ISSACK WAITHAKA
cs-sa07-24085

Security Assessments

- It is done to mainly to find and confirm vulnerabilities present so that we can patch, mitigate or remove them
- Black box pentesting is done with no knowledge of a network's configuration or application
- Grey box pentesting is done with little knowledge of the network
- White box pentesting is done with full access and knowledge of the network
- Vulnerability assessment looks for vulnerabilities without simulating attacks while penetration testing is mainly done by attacking the network or application
- Other types of assessments are: security audit, Bug bounties, Red Team assessment.
-

Vulnerability assessment

- Aim to identify and categorize risks for security weakness
- A vulnerability is a weakness or bug in system
- A threat is a malicious act performed by individuals with harmful intent.
- Exploit are any code or resources that can be used to take advantage of assets weakness
- Risk possibility of data or assets being destroyed

Common Vulnerability Scoring System

- This industry calculates the ratings of vulnerabilities
- This is calculated based on: Damage Potential, Reproducibility, Exploitability, Affected users and discoverability.

Common vulnerabilities and exposure

- It is a publicly available and known information-security vulnerabilities and exposure
- Each security issue has a CVE ID.

Vulnerability Scanning overview

- They do not exploit the vulnerabilities but need a human to manually validate scan issues
- Nesus is used to identify vulnerabilities in an environment. There are otherslike OpenVAS.

Nesus scan

- Can be configured by clicking New Scan and selecting a scan type
- Nesus also support credential scanning and also provide a lot of flexibility

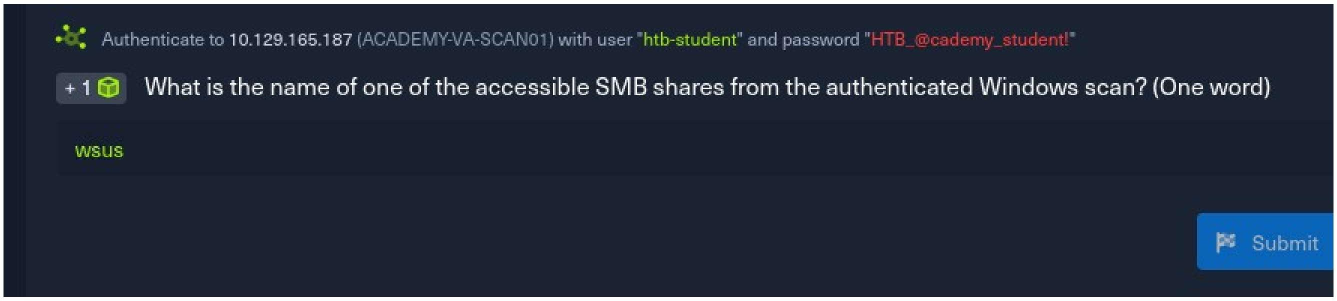
Advanced settings

- Nesus gives us an option to create a scan policy
- To create a scan policy we can click on the new policy button on top of the page and choose a scan type then choose advanced to create fully customized scan
- After that we click save and the new policy will appear
- Nesus works with plugins which contains information such as vulnerability name, impact, remediation. This plugins can target new vulnerabilities and CVEs

Nesus Skills Assessments

I launched the windows_basic_authed scan

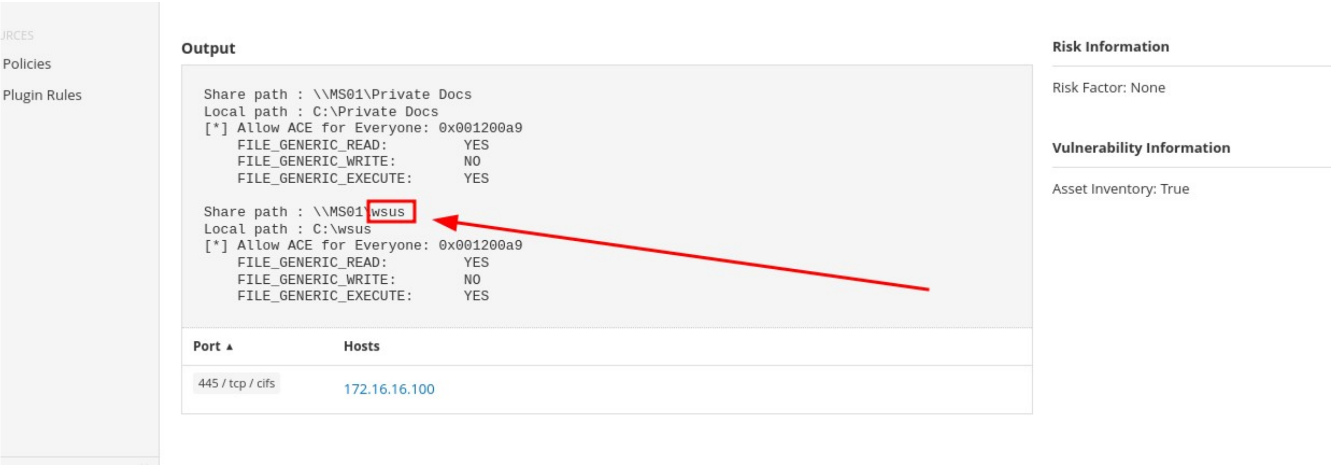
1.



