



## 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

Copyright © 2022 Network Development Group, Inc.  
[www.netdevgroup.com](http://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 SecurityOnion 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.....	24
3.3 Finish All Tasks and Close a Case.....	29

## Introduction

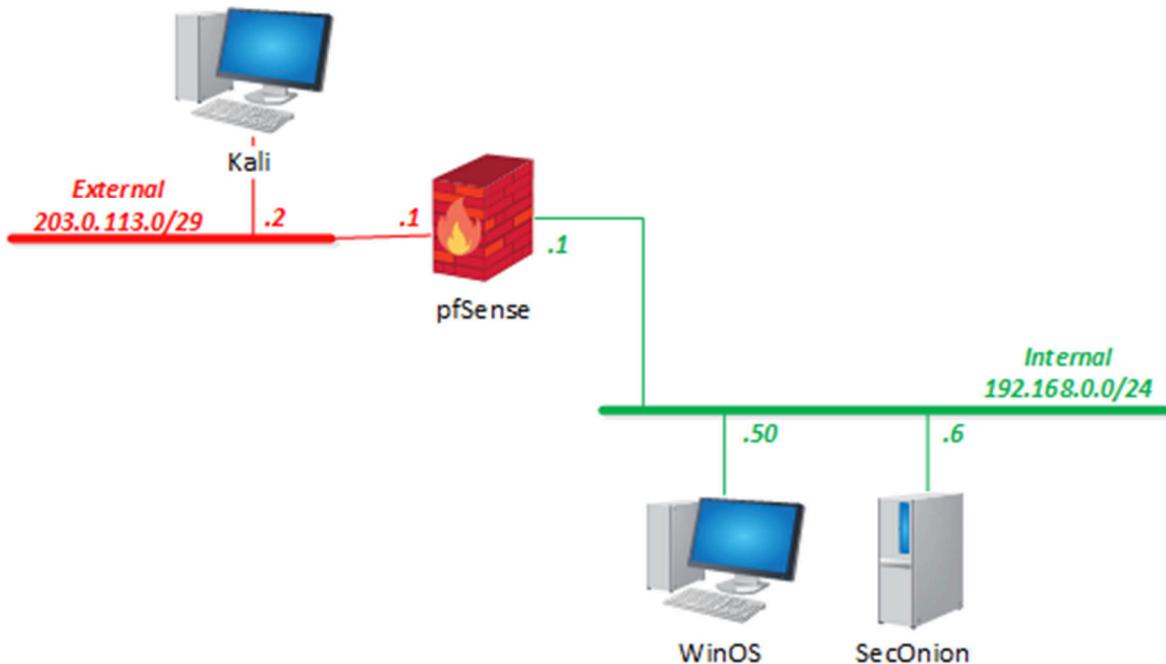
In this lab, you will be conducting network and host monitoring using various administrative tools.

## Objective

In this lab, you will perform the following tasks:

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

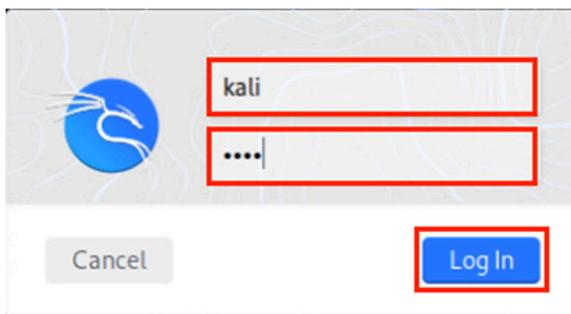
### 1.1 Disable Firewall

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**.



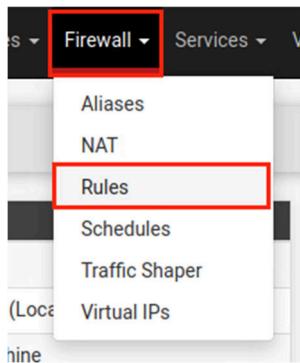
3. Click to open a browser window.



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.

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

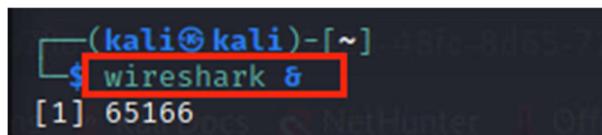
In this section, you will generate the traffic from an attacking machine, then capture and save it to a pcap file.

