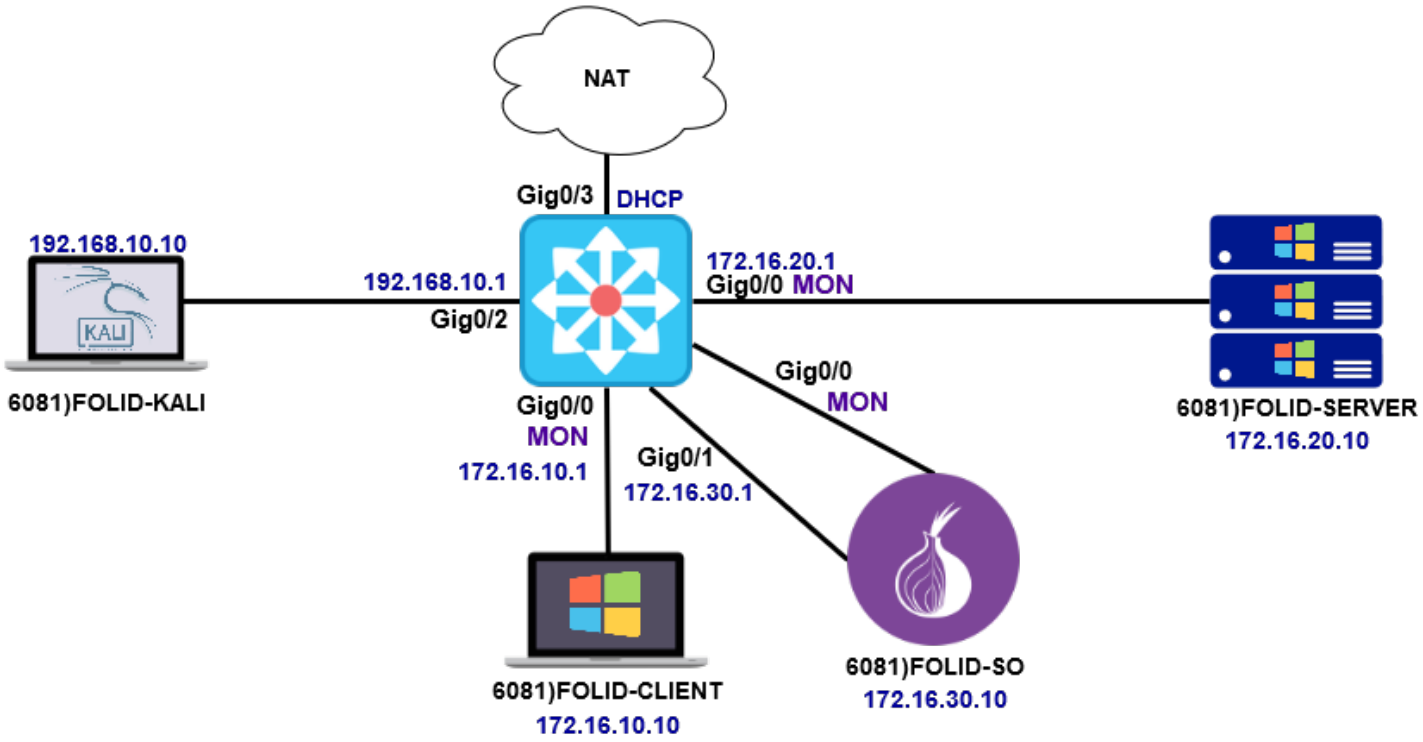
Lab 7 – NSM Consoles

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**

Submission Instructions

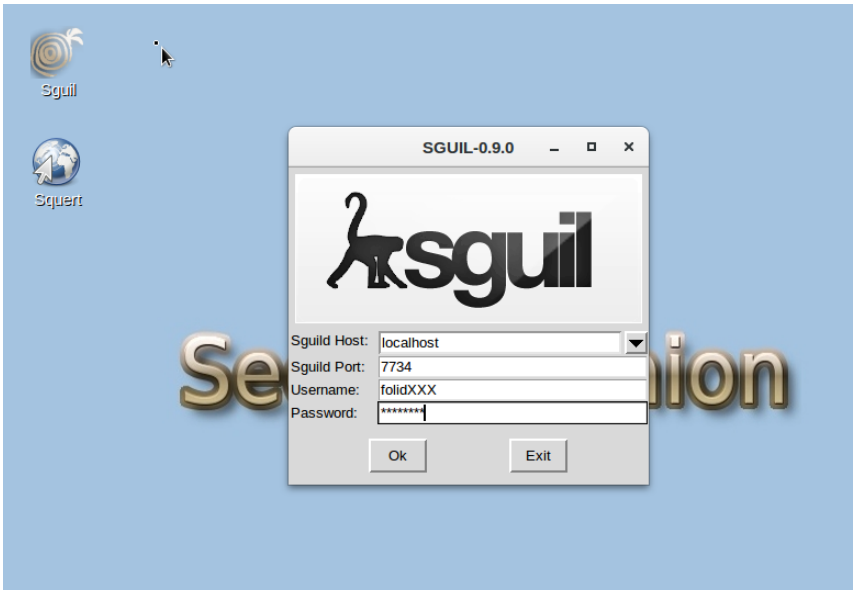
Submit your completed lab to the appropriate lab quiz on FOL

- 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)

