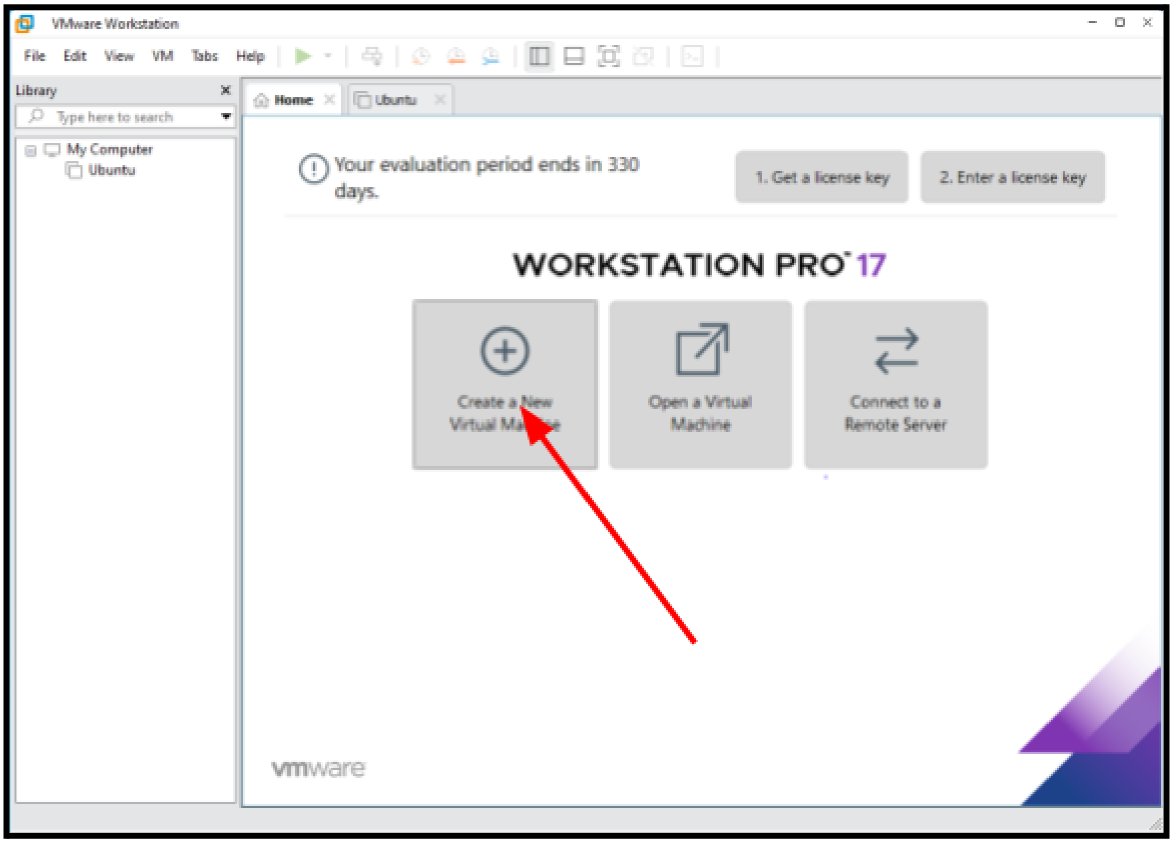
Installing Security Onion VM

1. Download Security Onion image file

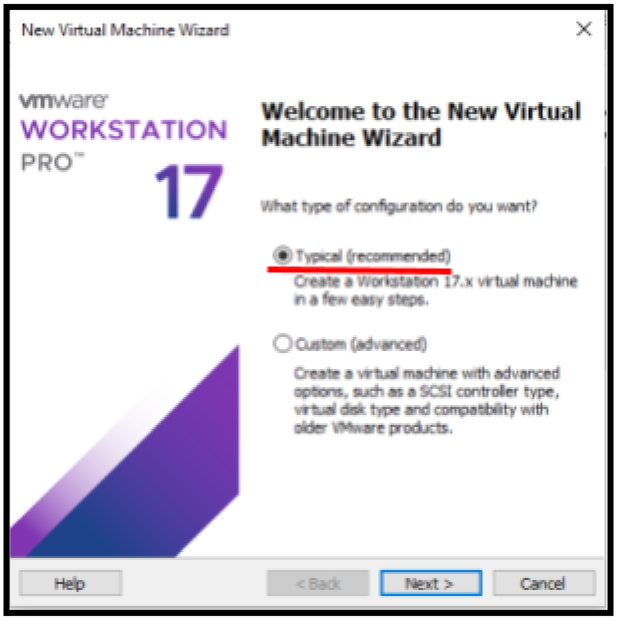
1.1. Download Security Onion image file from the link below and save it in the [D:\CID_2023\TeamX\Downloads] path. https://download.securityonion.net/file/securityonion/securityonion-2.3.220-20230301.iso

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]**



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

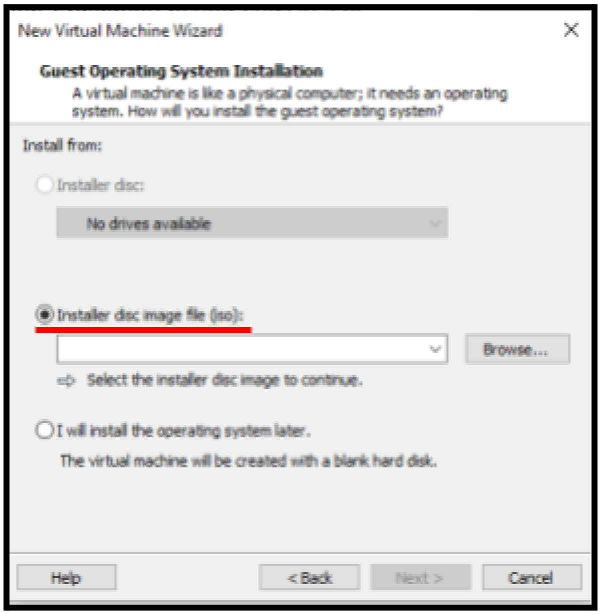
● Typical (recommended)

Create a Workstation 17.x virtual machine in a few easy steps.

○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

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



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

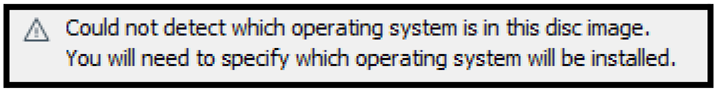
● Installer disc image file (iso):

⇨ Select the installer disc image to continue.

○ I will install the operating system later.

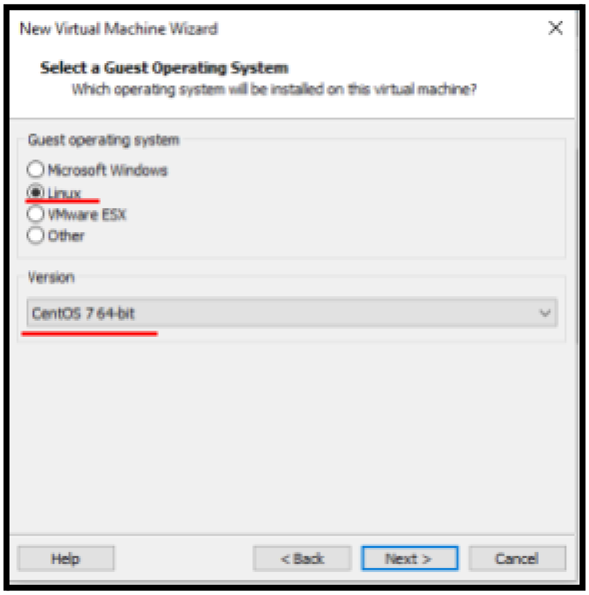
The virtual machine will be created with a blank hard disk.

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



Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

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



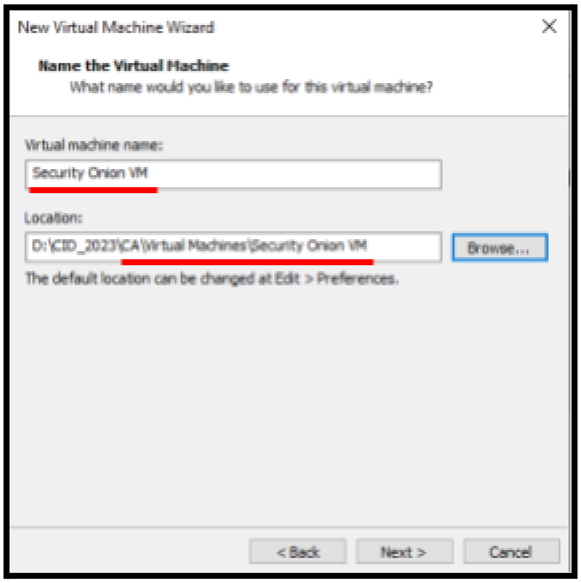
New Virtual Machine Wizard

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system
○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version
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**]



New Virtual Machine Wizard

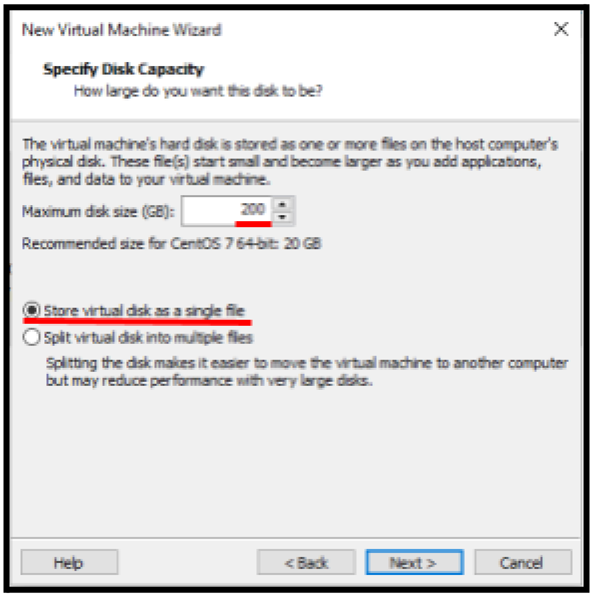
Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
Security Onion VM

Location:
D:\CID_2023\CA\Virtual Machines\Security Onion VM

The default location can be changed at Edit > Preferences.

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**.]



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 200

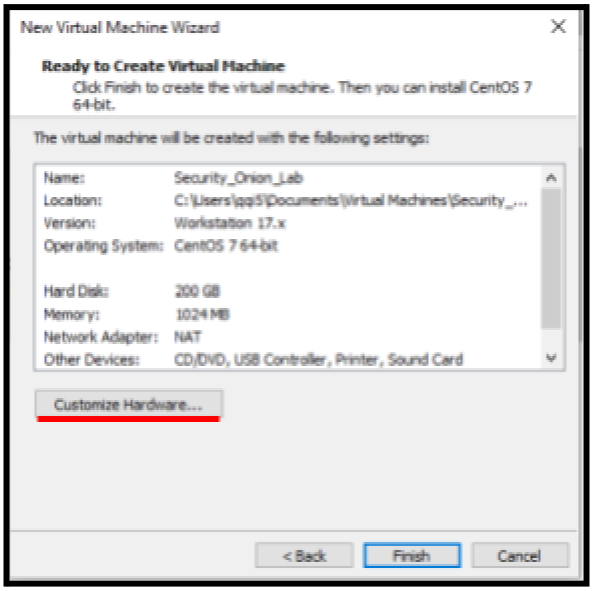
Recommended size for CentOS 7 64-bit: 20 GB

● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

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.



New Virtual Machine Wizard

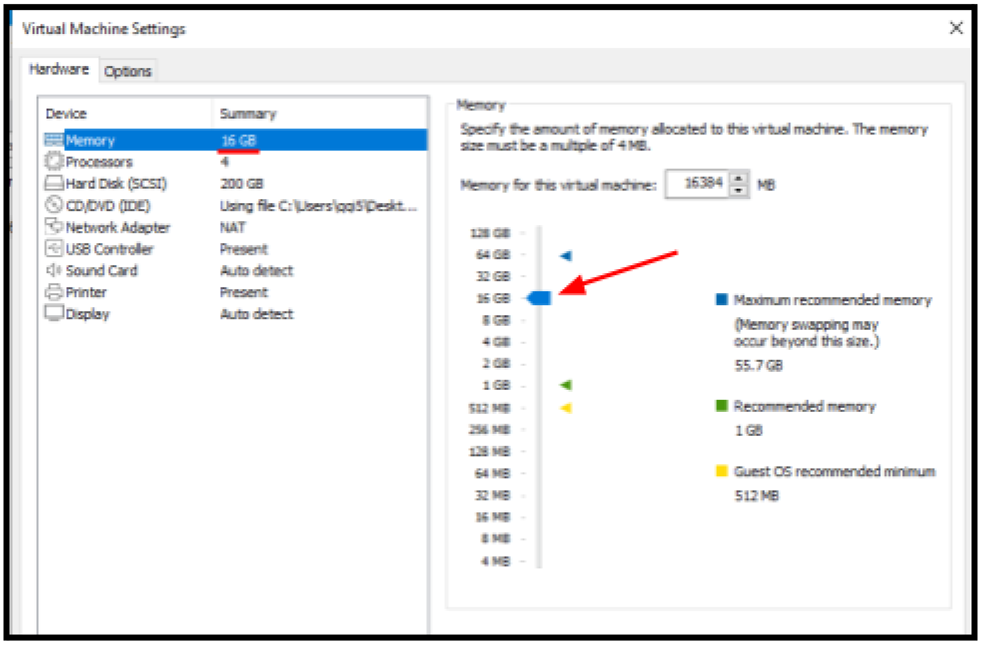
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install CentOS 7 64-bit.

The virtual machine will be created with the following settings:

Name:	Security_Onion_Lab
Location:	C:\Users\qq\5\Documents\Virtual Machines\Security_...
Version:	Workstation 17.x
Operating System:	CentOS 7 64-bit
Hard Disk:	200 GB
Memory:	1024 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

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



Virtual Machine Settings

Device	Summary
Memory	16 GB
Processors	4
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using file C:\Users\gqi5\Deskt...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

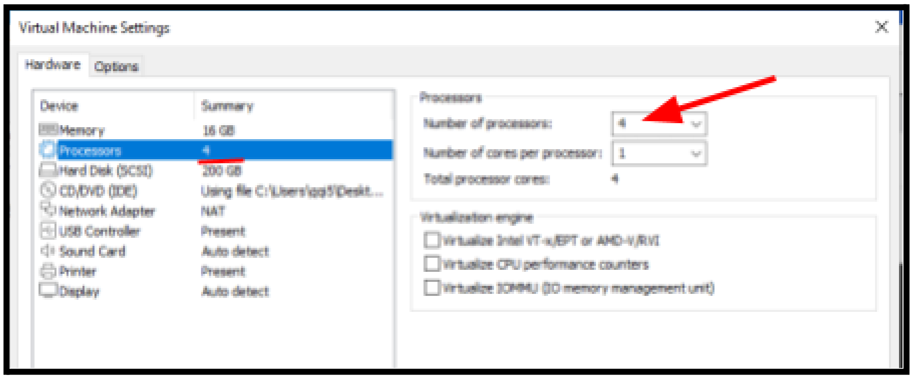
Memory for this virtual machine: 16384 MB

🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
55.7 GB

🟩 Recommended memory
1 GB

🟨 Guest OS recommended minimum
512 MB

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



Virtual Machine Settings

Device	Summary
Memory	16 GB
Processors	4
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using file C:\Users\gqi5\Deskt...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Processors

