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

# Contents

## Introduction

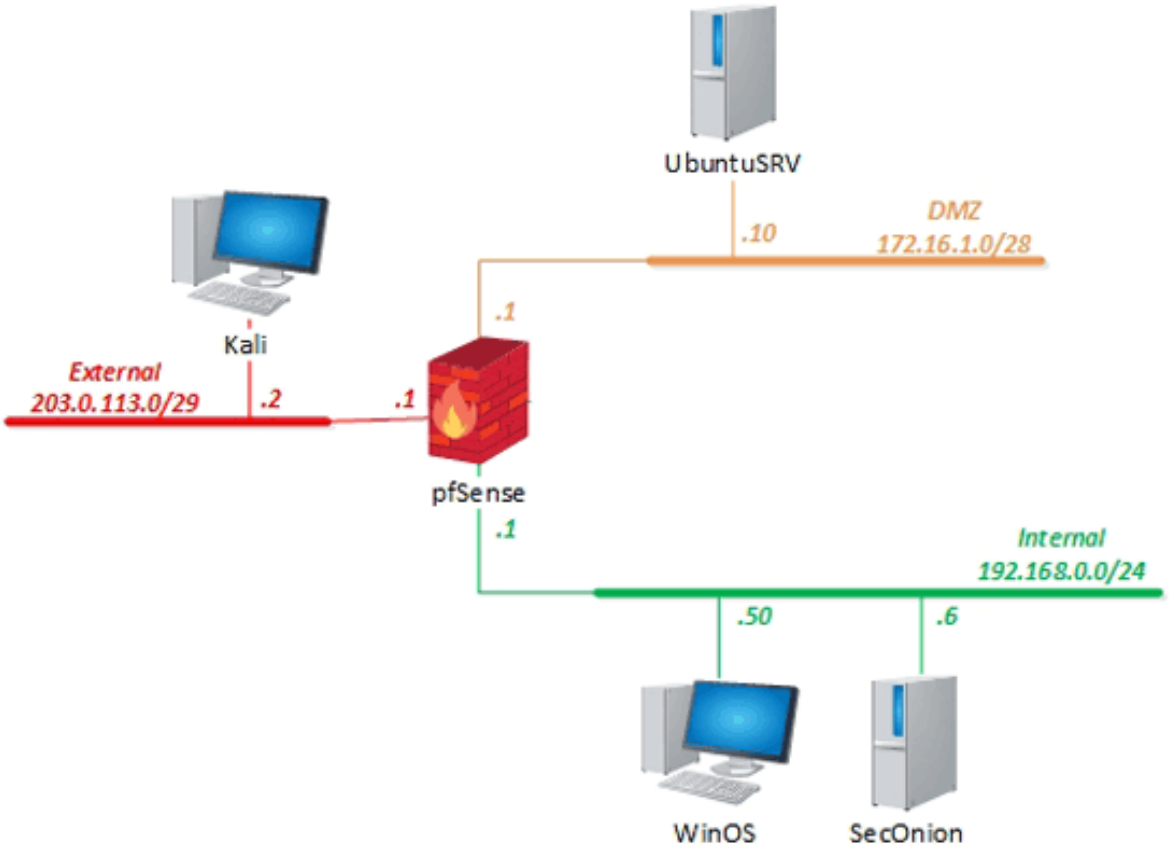
In this lab, you will be conducting network and host monitoring using various administrative tools.

## 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

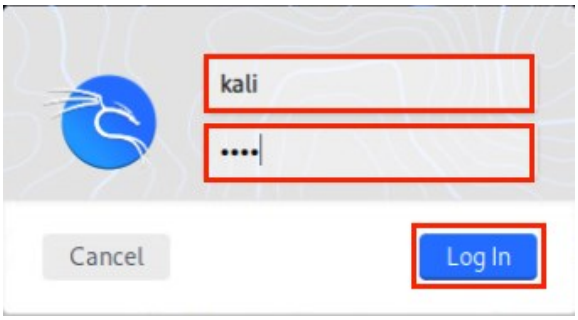
In this lab, we are using the standalone installation of *Security Onion* for all of the tasks. In a production line, you could use either a standalone or distributed installation. Because live capture will be covered in Lab 22, this lab will not use the live capture function. Instead, you will explore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

## 1.1 Disable Firewall

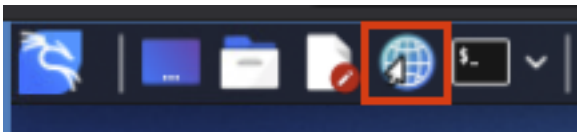
In this section, you will disable the Firewall to prepare for the traffic capture.

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


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

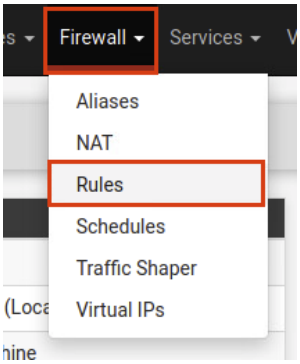



3. Click to open a browser window.

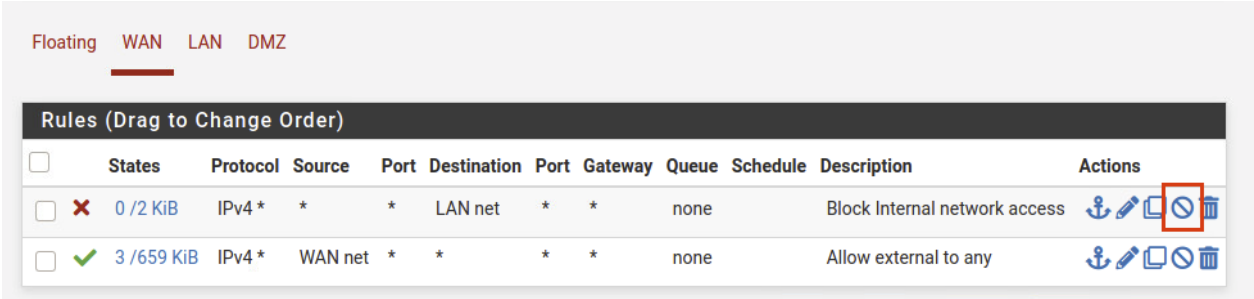


4. In the address bar, type `203.0.113.1` to go to the *pfSense* firewall management login page. Log in as username `admin`, password `NDGlabpass123!` and then click the **SIGN IN** button.

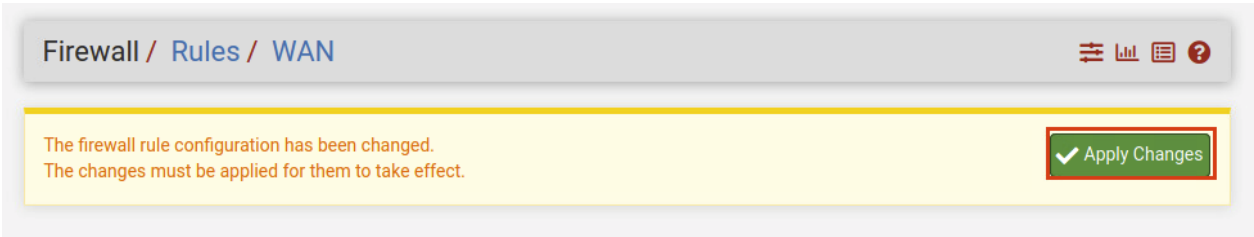
5. Once logged in, you will see the *Status/Dashboard* page; click the **Firewall** menu and select **Rules**.



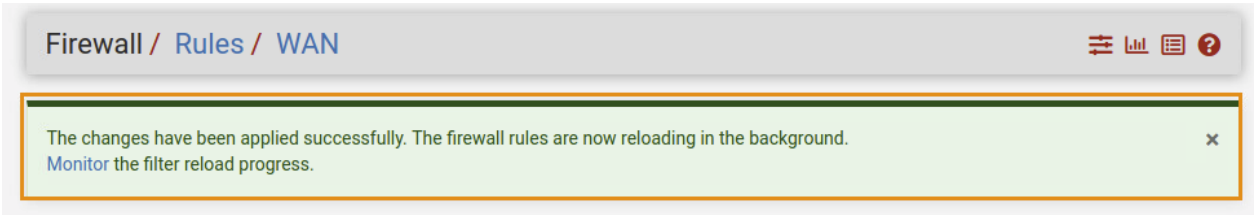

6. Click the **Disable** button to disable the **Block Internal network access** rule.




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




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



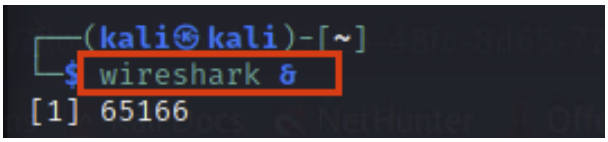
## 1.2 Capture the Traffic for Analysis

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

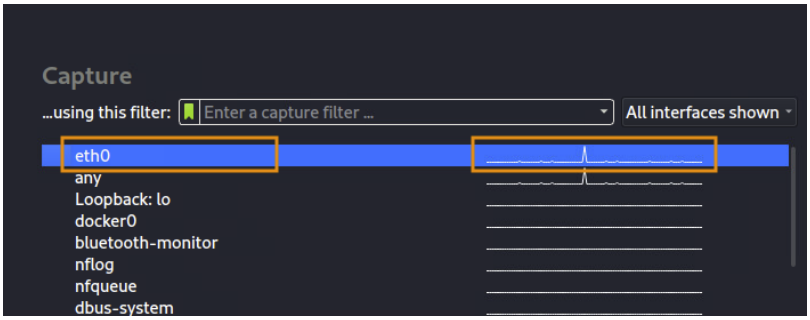
1. In the *Kali* VM, click **Terminal** to start a *Terminal* window.

