Implementing Security Monitoring and Logging (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 08

Student:	Email:
Mustafa Shah	ho3168@wayne.edu

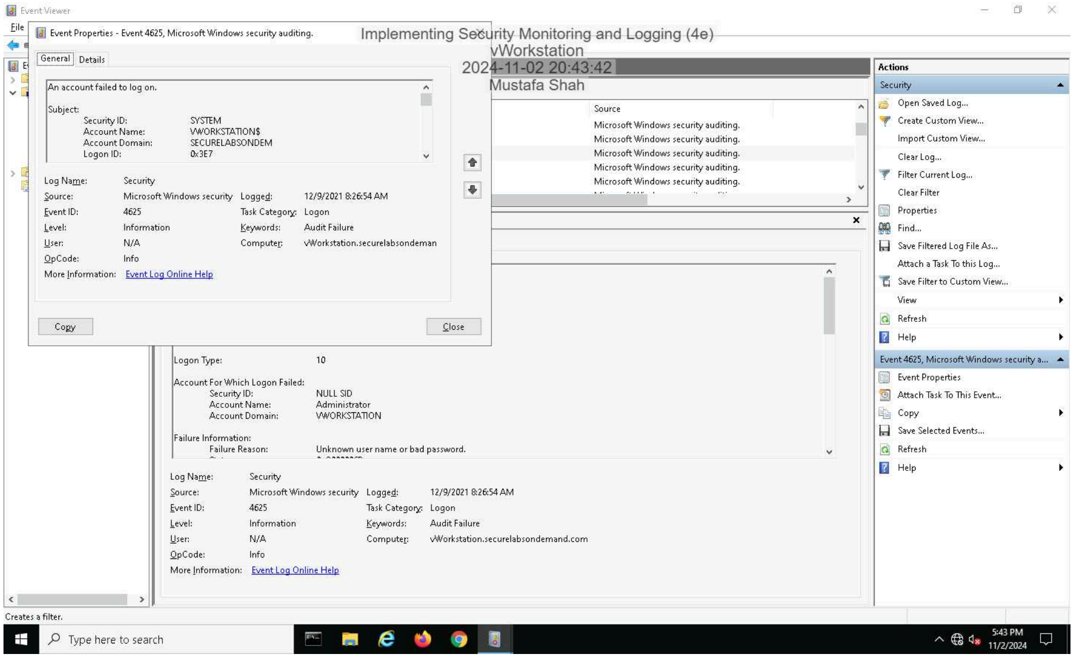
Time on Task:	Progress:
4 hours, 4 minutes	100%

Report Generated: Monday, November 4, 2024 at 8:53 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**.



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 20:43:42
Mustafa Shah

Event Properties - Event 4625, Microsoft Windows security auditing.

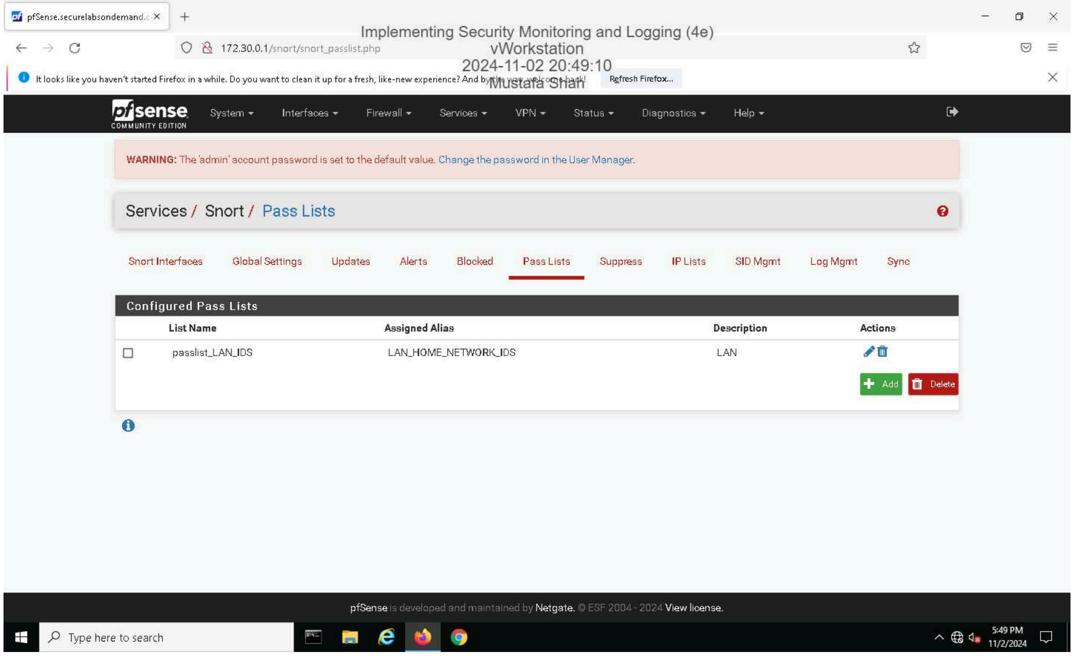
```
An account failed to log on.

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
```

```
Logon Type:                     10

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           Administrator
        Account Domain:         VWORKSTATION

Failure Information:
        Failure Reason:         Unknown user name or bad password.

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
```

