Implementing Security Monitoring and Logging (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 08

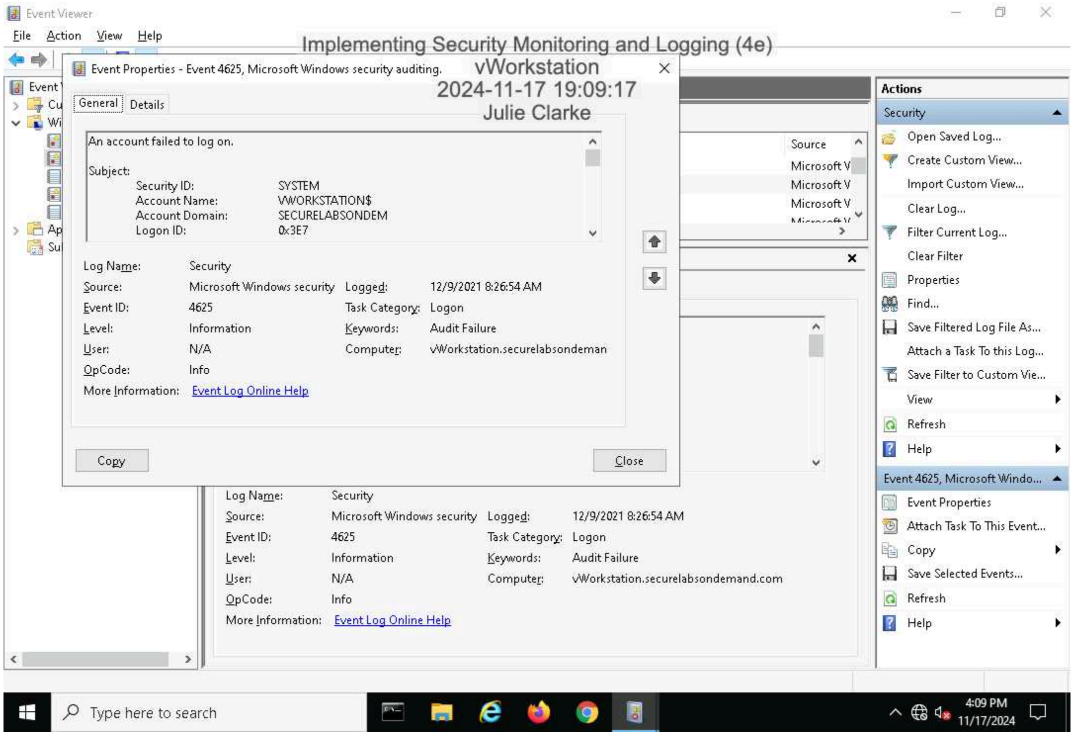
Student: Julie Clarke	Email: clarke323@usf.edu
Time on Task: 1 hour, 43 minutes	Progress: 100%

Report Generated: Sunday, November 17, 2024 at 8:27 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**.



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-17 19:09:17
Julie Clarke

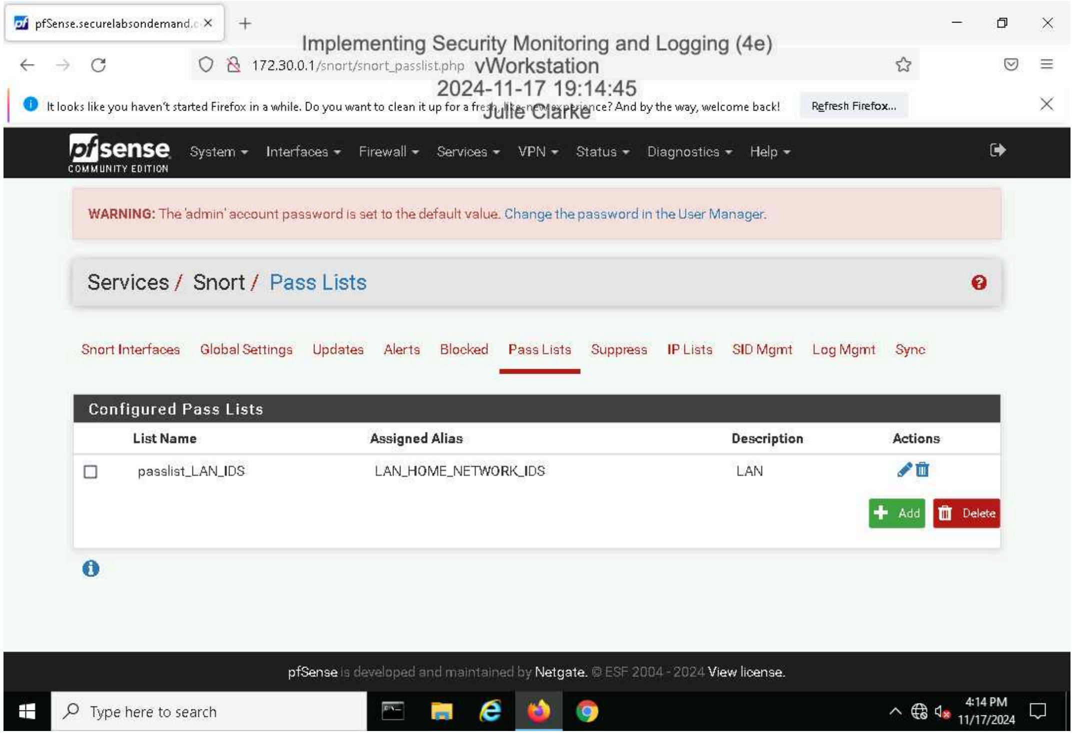
Event Properties - Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:        SYSTEM
        Account Name:       VWORKSTATION$
        Account Domain:     SECURELABSONDEM
        Logon ID:           0x3E7

