Implementing Security Monitoring and Logging (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 08

Student:	Email:
Marc Corona	coronami@calpoly.edu

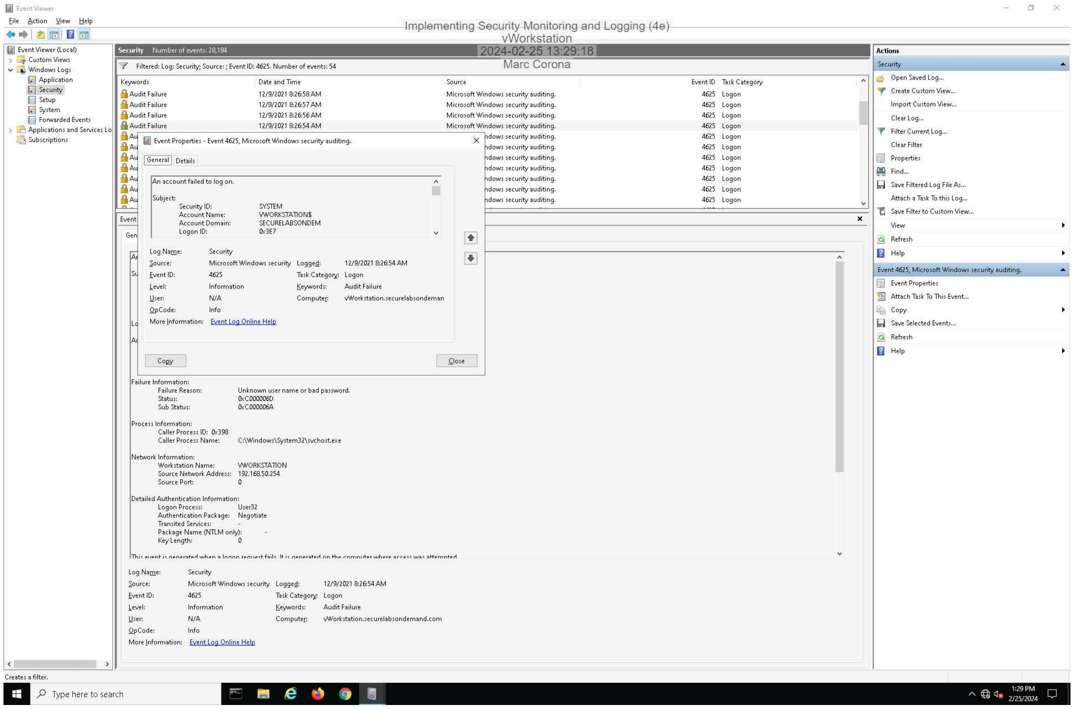
Time on Task:	Progress:
3 hours, 11 minutes	100%

Report Generated: Saturday, March 2, 2024 at 5:47 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**.



Security Number of events: 28,184

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 54

```
Keywords        Date and Time          Source                                  Event ID  Task Category
Audit Failure   12/9/2021 8:26:58 AM   Microsoft Windows security auditing.    4625      Logon
Audit Failure   12/9/2021 8:26:57 AM   Microsoft Windows security auditing.    4625      Logon
Audit Failure   12/9/2021 8:26:56 AM   Microsoft Windows security auditing.    4625      Logon
Audit Failure   12/9/2021 8:26:54 AM   Microsoft Windows security auditing.    4625      Logon
```

