

Student:  
Angie Rodriguez

Email:  
angie.rodriguez287@my.tccd.edu

Time on Task:  
5 hours, 18 minutes

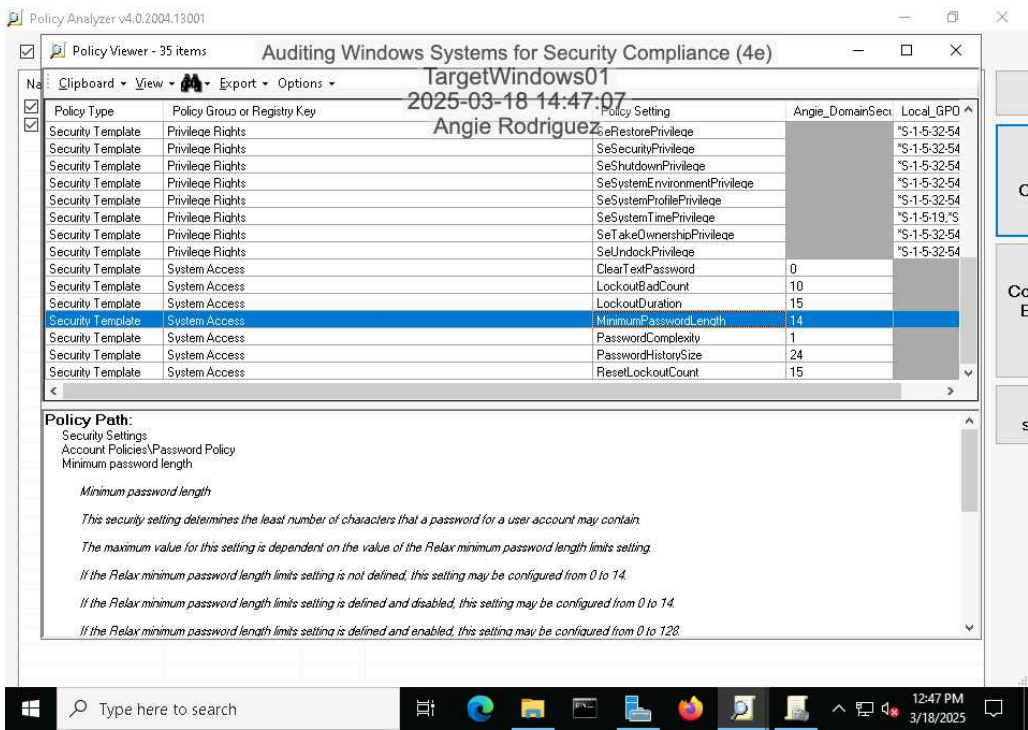
Progress:  
100%

Report Generated: Tuesday, August 12, 2025 at 8:28 PM

Section 1: Hands-On Demonstration

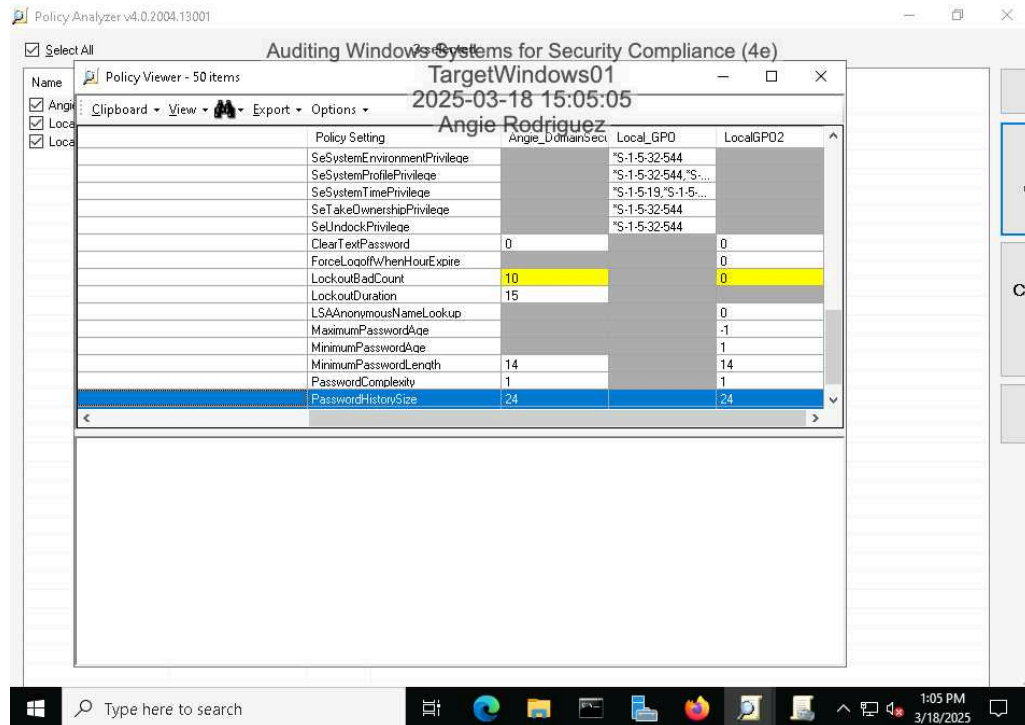
Part 1: Audit a Windows System Using Policy Analyzer

