

Implementing Security Monitoring and Logging (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 08

Student:
Brandon Trinkle

Email:
btrinkle52@gmail.com

Time on Task:
1 hour, 15 minutes

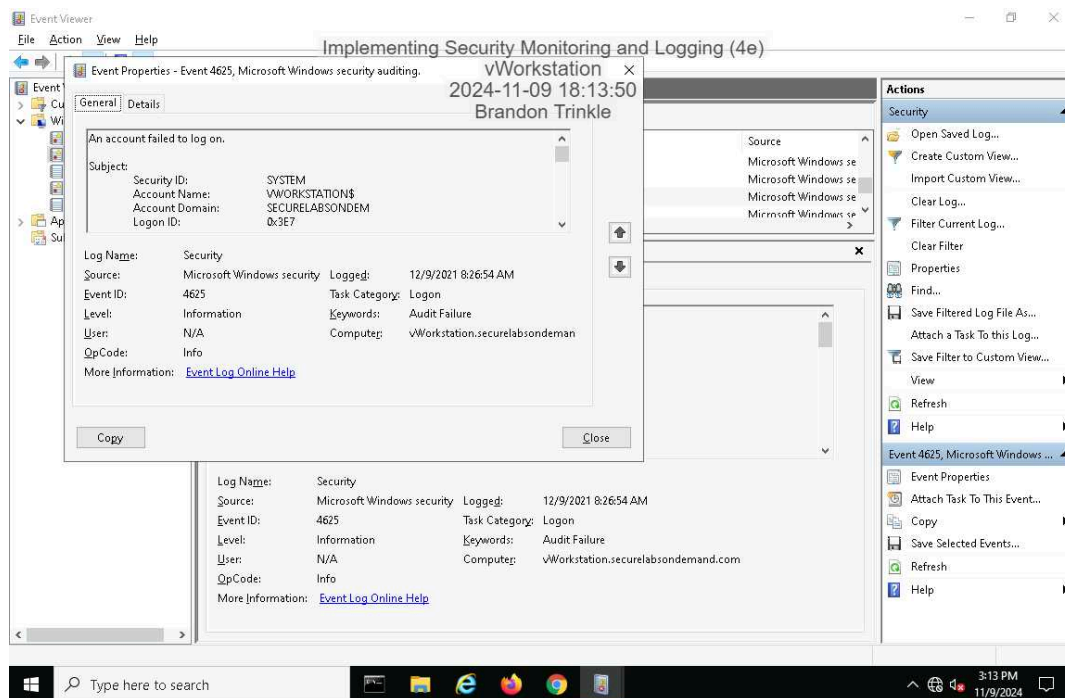
Progress:
100%

Report Generated: Saturday, November 9, 2024 at 7:01 PM

Section 1: Hands-On Demonstration

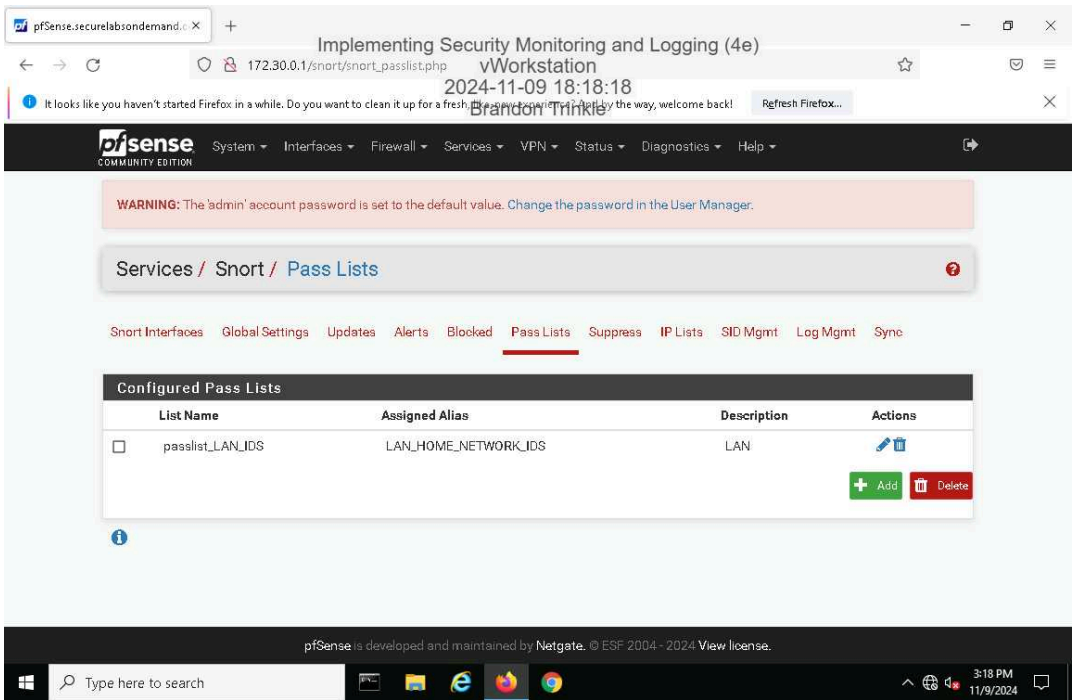
Part 1: Identify Failed Logon Attempts on Windows Systems

