SECURITY+ V4 LAB SERIES

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

Document Version: 2022-04-29

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

Contents

Introduction

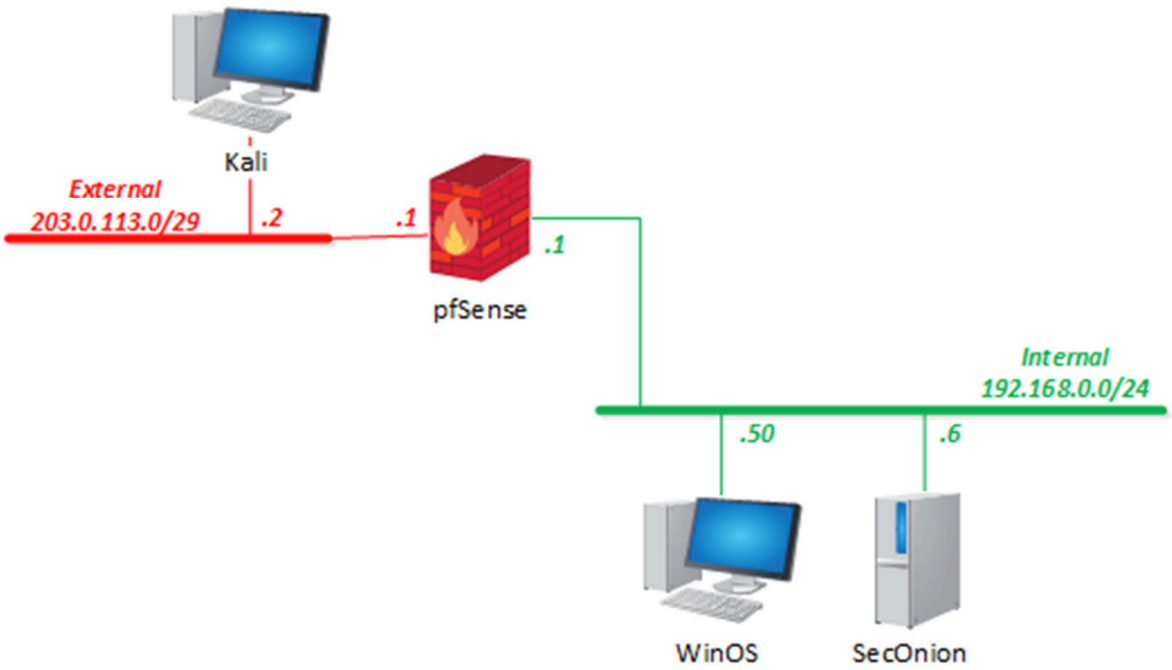
In this lab, you will be conducting network and host monitoring using various administrative tools.

Objective

In this lab, you will perform the following tasks:

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

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!
WinOS	192.168.0.50	Administrator	NDGlabpass123!

1 Load pcap File to SecurityOnion for Analysis

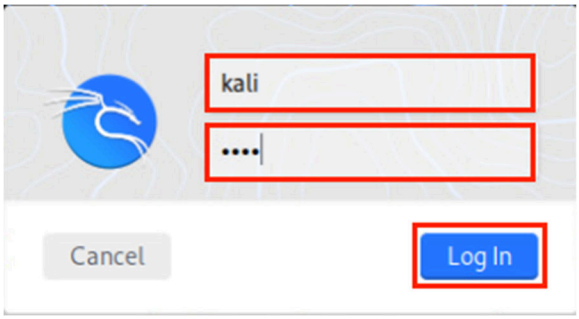
In this lab, we are using the standalone installation of SecurityOnion for all of the tasks. In a production line, you could use either a standalone or distributed installation. Because live capture will be covered in Lab 22, this lab will not use the live capture function. Instead, you will explore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

1.1 Disable Firewall

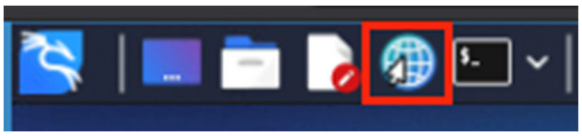
In this section, you will disable the Firewall to prepare for the traffic capture.

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

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

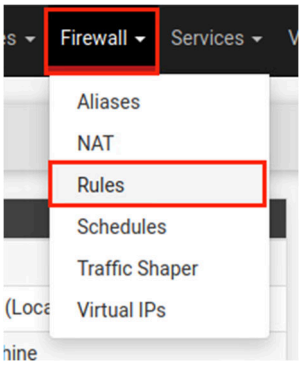


3. Click to open a browser window.

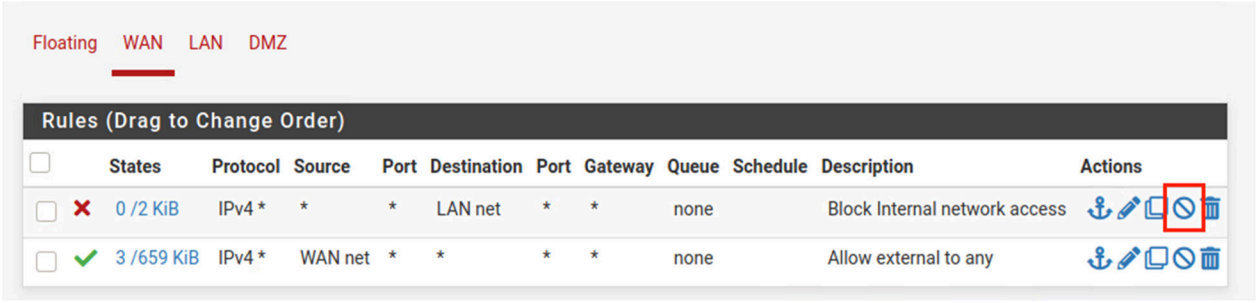


4. In the address bar, type `203.0.113.1` to go to the *pfSense* firewall management login page. Log in as username `admin`, password `NDGlabpass123!` and then click the **SIGN IN** button.

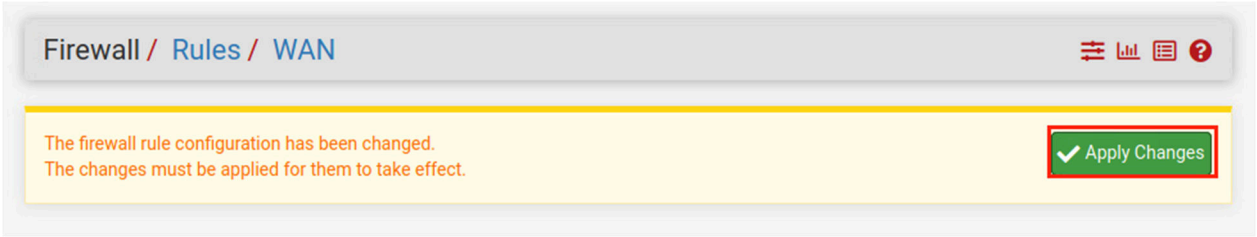
5. Once logged in, you will see the *Status/Dashboard* page; click the **Firewall** menu and select **Rules**.



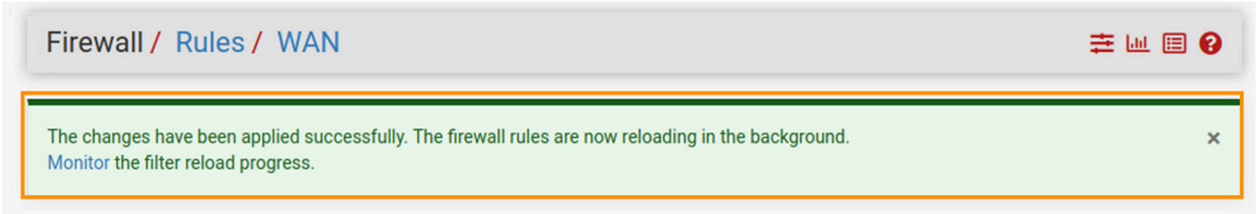
6. Click the **Disable** button to disable the **Block Internal network access** rule.



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.



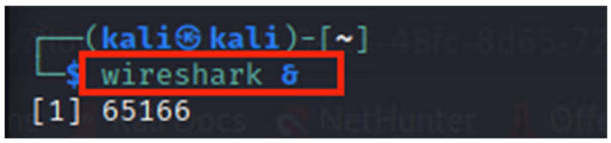
1.2 Capture the Traffic for Analysis

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

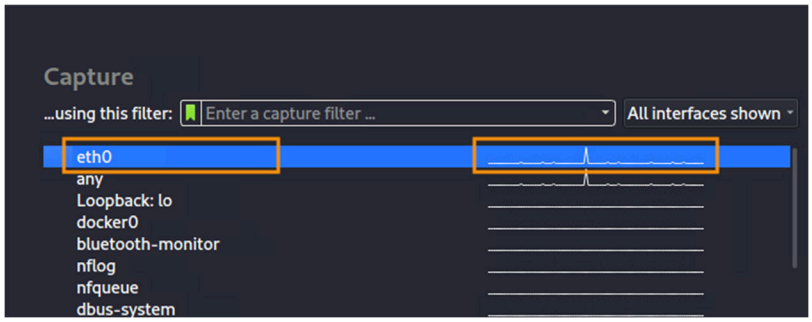
1. In the *Kali* VM, click **Terminal** to start a *Terminal* window.

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

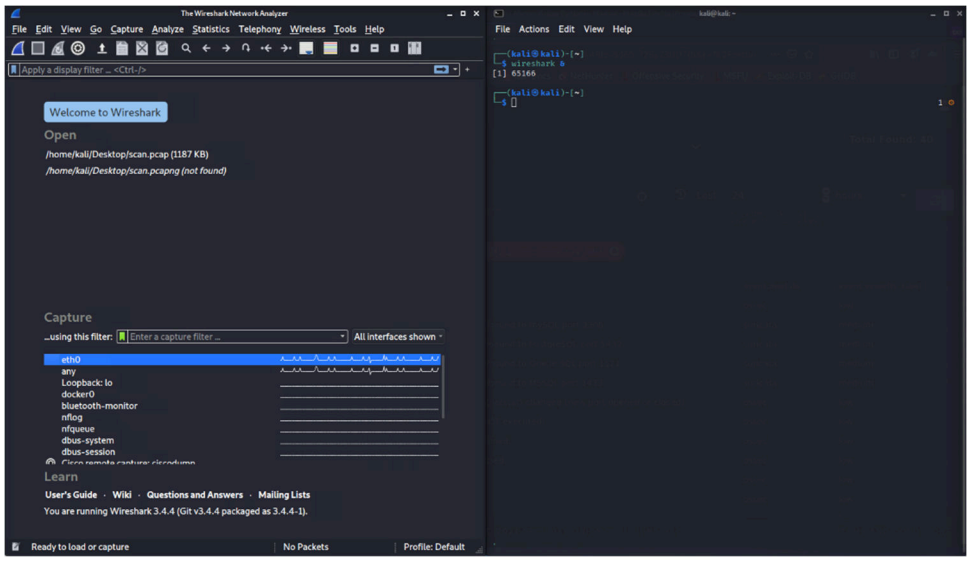
```
kali@kali$ wireshark &
```



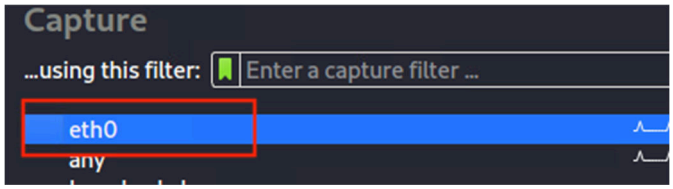
3. *Wireshark* should open, and on the *Welcome* page, you should see the wave line updating itself continuously on interface eth0.



