

BRYANT WATKINS

2/26/26

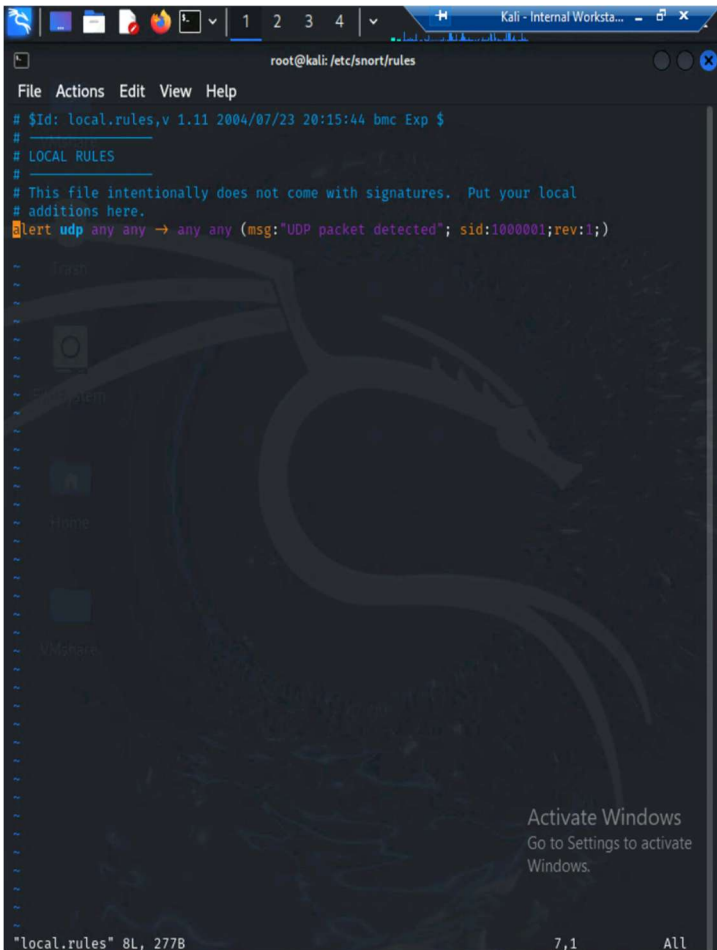
CYSE 601 Snort Lab

Dr. Cooper

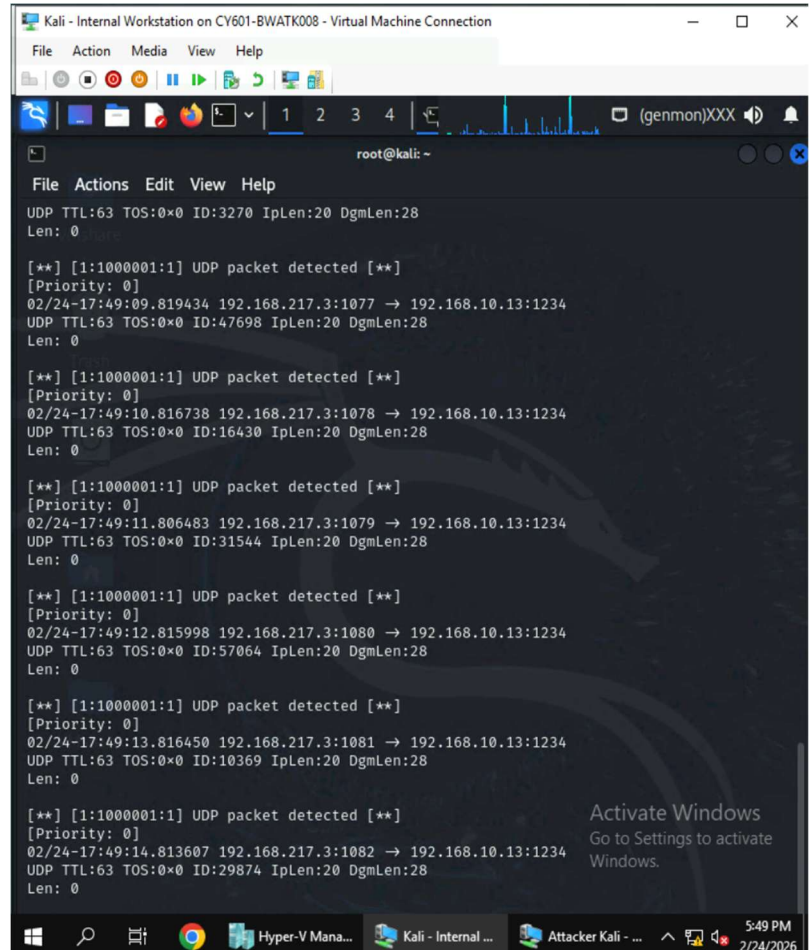
Relevant Systems

- 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



```
root@kali:/etc/snort/rules
File Actions Edit View Help
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
alert udp any any -> any any (msg:'UDP packet detected'; sid:1000001; rev:1;)
```



```
root@kali: ~
File Actions Edit View Help
UDP TTL:63 TOS:0x0 ID:3270 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000001:1] UDP packet detected [**]
[Priority: 0]
