

# Implementing Security Monitoring and Logging (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 08

Student:  
Sadam Hashi

Email:  
smhashi@asu.edu

Time on Task:  
6 hours, 2 minutes

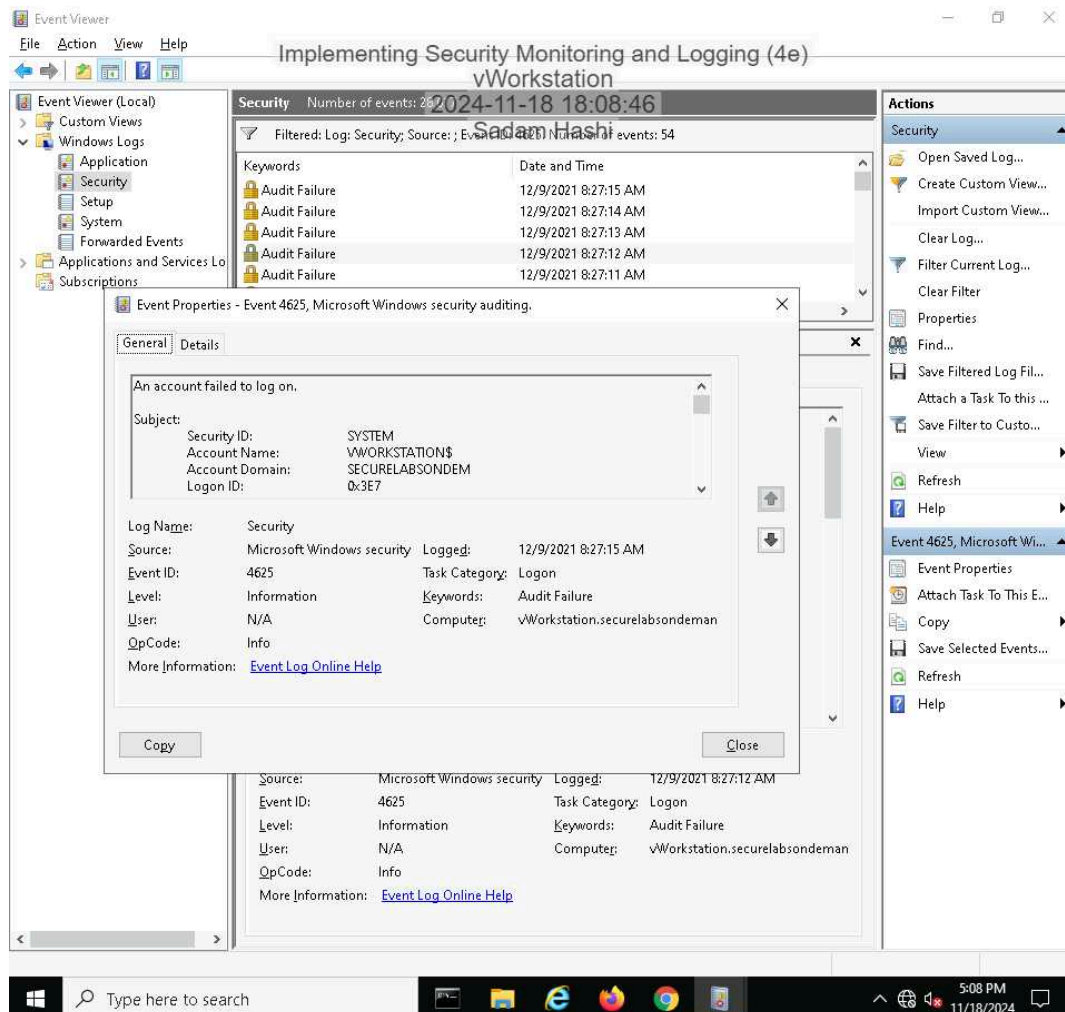
Progress:  
100%

Report Generated: Tuesday, November 19, 2024 at 1:06 AM

## Section 1: Hands-On Demonstration

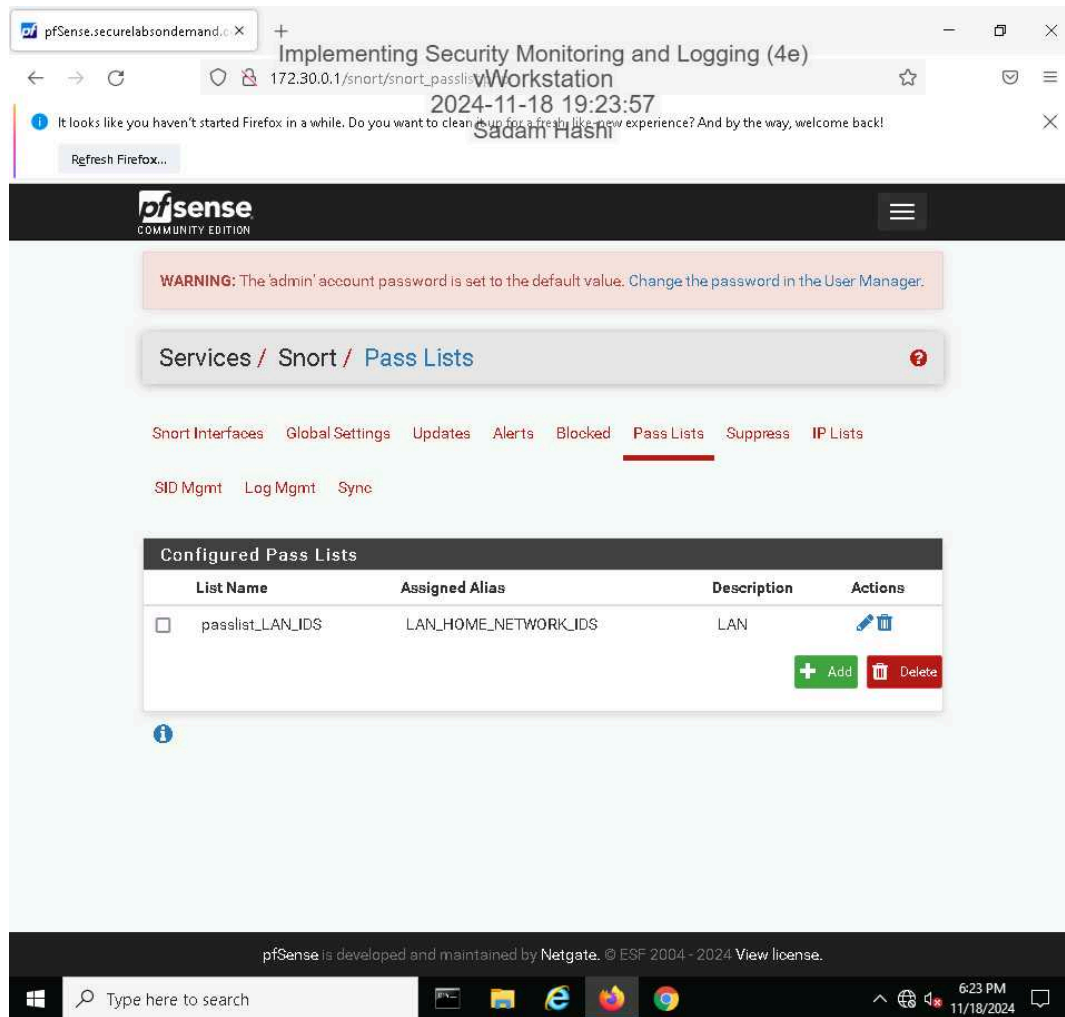
### Part 1: Identify Failed Logon Attempts on Windows Systems

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.