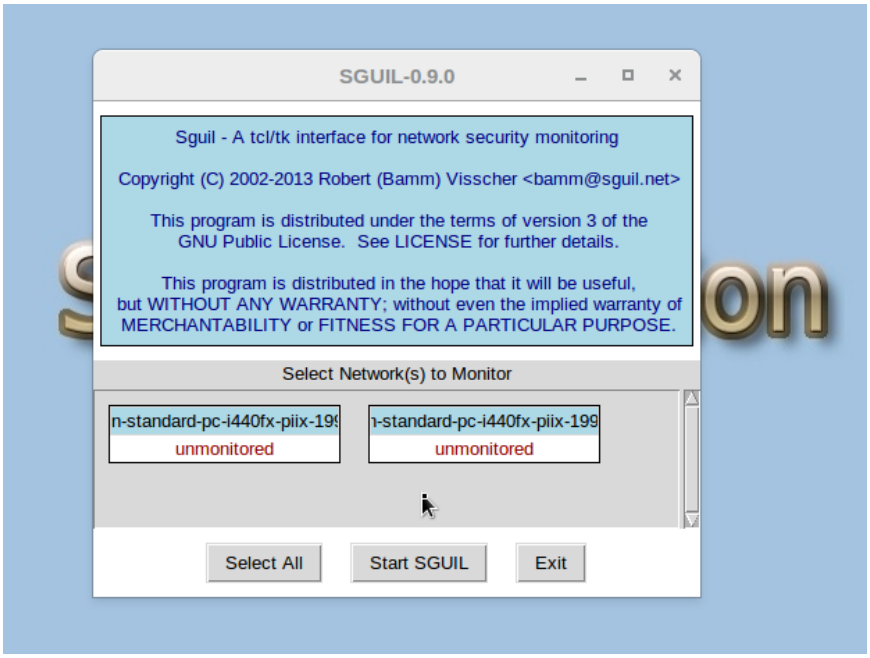
Lab 7 – NSM Consoles

Sguil

Sguil is the NSM console of choice for many analysts. Unlike most newer consoles, Sguil still relies on a “thick client” to access the interface. Start by logging into Sguil



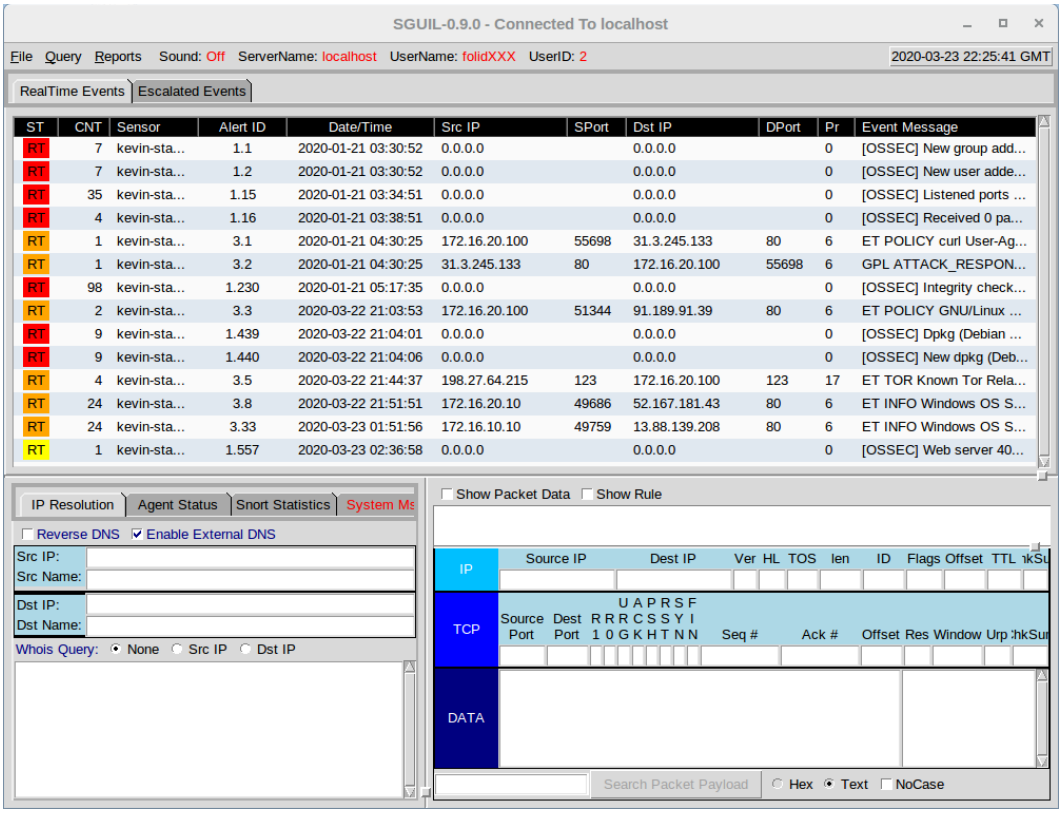
Enter the username and password that you setup in Lab 2



When prompted, select All Interfaces and start Sguil

Lab 7 – NSM Consoles

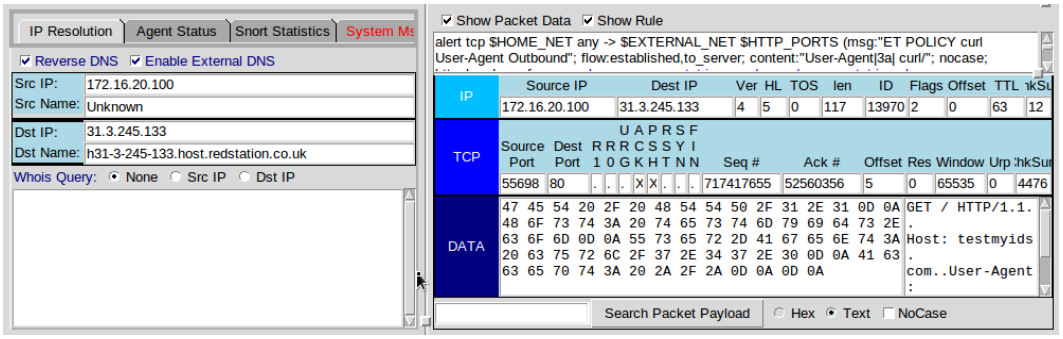
You will be presented with a window similar to that below (perhaps with less events)



What data is presented to you in this window?

