Vulnerability Assessment

INTRODUCTION

Security assessments are crucial for organizations to identify and address vulnerabilities in their networks, computers, and applications. These assessments help in patching, mitigating, or removing vulnerabilities, enhancing overall cybersecurity.

Types of Security Assessments:
1. **Vulnerability Assessments:**
• Suitable for all organizations.
• Based on security standards relevant to the organizationâ€™s industry, size, network type, and security maturity.
• May be performed independently or alongside other assessments.
• Involves compliance checks and vulnerability scans to identify potential issues.

• **Penetration Tests (Pentests):**
◇ Simulate cyber attacks to determine how vulnerabilities can be exploited.
◇ Conducted with legal consent and aim to improve security based on detailed reports.
◇ Types of pentests:■ **Black Box:** No prior knowledge of the network.
■ **Grey Box:** Limited knowledge, similar to an insider with restricted access.
■ **White Box:** Full access to systems and configurations.

◇ Specialized areas include application, network/infrastructure, physical, and social engineering pentests.
◇ Appropriate for organizations with medium to high security maturity levels.

• **Security Audits:**
◇ Mandated by external entities to ensure compliance with specific regulations (e.g., PCI-DSS).
◇ Organizations need to conduct vulnerability assessments to prepare for audits.

• **Bug Bounties:**
◇ Programs inviting the public to find and report vulnerabilities for monetary rewards.
◇ Suitable for large, mature organizations with the resources to manage and analyze bug reports.

• **Red Team Assessments:**
◇ Performed by experienced offensive security professionals.
◇ Simulate comprehensive cyber attacks with specific goals.
◇ Focus on critical vulnerabilities leading to the achievement of the goal, rather than all vulnerabilities.
◇ Suitable for organizations with advanced security maturity.

• **Purple Team Assessments:**
◇ Collaboration between offensive (red team) and defensive (blue team) security specialists.
◇ Aim to enhance security by combining red team insights with blue team defenses.
◇ Blue team is actively involved in the assessment process.

Comparison: Vulnerability Assessments vs. Penetration Tests:

◇ **Vulnerability Assessments:■** Identify potential vulnerabilities based on compliance standards.

■ Regularly performed to maintain security posture.

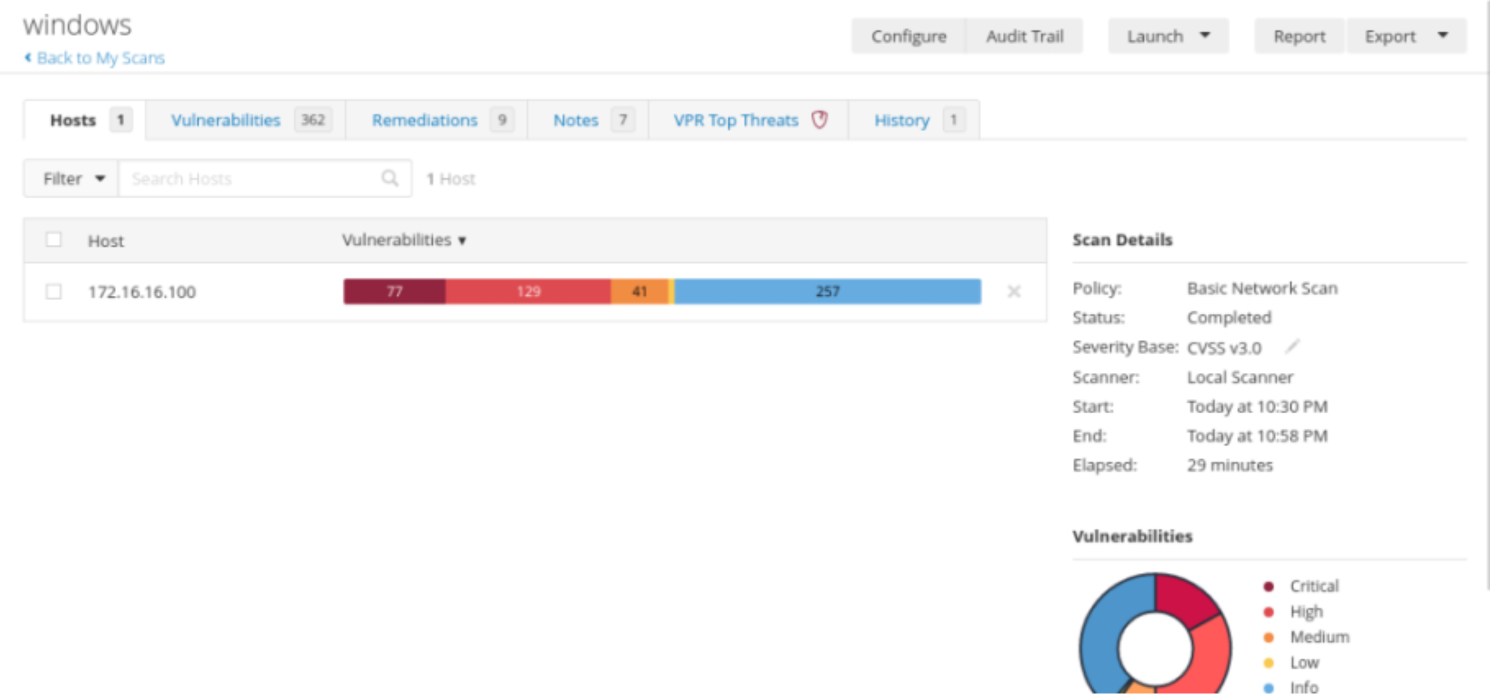
◇ **Penetration Tests:■** Simulate real-world attacks to exploit vulnerabilities.

