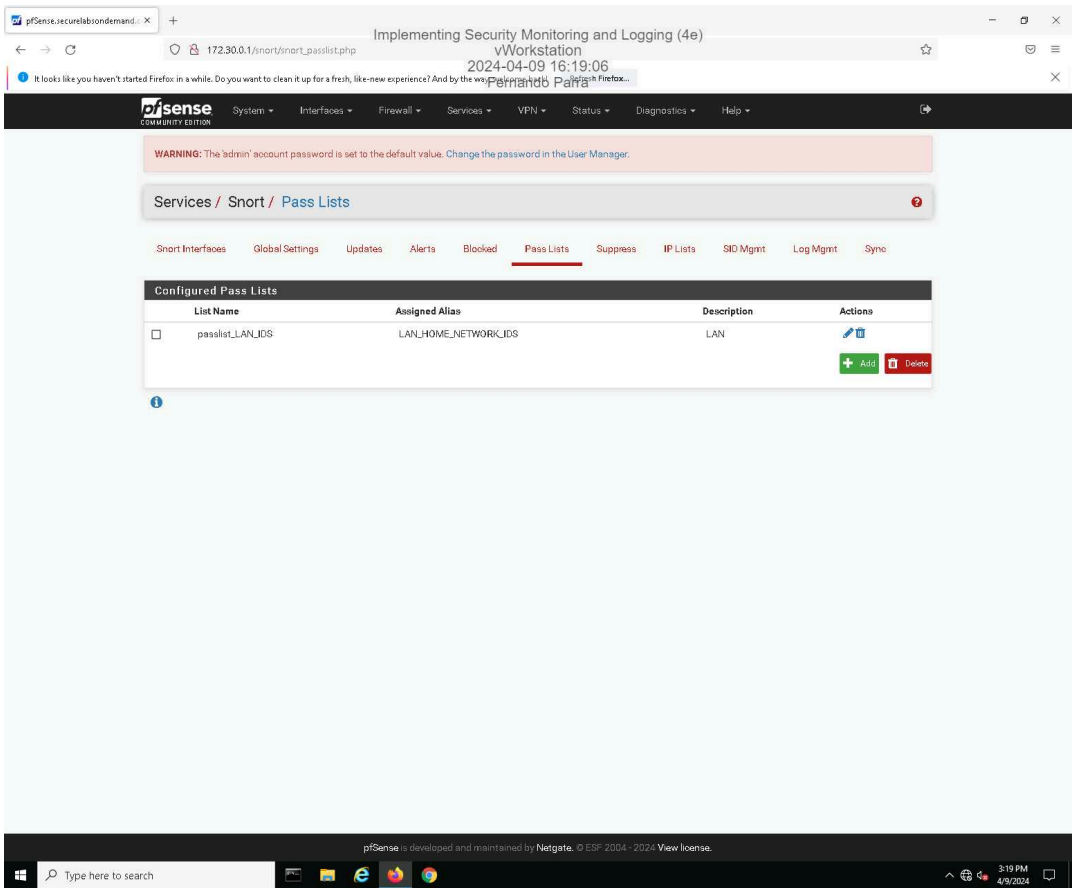


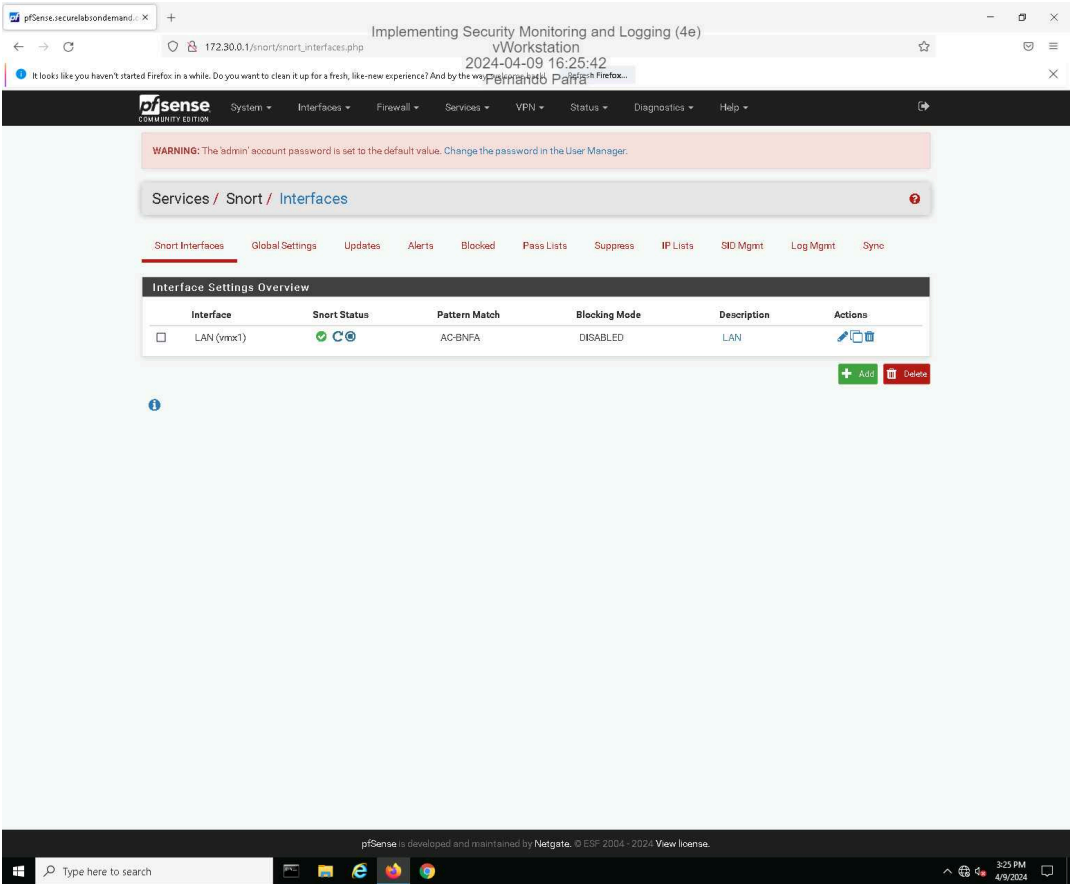
fparra1@msudenve.edu

100%