Log Name:          Security
Source:            Microsoft Windows security   Logged:          12/9/2021 8:26:54 AM
Event ID:          4625                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        vWorkstation.securelabsondeman
OpCode:            Info
More Information:  Event Log Online Help
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          12/9/2021 8:26:54 AM
Event ID:          4625                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        vWorkstation.securelabsondemand.com
OpCode:            Info
More Information:  Event Log Online Help
```

Part 2: Monitor Network Activity with Snort

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



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-17 19:14:45
Julie Clarke

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Pass Lists

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

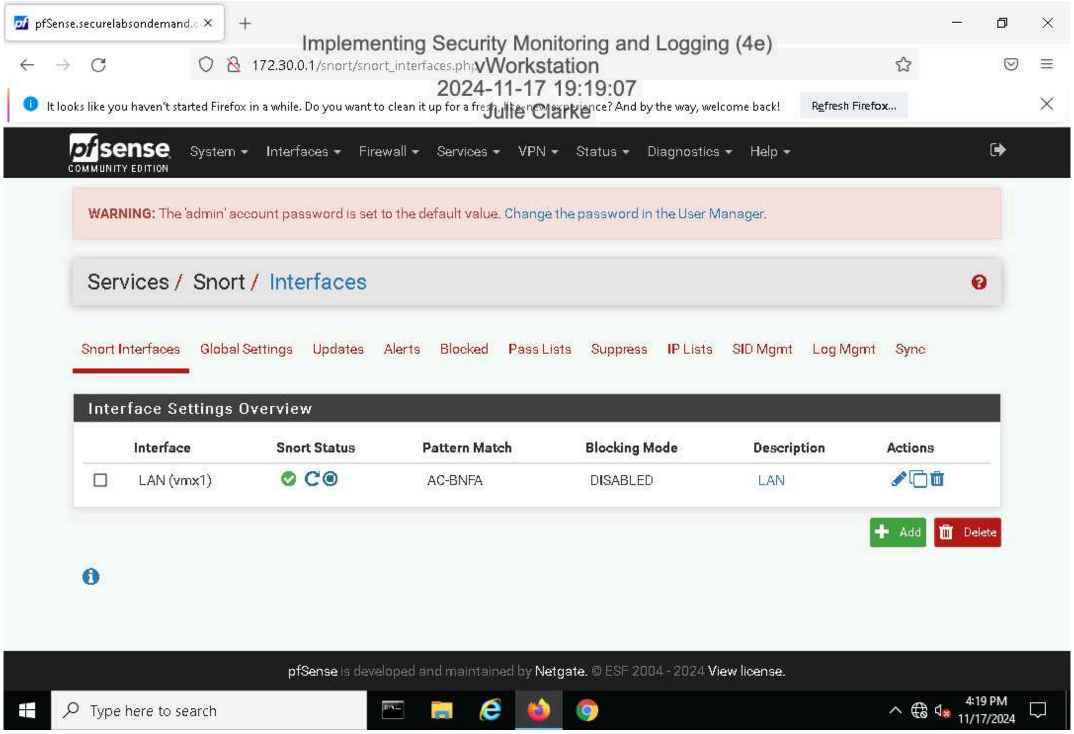
Configured Pass Lists

