



SECURITY+ V4 LAB SERIES

Lab 8: Identifying & Analyzing Network/Host Intrusion Detection System (NIDS/HIDS) Alerts

Document Version: **2024-01-29**

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	1.7: Summarize the techniques used in security assessments 3.2: Given a scenario, implement host or application security solutions 3.3: Given a scenario, implement secure network designs 4.3: Given an incident, utilize appropriate data sources to support an investigation
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	7: Security Assessments 18: Host and Application Security 19: Secure Network Design 28: Investigations

Copyright © 2024 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.
KALI LINUX™ is a trademark of Offensive Security.
Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.
VMware is a registered trademark of VMware, Inc.
SECURITY ONION is a trademark of Security Onion Solutions LLC.
Android is a trademark of Google LLC.
pfSense® is a registered mark owned by Electric Sheep Fencing LLC ("ESF").
All trademarks are property of their respective owners.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Load PCAP File to Security Onion for Analysis	6
1.1 Disable Firewall	6
1.2 Capture the Traffic for Analysis	8
1.3 Import the Traffic Capture	12
2 Analyze the Data and File a Case	16
3 Add a Case, Investigate, and Close the Case	19
3.1 Escalate an Alert to Add a Case	19
3.2 Add Observable and Tasks for Further Investigation	25
3.3 Finish All Tasks and Close a Case	29

Introduction

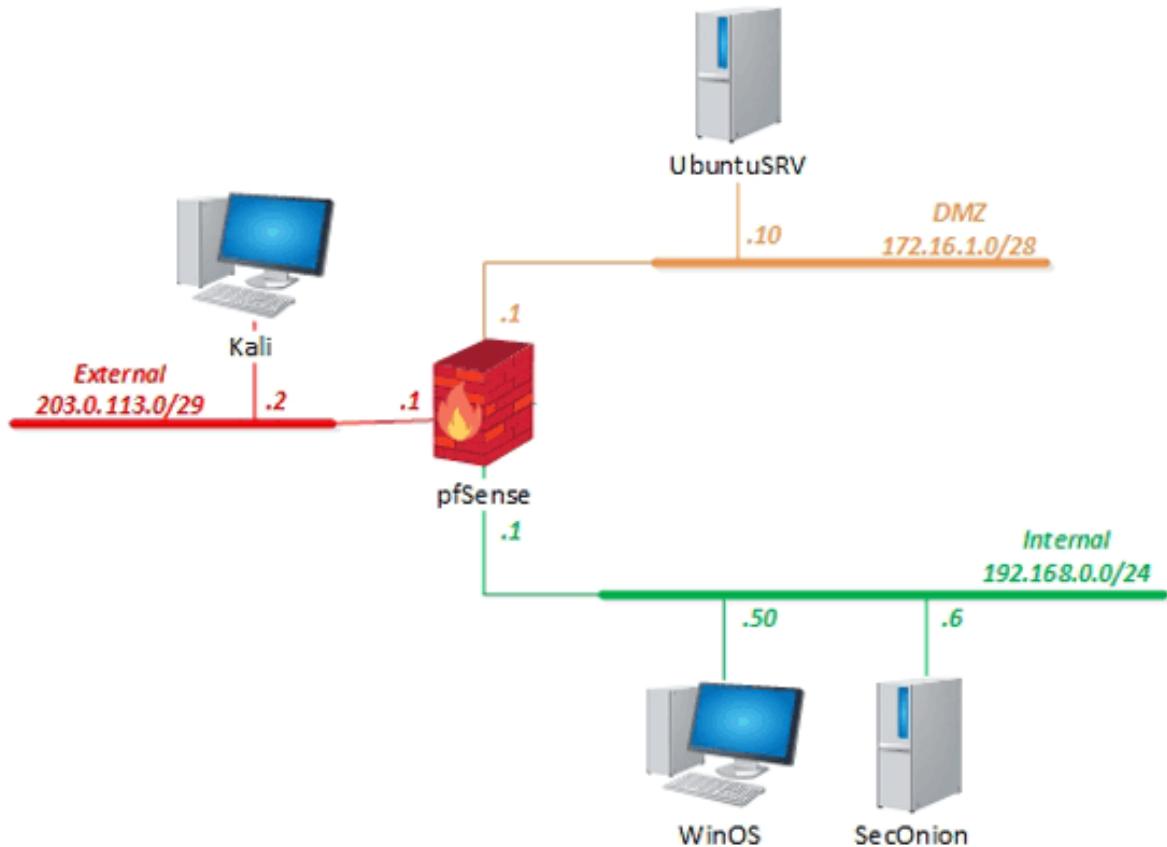
In this lab, you will be conducting network and host monitoring using various administrative tools.

Objective

In this lab, you will perform the following tasks:

- Perform network security packet analyzing with SecurityOnion
- Add and solve a case

Lab Topology



Lab Settings

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

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali	203.0.113.2	kali	kali
pfSense	192.168.0.1	sysadmin	NDGLabpass123!
SecOnion	192.168.0.6	sysadmin	NDGLabpass123!
UbuntuSRV	172.16.1.10	sysadmin	NDGLabpass123!
WinOS	192.168.0.50	Administrator	NDGLabpass123!

1 Load PCAP File to Security Onion for Analysis

In this lab, we are using the standalone installation of *Security Onion* for all of the tasks. In a production line, you could use either a standalone or distributed installation. Because live capture will be covered in Lab 22, this lab will not use the live capture function. Instead, you will explore the capture import function *Security Onion* provides. You will capture the traffic and import it to *Security Onion* for analysis.

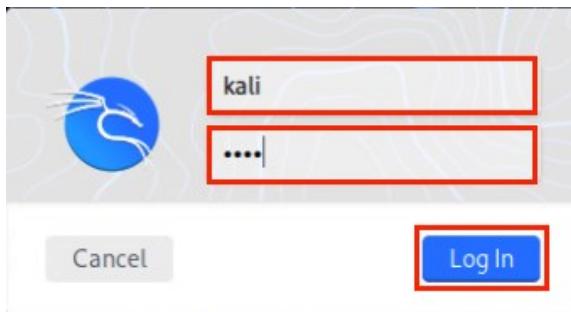
1.1 Disable Firewall

In this section, you will disable the Firewall to prepare for the traffic capture.

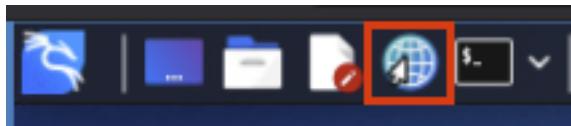
1. Click on the **Kali** tab to access the *Kali VM*.



2. Log in to the *Kali VM* as username **kali**, password **kali**.



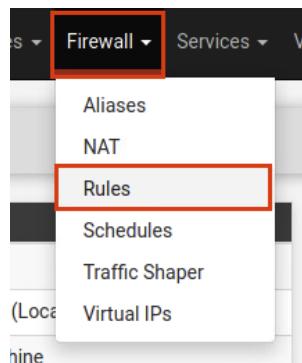
3. Click to open a browser window.



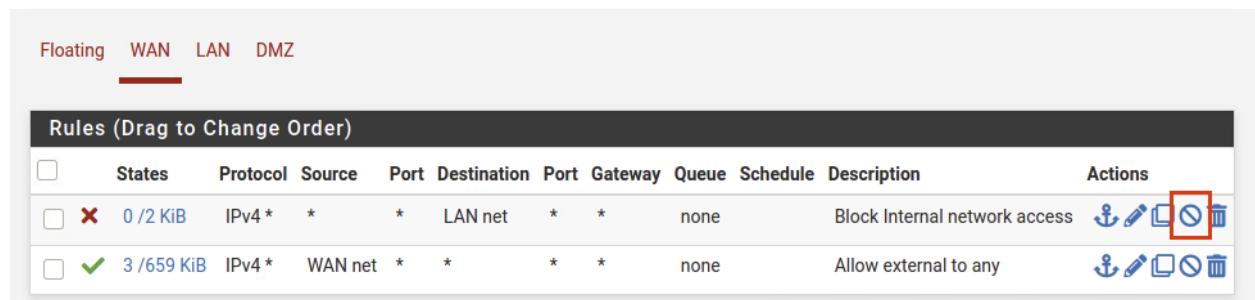
4. In the address bar, type **203.0.113.1** to go to the *pfSense* firewall management login page. Log in as username **admin**, password **NDGLabpass123!** and then click the **SIGN IN** button.



