Security Onion: Install and Initial Deployment

Branson Bailey

Home Lab Project

2 October 2024

Table of Contents

Project Focus

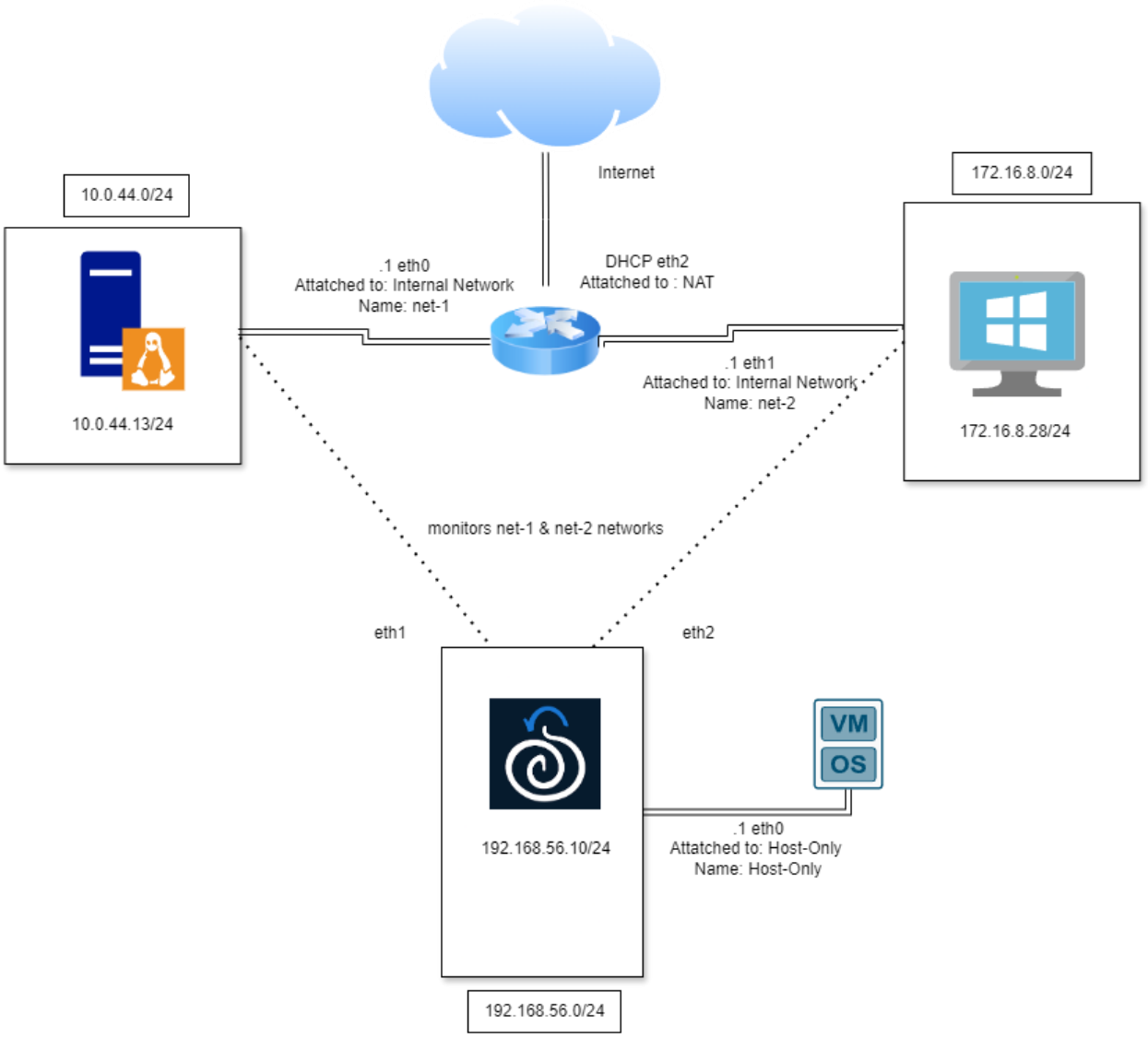
The focus of this project is to deploy Security Onion (2.4.100-20240903 ISO) in a home lab environment for hands-on traffic analysis. I will simulate real-world network scenarios, aiming to enhance my skills in threat detection and network monitoring using tools like Suricata, Zeek, and Elasticsearch. This setup provides a controlled environment for capturing and analyzing network traffic, improving the ability to detect and respond to cyber threats effectively.

Project Section Focus

The focus of this project section is to complete an initial installation and setup of Security Onion (2.4.100-20240903 ISO). The goal is to configure the platform's core components, such as Suricata, Zeek, and Elasticsearch, to ensure proper network traffic capture and analysis. I will work to establish a functional environment that will act as the base level for the rest of this project.

The Security Onion VM will be placed in a virtual network with a VyOS router, a Windows 11 VM, and an Ubuntu VM.

Attached below is a basic overview of the desired network topology for this home lab project:

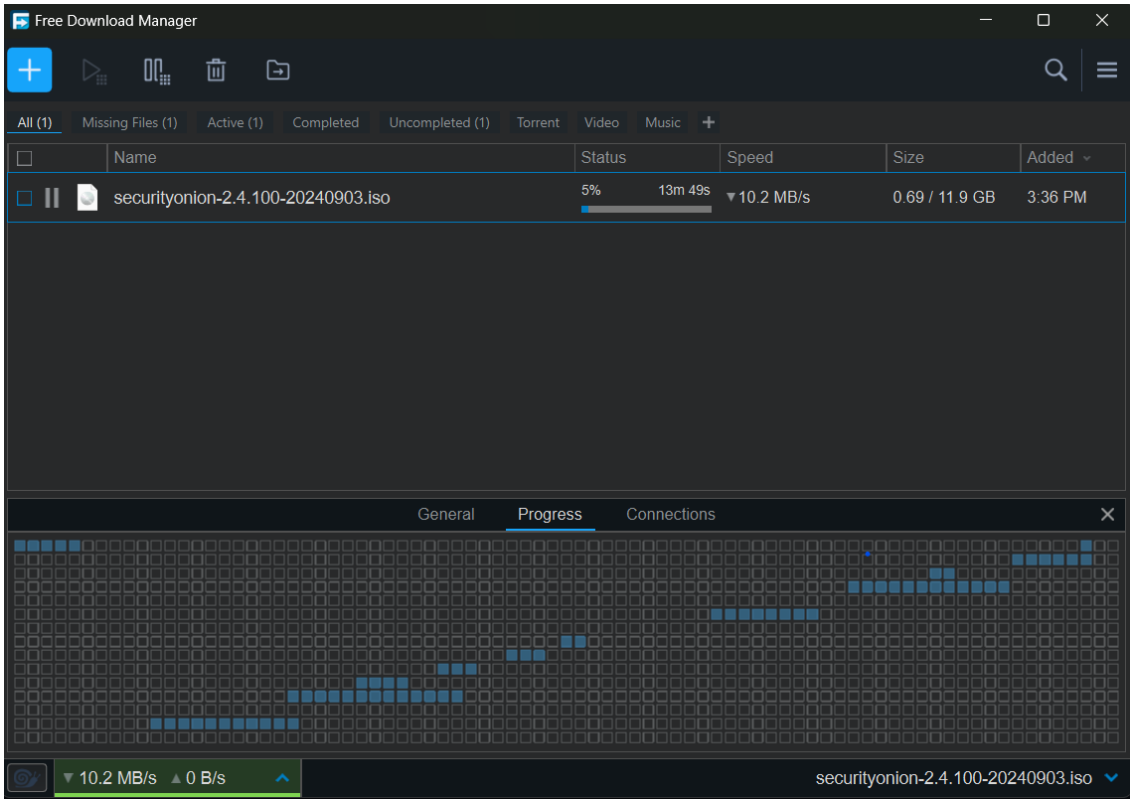


Network Topology

Install & Deployment process

In this part, I will display the process of the initial installation of Security Onion.

Link to ISO image: https://download.securityonion.net/file/securityonion/securityonion-2.4.100-20240903.iso



Installing ISO file

Initial Setup/Deployment

In this part, I will display the initial setup/deployment process of the network & Security Onion.

```
ethernet eth0 {
    address 10.0.44.1/24
    duplex auto
    hw-id 08:00:27:a0:ea:e4
    smp_affinity auto
    speed auto
}
ethernet eth1 {
    address 172.16.8.1/24
    duplex auto
    hw-id 08:00:27:60:aa:0d
    smp_affinity auto
    speed auto
}
ethernet eth2 {
    address dhcp
    duplex auto
    hw-id 08:00:27:b2:ee:4c
    smp_affinity auto
    speed auto
}
loopback lo {
}
[edit]
vyos@vyos# _
```

Setting up interfaces in VyOS

```
rule 10 {
    description "Network for Ubuntu"
    outbound-interface eth3
    source {
        address 10.0.44.0/24
    }
    translation {
        address masquerade
    }
}
```

Setting NAT source rules for Ubuntu network in VyOS

```
rule 20 {
    description "Network for Windows"
    outbound-interface eth3
    source {
        address 172.16.8.0/24
    }
    translation {
        address masquerade
    }
}
```

Setting NAT source rules for Windows network in VyOS

```
[edit]
vyos@vyos# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=54 time=9.28 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=54 time=9.01 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 9.017/9.153/9.289/0.136 ms
[edit]
vyos@vyos#
```

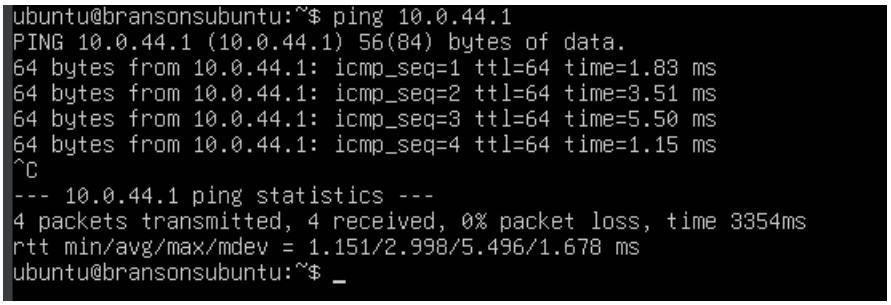
Testing Internet connectivity in VyOS

```
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  renderer: networkd
  ethernets:
        enp0s3:
                addresses:
                        - 10.0.44.13/24
                gateway4: 10.0.44.1
                nameservers:
                        addresses:
                                - 8.8.8.8
                                - 8.8.4.4
~
~
~
~
~
~
~
```

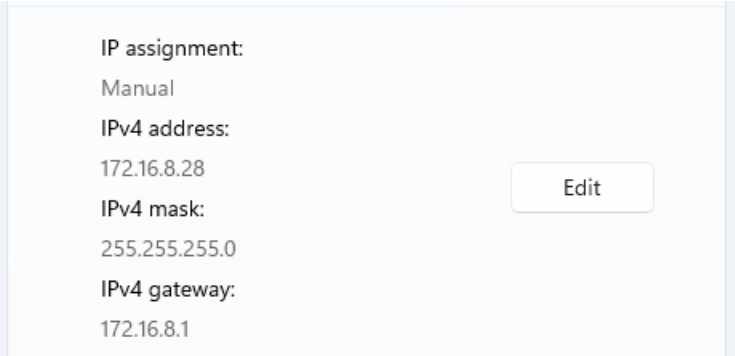
Editing /etc/netplan/ in Ubuntu to connect to VyOS router

```
ubuntu@bransonsubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=15.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=15.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=17.4 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2439ms
rtt min/avg/max/mdev = 15.416/16.158/17.387/0.875 ms
ubuntu@bransonsubuntu:~$
```

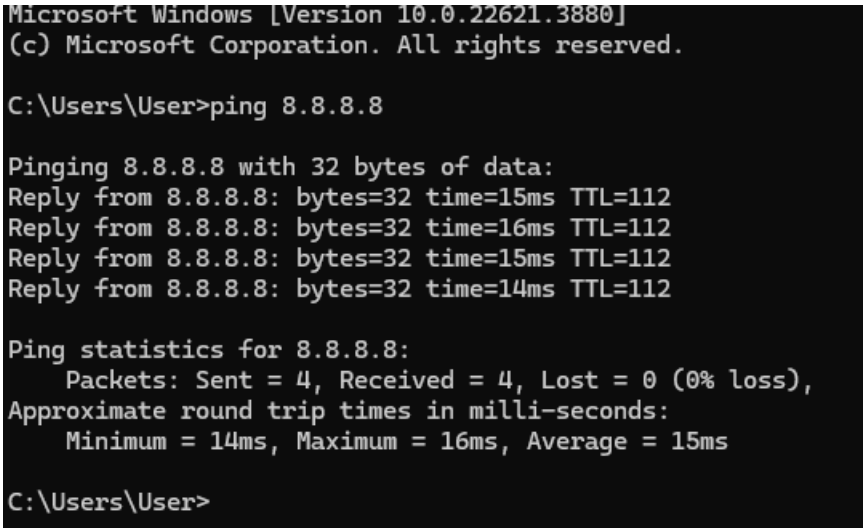
Testing Internet connectivity on Ubuntu server