Authenticate to 10.129.165.187 (ACADEMY-VA-SCAN01) with user "htb-student" and password "HTB_@cademy_student!"

+ 1 What is the name of one of the accessible SMB shares from the authenticated Windows scan? (One word)

wsus



Output

```
Share path : \\MS01\Private Docs
Local path : C:\Private Docs
[*] Allow ACE for Everyone: 0x001200a9
    FILE_GENERIC_READ:          YES
    FILE_GENERIC_WRITE:         NO
    FILE_GENERIC_EXECUTE:       YES

Share path : \\MS01\wsus
Local path : C:\wsus
[*] Allow ACE for Everyone: 0x001200a9
    FILE_GENERIC_READ:          YES
    FILE_GENERIC_WRITE:         NO
    FILE_GENERIC_EXECUTE:       YES
```

Port ▲	Hosts
445 / tcp / cifs	172.16.16.100

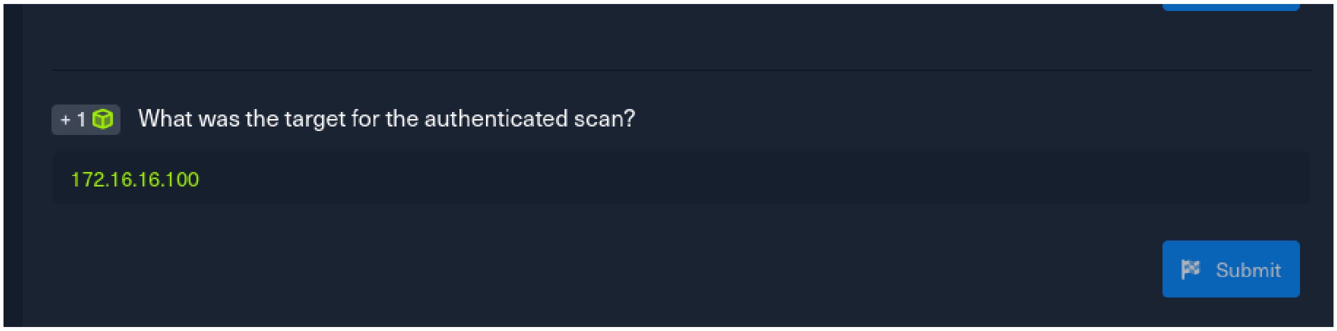
Risk Information

Risk Factor: None

Vulnerability Information

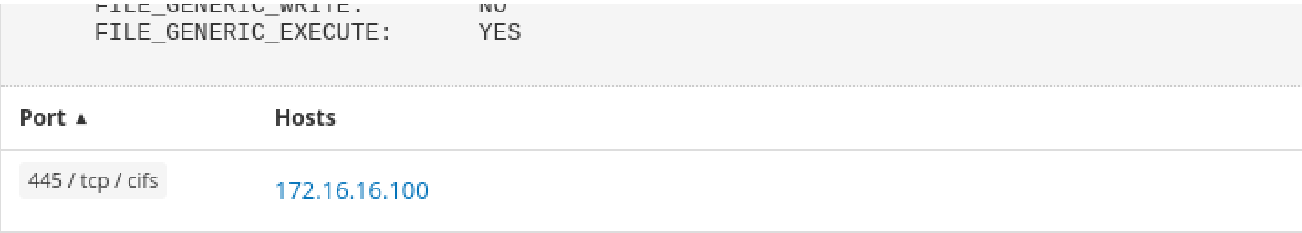
Asset Inventory: True

2.



+1 What was the target for the authenticated scan?

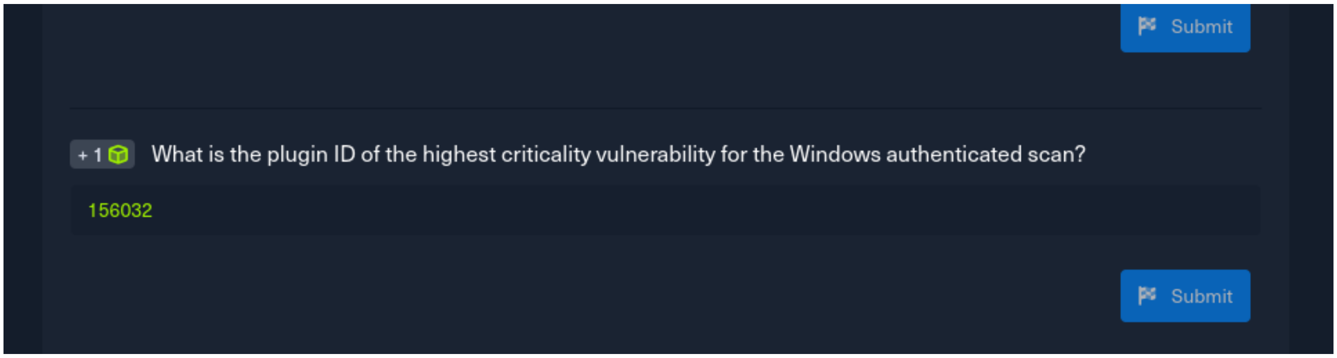
172.16.16.100



```
    FILE_GENERIC_WRITE:        NO
    FILE_GENERIC_EXECUTE:      YES
```

