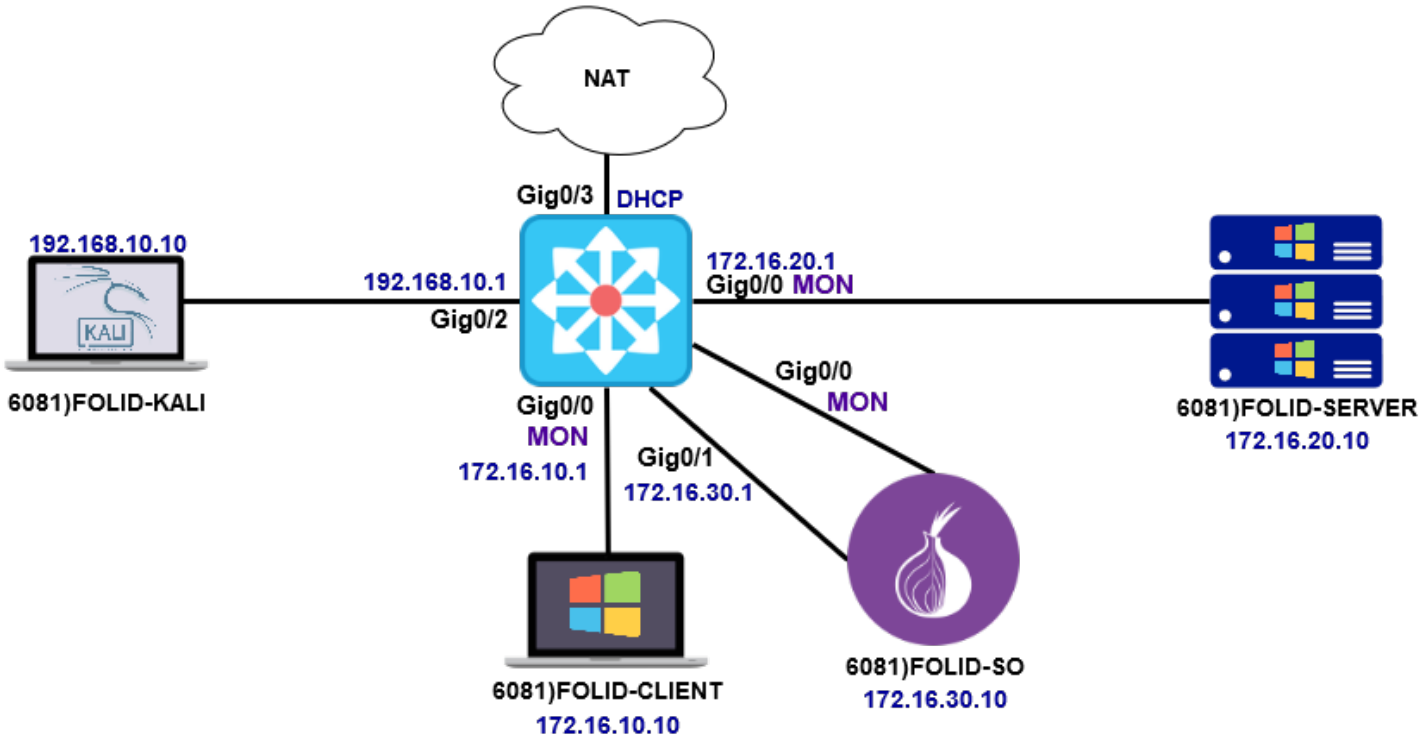
Lab 8 – NSM Consoles - Part 2

Lab Topology and Learning Goals



In this lab you learn how to perform basic operations on the NSM consoles that Security Onion offers