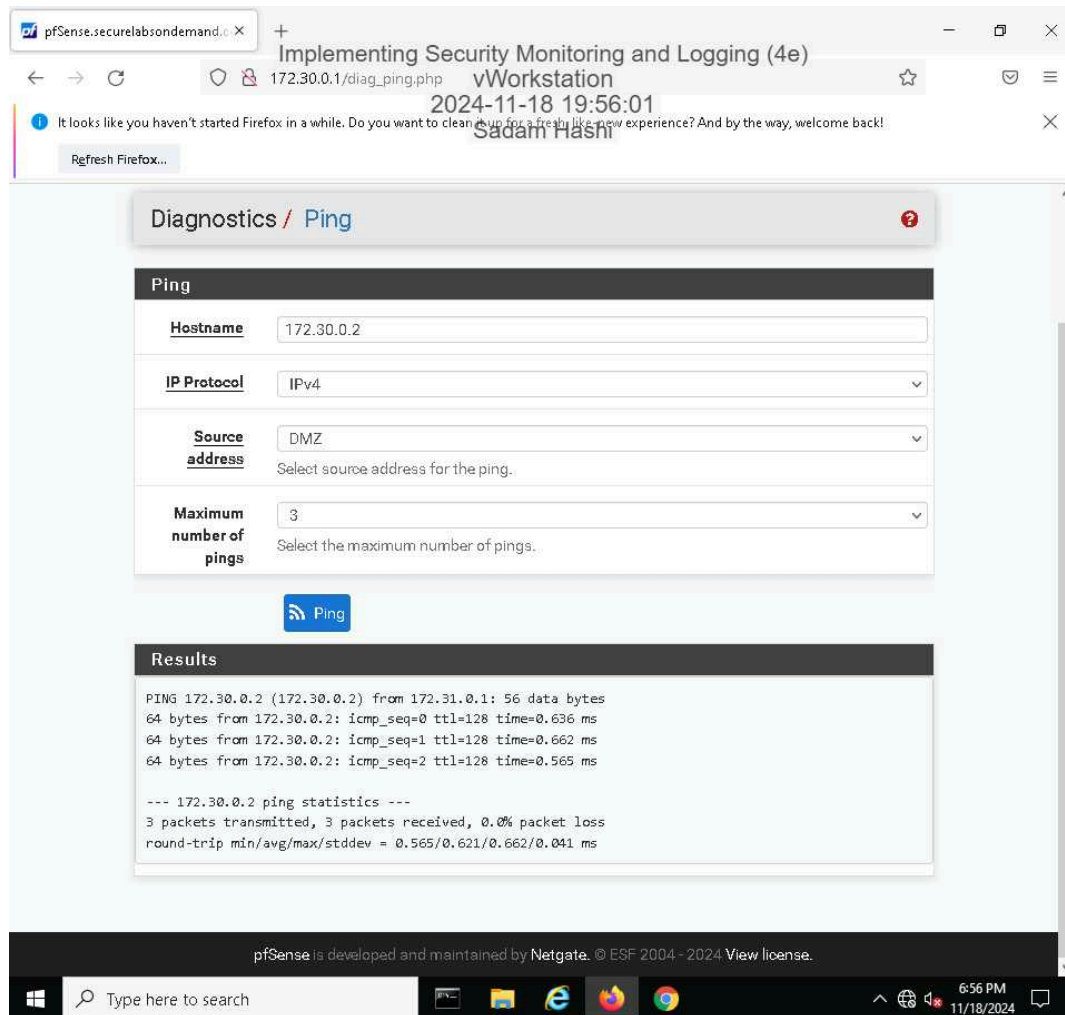
31. Make a screen capture showing the active Snort status on the LAN interface.

The screenshot shows the pfSense web interface in a browser window. The browser's address bar displays the URL `172.30.0.1/snort/snort_interfaces`. The page title is "Implementing Security Monitoring and Logging (4e)". The pfSense logo and "COMMUNITY EDITION" are visible in the top left. A warning message states: "WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)". The breadcrumb navigation shows "Services / Snort / Interfaces". The main navigation menu includes "Snort Interfaces", "Global Settings", "Updates", "Alerts", "Blocked", "Pass Lists", "Suppress", and "IP Lists". Below this, there are links for "SID Mgmt", "Log Mgmt", and "Sync". The "Interface Settings Overview" section contains a table with the following data:

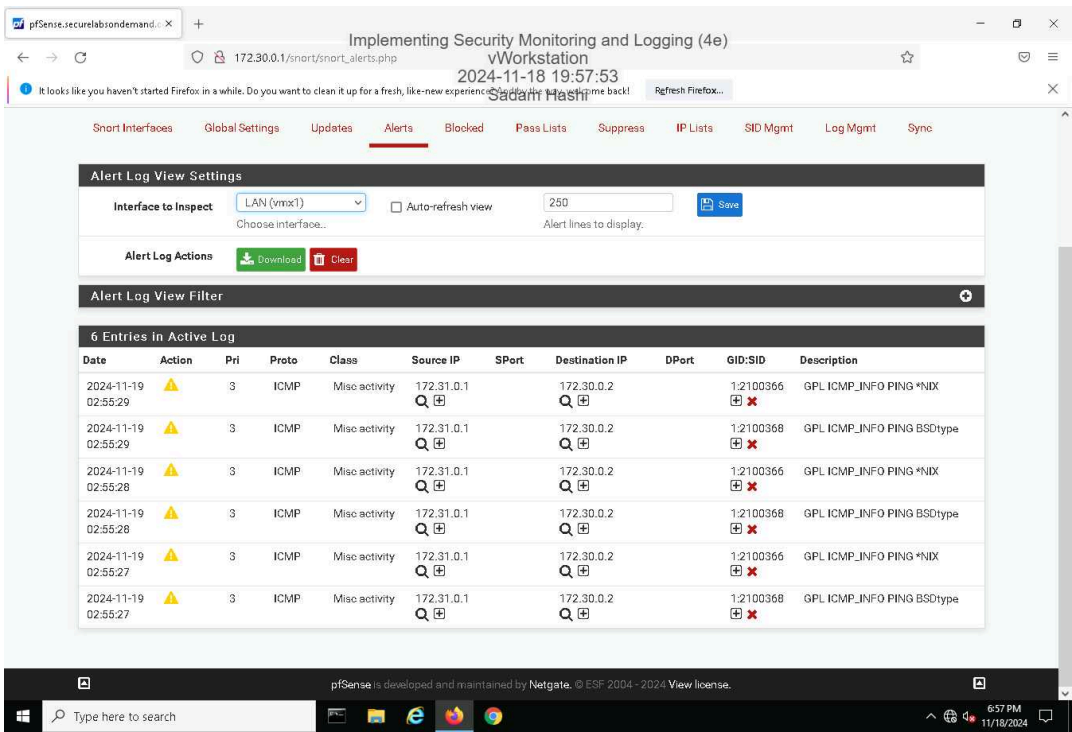
Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> LAN (vmx1)		AC-BNFA	DISABLED	LAN	

