

Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

Student:

Jacob Jeffers

Email:

jjeffers6151@ucumberlands.edu

Time on Task:

5 hours, 6 minutes

Progress:

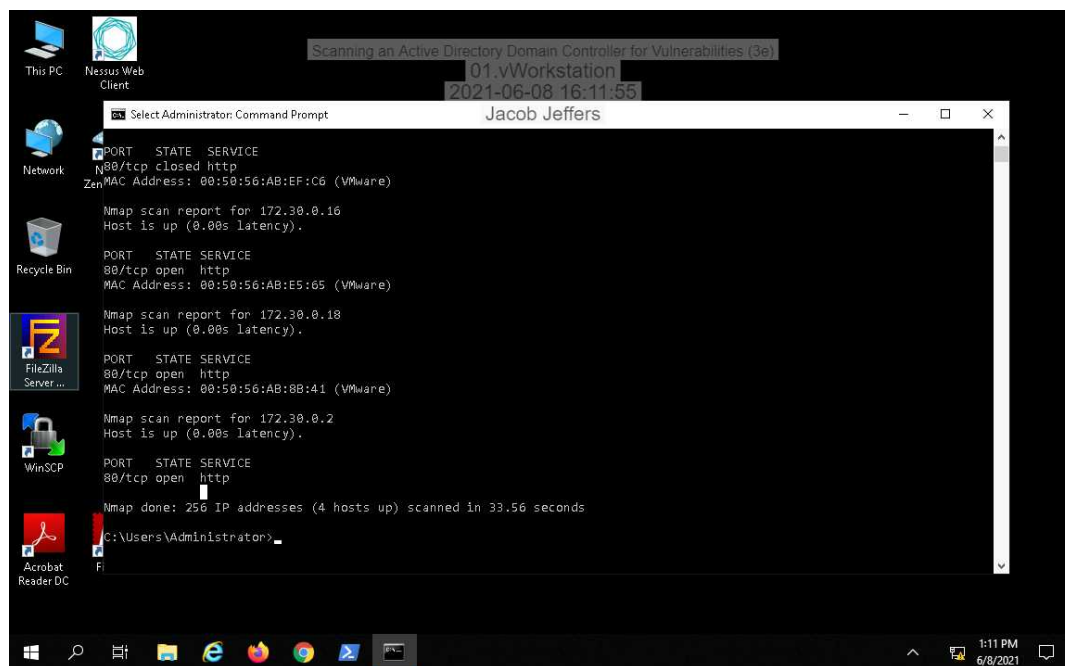
100%

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

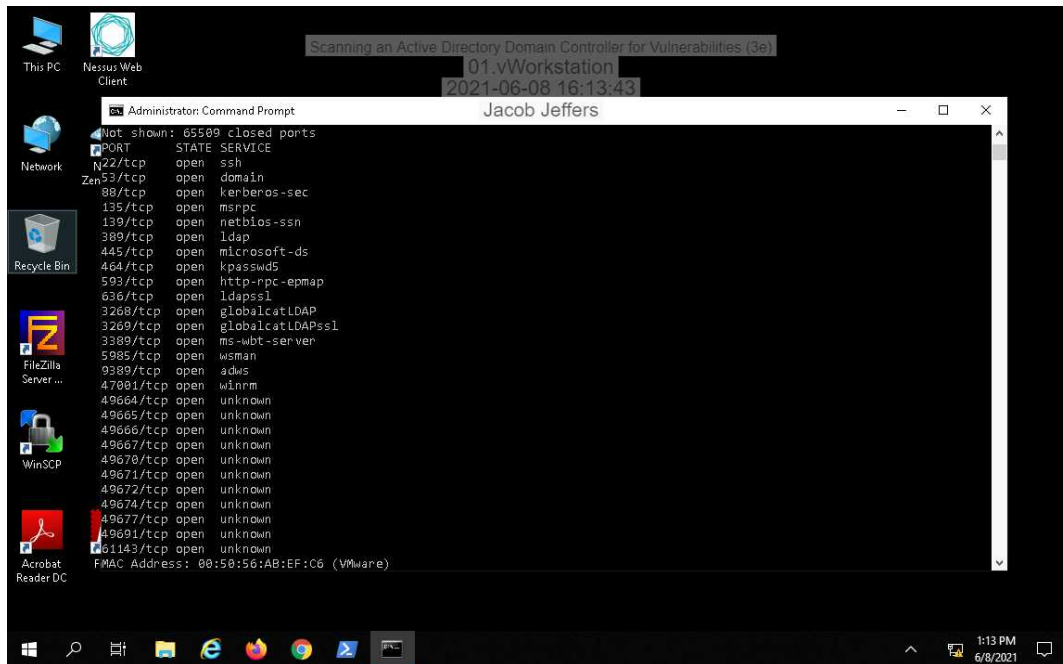
Section 1: Hands-On Demonstration

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.

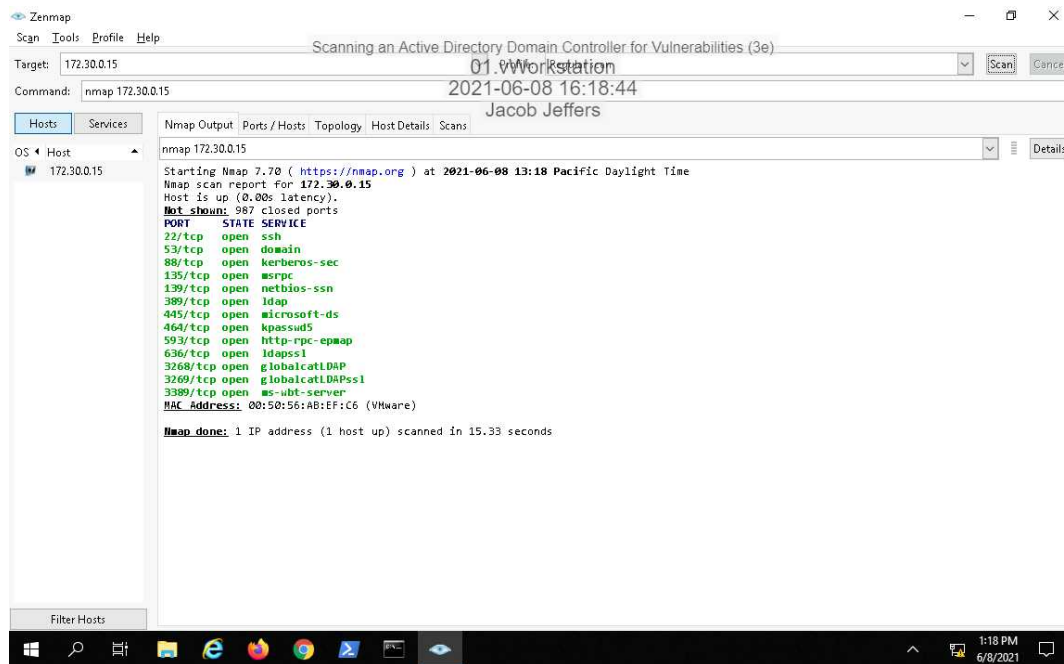
9. **Provide** one reason that you might perform an abbreviated scan.

