

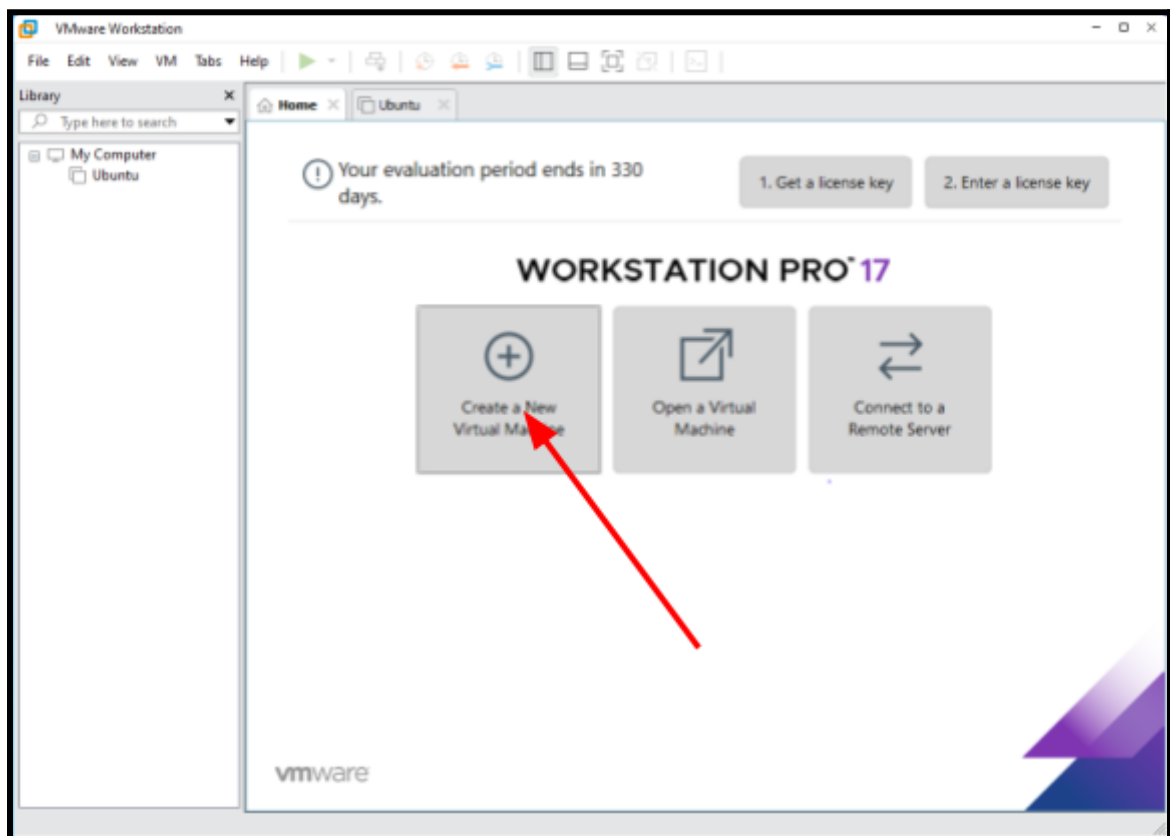
## Task 2: Installing Security Onion VM

### 1. Download Security Onion image file

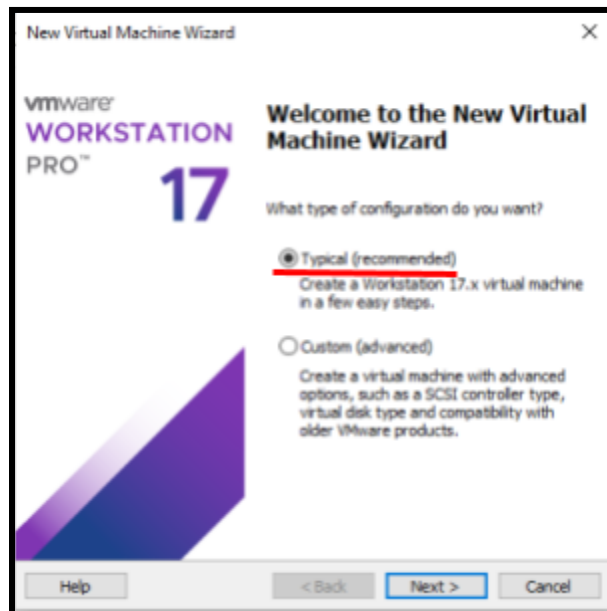
- 1.1. Download Security Onion image file from the link below and save it in the [D:\CID\_2023\TeamX\Downloads] path.  
<https://download.securityonion.net/file/securityonion/securityonion-2.3.220-20230301.iso>

### 2. Install the Security Onion on VMware

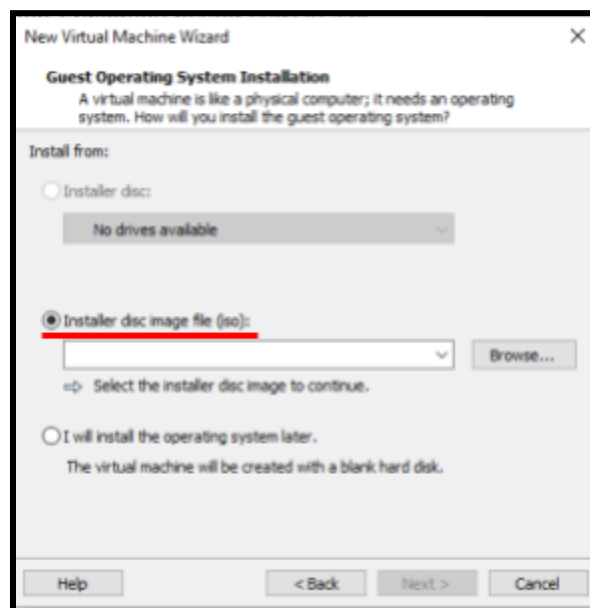
- 2.1. When you open the VMware, you should be able to see the [VMware workstation] as below. Click [Create a New Virtual Machine]



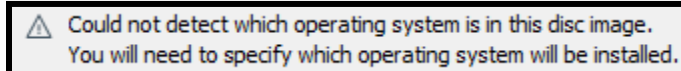
- 2.2. Select **[Typical (recommended)]** then click on **[Next]**



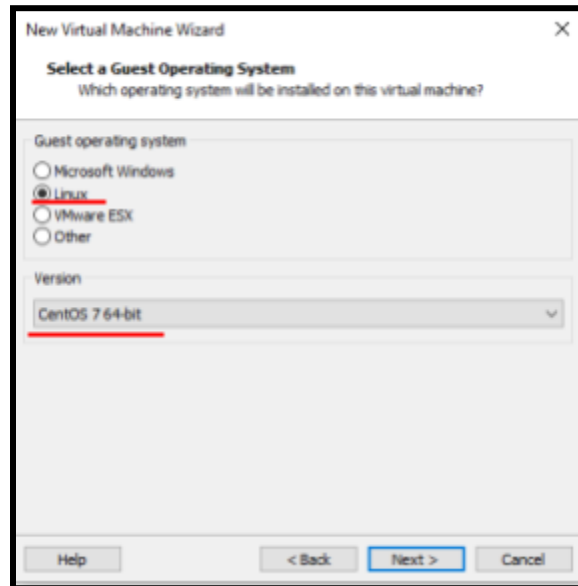
- 2.3. Click on **[Installer disc image file (iso)]**. Then click on **[Browse...]** and select Security Onion image file (.iso file).



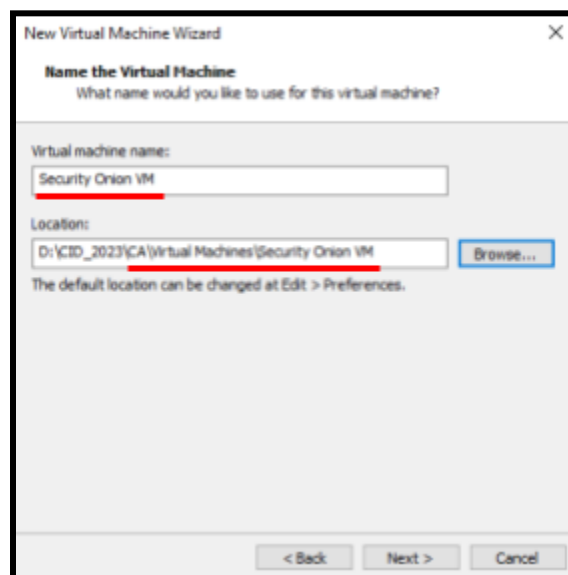
- 2.4. If you encounter the alert **[Could not detect which operating...]**, ignore it and proceed to the next step by clicking on **[Next]**



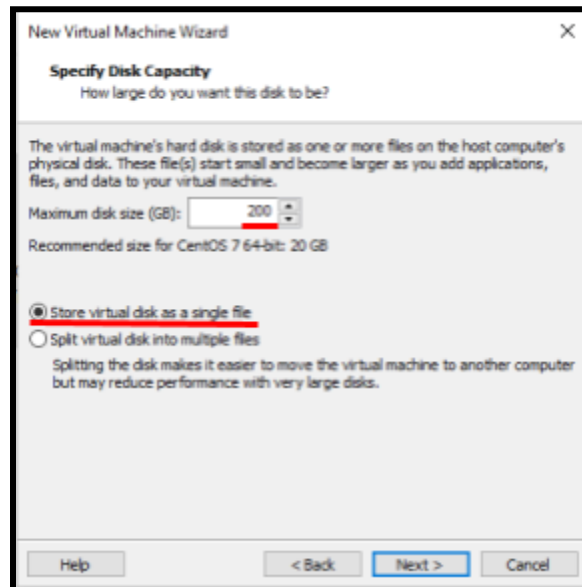
- 2.5. For the **[Guest operating system]** field, choose **[Linux]**. For the **[Version]** field, choose **[CentOS 7 64-bit]**



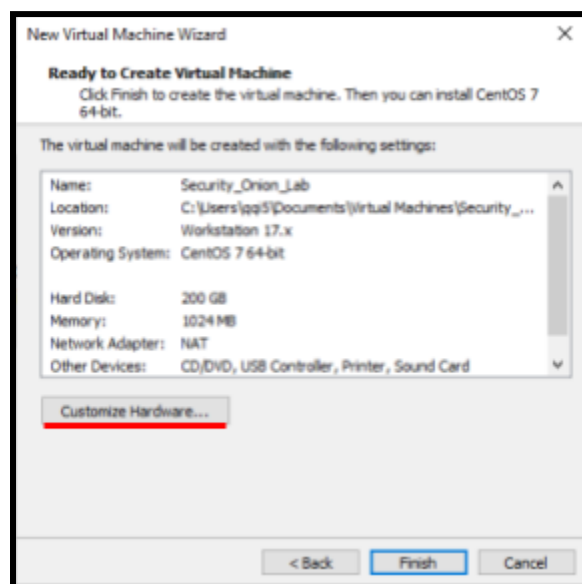
- 2.6. Set the Virtual Machine name as: **[Security Onion VM]**  
Specify the location as: **[D:\CID\_2023\TeamX\Virtual Machines\Security Onion VM]**. Then Click **[Next]**



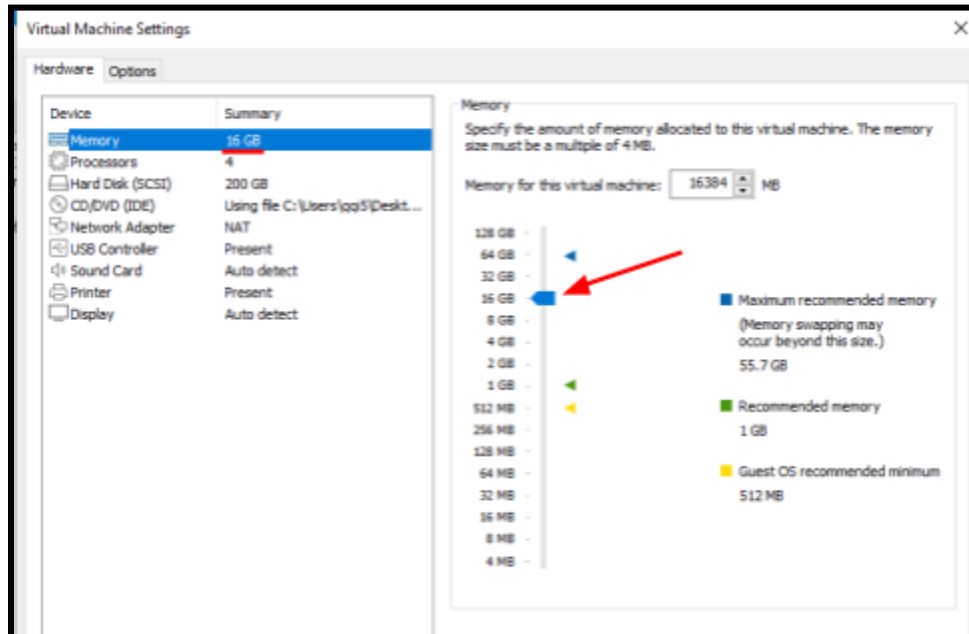
- 2.7. Change the **[Maximum disk size (GB)]** to be **[200 GB]** since the minimum requirement of Security Onion is 200 GB. Then select the option **[Store virtual disk as a single file.]**



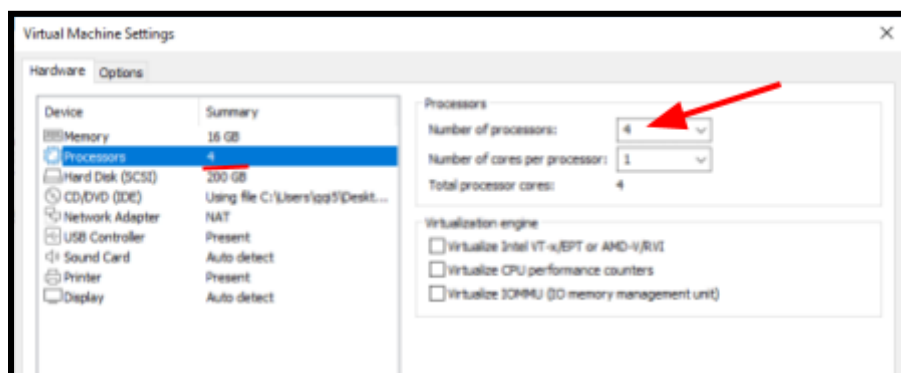
- 2.8. Click on **[Customize Hardware...]** to modify some of the settings based on the minimum hardware requirement for Security Onion. The minimum requirements for running Security Onion are: 12GB RAM, 4 CPU cores and 200GB storage.



