Student:	Email:
Brayden Mitchell	brayden.m.mitchell@gmail.com

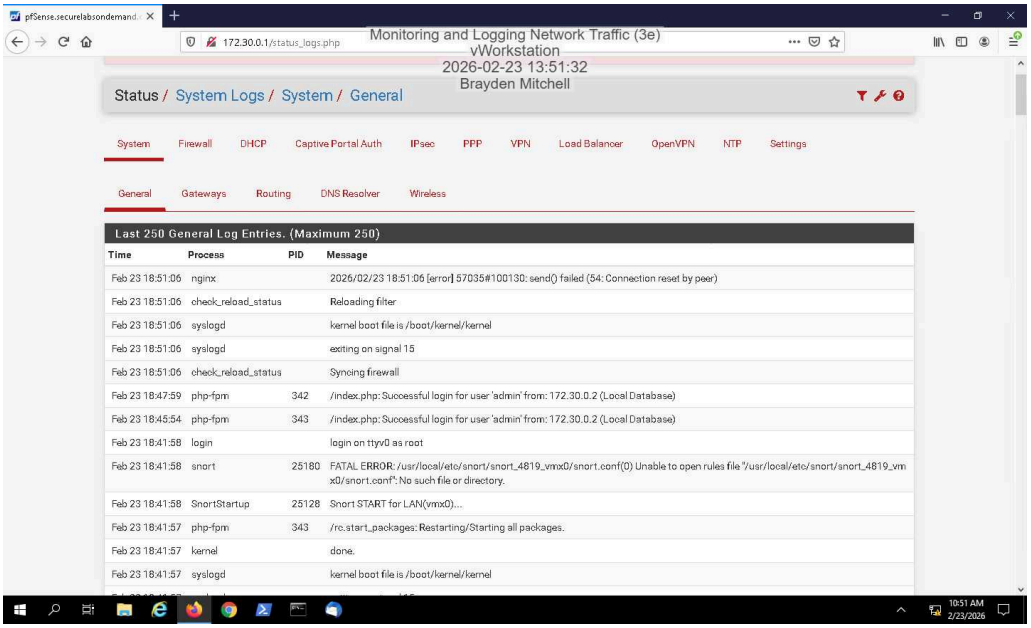
Time on Task:	Progress:
2 hours, 19 minutes	100%

