Vulnerability Assessment:

Link to challenge: https://academy.hackthebox.com/module/108/

(log in required)

Class: Tier 0 | Easy | Offensive

Nessus

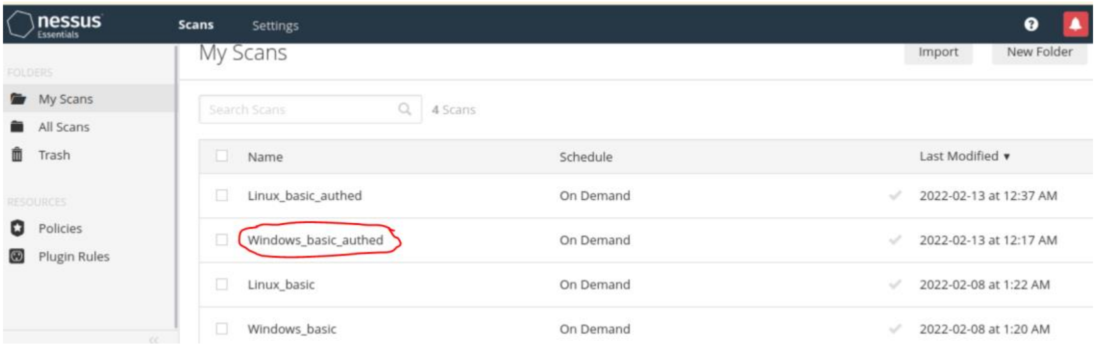
Nessus skill assessment:

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

Answer: wsus

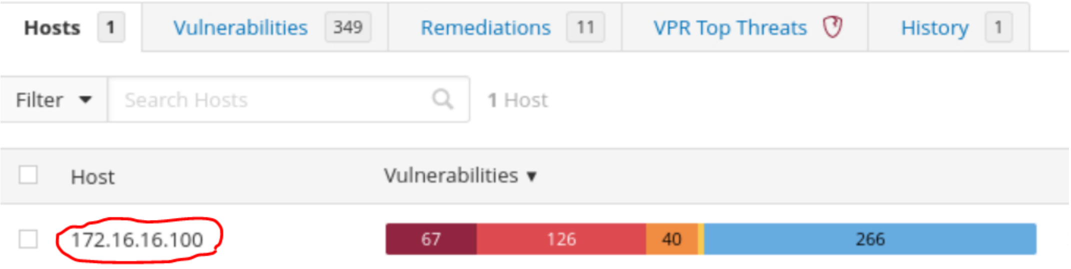
Method:

Enter to Windows_basic_authed



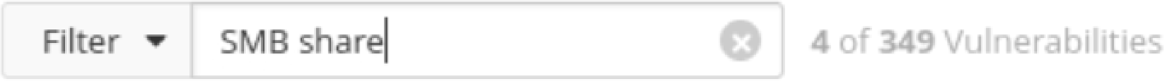
☐	Name	Schedule		Last Modified ▾
☐	Linux_basic_authed	On Demand	✓	2022-02-13 at 12:37 AM
☐	Windows_basic_authed	On Demand	✓	2022-02-13 at 12:17 AM
☐	Linux_basic	On Demand	✓	2022-02-08 at 1:22 AM
☐	Windows_basic	On Demand	✓	2022-02-08 at 1:20 AM

Select desired host:



☐	Host	Vulnerabilities ▾
☐	172.16.16.100	67 126 40 266

search for ‘SMB share’ on results:

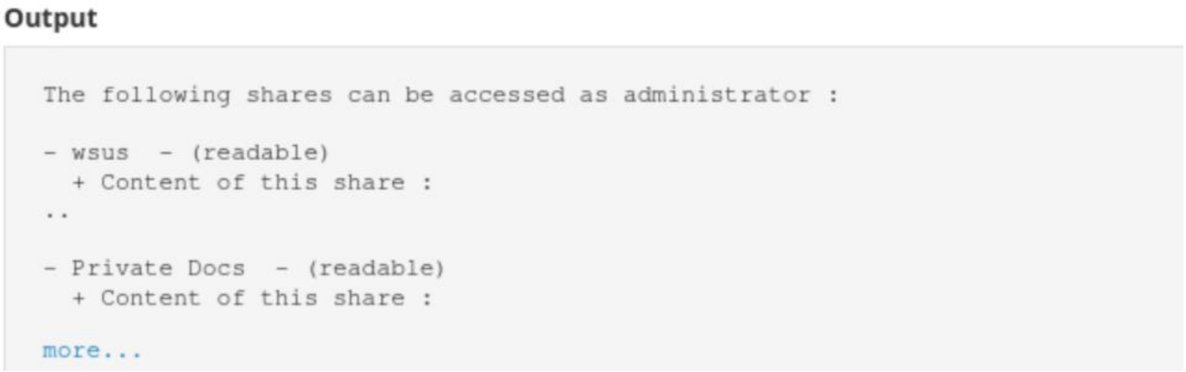


Filter ▾ | SMB share

4 of 349 Vulnerabilities

open the third option and observe on the output for: ‘The following shares can be accessed as administrator’..

You will spot one answer in the following list..