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

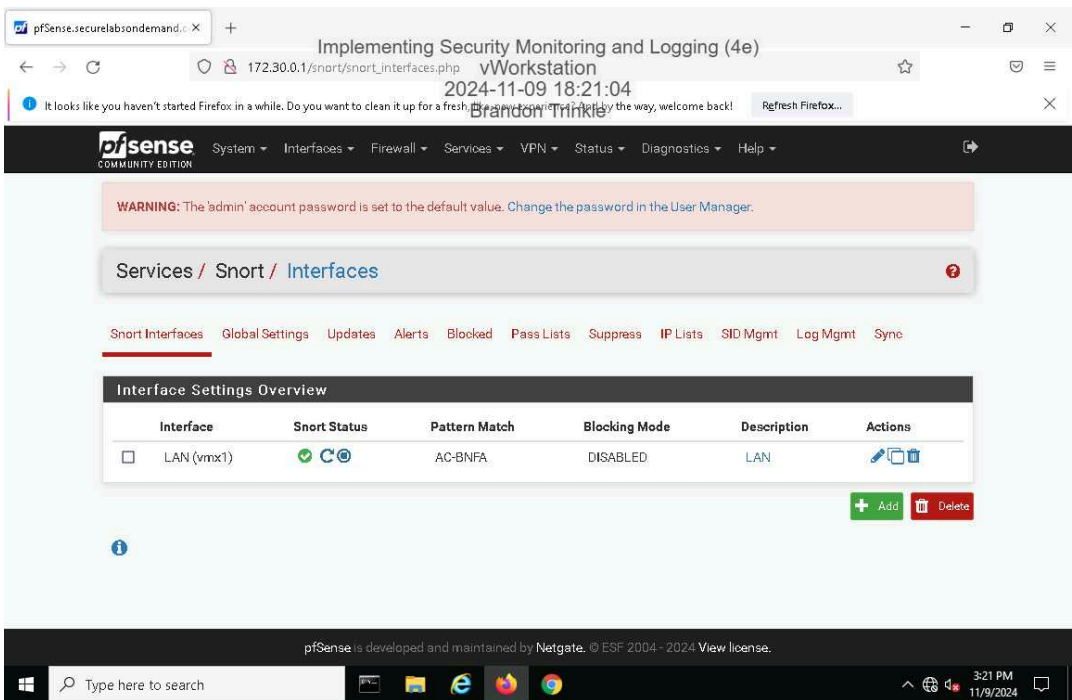


Part 2: Monitor Network Activity with Snort

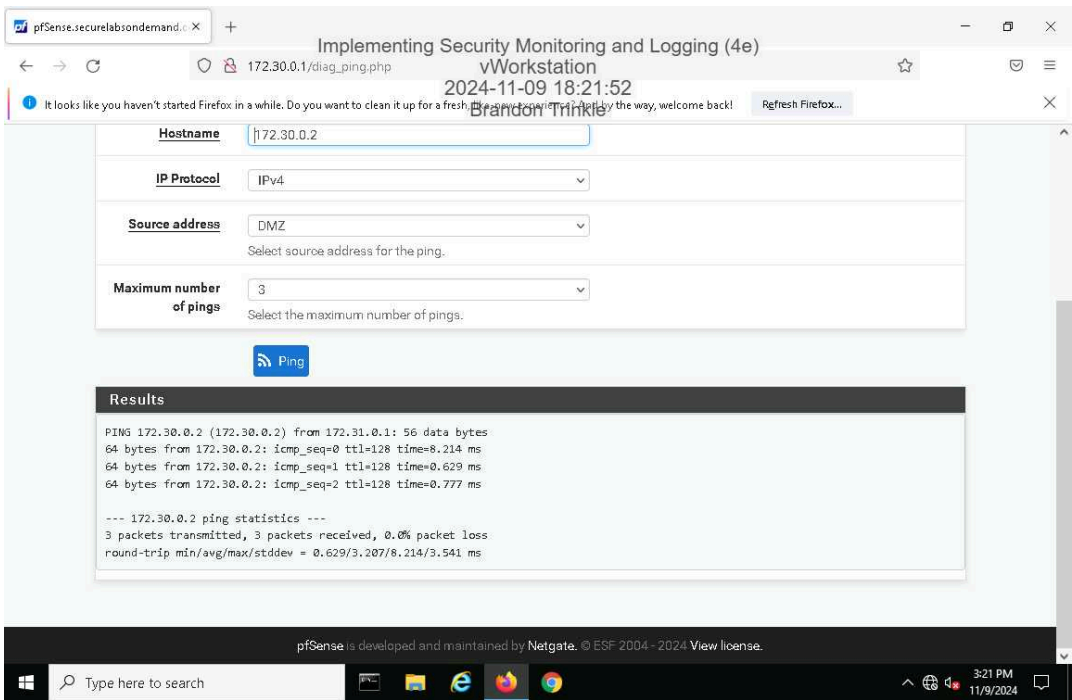
