

Implementing Security Monitoring and Logging (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 08

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

11 hours, 15 minutes

Progress:

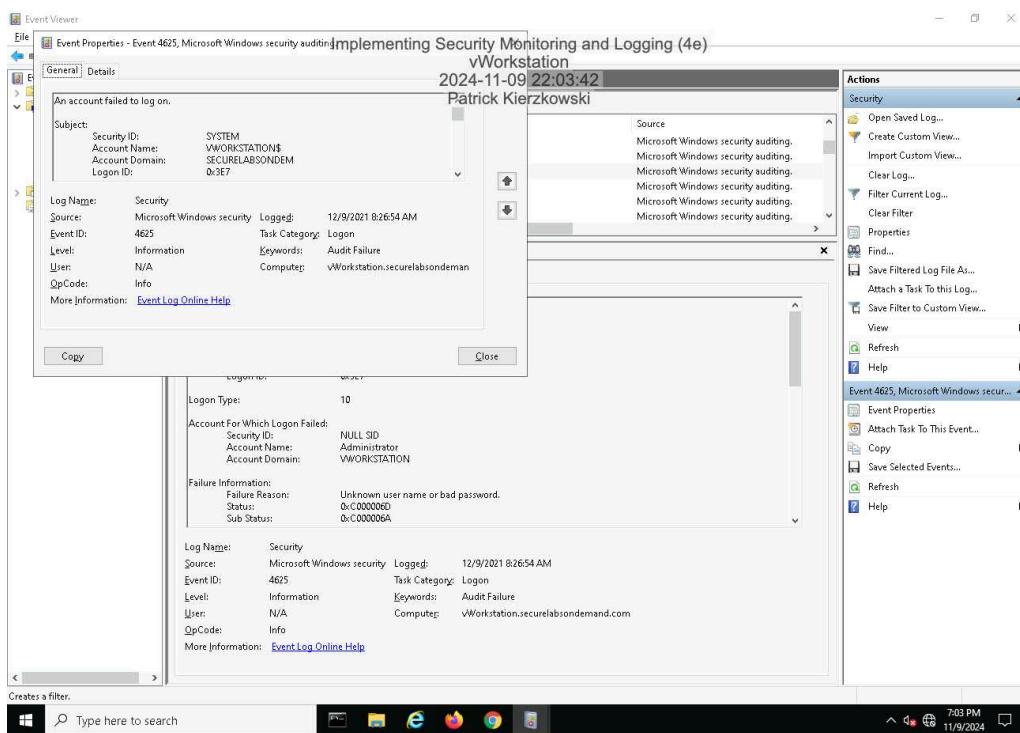
100%

Report Generated: Monday, July 7, 2025 at 9:50 PM

Hands-On Demonstration

Part 1: Identifying Failed Logon Attempts on Windows Systems

8. Make a screen capture showing the **Security Event Properties dialog box** on the vWorkstation.



Part 2: Monitoring Network Activity with Snort

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

The screenshot shows the pfSense web interface for Snort Pass Lists. The URL is 172.30.0.1/snort/snort_passlist.php. The page title is "Implementing Security Monitoring and Logging (4e) vWorkstation 2024-11-09 22:21:20". A warning message at the top says, "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Pass Lists" tab is selected in the navigation bar. The main content area displays a table titled "Configured Pass Lists" with one entry:

List Name	Assigned Alias	Description	Actions
passlist_LAN_IDS	LAN_HOME_NETWORK_IDS	LAN	

At the bottom right of the table are "Add" and "Delete" buttons. The browser's address bar shows "pfSense.securelabsondemand.com" and the status bar indicates "7:21 PM 11/9/2024".

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

The screenshot shows the pfSense web interface for Snort Interfaces. The URL is 172.30.0.1/snort/snort_interfaces.php. The page title is "Implementing Security Monitoring and Logging (4e) vWorkstation 2024-11-09 22:40:13". A warning message at the top says, "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Snort Interfaces" tab is selected in the navigation bar. The main content area displays a table titled "Interface Settings Overview" with one entry:

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

At the bottom right of the table are "Add" and "Delete" buttons. The browser's address bar shows "pfSense.securelabsondemand.com" and the status bar indicates "7:40 PM 11/9/2024".