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

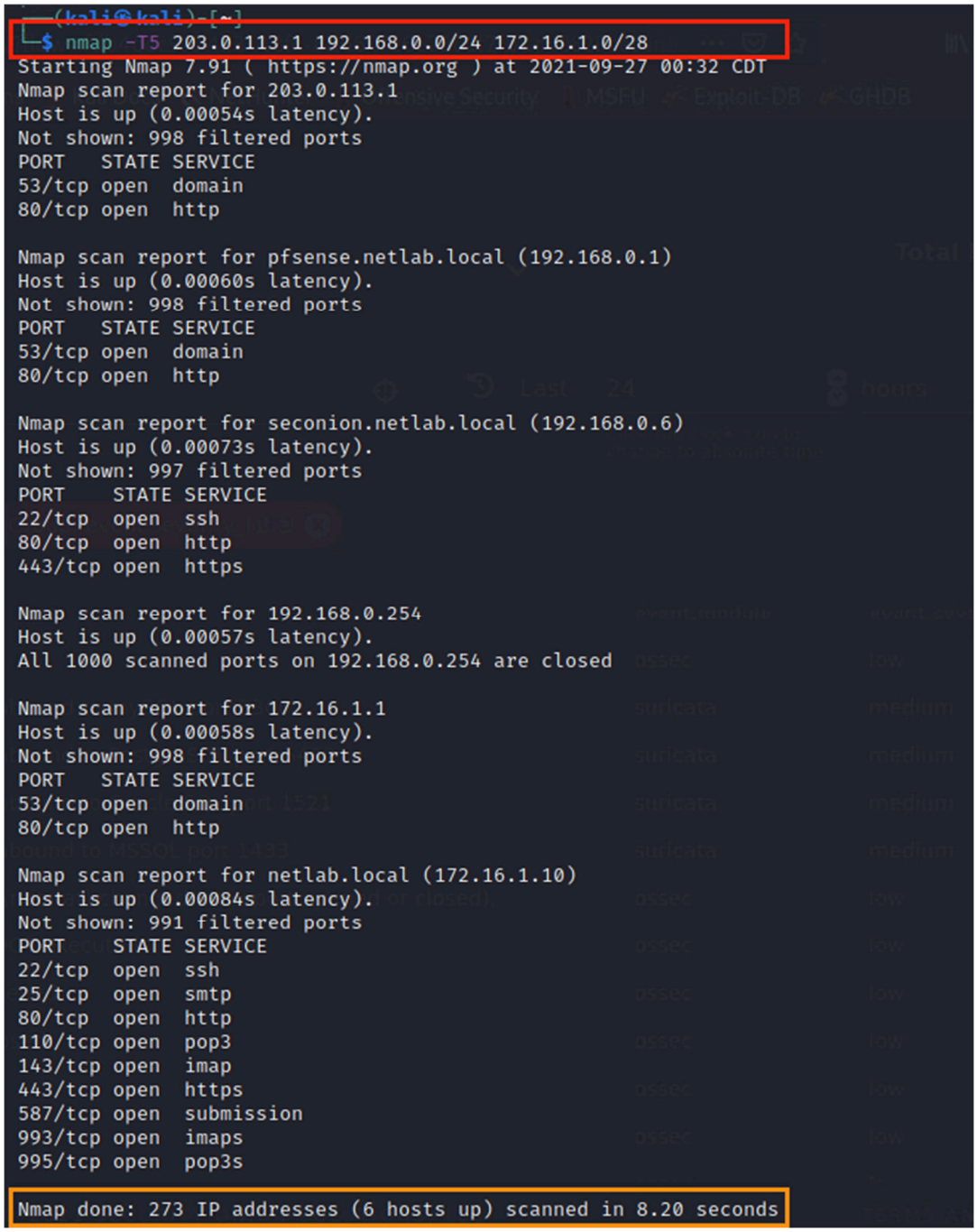


5. In the *Wireshark* window, double-click on **eth0** to start capturing traffic.



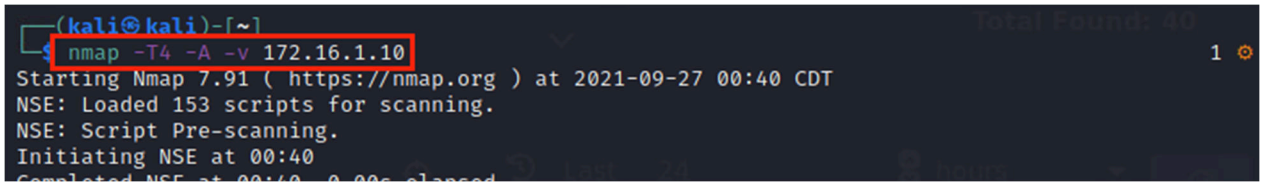
6. Keep the capture running and switch attention to the *Terminal* window. Type the following command to start an *nmap* scan.

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

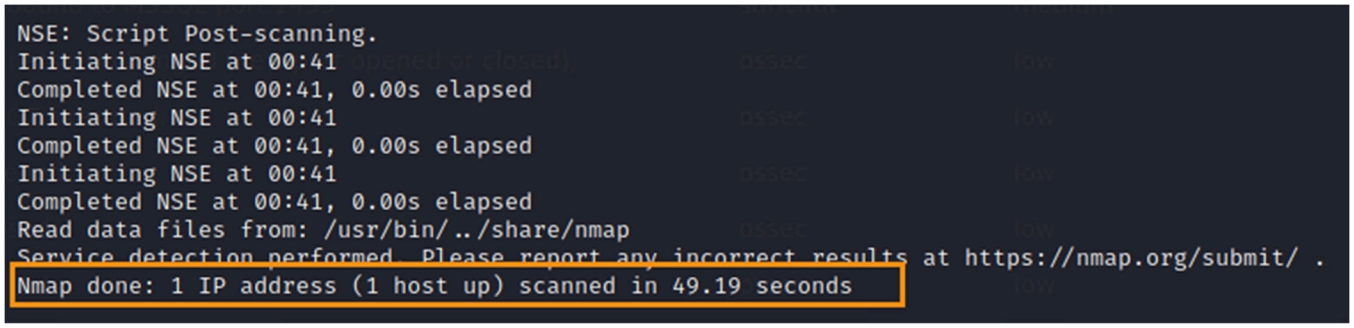


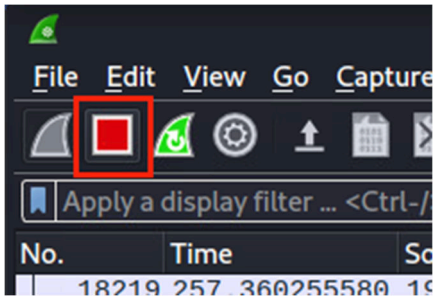
7. After the scan is finished, type the following command to target the 172.16.1.10 host to start an intensive scan. This may take 2-3 minutes to complete.

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

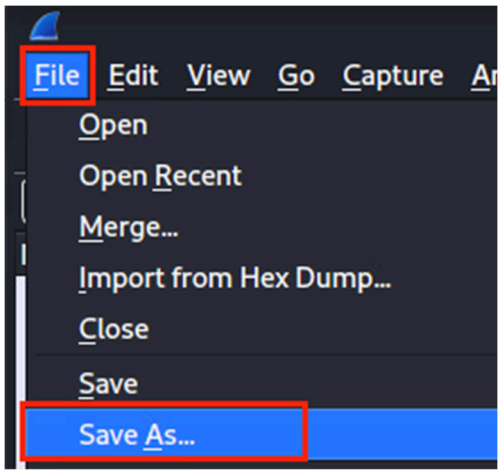


8. Once the scan is complete, it will say *Nmap done…* Stop the Wireshark capture by clicking the red square button.

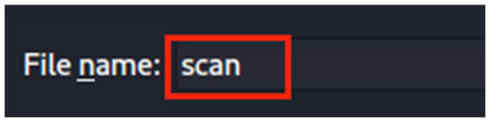




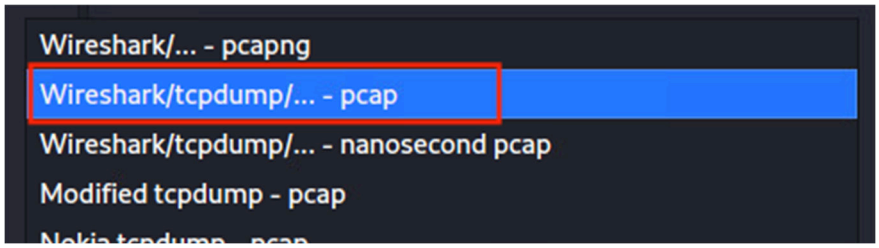
9. Click on **File**, then the **Save As…** option.



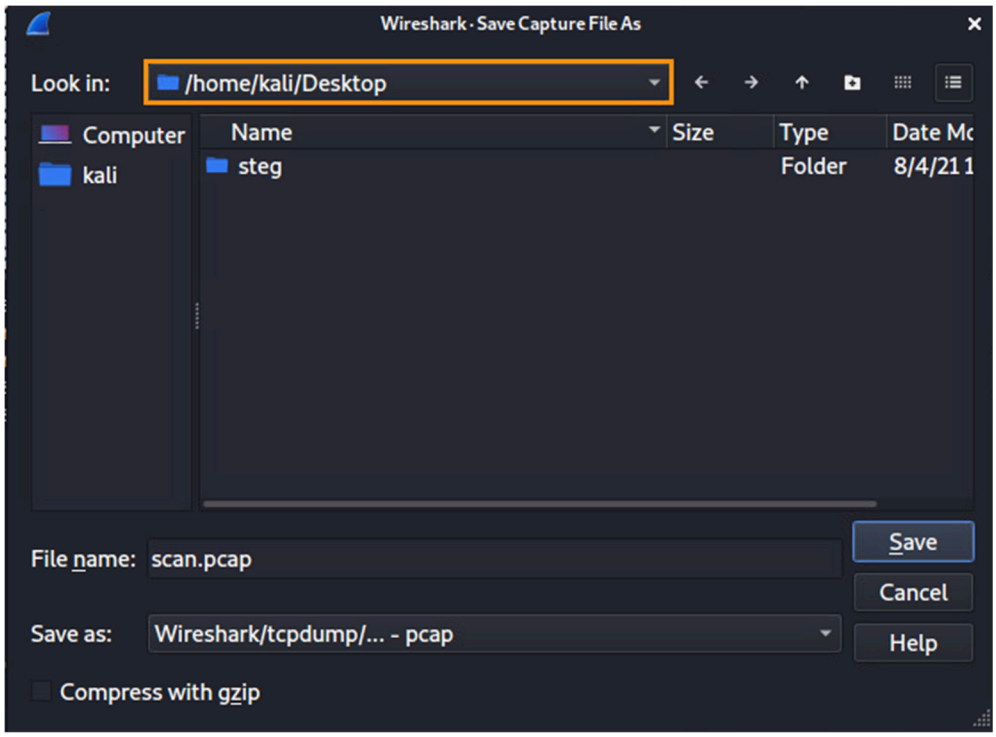
10. Type `scan` as the File name.



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.



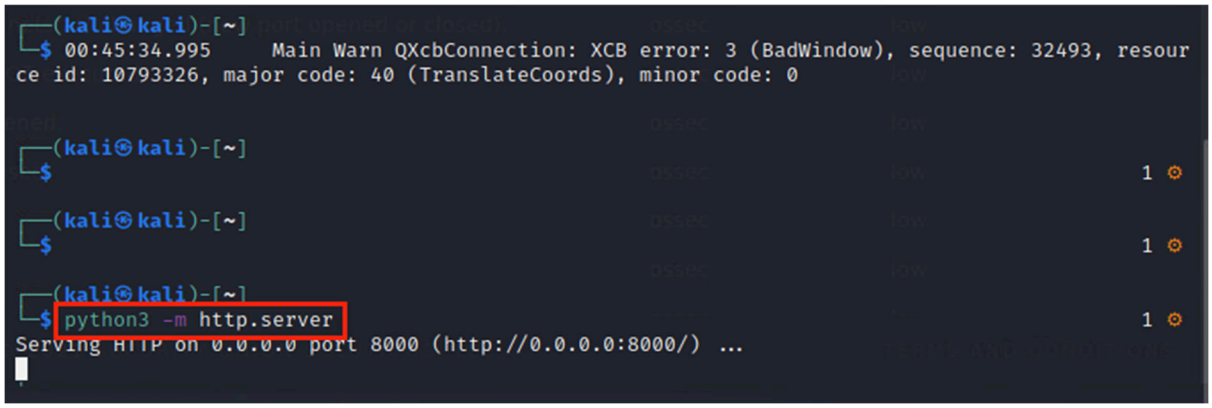
13. Leave the *Wireshark* window open and proceed to the next section.

1.3 Import the Traffic Capture

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

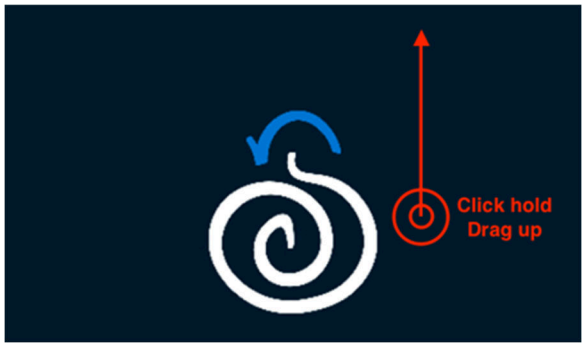
1. Switch back to the *Terminal* window. Press **Enter** a couple of times. Then, we will start a simple HTTP server by using the following command; the server will run on default port 8000.

