Student:	Email:
Vidhi Kadakia	jinsukrishna108@gmail.com

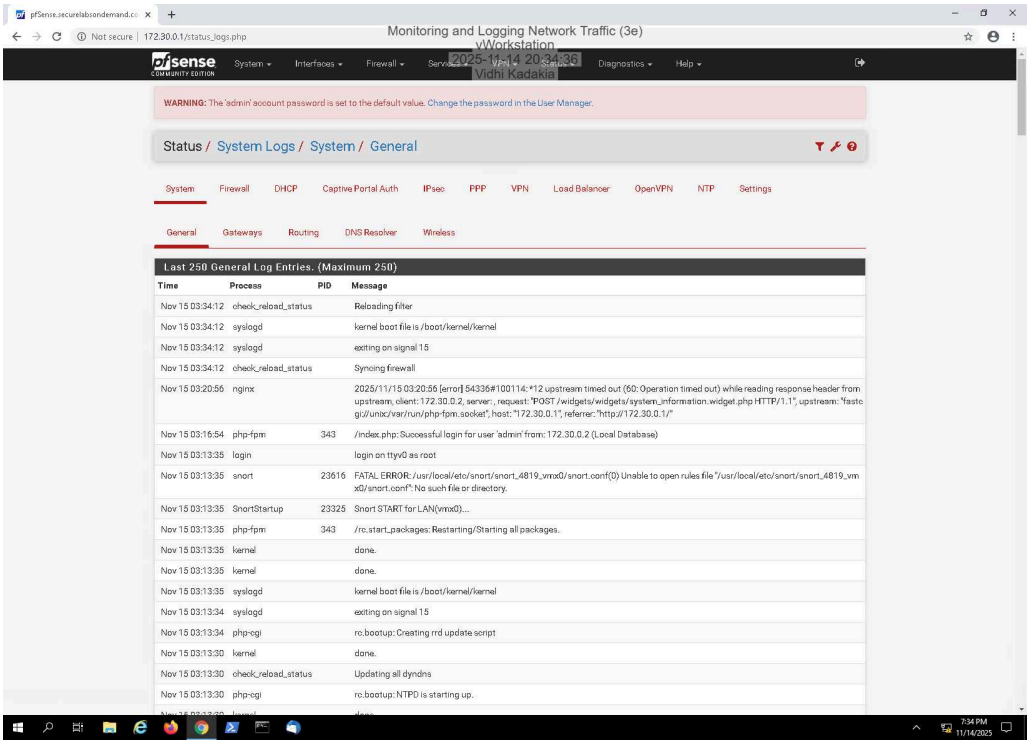
Time on Task:	Progress:
3 hours, 30 minutes	100%