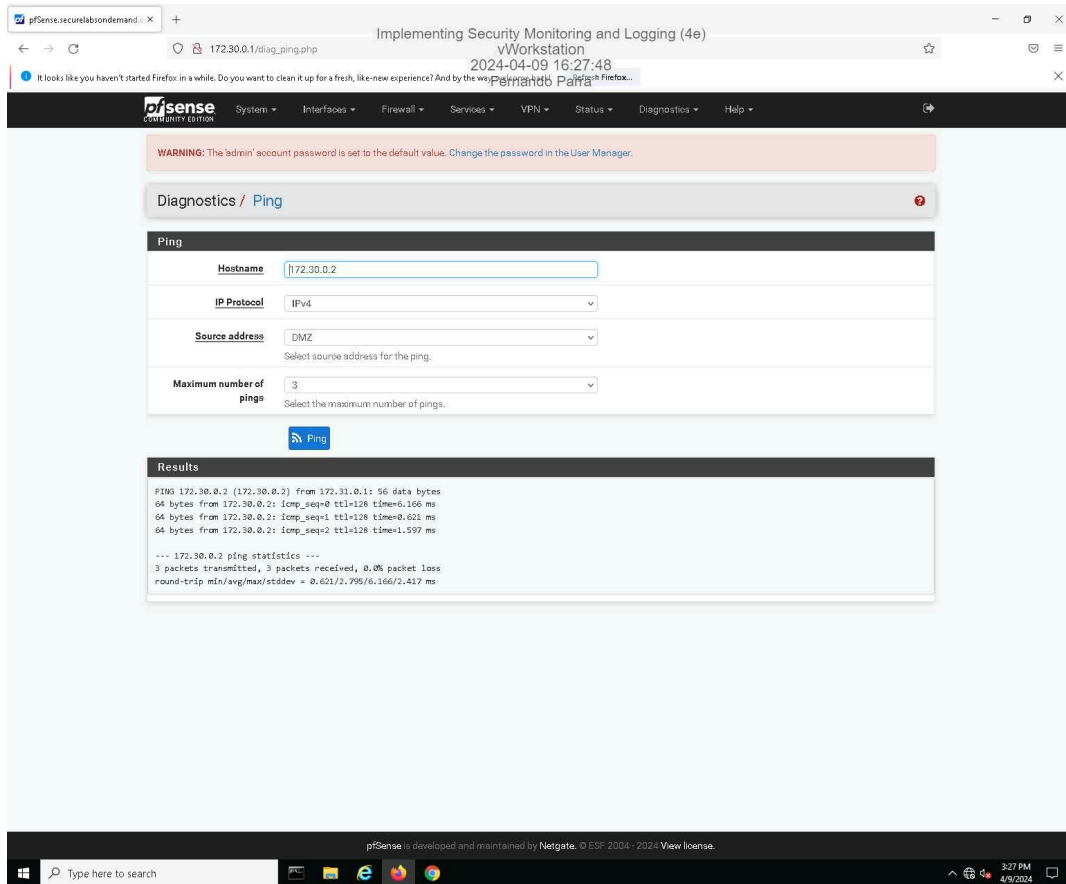
17. Make a screen capture showing the updated Pass Lists page.



