Student:	Email:
John Monteiro	jmonteiro48@bristolcc.edu

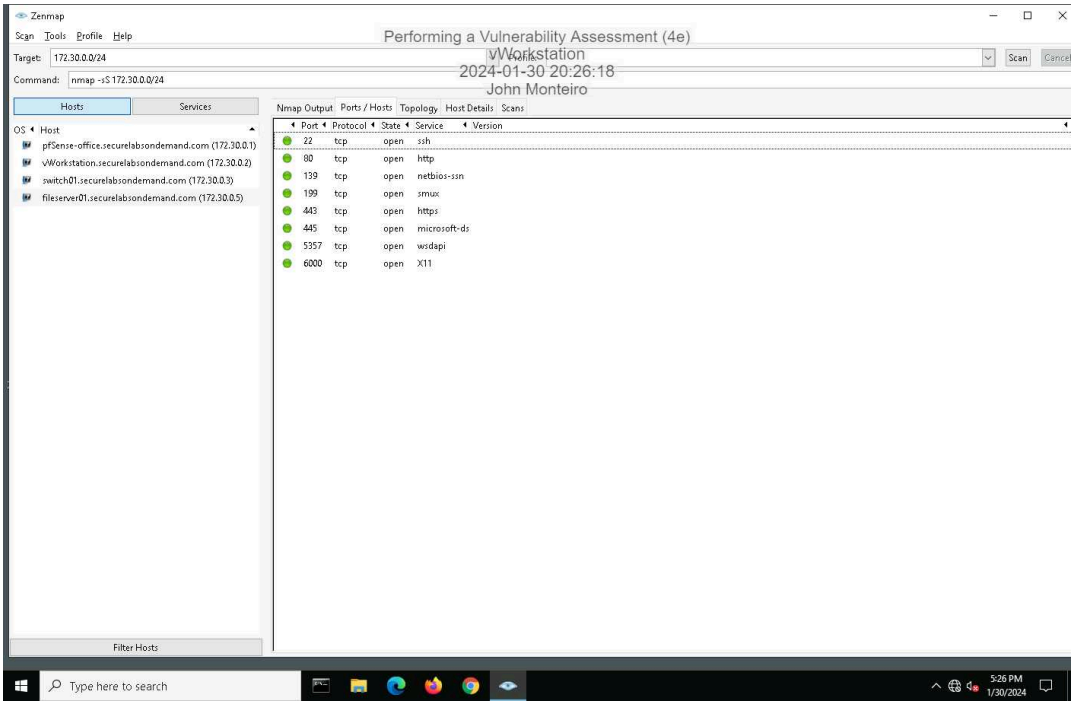
Time on Task:	Progress:
8 hours, 36 minutes	100%