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

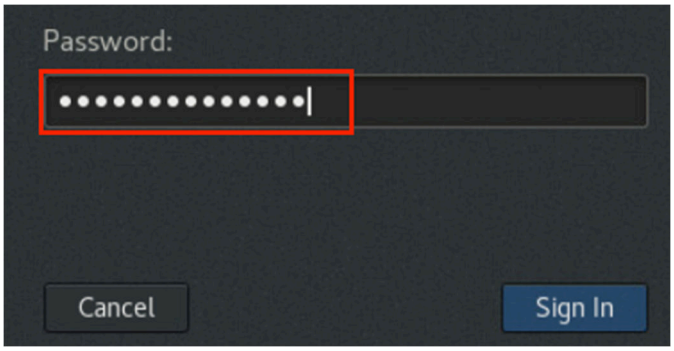


2. We will now log in to the *SecOnion* VM. Click on the **SecOnion** tab.

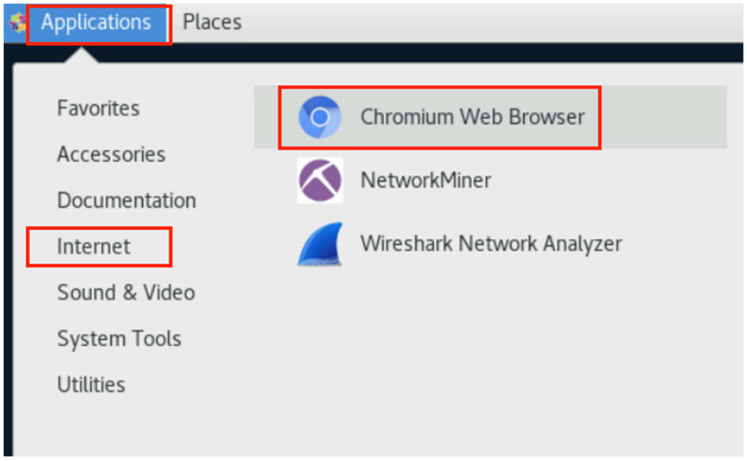
3. Then click and drag up to unlock the screen for a login prompt.



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.

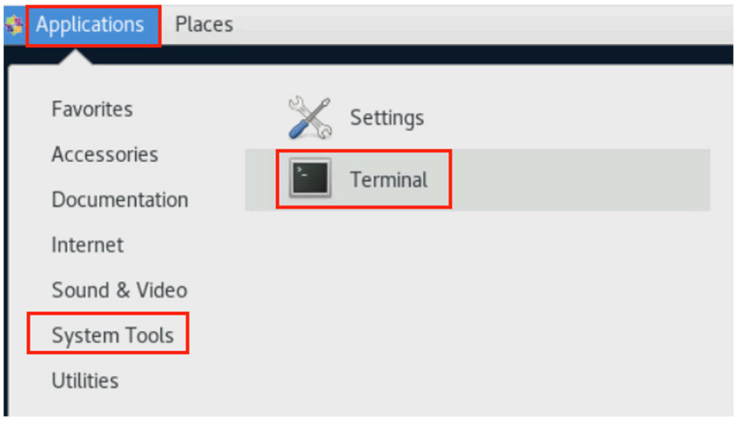


6. In the address bar, type the address `http://203.0.113.2:8000`.

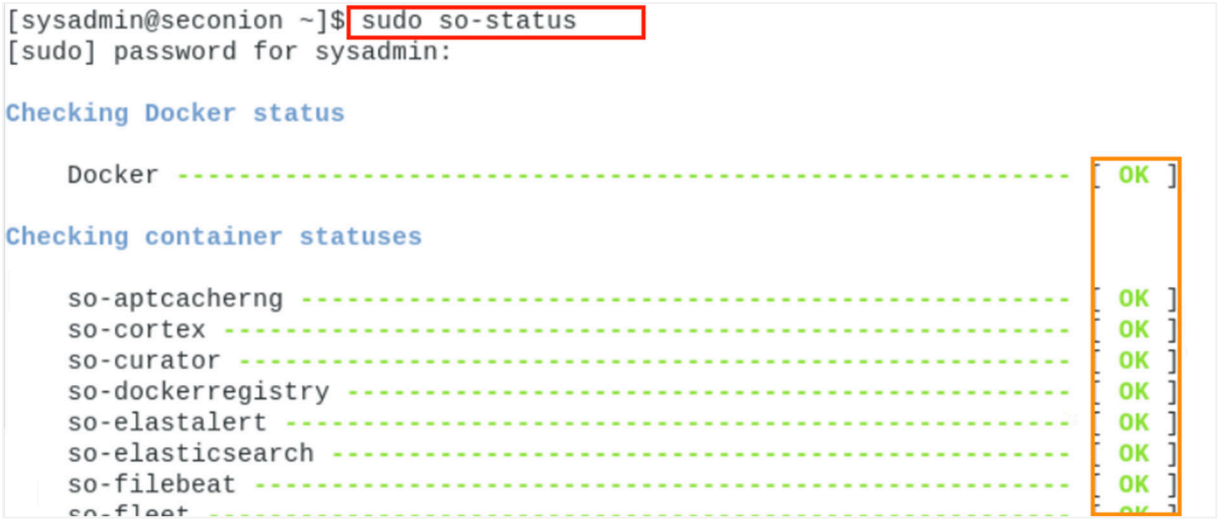
7. In the opened page, find and click on **Desktop**, then click on **scan.pcap** to download the file.

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 su 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 *SecurityOnion*. 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: 9e7bfd7e2f8e703ac2b2360fa2f4f872
- analyzing traffic with Suricata
- analyzing traffic with Zeek
- saving PCAP data spanning dates 2021-09-27 through 2021-09-27

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 co
py it into your browser:
https://192.168.0.6/#/hunt?q=import.id:9e7bfd7e2f8e703ac2b2360fa2f4f872%20%7C%20gro
upby%20event.module%20event.dataset&t=2021%2F09%2F27%2000%3A00%3A00%20AM%20-%202021
%2F09%2F28%2000%3A00%3A00%20AM&z=UTC

or you can manually set your Time Range to be (in UTC):
From: 2021-09-27    To: 2021-09-28

Please note that it may take 30 seconds or more for events to appear in Hunt.
```

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

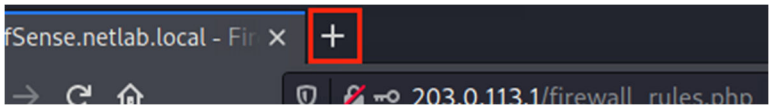
2 Analyze the Data and File a Case

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

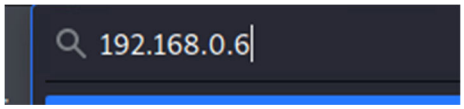
1. Switch to the *Kali* VM. In the *Terminal*, we should still have the server running. Press **Ctrl** + **C** to stop the process.

```
┌──(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 - - [27/Sep/2021 01:25:45] "GET / HTTP/1.1" 200 -
192.168.0.6 - - [27/Sep/2021 01:25:45] code 404, message File not found
192.168.0.6 - - [27/Sep/2021 01:25:45] "GET /favicon.ico HTTP/1.1" 404 -
192.168.0.6 - - [27/Sep/2021 01:26:19] "GET /Desktop/ HTTP/1.1" 200 -
192.168.0.6 - - [27/Sep/2021 01:27:33] "GET /Desktop/scan.pcap HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

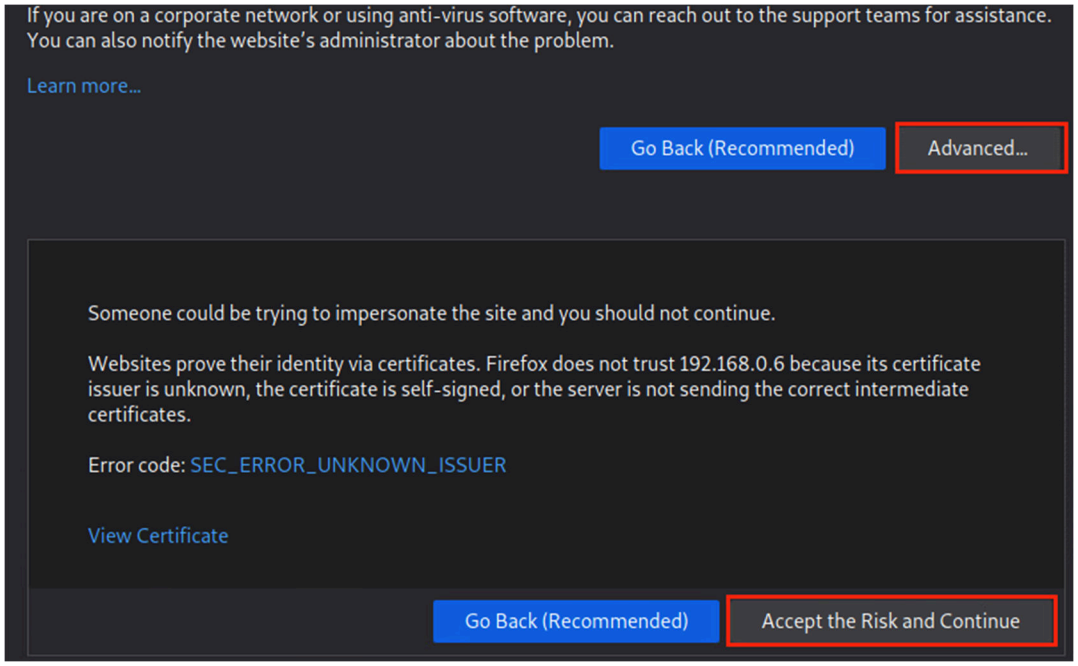
2. Switch back to the browser window, click the **+** to start a new tab.



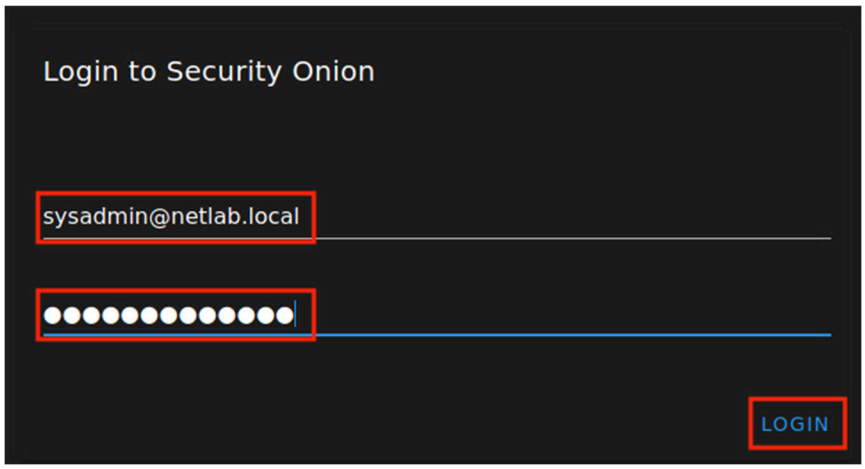
3. Type `192.168.0.6` and press **Enter** to visit the *SecurityOnion* main page.



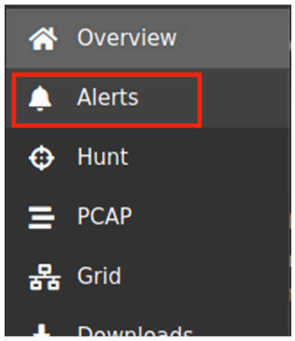
4. If the warning page shows up, click the **Advanced**… button. Then, scroll down and click **Accept the Risk and Continue**.



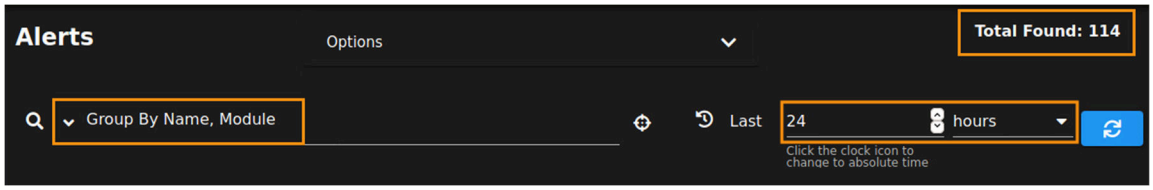
5. On the *Login* page, enter the *username* as `sysadmin@netlab.local` and the password as **NDGlabpass123!**. Click **LOGIN.**



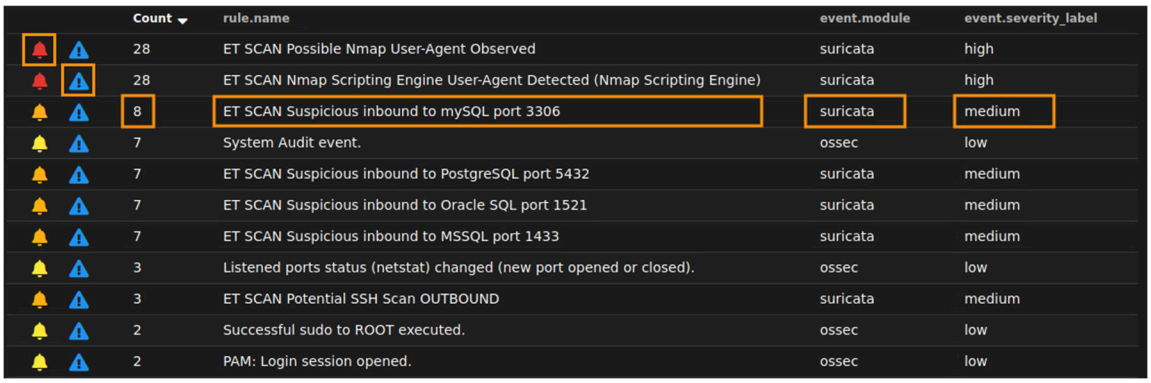
6. On the *Overview* page, click the menu button at the top-left corner. Then, click on **Alerts**.



7. If the import is finished, you will see the top of the screen like below, indicating there were *114* 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 to a case that will show up in *TheHive*. 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.