Event Viewer
File
General
Details
Copy
Close
Source
Microsoft Windows security auditing.
Microsoft Windows security auditing.
Microsoft Windows security auditing.
Microsoft Windows security auditing.
Microsoft Windows security auditing.
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help
Event 4625, Microsoft Windows security a...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help
Creates a filter.
Type here to search
5:43 PM
11/2/2024

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
2024-11-02 20:49:10
Mustafa Shah

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

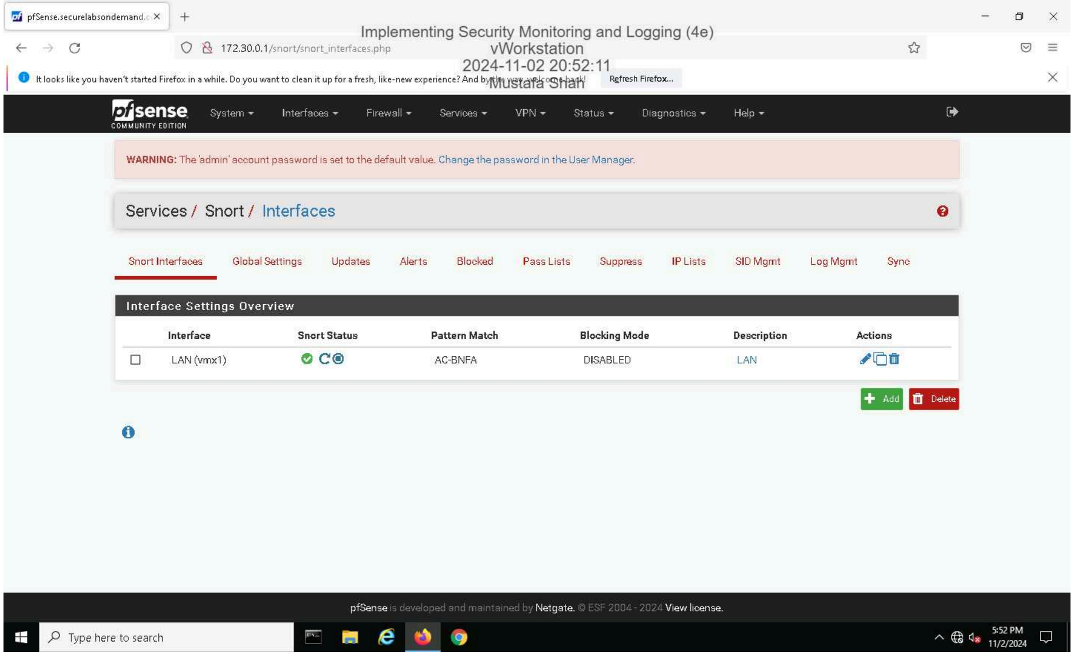
Configured Pass Lists

	List Name	Assigned Alias	Description	Actions
☐	passlist_LAN_IDS	LAN_HOME_NETWORK_IDS	LAN	

