Student:	Email:
Andrew Sweeney	asweene8@depaul.edu

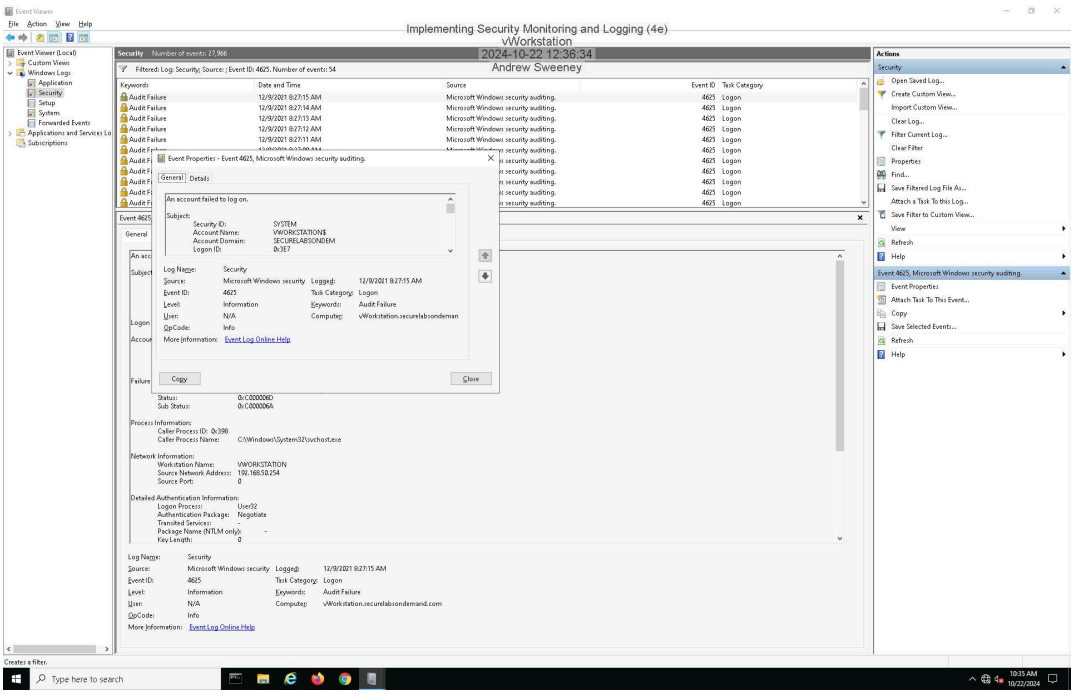
Time on Task:	Progress:
1 hour, 15 minutes	100%

Report Generated: Tuesday, October 22, 2024 at 3:51 PM

Section 1: Hands-On Demonstration

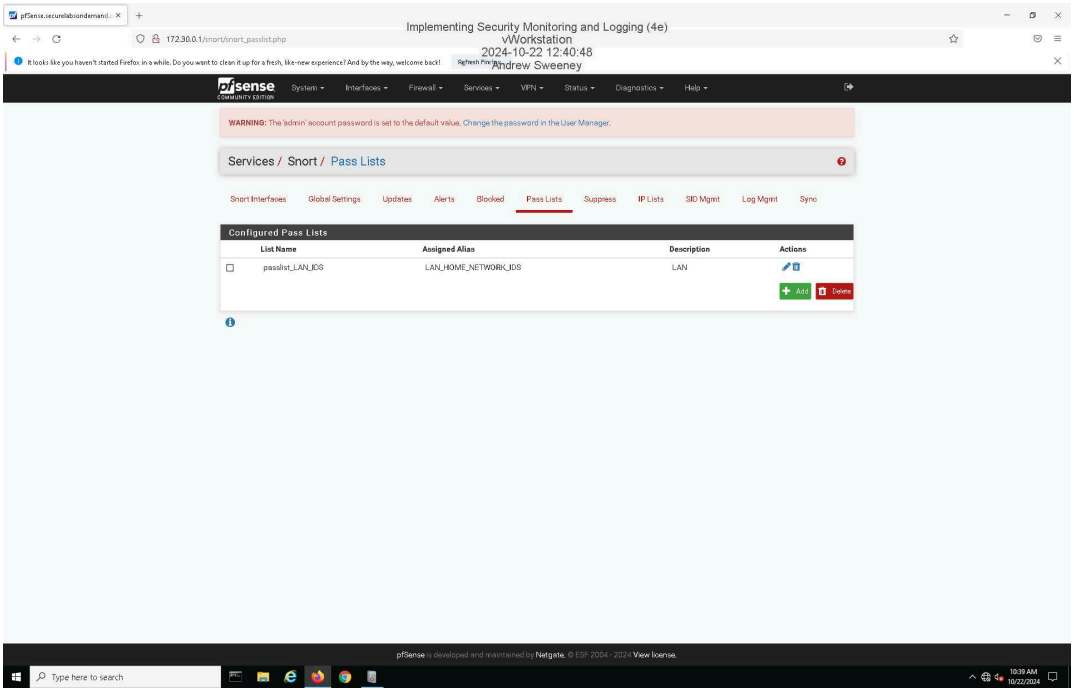
Part 1: Identify Failed Logon Attempts on Windows Systems