5. Once logged in, you will see the *Status/Dashboard* page; click the **Firewall** menu and select **Rules**.

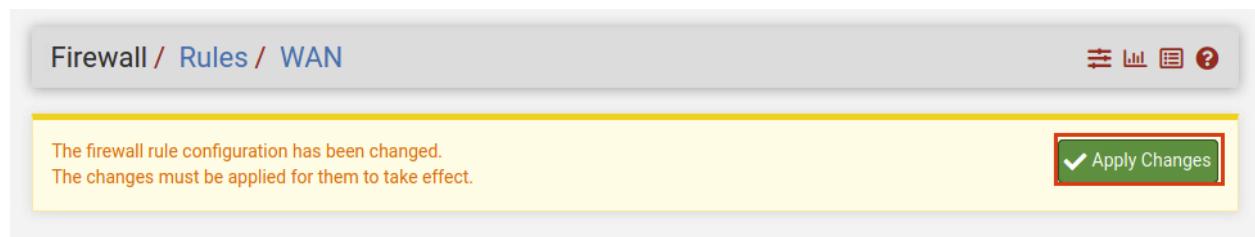


6. Click the **Disable** button to disable the **Block Internal network access** rule.



States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 /2 KiB	IPv4 *	*	LAN net	*	*	none		Block Internal network access	
<input type="checkbox"/>	3 /659 KiB	IPv4 *	WAN net	*	*	*	*	none	Allow external to any	

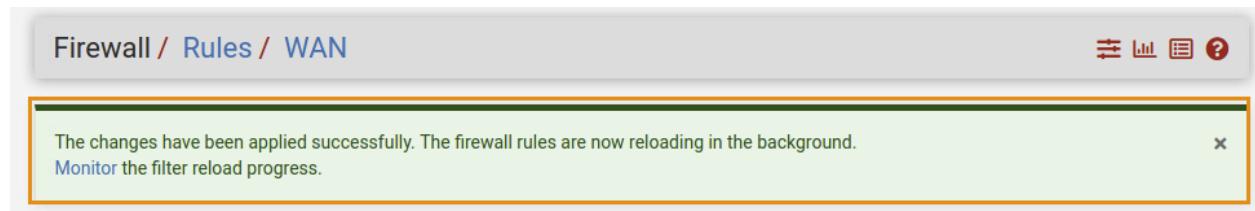
7. Then click the **Apply Changes** button to confirm the action.



The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

8. If you see a confirmation message, the change has been applied successfully. Minimize the browser window and proceed to the next section.



The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

1.2 Capture the Traffic for Analysis

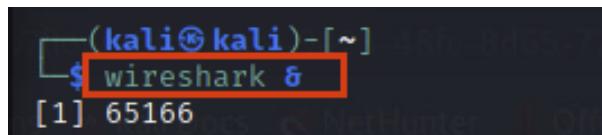
In this section, you will generate the traffic from an attacking machine, then capture and save it to a pcap file.

1. In the *Kali* VM, click **Terminal** to start a *Terminal* window.

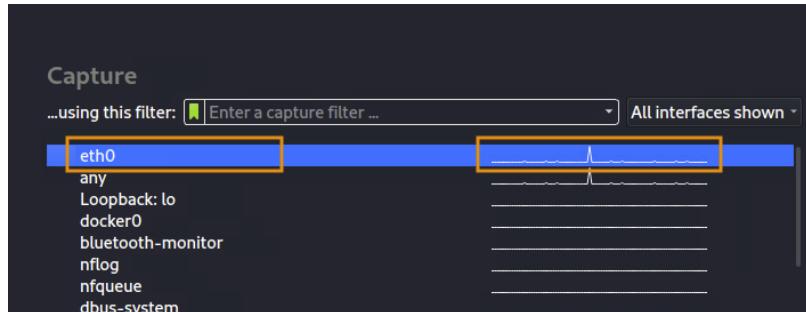


2. Type the following command to start *Wireshark* and keep the process in the background.

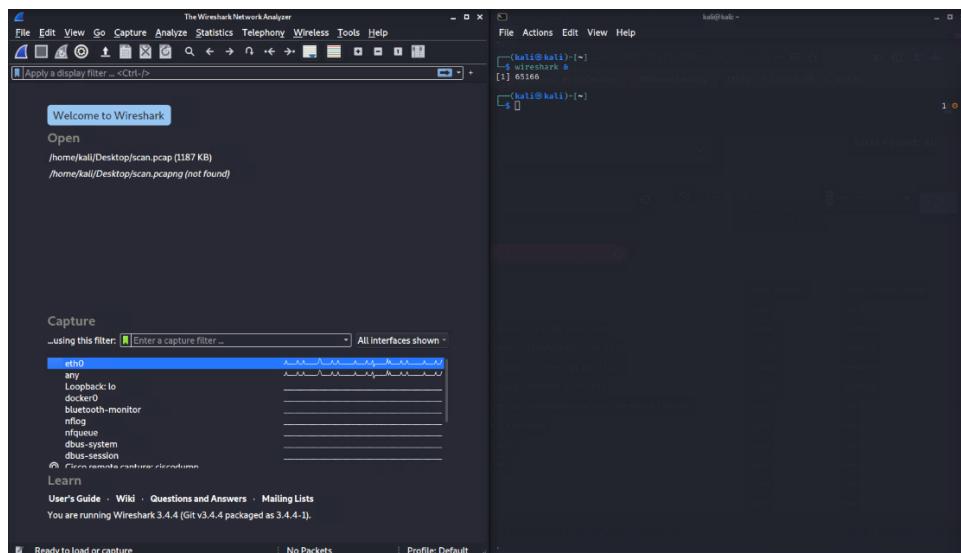
```
kali@kali$ wireshark &
```



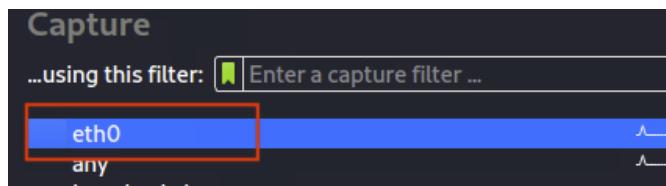
3. *Wireshark* should open, and on the *Welcome* page, you should see the wave line updating itself continuously on interface *eth0*.



4. Rearrange the windows, so you can see both *Wireshark* and the *Terminal* on the screen.



5. In the *Wireshark* window, double-click on **eth0** to start capturing traffic.



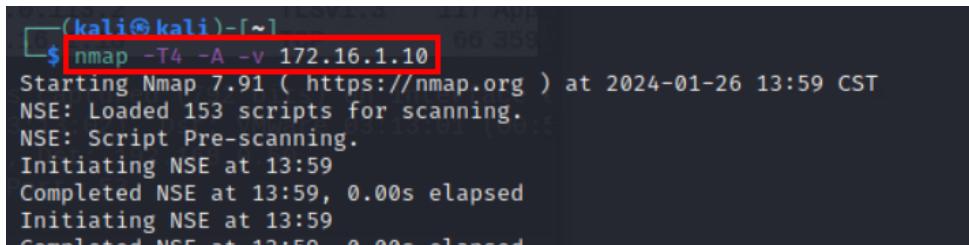
6. Keep the capture running and switch attention to the *Terminal* window. Type the following command to start an *nmap* scan.

```
kali㉿kali: ~ nmap -T5 203.0.113.1 192.168.0.0/24 172.16.1.0/28
```

```
nmap -T5 203.0.113.1 192.168.0.0/24 172.16.1.0/28
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-26 13:58 CST
Nmap scan report for 203.0.113.1
Host is up (0.00033s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain      DNS
80/tcp    open  http        DNS
Nmap scan report for pfsense.netlab.local (192.168.0.1)
Host is up (0.00042s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain      DNS
80/tcp    open  http        DNS
Nmap scan report for seconion.netlab.local (192.168.0.6)
Host is up (0.00043s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
Nmap scan report for 172.16.1.1
Host is up (0.00034s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00033s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
Nmap done: 273 IP addresses (5 hosts up) scanned in 8.63 seconds
```

