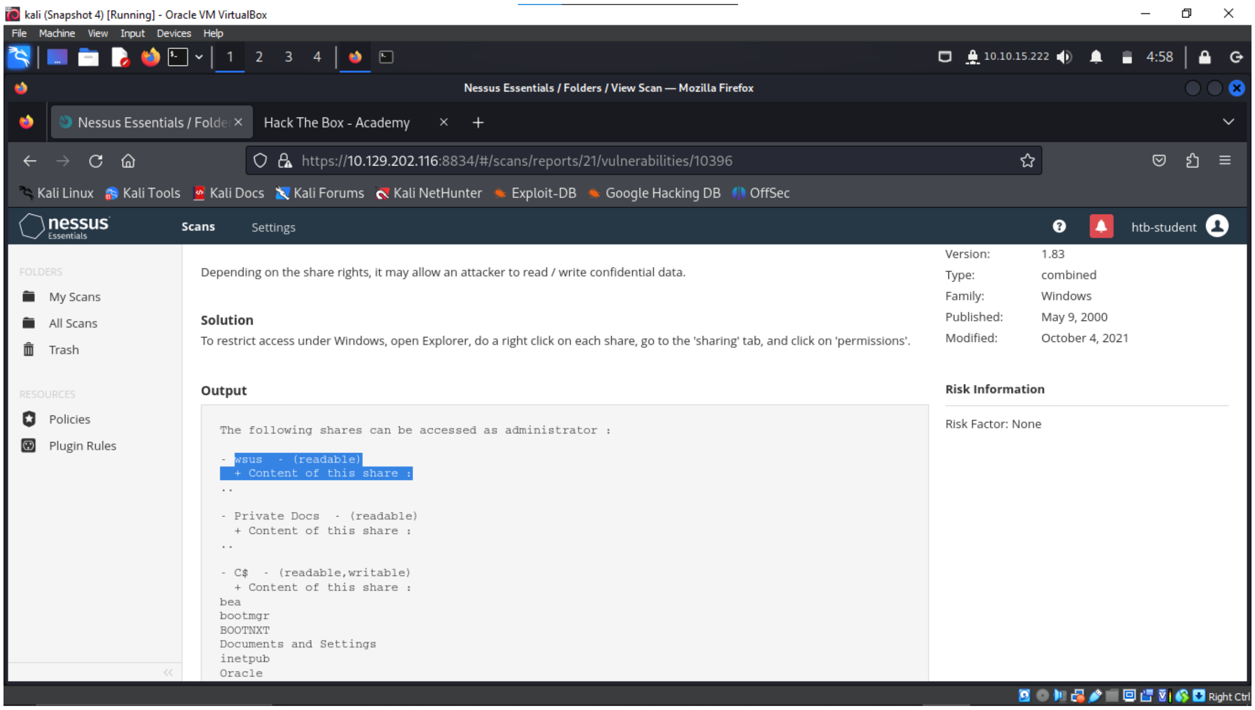
- *Target System*: Windows environments.
- *Authentication*: Requires valid credentials.
- *Key Findings*: System vulnerabilities and security weaknesses.

Analysis: Prioritizing critical vulnerabilities

Based on your Nessus Skills Assessment, here are my answers to the questions:

Q: Name of an Accessible SMB Share from the Authenticated Windows Scan:

A: wsus


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folders / View Scan — Mozilla Firefox
Nessus Essentials / Folde
Hack The Box - Academy
https://10.129.202.116:8834/#/scans/reports/21/vulnerabilities/10396
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus Essentials
Scans
Settings
htb-student
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules

Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Output

```
The following shares can be accessed as administrator :

- wsus  - (readable)
  + Content of this share :
..

- Private Docs  - (readable)
  + Content of this share :
..

- C$  - (readable,writable)
  + Content of this share :
bea
bootmgr
BOOTNXT
Documents and Settings
inetpub
Oracle
```

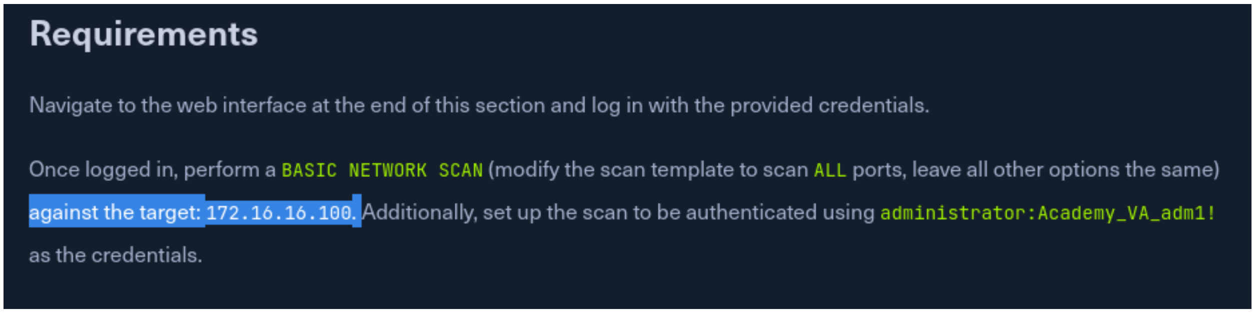
Version:	1.83
Type:	combined
Family:	Windows
Published:	May 9, 2000
Modified:	October 4, 2021

