VULNERABILITY ASSESSMENT

ASSIGNMENT REPORT

Peter Kinyumu,
cs-sa07-24067,
June 10th, 2024.

1. INTRODUCTION

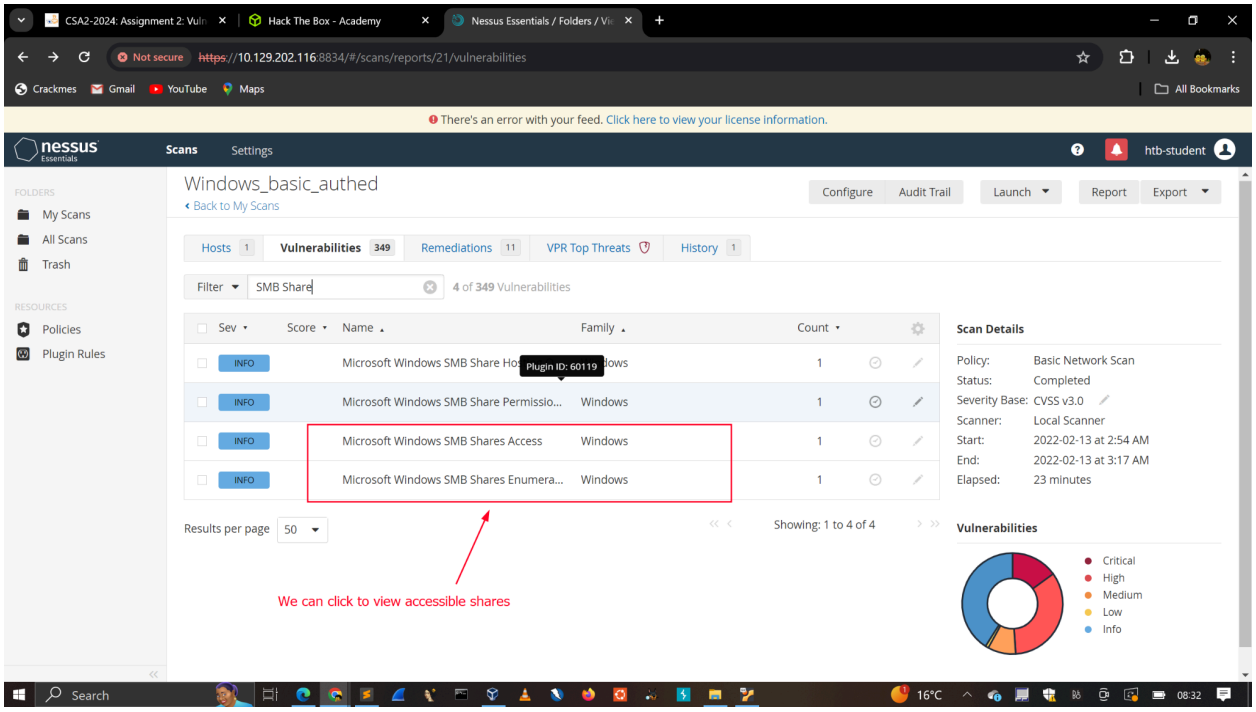
This module guided me through understanding Vulnerability Assessment, which is about identifying and categorizing risks for security weaknesses related to assets within an environment. It explains the steps of performing a network vulnerability assessment, the various ways to calculate the severity ratings of vulnerabilities, how to conduct vulnerability assessment with tools like Nessus and OpenVAS and how to clearly report findings.

