Student:	Email:
Angie Rodriguez	angie.rodriguez287@my.tccd.edu

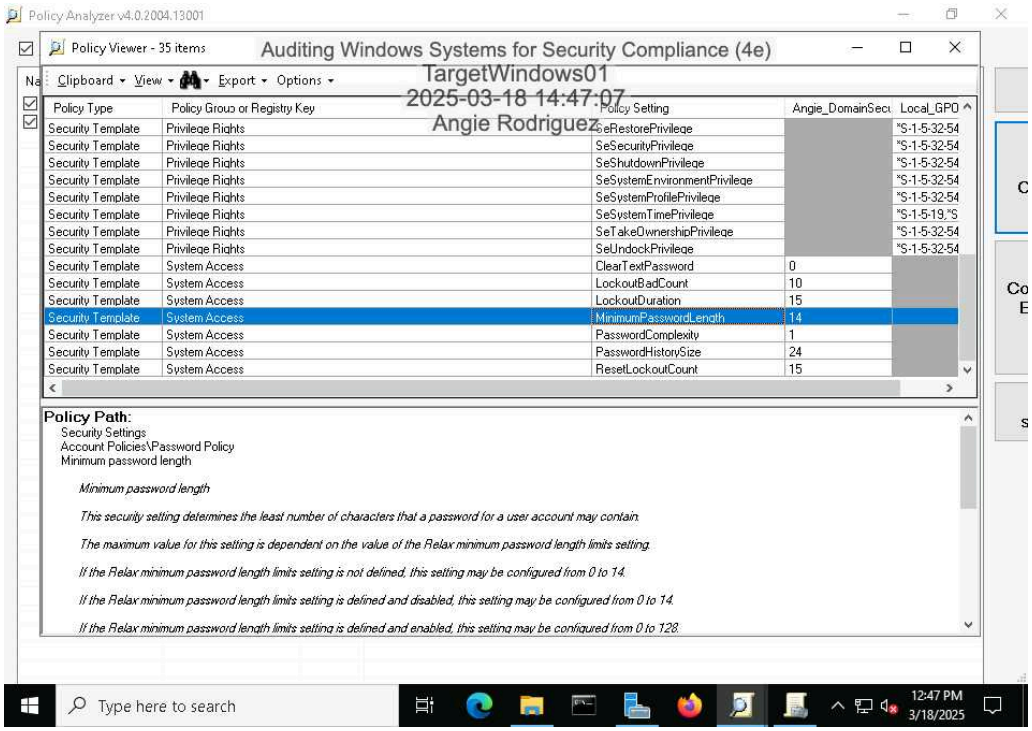
Time on Task:	Progress:
5 hours, 18 minutes	100%