8. **Make a screen capture** showing the **Security Event Properties dialog box on the vWorkstation**.

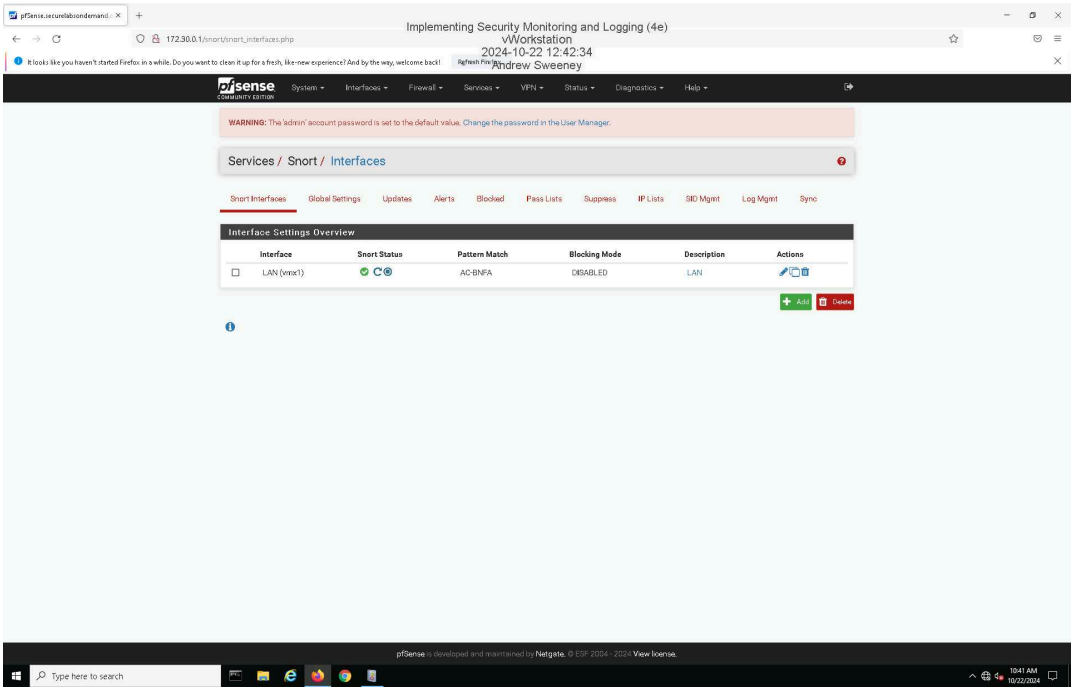


Part 2: Monitor Network Activity with Snort

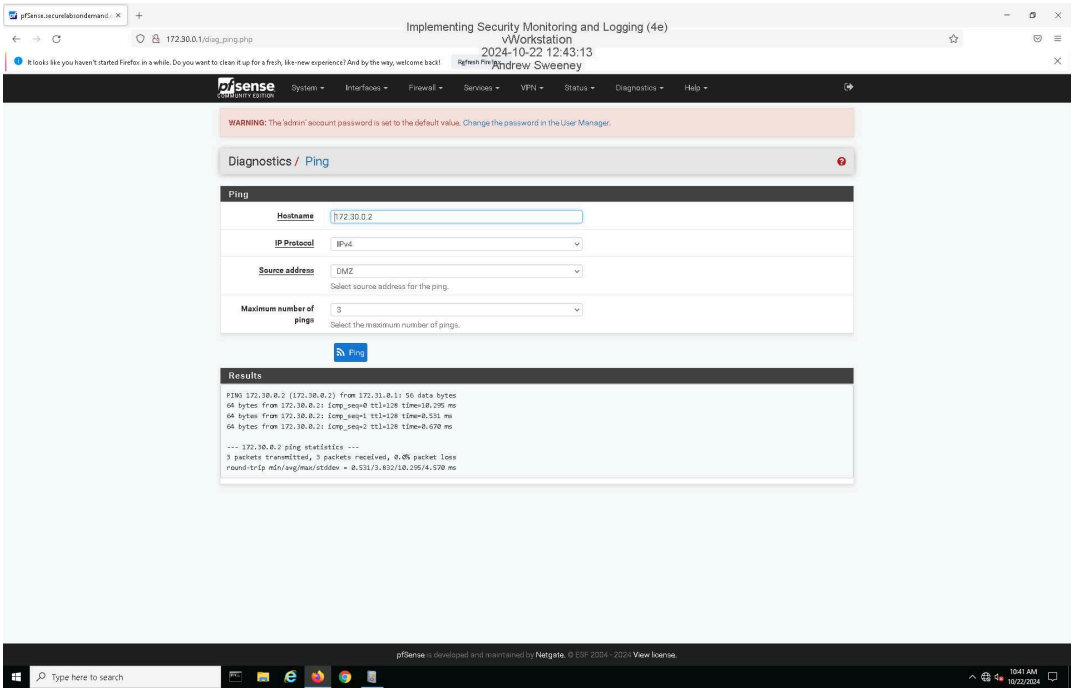
