Student:	Email:
Jacob Jeffers	jjeffers6151@ucumberlands.edu

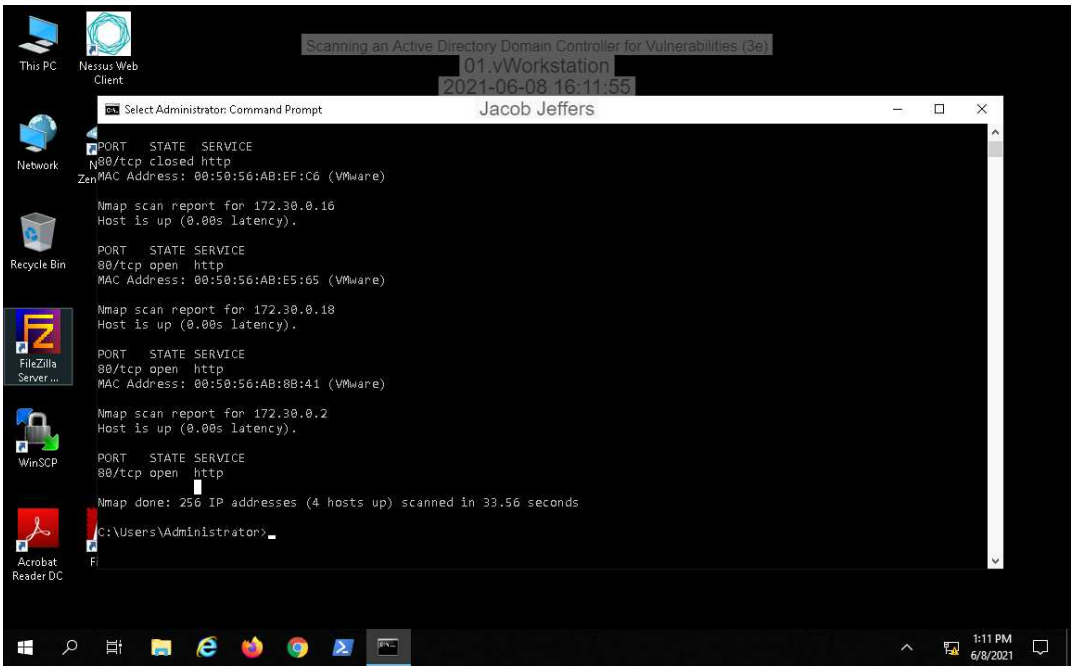
Time on Task:	Progress:
5 hours, 6 minutes	100%

Report Generated: Tuesday, June 8, 2021 at 5:49 PM

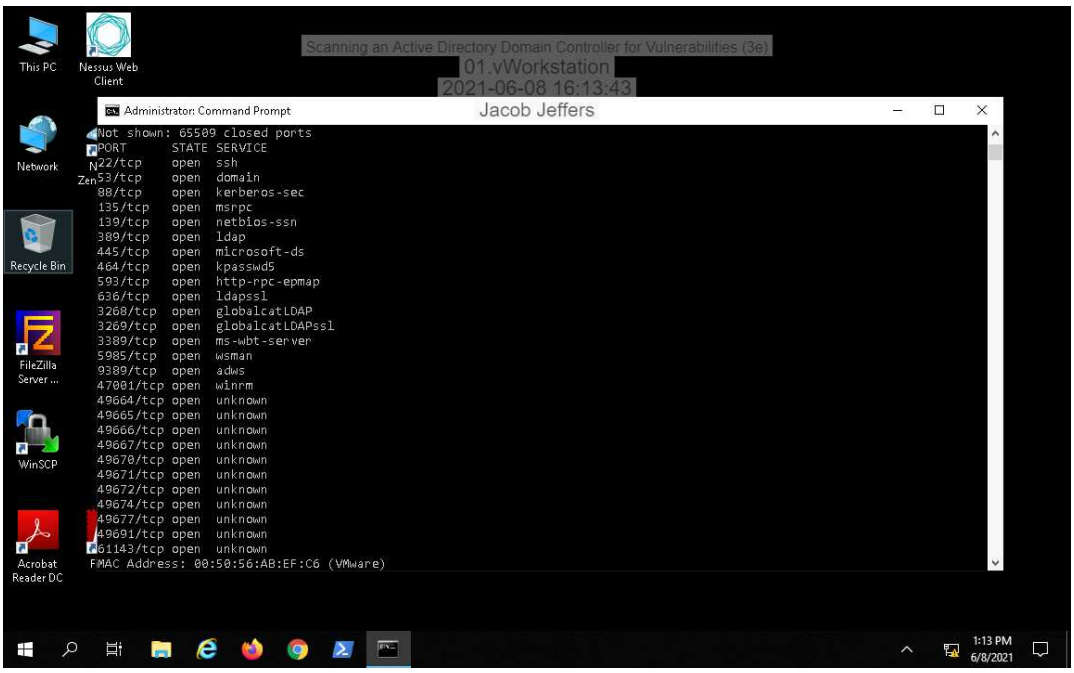
Section 1: Hands-On Demonstration

Part 1: Conduct a Port Scan

5. **Make a screen capture** showing the **nmap scan results for the targeted port scan of the 172.30.0.0/24 subnet**.



7. **Make a screen capture** showing the **nmap scan results of the full port scan of TargetWindows01**.



8. **Compare** the results of the default scan with the results of the full port scan. What are the differences between the two reports?

The default port scan doesn't test every port number like the full scan. Although the full scan took longer to perform, it provide a more detailed analysis.

9. **Provide** one reason that you might perform an abbreviated scan.

