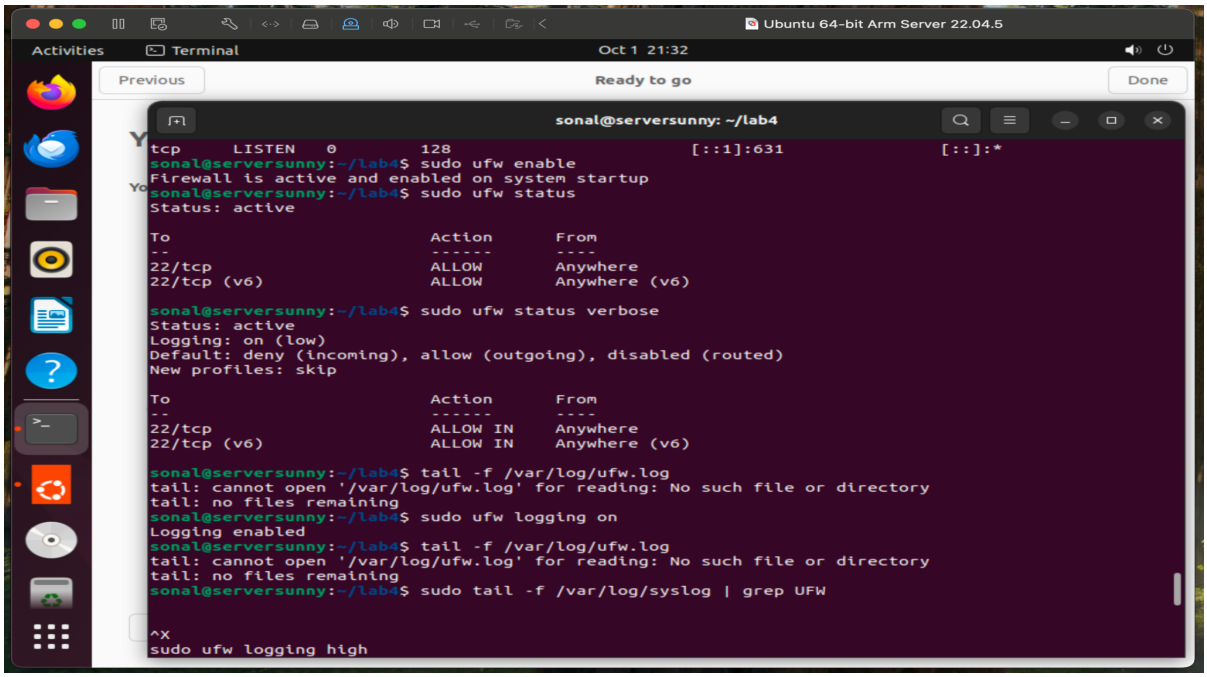
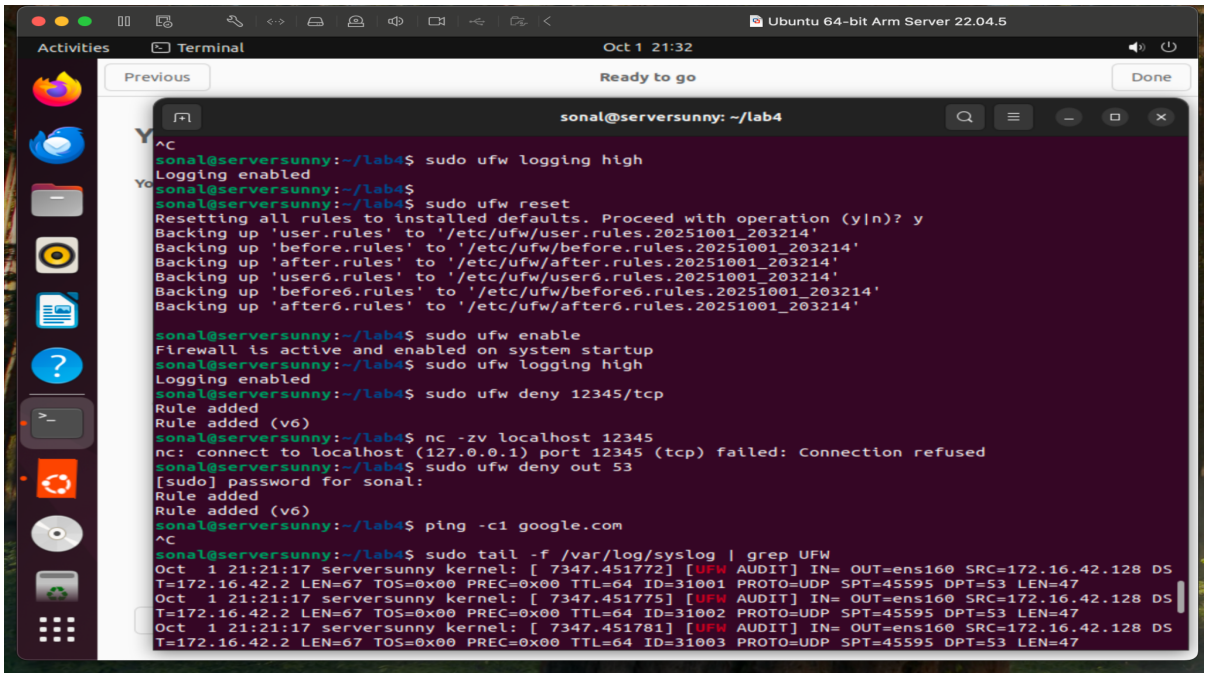
Lab 4: Firewall and Log Analysis