17. **Make a screen capture** showing the **updated Pass Lists page**.



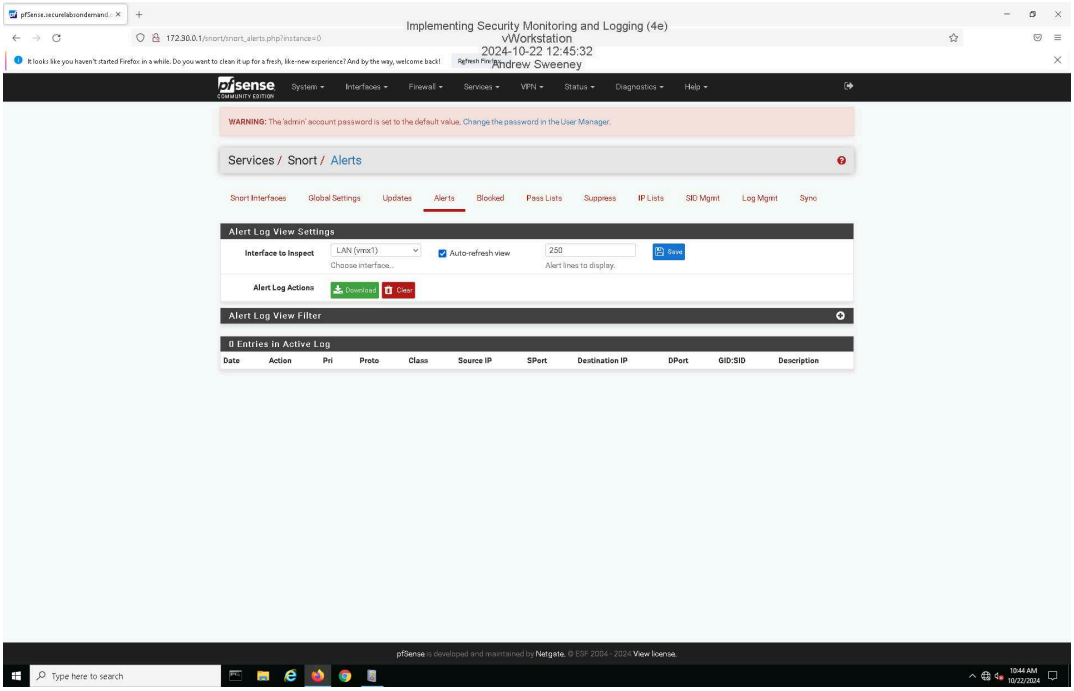
31. **Make a screen capture** showing the **active Snort status on the LAN interface**.



36. **Make a screen capture** showing the **successful ping results**.