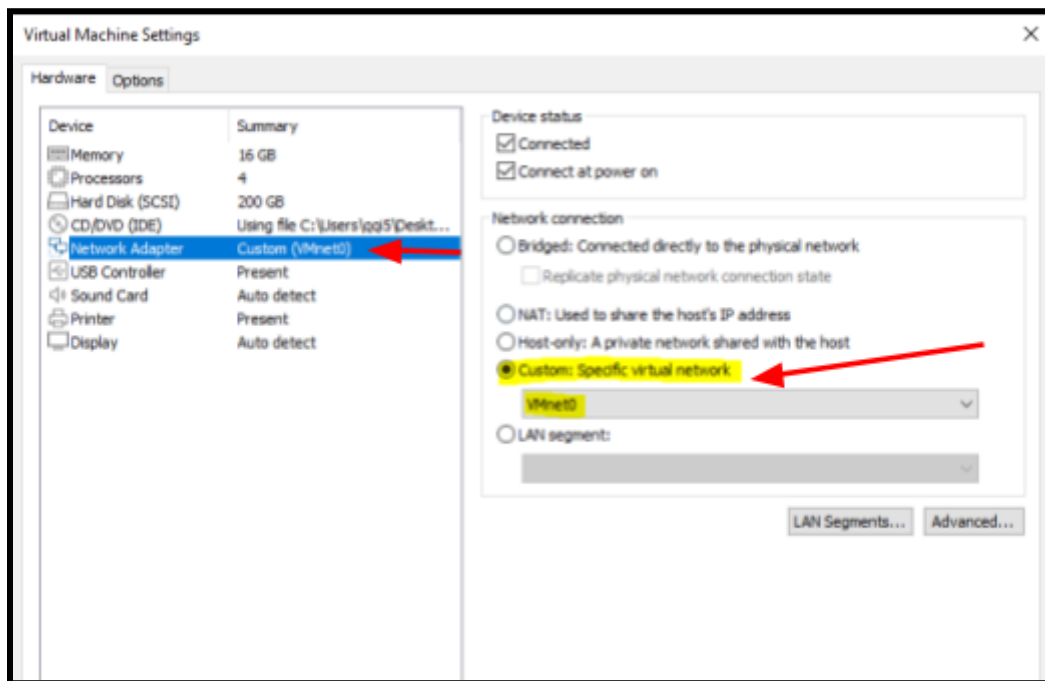
2.9. Modify the **[Memory]** to **[16 GB]**.



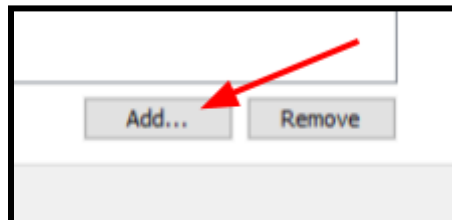
2.10. Modify the number of **[Processors]** to **4**.



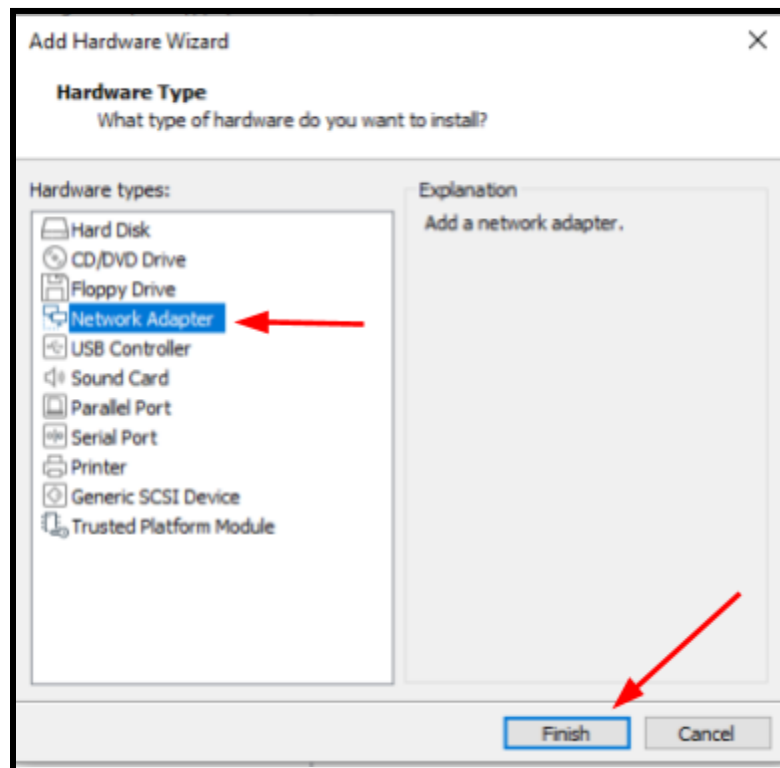
- 2.11. Change the type of the first network adapter to **Custom** and select **VMnet0** network.



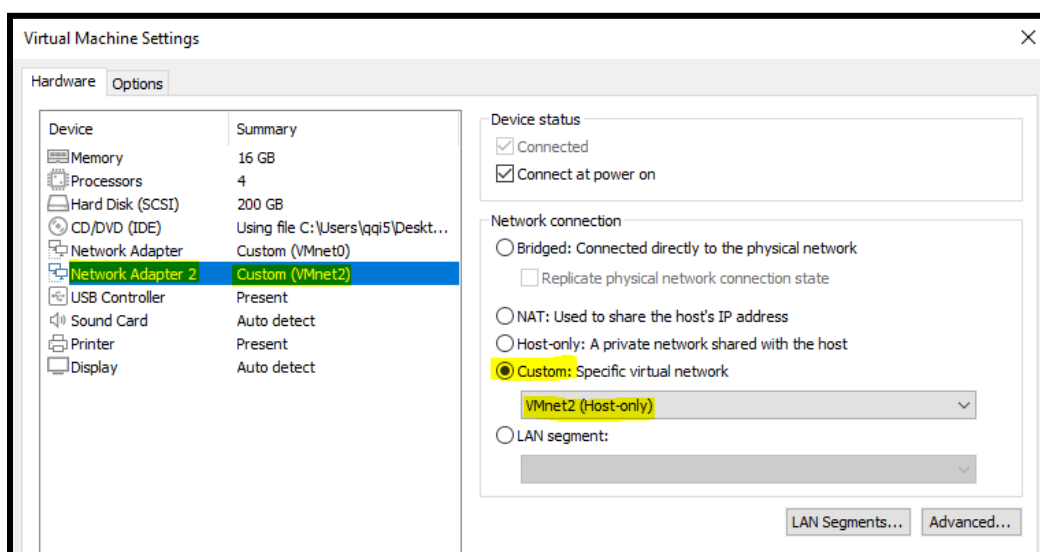
- 2.12. Click on **Add...** to add an additional **Network Adapter**.



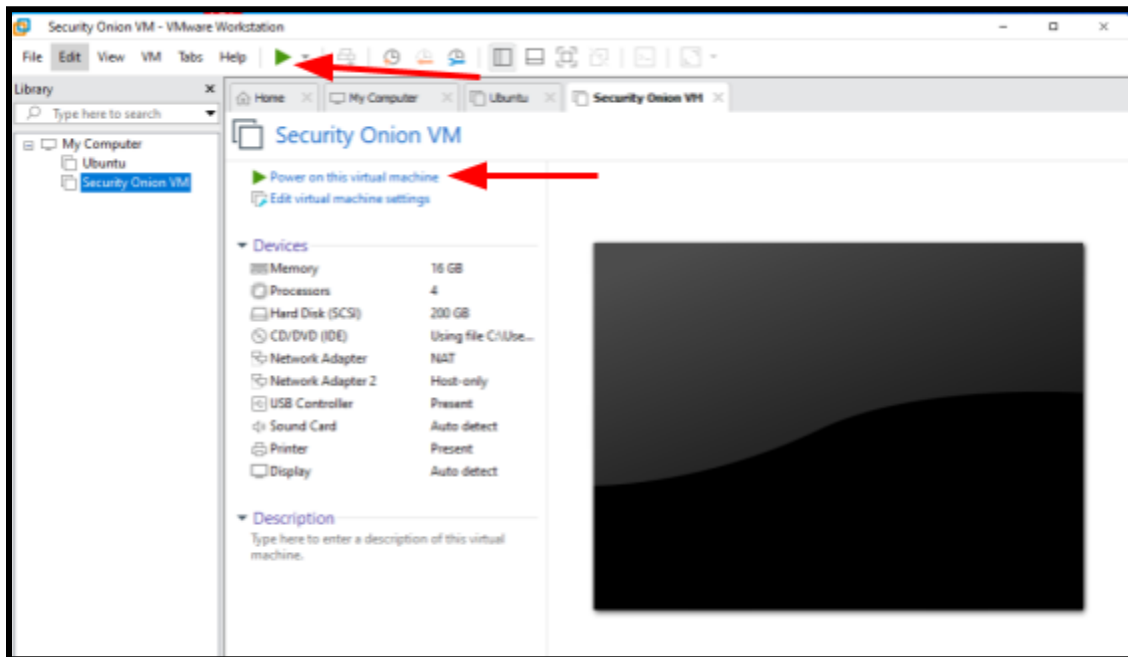
2.13. Add an additional **[Network Adapter]** then click **[Finish]**



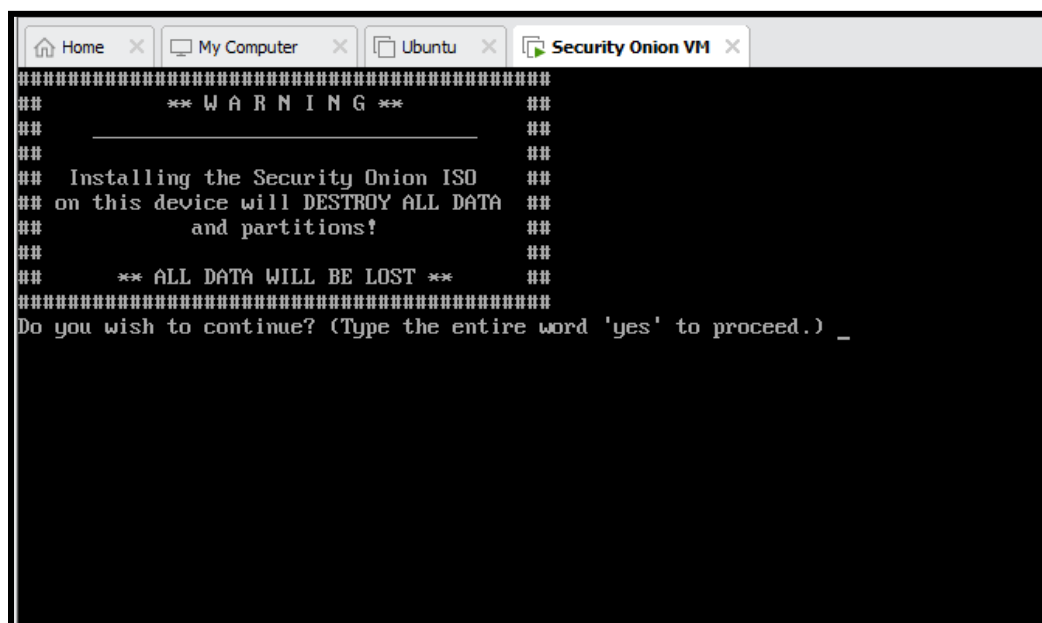
2.14. Modify the **[Network Connection]** type to be **[Custom]** and select **[VMnet2]** then click on **[OK]**



2.15. Now run the Security Onion VM



2.16. Wait until you get the following window.



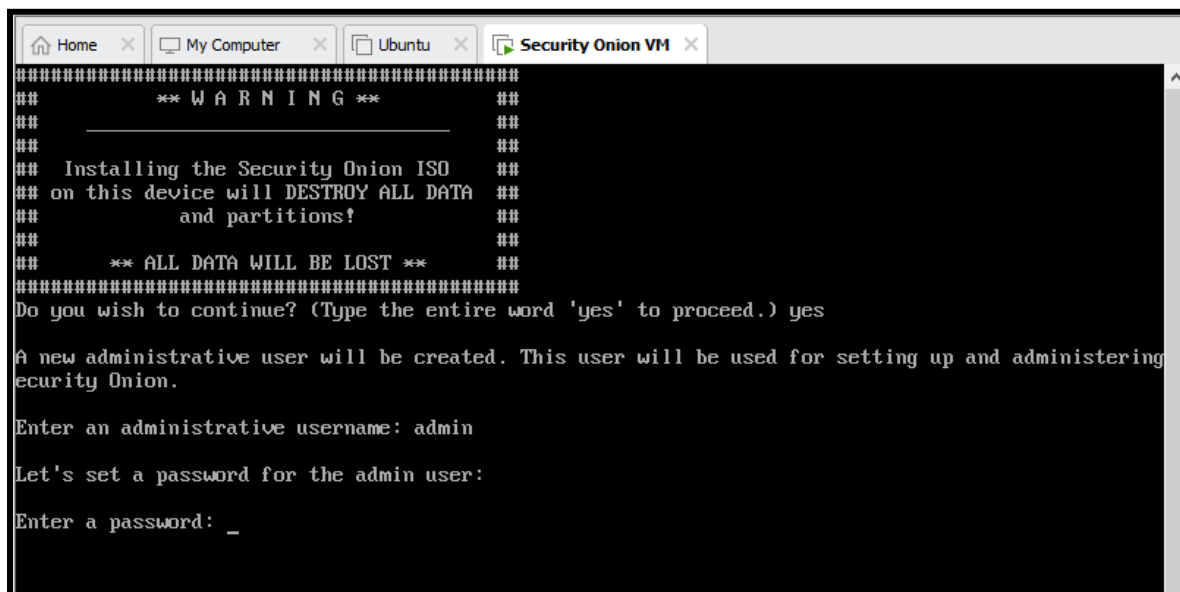


2.17. Type **[yes]** and press the **[Enter Key]**

2.18. You will be asked to set up an administrative account. We recommend you use the following:

**Username: admin**

**Password: admin**



```
#####
##                               ##
##  *** W A R N I N G ***       ##
##                               ##
##  Installing the Security Onion ISO  ##
##  on this device will DESTROY ALL DATA  ##
##  and partitions!                ##
##                               ##
##  *** ALL DATA WILL BE LOST ***      ##
##                               ##
#####
Do you wish to continue? (Type the entire word 'yes' to proceed.) yes

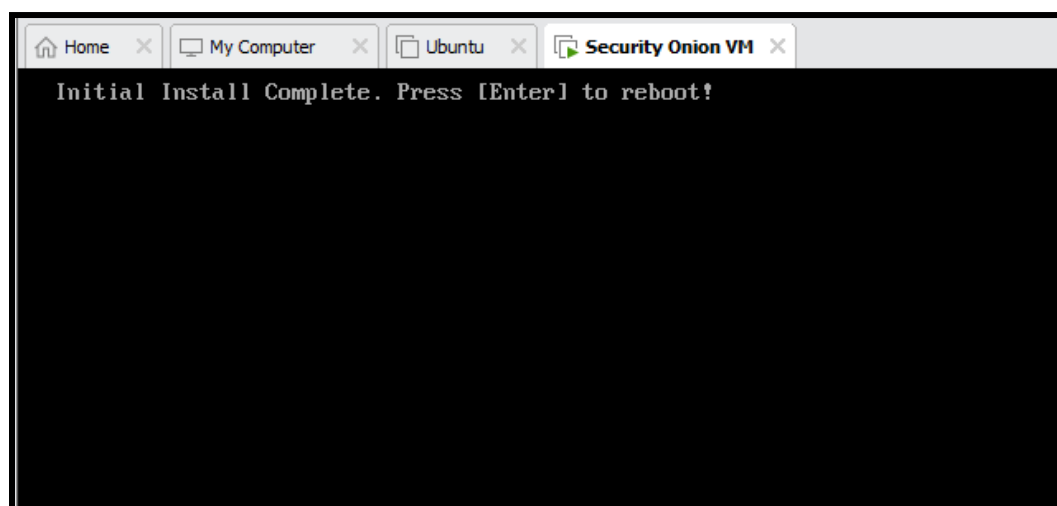
A new administrative user will be created. This user will be used for setting up and administering
ecurity Onion.

Enter an administrative username: admin

Let's set a password for the admin user:

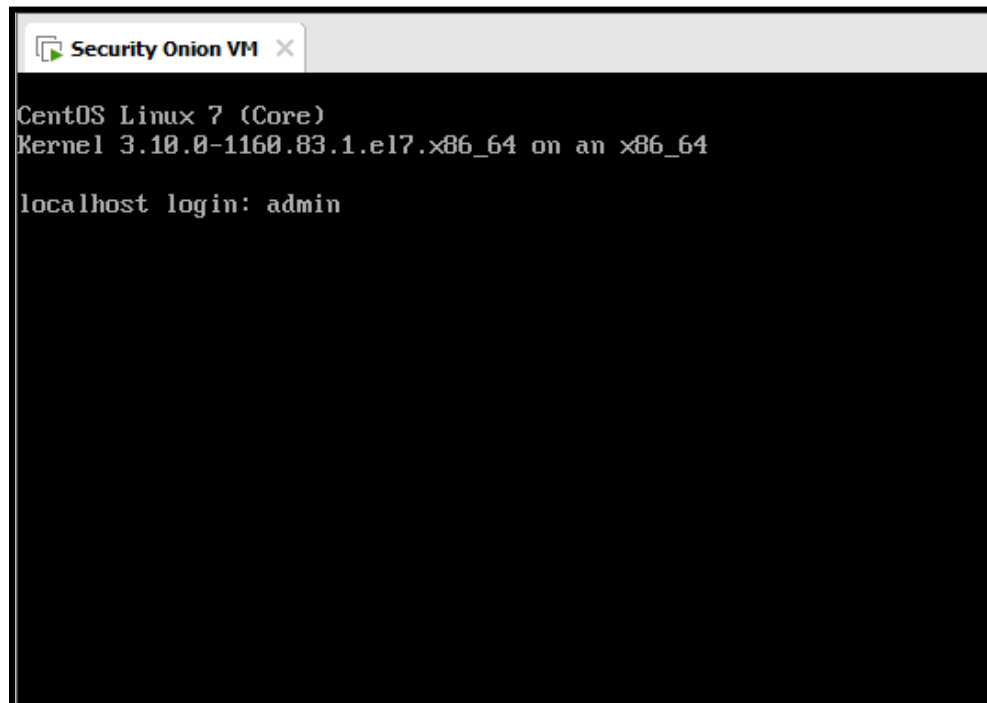
Enter a password: _
```

2.19. Then once the initial installation phase finishes, you will get the following message that asks you to press the **[Enter Key]** to reboot the VM.