Report Generated: Saturday, November 15, 2025 at 4:41 PM

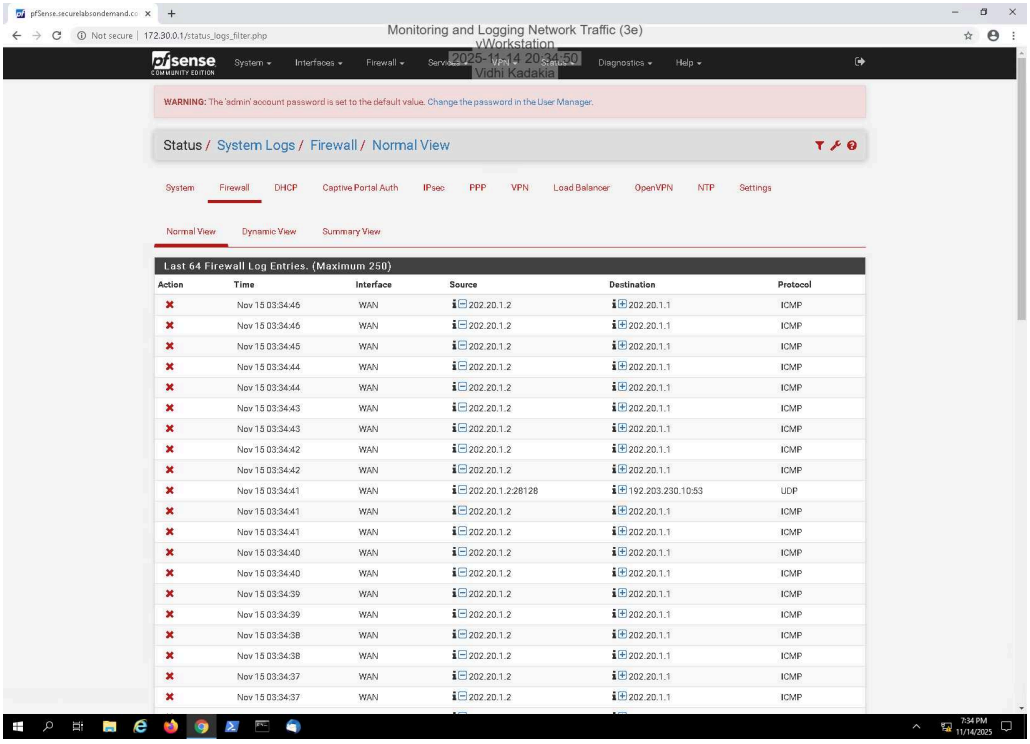
Section 1: Hands-On Demonstration

Part 1: Configure the pfSense Firewall Log

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

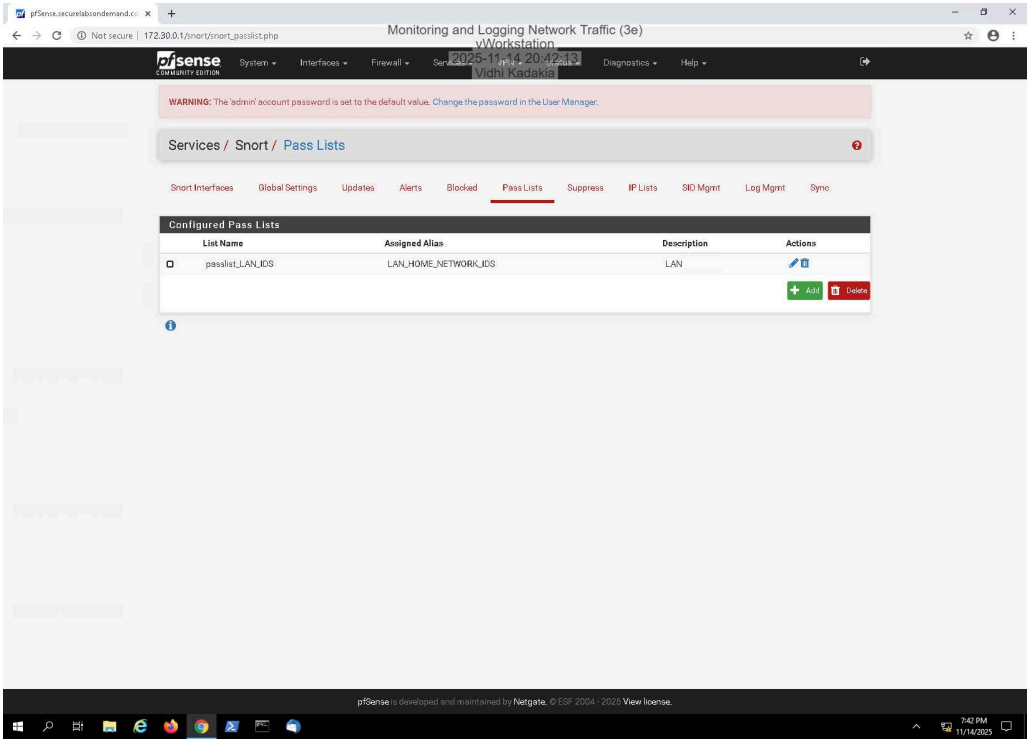


15. **Make a screen capture** showing the **firewall logs**.