Required Resources

- **VMware Workstation 15**

Active Hosts

- **6081)Router**
- **6081)FOLID-SO**
- **6081)FOLID-SERVER**
- **6081)FOLID-CLIENT**
- **6081)FOLID-KALI**

Submission Instructions

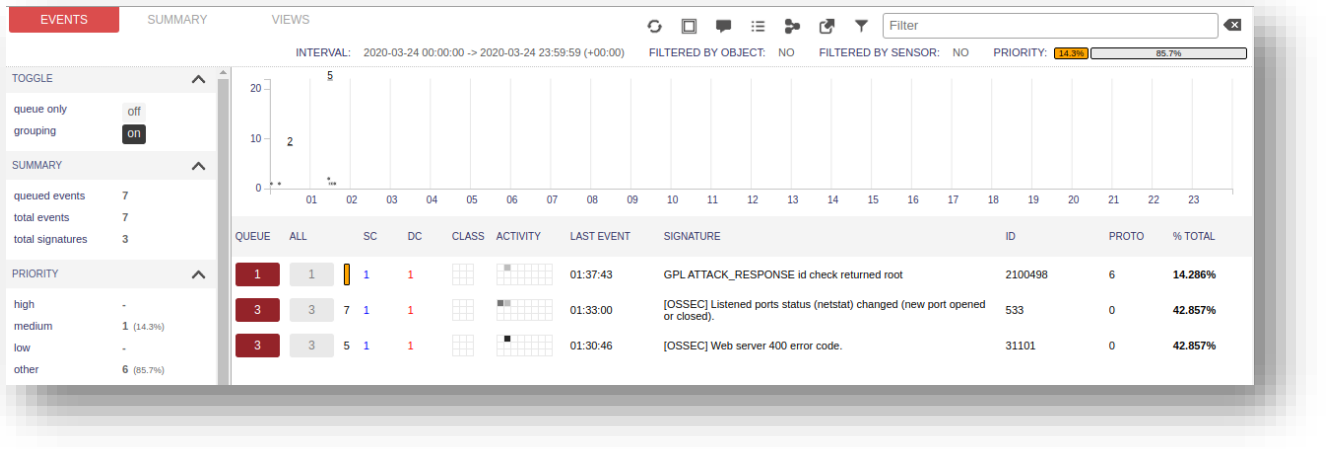
Submit your completed lab to the appropriate lab quiz on FOL

- You can attempt the quiz multiple time, but only the last attempt will be graded
- Submissions are accepted until 11:59 PM of the same day
- Submissions by email will not be accepted
- All screenshots must include you FOLID (where FOLID is your FOL username)

Lab 8 – NSM Consoles - Part 2

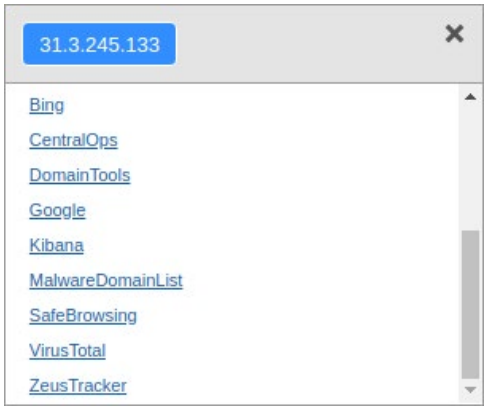
Kibana

Kibana is a new tool that appeared in recent versions of Security Onion (with the migration to elastic search). Kibana is can rerate dashboards to view data over time, includes powerful search capabilities and breaks data down to a very low level with Bro



We will start this lab where we ended the previous, when your setup has booted, start Squert and login to the dashboard