Pinging VyOS Router in Ubuntu Server



Setting network settings in Windows VM



Testing Internet connectivity in Windows VM

```
C:\Users\User>ping 172.16.8.1

Pinging 172.16.8.1 with 32 bytes of data:
Reply from 172.16.8.1: bytes=32 time=1ms TTL=64
Reply from 172.16.8.1: bytes=32 time=5ms TTL=64
Reply from 172.16.8.1: bytes=32 time=1ms TTL=64
Reply from 172.16.8.1: bytes=32 time=2ms TTL=64

Ping statistics for 172.16.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\Users\User>
```

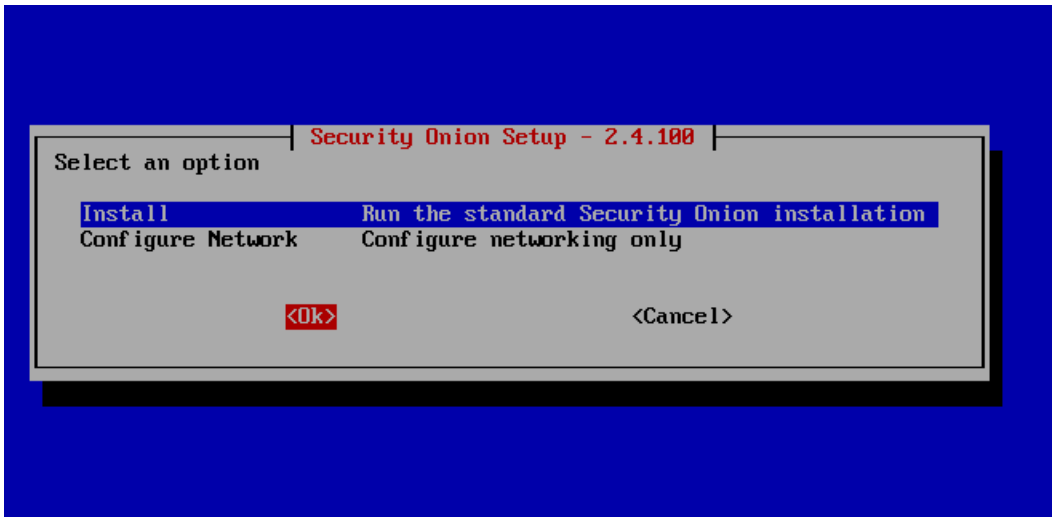
Pinging VyOS router in Windows VM

```
##############################################
##          ** 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 S
ecurity Onion.

Enter an administrative username: analyst

Let's set a password for the analyst user:

Enter a password:
```

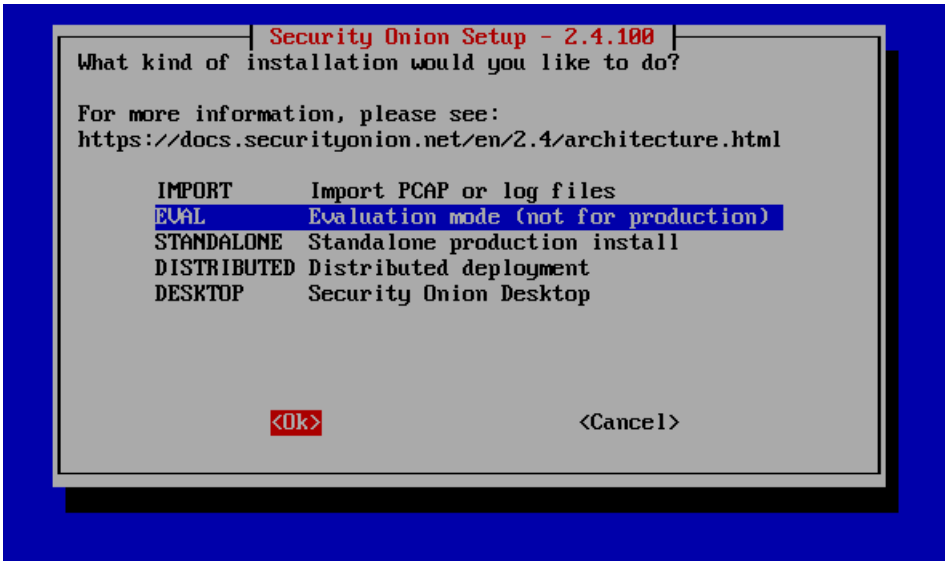
Setting up security onion administrator account

