BRYANT WATKINS

2/26/26

CYSE 601 Snort Lab

Dr. Cooper

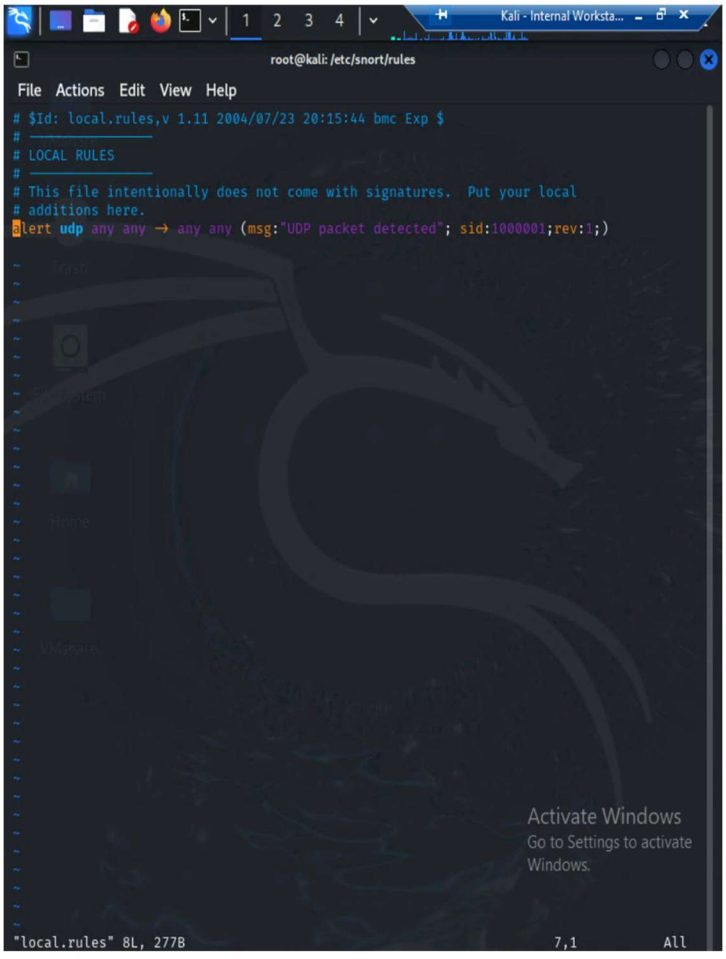
Relevant Systems

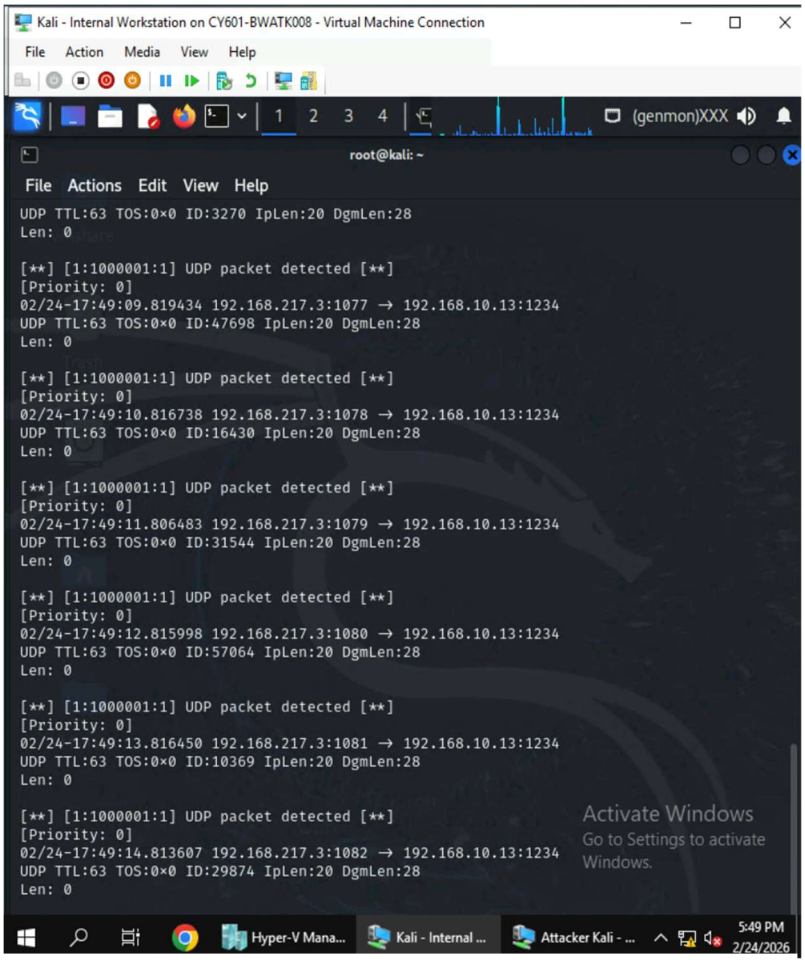
• pfSense firewall VM (IP: 192.168.10.2).