Number of processors: 4

Number of cores per processor: 1

Total processor cores: 4

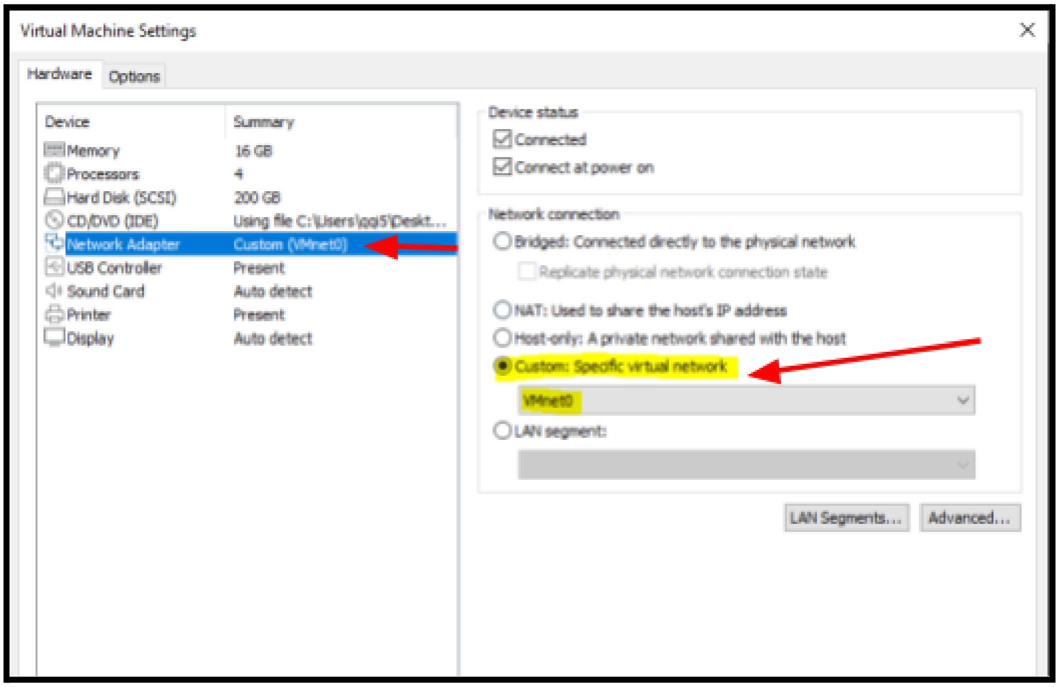
Virtualization engine

□ Virtualize Intel VT-x/EPT or AMD-V/RVI

□ Virtualize CPU performance counters

□ Virtualize IOMMU (IO memory management unit)

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



Device	Summary
Memory	16 GB
Processors	4
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using file C:\Users\gq5\Deskt...
Network Adapter	Custom (VMnet0)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

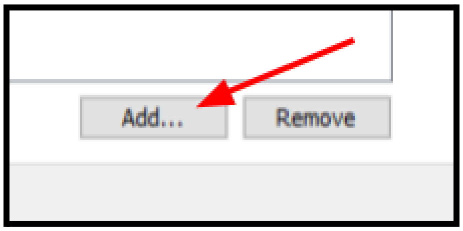
○ Host-only: A private network shared with the host

● Custom: Specific virtual network

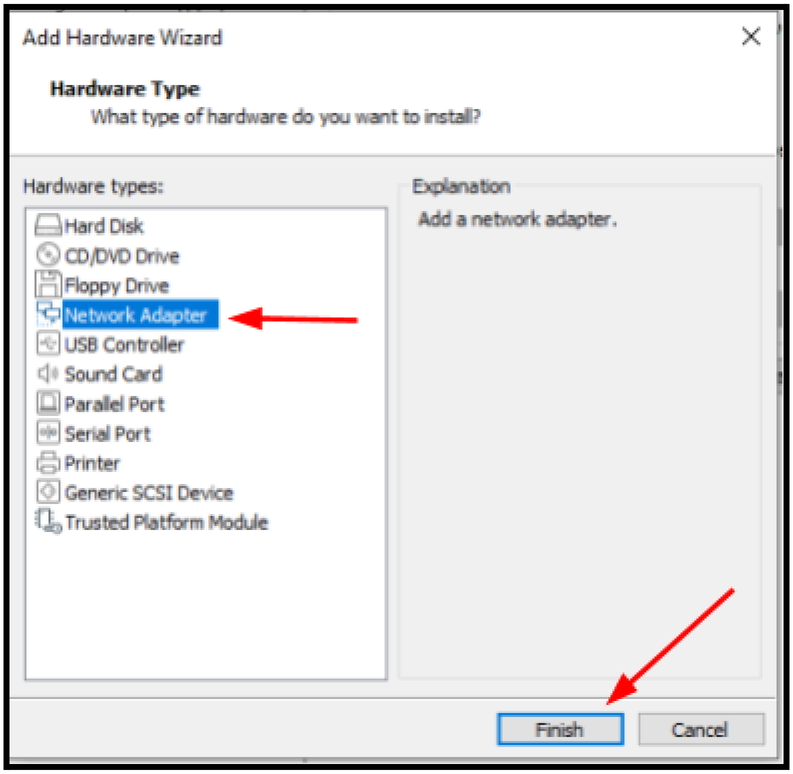
VMnet0

○ LAN segment:

2.12. Click on [**Add…**] to add an additional [**Network Adapter]**.



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



Add Hardware Wizard

Hardware Type

What type of hardware do you want to install?

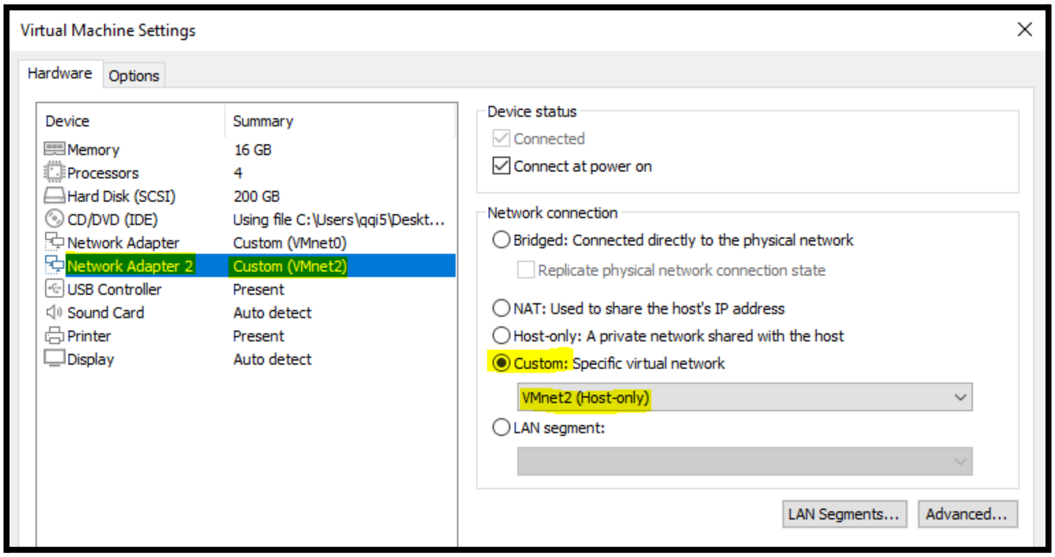
Hardware types:

- Hard Disk
- CD/DVD Drive
- Floppy Drive
- Network Adapter
- USB Controller
- Sound Card
- Parallel Port
- Serial Port
- Printer
- Generic SCSI Device
- Trusted Platform Module

Explanation

Add a network adapter.

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



Virtual Machine Settings

Device	Summary
Memory	16 GB
Processors	4
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using file C:\Users\qqi5\Deskt...
Network Adapter	Custom (VMnet0)
Network Adapter 2	Custom (VMnet2)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

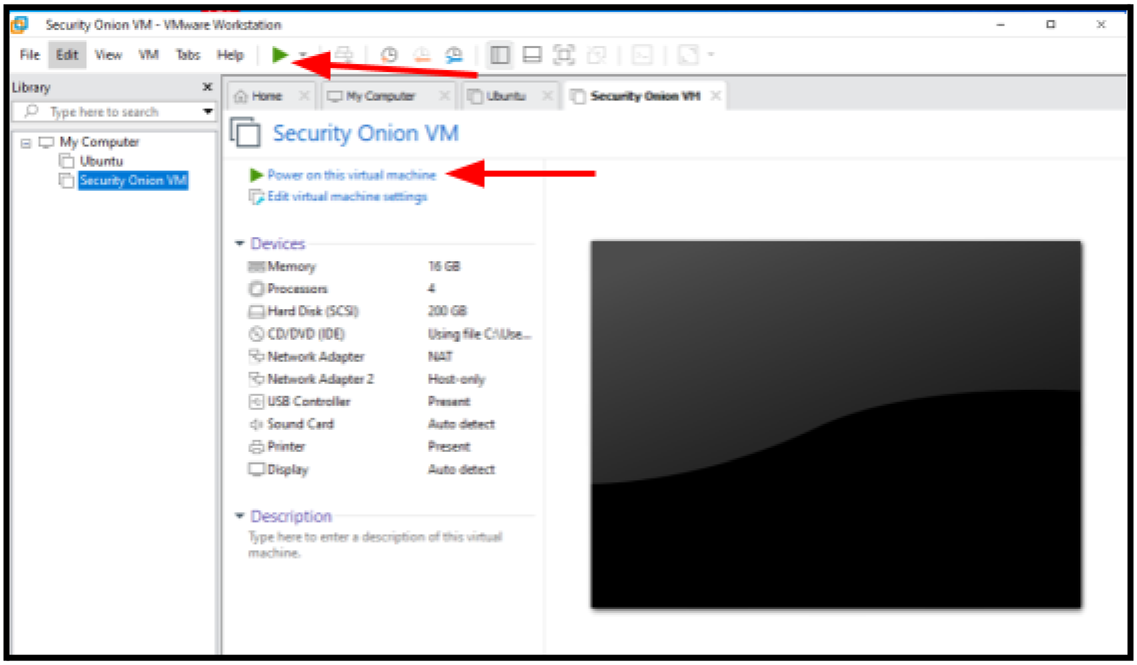
○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet2 (Host-only)

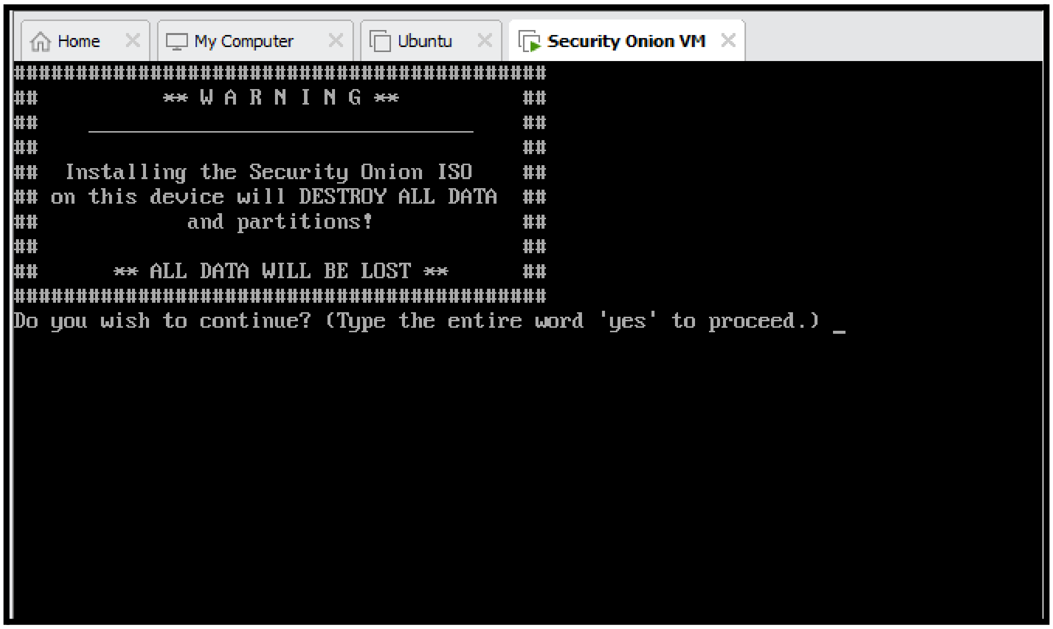
○ LAN segment:

2.15. Now run the Security Onion VM



Memory	16 GB
Processors	4
Hard Disk (SCSI)	200 GB
CD/DVD (IDE)	Using file C:\Use...
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

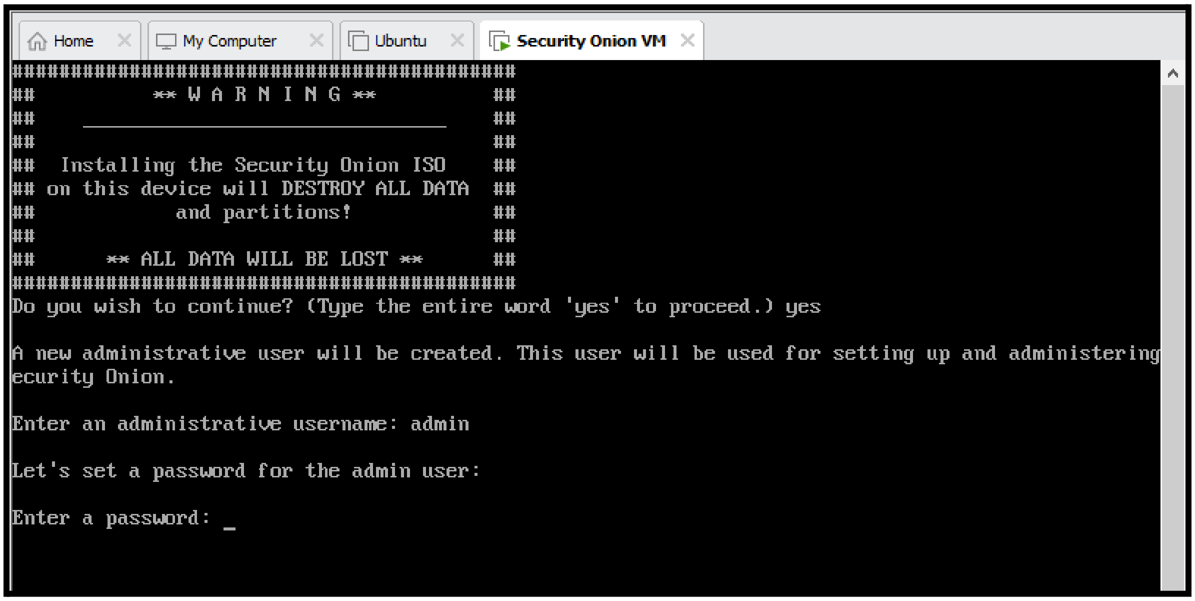
2.16. Wait until you get the following window.



```
##########################################
##          ** 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.) _
```

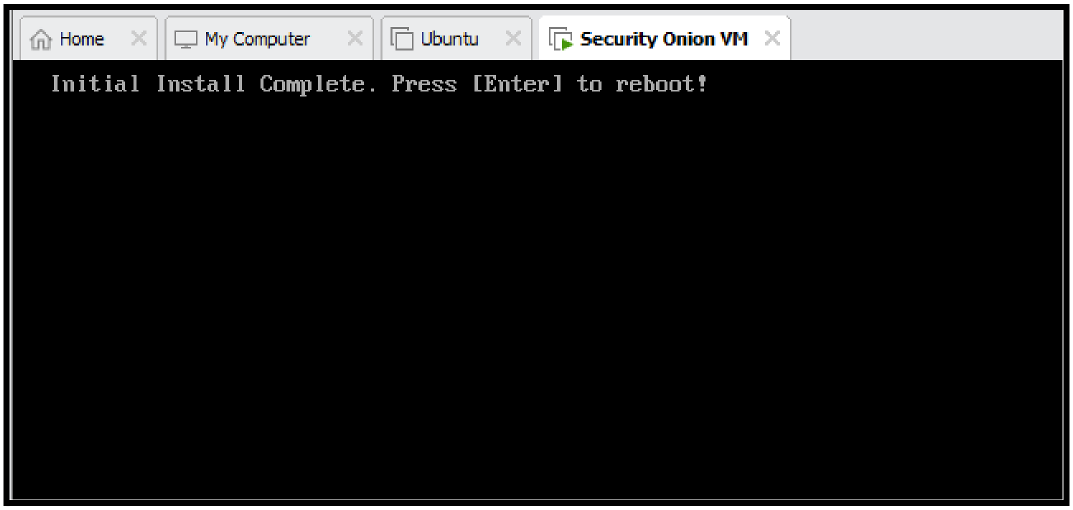
2.17. Type [**yes**] and press the [Enter Key]