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

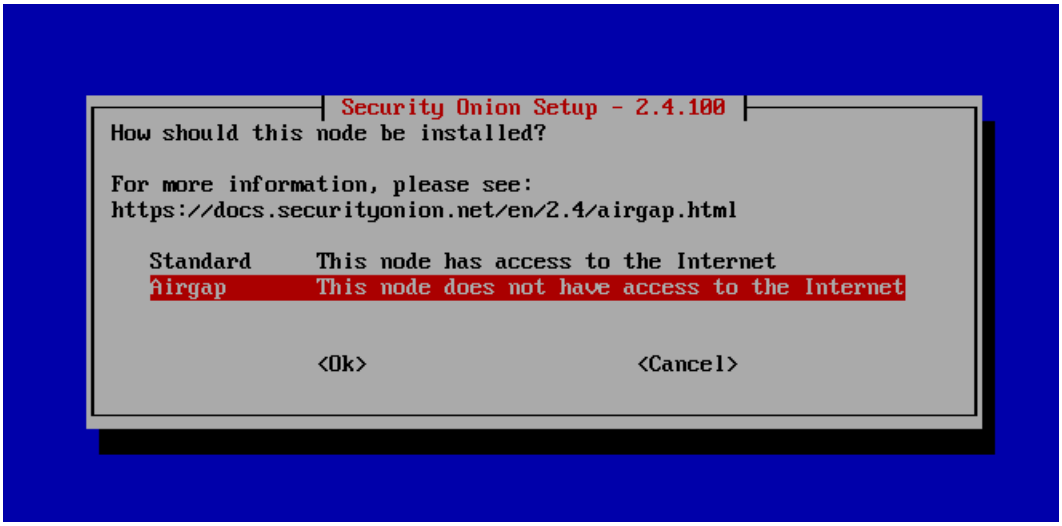
Successful install of SO



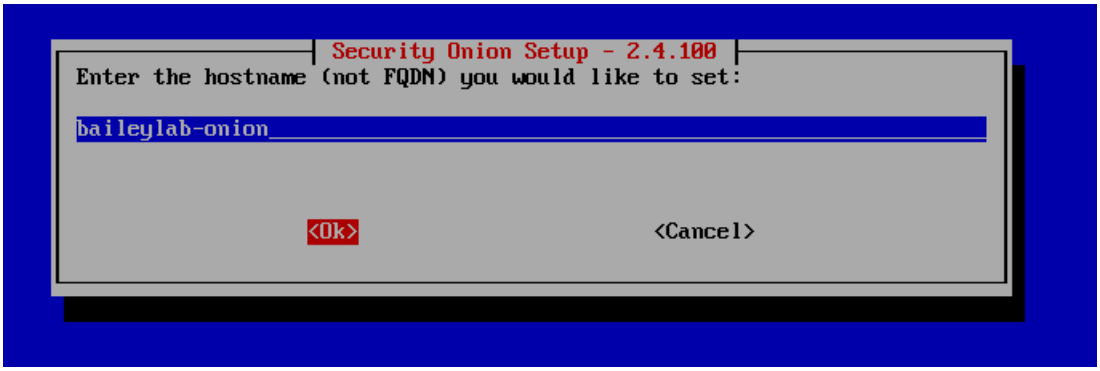
Installation of Security Onion Service



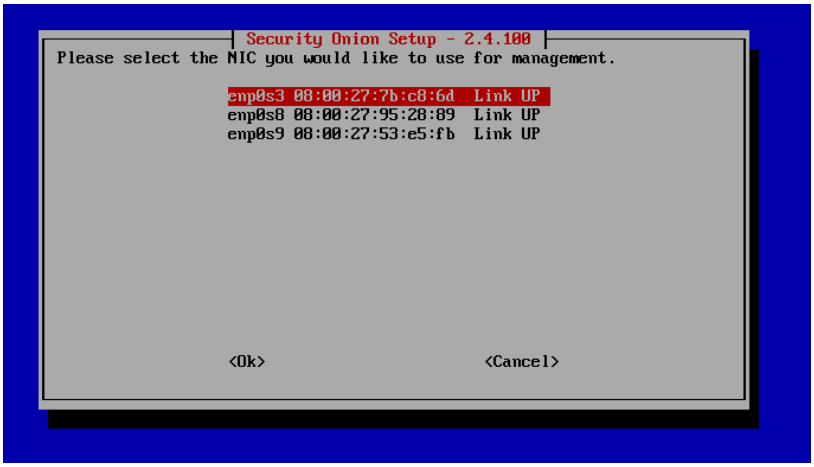
I will be using evaluation mode



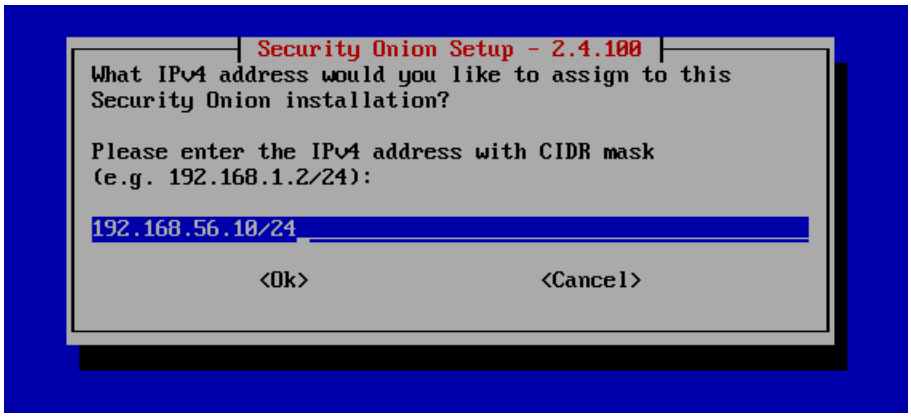
Because I want my Security Onion to be configured my host-only network, I am selecting air-gapped



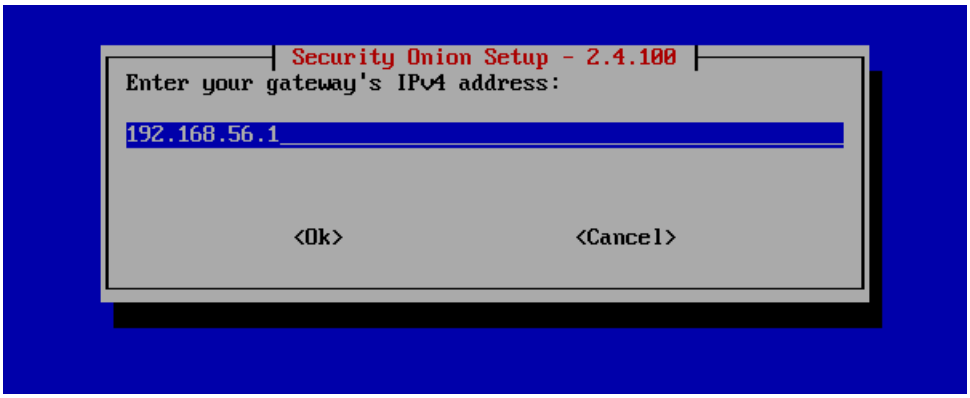
Setting hostname of Security Onion



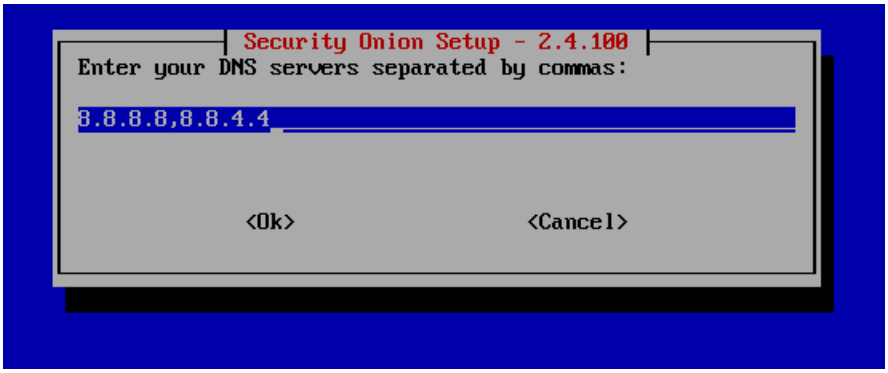
As depicted by the topology, enp0s3 is a host-only connection, enp0s8 is connected to the internal network “net-1”, and enp0s9 is connected to the internal network “net-2”. I am selecting enp0s3 as the management interface because it is connected to the host and I would like to monitor on the other two.