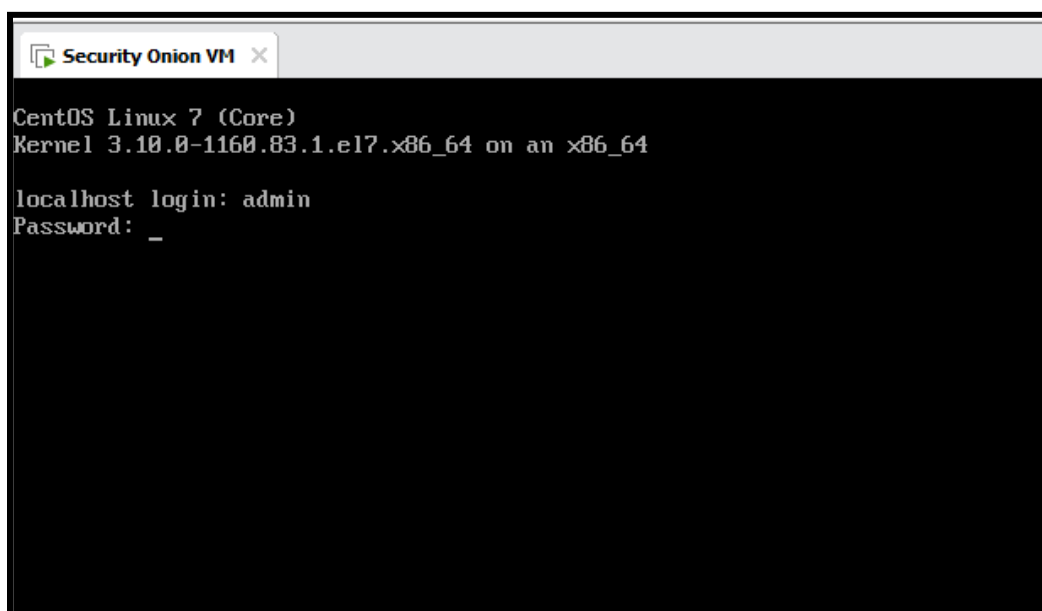
```
Initial Install Complete. Press [Enter] to reboot!
```

- 2.20. After the VM reboots you will be asked to provide the localhost login information, which we have setup previously. Enter the username **[admin]** press the **[Enter Key]**



The screenshot shows a terminal window titled "Security Onion VM". The text inside the terminal reads: "CentOS Linux 7 (Core)", "Kernel 3.10.0-1160.83.1.el7.x86\_64 on an x86\_64", and "localhost login: admin".

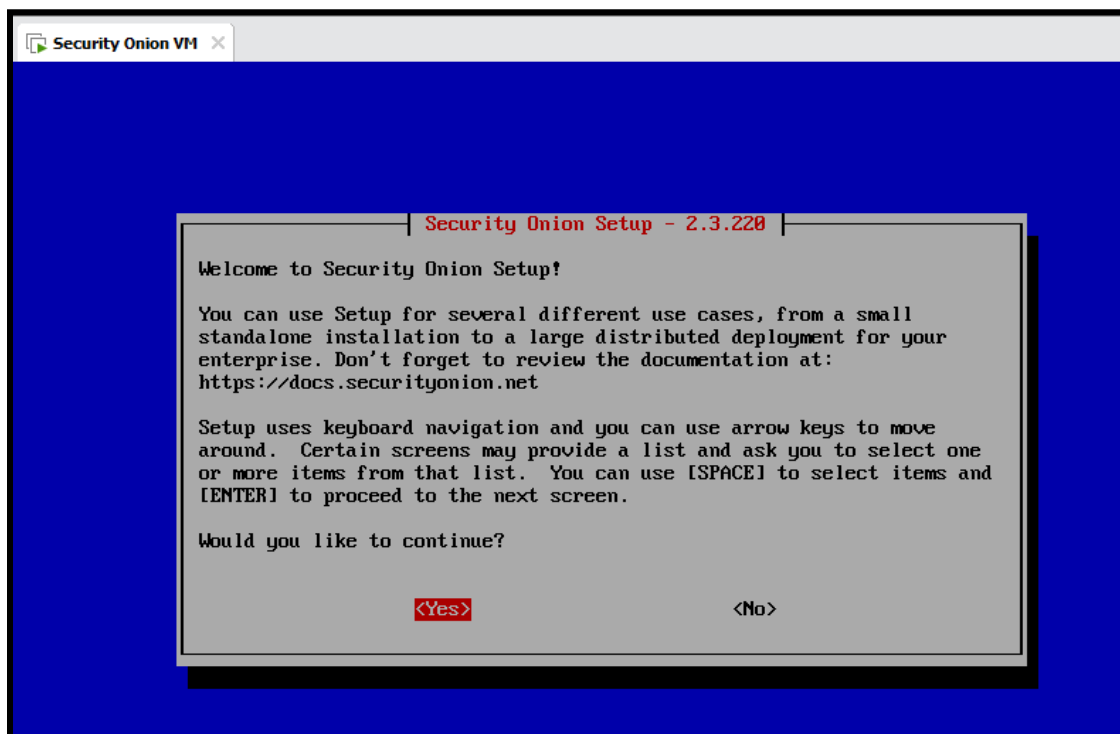
- 2.21. Enter your password **[admin]** and press the **[Enter Key]**



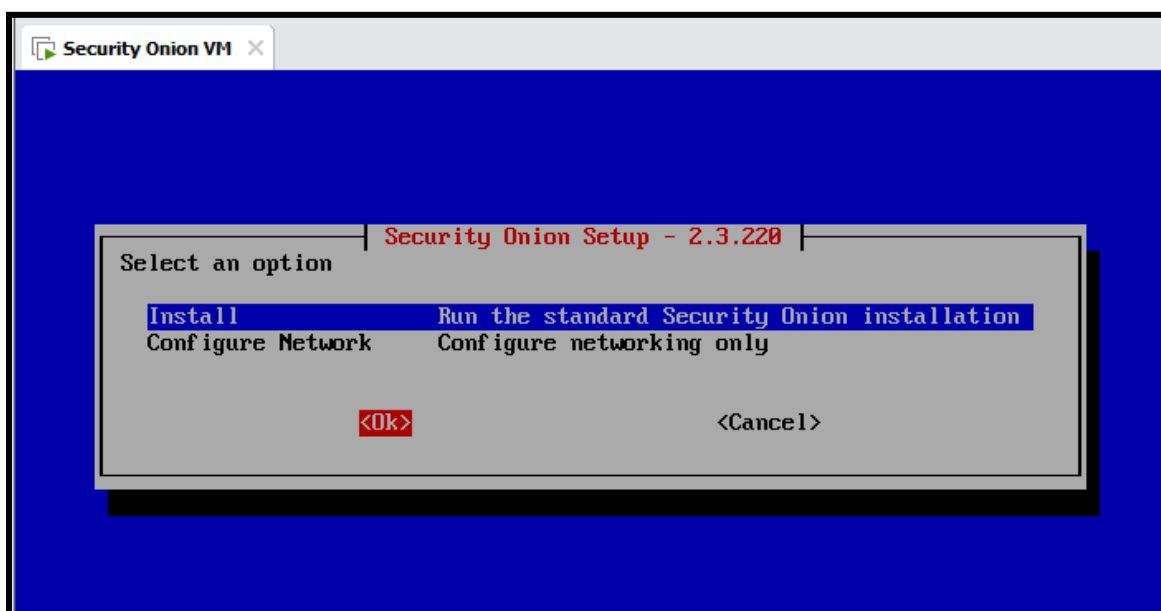
The screenshot shows the same terminal window as before. The text now includes "localhost login: admin" and "Password: \_", where the underscore represents the password being entered.

Now we will begin the configuration process of Security Onion VM

2.22. Choose [**Yes**] and press [**Enter**]

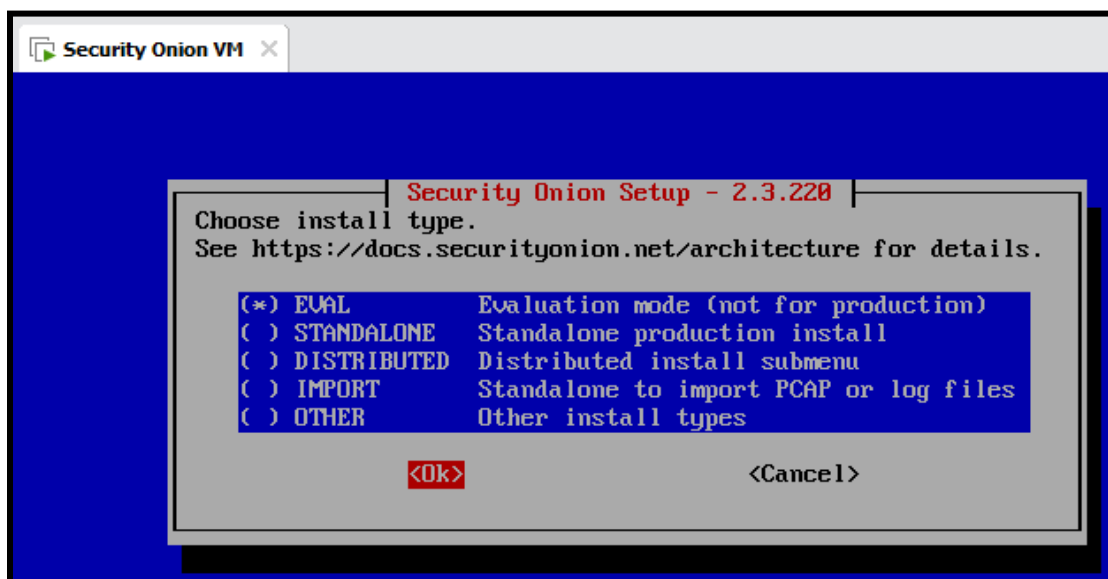


2.23. Choose [**Install**] option then press the [**Tap Key**] on your keyboard followed by the [**Enter Key**]

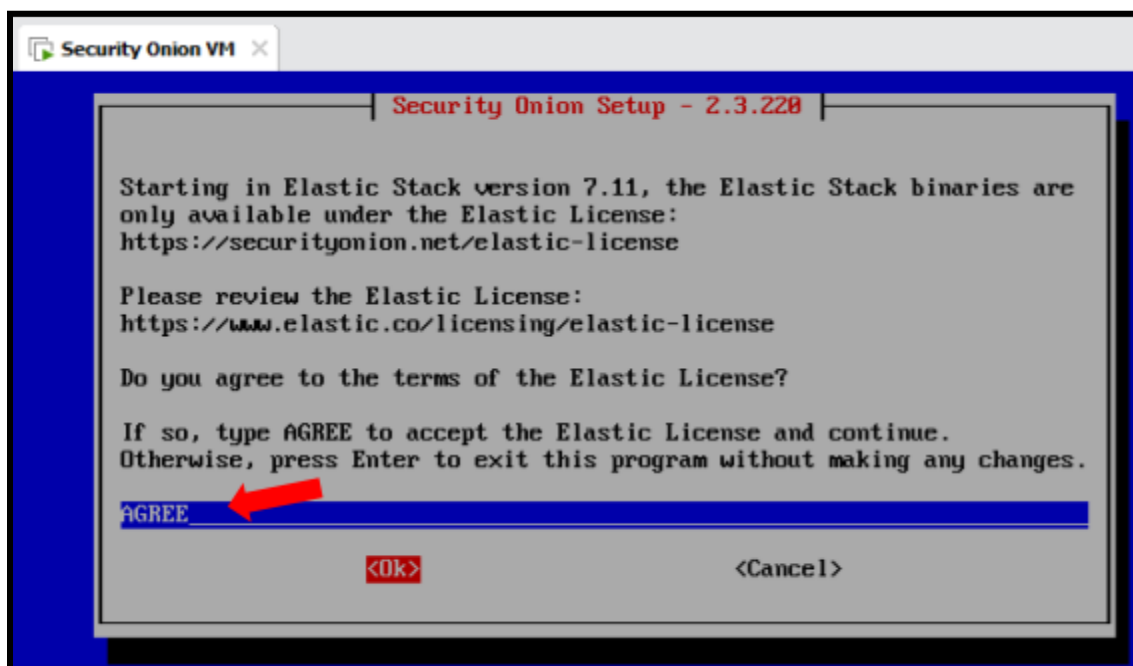


There are different modes of installation for Security Onion. For our lab environment we will use the **Evaluation Mode**. This mode is designed for a classroom or small lab environment. If you are interested in knowing more about the different installation modes of Security Onion refer to this [page](#) in Security Onion documentation.