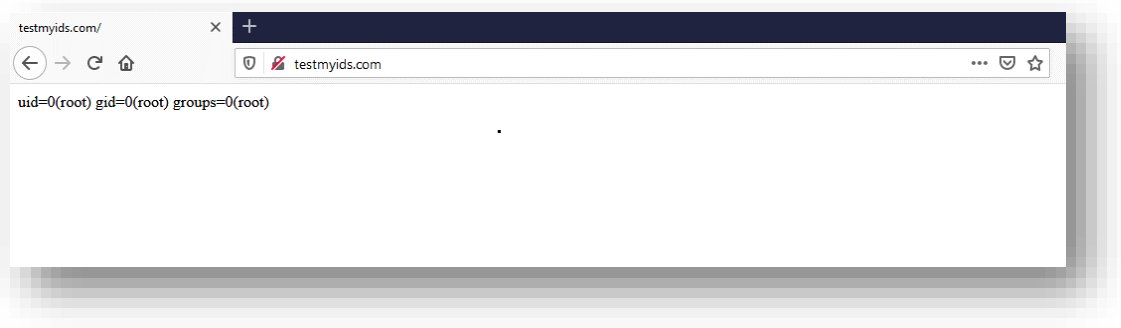
How can this data be used to discover intruders on the network?

Observe the source IPs listed in the window, identify the hosts that those IPs belong to.



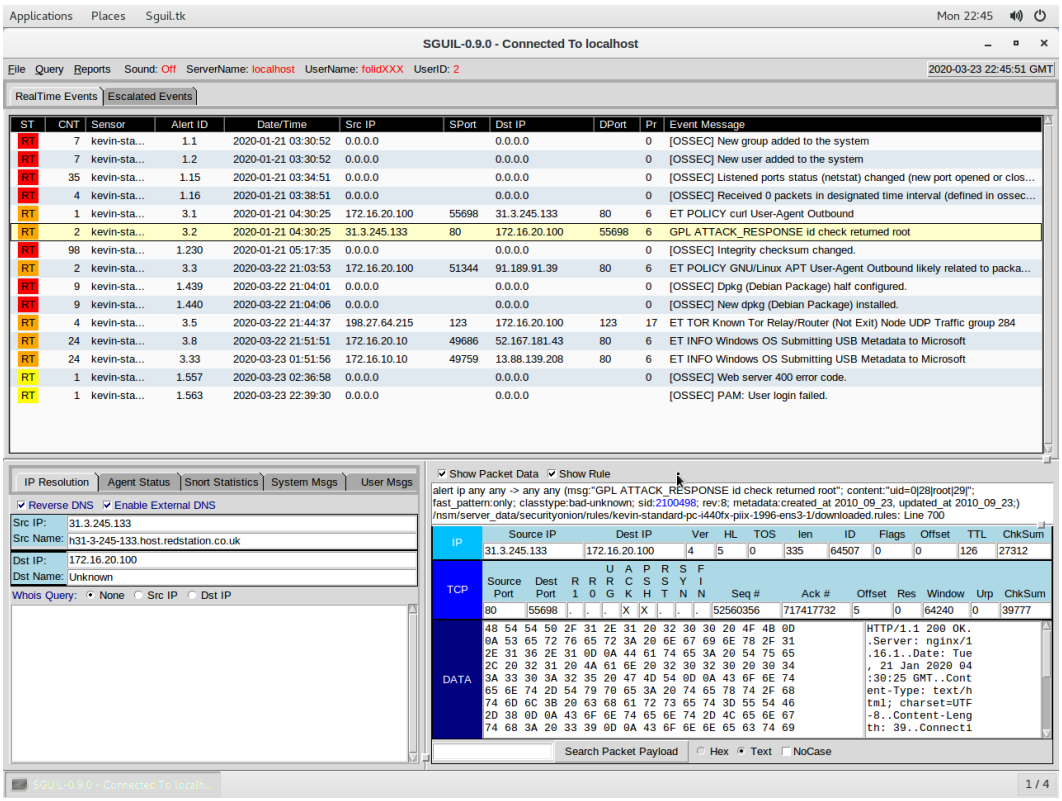
Get additional information by enabling the **Reverse DNS**, **Show Packet Data**, and **Show Rule** checkboxes

Lab 7 – NSM Consoles



On the Windows Client VM, generate some interesting traffic by opening Firefox and navigating to http://testmyids.fanco.ml

Observe the result in Sguil, can you find the new event related to HTTP (port 80)?

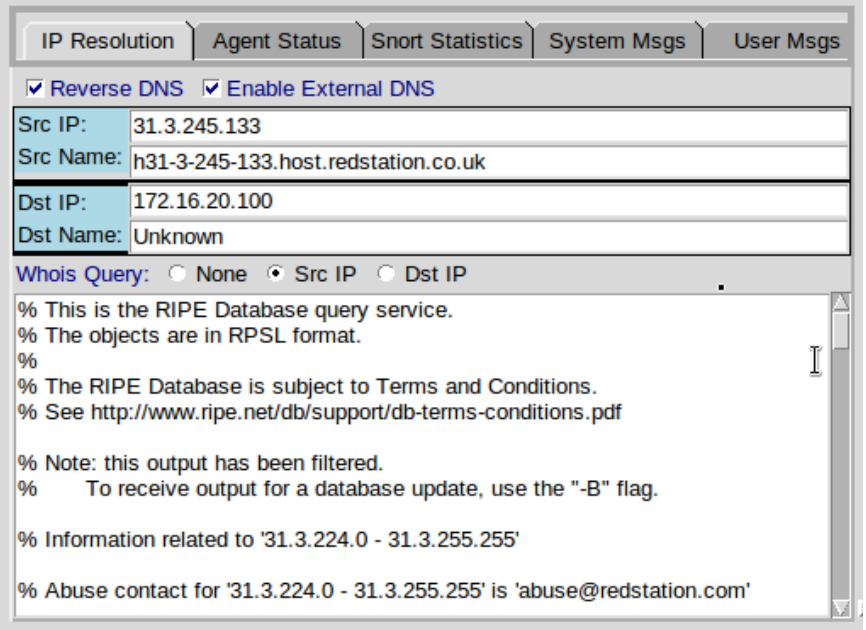


Highlight the event to see additional details in the lower panels

What is the name of the host that served the webpage according to reverse DNS?