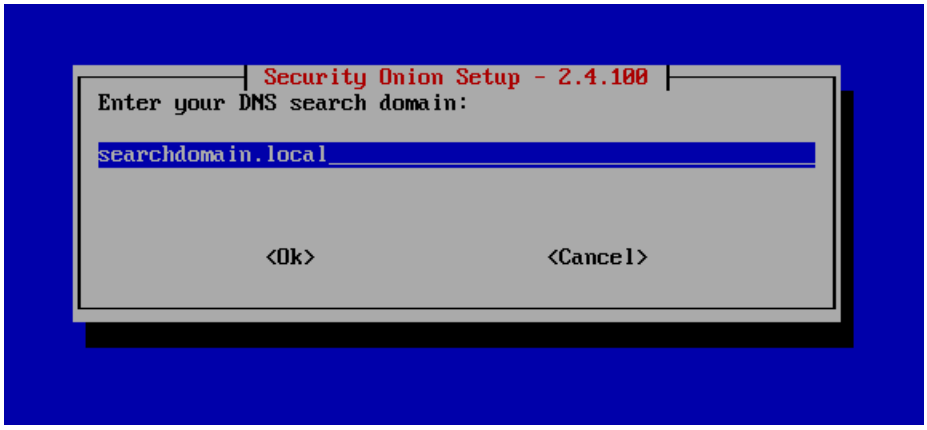
Selecting static IP of the Security Onion VM



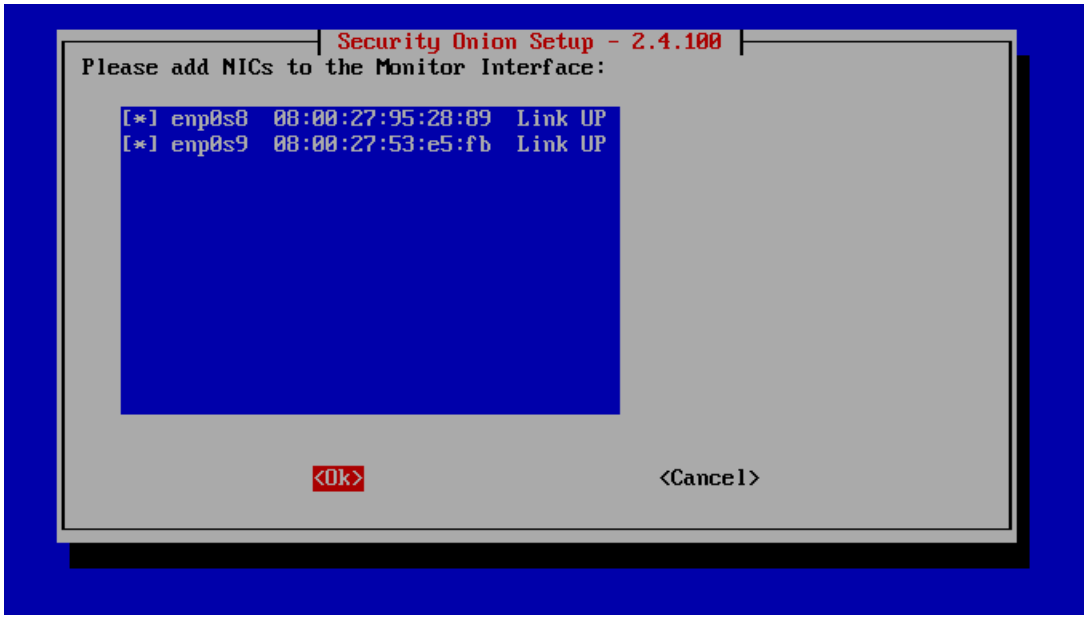
Setting the IP of the gateway (host-only network)