	List Name	Assigned Alias	Description	Actions
□	passlist_LAN_IDS	LAN_HOME_NETWORK_IDS	LAN	

Add | Delete

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-17 19:19:07
Julie Clarke

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Interfaces

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

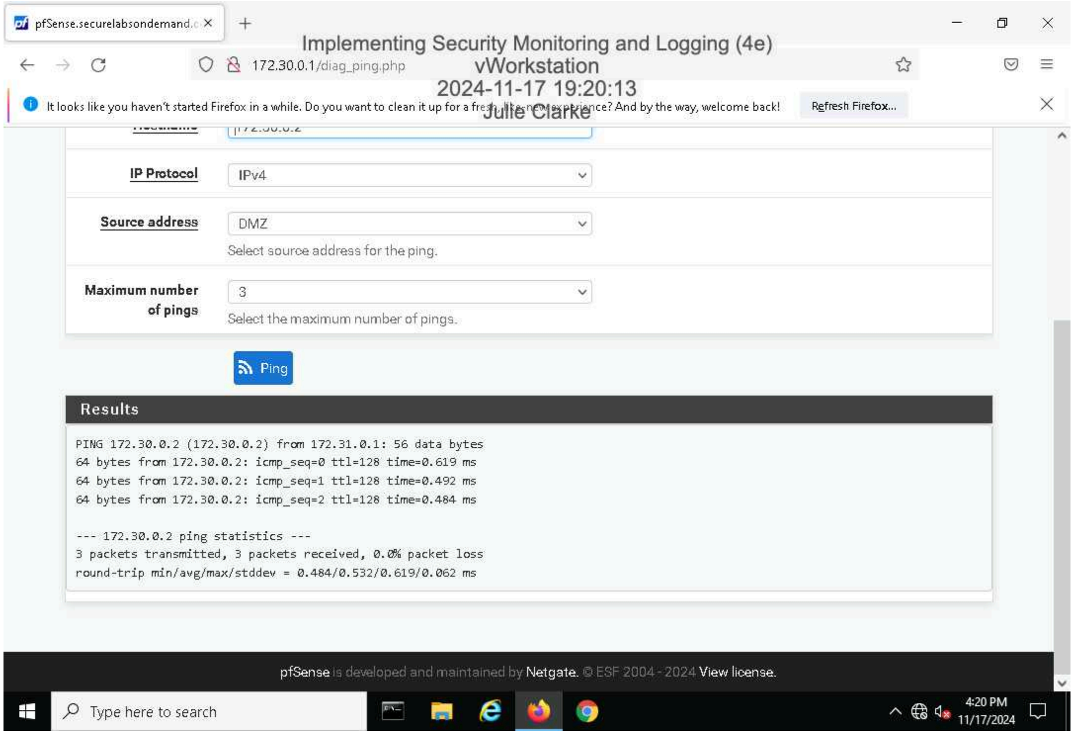
Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	LAN (vmx1)	✓	AC-BNFA	DISABLED	LAN	

Add | Delete

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



pfSense.securelabsondemand.c
172.30.0.1/diag_ping.php
Refresh Firefox...
Ping
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Type here to search
4:20 PM
11/17/2024

Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-17 19:20:13
Julie Clarke

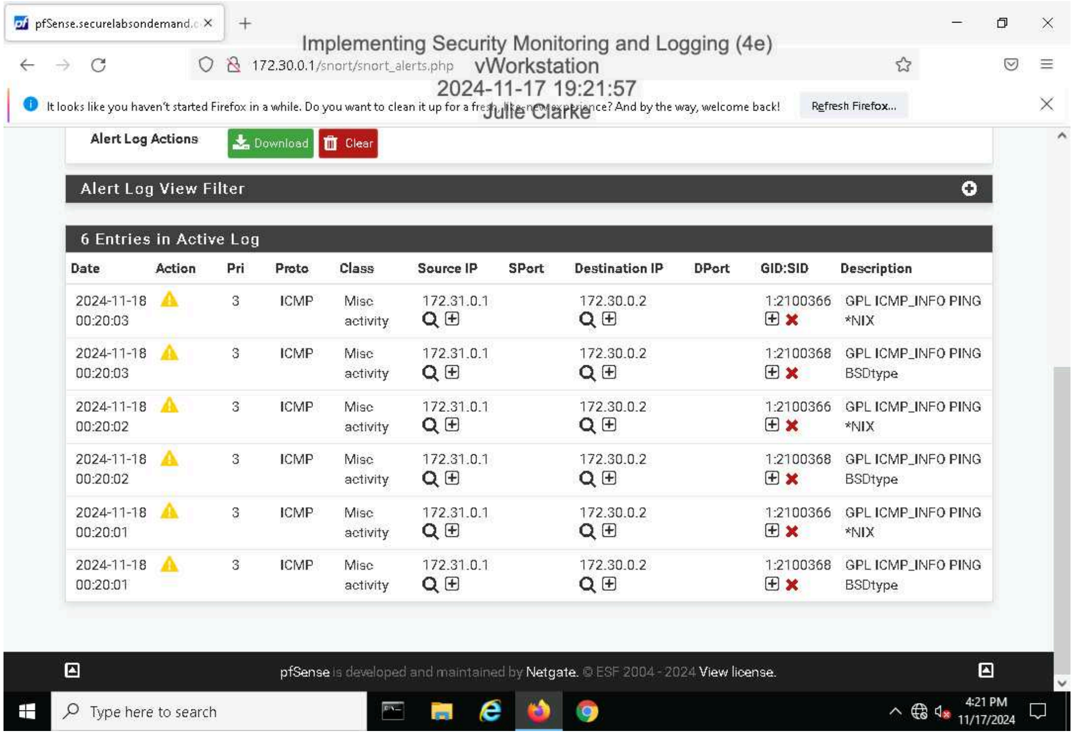
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

IP Protocol	IPv4
Source address	DMZ Select source address for the ping.
Maximum number of pings	3 Select the maximum number of pings.

Results