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

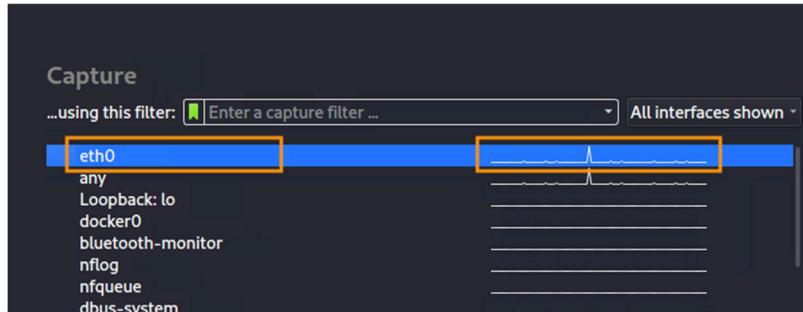


2. Type the following command to start *Wireshark* and keep the process in the background.

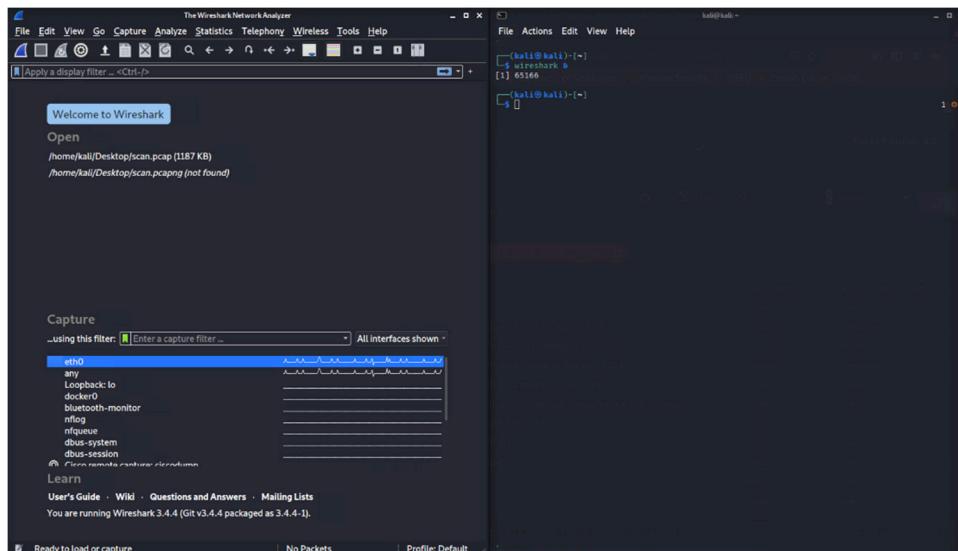
```
kali@kali$ wireshark &
```



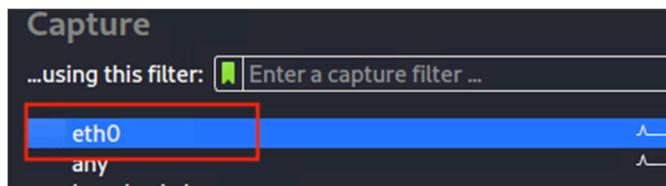
3. *Wireshark* should open, and on the *Welcome* page, you should see the wave line updating itself continuously on interface *eth0*.



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
```

```
(kali㉿kali: ~]$ $ nmap -T5 203.0.113.1 192.168.0.0/24 172.16.1.0/28
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 00:32 CDT
Nmap scan report for 203.0.113.1
Host is up (0.00054s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http

Nmap scan report for pfsense.netlab.local (192.168.0.1)
Host is up (0.00060s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http

Nmap scan report for seconion.netlab.local (192.168.0.6)
Host is up (0.00073s 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 192.168.0.254
Host is up (0.00057s latency).
All 1000 scanned ports on 192.168.0.254 are closed

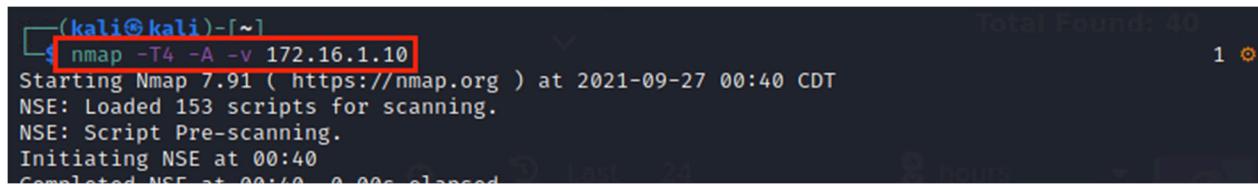
Nmap scan report for 172.16.1.1
Host is up (0.00058s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http

Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00084s 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 (6 hosts up) scanned in 8.20 seconds
```

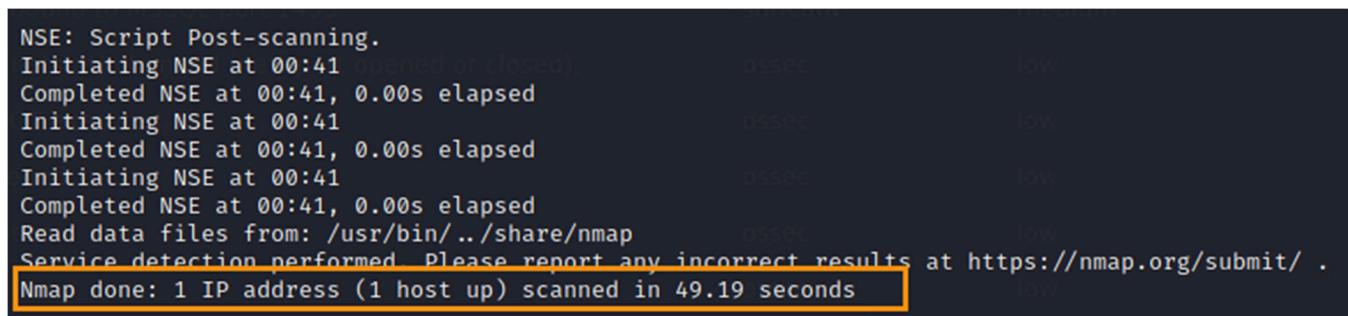
7. After the scan is finished, type the following command to target the 172.16.1.10 host to start an intensive scan. This may take 2-3 minutes to complete.

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

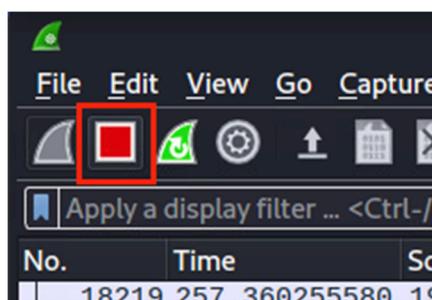


```
(kali㉿kali)-[~]
$ nmap -T4 -A -v 172.16.1.10
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 00:40 CDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:40
Completed NSE at 00:40, 0.00s elapsed
```

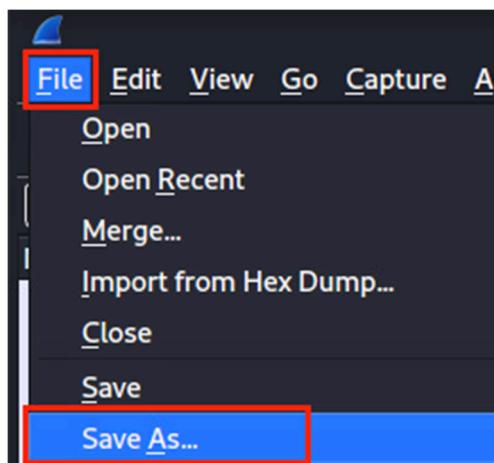
8. Once the scan is complete, it will say *Nmap done...* Stop the Wireshark capture by clicking the red square button.



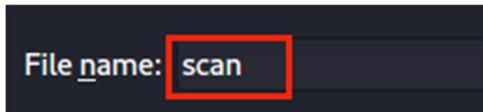
```
NSE: Script Post-scanning.
Initiating NSE at 00:41 opened or closed)
Completed NSE at 00:41, 0.00s elapsed
Initiating NSE at 00:41
Completed NSE at 00:41, 0.00s elapsed
Initiating NSE at 00:41
Completed NSE at 00:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed.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