Risk Information

Risk Factor: None

Q: Target for the Authenticated Scan:

A: 172.16.16.100



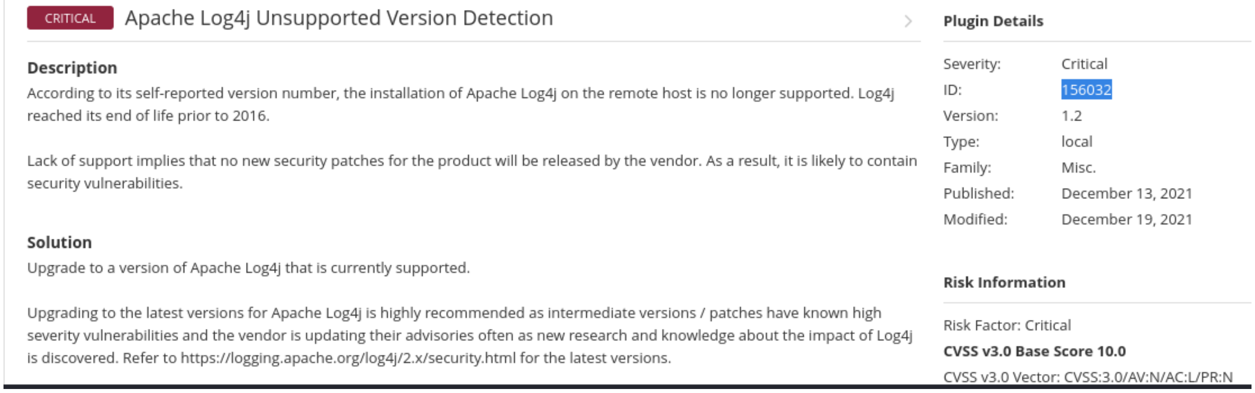
Requirements

Navigate to the web interface at the end of this section and log in with the provided credentials.

Once logged in, perform a `BASIC NETWORK SCAN` (modify the scan template to scan `ALL` ports, leave all other options the same) against the target: `172.16.16.100`. Additionally, set up the scan to be authenticated using `administrator:Academy_VA_adm1!` as the credentials.

Q: Plugin ID of the Highest Criticality Vulnerability for the Windows Authenticated Scan:

A: 156032



Apache Log4j Unsupported Version Detection

Description

According to its self-reported version number, the installation of Apache Log4j on the remote host is no longer supported. Log4j reached its end of life prior to 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.

Solution

Upgrade to a version of Apache Log4j that is currently supported.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Plugin Details

Severity:	Critical
ID:	156032
Version:	1.2
Type:	local
Family:	Misc.
Published:	December 13, 2021
Modified:	December 19, 2021