Below the table are buttons for "+ Add" and "Delete". At the bottom of the page, a footer states "pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)". The Windows taskbar at the bottom shows the search bar, task view, and several application icons, with the system clock displaying 6:44 PM on 11/18/2024.

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



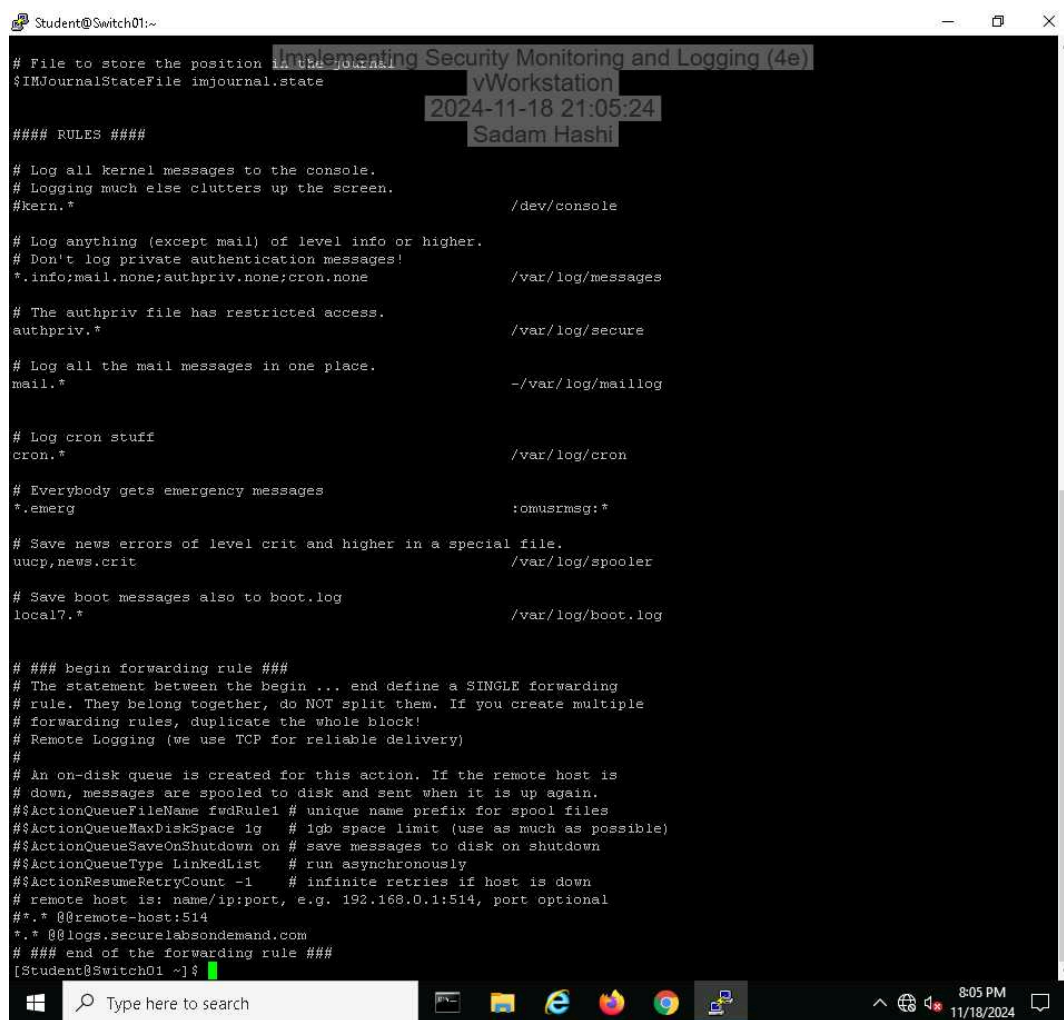
41. Make a screen capture showing the ICMP alerts in the Snort Active Log.