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
8	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium
7	System Audit event.	ossec	low
7	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
7	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
7	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
3	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
3	ET SCAN Potential SSH Scan OUTBOUND	suricata	medium
2	Successful sudo to ROOT executed.	ossec	low
2	PAM: Login session opened.	ossec	low

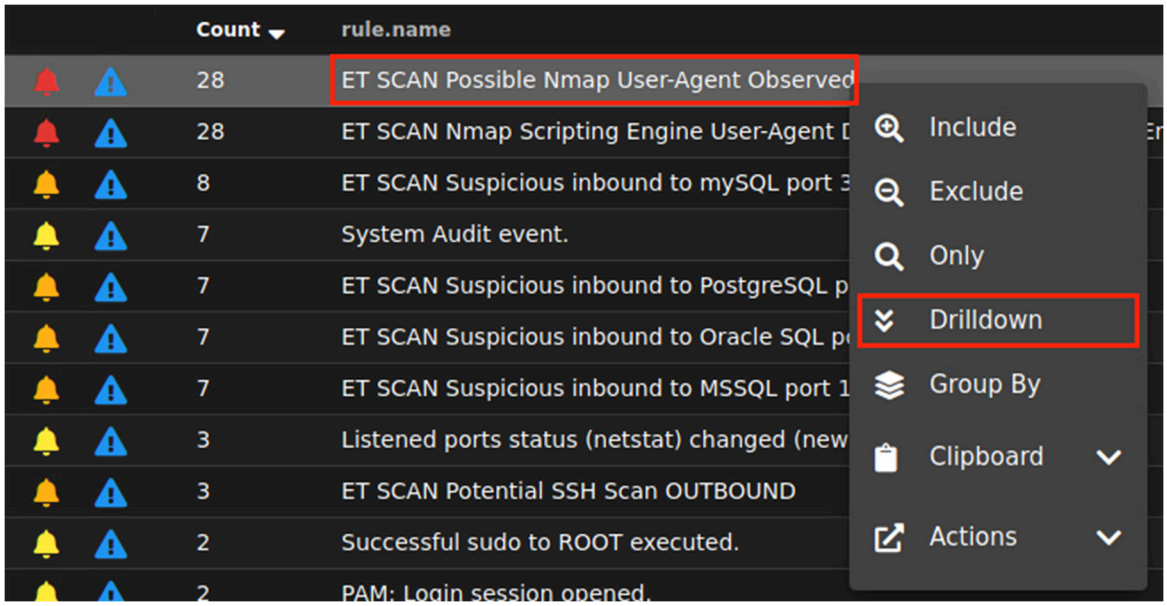
9. Leave the SecurityOnion window open and proceed to the next section.

3 Add a Case, Investigate, and Close the Case

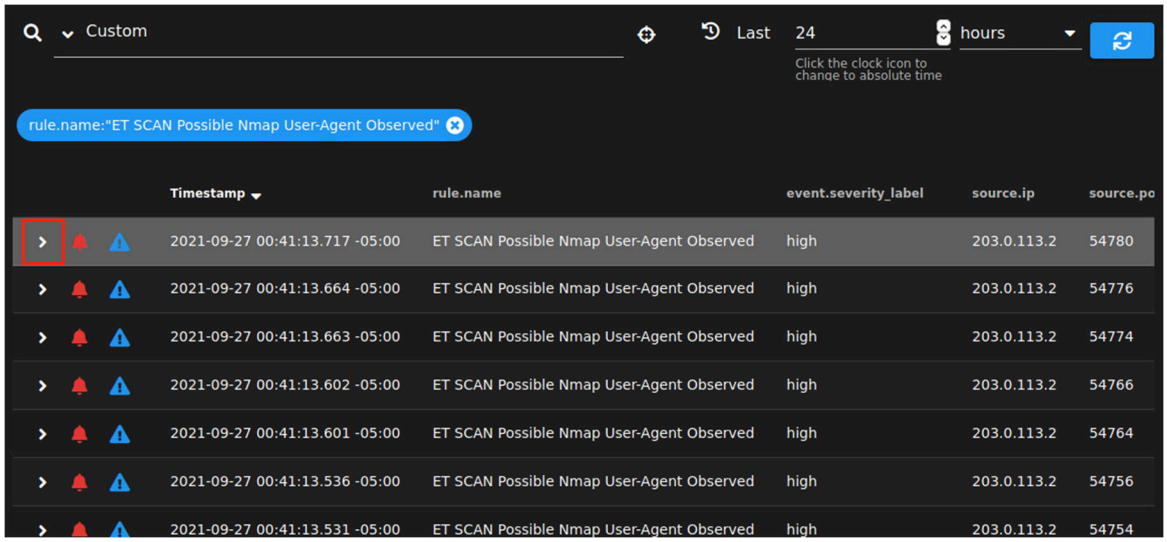
In this section, you will add a case, perform an investigation, and then close the case.

3.1 Escalate an Alert to Add a Case

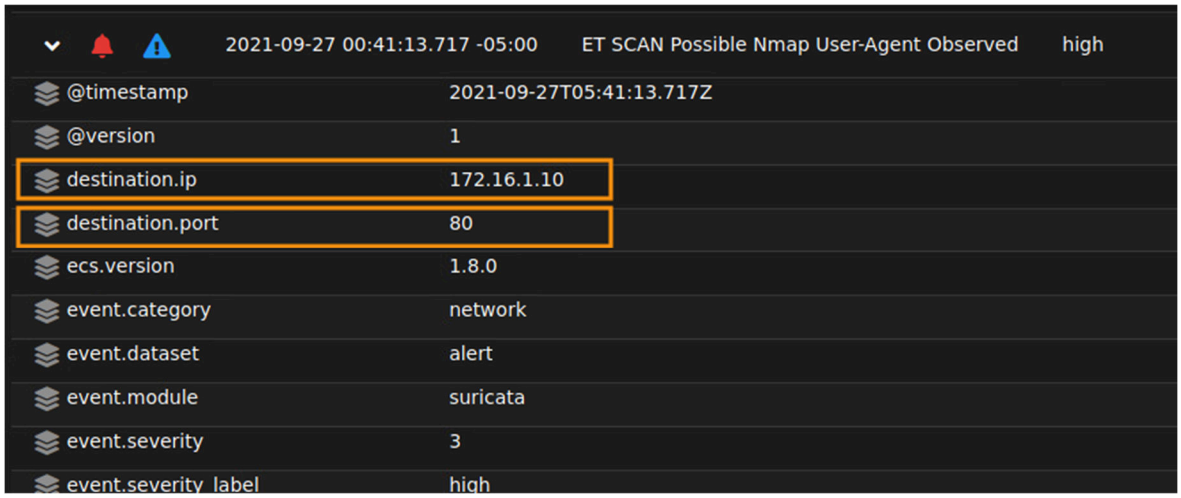
1. With the *SecurityOnion* still opened, let's examine the alerts and analyze a few of them. First, left-click on the **ET SCAN Possible Nmap User-Agent Observed** rule name, then select the **Drilldown** option.



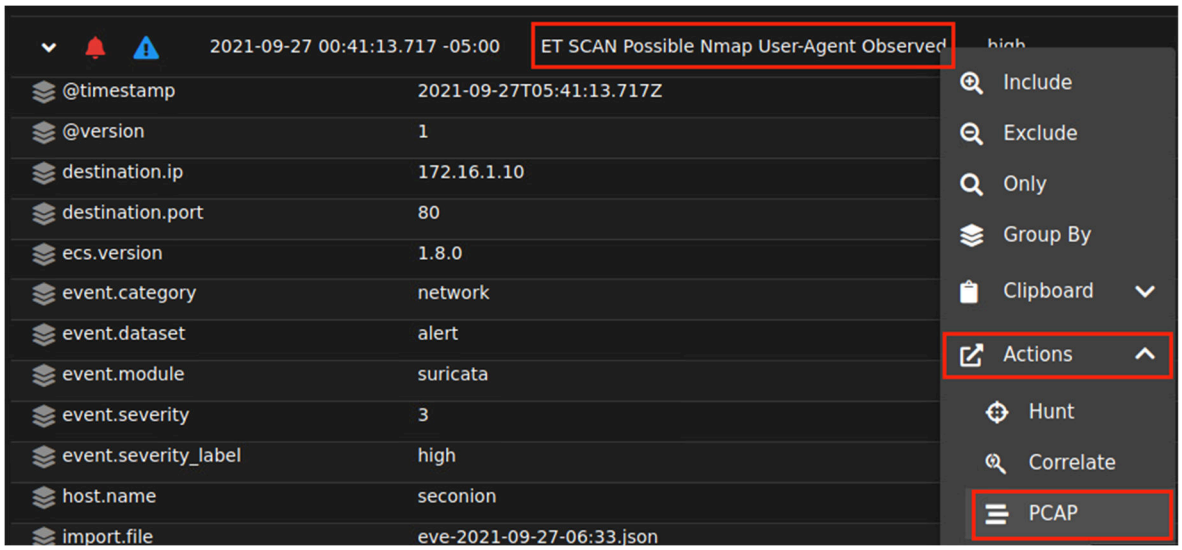
2. The view will be changed, and you should see something like below, click the **arrow** in front of the first entry.



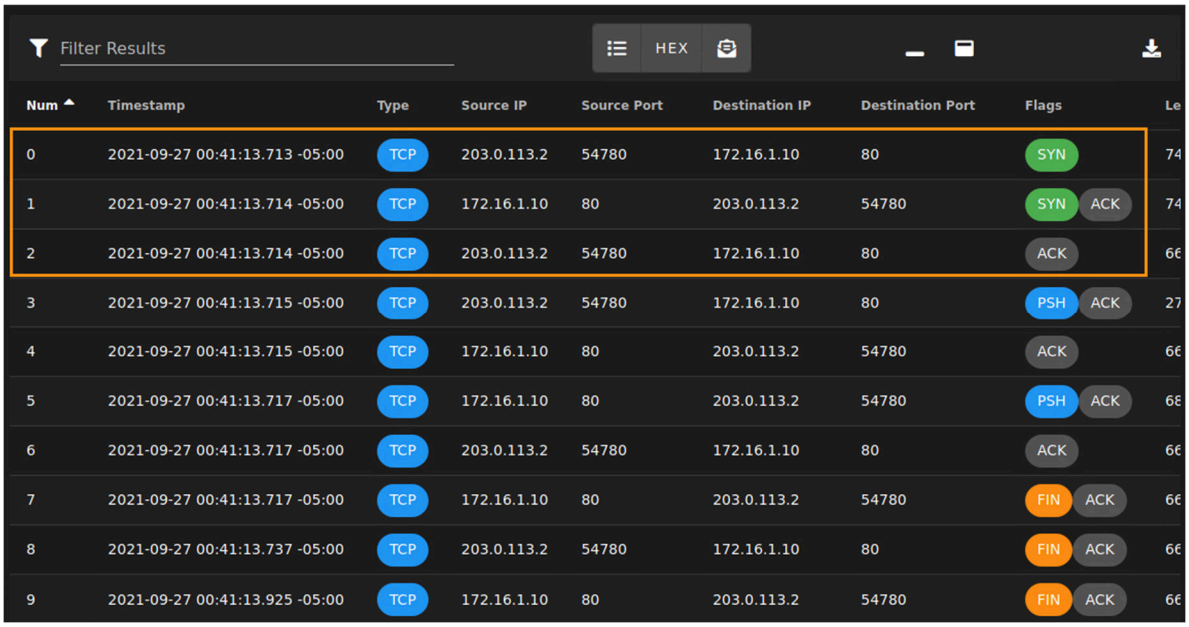
3. Detailed information about this alert will show up. Scroll down to learn more about it, e.g., *destination.ip*, *destination.port*, *source.ip*, *source.port*, *network.data.decoded*, *rule.rule, etc.*



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.