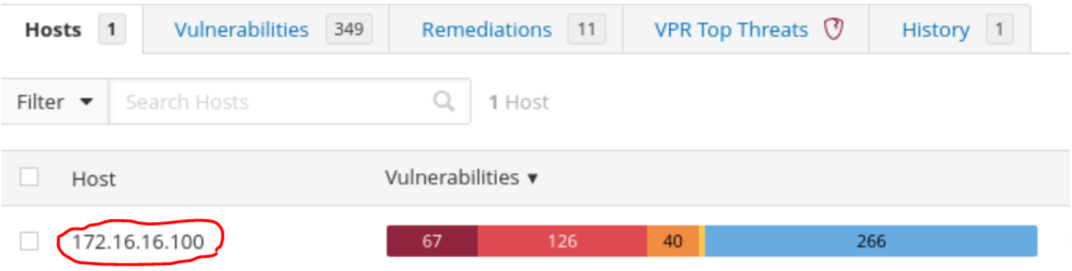
Output

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

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

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

more...
```

Question: What was the target for the authenticated scan?

Answer: 172.16.16.100

Method:



Hosts 1 | Vulnerabilities 349 | Remediations 11 | VPR Top Threats | History 1

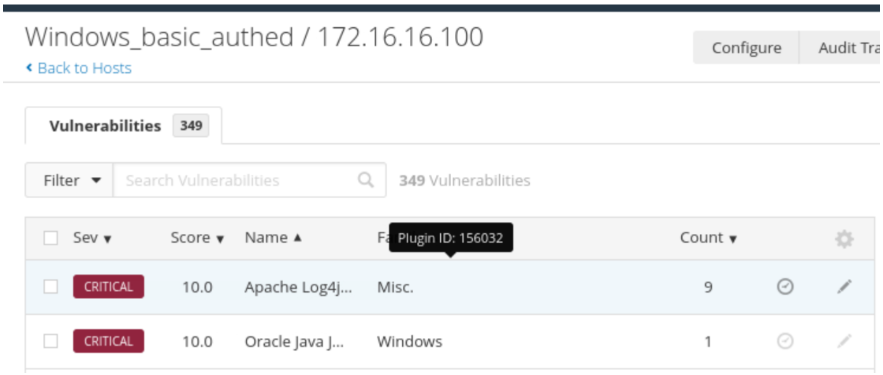
Filter ▾ | Search Hosts | 1 Host

□	Host	Vulnerabilities ▾
□	172.16.16.100	67 126 40 266

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

Answer: 156032

Method: observe the first vulnerability (highest up) ID



Windows_basic_authed / 172.16.16.100

‹ Back to Hosts

Vulnerabilities 349

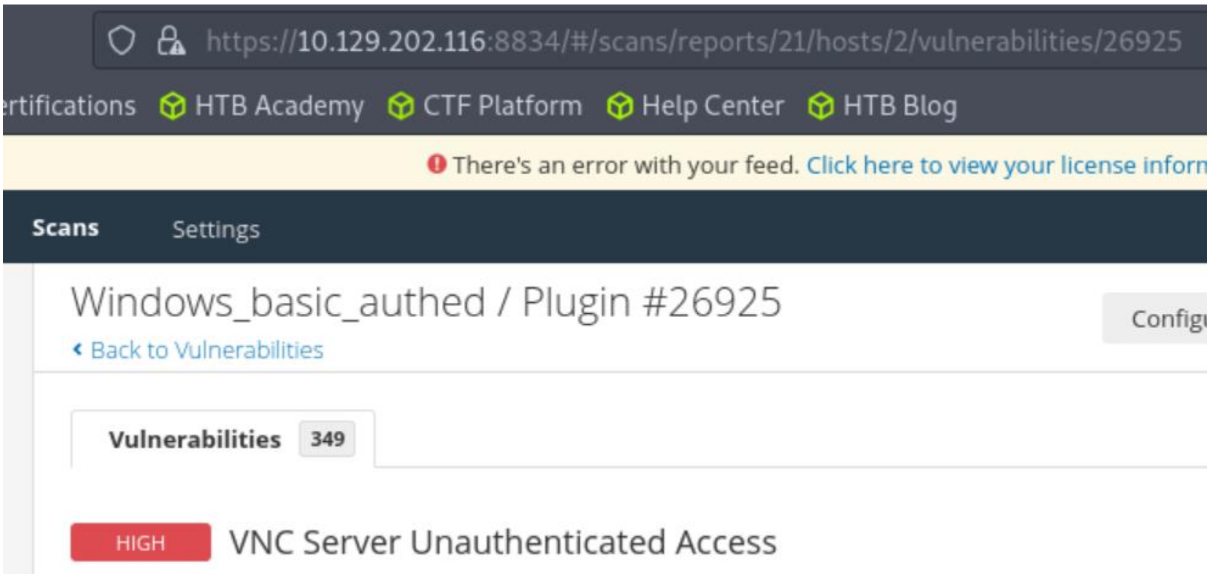
349 Vulnerabilities