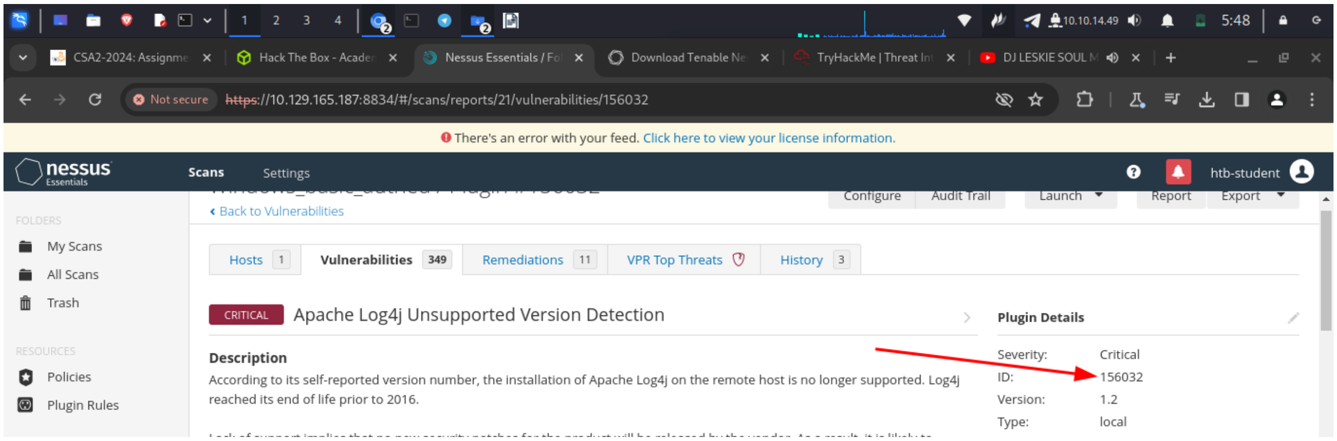
Port ▲	Hosts
445 / tcp / cifs	172.16.16.100

3.



+1 What is the plugin ID of the highest criticality vulnerability for the Windows authenticated scan?

156032



Not secure https://10.129.165.187:8834/#/scans/reports/21/vulnerabilities/156032

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

CRITICAL Apache Log4j Unsupported Version Detection

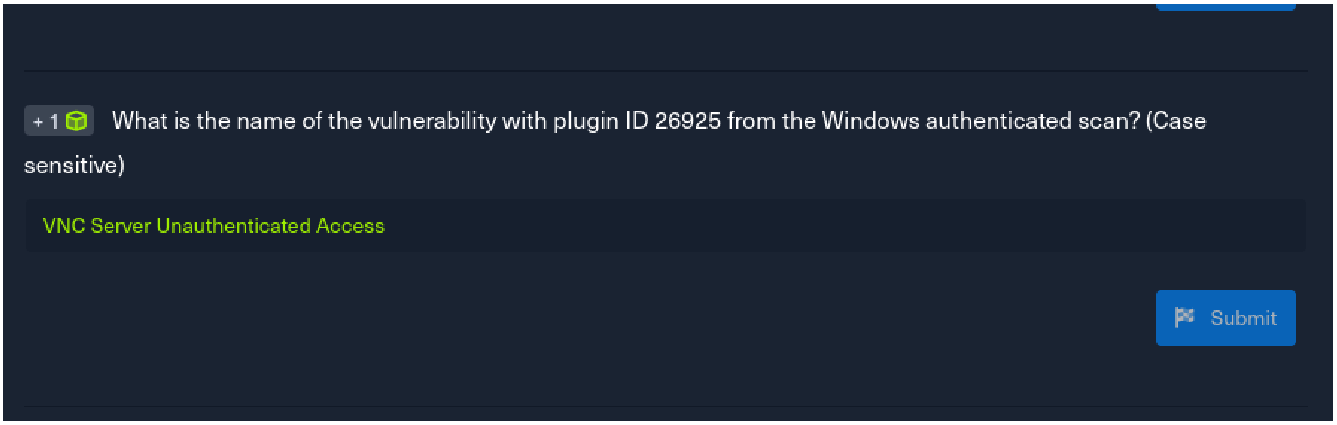
Description

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.