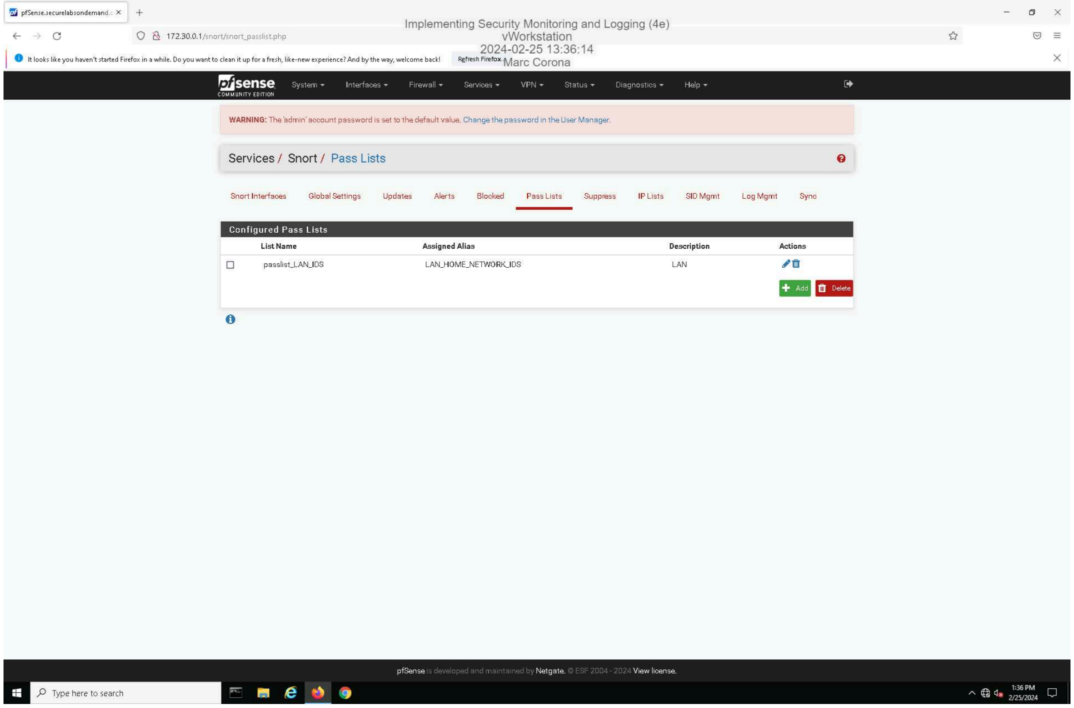
Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

```
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

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:  0x398
        Caller Process Name:    C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       VWORKSTATION
        Source Network Address: 192.168.50.254
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

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
2024-02-25 13:36:14
Marc Corona

172.30.0.1/snort/snort_passlist.php

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.

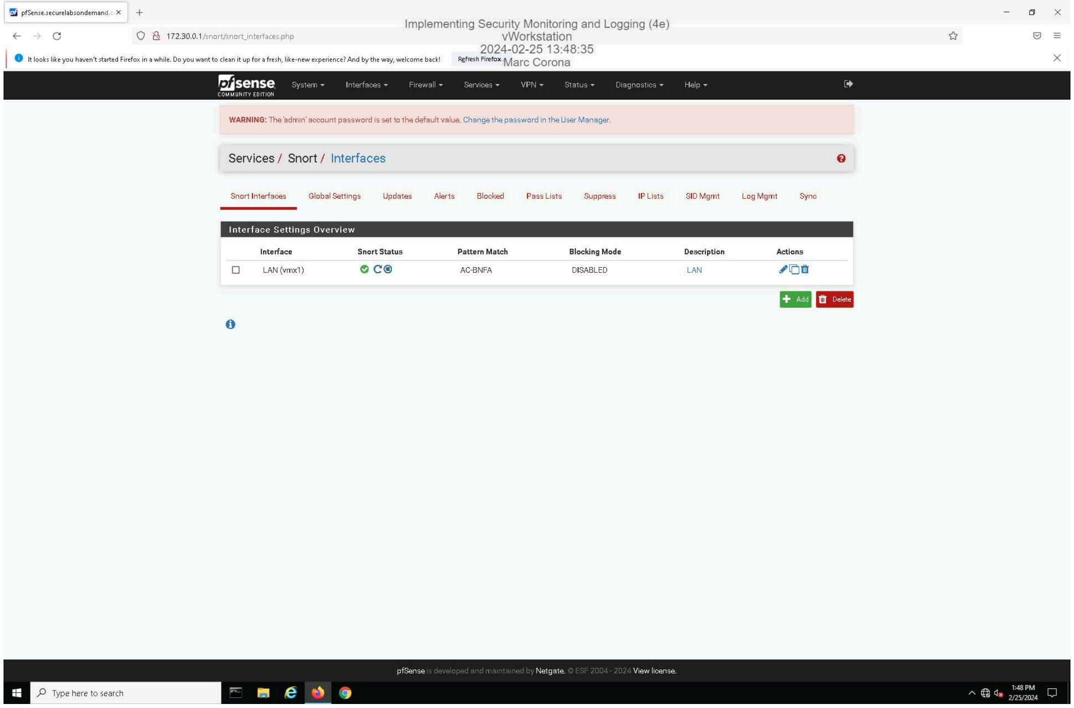
Services / Snort / Pass Lists

Configured Pass Lists

	List Name	Assigned Alias	Description
□	passlist_LAN_IDS	LAN_HOME_NETWORK_IDS	LAN

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
2024-02-25 13:48:35
Marc Corona

172.30.0.1/snort/snort_interfaces.php