Report Generated: Monday, February 23, 2026 at 4:03 PM

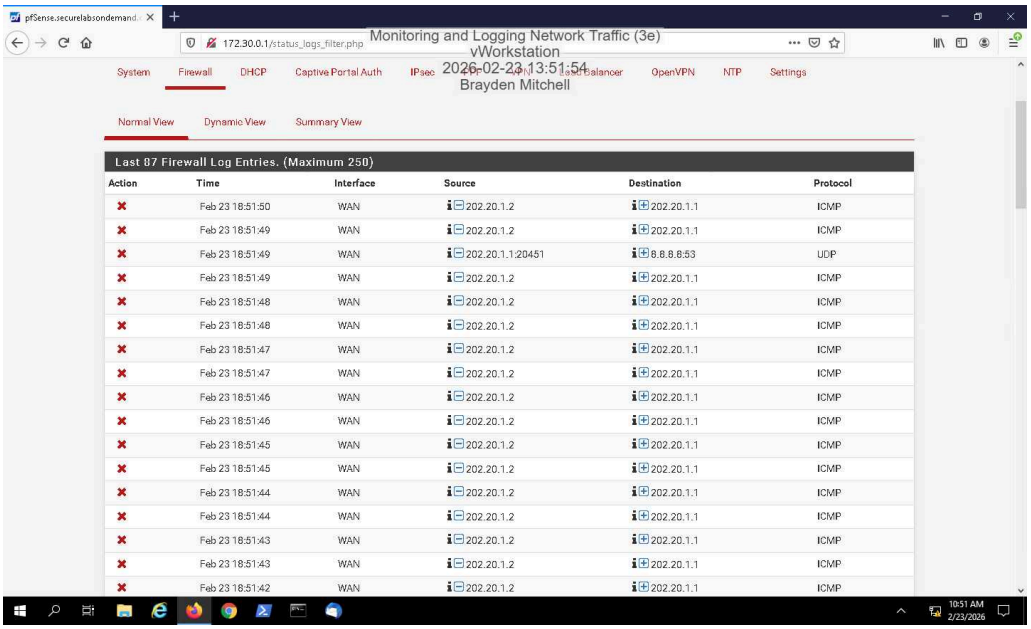
Section 1: Hands-On Demonstration

Part 1: Configure the pfSense Firewall Log

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

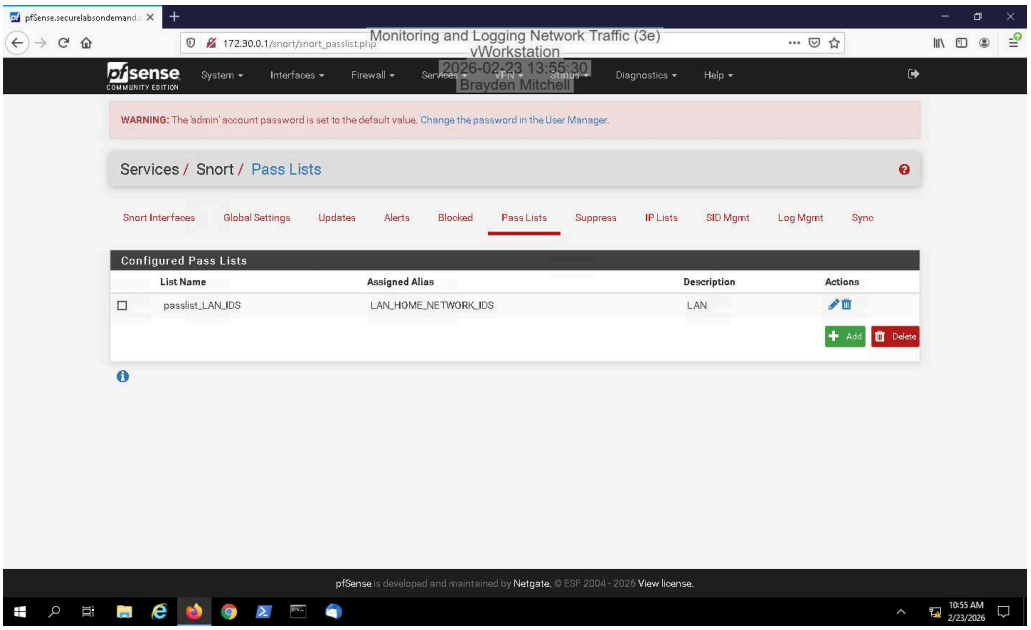


15. **Make a screen capture** showing the **firewall logs**.

