Student:	Email:
Roman Cassman	rcassman0001@kctcs.edu

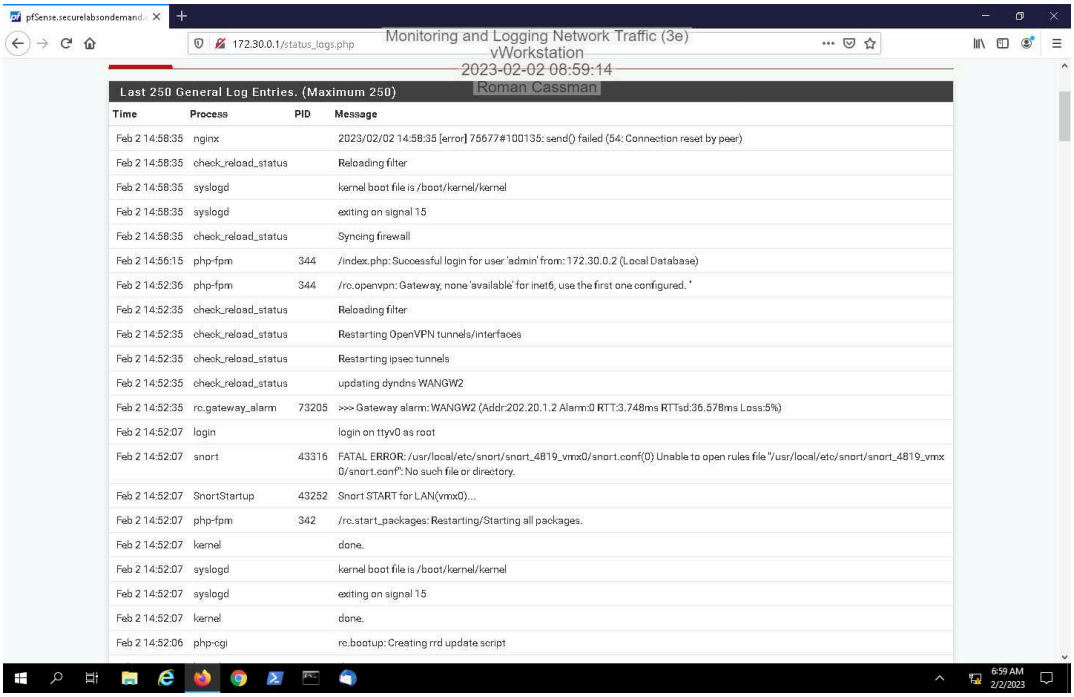
Time on Task:	Progress:
4 hours, 54 minutes	66%

