Student:	Email:
Isaiah Mosley	isaiahmosley80@gmail.com

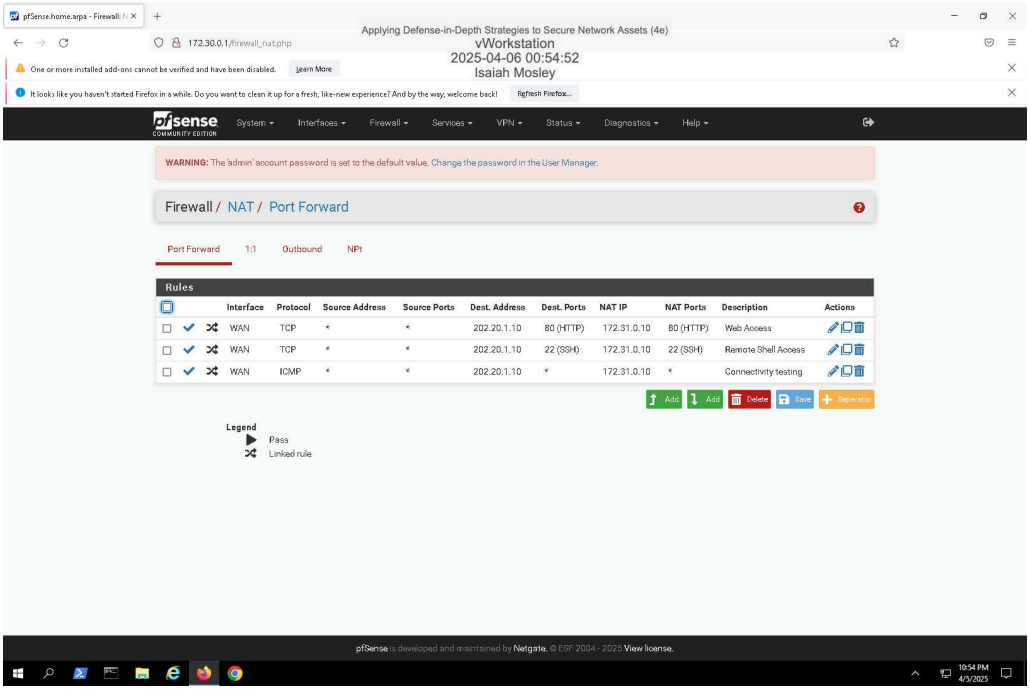
Time on Task:	Progress:
104 hours, 46 minutes	100%