Report Generated: Wednesday, January 31, 2024 at 1:32 PM

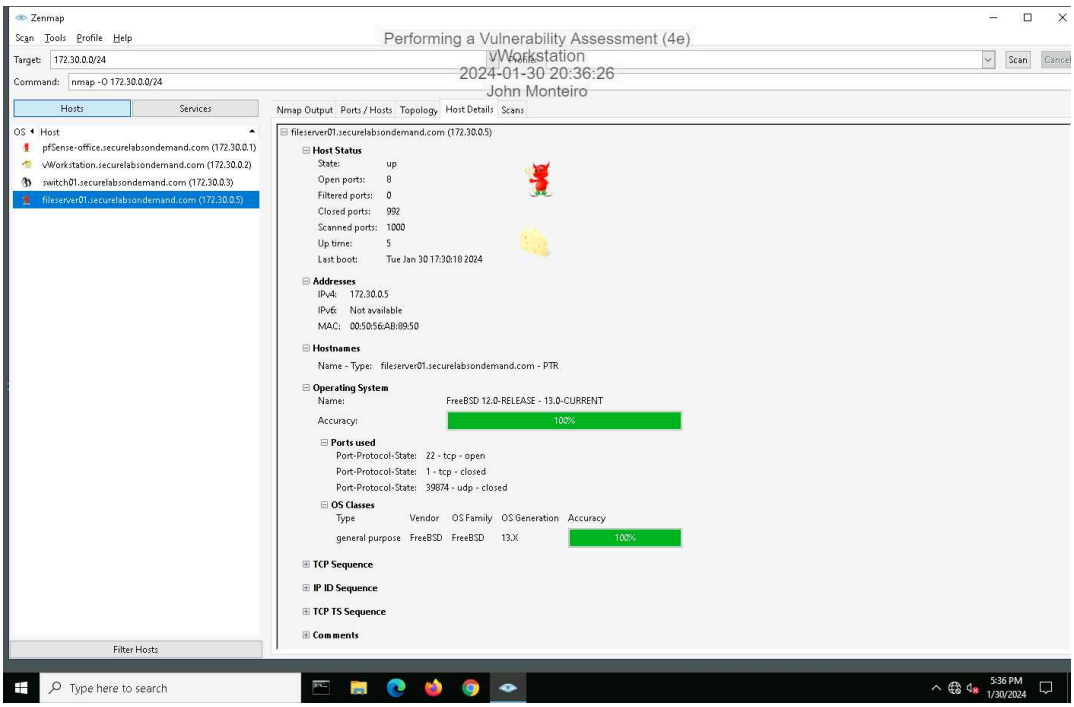
Section 1: Hands-On Demonstration

Part 1: Scan the Network with Zenmap

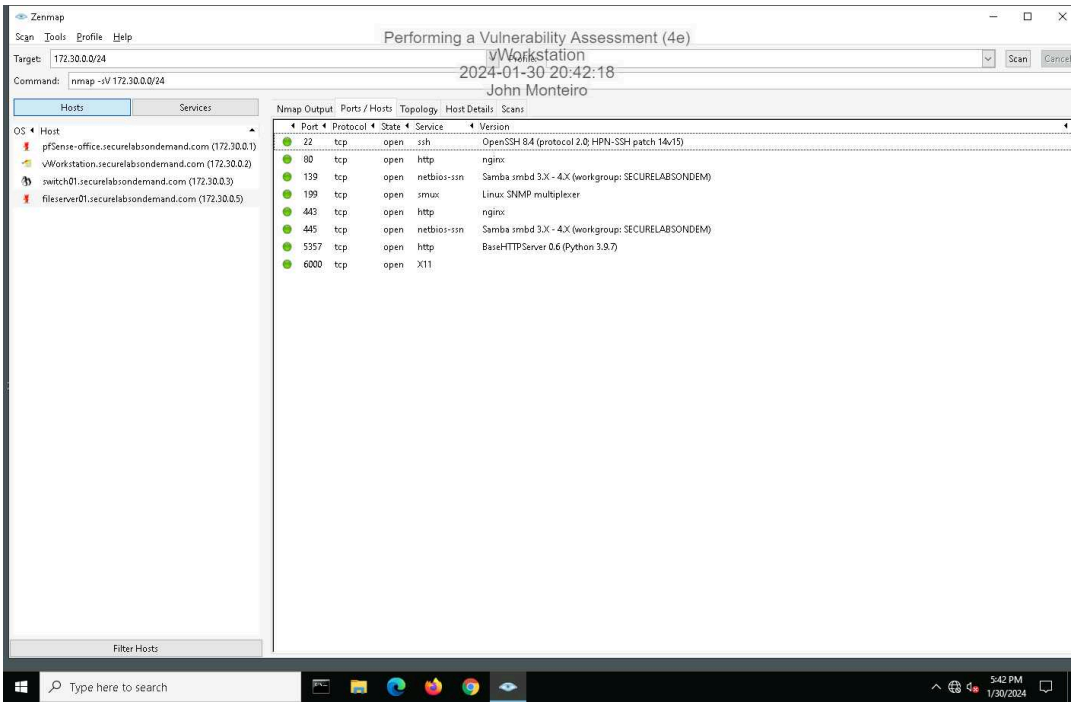
9. **Make a screen capture** showing the contents of the **Ports/Hosts tab from the SYN scan for fileserver01.securelabsondemand.com**.



15. **Make a screen capture** showing the contents of the **Host Details tab from the OS scan for fileserver01.securelabsondemand.com**.

