Security+ Lab Series

Lab 12: Identifying & Analyzing Network/Host Intrusion Detection System (NIDS/HIDS) Alerts

Document Version: 2018-08-28

Contents

Introduction 3
Lab Topology 4
Lab Settings 5
1 Use Zenmap to Scan Network Targets 6
2 Network Security Monitoring with Sguil 8
2.1 Running Sguil 8
2.2 Analyzing Network Events using Sguil 10
3 Network Security Monitoring with Squert 14
3.1 Analyzing Security Monitoring using Squert 14

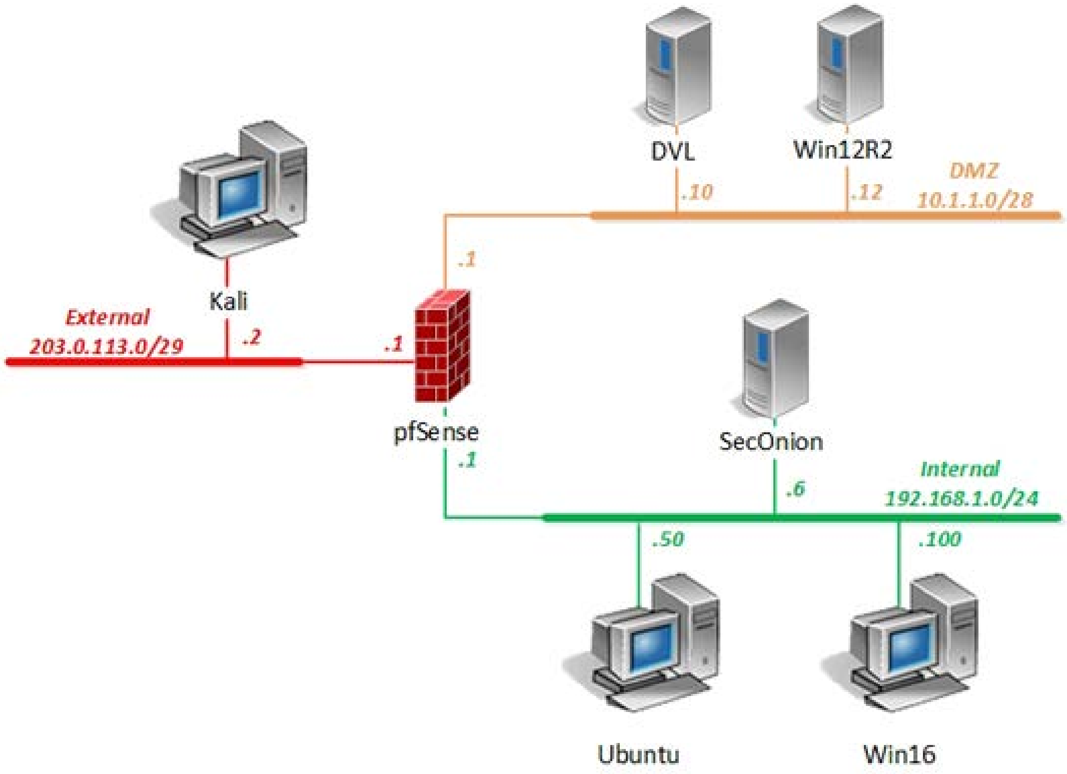
Introduction

In this lab, you will be conducting network and host monitoring using various administrative tools.

Objectives

- Troubleshoot common security issues.

Lab Topology



Lab Settings

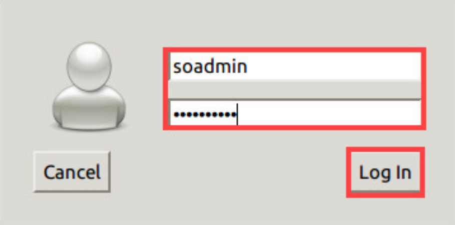
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
DVL	10.1.1.10 /28	root	toor
Kali	203.0.113.2 /29	root	toor
pfSense	eth0: 192.168.1.1 /24 eth1: 10.1.1.1 /28 eth2: 203.0.113.1 /29	admin	pfsense
SecOnion	192.168.1.6 /24	soadmin	mypassword
		root	mypassword
Ubuntu	192.168.1.50 /24	student	securepassword
		root	securepassword
Win12R2	10.1.1.12 /28	administrator	Train1ng$
Win16	192.168.1.100 /24	lab-user	Train1ng$
		Administrator	Train1ng$

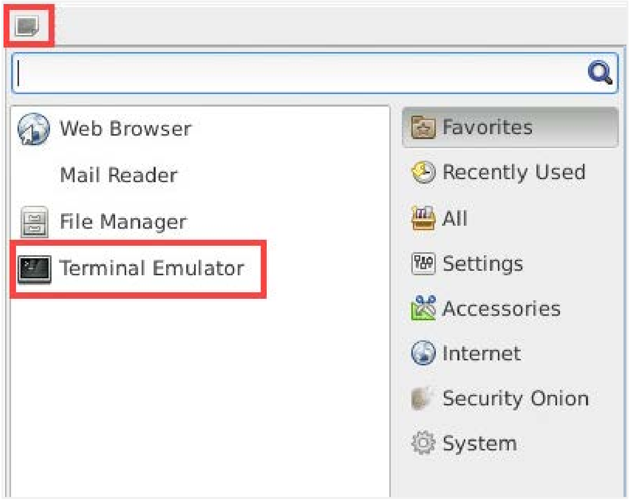
1 Use Zenmap to Scan Network Targets

In this task, you will use the integrated *zenmap* tool in *Kali* to create traffic data that can be later analyzed.

1. Launch the **SecOnion** virtual machine.
2. On the login screen, type **`soadmin`** as the username and **`mypassword`** as the password. Click **Log In**.