2. ANSWERS TO QUESTIONS

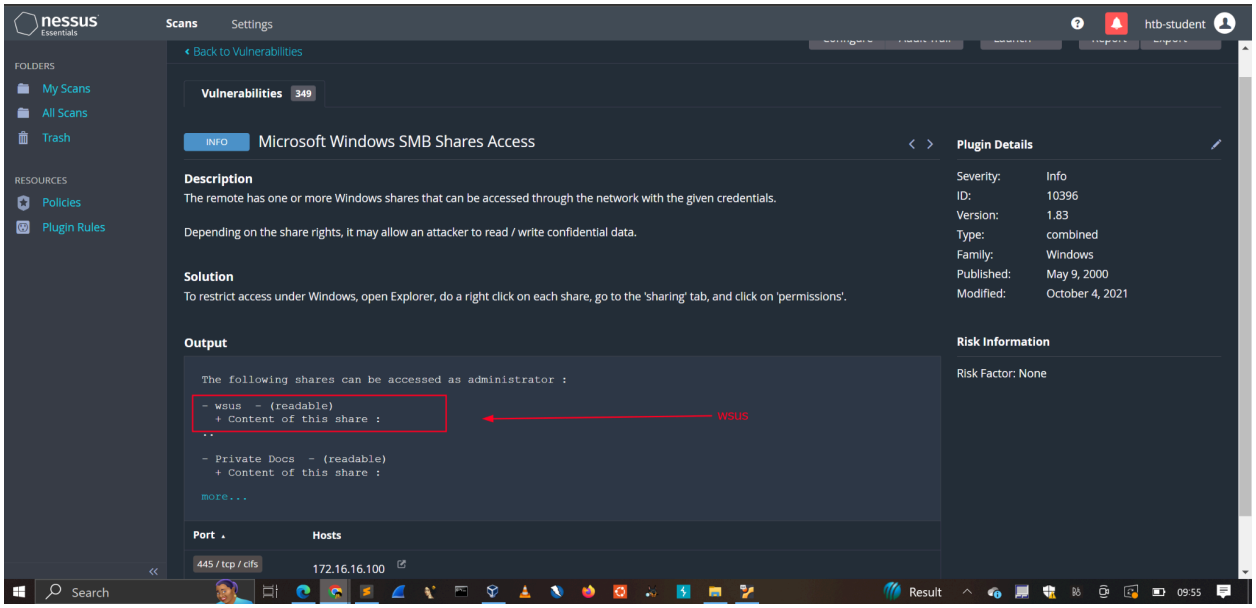
Nessus

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

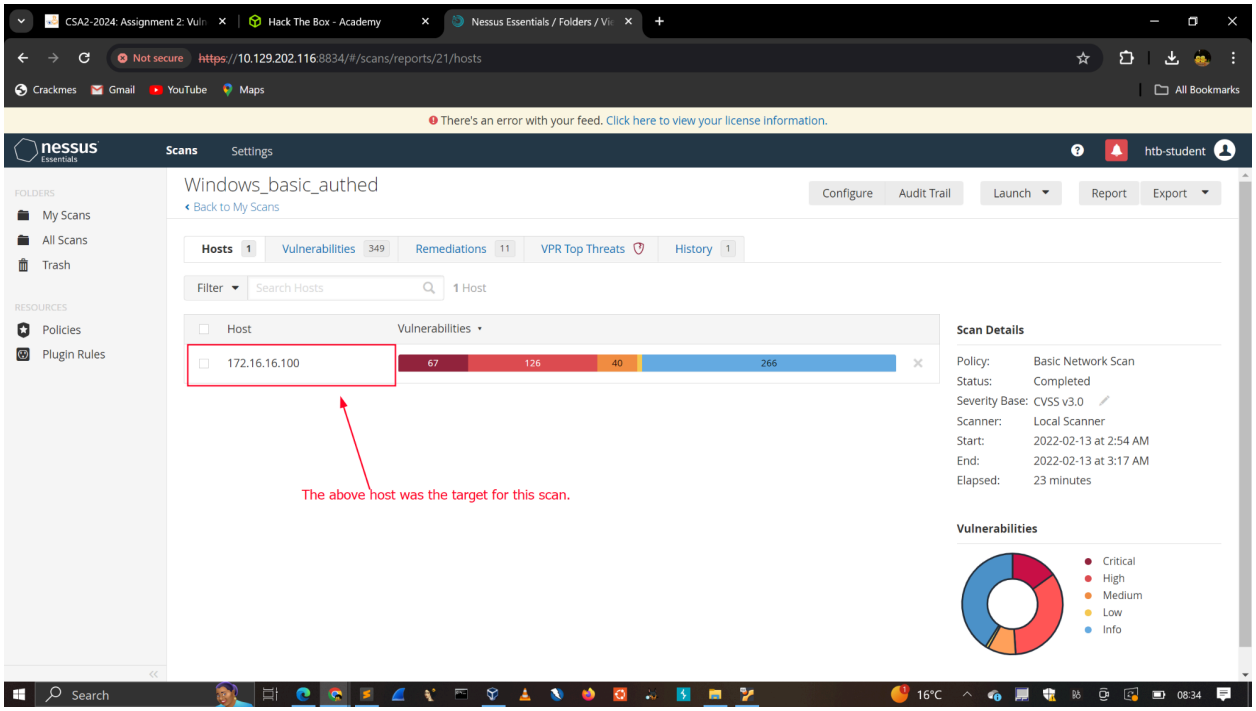
From the Vulnerabilities section of the Windows Authenticated scan, we can search for "SMB Shares" to filter the results.