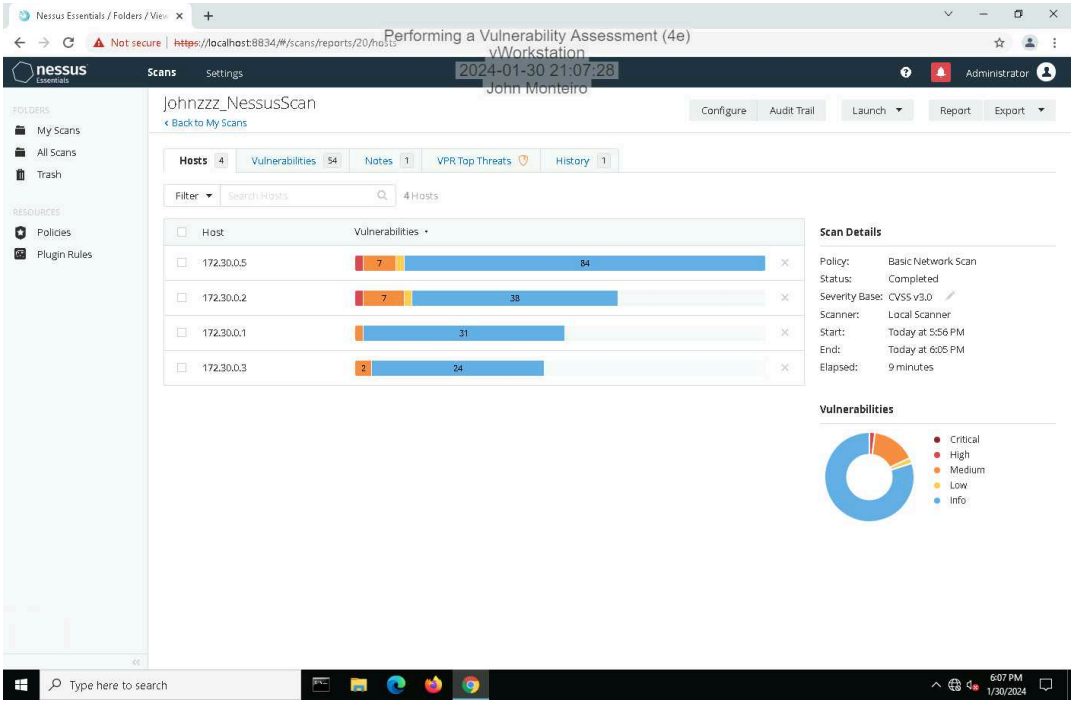


19. **Make a screen capture** showing the details in the **Ports/Hosts tab from the Service scan for fileserver01.securelabsondemand.com.**



Part 2: Conduct a Vulnerability Scan with Nessus

14. **Make a screen capture** showing the **Nessus report summary**.



Part 3: Evaluate Your Findings

11. **Summarize** the vulnerability you selected, including the CVSS risk score, and **recommend** a mitigation strategy.

Plugin ID 51192 SSL Certificate Cannot Be Trusted

Synopsis: The SSL certificate for this service cannot be Trusted

Summary: The servers certificate chain may have three potential issues. Firstly, the top chain might not descend from a recognized public certificate authority, possible due to an unrecognized self-signed certificate or missing intermediate certificates. Secondly, the chain may include a certificate that is not valid at the time of the scan, either because the scan occurs before the certificate's 'notBefore' date or after its 'noAfter' date. Lastly, the chain may contain a signature that doesn't match the certificate's information or cannot be verified, possibly due to the issuer using an unsupported or unrecognized signing algorithm. These issues can compromise the authenticity and identity verification of a public host in production, increasing the risk of man-in-the-middle attacks.