Report Generated: Tuesday, December 2, 2025 at 1:25 PM

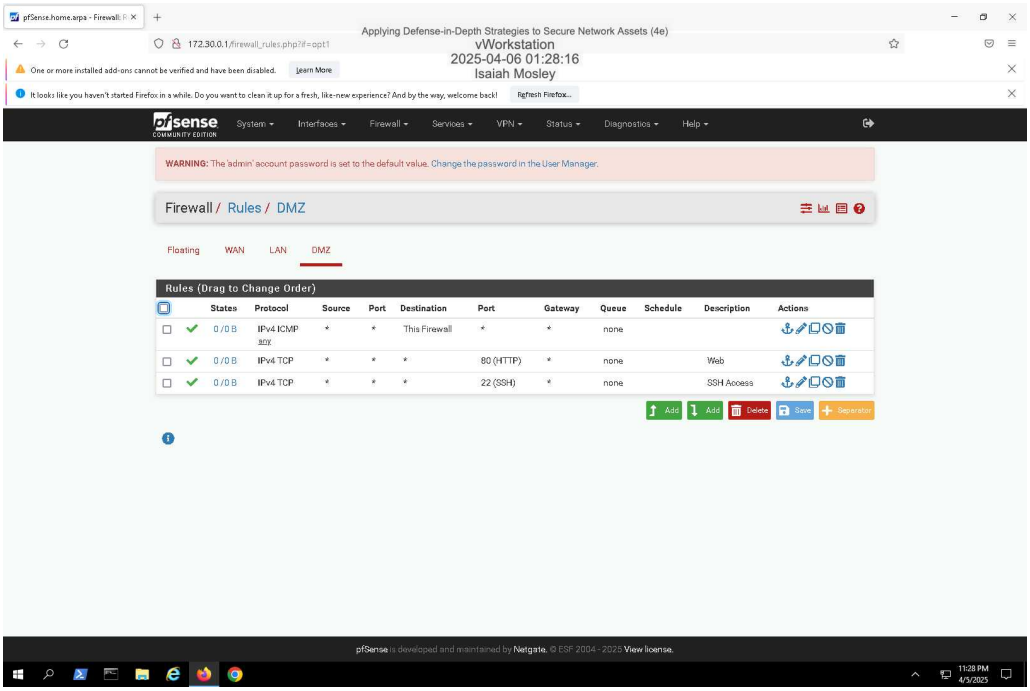
Hands-On Demonstration

Part 1: Update the Firewall Rules

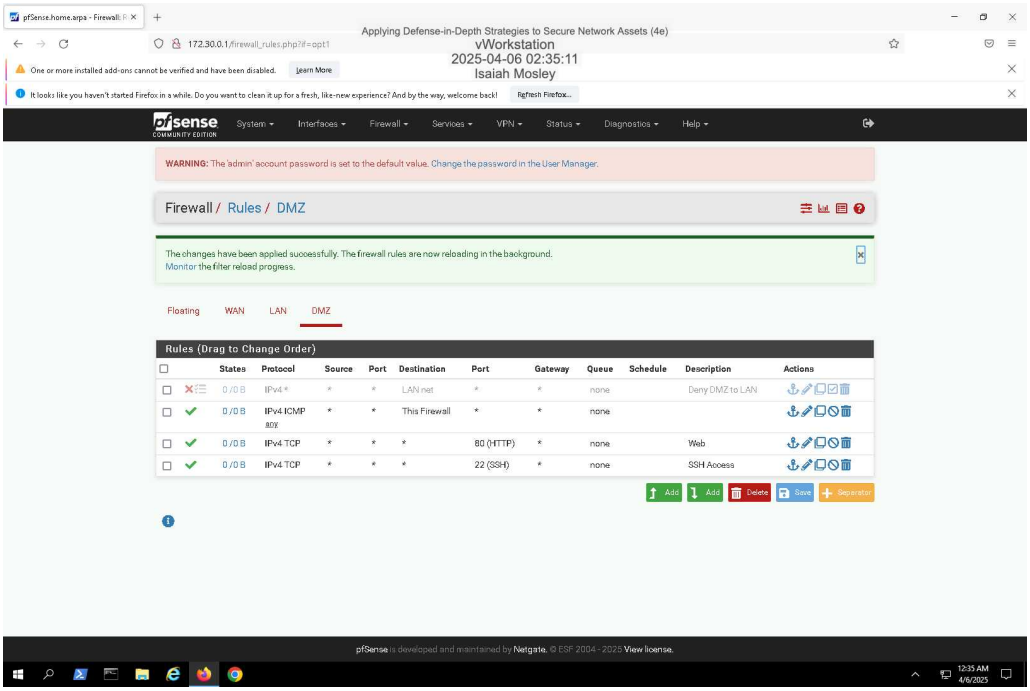
10. **Make a screen capture** showing the Port Forward rules for WebServer01.



14. **Make a screen capture** showing the permissive DMZ ruleset.

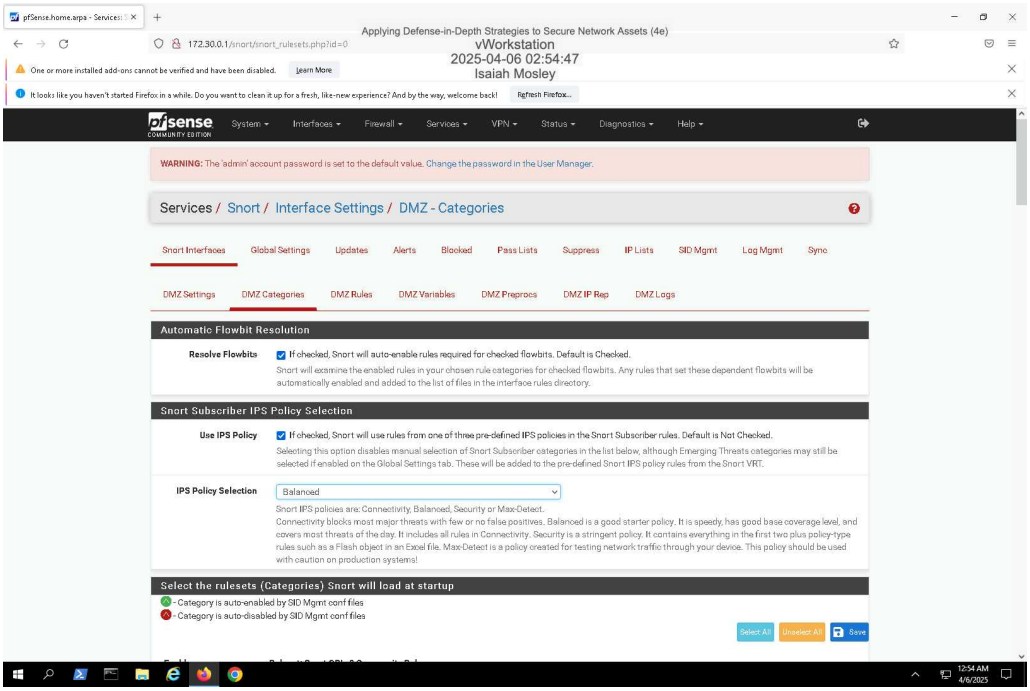


25. **Make a screen capture** showing the updated firewall ruleset for the DMZ.