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

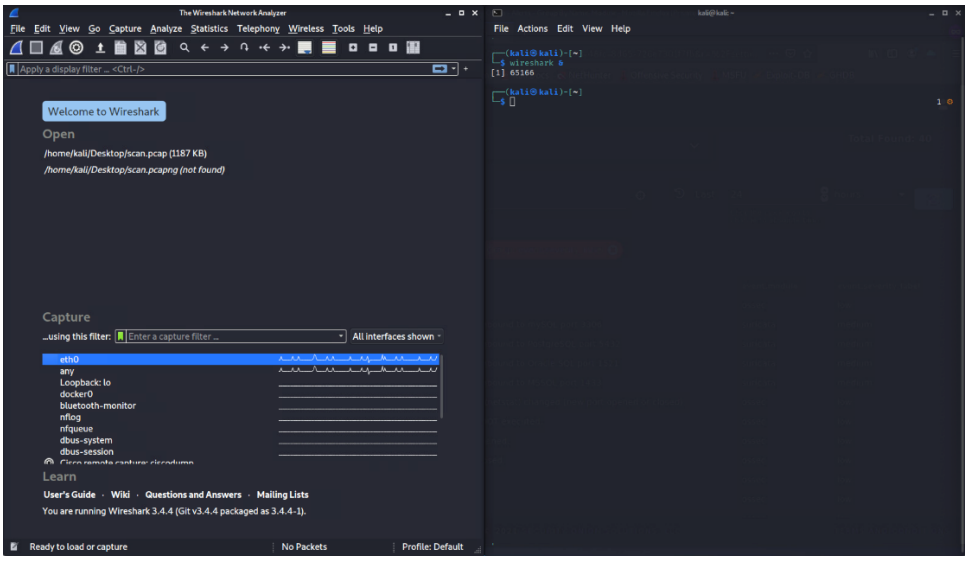
```
kali@kali$ wireshark &
```




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

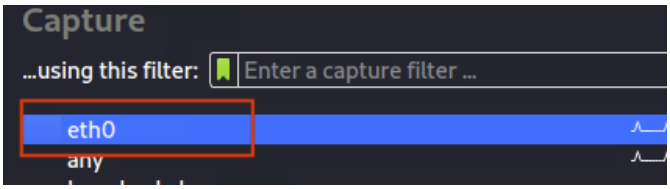



4. Rearrange the windows, so you can see both *Wireshark* and the *Terminal* on the screen.



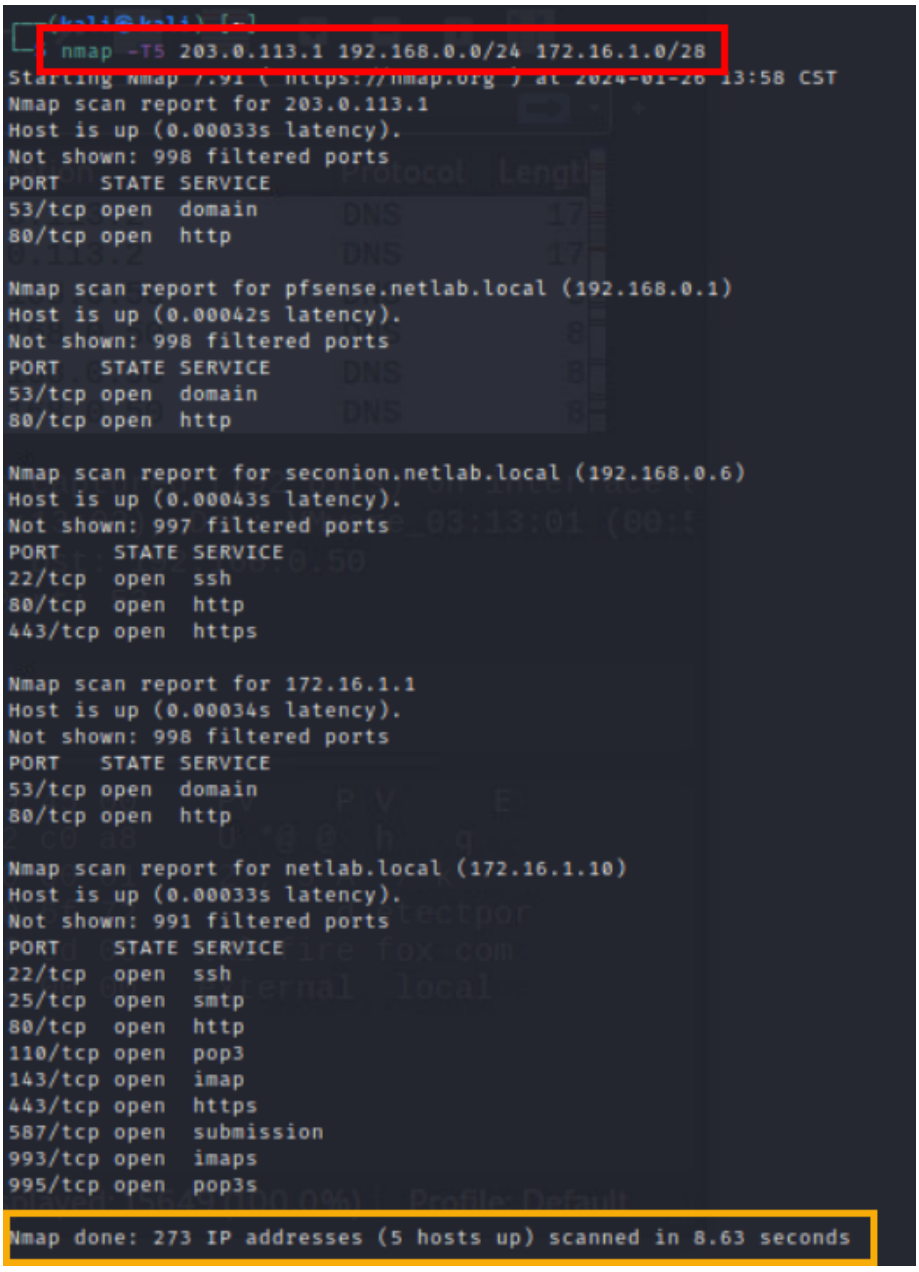

  

5. In the *Wireshark* window, double-click on **eth0** to start capturing traffic.




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

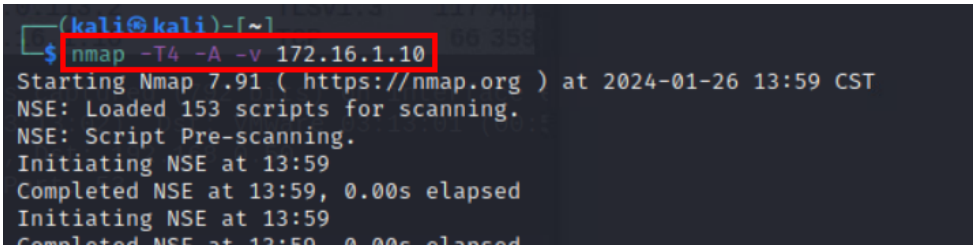
```
kali@kali$ nmap -T5 203.0.113.1 192.168.0.0/24 172.16.1.0/28
```



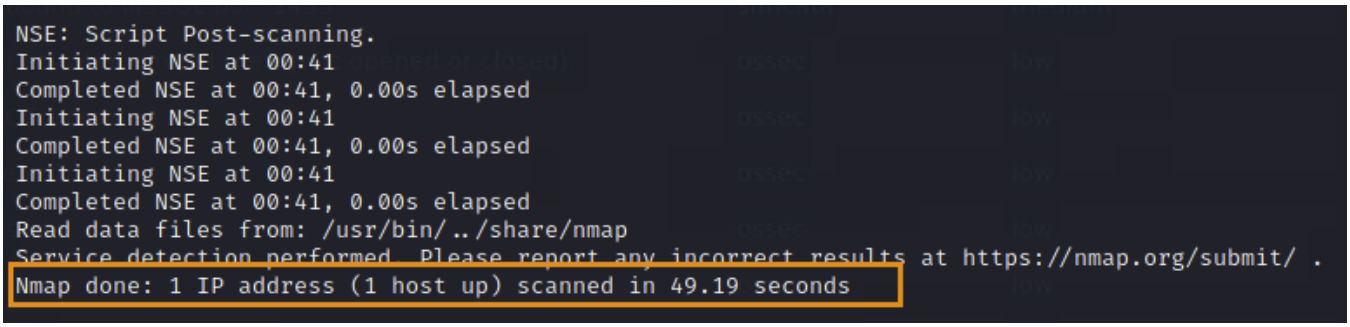

  

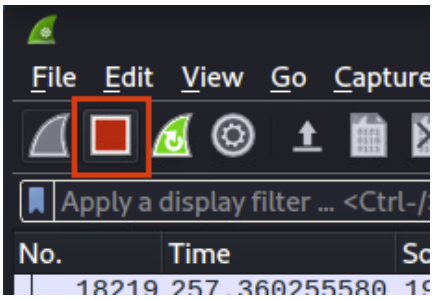
7. After the scan is finished, type the following command to target the 172.16.1.10 host to start an intensive scan. This may take 1-2 minutes to complete.

```
kali@kali$ nmap -T4 -A -v 172.16.1.10
```

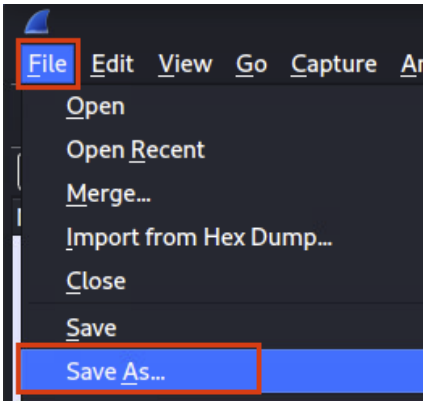



8. Once the scan is complete, it will say *Nmap done…* Stop the Wireshark capture by clicking the red square button.



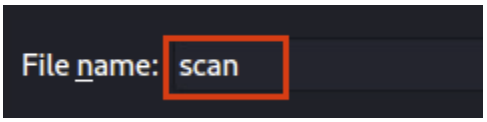




9. Click on **File**, then the **Save As…** option.

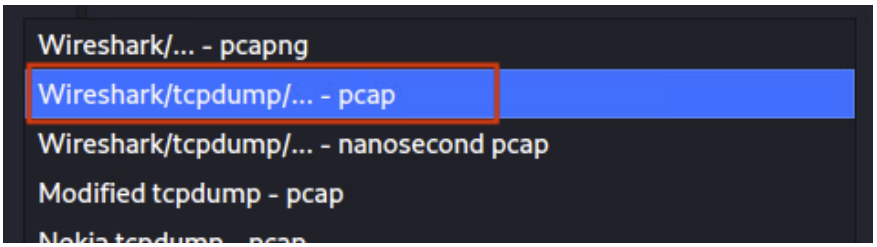


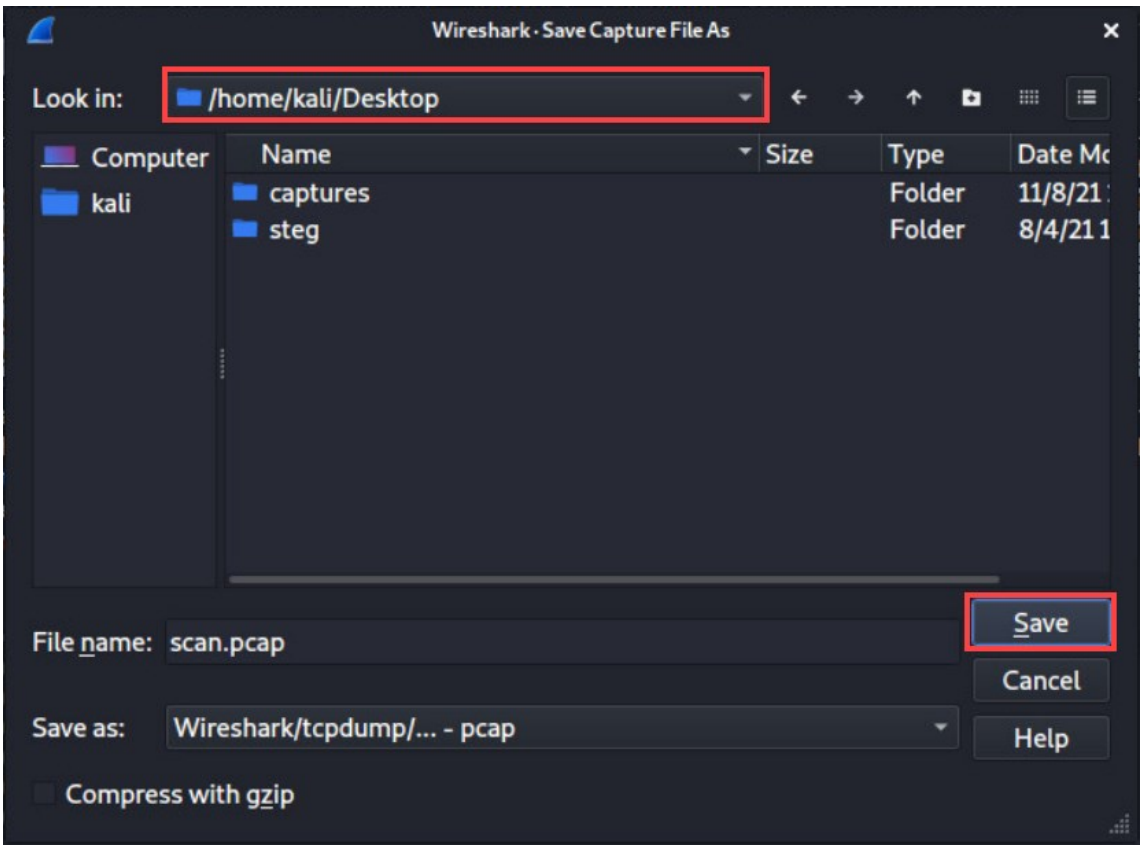
10. Type `scan` as the File name.