3. Once logged in, click the start button, followed by clicking on **Terminal Emulator** to launch a new *terminal*.



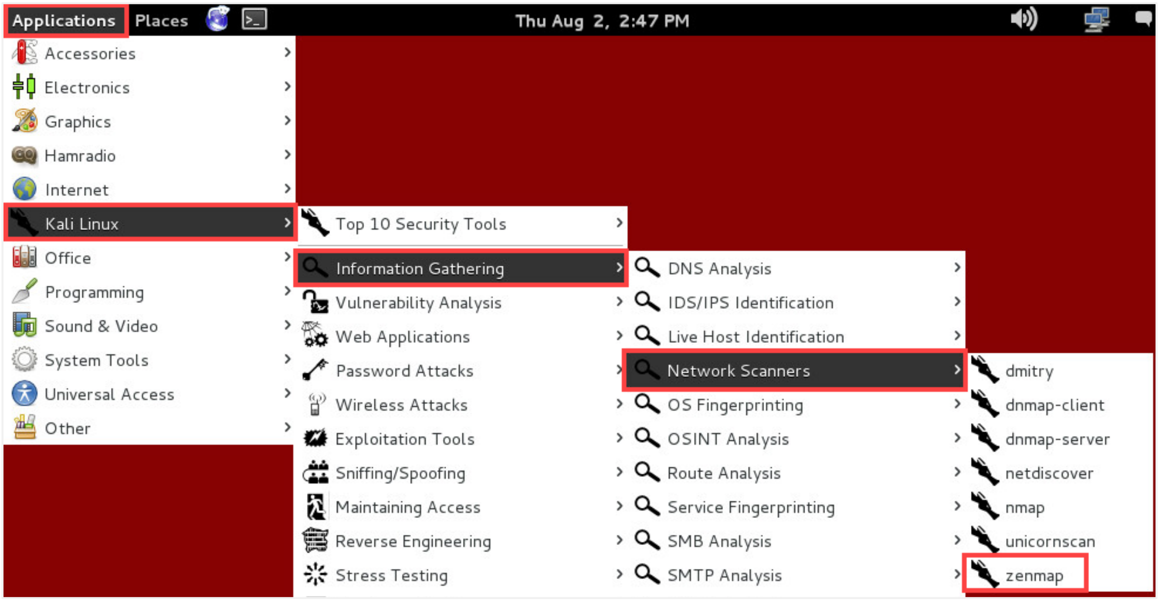
4. Type the command below, followed by pressing the **Enter** key. If prompted, enter **`mypassword`** for root privileges.

```
soadmin@Security-Onion:~$ sudo service nsm status
```

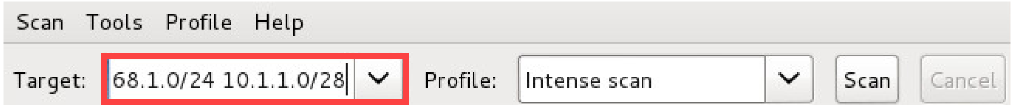
If *nsm status* reports back with all modules as *OK*, proceed to the next step. If not, then initiate the *service nsm start/restart* command.

5. Launch the **Kali** virtual machine to access the graphical login screen.
6. Log in as **`root`** with **`toor`** as the password. Open the **Kali** *PC Viewer*.

7. Click on the **Applications Menu** option located on the top menu pane and navigate to **Kali Linux > Information Gathering > Network Scanners > zenmap**.



8. A new *Zenmap* window will appear. Type `203.0.113.1 192.168.1.0/24 10.1.1.0/28` into the *Target* whitespace.

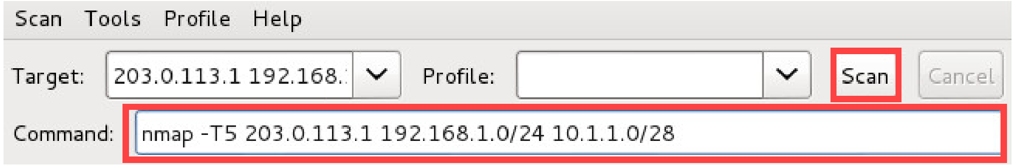


Target: 68.1.0/24 10.1.1.0/28

Profile: Intense scan

9. Modify the *Command* section so that it is written like so. Click the **Scan** button.

```
nmap –T5 203.0.113.1 192.168.1.0/24 10.1.1.0/28
```



Target: 203.0.113.1 192.168.1

Profile:

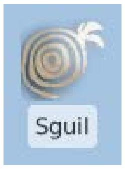
Command: nmap -T5 203.0.113.1 192.168.1.0/24 10.1.1.0/28

10. Once the scan finishes, examine the output and take notice of which common ports are opened on which system.

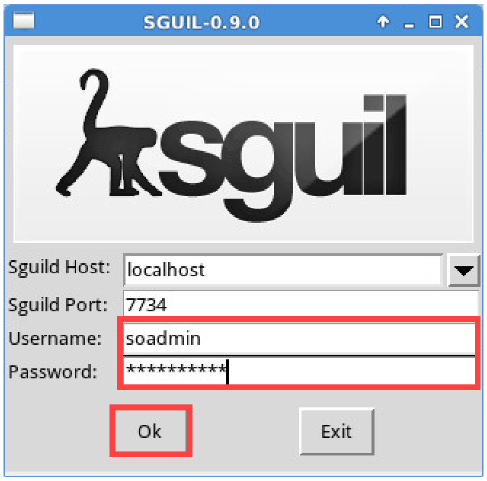
2 Network Security Monitoring with Sguil

2.1 Running Sguil

1. Change focus to the **SecOnion** system.
2. Double-click the **sguil** desktop icon to launch the application.

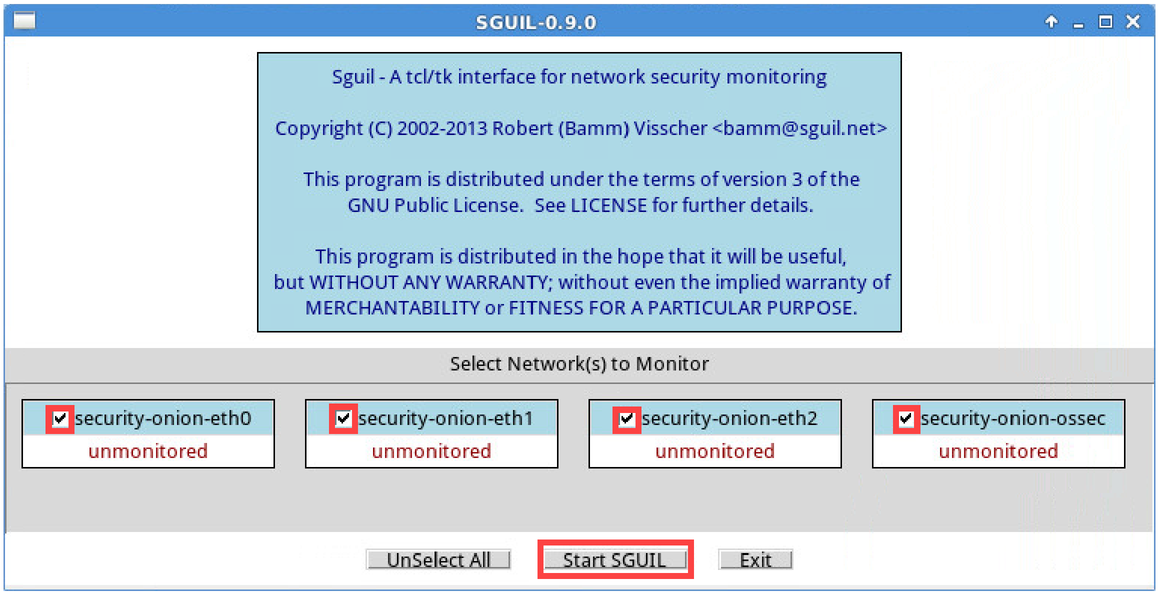


3. A new window will appear. Type **`soadmin`** for the *username* and **`mypassword`** as the *password*. Leave the remaining fields at default values. Click **Ok** to log in.



