Abdullrahman Alghanim

04/23/2025

CIS 3367

Module 14: LAB 11 - Windows Forensics & Logging

Capture the Advanced Audit Policy settings for the Logon/Logoff section.

A screenshot of a computer

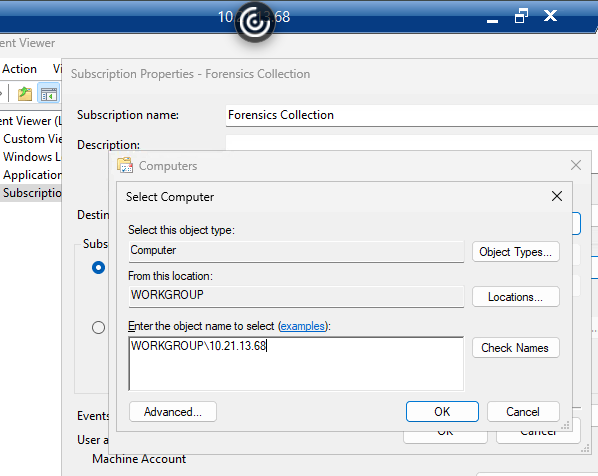
AI-generated content may be incorrect.

Terminal or Command Prompt showing successful gpudate

A screenshot of a computer program

AI-generated content may be incorrect.

The Computers window with the proper IP address added and checked to  
create an audit log subscription.



The completed subscription configuration

A screenshot of a computer

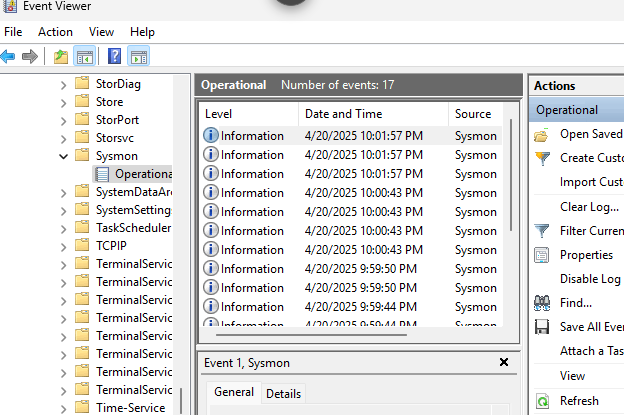
AI-generated content may be incorrect.

Terminal output showing successful Sysmon installation.

A screenshot of a computer program

AI-generated content may be incorrect.

Windows Event Viewer Sysmon logs.



Properties configuration for the System logs with the new settings

A screenshot of a computer

AI-generated content may be incorrect.