Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

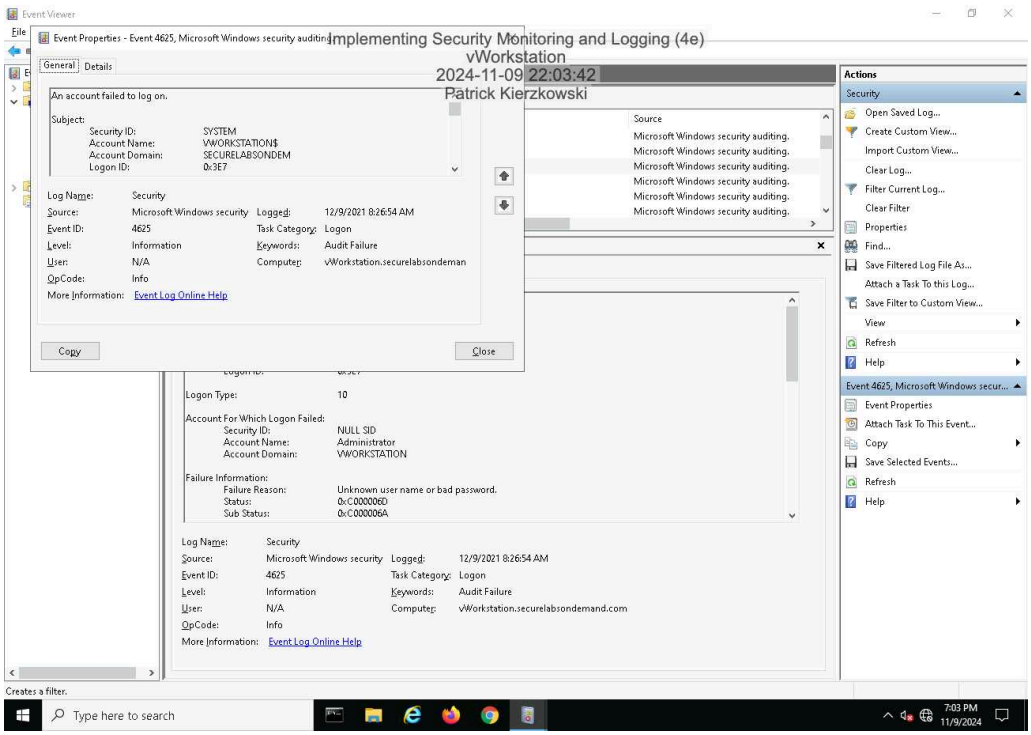
Time on Task:	Progress:
11 hours, 15 minutes	100%

Report Generated: Monday, July 7, 2025 at 9:50 PM

Hands-On Demonstration

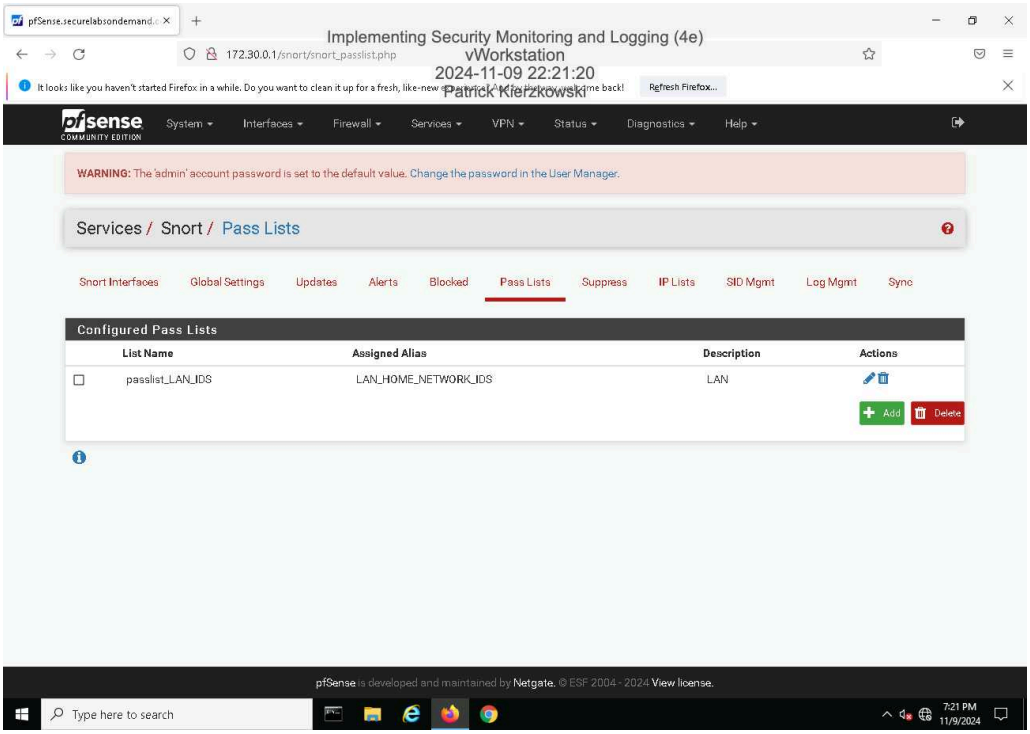
Part 1: Identifying Failed Logon Attempts on Windows Systems