## Section 2: Applied Learning

### Part 1: Identify Failed Logon Attempts on Linux Systems

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



```
# File to store the position of the journal
$IMJournalStateFile imjournal.state

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                     /dev/console

# 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

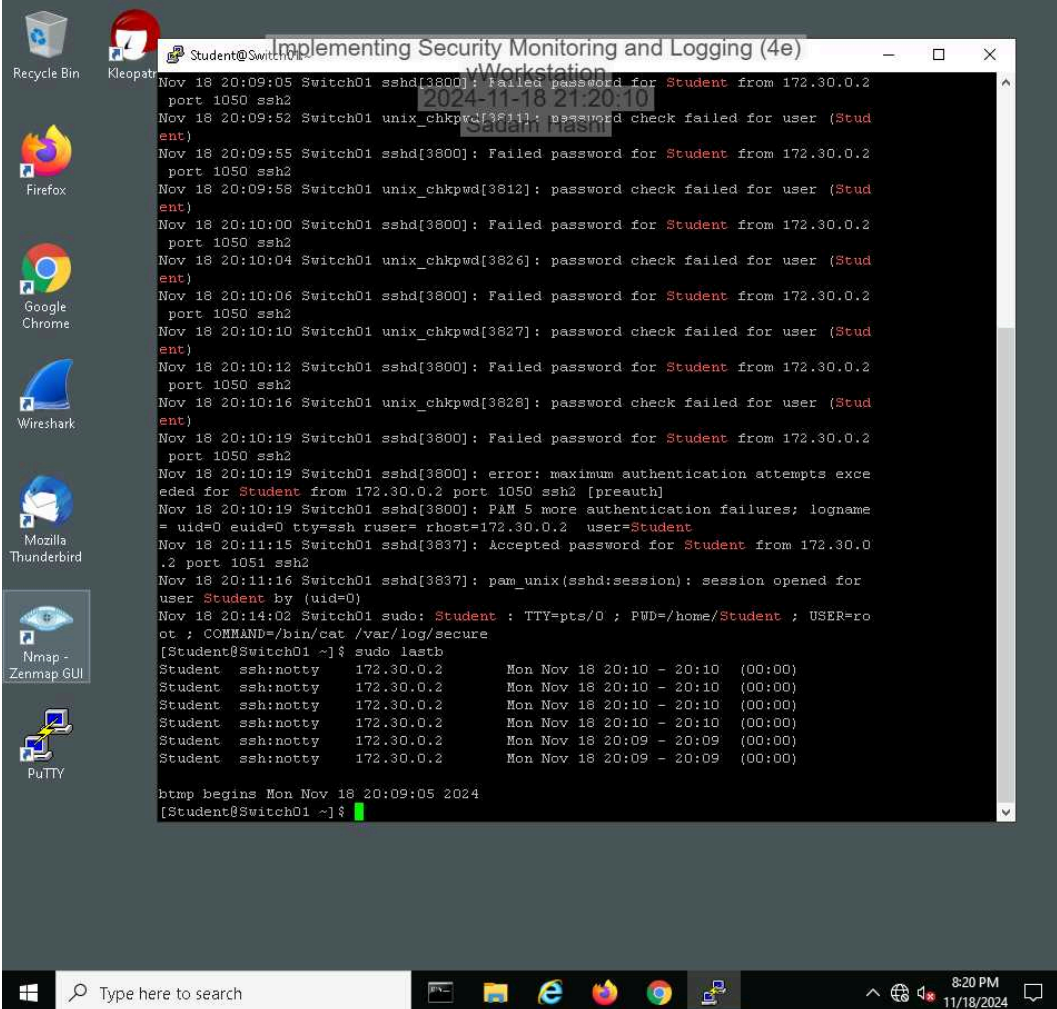
# Everybody gets emergency messages
*.emerg                                     :omusrmsg:*

# 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.



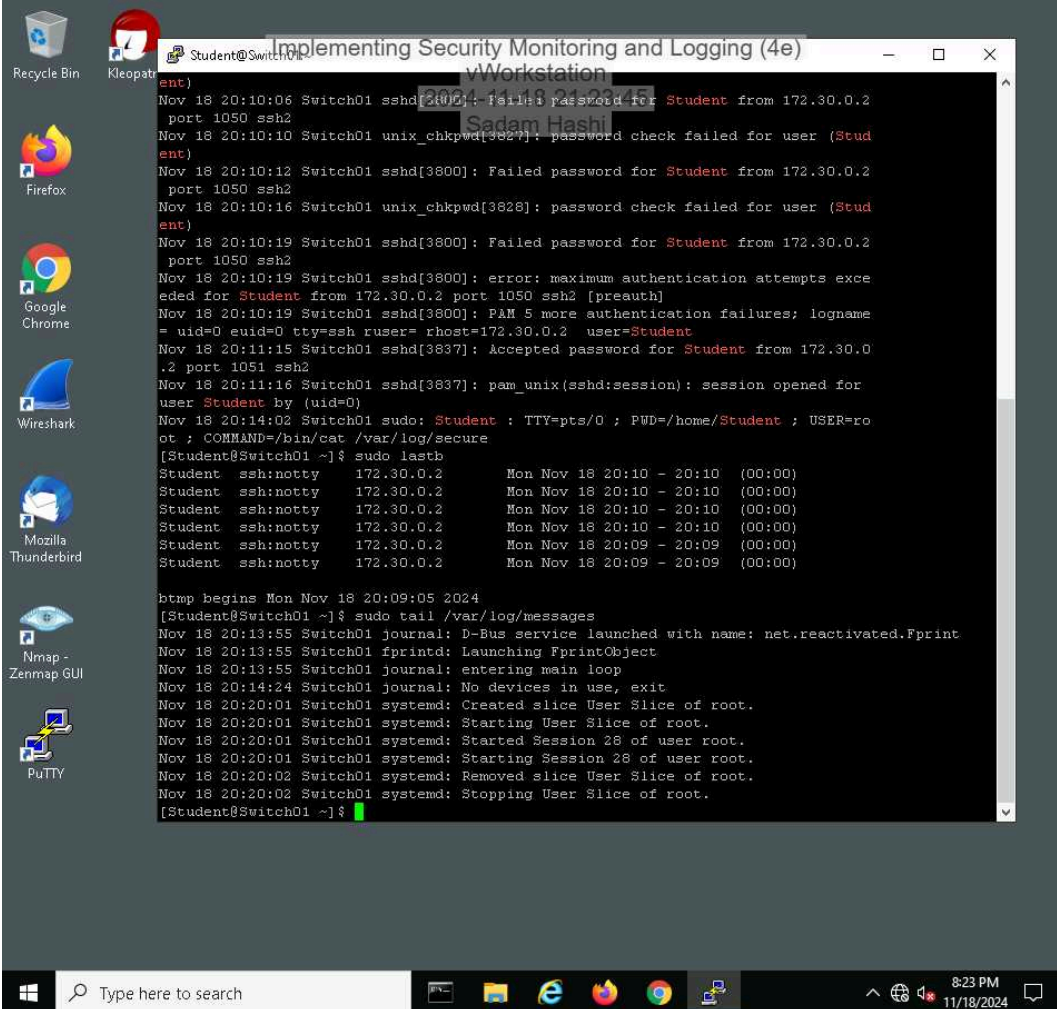
The screenshot shows a Windows desktop environment. On the left side, there is a vertical taskbar with icons for Recycle Bin, Kleopatra, Firefox, Google Chrome, Wireshark, Mozilla Thunderbird, Nmap - Zenmap GUI, and PuTTY. The main area of the desktop is occupied by a terminal window titled "Implementing Security Monitoring and Logging (4e)". The terminal displays a series of SSH login attempts from 172.30.0.2 to a switch named Switch01. The attempts show failed password checks for the user "Student" and a final successful login. The terminal output is as follows:

```
Nov 18 20:09:05 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:09:52 Switch01 unix_chkpwd[3811]: password check failed for user (Student)
Nov 18 20:09:55 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:09:58 Switch01 unix_chkpwd[3812]: password check failed for user (Student)
Nov 18 20:10:00 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:10:04 Switch01 unix_chkpwd[3826]: password check failed for user (Student)
Nov 18 20:10:06 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:10:10 Switch01 unix_chkpwd[3827]: password check failed for user (Student)
Nov 18 20:10:12 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:10:16 Switch01 unix_chkpwd[3828]: password check failed for user (Student)
Nov 18 20:10:19 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:10:19 Switch01 sshd[3800]: error: maximum authentication attempts exceeded for Student from 172.30.0.2 port 1050 ssh2 [preauth]
Nov 18 20:10:19 Switch01 sshd[3800]: PAM 5 more authentication failures; logname=uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2 user=Student
Nov 18 20:11:15 Switch01 sshd[3837]: Accepted password for Student from 172.30.0.2 port 1051 ssh2
Nov 18 20:11:16 Switch01 sshd[3837]: pam_unix(sshd:session): session opened for user Student by (uid=0)
Nov 18 20:14:02 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      Mon Nov 18 20:10 - 20:10 (00:00)
Student  ssh:notty      172.30.0.2      Mon Nov 18 20:10 - 20:10 (00:00)
Student  ssh:notty      172.30.0.2      Mon Nov 18 20:10 - 20:10 (00:00)
Student  ssh:notty      172.30.0.2      Mon Nov 18 20:10 - 20:10 (00:00)
Student  ssh:notty      172.30.0.2      Mon Nov 18 20:09 - 20:09 (00:00)
Student  ssh:notty      172.30.0.2      Mon Nov 18 20:09 - 20:09 (00:00)
btmp begins Mon Nov 18 20:09:05 2024
[Student@Switch01 ~]$
```

The taskbar at the bottom of the screen shows the Windows Start button, a search bar, and several application icons including File Explorer, Edge, Firefox, Chrome, and PuTTY. The system clock in the bottom right corner indicates the time is 8:20 PM on 11/18/2024.



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



The screenshot shows a Windows 10 desktop with a terminal window titled "Implementing Security Monitoring and Logging (4e)". The terminal displays system logs from a switch named Switch01. The logs show several failed password attempts for the user 'Student' from IP 172.30.0.2 on port 1050. After five failed attempts, the system logs a message: "PAM 5 more authentication failures; logname = uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2 user=Student". Subsequently, a successful login is recorded: "Accepted password for Student from 172.30.0.2 port 1051 ssh2". The user then runs 'sudo lastb', which displays a table of recent logins. Finally, the user runs 'sudo tail /var/log/messages', showing various system messages including D-Bus service launch, fprintd startup, and systemd user slice management.