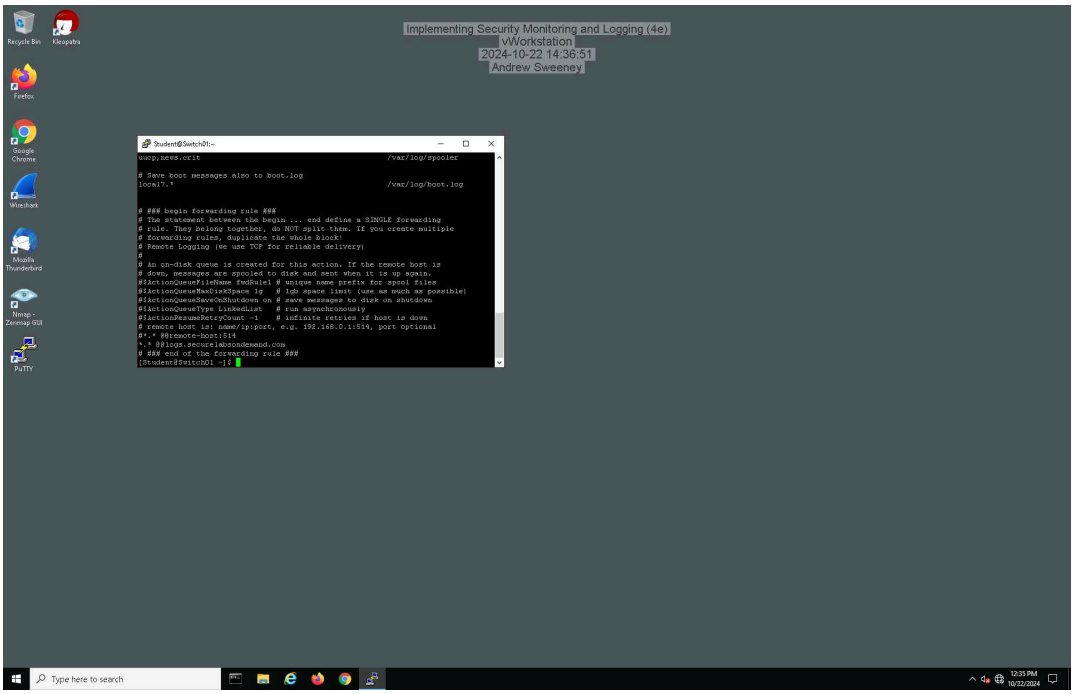
41. **Make a screen capture** showing the **ICMP alerts in the Snort Active Log**.