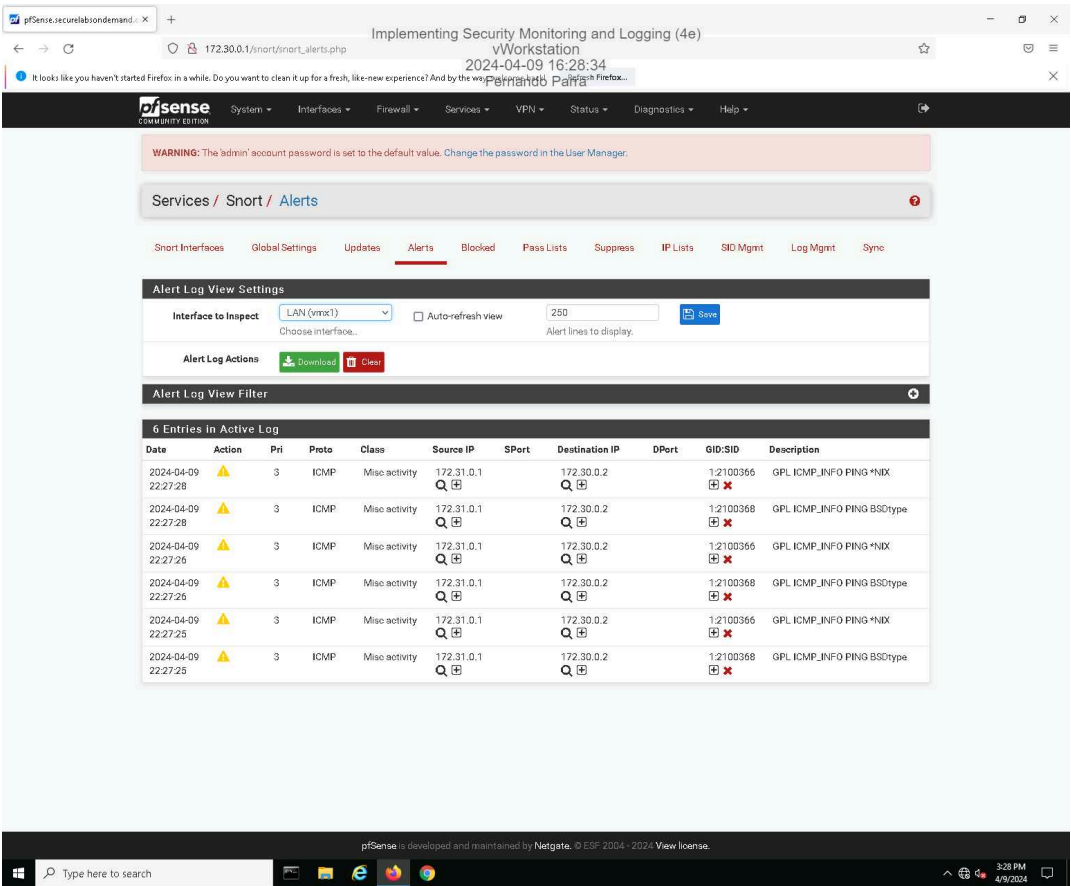
31. Make a screen capture showing the active Snort status on the LAN interface.