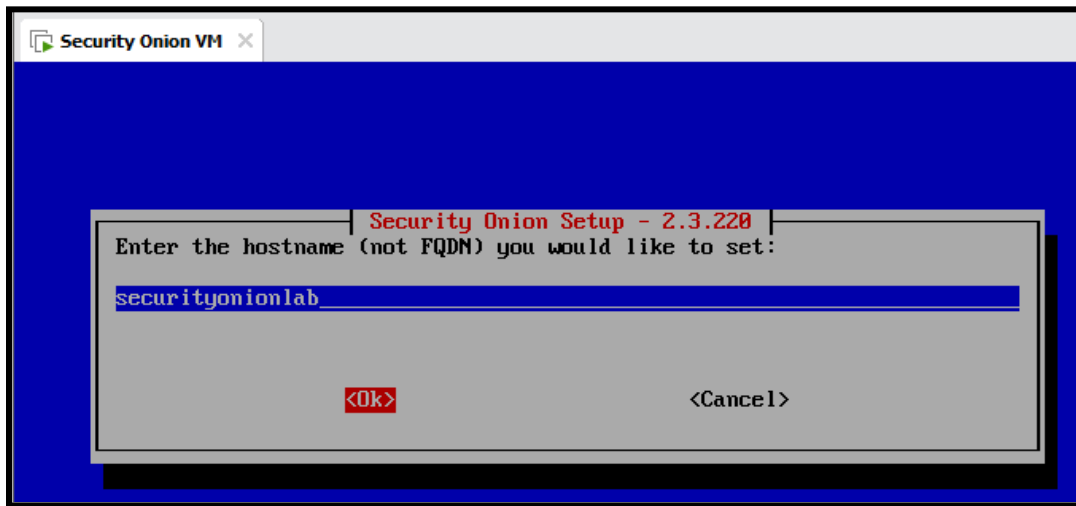
2.24. Choose [**Eval**] option and press the [**Tap key**], then press [**Enter**]



2.25. Type [**AGREE**] on the blue line. Then press the [**Tap Key**] followed by [**Enter Key**]

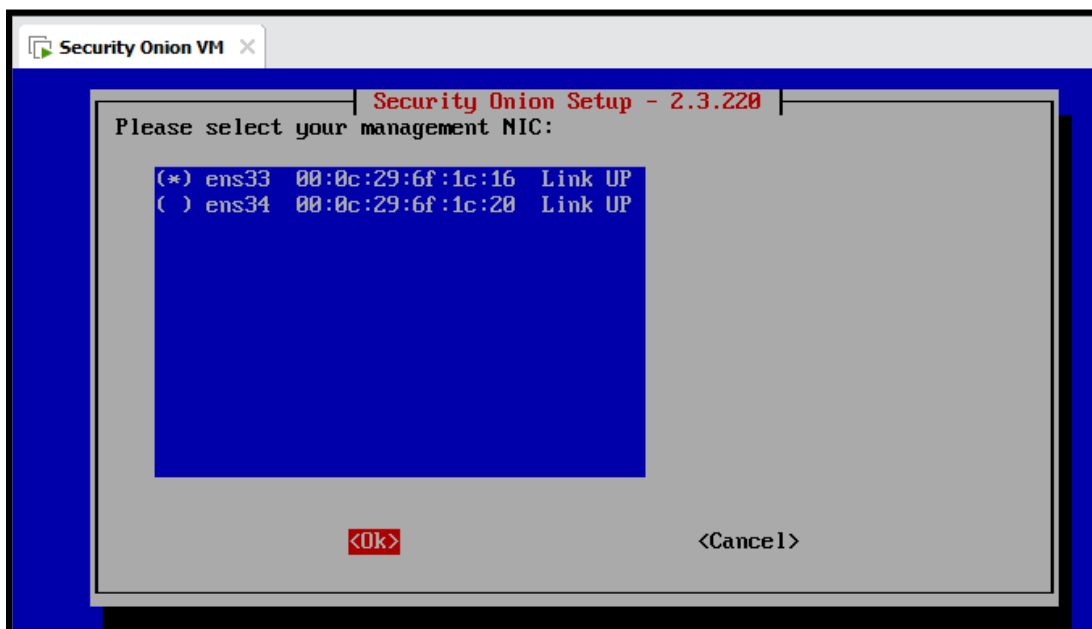


- 2.26. Change the hostname to **[securityonionlab]** then press the **[Tap Key]** followed by the **[Enter Key]**

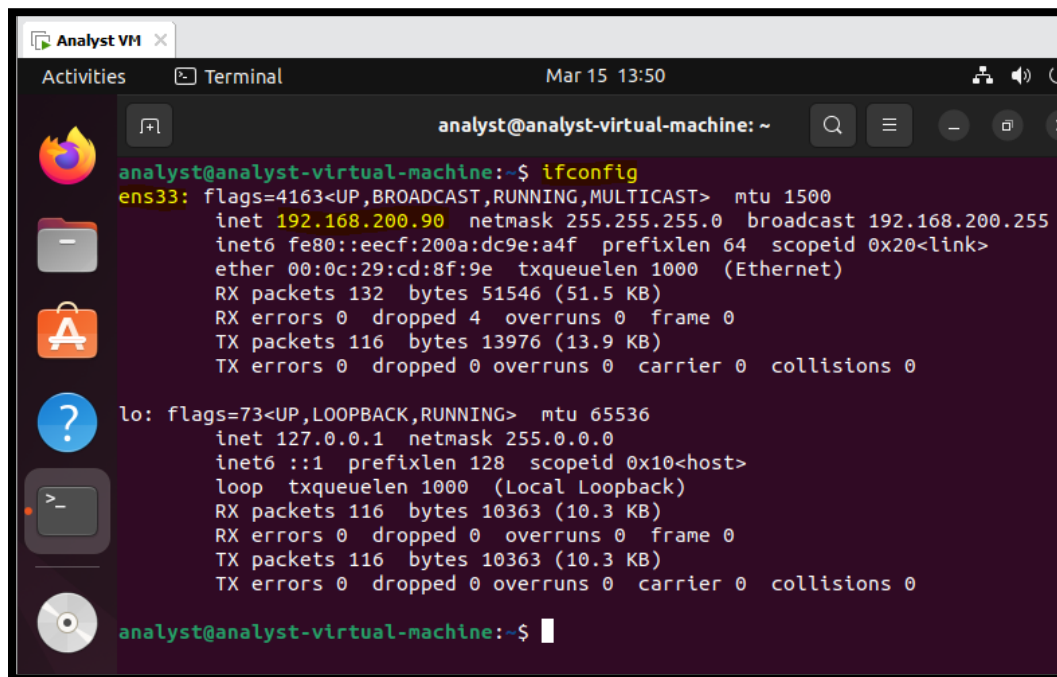


The following section is the most important part of the configuration process. If you could not complete this section correctly, you will have to reinstall the Security Onion VM from scratch.

- 2.27. As you can see from the picture below you are asked to identify the Management NIC. Since we have connected the Security Onion VM to two networks (VMnet0 and VMnet2), we see two network interfaces **[ens33]** and **[ens34]**. Your machine may show different names than those shown here.



In the first document of this lab [Importing the Analyst VM.pdf] in step [4.3], you were asked to connect the Analyst VM to [VMnet0] which is the *Management Network*. As shown in the picture below, when we used [ifconfig] in the analyst VM we were given the IP address of the Analyst VM in the management network as [192.168.200.90]. Also, we were given the Interface of the Management Network as: [ens33].

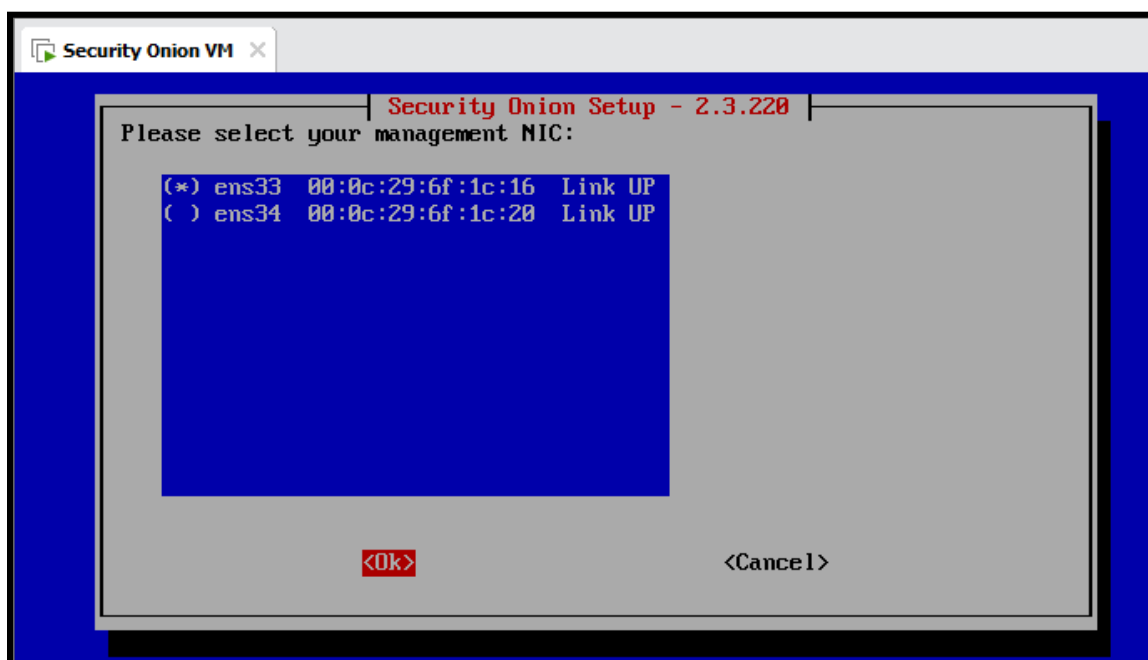


```
analyst@analyst-virtual-machine: ~  
analyst@analyst-virtual-machine:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.200.90  netmask 255.255.255.0  broadcast 192.168.200.255  
    inet6 fe80::eecf:200a:dc9e:a4f  prefixlen 64  scopeid 0x20<link>  
    ether 00:0c:29:cd:8f:9e  txqueuelen 1000  (Ethernet)  
    RX packets 132  bytes 51546 (51.5 KB)  
    RX errors 0  dropped 4  overruns 0  frame 0  
    TX packets 116  bytes 13976 (13.9 KB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
    inet 127.0.0.1  netmask 255.0.0.0  
    inet6 ::1  prefixlen 128  scopeid 0x10<host>  
    loop txqueuelen 1000  (Local Loopback)  
    RX packets 116  bytes 10363 (10.3 KB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 116  bytes 10363 (10.3 KB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
analyst@analyst-virtual-machine:~$
```

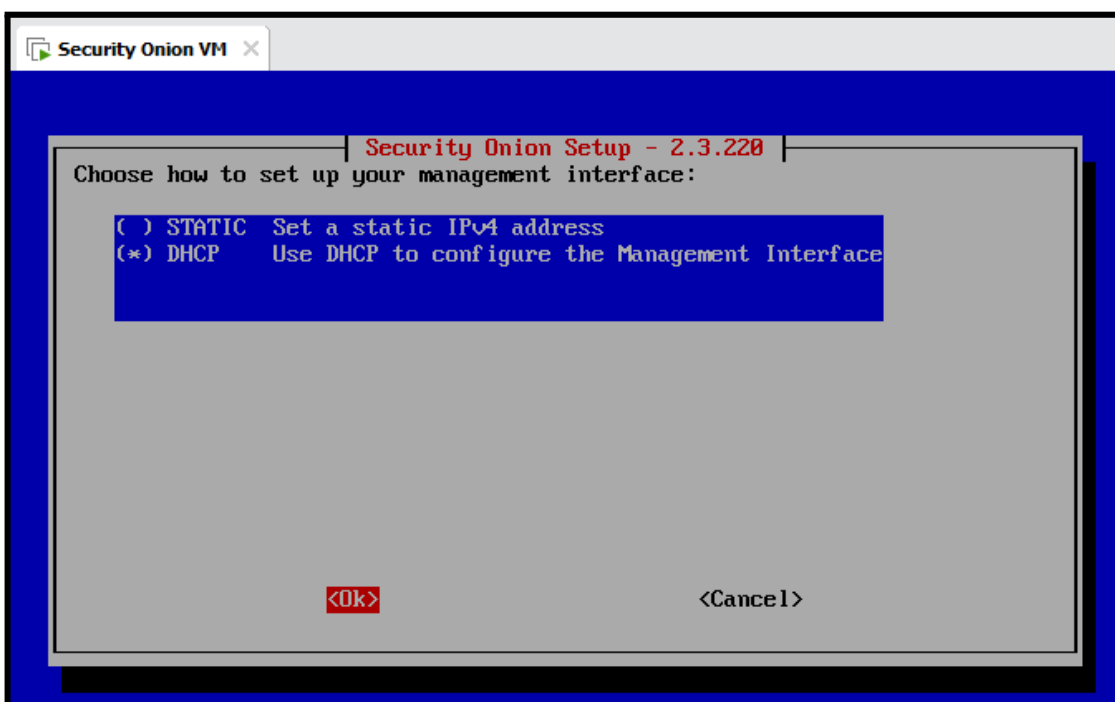
However, based on that information we are able to identify the interface [ens33] as the *Management Network Interface*. Therefore, we return to Security Onion VM and specify [ens33] as the *Management NIC*.

The name of the management interface may not be the same in your environment setup. You are required to fully understand the network setup (refer to the GitHub page of this lab). Additionally, you are required to correctly identify the interface for the *Management Network* and for the *Mentoring Network*.

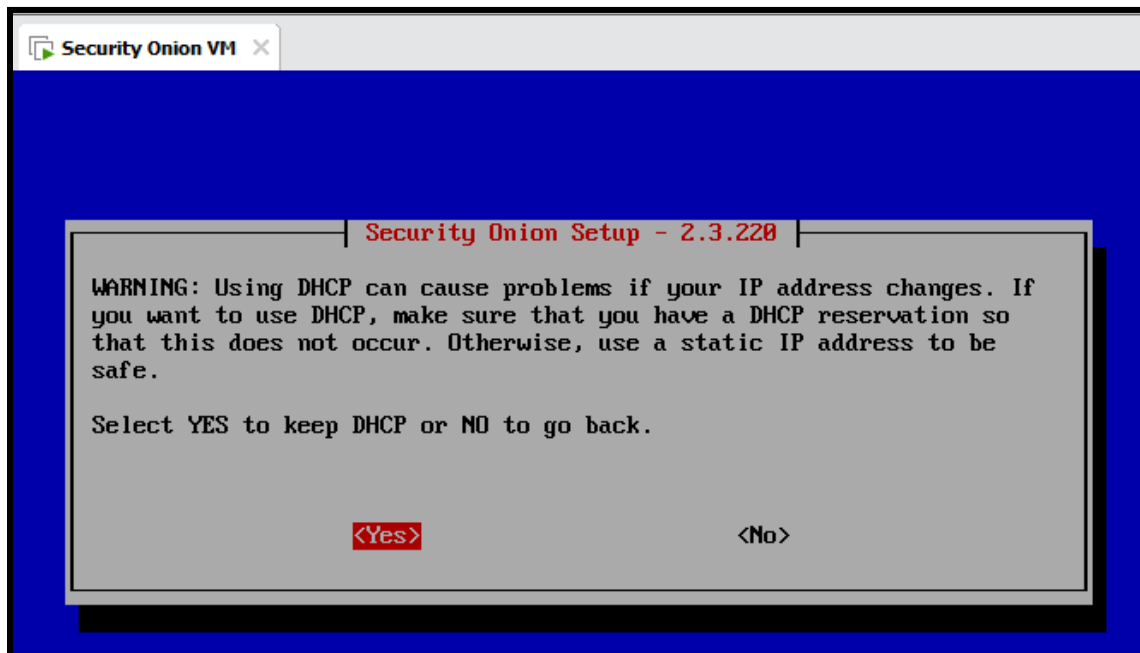
- 2.28. After going through the previous step, select the correct Management interface according to your specific lab environment by pressing the **[Space Key]**. Then press **[Tap Key]** followed by the **[Enter Key]**.