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

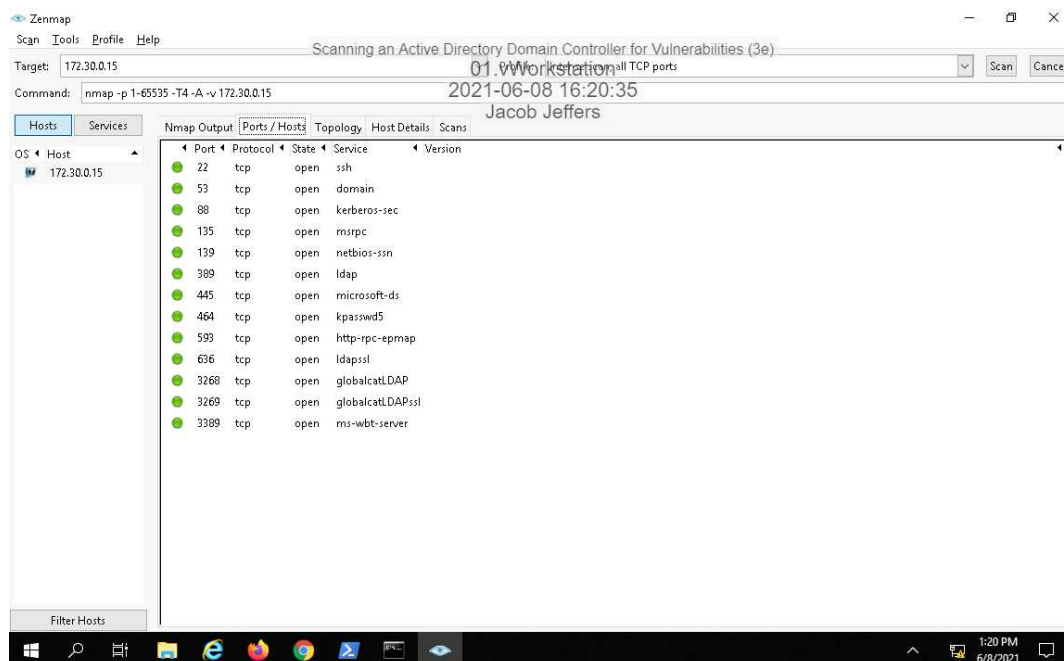
10. **Provide** one reason that you might perform a full scan.

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.