Sev	Score	Name	Fa	Count
CRITICAL	10.0	Apache Log4j...	Misc.	9
CRITICAL	10.0	Oracle Java J...	Windows	1

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

Answer: VNC Server Unauthenticated Access

Method: enter '/156032 in url to search for the ID's vulnerability:



https://10.129.202.116:8834/#/scans/reports/21/hosts/2/vulnerabilities/26925

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

Windows_basic_authed / Plugin #26925

‹ Back to Vulnerabilities

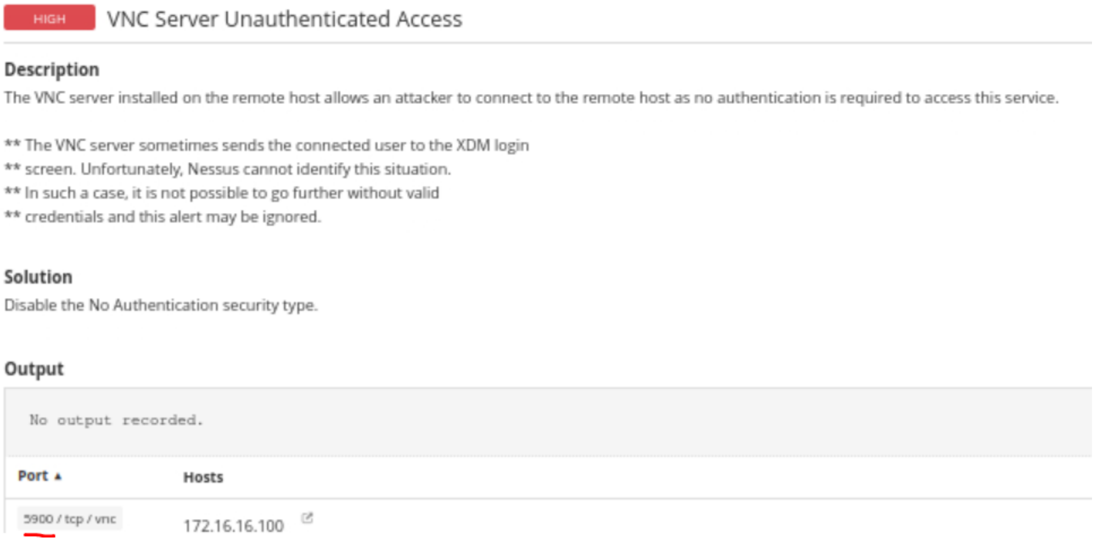
Vulnerabilities 349

HIGH VNC Server Unauthenticated Access

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

Answer: 5900

Method: on the same vulnerability from question above (ID 156032) – look for port number in vulnerability details



HIGH 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