■ Provide a deeper understanding of security weaknesses and their potential impact.

■ Recommended after vulnerability assessments have established a baseline security level.

Below is my approach on how I tackled each question.

So this is a screenshot of my complete scan using nessus against a windows machine.

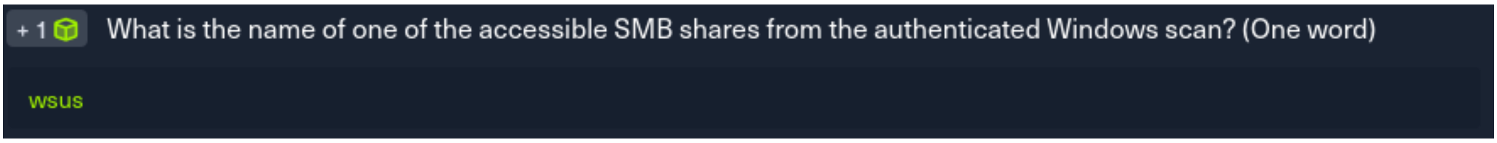


☐ Host	Vulnerabilities ▾
☐ 172.16.16.100	77 129 41 257

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:30 PM
End: Today at 10:58 PM
Elapsed: 29 minutes

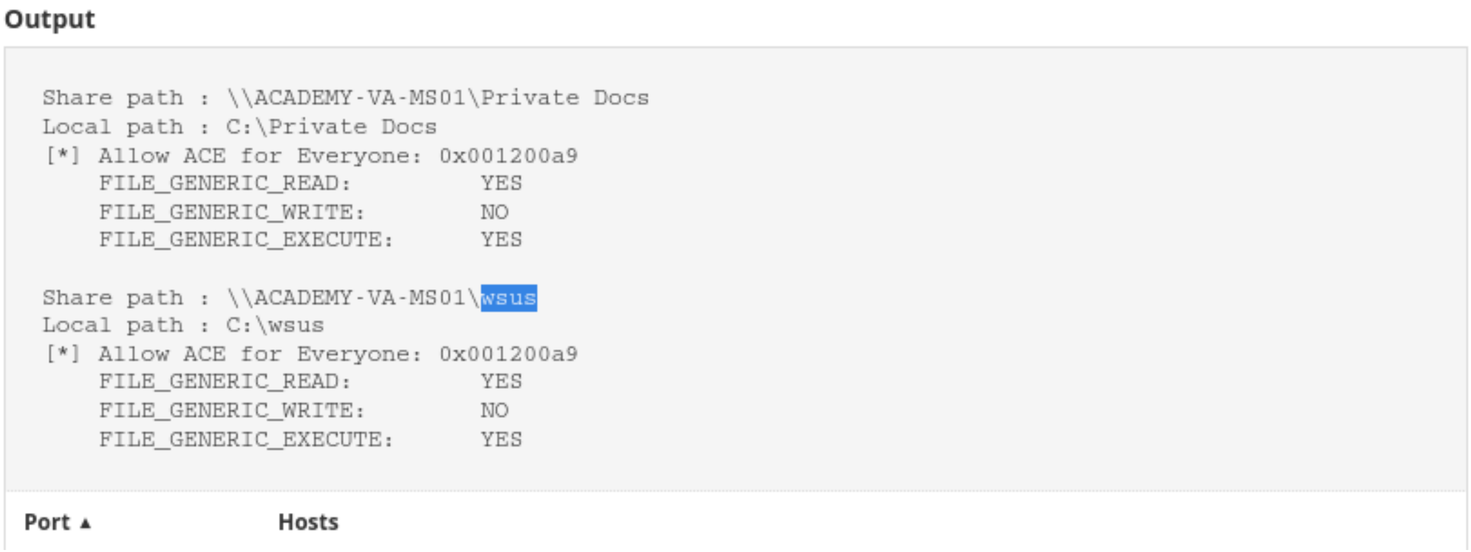
Vulnerabilities



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

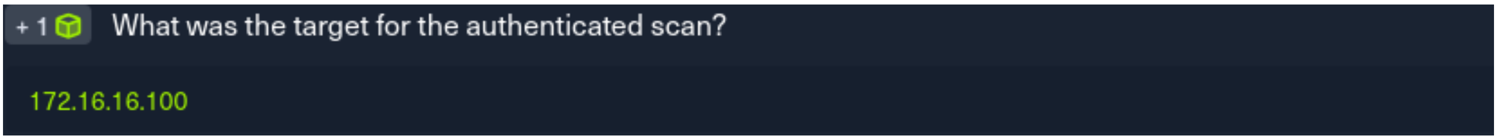
wsus

So from the image below, the share path : wsus as one of the accesssible smb shares.



