



# HACKTHEBOX

## Vulnerability Assessment



Tier 0 Easy Offensive

This module introduces the concept of Vulnerability Assessments. We will review the differences between vulnerability assessments and penetration tests, how to carry out a vulnerability assessment, how to interpret the assessment results, and how to deliver an effective vulnerability assessment report.

By Saezel

Last Updated: 27 October 2024

# Nessus Skills Assessment

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

Answer: wsus

The screenshot displays the Nessus Essentials web interface. The top navigation bar includes links to HTB Labs, HTB Certifications, HTB Academy, CTF Platform, Help Center, and HTB Blog. The main content area is divided into a left sidebar and a main panel. The sidebar shows 'FOLDERS' with 'My Scans' selected, and 'RESOURCES' with 'Policies' and 'Plugin Rules'. The main panel shows 'My Scans' with a search bar and a list of scans. The scan 'Windows\_basic\_authed' is highlighted. Below this, the 'Settings' page for 'Windows\_basic\_authed' is shown, featuring a 'Hosts' tab with 1 host, a 'Vulnerabilities' tab with 349 vulnerabilities, and a 'History' tab with 1 item. The host list shows '172.16.16.100' with a vulnerability score of 67 out of 126.

Nessus Essentials / Folder x

https://10.129.11.105:8834/#/scans/folders/my-scans

HTB Labs HTB Certifications HTB Academy CTF Platform Help Center HTB Blog

nessus Essentials Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

My Scans

Search Scans 4 Scans

- ☐ Name
- ☐ Linux\_basic\_authed
- ☐ Windows\_basic\_authed
- ☐ Linux\_basic
- ☐ Windows\_basic

Settings

Windows\_basic\_authed

[Back to My Scans](#)

Hosts 1 Vulnerabilities 349 Remediations 11 VPR Top Threats History 1

Filter Search Hosts 1 Host

<input type="checkbox"/> Host	Vulnerabilities ▼
<input type="checkbox"/> <u>172.16.16.100</u>	67 126

## Windows\_basic\_authed / 1 / 2.16.16.100

[← Back to Hosts](#)

Vulnerabilities 349

Filter ▾

smb



28 of 349 Vulnerabilities

☐ Save ▾ Score ▾ Name ▴

## Windows\_basic\_authed / Plugin #10396

[← Back to Vulnerabilities](#)

Vulnerabilities 349

INFO

### Microsoft Windows SMB Shares Access

#### Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

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 'pe

#### Output

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

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

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

```
more...
```

Port ▴

Hosts

445 / tcp / cifs

172.16.16.100



*What was the target for the authenticated scan?*

*Answer: 172.16.16.100*

Scans Settings


### Windows\_basic\_authed

[← Back to All Scans](#)

**Hosts** 1 **Vulnerabilities** 349 **Remediations** 11 **VPR Top Thr**

**Filter** ▼   1 Host

<input type="checkbox"/>	Host	Vulnerabilities ▼
<input type="checkbox"/>	172.16.16.100	67



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

Answer: 156032

Windows\_basic\_authed / 172.16.16.100

[Back to Hosts](#)

Vulnerabilities349

FilterSearch Vulnerabilities349 Vulnerabilities

<input type="checkbox"/>	Sev	Score	Name
<input type="checkbox"/>	CRITICAL	10.0	Apache Log4j Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0	Oracle Java JRE Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0	Oracle WebLogic Server Multiple Vulnerabilities (April 2017 CPU)

Windows\_basic\_authed / Plugin #156032

[Back to Vulnerabilities](#)

Vulnerabilities349

CRITICALApache Log4j Unsupported Version Detection

Description

According to its self-reported version number, the installation of Apache Log4j on the remote host is r  
life prior to 2016.

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

Answer: VNC Server Unauthenticated Access

Filters

Match

All

of the following:

Plugin ID

is equal to

26925

+

Apply

Cancel

Clear Filters

Windows\_basic\_authed / 172.16.16.100

[Back to Hosts](#)

Vulnerabilities 1

1 Filter Search Vulnerabilities 1 Vulnerability

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	HIGH	7.5 *	VNC Server Unauthenticated Access

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

*Answer: 5900*

windows\_basic\_authed / 1 / 2.16.16.100

[Back to Hosts](#)

Vulnerabilities 349

Filter  4 of 349 Vulnerabilities

<input type="checkbox"/>	Sev	Score	Name ▲
<input type="checkbox"/>	INFO		VNC HTTP Server Detection
<input type="checkbox"/>	INFO		VNC Server Security Type Detection
<input type="checkbox"/>	HIGH	7.5 *	VNC Server Unauthenticated Access
<input type="checkbox"/>	INFO		VNC Server Unencrypted Communication Detection

Results per page 50 ▼

## Windows\_basic\_authed / Plugin #26925

[Back to Vulnerabilities](#)

Vulnerabilities 349

### HIGH VNC Server Unauthenticated Access

#### Description

The VNC server installed on the remote host allows an attacker to connect to the remote ho