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.



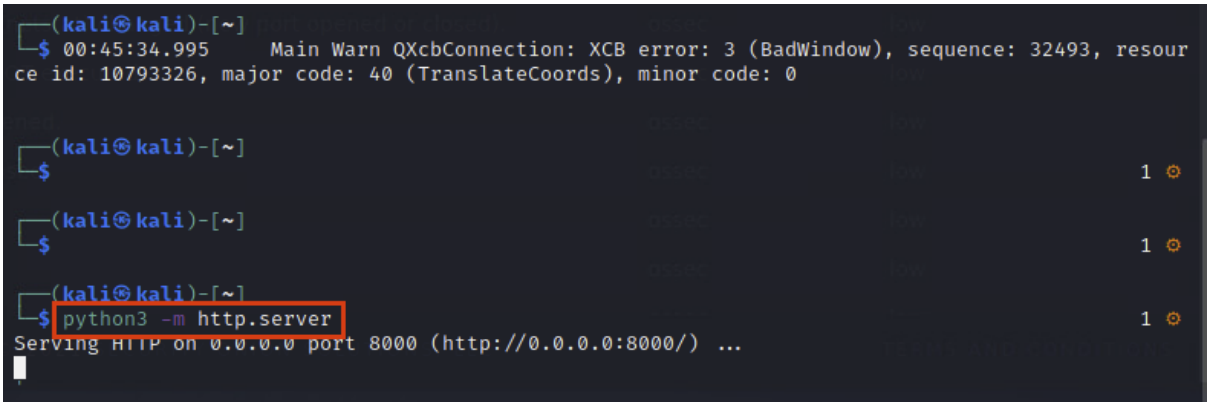

13. Leave the *Wireshark* window open and proceed to the next section.

## 1.3 Import the Traffic Capture

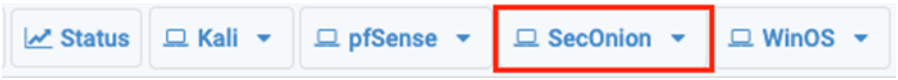
In this section, you will import the pcap file to the *Security Onion* for further analysis.

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.

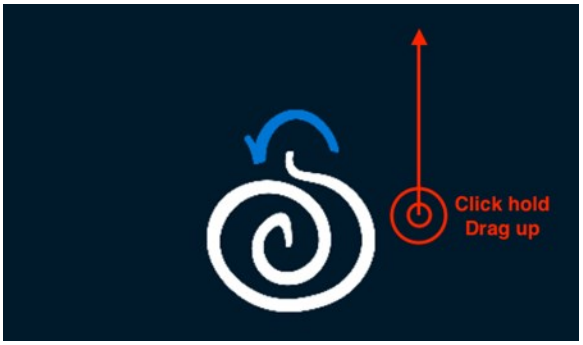
```
kali@kali$ python3 -m http.server
```




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

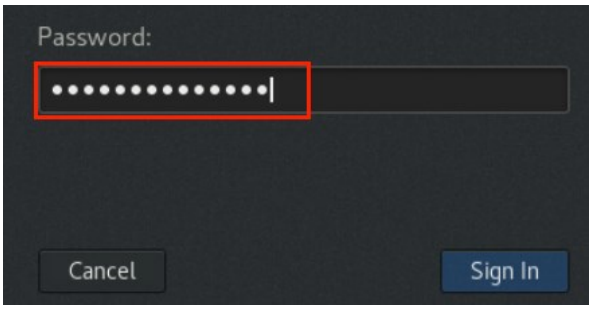



3. Then click and drag up to unlock the screen for a login prompt.

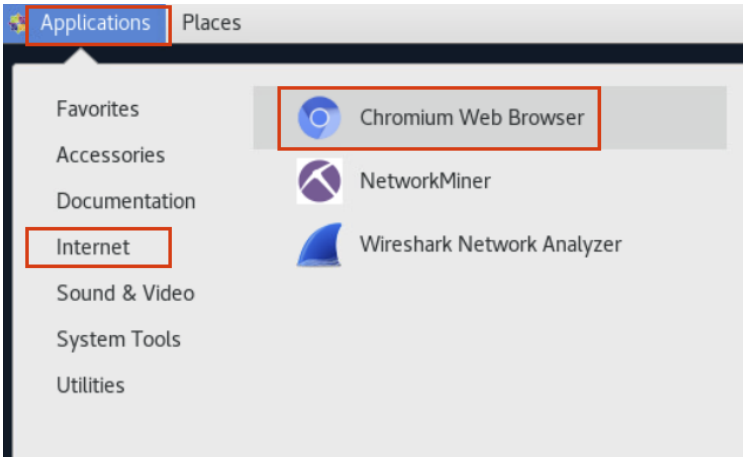


4. Type `sysadmin` as the username and `NDGlabpass123!` for the password.

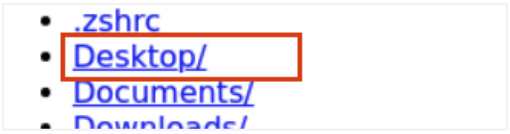




5. Once logged in, click **Applications > Internet > Chromium Web Browser** to start the browser.




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

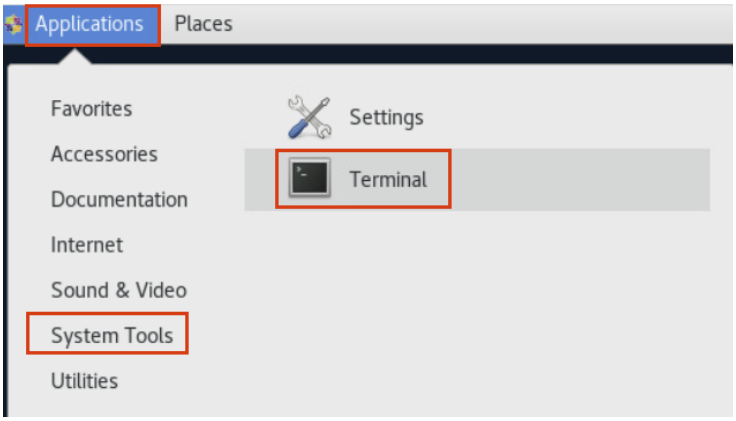
7. In the opened page, find and click on **Desktop**, then click on **scan.pcap** to download the file.



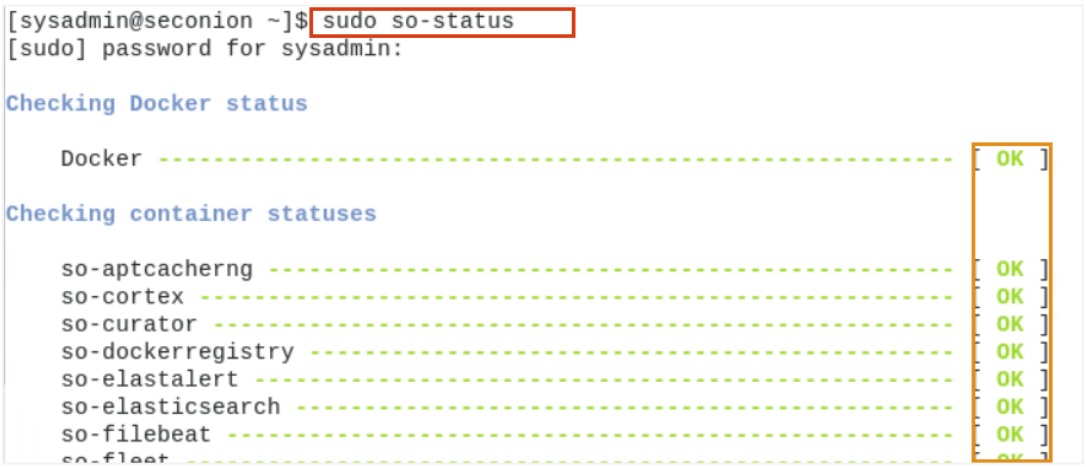


8. Once the file is downloaded (it takes about 5 seconds), close all the browser windows. If it prompts saying a download is in progress, do not close the window. Wait a little bit longer and try closing it again.

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*.