Sguild Host: localhost
Sguild Port: 7734
Username: soadmin
Password: **********

4. Check all checkboxes by clicking on the **Select All** button, followed by clicking on **Start SGUIL**.



Sguil - A tcl/tk interface for network security monitoring

Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>

This program is distributed under the terms of version 3 of the GNU Public License. See LICENSE for further details.

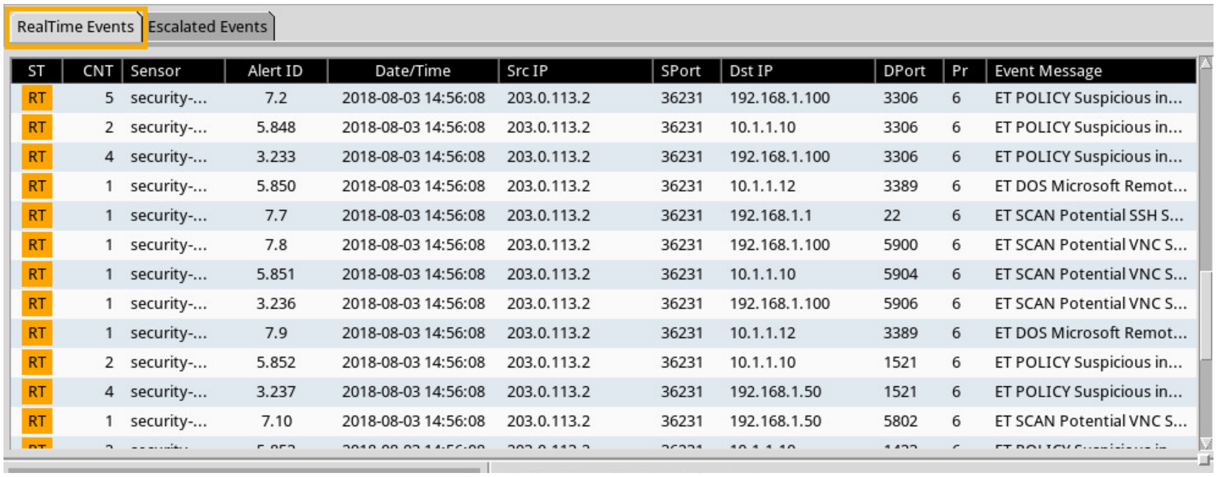
This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Select Network(s) to Monitor

☑ security-onion-eth0 unmonitored	☑ security-onion-eth1 unmonitored	☑ security-onion-eth2 unmonitored	☑ security-onion-ossec unmonitored

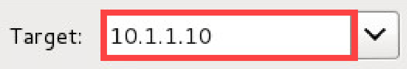
If the window is too small to check off all interfaces, expand the window size by placing the mouse on the edge of the window, clicking, and holding while moving in the direction to expand.

5. Notice upon login, the *RealTime Events* tab is already populated with events as *Sguil* is actively running in the background.



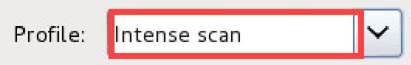
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	5	security-...	7.2	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.100	3306	6	ET POLICY Suspicious in...
RT	2	security-...	5.848	2018-08-03 14:56:08	203.0.113.2	36231	10.1.1.10	3306	6	ET POLICY Suspicious in...
RT	4	security-...	3.233	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.100	3306	6	ET POLICY Suspicious in...
RT	1	security-...	5.850	2018-08-03 14:56:08	203.0.113.2	36231	10.1.1.12	3389	6	ET DOS Microsoft Remot...
RT	1	security-...	7.7	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.1	22	6	ET SCAN Potential SSH S...
RT	1	security-...	7.8	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.100	5900	6	ET SCAN Potential VNC S...
RT	1	security-...	5.851	2018-08-03 14:56:08	203.0.113.2	36231	10.1.1.10	5904	6	ET SCAN Potential VNC S...
RT	1	security-...	3.236	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.100	5906	6	ET SCAN Potential VNC S...
RT	1	security-...	7.9	2018-08-03 14:56:08	203.0.113.2	36231	10.1.1.12	3389	6	ET DOS Microsoft Remot...
RT	2	security-...	5.852	2018-08-03 14:56:08	203.0.113.2	36231	10.1.1.10	1521	6	ET POLICY Suspicious in...
RT	4	security-...	3.237	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.50	1521	6	ET POLICY Suspicious in...
RT	1	security-...	7.10	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.50	5802	6	ET SCAN Potential VNC S...

6. Change focus to the **Kali** system.
7. Focus on the **Zenmap** application. If *Zenmap* is not already open, open a new **terminal** and type ***zenmap*** followed by pressing **Enter** to launch the application.
8. Within the *Zenmap* window, type `10.1.1.10` as the *Target*.



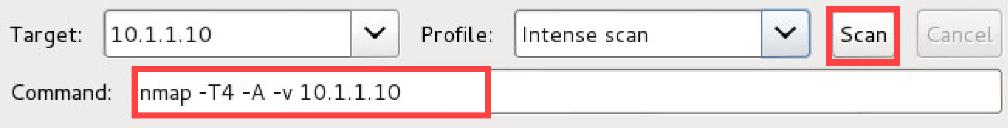
Target: 10.1.1.10

9. Select **Intense scan** as the *Profile*.



Profile: Intense scan

10. Verify that the command being used is set to **nmap -T4 -A -v 10.1.1.10**. Click **Scan**.



Target: 10.1.1.10 Profile: Intense scan

Command: nmap -T4 -A -v 10.1.1.10

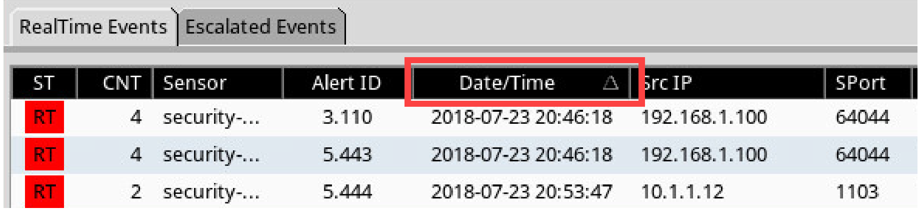
Please Note

The scan will take 2-3 minutes to complete.