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

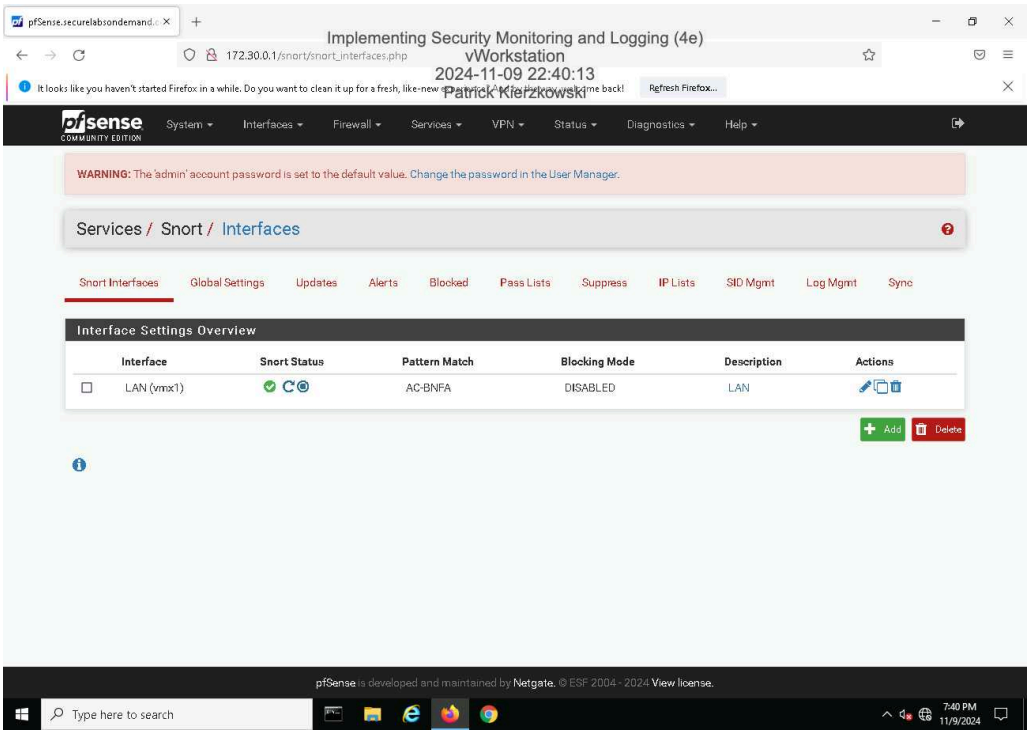


Part 2: Monitoring Network Activity with Snort

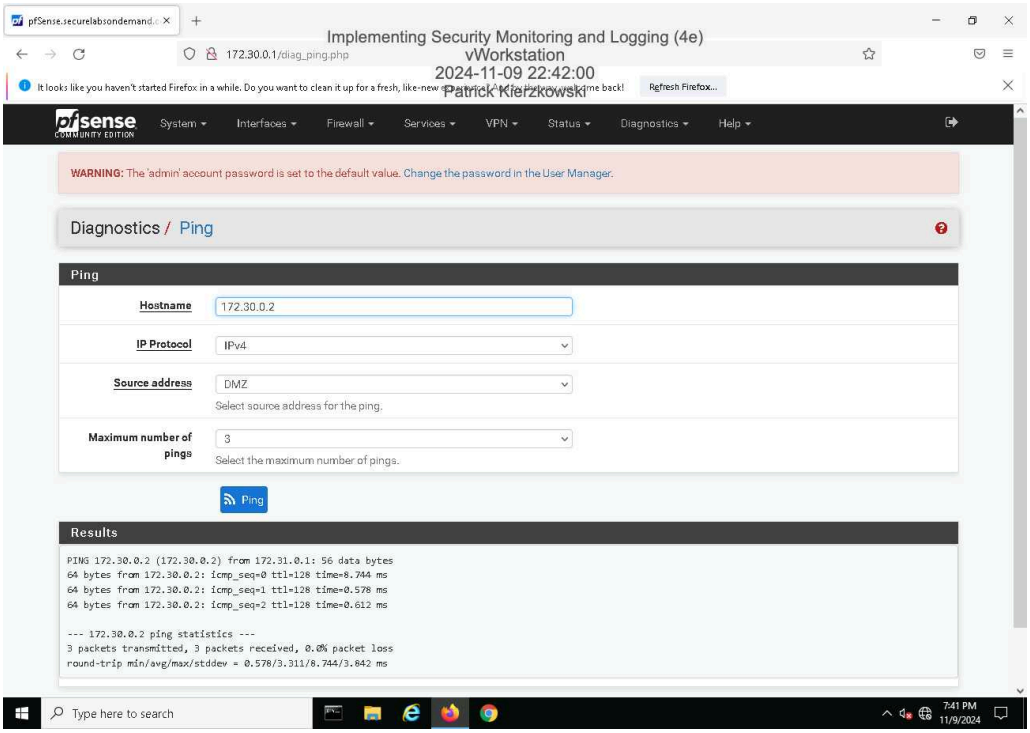