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 trip
le-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%20grou
pby%20-bar%20event.module%20%7C%20groupby%20event.dataset%20%7C%20groupby%20event.module%20%7C%2
0groupby%20event.category%20%7C%20groupby%20observer.name%20%7C%20groupby%20source.ip%20%7C%20gr
oupby%20destination.ip%20%7C%20groupby%20destination.port&t=2024%2F01%2F26%2000%3A00%3A00%20AM%2
0-%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.
```

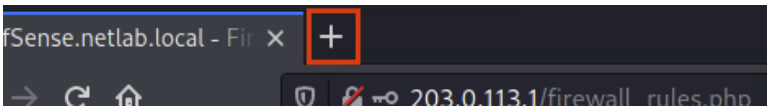
12. Leave the *Terminal* window open and proceed to the next section.

## 2 Analyze the Data and File a Case

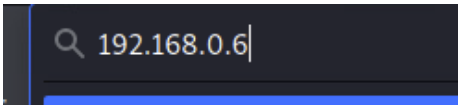
In this section, you will analyze the captured data and then create and solve the case.

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

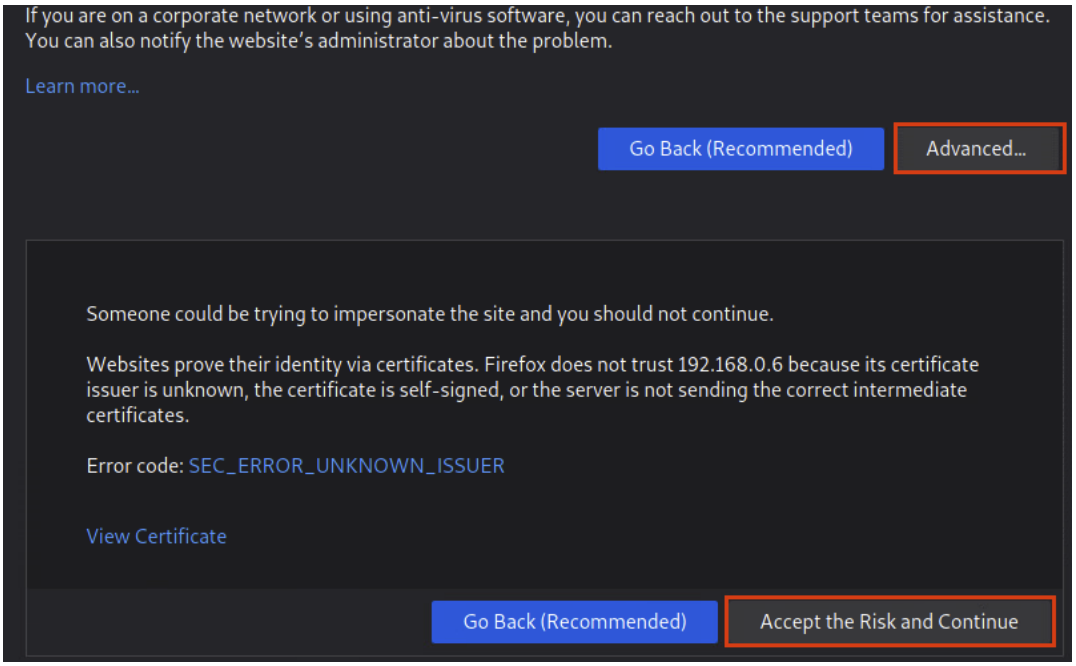

2. Switch back to the browser window, click the **+** to start a new tab.




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

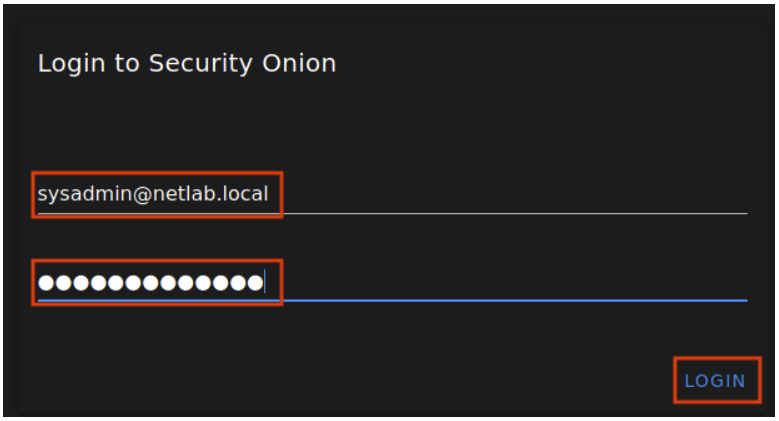



4. If the warning page shows up, click the **Advanced**… button. Then, scroll down and click **Accept the Risk and Continue**.

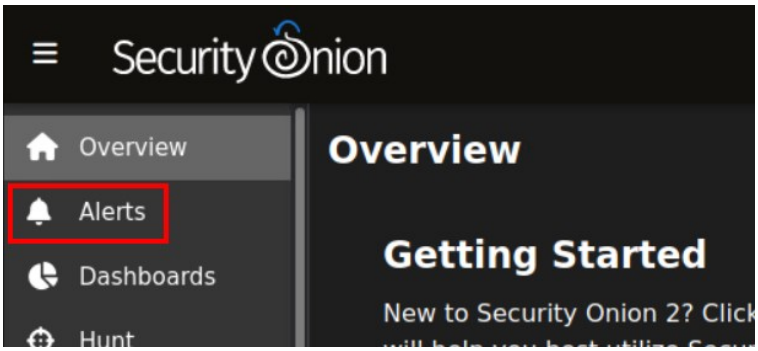


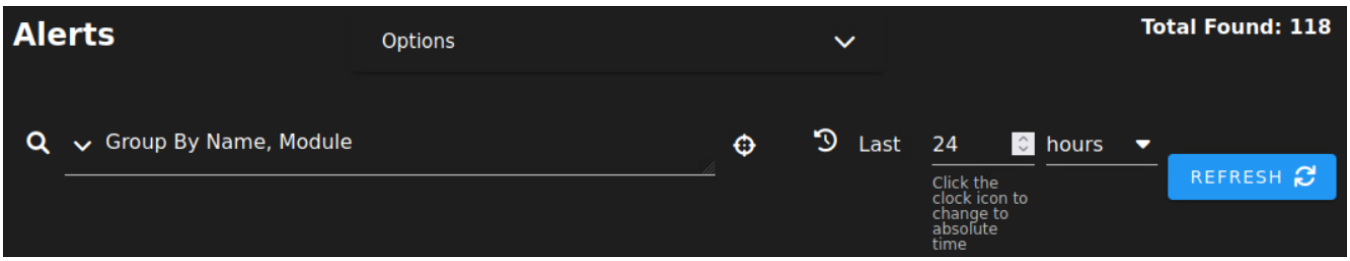
5. On the *Login* page, enter the *username* as **`sysadmin@netlab.local`** and the password as **NDGlabpass123!**. Click **LOGIN.**