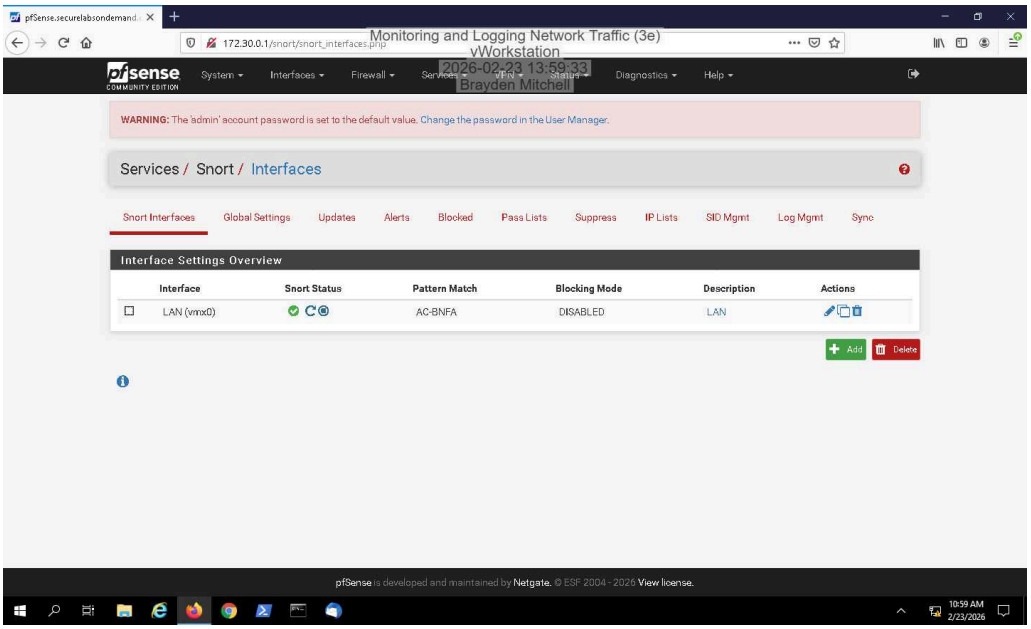


Part 2: Configure a Snort Intrusion Detection System

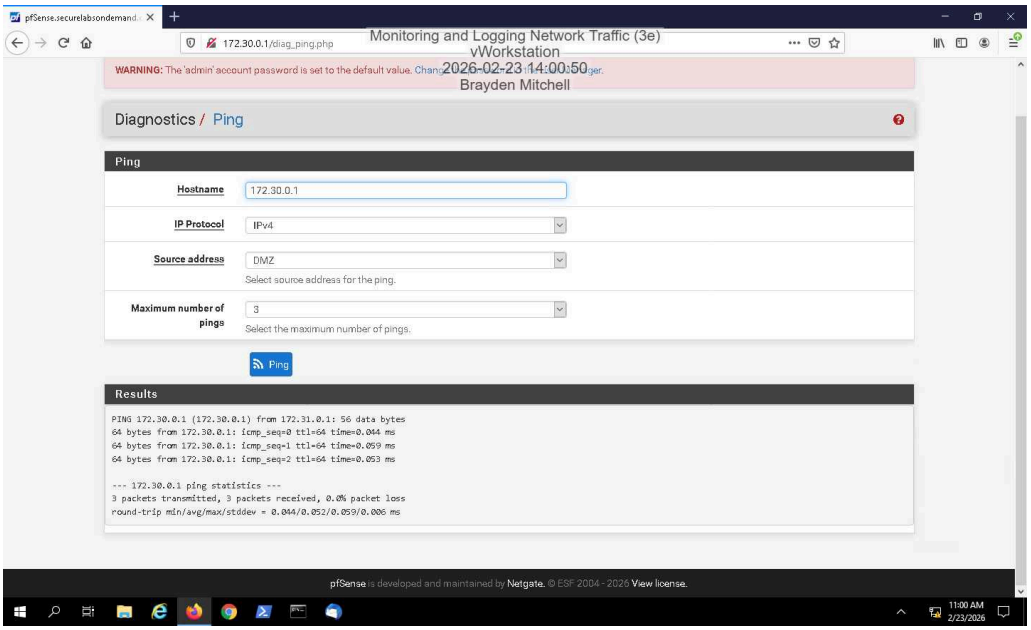
14. **Make a screen capture** showing the **updated Pass Lists page**.



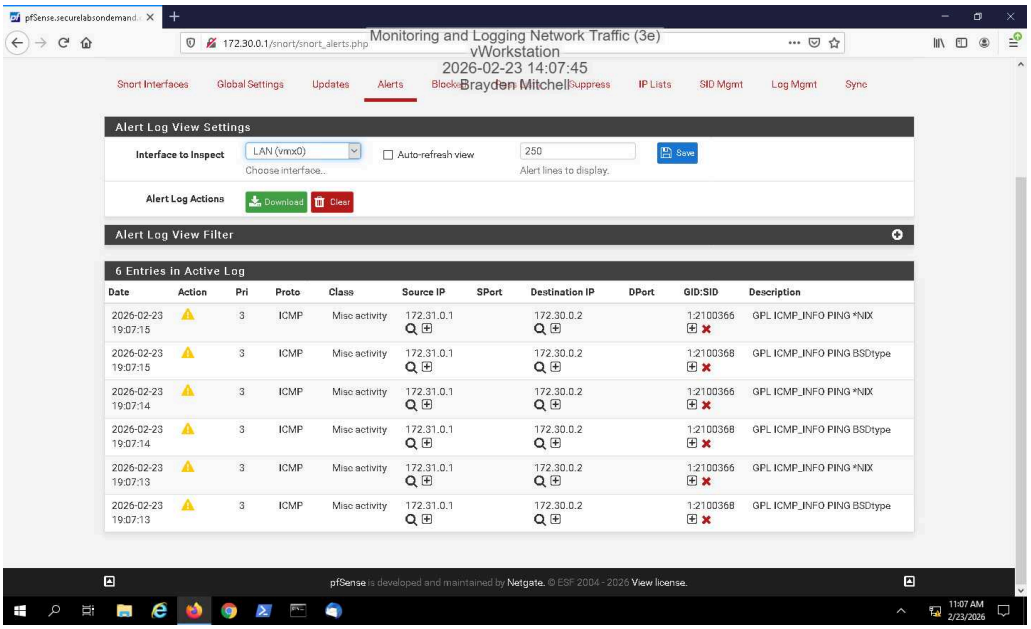
28. **Make a screen capture** showing the **active Snort status on the LAN interface**.