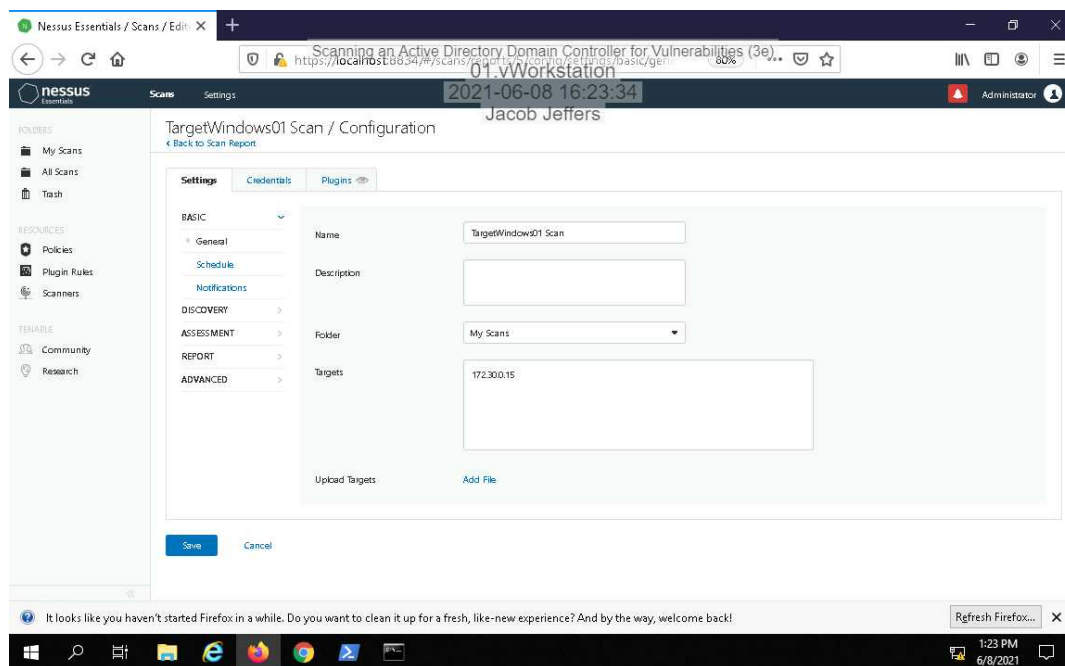


Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

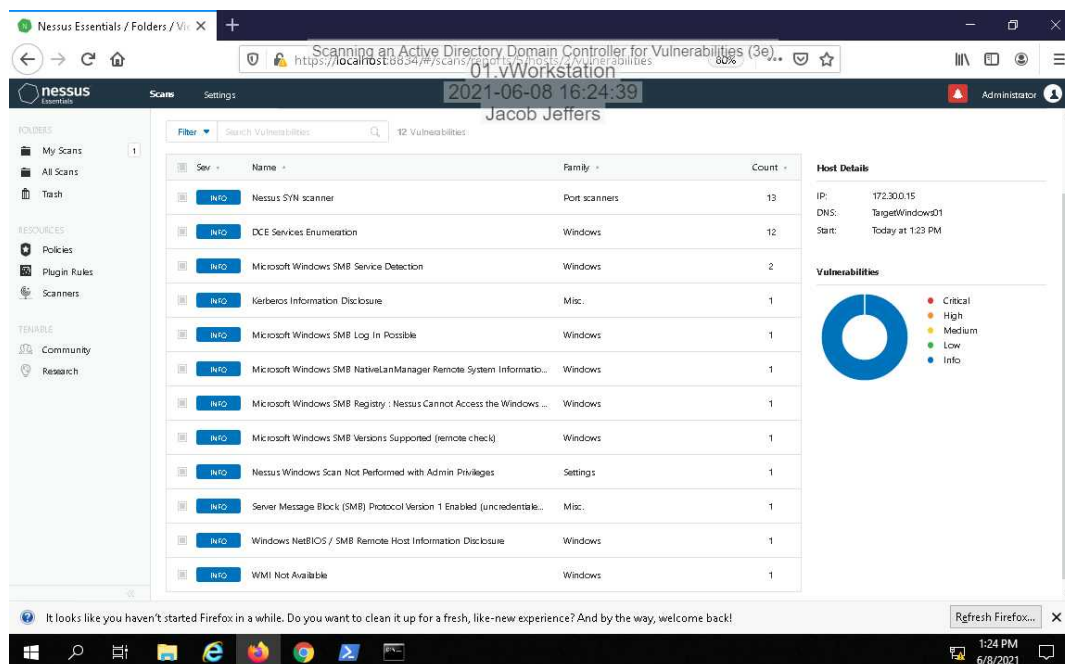
Access Control and Identity Management, Third Edition - Lab 08

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

Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

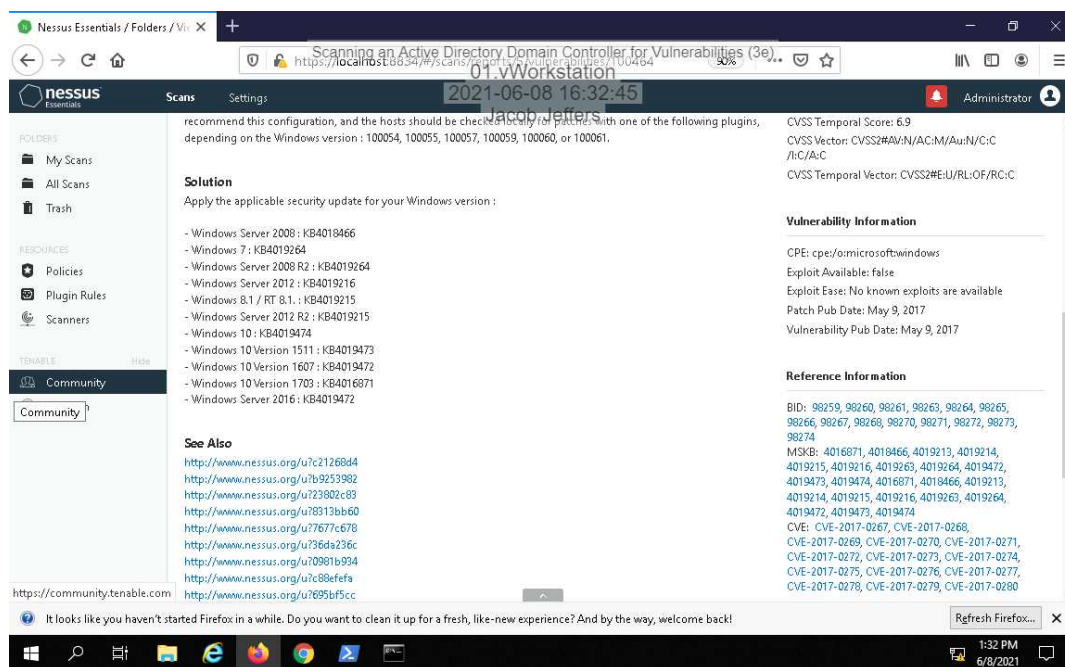
2. **Record** the number of Critical, High, Medium, and Low vulnerabilities in the initial scan of TargetWindows01.

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.

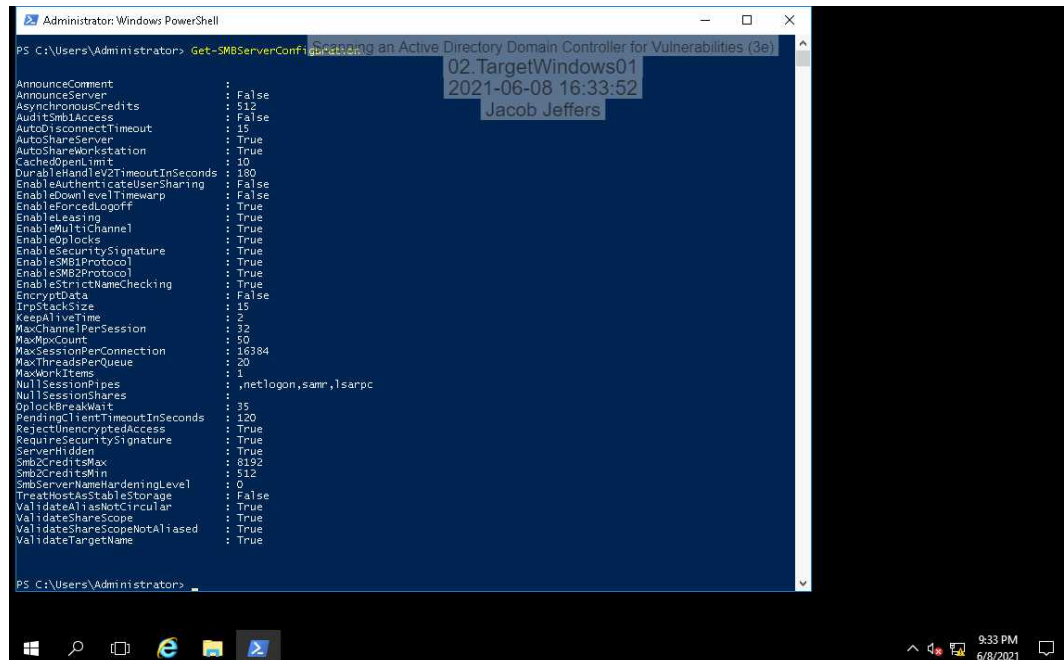
6. **Make a screen capture** showing the **detailed Microsoft SMBv1 Multiple Vulnerabilities** report.