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



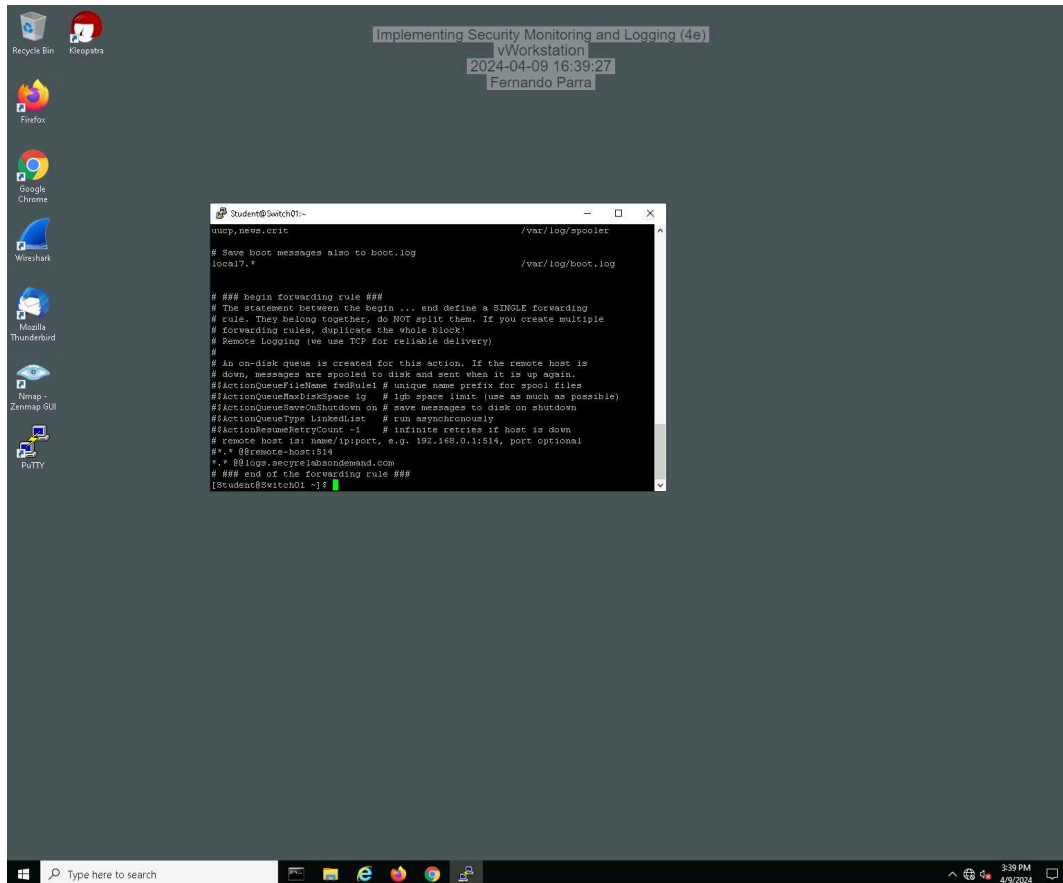
41. Make a screen capture showing the ICMP alerts in the Snort Active Log.