CVSS v2 Base Score: 6.5

CVSS v3 Base Score: 6.5

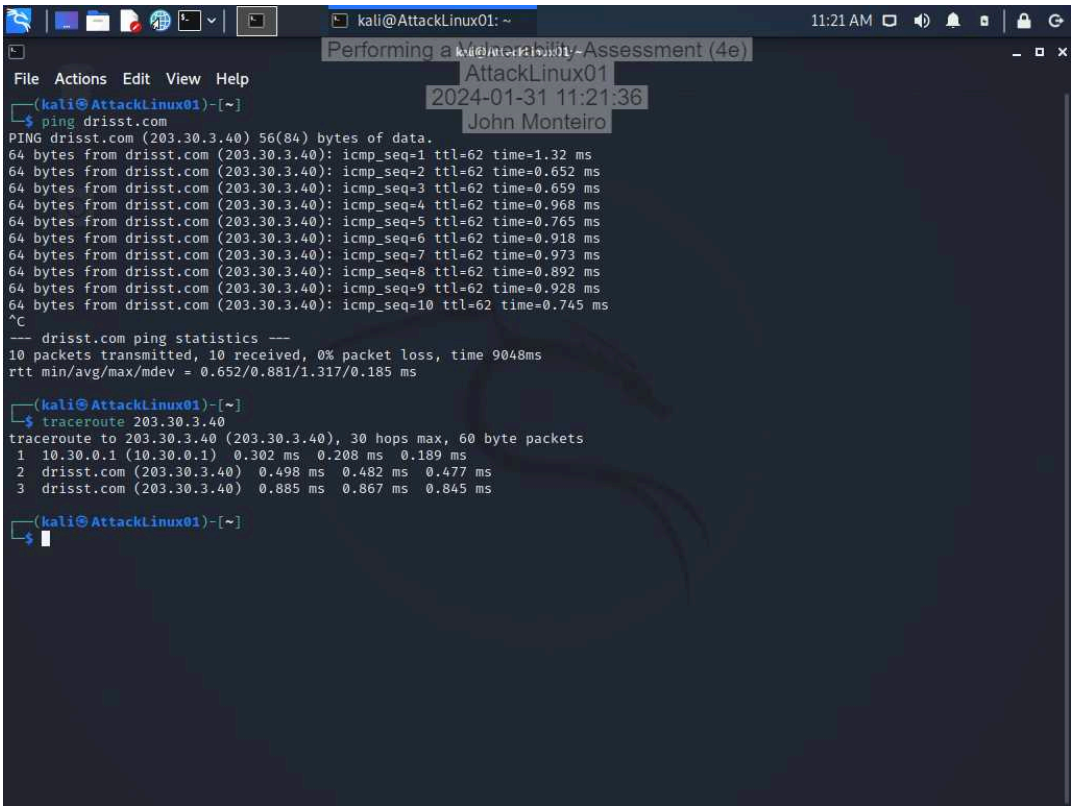
Risk Factor: Medium

Recommended Solution: Purchase or generate a proper SSL certificate for this service

