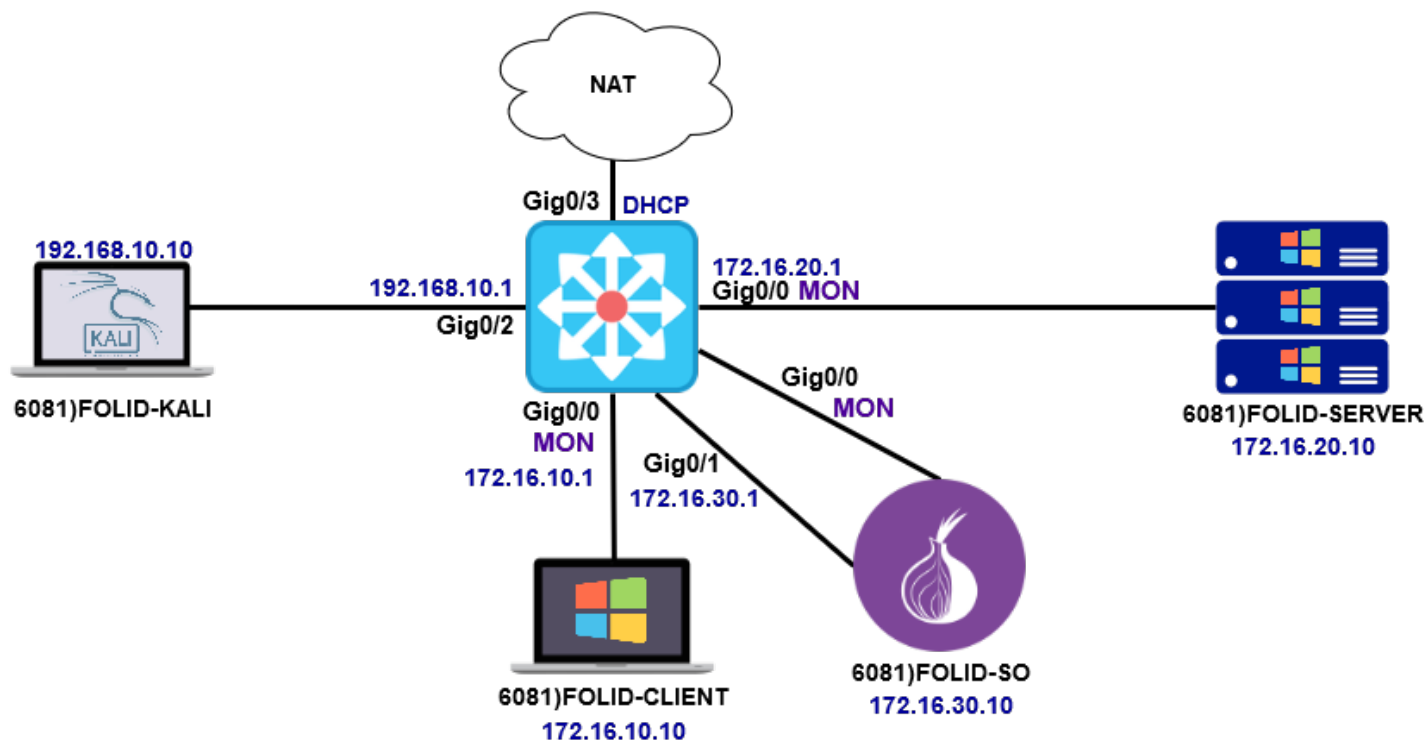


Lab 7 – NSM Consoles



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

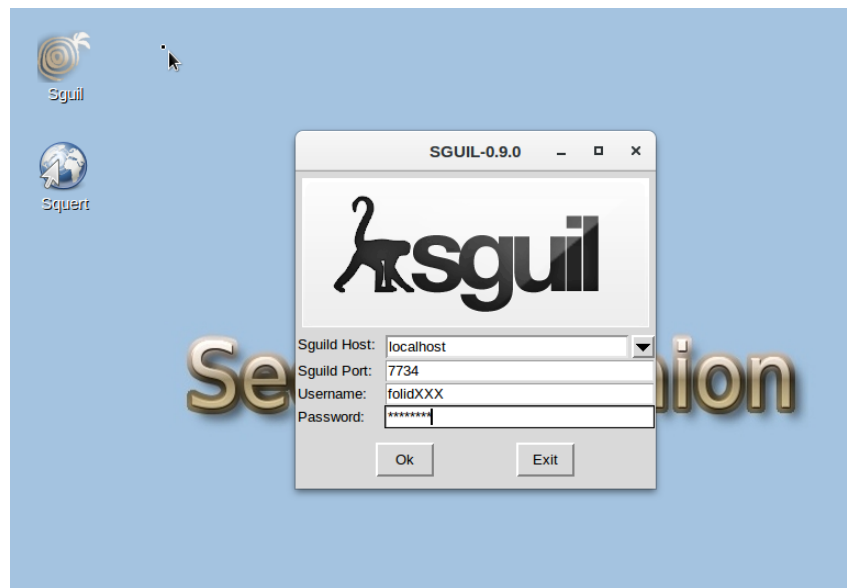
- You can attempt the quiz multiple time, but only the last attempt will be graded
- Submissions are accepted until 11:59 PM of the same day
- Submissions by email will not be accepted
- All screenshots must include you FOLID (where FOLID is your FOL username)

Lab 7 – NSM Consoles

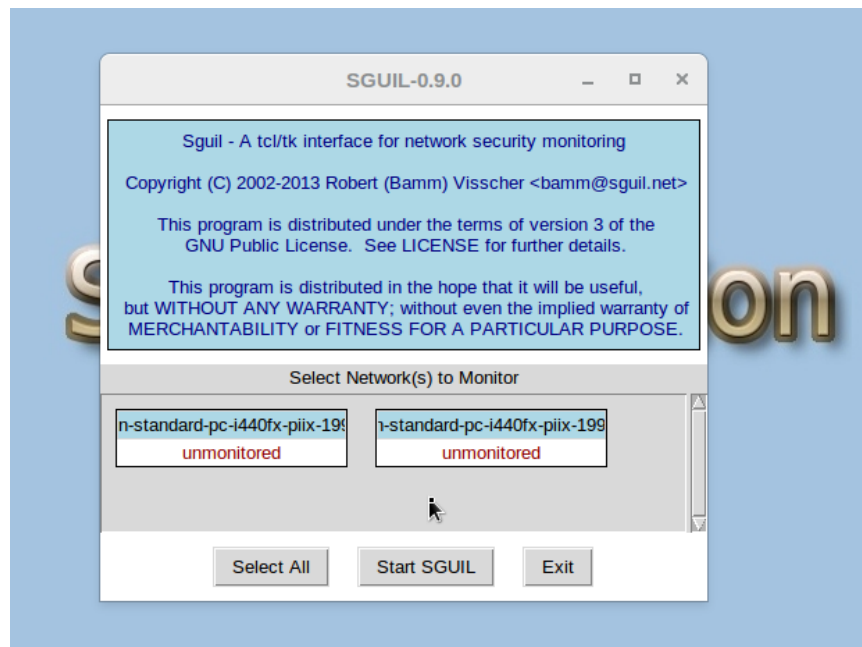


Sguil

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)

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: folidXXX UserID: 2 2020-03-23 22:25:41 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	kevin-sta...	1.1	2020-01-21 03:30:52	0.0.0.0		0.0.0.0		0	[OSSEC] New group add...
RT	7	kevin-sta...	1.2	2020-01-21 03:30:52	0.0.0.0		0.0.0.0		0	[OSSEC] New user adde...
RT	35	kevin-sta...	1.15	2020-01-21 03:34:51	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports ...
RT	4	kevin-sta...	1.16	2020-01-21 03:38:51	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 pa...
RT	1	kevin-sta...	3.1	2020-01-21 04:30:25	172.16.20.100	55698	31.3.245.133	80	6	ET POLICY curl User-Ag...
RT	1	kevin-sta...	3.2	2020-01-21 04:30:25	31.3.245.133	80	172.16.20.100	55698	6	GPL ATTACK_RESPON...
RT	98	kevin-sta...	1.230	2020-01-21 05:17:35	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity check...
RT	2	kevin-sta...	3.3	2020-03-22 21:03:53	172.16.20.100	51344	91.189.91.39	80	6	ET POLICY GNU/Linux ...
RT	9	kevin-sta...	1.439	2020-03-22 21:04:01	0.0.0.0		0.0.0.0		0	[OSSEC] Dpkg (Debian ...
RT	9	kevin-sta...	1.440	2020-03-22 21:04:06	0.0.0.0		0.0.0.0		0	[OSSEC] New dpkg (Deb...
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 Rela...
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 S...
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 S...
RT	1	kevin-sta...	1.557	2020-03-23 02:36:58	0.0.0.0		0.0.0.0		0	[OSSEC] Web server 40...