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.

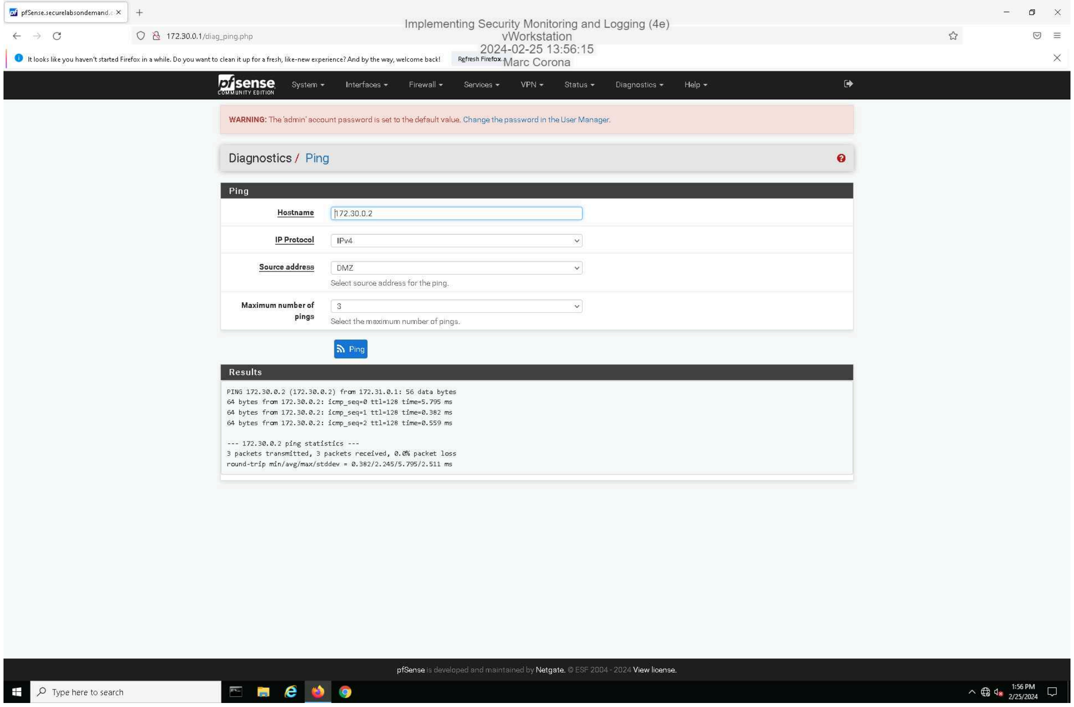
Services / Snort / Interfaces

Interface Settings Overview

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

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

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



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-02-25 13:56:15
Marc Corona

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.

Diagnostics / Ping

Ping

Hostname 172.30.0.2

IP Protocol IPv4

Source address DMZ
Select source address for the ping.

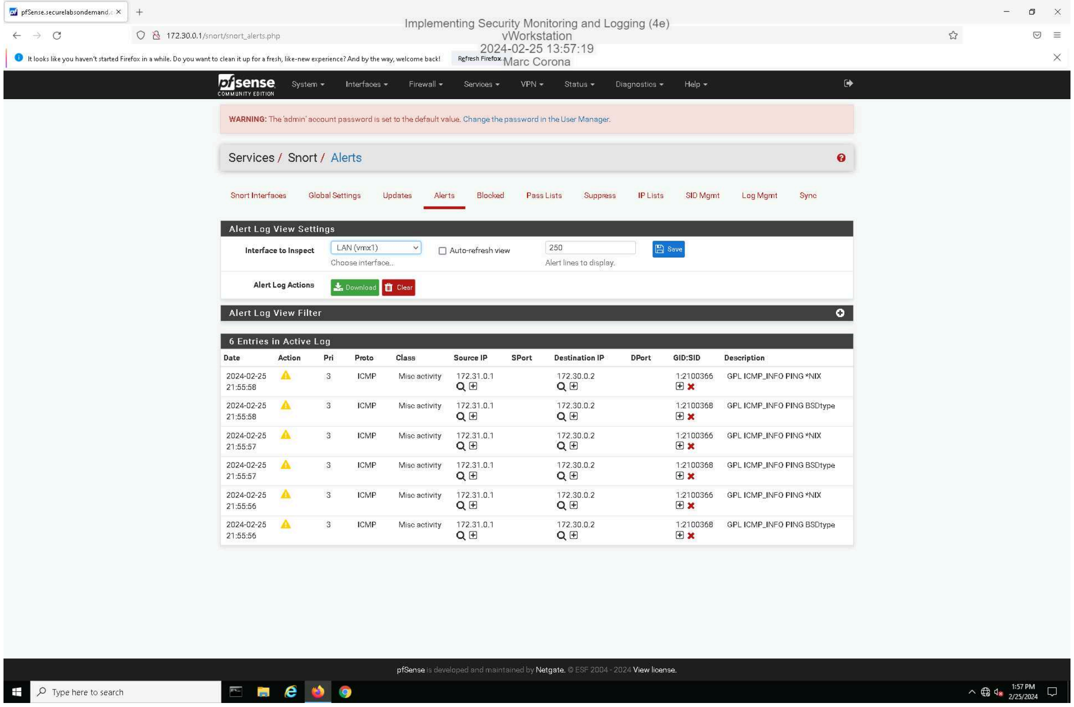
Maximum number of pings 3
Select the maximum number of pings.

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=5.795 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.382 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.559 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.382/2.245/5.795/2.511 ms
```