Add a screenshot showing the name to the Lab 7 quiz, make sure you include your UserName as displayed in the top of the Sguil window

Lab 7 – NSM Consoles



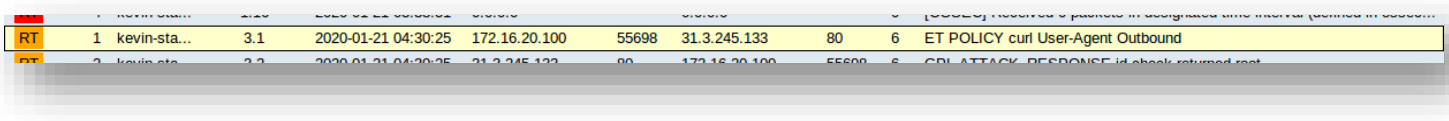
In the lower left panel, run a **whois** query on the source IP.

If this information is current, what is the name of the website owner?

In what country do could you assume the website is located in?

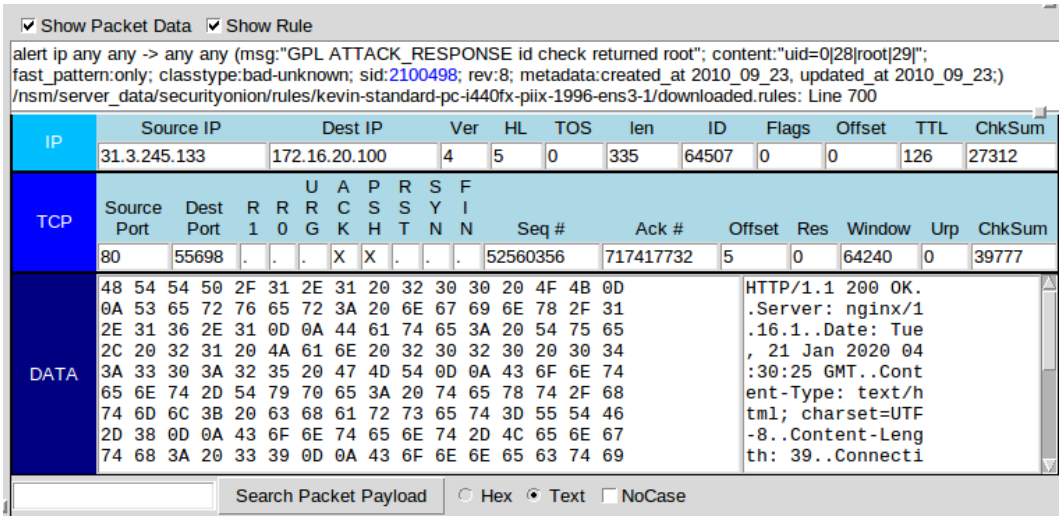
Run a whois query on the destination IP.

Can you find the owner of this address? If not, why do you think this is so?



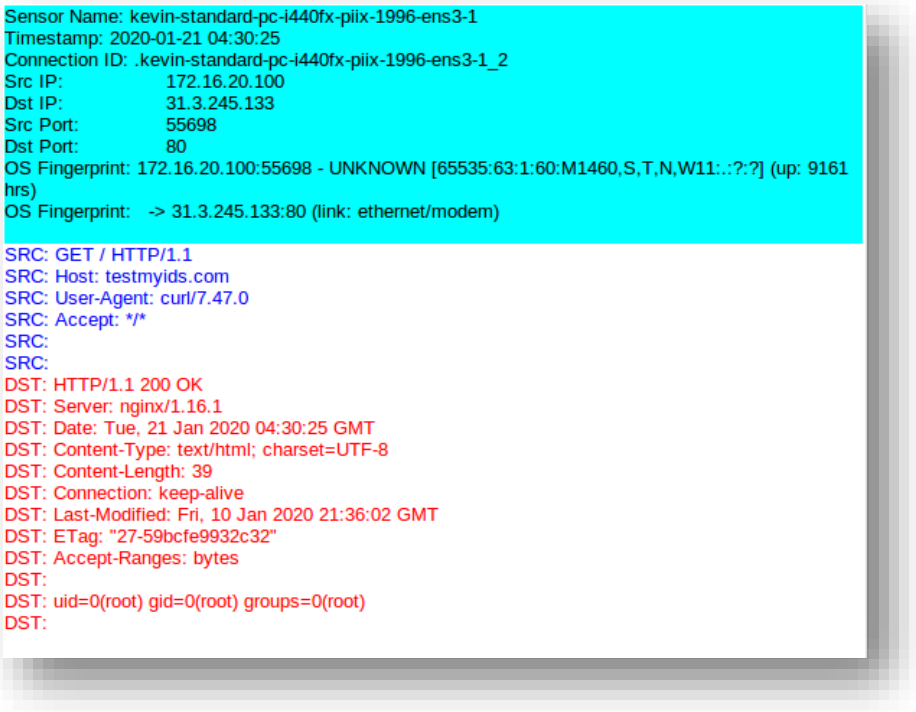
Observe the Event Message in the main panel. What is this event trying to communicate with you? (a web search may help you understand this).

Lab 7 – NSM Consoles



In the lower right panel, you can see the alert rule that the traffic triggered.