17. Make a screen capture showing the updated Pass Lists page.



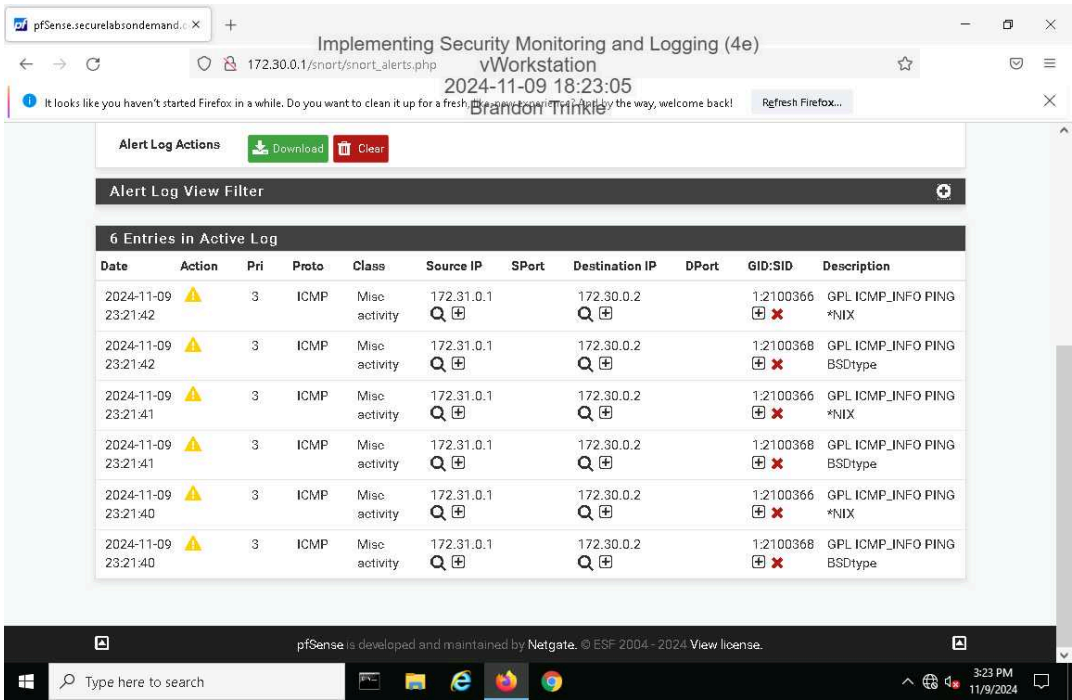
31. Make a screen capture showing the active Snort status on the LAN interface.