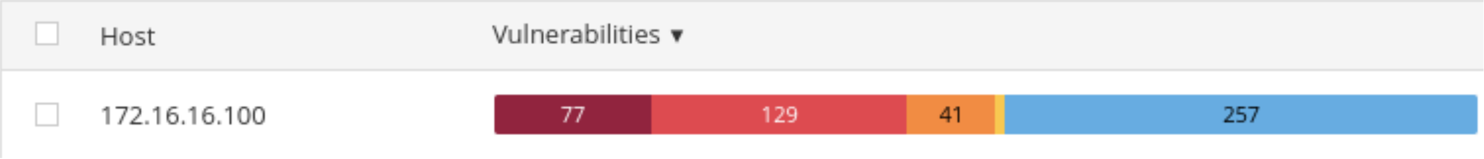
Output

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

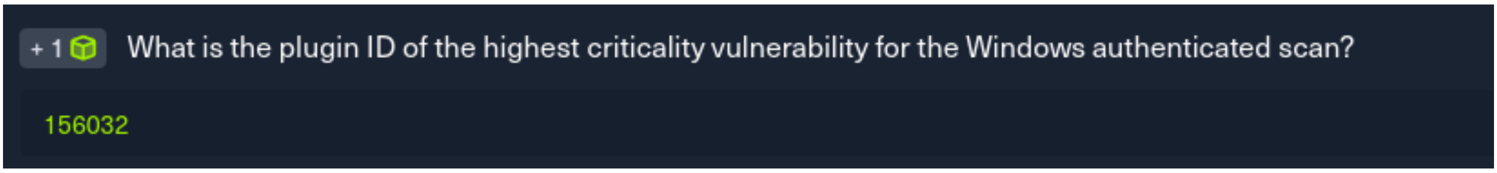


+1 What was the target for the authenticated scan?

172.16.16.100

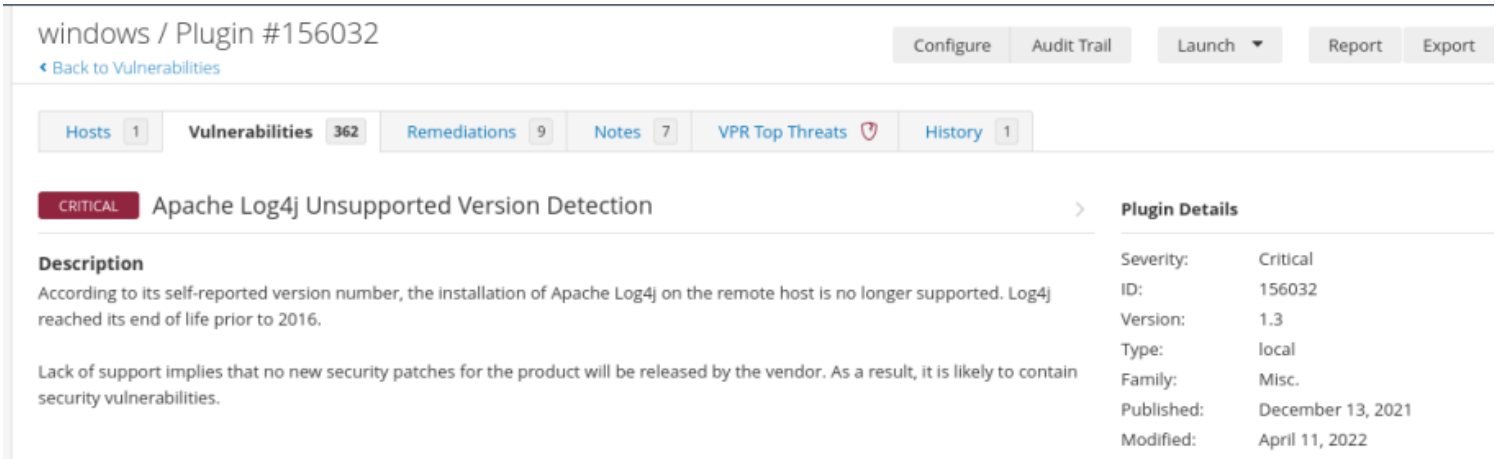


□	Host	Vulnerabilities ▾
□	172.16.16.100	77 129 41 257



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

156032



windows / Plugin #156032

CRITICAL Apache Log4j Unsupported Version Detection

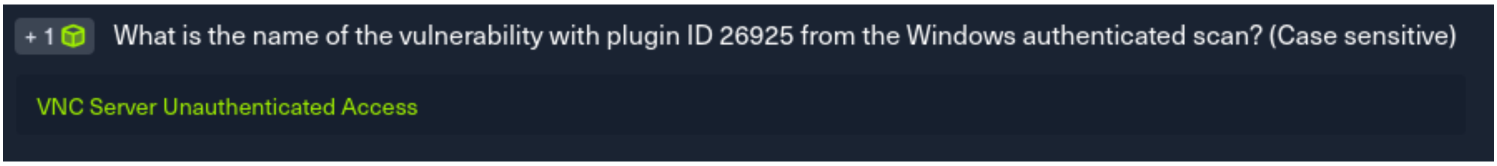
Description

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.