17. **Make a screen capture** showing the **updated Pass Lists page**.



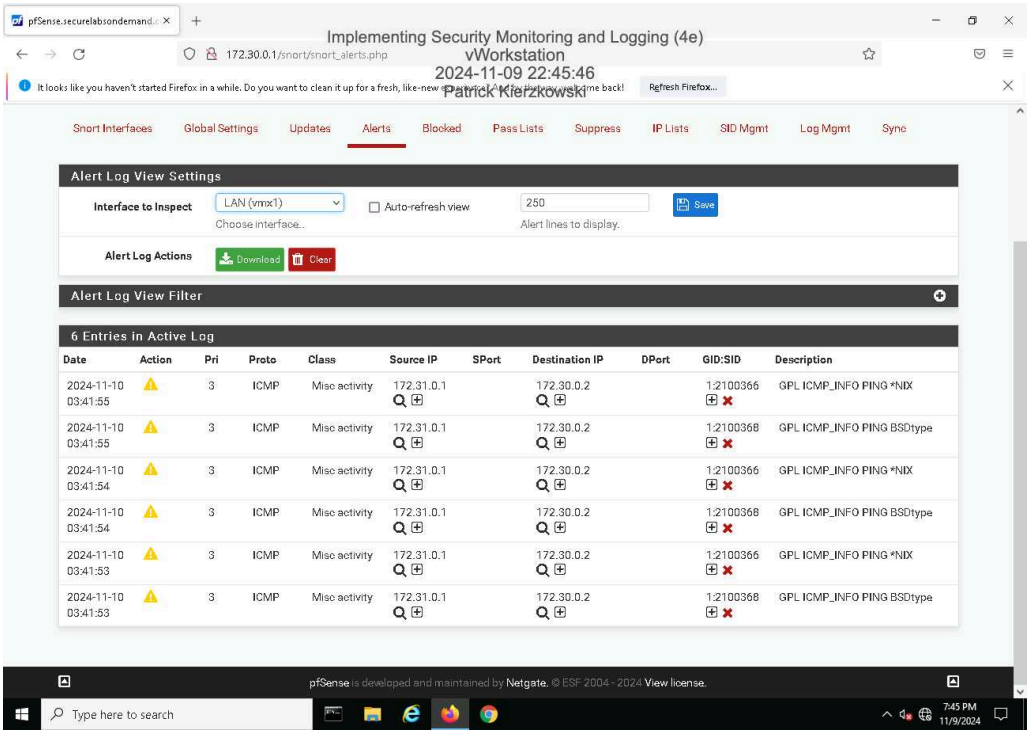
31. **Make a screen capture** showing the **active Snort status on the LAN interface**.