IP Resolution Agent Status Snort Statistics System Ms

☐ Reverse DNS ☒ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: ☒ None ☐ Src IP ☐ Dst IP

Show Packet Data Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ikSu
TCP	Source Port	Dest Port	RRRCSSYI	Seq #	Ack #	Offset	Res Window	Urp	hkSur		
DATA											

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

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.

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: folidXXX UserID: 2 2020-03-23 22:25:41 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	kevin-sta...	1.1	2020-01-21 03:30:52	0.0.0.0		0.0.0.0		0	[OSSEC] New group add...
RT	7	kevin-sta...	1.2	2020-01-21 03:30:52	0.0.0.0		0.0.0.0		0	[OSSEC] New user adde...
RT	35	kevin-sta...	1.15	2020-01-21 03:34:51	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports ...
RT	4	kevin-sta...	1.16	2020-01-21 03:38:51	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 pa...
RT	1	kevin-sta...	3.1	2020-01-21 04:30:25	172.16.20.100	55698	31.3.245.133	80	6	ET POLICY curl User-Ag...
RT	1	kevin-sta...	3.2	2020-01-21 04:30:25	31.3.245.133	80	172.16.20.100	55698	6	GPL ATTACK_RESPON...
RT	98	kevin-sta...	1.230	2020-01-21 05:17:35	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity check...
RT	2	kevin-sta...	3.3	2020-03-22 21:03:53	172.16.20.100	51344	91.189.91.39	80	6	ET POLICY GNU/Linux ...
RT	9	kevin-sta...	1.439	2020-03-22 21:04:01	0.0.0.0		0.0.0.0		0	[OSSEC] Dpkg (Debian ...
RT	9	kevin-sta...	1.440	2020-03-22 21:04:06	0.0.0.0		0.0.0.0		0	[OSSEC] New dpkg (Deb...
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 Rela...
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 S...
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 S...
RT	1	kevin-sta...	1.557	2020-03-23 02:36:58	0.0.0.0		0.0.0.0		0	[OSSEC] Web server 40...

IP Resolution Agent Status Snort Statistics System Ms

☒ Reverse DNS ☒ Enable External DNS

Src IP: 172.16.20.100
Src Name: Unknown
Dst IP: 31.3.245.133
Dst Name: h31-3-245-133.host.redstation.co.uk
Whois Query: ☒ None ☐ Src IP ☐ Dst IP

Show Packet Data Show Rule

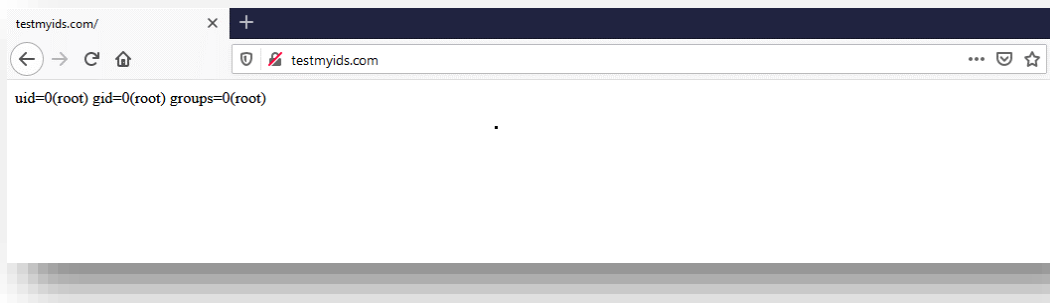
alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET POLICY curl User-Agent Outbound"; flow:established,to_server; content:"User-Agent[3a] curl/"; nocase;

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ikSu
TCP	Source Port	Dest Port	RRRCSSYI	Seq #	Ack #	Offset	Res Window	Urp	hkSur		
DATA											

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

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)?