Report Generated: Thursday, February 2, 2023 at 11:06 PM

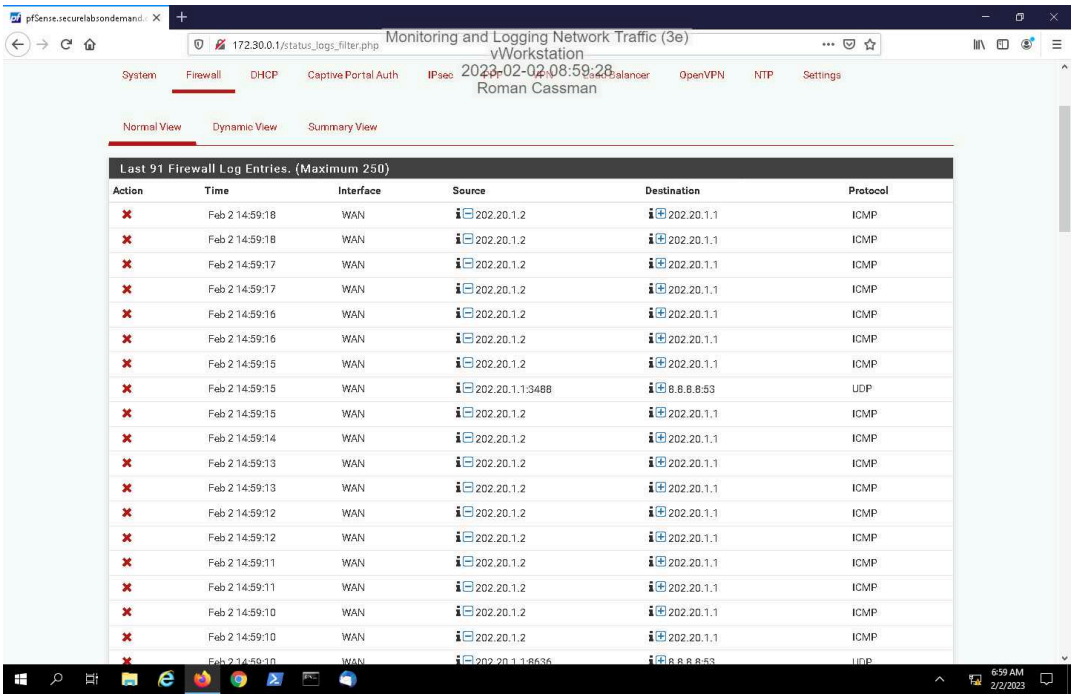
Section 1: Hands-On Demonstration

Part 1: Configure the pfSense Firewall Log

13. **Make a screen capture** showing the **system logs**.

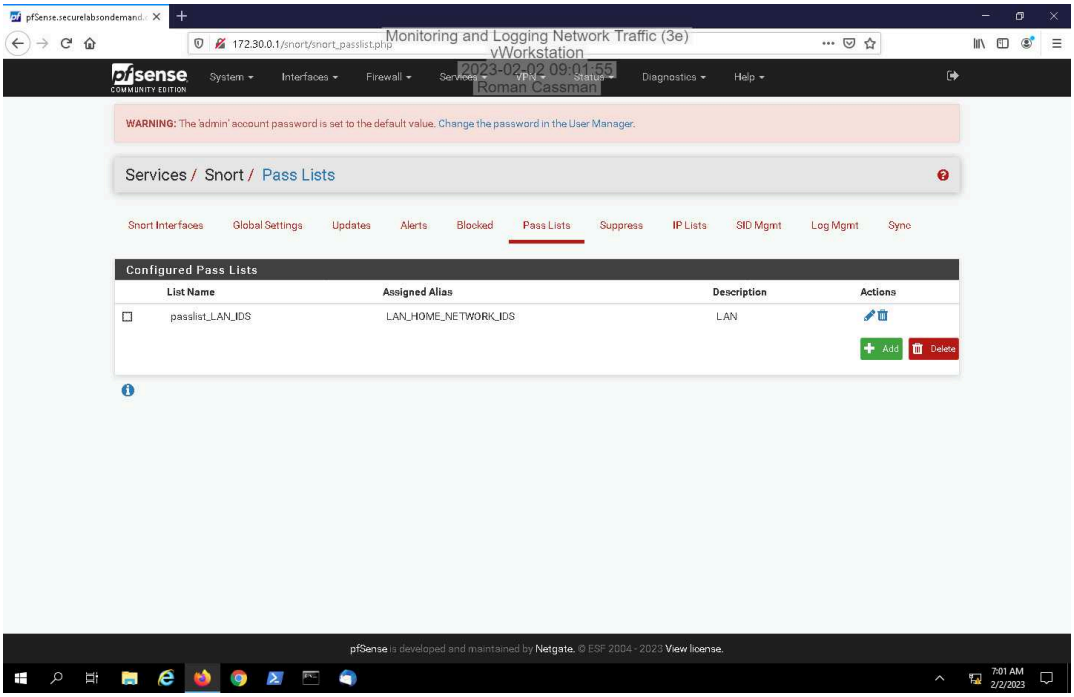


15. **Make a screen capture** showing the **firewall logs**.