11. Once the scan finishes, change focus back to the **SecOnion** system.

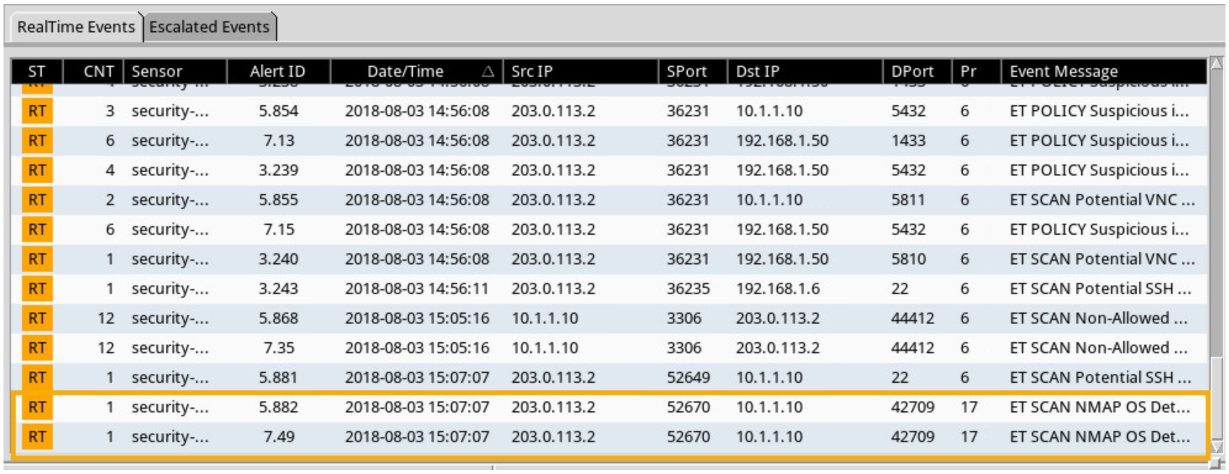
2.2 Analyzing Network Events using Sguil

1. While viewing the **Sguil** monitoring application, organize the events by date. Click on the **Date/Time** column header, making sure that the latest events show up in a descending order.



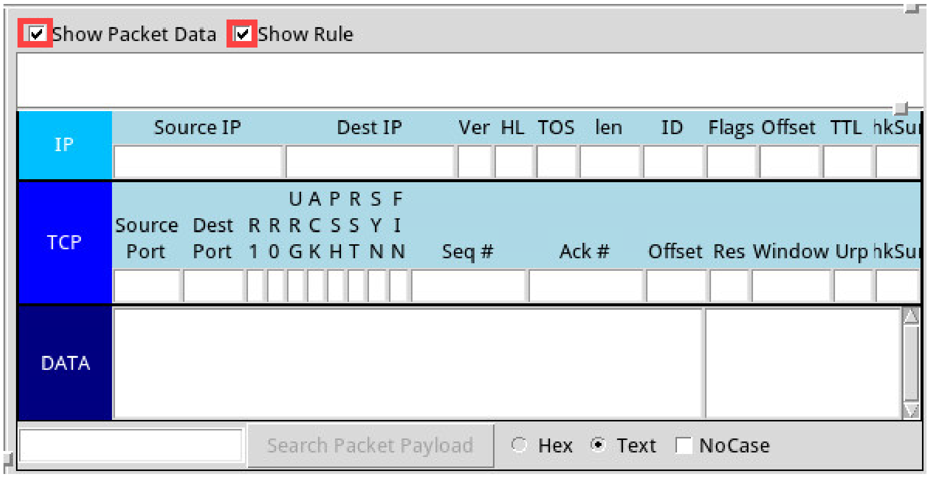
ST	CNT	Sensor	Alert ID	Date/Time △	Src IP	SPort
RT	4	security-...	3.110	2018-07-23 20:46:18	192.168.1.100	64044
RT	4	security-...	5.443	2018-07-23 20:46:18	192.168.1.100	64044
RT	2	security-...	5.444	2018-07-23 20:53:47	10.1.1.12	1103

2. Notice the event under *Event Message*, noting that an *ET SCAN NMAP OS Detection* has been detected. Select the **event**.



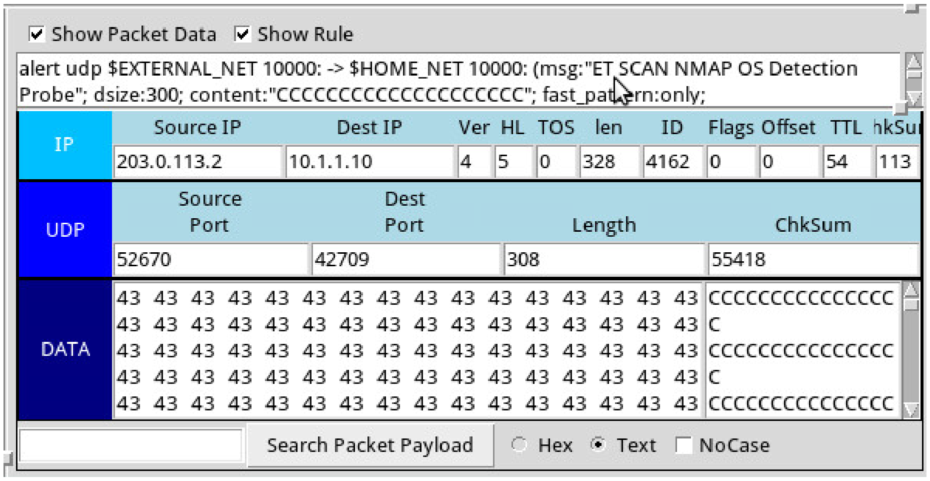
ST	CNT	Sensor	Alert ID	Date/Time △	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	3	security-...	5.854	2018-08-03 14:56:08	203.0.113.2	36231	10.1.1.10	5432	6	ET POLICY Suspicious i...
RT	6	security-...	7.13	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.50	1433	6	ET POLICY Suspicious i...
RT	4	security-...	3.239	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.50	5432	6	ET POLICY Suspicious i...
RT	2	security-...	5.855	2018-08-03 14:56:08	203.0.113.2	36231	10.1.1.10	5811	6	ET SCAN Potential VNC ...
RT	6	security-...	7.15	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.50	5432	6	ET POLICY Suspicious i...
RT	1	security-...	3.240	2018-08-03 14:56:08	203.0.113.2	36231	192.168.1.50	5810	6	ET SCAN Potential VNC ...
RT	1	security-...	3.243	2018-08-03 14:56:11	203.0.113.2	36235	192.168.1.6	22	6	ET SCAN Potential SSH ...
RT	12	security-...	5.868	2018-08-03 15:05:16	10.1.1.10	3306	203.0.113.2	44412	6	ET SCAN Non-Allowed ...
RT	12	security-...	7.35	2018-08-03 15:05:16	10.1.1.10	3306	203.0.113.2	44412	6	ET SCAN Non-Allowed ...
RT	1	security-...	5.881	2018-08-03 15:07:07	203.0.113.2	52649	10.1.1.10	22	6	ET SCAN Potential SSH ...
RT	1	security-...	5.882	2018-08-03 15:07:07	203.0.113.2	52670	10.1.1.10	42709	17	ET SCAN NMAP OS Det...
RT	1	security-...	7.49	2018-08-03 15:07:07	203.0.113.2	52670	10.1.1.10	42709	17	ET SCAN NMAP OS Det...