\*\* 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 <a href="#">🔗</a>

# OpenVAS Skills Assessment

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

*Answer: Ubuntu*

Greenbone Security Assistant

HTB Labs HTB Certifications HTB Academy CTF Platform Help Center HTB Blog

Dashboards Scans Assets

Operating Systems 6 of 6

Operating Systems by Severity Class (Total: 6)

Log High

...	o:windows_server_2016
cpe:/o:microsoft:windows	
...	ndows_server_2016:::x64

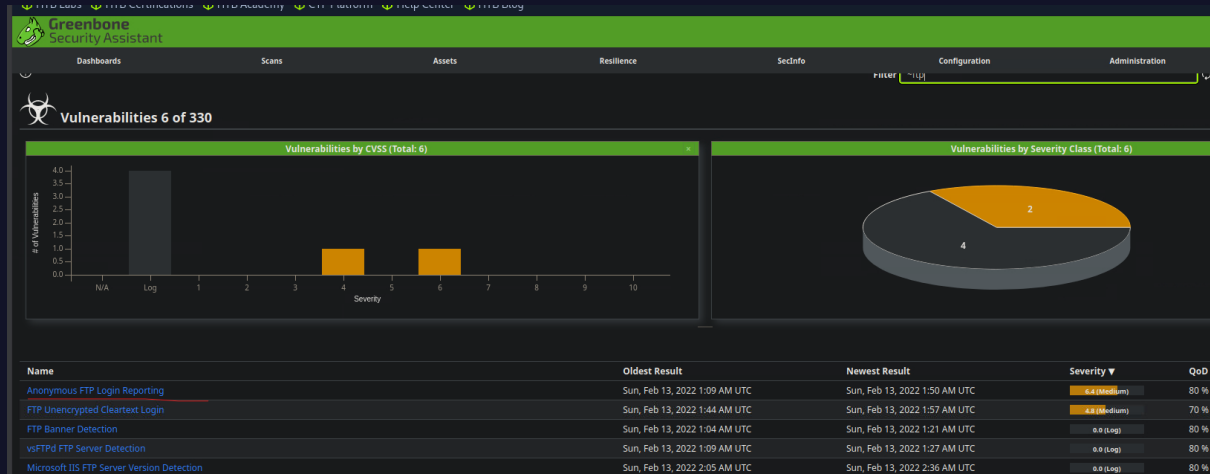
Name	Title
cpe:/o:microsoft:windows_server_2016	
cpe:/o:microsoft:windows_server_2016:::x64	
cpe:/o:microsoft:windows	
cpe:/o:linux:kernel	
cpe:/o:canonical:ubuntu_linux:18.04	Canonical <u>Ubuntu</u> Linux 18.04
cpe:/o:canonical:ubuntu_linux	

(Applied filter: sort-reverse=latest\_severity first=1 rows=10)



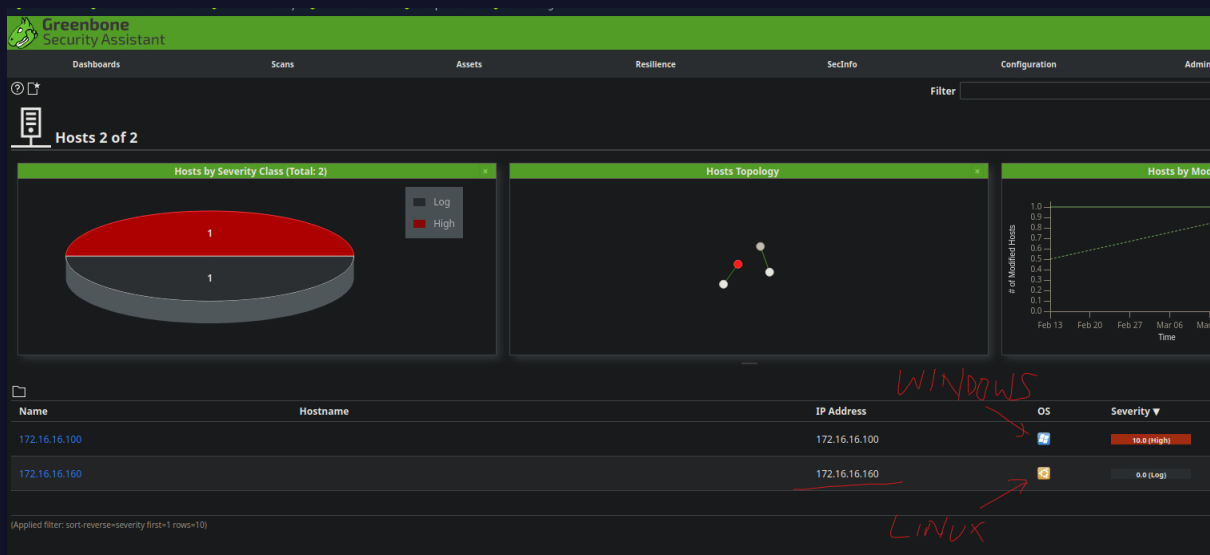
What type of FTP vulnerability is on the Linux host? (Case Sensitive, four words)

Answer: Anonymous FTP Login Reporting



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

Answer: 172.16.16.160



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

Answer: Cleartext Transmission of Sensitive Information via HTTP