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

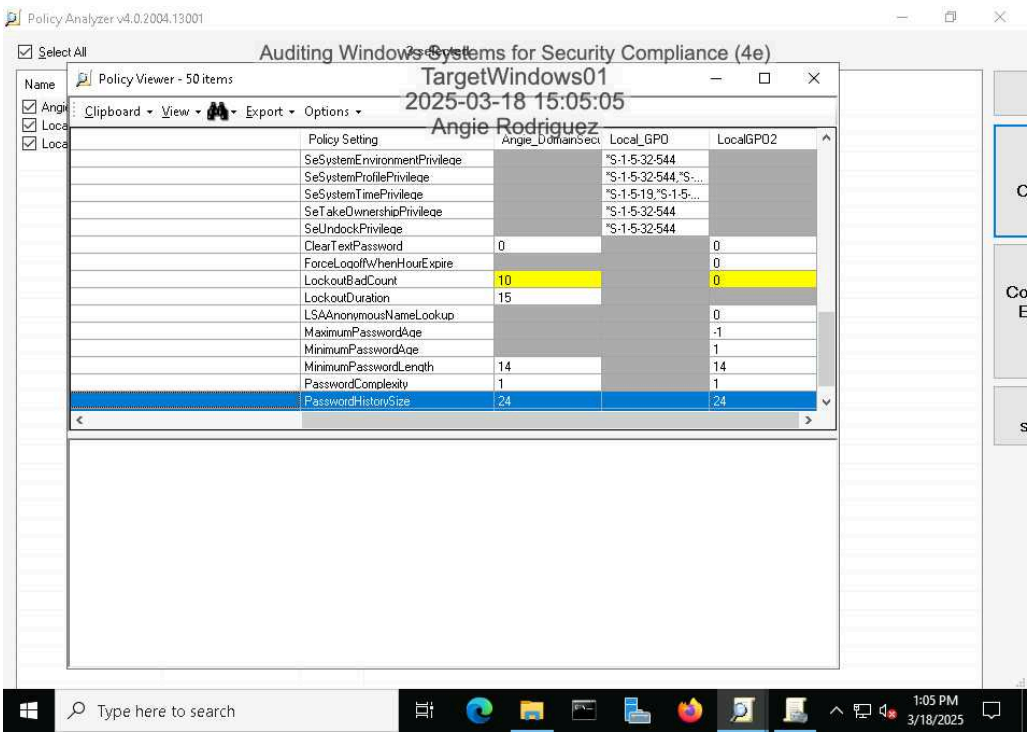
Section 1: Hands-On Demonstration

Part 1: Audit a Windows System Using Policy Analyzer

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

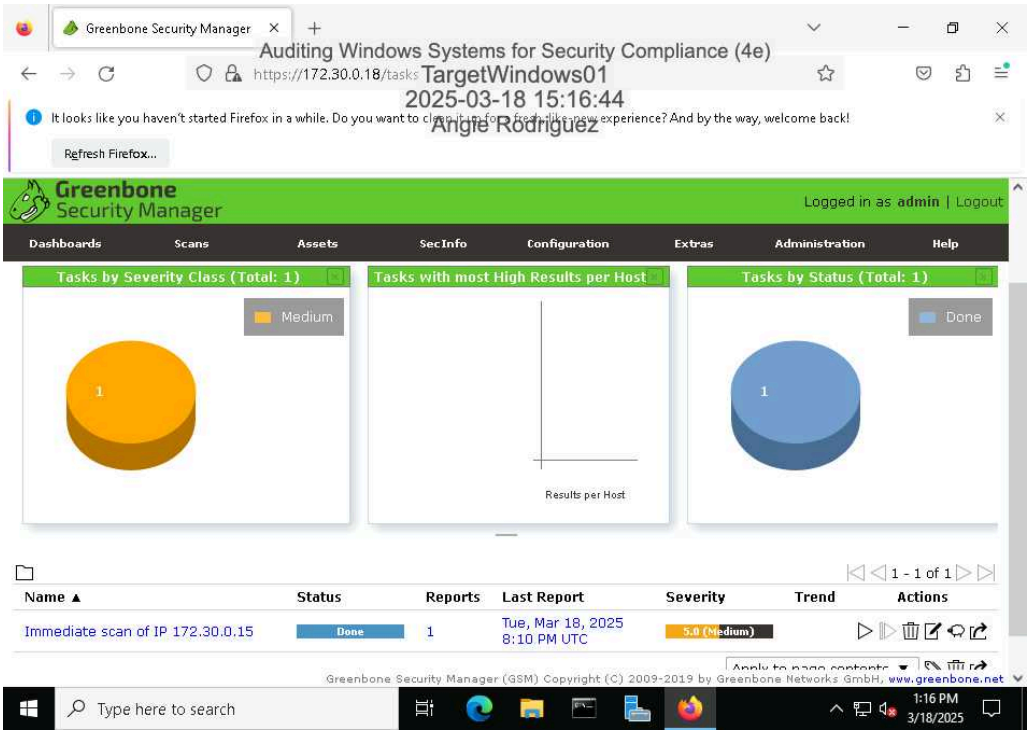


49. **Make a screen capture** showing the **updated MinimumPasswordLength** setting in the Policy Viewer.