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



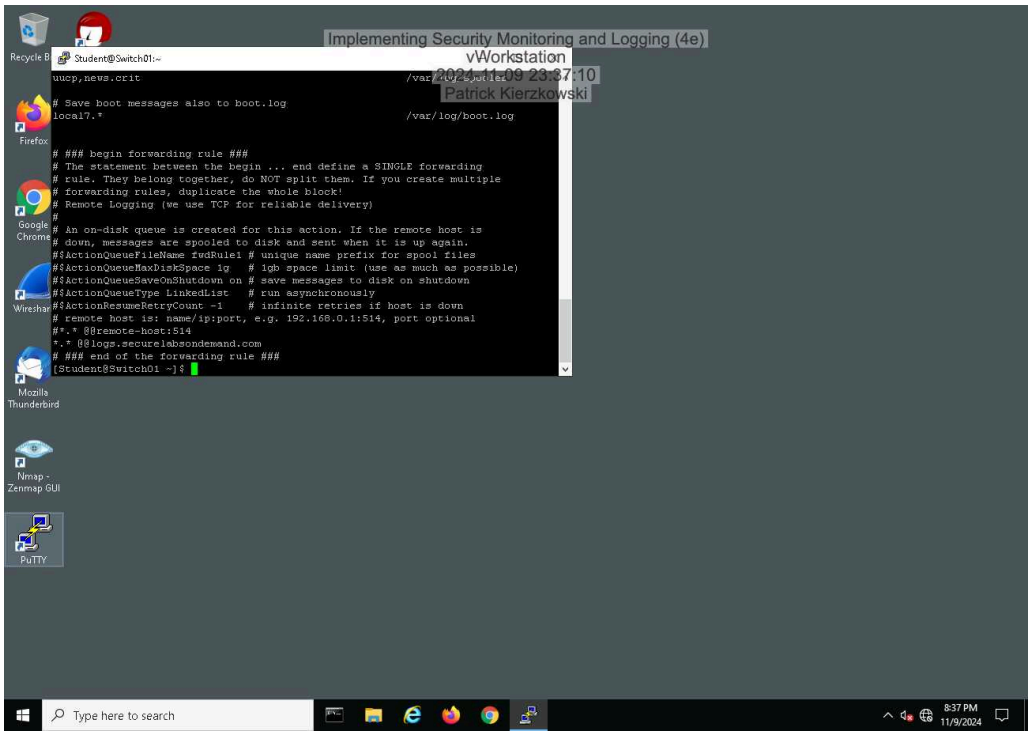
41. **Make a screen capture** showing the **ICMP alerts in the Snort Active Log**.