## Section 2: Applied Learning

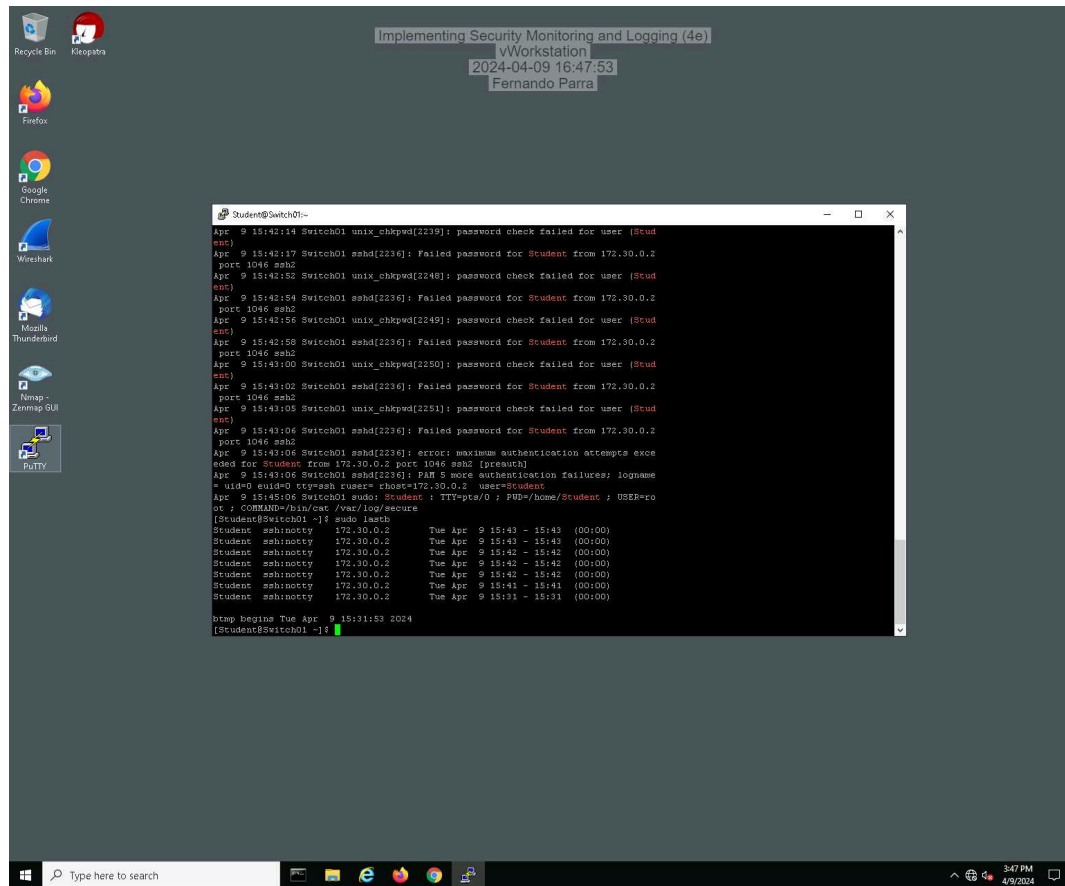
### Part 1: Identify Failed Logon Attempts on Linux Systems