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

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



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-02-25 13:57:19
Marc Corona

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 / Alerts

Alert Log View Settings

Interface to Inspect LAN (vmx1)
Choose interface..

□ Auto-refresh view

250
Alert lines to display.

Alert Log Actions

Alert Log View Filter

6 Entries in Active Log

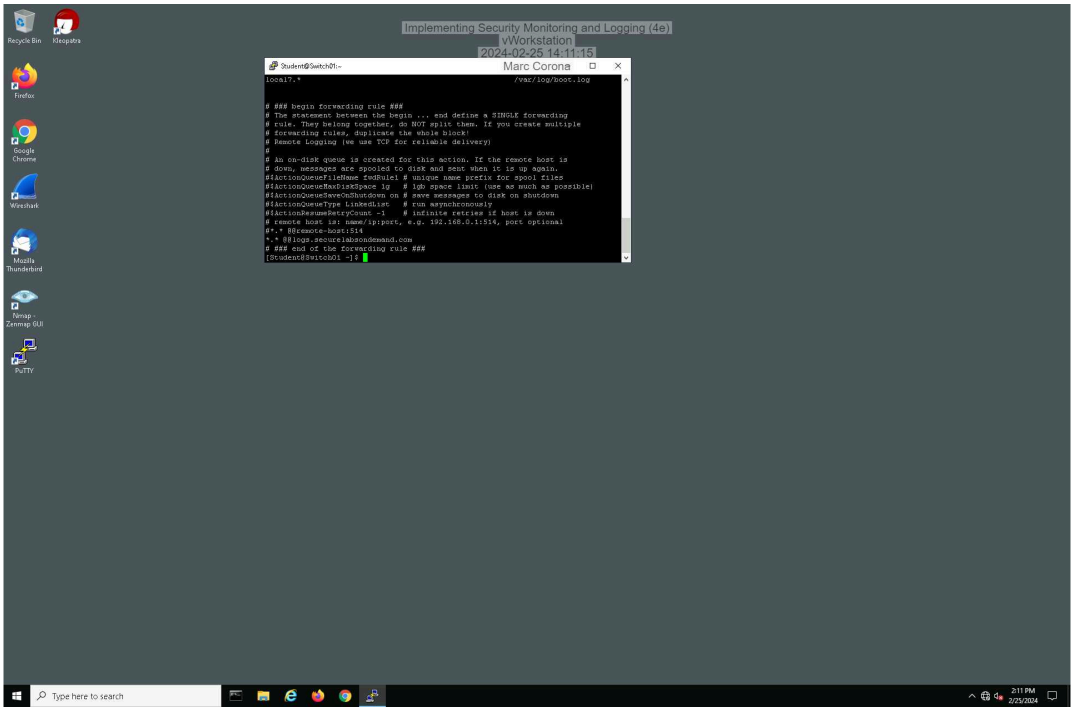
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-02-25 21:55:58	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-02-25 21:55:58	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2024-02-25 21:55:57	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-02-25 21:55:57	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2024-02-25 21:55:56	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-02-25 21:55:56	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype

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

Section 2: Applied Learning

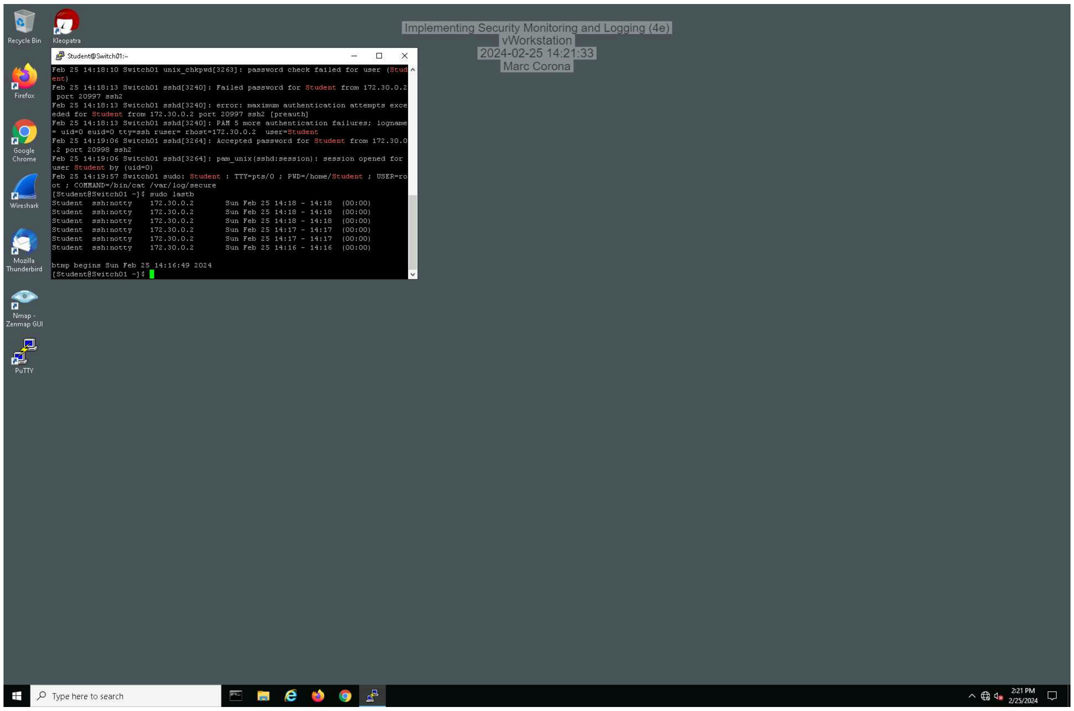
Part 1: Identify Failed Logon Attempts on Linux Systems

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



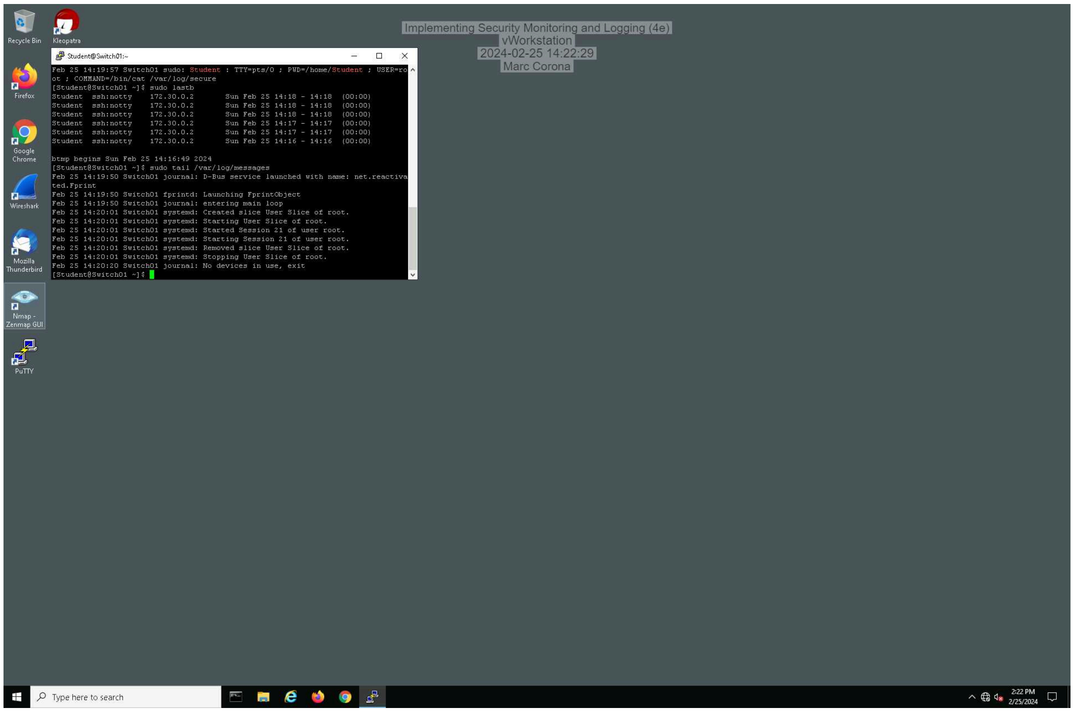
```
local7.*                                                /var/log/boot.log


# ### 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**.