30. Make a screen capture showing the current MinimumPasswordLength setting in the Policy Viewer.



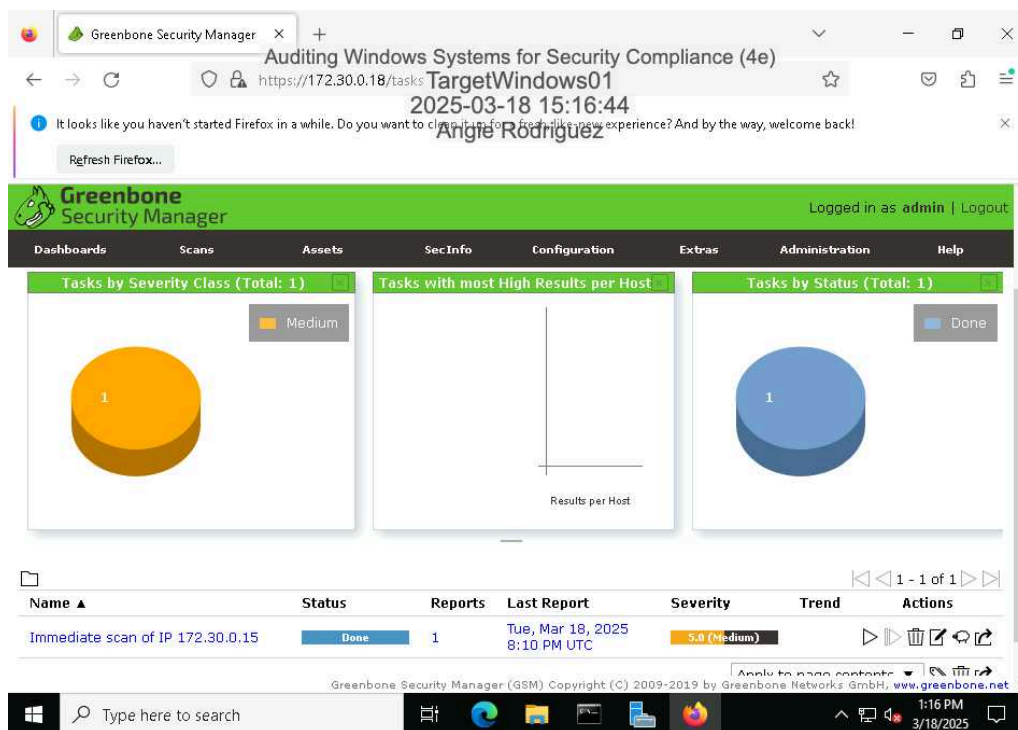
## Security Strategies in Windows Platforms and Applications 4e - Lab 6

49. **Make a screen capture** showing the **updated MinimumPasswordLength** setting in the Policy Viewer.