Screenshot 1



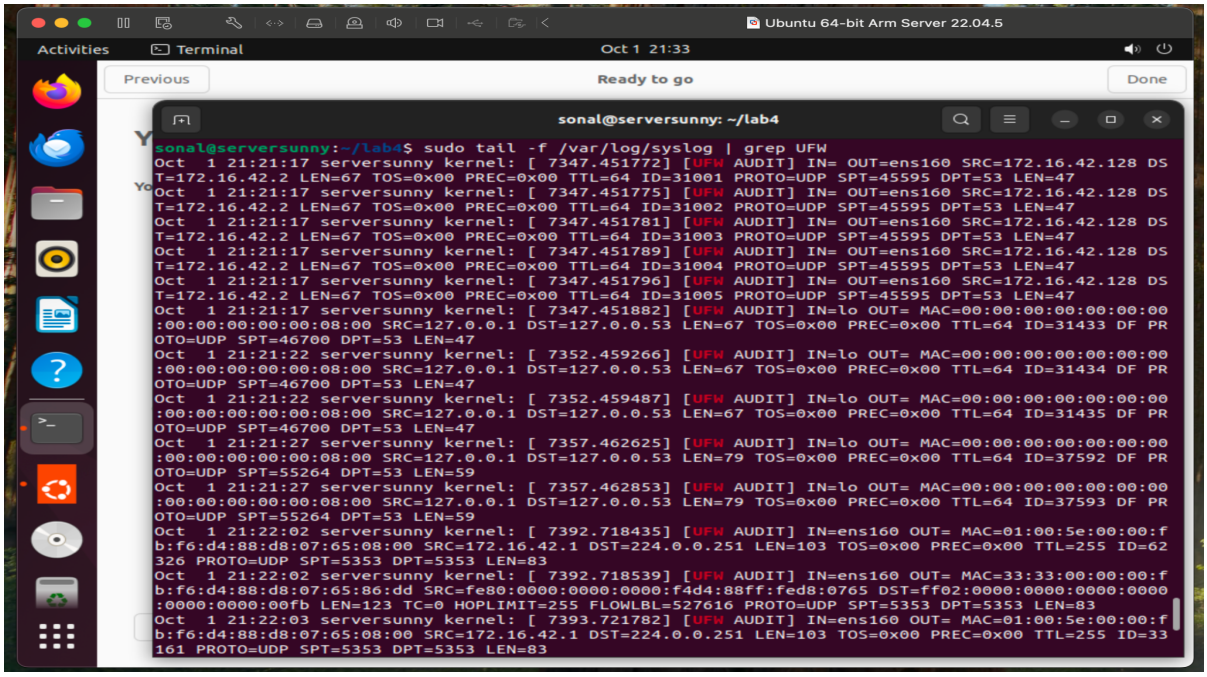
Here I enabled UFW (firewall) and checked its status. Then I turned on verbose mode and tried viewing log files, but they weren't available at first.