Risk Information

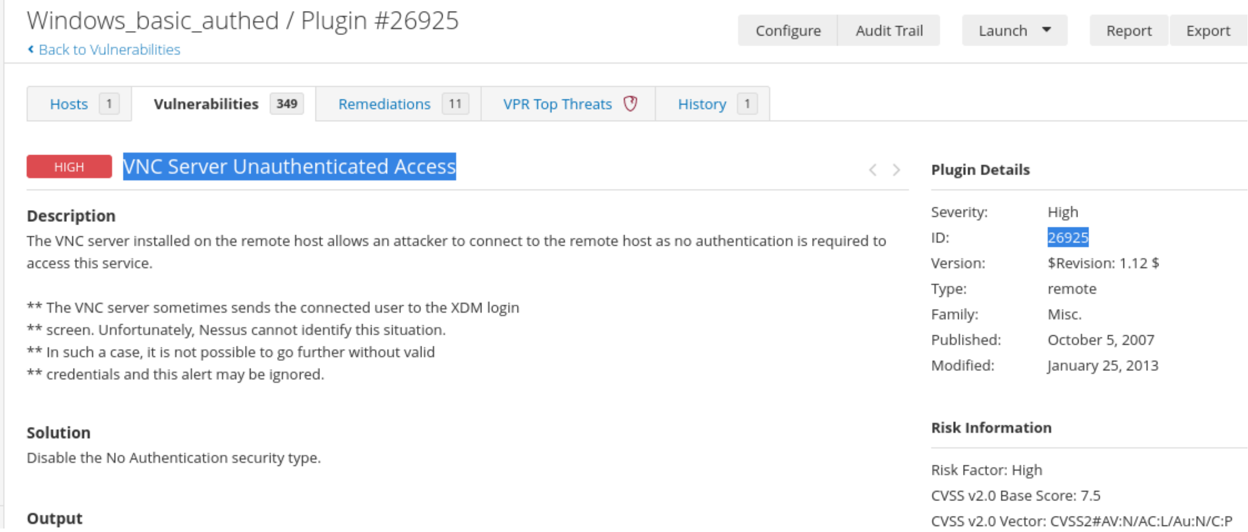
Risk Factor: Critical

CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N

Q: Name of the Vulnerability with Plugin ID 26925 from the Windows Authenticated Scan:

A: VNC Server Unauthenticated Access



Windows_basic_authed / Plugin #26925

VNC Server Unauthenticated Access

Description

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 VNC server sometimes sends the connected user to the XDM login
** screen. Unfortunately, Nessus cannot identify this situation.
** In such a case, it is not possible to go further without valid
** credentials and this alert may be ignored.
```

Solution

Disable the No Authentication security type.

Output

Plugin Details

Severity:	High
ID:	26925
Version:	$Revision: 1.12 $
Type:	remote
Family:	Misc.
Published:	October 5, 2007
Modified:	January 25, 2013

Risk Information

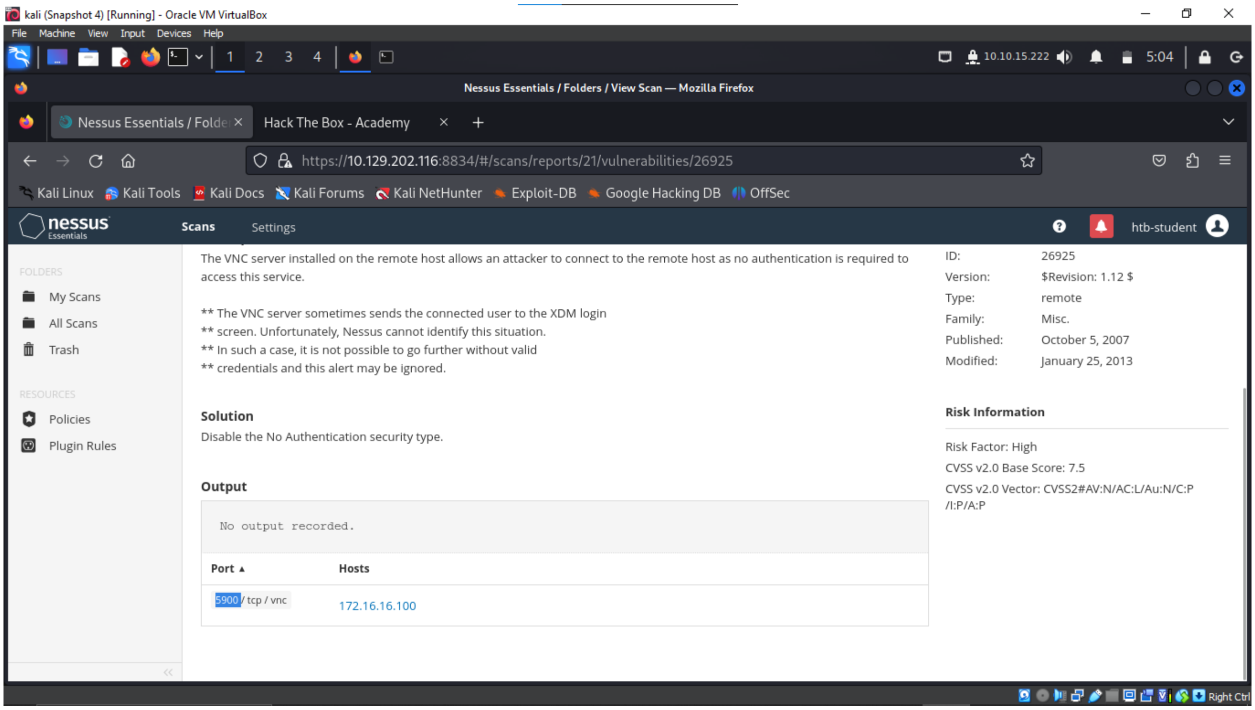
Risk Factor: High

CVSS v2.0 Base Score: 7.5

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

Q: Port on Which the VNC Server is Running in the Authenticated Windows Scan:

A:5900


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Nessus Essentials / Folders / View Scan — Mozilla Firefox
Nessus Essentials / Folde
Hack The Box - Academy
https://10.129.202.116:8834/#/scans/reports/21/vulnerabilities/26925
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus Essentials
Scans
Settings
htb-student
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules

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 VNC server sometimes sends the connected user to the XDM login
** screen. Unfortunately, Nessus cannot identify this situation.
** In such a case, it is not possible to go further without valid
** credentials and this alert may be ignored.

Solution

Disable the No Authentication security type.

Output