The Sguil-0.9.0 interface is shown with the 'Escalated Events' tab selected. The event list includes columns for ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. A specific event is highlighted in yellow.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	kevin-sta...	1.1	2020-01-21 03:30:52	0.0.0.0		0.0.0.0	0		[OSSEC] New group added to the system
RT	7	kevin-sta...	1.2	2020-01-21 03:30:52	0.0.0.0		0.0.0.0	0		[OSSEC] New user added to the system
RT	35	kevin-sta...	1.15	2020-01-21 03:34:51	0.0.0.0		0.0.0.0	0		[OSSEC] Listened ports status (netstat) changed (new port opened or clos...
RT	4	kevin-sta...	1.16	2020-01-21 03:38:51	0.0.0.0		0.0.0.0	0		[OSSEC] Received 0 packets in designated time interval (defined in ossec...
RT	1	kevin-sta...	3.1	2020-01-21 04:30:25	172.16.20.100	55698	31.3.245.133	80	6	ET POLICY curl User-Agent Outbound
RT	2	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
RT	98	kevin-sta...	1.230	2020-01-21 05:17:35	0.0.0.0		0.0.0.0	0		[OSSEC] Integrity checksum changed.
RT	2	kevin-sta...	3.3	2020-03-22 21:03:53	172.16.20.100	51344	91.189.91.39	80	6	ET POLICY GNU/Linux APT User-Agent Outbound likely related to packa...
RT	9	kevin-sta...	1.439	2020-03-22 21:04:01	0.0.0.0		0.0.0.0	0		[OSSEC] Dpkg (Debian Package) half configured.
RT	9	kevin-sta...	1.440	2020-03-22 21:04:06	0.0.0.0		0.0.0.0	0		[OSSEC] New dpkg (Debian Package) installed.
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
RT	1	kevin-sta...	1.557	2020-03-23 02:36:58	0.0.0.0		0.0.0.0	0		[OSSEC] Web server 400 error code.
RT	1	kevin-sta...	1.563	2020-03-23 22:39:30	0.0.0.0		0.0.0.0			[OSSEC] PAM: User login failed.

The detailed view of the selected event shows the following information:

- IP Resolution:** Reverse DNS, Enable External DNS. Src IP: 31.3.245.133, Src Name: h31-3-245-133.host.redstation.co.uk, Dst IP: 172.16.20.100, Dst Name: Unknown.
- Show Packet Data:** alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0[28]root[29]"; fast_pattern only; classtype:bad-unknown; sid:2100490; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;) /nsml/server_data/securityonion/rules/kevin-standard-pc-4440x-plix-1996-ens3-1/downloaded.rules. Line 700
- TCP:** Source Port: 55698, Dest Port: 80, Seq #: 52560356, Ack #: 717417732, Offset: 5, Window: 64240, Urg: 0, ChkSum: 39777.
- DATA:** HTTP/1.1 200 OK. Server: nginx/1.16.1..Date: Tue, 21 Jan 2020 04:30:25 GMT..Content-Type: text/html; charset=UTF-8..Content-Length: 39..Connect1

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



IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

☒ Reverse DNS ☒ Enable External DNS

Src IP: 31.3.245.133
Src Name: h31-3-245-133.host.redstation.co.uk
Dst IP: 172.16.20.100
Dst Name: Unknown

Whois Query: ☐ None ☒ Src IP ☐ Dst IP

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See <http://www.ripe.net/db/support/db-terms-conditions.pdf>
%
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.
%
% Information related to '31.3.224.0 - 31.3.255.255'
% Abuse contact for '31.3.224.0 - 31.3.255.255' is 'abuse@redstation.com'

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 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?