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

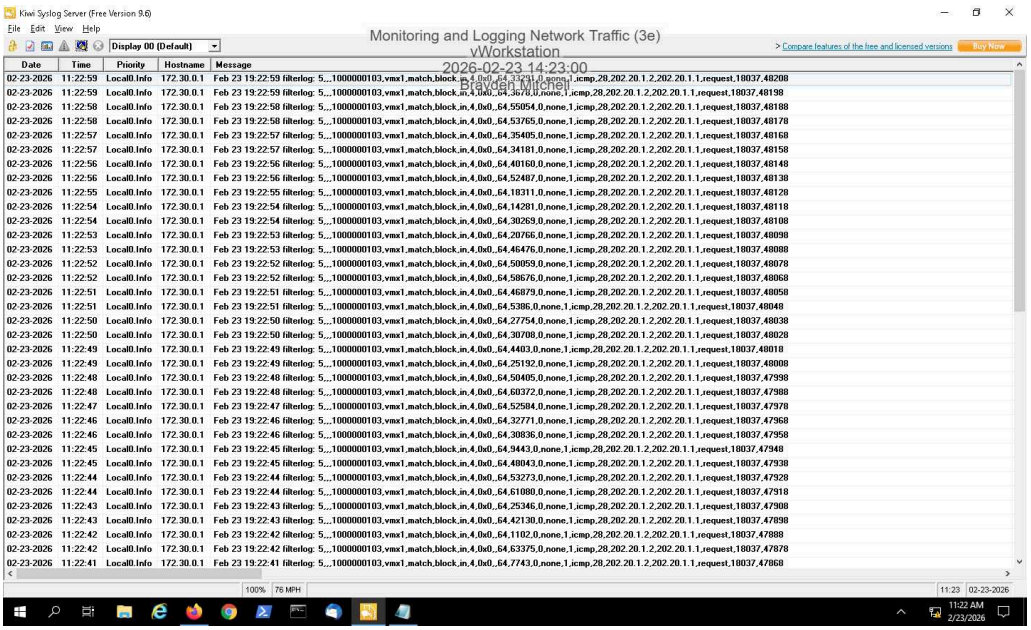


38. **Make a screen capture** showing the **ICMP alerts in the Snort Active Log**.



Part 3: Implement Firewall Log Forwarding with Kiwi Syslog Server

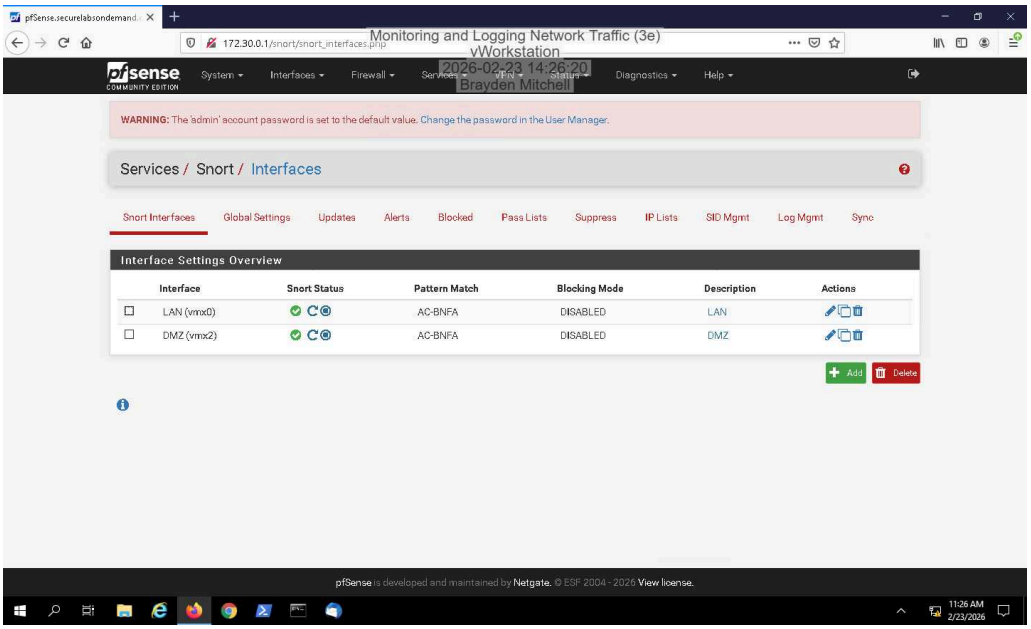
17. **Make a screen capture** showing the **pfSense firewall log events in Kiwi Syslog Server**.