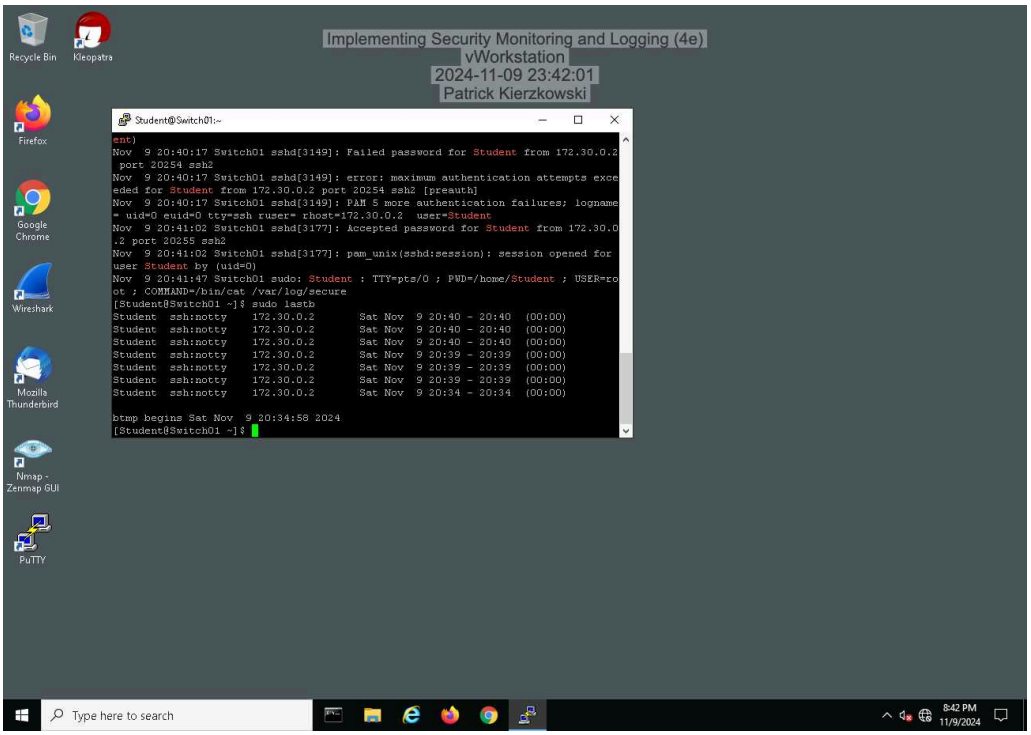
Applied Learning

Part 1: Identifying Failed Logon Attempts on Linux Systems

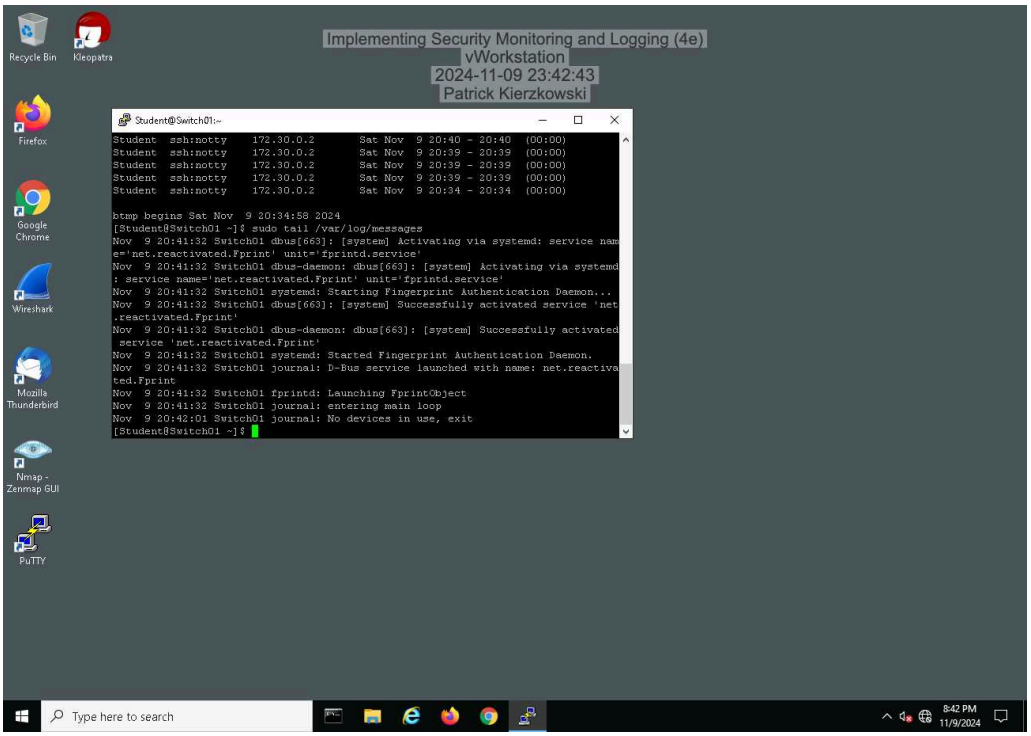
11. **Make a screen capture** showing the **edited rsyslog.conf file**.