Below this, you see the details of the full content data (capture/trace); what layers of the OSI model are displayed here?



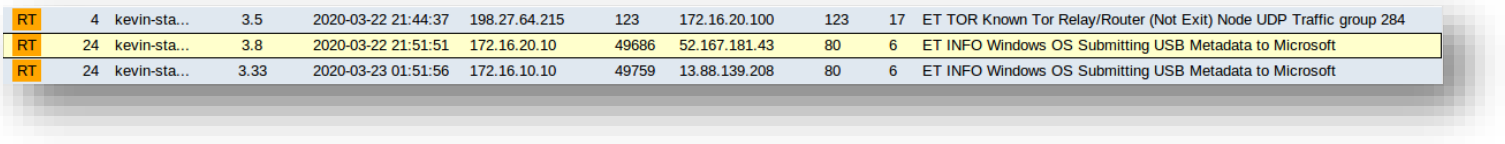
On the main panel, right-click the **Alert ID** of the event and view the **Transcript.**

A new window opens with the transcript shown.

Lab 7 – NSM Consoles

View Correlated Events

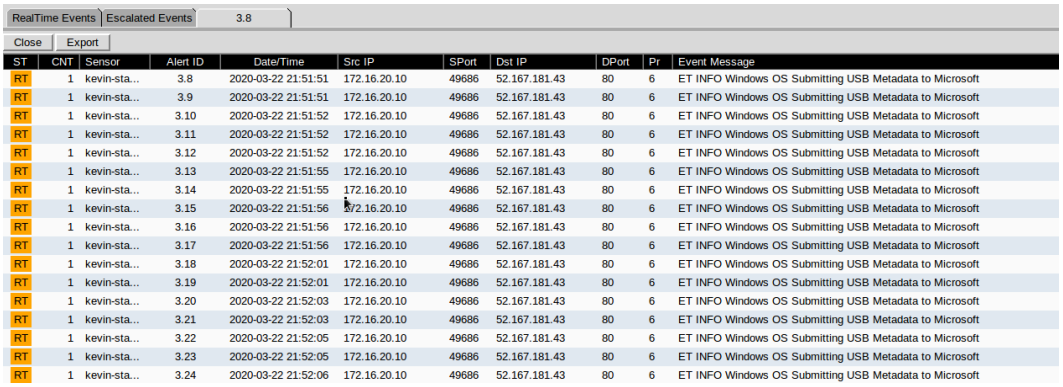
Sguil groups events that are related to each other to make the event easier to read and recognize.



RT	4	kevin-sta...	3.5	2020-03-22 21:44:37	198.27.64.215	123	172.16.20.100	123	17	ET TOR Known Tor Relay/Router (Not Exit) Node UDP Traffic group 284
RT	24	kevin-sta...	3.8	2020-03-22 21:51:51	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	24	kevin-sta...	3.33	2020-03-23 01:51:56	172.16.10.10	49759	13.88.139.208	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft

In the main panel, select an event that has a value greater than **1** in the CNT column.

Right-click the event and open **View Correlated Events** from the menu



RealTime Events | Escalated Events | 3.8

Close | Export

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	kevin-sta...	3.8	2020-03-22 21:51:51	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.9	2020-03-22 21:51:51	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.10	2020-03-22 21:51:52	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.11	2020-03-22 21:51:52	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.12	2020-03-22 21:51:52	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.13	2020-03-22 21:51:55	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.14	2020-03-22 21:51:55	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.15	2020-03-22 21:51:56	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.16	2020-03-22 21:51:56	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.17	2020-03-22 21:51:56	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.18	2020-03-22 21:52:01	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.19	2020-03-22 21:52:01	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.20	2020-03-22 21:52:03	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.21	2020-03-22 21:52:03	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.22	2020-03-22 21:52:05	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.23	2020-03-22 21:52:05	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft
RT	1	kevin-sta...	3.24	2020-03-22 21:52:06	172.16.20.10	49686	52.167.181.43	80	6	ET INFO Windows OS Submitting USB Metadata to Microsoft

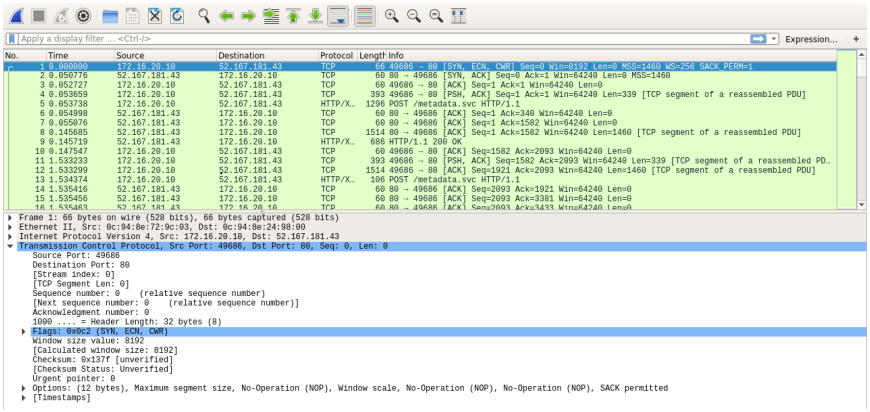
A new tab will open detailing every instance of the selected event.

Browse the information to see how long the sensor was tracking this event (the start and most recent dates)

Might this event be considered suspicious or malicious?