Plugin Details

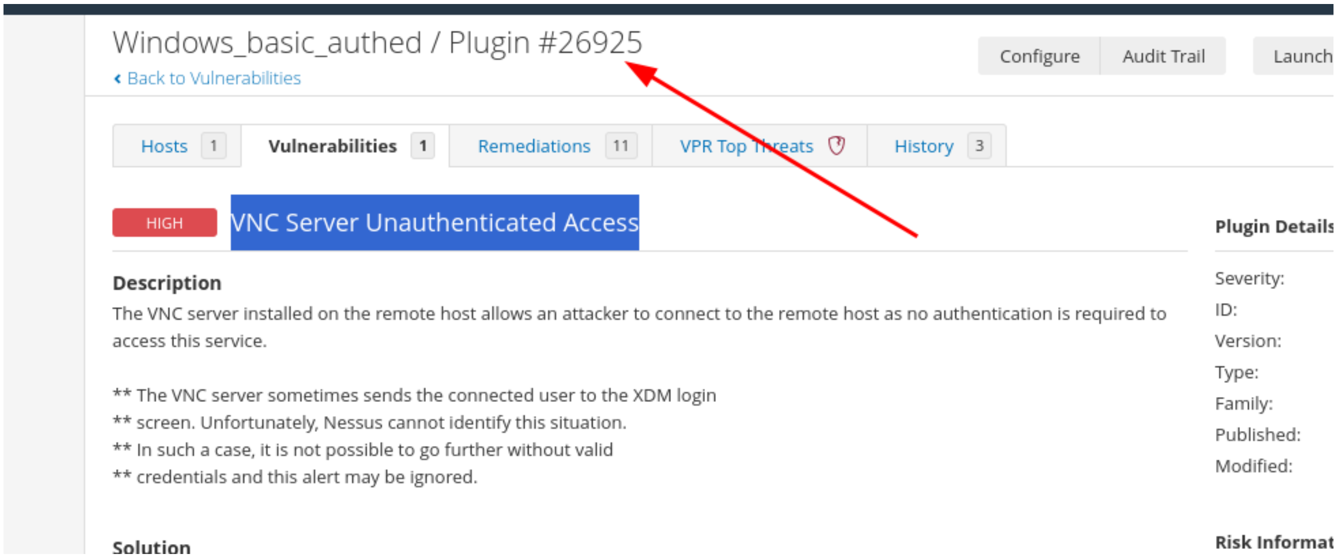
Severity:	Critical
ID:	156032
Version:	1.2
Type:	local

4.



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

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.
```

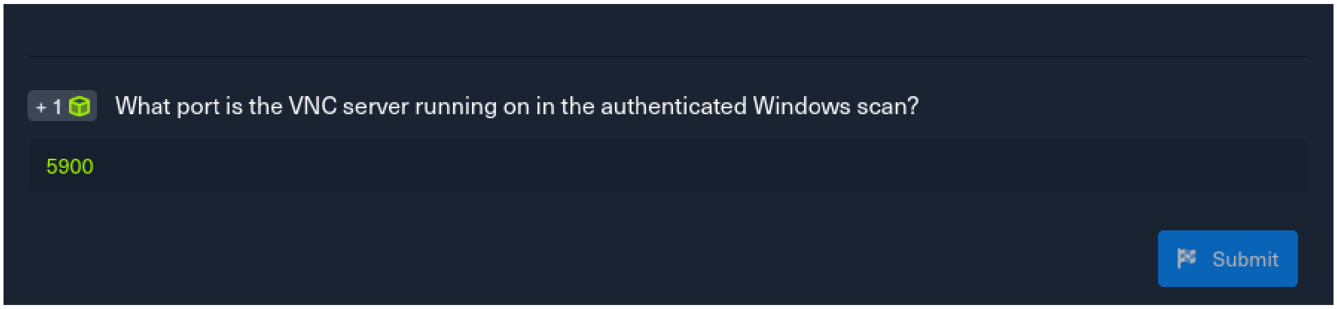
Solution

Plugin Details

Severity:
ID:
Version:
Type:
Family:
Published:
Modified:

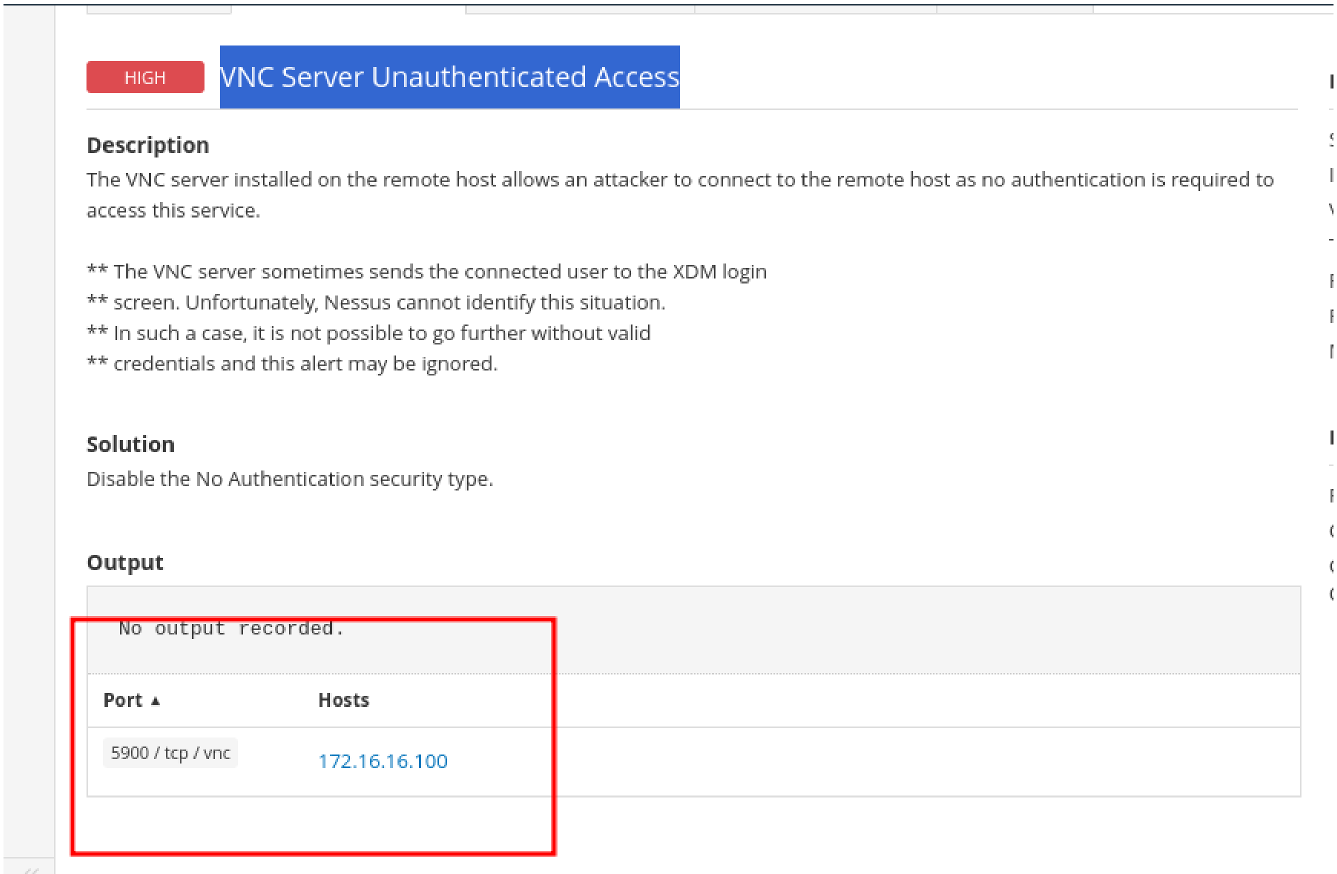
Risk Informat

5.



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

5900



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.
```