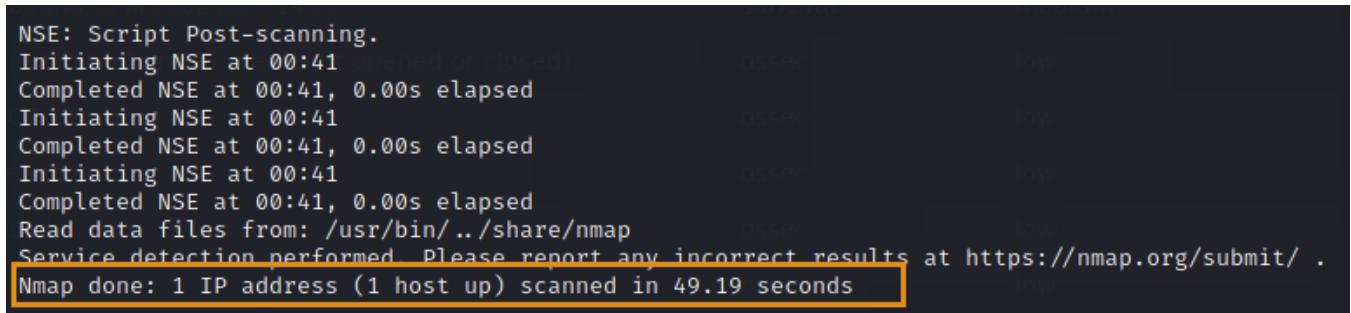
- After the scan is finished, type the following command to target the 172.16.1.10 host to start an intensive scan. This may take 1-2 minutes to complete.

```
kali㉿kali:~$ nmap -T4 -A -v 172.16.1.10
```

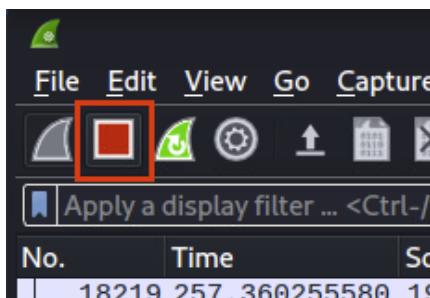


```
(kali㉿kali)-[~]
$ nmap -T4 -A -v 172.16.1.10
Starting Nmap 7.91 ( https://nmap.org ) at 2024-01-26 13:59 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:59
Completed NSE at 13:59, 0.00s elapsed
Initiating NSE at 13:59
Completed NSE at 13:59, 0.00s elapsed
```

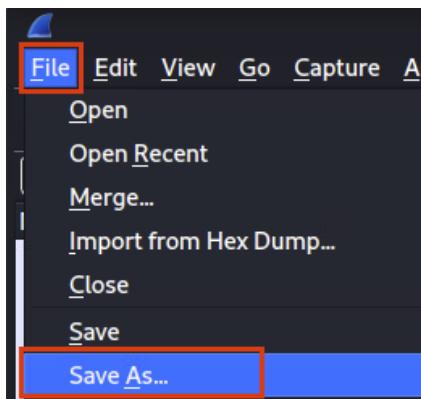
- Once the scan is complete, it will say *Nmap done...* Stop the Wireshark capture by clicking the red square button.



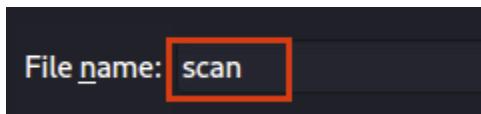
```
NSE: Script Post-scanning.
Initiating NSE at 00:41 (closed)
Completed NSE at 00:41, 0.00s elapsed
Initiating NSE at 00:41 (closed)
Completed NSE at 00:41, 0.00s elapsed
Initiating NSE at 00:41 (closed)
Completed NSE at 00:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 49.19 seconds
```



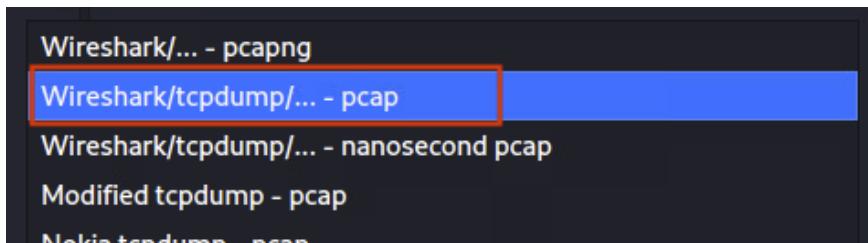
- Click on **File**, then the **Save As...** option.



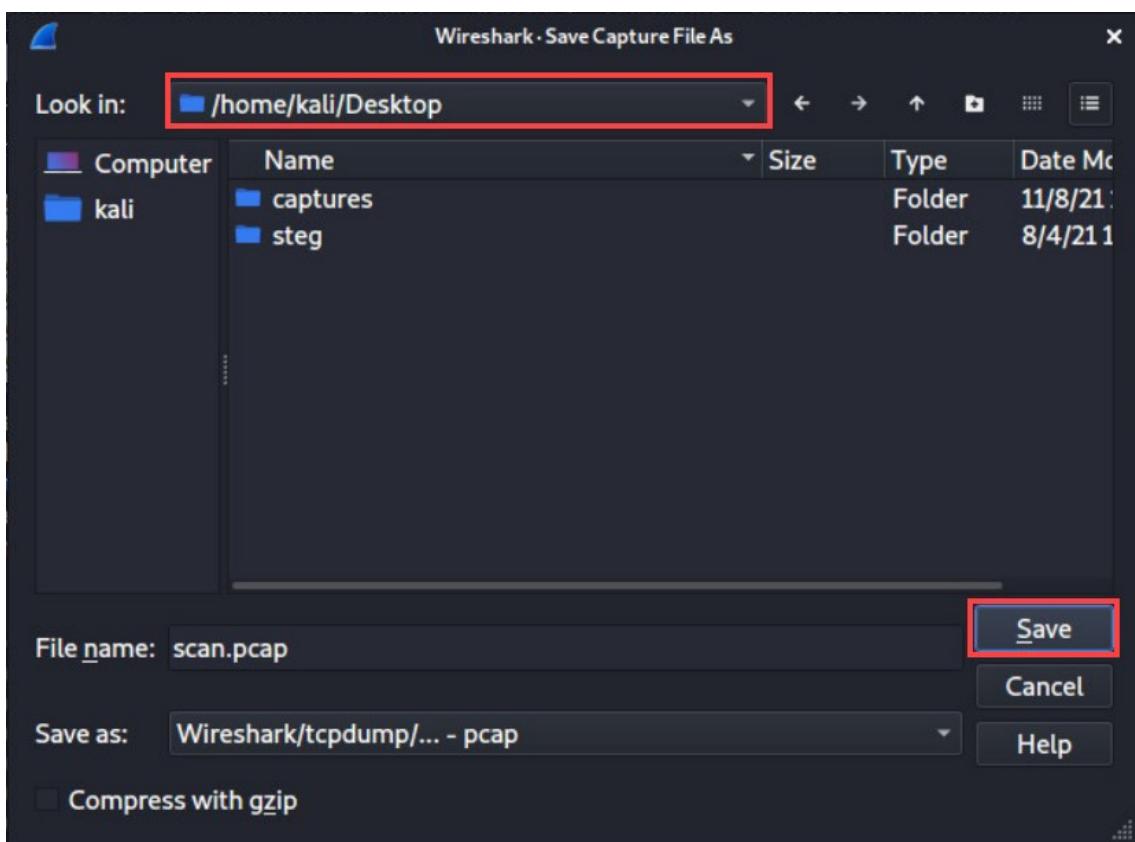
10. Type **scan** as the File name.



11. Then, click the dropdown box to the right side of **Save as:**, select the second option **Wireshark/tcpdump/... - pcap**.



12. Before you click the **Save** button, double-check the path to the file; we will save it to the **/home/kali/Desktop** folder. Then, click the **Save** button.



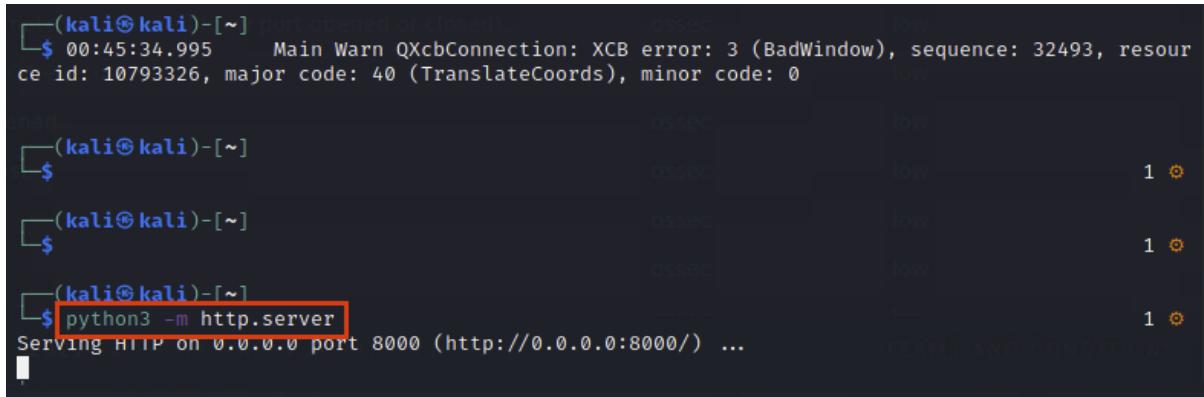
13. Leave the *Wireshark* window open and proceed to the next section.