RT	1	kevin-sta...	3.1	2020-01-21 04:30:25	172.16.20.100	55698	31.3.245.133	80	6	ET POLICY curl User-Agent Outbound
----	---	--------------	-----	---------------------	---------------	-------	--------------	----	---	------------------------------------

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



☒ Show Packet Data
 ☒ Show Rule

alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;)/nsm/server_data/securityonion/rules/kevin-standard-pc-i440fx-piix-1996-ens3-1/downloaded.rules: Line 700

IP	Source IP		Dest IP		Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	31.3.245.133		172.16.20.100		4	5	0	335	64507	0	0	126	27312

TCP	Source Port		Dest Port		R	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	80		55698		.	.	.	X	X	.	.	.	52560356	717417732	5	0	64240	0	39777

DATA	48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 31 2E 31 36 2E 31 0D 0A 44 61 74 65 3A 20 54 75 65 2C 20 32 31 20 4A 61 6E 20 32 30 32 30 20 30 34 3A 33 30 3A 32 35 20 47 4D 54 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65 78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74 3D 55 54 46 2D 38 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 33 39 0D 0A 43 6F 6E 6E 65 63 74 69																HTTP/1.1 200 OK. .Server: nginx/1 .16.1..Date: Tue , 21 Jan 2020 04 :30:25 GMT..Cont ent-Type: text/h tml; charset=UTF -8..Content-Leng th: 39..Connecti															
------	---	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

☐ Hex
 ☒ Text
 ☐ NoCase

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?

```
Sensor Name: kevin-standard-pc-i440fx-piix-1996-ens3-1
Timestamp: 2020-01-21 04:30:25
Connection ID: .kevin-standard-pc-i440fx-piix-1996-ens3-1_2
Src IP: 172.16.20.100
Dst IP: 31.3.245.133
Src Port: 55698
Dst Port: 80
OS Fingerprint: 172.16.20.100:55698 - UNKNOWN [65535:63:1:60:M1460,S,T,N,W11::?:?] (up: 9161 hrs)
OS Fingerprint: -> 31.3.245.133:80 (link: ethernet/modem)

SRC: GET / HTTP/1.1
SRC: Host: testmyids.com
SRC: User-Agent: curl/7.47.0
SRC: Accept: /*
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.16.1
DST: Date: Tue, 21 Jan 2020 04:30:25 GMT
DST: Content-Type: text/html; charset=UTF-8
DST: Content-Length: 39
DST: Connection: keep-alive
DST: Last-Modified: Fri, 10 Jan 2020 21:36:02 GMT
DST: ETag: "27-59bcfe9932c32"
DST: Accept-Ranges: bytes
DST:
DST: uid=0(root) gid=0(root) groups=0(root)
DST:
```

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

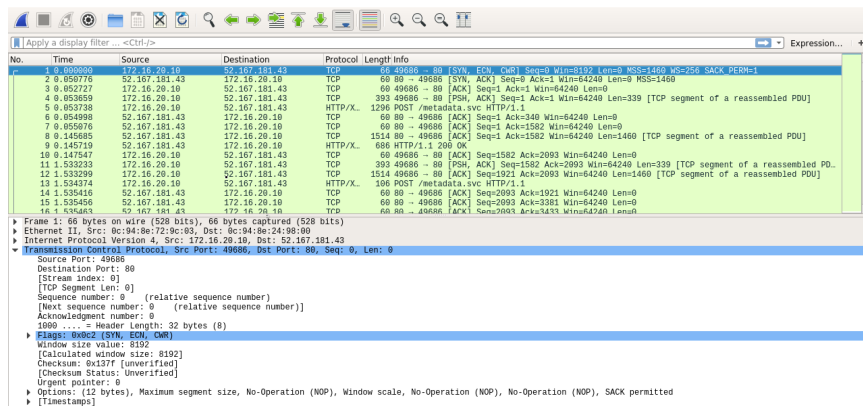
A new tab will open detailing every instance of the selected event.