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.

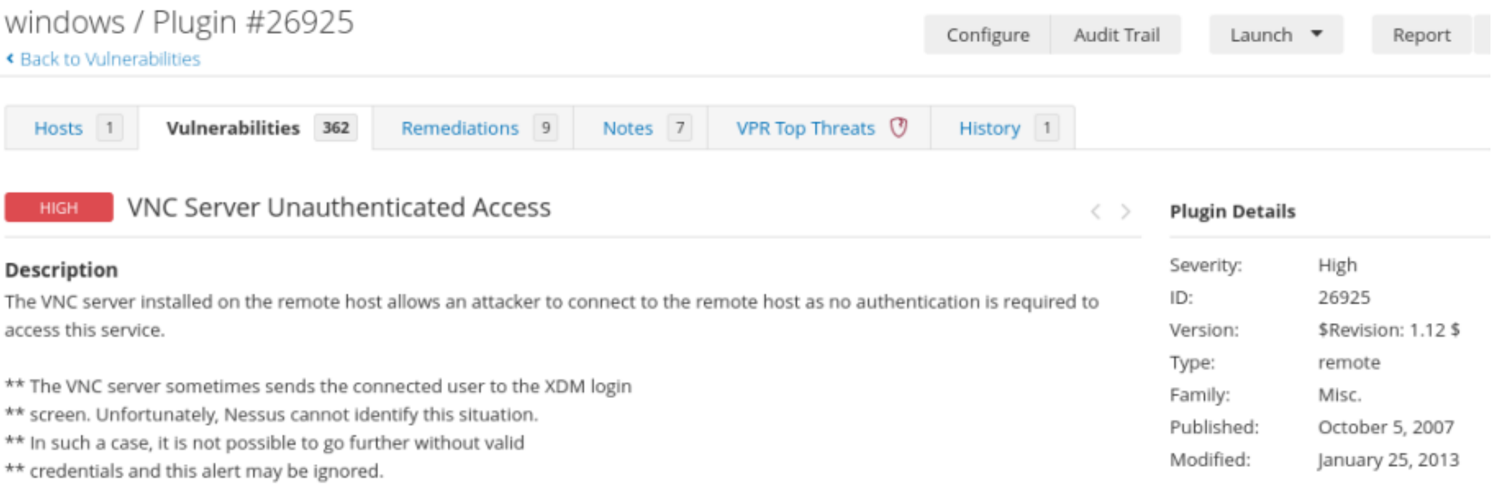
Plugin Details

Severity:	Critical
ID:	156032
Version:	1.3
Type:	local
Family:	Misc.
Published:	December 13, 2021
Modified:	April 11, 2022



+1 What is the name of the vulnerability with plugin ID 26925 from the Windows authenticated scan? (Case sensitive)