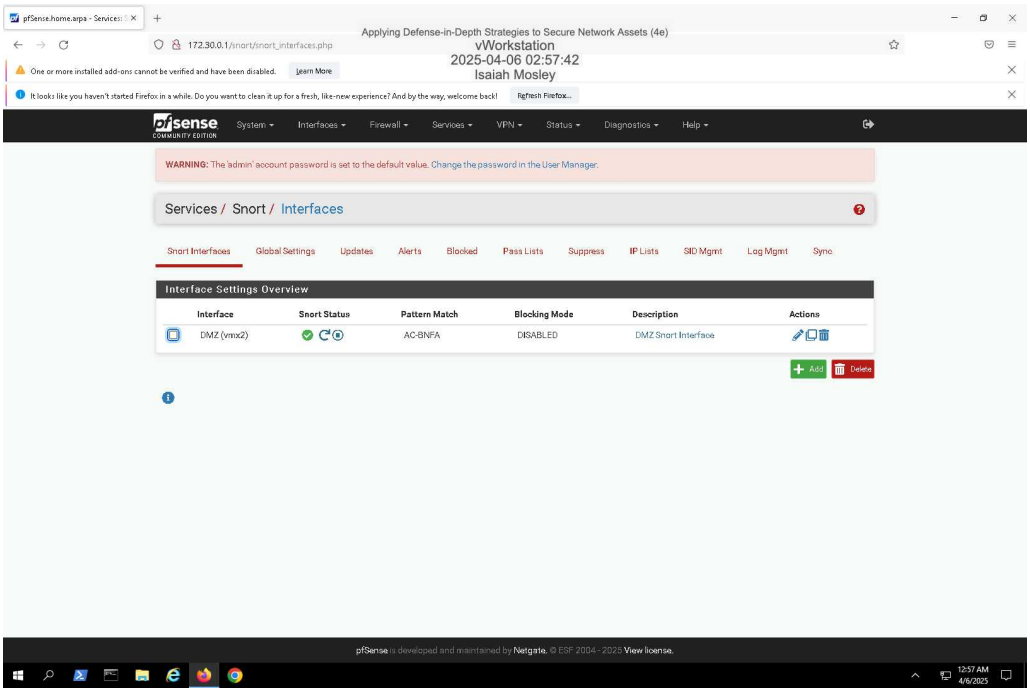


Part 2: Configure a Network-based IDS on pfSense

23. **Make a screen capture** showing a Balanced IPS policy.

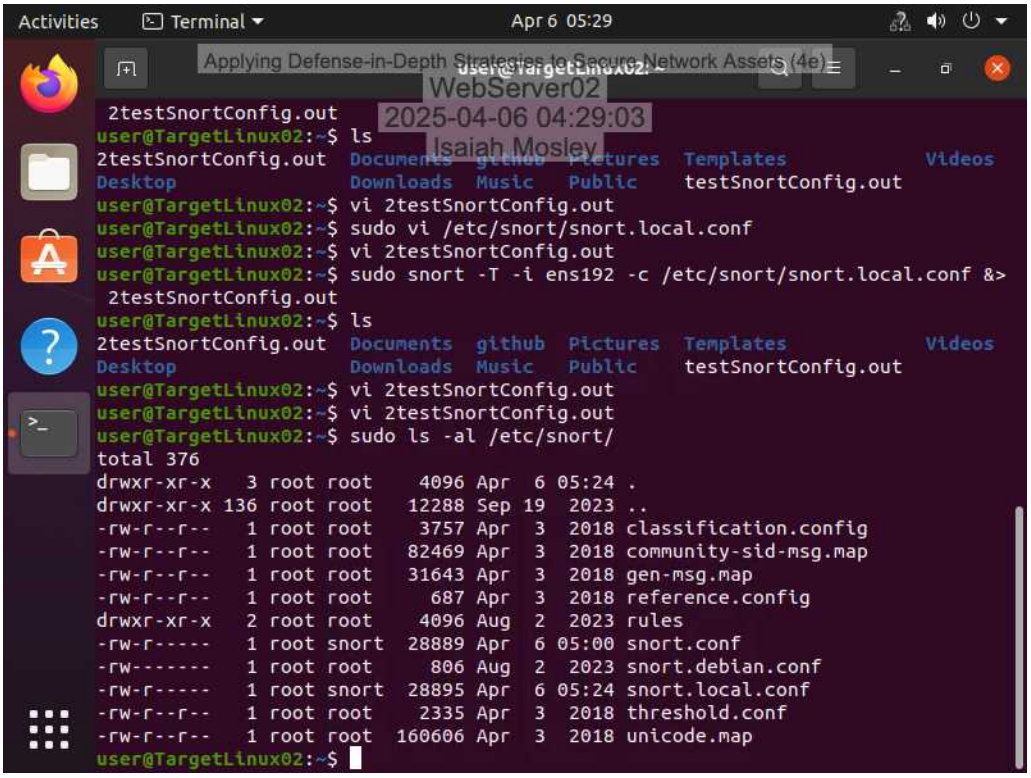


30. **Make a screen capture** showing that the Snort (DMZ) Interface is running in the Interface Settings Overview.