1.3 Import the Traffic Capture

In this section, you will import the pcap file to the *Security Onion* for further analysis.

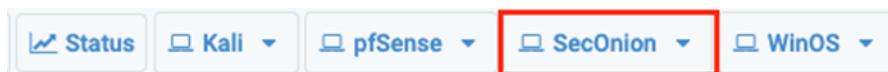
1. Switch back to the *Terminal* window. Press **Enter** a couple of times to bring back the prompt. Then, we will start a simple HTTP server by using the following command; the server will run on default port 8000.

```
kali㉿kali$ python3 -m http.server
```



```
(kali㉿kali)-[~]
$ 00:45:34.995      Main Warn QXcbConnection: XCB error: 3 (BadWindow), sequence: 32493, resource id: 10793326, major code: 40 (TranslateCoords), minor code: 0
...
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
TERMINAL AND CONSOLE
```

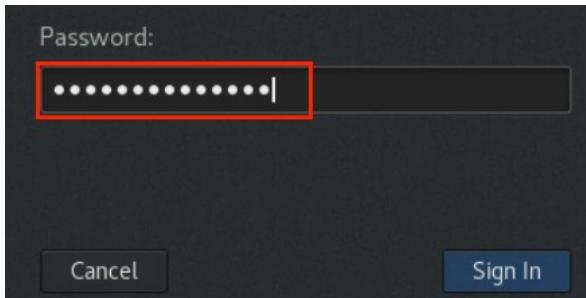
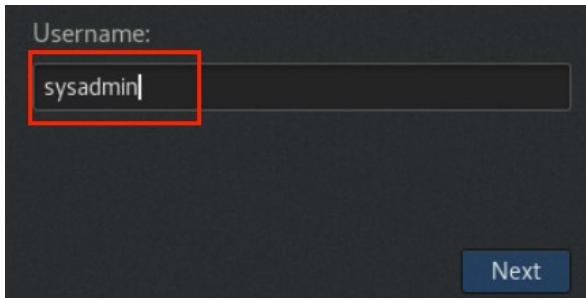
2. We will now log in to the *SecOnion* VM. Click on the **SecOnion** tab.



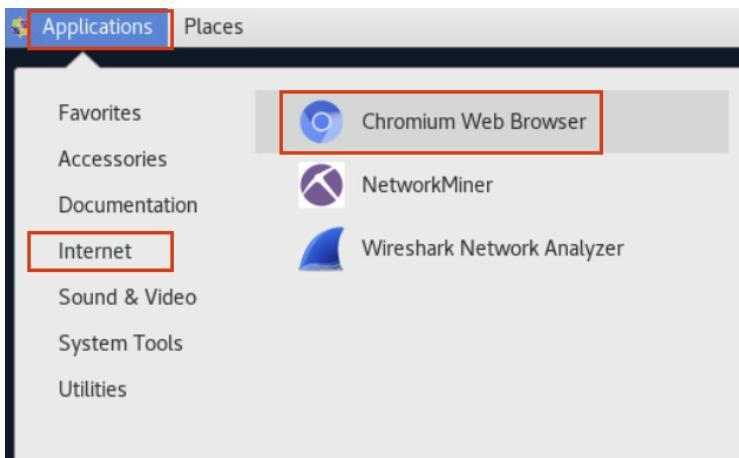
3. Then click and drag up to unlock the screen for a login prompt.



4. Type **sysadmin** as the username and **NDGLabpass123!** for the password.



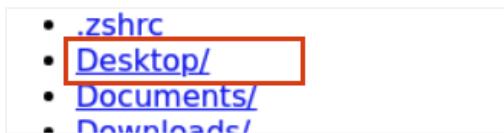
5. Once logged in, click **Applications > Internet > Chromium Web Browser** to start the browser.



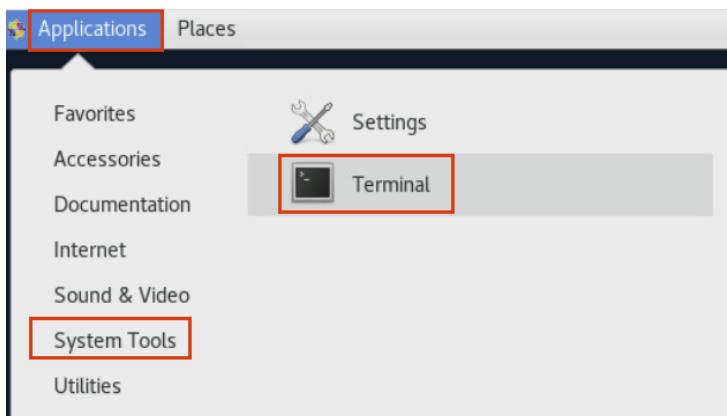
6. In the address bar, type the address **http://203.0.113.2:8000**.



7. In the opened page, find and click on **Desktop**, then click on **scan.pcap** to download the file.



8. Once the file is downloaded (it takes about 5 seconds), close all the browser windows. If it prompts saying a download is in progress, do not close the window. Wait a little bit longer and try closing it again.
9. Now, click **Applications** again, and then **System Tools**, then click **Terminal** to start a terminal window.



10. We will first check the status of the services required for this lab. In the *Terminal* window, type **sudo so-status**. When prompted for a password, type **NDGLabpass123!**. Then, the command will run and check all services. The result should show *OK* on all of them. If not, wait a couple of minutes and check again. The status of *OK* is critical to this lab; you will want to wait until all of them indicate *OK*.

```
[sysadmin@seconion ~]$ sudo so-status
[sudo] password for sysadmin:

Checking Docker status
Docker ----- [ OK ]
Checking container statuses
so-aptcacherng ----- [ OK ]
so-cortex ----- [ OK ]
so-curator ----- [ OK ]
so-dockerregistry ----- [ OK ]
so-elastalert ----- [ OK ]
so-elasticsearch ----- [ OK ]
so-filebeat ----- [ OK ]
so-fleet ----- [ OK ]
```

11. Next, we can import the pcap file to *SecOnion*. Type the following command; if prompted for a password, enter **NDGlabpass123!**. When the import completes, it will say that the events will *take 30 seconds or more to appear in Hunt*. We'll wait a little bit here.

```
[sysadmin@seconion ~]$ sudo so-import-pcap ~/Downloads/scan.pcap
```

```
[sysadmin@seconion ~]$ sudo so-import-pcap ~/Downloads/scan.pcap
Processing Import: /home/sysadmin/Downloads/scan.pcap
- verifying file
- assigning unique identifier to import: 1e652a11e7ed4c436cc8fce935206856
- analyzing traffic with Suricata
- analyzing traffic with Zeek
- saving PCAP data spanning dates 2024-01-26 through 2024-01-26
```

Cleaning up:

Import complete!

You can use the following hyperlink to view data in the time range of your import. You can triple-click to quickly highlight the entire hyperlink and you can then copy it into your browser:
<https://192.168.0.6/#/dashboards?q=import.id:1e652a11e7ed4c436cc8fce935206856%20%7C%20groupby%20-sankey%20event.dataset%20event.category%2a%20%7C%20groupby%20-pie%20event.category%20%7C%20grouby%20-bar%20event.module%20%7C%20groupby%20event.dataset%20%7C%20groupby%20event.module%20%7C%20groupby%20event.category%20%7C%20groupby%20observer.name%20%7C%20groupby%20source.ip%20%7C%20groupby%20destination.ip%20%7C%20groupby%20destination.port&t=2024%2F01%2F26%2000%3A00%3A00%20AM%20-%202024%2F01%2F27%2000%3A00%3A00%20AM&z=UTC>

or you can manually set your Time Range to be (in UTC):

From: 2024-01-26 To: 2024-01-27

Please note that it may take 30 seconds or more for events to appear in Security Onion Console.

12. Leave the *Terminal* window open and proceed to the next section.

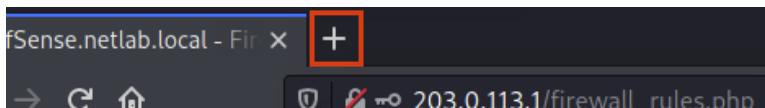
2 Analyze the Data and File a Case

In this section, you will analyze the captured data and then create and solve the case.