```
No output recorded.
```

Port ▲	Hosts
5900 / tcp / vnc	172.16.16.100

ID:	26925
Version:	$Revision: 1.12 $
Type:	remote
Family:	Misc.
Published:	October 5, 2007
Modified:	January 25, 2013

Risk Information

Risk Factor: High
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

.

4. OpenVAS (Greenbone Vulnerability Manager)

- *Overview*: Open-source network vulnerability scanner.
- *Installation*: Available on multiple platforms.
- *Configuration and Use*: Target setup and scan configurations.
- *Reporting*: Detailed and exportable reports.

5. OpenVAS Scan Process

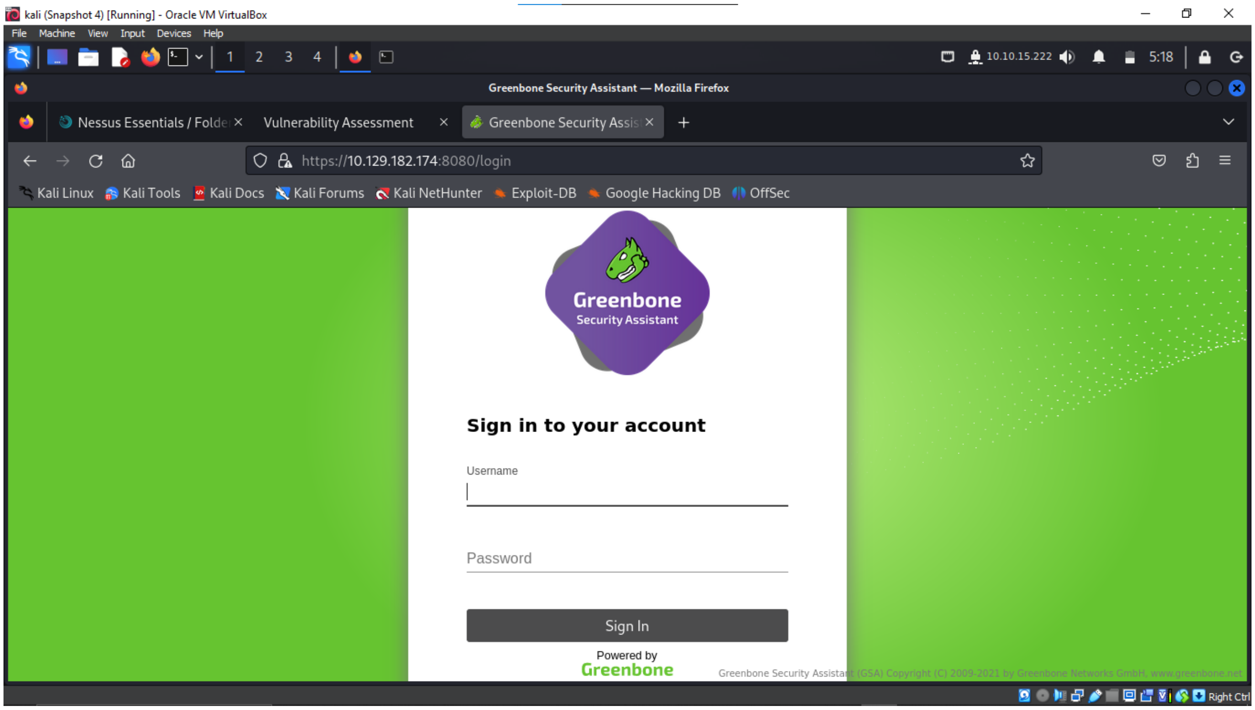
- *Scans Setup*: Scope definition and target selection.
- *Types of Scans*: Various scanning options.
- *Authenticated Scans*: In-depth scanning using privileged credentials.

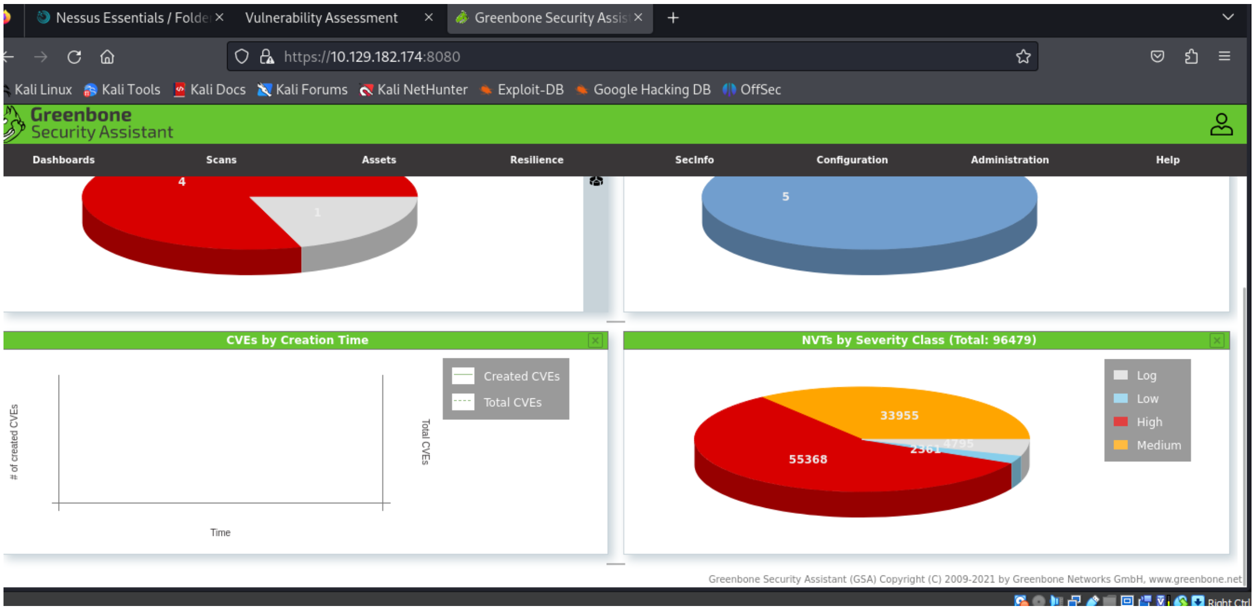
6. Exporting and Analysing OpenVAS Results

- *Report Access*: Via the OpenVAS interface.
- *Export Formats*: Multiple formats including XML, CSV, PDF.
- *Tools for Analysis*: Utilization of external tools for report analysis.

7. OpenVAS Skills Assessment

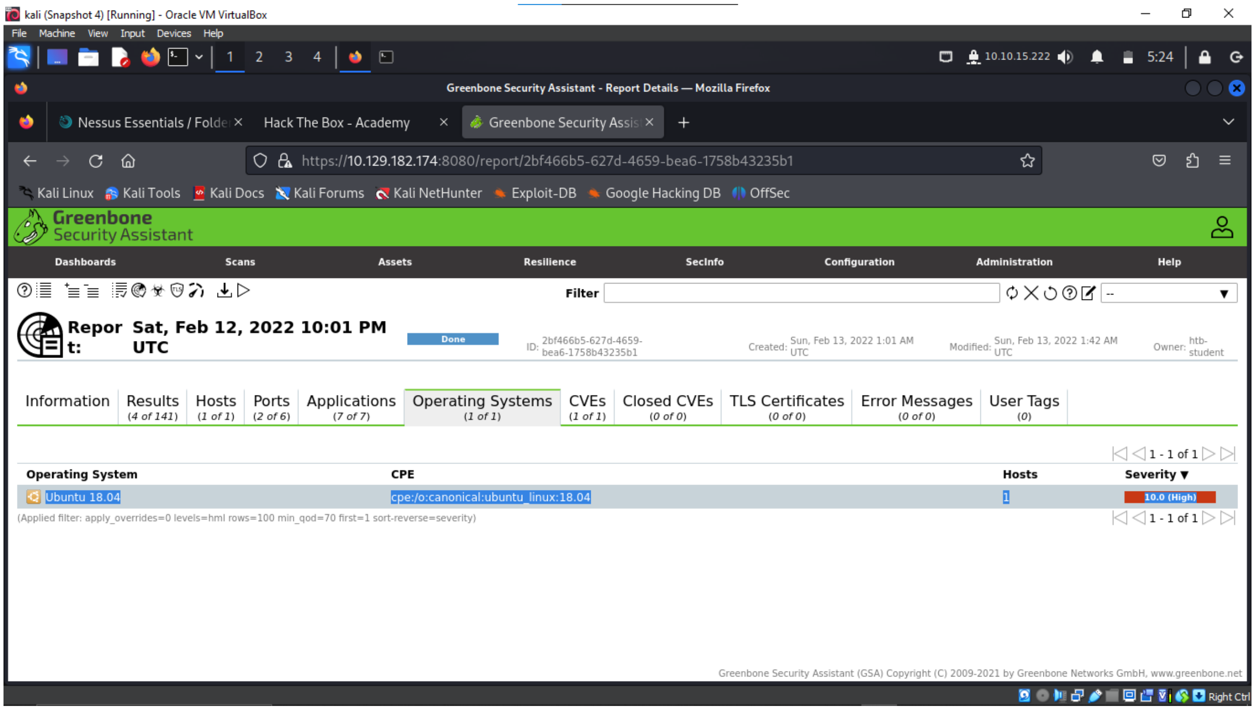
- *Scenario*: Vulnerability assessment for Inlanefreight.
- *Objective*: Authenticated scan on a Linux server.