```
[Student@Switch01 ~]$ sudo tail /var/log/messages
Nov 18 20:10:06 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:10:10 Switch01 unix_chkpwd[3827]: password check failed for user (Student)
Nov 18 20:10:12 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:10:16 Switch01 unix_chkpwd[3828]: password check failed for user (Student)
Nov 18 20:10:19 Switch01 sshd[3800]: Failed password for Student from 172.30.0.2 port 1050 ssh2
Nov 18 20:10:19 Switch01 sshd[3800]: error: maximum authentication attempts exceeded for Student from 172.30.0.2 port 1050 ssh2 [preauth]
Nov 18 20:10:19 Switch01 sshd[3800]: PAM 5 more authentication failures; logname = uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2 user=Student
Nov 18 20:11:15 Switch01 sshd[3837]: Accepted password for Student from 172.30.0.2 port 1051 ssh2
Nov 18 20:11:16 Switch01 sshd[3837]: pam_unix(sshd:session): session opened for user Student by (uid=0)
Nov 18 20:14:02 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      Mon Nov 18 20:10 - 20:10   (00:00)
Student  ssh:notty    172.30.0.2      Mon Nov 18 20:10 - 20:10   (00:00)
Student  ssh:notty    172.30.0.2      Mon Nov 18 20:10 - 20:10   (00:00)
Student  ssh:notty    172.30.0.2      Mon Nov 18 20:10 - 20:10   (00:00)
Student  ssh:notty    172.30.0.2      Mon Nov 18 20:09 - 20:09   (00:00)
Student  ssh:notty    172.30.0.2      Mon Nov 18 20:09 - 20:09   (00:00)

btmp begins Mon Nov 18 20:09:05 2024
[Student@Switch01 ~]$ sudo tail /var/log/messages
Nov 18 20:13:55 Switch01 journal: D-Bus service launched with name: net.reactivated.Fprint
Nov 18 20:13:55 Switch01 fprintd: Launching FprintObject
Nov 18 20:13:55 Switch01 journal: entering main loop
Nov 18 20:14:24 Switch01 journal: No devices in use, exit
Nov 18 20:20:01 Switch01 systemd: Created slice User Slice of root.
Nov 18 20:20:01 Switch01 systemd: Starting User Slice of root.
Nov 18 20:20:01 Switch01 systemd: Started Session 28 of user root.
Nov 18 20:20:01 Switch01 systemd: Starting Session 28 of user root.
Nov 18 20:20:02 Switch01 systemd: Removed slice User Slice of root.
Nov 18 20:20:02 Switch01 systemd: Stopping User Slice of root.
[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:~
Open Source Tripwire(R) 2.4.3-7 Integrity Check Report