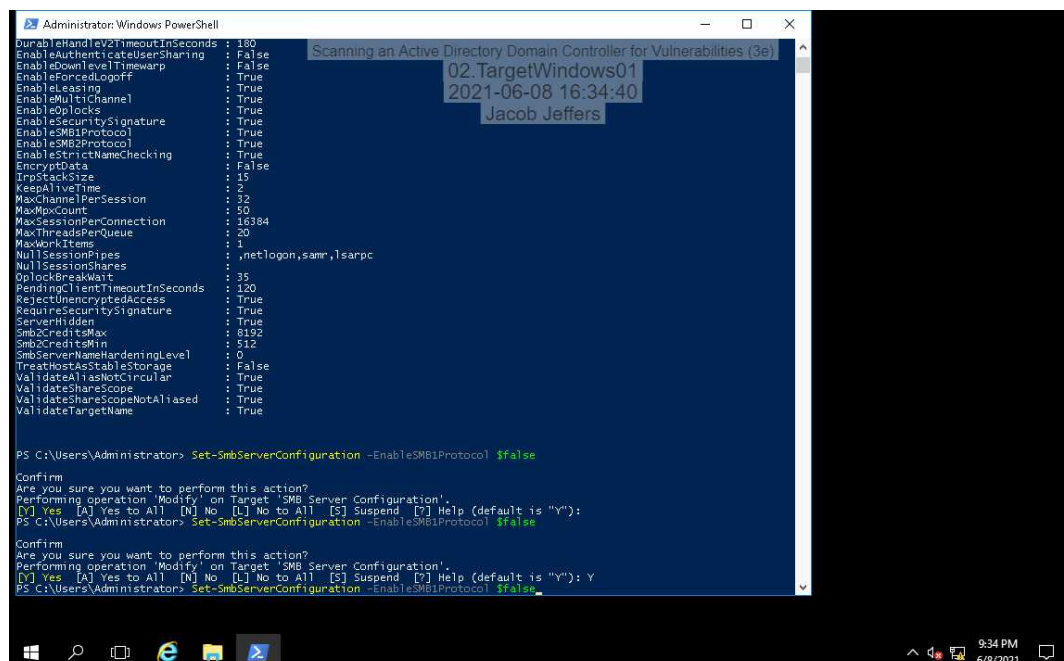
Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

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



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



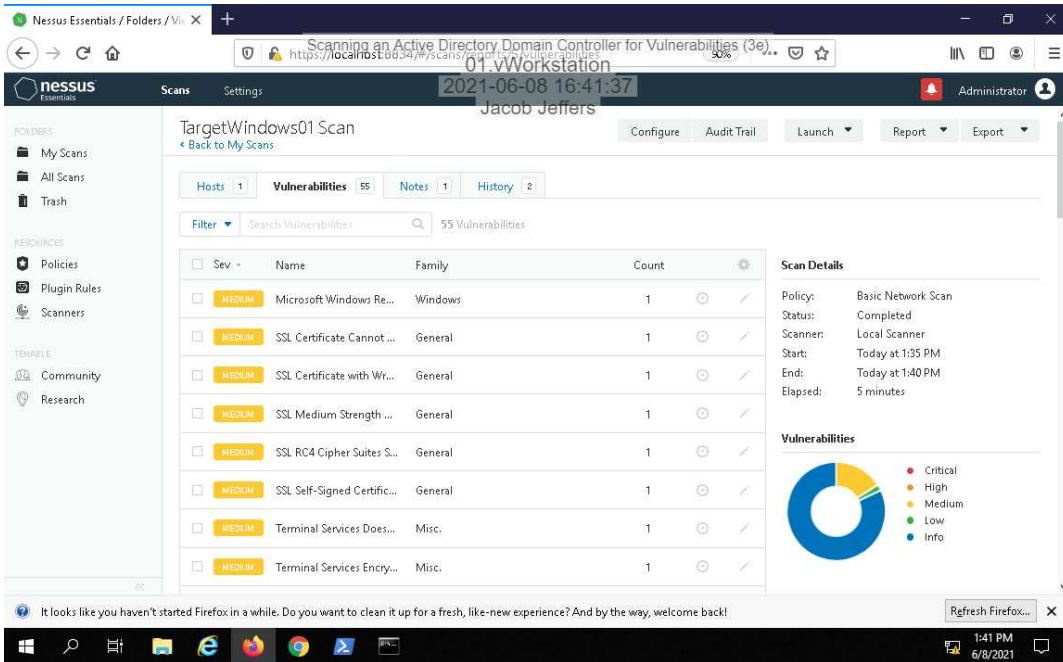
21. Record the number of Critical, High, Medium, and Low vulnerabilities in the second scan of TargetWindows01.

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

Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

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



The screenshot shows the Nessus Essentials web interface. The main content area displays the results for a scan named "TargetWindows01". The "Vulnerabilities" tab is selected, showing a list of 55 vulnerabilities. The table lists the severity, name, family, and count for each vulnerability. The "Scan Details" panel on the right provides information about the scan policy, status, scanner, start and end times, and elapsed time. A donut chart visualizes the distribution of vulnerability severity levels.