```
PING 172.30.0.2 (172.30.0.2) from 172.31.0.1: 56 data bytes
64 bytes from 172.30.0.2: icmp_seq=0 ttl=128 time=0.619 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.492 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.484 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.484/0.532/0.619/0.062 ms
```

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



pfSense.securelabsondemand.c
172.30.0.1/snort/snort_alerts.php
Refresh Firefox...
Alert Log Actions
Download
Clear
Alert Log View Filter
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Type here to search
4:21 PM
11/17/2024

Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-17 19:21:57
Julie Clarke

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

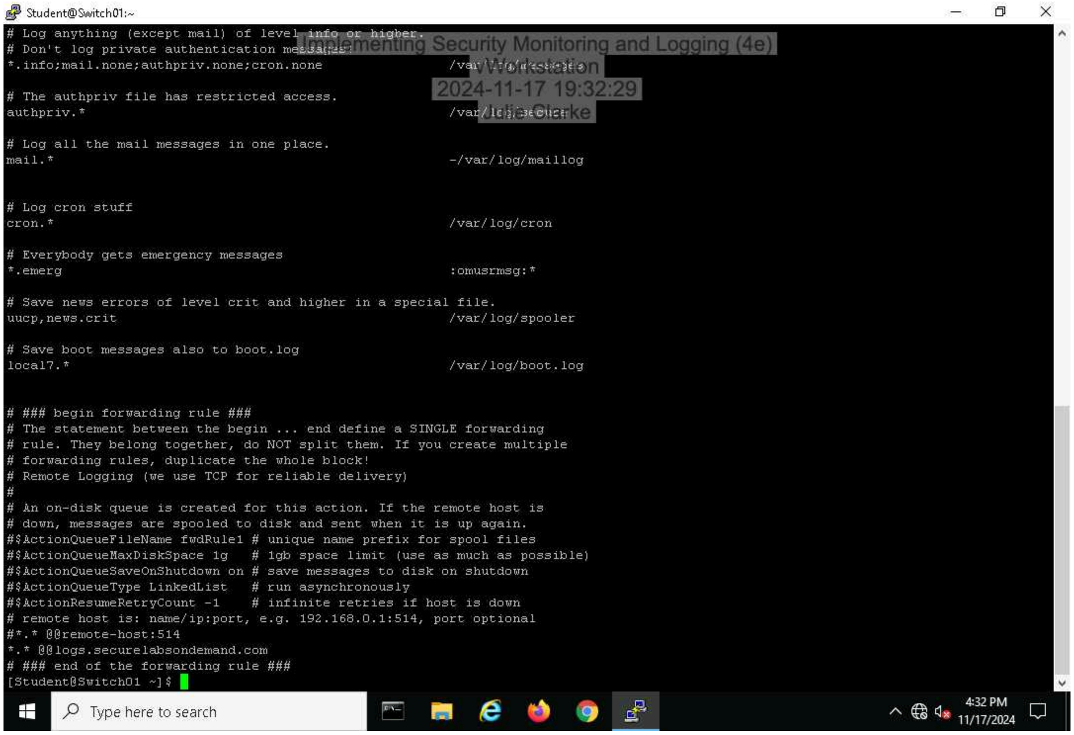