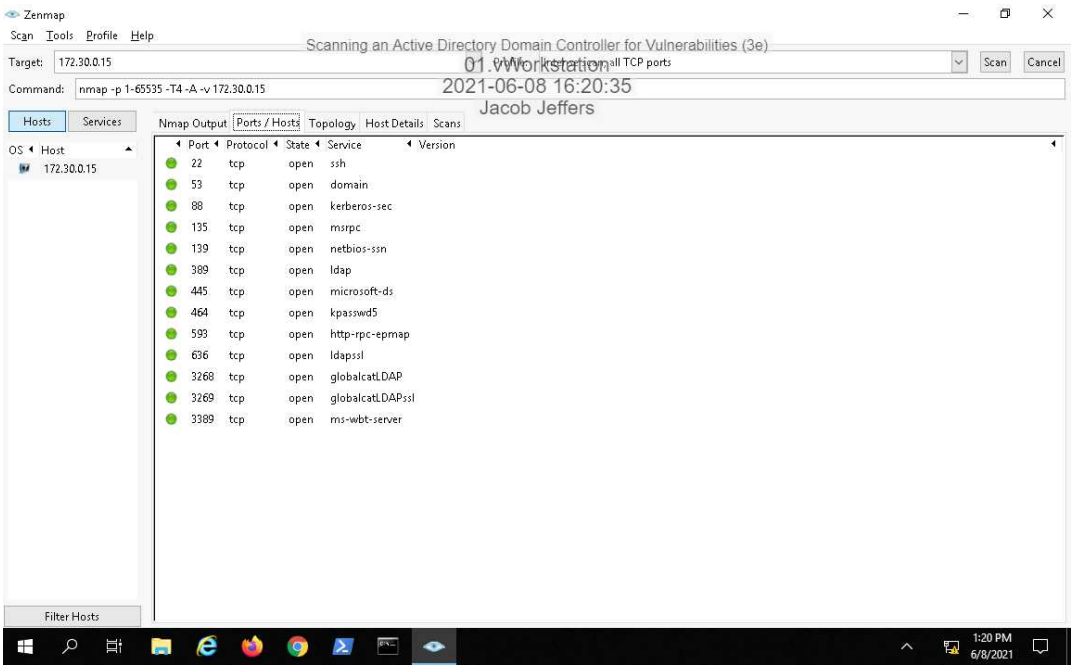
An abbreviated scan would be useful if the organization needs to analyze the commonly hacked ports.

10. **Provide** one reason that you might perform a full scan.

When writing a report, a full scan would provide the most accurate analysis.

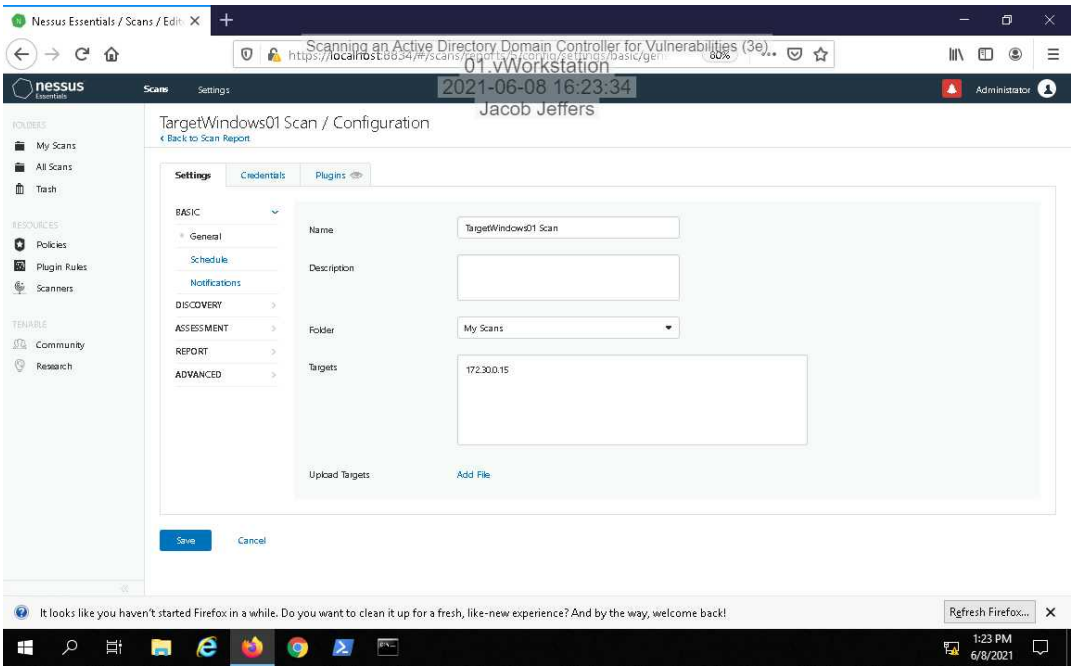
16. **Make a screen capture** showing the **Zenmap scan results for the regular scan of TargetWindows01**.

20. **Make a screen capture** showing the **Zenmap scan results for the intense scan of all TCP ports on TargetWindows01**.