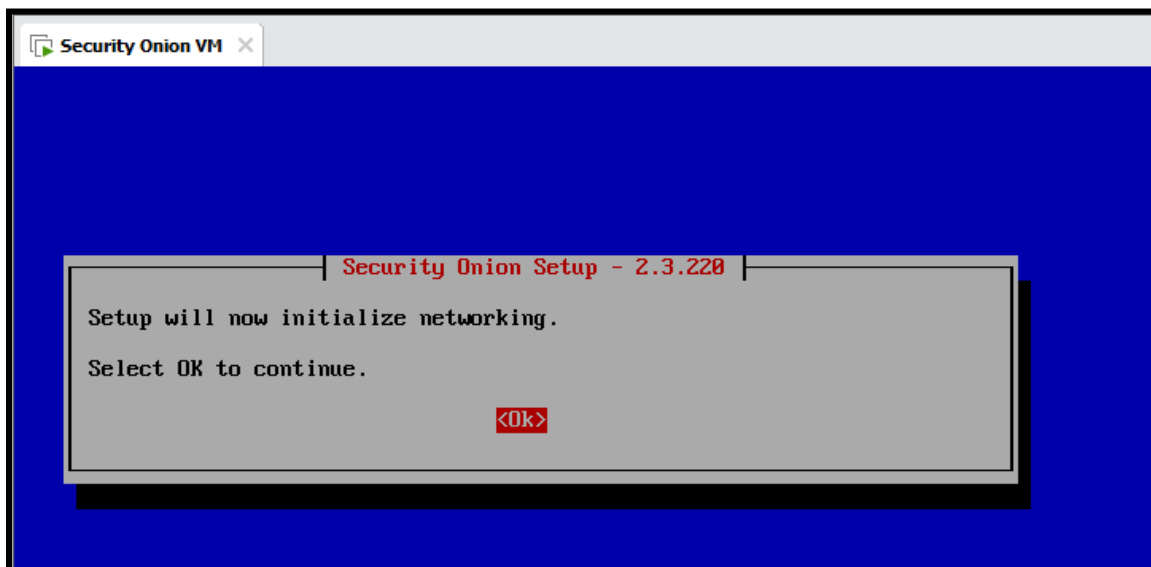
- 2.29. Choose **[DHCP]** option by clicking **[Space Key]**. Then use the **[Tap Key]** followed by the **[Enter key]**



2.30. Confirm that you still want to use **DHCP** by clicking on **[Yes]**

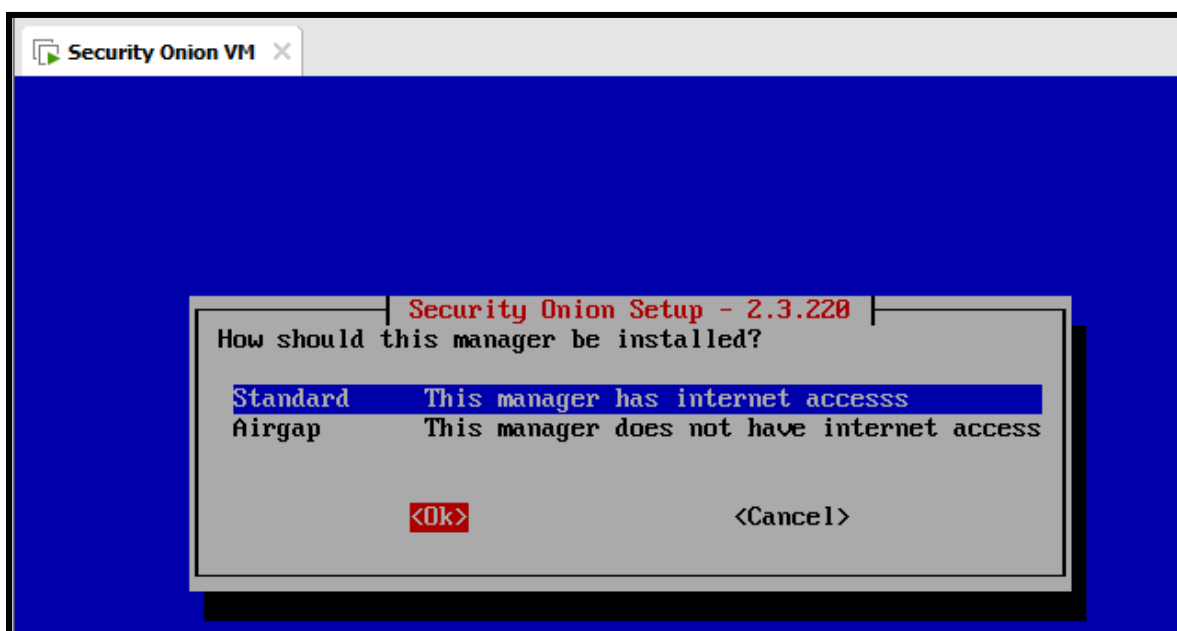


2.31. Click **[Ok]** to start initializing the network.





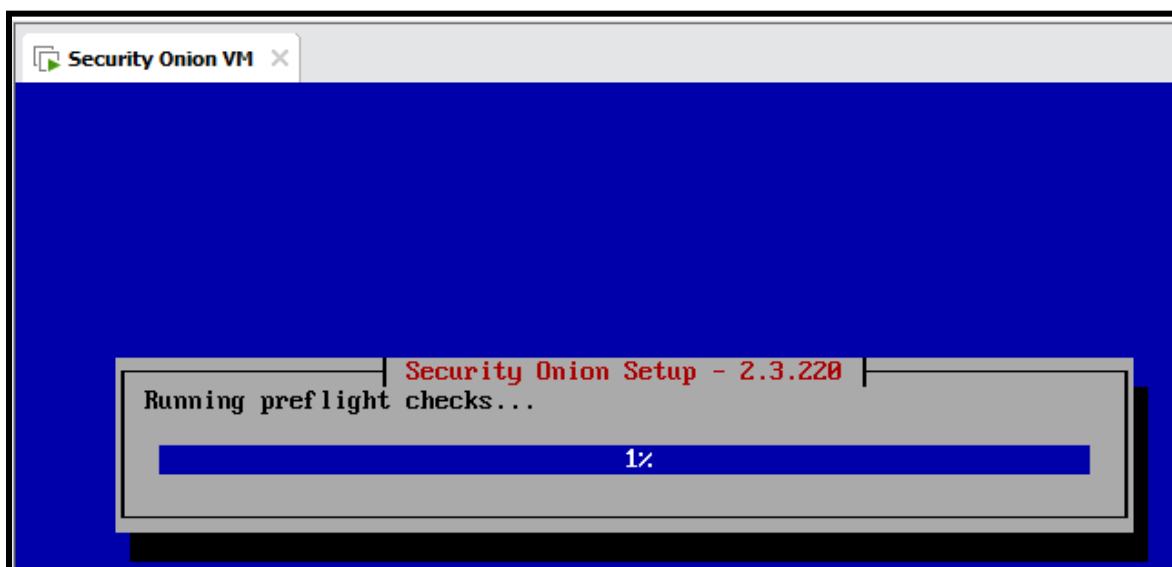
- 2.32. Select **[Standard]** option to allow the Security Onion Manager to access the internet, then click **[Enter Key]**



- 2.33. Select **[Direct]** option and click **[Tap Key]** followed by **[Enter Key]**

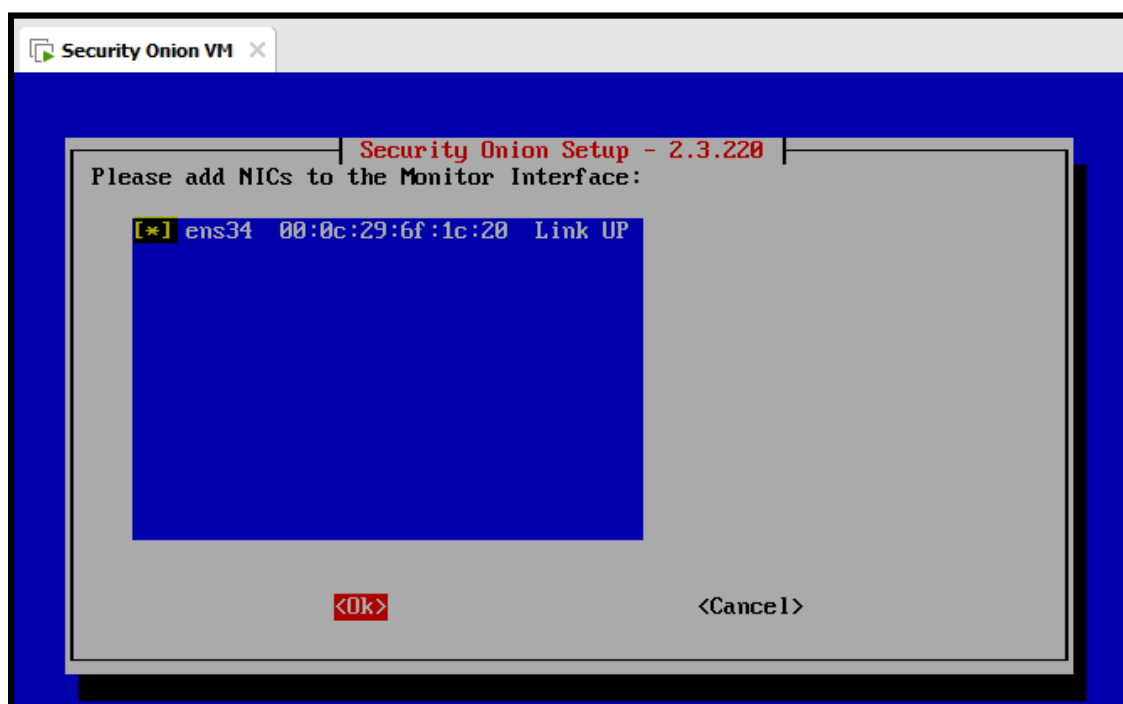


2.34. Wait a couple of minutes for the system to run all required checks.

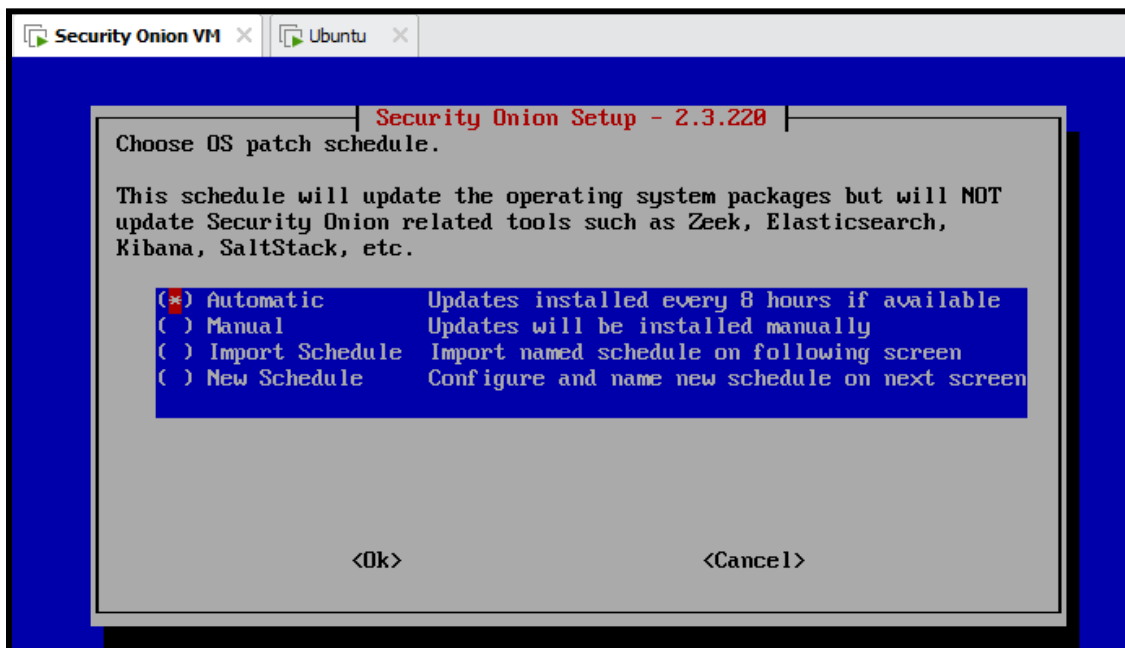


Now we should select the *Monitor Network Interface*. If you correctly identify the *Management Network Interface* previously, then the interface that will be shown in this window should be the correct Monitor Interface.

2.35. Select it by pressing the **[Space Key]** then **[Tap Key]** followed by **[Enter Key]**

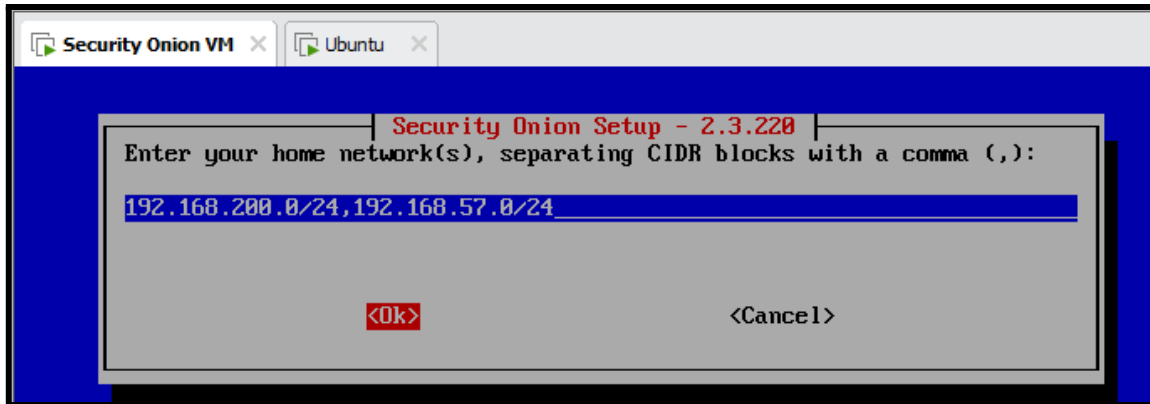


2.36. Set the OS patch schedule to **[Automatic]**

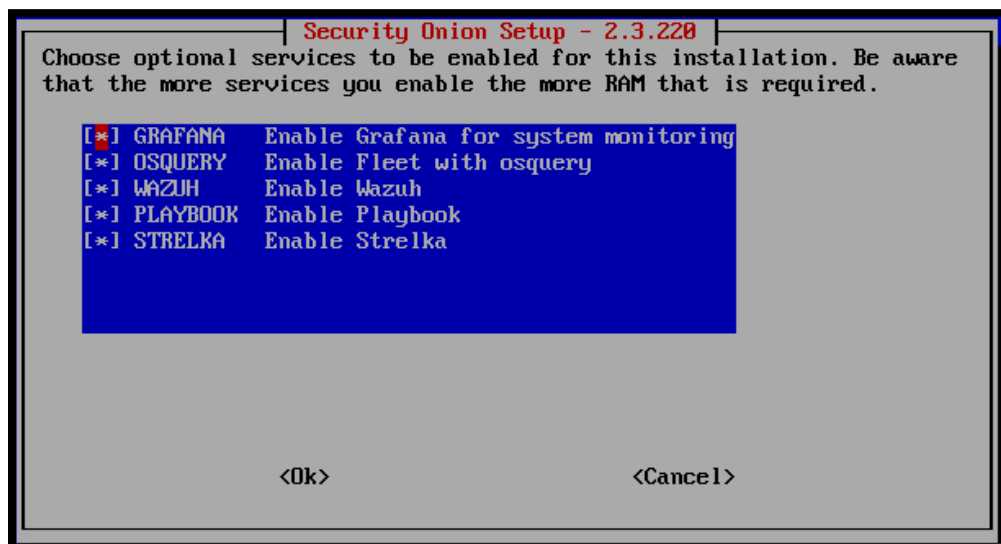


2.37. Enter the Classless Inter-Domain Routing (CIDR) blocks for both networks.

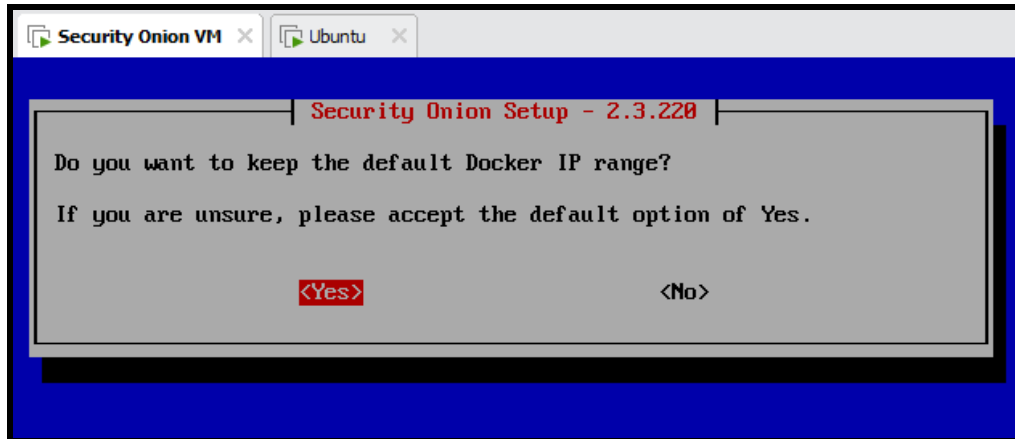
A CIDR address looks like a normal IP address, except that it ends with a slash followed by a number. By now you should be able to figure out the CIDR of the Management Network from the IP Address of the Analyst. In our own lab environment, we found that the Analyst IP Address is 192.168.200.90. This means that the CIDR IP Address of the Management Network is: 192.168.200.0/24. In a similar fashion, you should connect the Analyst VM to the Monitor Network [VMnet2]. Then use [ifconfig] to get the IP address and based on that you will figure the CIDR block for **your Monitor Network**. For our own lab environment, we have entered the following: 192.168.200.0/24, 192.168.57.0/24.