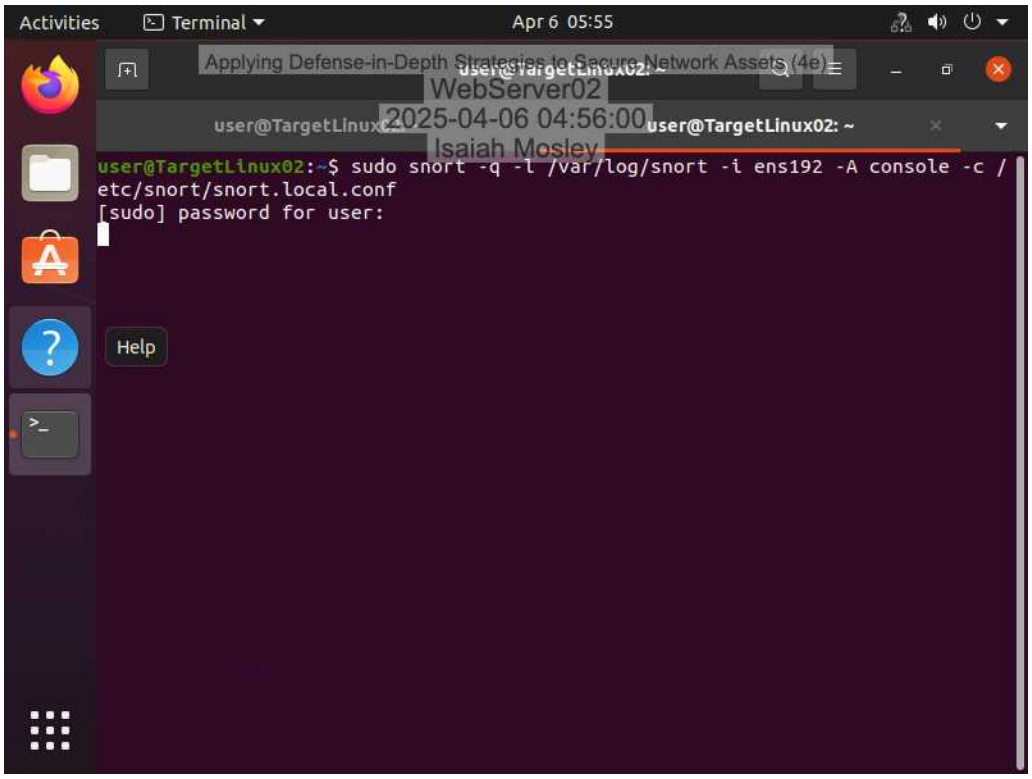


Part 3: Configure a Host-based IDS (HIDS) on Linux

38. **Make a screen capture** showing the **contents of the /etc/snort directory with your local config file**.



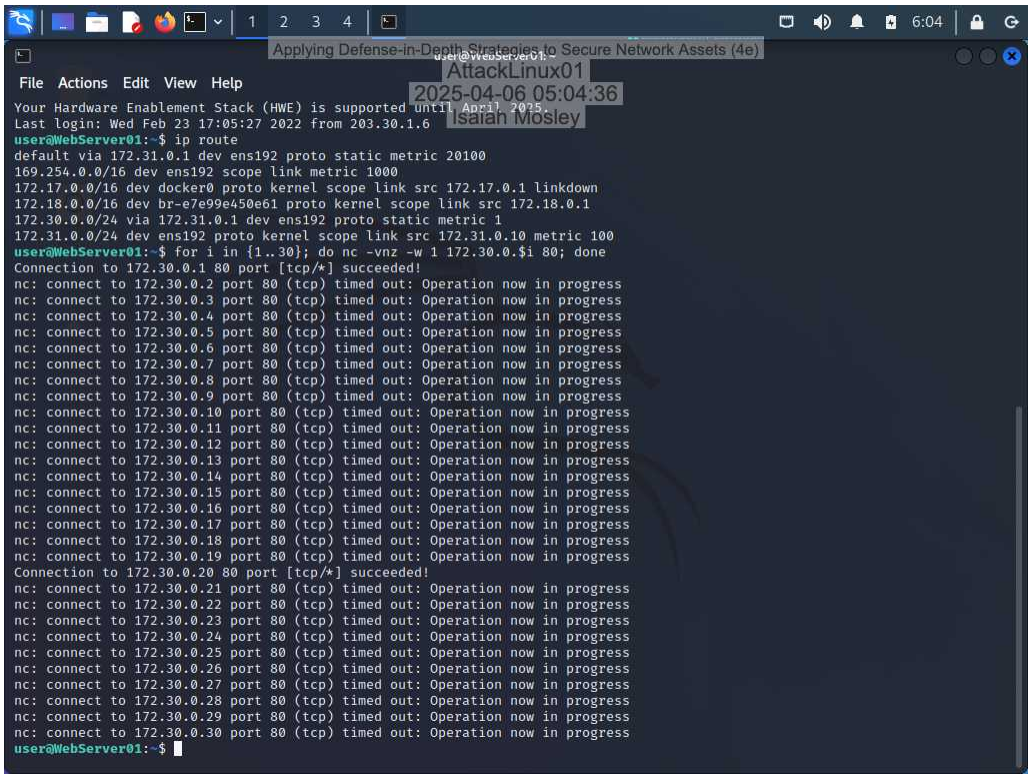
51. **Make a screen capture** showing the successful start of Snort as HIDS on WebServer02.