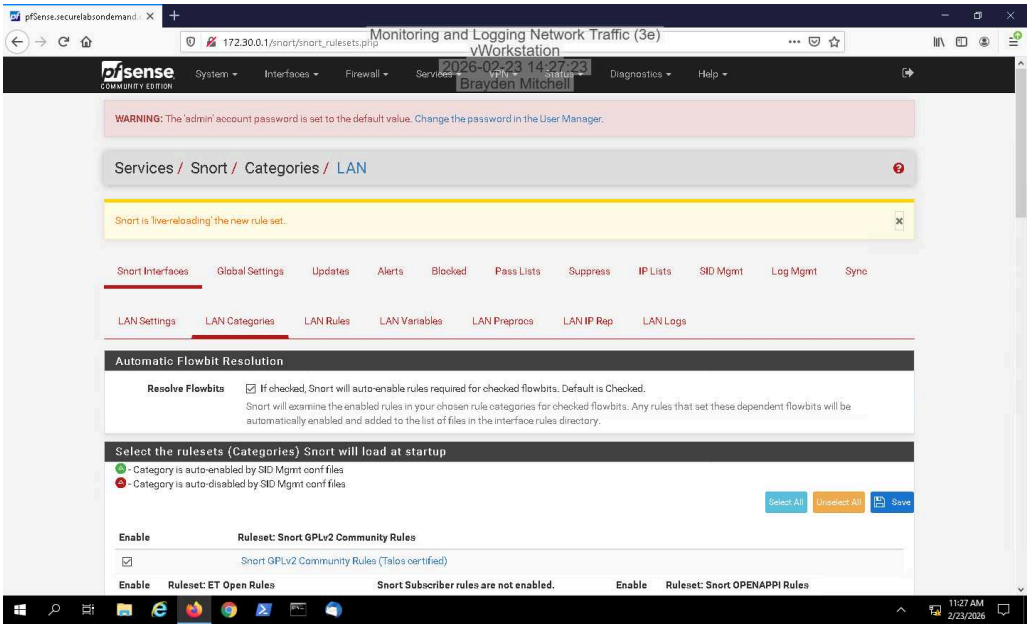
Section 2: Applied Learning

Part 1: Configure Snort Monitoring on the DMZ

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

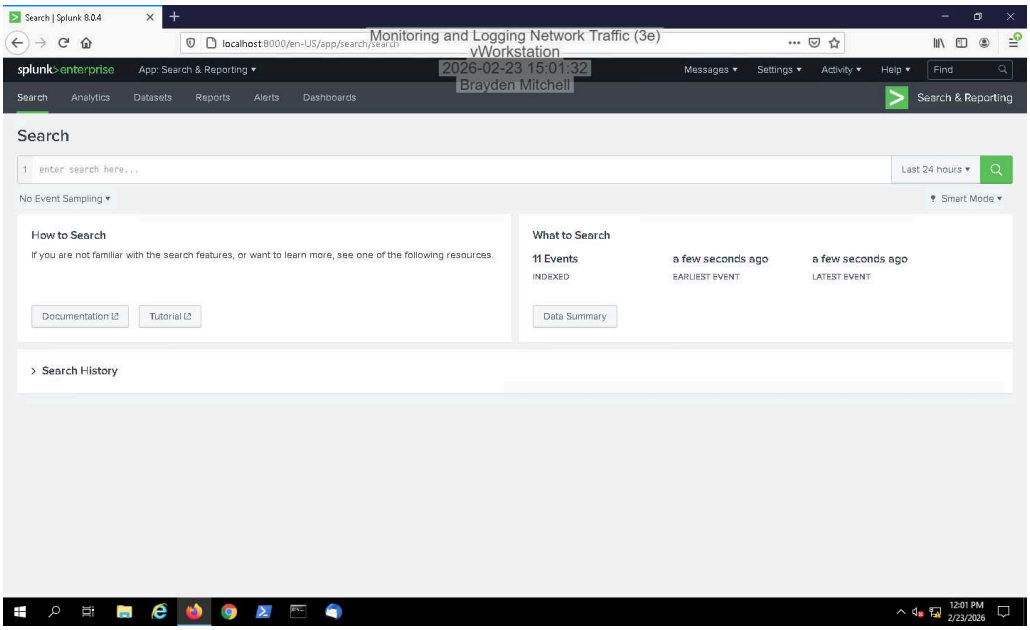


20. **Make a screen capture** showing the **Snort GPLv2 Community Rules enabled and "live-reloading" message**.