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

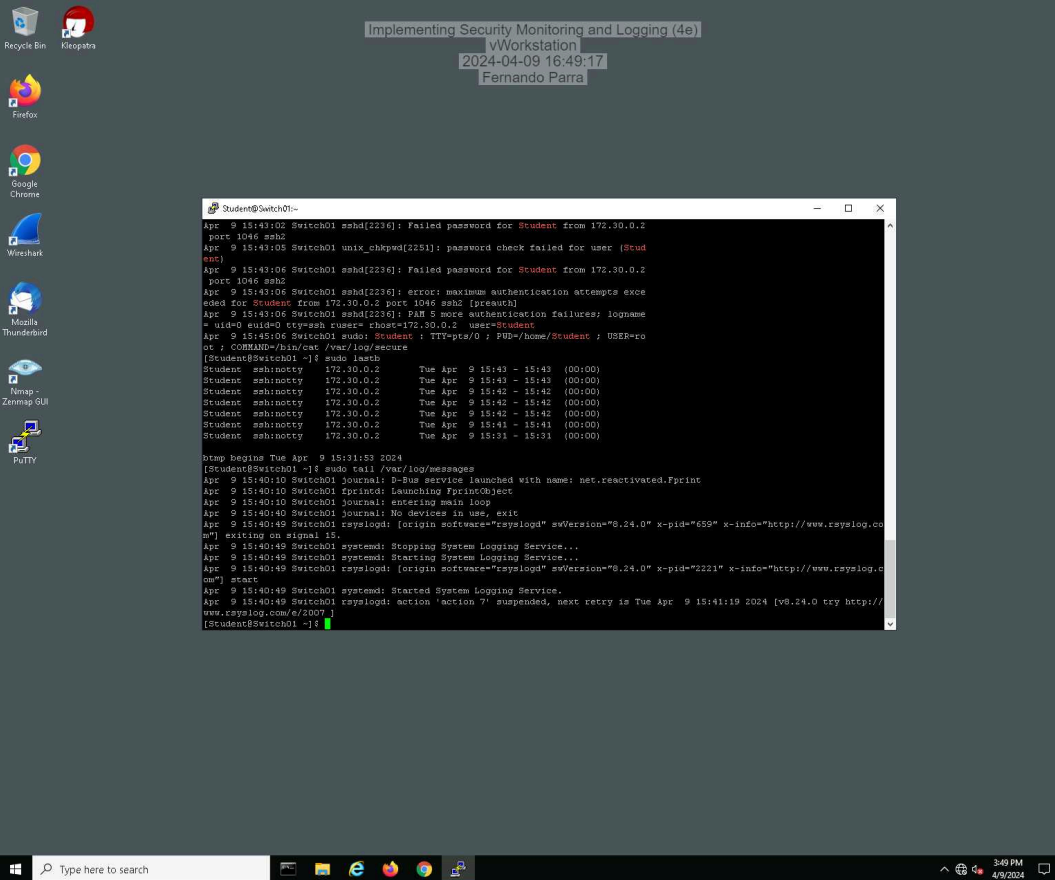


## Fundamentals of Information Systems Security, Fourth Edition - Lab 08

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



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



The screenshot shows a Windows desktop environment. In the center, a terminal window titled "Student@Switch01" is open, displaying a series of log messages. The messages include failed password attempts for the user "Student" from IP 172.30.0.2, a PAM authentication failure, and a successful login for the user "Student". The terminal also shows the output of the "last" command, which lists recent system logins. The desktop background is dark, and various application icons are visible on the left side. The taskbar at the bottom shows the Windows logo, a search bar, and several open applications.