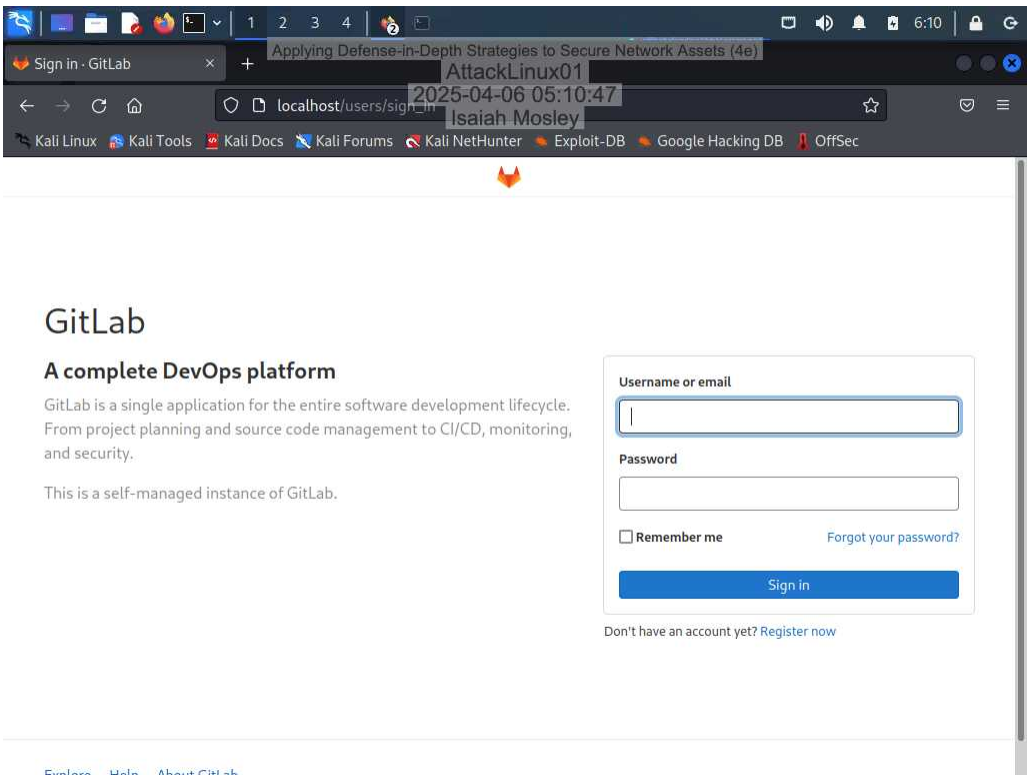
Applied Learning

Part 1: Validate Your IDS Security Controls

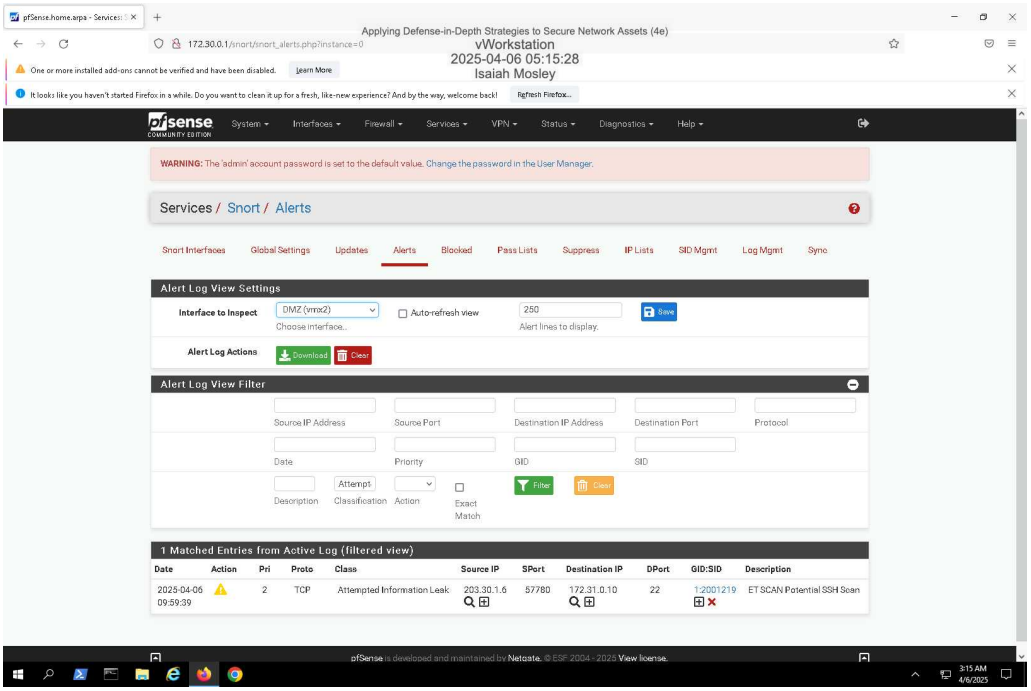
9. **Make a screen capture** showing the successful Netcat connection to WebServer02 at 172.30.0.20.