VNC Server Unauthenticated Access



VNC Server Unauthenticated Access

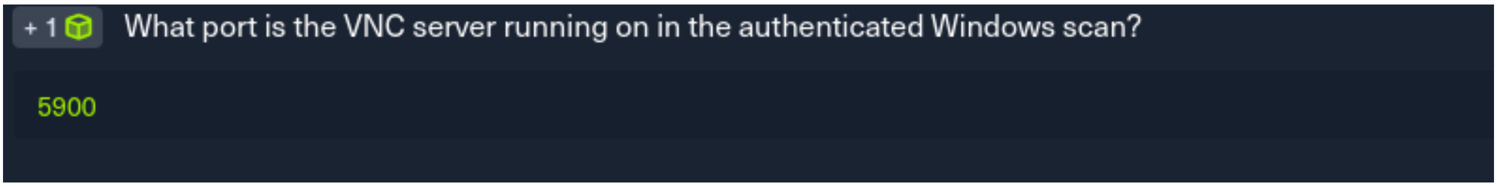
Description

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.
```

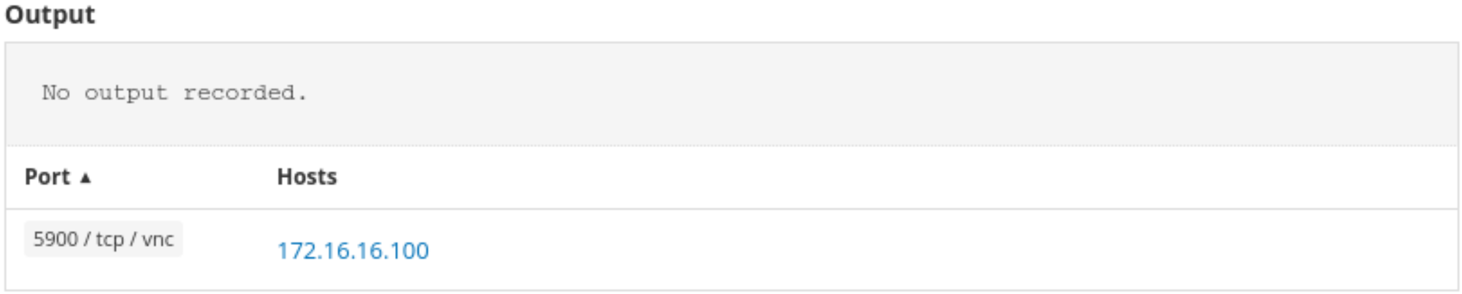
Plugin Details

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



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

5900

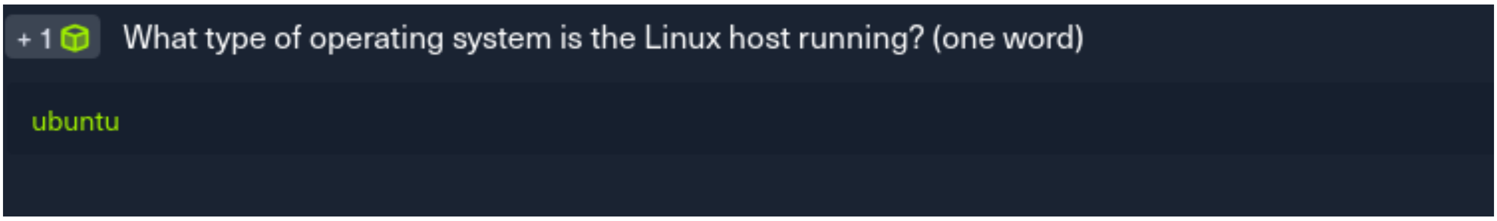


Output