Add a screenshot showing the correlated events to the Lab 7 Quiz, make sure you include your UserName as displayed in the top of the Sguil window

Lab 7 – NSM Consoles

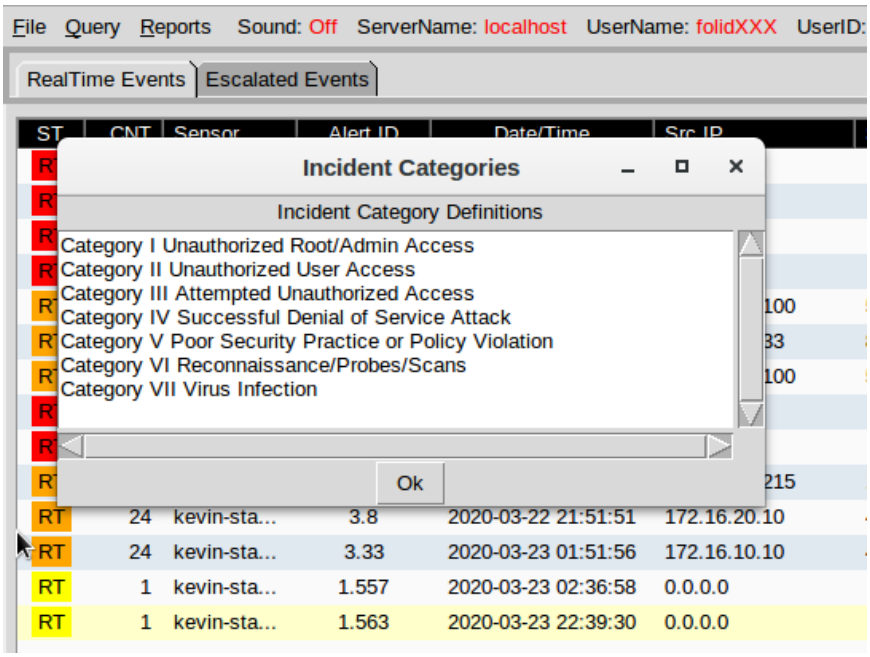


Select the first event in the window, right-click and open Wireshark

Use the techniques you learned in previous labs to find out many packets were exchanged between hosts, and how much data (in bytes) was transferred.

Are there any objects (files) that you can extract from the trace?

Close Wireshark and continue

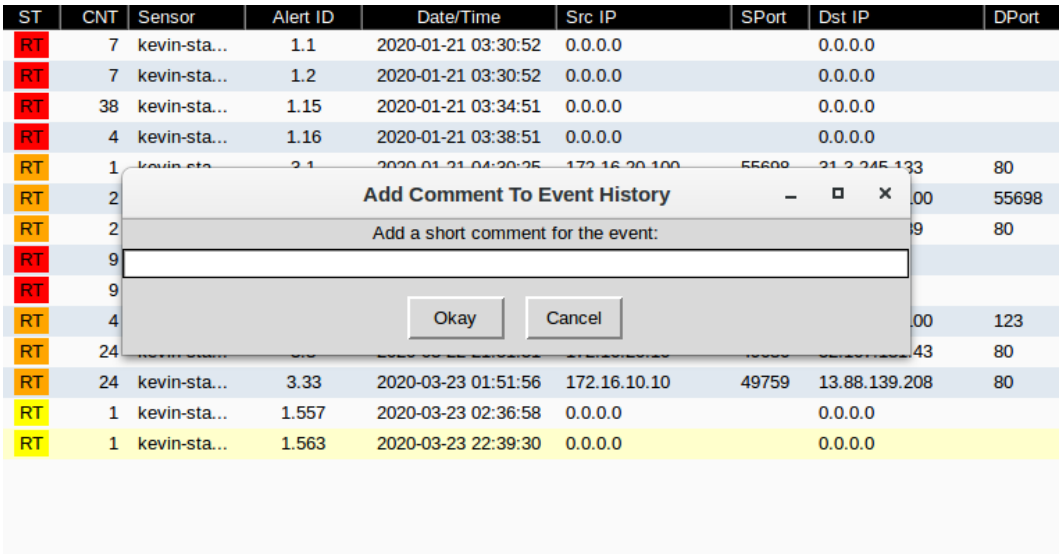


Back in the Real Time Events Tab, view the available event categories by clicking the file menu and selecting Display Incident Categories from the menu.

Make note of the category numbers (remember these are mapped to the F1-F7 keys)

Close the window.

Lab 7 – NSM Consoles



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort
RT	7	kevin-sta...	1.1	2020-01-21 03:30:52	0.0.0.0		0.0.0.0	
RT	7	kevin-sta...	1.2	2020-01-21 03:30:52	0.0.0.0		0.0.0.0	
RT	38	kevin-sta...	1.15	2020-01-21 03:34:51	0.0.0.0		0.0.0.0	
RT	4	kevin-sta...	1.16	2020-01-21 03:38:51	0.0.0.0		0.0.0.0	
RT	1							80
RT	2							55698
RT	2							80
RT	9							
RT	9							
RT	4							123
RT	24							80
RT	24	kevin-sta...	3.33	2020-03-23 01:51:56	172.16.10.10	49759	13.88.139.208	80
RT	1	kevin-sta...	1.557	2020-03-23 02:36:58	0.0.0.0		0.0.0.0	
RT	1	kevin-sta...	1.563	2020-03-23 22:39:30	0.0.0.0		0.0.0.0	

Escalate the event you generated by visiting http://testmyids.fanco.ml by highlighting the event and pressing the F9 key.

Add a comment that a senior analyst would see.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
ES	1	kevin-sta...	3.2	2020-01-21 04:30:25	31.3.245.133	80	172.16.20.100	55698	6	GPL ATTACK_RESPONSE id check returned root
ES	1	kevin-sta...	3.57	2020-03-23 22:42:23	31.3.245.133	80	172.16.10.10	49800	6	GPL ATTACK_RESPONSE id check returned root

Switch to the Escalated Events tab and notice that the event is now present in that tab.