We can then click the "Windows SMB Shares Access" to view the accessible SMB shares.

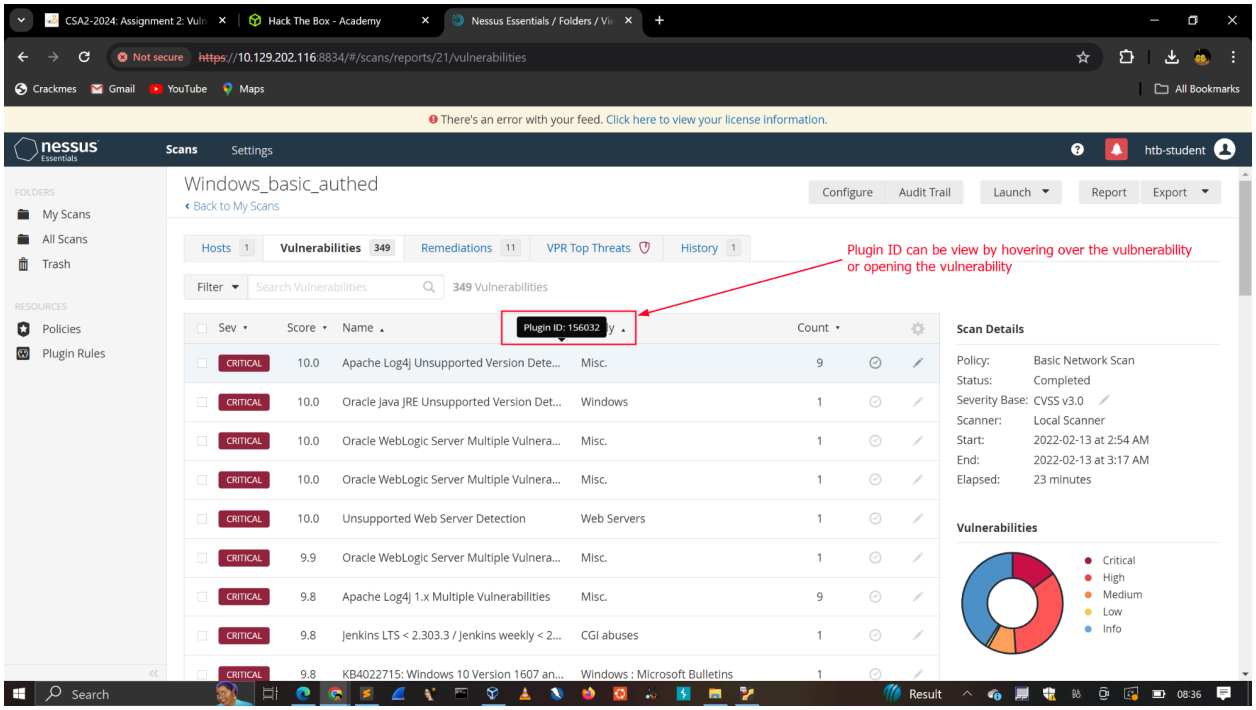


b. What was the target for the authenticated scan?