6 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-18 00:20:03	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-11-18 00:20:03	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2024-11-18 00:20:02	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-11-18 00:20:02	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2024-11-18 00:20:01	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-11-18 00:20:01	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype

Section 2: Applied Learning

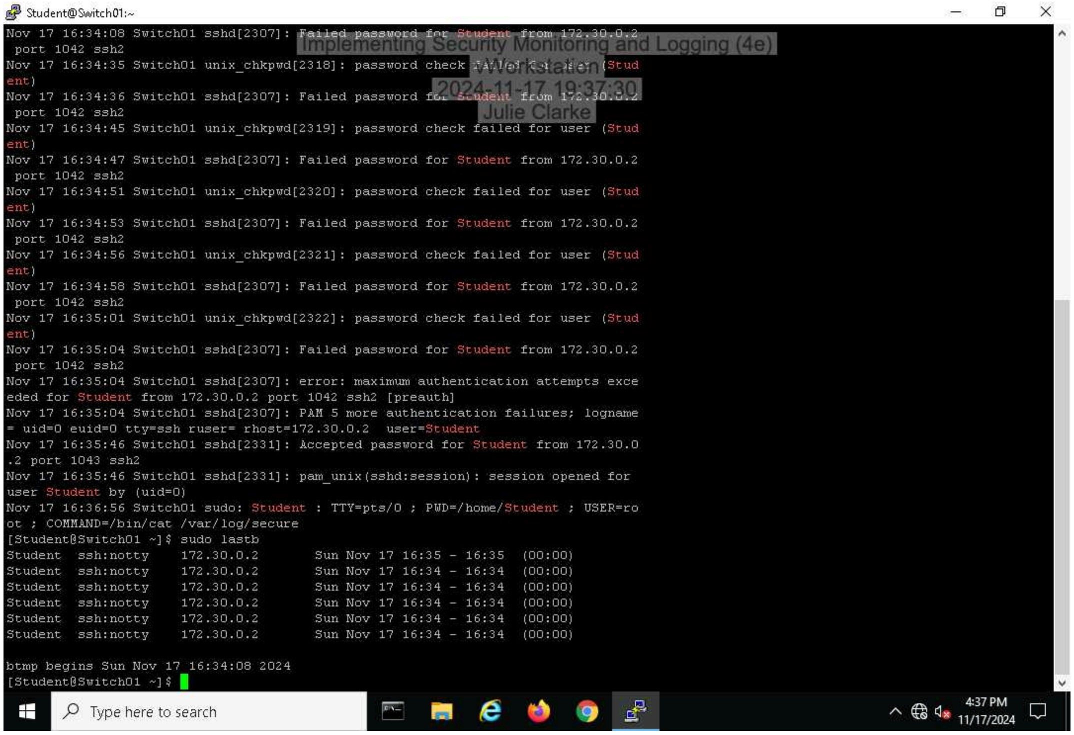
Part 1: Identify Failed Logon Attempts on Linux Systems

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



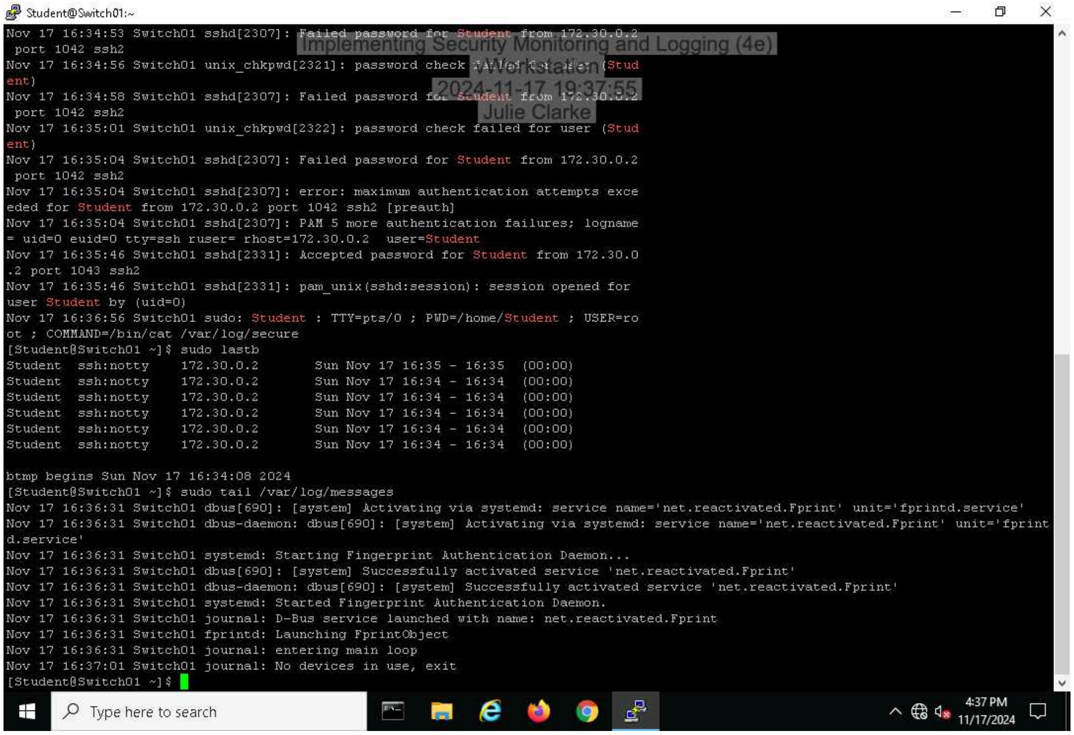
```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog


# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log


# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
*.* @@logs.securelabsondemand.com
# ### end of the forwarding rule ###
[Student@Switch01 ~]$
```

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



```
Nov 17 16:34:08 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:34:35 Switch01 unix_chkpwd[2318]: password check failed for user (Stud
ent)
Nov 17 16:34:36 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:34:45 Switch01 unix_chkpwd[2319]: password check failed for user (Stud
ent)
Nov 17 16:34:47 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:34:51 Switch01 unix_chkpwd[2320]: password check failed for user (Stud
ent)
Nov 17 16:34:53 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:34:56 Switch01 unix_chkpwd[2321]: password check failed for user (Stud
ent)
Nov 17 16:34:58 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:35:01 Switch01 unix_chkpwd[2322]: password check failed for user (Stud
ent)
Nov 17 16:35:04 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:35:04 Switch01 sshd[2307]: error: maximum authentication attempts exce
eded for Student from 172.30.0.2 port 1042 ssh2 [preauth]
Nov 17 16:35:04 Switch01 sshd[2307]: PAM 5 more authentication failures; logname
= uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2  user=Student
Nov 17 16:35:46 Switch01 sshd[2331]: Accepted password for Student from 172.30.0
.2 port 1043 ssh2
Nov 17 16:35:46 Switch01 sshd[2331]: pam_unix(sshd:session): session opened for
user Student by (uid=0)
Nov 17 16:36:56 Switch01 sudo: Student : TTY=pts/0 ; PWD=/home/Student ; USER=ro
ot ; COMMAND=/bin/cat /var/log/secure
[Student@Switch01 ~]$ sudo lastb
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:35 - 16:35  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)

btmp begins Sun Nov 17 16:34:08 2024
[Student@Switch01 ~]$
```

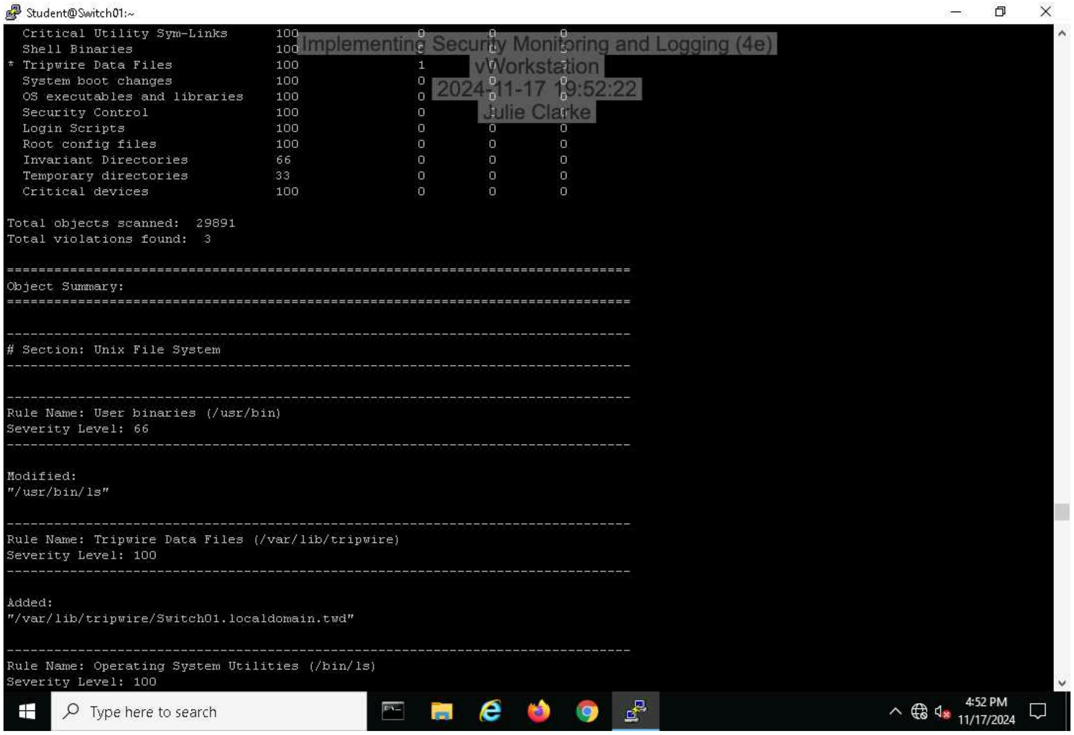
22. **Make a screen capture** showing the **last 10 log messages**.