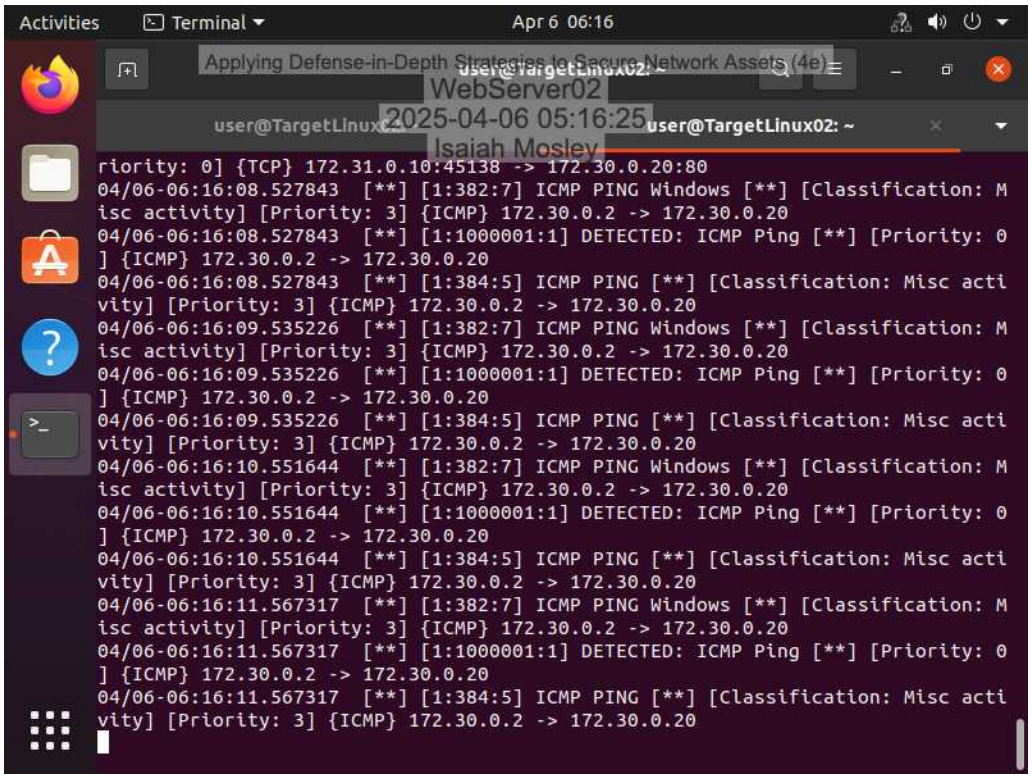
17. **Make a screen capture** showing the login page of the internal GitLab server at localhost/users/sign_in.



25. **Make a screen capture** showing the Attempted Information Leak alert.