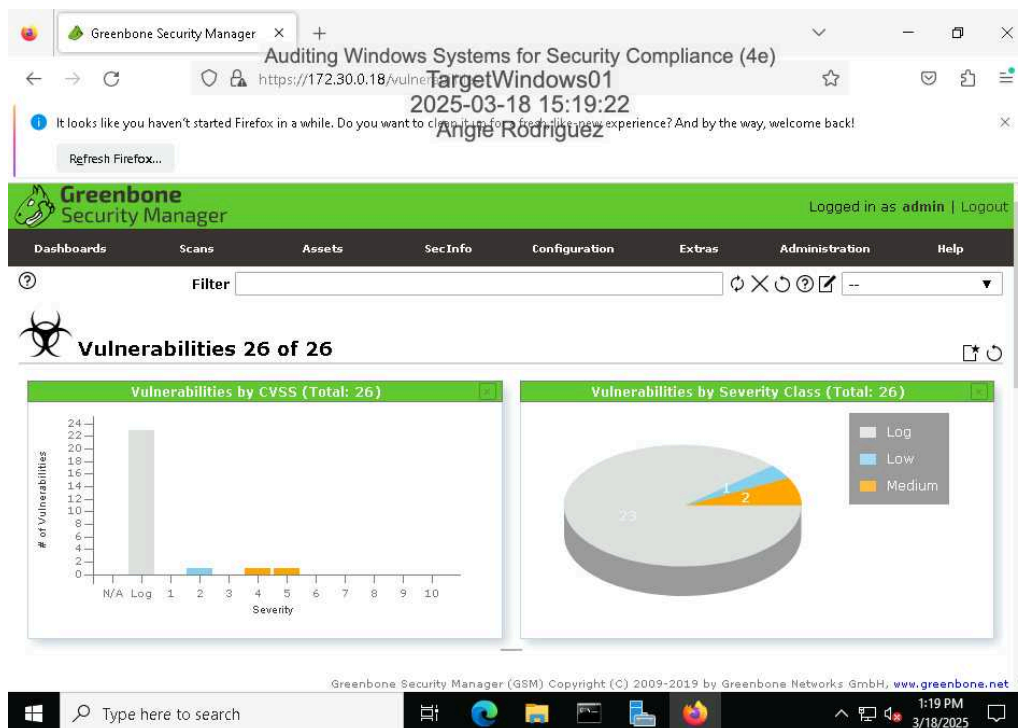


## Part 2: Audit a Windows System using OpenVAS

### 8. Make a screen capture showing the completed scan of TargetWindows01.



### 11. Make a screen capture showing the vulnerabilities from the completed scan of TargetWindows01.



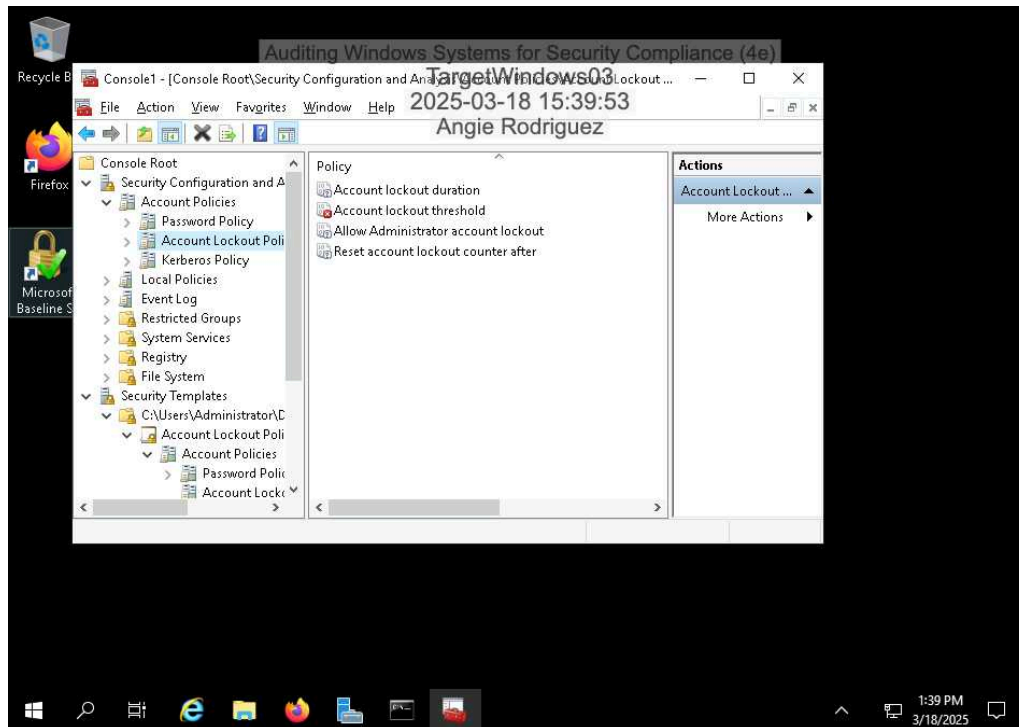
13. **Describe** remediation steps for the vulnerability you selected.

1. Remediation steps for MICROSOFT REMOTE PROCEDURE CALL.A) Restrict access to MSRPC unnecessary services (Block unnecessary ports, use windows firewall).B)Disable unnecessary MSRPC services (Netlogon, RPC locator).C)Patch vulnerabilities.D)Implement network segmentation.E)Use authentication and encryption.2. Remediation steps for distribution computer environment/remote procedure call:A)Restrict access to RPC services B)Disable Unnecessary RPC servicesC)Patch vulnerabilities.D)Use authentication and encryption for RPC/DECE)Limit RPC service exposure F)Segmentation and isolation