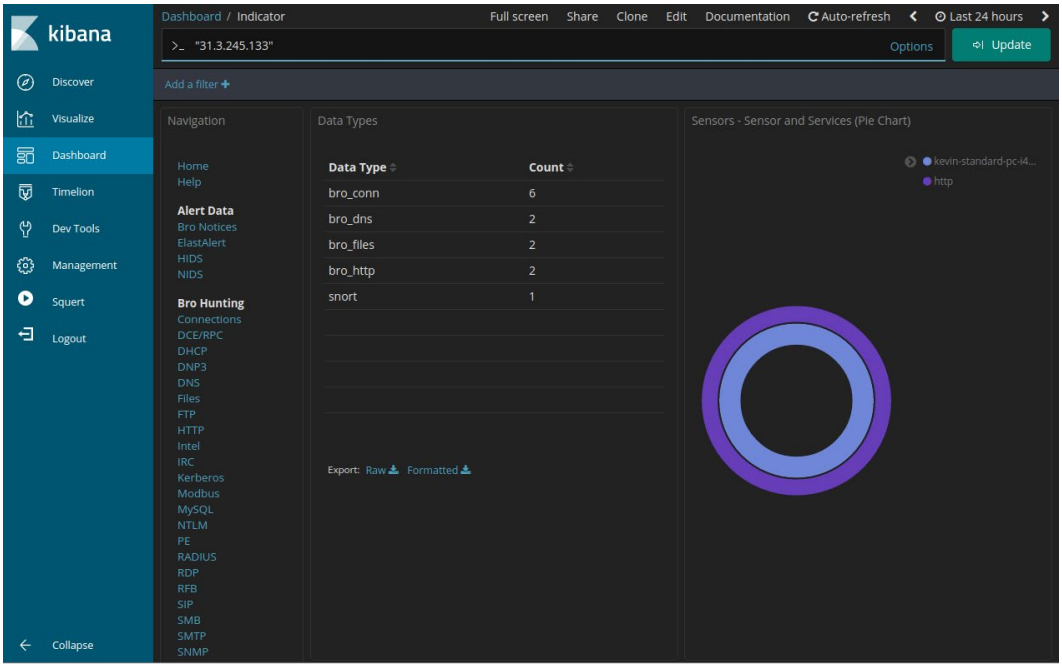
If the previous event (GPL_ATTACK_RESPONSE id check returned root) is not still present in the list, regenerate the event by visiting http://testmyids.com/ on the client machine (if you are having trouble getting the event to appear, try clearing your browsing history)



To pivot from Squert to Kibana, click the source IP address, and select Kibana from the pivot list

Kibana should automatically open in a new tab. It may take a minute for the page to fully load