```
Feb 25 14:18:10 Switch01 unix_chkpwd[3263]: password check failed for user (Stud
ent)
Feb 25 14:18:13 Switch01 sshd[3240]: Failed password for Student from 172.30.0.2
 port 20997 ssh2
Feb 25 14:18:13 Switch01 sshd[3240]: error: maximum authentication attempts exce
eded for Student from 172.30.0.2 port 20997 ssh2 [preauth]
Feb 25 14:18:13 Switch01 sshd[3240]: PAM 5 more authentication failures; logname
= uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2  user=Student
Feb 25 14:19:06 Switch01 sshd[3264]: Accepted password for Student from 172.30.0
.2 port 20998 ssh2
Feb 25 14:19:06 Switch01 sshd[3264]: pam_unix(sshd:session): session opened for
user Student by (uid=0)
Feb 25 14:19:57 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 Feb 25 14:18 - 14:18  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:18 - 14:18  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:18 - 14:18  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:17 - 14:17  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:17 - 14:17  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:16 - 14:16  (00:00)

btmp begins Sun Feb 25 14:16:49 2024
[Student@Switch01 ~]$
```

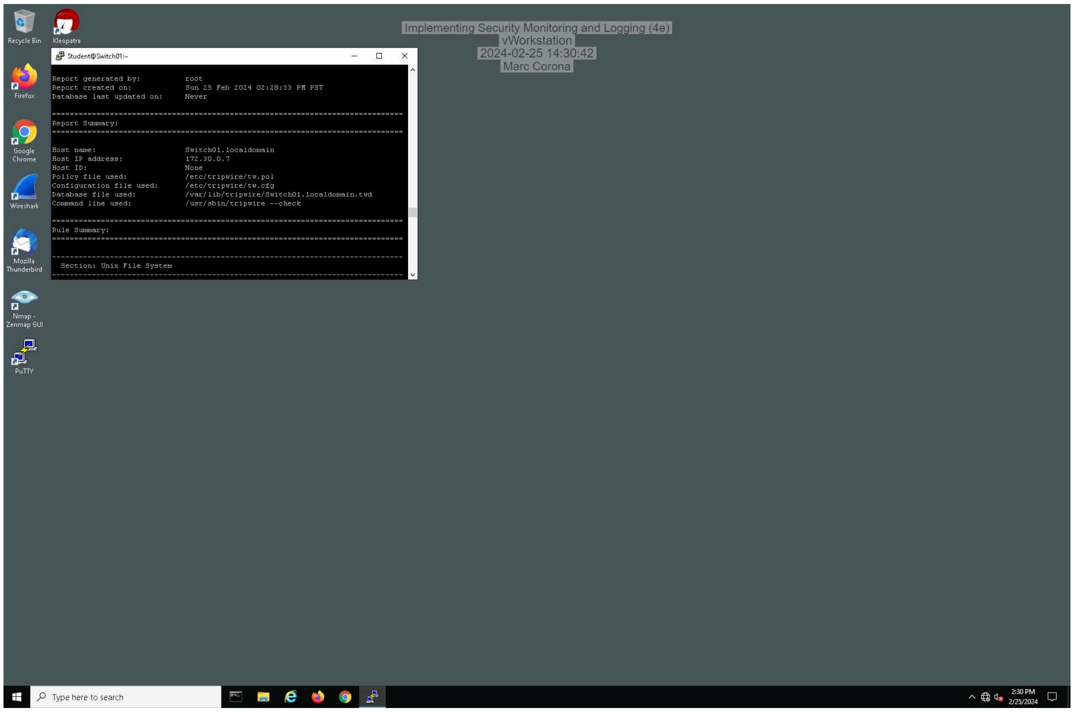
22. **Make a screen capture** showing the **last 10 log messages**.



```
Feb 25 14:19:57 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 Feb 25 14:18 - 14:18  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:18 - 14:18  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:18 - 14:18  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:17 - 14:17  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:17 - 14:17  (00:00)
Student  ssh:notty    172.30.0.2       Sun Feb 25 14:16 - 14:16  (00:00)

btmp begins Sun Feb 25 14:16:49 2024
[Student@Switch01 ~]$ sudo tail /var/log/messages
Feb 25 14:19:50 Switch01 journal: D-Bus service launched with name: net.reactiva
ted.Fprint
Feb 25 14:19:50 Switch01 fprintd: Launching FprintObject
Feb 25 14:19:50 Switch01 journal: entering main loop
Feb 25 14:20:01 Switch01 systemd: Created slice User Slice of root.
Feb 25 14:20:01 Switch01 systemd: Starting User Slice of root.
Feb 25 14:20:01 Switch01 systemd: Started Session 21 of user root.
Feb 25 14:20:01 Switch01 systemd: Starting Session 21 of user root.
Feb 25 14:20:01 Switch01 systemd: Removed slice User Slice of root.
Feb 25 14:20:01 Switch01 systemd: Stopping User Slice of root.
Feb 25 14:20:20 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**.