- *Credentials and Target*: Specific login for target scanning.
- *Methodology*: OpenVAS Default Scanner with specific configurations.

- 
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.15.222 5:18
Greenbone Security Assistant — Mozilla Firefox
Nessus Essentials / Folde
Vulnerability Assessment
Greenbone Security Assis
https://10.129.182.174:8080/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Sign in to your account
Username
Password
Sign In
Powered by Greenbone
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net
Right Ctrl

- 
Nessus Essentials / Folde
Vulnerability Assessment
Greenbone Security Assis
https://10.129.182.174:8080
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
4
1
5
CVEs by Creation Time
# of created CVEs
Time
Total CVEs
Created CVEs
Total CVEs
NVTs by Severity Class (Total: 96479)
33955
55368
2361
4795
Log
Low
High
Medium
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net
Right Ctrl

Based on the information provided and the questions you need to answer, here are my responses:

Type of Operating System on the Linux Host:
Answer: Ubuntu



kali (Snapshot 4) [Running] - Oracle VM VirtualBox
Greenbone Security Assistant - Report Details — Mozilla Firefox
Nessus Essentials / Folde
Hack The Box - Academy
Greenbone Security Assis
https://10.129.182.174:8080/report/2bf466b5-627d-4659-bea6-1758b43235b1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter

Report: Sat, Feb 12, 2022 10:01 PM UTC — Done

ID: 2bf466b5-627d-4659-bea6-1758b43235b1 Created: Sun, Feb 13, 2022 1:01 AM UTC Modified: Sun, Feb 13, 2022 1:42 AM UTC Owner: htb-student

Information | Results (4 of 141) | Hosts (1 of 1) | Ports (2 of 6) | Applications (7 of 7) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 1 of 1

Operating System	CPE	Hosts	Severity ▼
Ubuntu 18.04	cpe:/o:canonical:ubuntu_linux:18.04	1	10.0 (High)

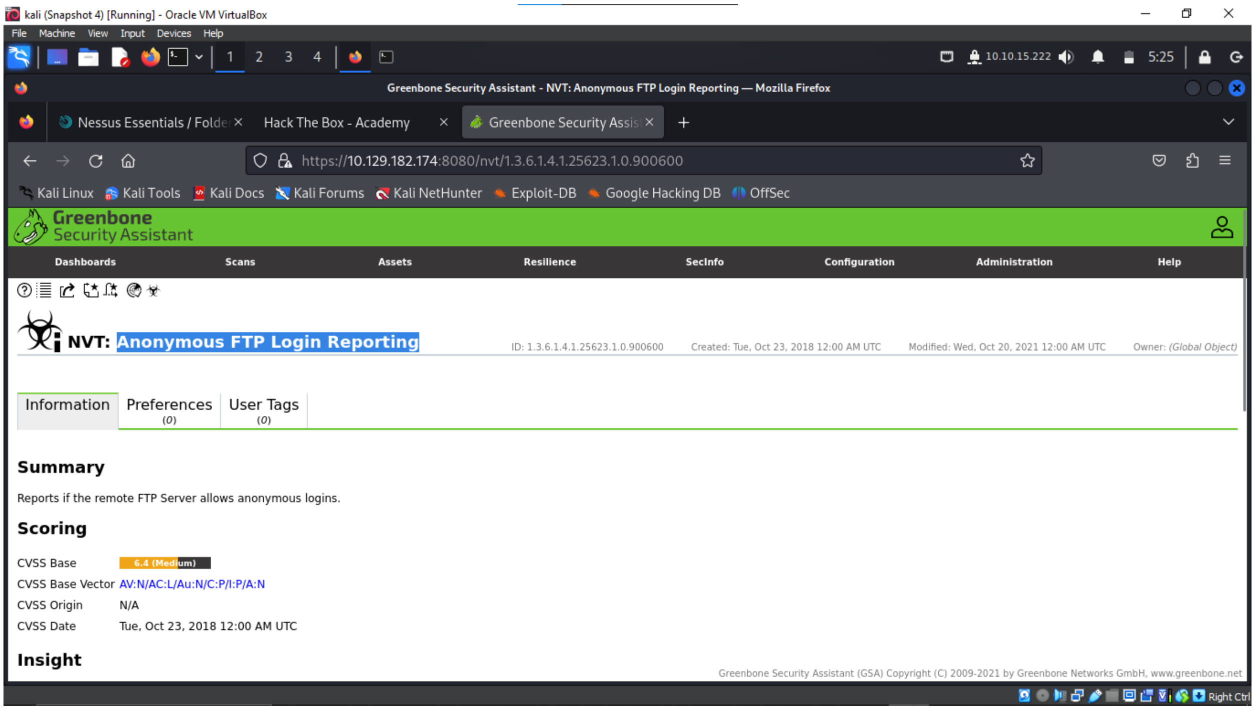
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 1 of 1

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Type of FTP Vulnerability on the Linux Host:

Answer: Anonymous FTP Login Reporting



kali (Snapshot 4) [Running] - Oracle VM VirtualBox
Greenbone Security Assistant - NVT: Anonymous FTP Login Reporting — Mozilla Firefox
Nessus Essentials / Folde
Hack The Box - Academy
Greenbone Security Assis
https://10.129.182.174:8080/nvt/1.3.6.1.4.1.25623.1.0.900600
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help

NVT: Anonymous FTP Login Reporting