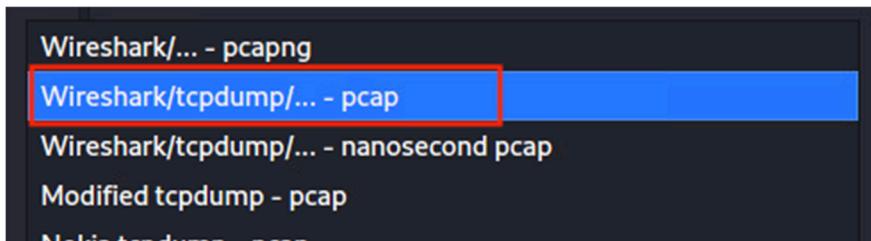
9. Click on **File**, then the **Save As...** option.



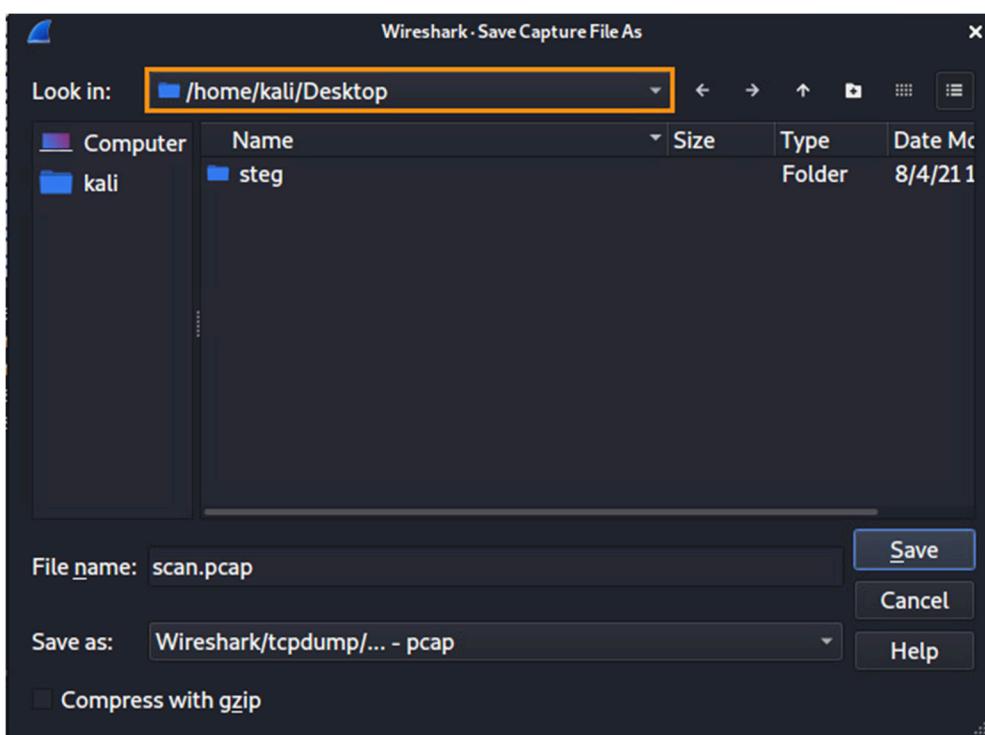
10. Type **scan** as the File name.



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

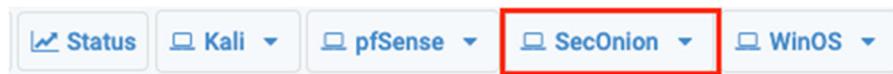
In this section, you will import the pcap file to the *SecurityOnion* for further analysis.