Report generated by:      root
Report created on:       Mon 18 Nov 2024 08:42:53 PM PST
Database last updated on: Never

=====
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
=====

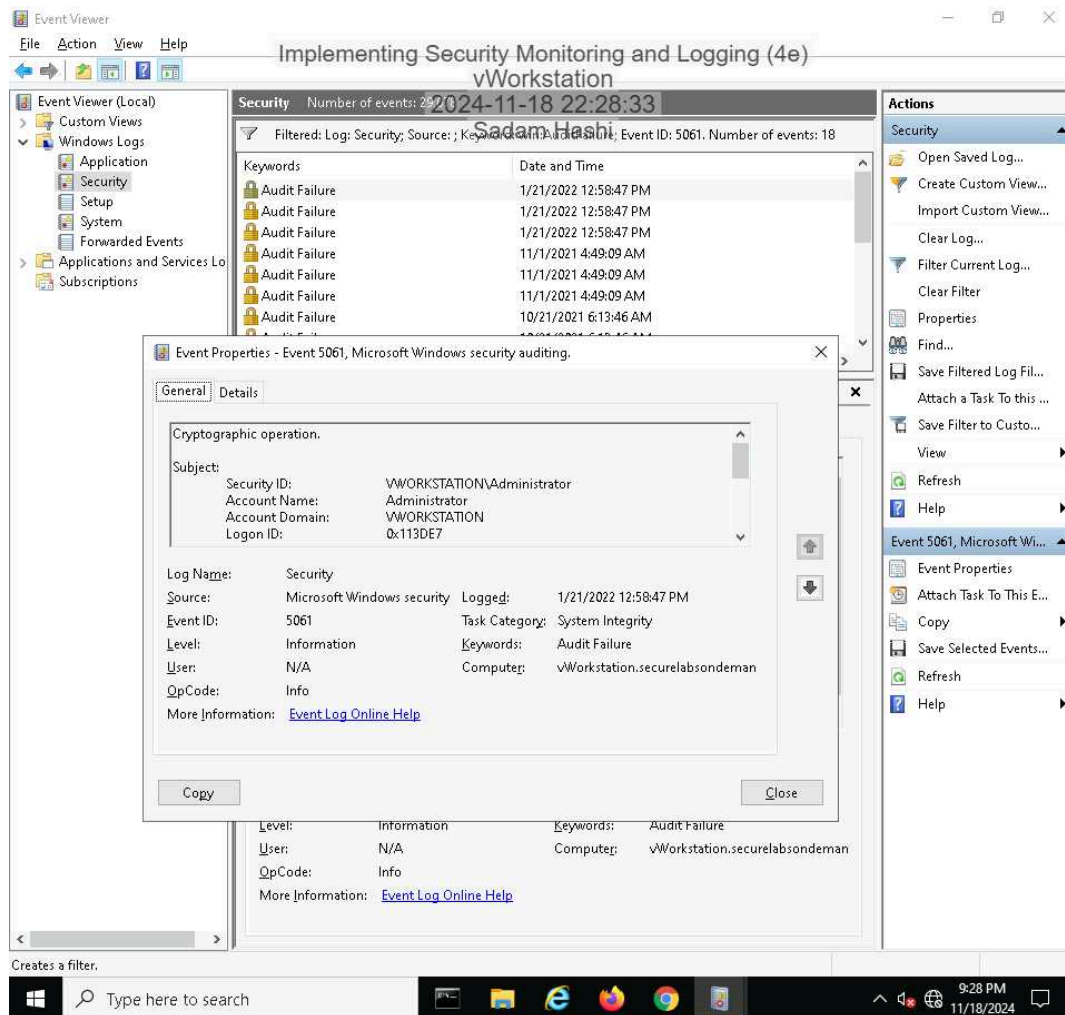
Rule Name                  Severity Level  Added  Removed  Modified
-----
* User binaries            66             0      0         1
Tripwire Binaries         100            0      0         0
Critical configuration files 100            0      0         0
Libraries                  66             0      0         0
* Operating System Utilities 100            0      0         1
Critical system boot files  100            0      0         0
File System and Disk Administration Programs
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
Hardware and Device Control Programs 100            0      0         0
System Information Programs 100            0      0         0
Application Information Programs
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
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

```

### 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 corresponds to cryptographic operations. Event ID 5061 occurs when an attempt to access cryptographic keys or even perform encryption or decryption operations. In this case, the audit failure associated with even ID 5061 means that a person tried to use a key but failed due to not having permission or the key simply not being valid.

#### Part 2: Configure Snort as an Intrusion Prevention System

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