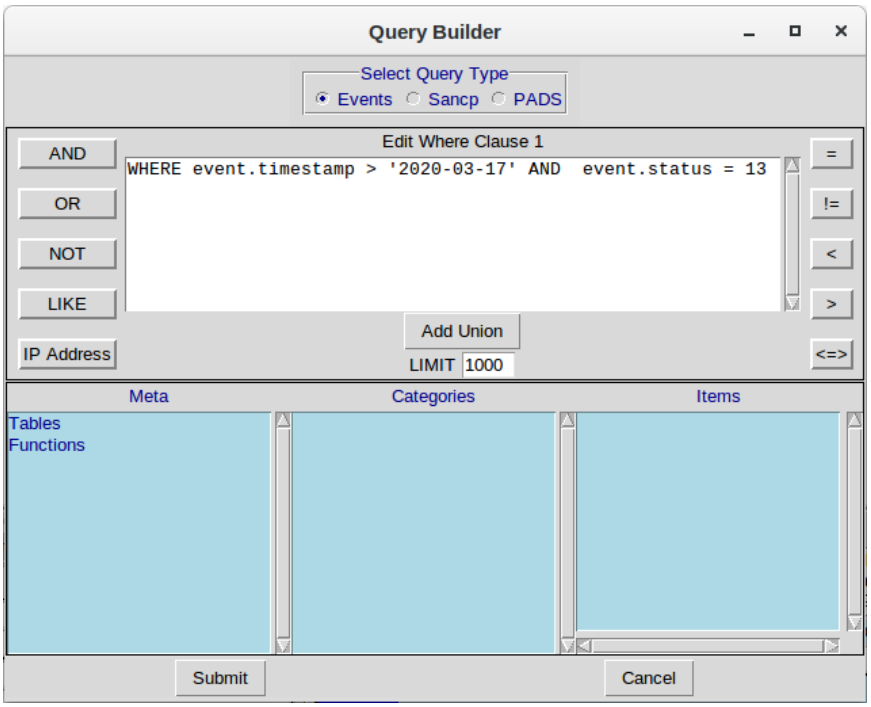
Right click the Alert ID value and select View Event History to view to comment that was applied

Categorize the event as an Attempted Unauthorized Access.

The event has disappeared from the console.

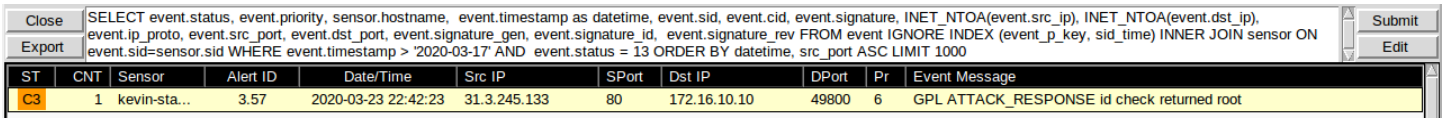
Lab 7 – NSM Consoles

To view dismissed events of a particular category, navigate to **Query** > **Query by Category** > **Cat III Attempted Unauthorized Access.**



The Query Builder window will open with a SQL query present in the window. You could customize this query to reduce the output of the query, but we are looking for only one event.

Submit the query.



You will now see the query that was run, and the event that you dismissed, updated with the Category III status indicator.

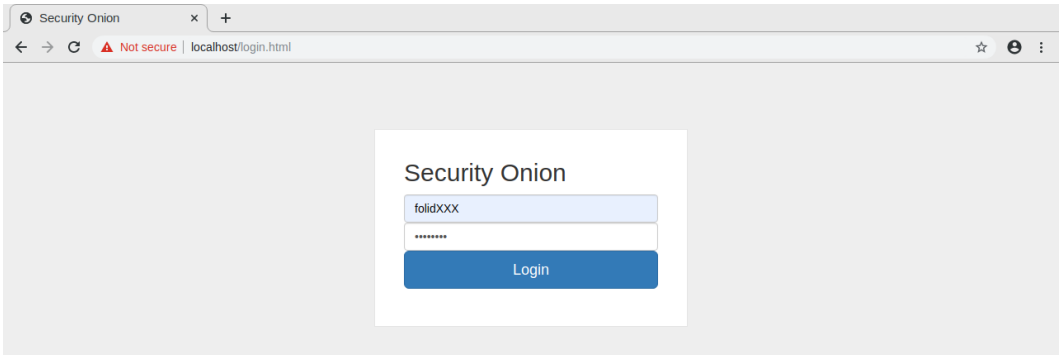
Add a screenshot showing the query results to the Lab 7 Quiz, make sure you include your UserName as displayed in the top of the Sguil window

Close Sguil

Lab 7 – NSM Consoles

Squert

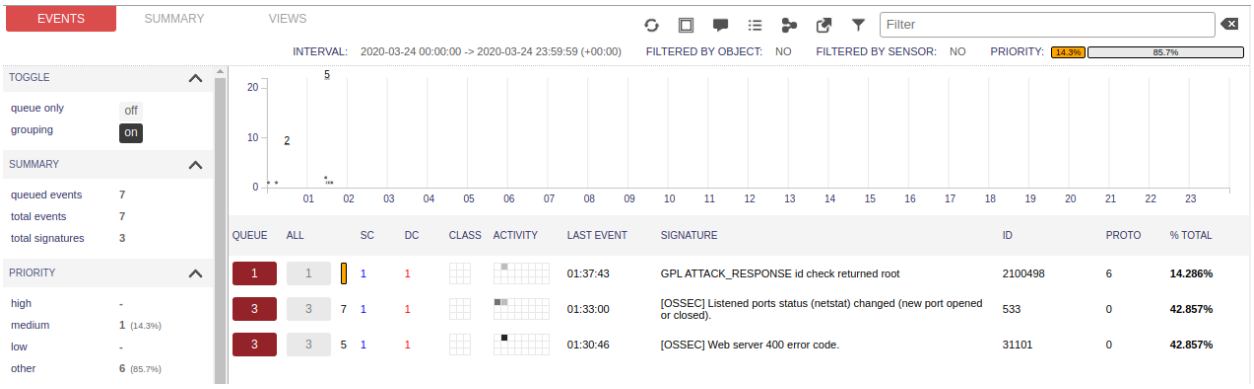
Squert allows you to access the Sguil database from your browser, as well as adding visual tools to interpret data.



