HTB ID: HTB-394CC3AD1E

HACK THE BOX

VULNERABILITY ASSESSMENT

Abbey Robinson

Time Management

Start Time: 9/17/25; 1:01 AM

End Time: 9/17/25 2:08 AM

Total Flags Captured: 9/9

Challenges/Roadblocks: I did not face any challenges or roadblocks on this HTB. I found it to be straightforward with searching through basic vulnerability scans. As long as you read all the directions it was not difficult.

Flag 1:

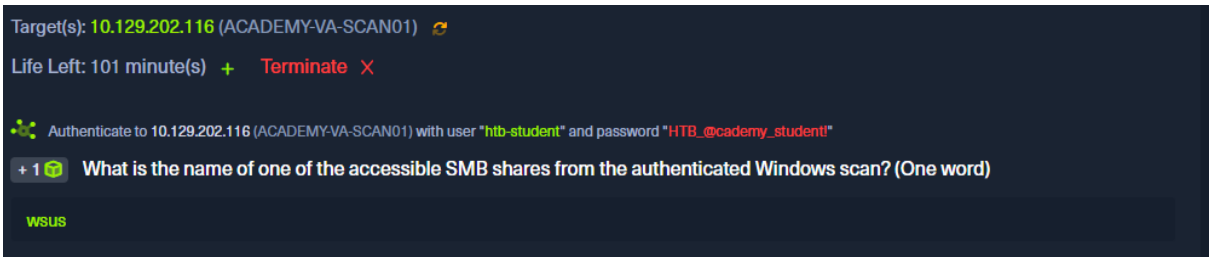
Flag Answer: wsus

Last Command Used: N/A

Steps:

1. First, I opened up Firefox to access Nessus. I plugged in the browser https://10.129.202.116:8834/ . This searches the target IP along with the port number, I found the correct port number in the information above.
2. Then I clicked on advanced to see more info and accepted the risk. I then used the given credentials to sign into Nessus.
3. In the directions from HTB, it says to use the pre populated scan so you do not have to wait the full 60 minutes. Therefore, I clicked on the windows basic authenticated scan and clicked on the only host scan. Then using the search bar I searched up smb shares, so it would only show me smb share files.
4. In the ouput, the first line is wsus which was the only one that was one word. Wsus is windows service update services.

Image/Screenshot:



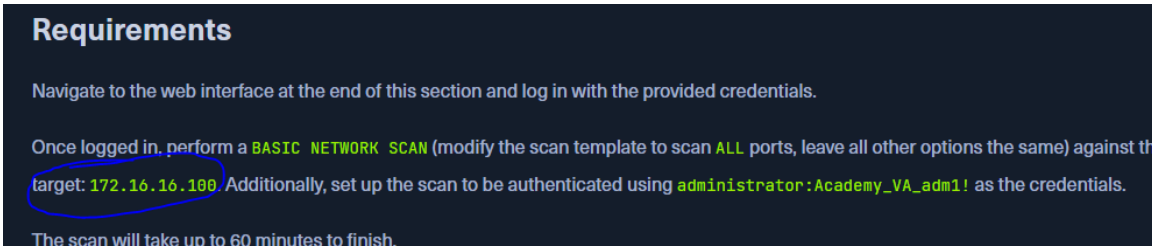
Flag 2:

Flag Answer: 172.16.16.100

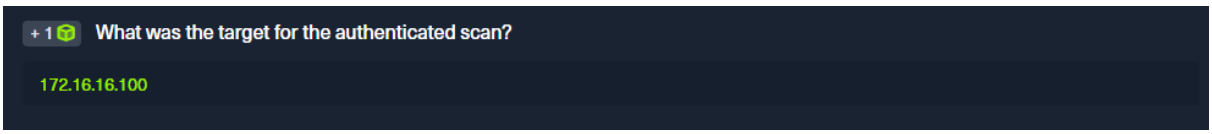
Last Command Used: N/A

Steps:

1. For this flag, I remember from reading under requirements they provided a target scan. Shown here:



Image/Screenshot:



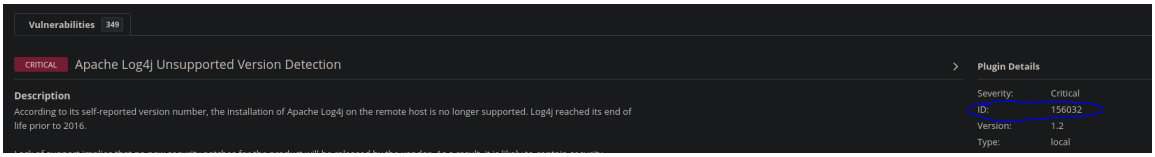
Flag 3:

Flag Answer: 156032

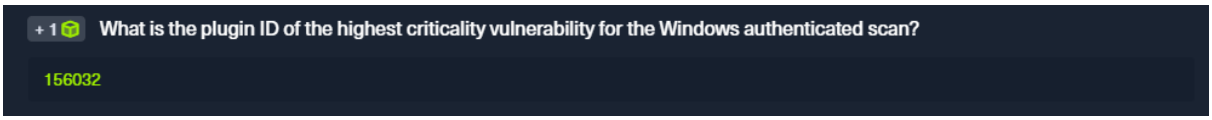
Last Command Used: N/A

Steps:

1. I clicked on the back arrow to go back to see all the critical vulnerabilities. There was only one that was windows, so I clicked on the one.
2. I then realized that didn't matter because it wanted the highest one at the top, so I clicked on the Apache one and scrolled over to find the ID. Here is where I found it:



Image/Screenshot:



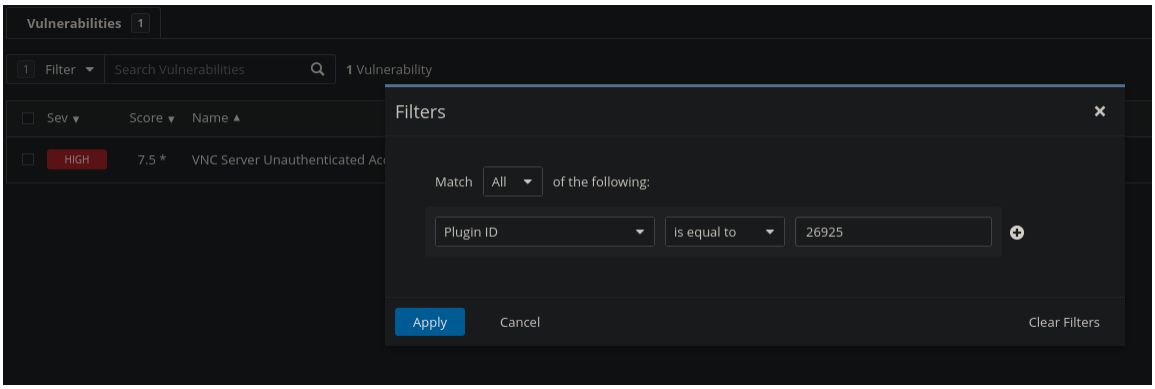
Flag 4:

Flag Answer: VNC Server Unauthenticated Access

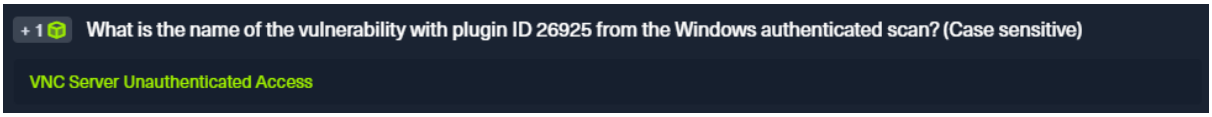
Last Command Used: N/A

Steps:

1. I knew that it would take forever to click through all of them, so instead I used the filter button. I scrolled down to look for ID, I used the plug in ID filter and typed in 26925.
2. The only vulnerability to pop up was the VNC Server. Here is how I did the filter:



Image/Screenshot:



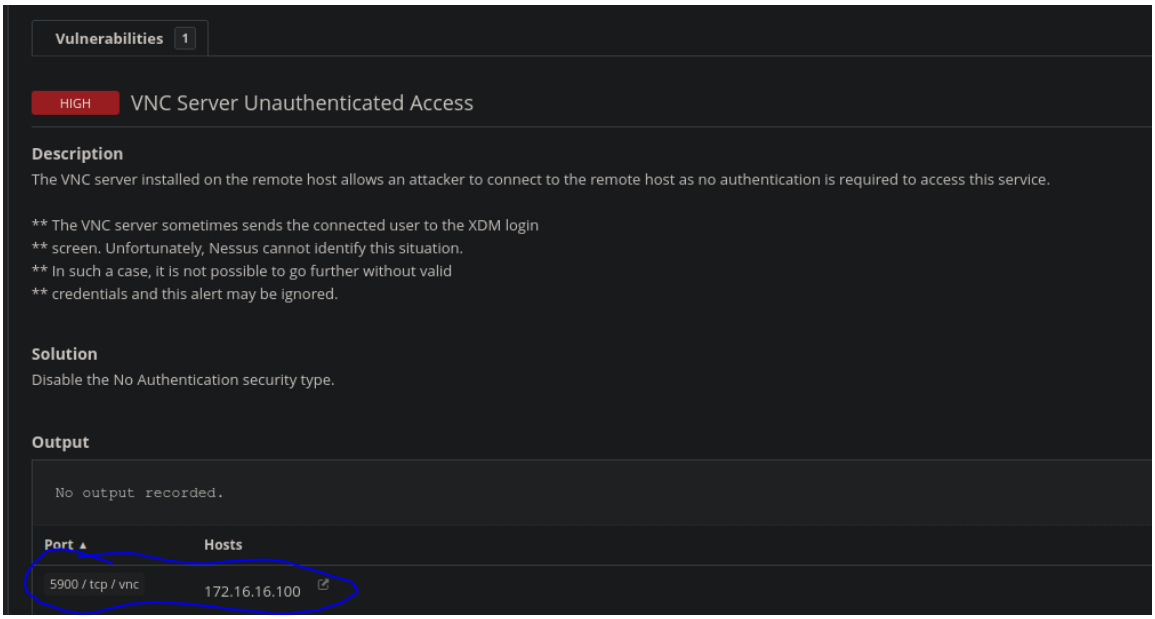
Flag 5:

Flag Answer: 5900

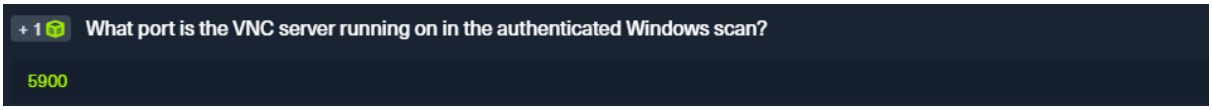
Last Command Used: N/A

Steps:

1. I went back into the VNC server and scrolled down, the only port was the 5900/tcp/vnc. Here is where I found it:



Image/Screenshot:



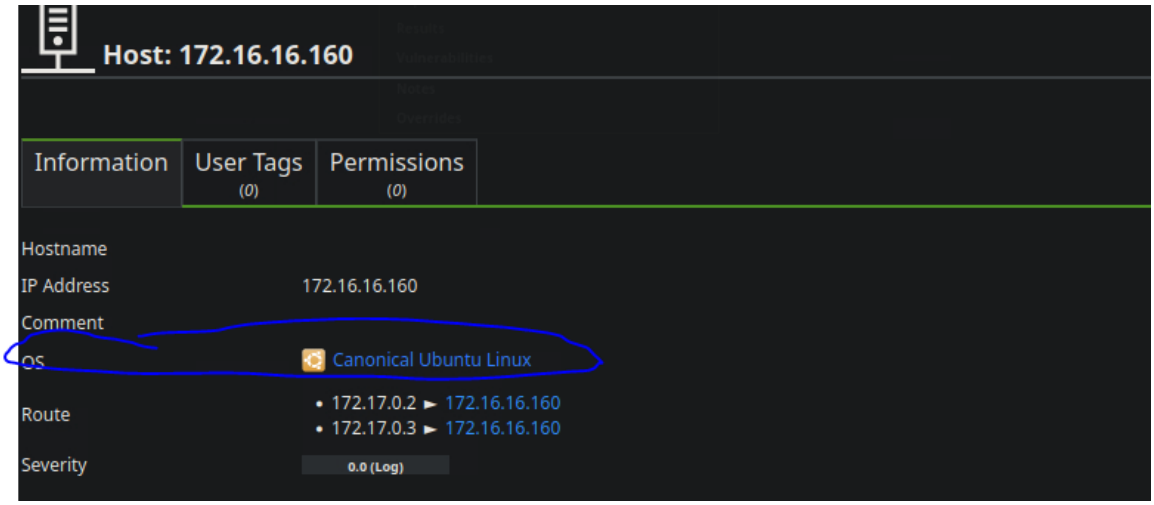
Flag 6:

Flag Answer: Ubuntu

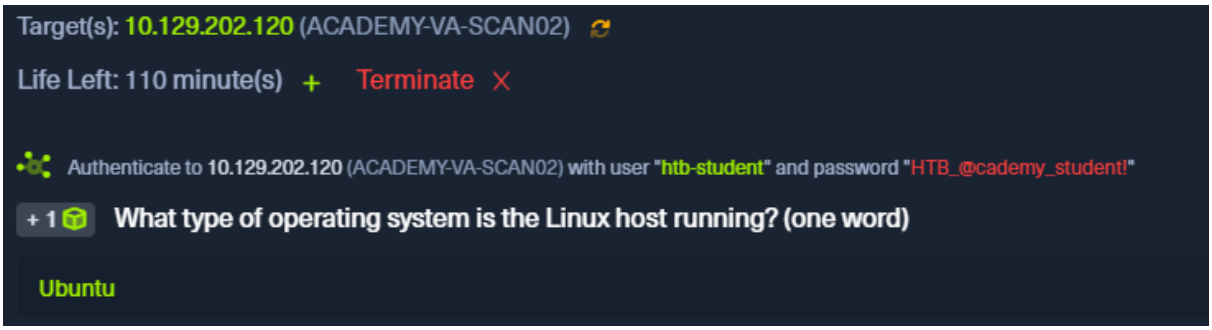
Last Command Used: N/A

Steps:

1. Now it wants me to use another vulnerability scanner which is OpenVAS, which we learned is more graphical. So, I open up a new browser and type in the new IP, which is https://10.129.202.120:8080/
2. I then use the given credentials to log in. I see that once again we are using the pre populated scan, so I find the scan tab and click on results to find all the vulnerabilities.
3. I saw that there was 600+ vulnerabilities, so again I went to the filter tab and used the given target IP under requirements to narrow down my search.
4. I clicked on the link of the IP from the most critical scan and found that the OS was Ubuntu. Here is where I found it:



Image/Screenshot:



Flag 7:

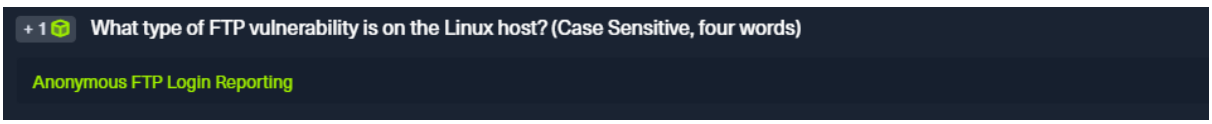
Flag Answer: Anonymous FTP Login Reporting

Last Command Used: N/A

Steps:

1. I went back to all of the vulnerabilities for the given target and looked for FTP. I saw FTP Anonymous Login Report as one of the options. Found it here:

Image/Screenshot:



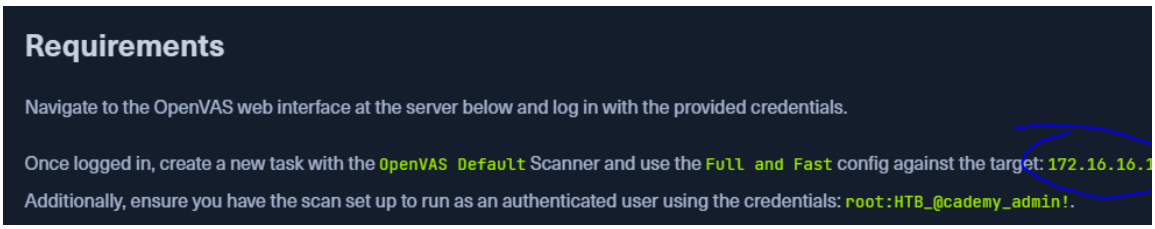
Flag 8:

Flag Answer: 172.16.16.160

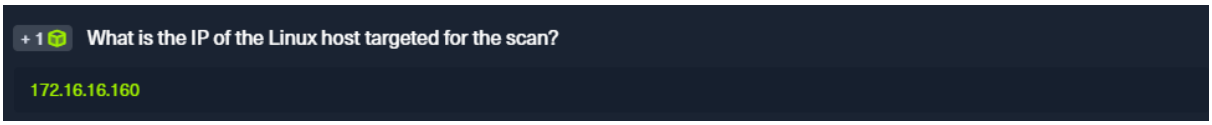
Last Command Used: N/A

Steps:

1. Once again, the IP was located under requirements from HTB directions. Found here:



Image/Screenshot:



Flag 9:

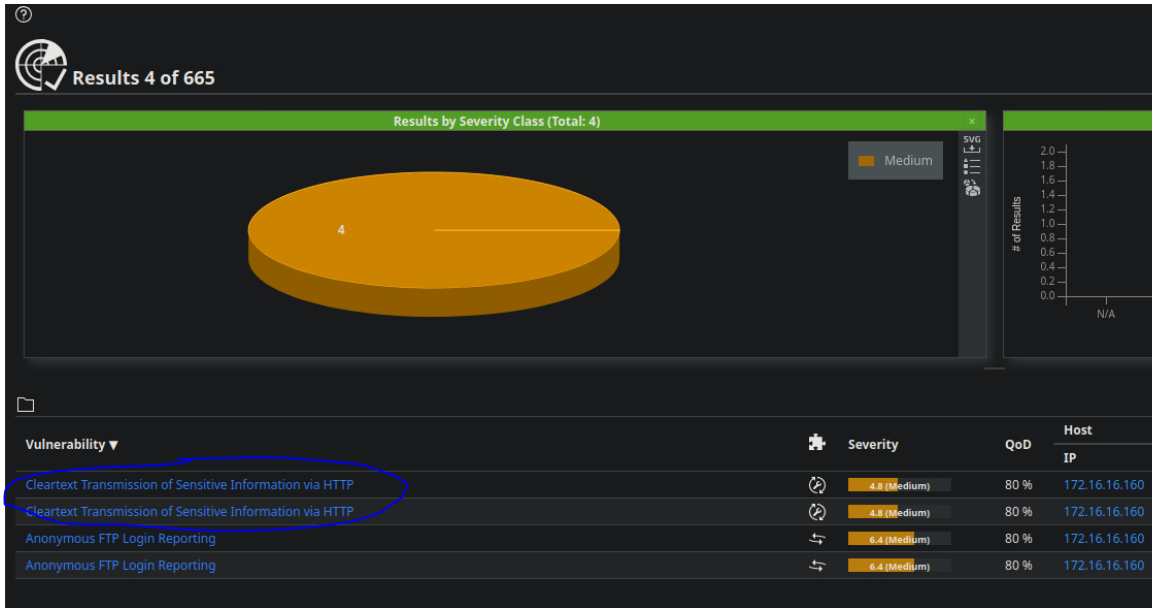
Flag Answer: Cleartext Transmission of Sensitive Information via HTTP

Last Command Used: N/A

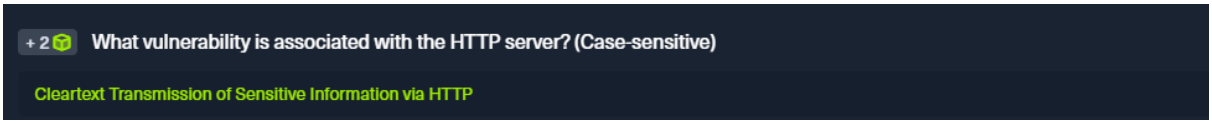
Steps:

1. At first I with the filter I search HTTP and guessed Apache HTTP Server Detection Consolidation. This was wrong.
2. I used the pie chart to click through high, medium, and low. When I clicked on the medium slice I saw Cleartext Transmission of Sensitive Information via HTTP. This was

the flag and it was shown here:



Image/Screenshot:



Summary

Overall, I did not find this HTB to be difficult at all. I was familiar with doing vulnerability scanning from 350/375 labs and 380. I know that using the filters is important to find certain vulnerabilities and to investigate the critical and medium ones first.