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

5:49 PM
11/2/2024

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



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 20:52:11
Mustafa Shah

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

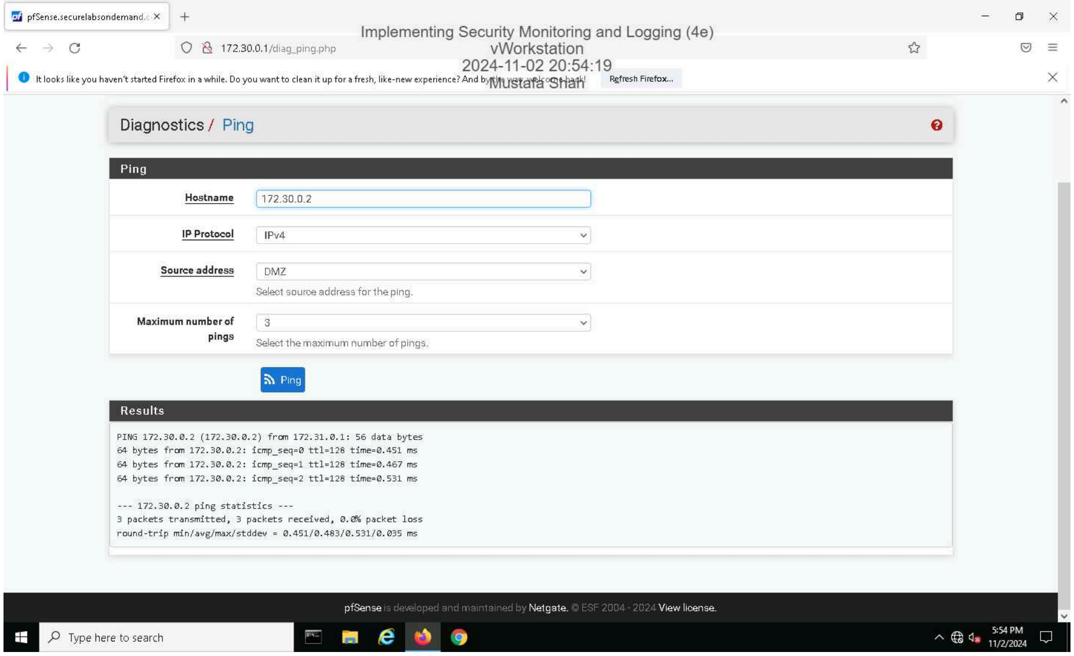
Interface Settings Overview

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

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

5:52 PM
11/2/2024

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



pfSense.securelabsondemand.c
172.30.0.1/diag_ping.php
Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 20:54:19
Mustafa Shah
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!
Refresh Firefox...
Type here to search
5:54 PM
11/2/2024

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.