Screenshot 2



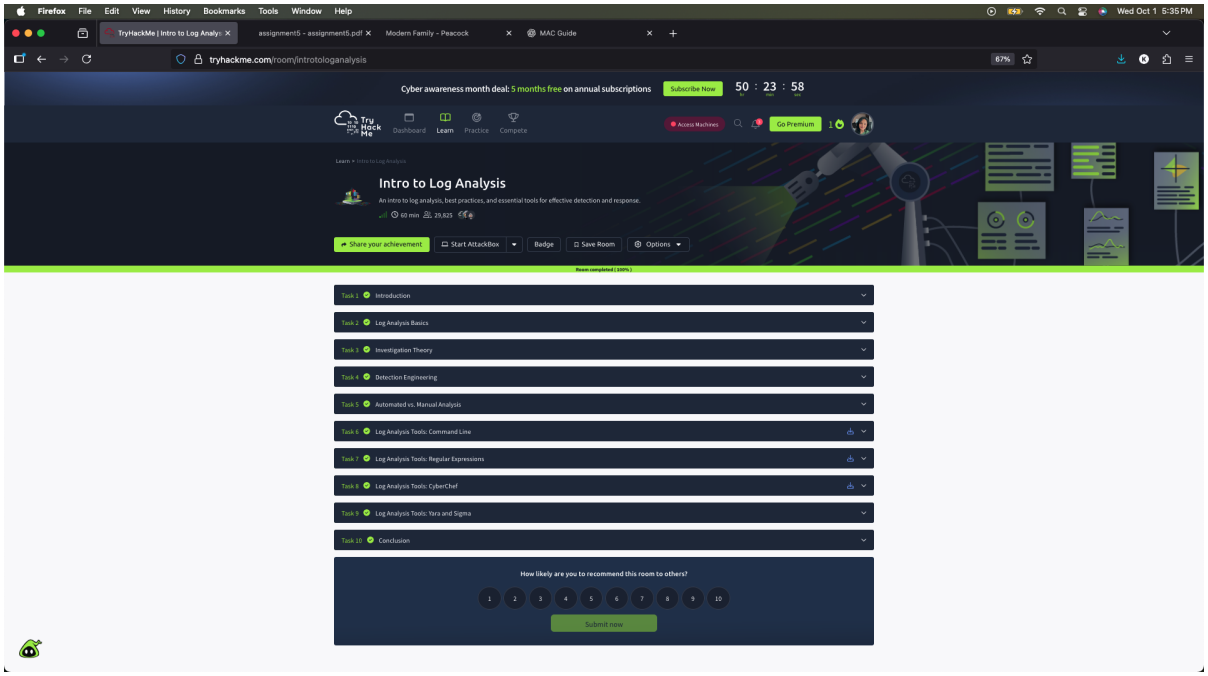
I reset the firewall, enabled logging, and denied access to port 12345. Then I tested with nc (netcat) and confirmed the connection was refused.

Screenshot 3



Here I ran a ping test and checked logs with syslog. This showed UFW audit logs capturing blocked traffic, confirming that firewall rules were being enforced.

TryHackMe Log Analysis Completion



I also completed the TryHackMe ‘Intro to Log Analysis’ module, which covered basics, detection engineering, and log analysis tools.