- 2.38. **After** you finish the previous step, make sure that your Analyst VM is connected to the Management Network only [VMnet0].
- 2.39. Make sure all services are enabled and then press [Tap Key] followed by the [Enter Key]

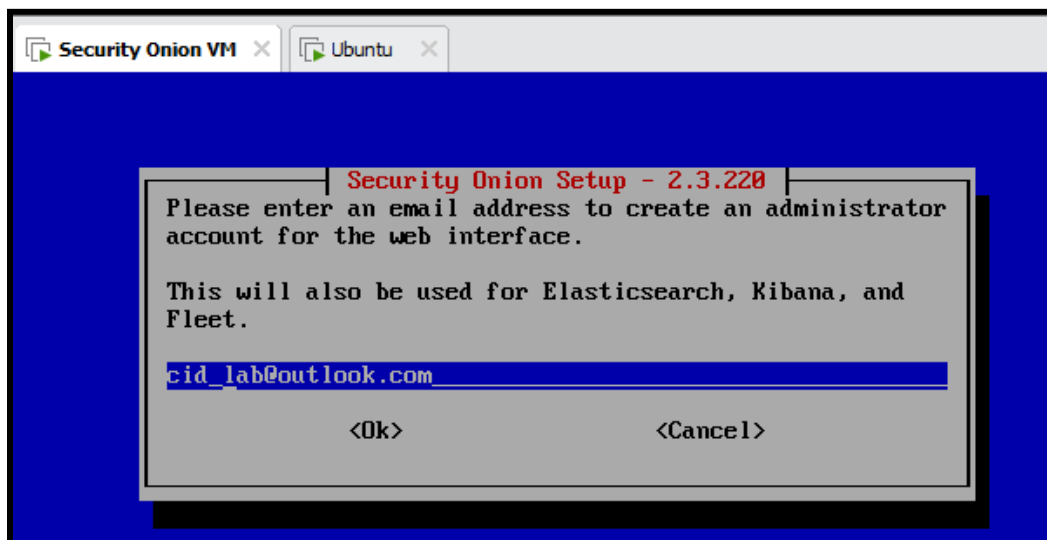


- 2.40. Select Yes and press [Enter Key]

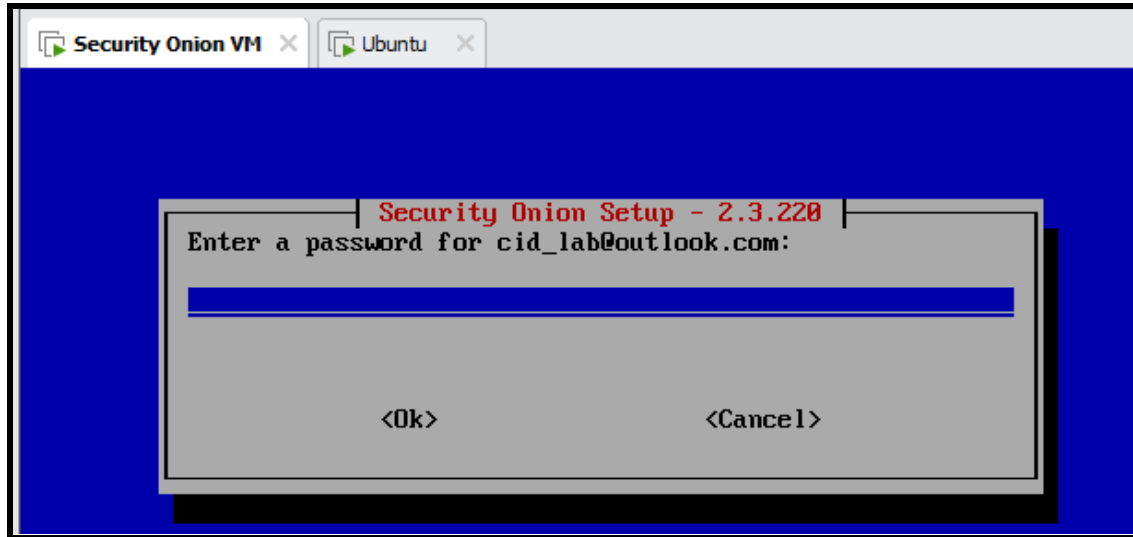


- 2.41. Type the email address that will be used to access the web interface of the Security Onion Manager

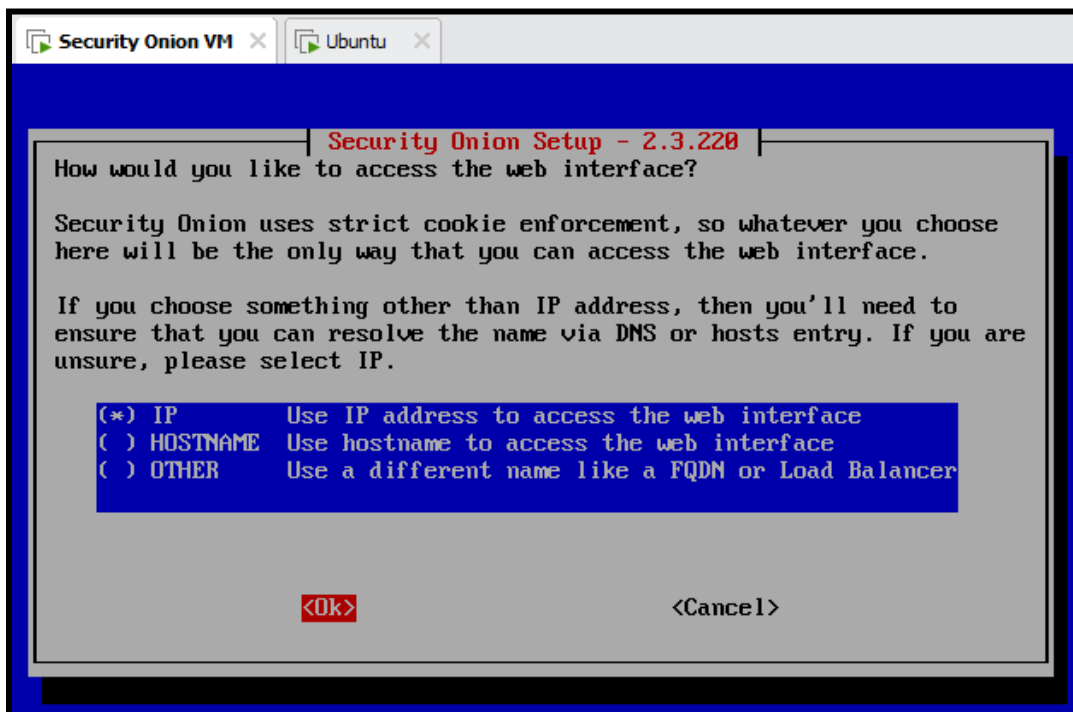
Setup the email address to [cid\_lab@outlook.com]



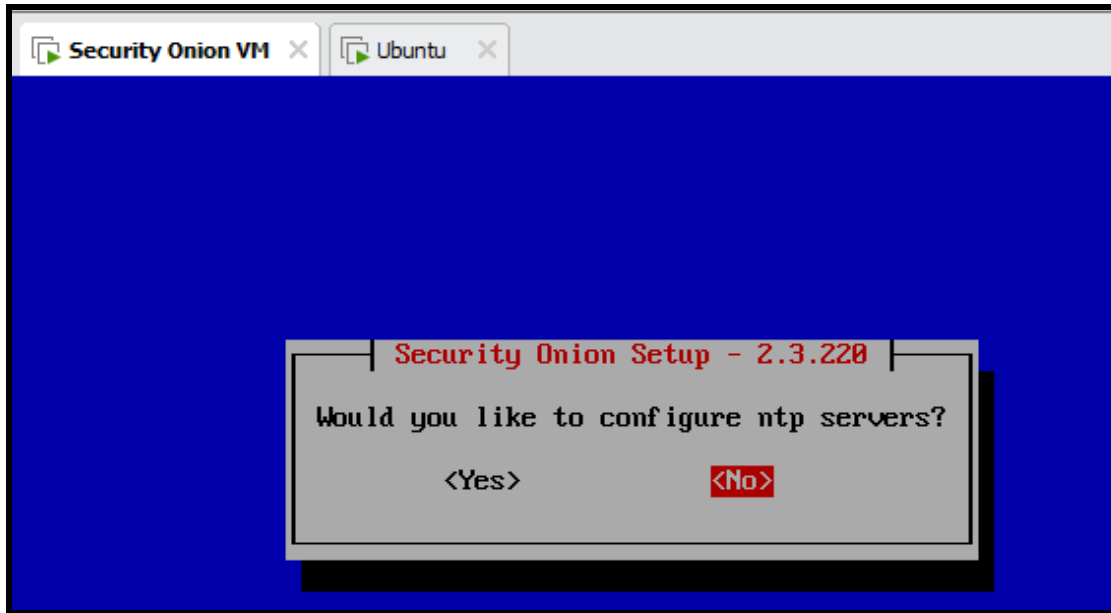
- 2.42. Set up a password that will be used to access the web interface of the Security Onion Manager  
Password: **cid\_lab@123**



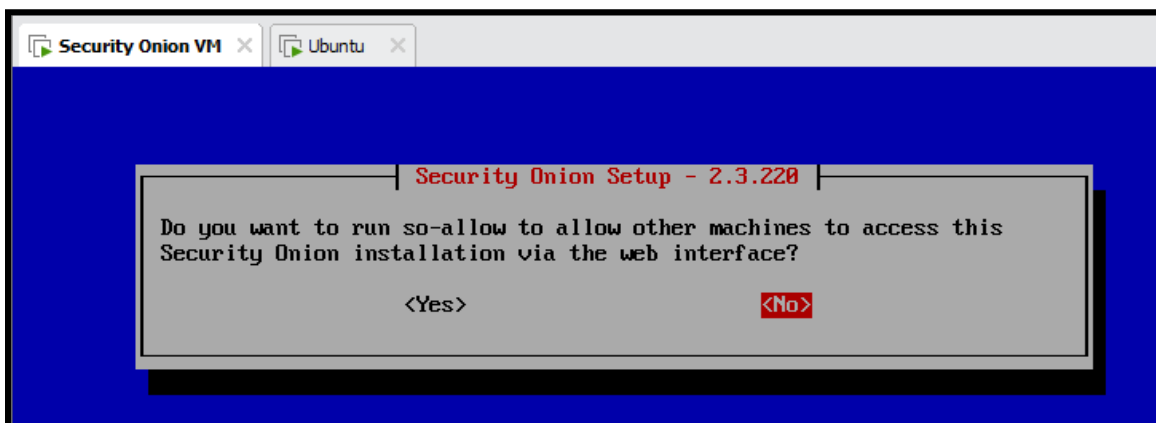
- 2.43. Then reenter the password for confirmation.
- 2.44. Select the [IP] option as the method that you will use to access the web interface. Then press [Tap key] followed by the [Enter Key].



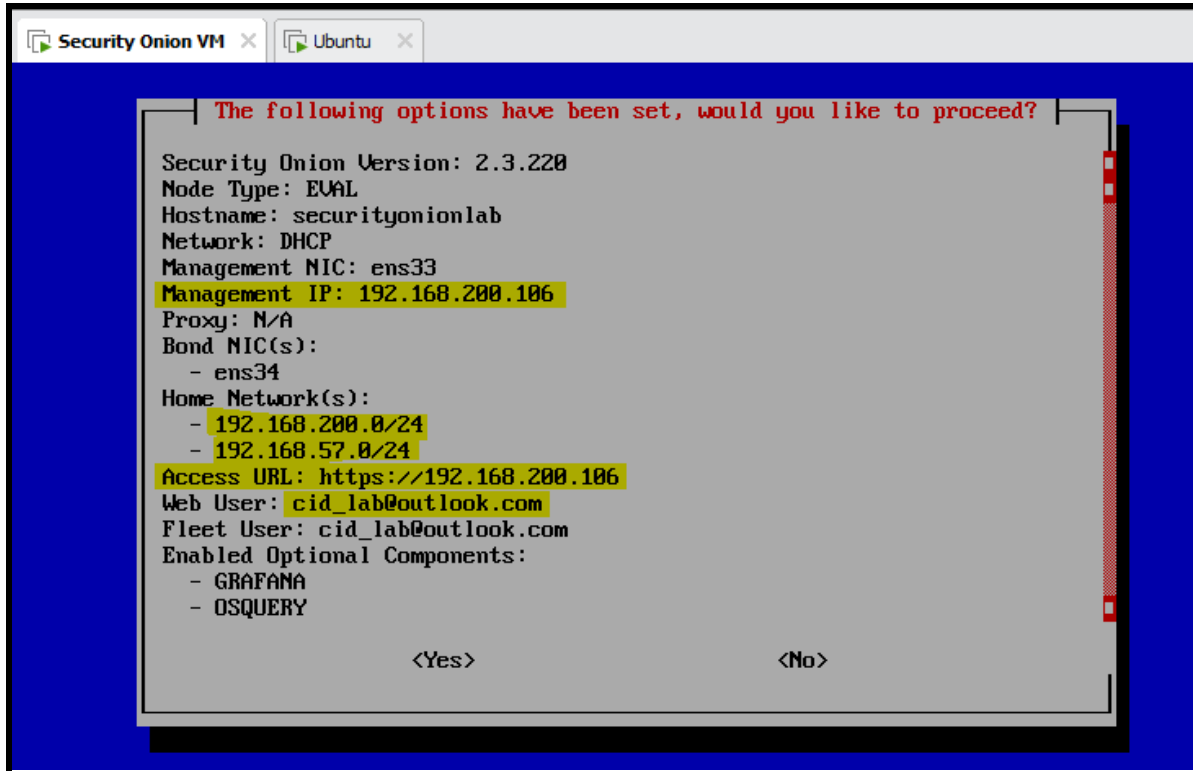
- 2.45. Choose [No] when asked about configuring the NTP servers.