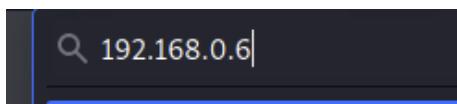
1. Switch to the *Kali VM*. In the *Terminal*, we should still have the server running. Press **Ctrl + C** to stop the process.

```
(kali㉿kali)-[~]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.0.6 - - [26/Jan/2024 14:12:49] "GET / HTTP/1.1" 200 -
192.168.0.6 - - [26/Jan/2024 14:12:49] code 404, message File not found
192.168.0.6 - - [26/Jan/2024 14:12:49] "GET /favicon.ico HTTP/1.1" 404 -
192.168.0.6 - - [26/Jan/2024 14:12:53] "GET /Desktop/ HTTP/1.1" 200 -
192.168.0.6 - - [26/Jan/2024 14:12:56] "GET /Desktop/scan.pcap HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

2. Switch back to the browser window, click the **+** to start a new tab.



3. Type **192.168.0.6** and press **Enter** to visit the *SecurityOnion* main page.



4. If the warning page shows up, click the **Advanced...** button. Then, scroll down and click **Accept the Risk and Continue**.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#) **Advanced...**

Someone could be trying to impersonate the site and you should not continue.

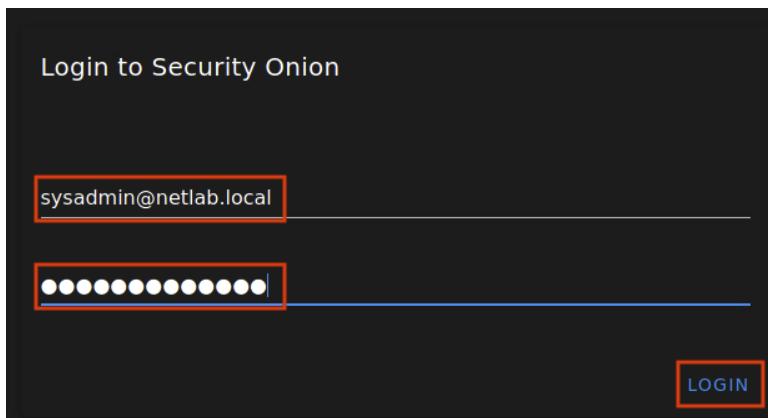
Websites prove their identity via certificates. Firefox does not trust 192.168.0.6 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

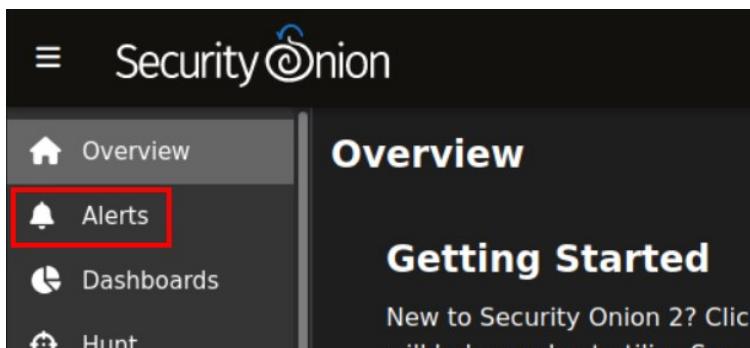
[View Certificate](#)

[Go Back \(Recommended\)](#) **Accept the Risk and Continue**

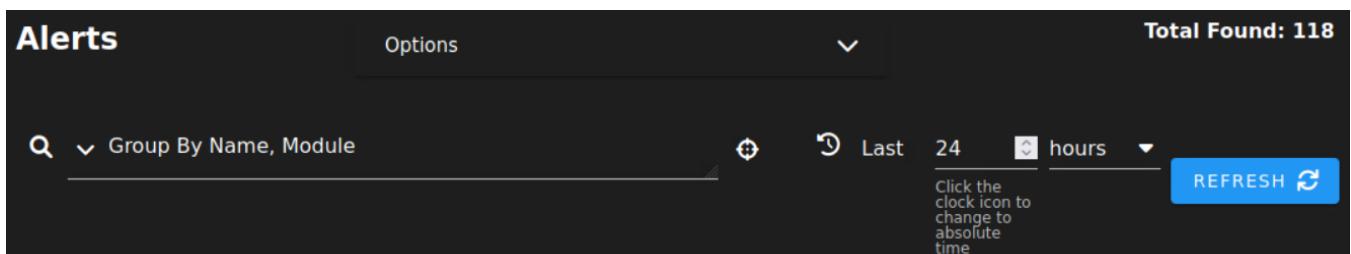
5. On the *Login* page, enter the *username* as `sysadmin@netlab.local` and the password as `NDGlabpass123!`. Click **LOGIN**.



6. On the *Overview* page, click the menu button at the top-left corner. Then, click on **Alerts**.



7. If the import is finished, you will see the top of the screen like below, indicating there were **118** alerts found; they were grouped by name and module, and you can change the time of the findings.



8. At the bottom half of the screen, in the list, the colored bell icon indicates the severity; however, please note that clicking on the icon will acknowledge the alert instead of opening the details of the alert. The blue triangle with an exclamation mark inside is the *Escalate* button. Clicking on it will raise the alert so that it can be added to a case. We will cover it in the following section. The third column in the list shows the number of alerts grouped by the rule name (fourth column) and module (fifth column). The last column shows the severity of the alert. You may need to hide the navigation pane on the left to see all the columns.

Count	rule.name		event.module		event.severity_label
28	ET SCAN Possible Nmap User-Agent Observed		suricata		high
28	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)		suricata		high
7	System Audit event.		ossec		low
7	ET SCAN Suspicious inbound to mySQL port 3306		suricata		medium
7	ET SCAN Suspicious inbound to PostgreSQL port 5432		suricata		medium

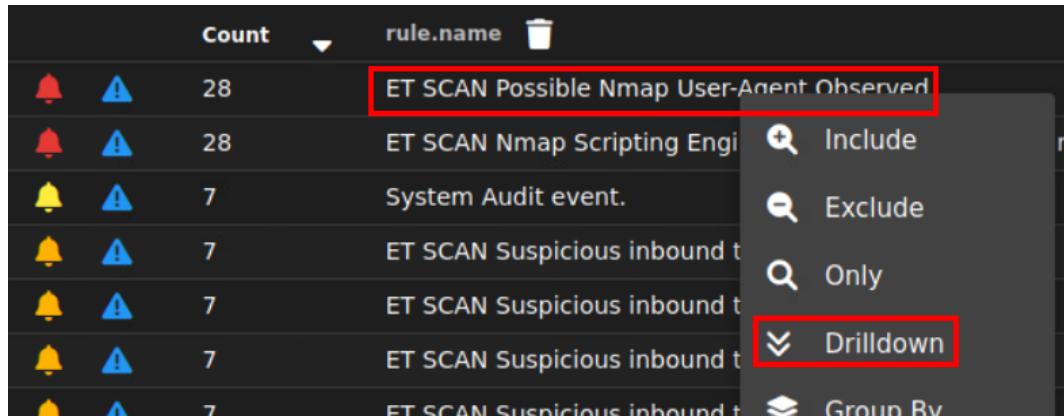
9. Leave the SecurityOnion window open and proceed to the next section.

3 Add a Case, Investigate, and Close the Case

In this section, you will add a case, perform an investigation, and then close the case.

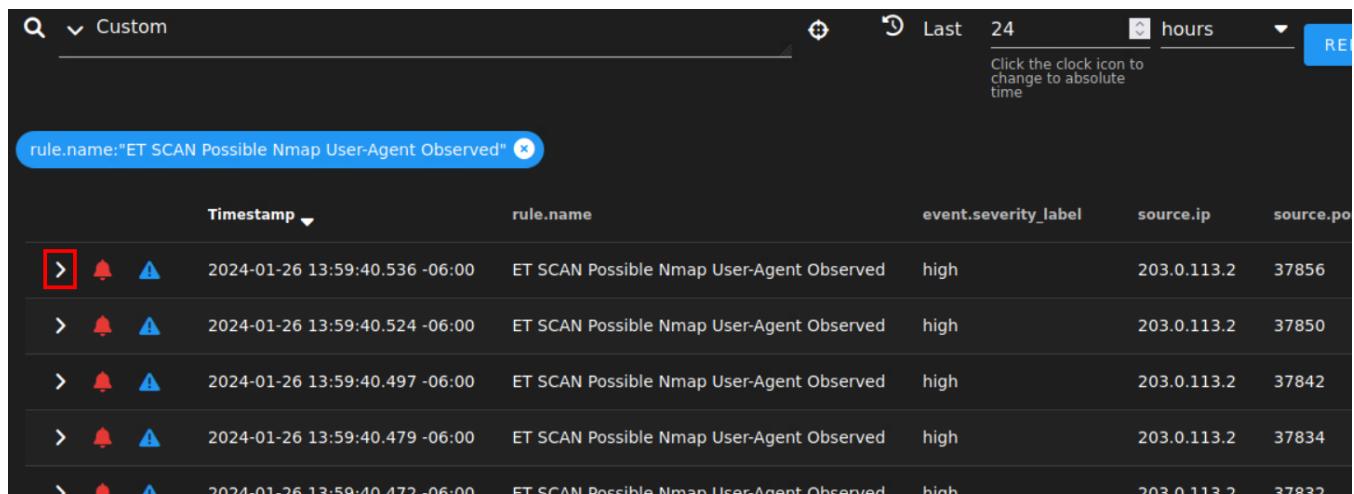
3.1 Escalate an Alert to Add a Case

- With the *SecurityOnion* still opened, let's examine the alerts and analyze a few of them. First, left-click on the **ET SCAN Possible Nmap User-Agent Observed** rule name, then select the **Drilldown** option.



A screenshot of the SecurityOnion interface showing a dropdown menu. The menu items are: Include, Exclude, Only, Drilldown, and Group By. The 'Drilldown' option is highlighted with a red box.