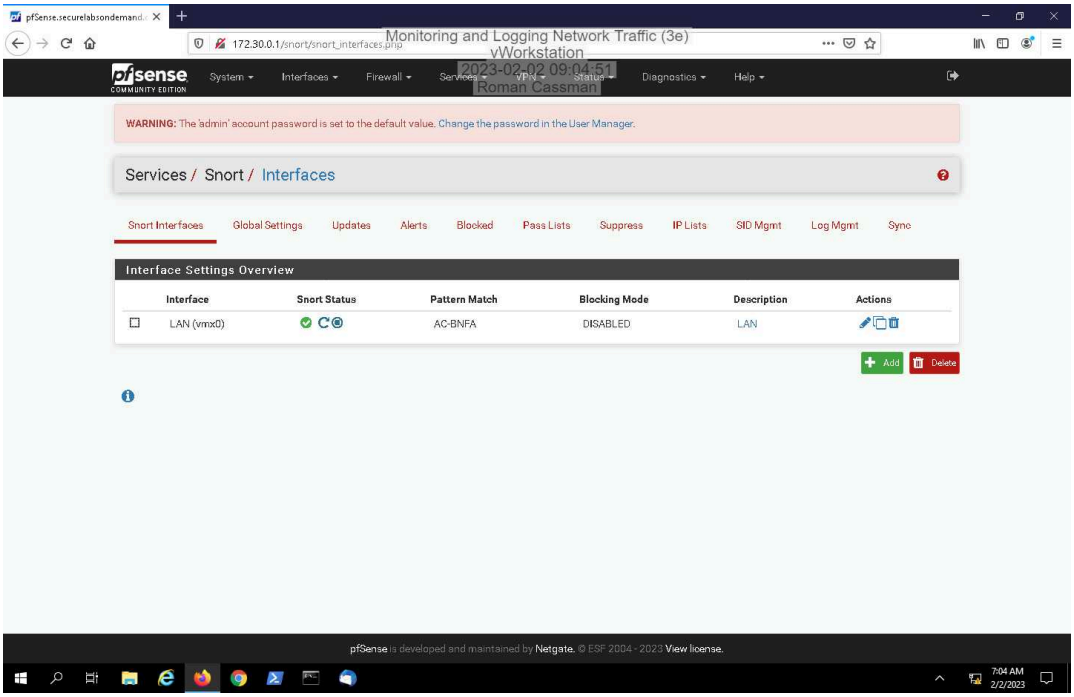


Part 2: Configure a Snort Intrusion Detection System

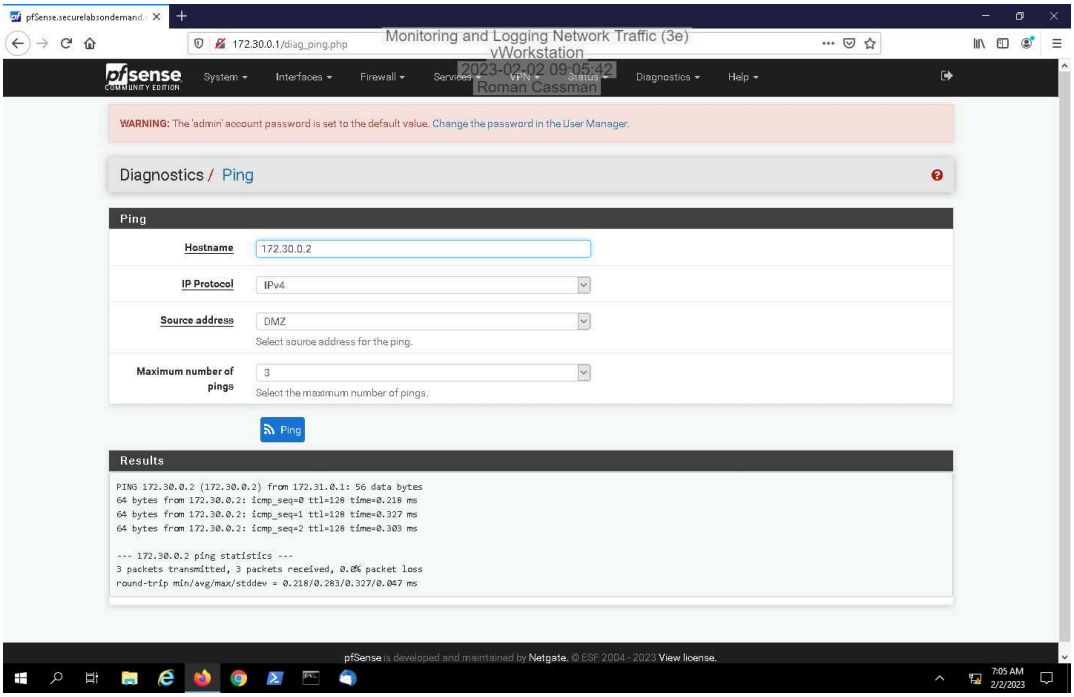
14. **Make a screen capture** showing the **updated Pass Lists page**.