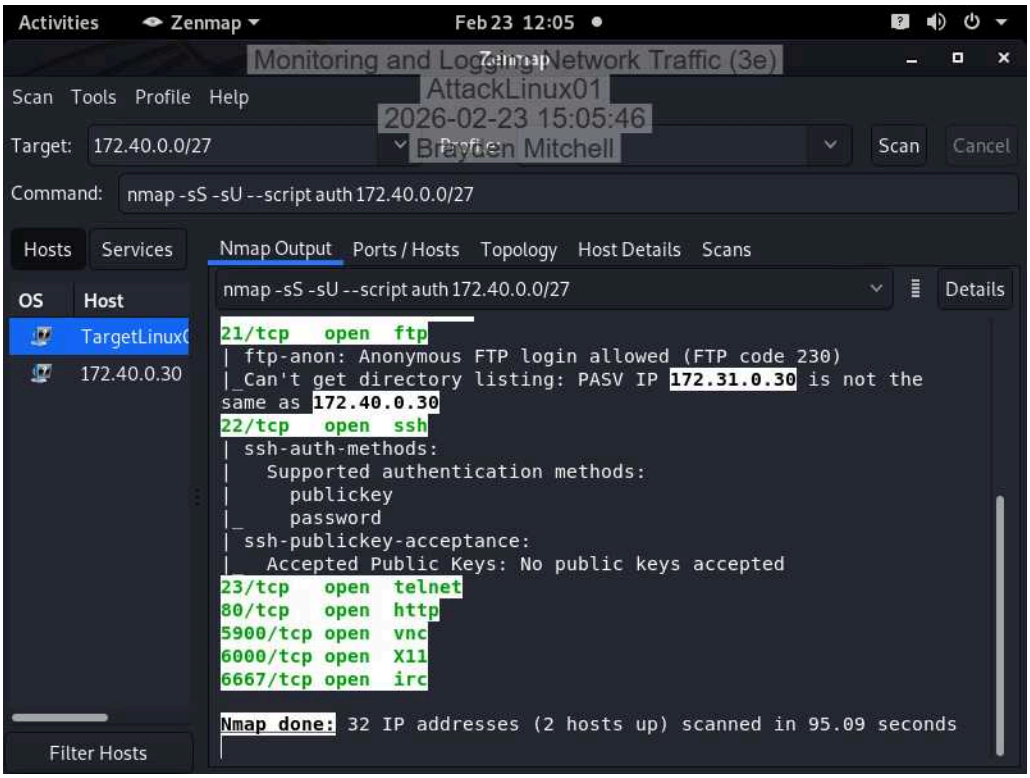
Part 2: Implement Security Information and Event Management with Splunk