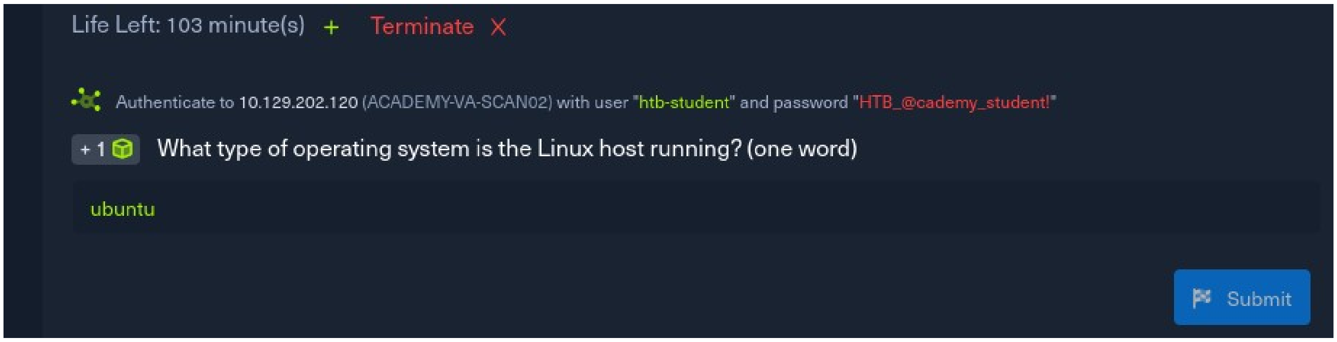
Port ▲	Hosts
5900 / tcp / vnc	172.16.16.100

OpenVAS

- It is a publicly available vulnerability scanner
- We installed and configured it

Questions

1.