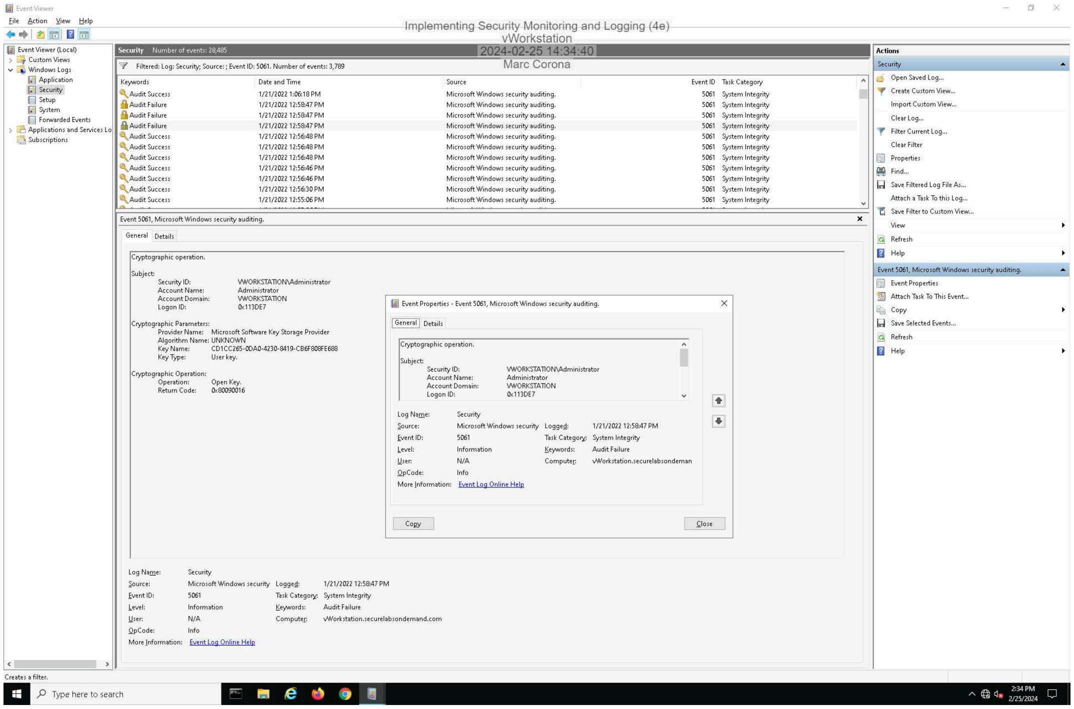


```
Report generated by:          root
Report created on:            Sun 25 Feb 2024 02:28:33 PM PST
Database last updated on:     Never

===============================================================================
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
-------------------------------------------------------------------------------
```

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**.



Security Number of events: 28,485

Filtered: Log: Security; Source: ; Event ID: 5061. Number of events: 3,789

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/21/2022 1:06:18 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Failure	1/21/2022 12:58:47 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Failure	1/21/2022 12:58:47 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Failure	1/21/2022 12:58:47 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	1/21/2022 12:56:48 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	1/21/2022 12:56:48 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	1/21/2022 12:56:48 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	1/21/2022 12:56:46 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	1/21/2022 12:56:46 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	1/21/2022 12:56:30 PM	Microsoft Windows security auditing.	5061	System Integrity
Audit Success	1/21/2022 12:55:06 PM	Microsoft Windows security auditing.	5061	System Integrity

Event 5061, Microsoft Windows security auditing.

General Details

```
Cryptographic operation.

Subject:
        Security ID:        VWORKSTATION\Administrator
        Account Name:       Administrator
        Account Domain:     VWORKSTATION
        Logon ID:           0x113DE7

Cryptographic Parameters:
        Provider Name:  Microsoft Software Key Storage Provider
        Algorithm Name: UNKNOWN
        Key Name:       CD1CC265-0DA0-4230-8419-CB6F808FE688
        Key Type:       User key.

Cryptographic Operation:
        Operation:      Open Key.
        Return Code:    0x80090016
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          1/21/2022 12:58:47 PM
Event ID:          5061                         Task Category:   System Integrity
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        vWorkstation.securelabsondemand.com
OpCode:            Info
More Information:  Event Log Online Help
```

Event Properties - Event 5061, Microsoft Windows security auditing.