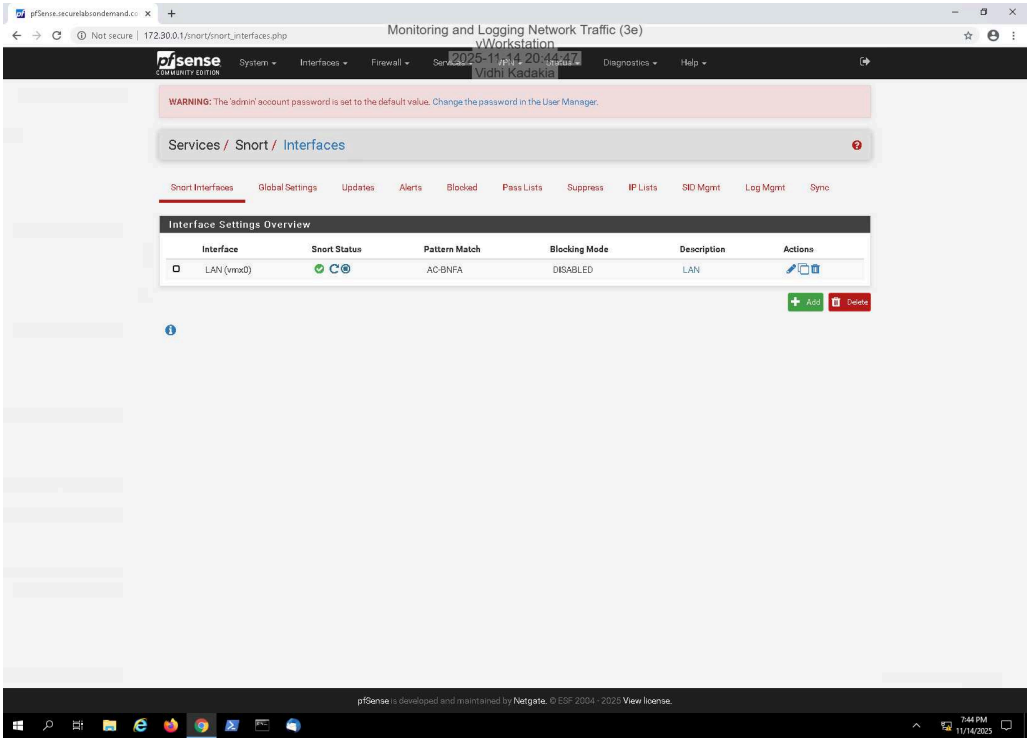


Part 2: Configure a Snort Intrusion Detection System

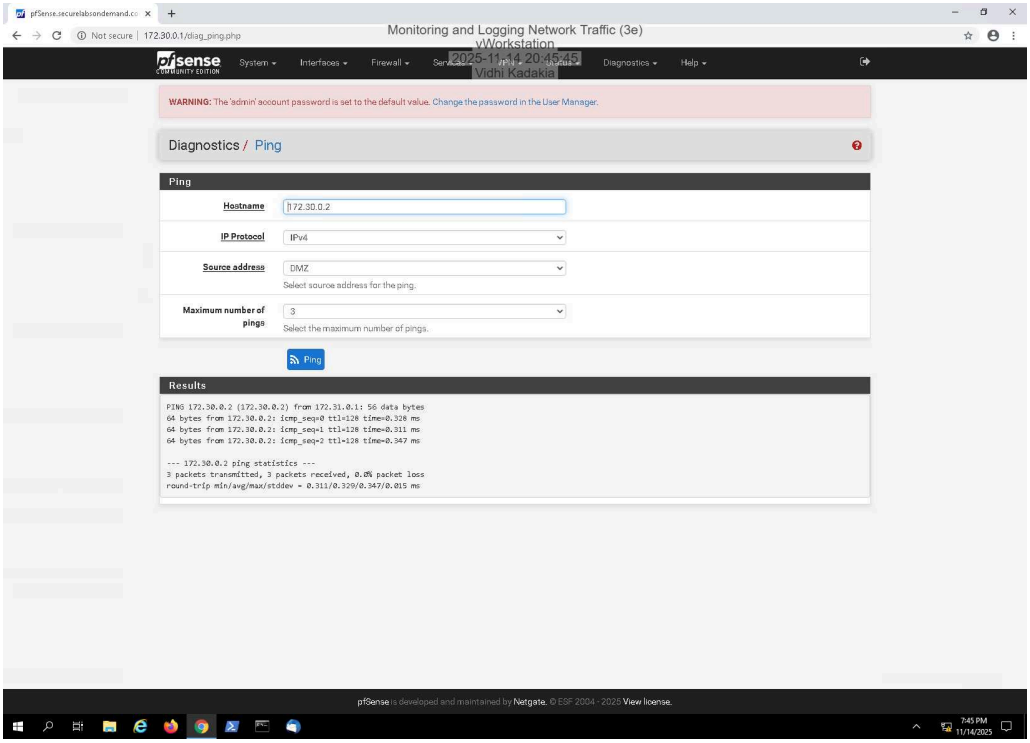
14. **Make a screen capture** showing the **updated Pass Lists page**.



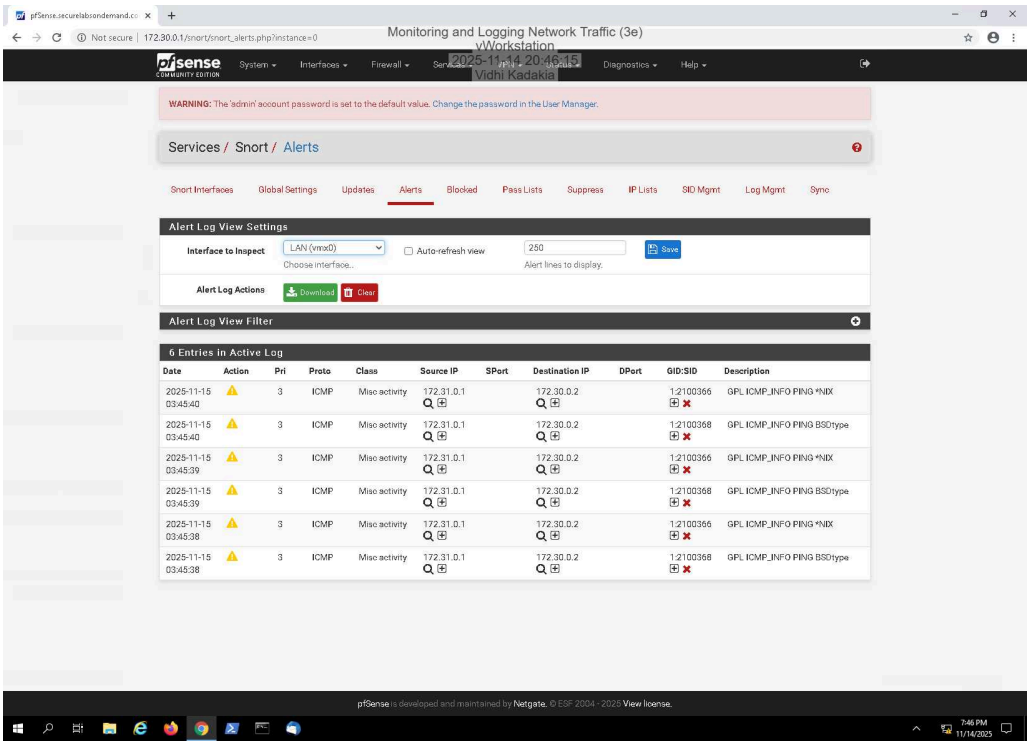
28. **Make a screen capture** showing the **active Snort status on the LAN interface**.