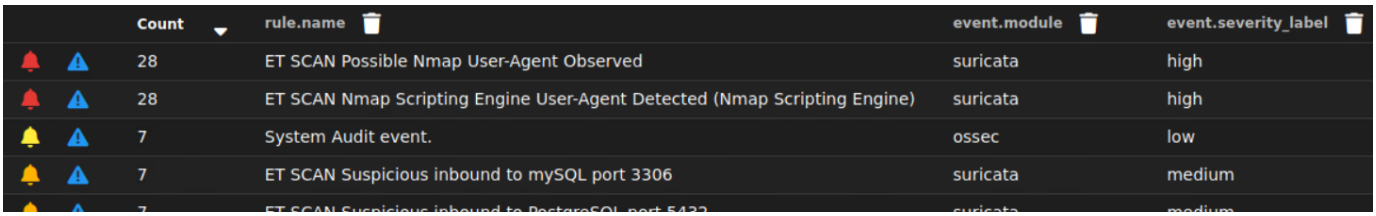

6. On the *Overview* page, click the menu button at the top-left corner. Then, click on **Alerts**.




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 |

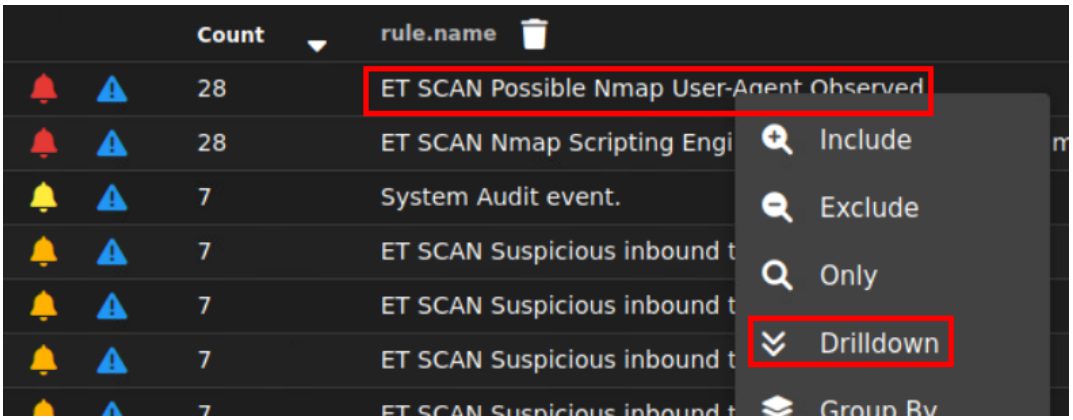
9. Leave the SecurityOnion window open and proceed to the next section.

# 3 Add a Case, Investigate, and Close the Case

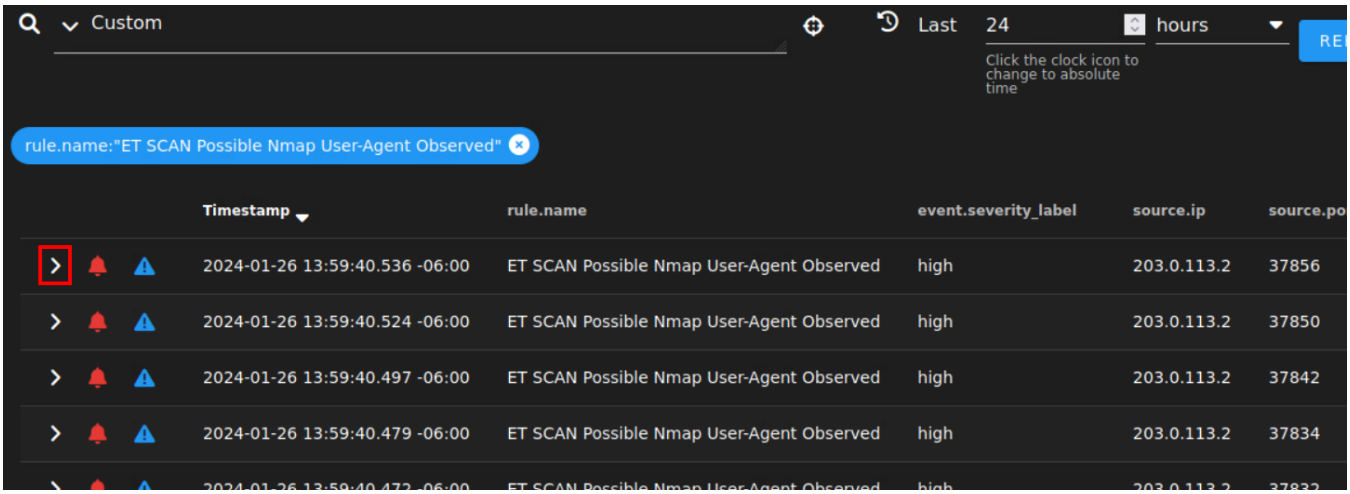
In this section, you will add a case, perform an investigation, and then close the case.

## 3.1 Escalate an Alert to Add a Case

1. 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.

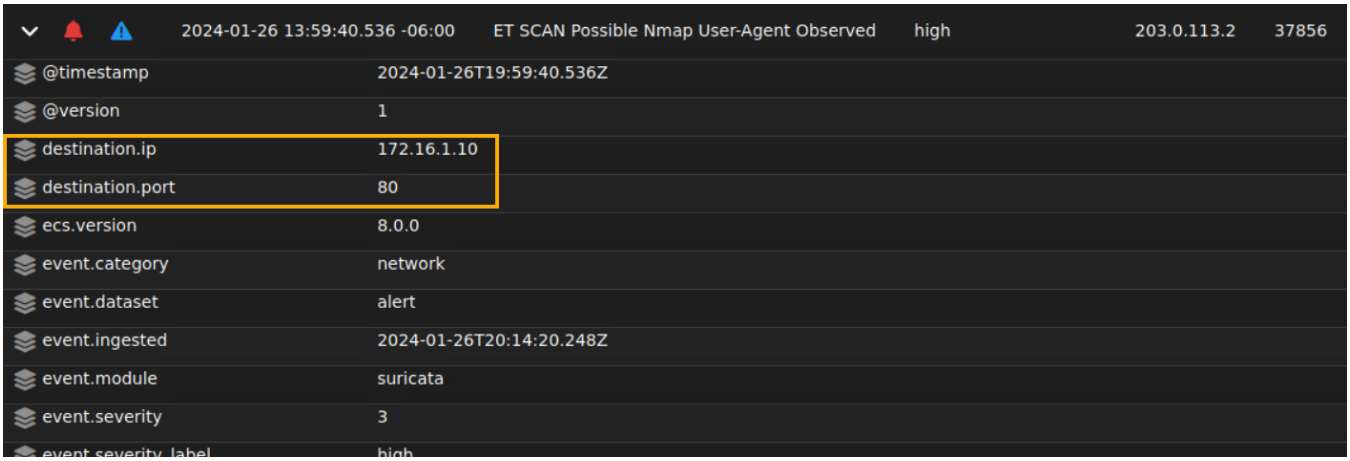



2. The view will be changed, and you should see something like below, click the **arrow** in front of the first entry.

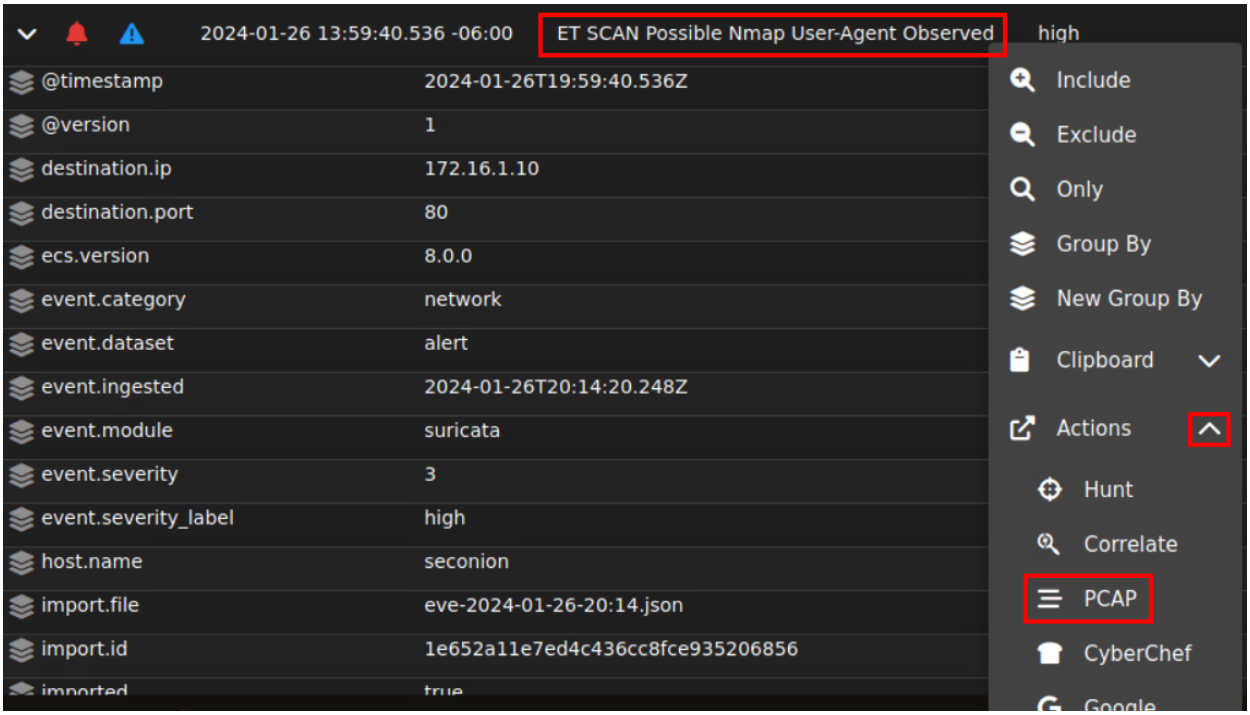


3. Detailed information about this alert will show up. Scroll down to learn more about it, e.g., *destination.ip*, *destination.port*, *source.ip*, *source.port*, *network.data.decoded*, *rule.rule, etc.*

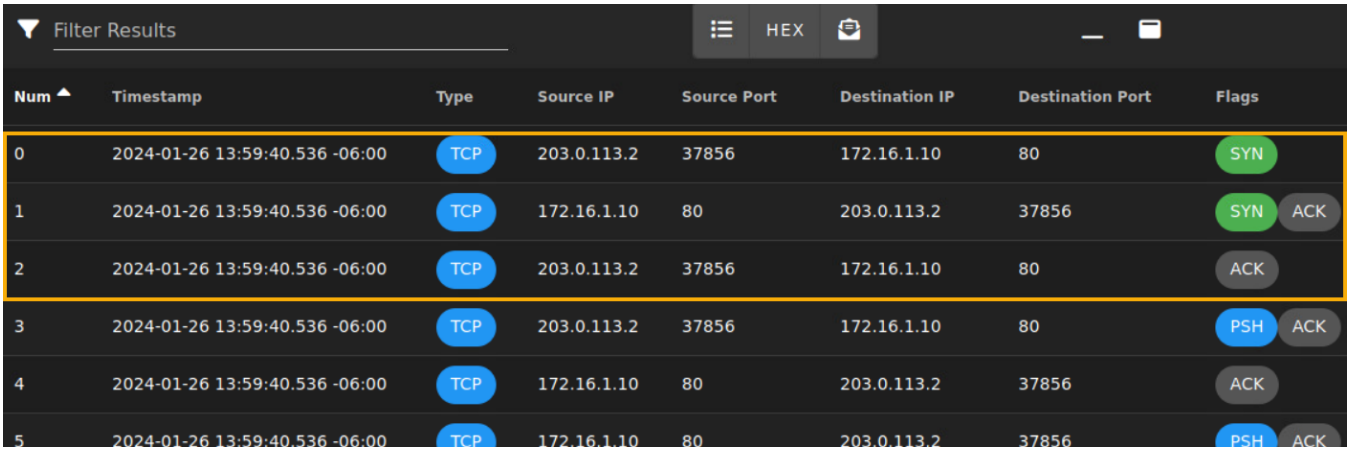



4. Once again, left-click on the **ET SCAN Possible Nmap User-Agent Observed** rule name, then select **Actions**, then **PCAP** to show the captured packet for this alert.

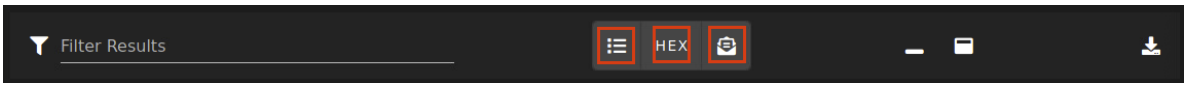


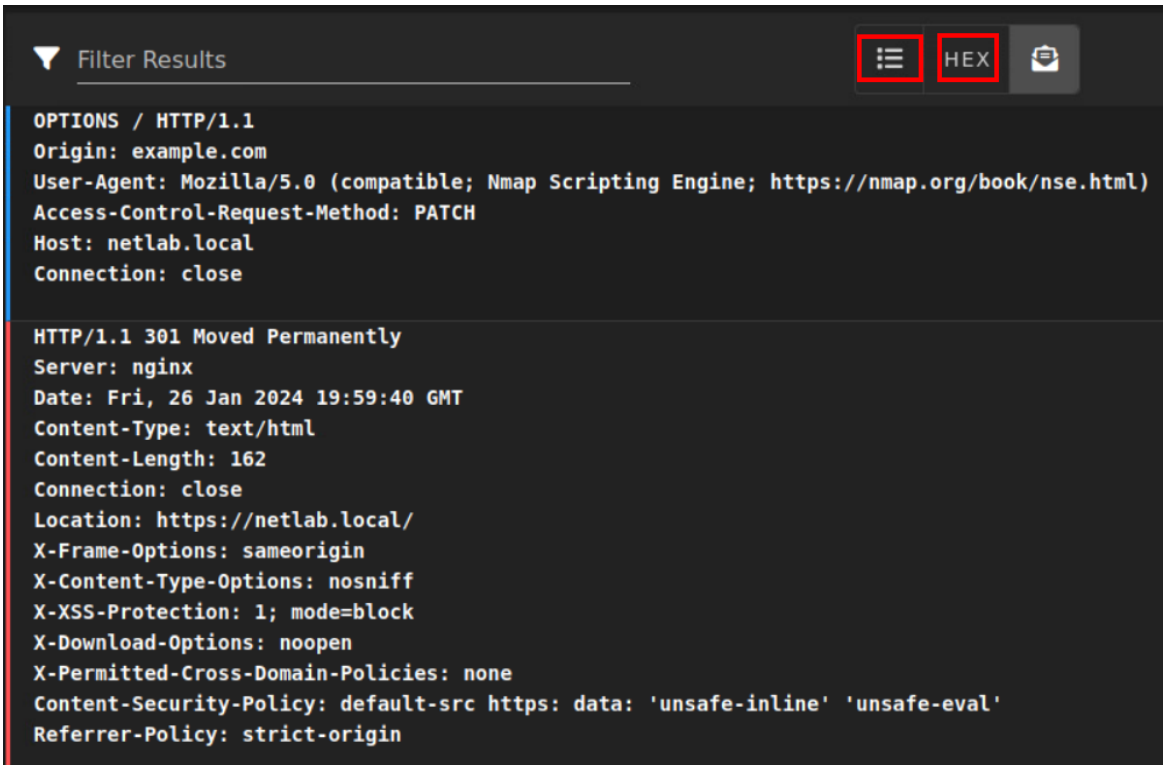