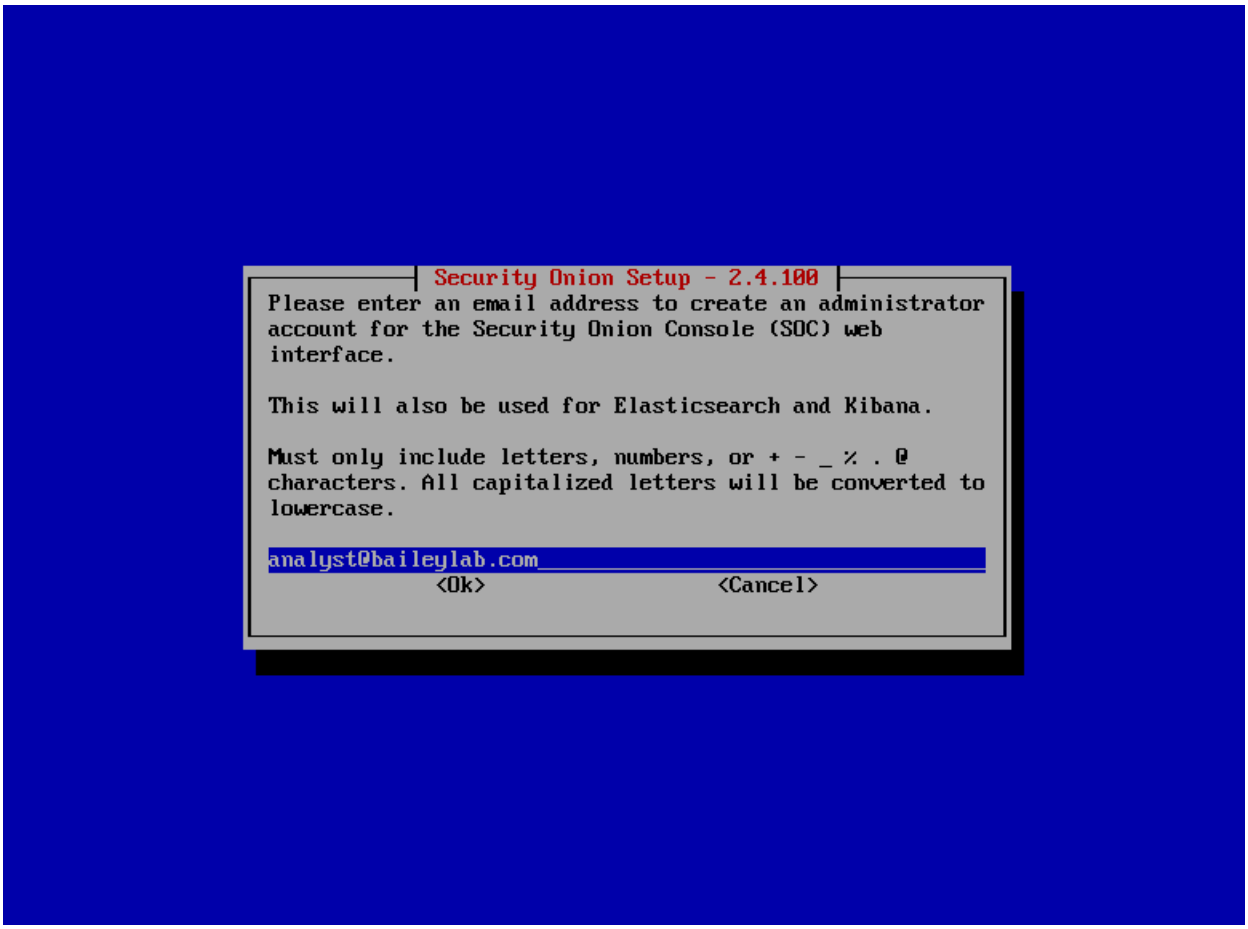
I will use the default DNS servers for this project



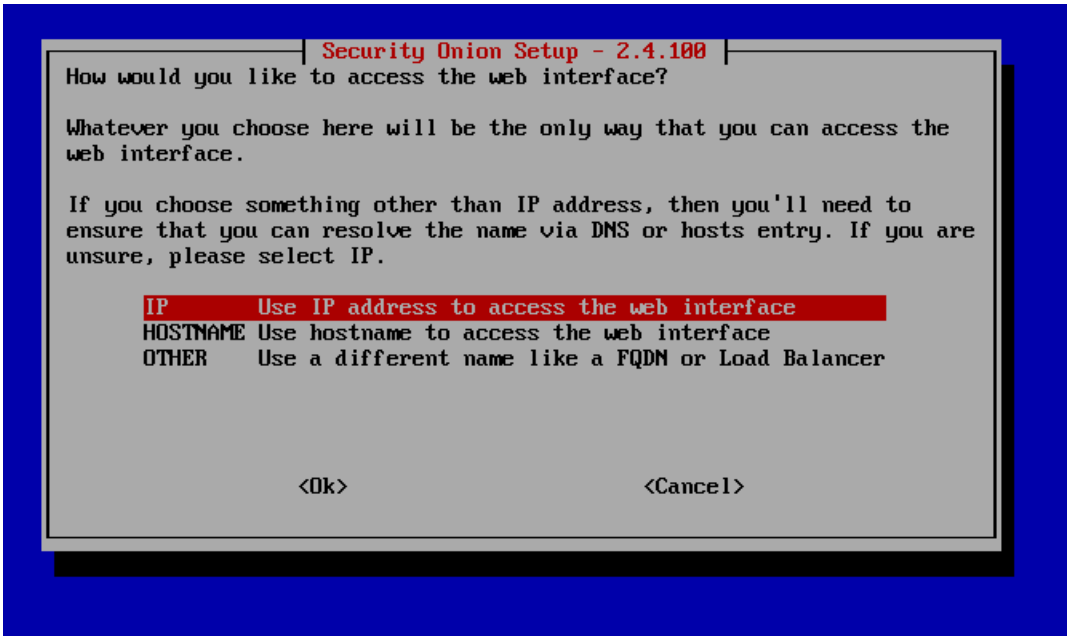
I will also use the default DNS search domain



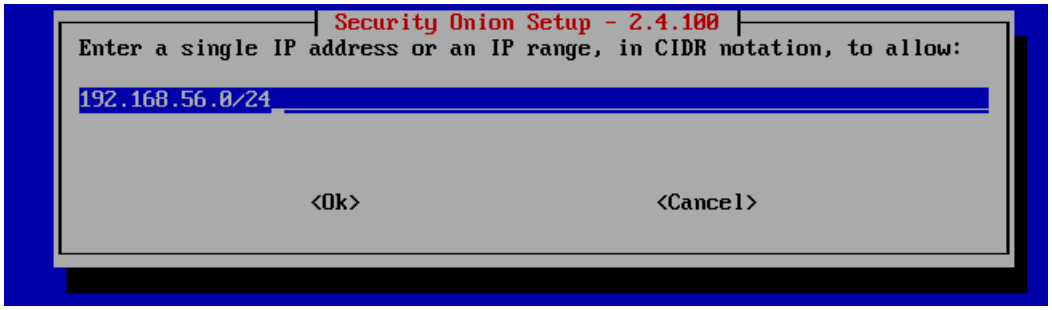
Now I will add the adapters connected to the networks I want to monitor