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

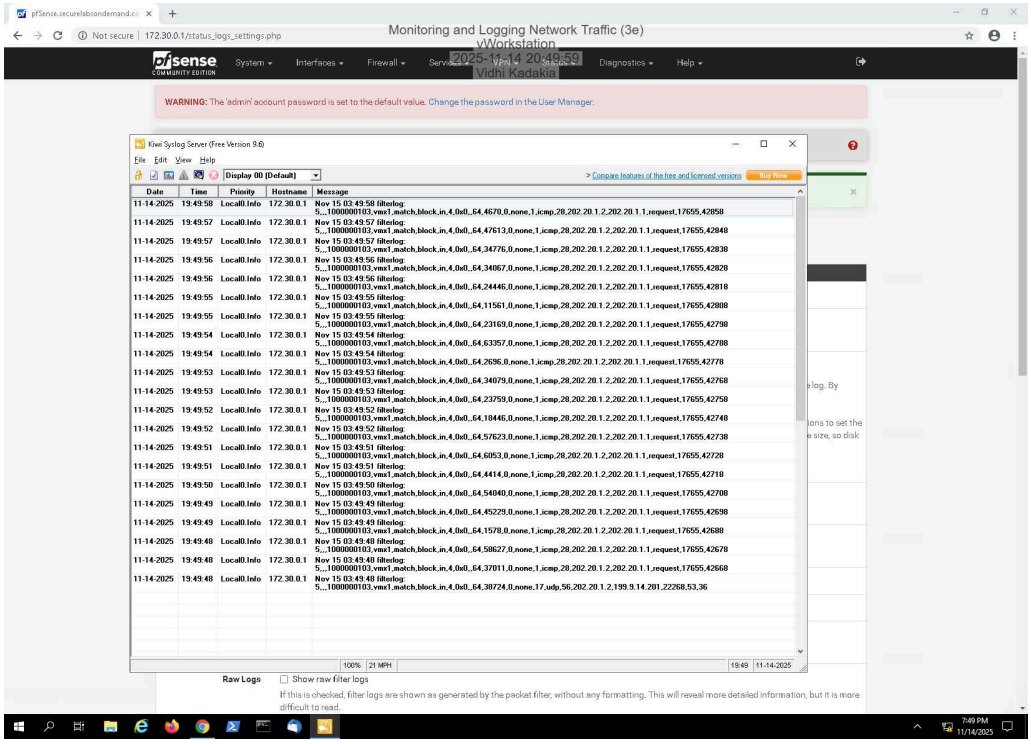


38. **Make a screen capture** showing the **ICMP alerts in the Snort Active Log**.



Part 3: Implement Firewall Log Forwarding with Kiwi Syslog Server

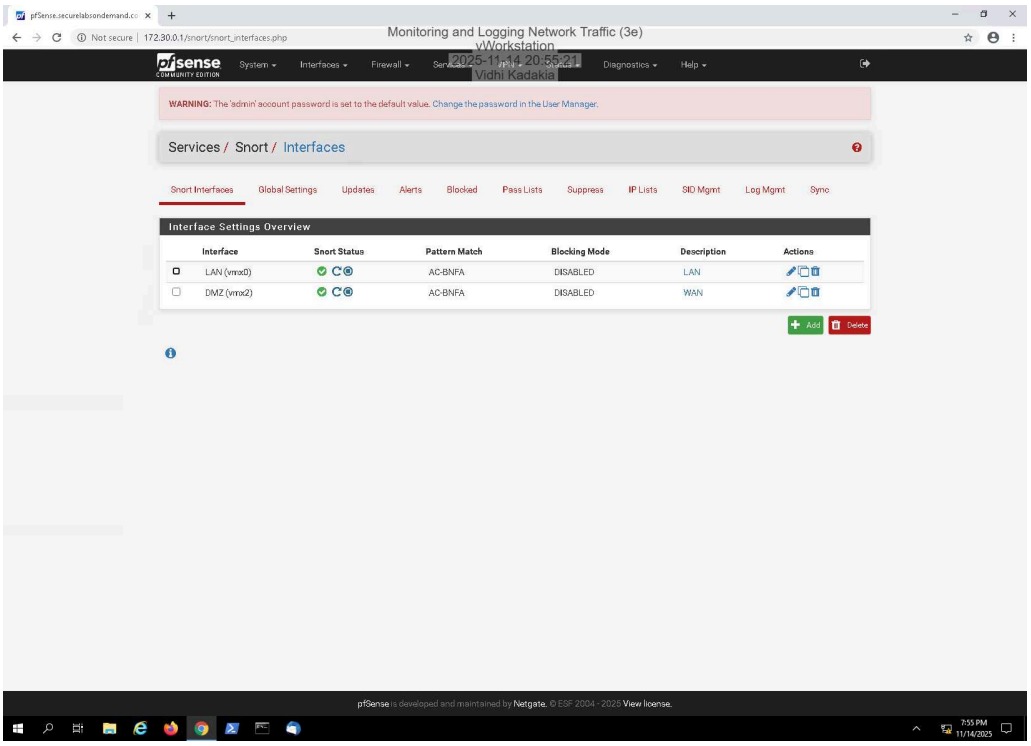
17. **Make a screen capture** showing the **pfSense firewall log events in Kiwi Syslog Server**.