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

The screenshot shows the pfSense web interface with the title "Implementing Security Monitoring and Logging (4e)". The main content area is titled "Diagnostics / Ping". In the "Ping" section, the "Hostname" field is set to "172.30.0.2", "IP Protocol" is "IPv4", "Source address" is "DMZ", and "Maximum number of pings" is set to "3". Below these fields is a "Ping" button. The "Results" section displays the output of a ping command:

```
PING 172.30.0.2 (172.31.0.1) 56 data bytes
64 bytes from 172.30.0.2: icmp_seq=0 ttl=128 time=8.744 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.578 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.612 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.578/3.311/8.744/3.842 ms
```

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

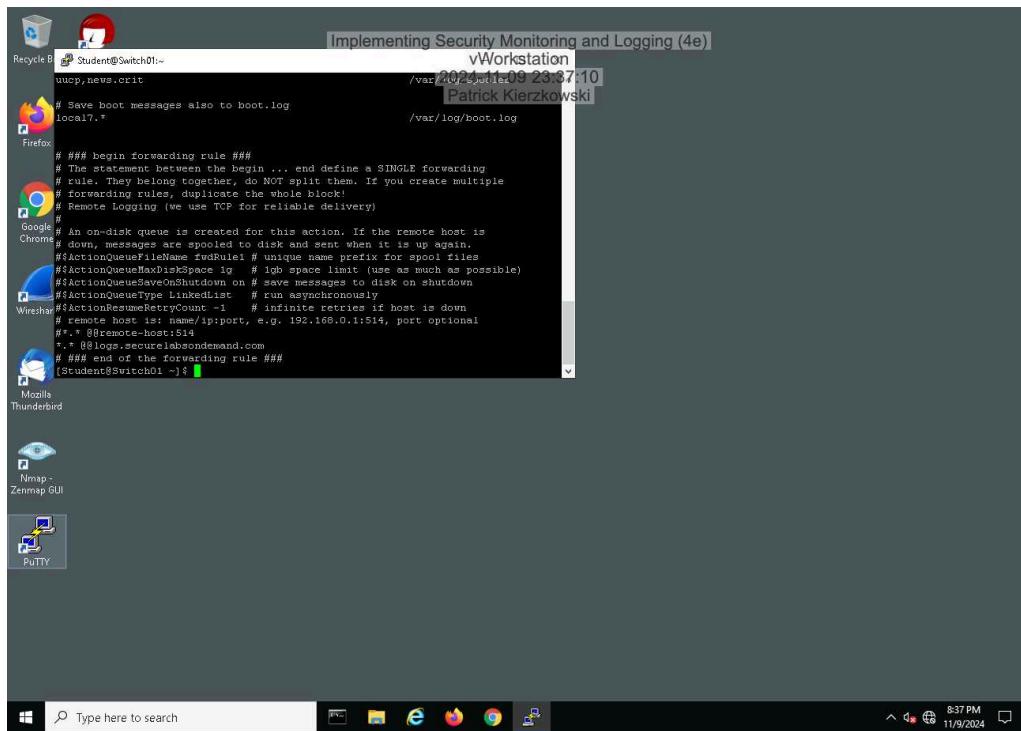
The screenshot shows the pfSense web interface with the title "Implementing Security Monitoring and Logging (4e)". The main content area is titled "Snort Interfaces". The "Alerts" tab is selected. The "Alert Log View Settings" section shows "Interface to Inspect" as "LAN (vmx1)", "Auto-refresh view" checked, and "250" alert lines to display. Below this is the "Alert Log Actions" section with "Download" and "Clear" buttons. The "Alert Log View Filter" section has a "6 Entries in Active Log" table:

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-10 03:41:55	⚠️	3	ICMP	Misc activity	172.31.0.1	Q ⊕	172.30.0.2	Q ⊕	1:2100366	GPL ICMP_INFO PING *NDX
2024-11-10 03:41:55	⚠️	3	ICMP	Misc activity	172.31.0.1	Q ⊕	172.30.0.2	Q ⊕	1:2100368	GPL ICMP_INFO PING BSDtype
2024-11-10 03:41:54	⚠️	3	ICMP	Misc activity	172.31.0.1	Q ⊕	172.30.0.2	Q ⊕	1:2100366	GPL ICMP_INFO PING *NDX
2024-11-10 03:41:54	⚠️	3	ICMP	Misc activity	172.31.0.1	Q ⊕	172.30.0.2	Q ⊕	1:2100368	GPL ICMP_INFO PING BSDtype
2024-11-10 03:41:53	⚠️	3	ICMP	Misc activity	172.31.0.1	Q ⊕	172.30.0.2	Q ⊕	1:2100366	GPL ICMP_INFO PING *NDX
2024-11-10 03:41:53	⚠️	3	ICMP	Misc activity	172.31.0.1	Q ⊕	172.30.0.2	Q ⊕	1:2100368	GPL ICMP_INFO PING BSDtype

Applied Learning

Part 1: Identifying Failed Logon Attempts on Linux Systems

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



The screenshot shows a Windows desktop with a terminal window open. The terminal window title is "Implementing Security Monitoring and Logging (4e)" and the command run is "cat /etc/rsyslog.conf". The terminal content displays the configuration for rsyslog, including rules for local logs and remote forwarding. The desktop background is dark, and various icons for applications like Firefox, Google Chrome, and Putty are visible in the taskbar.

```
# 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.
#$ActionQueueName fwdRule1 # unique name prefix for spool files
#$ActionQueueDiskSize 1G      # high space limit (use as much as possible)
#$ActionQueueShutdownOn 0      # 0=keep messages to disk on shutdown
#$ActionQueueType LinkedList # run asynchronously
#$ActionQueueRetryCount -1    # infinite retries if host is down
# $remoteHost is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule #####
#
```