5. We will be brought to the *PCAP* view, which shows the stream of this traffic, starting from the three-way handshake.




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

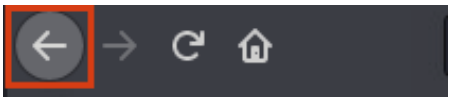



7. If you are familiar with the *Follow Stream* on *Wireshark*, you may find this view also exists in the *Security Onion PCAP* module (click the first list toggle, then the HEX toggle).

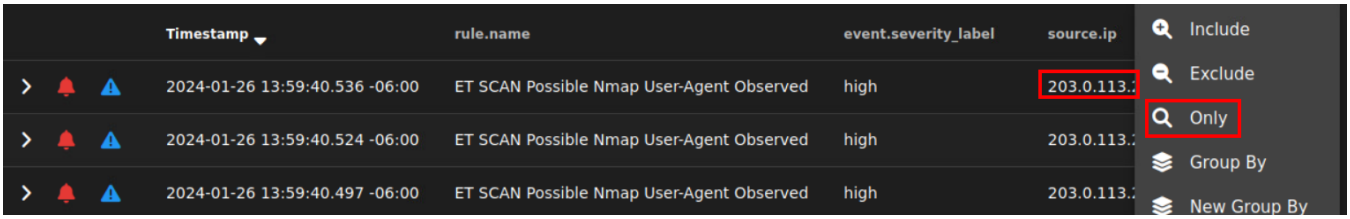


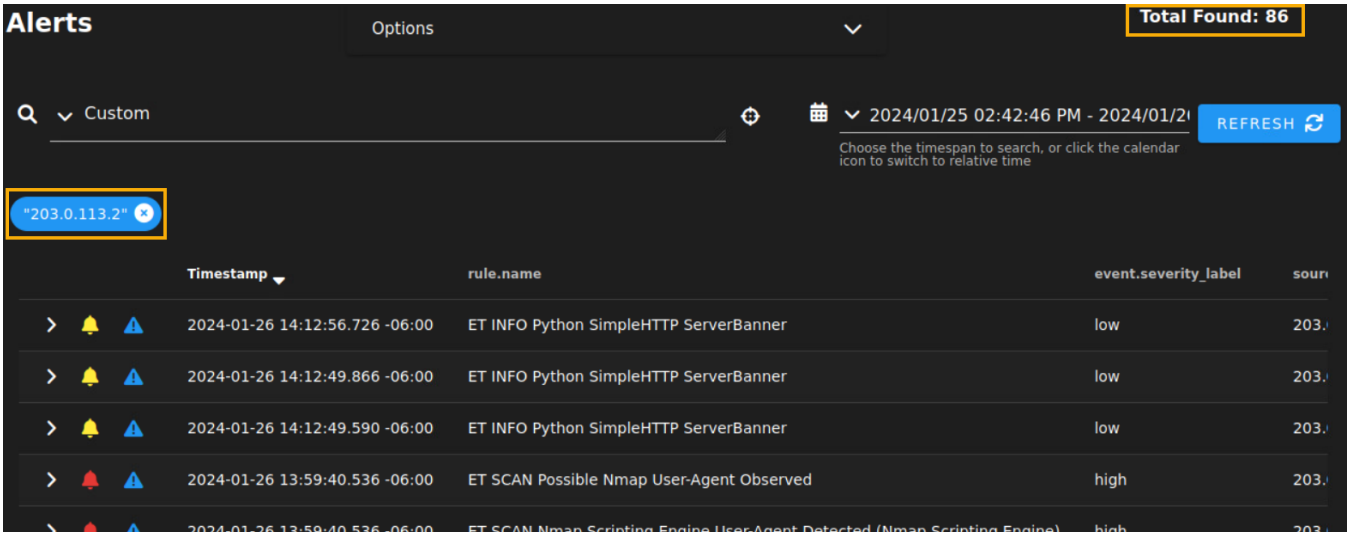
8. Next, let's go back by clicking the **Back** button in the browser.



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.

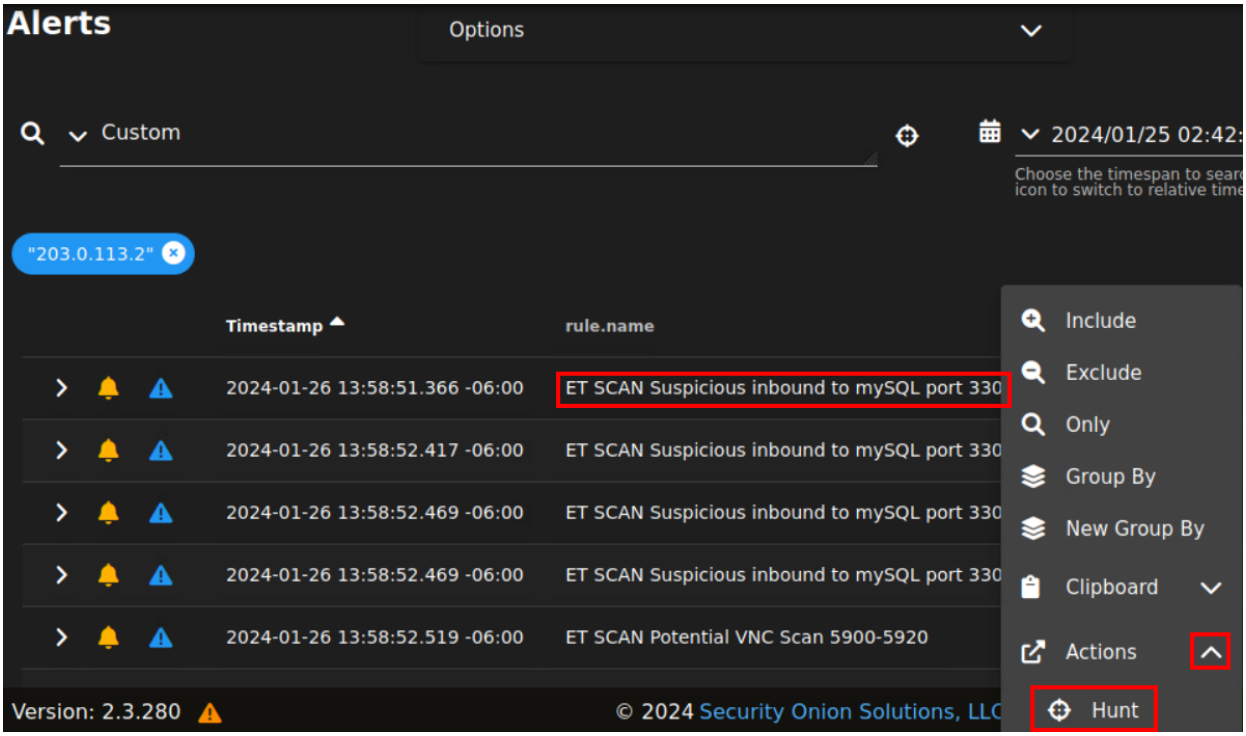



10. Now, we can see that *86* of the alerts are filtered, and they were all originated from the *Kali* VM. Feel free to scroll up and down to see the severity levels of those alerts.

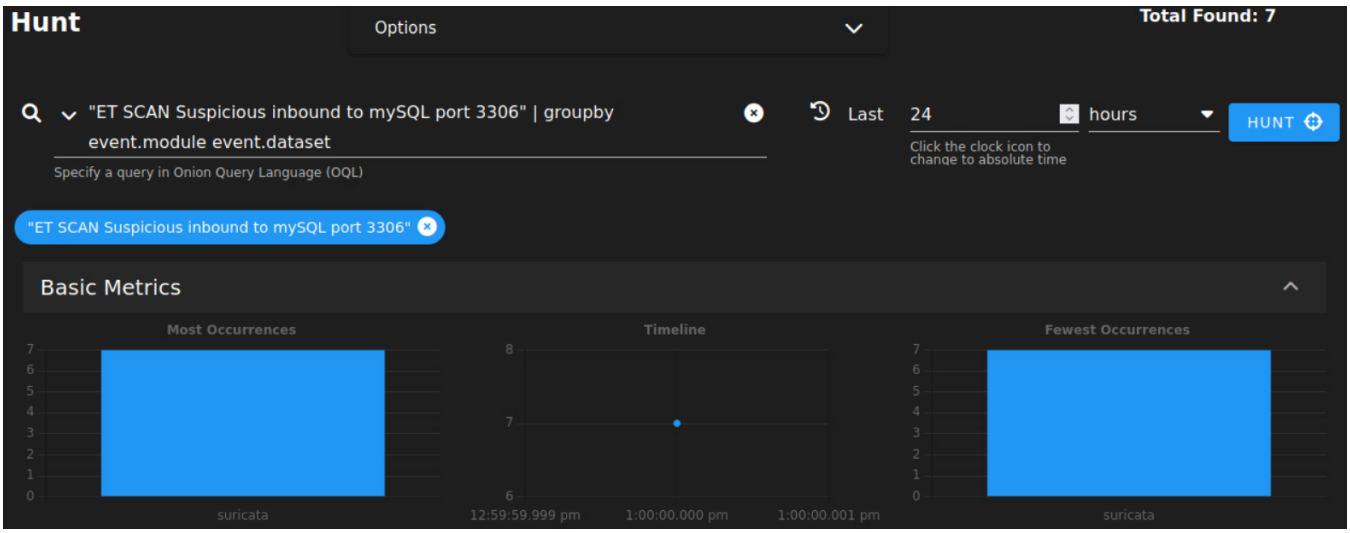


11. Click on the **Timestamp** column header to list the results in chronological order. Now we see that the first alert is a medium severity with suspicious inbound activity. Once again, let's left-click on the name and select **Actions**, then select **Hunt.** If you don't see a brute force rule name,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

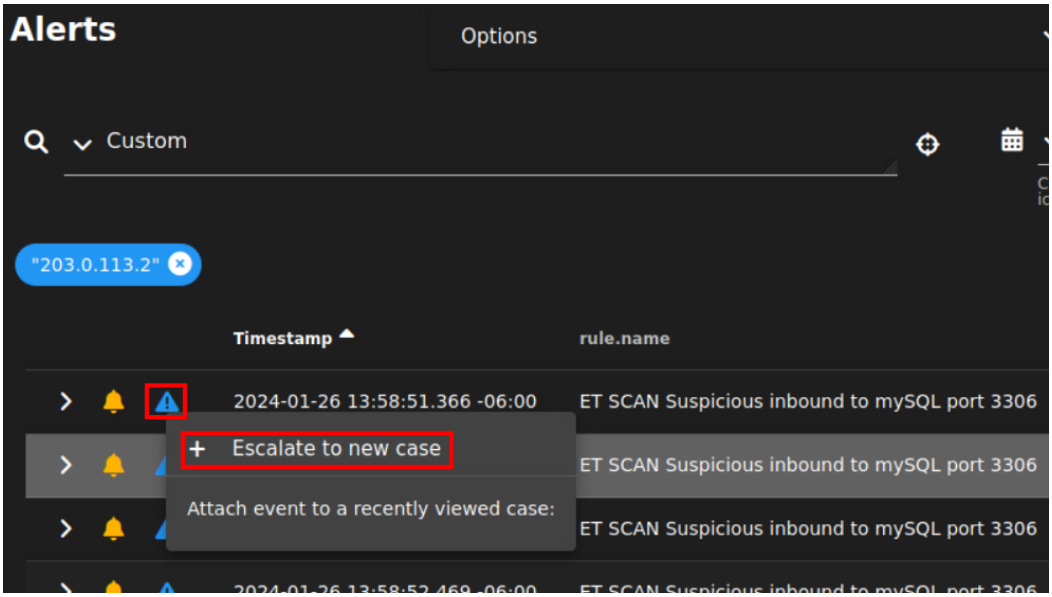