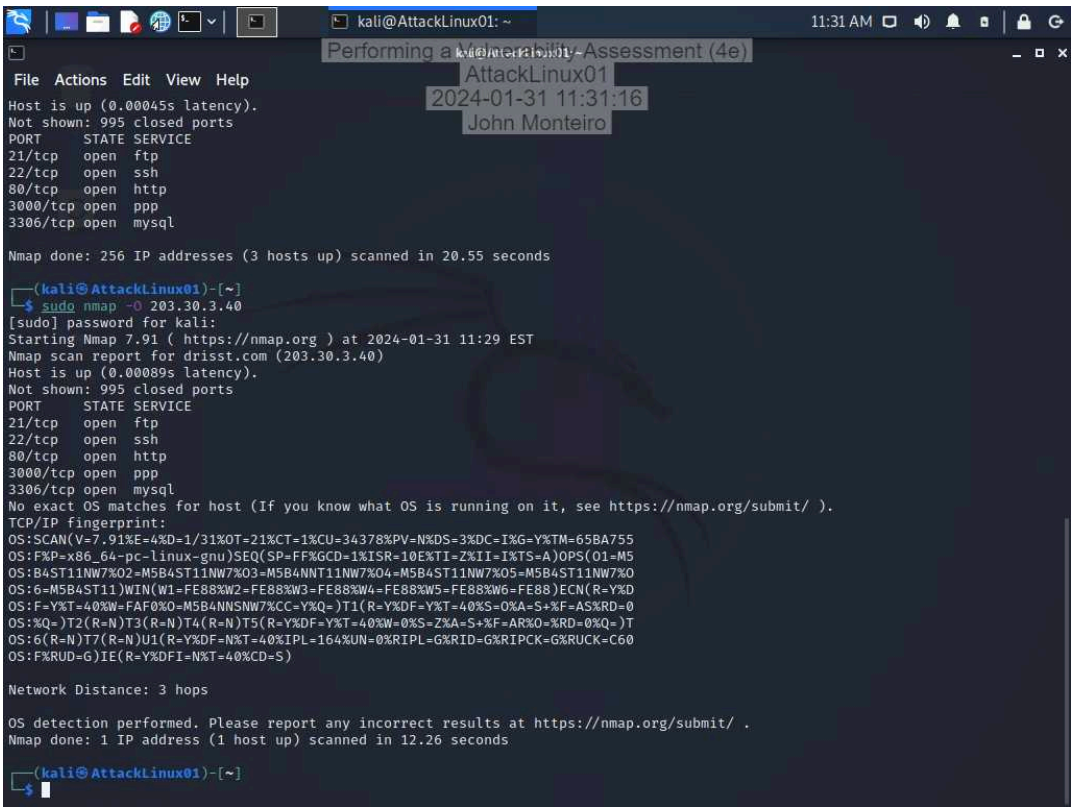
Section 2: Applied Learning

Part 1: Scan the Network with Nmap

6. **Make a screen capture** showing the **results of the traceroute command**.

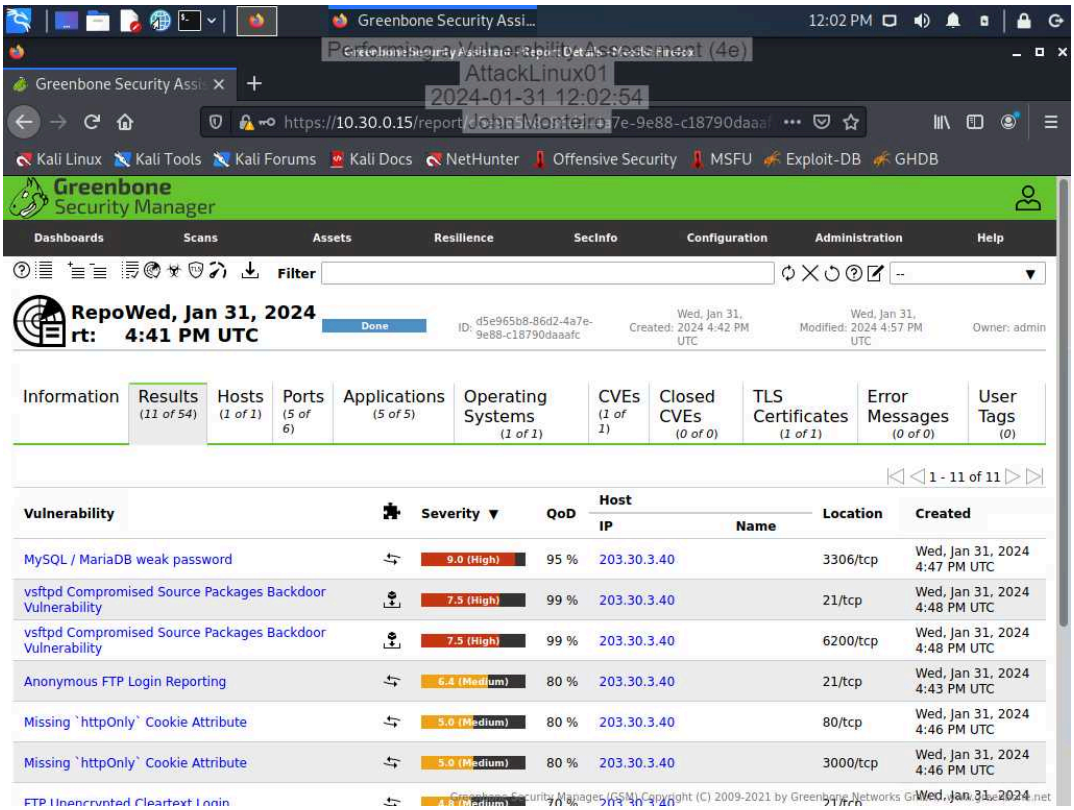


10. **Make a screen capture** showing the **results of the Nmap scan with OS detection activated**.



Part 2: Conduct a Vulnerability Scan with OpenVAS

13. **Make a screen capture** showing the **detailed OpenVAS scan results**.



Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

drisst.com 203.30.3.40

Completed by

Insert your name here.

John Monteiro

On

Insert current date here.

January 31, 2024

Purpose

Identify the purpose of the penetration test.

conducting a vulnerability scan to check for vulnerabilities on drisst.com using obtained web server host ip address of 203.30.3.40

Scope

Identify the scope of the penetration test.

simple vulnerability scan of the drisst.com web server to identify the three highest severity vulnerabilities identified by the OpenVAS scan results

Summary of Findings

Identify and summarize each of the three high-severity vulnerabilities identified during your penetration test. For each vulnerability, identify the severity, describe the issue, and recommend a remediation.

Summary of the three highest severity vulnerabilities found by scan:

MySQL/MariaDB weak Password - *Severity* (HIGH 9.0), *Issue* (Possible to login into the remote mySQL as root using weak credentials. I was possible to login using password "password", *Solution* (Change the password as soon as possible)

vsftpd Compromised Source Packages Backdoor Vulnerability - *Severity* (HIGH 7.5), *Issue* (vsftpd is prone to a backdoor vulnerability, it was detected according to the Detection Method), *Impact* (Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.), *Solution* (The repaired package can be downloaded from the link "vendorfix". Validate the package with its signature)

vsftpd Compromised Source Packages Backdoor Vulnerability - *Severity* (HIGH 7.5), *Issue* (vsftpd prone to a backdoor vulnerability, was detected according to the Detection Method.), *Impact* (Attackers can use this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.) *Solution* (The repair package can be downloaded from "vendorfix" validate package with its signature).

Conclusion

Identify your key findings.

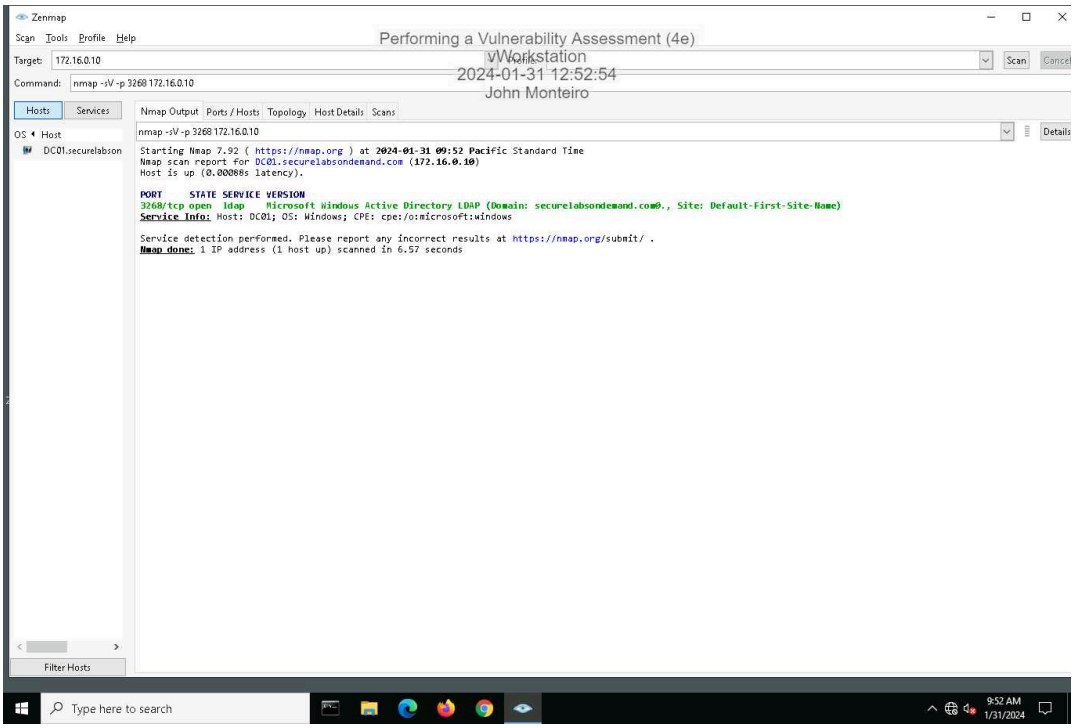
The vulnerability assessment has identified three high severity vulnerabilities:

[redacted]