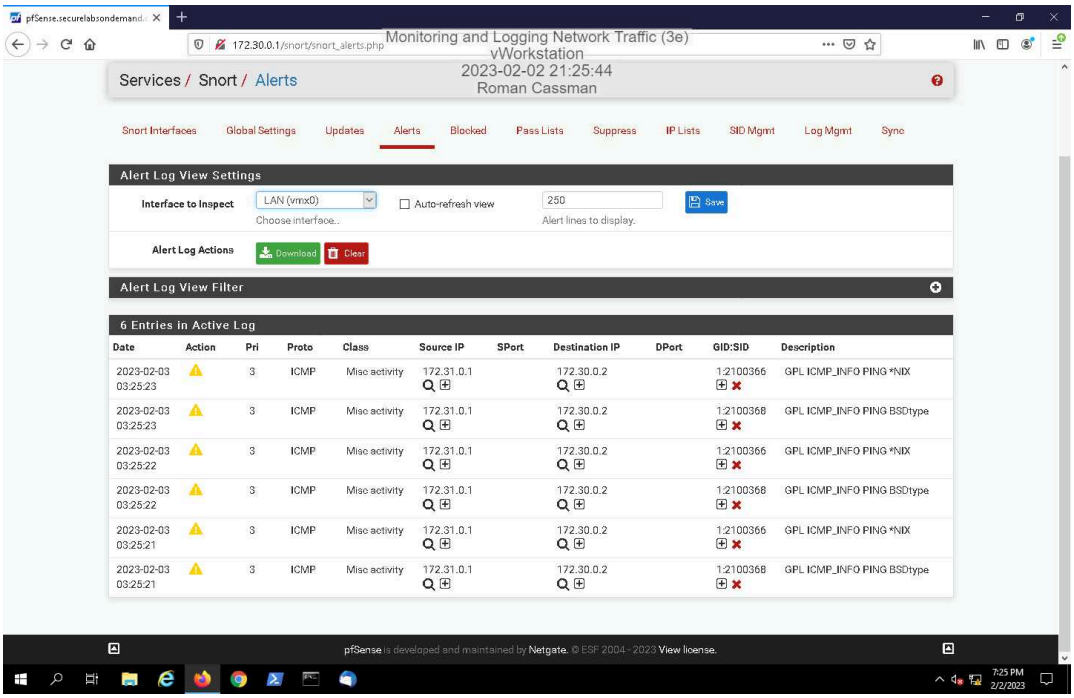
28. **Make a screen capture** showing the **active Snort status on the LAN interface**.