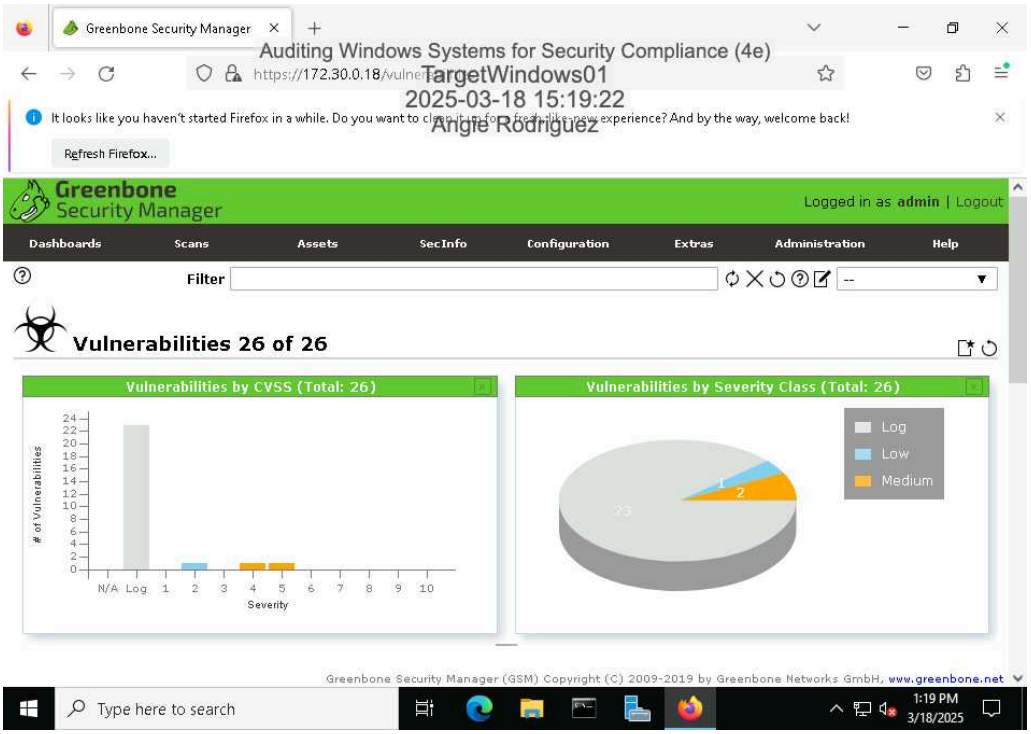


Part 2: Audit a Windows System using OpenVAS

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**.



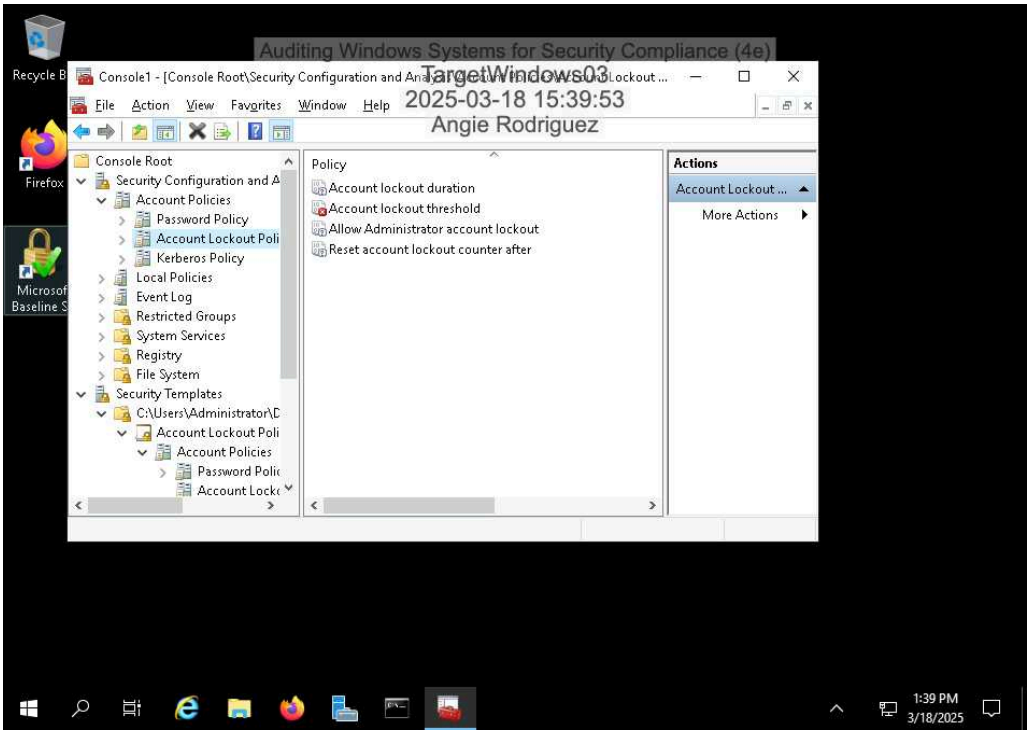
13. **Describe** remediation steps for the vulnerability you selected.

1. Remediation steps for MICROSOFT REMOTE PROCEDURE CALL.A) Restric access to MSRPC unnecessary services (Block unnecessaary ports, use windows firewall).B)Disable unneccessary MSRPC services (Netlogon, RPC locator).C)Patch vulnerabilities.D)Implement network segmentation.E)Use authentication and encryption.2. Remediation steps for disctribution computer environment/remote procedure call:A)Restric 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