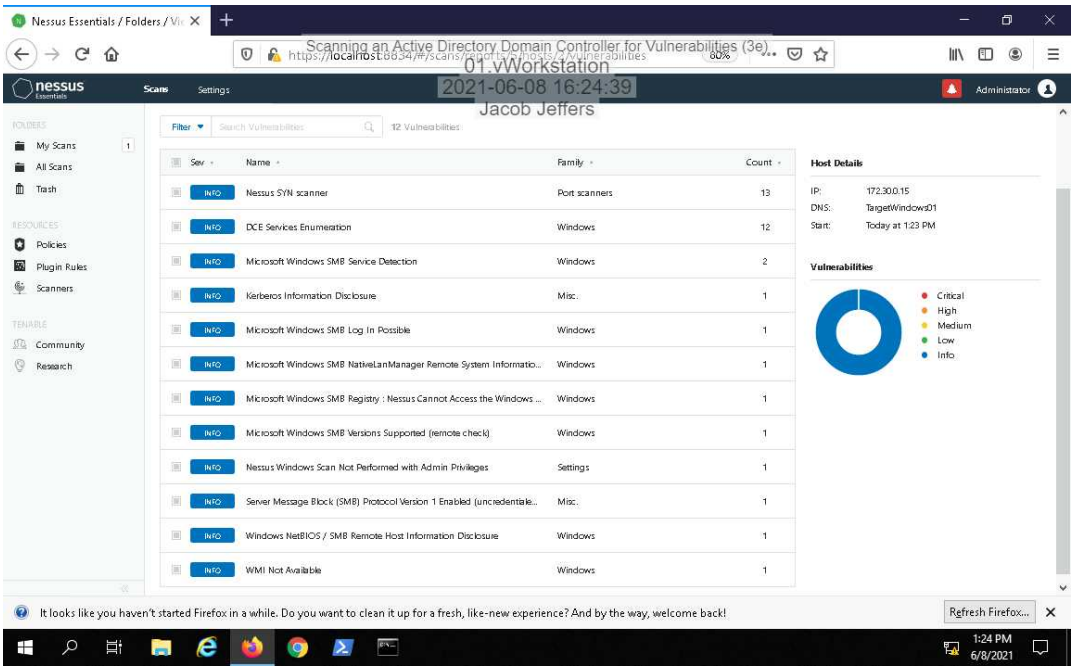


Part 2: Conduct a Network Vulnerability Scan

7. **Make a screen capture** showing the **TargetWindows01 Scan configuration**.



11. **Make a screen capture** showing the **TargetWindows01 Scan results**.



Part 3: Interpret the Results of a Network Vulnerability Scan

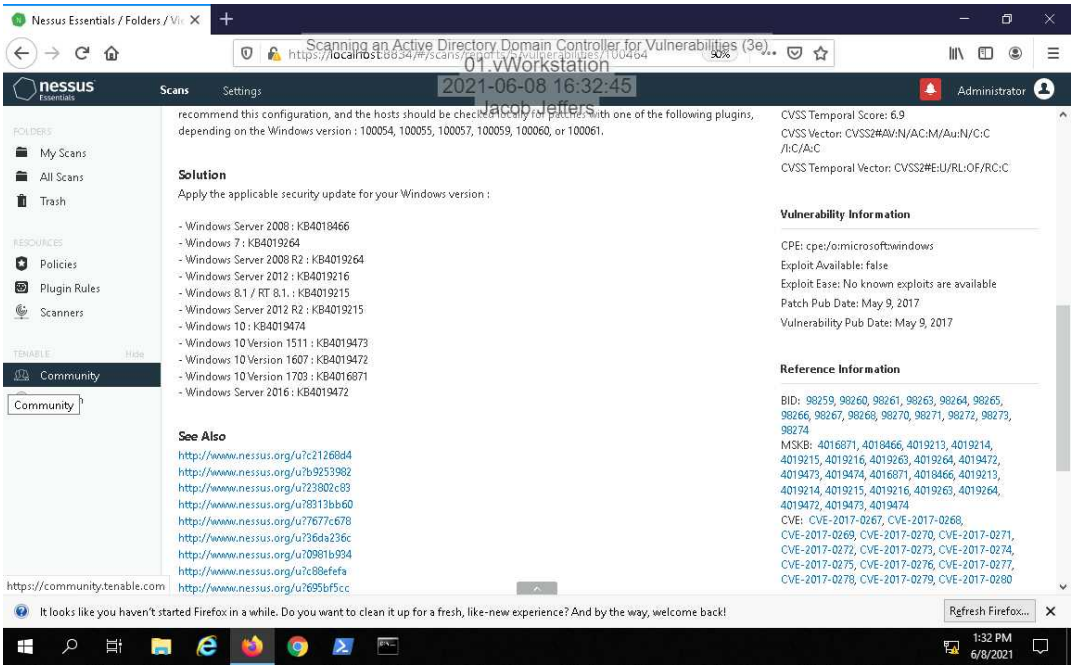
2. **Record** the number of Critical, High, Medium, and Low vulnerabilities in the initial scan of TargetWindows01.

Critical - 0 High - 2 Medium - 9 Low - 1

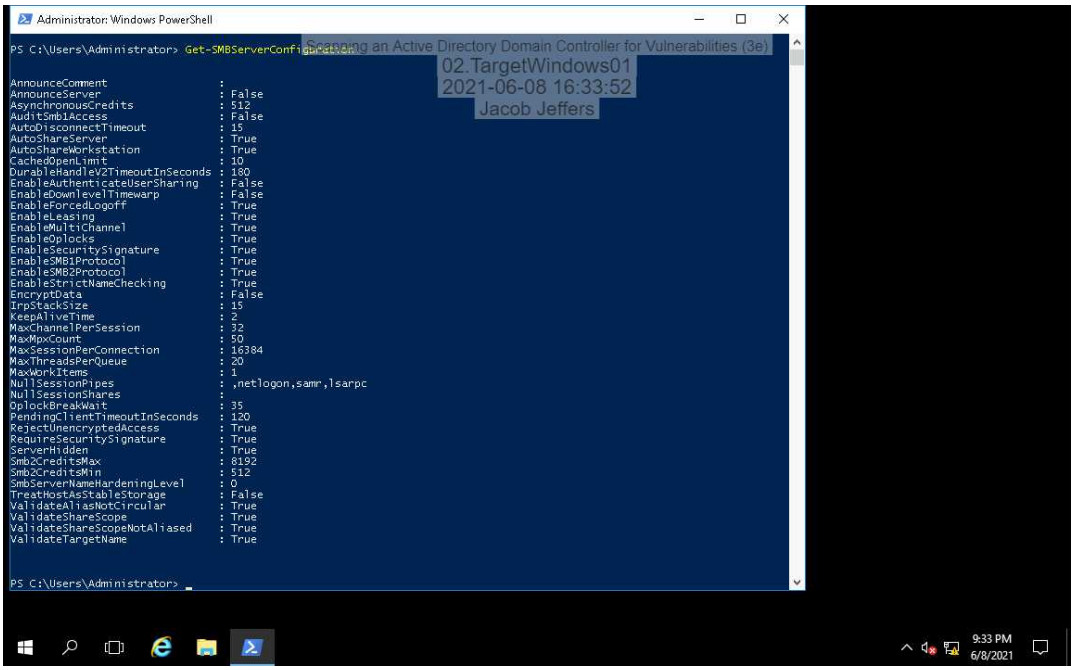
5. **Describe** one method that you could use to correct the vulnerability.