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

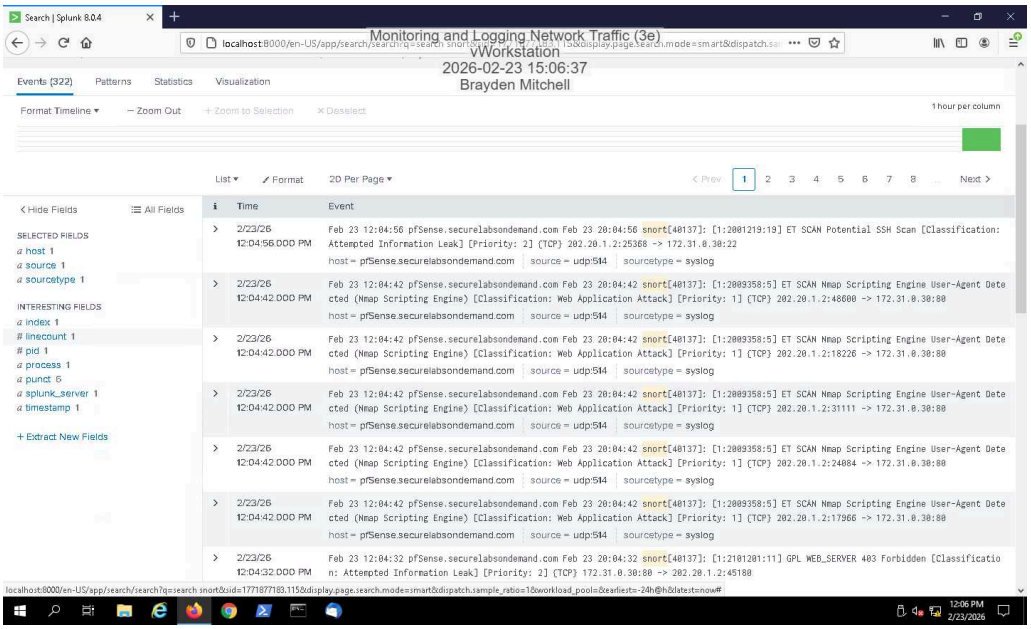


Part 3: Simulate and Detect a Perimeter Network Attack

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



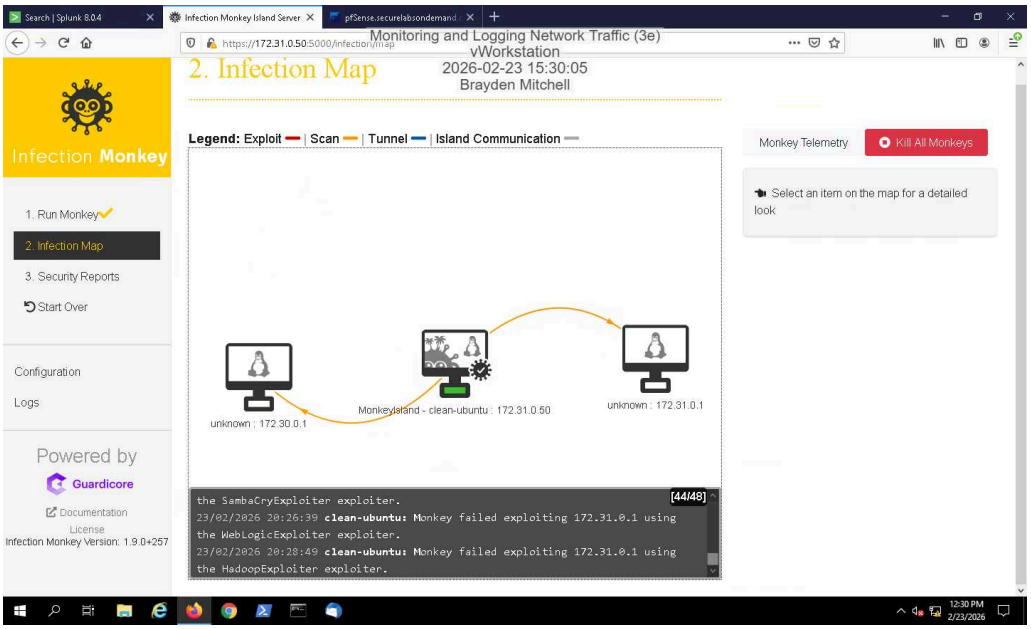
9. **Make a screen capture** showing the **search results in Splunk**.