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
```

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

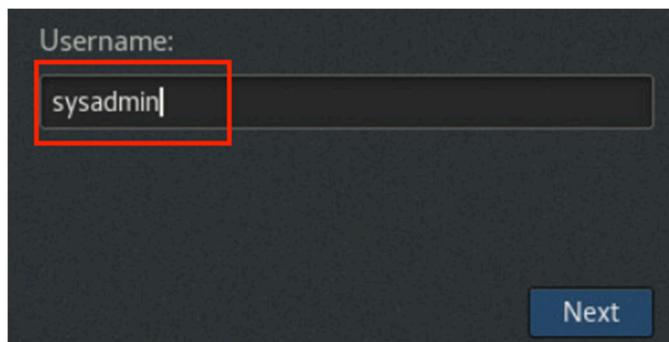
2. We will now log in to the *SecOnion* VM. Click on the **SecOnion** tab.

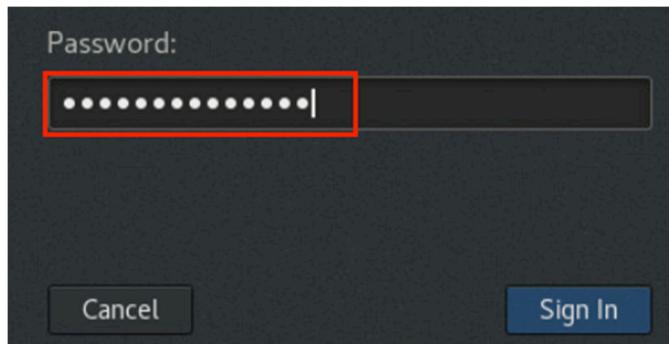


3. Then click and drag up to unlock the screen for a login prompt.

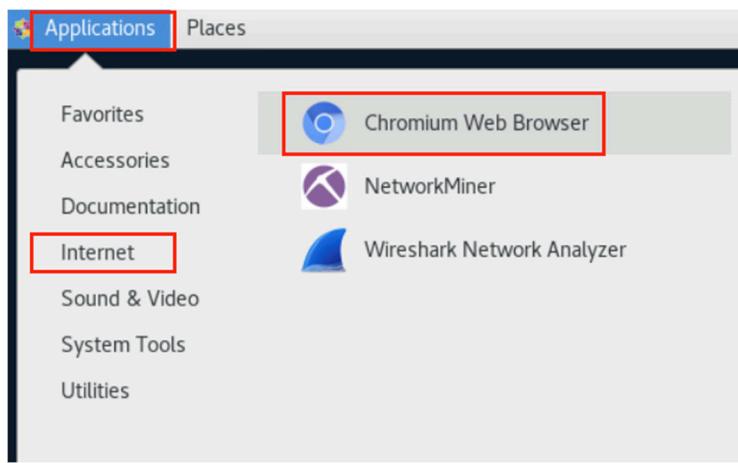


4. Type **sysadmin** as the username and **NDGLabpass123!** for the password.





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**.

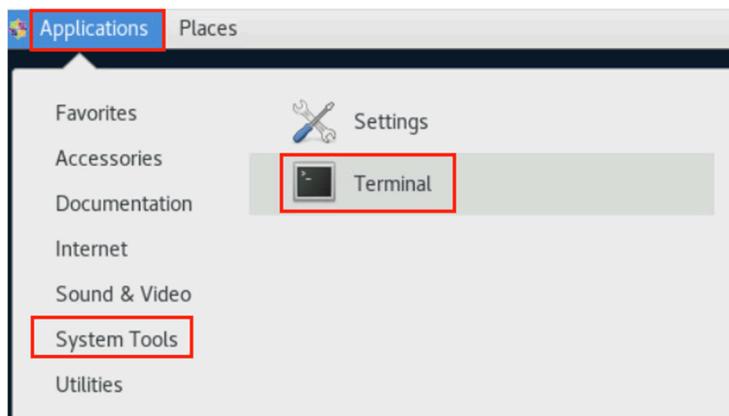


7. In the opened page, find and click on **Desktop**, then click on **scan.pcap** to download the file.



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*.

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

Checking Docker status

Docker ----- [OK]

Checking container statuses

so-aptcacherng -----
so-cortex -----
so-curator -----
so-dockerregistry -----
so-elastalert -----
so-elasticsearch -----
so-filebeat -----
so-fleet ----- [OK]
[OK]
[OK]
[OK]
[OK]
[OK]
[OK]
[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 copy it into your browser:

<https://192.168.0.6/#/hunt?q=import.id:9e7bfd7e2f8e703ac2b2360fa2f4f872%20group%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.

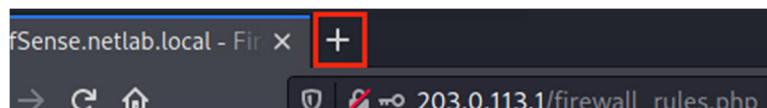
## 2 Analyze the Data and File a Case

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

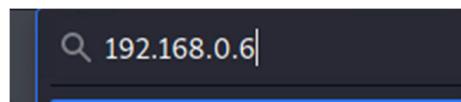
1. Switch to the *Kali VM*. In the *Terminal*, we should still have the server running. Press **Ctrl + C** to stop the process.

```
(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] "GET /favicon.ico HTTP/1.1" 404 -
192.168.0.6 - - [27/Sep/2021 01:25:45] "GET /Desktop/ HTTP/1.1" 200 -
192.168.0.6 - - [27/Sep/2021 01:26:19] "GET /Desktop/scan.pcap HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

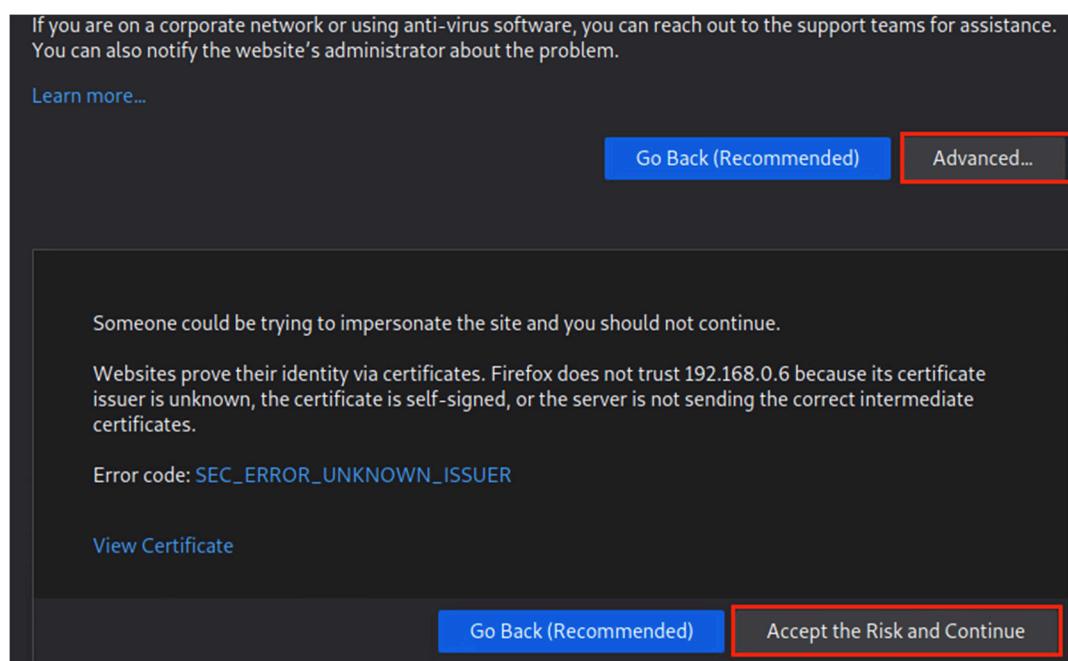
2. Switch back to the browser window, click the **+** to start a new tab.