This vulnerability could be solved with a security patch update.

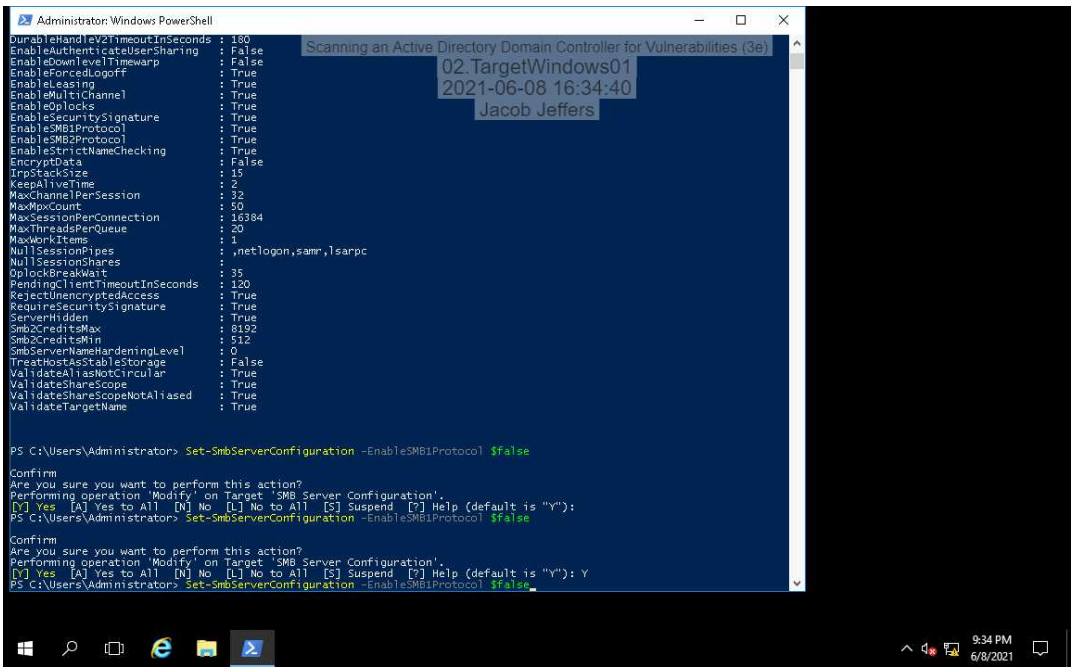
6. **Make a screen capture** showing the **detailed Microsoft SMBv1 Multiple Vulnerabilities report**.



11. **Make a screen capture** showing the **EnableSMB1Protocol status**.



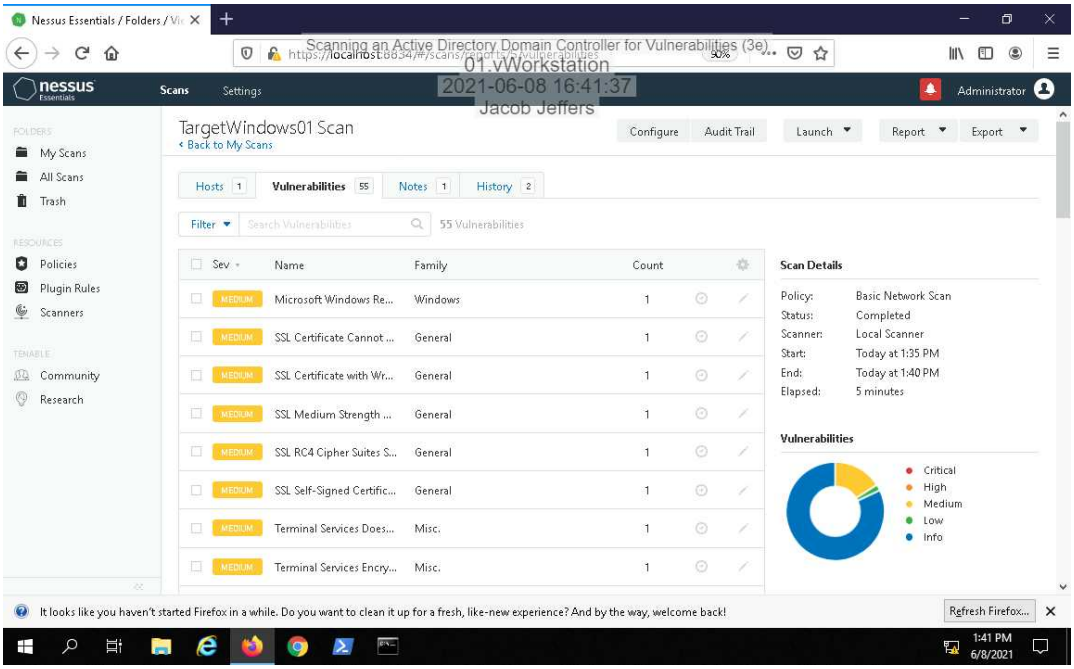
14. **Make a screen capture** showing the **executed Set-SmbServerConfiguration cmdlet**.



21. **Record** the number of Critical, High, Medium, and Low vulnerabilities in the second scan of TargetWindows01.