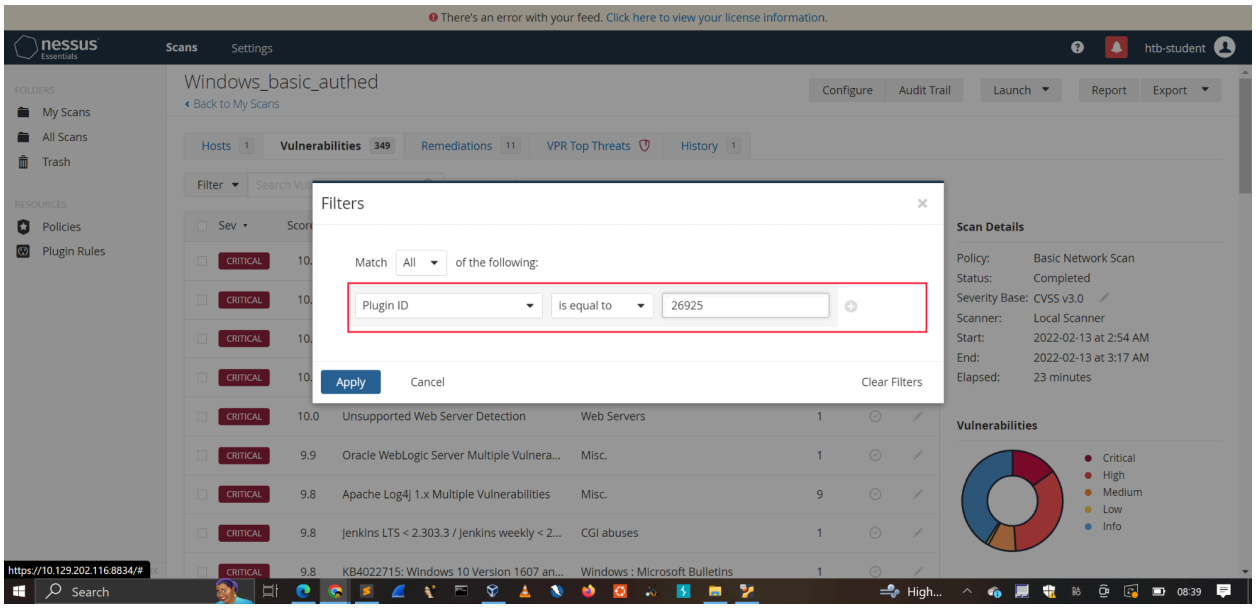


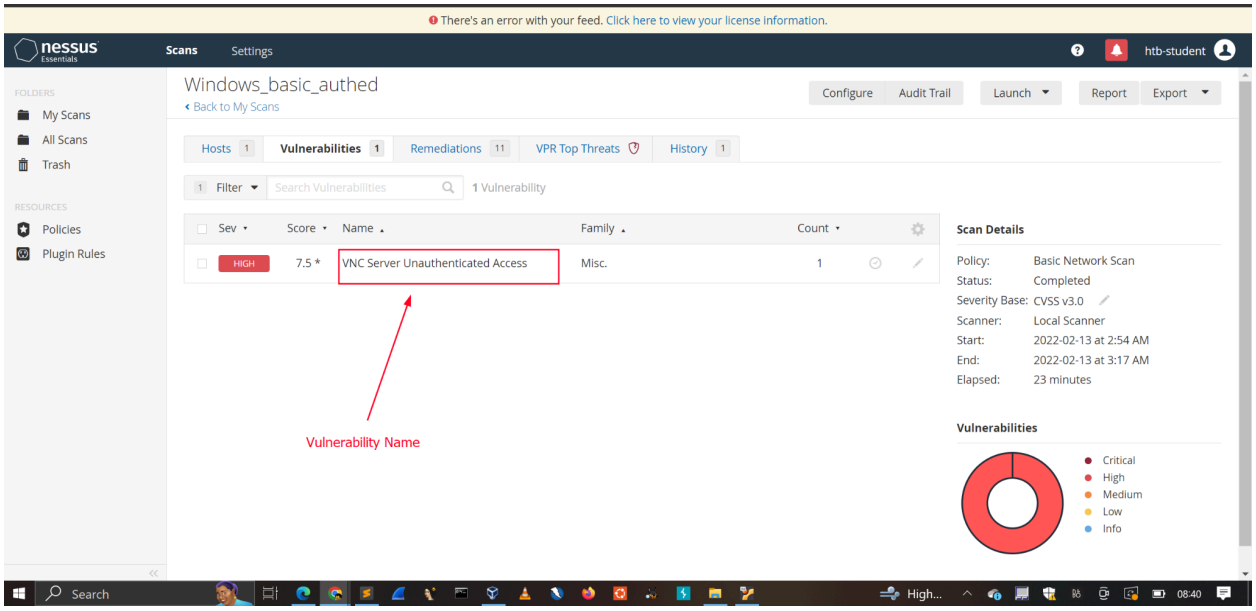
c. What is the plugin ID of the highest criticality vulnerability for the Windows authenticated scan?

The first listed vulnerability is the one with the highest criticality. If we hover over it, we see the plugin ID used.