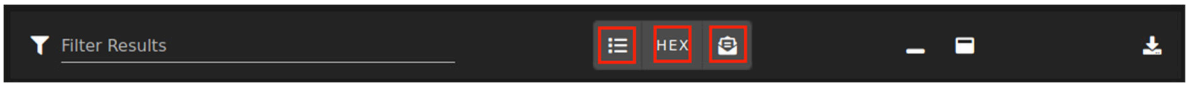


5. We will be brought to the *PCAP* view, which shows the stream of this traffic, starting from the three-way handshake.

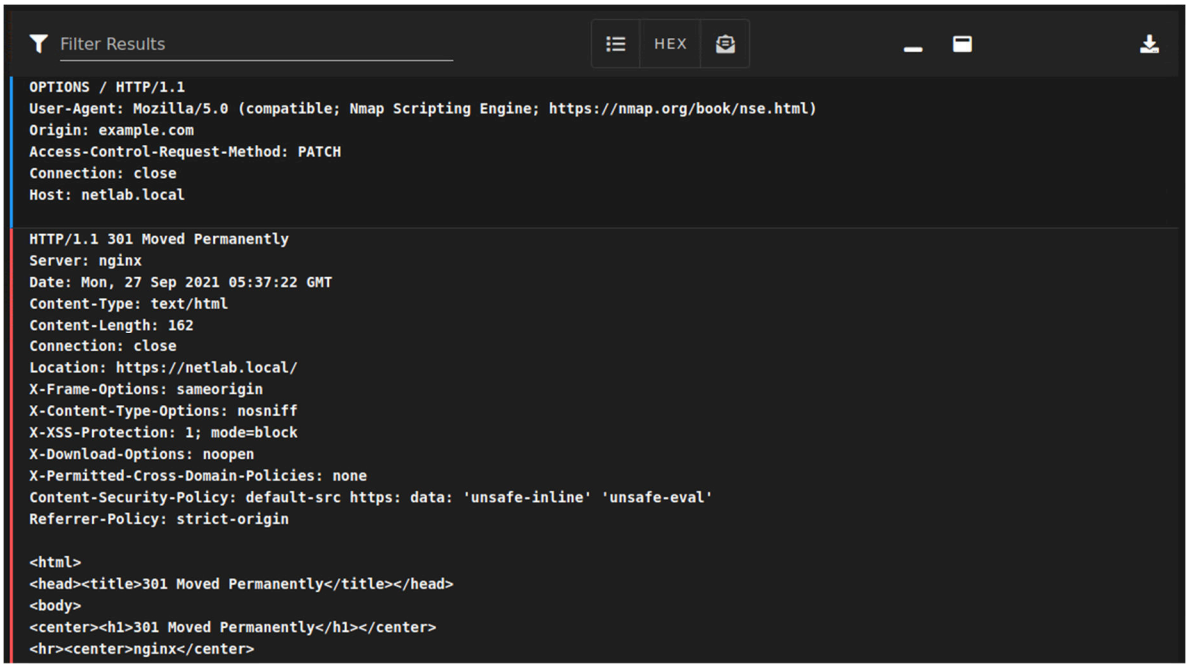


Num	Timestamp	Type	Source IP	Source Port	Destination IP	Destination Port	Flags	Le
0	2021-09-27 00:41:13.713 -05:00	TCP	203.0.113.2	54780	172.16.1.10	80	SYN	74
1	2021-09-27 00:41:13.714 -05:00	TCP	172.16.1.10	80	203.0.113.2	54780	SYN ACK	74
2	2021-09-27 00:41:13.714 -05:00	TCP	203.0.113.2	54780	172.16.1.10	80	ACK	66
3	2021-09-27 00:41:13.715 -05:00	TCP	203.0.113.2	54780	172.16.1.10	80	PSH ACK	27
4	2021-09-27 00:41:13.715 -05:00	TCP	172.16.1.10	80	203.0.113.2	54780	ACK	66
5	2021-09-27 00:41:13.717 -05:00	TCP	172.16.1.10	80	203.0.113.2	54780	PSH ACK	68
6	2021-09-27 00:41:13.717 -05:00	TCP	203.0.113.2	54780	172.16.1.10	80	ACK	66
7	2021-09-27 00:41:13.717 -05:00	TCP	172.16.1.10	80	203.0.113.2	54780	FIN ACK	66
8	2021-09-27 00:41:13.737 -05:00	TCP	203.0.113.2	54780	172.16.1.10	80	FIN ACK	66
9	2021-09-27 00:41:13.925 -05:00	TCP	172.16.1.10	80	203.0.113.2	54780	FIN ACK	66

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

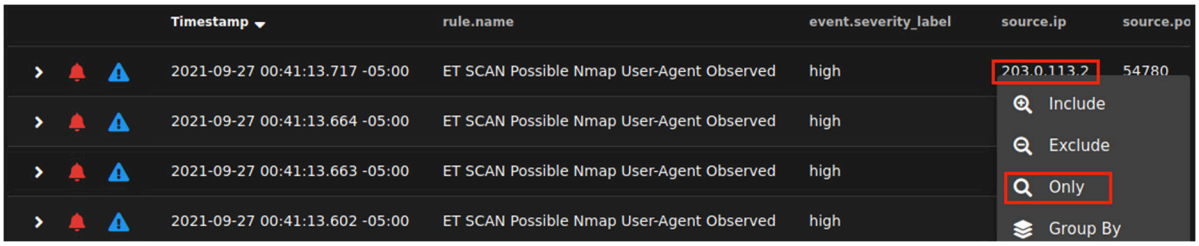


7. If you are familiar with the *Follow Stream* on *Wireshark*, you may find this view also exists in the *SecurityOnion PCAP* module (click the first list toggle, then the HEX toggle).

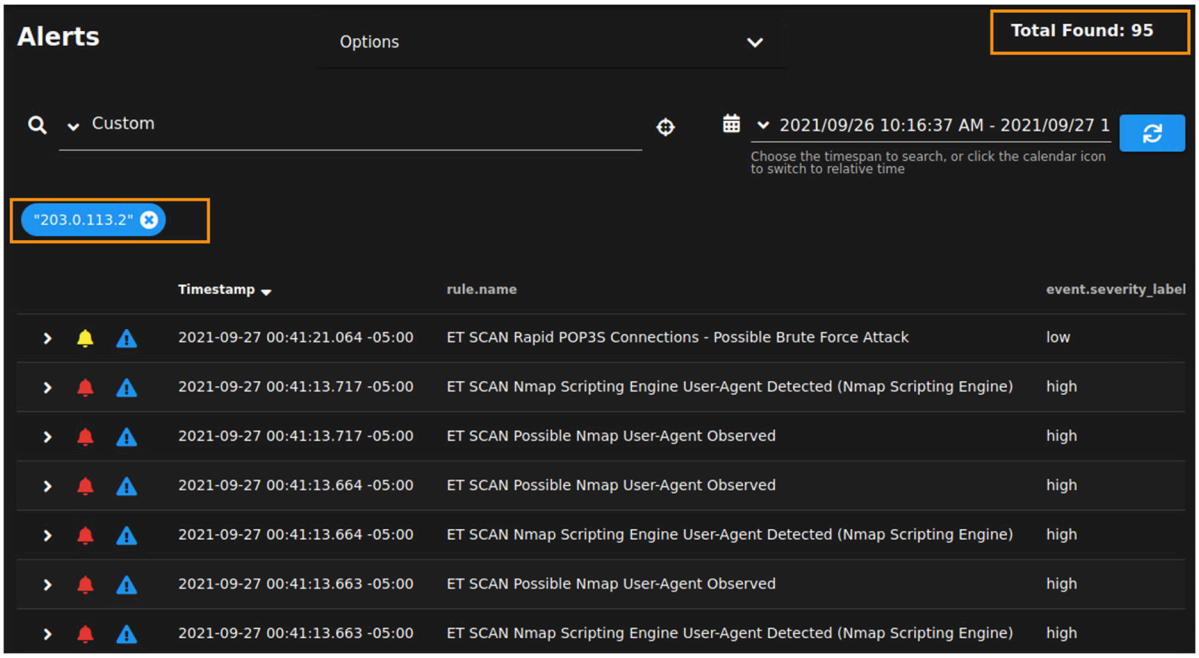


8. Next, let's go back by clicking the **Back** button in the browser.

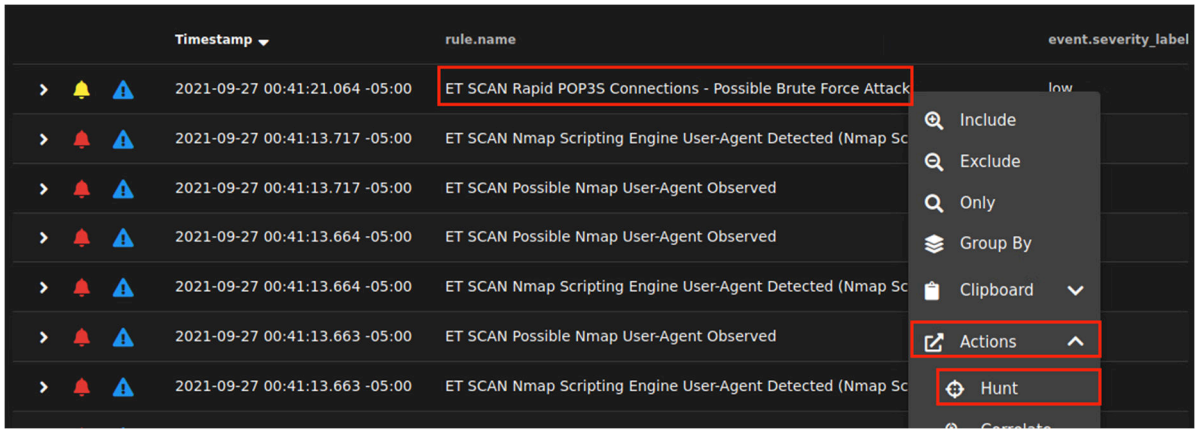
9. Once the page is loaded, left-click on the **source.ip** of **203.0.113.2** and select the **Only** option. This will filter the alerts to only show the ones that originated from the source ip of *203.0.113.2,* which is our *Kali* VM.



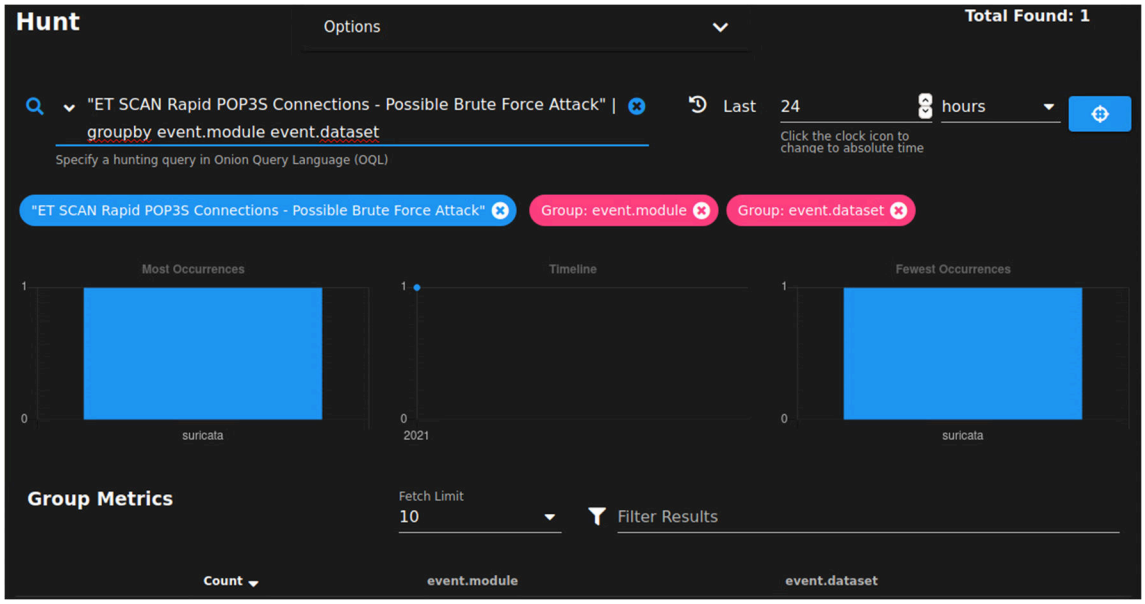
10. Now, we can see that *95* of the alerts are filtered, and they were all originated from the *Kali* VM. Feel free to scroll up and down to see the severity levels of those alerts.



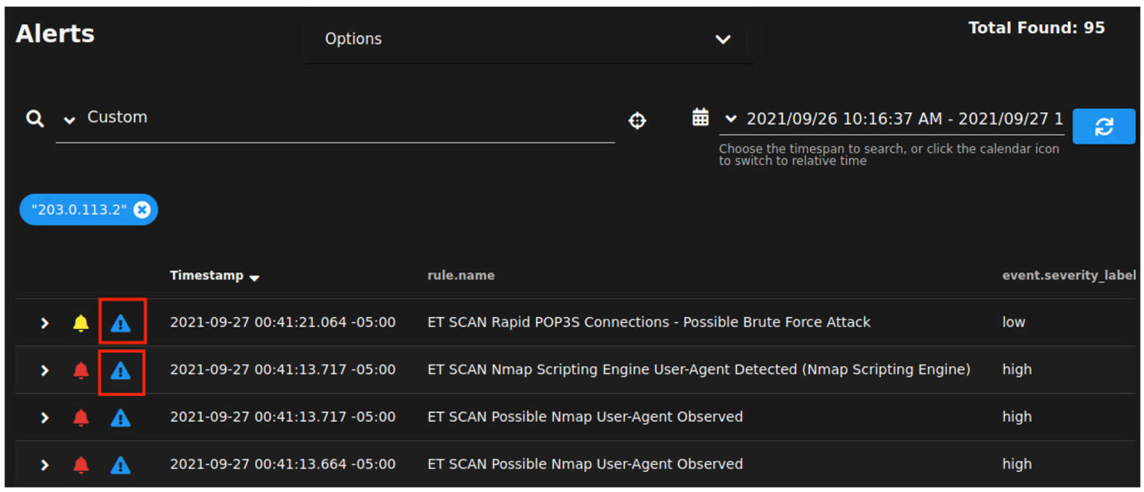
11. Now we see that the first alert is a low severity but a **Possible Brute Force Attack**. Once again, let's left-click on the name and select **Actions**, then select **Hunt.**



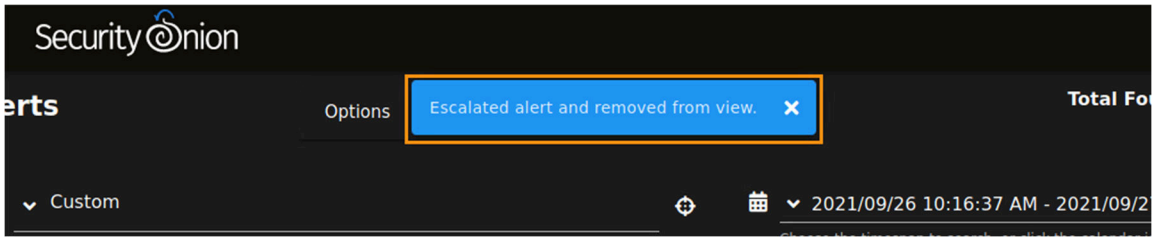
12. You will see the *Hunt* tool page as shown below. On this page, it will bring more details about this alert most of the time. *Hunt* is used to find similar events, track down malicious files, and observe malicious behaviors. We will not go into details about how to use *Hunt* in this lab.