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.

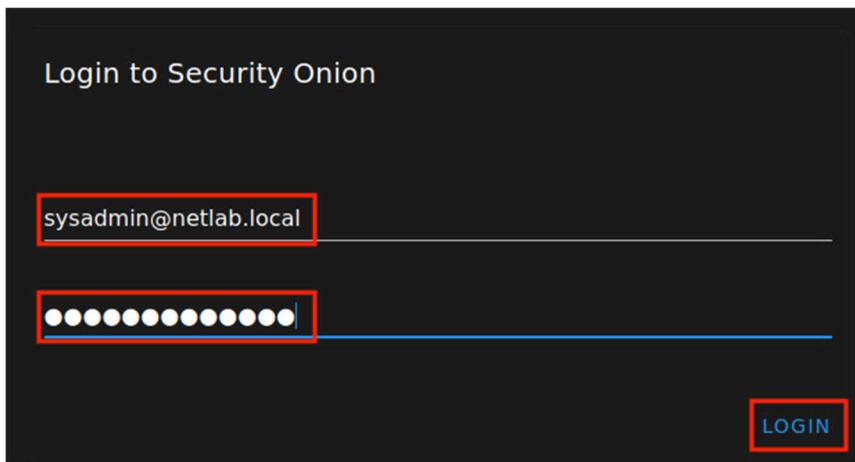
Websites prove their identity via certificates. Firefox does not trust 192.168.0.6 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC\_ERROR\_UNKNOWN\_ISSUER

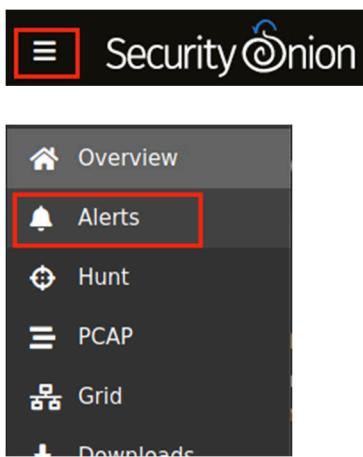
[View Certificate](#)

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

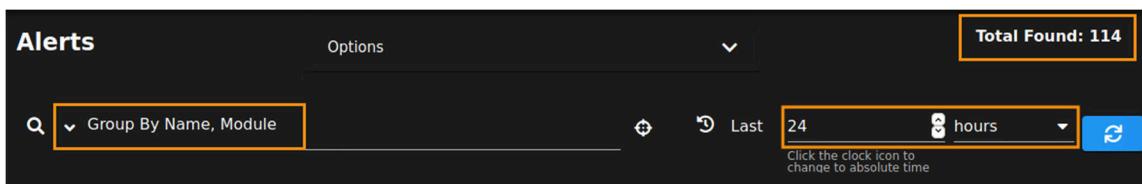
5. On the *Login* page, enter the *username* as `sysadmin@netlab.local` and the password as `NDGLabpass123!`. Click **LOGIN**.



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 **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

- 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.

	Count ▾	rule.name
	28	ET SCAN Possible Nmap User-Agent Observed
	28	ET SCAN Nmap Scripting Engine User-Agent D...
	8	ET SCAN Suspicious inbound to MySQL port 3...
	7	System Audit event.
	7	ET SCAN Suspicious inbound to PostgreSQL p...
	7	ET SCAN Suspicious inbound to Oracle SQL p...
	7	ET SCAN Suspicious inbound to MSSQL port 1...
	3	Listened ports status (netstat) changed (new)
	3	ET SCAN Potential SSH Scan OUTBOUND
	2	Successful sudo to ROOT executed.
	2	PAM: Login session opened.

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

	Timestamp ▾	rule.name	event.severity_label	source.ip	source.po
	2021-09-27 00:41:13.717 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54780
	2021-09-27 00:41:13.664 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54776
	2021-09-27 00:41:13.663 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54774
	2021-09-27 00:41:13.602 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54766
	2021-09-27 00:41:13.601 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54764
	2021-09-27 00:41:13.536 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54756
	2021-09-27 00:41:13.531 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54754

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.

▼	⚠	2021-09-27 00:41:13.717 -05:00	ET SCAN Possible Nmap User-Agent Observed	high
⌚	@timestamp	2021-09-27T05:41:13.717Z		
⌚	@version	1		
⌚	destination.ip	172.16.1.10		
⌚	destination.port	80		
⌚	ecs.version	1.8.0		
⌚	event.category	network		
⌚	event.dataset	alert		
⌚	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.

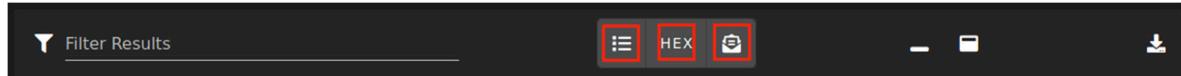
▼	⚠	2021-09-27 00:41:13.717 -05:00	ET SCAN Possible Nmap User-Agent Observed	high
⌚	@timestamp	2021-09-27T05:41:13.717Z		
⌚	@version	1		
⌚	destination.ip	172.16.1.10		
⌚	destination.port	80		
⌚	ecs.version	1.8.0		
⌚	event.category	network		
⌚	event.dataset	alert		
⌚	event.module	suricata		
⌚	event.severity	3		
⌚	event.severity_label	high		
⌚	host.name	seconion		
⌚	import.file	eve-2021-09-27-06:33.json		

Include
Exclude
Only
Group By
Clipboard
Actions
Hunt
Correlate
PCAP

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	66
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).

```

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

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Mon, 27 Sep 2021 05:37:22 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

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>

```

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	source.po
> 2021-09-27 00:41:13.717 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	203.0.113.2	54780
> 2021-09-27 00:41:13.664 -05:00	ET SCAN Possible Nmap User-Agent Observed	high		
> 2021-09-27 00:41:13.663 -05:00	ET SCAN Possible Nmap User-Agent Observed	high		
> 2021-09-27 00:41:13.602 -05:00	ET SCAN Possible Nmap User-Agent Observed	high		

A context menu is open over the first row, with the "Only" option highlighted with a red box. Other options include "Include", "Exclude", and "Group By".