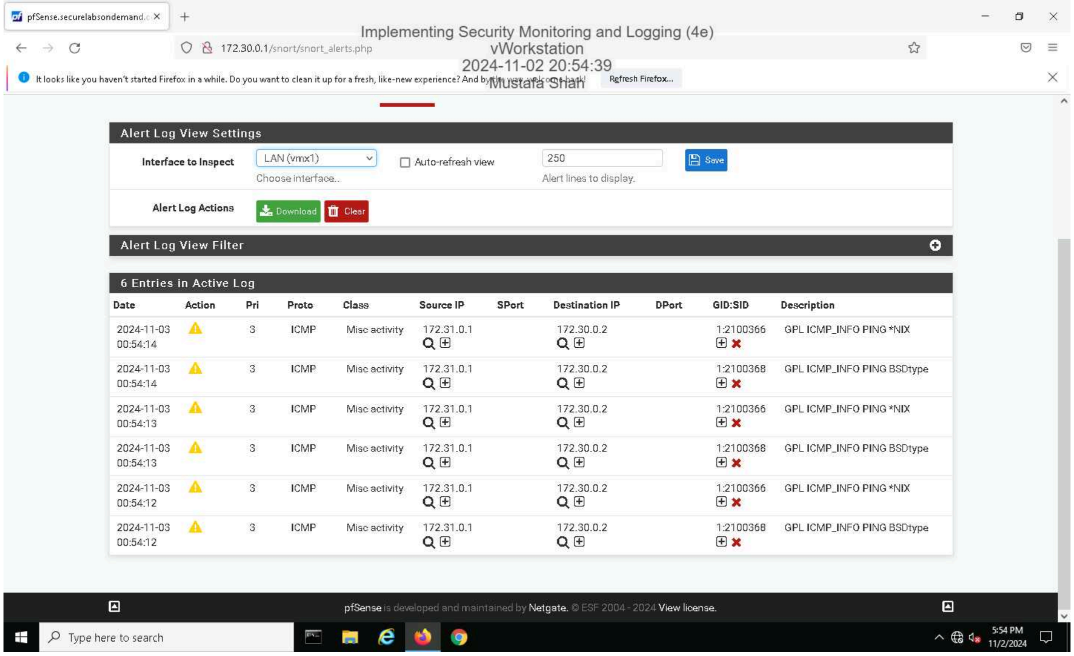
Ping

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=0.451 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.467 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.531 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.451/0.483/0.531/0.035 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**.



pfSense.securelabsondemand.c
172.30.0.1/snort/snort_alerts.php
Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 20:54:39
Mustafa Shah
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!
Refresh Firefox...
Type here to search
5:54 PM
11/2/2024

Alert Log View Settings

Interface to Inspect	LAN (vmx1) Choose interface..	□ Auto-refresh view	250 Alert lines to display.
Alert Log Actions	Download Clear		

Save

Alert Log View Filter

6 Entries in Active Log

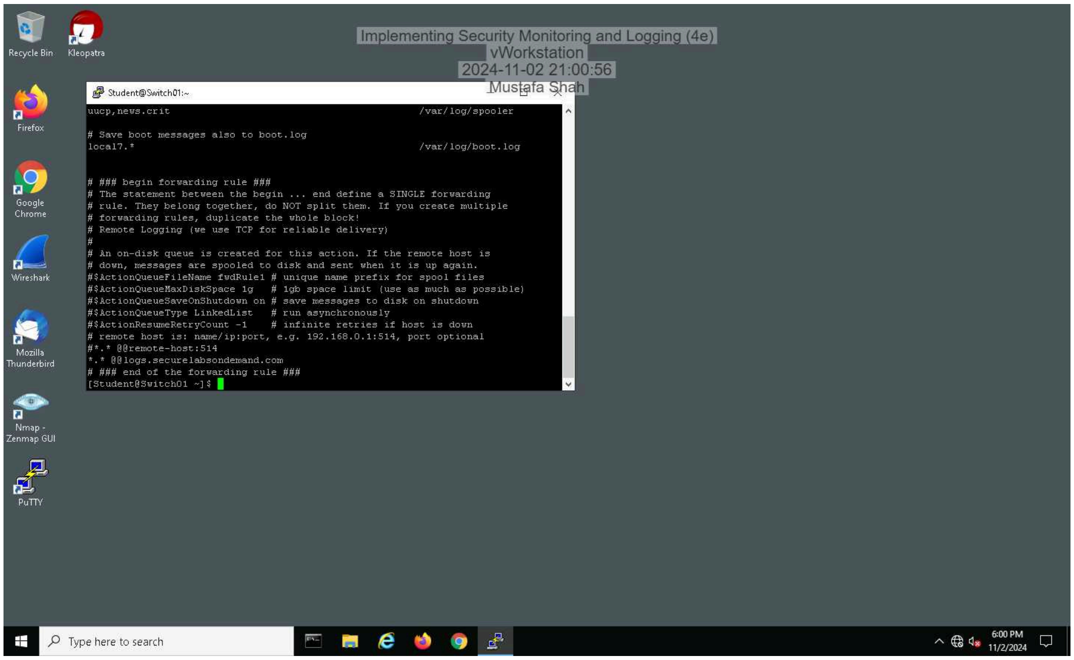
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-03 00:54:14	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-11-03 00:54:14	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2024-11-03 00:54:13	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-11-03 00:54:13	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2024-11-03 00:54:12	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2024-11-03 00:54:12	⚠	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