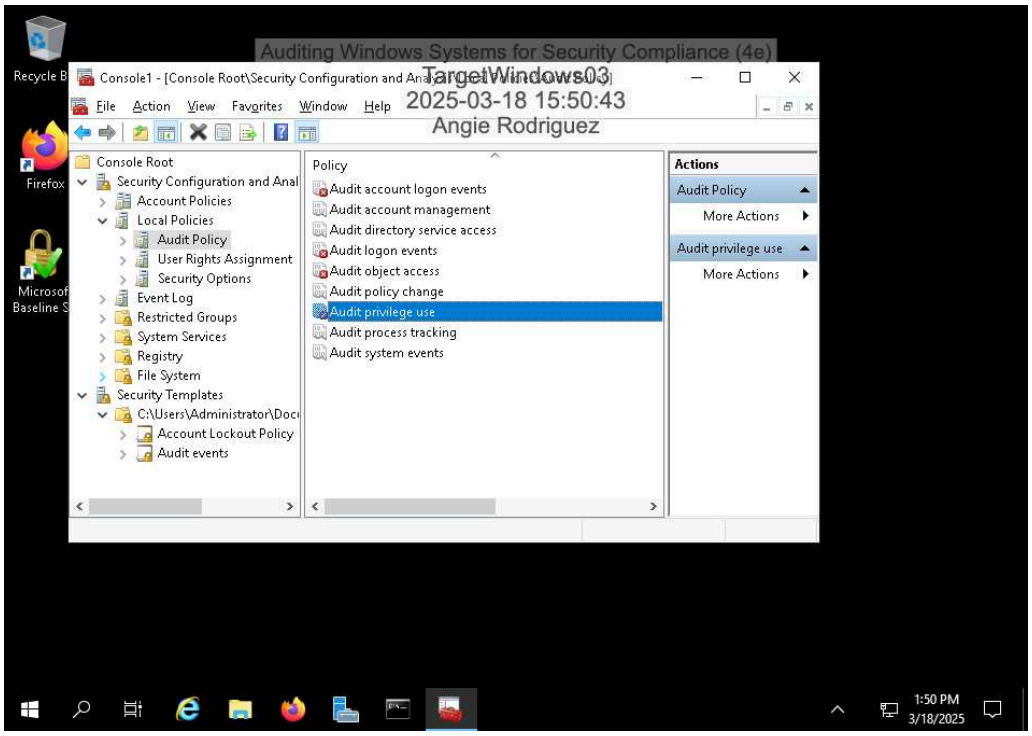
Part 1: Profiling a Windows System with the Security Configuration and Analysis (SCA) Tool

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



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

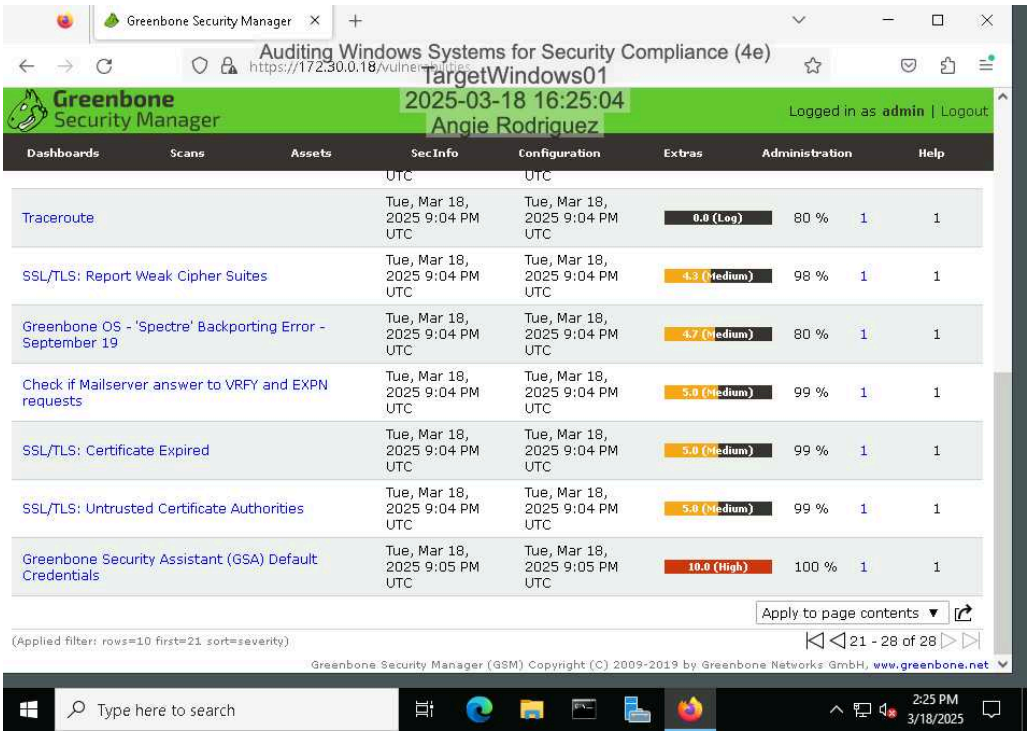
8. **Make a screen capture** showing the **results of the SCA scan**.



Section 3: Challenge and Analysis

Part 1: Generate a Report of All Vulnerabilities

Make a screen capture of the **generated report**.



Part 2: Add Remediation Steps and Options

Make a screen capture of your **final report**.