3. In the bottom-right pane, check the box for **Show Packet Data** and **Show Rule**.


☑ Show Packet Data ☑ Show Rule

○ Hex ● Text □ NoCase

4. Analyze the packet data.



☑ Show Packet Data ☑ Show Rule

```
alert udp $EXTERNAL_NET 10000: -> $HOME_NET 10000: (msg:"ET SCAN NMAP OS Detection
Probe"; dsize:300; content:"CCCCCCCCCCCCCCCCCCCC"; fast_pattern:only;
```

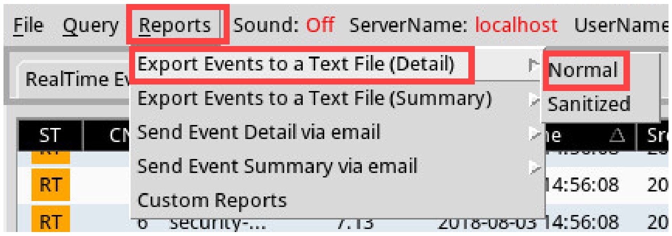
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hkSu
	203.0.113.2	10.1.1.10	4	5	0	328	4162	0	0	54	113

UDP	Source Port	Dest Port	Length	ChkSum
	52670	42709	308	55418

DATA

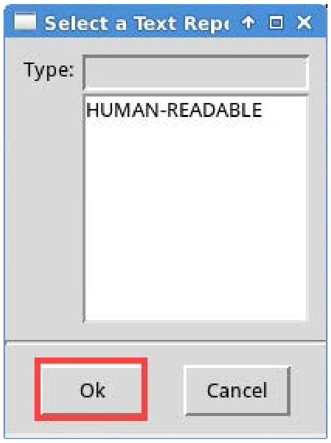
```
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 C
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 C
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
```

5. Export a detailed report for this specific event to present to management. While having the event selected (**highlighted**), click on the **Reports** menu option located on the top menu pane and select **Export Events to a Text File (Detail) > Normal**.

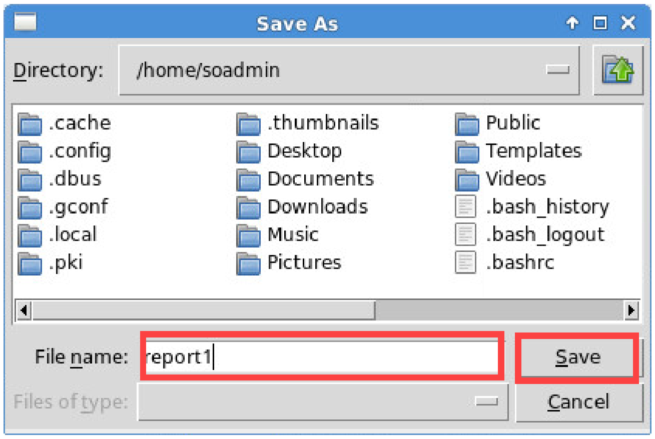


File Query Reports Sound: Off ServerName: localhost UserName
RealTime Ev
Export Events to a Text File (Detail)
Export Events to a Text File (Summary)
Send Event Detail via email
Send Event Summary via email
Custom Reports
Normal
Sanitized
ST
CN
RT
RT
14:56:08
2018-08-03 14:56:08
20

6. In the *Select a Text Report Type* window, click **OK** to continue.



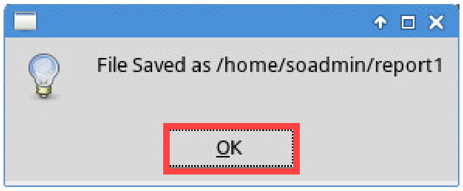
7. In the *Save As* window, verify the directory is set to **/home/soadmin**. Type `report1` as the *filename* and click **Save**.



Directory: /home/soadmin

File name: report1

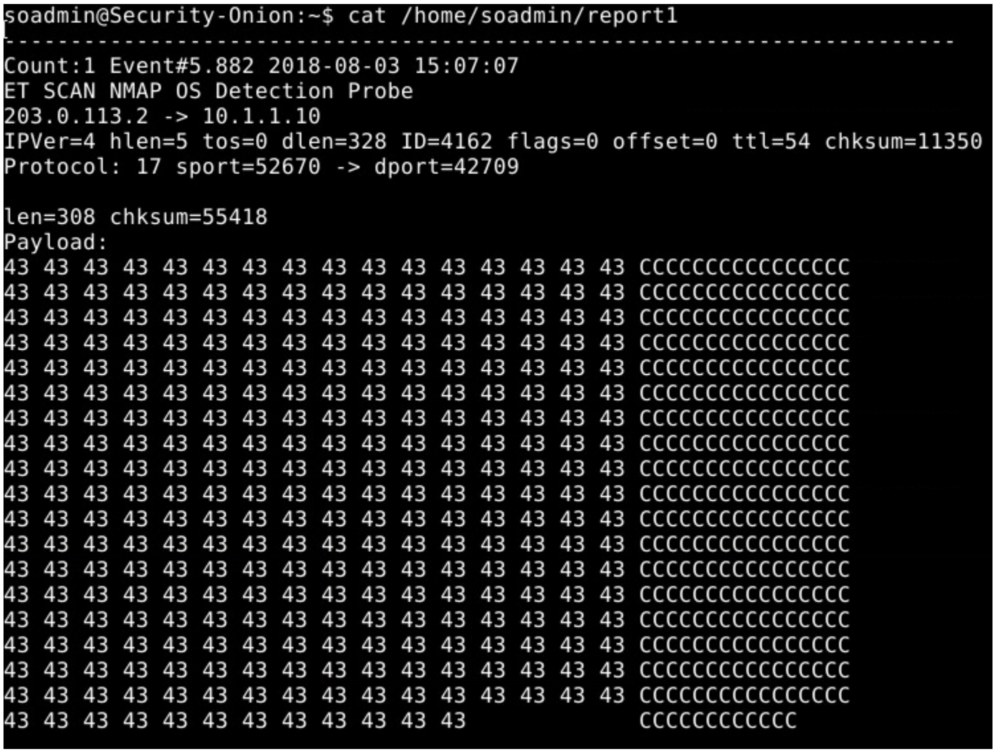
8. Click **OK** to confirm the file has been saved.