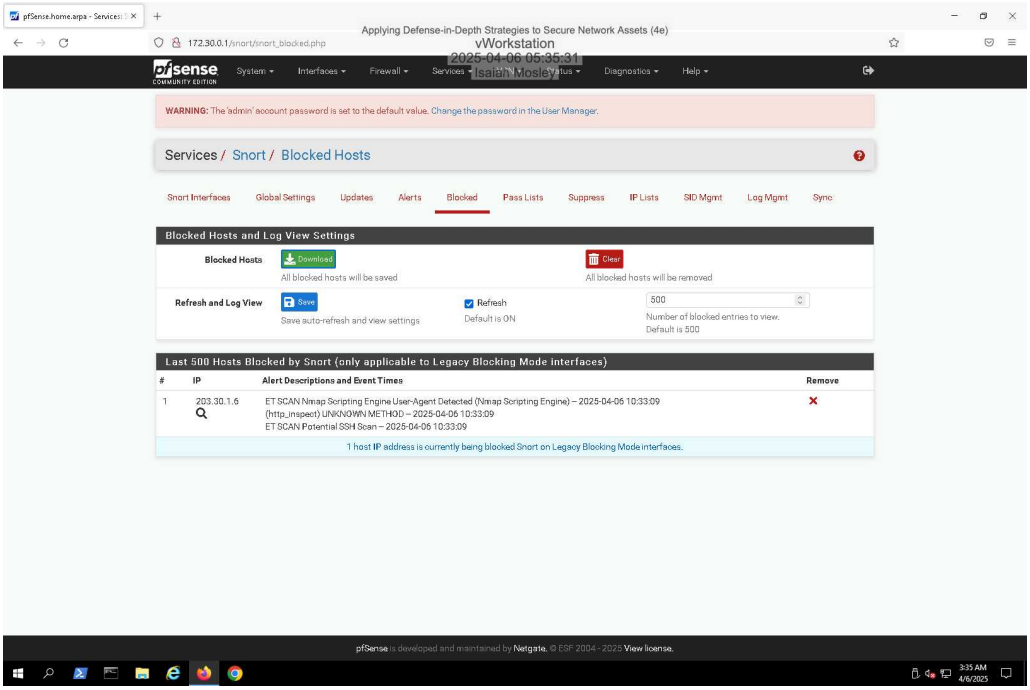


30. **Make a screen capture** showing these Snort HIDS alerts.

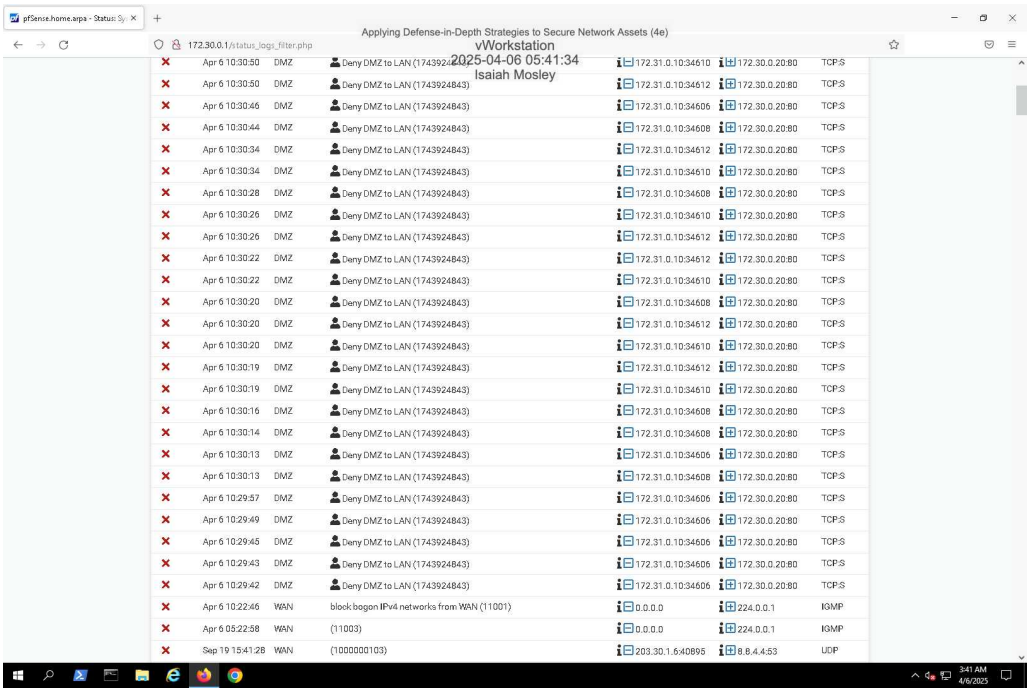


Part 2: Configure and Validate Protection Mode (IPS) on Network-based IDS

27. **Make a screen capture** showing the blocked IP in the *Last 500 Hosts Blocked by Snort* widget.