Section 3: Challenge and Analysis

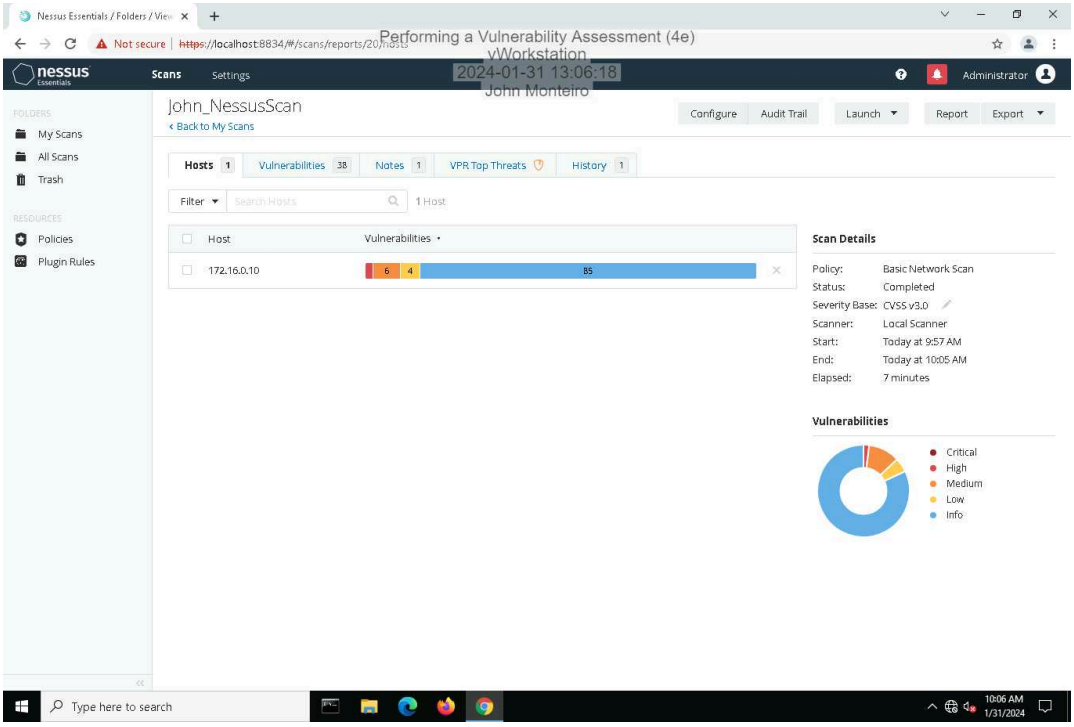
Part 1: Scan the Domain Controller with Nmap

Make screen capture showing the **results of your targeted port scan on the domain controller**.



Part 2: Scan the Domain Controller with Nessus

Make a screen capture showing the **Nessus report summary for the domain controller**.



Part 3: Prepare a Penetration Test Report

Target

Insert the target here.

Secure Labs on Demand Domain Controller host ip address 172.16.0.10

Completed by

Insert your name here.

John Monteiro

On

Insert current date here.

January 31, 2024

Purpose

Identify the purpose of the penetration test.

conducting a vulnerability scan to check for vulnerabilities on Domain Controller ip 172.16.0.10

Scope

Identify the scope of the penetration test.

penetration vulnerability scan of the Domain controller to identify the highest severity vulnerabilities identified by the Nessus Scan results.

Summary of Findings

Identify and summarize each vulnerability identified during your penetration test. For each vulnerability, identify the severity, describe the issue, and recommend a remediation.

Remote Desktop Protocol Server Man-in-the-Middle Weakness

Severity is *medium*

CVSS v2 *Base Score: 5.1*

CVSS v3 *Base Score: 6.5*

It may be possible to gain access to the remote host via vulnerability to a man-in-the-middle (MiTM) attack. The RDP client makes no effor to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. This type of attack would allow the attacker to obtain sensitive information being transmitted, including authentication credentials.

Remediation Recommendation:

Force the use of SSL as a transport layer for this service if supported and/or

On Microsoft Windows OS select ***'Allow connections only from computers running Remote Desktop with Network Level Authentication'*** setting if it is available.

Conclusion

Identify your key findings.

[redacted]