ID: 1.3.6.1.4.1.25623.1.0.900600 Created: Tue, Oct 23, 2018 12:00 AM UTC Modified: Wed, Oct 20, 2021 12:00 AM UTC Owner: *(Global Object)*

Information | Preferences (0) | User Tags (0)

Summary

Reports if the remote FTP Server allows anonymous logins.

Scoring

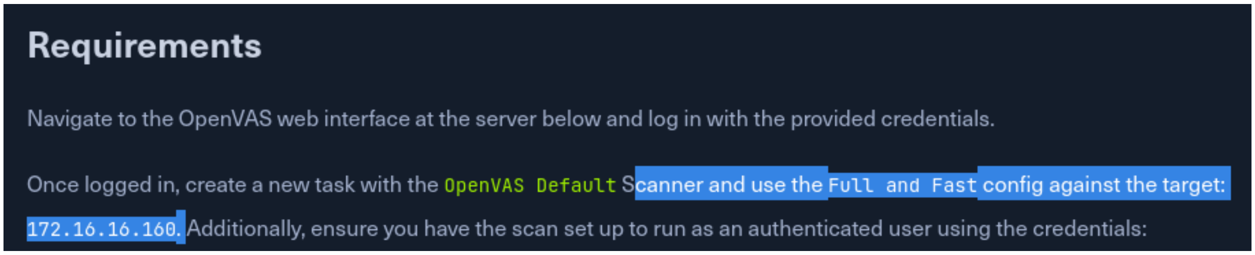
CVSS Base	6.4 (Medium)
CVSS Base Vector	AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Origin	N/A
CVSS Date	Tue, Oct 23, 2018 12:00 AM UTC

Insight

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

IP of the Linux Host Targeted for the Scan:

Answer: 172.16.16.160



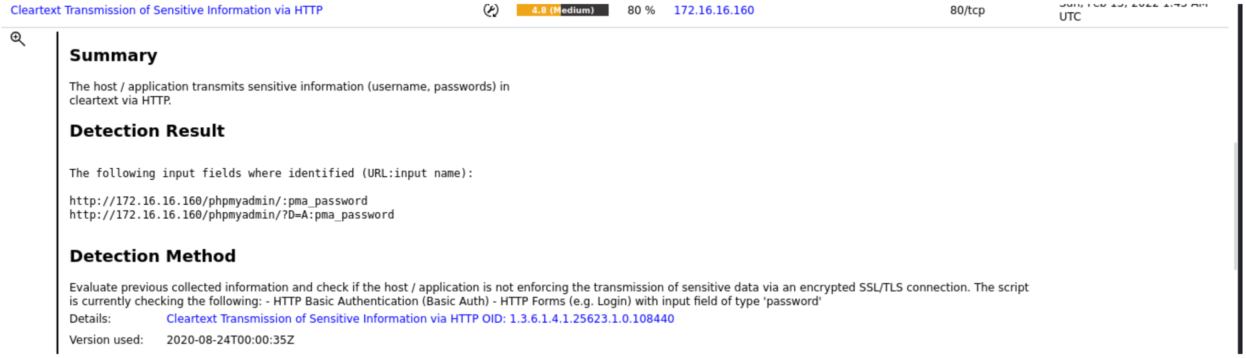
Requirements

Navigate to the OpenVAS web interface at the server below and log in with the provided credentials.

Once logged in, create a new task with the `OpenVAS Default` Scanner and use the `Full and Fast` config against the target: `172.16.16.160`. Additionally, ensure you have the scan set up to run as an authenticated user using the credentials:

Vulnerability Associated with the HTTP Server:

Answer: Cleartext Transmission of Sensitive Information via HTTP



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

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Detection Result