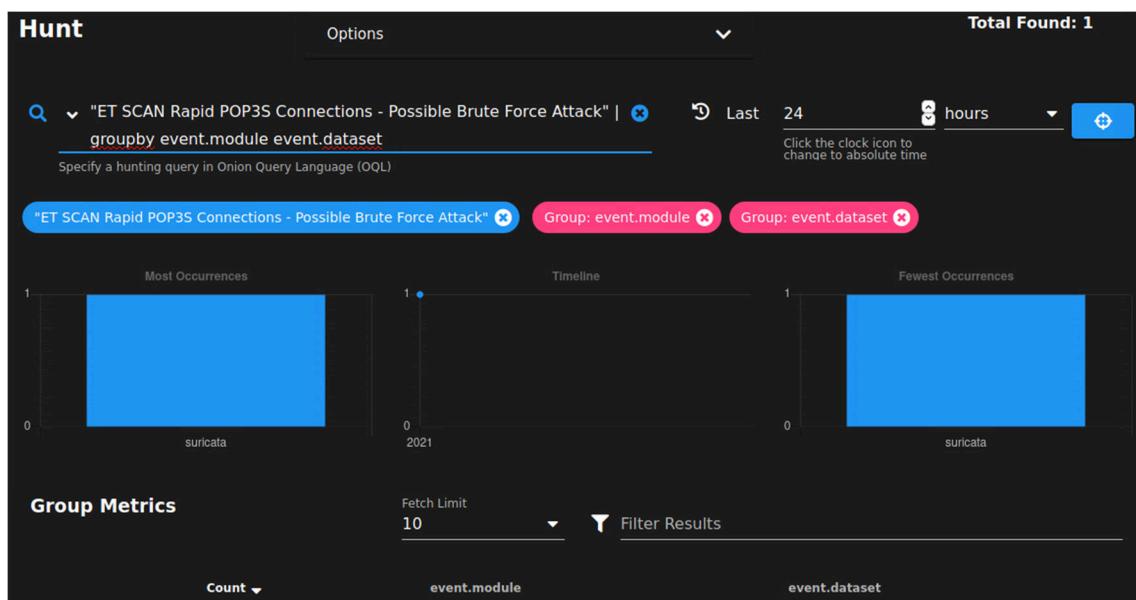
10. Now, we can see that 95 of the alerts are filtered, and they were all originated from the *Kali* VM. Feel free to scroll up and down to see the severity levels of those alerts.

Alerts		Options	Total Found: 95
Q	Custom	⊕ ⏳ 2021/09/26 10:16:37 AM - 2021/09/27 1	Choose the timespan to search, or click the calendar icon to switch to relative time
<input type="text" value="203.0.113.2"/> <span>×</span>			
Timestamp	rule.name	event.severity_label	
> 2021-09-27 00:41:21.064 -05:00	ET SCAN Rapid POP3S Connections - Possible Brute Force Attack	low	
> 2021-09-27 00:41:13.717 -05:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	
> 2021-09-27 00:41:13.717 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	
> 2021-09-27 00:41:13.664 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	
> 2021-09-27 00:41:13.664 -05:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	
> 2021-09-27 00:41:13.663 -05:00	ET SCAN Possible Nmap User-Agent Observed	high	
> 2021-09-27 00:41:13.663 -05:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	high	

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**.

Timestamp ▾	rule.name	event.severity_label
> <span style="color: yellow;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:21.064 -05:00	ET SCAN Rapid POP3S Connections - Possible Brute Force Attack	low
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.717 -05:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Sc	
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.717 -05:00	ET SCAN Possible Nmap User-Agent Observed	
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.664 -05:00	ET SCAN Possible Nmap User-Agent Observed	
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.664 -05:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Sc	
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.663 -05:00	ET SCAN Possible Nmap User-Agent Observed	
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.663 -05:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Sc	

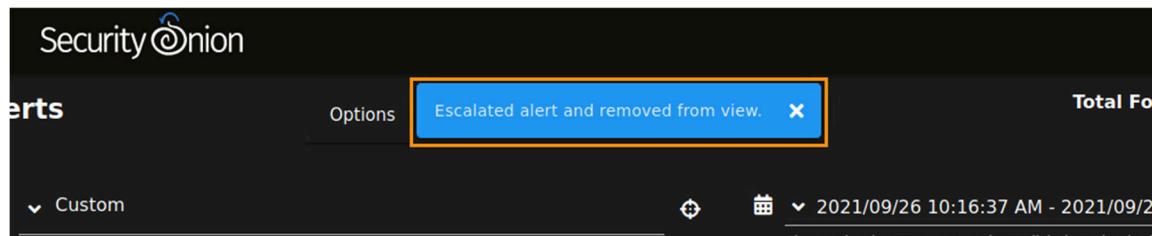
12. You will see the *Hunt* tool page as shown below. On this page, it will bring more details about this alert most of the time. *Hunt* is used to find similar events, track down malicious files, and observe malicious behaviors. We will not go into details about how to use *Hunt* in this lab.



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.