```
No output recorded.
```

Port ▲	Hosts
5900 / tcp / vnc	172.16.16.100

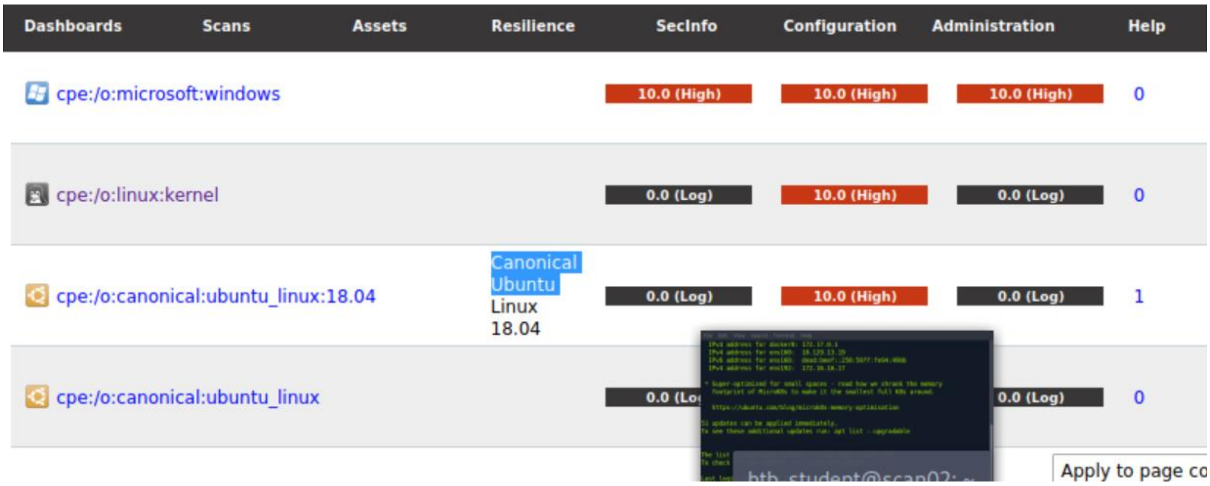
OpenVAS

OpenVAS skill assessment:

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

Answer: ubuntu

Method: Assets > opetating systems:

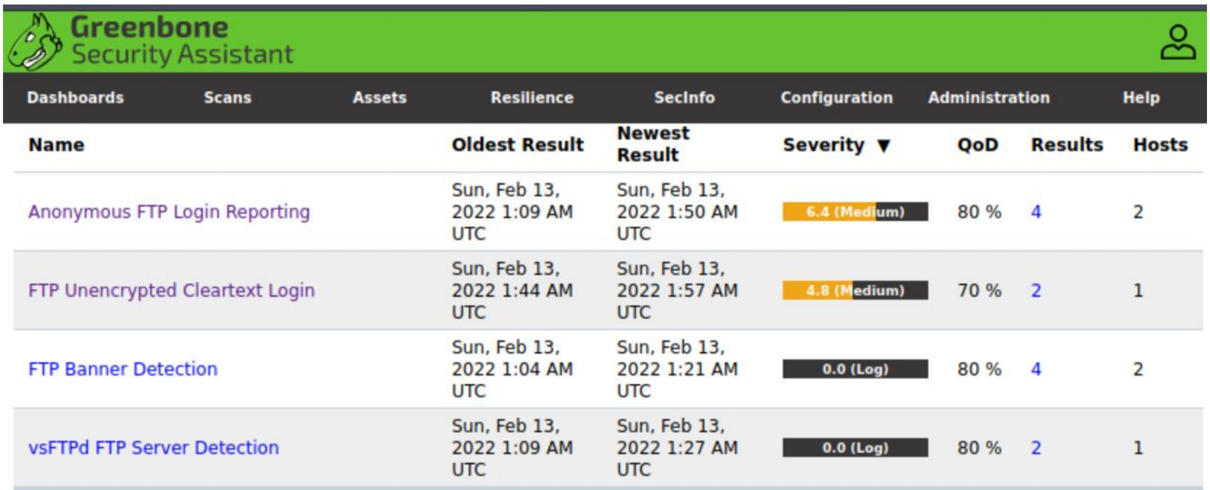


cpe:/o:microsoft:windows		10.0 (High)	10.0 (High)	10.0 (High)	0
cpe:/o:linux:kernel		0.0 (Log)	10.0 (High)	0.0 (Log)	0
cpe:/o:canonical:ubuntu_linux:18.04	Canonical Ubuntu Linux 18.04	0.0 (Log)	10.0 (High)	0.0 (Log)	1
cpe:/o:canonical:ubuntu_linux		0.0 (Lo		0.0 (Log)	0

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

Answer: Anonymous FTP Login Reporting

Method: Scans -> Vulnerabilities -> filter for 'ftp'



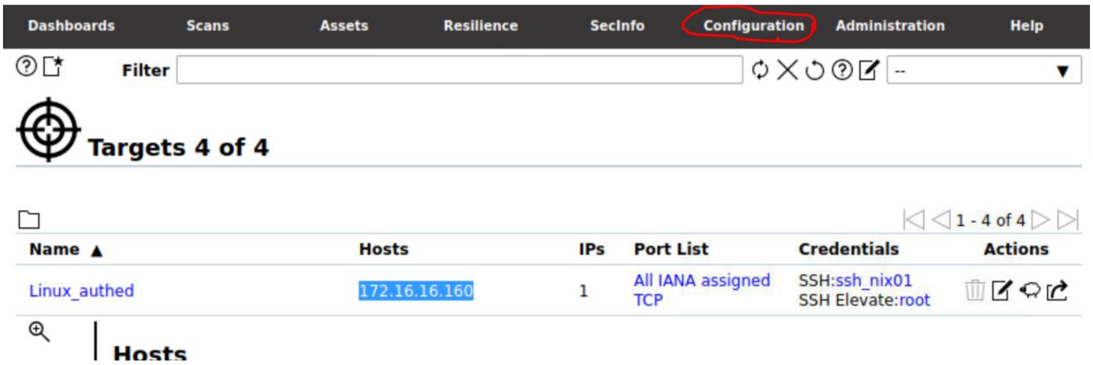
Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
Anonymous FTP Login Reporting	Sun, Feb 13, 2022 1:09 AM UTC	Sun, Feb 13, 2022 1:50 AM UTC	6.4 (Medium)	80 %	4	2
FTP Unencrypted Cleartext Login	Sun, Feb 13, 2022 1:44 AM UTC	Sun, Feb 13, 2022 1:57 AM UTC	4.8 (Medium)	70 %	2	1
FTP Banner Detection	Sun, Feb 13, 2022 1:04 AM UTC	Sun, Feb 13, 2022 1:21 AM UTC	0.0 (Log)	80 %	4	2
vsFTPd FTP Server Detection	Sun, Feb 13, 2022 1:09 AM UTC	Sun, Feb 13, 2022 1:27 AM UTC	0.0 (Log)	80 %	2	1

Cross checking with the hosts IP addresses revealed that out of the 2 vulnerabilities shown – the first one belongs to the Linux host, the second is to another irrelevant machine.

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

Answer: 172.16.16.160

Method: Configurations -> targets -> linux host:



Name ▲	Hosts	IPs	Port List	Credentials	Actions
Linux_authed	172.16.16.160	1	All IANA assigned TCP	SSH:ssh_nix01 SSH Elevate:root	

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

Answer: Cleartext Transmission of Sensitive Information via HTTP

Method: Scans -> Vulnerabilities -> filter for ‘http’.

Search for the vulnerability with the http keyword in it (NOT https)