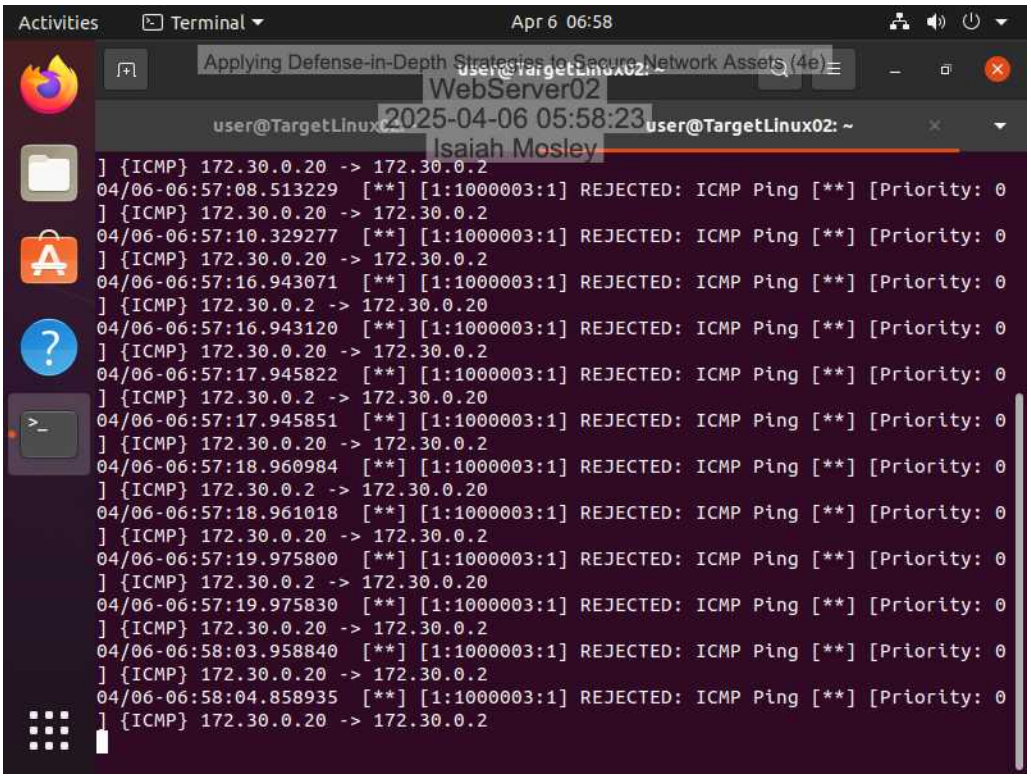


30. **Make a screen capture** showing the blocked connection from the DMZ to the LAN.

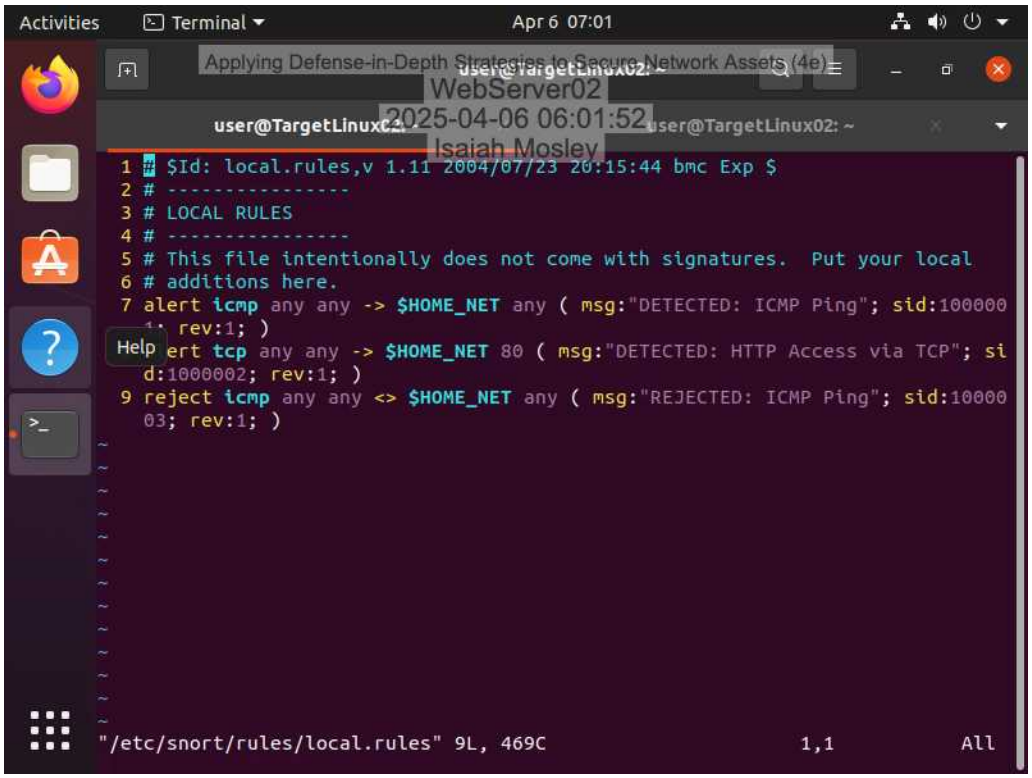


Part 3: Explore Protection Mode Options (HIPS) on Host-based IDS

24. **Make a screen capture** showing the ping responses from WebServer02.



26. **Make a screen capture** showing output that indicates that the rejection rules fired.



27. **Document this protection deficiency and suggest an alternative** for protecting the vulnerable WebServer02 from insider attacks for Secure Labs on Demand.

Snort needs to operate in inline mode for the "drops" features to take effect. Additionally, alerting needs to be initiated for the specified alert/drop option pair, which enables the "drops" options function successfully.

"enable_decode_drops"-This is the option if in inline mode, which alerts drop packets are on.

Challenge and Analysis

Part 1: Snort: Identifying and Suppressing False Positive Alerts

Record your reasoning that leads to the conclusion that these alerts are false positives.

After viewing the http_inspect alerts, i concluded that they were set off by a authorized HTTP traffic that doesn't present as a malicious threat. The alerts are constant with normal behavior within the environment, which is classified as false positives. By suppressing them, it will help minimize the alert fatigue and focus the attention on actual threats.

Make a screen capture showing the **suppression list** in the Snort interface.