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

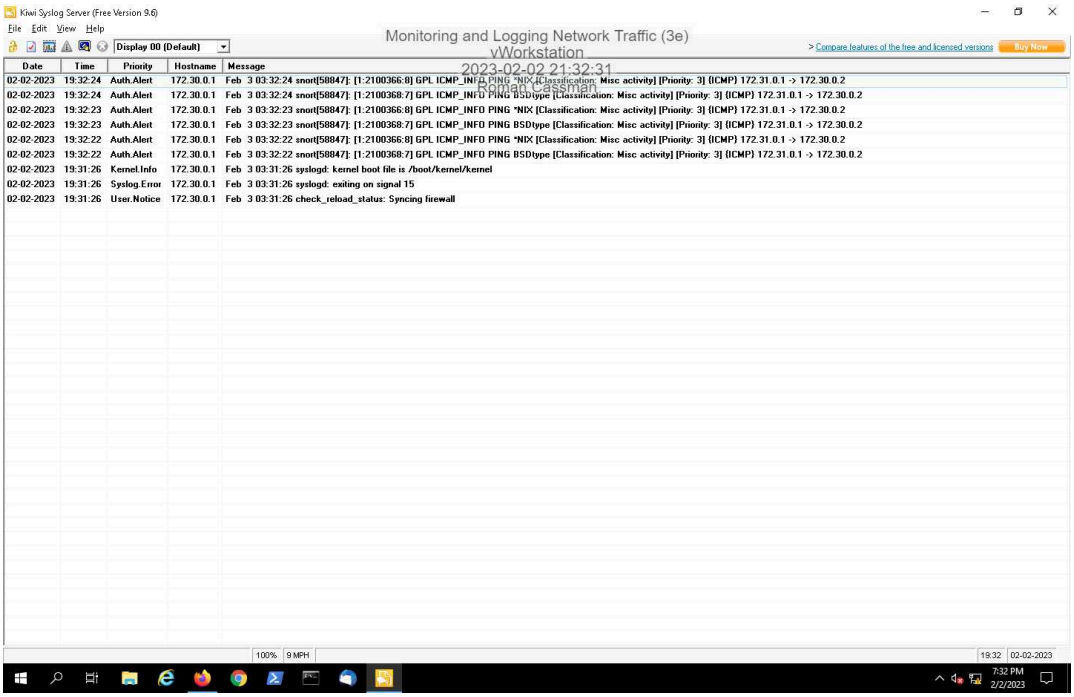


38. **Make a screen capture** showing the **ICMP alerts in the Snort Active Log**.



Part 3: Implement Firewall Log Forwarding with Kiwi Syslog Server

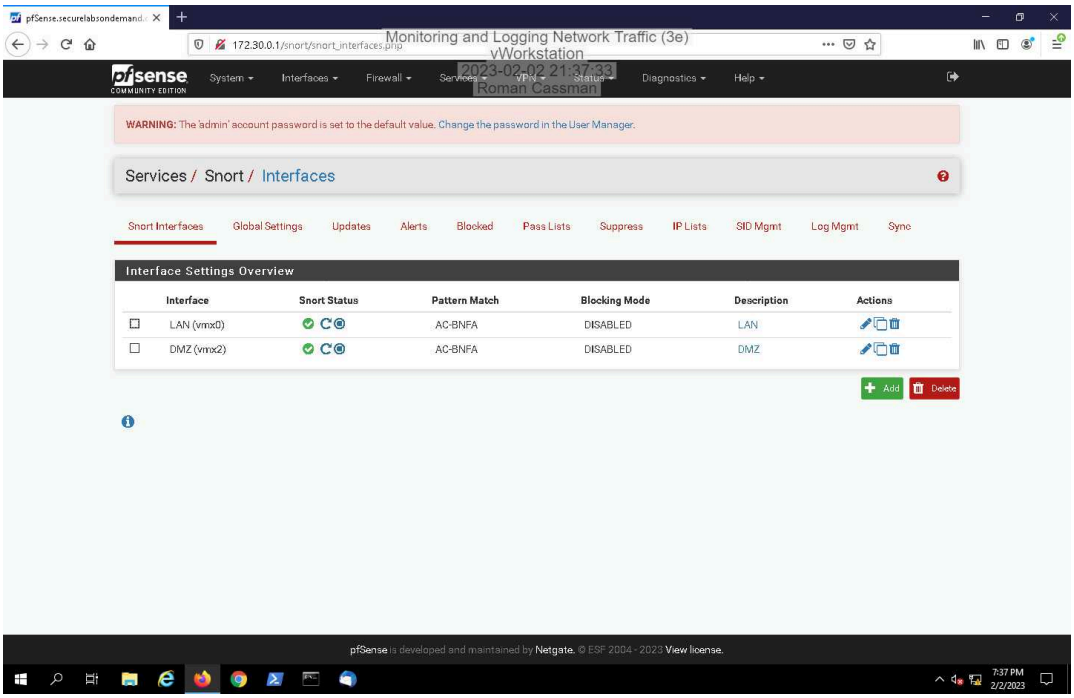
17. **Make a screen capture** showing the **pfSense firewall log events in Kiwi Syslog Server**.