Sev	Name	Family	Count
MEDIUM	Microsoft Windows Remote Desktop	Windows	1
MEDIUM	SSL Certificate Cannot Be Verified	General	1
MEDIUM	SSL Certificate with Weak Signature Algorithm	General	1
MEDIUM	SSL Medium Strength Cryptography	General	1
MEDIUM	SSL RC4 Cipher Suites Supported	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
MEDIUM	Terminal Services Does Not Support Secure Channel	Misc.	1
MEDIUM	Terminal Services Encryption Not Enabled	Misc.	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 1:35 PM
- End: Today at 1:40 PM
- Elapsed: 5 minutes

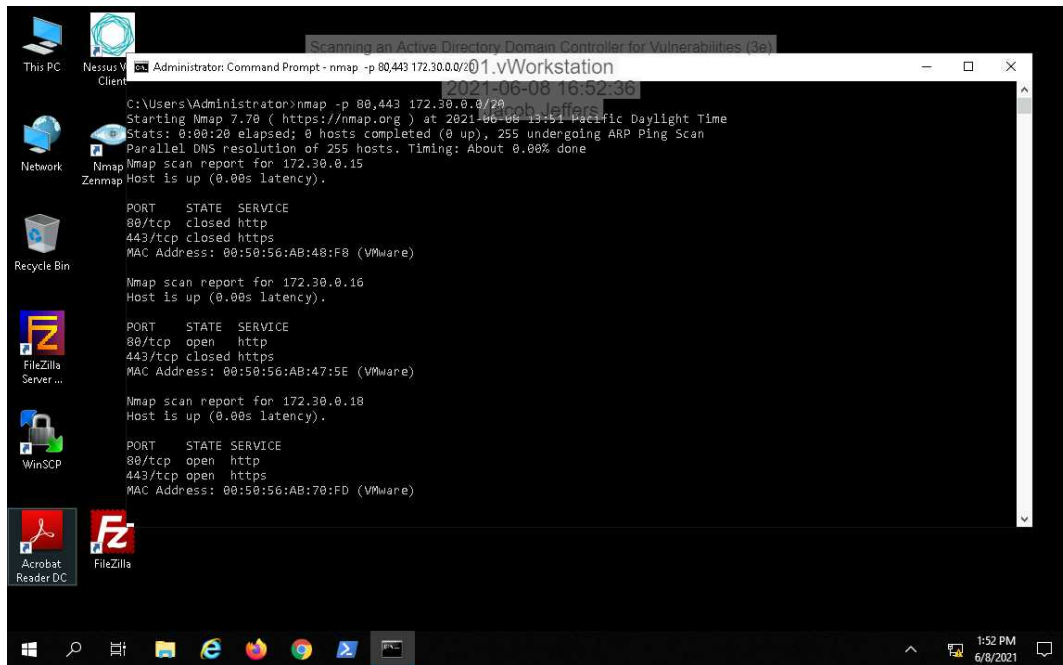
Vulnerabilities

- Critical (red)
- High (orange)
- Medium (yellow)
- Low (green)
- Info (blue)