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



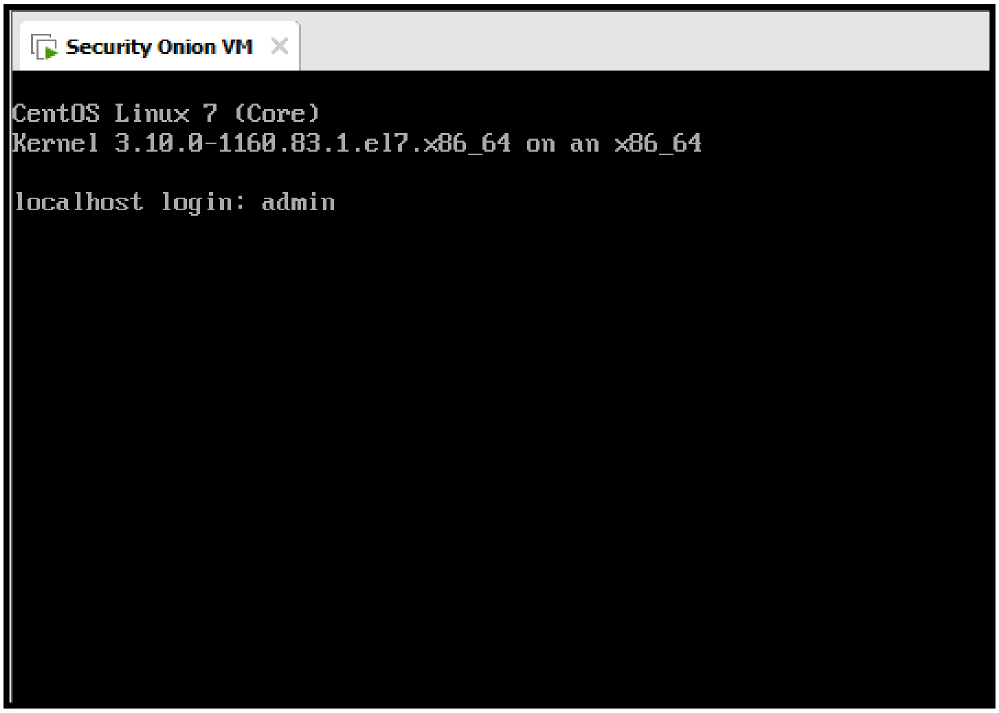
```
###########################################
##          ** W A R N I N G **          ##
##    _______________________________    ##
##                                       ##
##  Installing the Security Onion ISO    ##
## on this device will DESTROY ALL DATA  ##
##           and partitions!             ##
##                                       ##
##      ** 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.



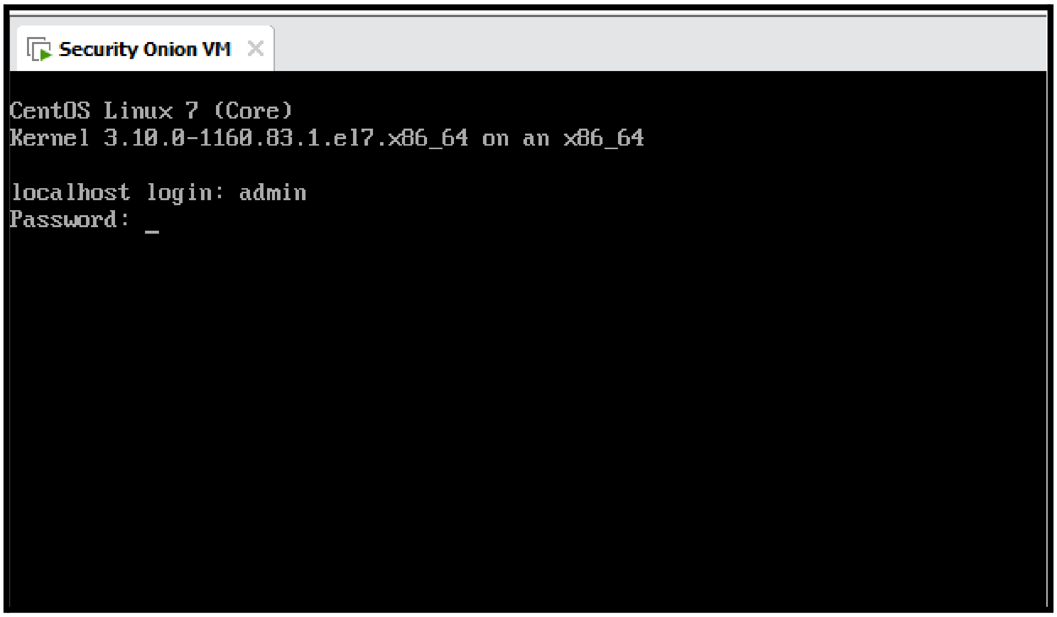
```
Initial Install Complete. Press [Enter] to reboot!
```

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**]



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.83.1.el7.x86_64 on an x86_64

localhost login: admin
```

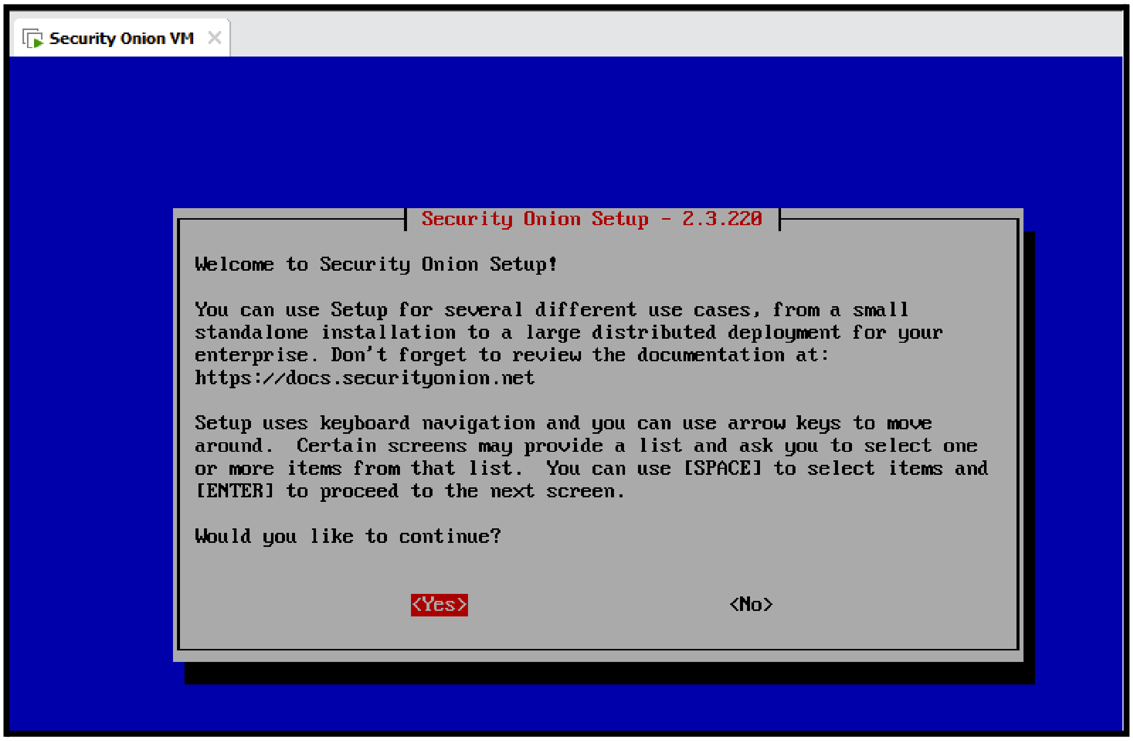
2.21. Enter your password [**admin**] and press the [**Enter Key**]



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.83.1.el7.x86_64 on an x86_64

localhost login: admin
Password: _
```

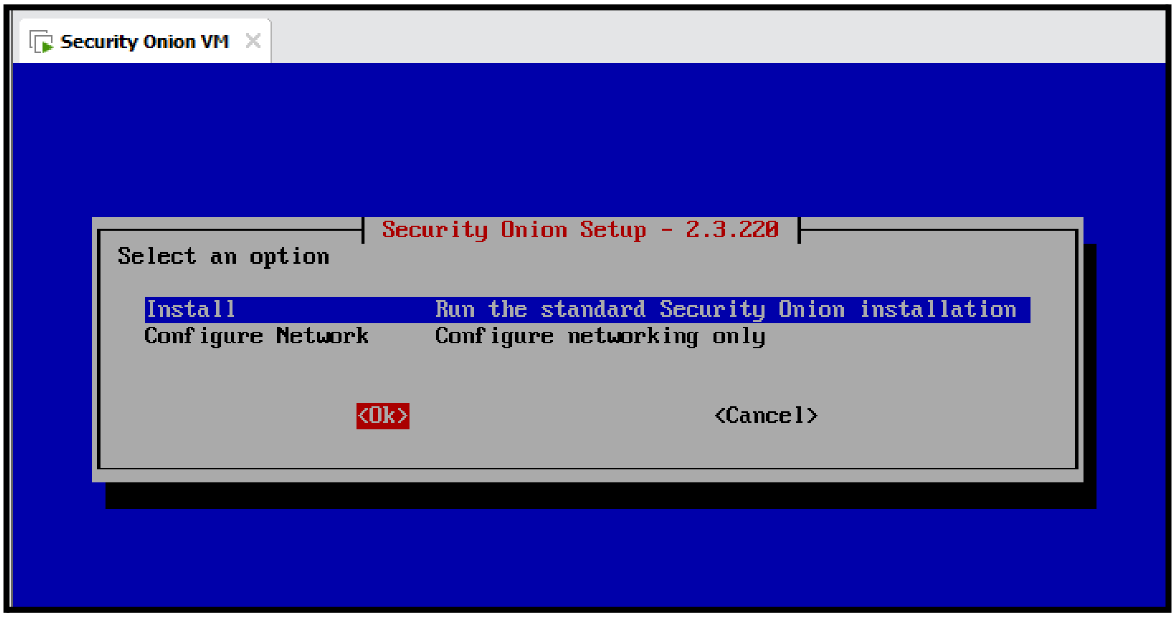
Now we will begin the configuration process of Security Onion VM

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



```
Security Onion Setup - 2.3.220

Welcome to Security Onion Setup!

You can use Setup for several different use cases, from a small
standalone installation to a large distributed deployment for your
enterprise. Don't forget to review the documentation at:
https://docs.securityonion.net

Setup uses keyboard navigation and you can use arrow keys to move
around.  Certain screens may provide a list and ask you to select one
or more items from that list.  You can use [SPACE] to select items and
[ENTER] to proceed to the next screen.

Would you like to continue?

                    <Yes>                    <No>
```

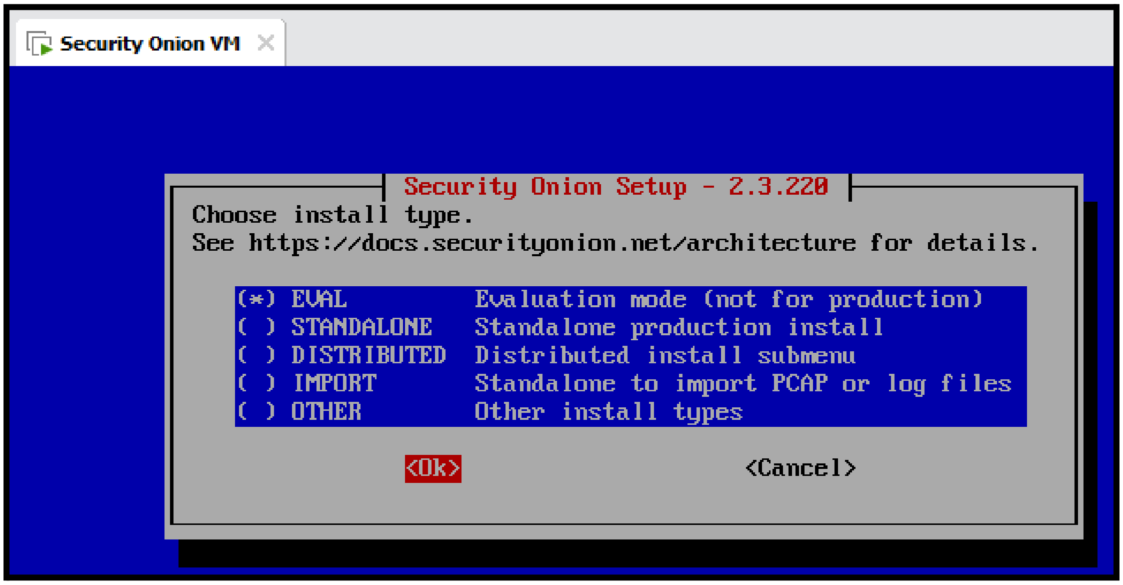
2.23. Choose [**Install**] option then press the [**Tap Key**] on your keyboard followed by the [**Enter Key**]



```
Security Onion Setup - 2.3.220
Select an option

  Install             Run the standard Security Onion installation
  Configure Network   Configure networking only

           <Ok>                    <Cancel>
```

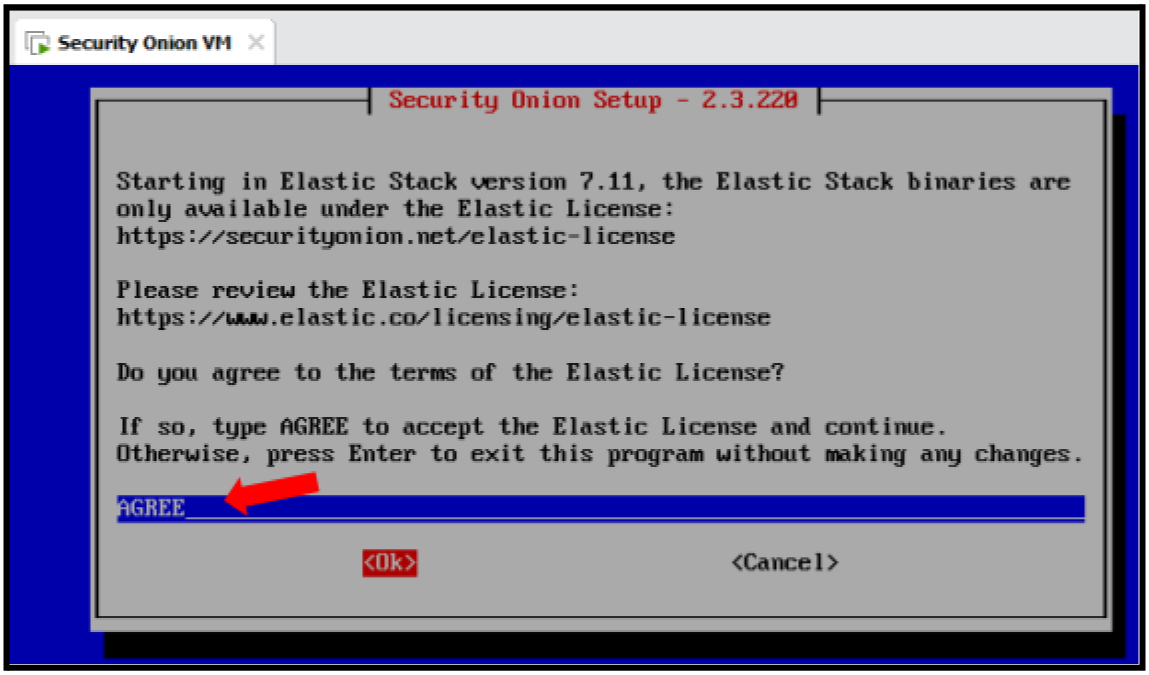
There are different modes of installation for Security Onion. For our lab environment we will use the **Evaluation Mode**. This mode is designed for a classroom or small lab environment. If you are interested in knowing more about the different installation modes of Security Onion refer to this page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

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



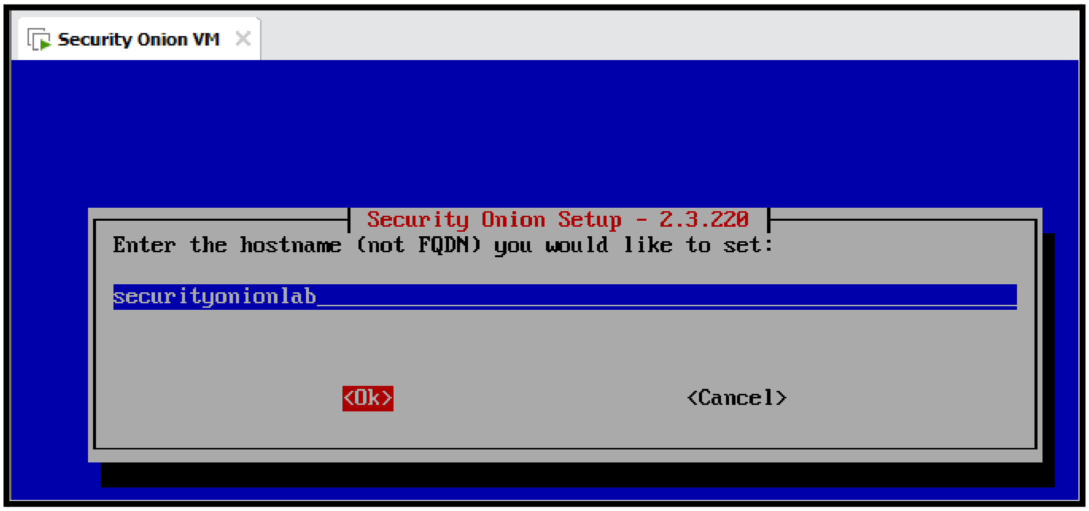
```
Security Onion Setup - 2.3.220
Choose install type.
See https://docs.securityonion.net/architecture for details.