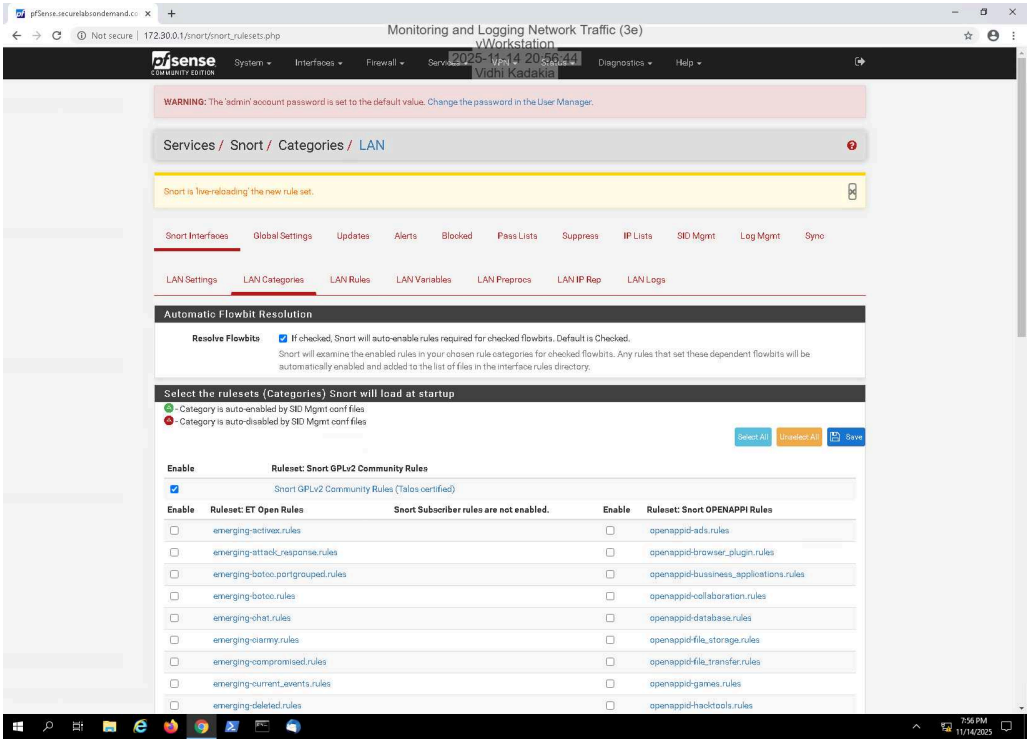
Section 2: Applied Learning

Part 1: Configure Snort Monitoring on the DMZ

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

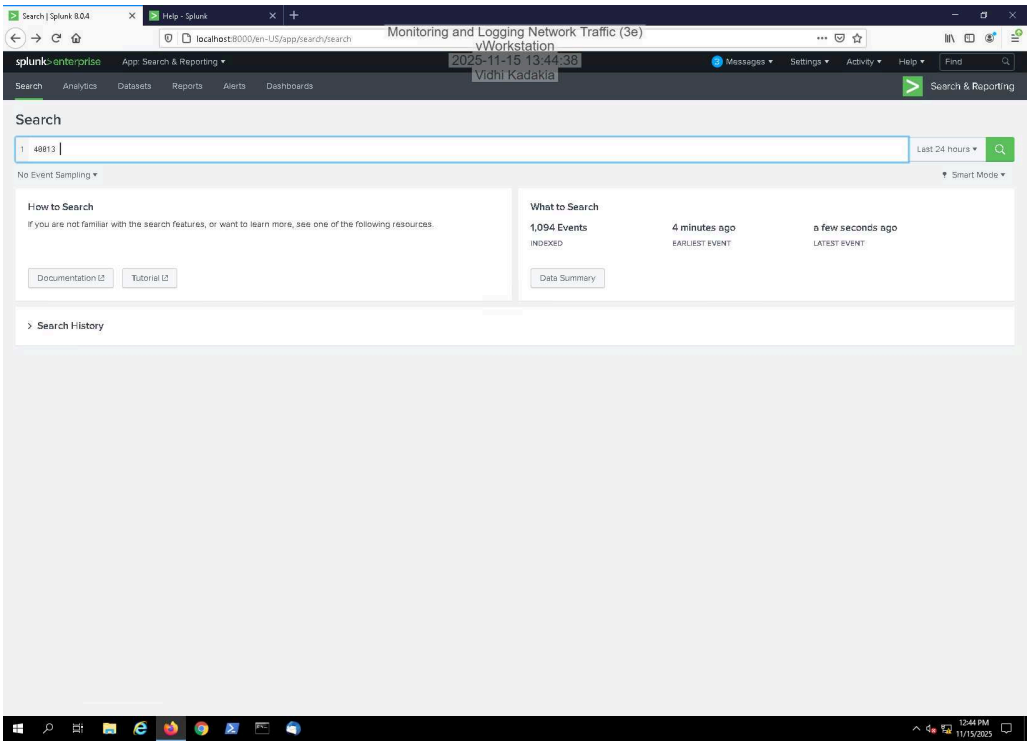