```
No output recorded.
```

Port ▲	Hosts
5900 / tcp / vnc	172.16.16.100

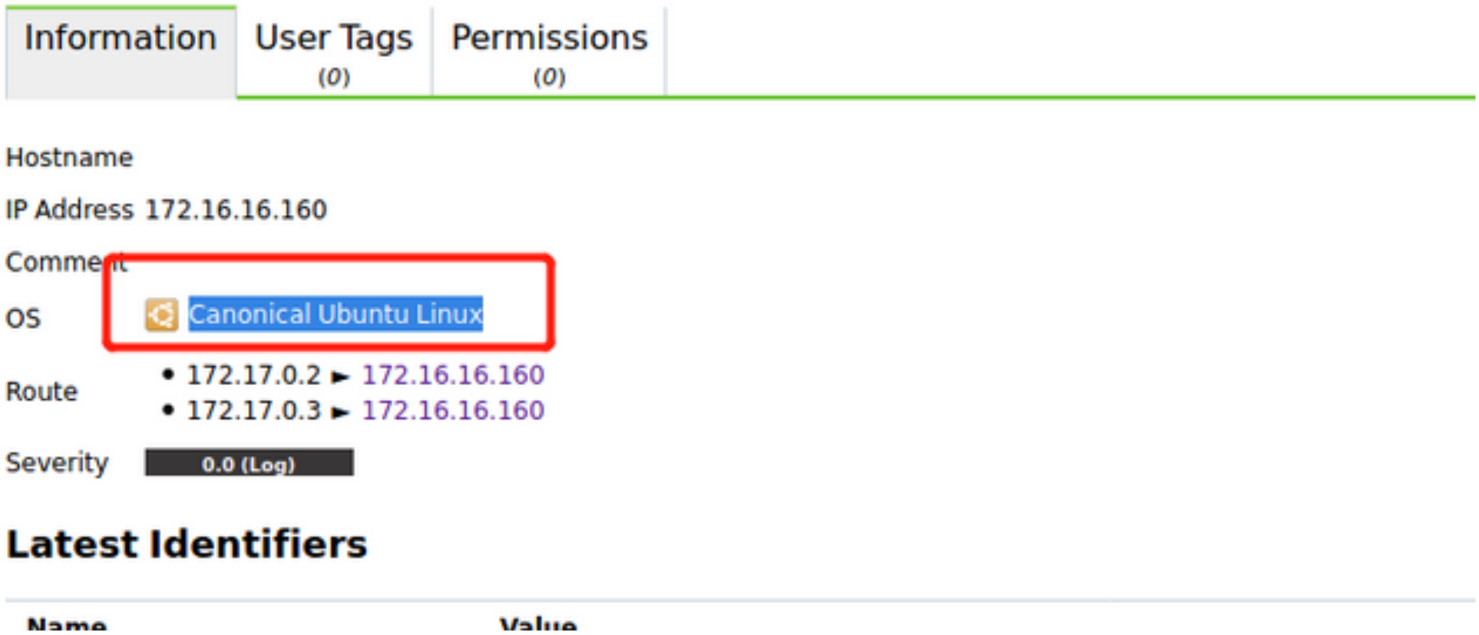
The images below shows how I approached a linux machine for a vulnerability assessment using openvas.



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

ubuntu

From the image below, ubuntu was the type of os the linux host was running on.



Hostname

IP Address 172.16.16.160

Comment

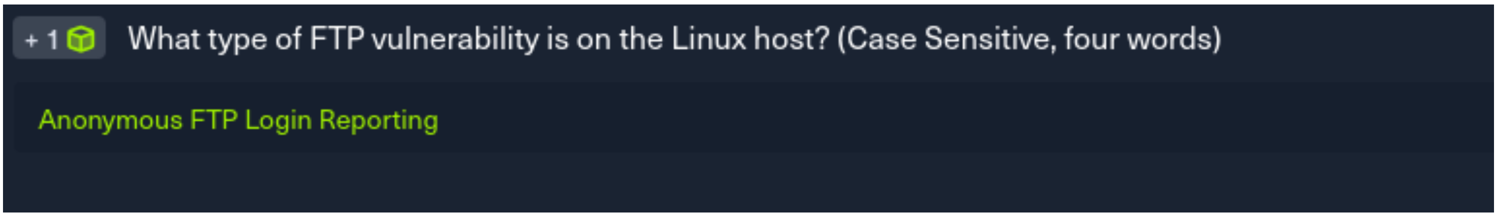
OS Canonical Ubuntu Linux

Route
- 172.17.0.2 ► 172.16.16.160