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



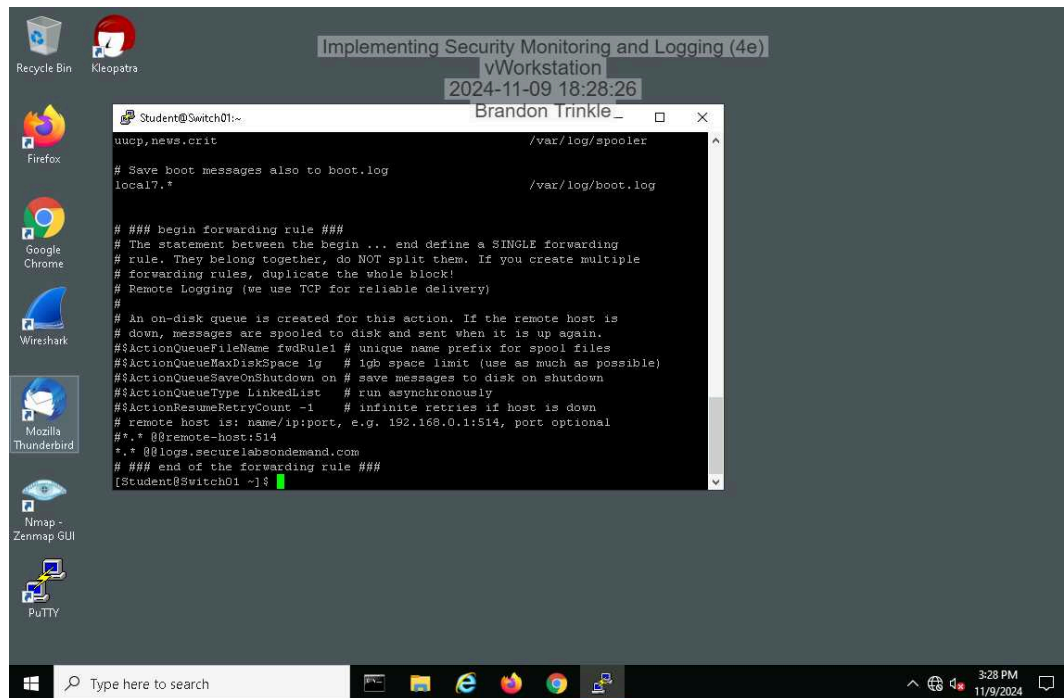
41. Make a screen capture showing the ICMP alerts in the Snort Active Log.