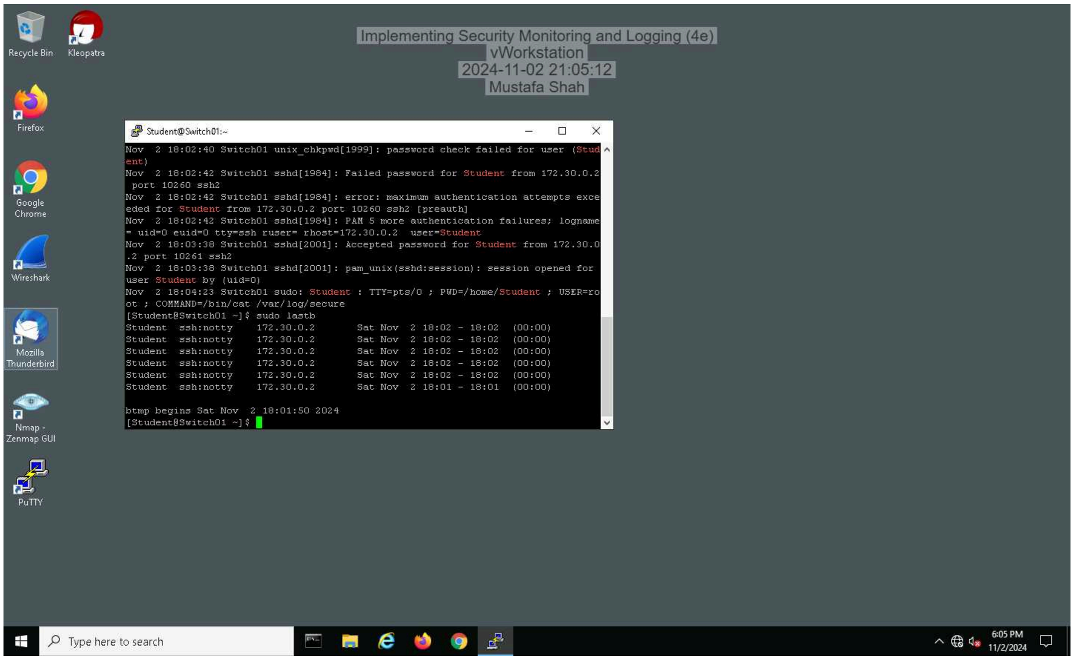
10. **Make a screen capture** showing the **edited rsyslog.conf file**.



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 21:00:56
Mustafa Shah

```
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
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
*.* @@logs.securelabsondemand.com
# ### end of the forwarding rule ###
[Student@Switch01 ~]$
```

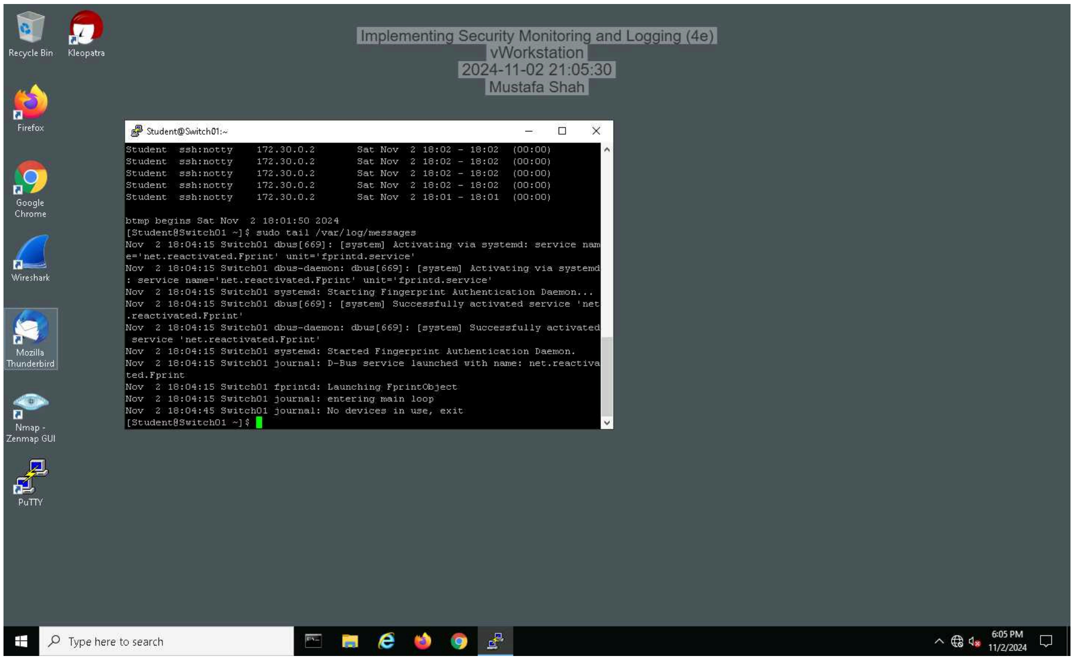
20. **Make a screen capture** showing the **failed login attempts**.



Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 21:05:12
Mustafa Shah

```
Nov  2 18:02:40 Switch01 unix_chkpwd[1999]: password check failed for user (Stud
ent)
Nov  2 18:02:42 Switch01 sshd[1984]: Failed password for Student from 172.30.0.2
 port 10260 ssh2
Nov  2 18:02:42 Switch01 sshd[1984]: error: maximum authentication attempts exce
eded for Student from 172.30.0.2 port 10260 ssh2 [preauth]
Nov  2 18:02:42 Switch01 sshd[1984]: PAM 5 more authentication failures; logname
= uid=0 euid=0 tty=ssh ruser= rhost=172.30.0.2  user=Student
Nov  2 18:03:38 Switch01 sshd[2001]: Accepted password for Student from 172.30.0
.2 port 10261 ssh2
Nov  2 18:03:38 Switch01 sshd[2001]: pam_unix(sshd:session): session opened for
user Student by (uid=0)
Nov  2 18:04:23 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       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:01 - 18:01  (00:00)

btmp begins Sat Nov  2 18:01:50 2024
[Student@Switch01 ~]$
```

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

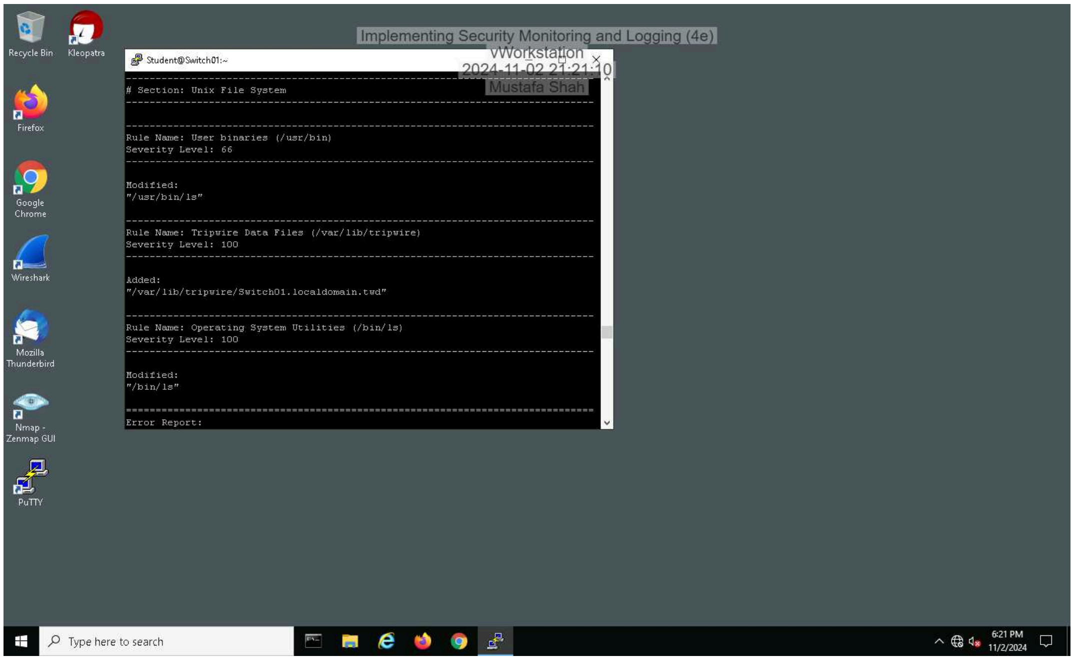


Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 21:05:30
Mustafa Shah

```
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:02 - 18:02  (00:00)
Student  ssh:notty    172.30.0.2       Sat Nov  2 18:01 - 18:01  (00:00)

btmp begins Sat Nov  2 18:01:50 2024
[Student@Switch01 ~]$ sudo tail /var/log/messages