```
Nov 17 16:34:53 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:34:56 Switch01 unix_chkpwd[2321]: password check failed for user (Stud
ent)
Nov 17 16:34:58 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:35:01 Switch01 unix_chkpwd[2322]: password check failed for user (Stud
ent)
Nov 17 16:35:04 Switch01 sshd[2307]: Failed password for Student from 172.30.0.2
 port 1042 ssh2
Nov 17 16:35:04 Switch01 sshd[2307]: error: maximum authentication attempts exce
eded for Student from 172.30.0.2 port 1042 ssh2 [preauth]
Nov 17 16:35:04 Switch01 sshd[2307]: PAM 5 more authentication failures; logname
= uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2  user=Student
Nov 17 16:35:46 Switch01 sshd[2331]: Accepted password for Student from 172.30.0
.2 port 1043 ssh2
Nov 17 16:35:46 Switch01 sshd[2331]: pam_unix(sshd:session): session opened for
user Student by (uid=0)
Nov 17 16:36:56 Switch01 sudo: Student : TTY=pts/0 ; PWD=/home/Student ; USER=ro
ot ; COMMAND=/bin/cat /var/log/secure
[Student@Switch01 ~]$ sudo lastb
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:35 - 16:35  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)
Student  ssh:notty    172.30.0.2       Sun Nov 17 16:34 - 16:34  (00:00)

btmp begins Sun Nov 17 16:34:08 2024
[Student@Switch01 ~]$ sudo tail /var/log/messages
Nov 17 16:36:31 Switch01 dbus[690]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service'
Nov 17 16:36:31 Switch01 dbus-daemon: dbus[690]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprint
d.service'
Nov 17 16:36:31 Switch01 systemd: Starting Fingerprint Authentication Daemon...
Nov 17 16:36:31 Switch01 dbus[690]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 17 16:36:31 Switch01 dbus-daemon: dbus[690]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 17 16:36:31 Switch01 systemd: Started Fingerprint Authentication Daemon.
Nov 17 16:36:31 Switch01 journal: D-Bus service launched with name: net.reactivated.Fprint
Nov 17 16:36:31 Switch01 fprintd: Launching FprintObject
Nov 17 16:36:31 Switch01 journal: entering main loop
Nov 17 16:37:01 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**.

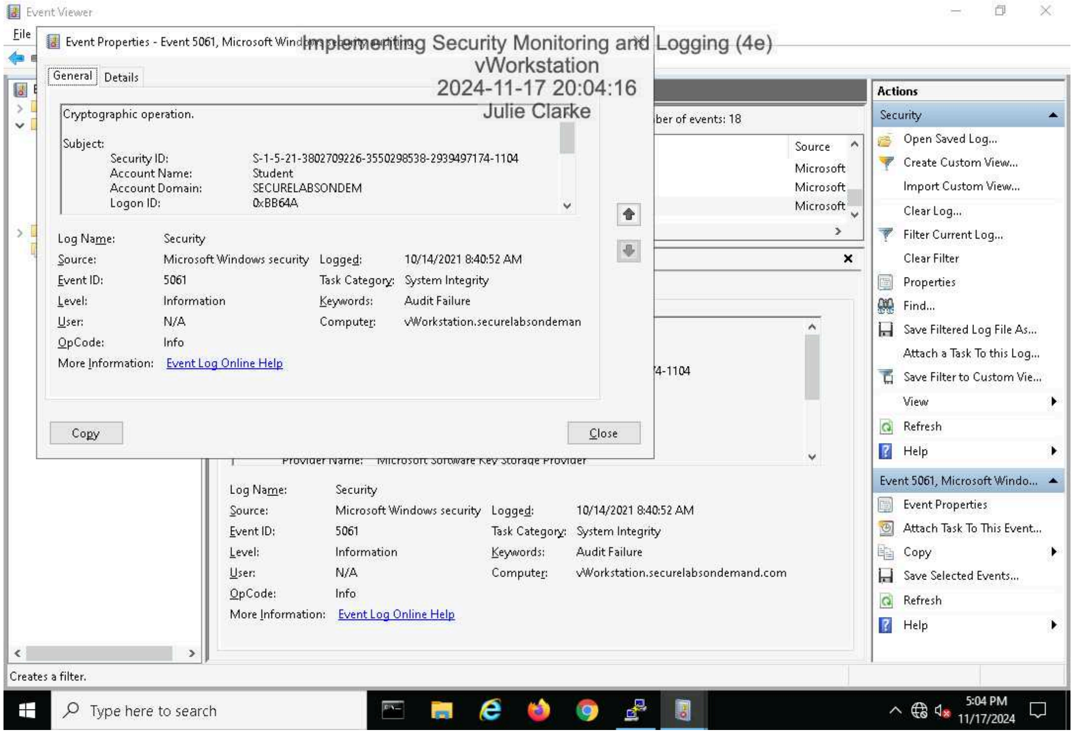


```
  Critical Utility Sym-Links      100              0        0        0
  Shell Binaries                  100              0        0        0
* Tripwire Data Files             100              1        0        0
  System boot changes             100              0        0        0
  OS executables and libraries    100              0        0        0
  Security Control                100              0        0        0
  Login Scripts                   100              0        0        0
  Root config files               100              0        0        0
  Invariant Directories           66               0        0        0
  Temporary directories           33               0        0        0
  Critical devices                100              0        0        0

Total objects scanned:  29891
Total violations found:  3

===============================================================================
Object Summary:
===============================================================================

-------------------------------------------------------------------------------
# Section: Unix File System
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Rule Name: User binaries (/usr/bin)
Severity Level: 66
-------------------------------------------------------------------------------

Modified:
"/usr/bin/ls"

-------------------------------------------------------------------------------
Rule Name: Tripwire Data Files (/var/lib/tripwire)
Severity Level: 100
-------------------------------------------------------------------------------

Added:
"/var/lib/tripwire/Switch01.localdomain.twd"

-------------------------------------------------------------------------------
Rule Name: Operating System Utilities (/bin/ls)
Severity Level: 100
```

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**.