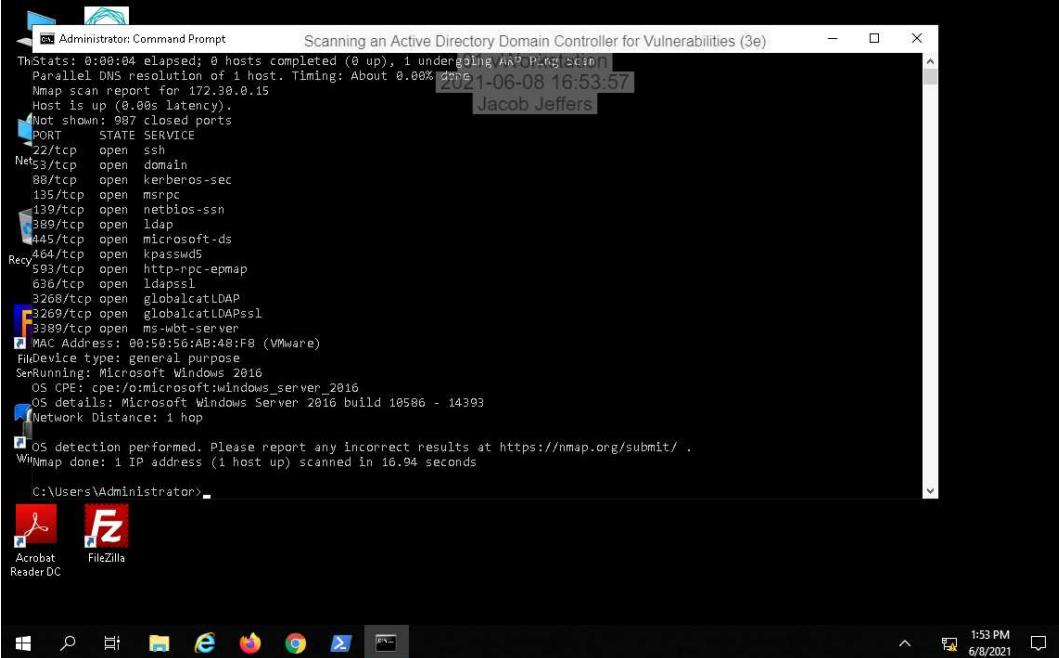
Section 2: Applied Learning

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.



```
Administrator: Command Prompt
Scanning an Active Directory Domain Controller for Vulnerabilities (3e)
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping
Parallel DNS resolution of 1 host. Timing: About 0.00% done.
Nmap scan report for 172.30.0.15
Host is up (0.00s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
MAC Address: 00:50:56:AB:48:F8 (VMware)
FileDevice type: general purpose
ServiceRunning: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 1 hop

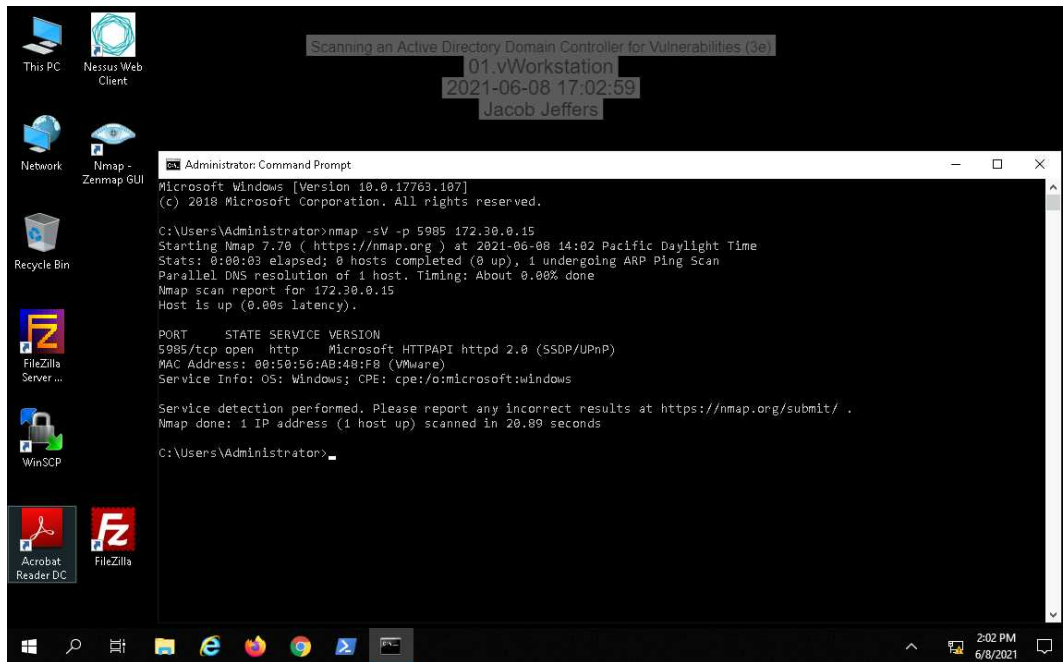
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.94 seconds

C:\Users\Administrator>
```

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.

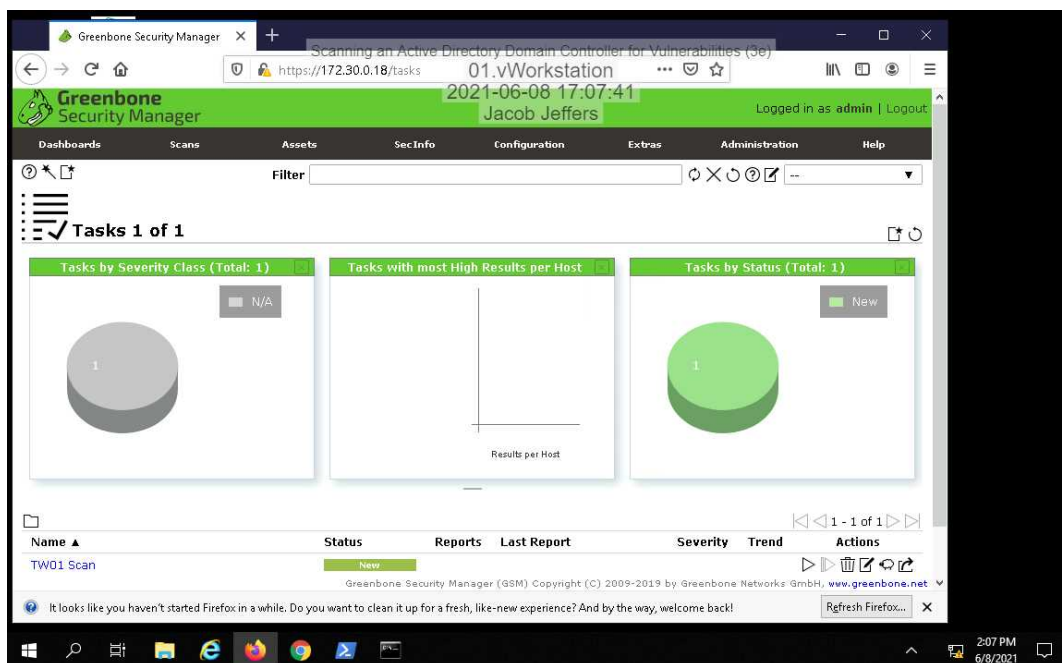
Microsoft HTTPAPI httpd 2.0

Part 2: Conduct a Network Vulnerability Scan with OpenVAS

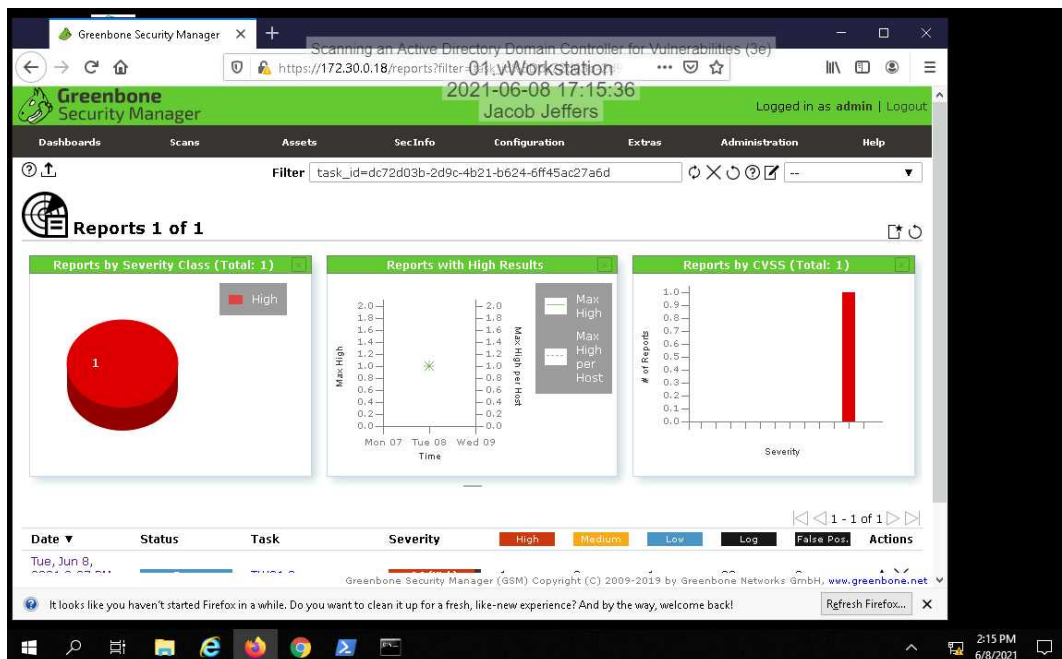
Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