20. **Make a screen capture** showing the **Snort GPLv2 Community Rules enabled and "live-reloading" message**.



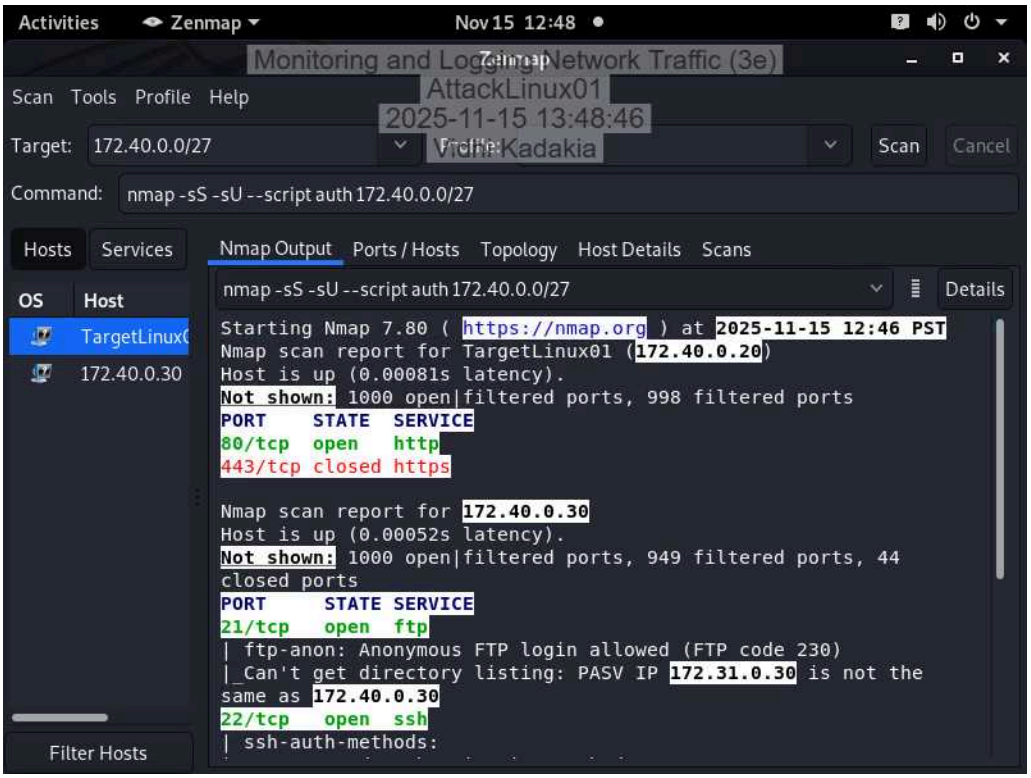
Part 2: Implement Security Information and Event Management with Splunk