File Saved as /home/soadmin/report1

9. While on the *SecOnion* system, open a **terminal** and type the command below to view the contents of the report.

```
soadmin@Security-Onion:~$ cat /home/soadmin/report1
```



```
soadmin@Security-Onion:~$ cat /home/soadmin/report1
------------------------------------------------------------------------
Count:1 Event#5.882 2018-08-03 15:07:07
ET SCAN NMAP OS Detection Probe
203.0.113.2 -> 10.1.1.10
IPVer=4 hlen=5 tos=0 dlen=328 ID=4162 flags=0 offset=0 ttl=54 chksum=11350
Protocol: 17 sport=52670 -> dport=42709

len=308 chksum=55418
Payload:
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC
43 43 43 43 43 43 43 43 43 43 43 43             CCCCCCCCCCCC
```

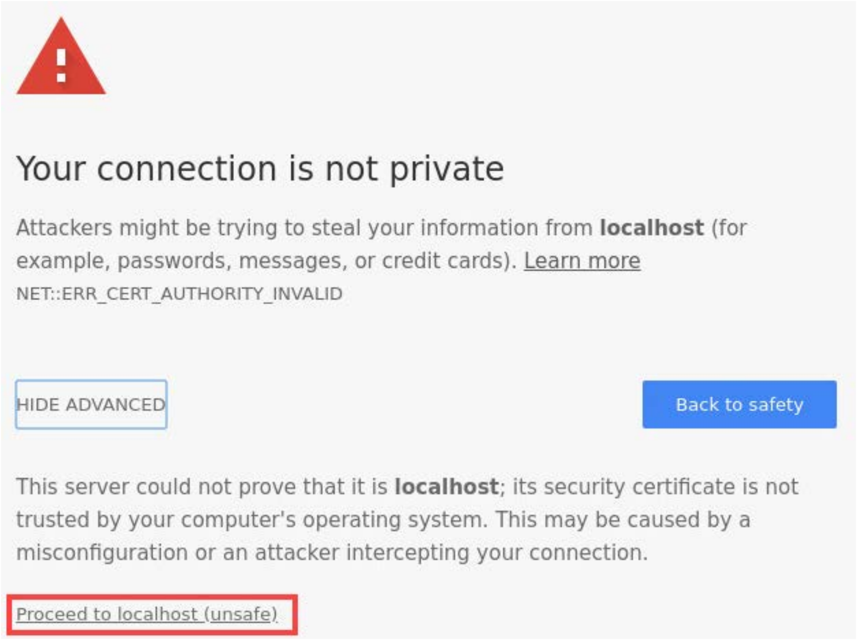
10. After viewing the report in the terminal, **close** the *terminal* window.
11. **Close** the *Sguil* application.
12. Leave the SecOnion viewer open to continue with the next task.

3 Network Security Monitoring with Squert

3.1 Analyzing Security Monitoring using Squert

1. While on the *SecOnion* system, double-click on the **Squert** desktop icon.

2. A *Firefox* web browser should appear. Verify the address field is populated with the following: **https://localhost/squert**. Click on **Advanced** followed by clicking the **Proceed to localhost** link.



Your connection is not private

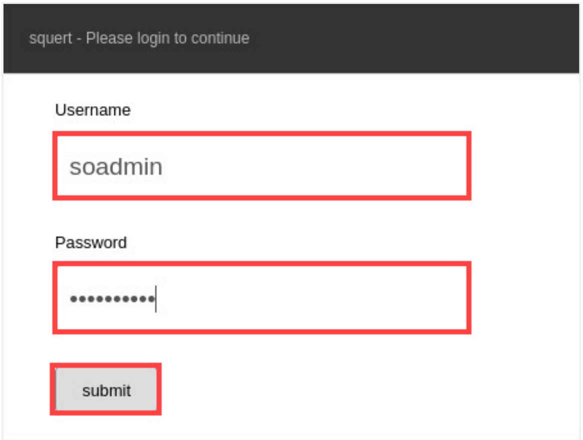
Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **localhost**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to localhost (unsafe)

3. For the *Squert* login page, type `soadmin` as the *Username* and `mypassword` as the *Password*. Click **Submit**.

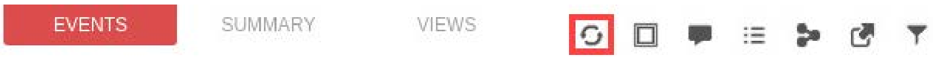


squert - Please login to continue

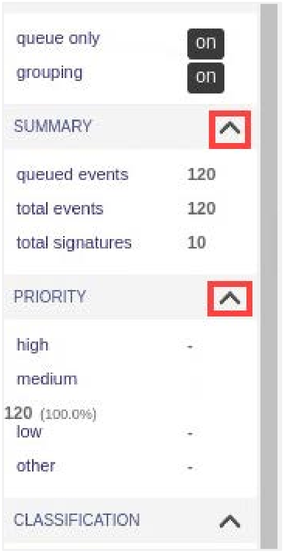
Username: soadmin

Password: ••••••••••

4. To ensure the latest events are being populated, click the **Refresh** icon located at the top of the dashboard.



5. On the left side, click the up arrow to collapse both **Summary** and **Priority**.



queue only	on
grouping	on

SUMMARY

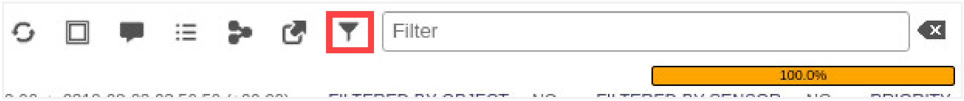
queued events	120
total events	120
total signatures	10

PRIORITY

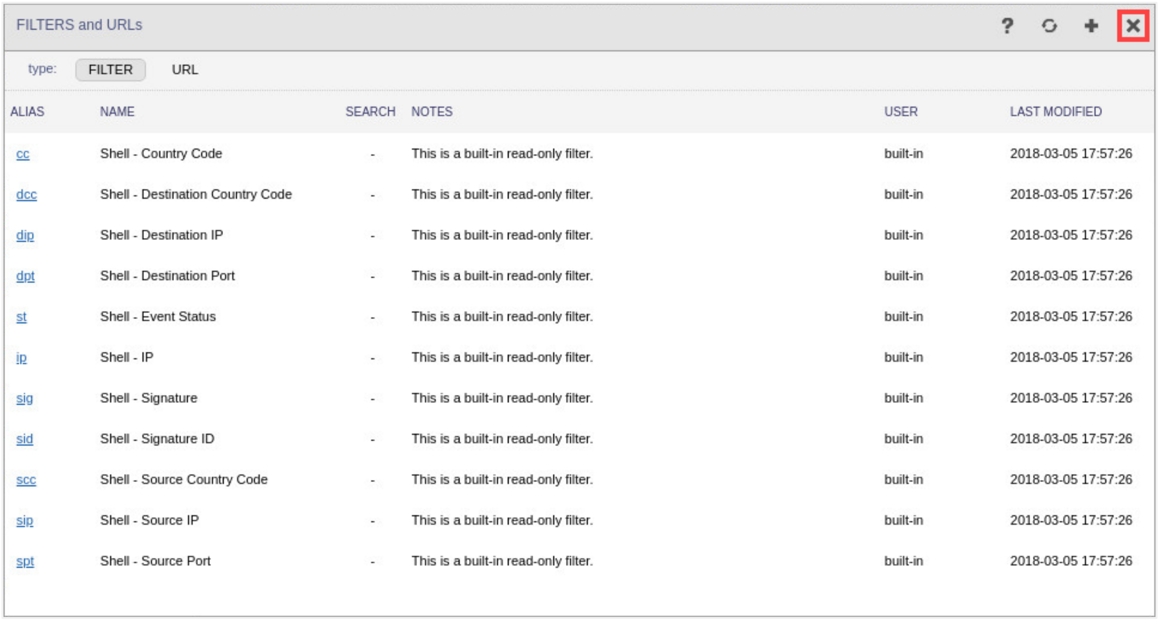
high	-
medium	120 (100.0%)
low	-
other	-

CLASSIFICATION

6. Click on the **filters** icon at the top of the page.



7. A new pop-window will appear, showing the different alias options that can be used for filtering events. Review the output and **close** the pop-up window.