13. Click the browser **Back** button again. Let's say that we need to escalate and create a case for the *Possible Brute Force Attack* and *nmap* scan alert. Click on the **blue triangles** to escalate a case.

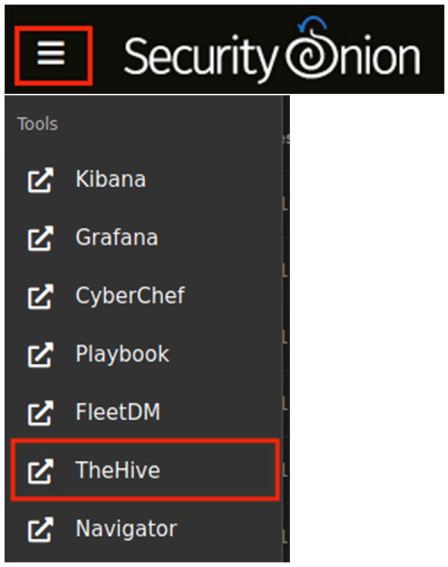


14. Once added, it's going to prompt and say *Escalated alert and removed from view*. Leave the window opened and proceed to the next section.

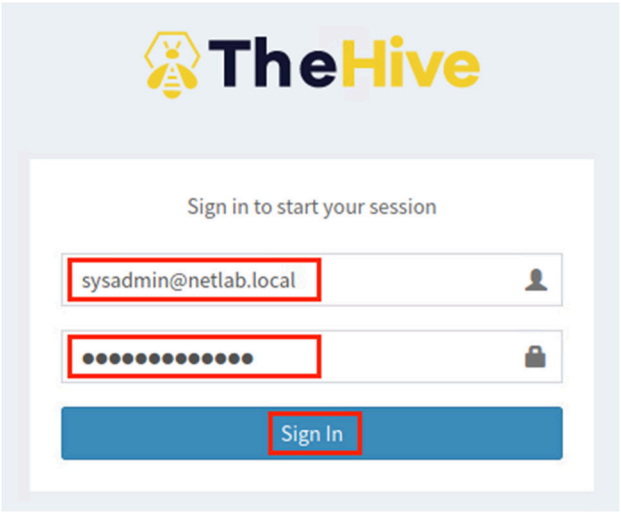


3.2 Add Observable and Tasks for Further Investigation

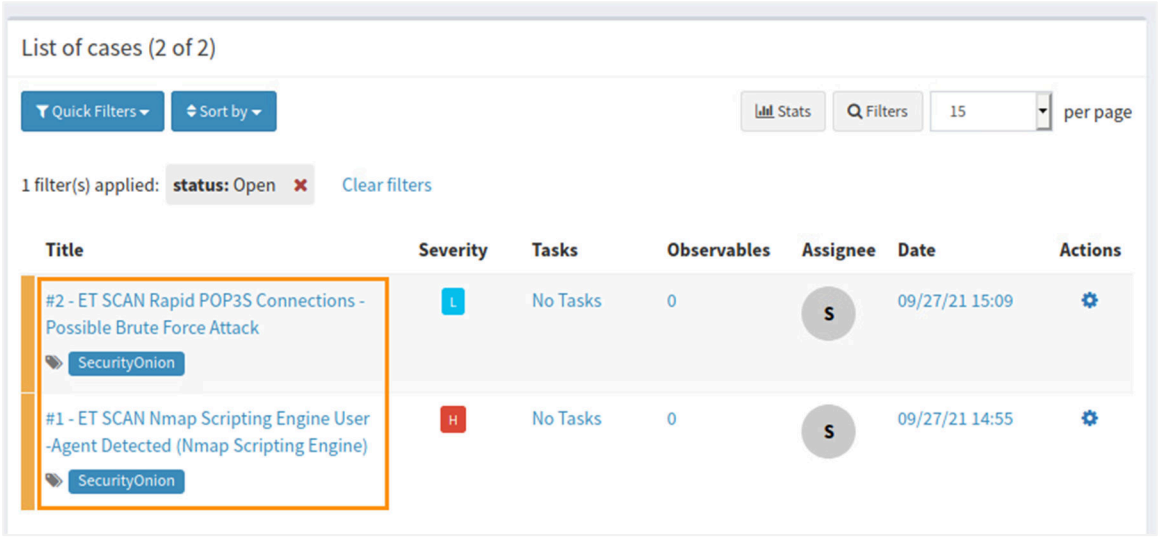
1. We will check the cases in *TheHive*. At the top-left corner, click the **Menu** button, then select **TheHive** option in the *Tools* section. This will open a new page.



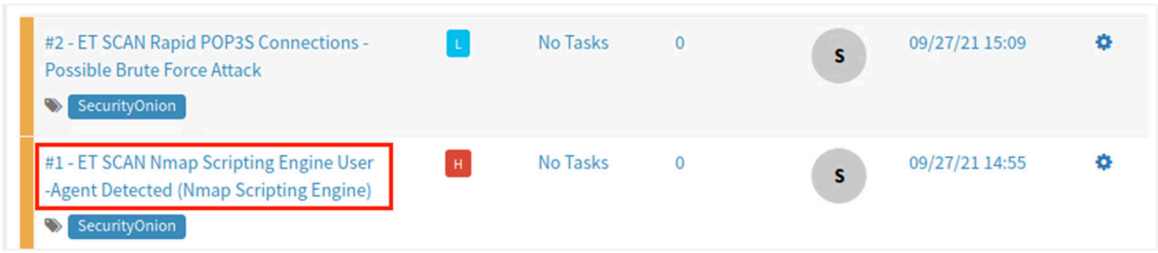
2. Enter the username `sysadmin@netlab.local` and the password as `NDGlabpass123!.` Press the **Sign In** button.



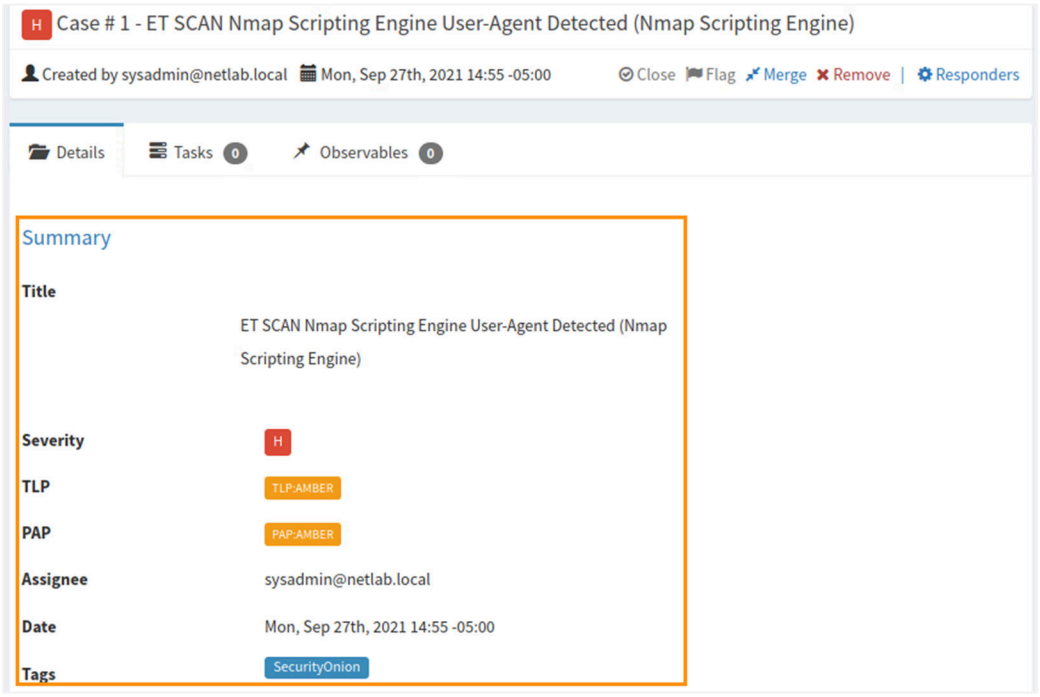
3. Once logged in, you should see our case list with the newly added *Brute Force* and *nmap* cases.



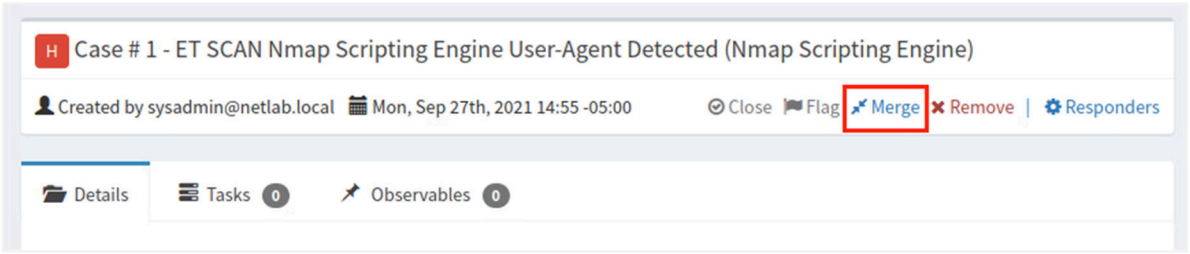
4. Let's click on the *nmap* entry to enter the case.



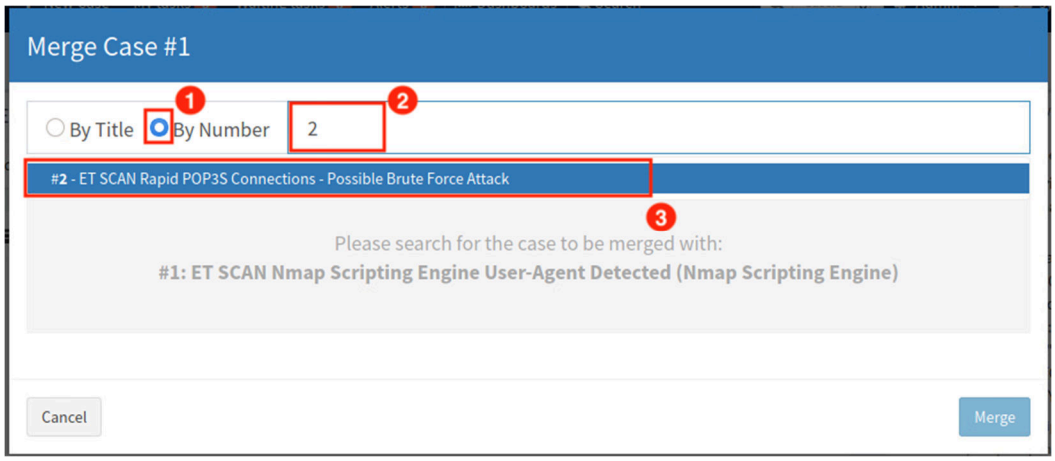
5. You will see the case *Details* page, with *Summary* at the top and *Description* at the bottom(scroll down to see).