Critical - 0 High - 0 Medium - 9 Low - 1

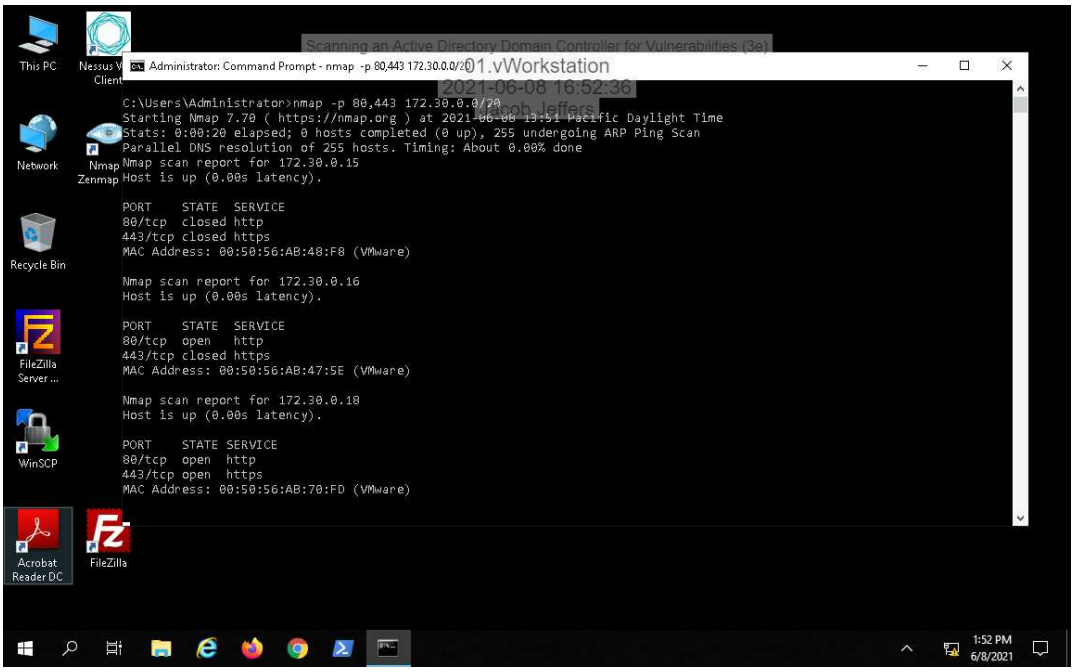
22. **Make a screen capture** showing the **updated TargetWindows01 vulnerability list**.



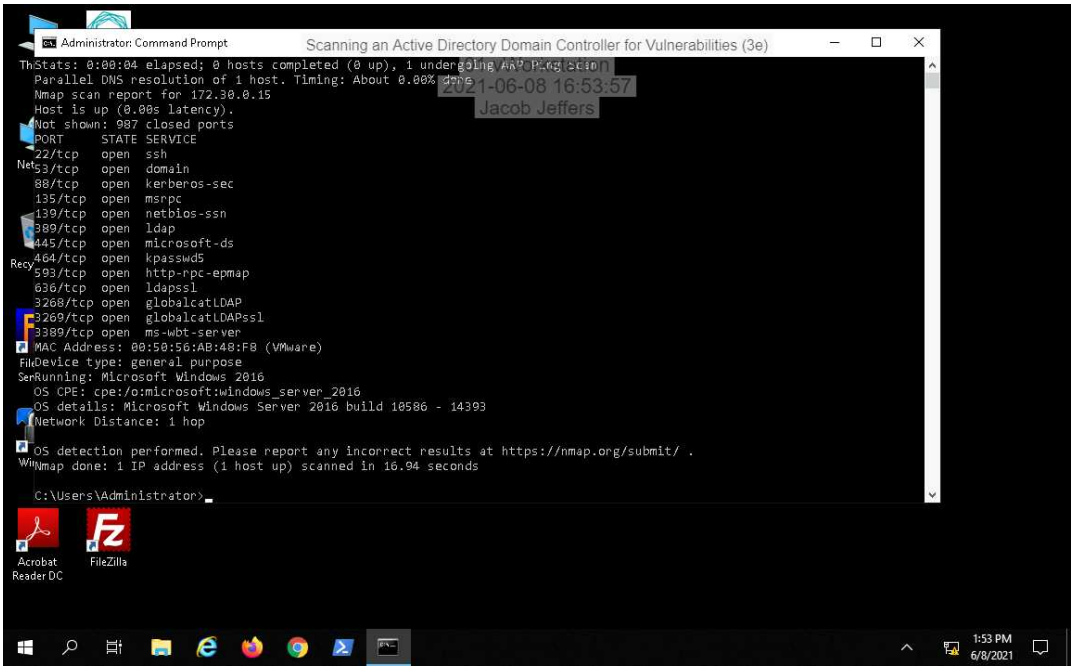
Section 2: Applied Learning

Part 1: Conduct a Port Scan

5. **Make a screen capture** showing the **nmap scan results for the targeted port scan of the 172.30.0.0-20 IP address range**.