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

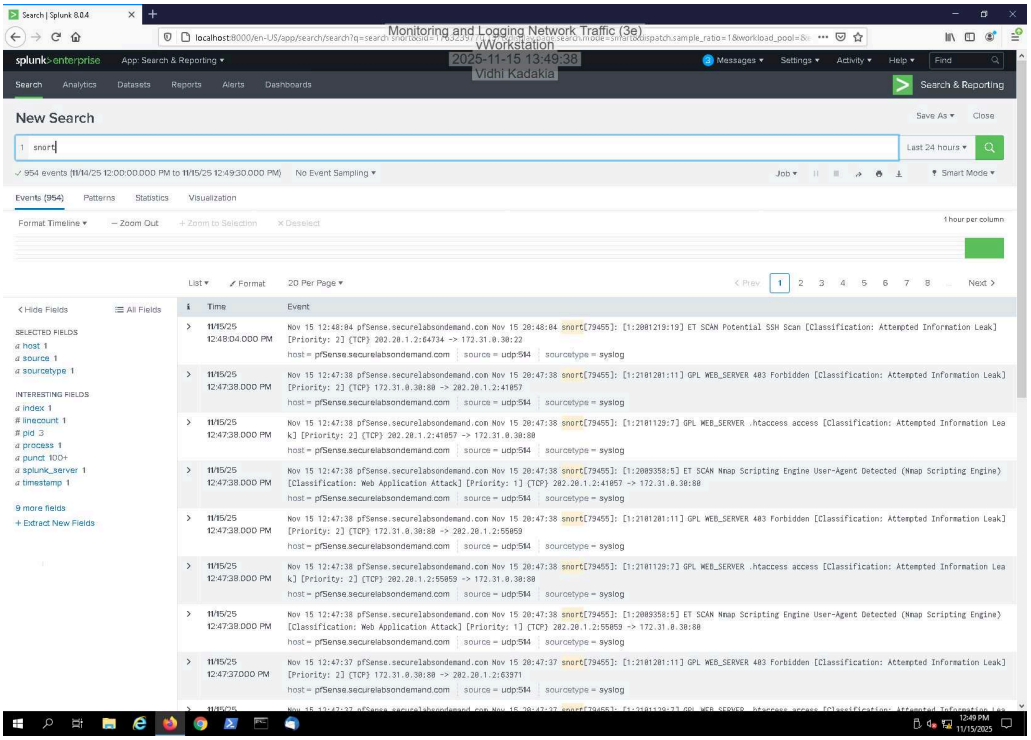


Part 3: Simulate and Detect a Perimeter Network Attack

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



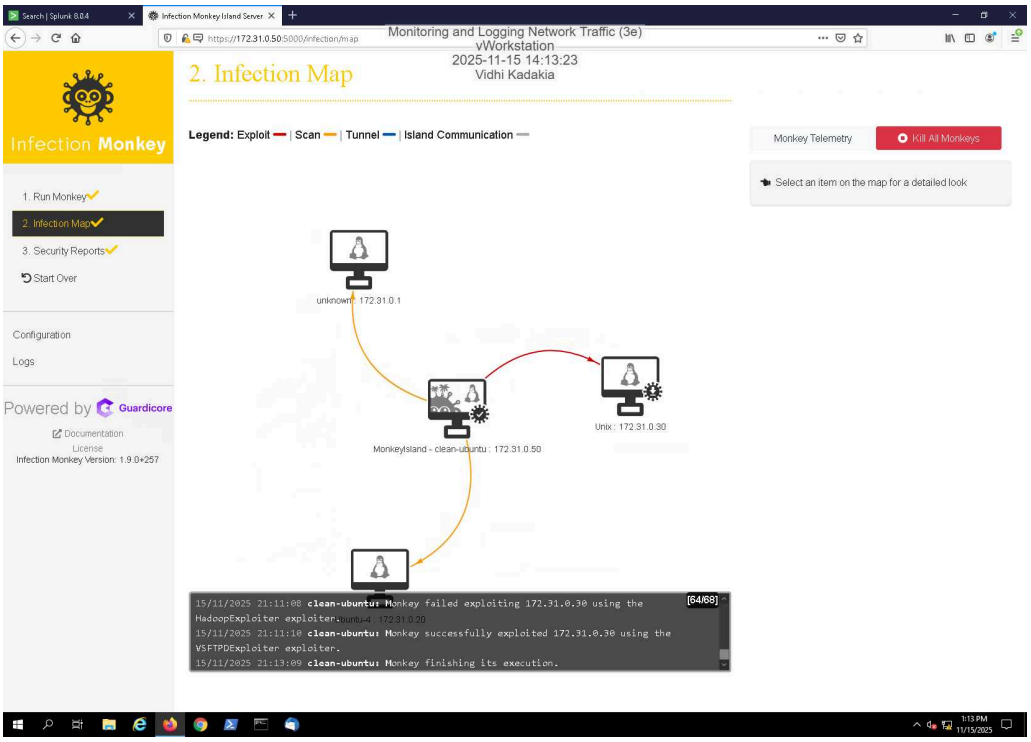
9. **Make a screen capture** showing the **search results in Splunk**.