- 172.17.0.3 ► 172.16.16.160

Severity 0.0 (Log)

Latest Identifiers

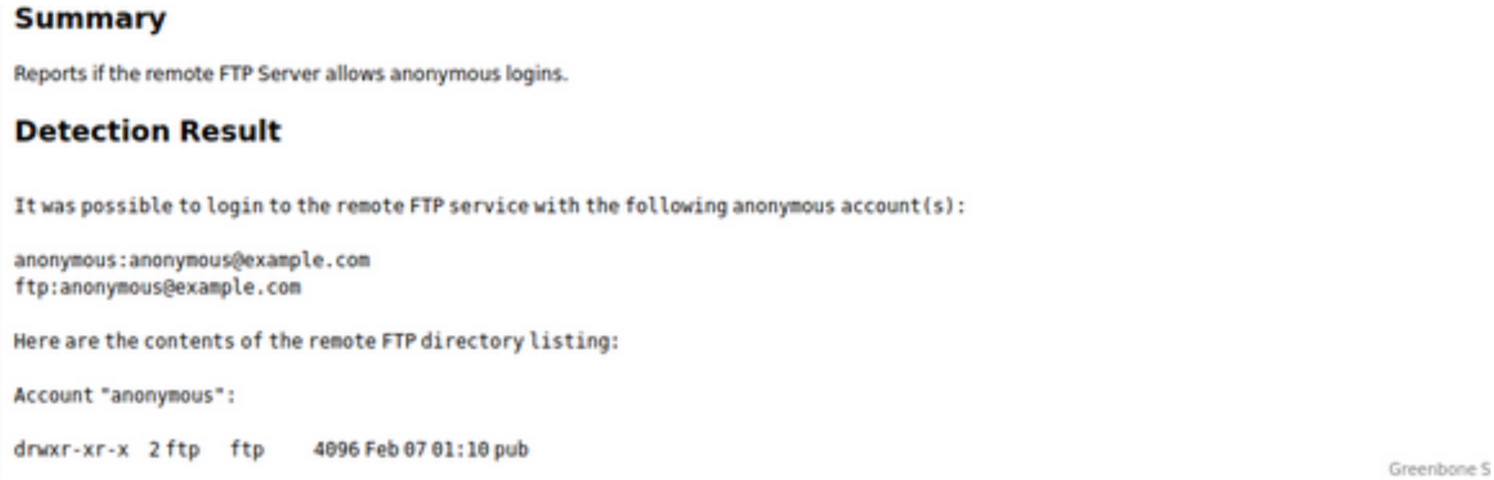
Name	Value



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

Anonymous FTP Login Reporting

The linux host allowed anonymous ftp login, and this could be leveraged by an attacker to cause more impact on the target.

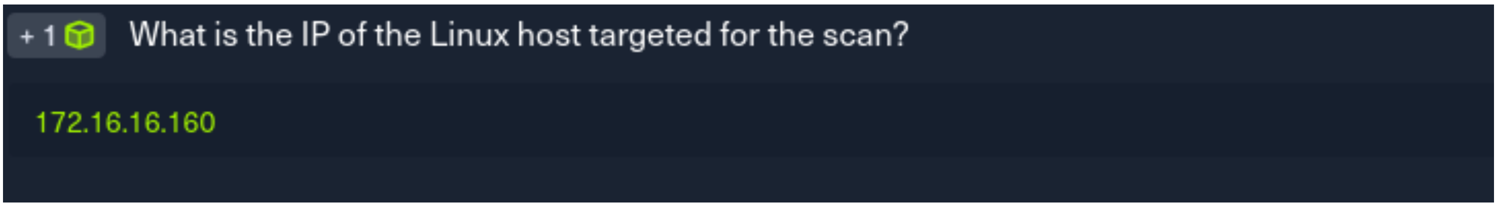


Summary

Reports if the remote FTP Server allows anonymous logins.

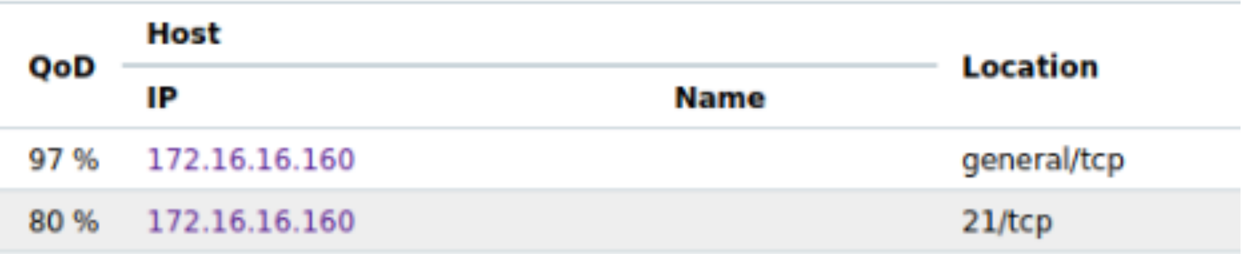
Detection Result