Open Squert from the desktop and login with the user you created in lab 3.

You may have less event data in Squert than you did in the Sguil console.

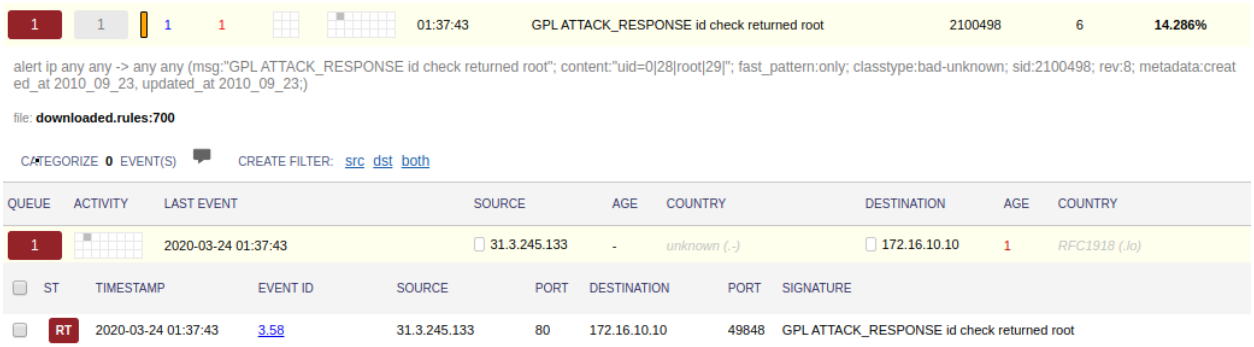
Regenerate the event you created earlier on the Windows client by clearing your history and then revisiting http://testmyids.fanco.ml



Observe the event in Squert, noticing that the dashboard does not present as much information as the Sguil dashboard.

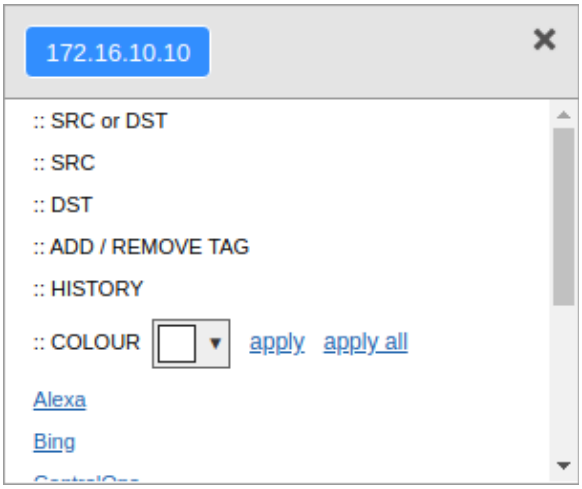
Click on the event to display alert information above the event.

Lab 7 – NSM Consoles



Click on the event lower in the list to display full event information such as source IP etc.

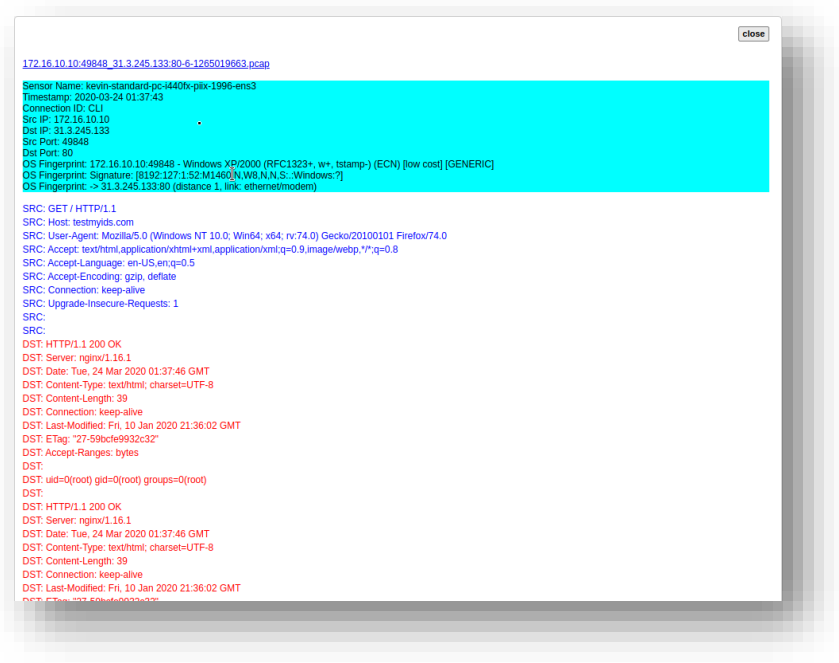
One benefit of Squert is the ease at which new filters and queries can be applied.



Click the Destination IP to bring up the query window, then click DST to apply the query.

Add a screenshot showing the query results to the Lab 7 Quiz, make sure you include the query in the search box and your UserName as displayed at the bottom-left of the Squert window

Lab 7 – NSM Consoles



To the session transcript, click the Event ID value in the lower section. A new CapME tab will open with the event transcript.

Close the CapME tab.

As this event is correlated to the previous events that were classified in Sguil, you can access any comments my clicking the message box

Add a screenshot showing the correlated events and comments to the Lab 7 Quiz, make sure you include the query in the search box and your UserName as displayed at the bottom-left of the Squert window

Take a running snapshot of your **SO** host called **Lab 7 Complete**, then shutdown.

Shutdown the other hosts and take a snapshot called **Lab 7 complete**

Submit your completed **Lab 7** quiz