02/24-17:49:09.819434 192.168.217.3:1077 -> 192.168.10.13:1234
UDP TTL:63 TOS:0x0 ID:47698 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000001:1] UDP packet detected [**]
[Priority: 0]
02/24-17:49:10.816738 192.168.217.3:1078 -> 192.168.10.13:1234
UDP TTL:63 TOS:0x0 ID:16430 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000001:1] UDP packet detected [**]
[Priority: 0]
02/24-17:49:11.806483 192.168.217.3:1079 -> 192.168.10.13:1234
UDP TTL:63 TOS:0x0 ID:31544 IpLen:20 DgmLen:28
Len: 0

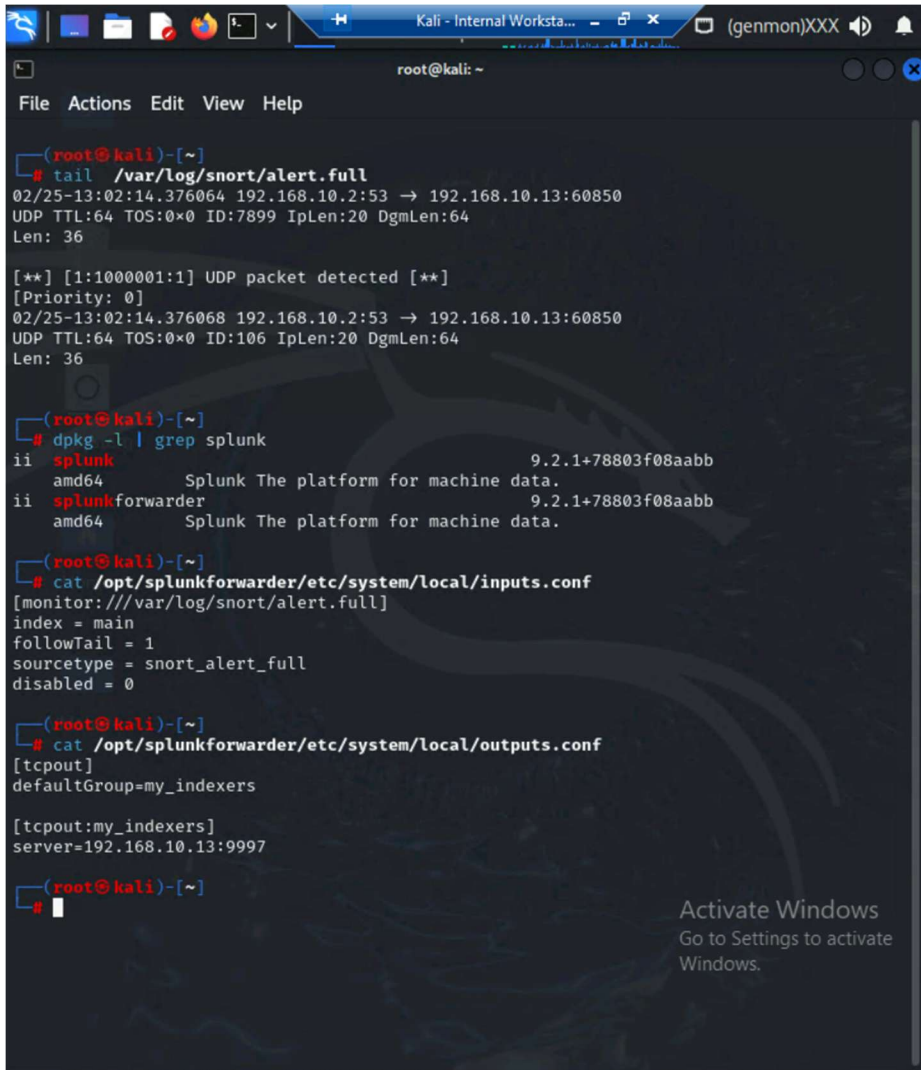
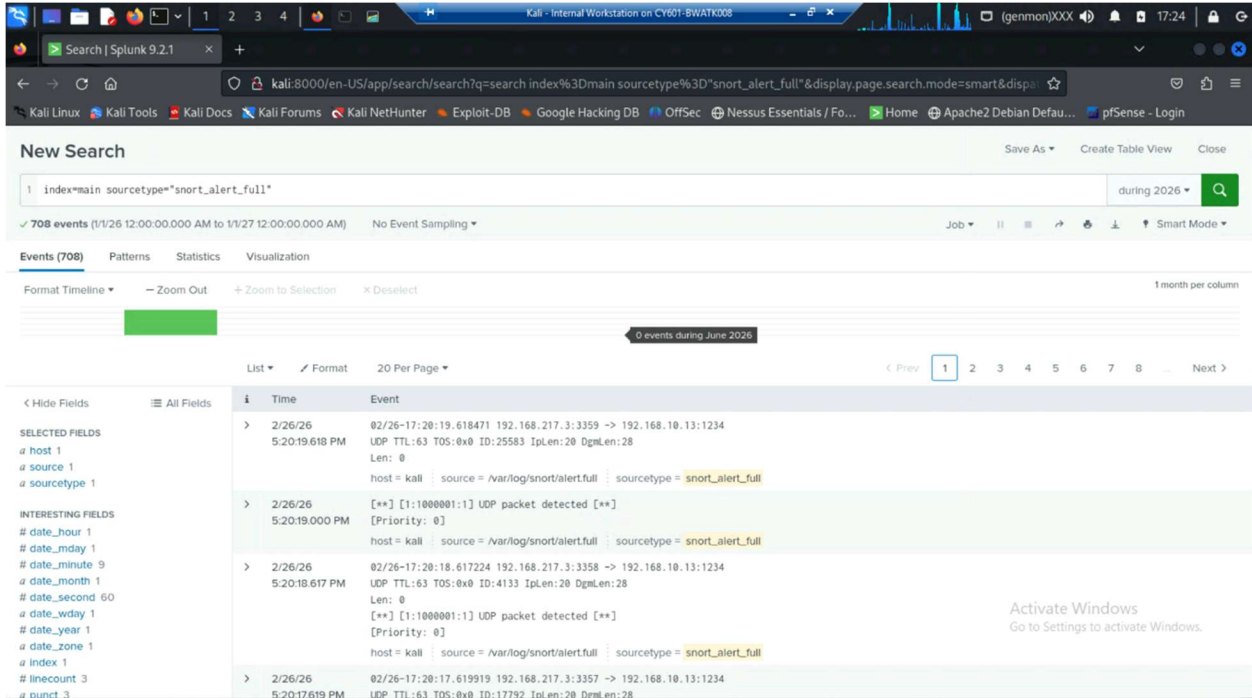
[**] [1:1000001:1] UDP packet detected [**]
[Priority: 0]
02/24-17:49:12.815998 192.168.217.3:1080 -> 192.168.10.13:1234
UDP TTL:63 TOS:0x0 ID:57064 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000001:1] UDP packet detected [**]
[Priority: 0]
02/24-17:49:13.816450 192.168.217.3:1081 -> 192.168.10.13:1234
UDP TTL:63 TOS:0x0 ID:10369 IpLen:20 DgmLen:28
Len: 0

[**] [1:1000001:1] UDP packet detected [**]
[Priority: 0]
02/24-17:49:14.813607 192.168.217.3:1082 -> 192.168.10.13:1234
UDP TTL:63 TOS:0x0 ID:29874 IpLen:20 DgmLen:28
Len: 0
```

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.