(*) EVAL          Evaluation mode (not for production)
( ) STANDALONE    Standalone production install
( ) DISTRIBUTED   Distributed install submenu
( ) IMPORT        Standalone to import PCAP or log files
( ) OTHER         Other install types

            <Ok>                    <Cancel>
```

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



```
Security Onion Setup - 2.3.220

Starting in Elastic Stack version 7.11, the Elastic Stack binaries are
only available under the Elastic License:
https://securityonion.net/elastic-license

Please review the Elastic License:
https://www.elastic.co/licensing/elastic-license

Do you agree to the terms of the Elastic License?

If so, type AGREE to accept the Elastic License and continue.
Otherwise, press Enter to exit this program without making any changes.

AGREE_

            <Ok>                    <Cancel>
```

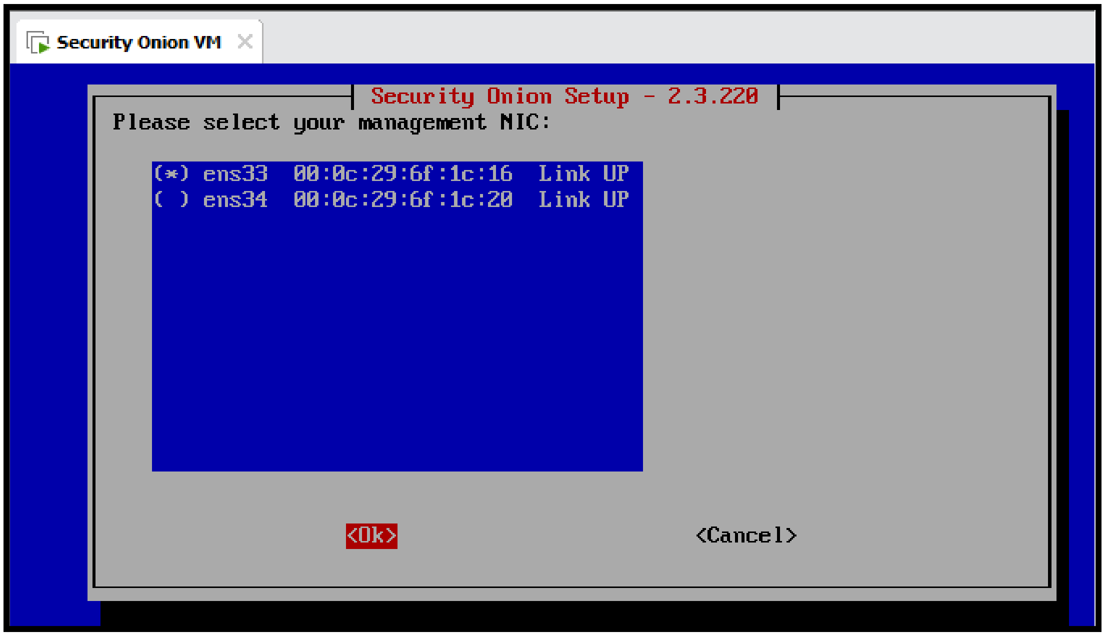
2.26. Change the hostname to [**securityonionlab**] then press the [**Tap Key**] followed by the [**Enter Key**]



```
Security Onion Setup - 2.3.220
Enter the hostname (not FQDN) you would like to set:

securityonionlab_

          <Ok>                          <Cancel>
```

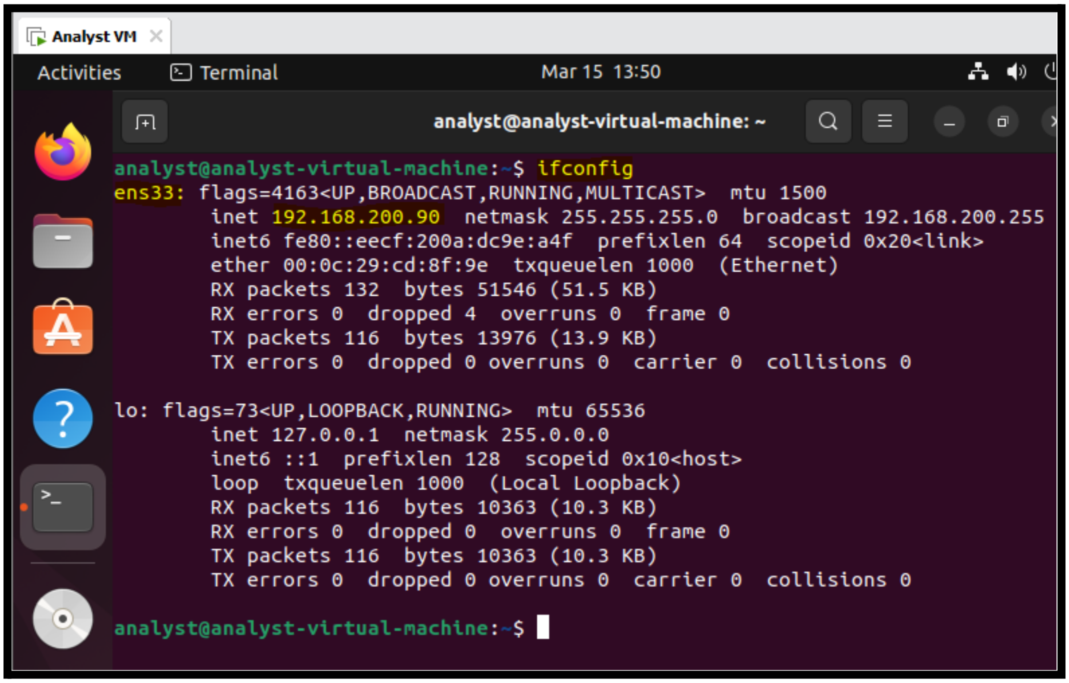
The following section is the most important part of the configuration process. If you could not complete this section correctly, you will have to reinstall the Security Onion VM from scratch.

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.



```
Security Onion Setup - 2.3.220
Please select your management NIC:

  (*) ens33  00:0c:29:6f:1c:16  Link UP
  ( ) ens34  00:0c:29:6f:1c:20  Link UP

          <Ok>                          <Cancel>
```

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**].

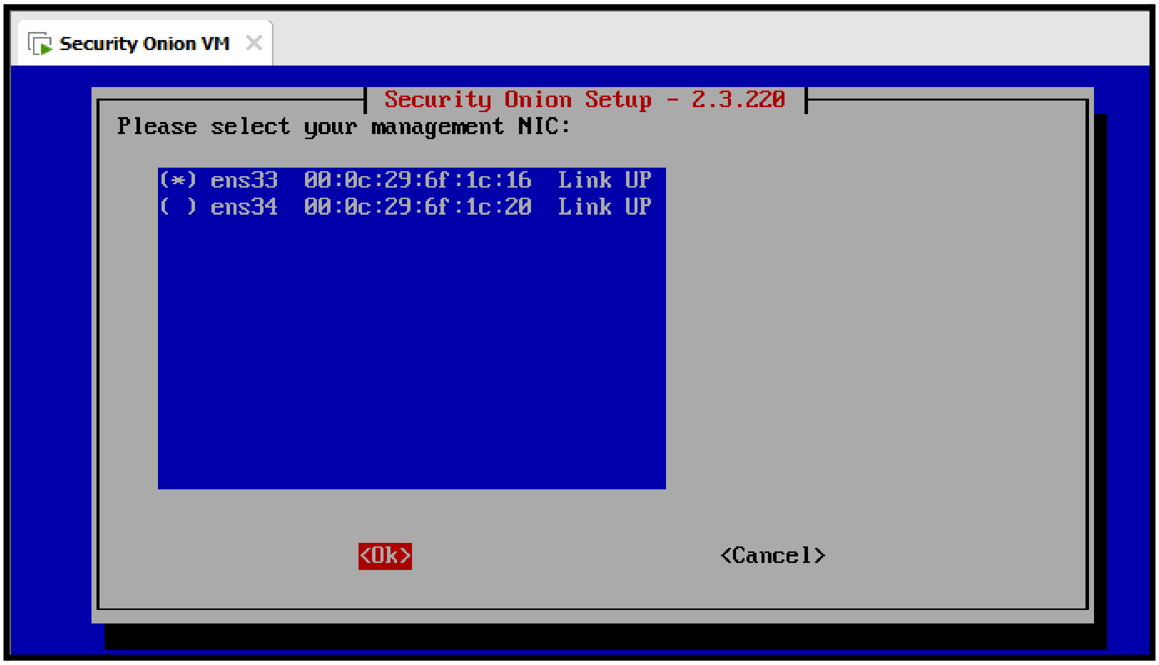


```
analyst@analyst-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.90  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::eecf:200a:dc9e:a4f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:cd:8f:9e  txqueuelen 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*.

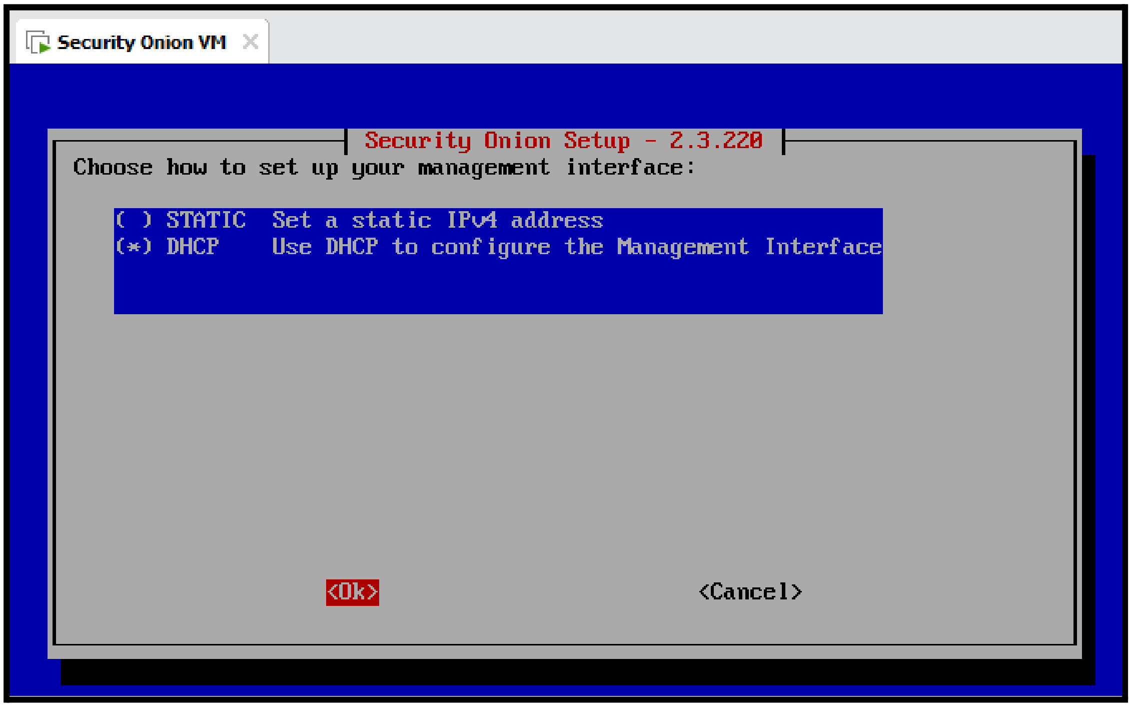
The name of the management interface may not be the same in your environment setup. You are required to fully understand the network setup (refer to the GitHub page of this lab). Additionally, you are required to correctly identify the interface for the *Management Network* and for the *Mentoring Network*.

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**].



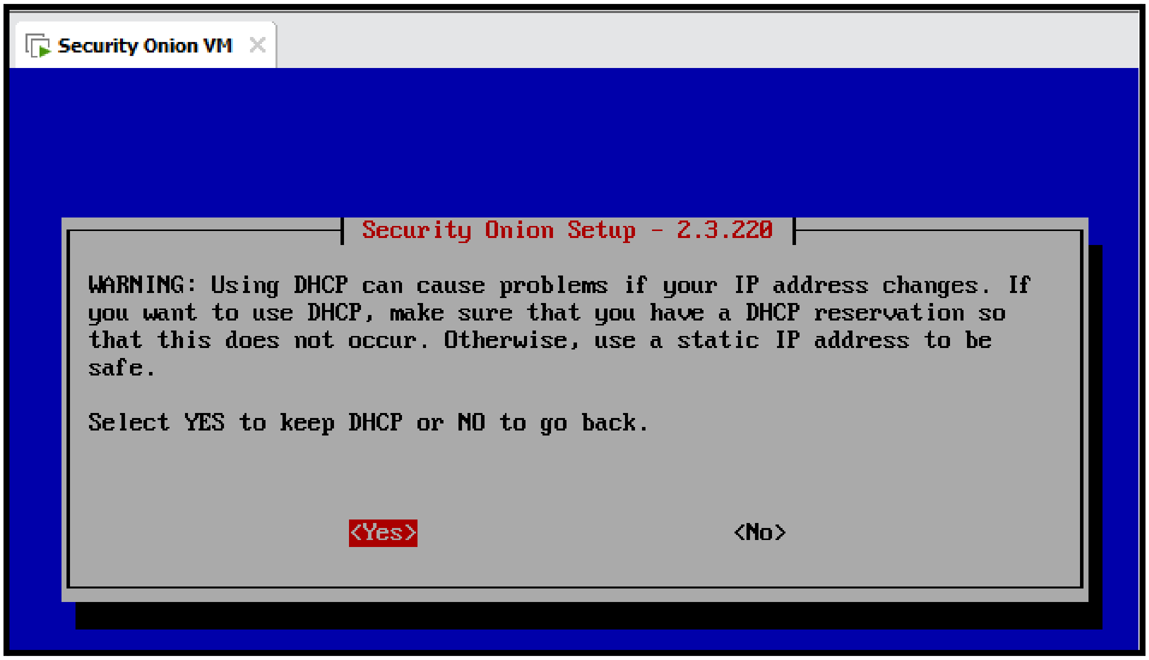
```
Security Onion Setup - 2.3.220
Please select your management NIC:

(*) ens33  00:0c:29:6f:1c:16  Link UP
( ) ens34  00:0c:29:6f:1c:20  Link UP

<Ok>                     <Cancel>
```

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



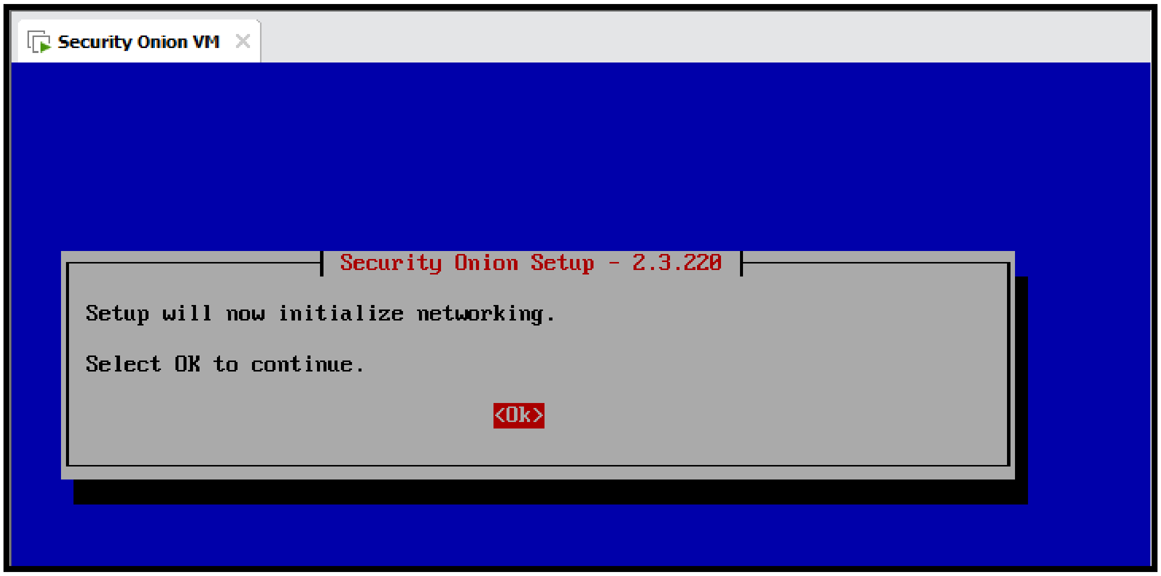
```
Security Onion Setup - 2.3.220
Choose how to set up your management interface:

( ) STATIC   Set a static IPv4 address
(*) DHCP     Use DHCP to configure the Management Interface

<Ok>                     <Cancel>
```