### Section 2: Applied Learning

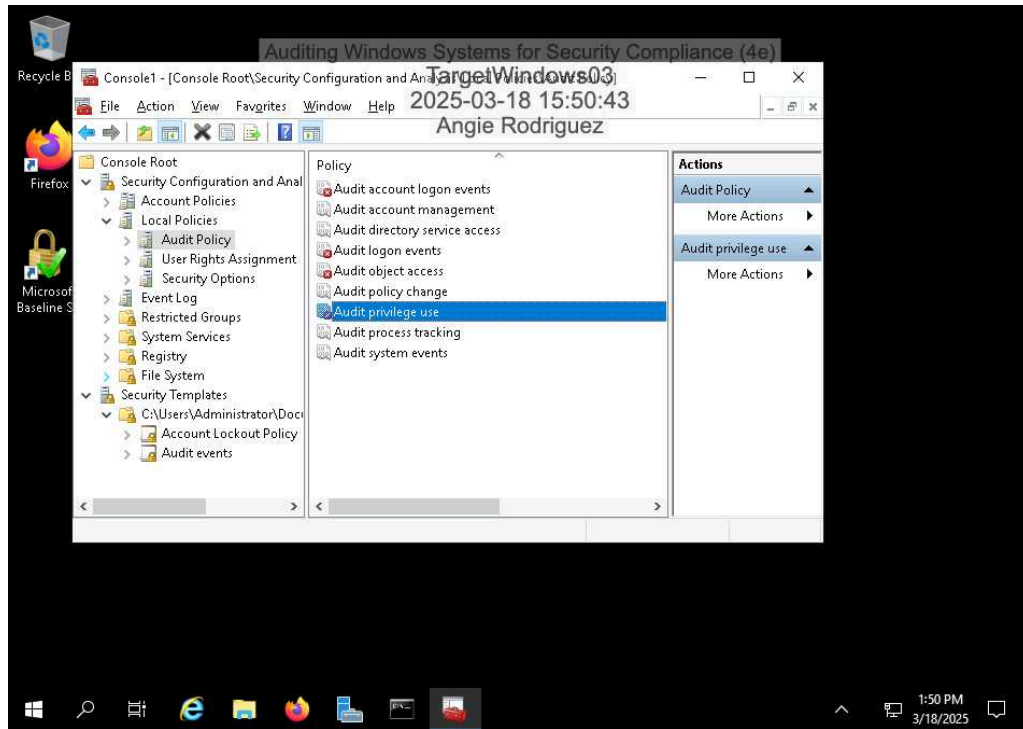
#### Part 1: Profiling a Windows System with the Security Configuration and Analysis (SCA) Tool

19. Make a screen capture showing the results of the SCA scan.



#### Part 2: Modify a Windows System's Audit Settings using SCA

### 8. Make a screen capture showing the results of the SCA scan.



### Section 3: Challenge and Analysis

#### Part 1: Generate a Report of All Vulnerabilities

Make a screen capture of the generated report.

The screenshot displays the Greenbone Security Manager (GSM) interface. The browser address bar shows the URL <https://172.30.0.18/vulnerability>. The page title is "Auditing Windows Systems for Security Compliance (4e) TargetWindows01". The user is logged in as "admin" and the session expires on "2025-03-18 16:25:04". The interface includes a navigation menu with options: Dashboards, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area shows a table of vulnerabilities for the target "TargetWindows01". The table has columns for the vulnerability name, the date and time of the scan, the severity score, the percentage of affected systems, and the number of affected systems. The vulnerabilities listed are: Traceroute (0.0 Log), SSL/TLS: Report Weak Cipher Suites (4.3 Medium), Greenbone OS - 'Spectre' Backporting Error - September 19 (4.7 Medium), Check if Mailserver answer to VRFY and EXPN requests (5.9 Medium), SSL/TLS: Certificate Expired (5.9 Medium), SSL/TLS: Untrusted Certificate Authorities (5.8 Medium), and Greenbone Security Assistant (GSA) Default Credentials (10.0 High). The table is filtered by rows=10, first=21, and sort=severity. The footer of the interface shows the copyright information: "Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net".

Vulnerability	Scan Date/Time	Severity	Percentage	Count
Traceroute	Tue, Mar 18, 2025 9:04 PM UTC	0.0 (Log)	80 %	1
SSL/TLS: Report Weak Cipher Suites	Tue, Mar 18, 2025 9:04 PM UTC	4.3 (Medium)	98 %	1
Greenbone OS - 'Spectre' Backporting Error - September 19	Tue, Mar 18, 2025 9:04 PM UTC	4.7 (Medium)	80 %	1
Check if Mailserver answer to VRFY and EXPN requests	Tue, Mar 18, 2025 9:04 PM UTC	5.9 (Medium)	99 %	1
SSL/TLS: Certificate Expired	Tue, Mar 18, 2025 9:04 PM UTC	5.9 (Medium)	99 %	1
SSL/TLS: Untrusted Certificate Authorities	Tue, Mar 18, 2025 9:04 PM UTC	5.8 (Medium)	99 %	1
Greenbone Security Assistant (GSA) Default Credentials	Tue, Mar 18, 2025 9:05 PM UTC	10.0 (High)	100 %	1

#### Part 2: Add Remediation Steps and Options

# Auditing Windows Systems for Security Compliance (4e)

## Security Strategies in Windows Platforms and Applications 4e - Lab 6

Make a screen capture of your final report.