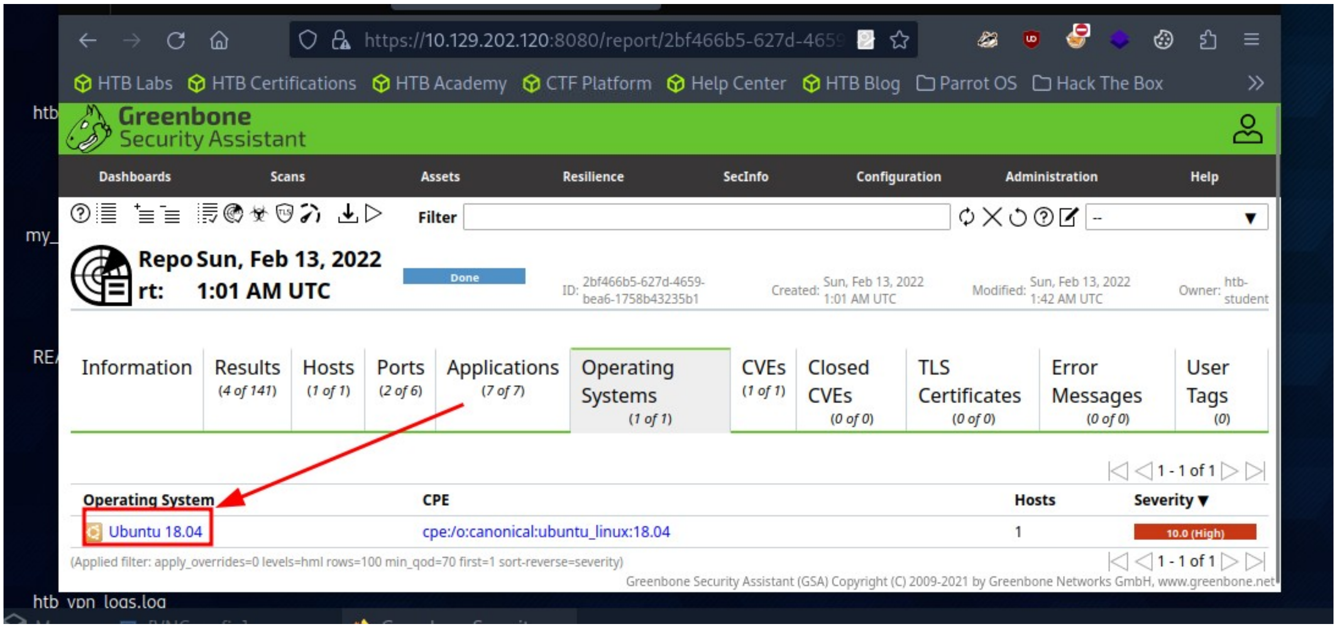


Life Left: 103 minute(s) + Terminate ✕

Authenticate to 10.129.202.120 (ACADEMY-VA-SCAN02) with user "htb-student" and password "HTB_@cademy_student!"

+ 1 What type of operating system is the Linux host running? (one word)

ubuntu



Report: Sun, Feb 13, 2022 1:01 AM 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)

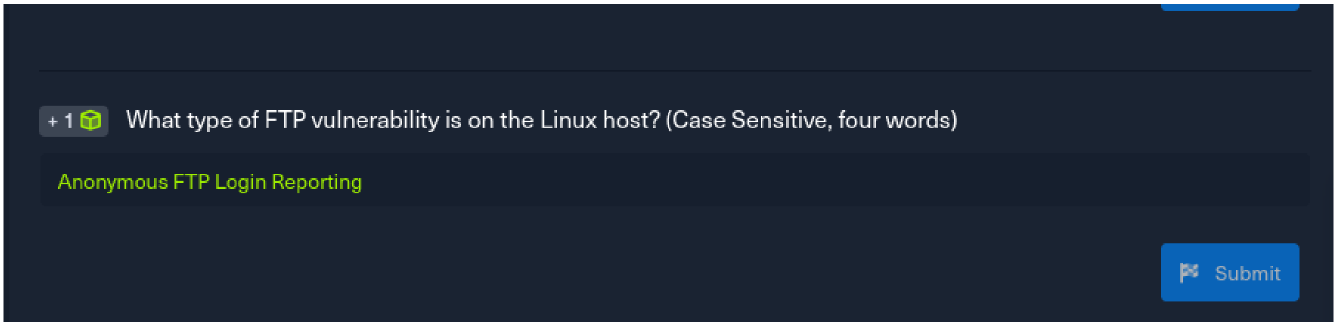
1 - 1 of 1

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)

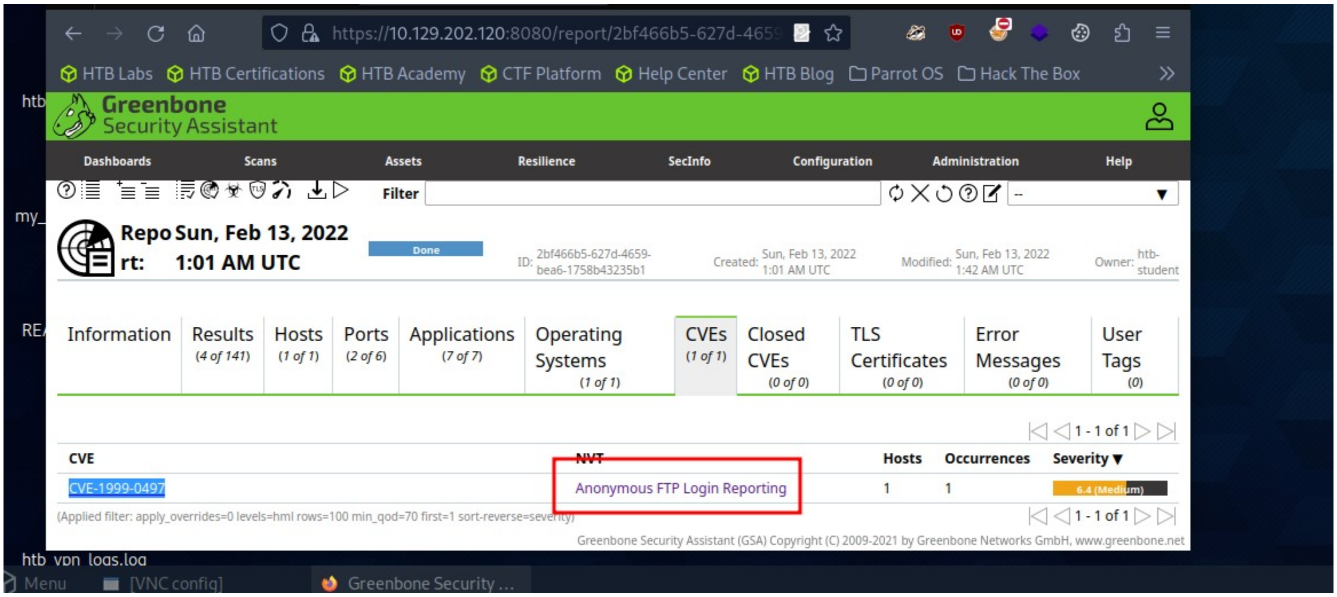
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