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



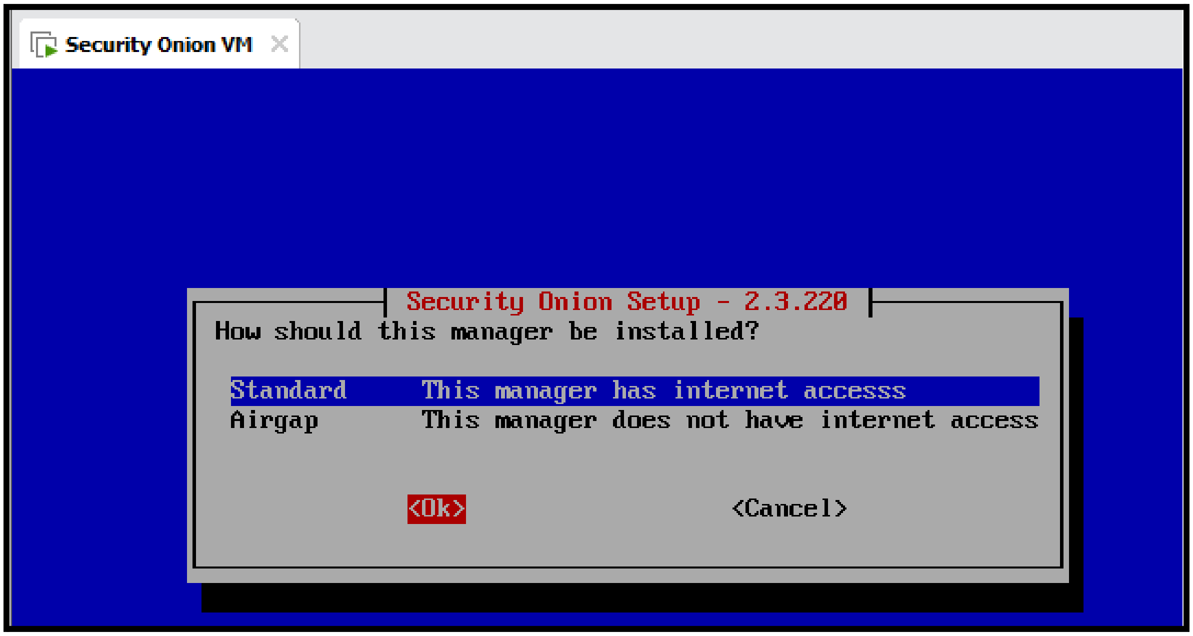
```
Security Onion Setup - 2.3.220

WARNING: Using DHCP can cause problems if your IP address changes. If
you want to use DHCP, make sure that you have a DHCP reservation so
that this does not occur. Otherwise, use a static IP address to be
safe.

Select YES to keep DHCP or NO to go back.

<Yes>                    <No>
```

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



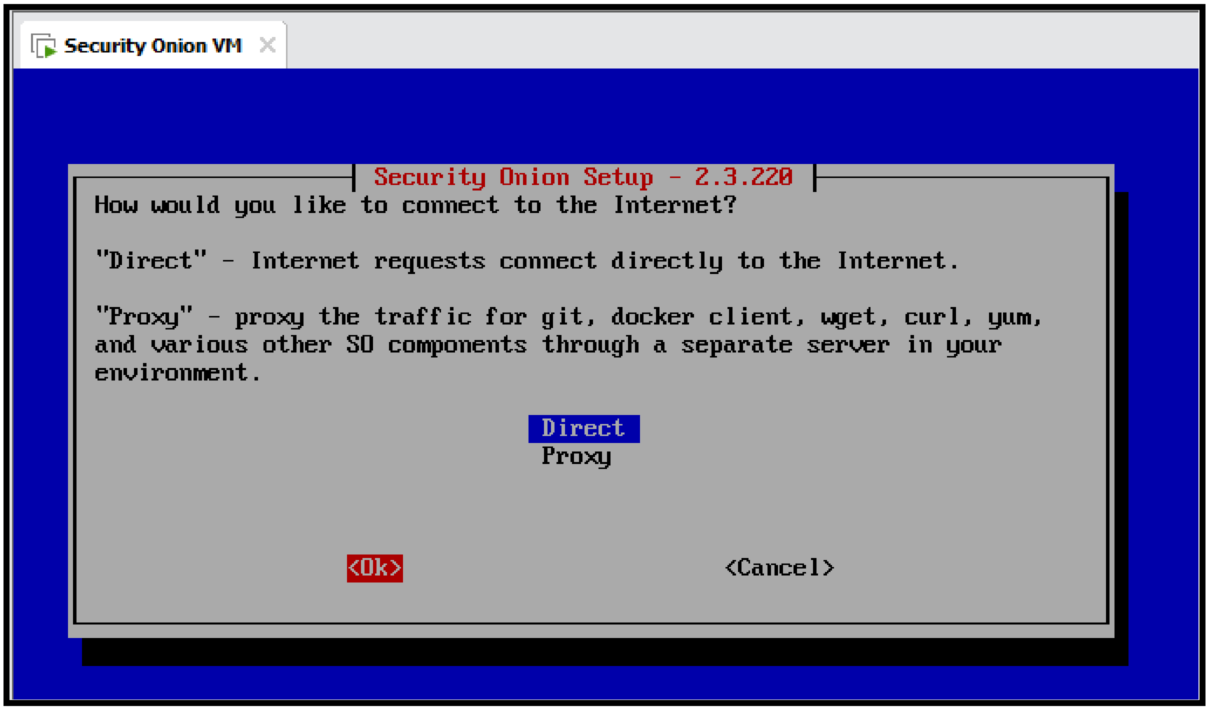
```
Security Onion Setup - 2.3.220

Setup will now initialize networking.

Select OK to continue.

<Ok>
```

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



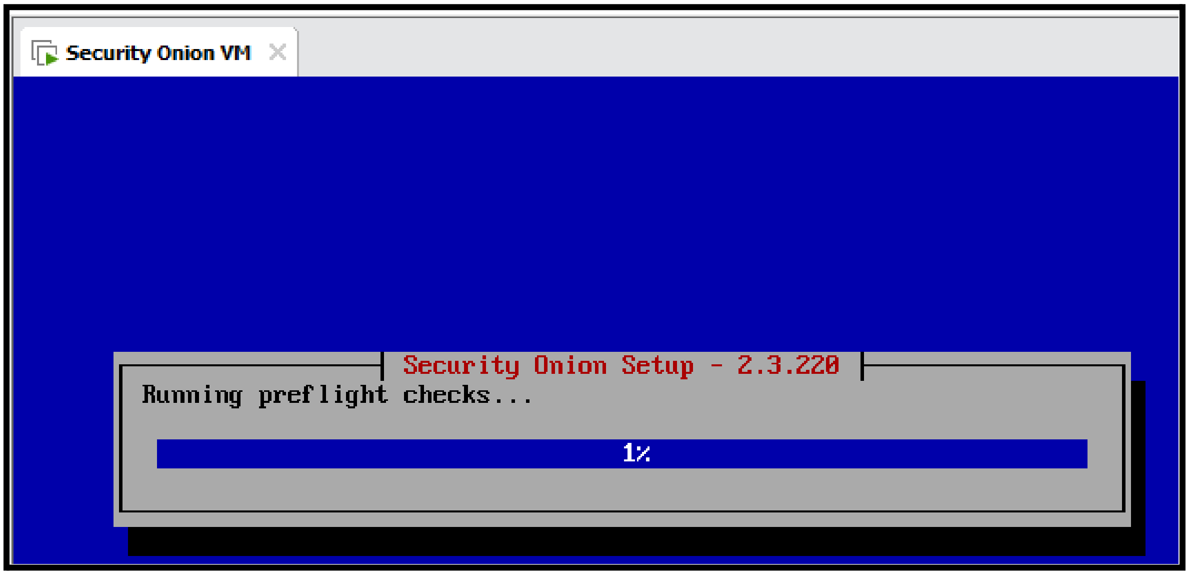
```
Security Onion Setup - 2.3.220
How should this manager be installed?

 Standard     This manager has internet accesss
 Airgap       This manager does not have internet access

            <Ok>                    <Cancel>
```

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



```
Security Onion Setup - 2.3.220
How would you like to connect to the Internet?

"Direct" - Internet requests connect directly to the Internet.

"Proxy" - proxy the traffic for git, docker client, wget, curl, yum,
and various other SO components through a separate server in your
environment.

                          Direct
                          Proxy

          <Ok>                       <Cancel>
```

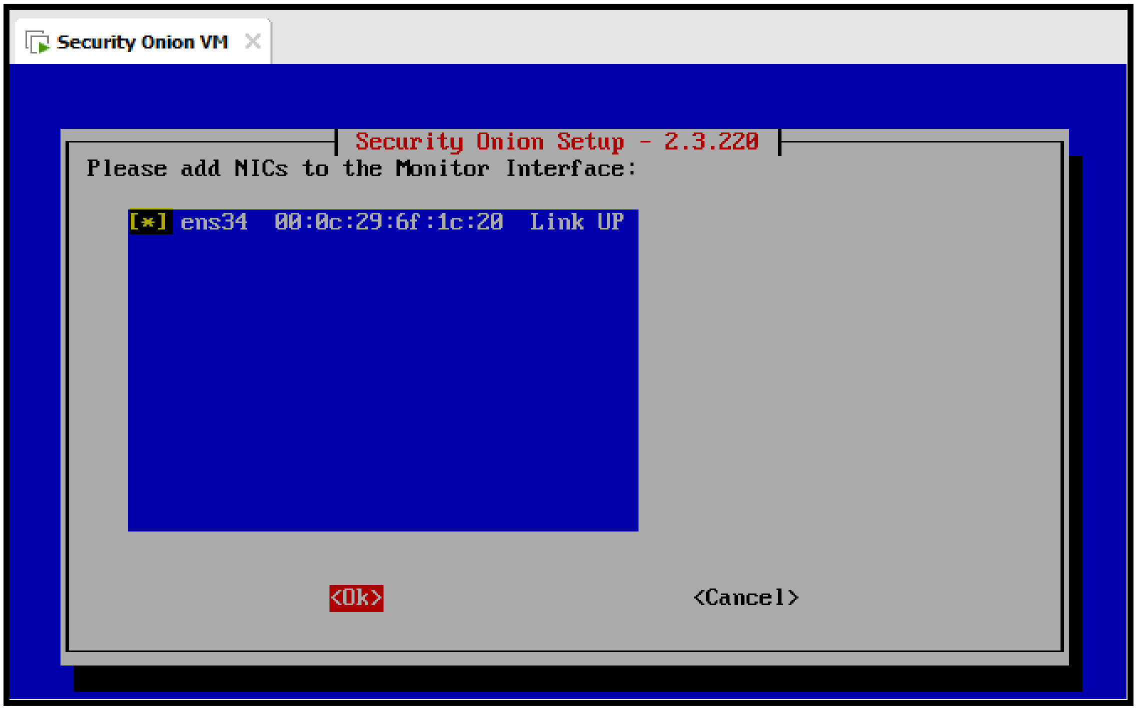
2.34. Wait a couple of minutes for the system to run all required checks.



```
Security Onion Setup - 2.3.220
Running preflight checks...
1%
```

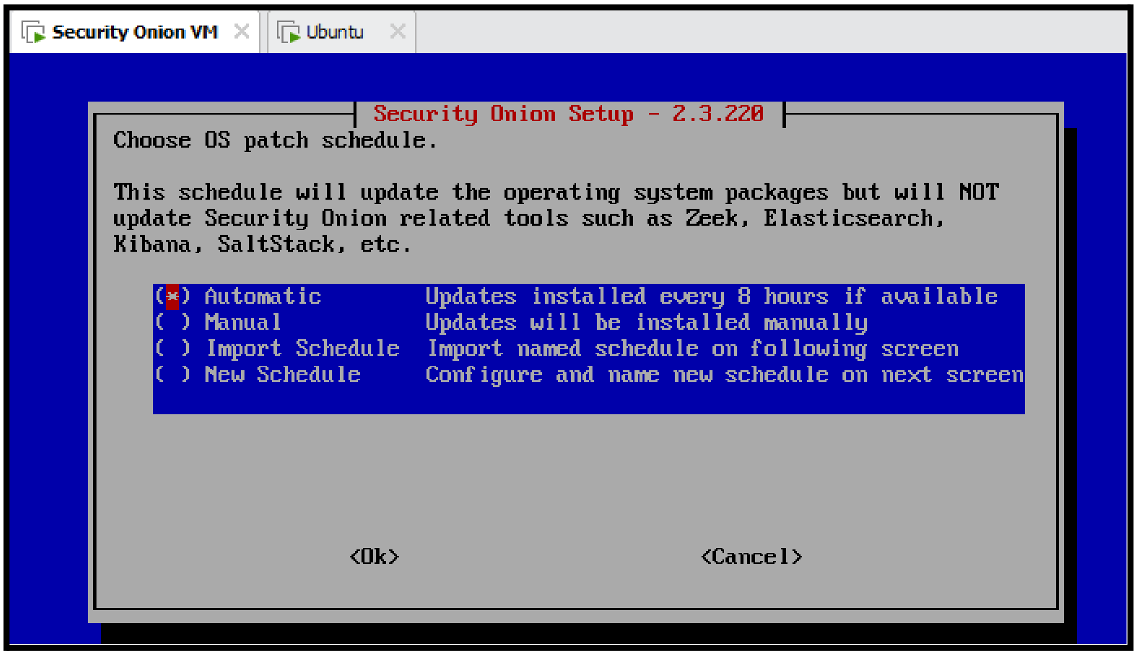
Now we should select the *Monitor Network Interface*. If you correctly identify the *Management Network Interface* previously, then the interface that will be shown in this window should be the correct Monitor Interface.

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



```
Security Onion Setup - 2.3.220
Please add NICs to the Monitor Interface:

[*] ens34   00:0c:29:6f:1c:20   Link UP
```

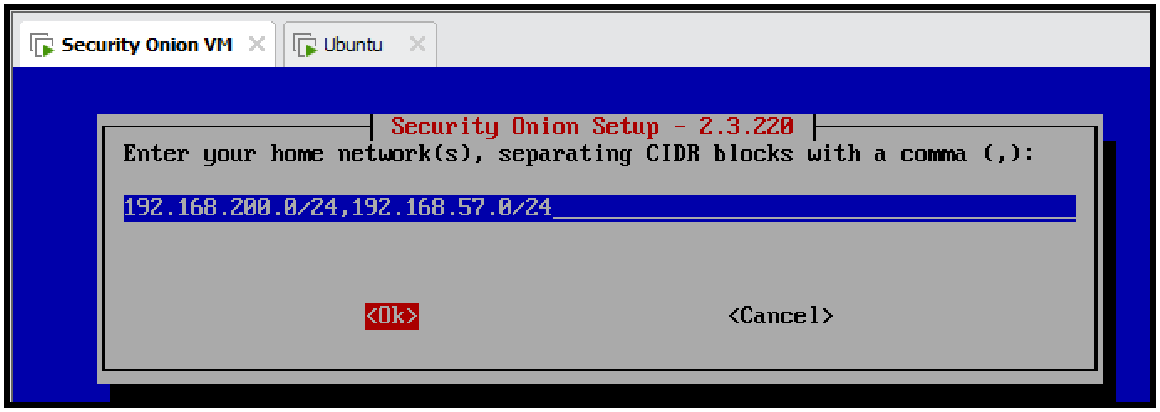
2.36. Set the OS patch schedule to [**Automatic**]



```
Security Onion Setup - 2.3.220
Choose OS patch schedule.

This schedule will update the operating system packages but will NOT
update Security Onion related tools such as Zeek, Elasticsearch,
Kibana, SaltStack, etc.

(*) Automatic          Updates installed every 8 hours if available
( ) Manual             Updates will be installed manually
( ) Import Schedule    Import named schedule on following screen
( ) New Schedule       Configure and name new schedule on next screen

              <Ok>                         <Cancel>
```