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

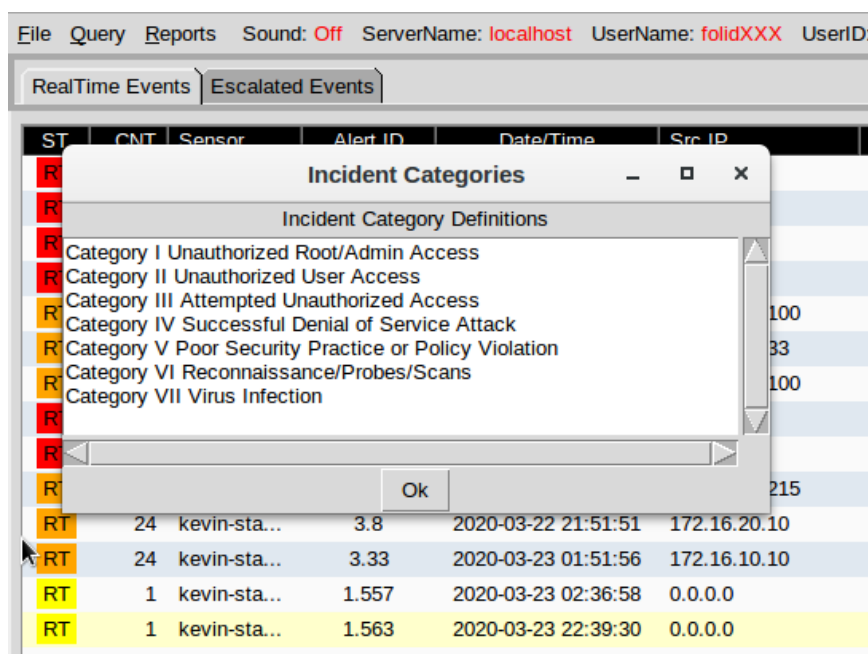


Select the first event in the window, right-click and open Wireshark

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	kevin-sta...	3.1	2020-01-21 04:30:25	172.16.20.100	55698	31.3.245.133	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**.

Query Builder

Select Query Type
☒ Events ☐ Sane ☐ PADS

AND OR NOT LIKE

Edit Where Clause 1
WHERE event.timestamp > '2020-03-17' AND event.status = 13

Add Union

IP Address LIMIT 1000

Meta Categories Items

Tables Functions

Submit Cancel

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.

Close	SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.src_port, event.dst_port, event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event_p_key, sid_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE event.timestamp > '2020-03-17' AND event.status = 13 ORDER BY datetime, src_port ASC LIMIT 1000									Submit
Export										Edit
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
C3	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

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

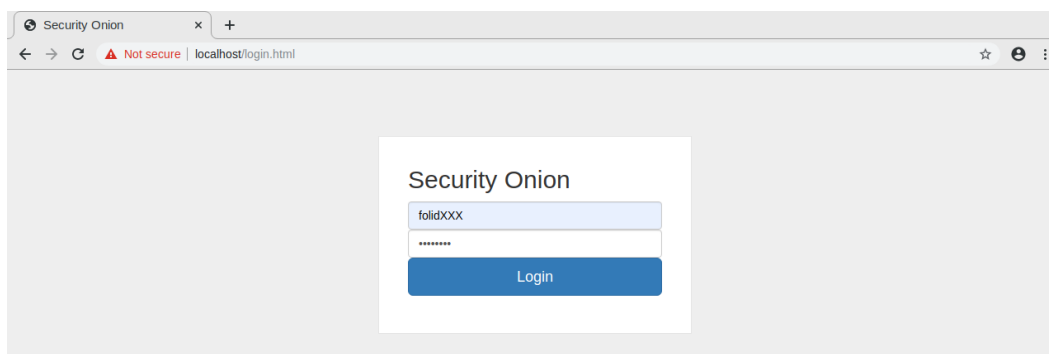
Close Sguil

Lab 7 – NSM Consoles



Squert

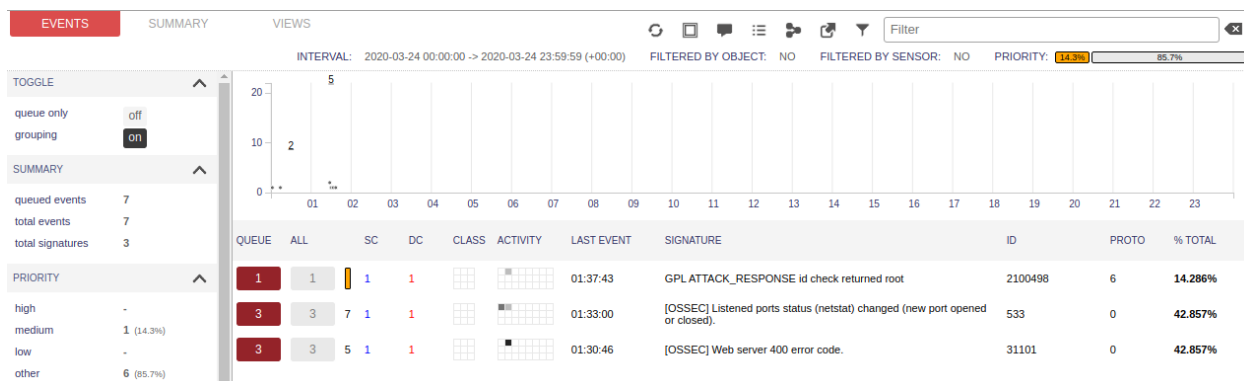
Squert allows you to access the Sguil database from your browser, as well as adding visual tools to interpret data.