22. Make a screen capture showing the failed login attempts.

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Student@Switch01:~". The terminal displays several failed password attempts for the user "Student" from an IP address 172.30.0.2. The log entries are as follows:

```
Nov 9 20:40:17 Switch01 sshd[3149]: Failed password for Student from 172.30.0.2 port 20254 ssh2
Nov 9 20:40:17 Switch01 sshd[3149]: error: maximum authentication attempts exceeded for Student from 172.30.0.2 port 20254 ssh2 [preauth]
Nov 9 20:41:02 Switch01 sshd[3149]: pam_unix(sshd:session): session opened for user Student by (uid=0)
Nov 9 20:41:02 Switch01 sshd[3177]: Accepted password for Student from 172.30.0.2 port 20255 ssh2
Nov 9 20:41:02 Switch01 sudo: Student : TTY=pts/0 ; PWD=/home/Student ; USER=root
ot: COMMAND=/bin/cat /var/log/secure
[Student@Switch01 ~]$ sudo lastb
Student sshnotty 172.30.0.2 Sat Nov 9 20:40 - 20:45 (00:05)
Student sshnotty 172.30.0.2 Sat Nov 9 20:45 - 20:45 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:45 - 20:45 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:40 (00:01)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:39 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:39 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:39 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:34 - 20:34 (00:00)
btmp begins Sat Nov 9 20:34:58 2024
[Student@Switch01 ~]$
```

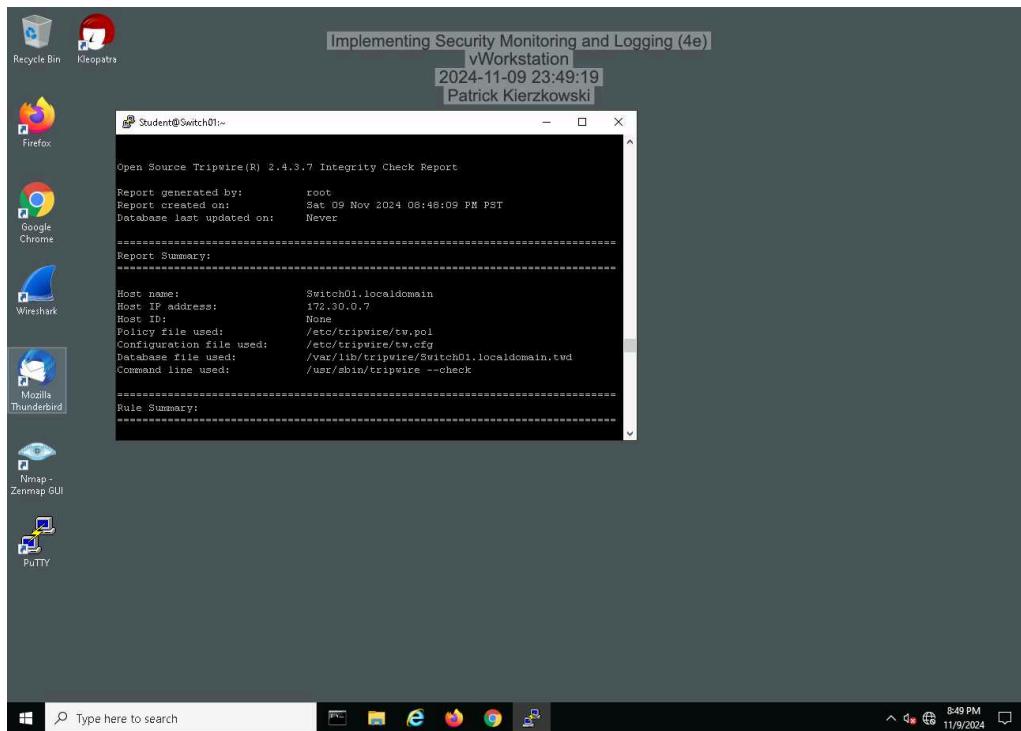
24. Make a screen capture showing the last 10 log messages.