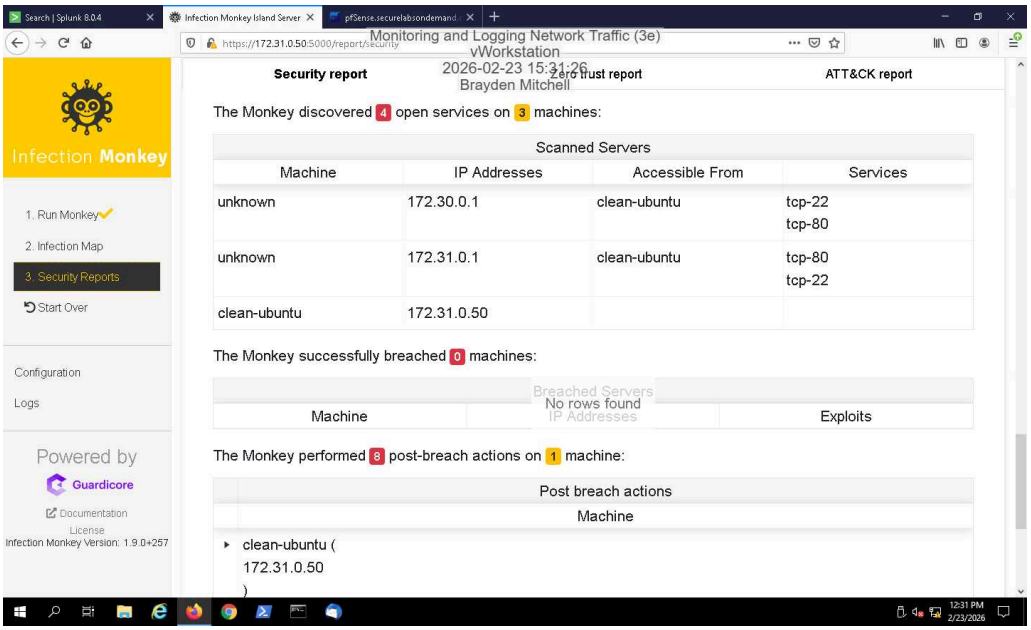
Section 3: Challenge and Analysis

Part 1: Simulate a DMZ Breach with Infection Monkey

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



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

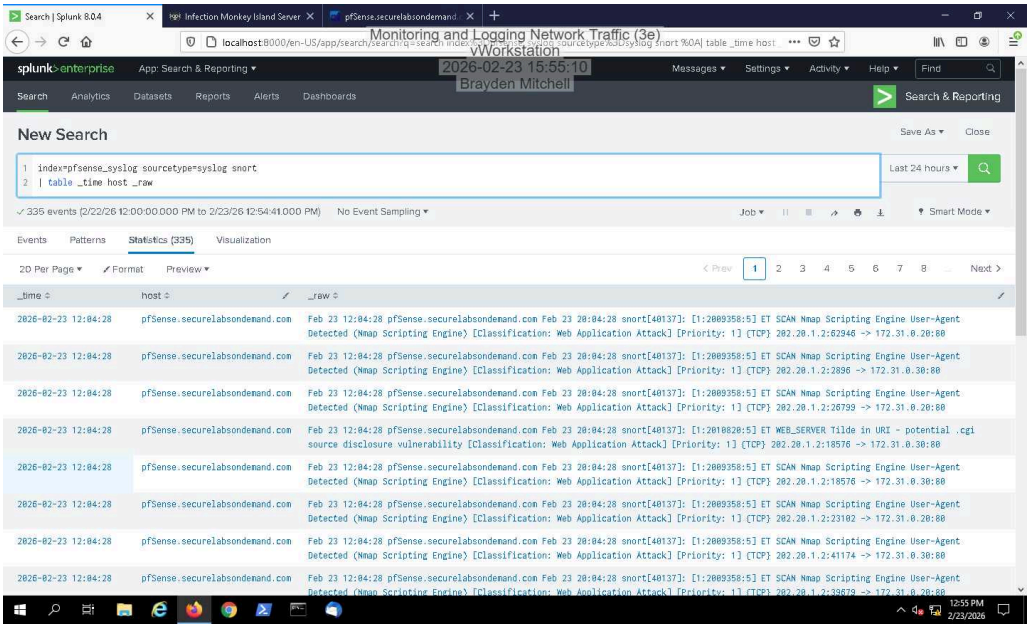


Summarize your DMZ breach simulation results, highlighting what you found to be the greatest concerns from a network monitoring perspective.

The DMZ breach simulation using Infection Monkey demonstrated how quickly an attacker could pivot from a compromised DMZ host into the internal LAN. By launching the scan from AttackMonkey in the DMZ, the exercise effectively simulated a real-world perimeter breach followed by lateral movement attempts. Overall, the greatest concerns were inadequate segmentation between DMZ and LAN.

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**.



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?

The Splunk query results revealed several concerns regarding both the structure of the data and the usability of the fields for effective log analysis. Because the Snort alerts were ingested through pfSense using the syslog sourcetype, much of the alert information appeared embedded within the _raw message field rather than being properly parsed into structured fields. This significantly reduces the efficiency of analysis, as analysts must manually interpret long raw log strings instead of leveraging indexed fields for filtering, correlation, and reporting.

To improve log analysis effectiveness, I would add structured field extractions for src_ip, dest_ip, src_port, and dest_port. I would remove unnecessary verbose raw text duplication if structured fields are available.

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?

To: Security ManagerFrom: Brayden MitchellSubject: How Splunk Performed During the DMZ Breach SimulationDate: 2/23/26
During the DMZ breach simulation, I reviewed how well Splunk detected signs of the simulated attack. Overall, Splunk was helpful in finding Snort alerts related to scanning and suspicious traffic coming from the DMZ system. It confirmed that our IDS logs are being collected and can be searched to identify potential threats.
However, the logs were not very organized. Many important details like source IP, destination IP, alert name, and severity were buried inside long raw messages instead of being clearly separated into searchable fields. This made it harder and slower to analyze the data.
To improve Splunk's effectiveness, I recommend:
Properly configuring field extractions so key data (IP addresses, alert names, severity levels) are clearly separated and searchable.
Building simple dashboards to quickly view IDS alerts and scanning activity.
Overall, Splunk is working and can detect signs of a breach, but with better log formatting and alert configuration, it would be much easier and faster to identify suspicious activity and respond quickly.