General Details

```
Cryptographic operation.

Subject:
        Security ID:        VWORKSTATION\Administrator
        Account Name:       Administrator
        Account Domain:     VWORKSTATION
        Logon ID:           0x113DE7
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          1/21/2022 12:58:47 PM
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
```

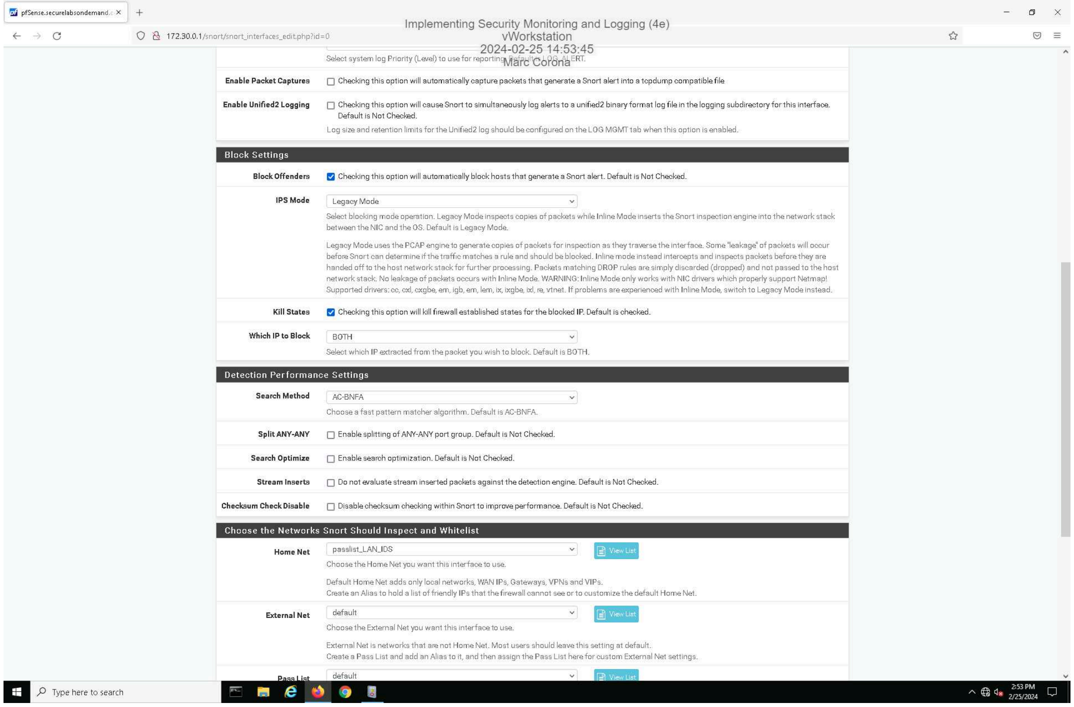
Copy Close

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

An event ID of 5061 pertains to a cryptographic operation. This event is logged when a cryptographic operation is attempted, such as the use of a cryptographic key, and involves operations like key export, key import, data encryption, data decryption, signing, and more. This event is crucial for monitoring and auditing cryptographic activities within a system to ensure security policies are followed, to identify potential unathorized access to cryptographic keys, or to detect other security relevant activities involving cryptographic operations.

Part 2: Configure Snort as an Intrusion Prevention System

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


pfSense.securelabsondemand.
172.30.0.1/snort/snort_interfaces_edit.php?id=0
Type here to search
2:53 PM
2/25/2024

Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-02-25 14:53:45
Marc Corona

Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.

Enable Packet Captures □ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Enable Unified2 Logging □ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

Block Offenders ☑ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode Legacy Mode
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: cc, cxl, cxgbe, em, igb, em, lem, ix, ixgbe, ixl, re, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States ☑ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block BOTH
Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performance Settings

Search Method AC-BNFA
Choose a fast pattern matcher algorithm. Default is AC-BNFA.

Split ANY-ANY □ Enable splitting of ANY-ANY port group. Default is Not Checked.

Search Optimize □ Enable search optimization. Default is Not Checked.

Stream Inserts □ Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.

Checksum Check Disable □ Disable checksum checking within Snort to improve performance. Default is Not Checked.

Choose the Networks Snort Should Inspect and Whitelist

Home Net passlist_LAN_IDS View List
Choose the Home Net you want this interface to use.

Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.
Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

External Net default View List
Choose the External Net you want this interface to use.

External Net is networks that are not Home Net. Most users should leave this setting at default.
Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

Pass List default View List