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

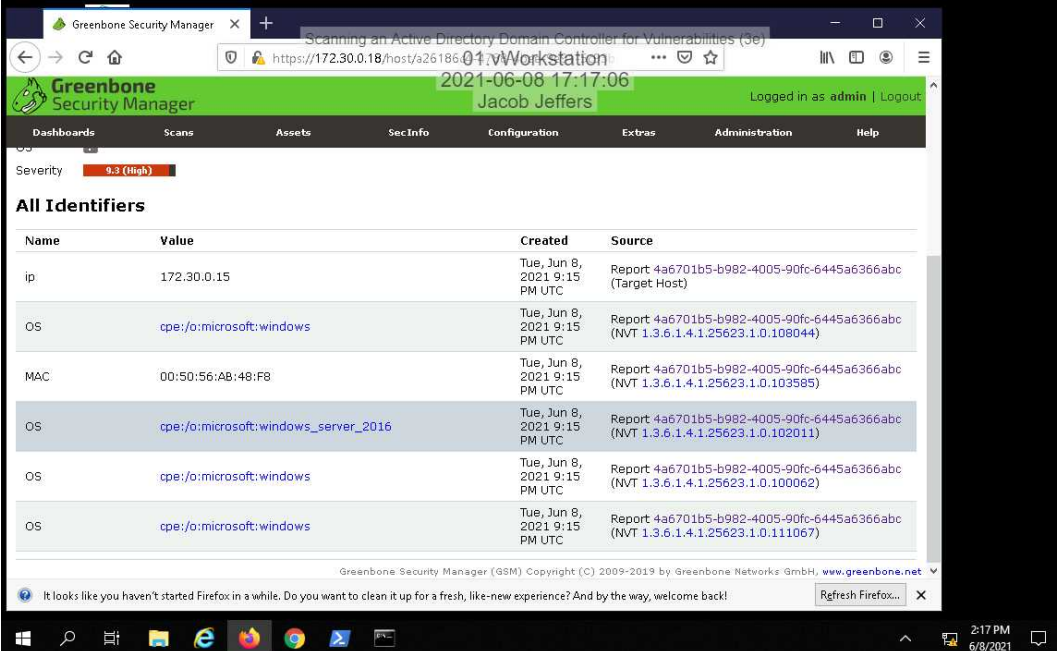
Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

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.



The screenshot displays the Greenbone Security Manager (GSM) web interface. The browser address bar shows the URL `https://172.30.0.18/host/a2618601.vWorkstation`. The interface includes a navigation menu with options like Dashboards, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area shows a severity level of 9.3 (High) and a section titled "All Identifiers". Below this, a table lists various system identifiers:

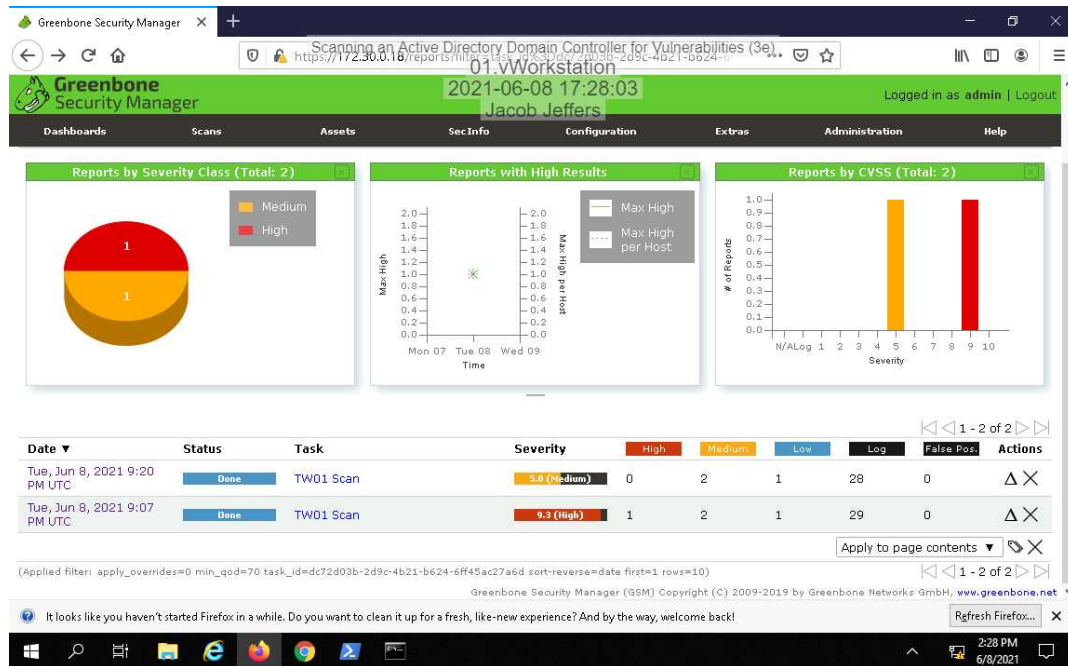
Name	Value	Created	Source
ip	172.30.0.15	Tue, Jun 8, 2021 9:15 PM UTC	Report 4a6701b5-b982-4005-90fc-6445a6366abc (Target Host)
OS	<code>cpe:/o:microsoft:windows</code>	Tue, Jun 8, 2021 9:15 PM UTC	Report 4a6701b5-b982-4005-90fc-6445a6366abc (NVT 1.3.6.1.4.1.25623.1.0.108044)
MAC	00:50:56:A8:48:F8	Tue, Jun 8, 2021 9:15 PM UTC	Report 4a6701b5-b982-4005-90fc-6445a6366abc (NVT 1.3.6.1.4.1.25623.1.0.103585)
OS	<code>cpe:/o:microsoft:windows_server_2016</code>	Tue, Jun 8, 2021 9:15 PM UTC	Report 4a6701b5-b982-4005-90fc-6445a6366abc (NVT 1.3.6.1.4.1.25623.1.0.102011)
OS	<code>cpe:/o:microsoft:windows</code>	Tue, Jun 8, 2021 9:15 PM UTC	Report 4a6701b5-b982-4005-90fc-6445a6366abc (NVT 1.3.6.1.4.1.25623.1.0.100062)
OS	<code>cpe:/o:microsoft:windows</code>	Tue, Jun 8, 2021 9:15 PM UTC	Report 4a6701b5-b982-4005-90fc-6445a6366abc (NVT 1.3.6.1.4.1.25623.1.0.111067)