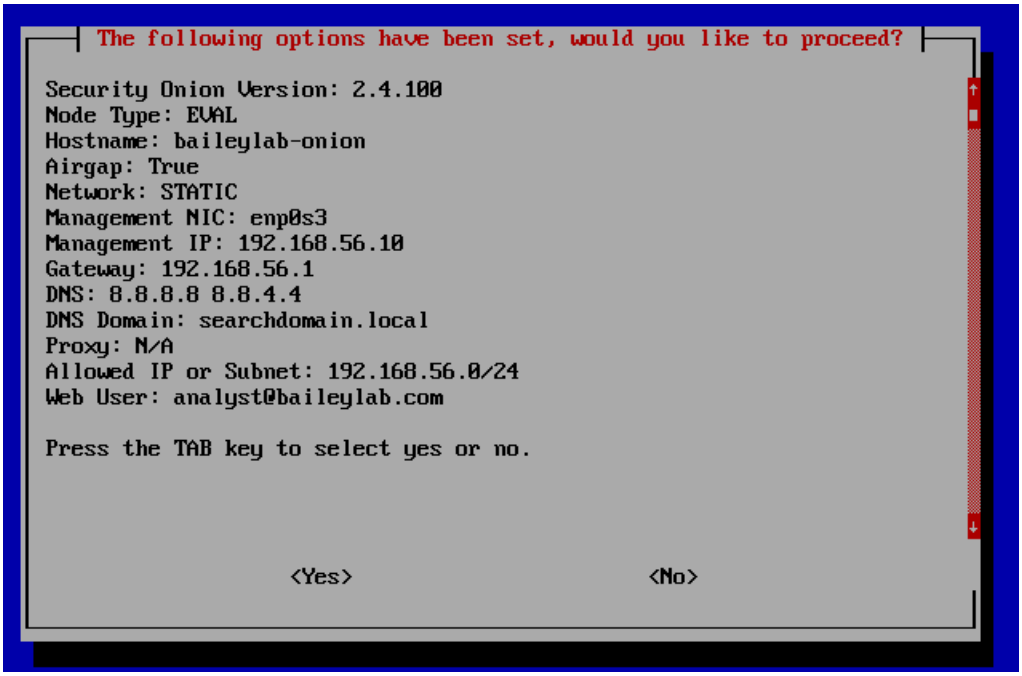
After configuring the network, I set the username for the web interface administrator



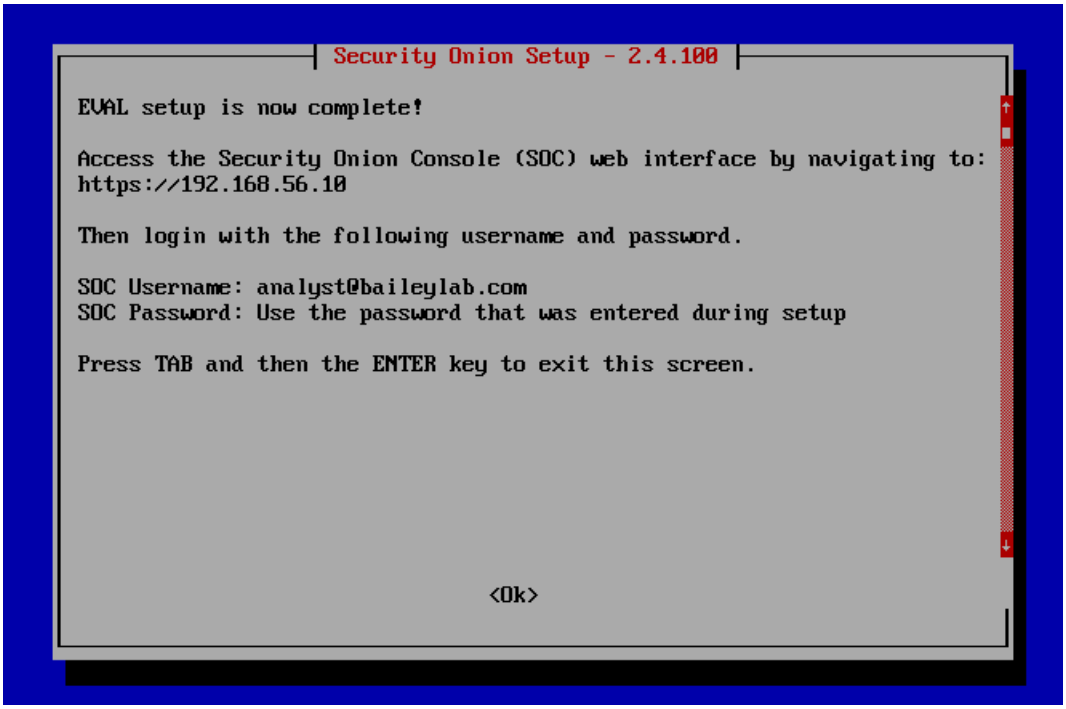
I will be accessing this via IP



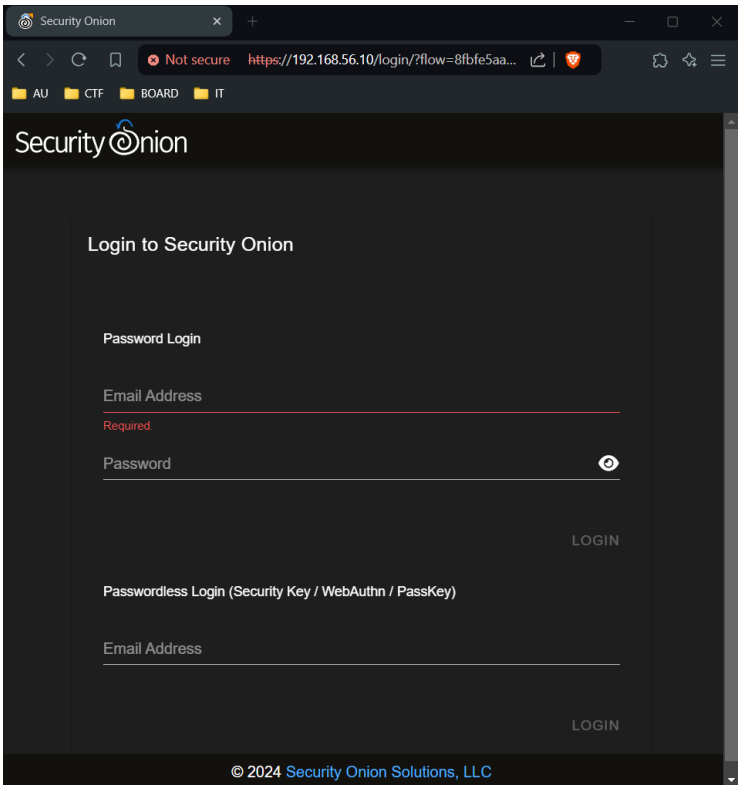
Entering valid IP range for connection to web interface