- The view will be changed, and you should see something like below, click the arrow in front of the first entry.



A screenshot of the SecurityOnion interface showing a detailed list of alerts. The search bar at the top contains the query: rule.name:"ET SCAN Possible Nmap User-Agent Observed". The results table has columns: Timestamp, rule.name, event.severity_label, source.ip, and source.port. The first row is expanded, indicated by a red box around the greater-than sign (>) in the Timestamp column. The expanded row shows the full timestamp (2024-01-26 13:59:40.536 -06:00), rule name (ET SCAN Possible Nmap User-Agent Observed), severity (high), source IP (203.0.113.2), and source port (37856).

Timestamp	rule.name	event.severity_label	source.ip	source.port
> 2024-01-26 13:59:40.536 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	37856
> 2024-01-26 13:59:40.524 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	37850
> 2024-01-26 13:59:40.497 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	37842
> 2024-01-26 13:59:40.479 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	37834
> 2024-01-26 13:59:40.472 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	37832

3. Detailed information about this alert will show up. Scroll down to learn more about it, e.g., *destination.ip*, *destination.port*, *source.ip*, *source.port*, *network.data.decoded*, *rule.rule*, etc.

v	!	⚠	2024-01-26 13:59:40.536 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	37856
☰	@timestamp	2024-01-26T19:59:40.536Z					
☰	@version	1					
☰	destination.ip	172.16.1.10					
☰	destination.port	80					
☰	ecs.version	8.0.0					
☰	event.category	network					
☰	event.dataset	alert					
☰	event.ingested	2024-01-26T20:14:20.248Z					
☰	event.module	suricata					
☰	event.severity	3					
☰	event.severity_label	high					

4. Once again, left-click on the **ET SCAN Possible Nmap User-Agent Observed** rule name, then select **Actions**, then **PCAP** to show the captured packet for this alert.

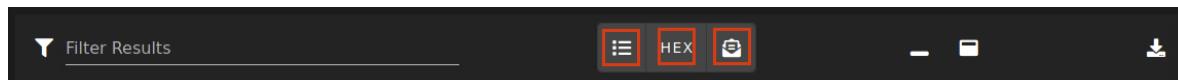
v	!	⚠	2024-01-26 13:59:40.536 -06:00	ET SCAN Possible Nmap User-Agent Observed	high		
☰	@timestamp	2024-01-26T19:59:40.536Z					
☰	@version	1					
☰	destination.ip	172.16.1.10					
☰	destination.port	80					
☰	ecs.version	8.0.0					
☰	event.category	network					
☰	event.dataset	alert					
☰	event.ingested	2024-01-26T20:14:20.248Z					
☰	event.module	suricata					
☰	event.severity	3					
☰	event.severity_label	high					
☰	host.name	seconion					
☰	import.file	eve-2024-01-26-20:14.json					
☰	import.id	1e652a11e7ed4c436cc8fce935206856					
☰	imported	true					

Include
Exclude
Only
Group By
New Group By
Clipboard
Actions
Hunt
Correlate
PCAP
CyberChef
Google

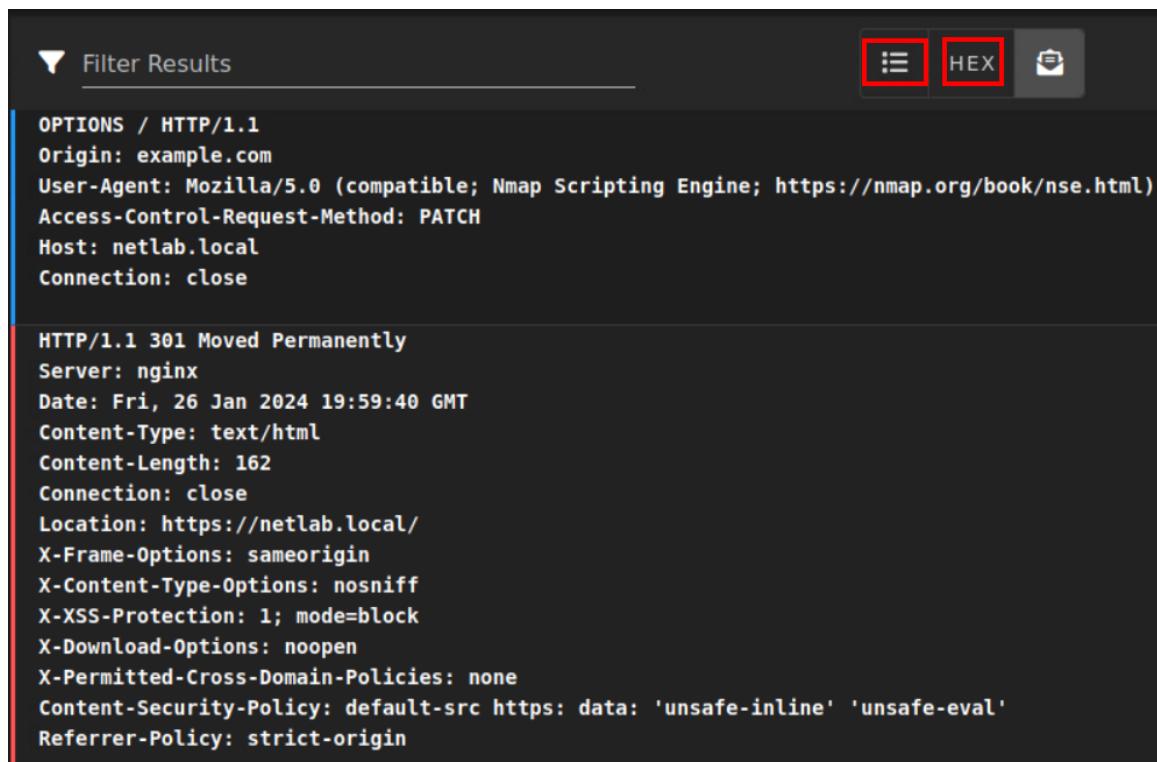
5. We will be brought to the *PCAP* view, which shows the stream of this traffic, starting from the three-way handshake.

Num	Timestamp	Type	Source IP	Source Port	Destination IP	Destination Port	Flags
0	2024-01-26 13:59:40.536 -06:00	TCP	203.0.113.2	37856	172.16.1.10	80	SYN
1	2024-01-26 13:59:40.536 -06:00	TCP	172.16.1.10	80	203.0.113.2	37856	SYN ACK
2	2024-01-26 13:59:40.536 -06:00	TCP	203.0.113.2	37856	172.16.1.10	80	ACK
3	2024-01-26 13:59:40.536 -06:00	TCP	203.0.113.2	37856	172.16.1.10	80	PSH ACK
4	2024-01-26 13:59:40.536 -06:00	TCP	172.16.1.10	80	203.0.113.2	37856	ACK
5	2024-01-26 13:59:40.536 -06:00	TCP	172.16.1.10	80	203.0.113.2	37856	PSH ACK

6. Feel free to switch on and off the toggles to see different views of the captured traffic.



7. If you are familiar with the *Follow Stream* on Wireshark, you may find this view also exists in the *Security Onion PCAP* module (click the first list toggle, then the HEX toggle).