Lab 8 – NSM Consoles - Part 2

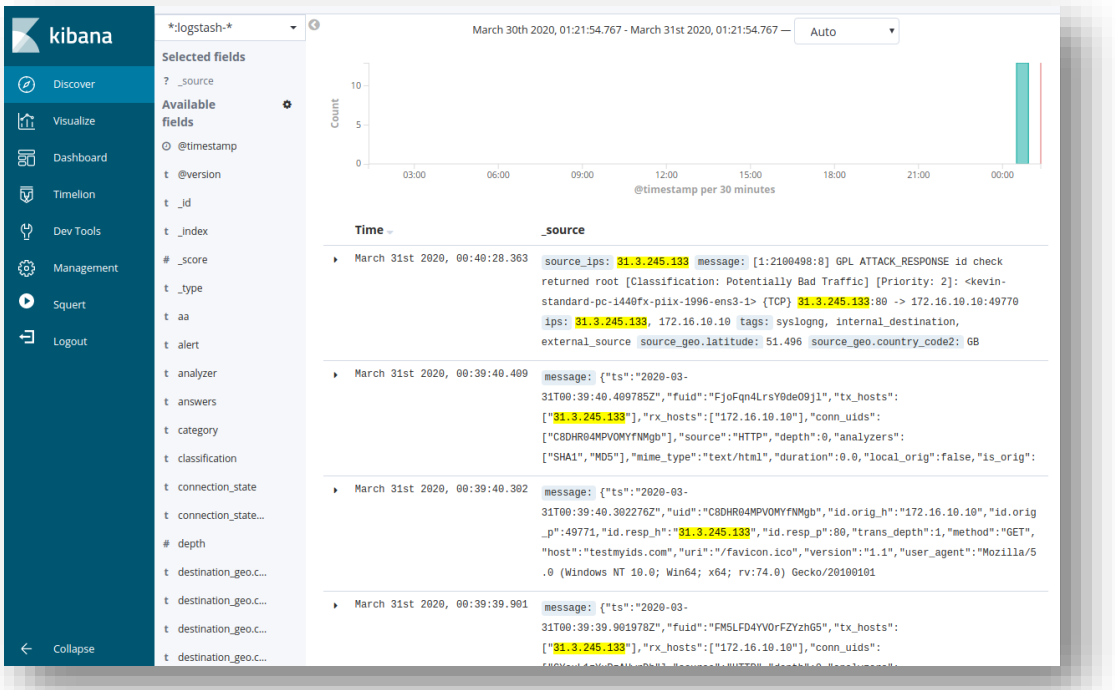


Kibana displays a wealth of information related to the IP address including, the source of the data (Bro log, NIDS, HIDS), statistics about the most frequent IP addresses, DNS queries, HTTP/SSL information, HTTP MIME types, etc. Many of the fields are clickable and refine the dashboard information to the selected datapoint.

Add a screenshot showing the All Logs section related to the IP address to the Lab 8 quiz, make sure you include your FOLID as displayed in the Squert tab

Notice the value of the search at the top of the page, copy the search term and click on the Discover menu item, then paste the string and search

Lab 8 – NSM Consoles - Part 2



The information that is returned details all the data that is available in Elasticsearch for the specified IP address. Expand each item, paying attention to the event_type field to determine the source of the data.

Return to the Dashboard menu item and do a search for the IP address of your Windows server

Add a screenshot showing top 10 DNS queries to the Lab 8 quiz, make sure you include your FOLID as displayed in the Squert tab

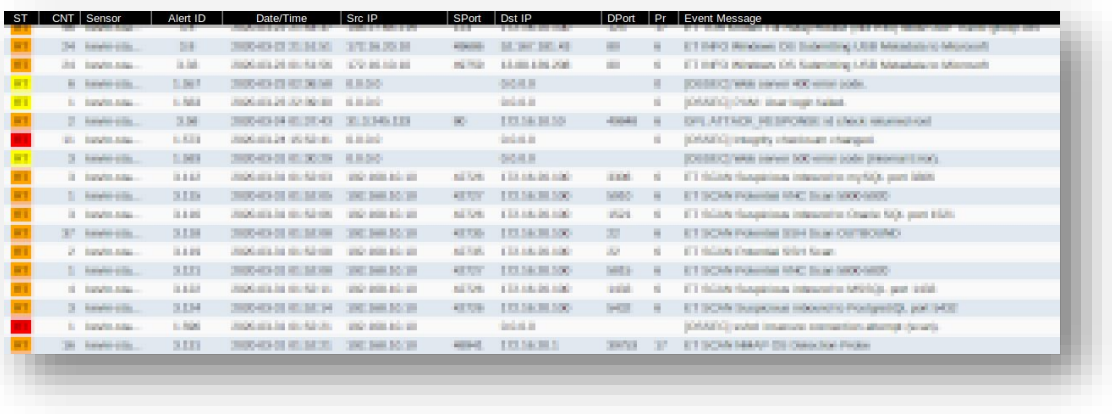
Lab 8 – NSM Consoles - Part 2

Network Scanning

If not already running, power on your Kali Linux host.

From the terminal, run a nmap intense scan without ping (-T4 -A -v -Pn) on the network 172.16.20.0/24

When the scan is complete, you can shut down Kali Linux.



On your SO sensor, open Sguil and observe the new events that have appeared in the RealTime Events tab.

In Squert, filter the results by searching for the source IP address of your Kali Linux host.

Pivot to Kibana using the source IP address for the Kali Linux host.

Provide answer to the questions found in the Lab 8 quiz, using the collected event data as the source of your answers:

Take a running snapshot of your **SO** host called **Lab 8 Complete**, then shutdown.

Shutdown the other hosts and take a snapshot called **Lab 8 complete**

Submit your completed **Lab 8** quiz