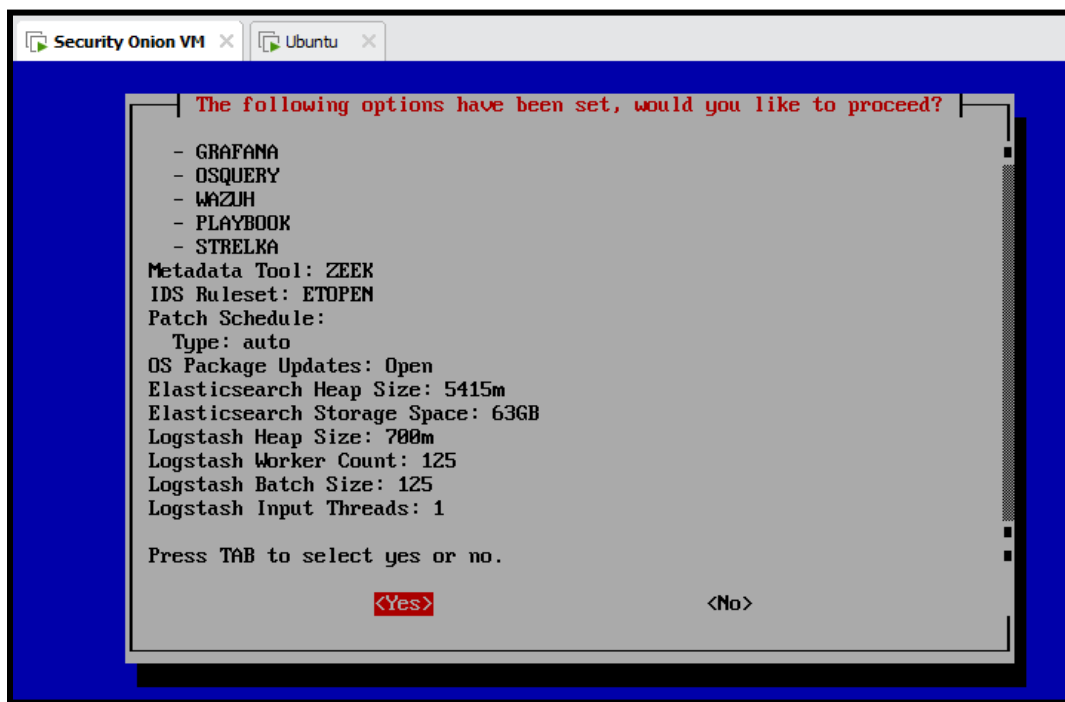
2.46. We will configure the so-allow in a later step so select **[No]** when asked if you want to run so-allow utility.



2.47. Now you will be given a summary of all the network configuration details. Make sure you take a screenshot of this window. Specifically, you must write the Access URL that we will need to use to access the Security Onion dashboard. Take a screenshot of it.

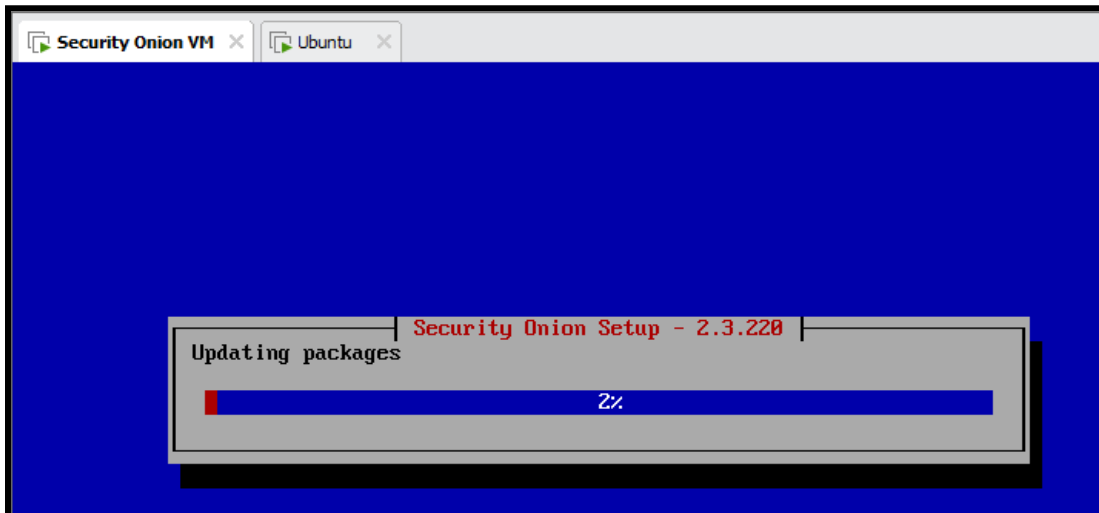


- 2.48. Press the **[Down arrow]** until you reach the end of the window, then press the **[Tap key]** followed by the **[Enter Key]**

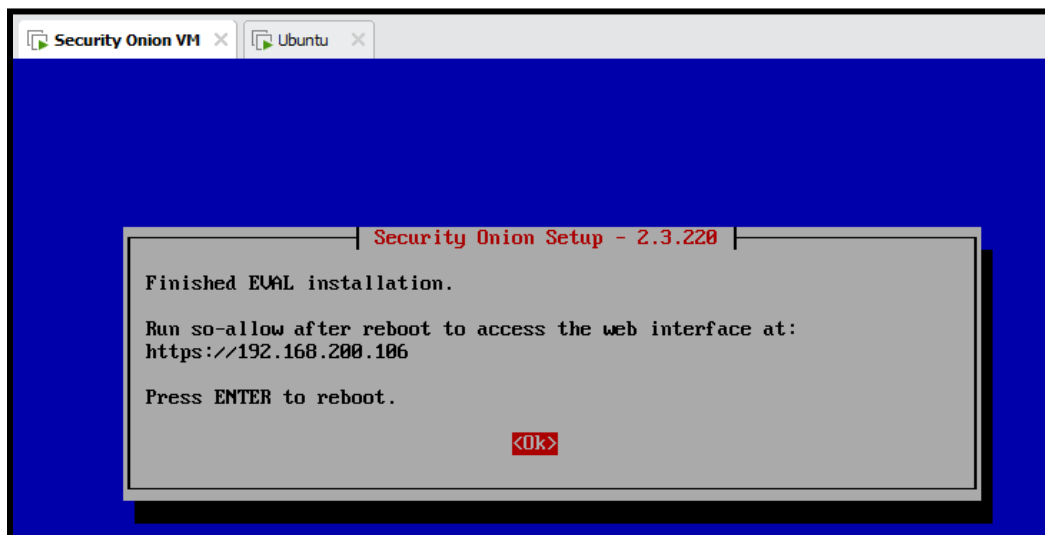




2.49. Wait for the update process to finish, this step may take up to 20 minutes.



2.50. Once the update process has finished you will see the following window. Press [Enter] and it will reboot the VM.



You have successfully installed Security Onion Machine, using the evaluation mode.

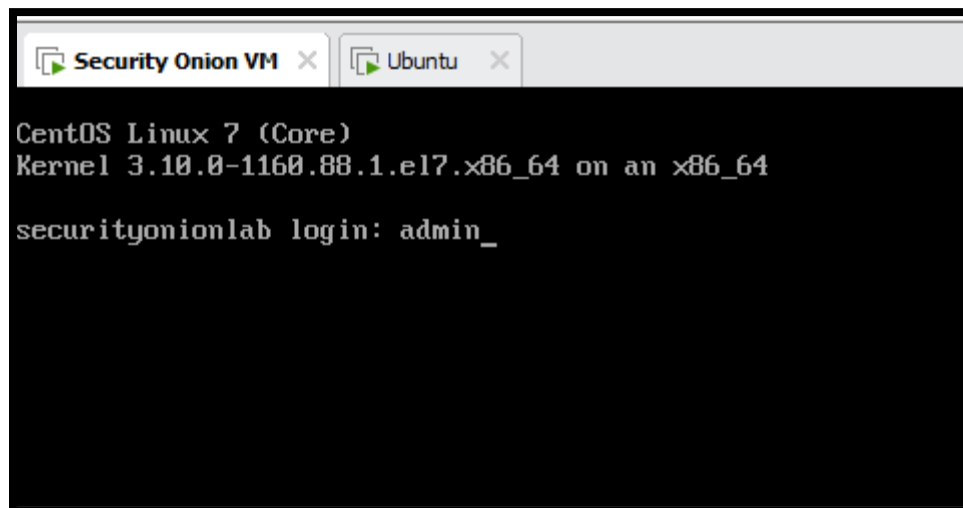
### 3. Connect the Analyst VM to Security Onion VM

Now we will configure the so-allow utility that will enable the Analyst Machine to connect to Security Onion Interface through the web. This section should be followed right after installing and configuring Security Onion VM.

- 3.1. After you reboot Security Onion VM, enter your login information.

**Username: admin**

**Password: admin**

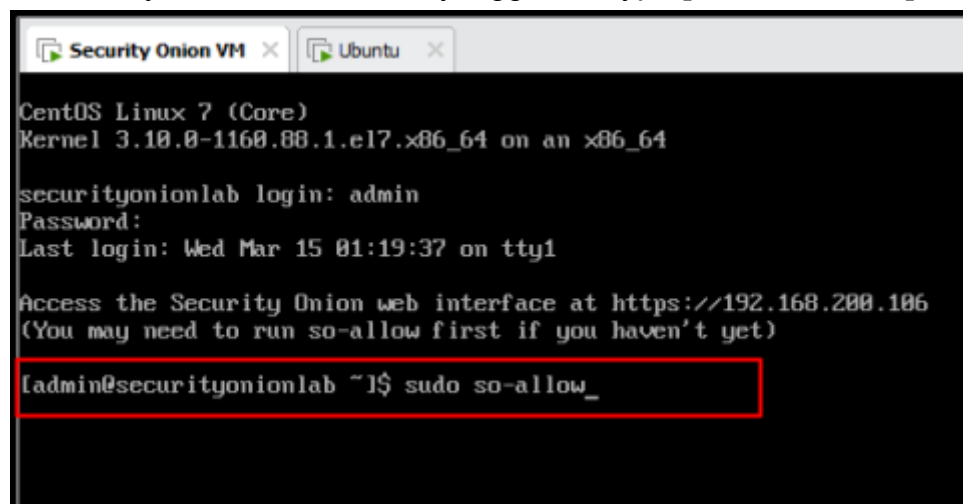


A terminal window titled "Security Onion VM" with a tab for "Ubuntu". The terminal output shows the CentOS Linux 7 (Core) kernel version 3.10.0-1160.88.1.el7.x86\_64 on an x86\_64 architecture. The prompt "securityonionlab login:" is followed by the input "admin\_".

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.88.1.el7.x86_64 on an x86_64

securityonionlab login: admin_
```

- 3.2. Once you have successfully logged in, type **[sudo so-allow]**



A terminal window titled "Security Onion VM" with a tab for "Ubuntu". The terminal output shows the CentOS Linux 7 (Core) kernel version 3.10.0-1160.88.1.el7.x86\_64 on an x86\_64 architecture. The prompt "securityonionlab login:" is followed by the input "admin". The password is entered, and the last login is shown as "Wed Mar 15 01:19:37 on tty1". The prompt "Access the Security Onion web interface at https://192.168.200.106 (You may need to run so-allow first if you haven't yet)" is displayed. The command "sudo so-allow\_" is entered and highlighted with a red box.

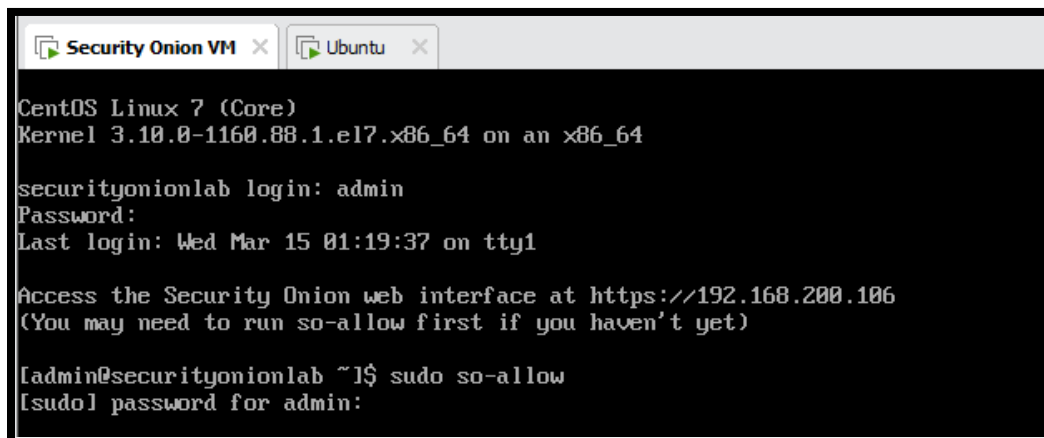
```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.88.1.el7.x86_64 on an x86_64

securityonionlab login: admin
Password:
Last login: Wed Mar 15 01:19:37 on tty1

Access the Security Onion web interface at https://192.168.200.106
(You may need to run so-allow first if you haven't yet)

[admin@securityonionlab ~]$ sudo so-allow_
```

3.3. Then you will be asked to enter the administrative password [admin]



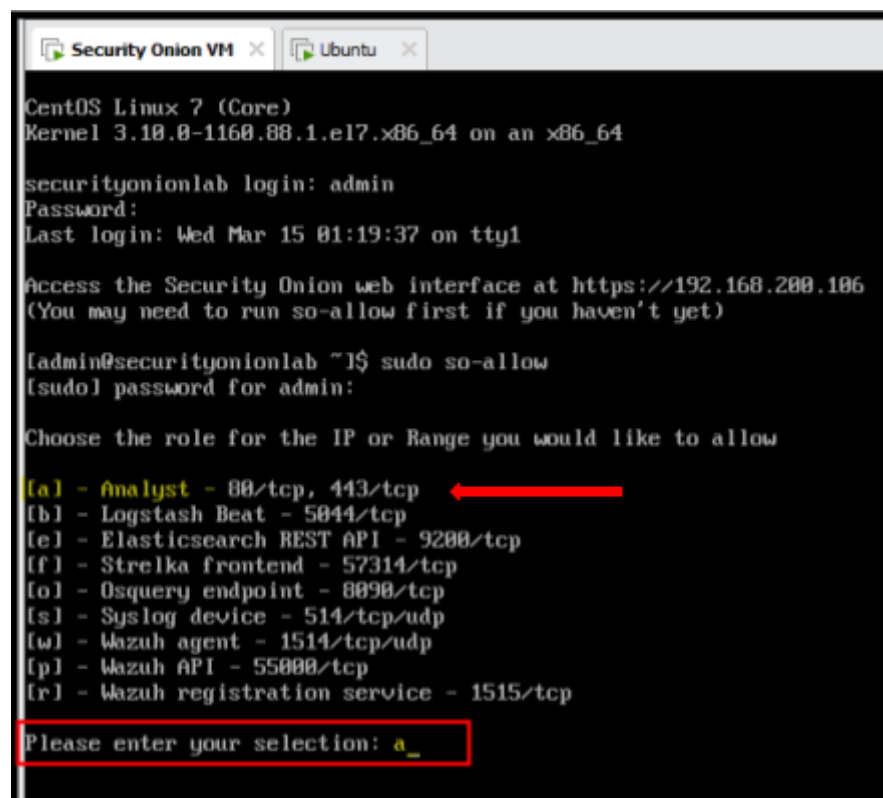
```
Security Onion VM x Ubuntu x
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.88.1.el7.x86_64 on an x86_64

securityonionlab login: admin
Password:
Last login: Wed Mar 15 01:19:37 on tty1

Access the Security Onion web interface at https://192.168.200.106
(You may need to run so-allow first if you haven't yet)