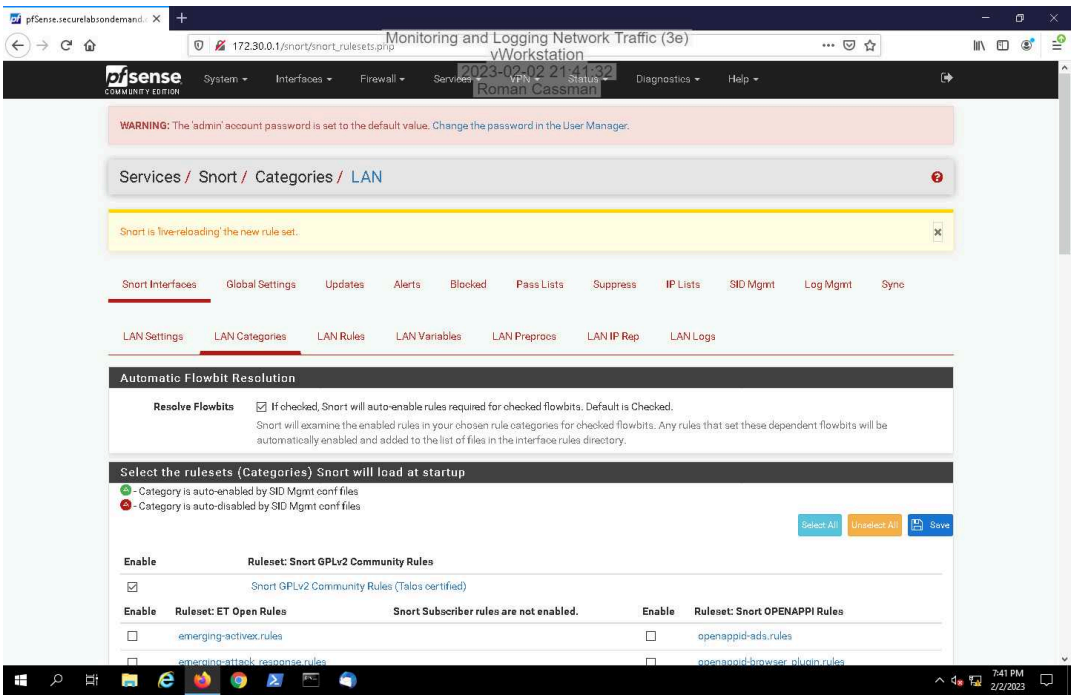
Section 2: Applied Learning

Part 1: Configure Snort Monitoring on the DMZ

17. **Make a screen capture** showing the **active Snort status on the DMZ interface**.