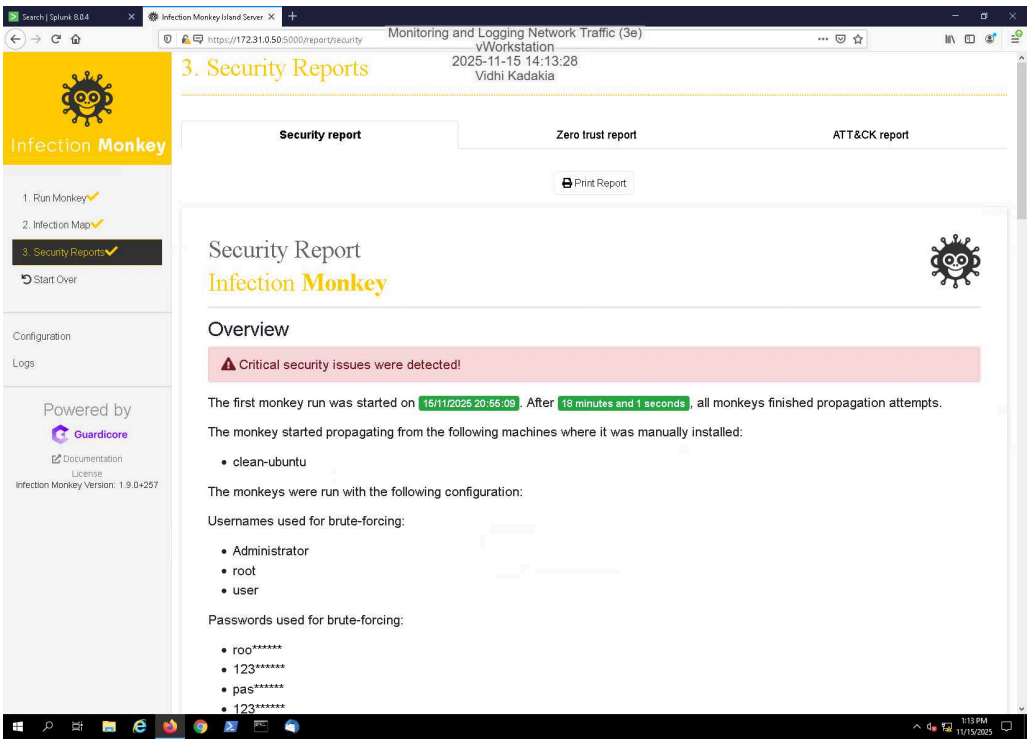
Section 3: Challenge and Analysis

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**.

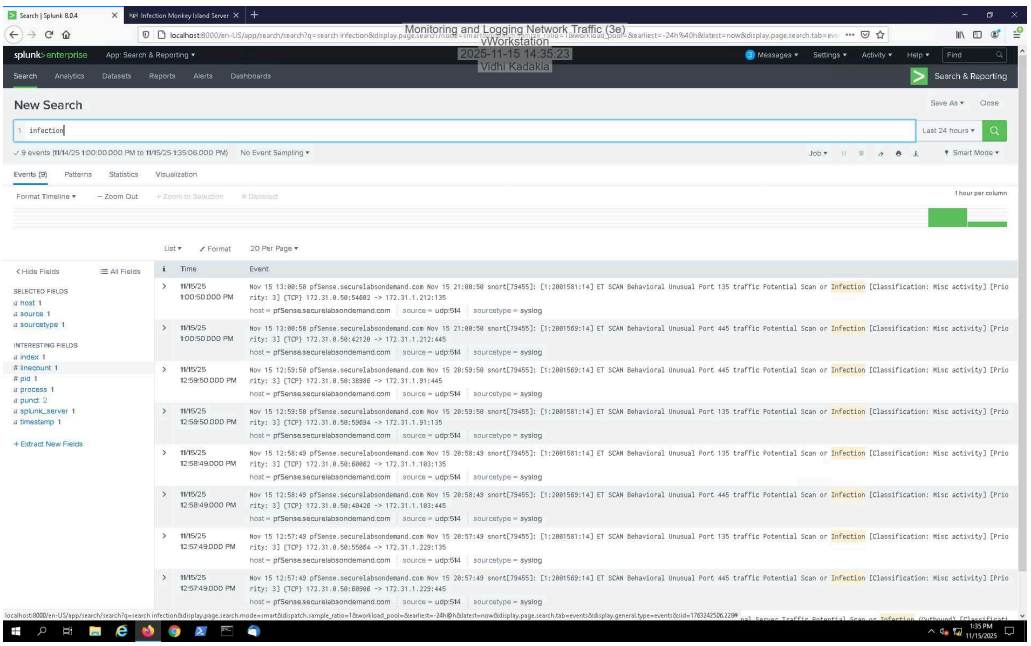


Summarize your DMZ breach simulation results, highlighting what you found to be the greatest concerns from a network monitoring perspective.

The DMZ breach simulation revealed several major security concerns. Infection Monkey successfully exploited a critical VSFTPD vulnerability, showing that unpatched services pose an immediate risk. The monkey was able to move laterally from the DMZ into the internal LAN, indicating weak network segmentation and insufficient firewall controls. Multiple reused or weak credentials were discovered, making lateral movement even easier. The simulation also showed that hosts across different network segments could communicate freely without restriction. Most importantly, none of the monkey's exploit attempts, scanning behavior, or credential attacks were detected or blocked, revealing significant gaps in network monitoring. Overall, the results demonstrate that both patching and internal visibility need major improvement.

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 Snort logs in Splunk were hard to read because most of the important details were buried inside long syslog messages instead of being broken into clear fields. It was difficult to quickly see things like source IP, destination IP, or the signature that triggered the alert. To make the logs easier to analyze, I would add proper field extractions for IPs, ports, severity, and signature names. I would also remove extra syslog noise and add labels for network zones so it’s easier to understand where the traffic came from

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?

Splunk was able to capture Snort alerts from the Infection Monkey scan, so it does detect traces of the attack, but it didn’t highlight them clearly without manual searching. I recommend enabling better field parsing for Snort logs and creating alerts for suspicious scans or DMZ-to-LAN traffic. Adding dashboards and automated correlation rules would make Splunk far more helpful during real incidents. With these improvements, Splunk would provide clearer and faster detection of similar breaches in the future.