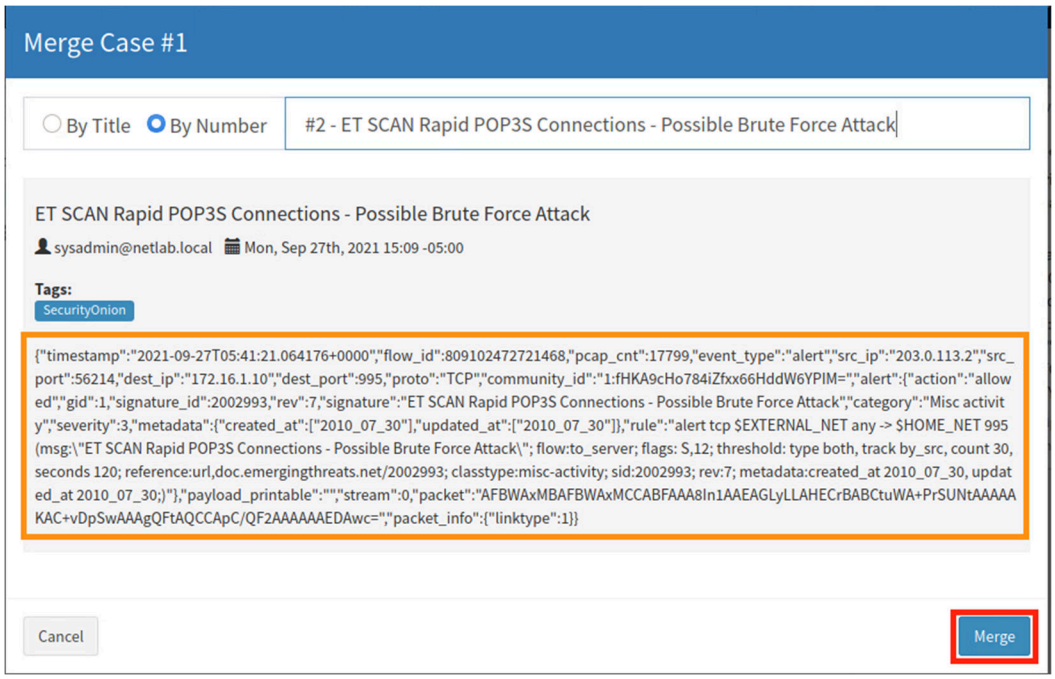
6. Because the *Brute Force Attack* and the *nmap* were from the same IP address, let's merge them together. Above the *Details* field, look for a button name **Merge** and click it once.



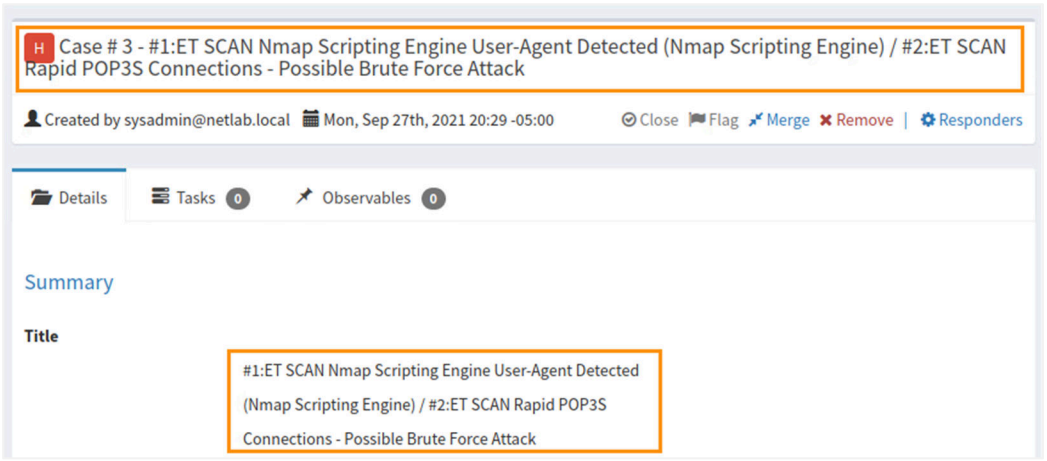
7. A *Merge* window will appear. Check the **By Number** radio button, then in the textbox, type 2. As we are typing, the #2 result will show up. Click on it to expand the details.



8. The details about #2 will show, and the *Merge* button will become clickable. Click the **Merge** button.

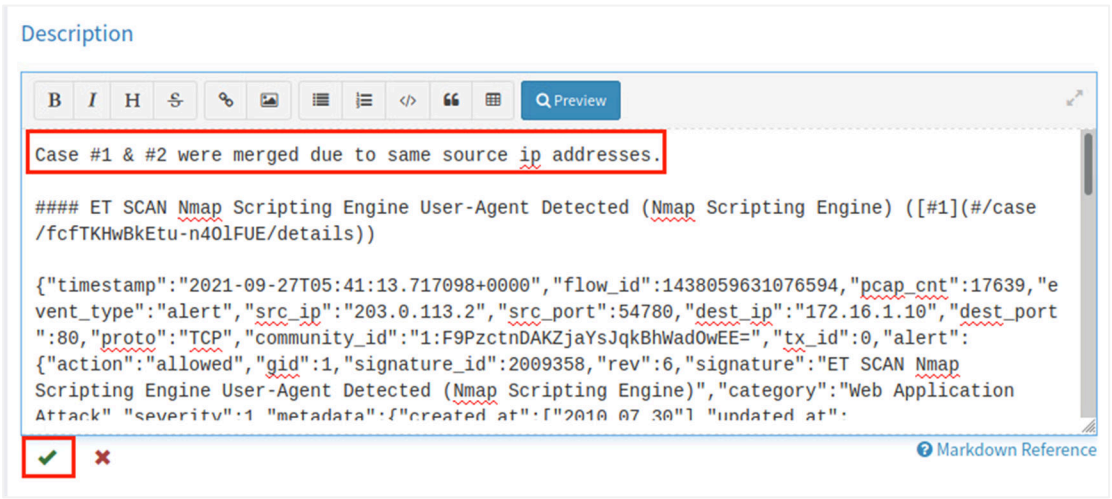


9. The system will then merge the case 1 and 2 to form case #3, as shown in the screenshot below:

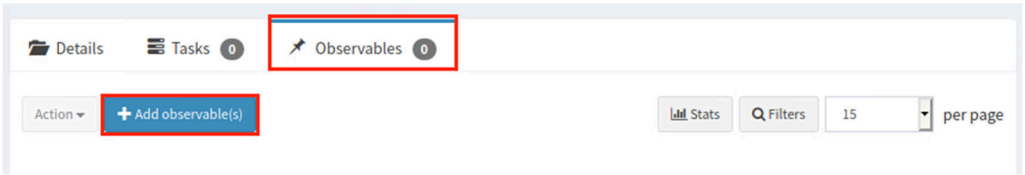


10. Scroll down to the *Description* area and click the **Edit** button.

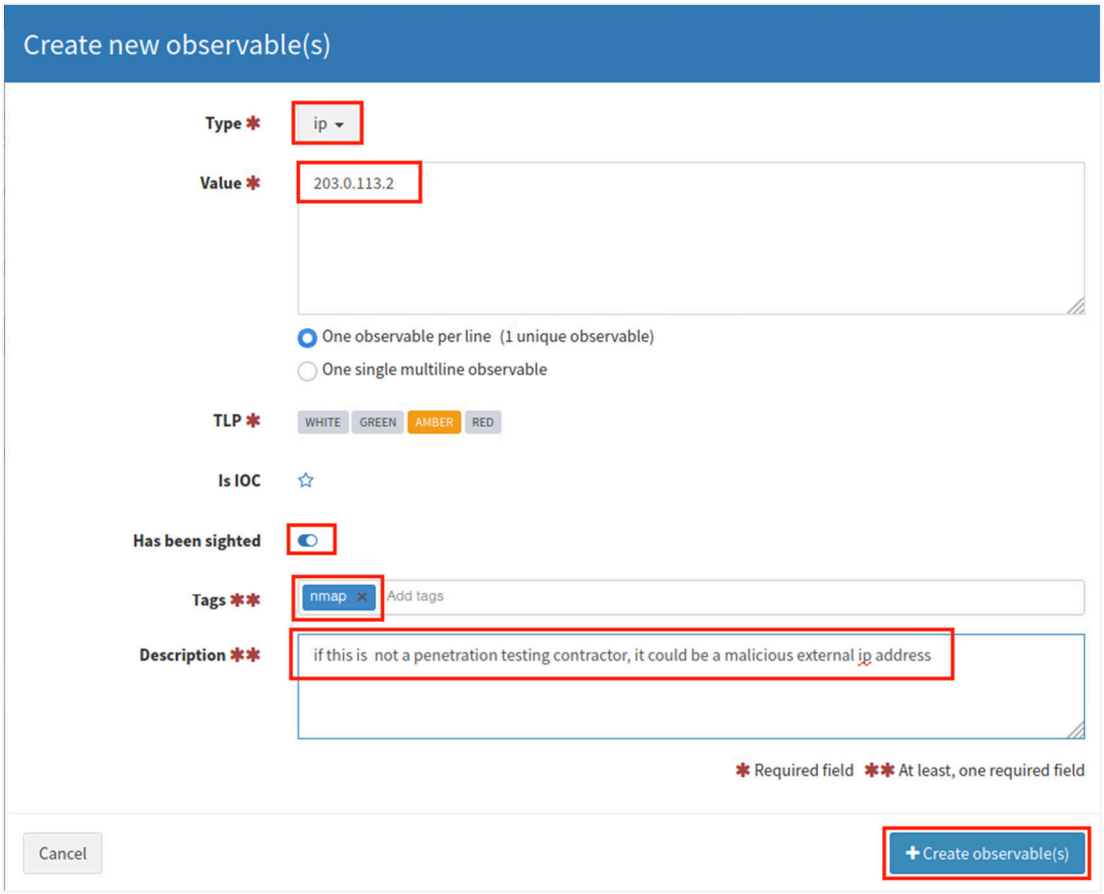
11. Add a note to the very beginning of the description. For example, write the note as: `Case #1 & #2 were merged due to same source ip addresses`. Then, click the **checkmark** to save it.



12. Once saved, let's scroll back to the top. We are going to add some extra notes. Click the **Observables** button, then click **Add observable(s)**.

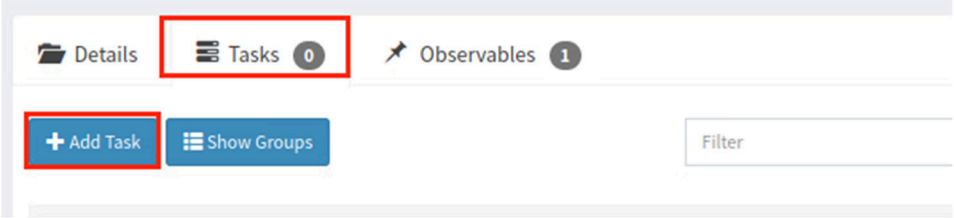


13. In the new window, type the following information, then click the **Create observable(s)** button.
    a. *Type*: `ip`
    b. *Value*: `203.0.113.2`
    c. *Has been sighted*: flip the switch
    d. *Tags*: `nmap`
    e. *Description*: `if this is not a penetration testing contractor, it could be a malicious external ip address`.

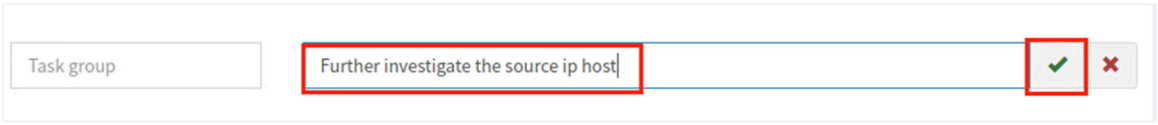


An observable is an extra piece of information we can add to aid the security team for further investigation.

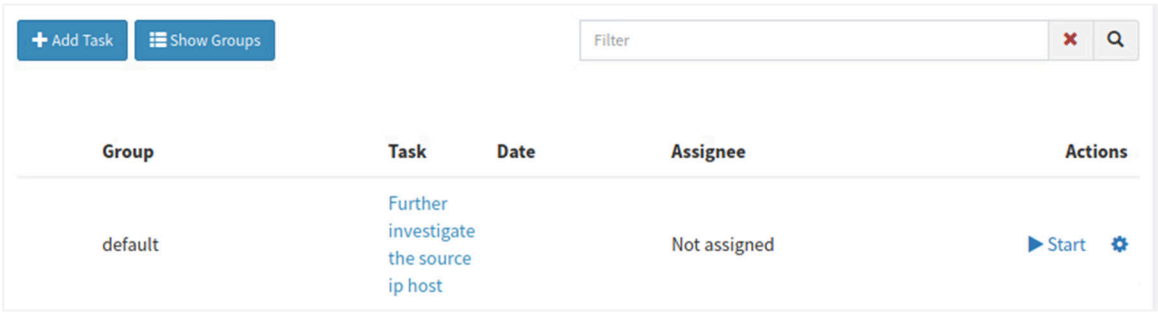
14. Next step, let's add some tasks. Click on the **Tasks**, then click the **Add Task** button.



15. Type `Further investigate the source ip host`, click the **checkmark** to confirm.



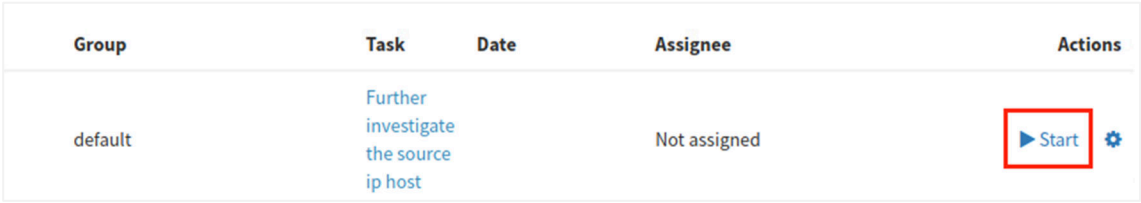
16. Now you should see the task being generated. Leave the page opened, proceed to the next section.