[admin@securityonionlab ~]$ sudo so-allow
[sudo] password for admin:
```

3.4. There are a set of roles that you could configure. To allow the Analyst role, type the letter **[a]** and press **[Enter Key]**



```
Security Onion VM x Ubuntu x
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.88.1.el7.x86_64 on an x86_64

securityonionlab login: admin
Password:
Last login: Wed Mar 15 01:19:37 on tty1

Access the Security Onion web interface at https://192.168.200.106
(You may need to run so-allow first if you haven't yet)

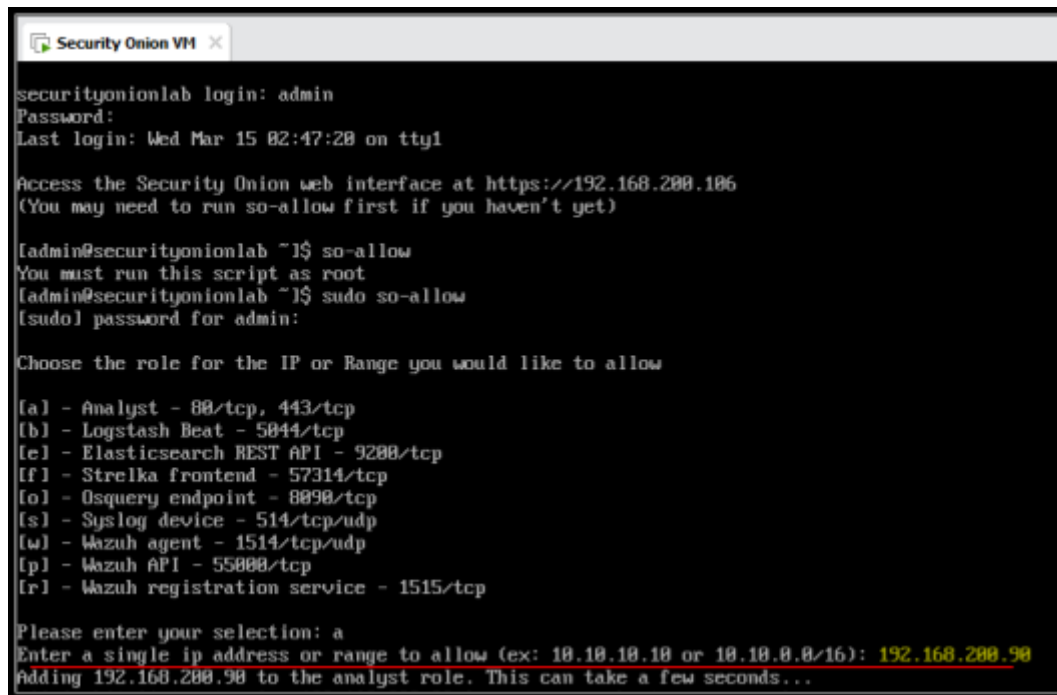
[admin@securityonionlab ~]$ sudo so-allow
[sudo] password for admin:

Choose the role for the IP or Range you would like to allow

[a] - Analyst - 88/tcp, 443/tcp
[b] - Logstash Beat - 5044/tcp
[c] - Elasticsearch REST API - 9200/tcp
[d] - Strelka frontend - 57314/tcp
[e] - Osquery endpoint - 8090/tcp
[f] - Syslog device - 514/tcp/udp
[g] - Wazuh agent - 1514/tcp/udp
[h] - Wazuh API - 55000/tcp
[i] - Wazuh registration service - 1515/tcp

Please enter your selection: a_
```

- 3.5. Then you should specify the IP address that you will allow for the analyst role. This should be the IP Address of your Analyst VM that is connected to VMnet0 (Management Network). Based on our environment setup the Analyst machine have the IP Address: 192.168.200.90
- 3.6. Enter the IP address of your Analyst VM then press [Enter Key]



```
securityonionlab login: admin
Password:
Last login: Wed Mar 15 02:47:28 on tty1

Access the Security Onion web interface at https://192.168.200.106
(You may need to run so-allow first if you haven't yet)

[admin@securityonionlab ~]$ so-allow
You must run this script as root
[admin@securityonionlab ~]$ sudo so-allow
[sudo] password for admin:

Choose the role for the IP or Range you would like to allow

[a] - Analyst - 80/tcp, 443/tcp
[b] - Logstash Beat - 5044/tcp
[c] - Elasticsearch REST API - 9200/tcp
[d] - Strelka frontend - 57314/tcp
[e] - Osquery endpoint - 8080/tcp
[f] - Syslog device - 514/tcp/udp
[g] - Wazuh agent - 1514/tcp/udp
[h] - Wazuh API - 55000/tcp
[i] - Wazuh registration service - 1515/tcp

Please enter your selection: a
Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 192.168.200.90
Adding 192.168.200.90 to the analyst role. This can take a few seconds...
```

- 3.7. The Security Onion Manager will take a couple of seconds to set up the Analyst role to the IP Address that we have provided.

```
Added whitelist entry for 192.168.200.90 from /nsm/wazuh/etc/ossec.conf
Restarting OSSEC Server...
=====
Restarting wazuh...

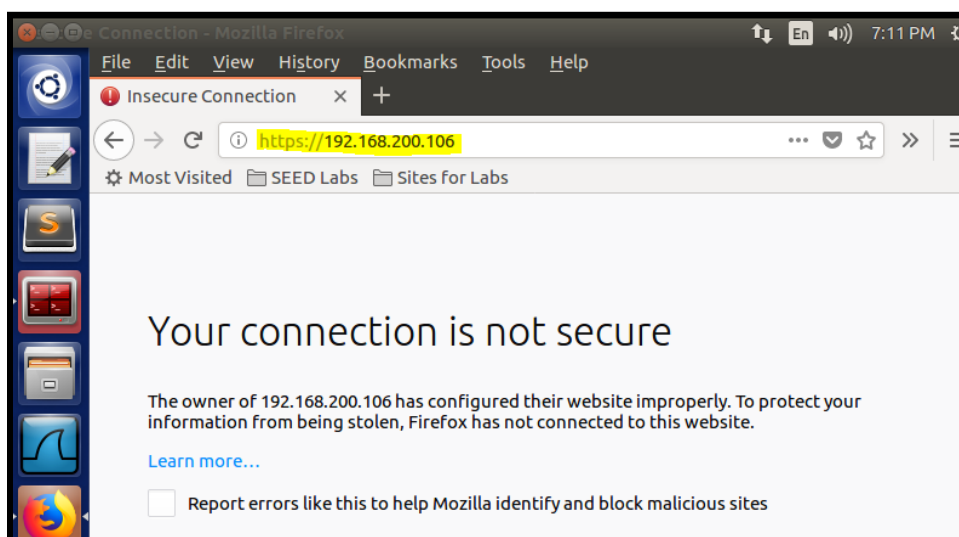
This could take a while if another Salt job is running.
Run this command with --force to stop all Salt jobs before proceeding.
=====
```

3.8. Wait until the process ends.

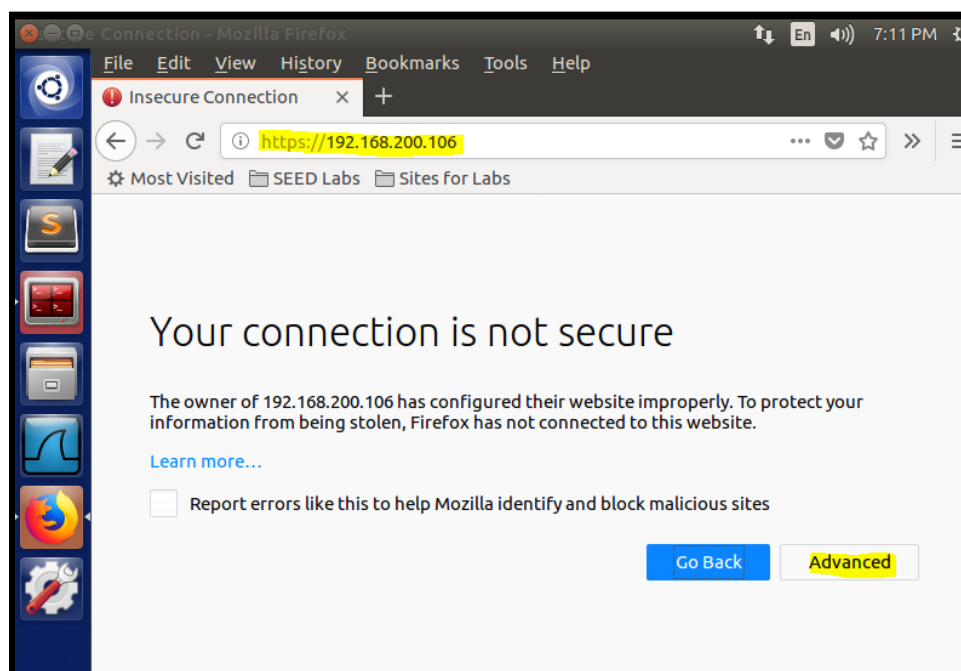
```
      ID: /opt/so/rules/hids/local_rules.xml
Function: file.symlink
Result: True
Comment: Symlink /opt/so/rules/hids/local_rules.xml is present and owned by root:r
Started: 19:09:33.426041
Duration: 1.305 ms
Changes:
-----
      ID: /opt/so/rules/hids/ruleset
Function: file.symlink
Result: True
Comment: Symlink /opt/so/rules/hids/ruleset is present and owned by root:root
Started: 19:09:33.427415
Duration: 1.163 ms
Changes:

Summary for local
-----
Succeeded: 20 (changed=5)
Failed:    0
-----
Total states run:    20
Total run time:    2.169 s
[admin@securityonionlab ~]$
```

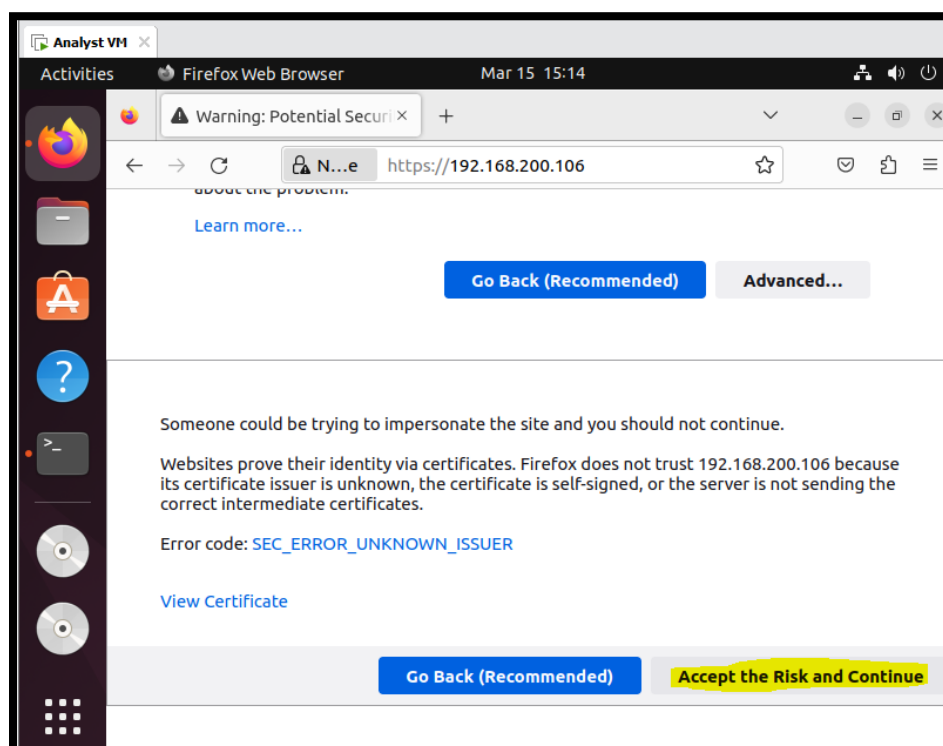
3.9. Then refer to the Analyst VM and open the browser and try to access the URL given earlier: **https://192.168.200.106**.



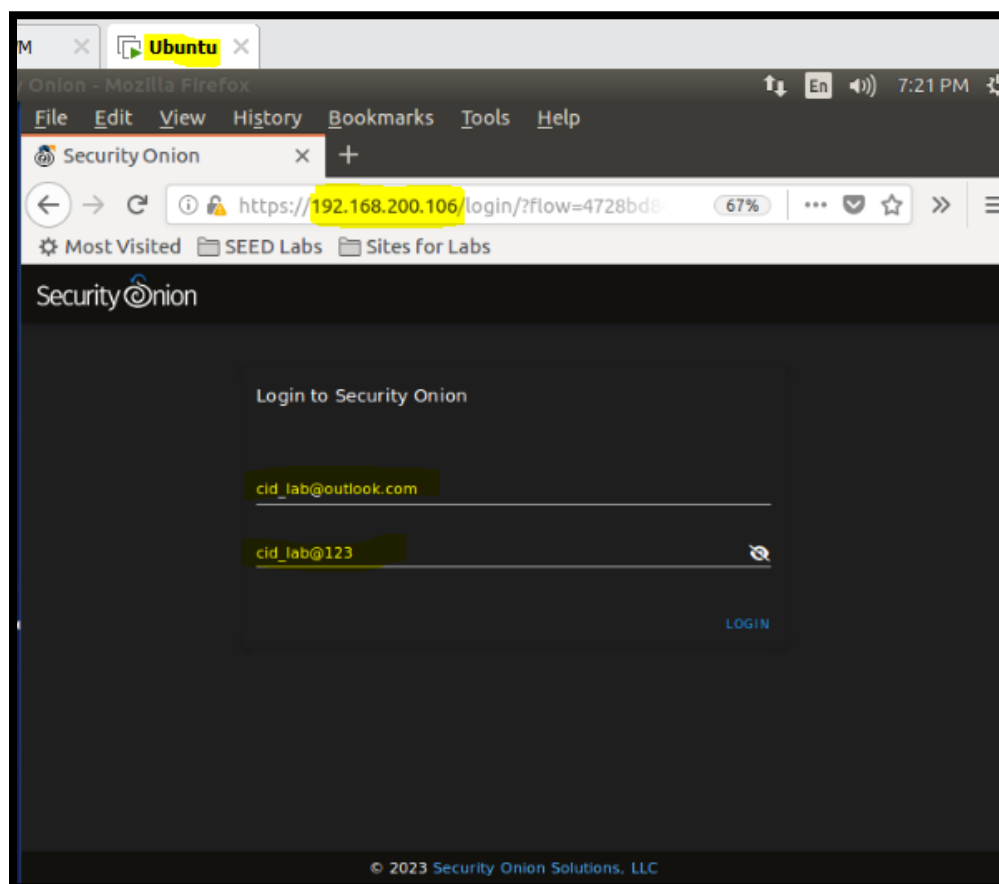
3.10. Click on **[Advanced]** then scroll down to the bottom of the webpage.



3.11. Click on **[Accept the Risk and Continue]**



- 3.12. Now you will be able to access the Security Onion Interface. Enter the email and the password that we have setup previously.



Once you reach this step then you have successfully allowed the analyst VM to access the Security Onion Console.

## Tasks

Task 2.1: provide a screenshot of the summary generated after installing Security Onion VM

Task 2.2: provide screenshot of the Analyst VM while successfully accessing the Security Onion Interface using the browser