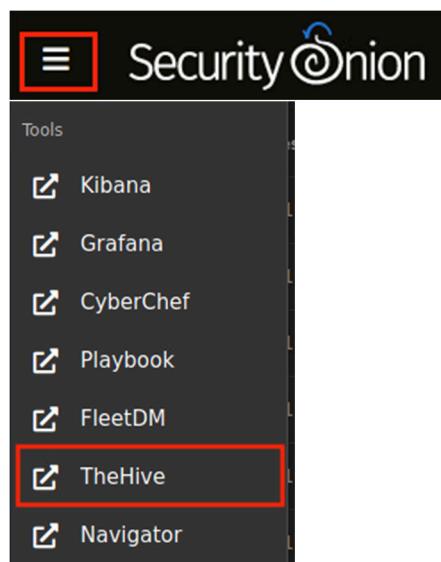
Timestamp ▾	rule.name	event.severity_label
> <span style="color: yellow;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:21.064 -05:00	ET SCAN Rapid POP3S Connections - Possible Brute Force Attack	low
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.717 -05:00	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Sc	high
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.717 -05:00	ET SCAN Possible Nmap User-Agent Observed	high
> <span style="color: red;">!</span> <span style="color: blue;">!</span> 2021-09-27 00:41:13.664 -05:00	ET SCAN Possible Nmap User-Agent Observed	high

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.

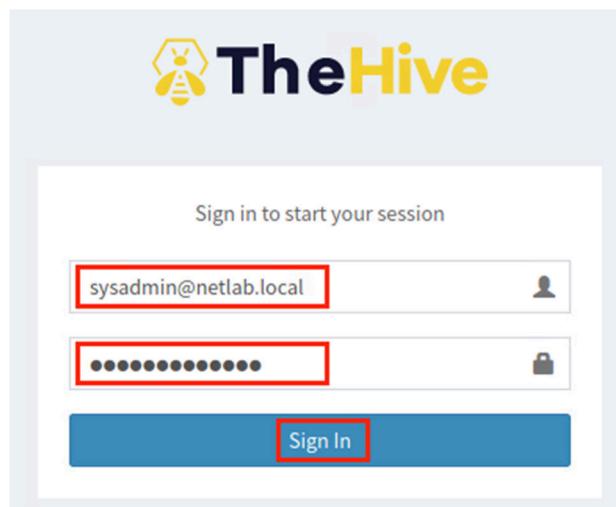


### 3.2 Add Observable and Tasks for Further Investigation

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.

List of cases (2 of 2)

Quick Filters ▾ Sort by ▾ Stats Filters 15 per page

1 filter(s) applied: status: Open × Clear filters

Title	Severity	Tasks	Observables	Assignee	Date	Actions
#2 - ET SCAN Rapid POP3S Connections - Possible Brute Force Attack  SecurityOnion	L	No Tasks	0	S	09/27/21 15:09	
#1 - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)  SecurityOnion	H	No Tasks	0	S	09/27/21 14:55	

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

#2 - ET SCAN Rapid POP3S Connections - Possible Brute Force Attack  SecurityOnion	L	No Tasks	0	S	09/27/21 15:09	
#1 - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)  SecurityOnion	H	No Tasks	0	S	09/27/21 14:55	

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

Case #1 - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)

Created by sysadmin@netlab.local Mon, Sep 27th, 2021 14:55 -05:00

Details Tasks 0 Observables 0

**Summary**

**Title**  
ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)

**Severity**   
**TLP**   
**PAP**   
**Assignee** sysadmin@netlab.local  
**Date** Mon, Sep 27th, 2021 14:55 -05:00  
**Tags** SecurityOnion

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.

The screenshot shows a software interface for managing network alerts. At the top, there's a header bar with a red 'H' icon, the text 'Case # 1 - ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)', and several action buttons: 'Close', 'Flag', 'Merge' (which is highlighted with a red box), 'Remove', and 'Responders'. Below the header are three tabs: 'Details' (selected), 'Tasks' (0), and 'Observables' (0). The main content area displays the alert details.

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.

The screenshot shows a 'Merge Case #1' dialog box. It has two radio buttons: 'By Title' (unchecked) and 'By Number' (checked, marked with a red circle 1). Below the radio buttons is a search input field containing '#2 - ET SCAN Rapid POP3S Connections - Possible Brute Force Attack' (marked with a red box 2). Underneath the input field, there's a message: 'Please search for the case to be merged with:' followed by the alert title '#1: ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)'. At the bottom right is a 'Merge' button (highlighted with a red box 3).

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

The screenshot shows the 'Merge Case #1' dialog box again, but now the 'Merge' button is visible and highlighted with a red box. The alert details for '#2 - ET SCAN Rapid POP3S Connections - Possible Brute Force Attack' are displayed, including the JSON payload:

```
{"timestamp": "2021-09-27T05:41:21.064176+0000", "flow_id": "809102472721468", "pcap_cnt": 17799, "event_type": "alert", "src_ip": "203.0.113.2", "src_port": 56214, "dest_ip": "172.16.1.10", "dest_port": 995, "proto": "TCP", "community_id": "1:fIK9cHo784iZfx66HddW6YPM=", "alert": {"action": "allow ed", "gid": 1, "signature_id": 2002993, "rev": 7, "signature": "ET SCAN Rapid POP3S Connections - Possible Brute Force Attack"}, "category": "Misc activity", "severity": 3, "metadata": {"created_at": ["2010_07_30"], "updated_at": ["2010_07_30"]}, "rule": "alert tcp $EXTERNAL_NET any -> SHOME_NET 995 (msg:\'ET SCAN Rapid POP3S Connections - Possible Brute Force Attack\'); flow:to_server; flags: S,12; threshold: type both, track_by_src, count 30, seconds 120; reference:url,doc.emergingthreats.net/2002993; classtype:misc-activity; sid:2002993; rev:7; metadata:created_at 2010_07_30, updated_at 2010_07_30;"}, "payload_hex": "KAC+vDpSwAAgQFtAQCCApC/QF2AAAAAEDAwc=", "packet_info": {"linktype": 1}}
```

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

The screenshot shows a merged alert titled "Case #3 - #1:ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) / #2:ET SCAN Rapid POP3S Connections - Possible Brute Force Attack". The alert was created by sysadmin@netlab.local on Mon, Sep 27th, 2021 20:29 -05:00. The "Title" field contains the merged alert text, which is highlighted with a red box.

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

The screenshot shows the "Description" section of the alert. An edit button (pencil icon) is highlighted with a red box. The text in the description area is: "ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) (#1)". Below the text is some JSON log data.