```
It was possible to login to the remote FTP service with the following anonymous account(s):

anonymous:anonymous@example.com
ftp:anonymous@example.com

Here are the contents of the remote FTP directory listing:

Account "anonymous":

drwxr-xr-x   2 ftp    ftp      4096 Feb 07 01:10 pub
```

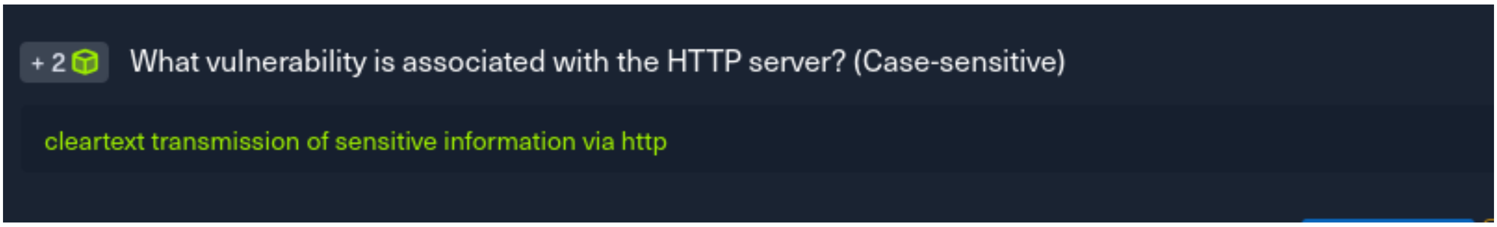


What is the IP of the Linux host targeted for the scan?

172.16.16.160



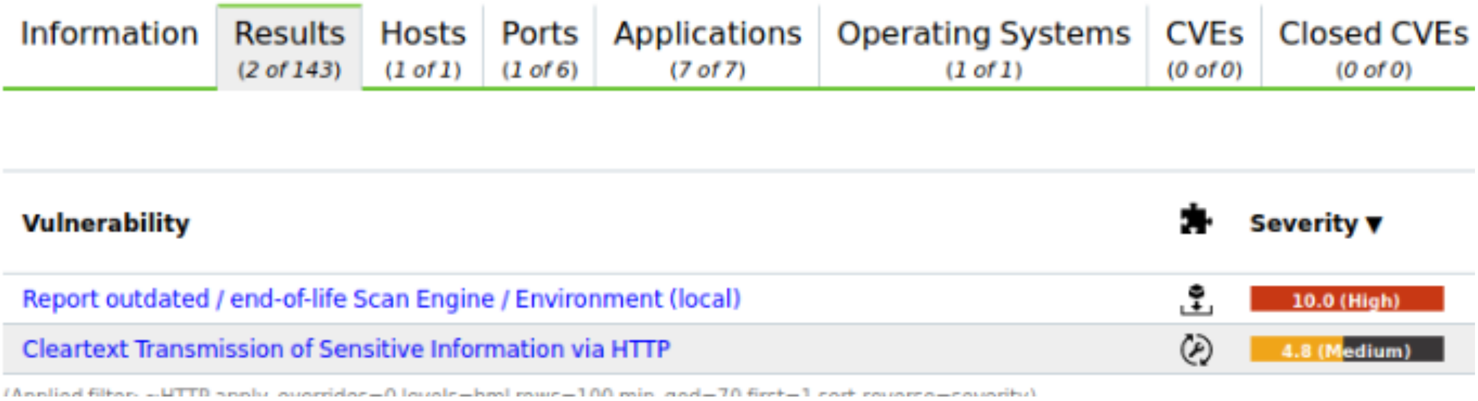
QoD	Host		Location
	IP	Name	
97 %	172.16.16.160		general/tcp
80 %	172.16.16.160		21/tcp



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

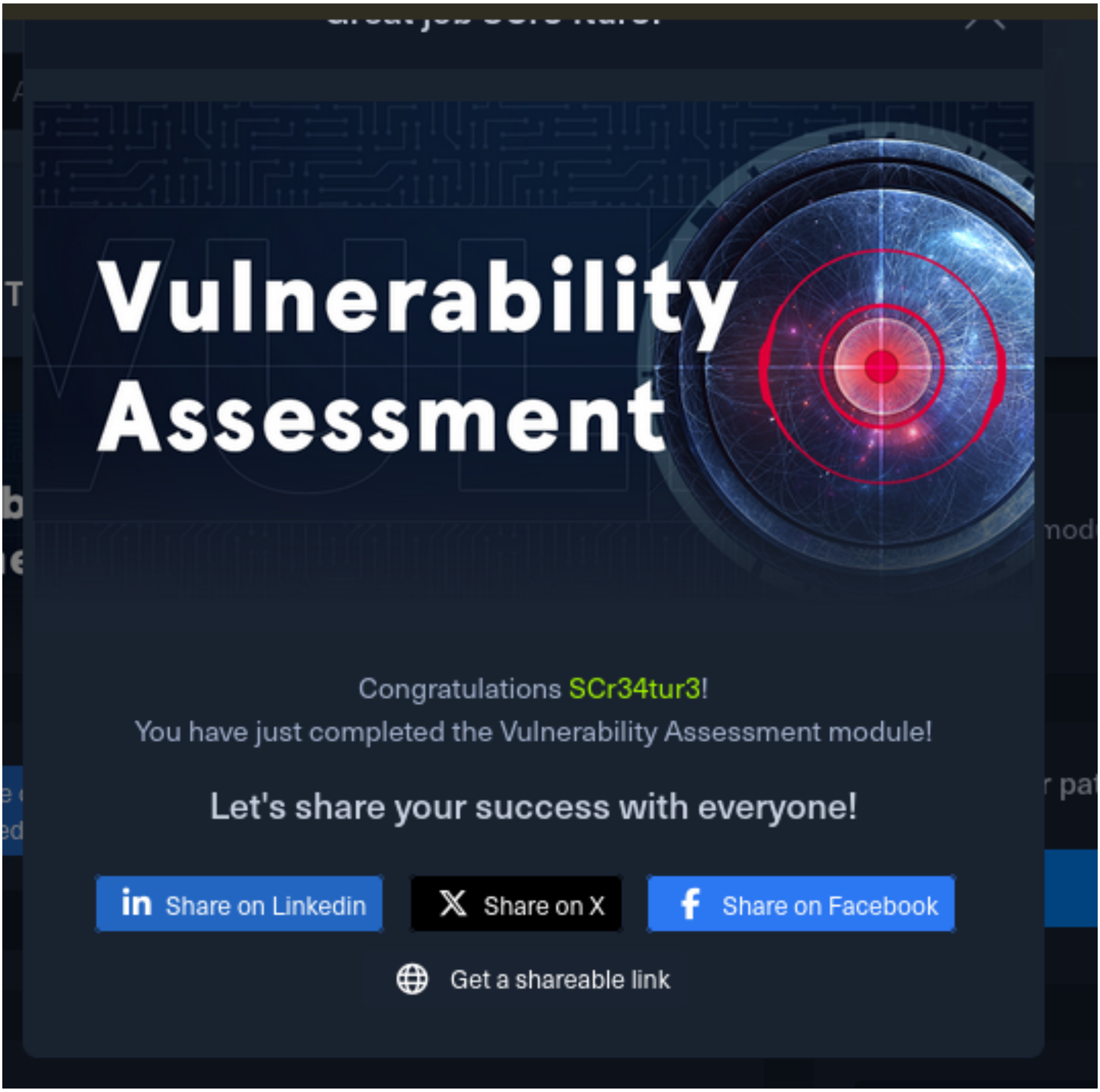
cleartext transmission of sensitive information via http

The http server allowed tramsmission of data in cleartext, and this can lead to compromise of the CIA when this data falls into unintended users.



Vulnerability		Severity ▼
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)

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



Congratulations SCr34tur3!

You have just completed the Vulnerability Assessment module!

Let's share your success with everyone!

https://academy.hackthebox.com/achievement/1287818/108

Conclusion:

Organizations must choose the appropriate type of security assessment based on their security maturity, specific needs, and compliance requirements. Regular vulnerability assessments and penetration tests, complemented by advanced assessments like red and purple team engagements, ensure a robust and dynamic cybersecurity strategy.