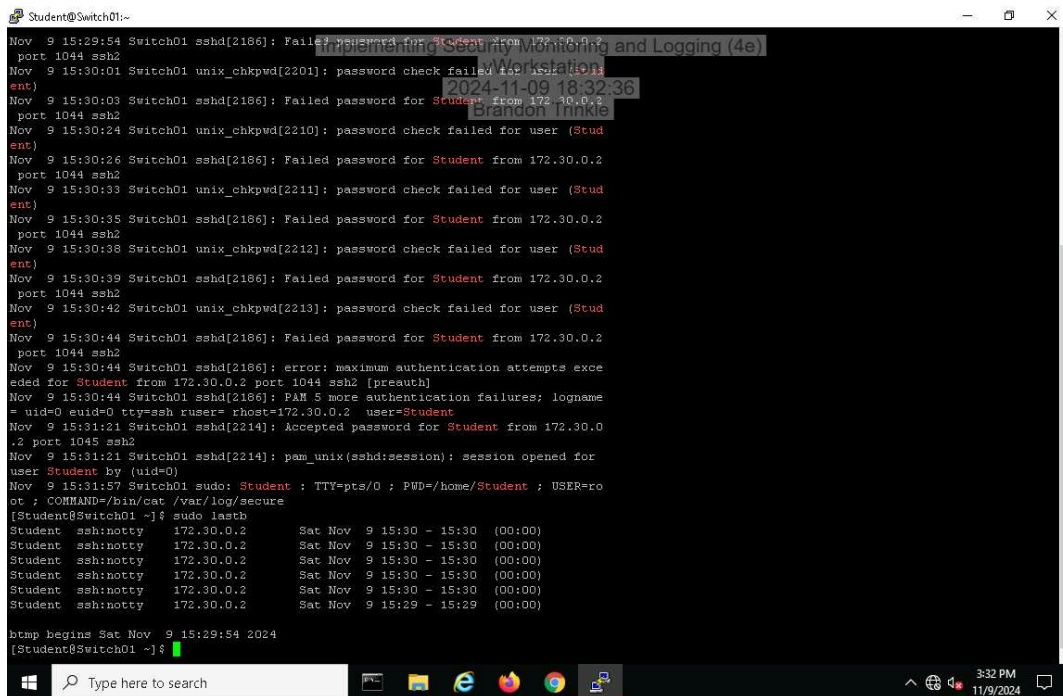
Section 2: Applied Learning

Part 1: Identify Failed Logon Attempts on Linux Systems

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

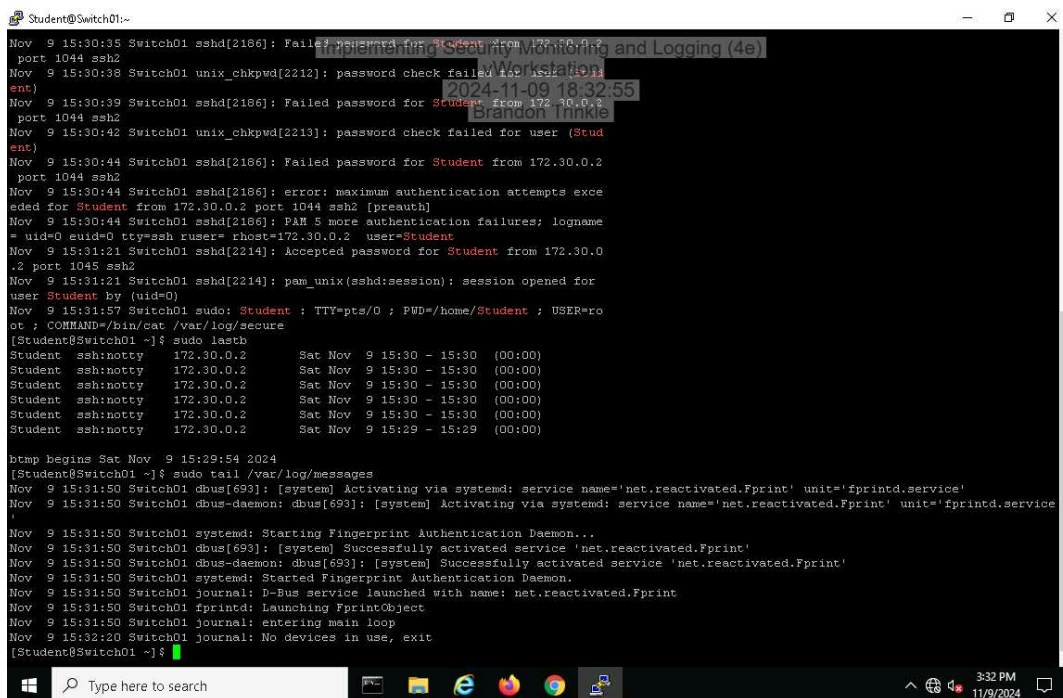


20. Make a screen capture showing the failed login attempts.



```
Student@Switch01:~$  
Nov 9 15:29:54 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:01 Switch01 unix_chkpwd[2201]: password check failed for user 'Student'  
Nov 9 15:30:03 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:24 Switch01 unix_chkpwd[2210]: password check failed for user 'Student'  
Nov 9 15:30:26 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:33 Switch01 unix_chkpwd[2211]: password check failed for user 'Student'  
Nov 9 15:30:35 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:38 Switch01 unix_chkpwd[2212]: password check failed for user 'Student'  
Nov 9 15:30:39 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:42 Switch01 unix_chkpwd[2213]: password check failed for user 'Student'  
Nov 9 15:30:44 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:44 Switch01 sshd[2186]: error: maximum authentication attempts exceeded for 'Student' from 172.30.0.2 port 1044 ssh2 [preauth]  
Nov 9 15:30:44 Switch01 sshd[2186]: PAM 5 more authentication failures; logname='uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2 user=Student'  
Nov 9 15:31:21 Switch01 sshd[2214]: Accepted password for 'Student' from 172.30.0.2 port 1045 ssh2  
Nov 9 15:31:21 Switch01 sshd[2214]: pam_unix(sshd:session): session opened for user 'Student' by (uid=0)  
Nov 9 15:31:57 Switch01 sudo: Student : TTY=pts/0 : PWD=/home/Student : USER=root : COMMAND=/bin/cat /var/log/secure  
[Student@Switch01 ~]$ sudo lastb  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:29 - 15:29 (00:00)  
btmp begins Sat Nov 9 15:29:54 2024  
[Student@Switch01 ~]$
```