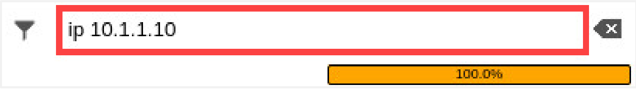


FILTERS and URLs

type: FILTER URL

ALIAS	NAME	SEARCH	NOTES	USER	LAST MODIFIED
cc	Shell - Country Code	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
dcc	Shell - Destination Country Code	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
dip	Shell - Destination IP	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
dpt	Shell - Destination Port	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
st	Shell - Event Status	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
ip	Shell - IP	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
sig	Shell - Signature	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
sid	Shell - Signature ID	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
scc	Shell - Source Country Code	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
sip	Shell - Source IP	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26
spt	Shell - Source Port	-	This is a built-in read-only filter.	built-in	2018-03-05 17:57:26

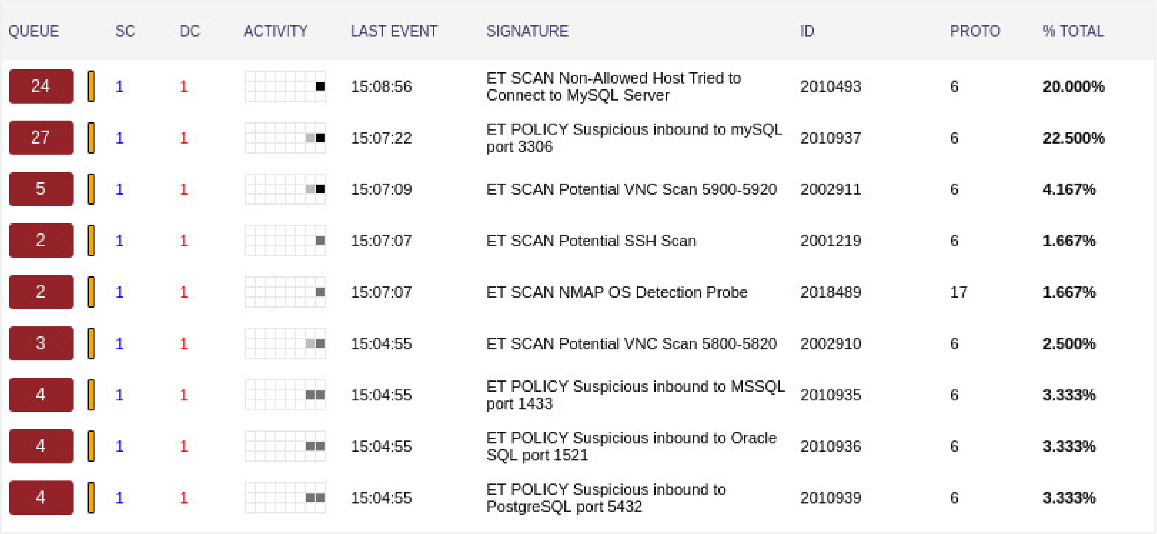
8. Filter the events to only show what is hitting the *DVL Server* on the network. In the filter text field, type `ip 10.1.1.10` followed by pressing **Enter**.



ip 10.1.1.10

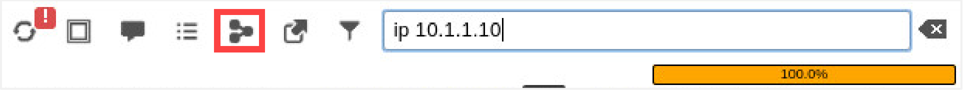
100.0%

9. Notice that all recent events relating to the *DVL Server* is populating the event list.



QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
24	1	1		15:08:56	ET SCAN Non-Allowed Host Tried to Connect to MySQL Server	2010493	6	**20.000%**
27	1	1		15:07:22	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	**22.500%**
5	1	1		15:07:09	ET SCAN Potential VNC Scan 5900-5920	2002911	6	**4.167%**
2	1	1		15:07:07	ET SCAN Potential SSH Scan	2001219	6	**1.667%**
2	1	1		15:07:07	ET SCAN NMAP OS Detection Probe	2018489	17	**1.667%**
3	1	1		15:04:55	ET SCAN Potential VNC Scan 5800-5820	2002910	6	**2.500%**
4	1	1		15:04:55	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	**3.333%**
4	1	1		15:04:55	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	**3.333%**
4	1	1		15:04:55	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	**3.333%**

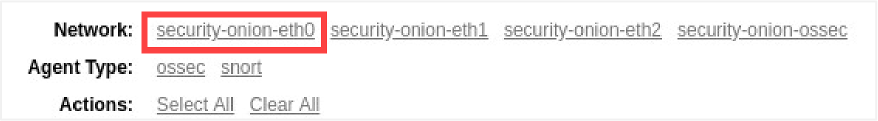
10. We can also filter events by which sensor is picking up the traffic. Click on the **sensors** icon located at the top.



ip 10.1.1.10

100.0%

11. A new pop-up window should appear. Notice the different sensors listed along with the agent operating on each sensor. From the *Network* options, click the **security-onion-eth0** option to only show events picked up by this sensor.

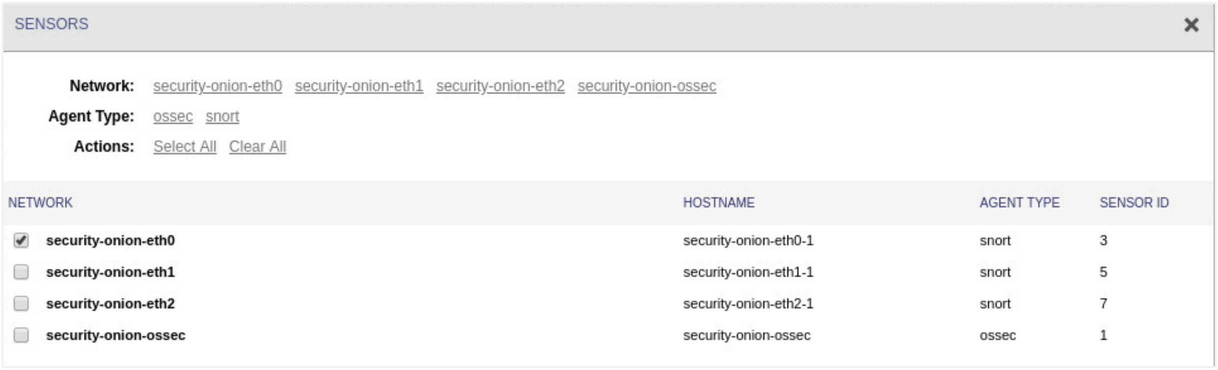


Network: security-onion-eth0 security-onion-eth1 security-onion-eth2 security-onion-ossec