12. You will see the *Hunt* tool page as shown below. On this page, it will bring more details about this alert most of the time. *Hunt* is used to find similar events, track down malicious files, and observe malicious behaviors. We will not go into details about how to use *Hunt* in this lab.

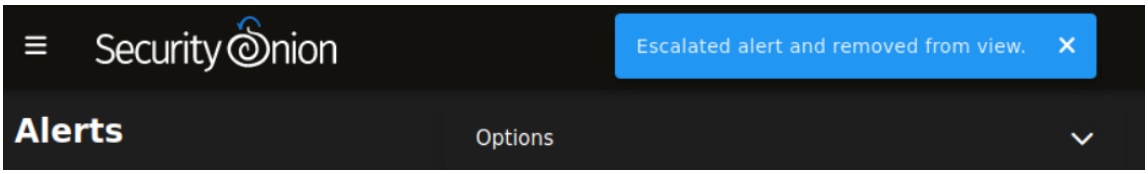


13. Click the browser **Back** button again. Let's say that we need to escalate and create a case for the suspicious inbound activity and *nmap* scan alert. If you don't see the following selections, you may select another alert of your choice to proceed to the next steps. Click on the first **blue triangle**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



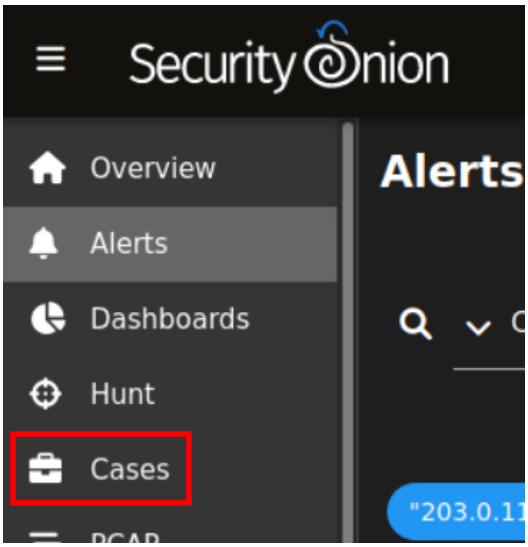

14. Once added, it's going to prompt and say *Escalated alert and removed from view*.



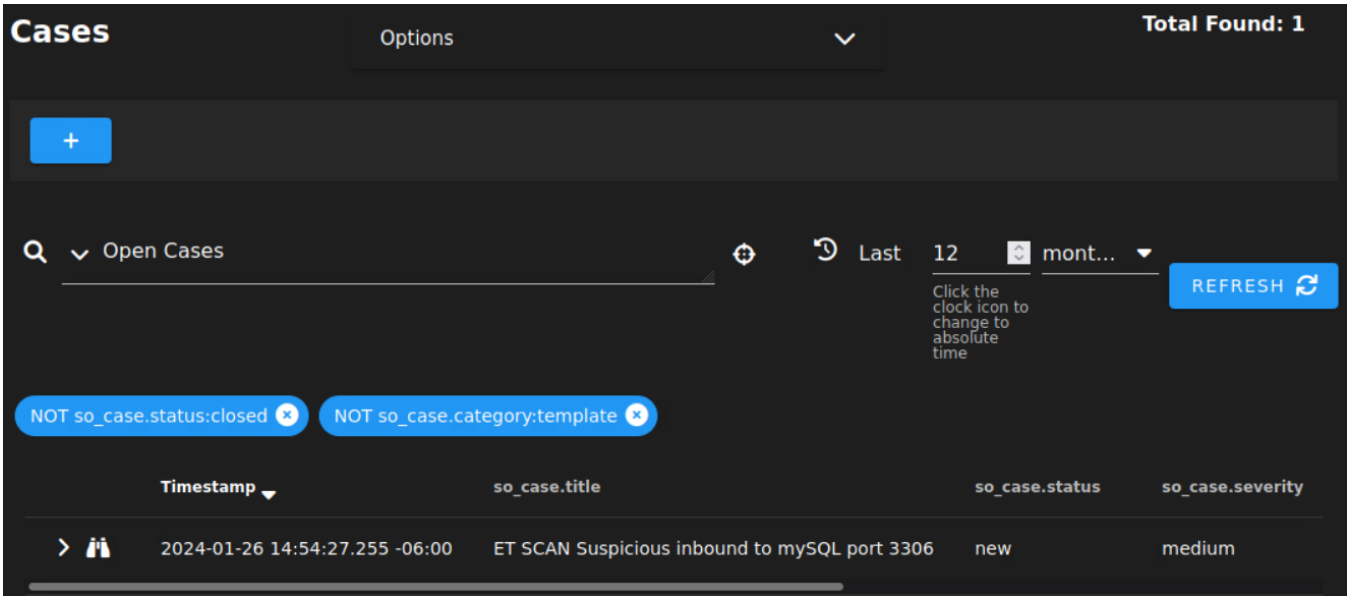

15. Leave the window open to continue with the next task.

## 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.

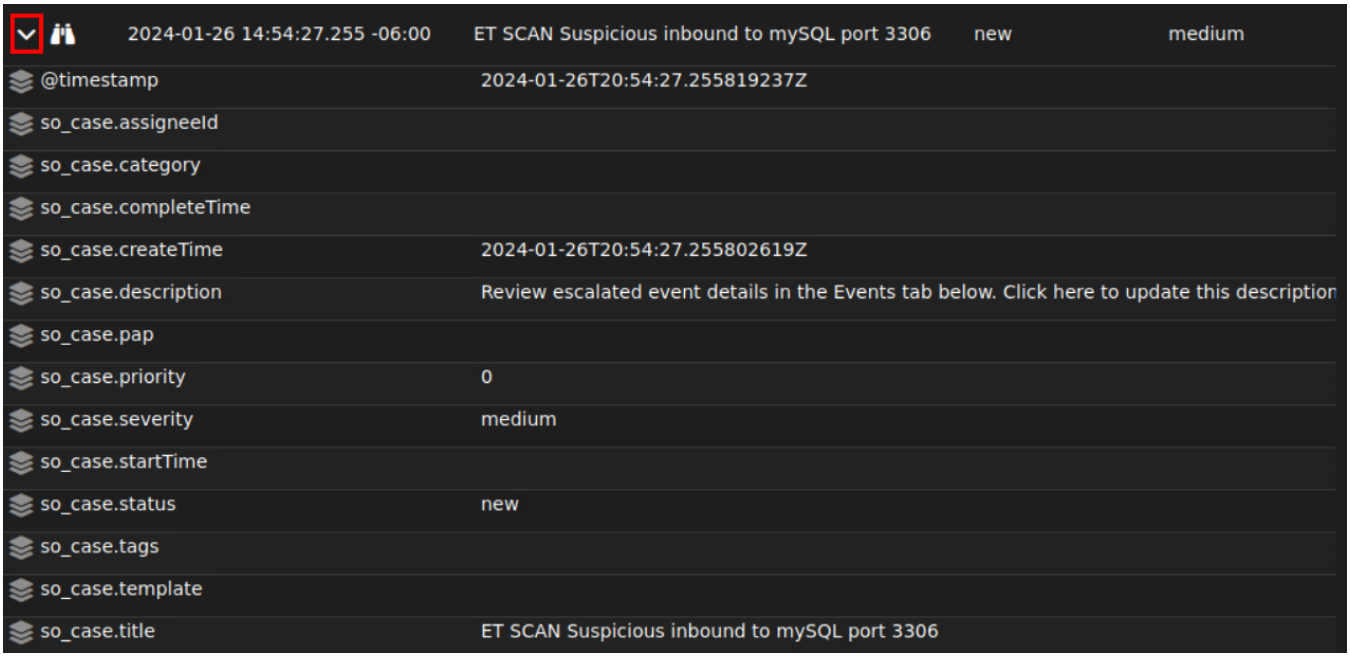



2. You should see the case list with the newly added cases.

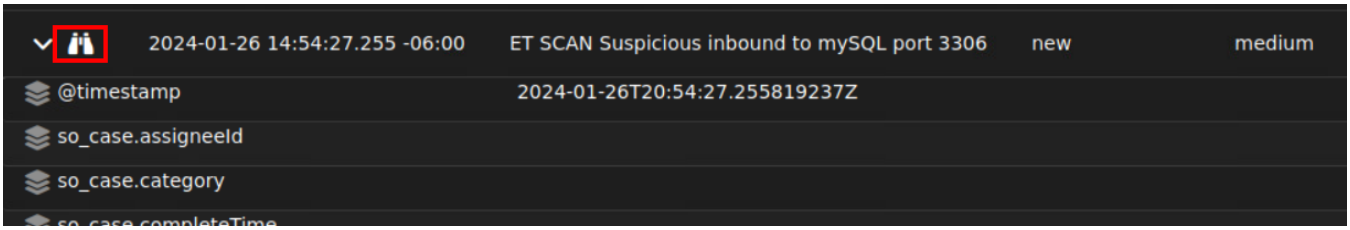


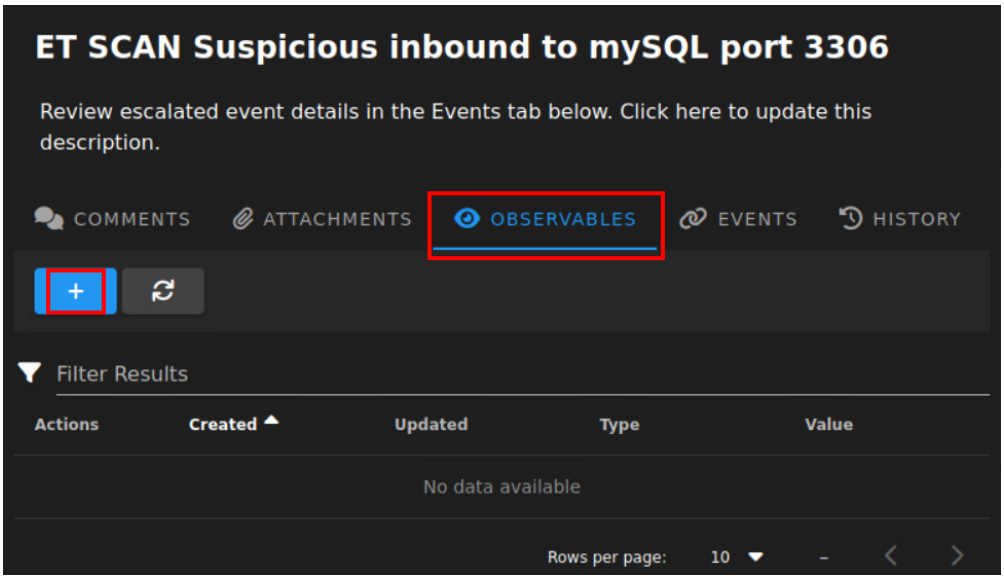
3. Click on the right arrow next to the first case entry to view additional details related to the case. Review the information.




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