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.

The screenshot shows the "Description" section with a note added: "Case #1 & #2 were merged due to same source ip addresses." This note is highlighted with a red box. Below the note is the merged alert text and JSON log data. A save button (checkmark icon) is highlighted with a red box at the bottom left of the editor.

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)**.

The screenshot shows the "Observables" tab selected. A "Add observable(s)" button is highlighted with a red box at the bottom left of the toolbar.

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.

**Create new observable(s)**

Type *	<input type="text" value="ip"/>
Value *	<input type="text" value="203.0.113.2"/>
<input checked="" type="radio"/> One observable per line (1 unique observable) <input type="radio"/> One single multiline observable	
TLP *	<input type="button" value="WHITE"/> <input type="button" value="GREEN"/> <input type="button" value="AMBER"/> <input type="button" value="RED"/>
Is IOC	<input type="checkbox"/>
Has been sighted	<input checked="" type="checkbox"/>
Tags **	<input type="text" value="nmap"/> <input type="button" value="Add tags"/>
Description **	<input type="text" value="if this is not a penetration testing contractor, it could be a malicious external ip address"/>

\* Required field \*\* At least, one required field

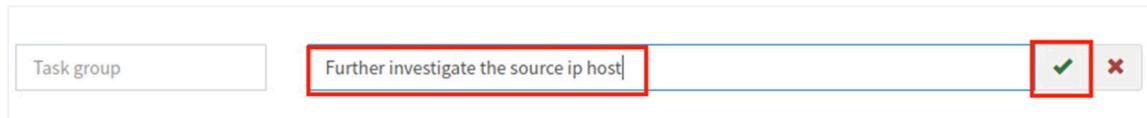


An observable is an extra piece of information we can add to aid the security team for further investigation.

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

The screenshot shows a navigation bar with three tabs: 'Details', 'Tasks (0)', and 'Observables (1)'. Below the tabs are two buttons: '+ Add Task' (highlighted with a red box) and 'Show Groups'. There is also a 'Filter' input field.

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.

Group	Task	Date	Assignee	Actions
default	Further investigate the source ip host		Not assigned	▶ Start ⚙

### 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.

Group	Task	Date	Assignee	Actions
default	Further investigate the source ip host		Not assigned	▶ Start ⚙

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.

Task logs

Markdown Reference

**Add log**

After receiving the confirmation from the CISO, the source ip host is a penetration testing contractor. |

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

Basic Information

**Close**

Title	Further investigate the source ip host	Date	Mon, Sep 27th, 2021 21:20 -05:00
Group	default	Duration	Started 11 minutes ago

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

**Tasks**

Group	Task	Date	Assignee	Actions
✓ default	Further investigate the source ip host Closed after 7 minutes	Mon, Sep 27th, 2021 21:20 -05:00	sysadmin@netlab.local	<b>Reopen</b>

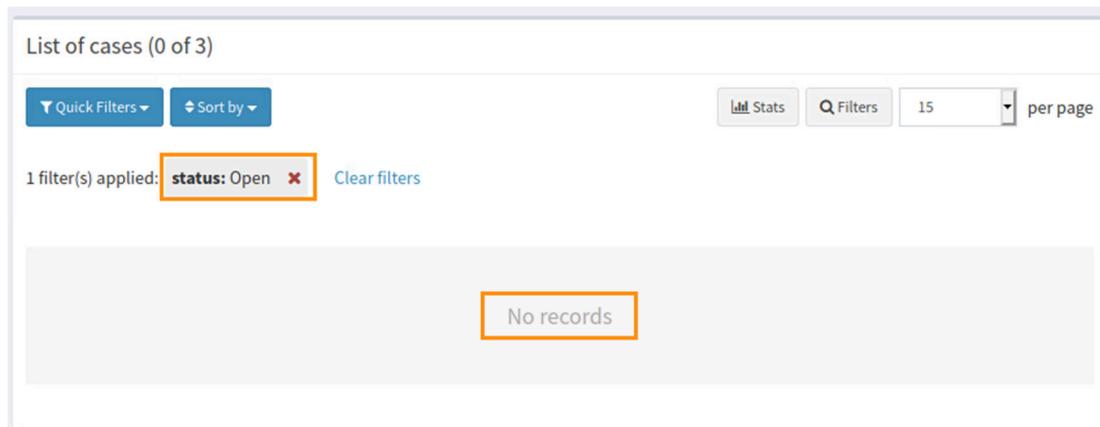
6. Since this case is solved, we can now close it. Click the **Close** button at the top.

The screenshot shows a 'Case #3 - #1:ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) / #2:ET SCAN Rapid POP3S Connections - Possible Brute Force Attack' window. At the top right, there is a 'Close' button with a red box around it. Below the title bar are tabs for 'Details', 'Tasks' (with 1 notification), and 'Observables' (with 1 notification). There are also buttons for '+ Add Task', 'Show Groups', and a 'Filter' search bar. The main area contains the case details.

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

The 'Close Case #3' dialog box has a blue header. A red banner at the top asks 'You are about to close Case #3. Are you sure you want to continue?'. Below it, the 'Status' field is set to 'True Positive' (highlighted with a red box). A note says 'Investigation clearly demonstrates that there is something malicious (scam, phishing, malspam, malware, cybersquatting...)'. The 'Impact' field is set to 'No' (highlighted with a red box). A note says 'Security measures blocked the attack or infection'. The 'Summary' field contains the text 'Penetration testing contractor was doing their job, our system successfully detected the threat. Case closed.' (highlighted with a red box). At the bottom, there are 'Cancel' and 'Close case' buttons, with 'Close case' highlighted with a red box.

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



The screenshot shows a web-based application interface titled "List of cases (0 of 3)". At the top, there are several navigation and filtering options: "Quick Filters", "Sort by", "Stats", "Filters", a dropdown for "per page" set to 15, and a "Clear filters" link. Below these, a message indicates "1 filter(s) applied: status: Open" with a red "X" button to clear it. The main content area displays a large gray box with the text "No records".

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