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

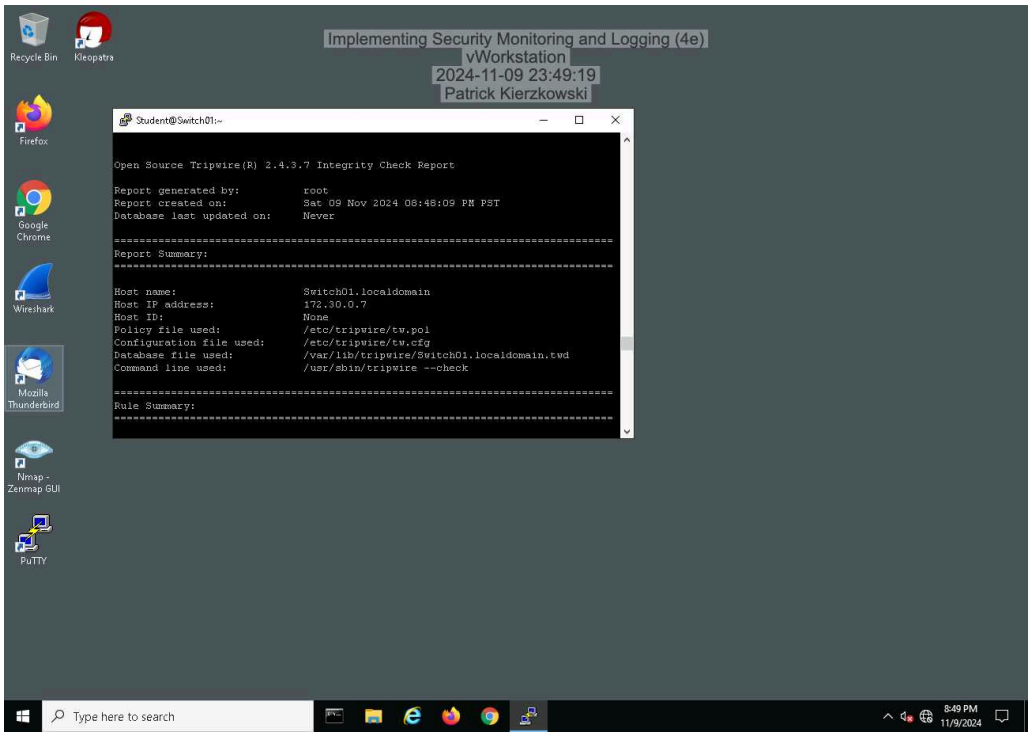


24. **Make a screen capture** showing the **last 10 log messages**.



Part 2: Monitoring File Integrity with Tripwire

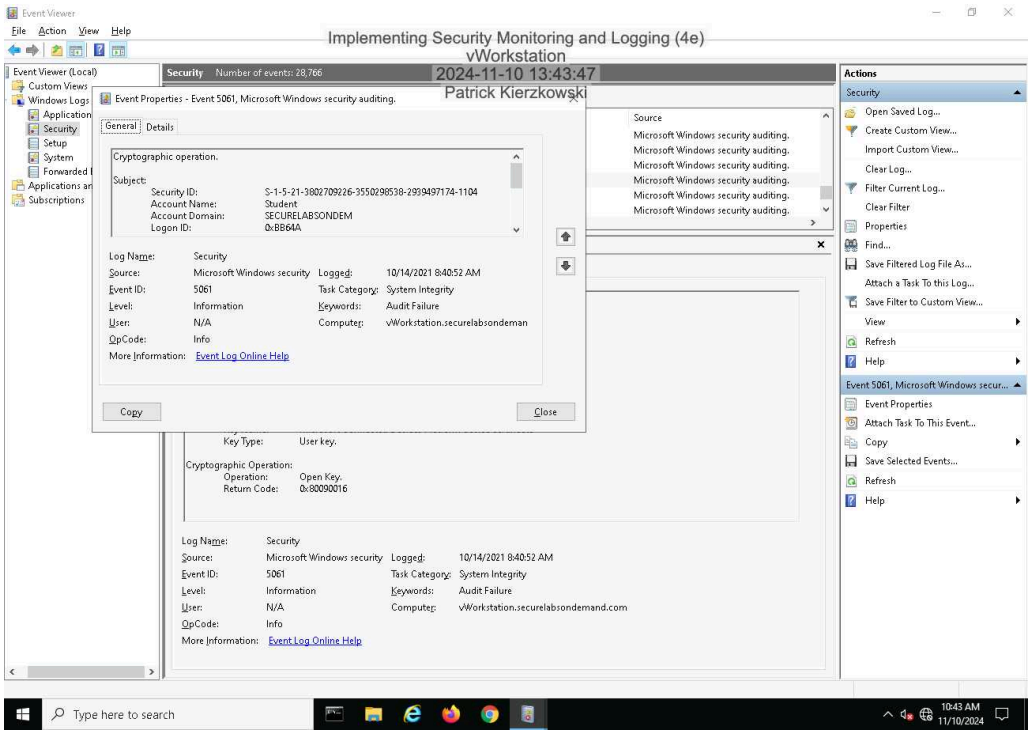
12. **Make a screen capture** showing the **Object Summary section for the Tripwire report**.



Challenge and Analysis

Part 1: Identifying 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.

An operation that would generate a security event with Event 5061 is a cryptographic operation. This means that creating, opening or using a key was performed on a system

Part 2: Configuring Snort as an Intrusion Prevention System

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