2.



+ 1 What type of FTP vulnerability is on the Linux host? (Case Sensitive, four words)

Anonymous FTP Login Reporting



Report: Sun, Feb 13, 2022 1:01 AM 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)

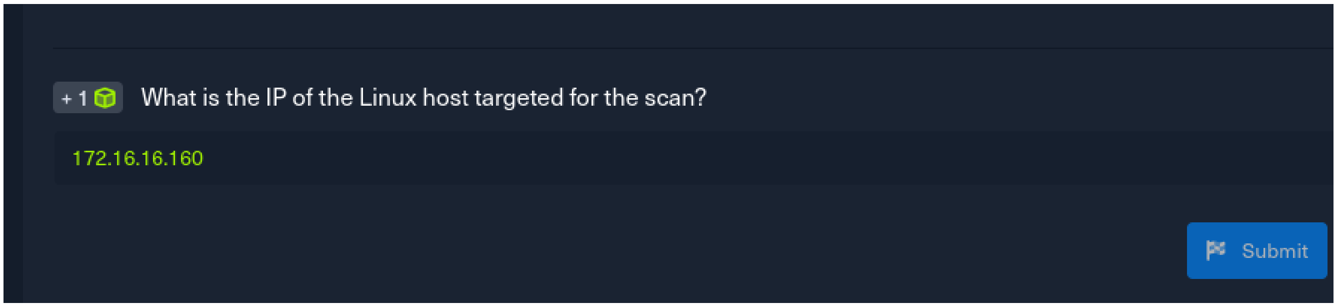
1 - 1 of 1

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0497	Anonymous FTP Login Reporting	1	1	6.4 (Medium)

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

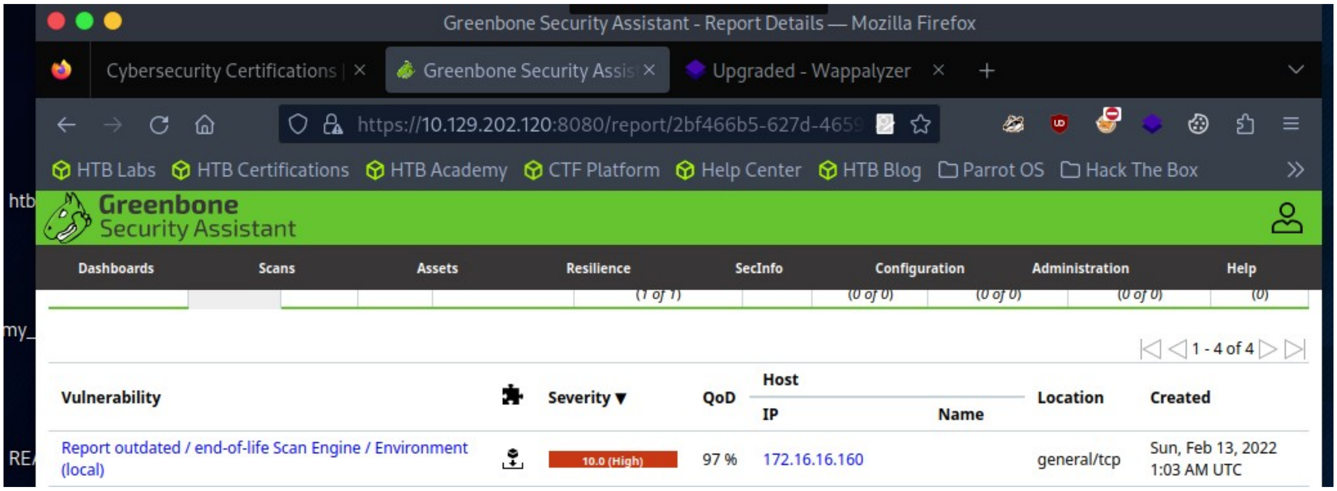
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

3.