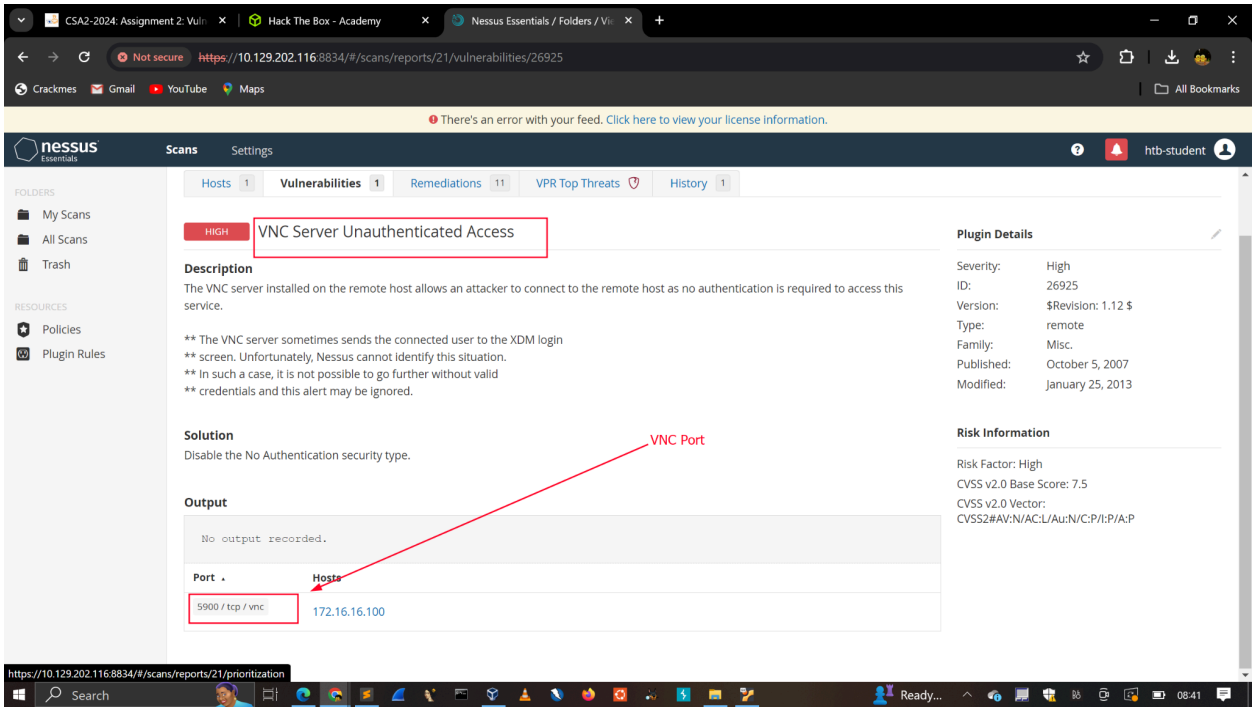


d. What is the name of the vulnerability with plugin ID 26925 from the Windows authenticated scan? (Case sensitive)