The footer of the interface includes copyright information: "Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net". A notification at the bottom states: "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!" with a "Refresh Firefox..." button.

Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

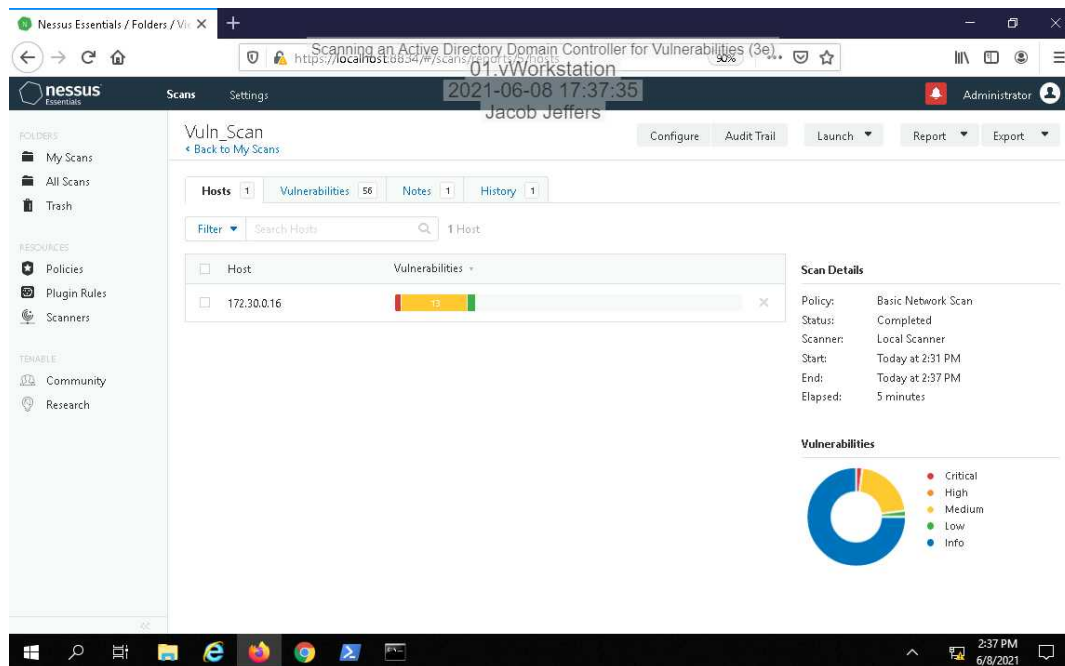
11. Make a screen capture showing the OpenVAS scan report without the SMBv1-related vulnerabilities.



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

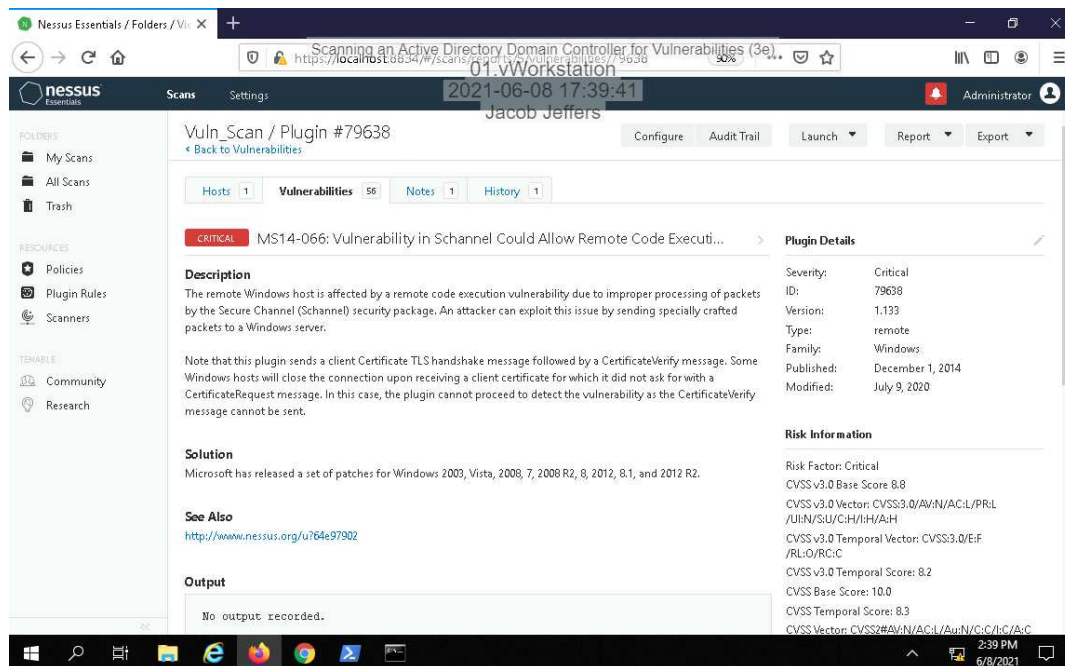
Describe the vulnerability and its potential impact, including an example of how the vulnerability might be exploited.

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.

Scanning an Active Directory Domain Controller for Vulnerabilities (3e)

Access Control and Identity Management, Third Edition - Lab 08

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