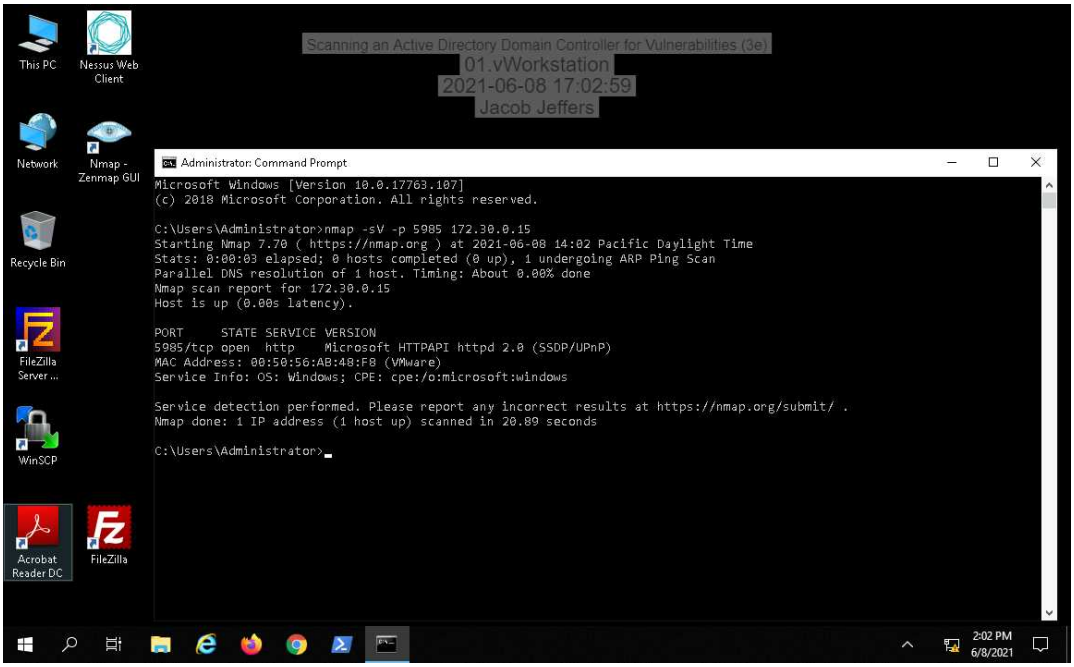
7. **Make a screen capture** showing the **nmap scan results of the Operating System detection scan**.



8. **Identify** the Operating System identified for TargetWindows01.

Microsoft Windows Server 2016 build 10586 - 14393

10. **Make a screen capture** showing the **nmap scan results of the Service Version detection scan**.

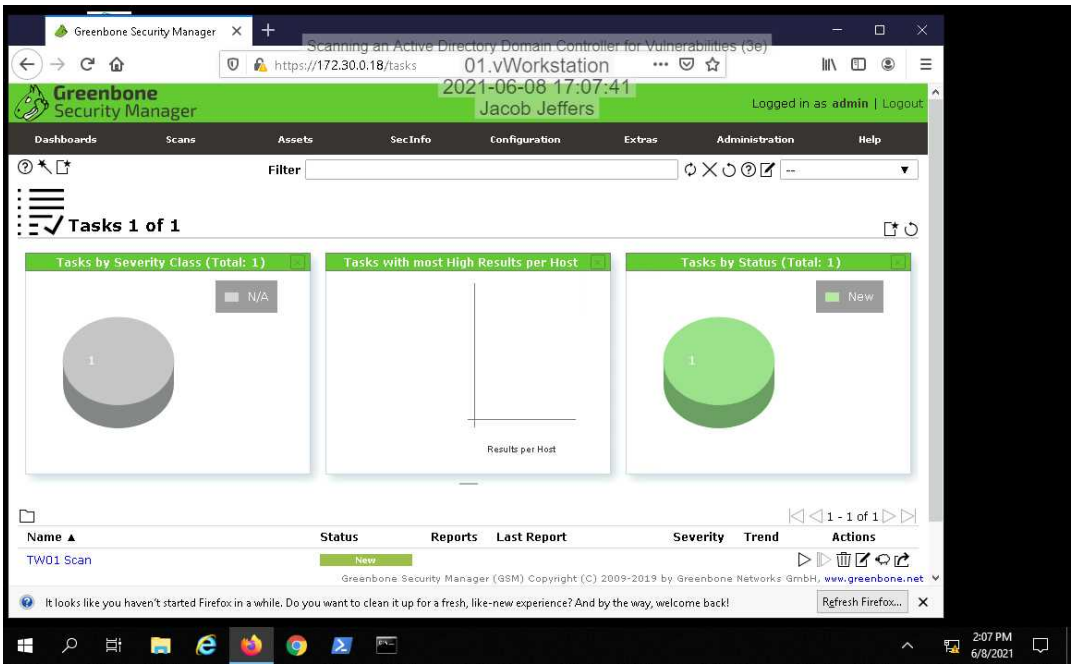


11. **Identify** the service and version running on TCP port 5985.

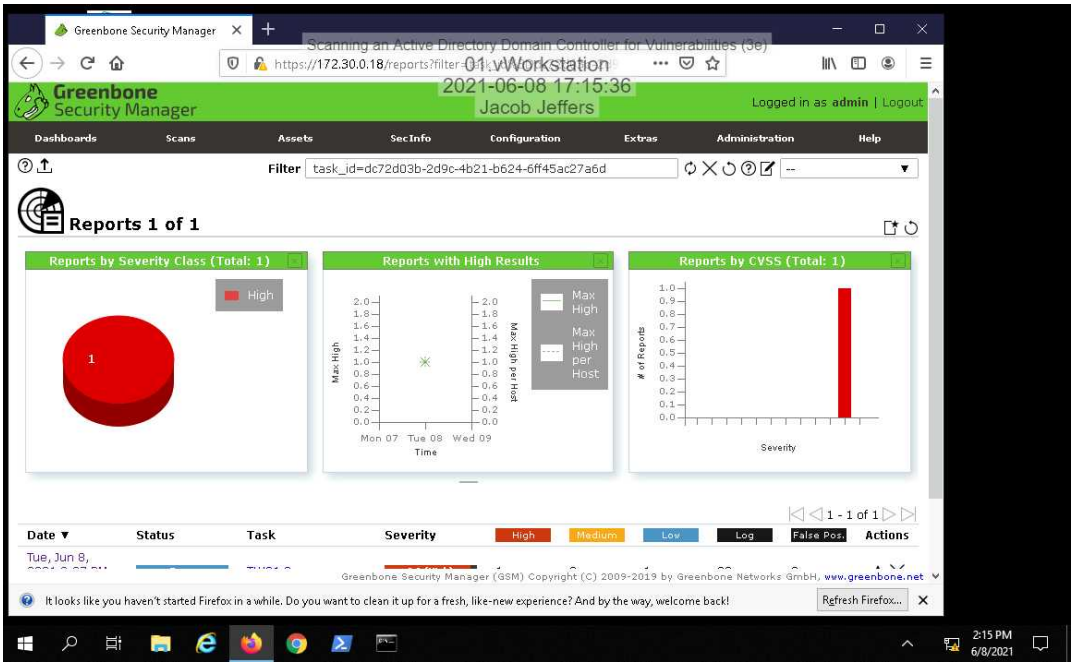
Microsoft HTTPAPI httpd 2.0

Part 2: Conduct a Network Vulnerability Scan with OpenVAS

7. **Make a screen capture** showing the **new OpenVAS task**.