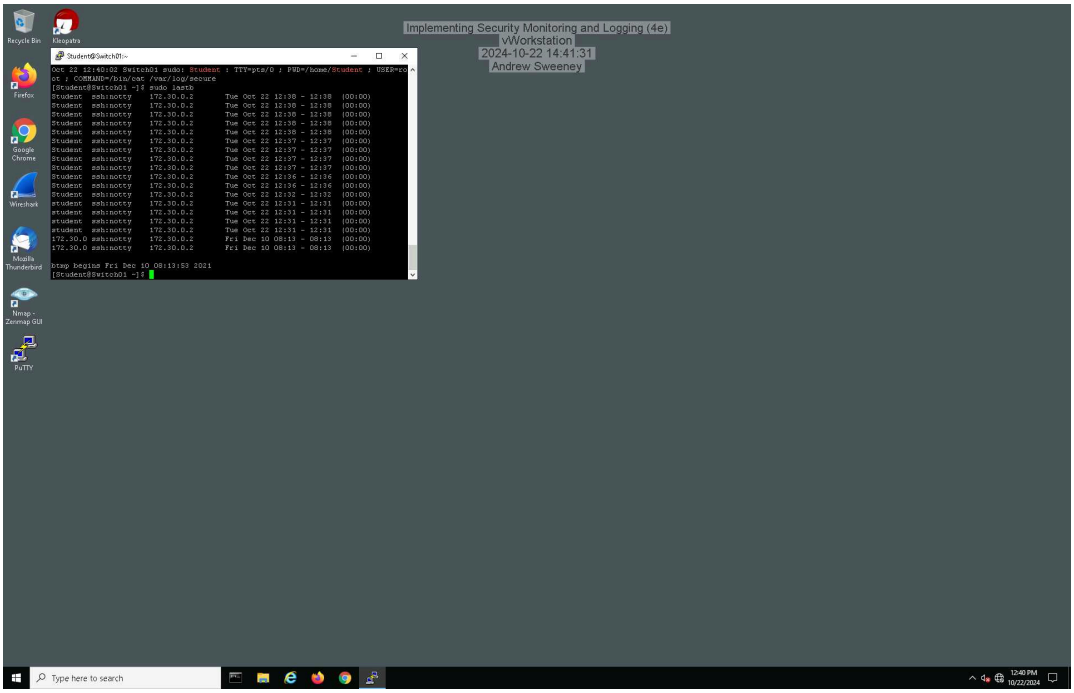
Section 2: Applied Learning

Part 1: Identify Failed Logon Attempts on Linux Systems

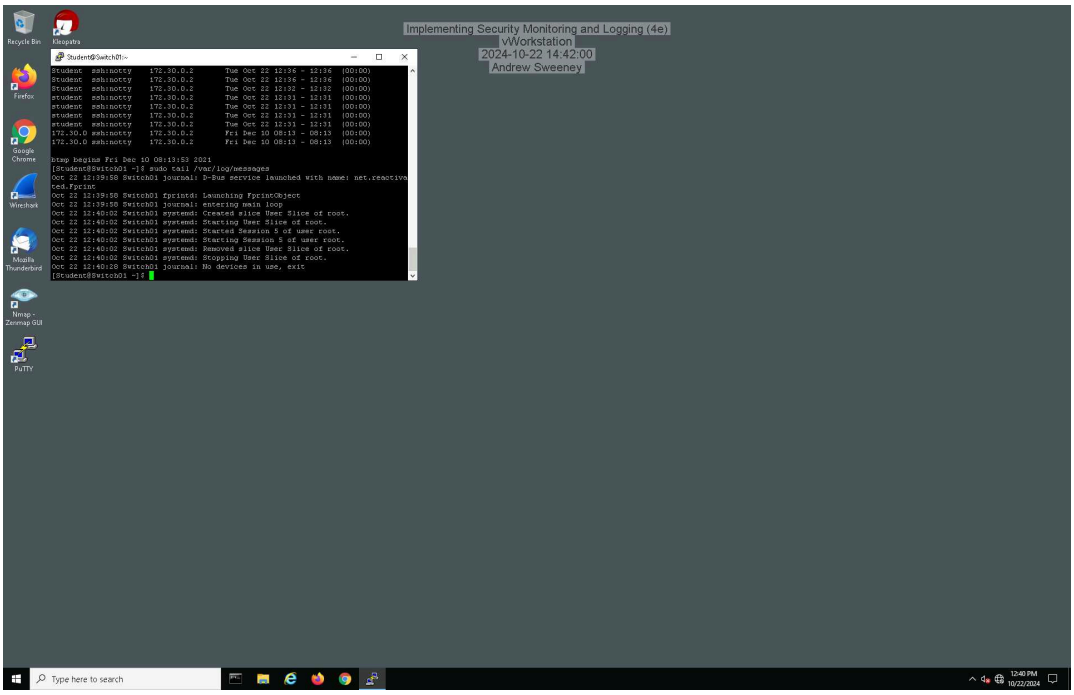
10. **Make a screen capture** showing the **edited rsyslog.conf file**.



20. **Make a screen capture** showing the **failed login attempts**.