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



```
Student@Switch01:~$  
Nov 9 15:30:35 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:38 Switch01 unix_chkpwd[2212]: password check failed for user 'Student'  
Nov 9 15:30:39 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:42 Switch01 unix_chkpwd[2213]: password check failed for user 'Student'  
Nov 9 15:30:44 Switch01 sshd[2186]: Failed password for 'Student' from 172.30.0.2 port 1044 ssh2  
Nov 9 15:30:44 Switch01 sshd[2186]: error: maximum authentication attempts exceeded for 'Student' from 172.30.0.2 port 1044 ssh2 [preauth]  
Nov 9 15:30:44 Switch01 sshd[2186]: PAM 5 more authentication failures; logname='uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2 user=Student'  
Nov 9 15:31:21 Switch01 sshd[2214]: Accepted password for 'Student' from 172.30.0.2 port 1045 ssh2  
Nov 9 15:31:21 Switch01 sshd[2214]: pam_unix(sshd:session): session opened for user 'Student' by (uid=0)  
Nov 9 15:31:57 Switch01 sudo: Student : TTY=pts/0 : PWD=/home/Student : USER=root : COMMAND=/bin/cat /var/log/secure  
[Student@Switch01 ~]$ sudo lastb  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:30 - 15:30 (00:00)  
Student ssh:notty 172.30.0.2 Sat Nov 9 15:29 - 15:29 (00:00)  
btmp begins Sat Nov 9 15:29:54 2024  
[Student@Switch01 ~]$ sudo tail /var/log/messages  
Nov 9 15:31:50 Switch01 dbus-daemon[693]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service'  
Nov 9 15:31:50 Switch01 dbus-daemon[693]: [system] Successfully activated service 'net.reactivated.Fprint'  
Nov 9 15:31:50 Switch01 systemd: Starting Fingerprint Authentication Daemon...  
Nov 9 15:31:50 Switch01 dbus-daemon[693]: [system] Successfully activated service 'net.reactivated.Fprint'  
Nov 9 15:31:50 Switch01 systemd: Started Fingerprint Authentication Daemon.  
Nov 9 15:31:50 Switch01 journal: D-Bus service launched with name: net.reactivated.Fprint  
Nov 9 15:31:50 Switch01 fprintd: Launching FprintObject  
Nov 9 15:31:50 Switch01 journal: entering main loop  
Nov 9 15:32:20 Switch01 journal: No devices in use, exit  
[Student@Switch01 ~]$
```