Nov  2 18:04:15 Switch01 dbus[669]: [system] Activating via systemd: service nam
e='net.reactivated.Fprint' unit='fprintd.service'
Nov  2 18:04:15 Switch01 dbus-daemon: dbus[669]: [system] Activating via systemd
: service name='net.reactivated.Fprint' unit='fprintd.service'
Nov  2 18:04:15 Switch01 systemd: Starting Fingerprint Authentication Daemon...
Nov  2 18:04:15 Switch01 dbus[669]: [system] Successfully activated service 'net
.reactivated.Fprint'
Nov  2 18:04:15 Switch01 dbus-daemon: dbus[669]: [system] Successfully activated
 service 'net.reactivated.Fprint'
Nov  2 18:04:15 Switch01 systemd: Started Fingerprint Authentication Daemon.
Nov  2 18:04:15 Switch01 journal: D-Bus service launched with name: net.reactiva
ted.Fprint
Nov  2 18:04:15 Switch01 fprintd: Launching FprintObject
Nov  2 18:04:15 Switch01 journal: entering main loop
Nov  2 18:04:45 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**.



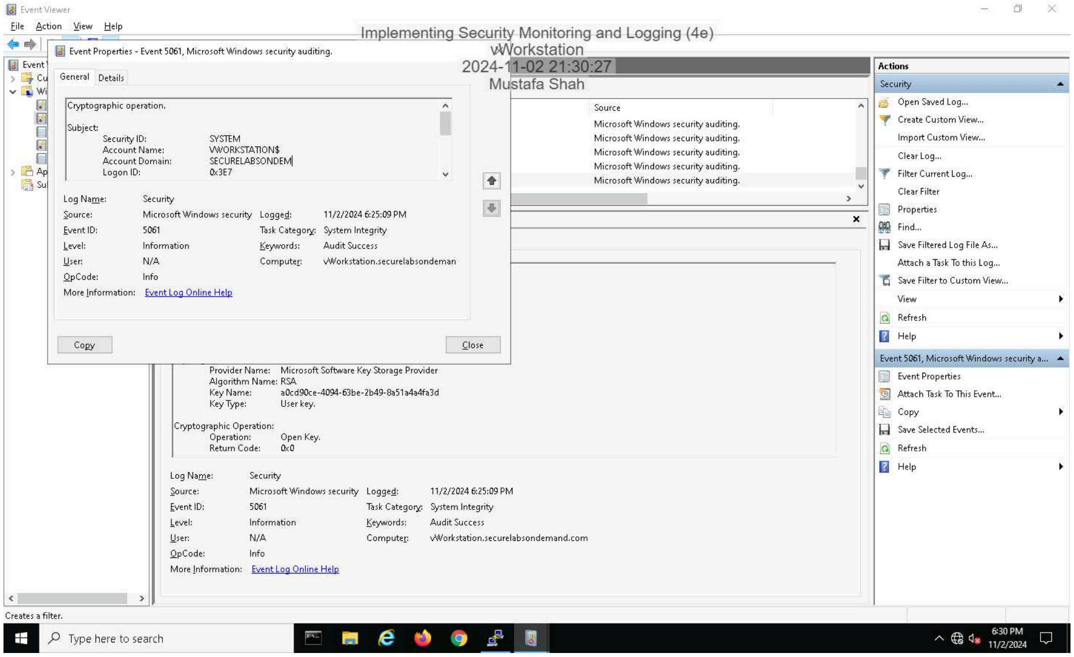
Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 21:21:10
Mustafa Shah

```
-------------------------------------------------------------------------------
# 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
-------------------------------------------------------------------------------

Modified:
"/bin/ls"

===============================================================================
Error Report:
```

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**.