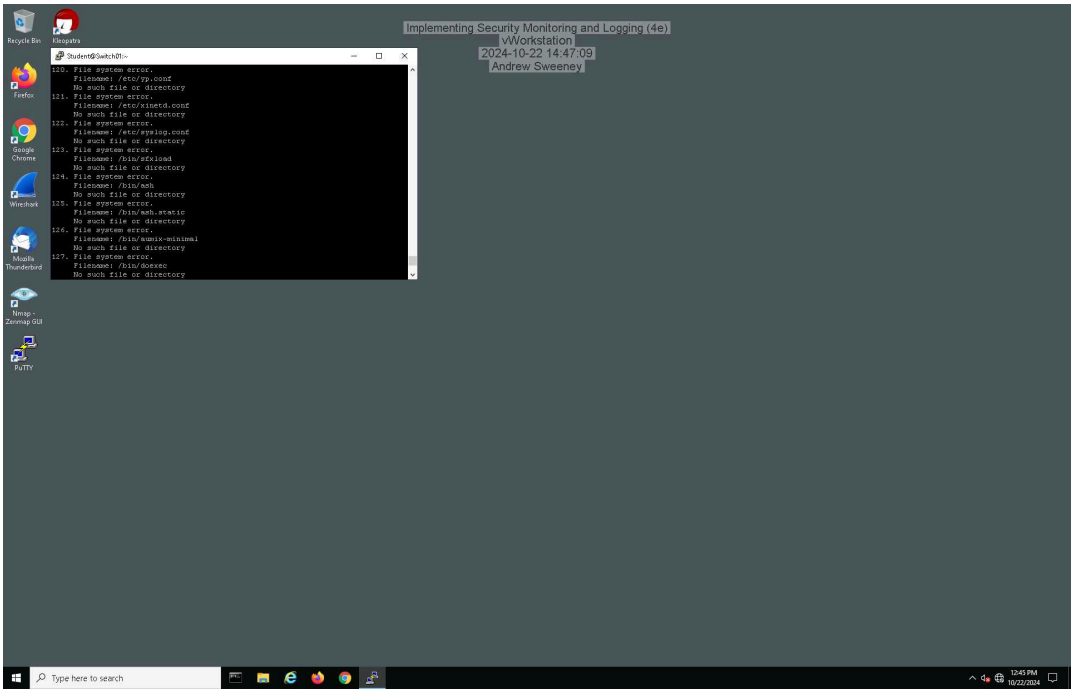


22. **Make a screen capture** showing the **last 10 log messages**.



Part 2: Monitor File Integrity with Tripwire

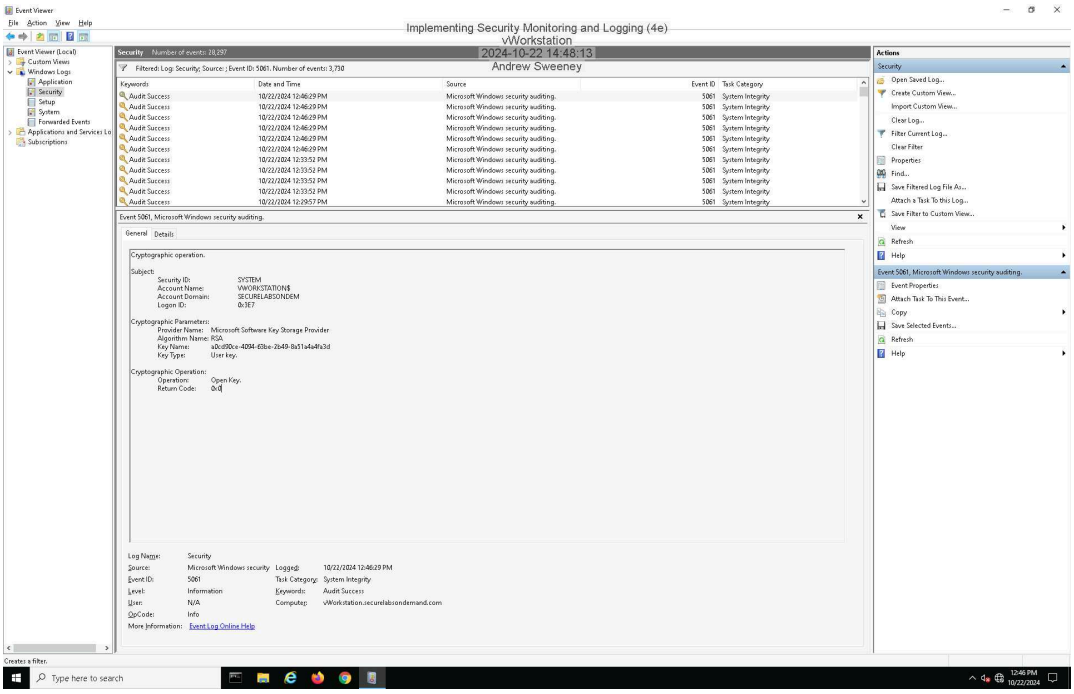
12. **Make a screen capture** showing the **Object Summary section for the Tripwire report**.



Section 3: Challenge and Analysis

Part 1: Identify Additional Event Types in the Event Viewer

Make a screen capture showing the **Security Event Properties dialog box for an Audit Failure associated with Event ID 5061**.



Provide a brief explanation of the operation that would generate a security event with Event ID 5061.

Event ID 5061 in the Windows Event Viewer typically indicates a cryptographic operation failure related to the Windows Cryptographic Next Generation (CNG) Key Isolation service
Corrupted Certificates or Keys: If a certificate or key used by the CNG service is corrupted, missing, or improperly configured, you may see this event.
Permission Issues: The account running the service or performing the operation may not have adequate permissions to access the cryptographic keys.
Service Issues: Problems with the CNG Key Isolation service itself, such as it not starting or crashing, can cause event 5061.

Part 2: Configure Snort as an Intrusion Prevention System

Make a screen capture showing the **Legacy Blocking Mode enabled on the LAN interface**.