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

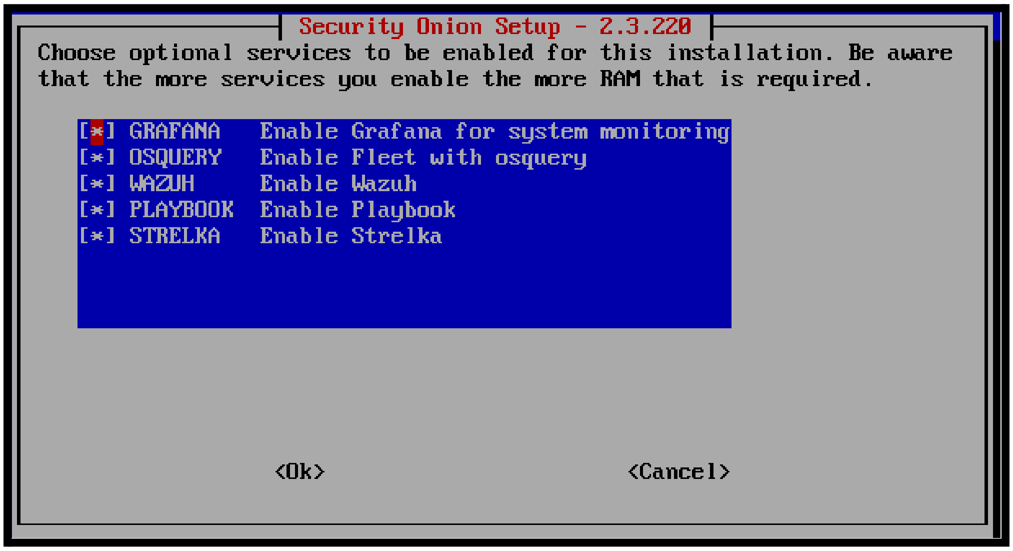
A CIDR address looks like a normal IP address, except that it ends with a slash followed by a number. By now you should be able to figure out the CIDR of the Management Network from the IP Address of the Analyst. In our own lab environment, we found that the Analyst IP Address is 192.168.200.90. This 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.



```
Security Onion Setup - 2.3.220
Enter your home network(s), separating CIDR blocks with a comma (,):

192.168.200.0/24,192.168.57.0/24

            <Ok>                          <Cancel>
```

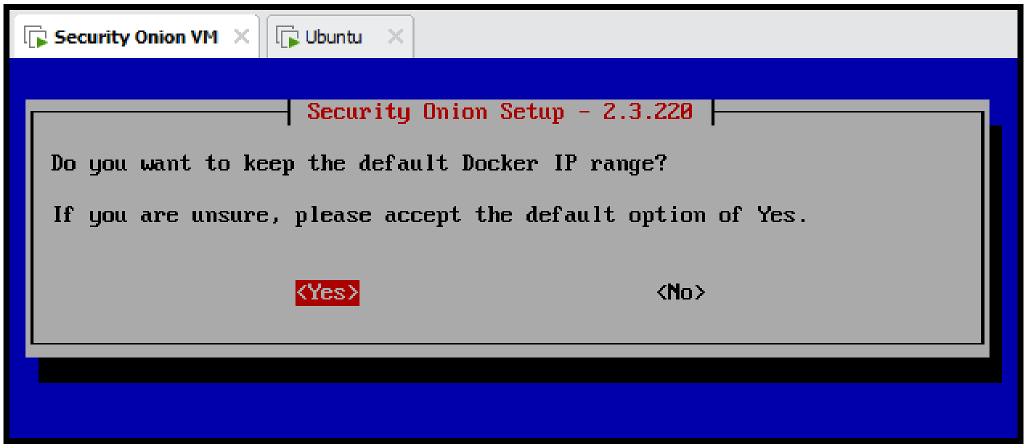
2.38. **After** you finish the previous step, make sure that your Analyst VM is connected to the Management Network only [**VMnet0**].

2.39. Make sure all services are enabled and then press [**Tap Key**] followed by the [**Enter Key**]



```
Security Onion Setup - 2.3.220
Choose optional services to be enabled for this installation. Be aware
that the more services you enable the more RAM that is required.

[*] GRAFANA   Enable Grafana for system monitoring
[*] OSQUERY   Enable Fleet with osquery
[*] WAZUH     Enable Wazuh
[*] PLAYBOOK  Enable Playbook
[*] STRELKA   Enable Strelka

            <Ok>                          <Cancel>
```

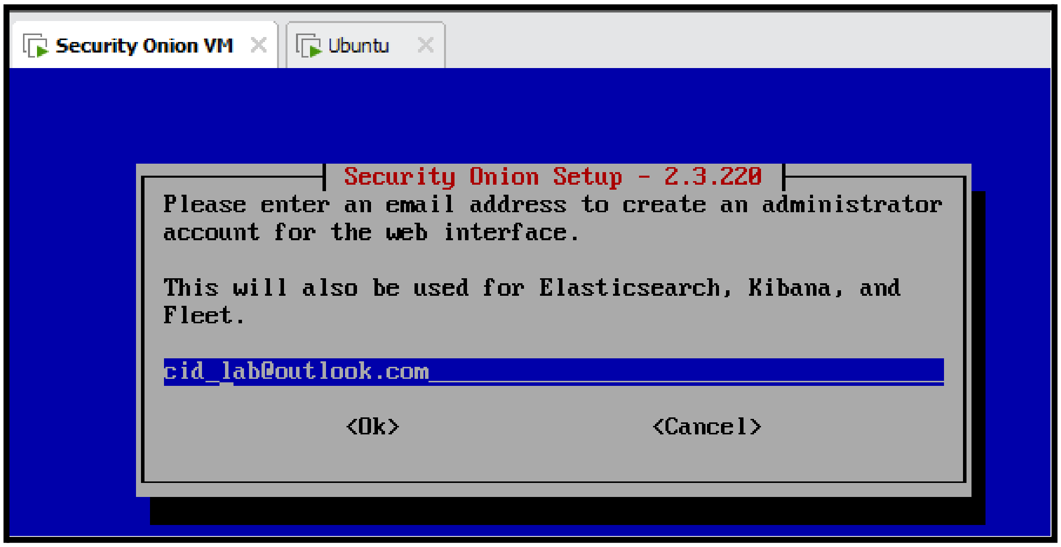
2.40. Select Yes and press [**Enter Key**]



```
Security Onion Setup - 2.3.220

Do you want to keep the default Docker IP range?

If you are unsure, please accept the default option of Yes.

<Yes>                    <No>
```

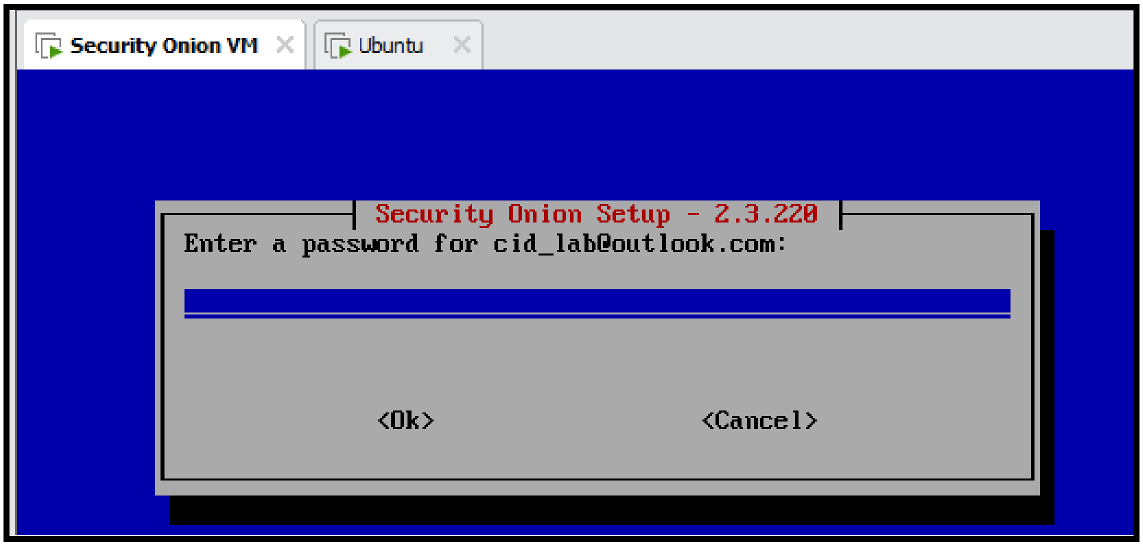
2.41. Type the email address that will be used to access the web interface of the Security Onion Manager

Setup the email address to [**cid_lab@outlook.com**]



```
Security Onion Setup - 2.3.220
Please enter an email address to create an administrator
account for the web interface.

This will also be used for Elasticsearch, Kibana, and
Fleet.

cid_lab@outlook.com

<Ok>                    <Cancel>
```

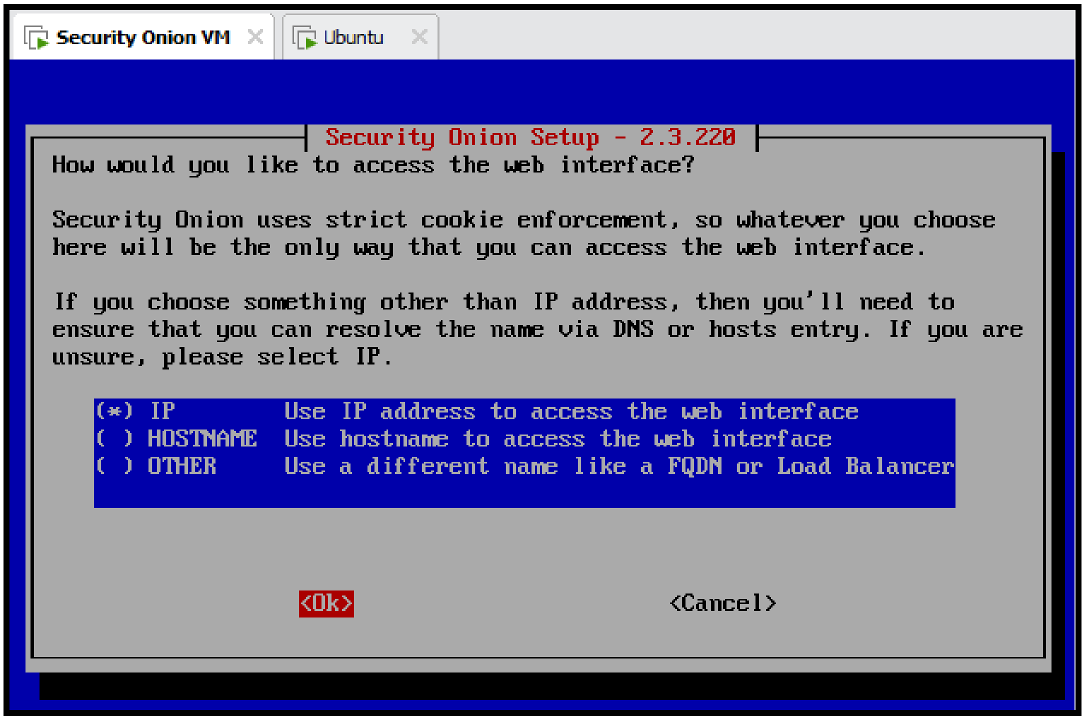
2.42. Set up a password that will be used to access the web interface of the Security Onion Manager
Password: **cid_lab@123**



```
Security Onion Setup - 2.3.220
Enter a password for cid_lab@outlook.com:

<Ok>                    <Cancel>
```

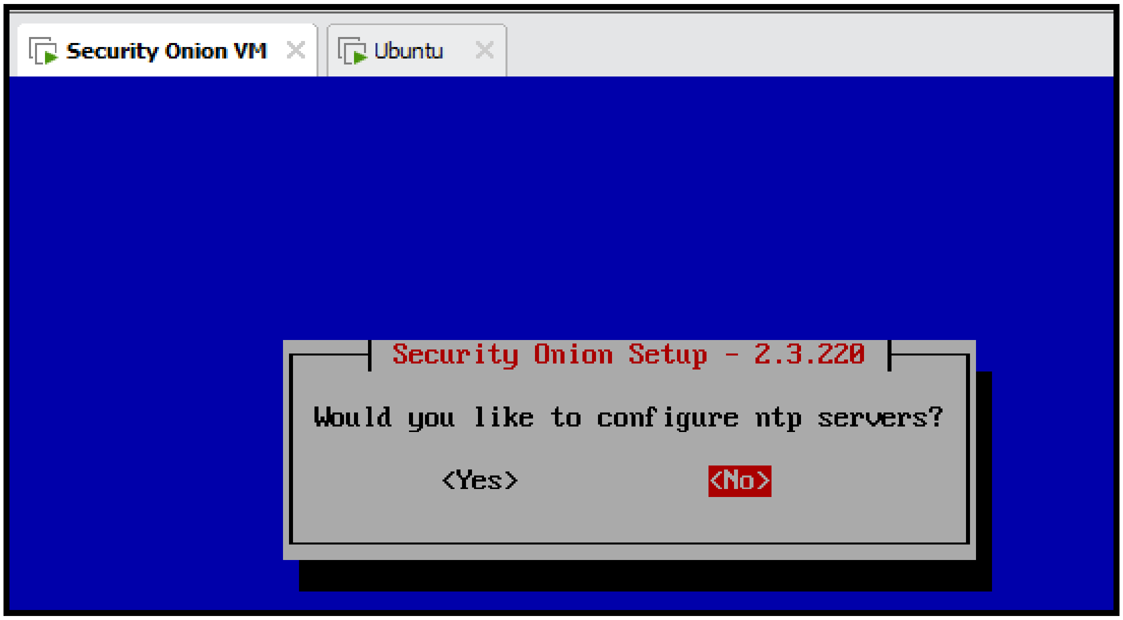
2.43. Then reenter the password for confirmation.

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**].



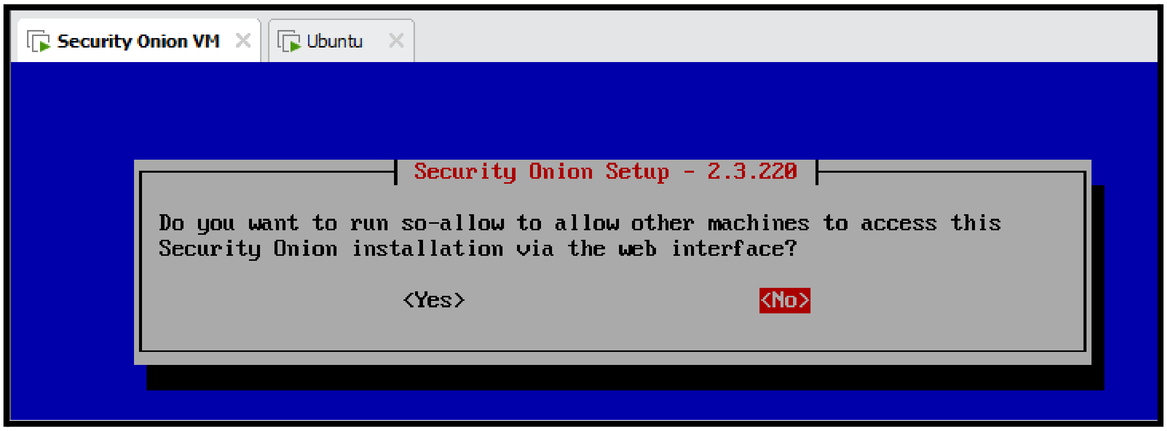
```
Security Onion Setup - 2.3.220
How would you like to access the web interface?

Security Onion uses strict cookie enforcement, so whatever you choose
here will be the only way that you can access the web interface.

If you choose something other than IP address, then you'll need to
ensure that you can resolve the name via DNS or hosts entry. If you are
unsure, please select IP.

   (*) IP         Use IP address to access the web interface
   ( ) HOSTNAME   Use hostname to access the web interface
   ( ) OTHER      Use a different name like a FQDN or Load Balancer

                <Ok>                    <Cancel>
```

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



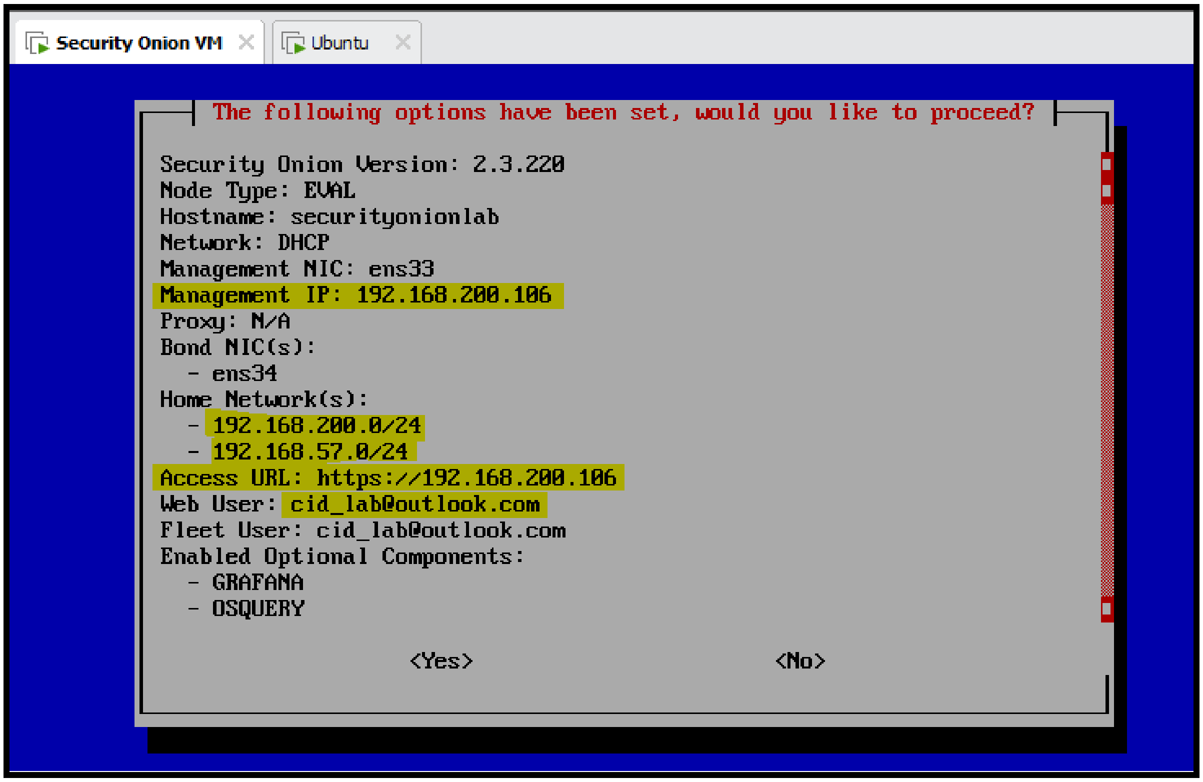
Would you like to configure ntp servers?