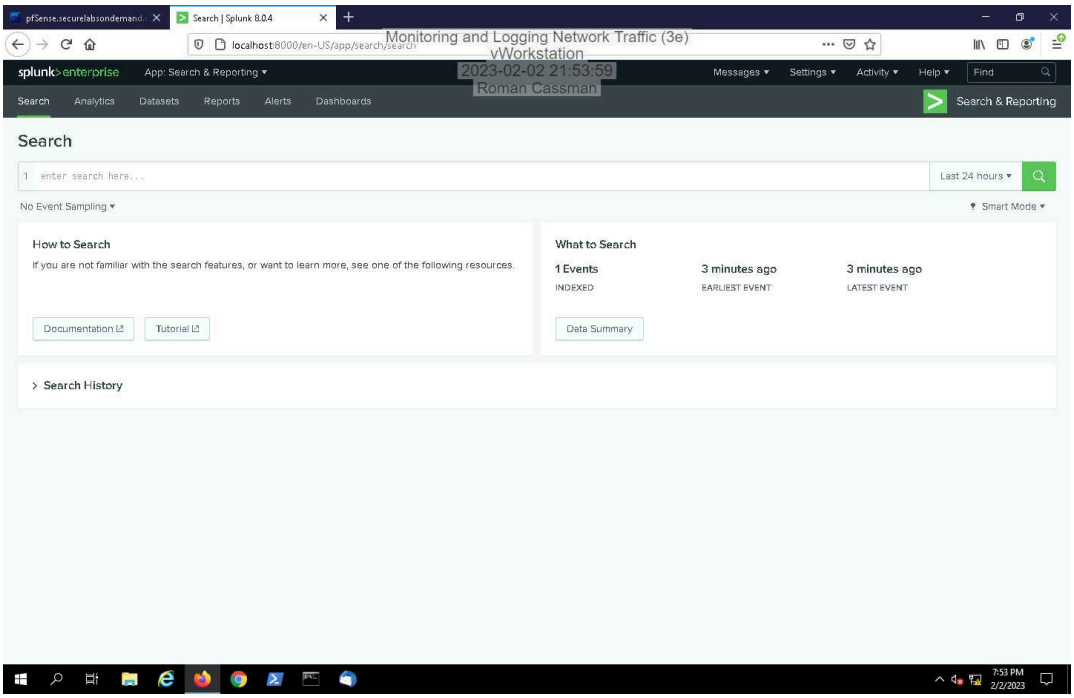


20. **Make a screen capture** showing the **Snort GPLv2 Community Rules enabled and "live-reloading" message**.



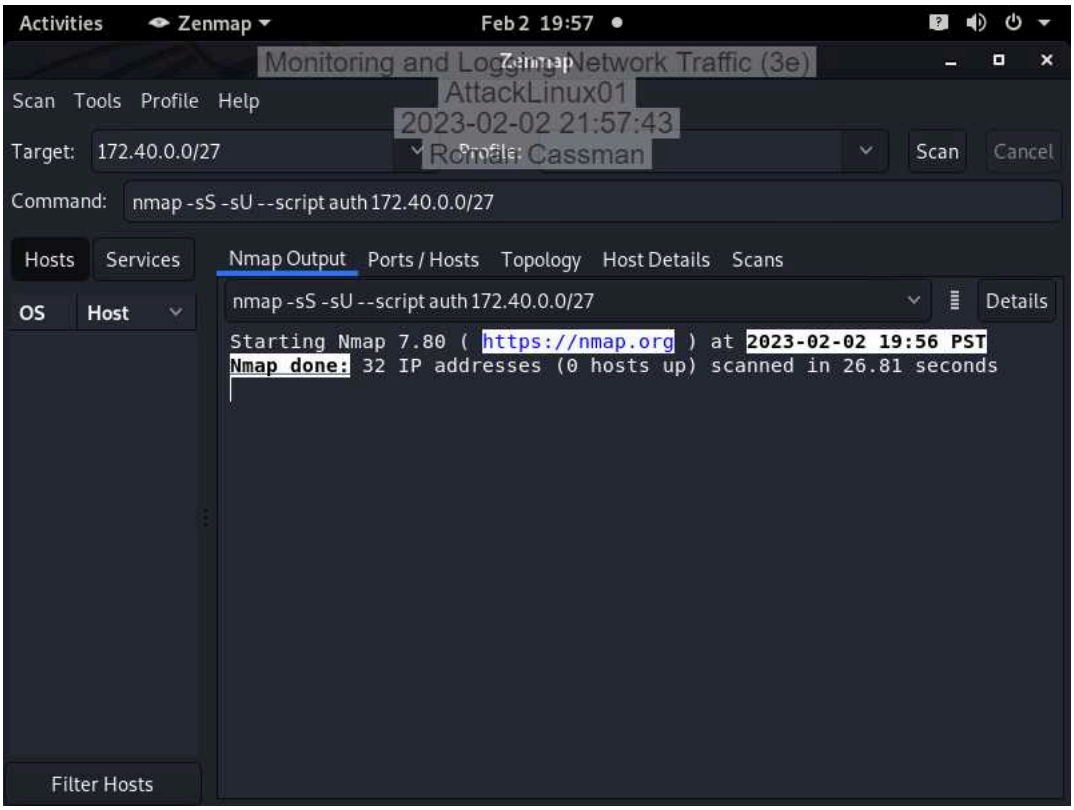
Part 2: Implement Security Information and Event Management with Splunk

13. **Make a screen capture** showing the **indexed events in Splunk**.