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Student@Switch01:~". The terminal displays the last 10 log messages from the system log file. The log entries are as follows:

```
Student sshnotty 172.30.0.2 Sat Nov 9 20:40 - 20:40 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:39 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:39 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:39 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:39 - 20:39 (00:00)
Student sshnotty 172.30.0.2 Sat Nov 9 20:34 - 20:34 (00:00)
btmp begins Sat Nov 9 20:34:58 2024
[Student@Switch01 ~]$ sudo tail /var/log/messages
Nov 9 20:41:32 Switch01 dbus[663]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service'
Nov 9 20:41:32 Switch01 dbus-daemon: dbus[663]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service'
Nov 9 20:41:32 Switch01 systemd: Starting Fingerprint Authentication Daemon...
Nov 9 20:41:32 Switch01 dbus[663]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 9 20:41:32 Switch01 dbus-daemon: dbus[663]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 9 20:41:32 Switch01 systemd: Started Fingerprint Authentication Daemon.
Nov 9 20:41:32 Switch01 journal: D-Bus service launched with name: net.reactivated.Fprint
Nov 9 20:41:32 Switch01 fprintd: Launching FprintObject
Nov 9 20:41:32 Switch01 journal: entering main loop
Nov 9 20:42:01 Switch01 journal: No devices in use, exit
[Student@Switch01 ~]$
```

Part 2: Monitoring File Integrity with Tripwire

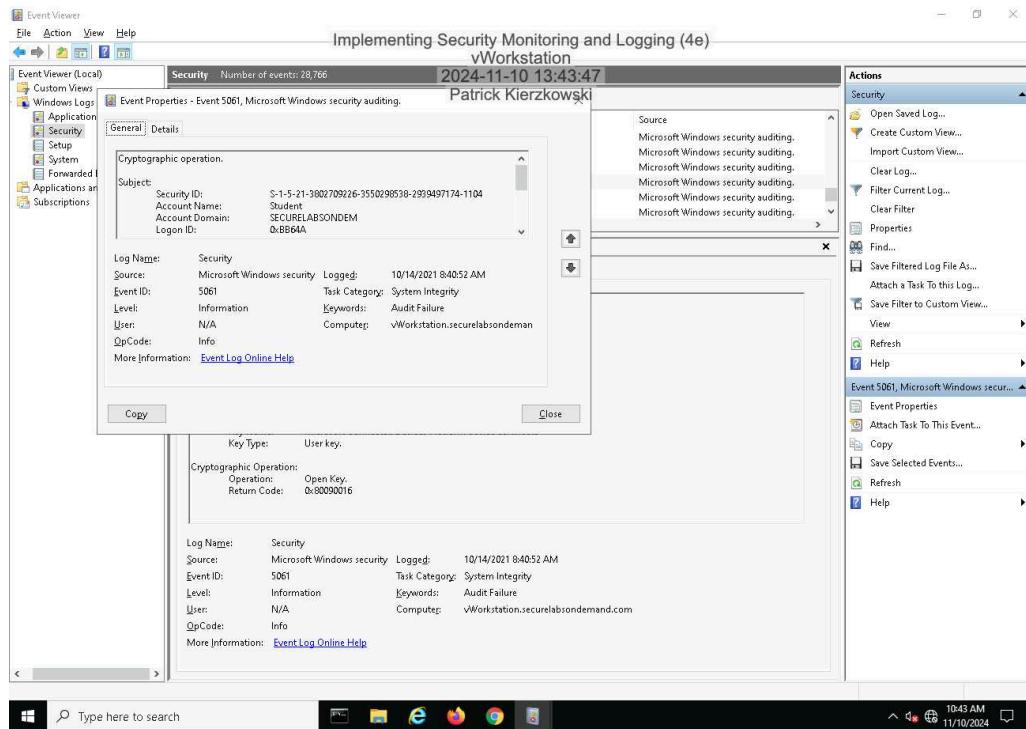
12. Make a screen capture showing the Object Summary section for the Tripwire report.



Challenge and Analysis

Part 1: Identifying 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.

An operation that would generate a security event with Event 5061 is a cryptographic operation. This means that creating, opening or using a key was performed on a system

Part 2: Configuring Snort as an Intrusion Prevention System

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

The screenshot shows the pfSense web interface for managing Snort interfaces. The title bar indicates the page is 'Implementing Security Monitoring and Logging (4e)' and the user is 'Patrick Kierzkowski'. A warning message at the top states: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' The main navigation menu includes 'System', 'Interfaces', 'Firewall', 'Services', 'Status', 'Diagnostics', and 'Help'. Below the menu, the URL is 'Not secure | 172.30.0.1/snort/snort_interfaces.php'.

The current tab is 'Snort Interfaces'. The table below lists the 'Interface Settings Overview' for the 'LAN (vmx1)' interface. The 'Blocking Mode' column shows 'LEGACY MODE'.

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
LAN (vmx1)	ON C@	AC-BNFA	LEGACY MODE	LAN	

At the bottom of the interface, there are buttons for '+ Add' and 'Delete'. The pfSense footer includes the license information: 'pfSense is developed and maintained by Netgate. © ESF 2004-2024 View license.' and the date '11/10/2024'.