```
Cryptographic operation.

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

Log Name:          Security
Source:            Microsoft Windows security   Logged:          11/2/2024 6:25:09 PM
Event ID:          5061                         Task Category:   System Integrity
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        vWorkstation.securelabsondeman
OpCode:            Info
More Information:  Event Log Online Help
```

```
Microsoft Windows security auditing.
Microsoft Windows security auditing.
Microsoft Windows security auditing.
Microsoft Windows security auditing.
Microsoft Windows security auditing.
```

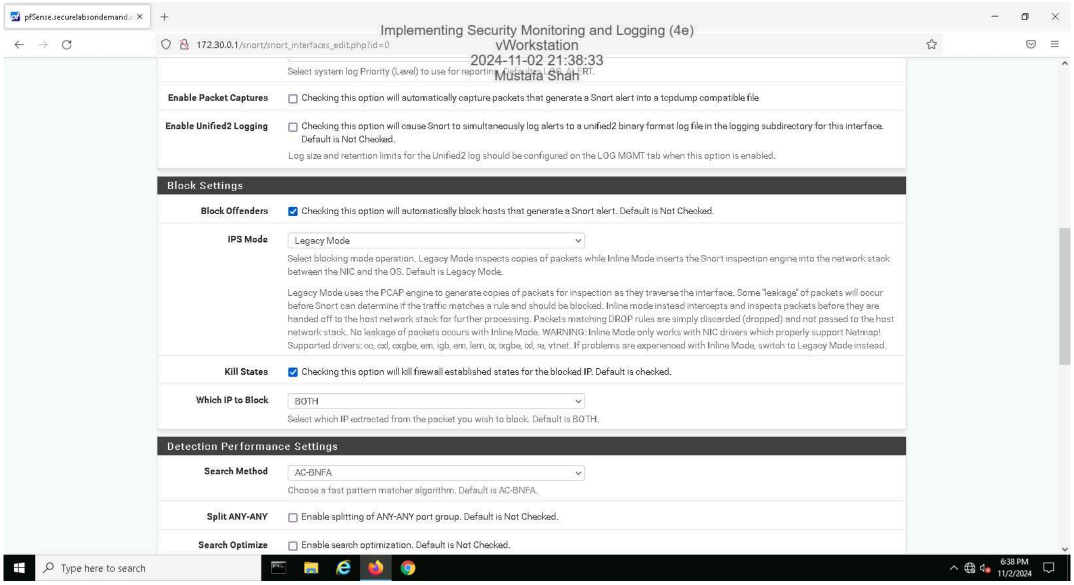
```
        Provider Name:   Microsoft Software Key Storage Provider
        Algorithm Name:  RSA
        Key Name:        a0cd90ce-4094-63be-2b49-8a51a4a4fa3d
        Key Type:        User key.

Cryptographic Operation:
        Operation:       Open Key.
        Return Code:     0x0

Log Name:          Security
Source:            Microsoft Windows security   Logged:          11/2/2024 6:25:09 PM
Event ID:          5061                         Task Category:   System Integrity
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        vWorkstation.securelabsondemand.com
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 is related to the auditing of cryptographic operations in Windows. This event occurs when a protected process or a cryptographic key is accessed or used in an operation, such as encryption, decryption, or signing data. Event ID 5061 is logged when there's an attempt to use a cryptographic key that's managed by the Data Protection API (DPAPI), which is part of Windows' security to protect sensitive data.

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.c
172.30.0.1/snort/snort_interfaces_edit.php?id=0
Implementing Security Monitoring and Logging (4e)
vWorkstation
2024-11-02 21:38:33
Mustafa Shah
Type here to search
6:38 PM
11/2/2024

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.