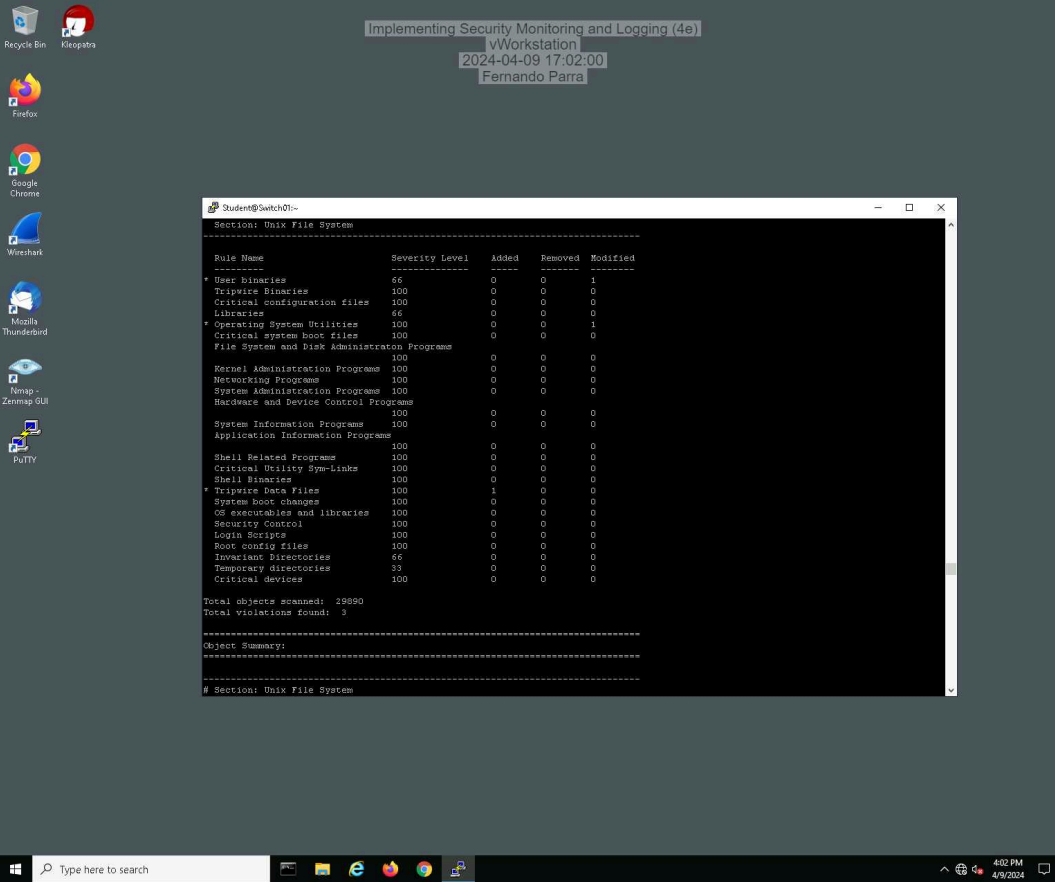
```
Student@Switch01:~$ tail -n 10 /var/log/messages
Apr 9 15:43:00 Switch01 sshd[2236]: Failed password for Student from 172.30.0.2
Apr 9 15:43:05 Switch01 unix_chkpwd[2251]: password check failed for user (Stud
Apr 9 15:43:06 Switch01 sshd[2236]: Failed password for Student from 172.30.0.2
Apr 9 15:43:06 Switch01 sshd[2236]: error: maximum authentication attempts exce
Apr 9 15:43:06 Switch01 sshd[2236]: PAM 5 more authentication failures; logname
Apr 9 15:45:06 Switch01 sudo: Student : TTY=pts/0 : PWD=/home/Student : USER=ro
ot : COMMAND=/bin/cat /var/log/secure
(Student@Switch01) ~$ sudo lasteb
Student      sshinotty    172.30.0.2          Tue Apr 9 15:43 - 15:43 (00:00)
Student      sshinotty    172.30.0.2          Tue Apr 9 15:43 - 15:43 (00:00)
Student      sshinotty    172.30.0.2          Tue Apr 9 15:42 - 15:42 (00:00)
Student      sshinotty    172.30.0.2          Tue Apr 9 15:42 - 15:42 (00:00)
Student      sshinotty    172.30.0.2          Tue Apr 9 15:42 - 15:42 (00:00)
Student      sshinotty    172.30.0.2          Tue Apr 9 15:41 - 15:41 (00:00)
Student      sshinotty    172.30.0.2          Tue Apr 9 15:31 - 15:31 (00:00)

btmp begins Tue Apr 9 15:31:53 2024
(Student@Switch01) ~$ sudo tail /var/log/messages
Apr 9 15:40:10 Switch01 journal: s-bus service launched with name: net.reactivat
Apr 9 15:40:10 Switch01 cprintd: Launching FprintObject
Apr 9 15:40:10 Switch01 journal: entering main loop
Apr 9 15:40:40 Switch01 journal: No devices in use, exit
Apr 9 15:40:49 Switch01 rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="659" x-info="http://www.rsyslog.com"] exiting on signal 15.
Apr 9 15:40:49 Switch01 systemd: Stopping System Logging Service...
Apr 9 15:40:49 Switch01 systemd: Starting System Logging Service...
Apr 9 15:40:49 Switch01 rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="2221" x-info="http://www.rsyslog.com"] start.
Apr 9 15:40:49 Switch01 systemd: Started System Logging Service.
Apr 9 15:40:49 Switch01 rsyslogd: action 'action 7' suspended, next retry is Tue Apr 9 15:41:19 2024 [v8.24.0 try http://www.rsyslog.com/e/2007 ]
(Student@Switch01) ~$
```