• External Kali Linux machine (IP: 192.168.217.3).

• Internal Kali Linux machine (IP: 192.168.10.13).

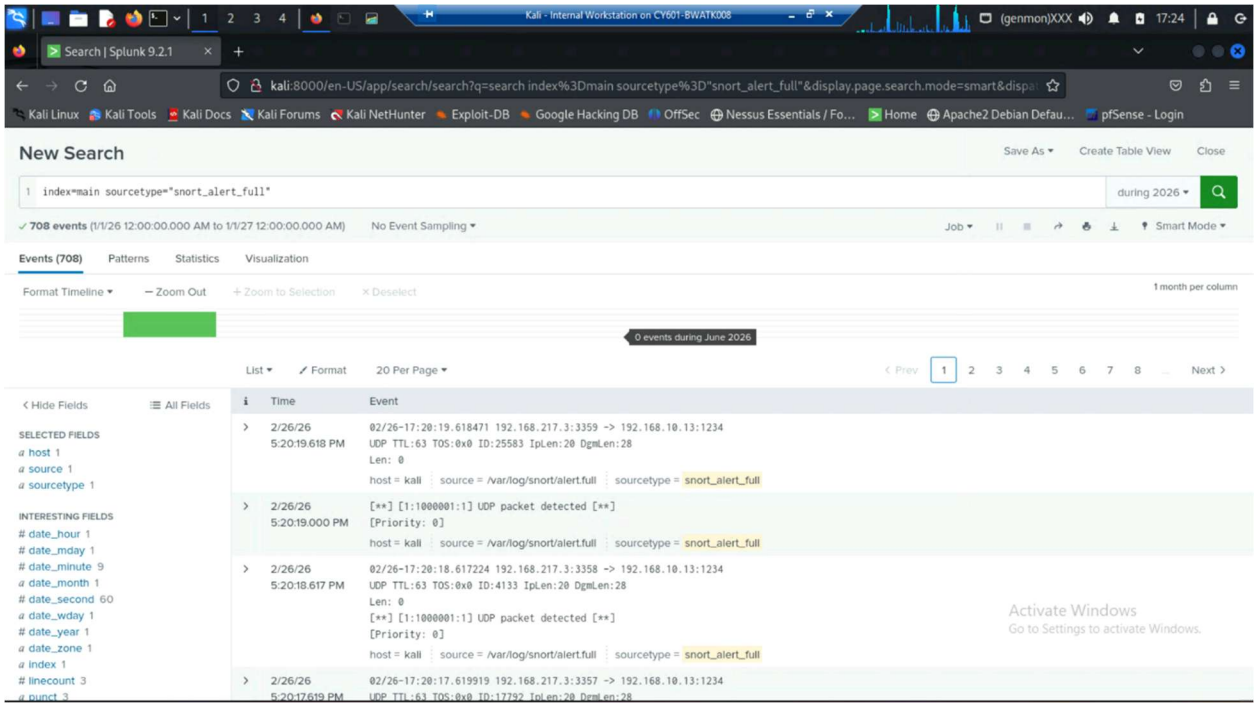
Snort Rule Creation for UDP Alerts

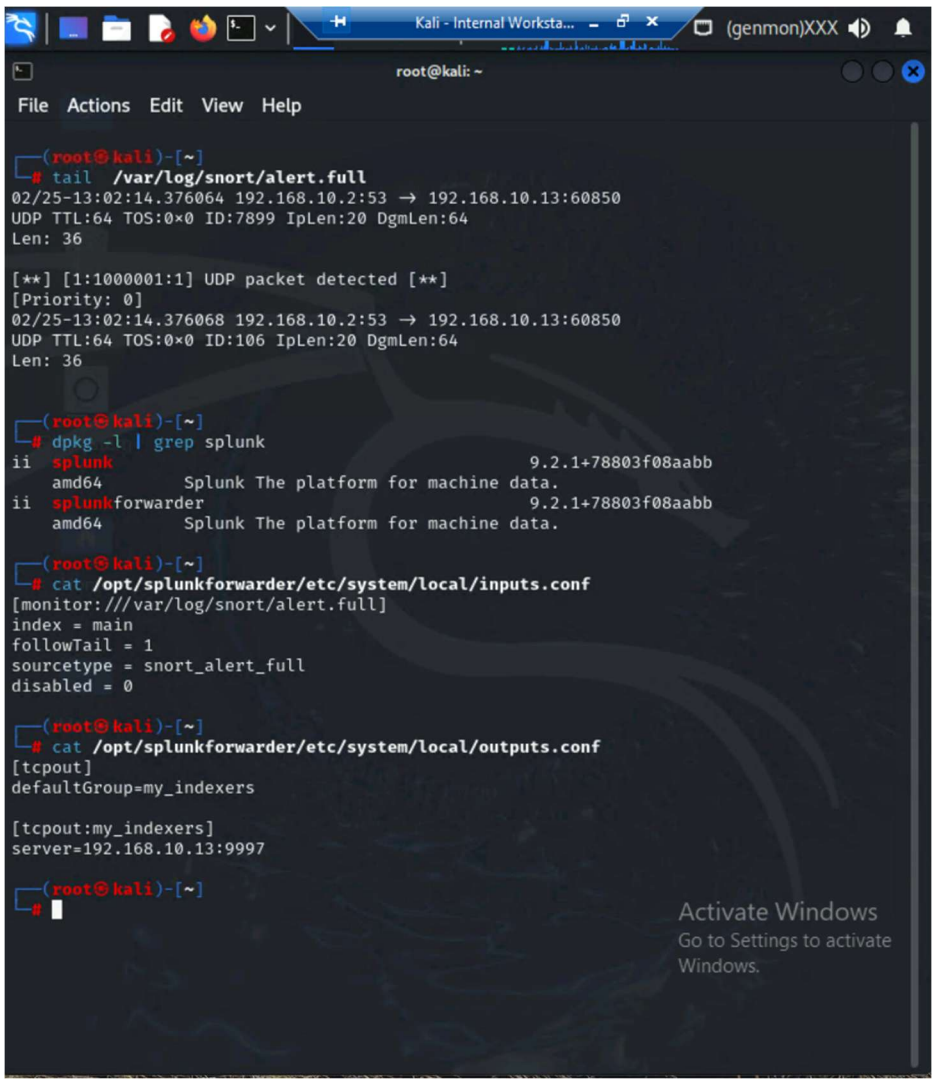




These images illustrate the successful creation of a Snort rule for UDP alerts. The shell scripting, as well as alerts triggered, can be observed.

Integration With Splunk





These images display the successful integration of the splunk tool. Splunk was integrated to monitor and observe UDP intrusion alerts (from Ext Kali to Int Kali) previously configured through snort. The splunk log, as well as the contents of the configuration files, can be observed.