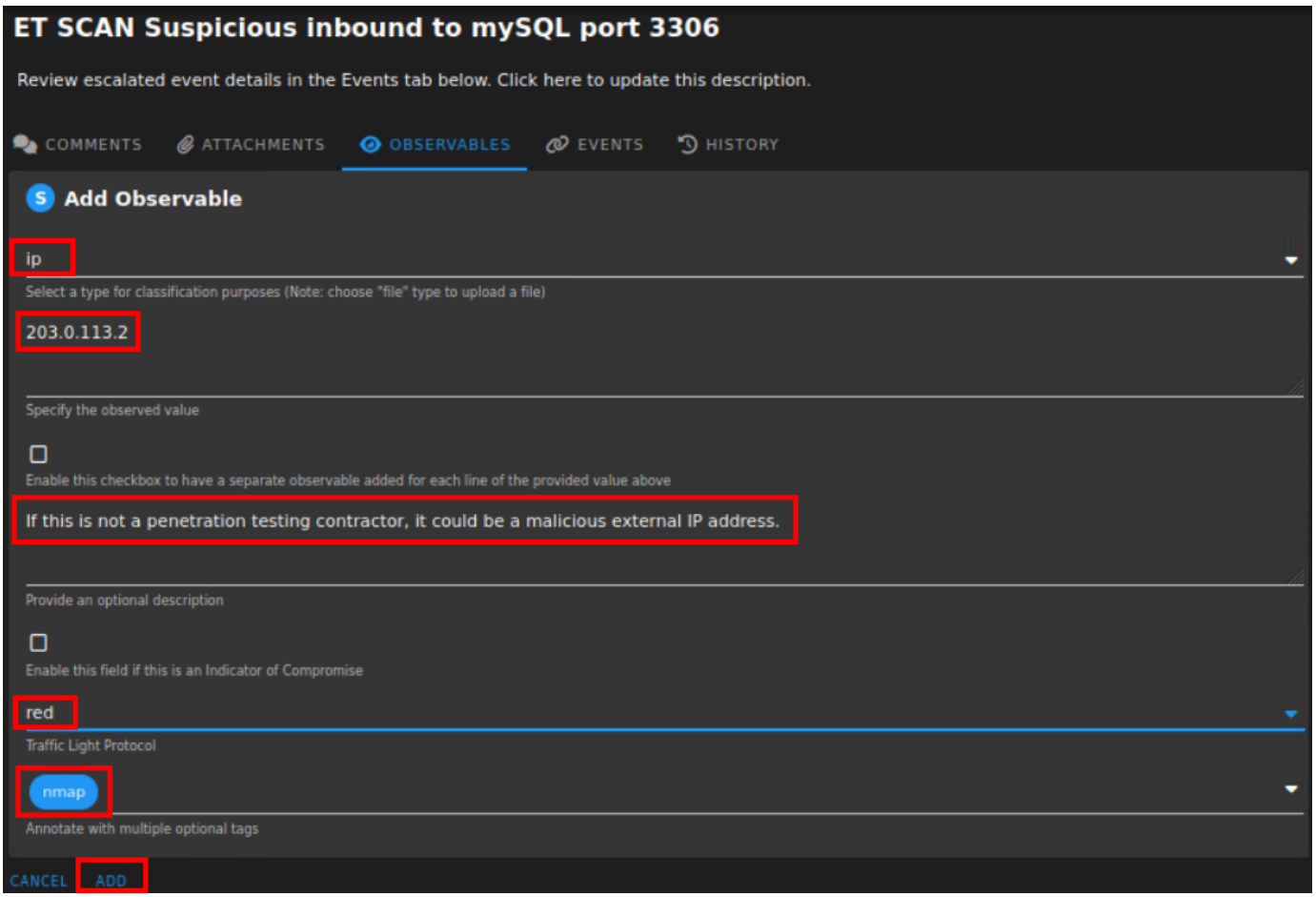



5. We are going to add some extra notes. Click the **Observables** button, then click **Add a new observable to this case**.



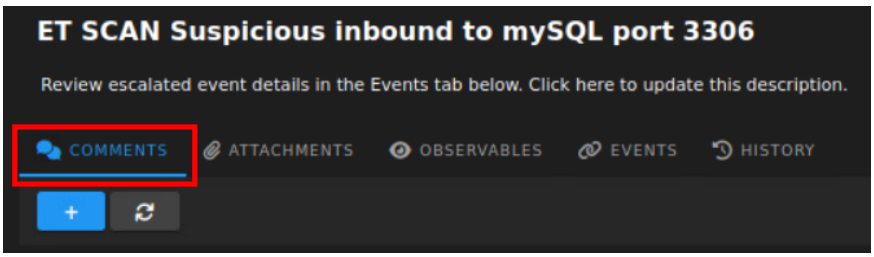

  

6. In the new window, type the following information, then click the **Add** button.
   a. *Type*: `ip`
   b. *Value*: `203.0.113.2`
   c. *Description*: `If this is not a penetration testing contractor, it could be a malicious external IP address.`
   d. *Traffic Light Protocol*: **red**
   e. *Tags*: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



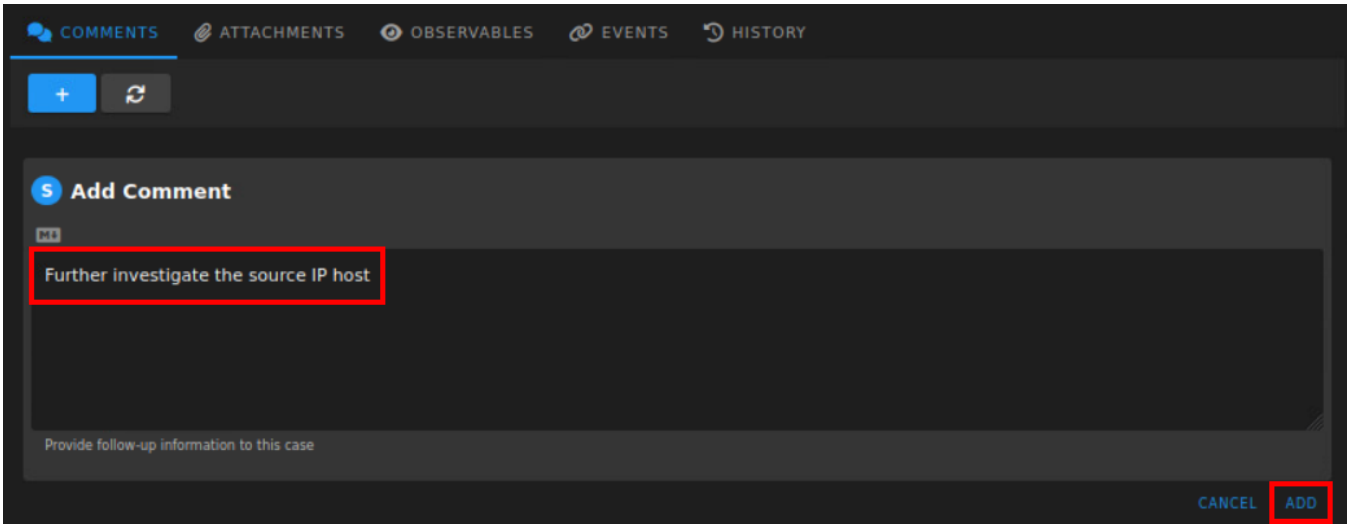

An observable is an extra piece of information we can add to aid the security team for further investigation.

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

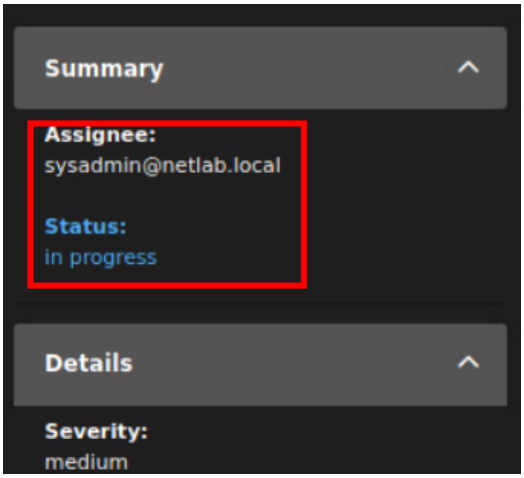


8. Type `Further investigate the source IP host`, click the **Add** button to confirm.




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

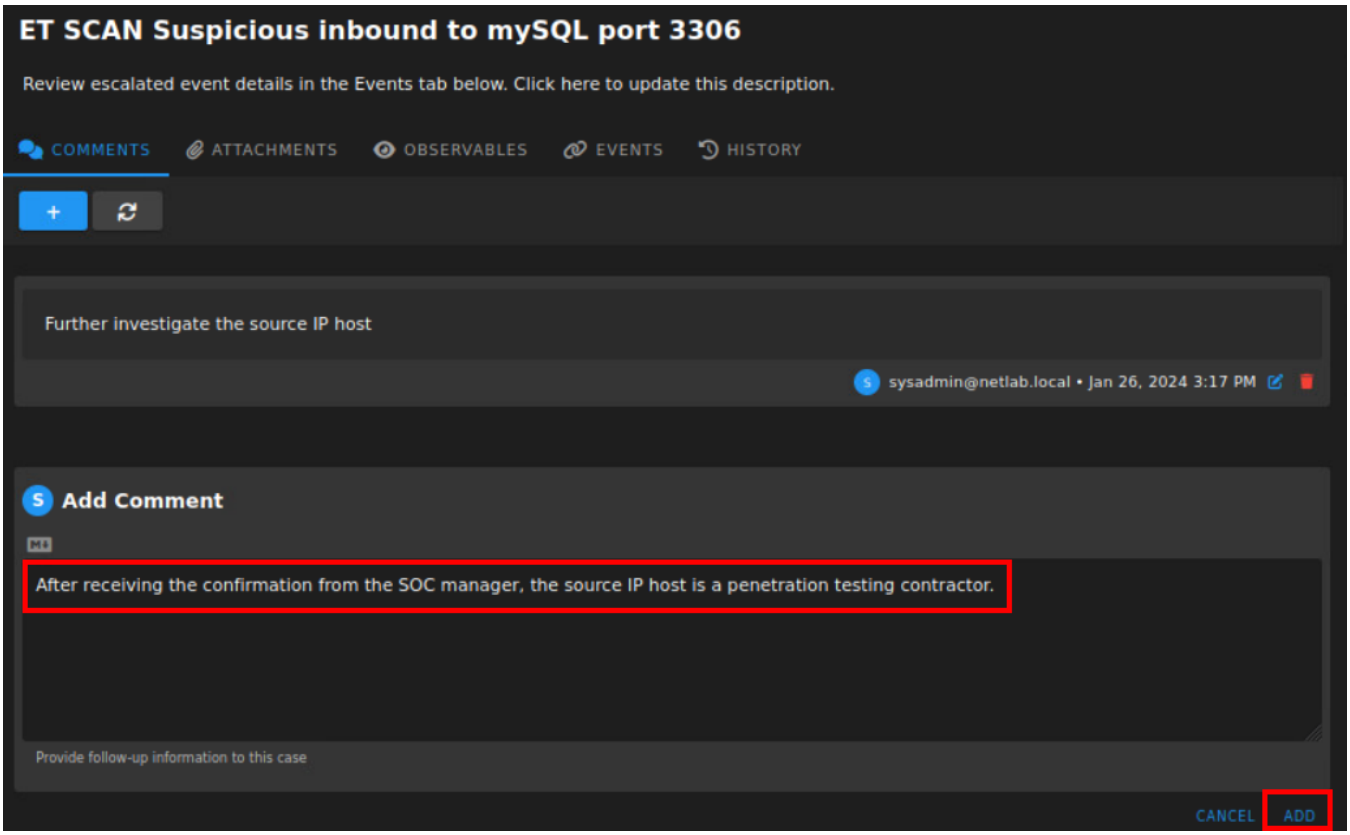



10. Leave the window open to continue on with the next task.

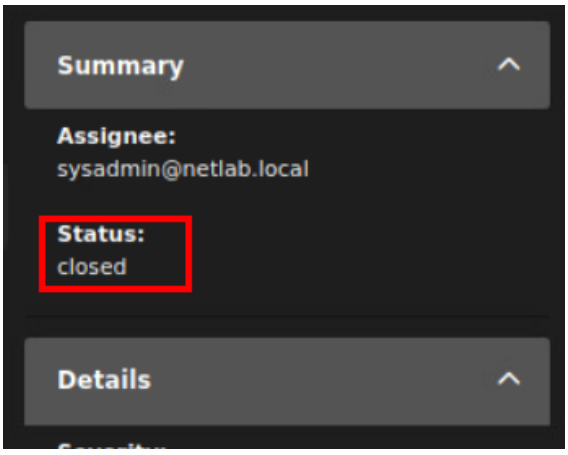
## 3.3 Finish All Tasks and Close a Case

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.




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




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