11. **Make a screen capture** showing the **OpenVAS scan report**.

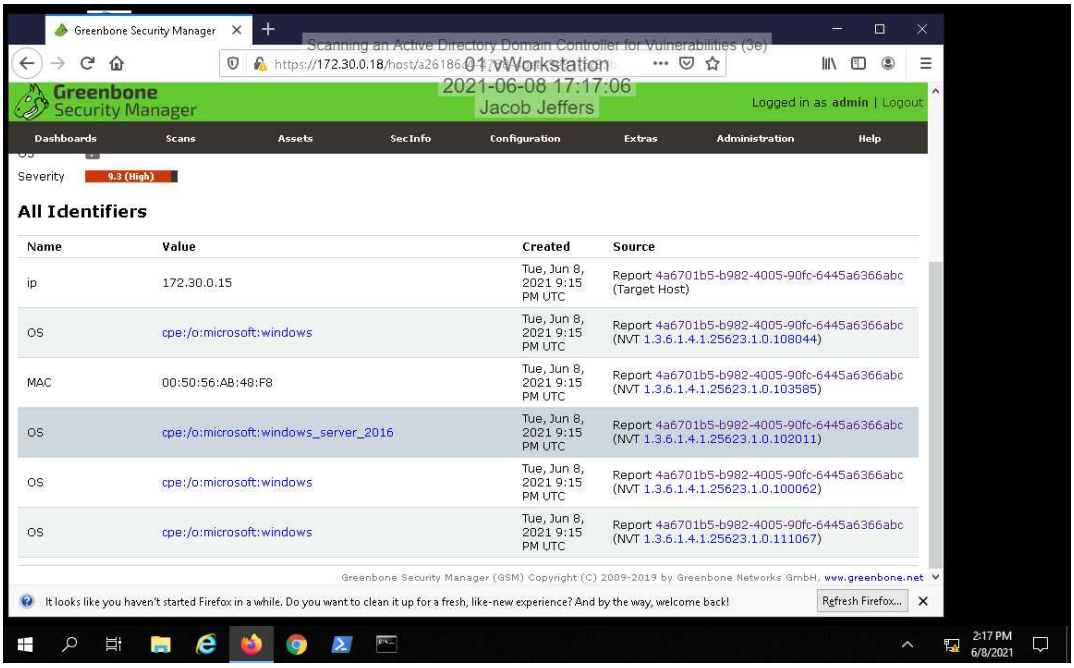


Part 3: Interpret an OpenVAS Report

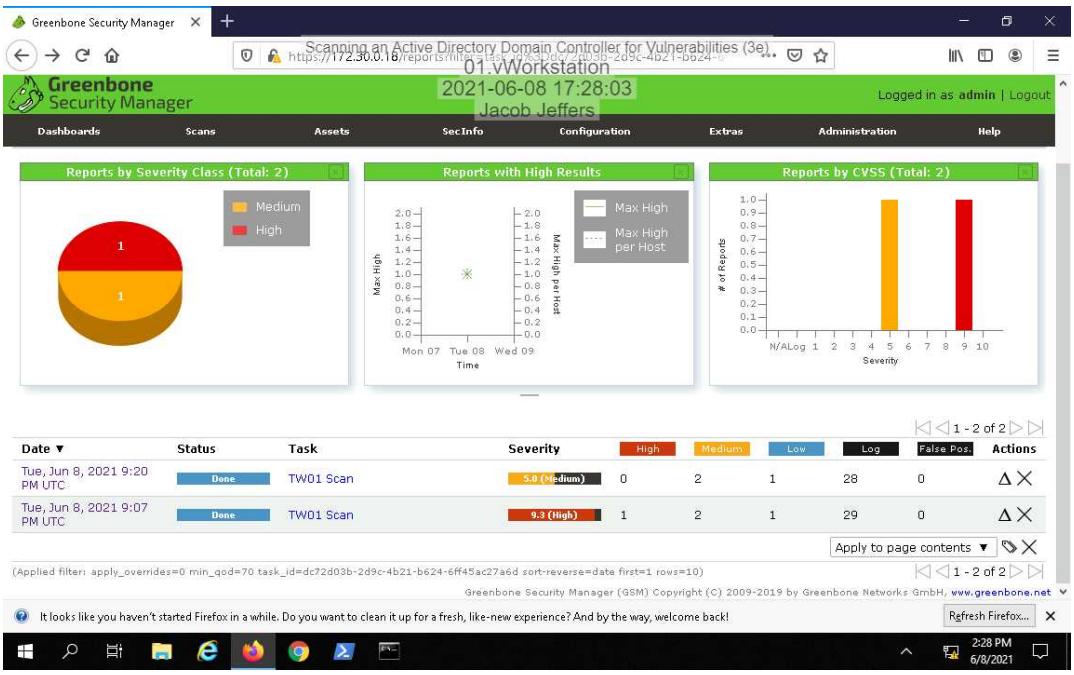
4. **Describe** one method that you could use to correct the vulnerability.

We could disable the port 445.

5. **Make a screen capture** showing the **detailed OpenVAS vulnerability report**.