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-17 20:04:16
Julie Clarke

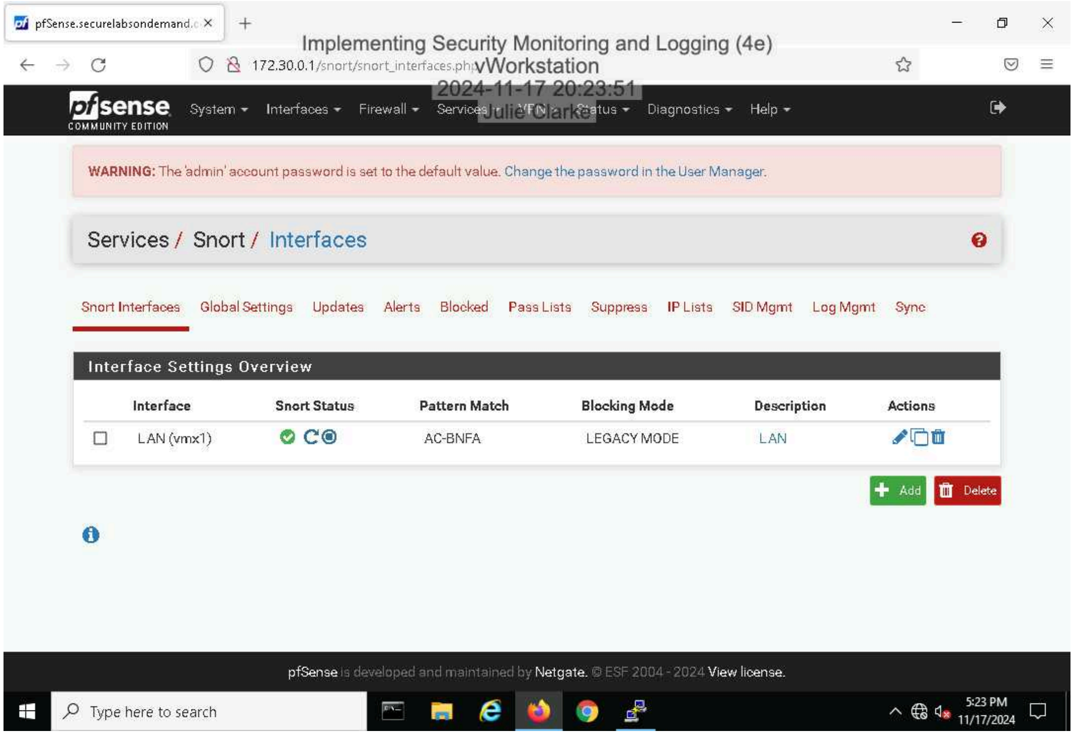
```
Cryptographic operation.

Subject:
        Security ID:        S-1-5-21-3802709226-3550298538-2939497174-1104
        Account Name:       Student
        Account Domain:     SECURELABSONDEM
        Logon ID:           0xBB64A

Log Name:          Security
Source:            Microsoft Windows security   Logged:         10/14/2021 8:40:52 AM
Event ID:          5061                         Task Category:  System Integrity
Level:             Information                  Keywords:       Audit Failure
User:              N/A                          Computer:       vWorkstation.securelabsondeman
OpCode:            Info
More Information:  Event Log Online Help
```

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

Event ID 5061 in the Windows Security log, under the System Integrity category, is associated with the Cryptographic API (CAPI) and the Key Isolation service, and it typically occurs when a cryptographic key is accessed for operations like encryption or decryption. In this instance, the event shows an "open key" operation attempt, which failed due to a "Key not valid for use in specified state" error, indicated by return code `0x80090016`. This error suggests the key could not be accessed, likely due to misconfiguration, permission issues, or an integrity problem with the cryptographic service. The event is marked as "Audit Failure" for the account "Student" in the "SECURELABSONDEM" domain, meaning the access attempt did not succeed. This could point to unauthorized access or simply a key-related configuration issue, which is essential to monitor in secure environments like "Workstation.securelabsondemand.com."

Part 2: Configure Snort as an Intrusion Prevention System

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



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-17 20:23:51
Julie Clarke

172.30.0.1/snort/snort_interfaces.php

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Interfaces

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	LAN (vmx1)	✓	AC-BNFA	LEGACY MODE	LAN	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.