```
The following input fields where identified (URL:input name):

http://172.16.16.160/phpmyadmin/:pma_password
http://172.16.16.160/phpmyadmin/?D=A:pma_password
```

Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password'

Details: Cleartext Transmission of Sensitive Information via HTTP OID: 1.3.6.1.4.1.25623.1.0.108440

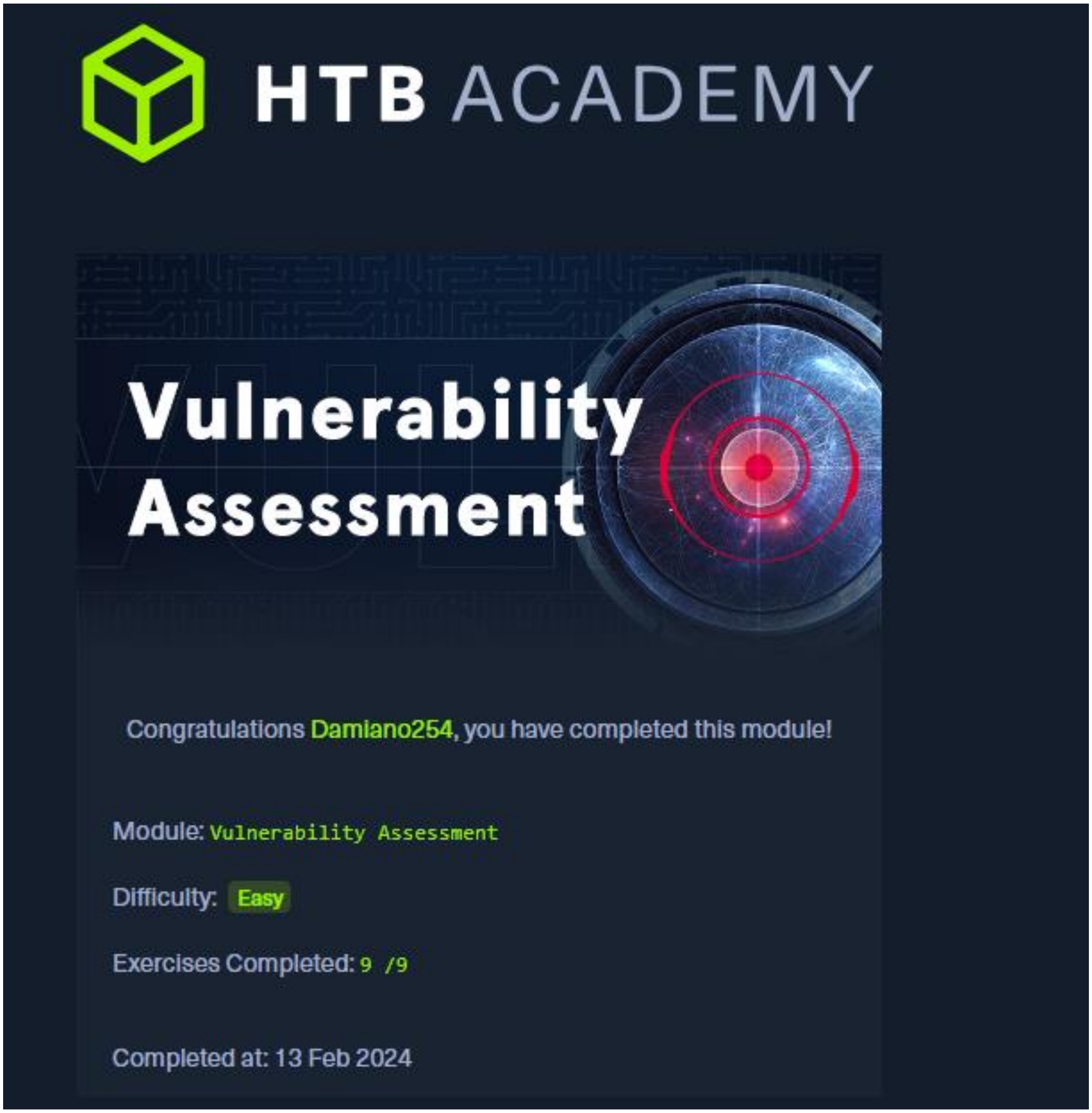
Version used: 2020-08-24T00:00:35Z

8. Reporting Vulnerability Assessments

- *Importance*: Translating technical findings into actionable insights.
- *Structure*: Includes key sections like Executive Summary and Recommendations.
- *Audience*: Suitable for technical and non-technical stakeholders.
- *Content*: Detailed findings with remediation steps.

Conclusion

The employment of Nessus and OpenVAS in vulnerability assessments is vital for uncovering and addressing network and system vulnerabilities. These tools not only reveal security gaps but also aid in guiding effective remediation strategies. Their effective use and the clear communication of their findings are essential in maintaining robust cybersecurity defences in an ever-evolving threat landscape.



HTB ACADEMY

Vulnerability Assessment

Congratulations Damiano254, you have completed this module!

Module: `Vulnerability Assessment`

Difficulty: Easy

Exercises Completed: `9 /9`

Completed at: 13 Feb 2024