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.



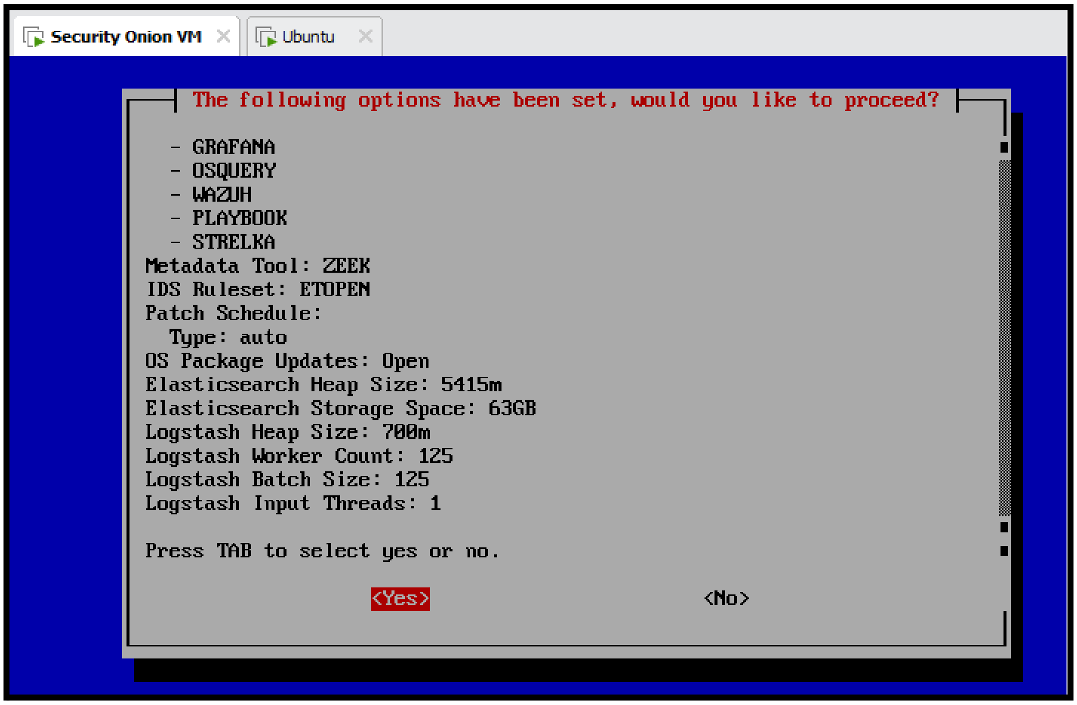
Do you want to run so-allow to allow other machines to access this Security Onion installation via the web interface?

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.



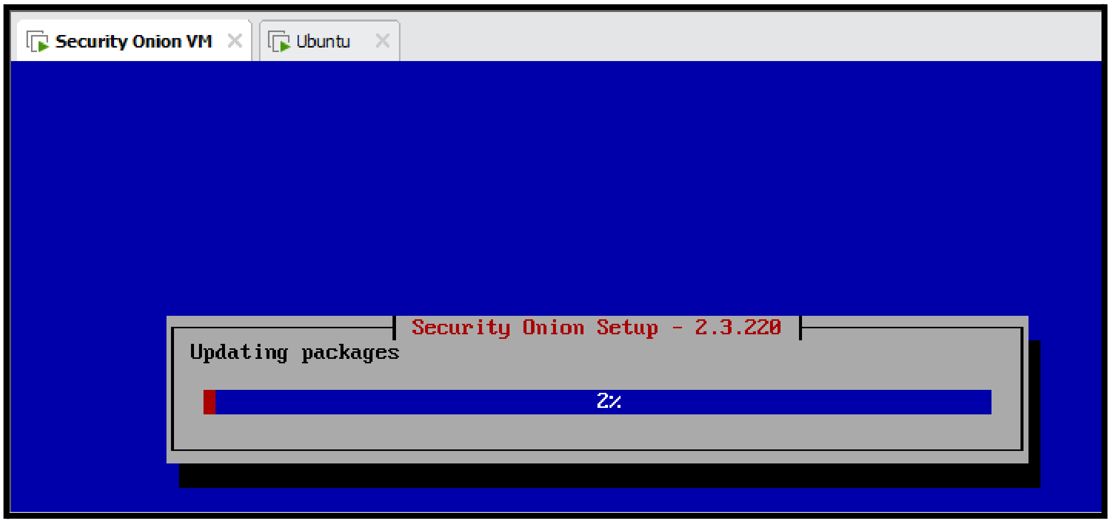
```
The following options have been set, would you like to proceed?

Security Onion Version: 2.3.220
Node Type: EVAL
Hostname: securityonionlab
Network: DHCP
Management NIC: ens33
Management IP: 192.168.200.106
Proxy: N/A
Bond NIC(s):
  - ens34
Home Network(s):
  - 192.168.200.0/24
  - 192.168.57.0/24
Access URL: https://192.168.200.106
Web User: cid_lab@outlook.com
Fleet User: cid_lab@outlook.com
Enabled Optional Components:
  - GRAFANA
  - OSQUERY

                    <Yes>                       <No>
```

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



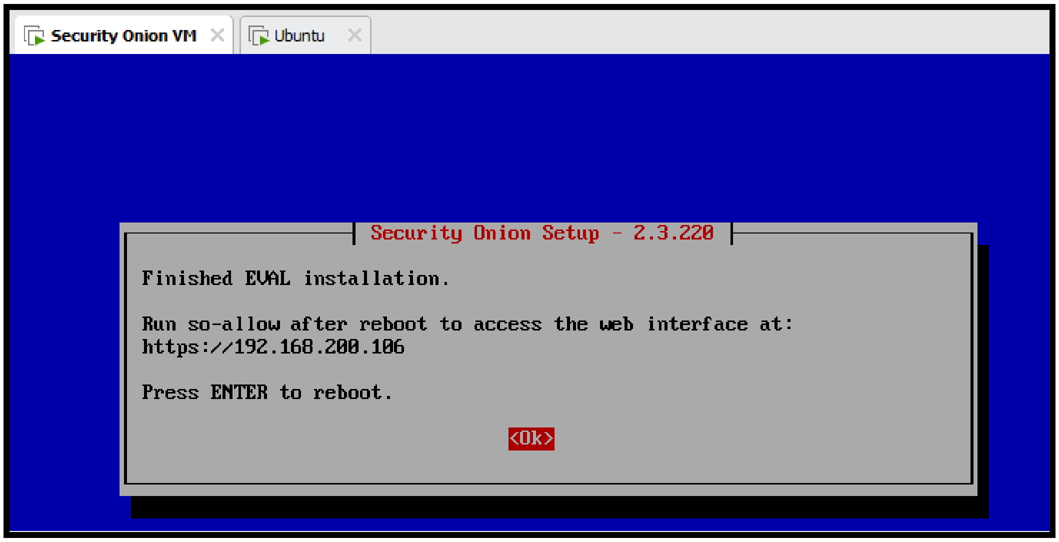
```
The following options have been set, would you like to proceed?

  - GRAFANA
  - OSQUERY
  - WAZUH
  - PLAYBOOK
  - STRELKA
Metadata Tool: ZEEK
IDS Ruleset: ETOPEN
Patch Schedule:
  Type: auto
OS Package Updates: Open
Elasticsearch Heap Size: 5415m
Elasticsearch Storage Space: 63GB
Logstash Heap Size: 700m
Logstash Worker Count: 125
Logstash Batch Size: 125
Logstash Input Threads: 1

Press TAB to select yes or no.

                    <Yes>                       <No>
```

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



```
Security Onion Setup - 2.3.220
Updating packages
2%
```

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



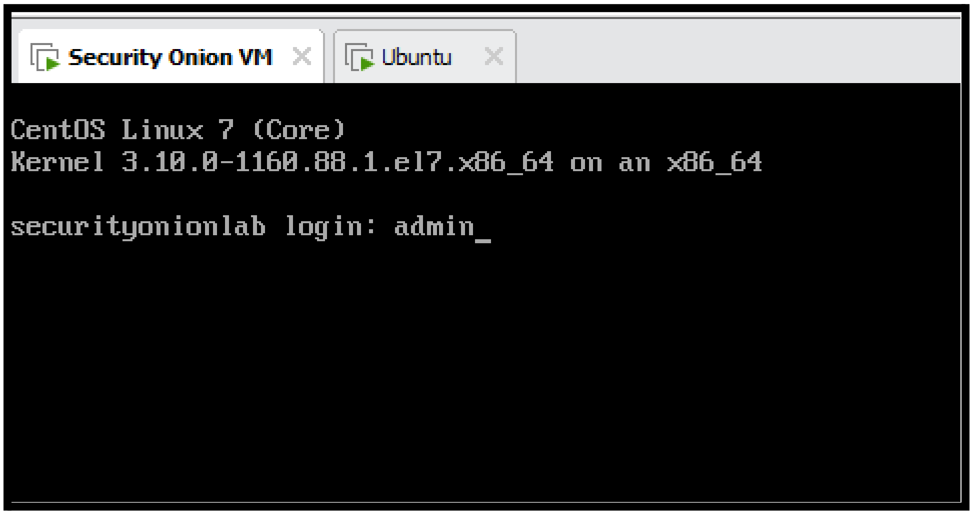
```
Security Onion Setup - 2.3.220
Finished EVAL installation.

Run so-allow after reboot to access the web interface at:
https://192.168.200.106

Press ENTER to reboot.

<Ok>
```

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

3. Connect the Analyst VM to Security Onion VM

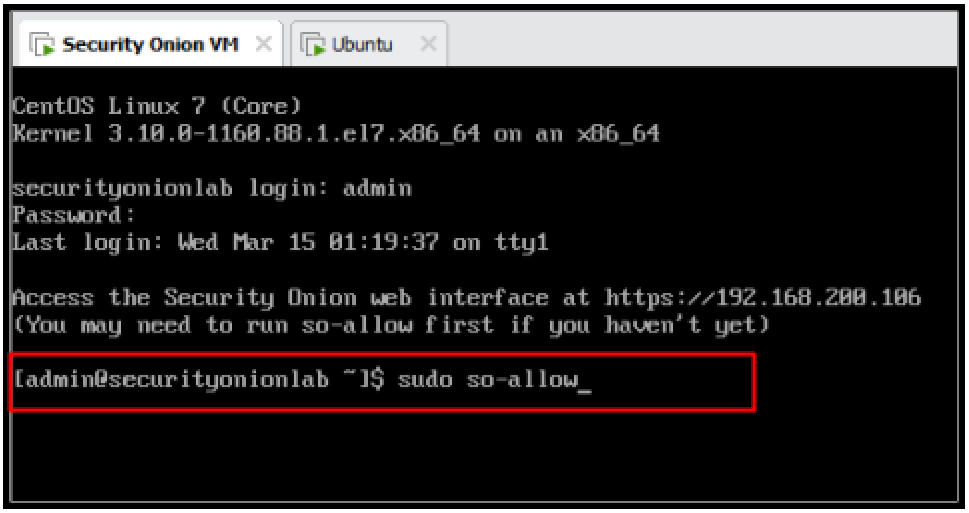
Now we will configure the so-allow utility that will enable the Analyst Machine to connect to Security Onion Interface through the web. This section should be followed right after installing and configuring Security Onion VM.

3.1. After you reboot Security Onion VM, enter your login information.
Username: admin
Password: admin



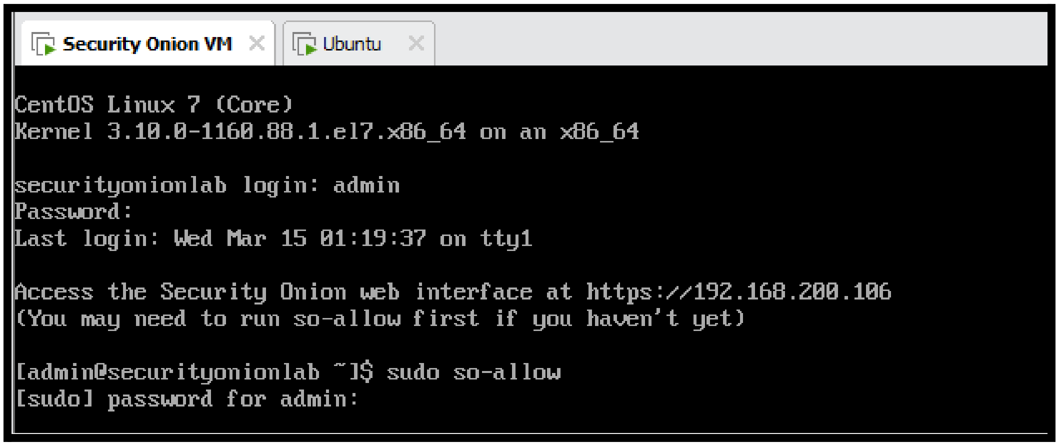
```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.88.1.el7.x86_64 on an x86_64

securityonionlab login: admin_
```

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



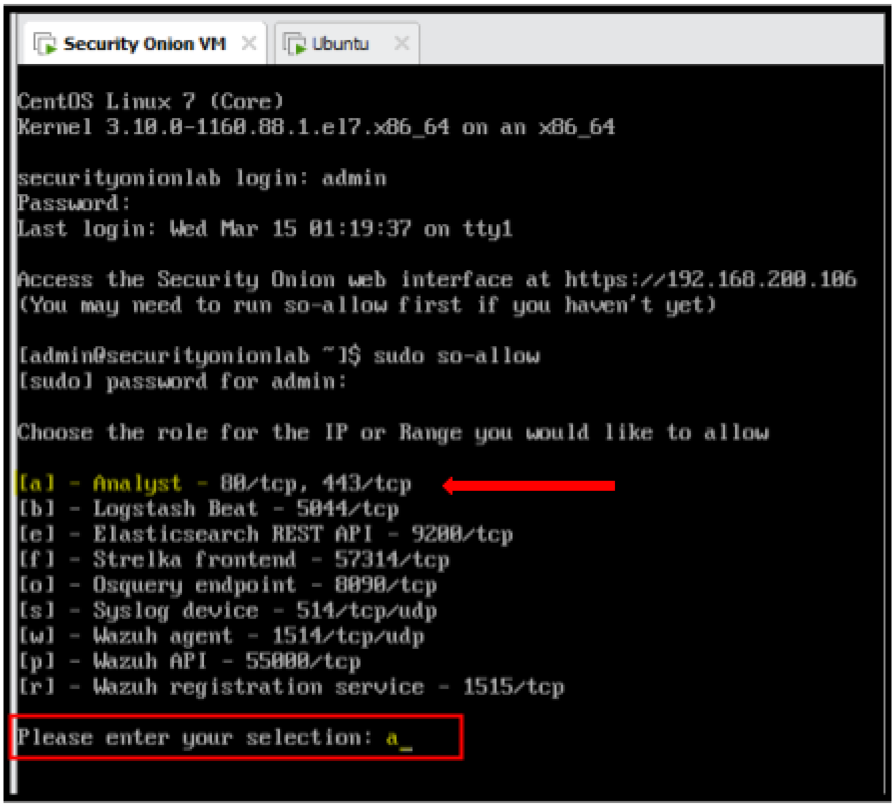
```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.88.1.el7.x86_64 on an x86_64

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]