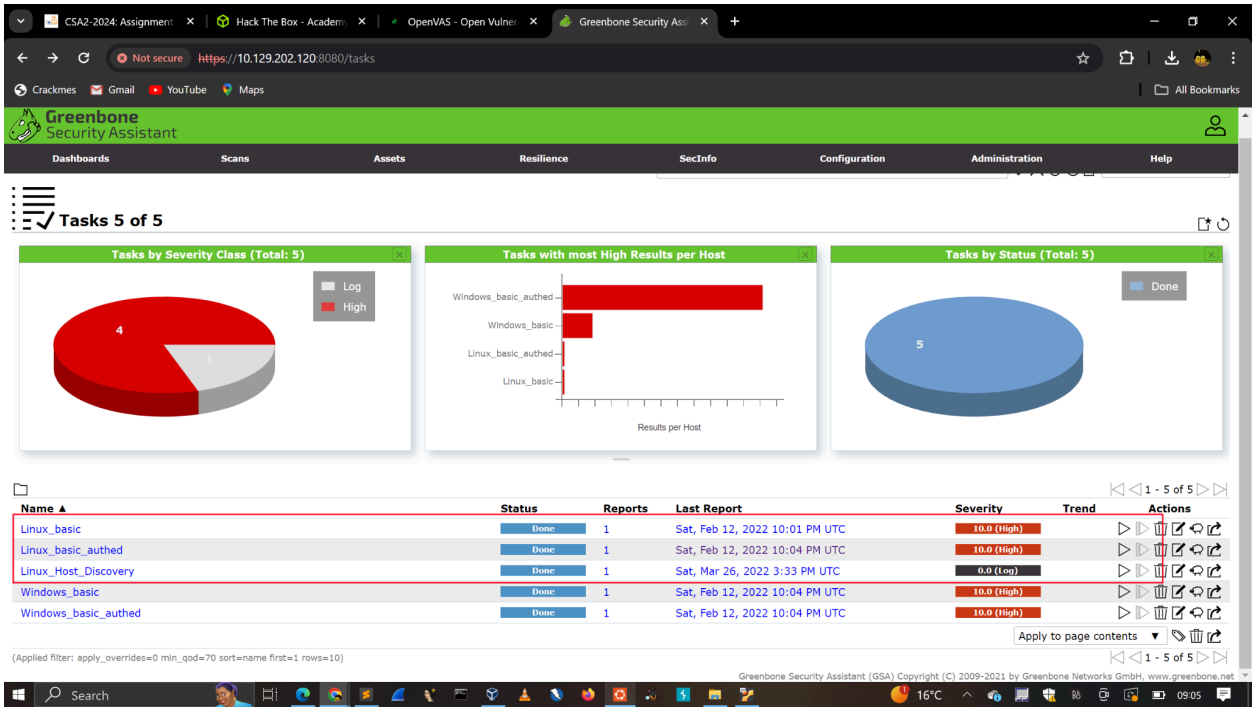




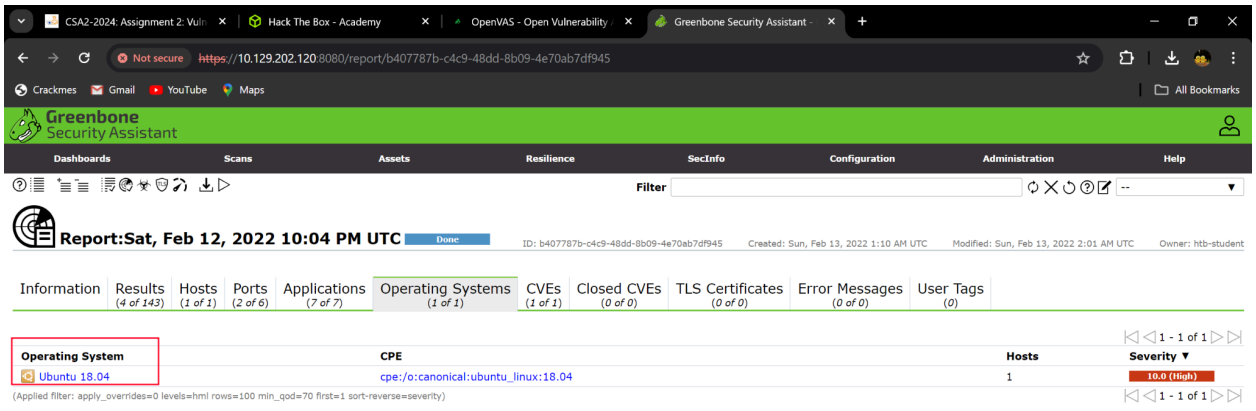
e. What port is the VNC server running on in the authenticated Windows scan?