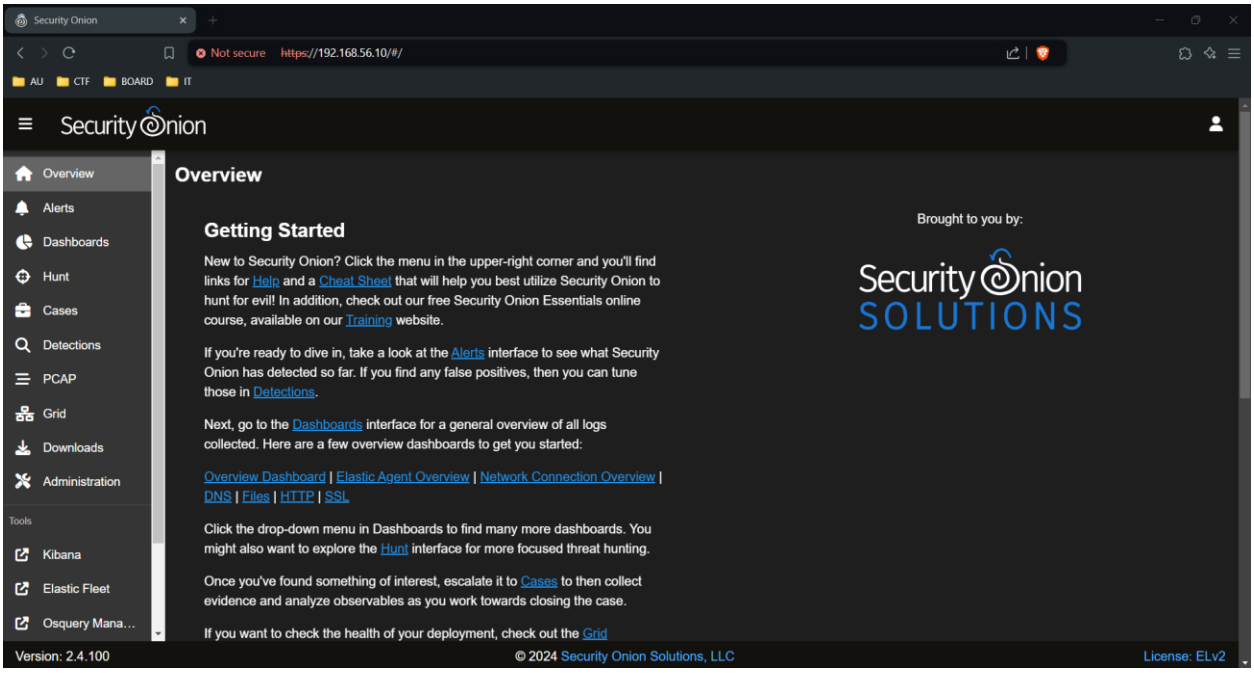
Overview of setup



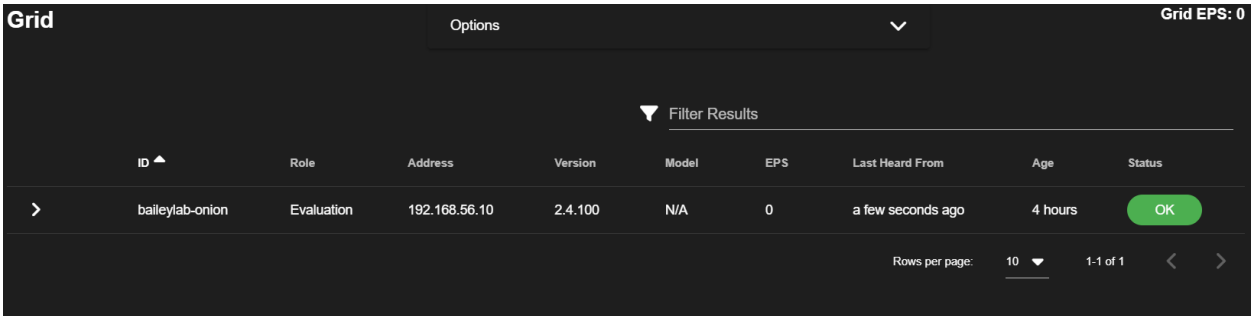
Setup is complete!!



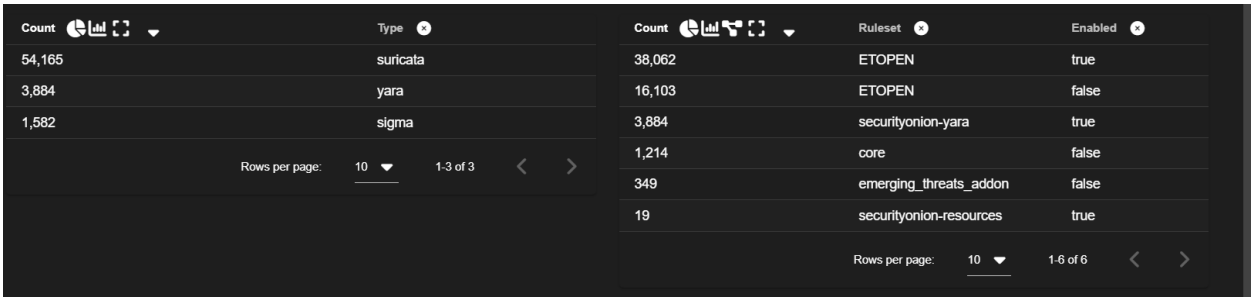
Accessing the web interface



Successful login!



Checking Security Onion Node on deployment



Ensuring the sensors work properly

Write-up & Summary

In this project section, I successfully configured a multi-layered network environment using a VyOS router, Ubuntu server, Windows 11 VM, and Security Onion for monitoring. VyOS has three network adapters: a NAT for any outbound traffic, and two internal networks, “net-1” (10.0.44.0/24) and “net-2” (172.16.8.0/24). The Ubuntu server is assigned a static IP on “net-1” (10.0.44.13), and the Windows 11 VM is assigned a static IP on “net-2” (172.16.8.23). Security Onion has three network adapters as well: a host-only connection, setup for management, and two adapters, one for monitoring each internal network. In this project, after the setup, I accessed the Security Onion web interface, ensuring the monitoring capabilities and overall workings of the setup were functional. This will act as a building block for future projects. I am looking forward to the rest of this project, which will involve working more with Security Onion to learn all of the features and improve my threat-hunting/network analysis skills. I hope you have enjoyed this project section!

References

Draw.io - free flowchart maker and diagrams online. Flowchart Maker & Online Diagram Software. (n.d.). https://app.diagrams.net/

Security Onion Solutions. (n.d.). https://securityonionsolutions.com/