```
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:
```

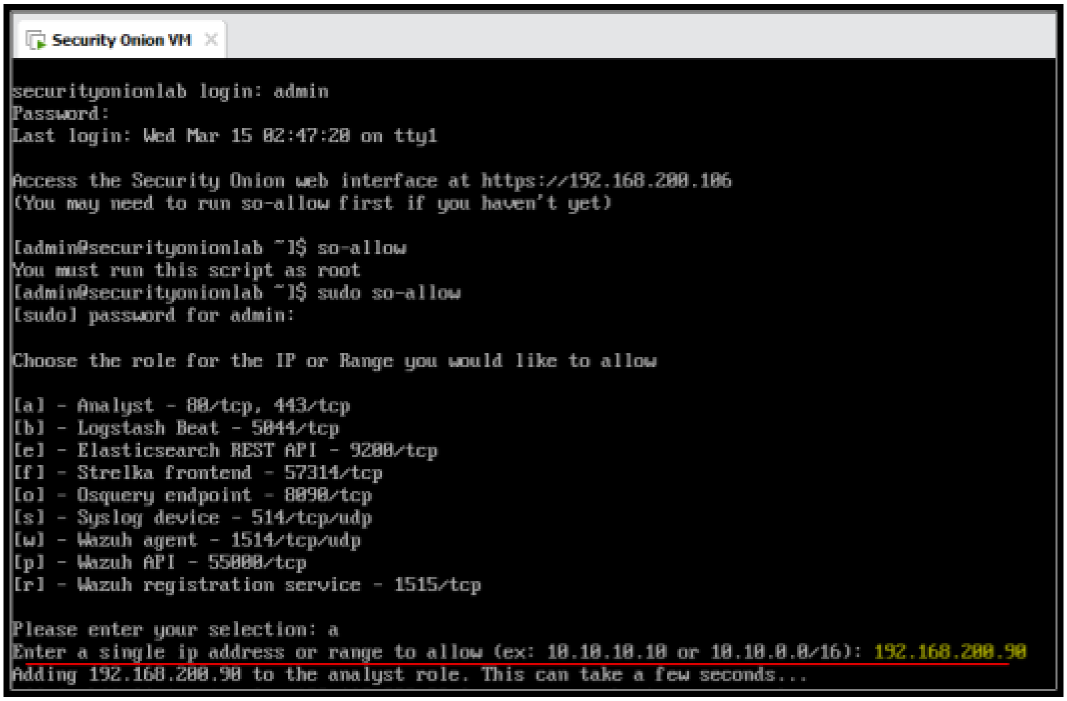
3.4. There are a set of roles that you could configure. To allow the Analyst role, type the letter **[a]** and press **[Enter Key]**



```
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 - 80/tcp, 443/tcp
[b] - Logstash Beat - 5044/tcp
[e] - Elasticsearch REST API - 9200/tcp
[f] - Strelka frontend - 57314/tcp
[o] - Osquery endpoint - 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection: a_
```

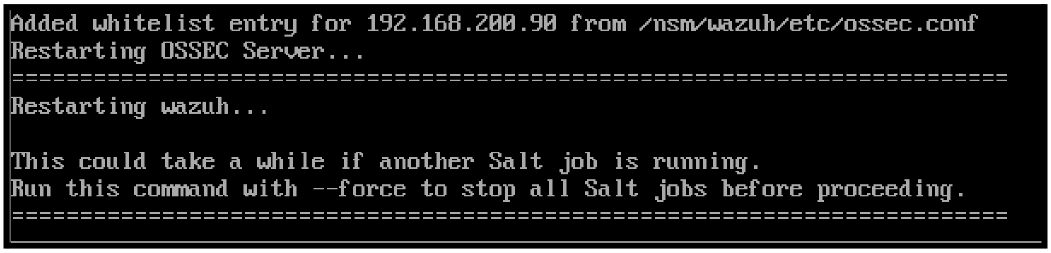
3.5. Then you should specify the IP address that you will allow for the analyst role. This should be the IP Address of your Analyst VM that is connected to VMnet0 (Management Network). Based on our environment setup the Analyst machine have the IP Address: 192.168.200.90

3.6. Enter the IP address of your Analyst VM then press [Enter Key]



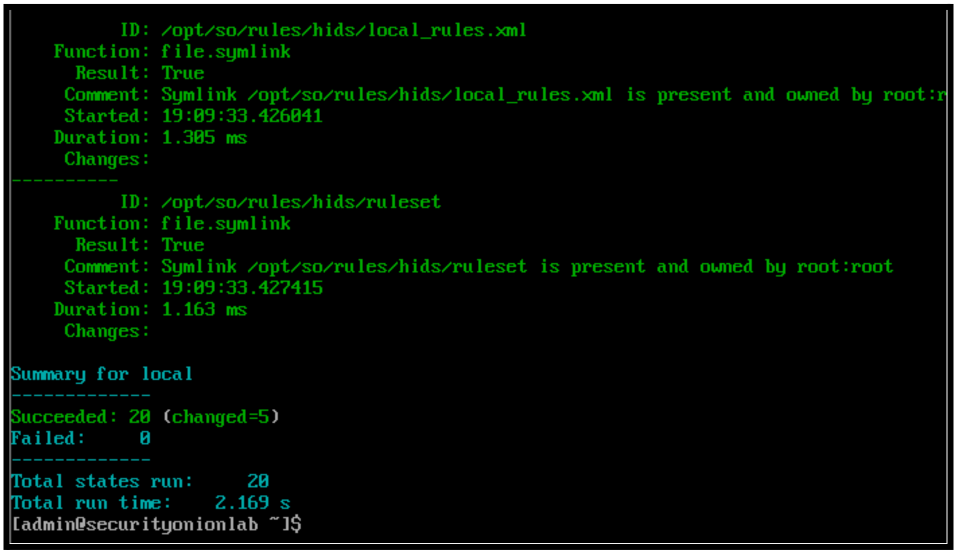
```
securityonionlab login: admin
Password:
Last login: Wed Mar 15 02:47:20 on tty1

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
[e] - Elasticsearch REST API - 9200/tcp
[f] - Strelka frontend - 57314/tcp
[o] - Osquery endpoint - 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55000/tcp
[r] - 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.



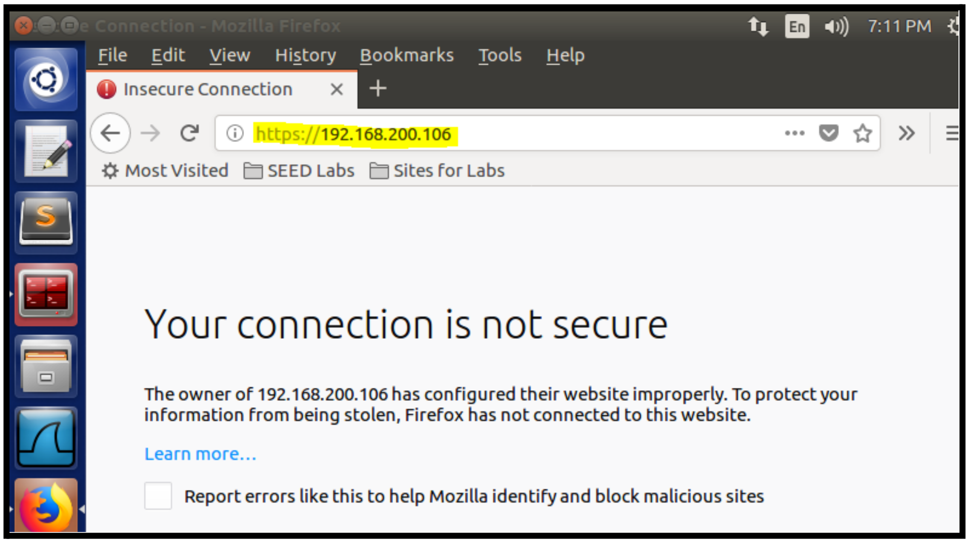
```
Added whitelist entry for 192.168.200.90 from /nsm/wazuh/etc/ossec.conf
Restarting OSSEC Server...
=========================================================================
Restarting wazuh...

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.**



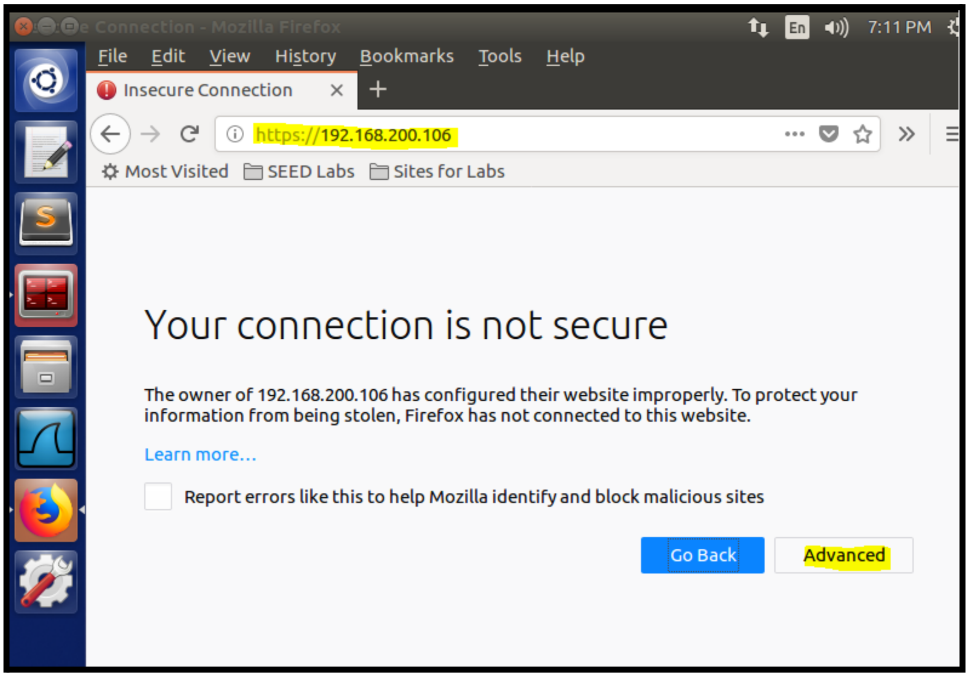
Your connection is not secure

The owner of 192.168.200.106 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

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



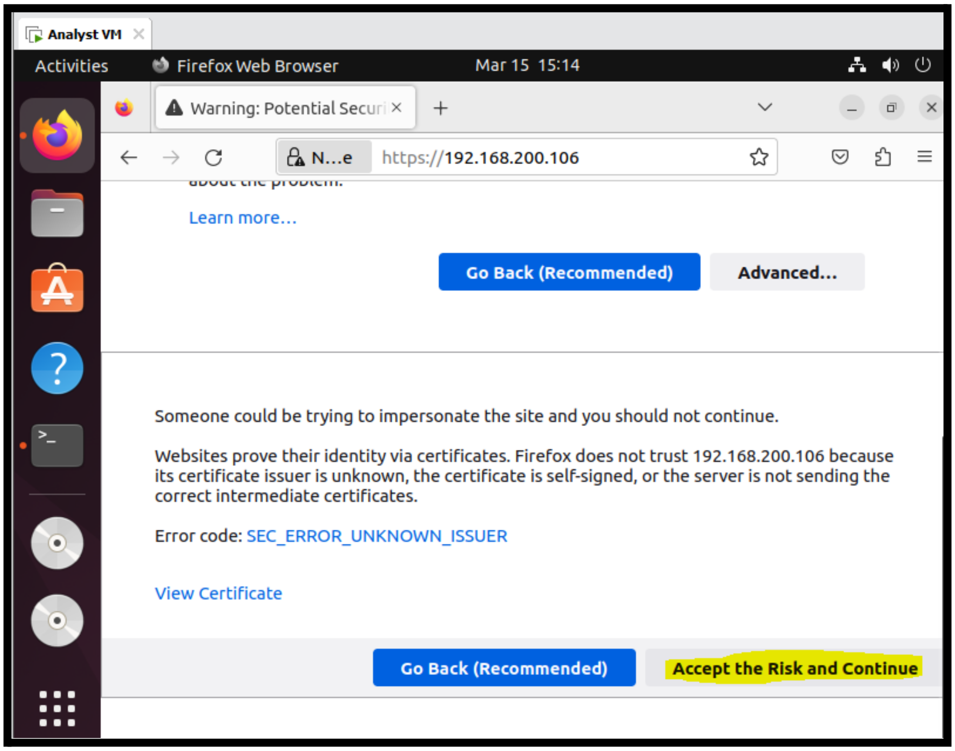
Your connection is not secure

The owner of 192.168.200.106 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

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



about the problem.

Learn more…

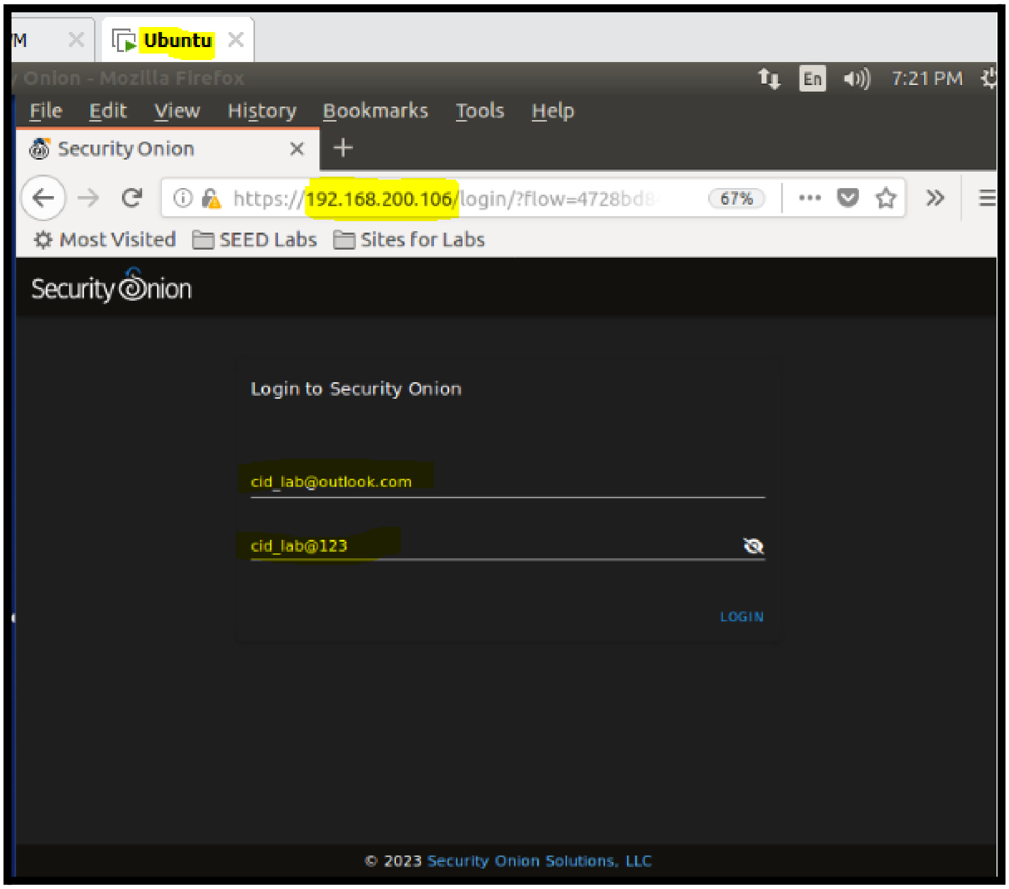
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.200.106 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

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



Ubuntu
Onion - Mozilla Firefox
7:21 PM
File Edit View History Bookmarks Tools Help
Security Onion
https://192.168.200.106/login/?flow=4728bd8
67%
Most Visited
SEED Labs
Sites for Labs
Security Onion

Login to Security Onion

cid_lab@outlook.com

cid_lab@123

LOGIN
© 2023 Security Onion Solutions, LLC

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