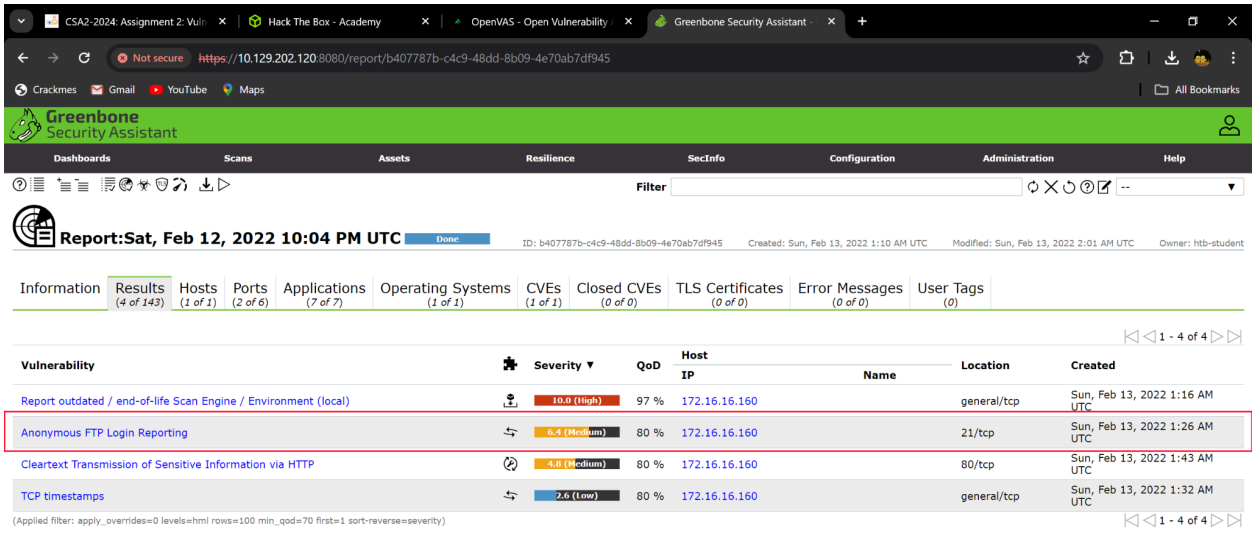
OpenVAS



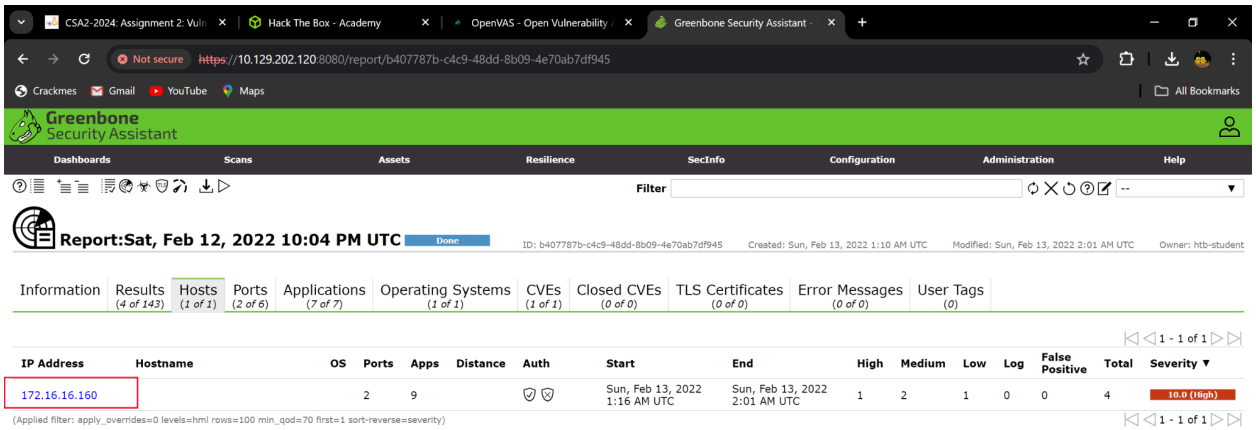
a. **What type of operating system is the Linux host running? (one word)**



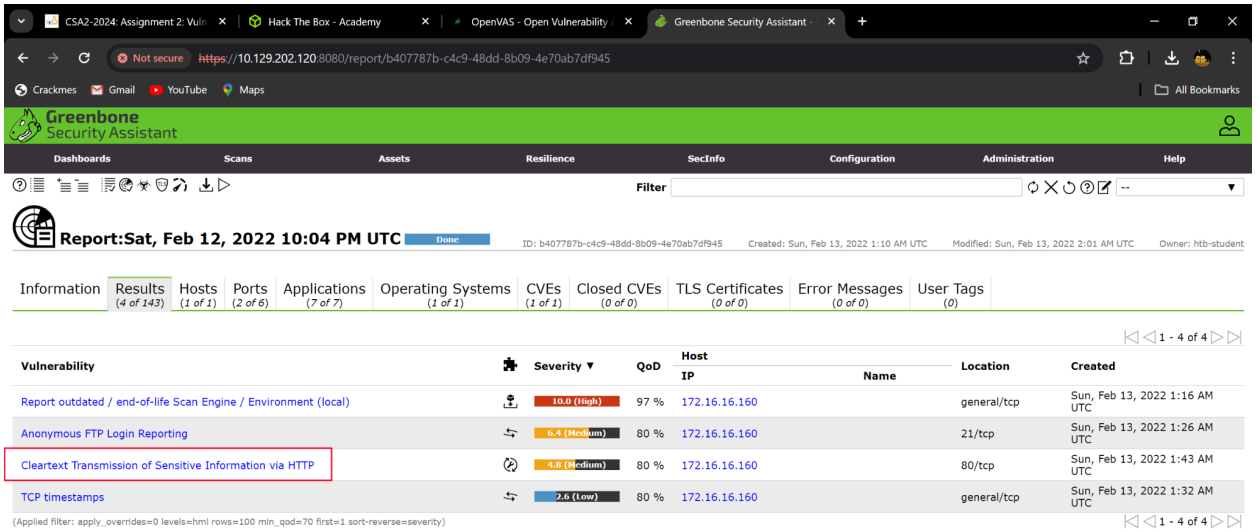
b. What type of FTP vulnerability is on the Linux host? (Case Sensitive, four words)