Agent Type: ossec snort

Actions: Select All Clear All

12. Confirm that **1 check** has been marked for *security-onion-eth0* and close the pop-up window.

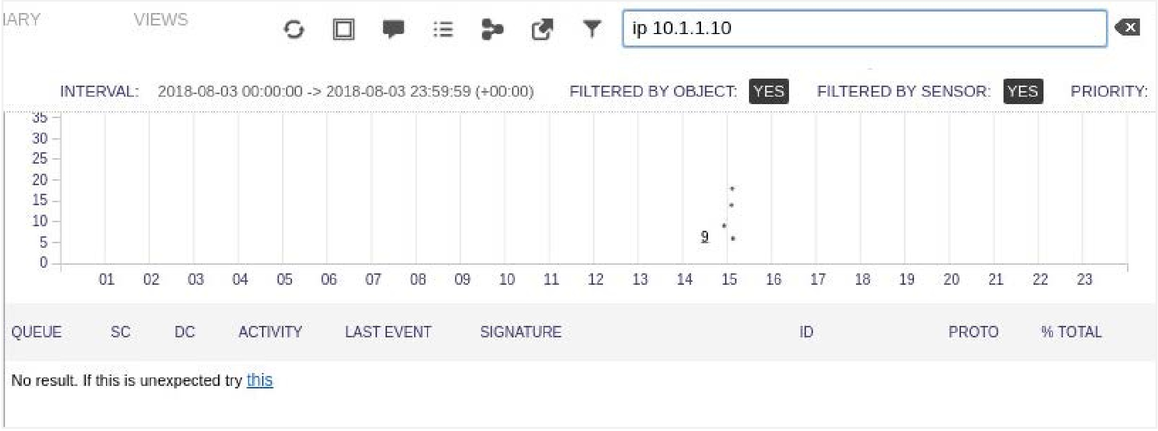


SENSORS ✕

Network: security-onion-eth0 security-onion-eth1 security-onion-eth2 security-onion-ossec
Agent Type: ossec snort
Actions: Select All Clear All

NETWORK	HOSTNAME	AGENT TYPE	SENSOR ID
☑ security-onion-eth0	security-onion-eth0-1	snort	3
□ security-onion-eth1	security-onion-eth1-1	snort	5
□ security-onion-eth2	security-onion-eth2-1	snort	7
□ security-onion-ossec	security-onion-ossec	ossec	1

13. Verify that `ip 10.1.1.10` is typed into the *filter* text field. Click within the **filter text field**, and press **Enter** to initialize the search with the new sensor filter.
14. Notice that no events are presented using this filter option. The reason being is that *10.1.1.10* is on a different network leg in which sensor *eth1* is picking up traffic. Since we filtered using the *eth0* sensor, no matches are found.



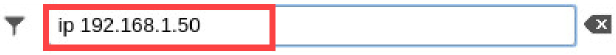
ip 10.1.1.10

INTERVAL: 2018-08-03 00:00:00 -> 2018-08-03 23:59:59 (+00:00) FILTERED BY OBJECT: YES FILTERED BY SENSOR: YES PRIORITY:

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL

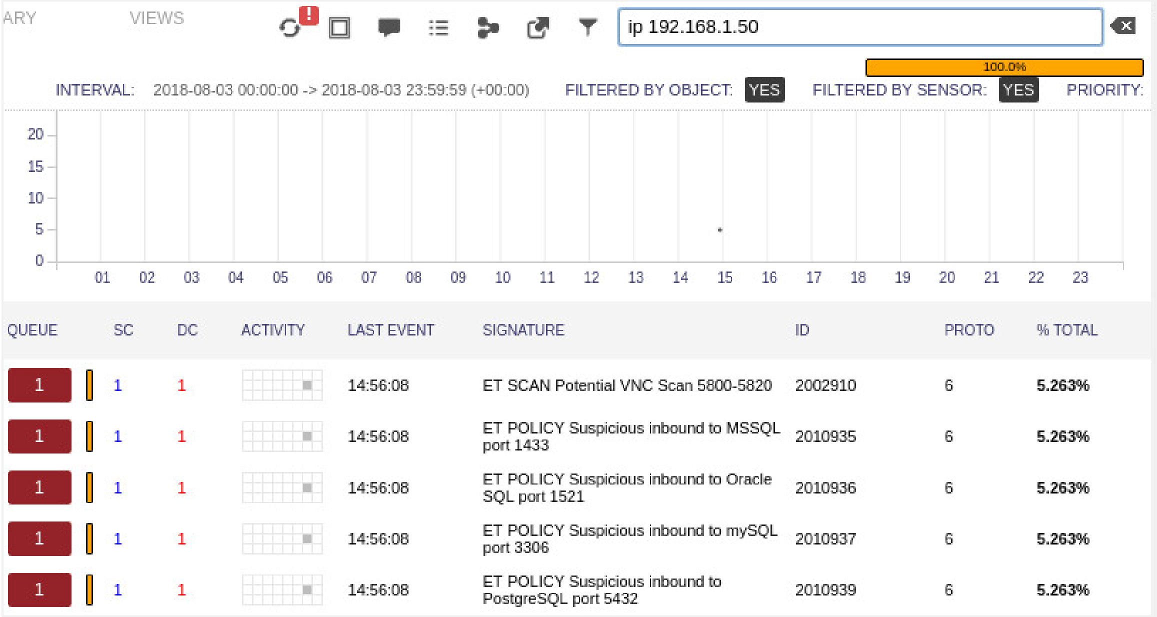
No result. If this is unexpected try this

15. Type `ip 192.168.1.50` into the *white filter space* followed by pressing the **Enter** key.



ip 192.168.1.50

16. Notice the *event list* is now populated with the combined filter settings.



ip 192.168.1.50

INTERVAL: 2018-08-03 00:00:00 -> 2018-08-03 23:59:59 (+00:00) FILTERED BY OBJECT: YES FILTERED BY SENSOR: YES PRIORITY:

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
1	1	1		14:56:08	ET SCAN Potential VNC Scan 5800-5820	2002910	6	**5.263%**
1	1	1		14:56:08	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	**5.263%**
1	1	1		14:56:08	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	**5.263%**
1	1	1		14:56:08	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	**5.263%**
1	1	1		14:56:08	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	**5.263%**

17. The lab is now complete; you may end the reservation.