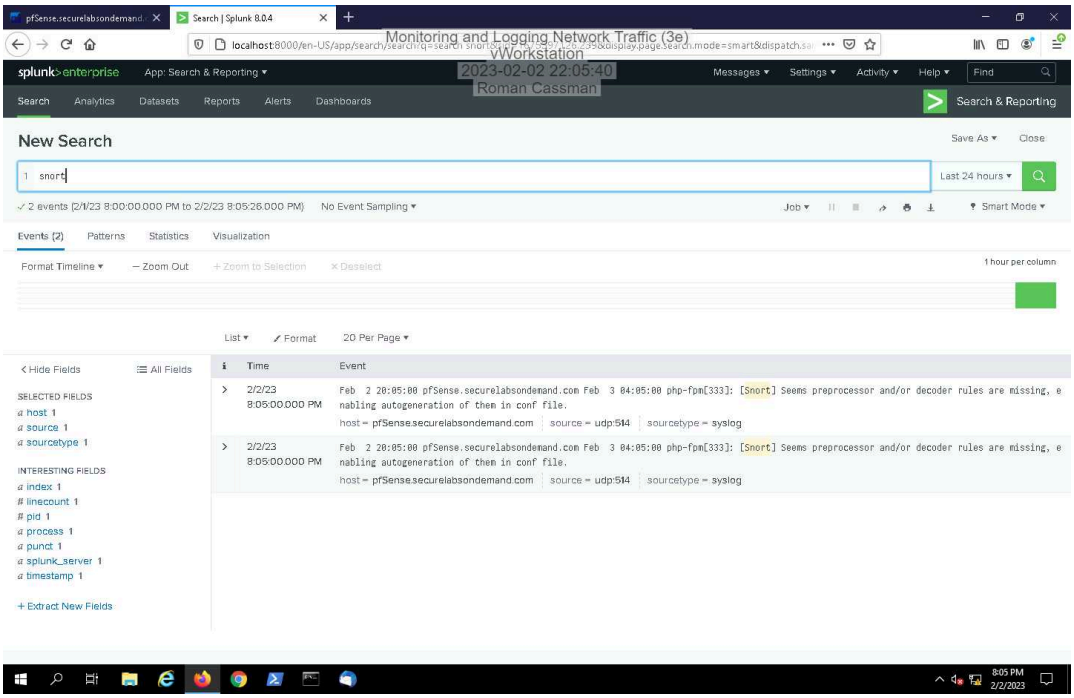


Part 3: Simulate and Detect a Perimeter Network Attack

6. **Make a screen capture** showing the **Nmap scan report**.



9. **Make a screen capture** showing the **search results in Splunk**.



Section 3: Challenge and Analysis

Part 1: Simulate a DMZ Breach with Infection Monkey

Make a screen capture showing the **resulting Infection Map**.

Incomplete

Make a screen capture showing the **resulting Security Report**.

Incomplete

Summarize your DMZ breach simulation results, highlighting what you found to be the greatest concerns from a network monitoring perspective.

Incomplete

Part 2: Detect a Simulated DMZ Breach with Snort and Splunk

Make a screen capture showing the **results of your search query for Infection Monkey traffic in Splunk**.

Incomplete

Describe any concerns about the structure of the query result or the data elements it contains. What data fields would you add, remove, or edit to make log analysis more effective?

Incomplete

Write a brief memo to your manager describing Splunk's usefulness in detecting traces of your simulated breach. What configuration changes would you recommend? How would you enhance its functionality?

Incomplete