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

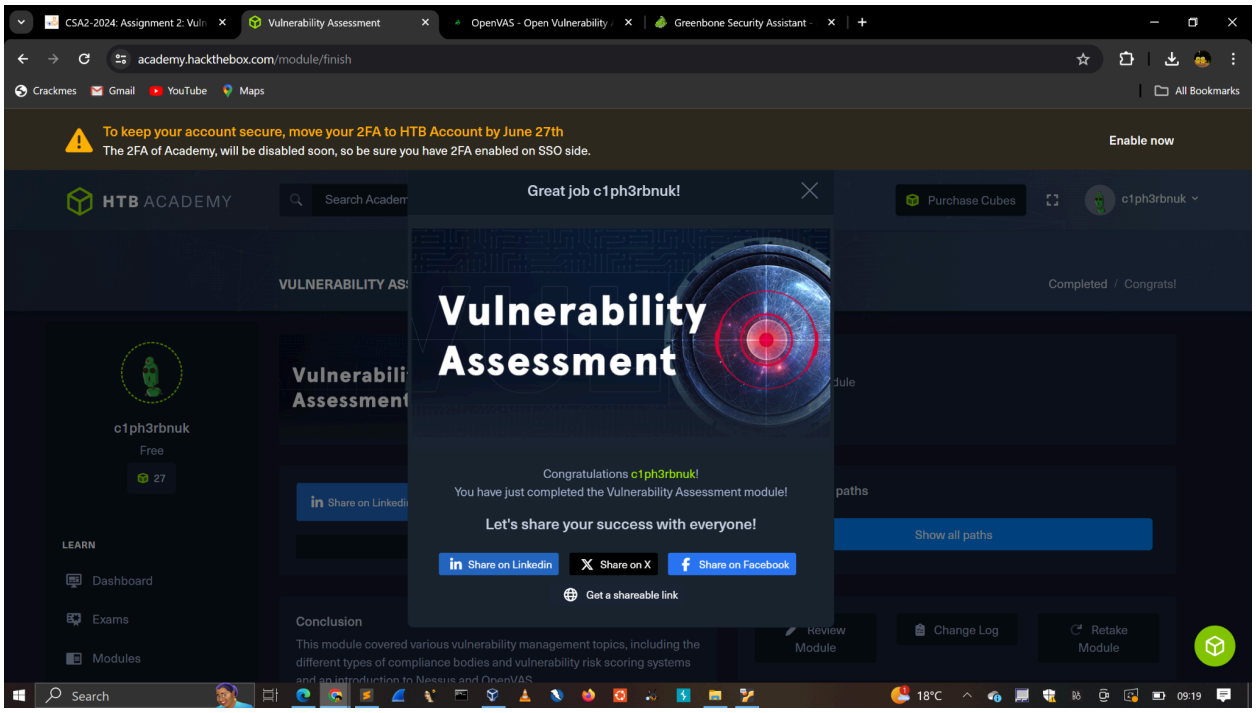


d. What vulnerability is associated with the HTTP server? (Case-sensitive)



3. MODULE COMPLETION

https://academy.hackthebox.com/achievement/144829/108



4. CONCLUSION

This assignment has taught me a lot about Vulnerability Assessment. Through it, I have learned the methodology to follow when performing a vulnerability assessment. I have also learned of various assessment standards that ensure thorough assessment. Additionally, I have learned how to use vulnerability scanners like Nessus and OpenVAS to conduct vulnerability assessments. Lastly, I have learned how to clearly report the findings of the vulnerability assessment in a way that is concise, clear and easy to read and understand.