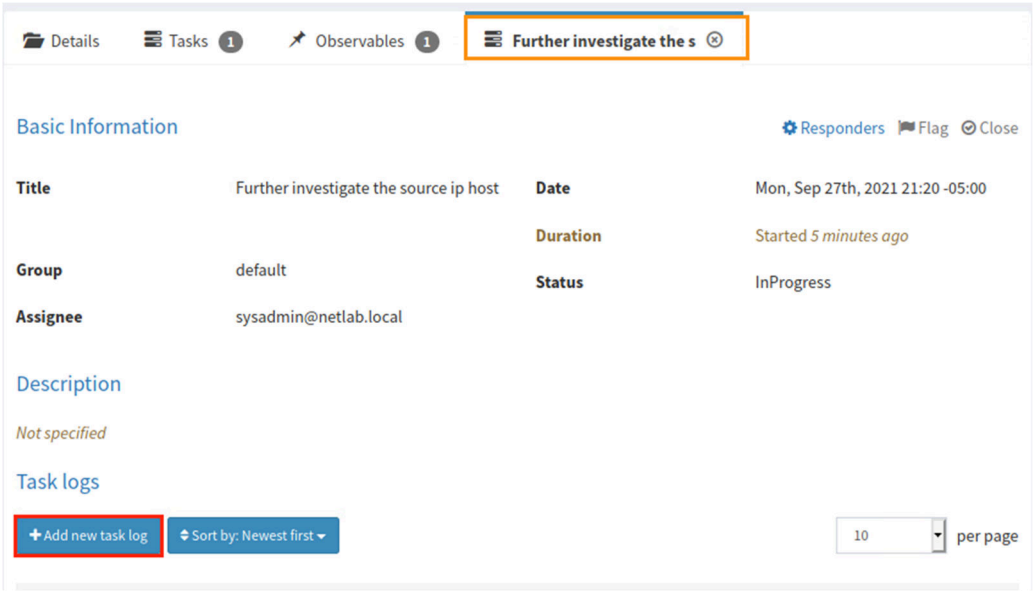
3.3 Finish All Tasks and Close a Case

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

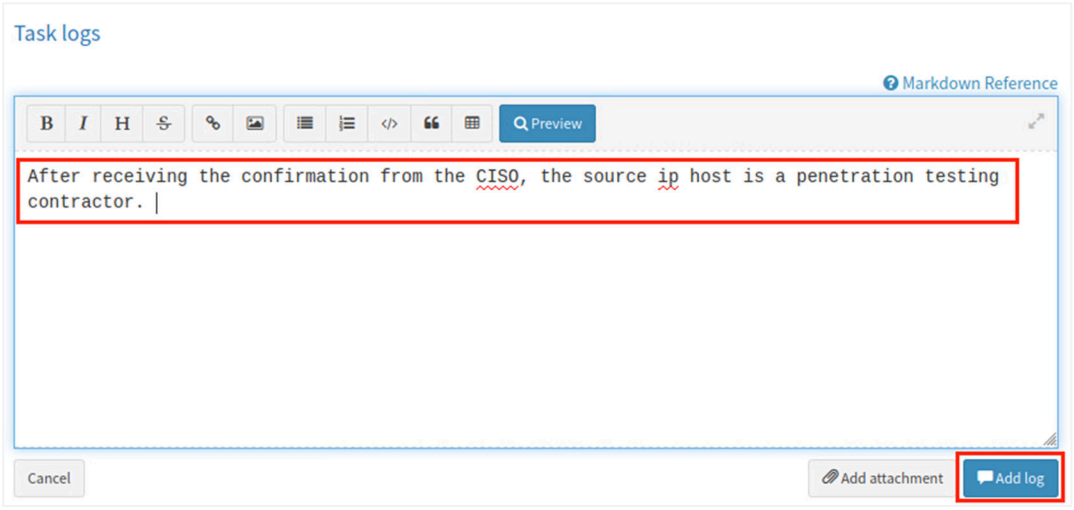
1. In the *Tasks* tab, click the **Start** button.



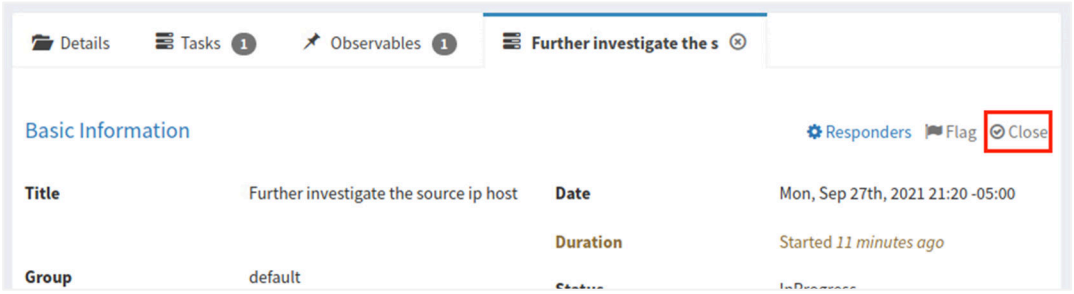
2. A new tab will open; this is the task we are working on. Click the **Add new task log** button.



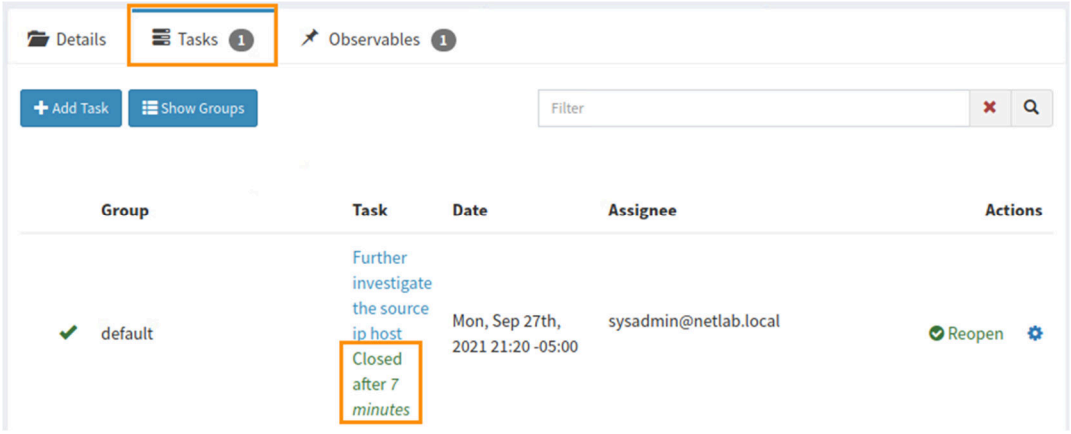
3. Let's assume the source ip is a penetration testing contractor. Therefore, we should add it to the task log as shown below. Press the **Add log** button to save.



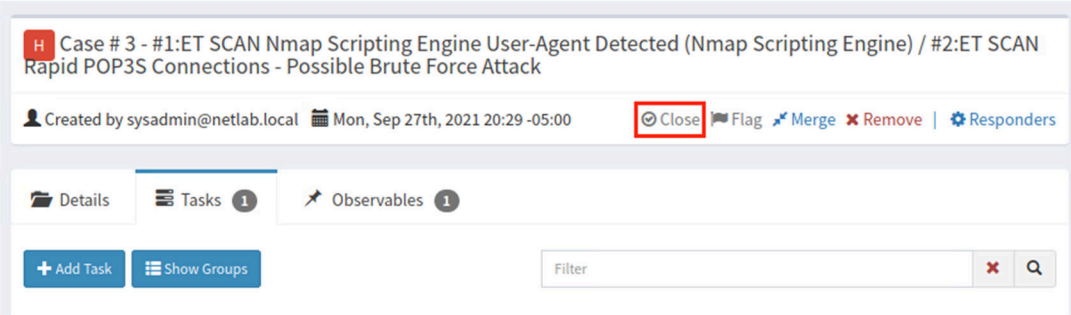
4. Then, we can close this task by clicking the **Close** button at the top-right corner.



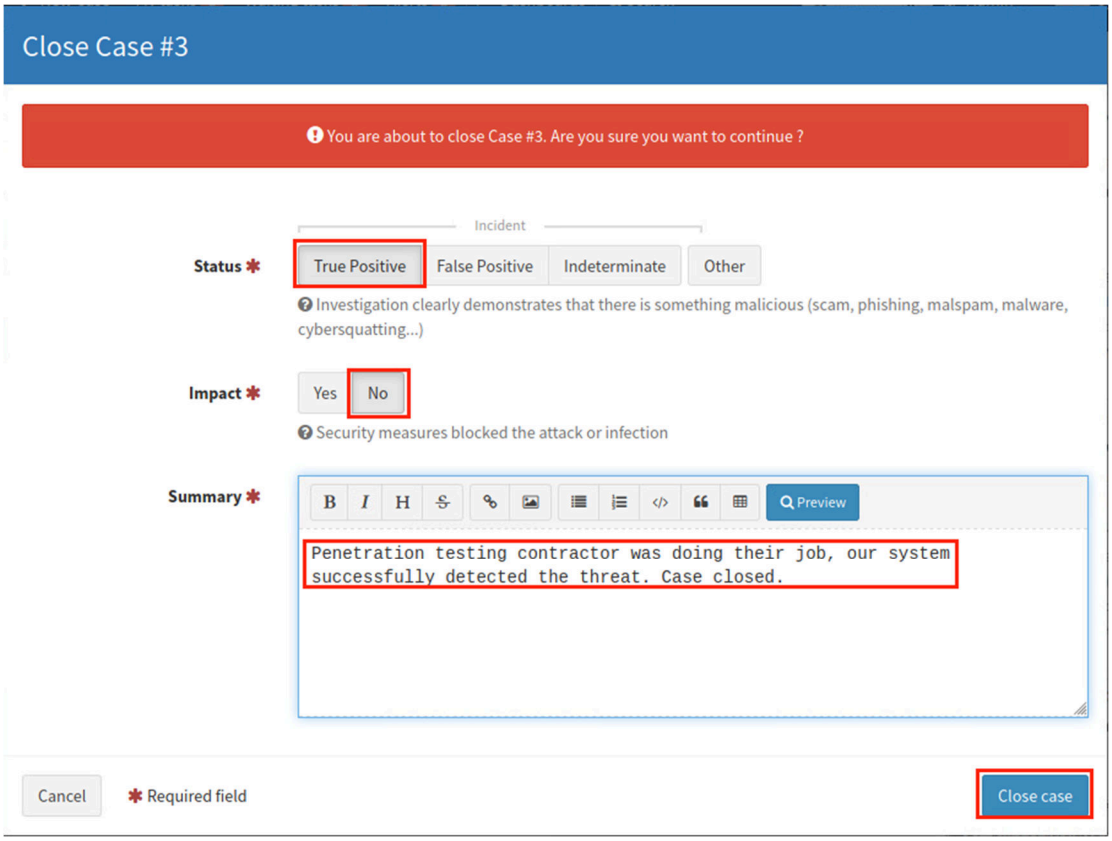
5. We are then brought back to the *Tasks* tab. The task is now showing as closed.



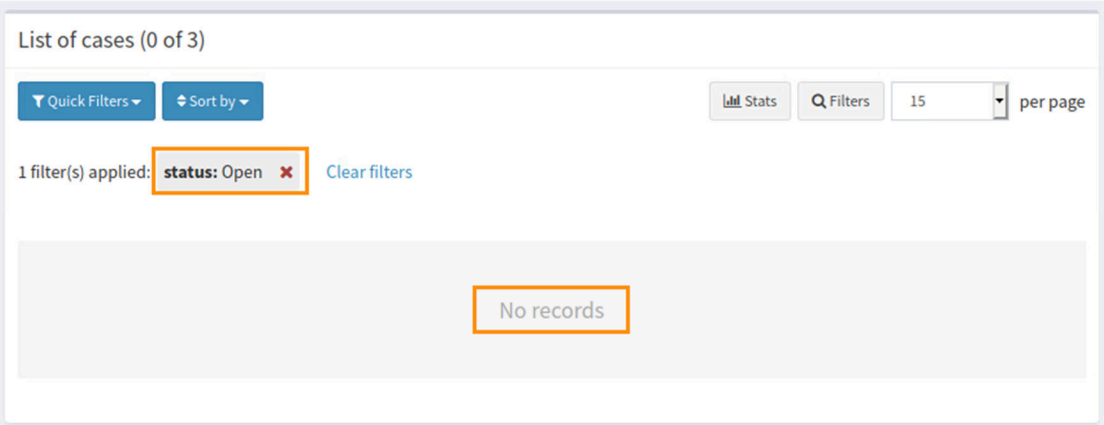
6. Since this case is solved, we can now close it. Click the **Close** button at the top.



7. A *Close Case #3* window will open, make sure you provide the following information, and then click the **Close case** button.
   a. *Status*: **True positive**
   b. *Impact*: **No**
   c. *Summary*: `Penetration testing contractor was doing their job, our system successfully detected the threat. Case closed.`



8. The list of cases page will appear, and there will be no open cases left on that page.



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