Part 2: Monitor File Integrity with Tripwire

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

```
Student@Switch01:~$ tripwire --check
=====
Report Summary:
=====
Host name:                Switch01.localdomain
Host IP address:          172.30.0.7
Host ID:                  None
Policy file used:         /etc/tripwire/tw.pol
Configuration file used:  /etc/tripwire/tw.cfg
Database file used:       /var/lib/tripwire/Switch01.localdomain.twd
Command line used:        /usr/sbin/tripwire --check
=====

Rule Summary:
=====

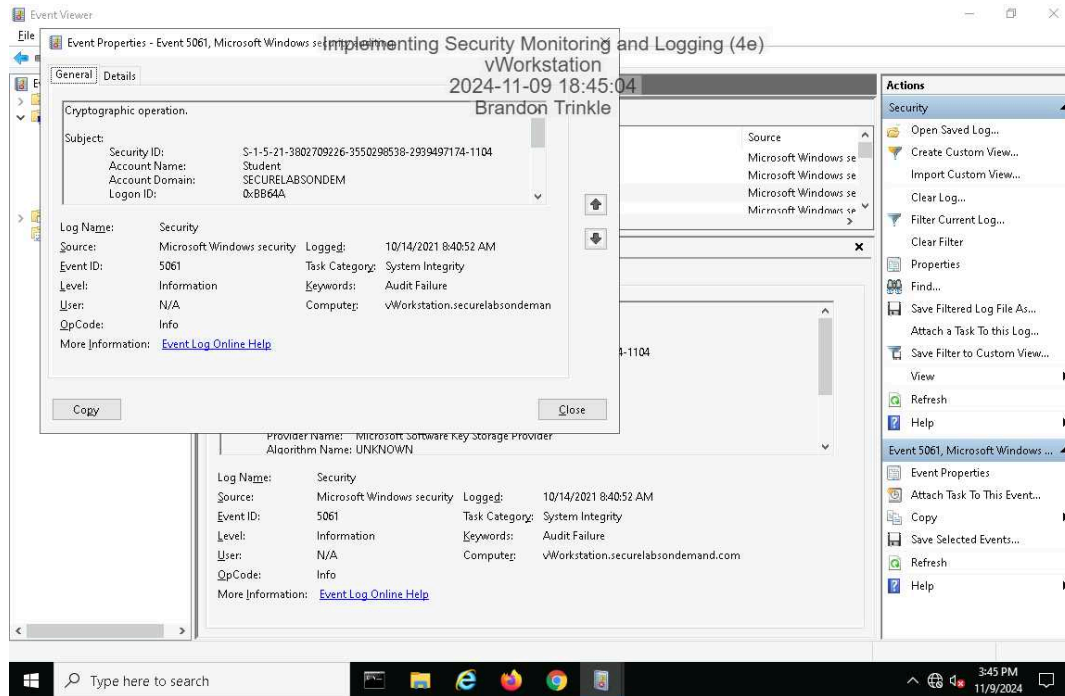
Section: Unix File System
=====

Rule Name                  Severity Level  Added  Removed  Modified
-----
* User Binaries             66             0      0        1
Tripwire Binaries          100            0      0        0
Critical configuration files 100            0      0        0
Libraries                   66             0      0        0
* Operating System Utilities 100            0      0        1
Critical system boot files  100            0      0        0
File System and Disk Administration Programs
100                      0      0        0
Kernel Administration Programs 100          0      0        0
Networking Programs        100           0      0        0
System Administration Programs 100          0      0        0
Hardware and Device Control Programs
100                      0      0        0
System Information Programs 100           0      0        0
Application Information Programs
100                      0      0        0
Shell Related Programs      100           0      0        0
Critical Utility Sym-Links   100           0      0        0
Shell Binaries              100           0      0        0
* Tripwire Data Files        100           1      0        0
```


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.

The presence of Event ID 5061 in the Windows Event Viewer indicates that a cryptographic operation failed on the company workstation. This event, logged under the Security category, is associated with Microsoft Windows security auditing and is classified under the System Integrity task category. Specifically, the entry shows that the Microsoft Software Key Storage Provider was involved, yet the cryptographic algorithm used is labeled as "UNKNOWN."

The audit failure reflected in this log suggests that there was an attempt to access or perform operations using a cryptographic key managed by the Key Storage Provider, but the operation did not complete successfully. This could happen for several reasons, such as insufficient permissions assigned to the user account attempting the cryptographic operation, a misconfiguration in the Key Storage Provider, or possibly the absence or corruption of the necessary cryptographic key or certificate.

Given that the event details do not specify a particular cryptographic algorithm, it implies that the system could not recognize or access the required algorithm, which further indicates a possible issue with the system's cryptographic configuration. It is also possible that the cryptographic service on this workstation may not be functioning correctly, thereby preventing successful operations.

In summary, this error log highlights a failure in the system's ability to carry out a secure cryptographic operation, potentially impacting any applications or services that rely on secure key storage and cryptographic functions. Further investigation into the permissions assigned to the involved user account, as well as the health of the cryptographic service and key storage configuration, would be necessary to resolve this issue and prevent similar audit failures in the future.

Part 2: Configure Snort as an Intrusion Prevention System

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