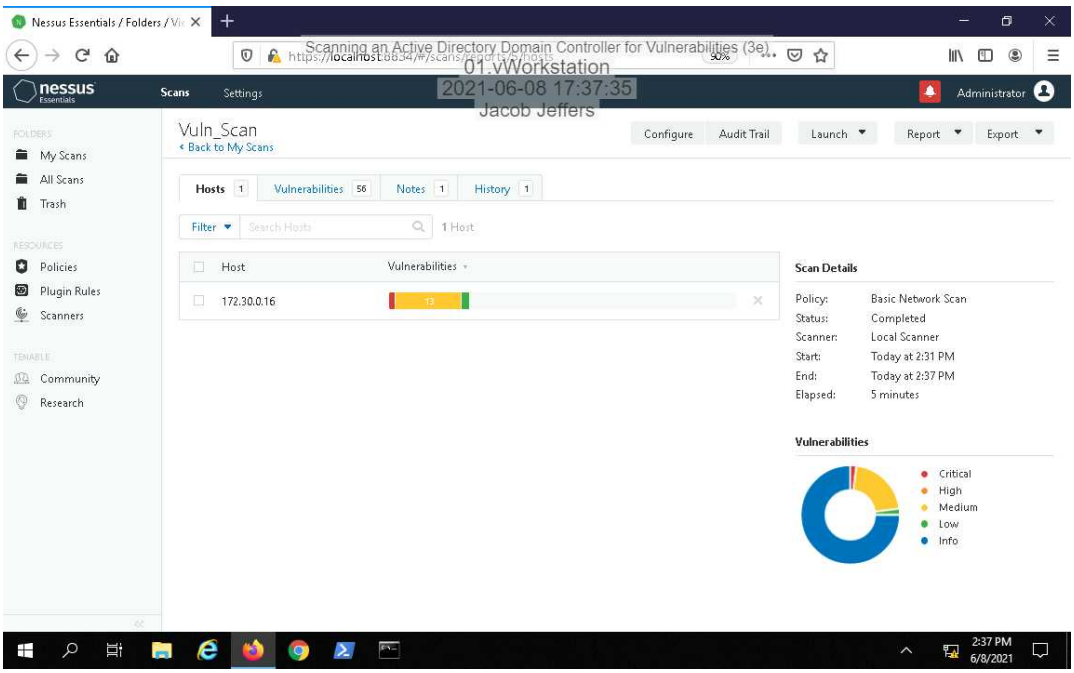
11. **Make a screen capture** showing the **OpenVAS scan report without the SMBv1-related vulnerabilities**.



Section 3: Challenge and Analysis

Part 1: Conduct a Vulnerability Scan

Make a screen capture showing the scan results overview, with the vulnerabilities identified by the scan.

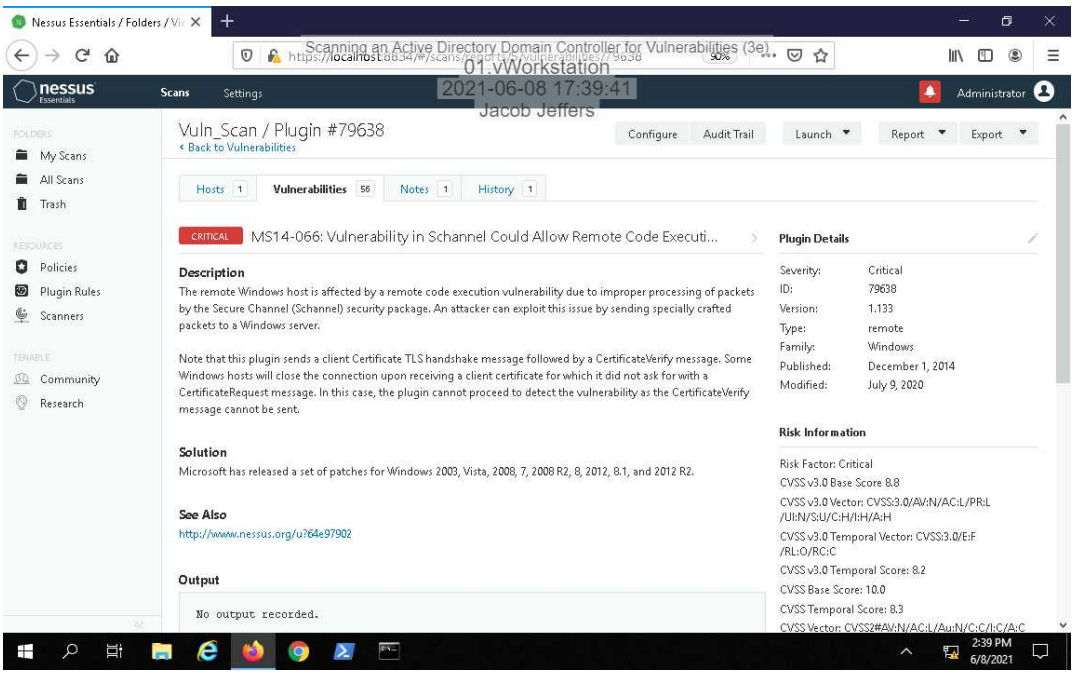


Part 2: Interpret the Vulnerability Scan

Describe the vulnerability and its potential impact, including an example of how the vulnerability might be exploited.

The vulnerability comes about from an improper processing of packets by the Schannel security package. The potential for this is that it allows hackers to remotely exploit the vulnerability allowing for access into the network.

Make a screen capture showing the detailed vulnerability report for the vulnerability you selected.



Report whether the vulnerability is valid or is a false positive and **describe** how you came to that conclusion.

This wasn't a valid vulnerability because the response time didn't change according to the delay.

Part 3: Analyze the CVSS Score

Identify the CVSS score and CVSS string for the vulnerability you selected in Part 2.

CVSS Base Score: 8.8 CVSS String: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- What is the overall CVSS severity rating for the vulnerability you chose? Provide both the numeric score and the qualitative rating.

The overall score is 10, and it is critical.

- The Privileges Required (PR) metric in a CVSS string describes the level of access that an attacker must have to exploit the vulnerability. What level of access is required for the vulnerability you identified?

Remote