```

OPTIONS / HTTP/1.1
Origin: example.com
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
Access-Control-Request-Method: PATCH
Host: netlab.local
Connection: close

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Fri, 26 Jan 2024 19:59:40 GMT
Content-Type: text/html
Content-Length: 162
Connection: close
Location: https://netlab.local/
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Referrer-Policy: strict-origin

```

8. Next, let's go back by clicking the **Back** button in the browser.



9. Once the page is loaded, left-click on the **source.ip** of **203.0.113.2** and select the **Only** option. This will filter the alerts to only show the ones that originated from the source IP of 203.0.113.2, which is our *Kali* VM.

Timestamp	rule.name	event.severity_label	source.ip	
> 2024-01-26 13:59:40.536 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	Include
> 2024-01-26 13:59:40.524 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	Exclude
> 2024-01-26 13:59:40.497 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	Only

10. Now, we can see that **86** of the alerts are filtered, and they were all originated from the *Kali* VM. Feel free to scroll up and down to see the severity levels of those alerts.

Timestamp	rule.name	event.severity_label	source.ip
> 2024-01-26 14:12:56.726 -06:00	ET INFO Python SimpleHTTP ServerBanner	low	203.0.113.2
> 2024-01-26 14:12:49.866 -06:00	ET INFO Python SimpleHTTP ServerBanner	low	203.0.113.2
> 2024-01-26 14:12:49.590 -06:00	ET INFO Python SimpleHTTP ServerBanner	low	203.0.113.2
> 2024-01-26 13:59:40.536 -06:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2
> 2024-01-26 13:59:40.536 -06:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	203.0.113.2

11. Click on the **Timestamp** column header to list the results in chronological order. Now we see that the first alert is a medium severity with suspicious inbound activity. Once again, let's left-click on the name and select **Actions**, then select **Hunt**. If you don't see a brute force rule name, you may select another alert of your choice to proceed in the next steps.

The screenshot shows the 'Alerts' page of the Security Onion interface. The main table lists network events with columns for 'Timestamp' and 'rule.name'. The first event in the list is 'ET SCAN Suspicious inbound to mySQL port 3306'. A context menu is open over this event, with the 'Actions' option selected. At the bottom right of the interface, the 'Hunt' button is also highlighted with a red box.

12. You will see the *Hunt* tool page as shown below. On this page, it will bring more details about this alert most of the time. *Hunt* is used to find similar events, track down malicious files, and observe malicious behaviors. We will not go into details about how to use *Hunt* in this lab.

The screenshot shows the 'Hunt' tool page of the Security Onion interface. The search bar contains the query 'ET SCAN Suspicious inbound to mySQL port 3306' | groupby event.module event.dataset. Below the search bar are three charts: 'Most Occurrences' (suricata), 'Timeline' (a single point at 1:00:00.000 pm), and 'Fewest Occurrences' (suricata).

13. Click the browser **Back** button again. Let's say that we need to escalate and create a case for the suspicious inbound activity and *nmap* scan alert. If you don't see the following selections, you may select another alert of your choice to proceed to the next steps. Click on the first **blue triangle** and then select **+ Escalate to new case**.

The screenshot shows the Security Onion Alerts interface. A search bar at the top has the query "203.0.113.2". Below it is a table with columns "Timestamp" and "rule.name". The first row shows an alert from "2024-01-26 13:58:51.366 -06:00" with the rule name "ET SCAN Suspicious inbound to MySQL port 3306". A blue triangle icon is to the left of the timestamp. A context menu is open over this row, with the option "+ Escalate to new case" highlighted by a red box. Other options in the menu include "Attach event to a recently viewed case:" and "ET SCAN Suspicious inbound to MySQL port 3306".

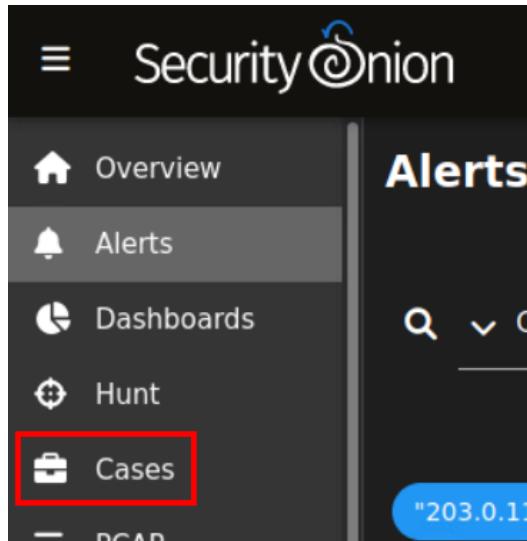
14. Once added, it's going to prompt and say *Escalated alert and removed from view.*

The screenshot shows the Security Onion Alerts interface. At the top, there is a banner message "Escalated alert and removed from view. X". Below it is the same alerts table as the previous screenshot. The first row is visible again, showing the alert from "2024-01-26 13:58:51.366 -06:00" with the rule name "ET SCAN Suspicious inbound to MySQL port 3306".

15. Leave the window open to continue with the next task.

3.2 Add Observable and Tasks for Further Investigation