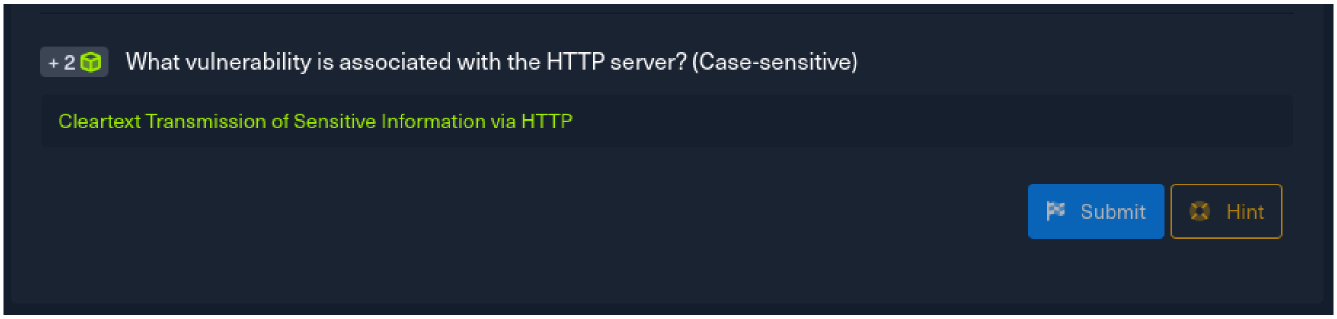
+1 What is the IP of the Linux host targeted for the scan?

172.16.16.160



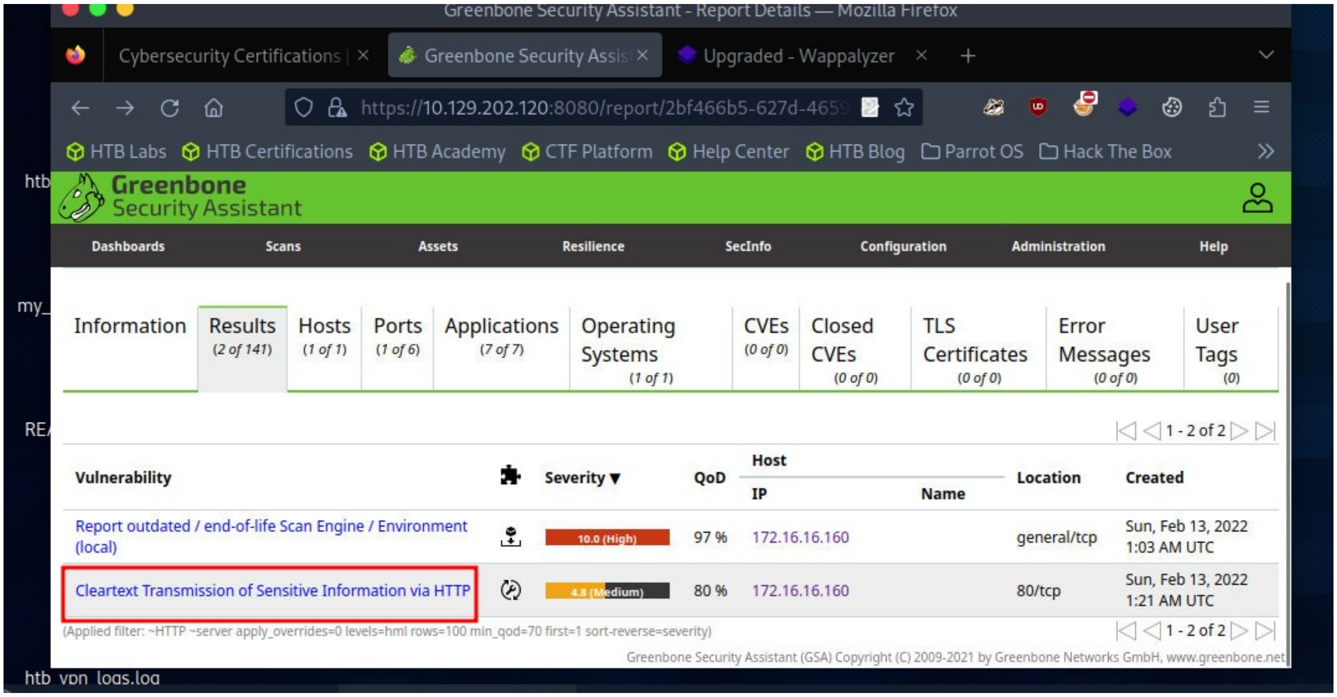
Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	172.16.16.160		general/tcp	Sun, Feb 13, 2022 1:03 AM UTC

4.



+2 What vulnerability is associated with the HTTP server? (Case-sensitive)

Cleartext Transmission of Sensitive Information via HTTP



Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	172.16.16.160		general/tcp	Sun, Feb 13, 2022 1:03 AM UTC
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80 %	172.16.16.160		80/tcp	Sun, Feb 13, 2022 1:21 AM UTC

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

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