## Part 2: Monitor File Integrity with Tripwire



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



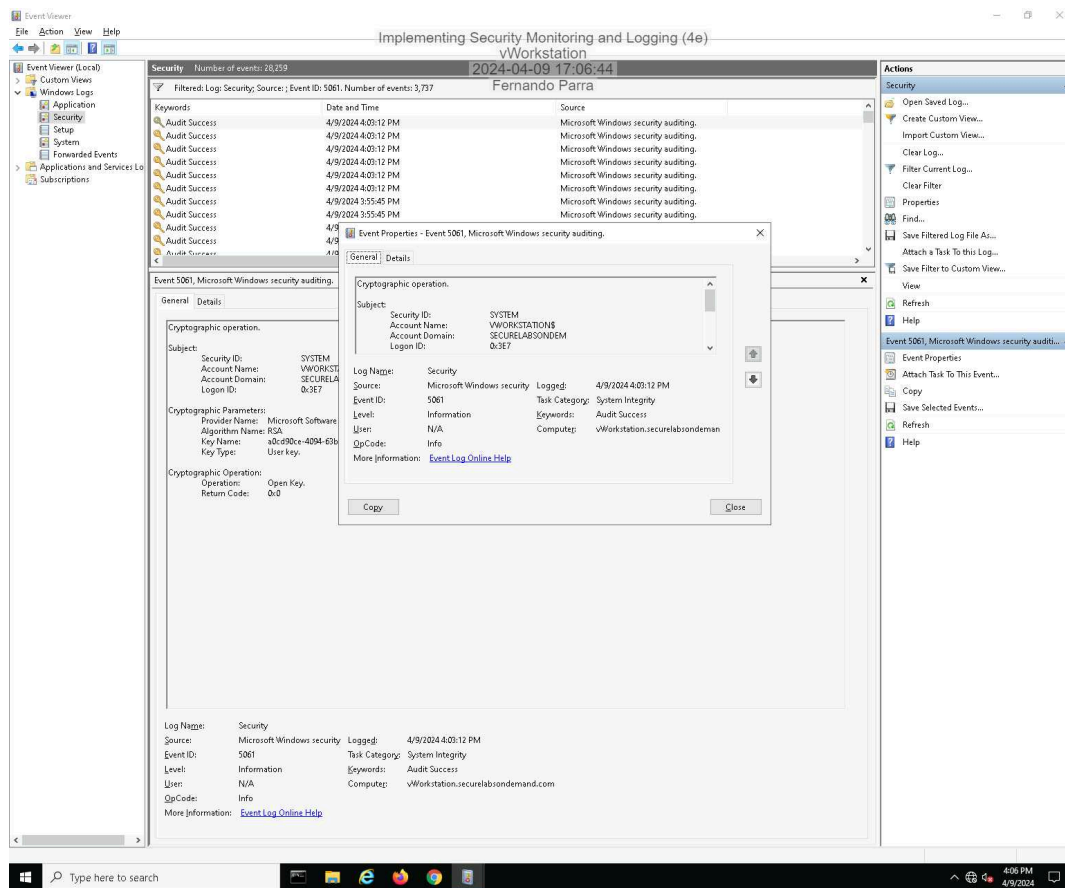
Implementing Security Monitoring and Logging (4e)  
vWorkstation  
2024-04-09 17:02:00  
Fernando Parra

```
Student@Switch01:~$  
-----  
# Section: Unix File System  
-----  
Rule Name          Severity Level  Added  Removed  Modified  
-----  
* Usec 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  
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: 28980  
Total violations found: 3  
  
-----  
Object Summary:  
-----  
# Section: Unix File System
```

## 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 Event ID 5061 in Windows Event Viewer is related to a cryptographic operations. The details tab in the security event properties dialog box show that opening a key such as the Microsoft Software Key Storage Provider will be logged for auditing, this is essential for monitoring cryptographic keys.

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

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