1. View the Cases dashboard by navigating to the top-left corner, clicking the **Menu** button, then selecting the **Cases** menu option.



2. You should see the case list with the newly added cases.

Cases		Options	Total Found: 1
+			
Open Cases		Last 12 months	REFRESH
		Click the clock icon to change to absolute time	
NOT so_case.status:closed	NOT so_case.category:template		
Timestamp	so_case.title	so_case.status	so_case.severity
2024-01-26 14:54:27.255 -06:00	ET SCAN Suspicious inbound to MySQL port 3306	new	medium

3. Click on the right arrow next to the first case entry to view additional details related to the case. Review the information.

<input checked="" type="checkbox"/>		2024-01-26 14:54:27.255 -06:00	ET SCAN Suspicious inbound to mySQL port 3306	new	medium
	@timestamp	2024-01-26T20:54:27.255819237Z			
	so_case.assigneeId				
	so_case.category				
	so_case.completeTime				
	so_case.createTime	2024-01-26T20:54:27.255802619Z			
	so_case.description	Review escalated event details in the Events tab below. Click here to update this description			
	so_case.pap				
	so_case.priority	0			
	so_case.severity	medium			
	so_case.startTime				
	so_case.status	new			
	so_case.tags				
	so_case.template				
	so_case.title	ET SCAN Suspicious inbound to mySQL port 3306			

4. Click the View button for the case entry to view more action items.

<input checked="" type="checkbox"/>		2024-01-26 14:54:27.255 -06:00	ET SCAN Suspicious inbound to mySQL port 3306	new	medium
	@timestamp	2024-01-26T20:54:27.255819237Z			
	so_case.assigneeId				
	so_case.category				
	so_case.completeTime				

5. We are going to add some extra notes. Click the **Observables** button, then click **Add a new observable to this case**.

ET SCAN Suspicious inbound to mySQL port 3306

Review escalated event details in the Events tab below. Click here to update this description.

COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

+

Filter Results

Actions	Created ▲	Updated	Type	Value
				No data available

Rows per page: 10 ▾ - < >

6. In the new window, type the following information, then click the **Add** button.
 - a. *Type:* ip
 - b. *Value:* 203.0.113.2
 - c. *Description:* If this is not a penetration testing contractor, it could be a malicious external IP address.
 - d. *Traffic Light Protocol:* red
 - e. *Tags:* nmap

ET SCAN Suspicious inbound to mySQL port 3306

Review escalated event details in the Events tab below. Click here to update this description.

COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

S Add Observable

ip
Select a type for classification purposes (Note: choose "file" type to upload a file)

203.0.113.2

Specify the observed value
 Enable this checkbox to have a separate observable added for each line of the provided value above
If this is not a penetration testing contractor, it could be a malicious external IP address.

Provide an optional description
 Enable this field if this is an Indicator of Compromise

red
Traffic Light Protocol
nmap
Annotate with multiple optional tags

CANCEL ADD



An observable is an extra piece of information we can add to aid the security team for further investigation.

7. Next step, let's add some comments. Click on the **Comments** button.

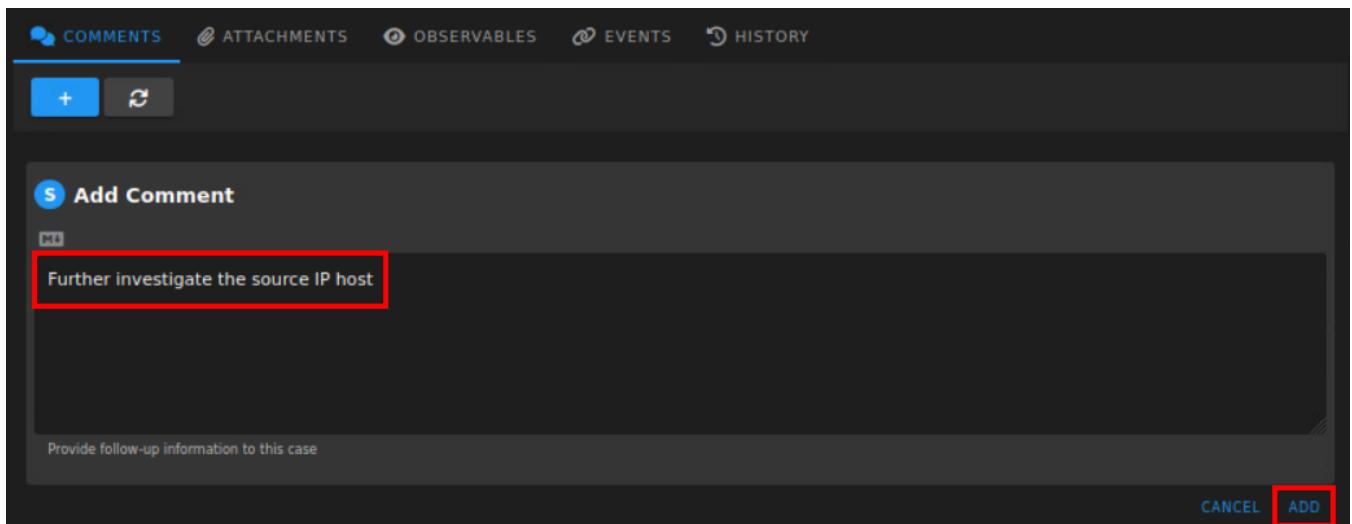
ET SCAN Suspicious inbound to mySQL port 3306

Review escalated event details in the Events tab below. Click here to update this description.

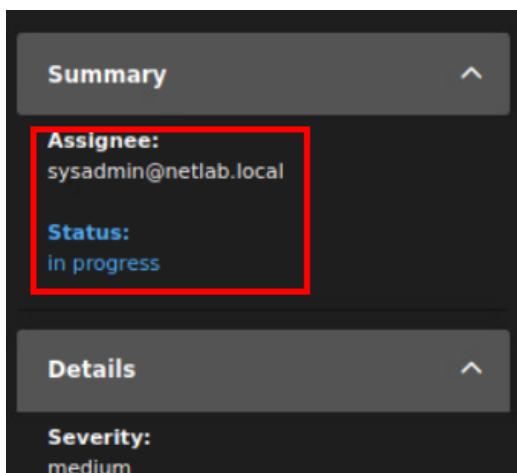
COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

+ **×**

- Type Further investigate the source IP host, click the Add button to confirm.



- In the *Summary* pane to the right, select **sysadmin@netlab.local** as the *Assignee* and **in progress** as the *Status*.

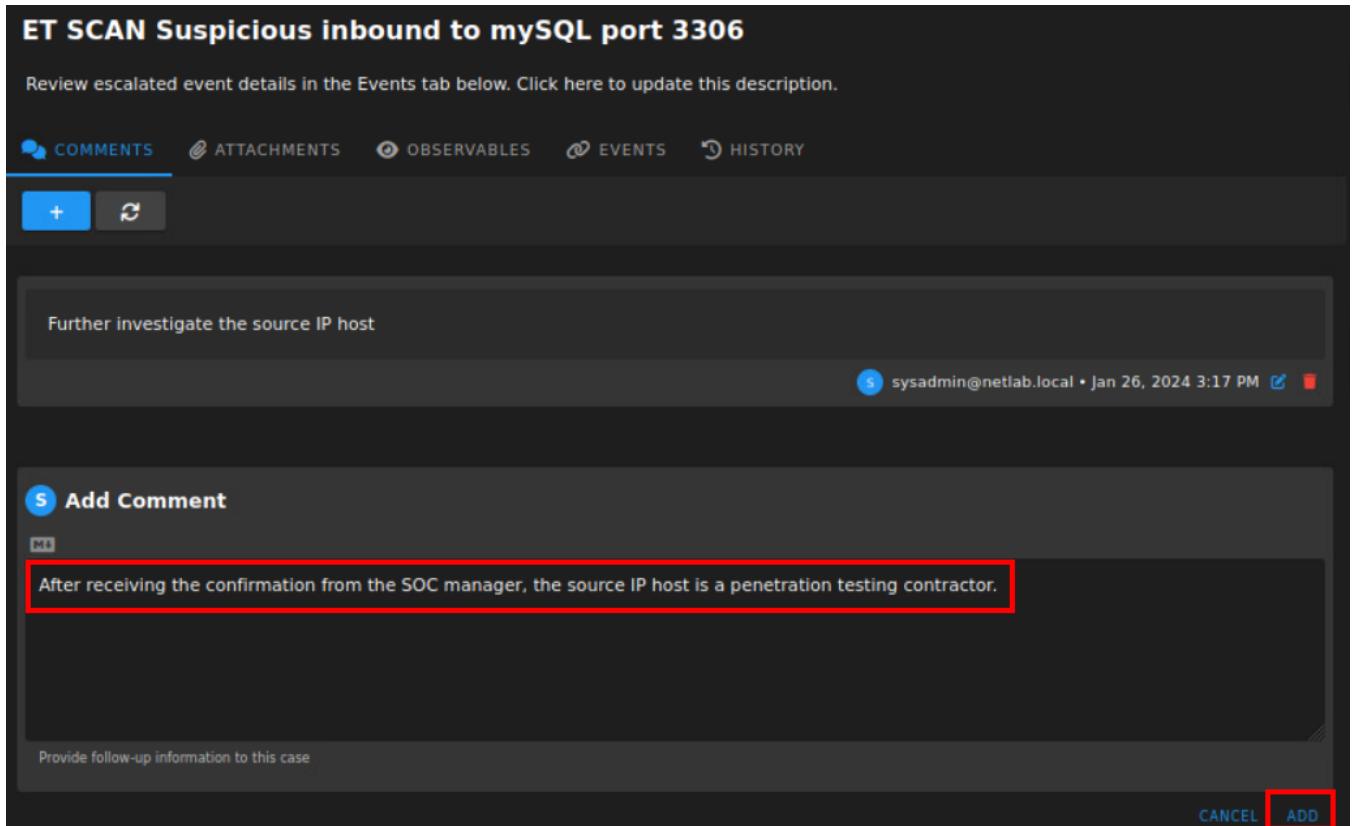


- Leave the window open to continue on with the next task.

3.3 Finish All Tasks and Close a Case

Let's assume that we are assigned to perform the task.

1. Let's assume the source IP is a penetration testing contractor. Therefore, we should add it to the log as shown below. Press the **Add log** button to save.



ET SCAN Suspicious inbound to mySQL port 3306

Review escalated event details in the Events tab below. Click here to update this description.

COMMENTS ATTACHMENTS OBSERVABLES EVENTS HISTORY

+ ⟳

Further investigate the source IP host

sysadmin@netlab.local • Jan 26, 2024 3:17 PM 🔗 ✖

S Add Comment

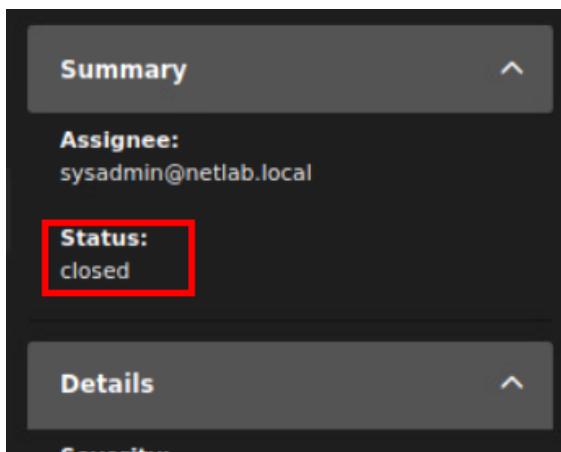
ME

After receiving the confirmation from the SOC manager, the source IP host is a penetration testing contractor.

Provide follow-up information to this case

CANCEL ADD

2. Then, we can close this task by selecting **closed** from the *Summary* pane.



Summary

Assignee:
sysadmin@netlab.local

Status:
closed

Details

Comments

3. The lab is now completed; you may end the reservation.