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.

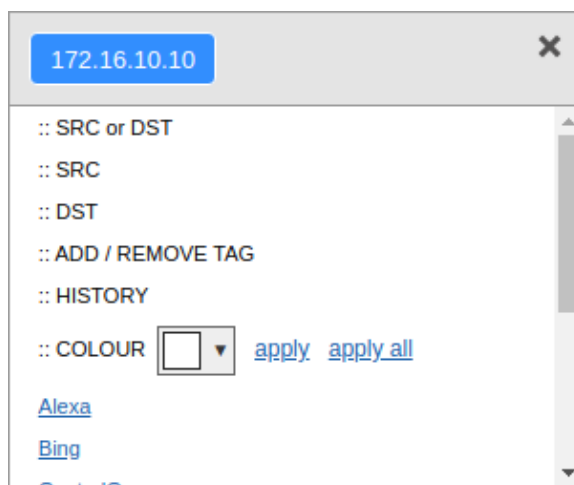
Lab 7 – NSM Consoles



1	1	1	1	01:37:43	GPL ATTACK_RESPONSE id check returned root	2100498	6	14.286%
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0 28 root 29"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23;)								
file: downloaded.rules:700								
CATEGORIZE 0 EVENT(S) CREATE FILTER: src dst both								
QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
1		2020-03-24 01:37:43	31.3.245.133	-	unknown (-)	172.16.10.10	1	RFC1918 (Jo)
ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE	
RT	2020-03-24 01:37:43	3.58	31.3.245.133	80	172.16.10.10	49848	GPL ATTACK_RESPONSE id check returned root	

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



```
172.16.10.10:49848 - 31.3.245.133:80-6-1265019663.ncap

Sensor Name: kevin-standard-pc-440K-pix-1996-ens3
Timestamp: 2020-03-24 01:37:43
Connection ID: CUI
Src IP: 172.16.10.10
Dst IP: 31.3.245.133
Src Port: 49848
Dst Port: 80
OS Fingerprint: 172.16.10.10:49848 - Windows XP/2000 (RFC1323+, w+, timestamp-) (ECN) [low cost] [GENERIC]
OS Fingerprint: Signature: [8192:127:1:52:M1460:N,W8,N,N,S:Windows:7]
OS Fingerprint: -> 31.3.245.133:80 (distance 1, link: ethernetmodem)

SRC: GET / HTTP/1.1
SRC: Host: testmyids.com
SRC: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
SRC: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Connection: keep-alive
SRC: Upgrade-Insecure-Requests: 1
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.16.1
DST: Date: Tue, 24 Mar 2020 01:37:46 GMT
DST: Content-Type: text/html; charset=UTF-8
DST: Content-Length: 39
DST: Connection: keep-alive
DST: Last-Modified: Fri, 10 Jan 2020 21:36:02 GMT
DST: ETag: "27-59bce9932c32"
DST: Accept-Ranges: bytes
DST:
DST: uid=0(root) gid=0(root) groups=0(root)
DST:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.16.1
DST: Date: Tue, 24 Mar 2020 01:37:46 GMT
DST: Content-Type: text/html; charset=UTF-8
DST: Content-Length: 39
DST: Connection: keep-alive
DST: Last-Modified: Fri, 10 Jan 2020 21:36:02 GMT
DST: ETag: "27-59bce9932c32"
DST: Accept-Ranges: bytes
```

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