

SECURITY ONION

GROUP-2
SRIRAM RAYALA

Lab 1: Setting up and Configuring Security Onion

Introduction

In this lab, I deployed and configured a Security Onion VM. This lab covered the following topics:

1. Deploying the Security Onion VM & Configuring Security Onion
2. Installing VMware Tools
3. Updating Suricata Rulesets & Adding a Web Portal User
4. Deploying Wazuh Agents

Objective 1: Deploying the Security Onion VM

I deployed a Security Onion VM for my lab environment. Below are the steps I followed:

I downloaded the latest version of the Security Onion appliance from <https://securityonionsolutions.com/software/>.

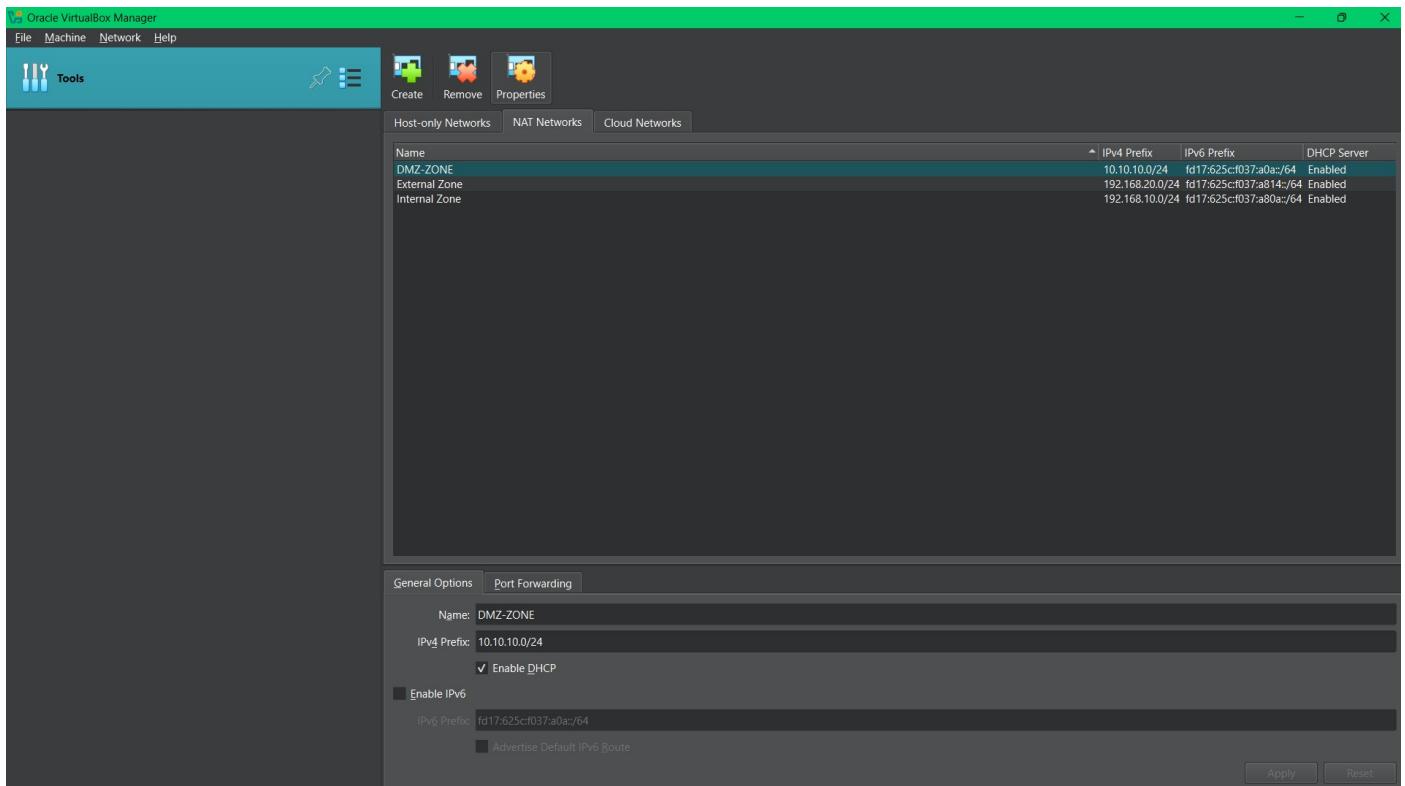
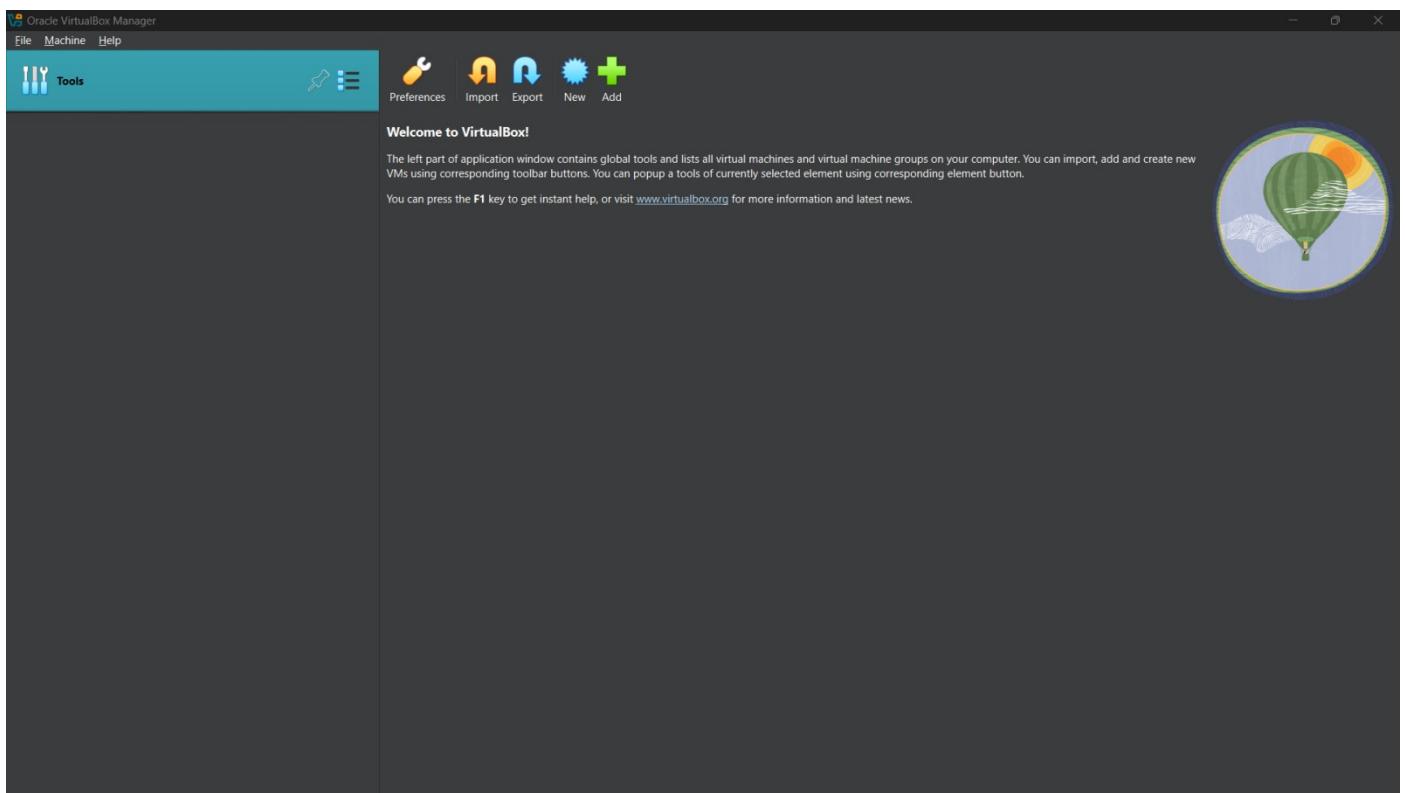
The screenshot shows the official website for Security Onion Solutions. The main header includes the SOS logo and navigation links for Overview, Pro, Software, Hardware, Training, Certification, Support, Conference, and Blog. A social media sharing bar is at the top right. The main content area features a large banner for "Security Onion 2" with the subtitle "Latest version: 2.4.120". Below the banner are four download buttons: "Download", "Amazon Cloud", "Azure Cloud", and "Google Cloud", each with a corresponding blue button. A "Documentation" button is also present. To the right of the download buttons is a partial view of a dashboard titled "Security@Onion" showing "Basic Metrics" like "Total Occurrences" and "Group Metrics" with a treemap visualization. The bottom section has a blue background with the heading "Overview" and a paragraph about Security Onion being a free and open platform for defenders. It also mentions "For network visibility, we offer signature based detection via".

I have also downloaded VirtualBox and added 3 NAT networks to VirtualBox to be assigned to Virtual Machines. The 3 NAT networks include:

DMZ ZONE : 10.10.10.0/24

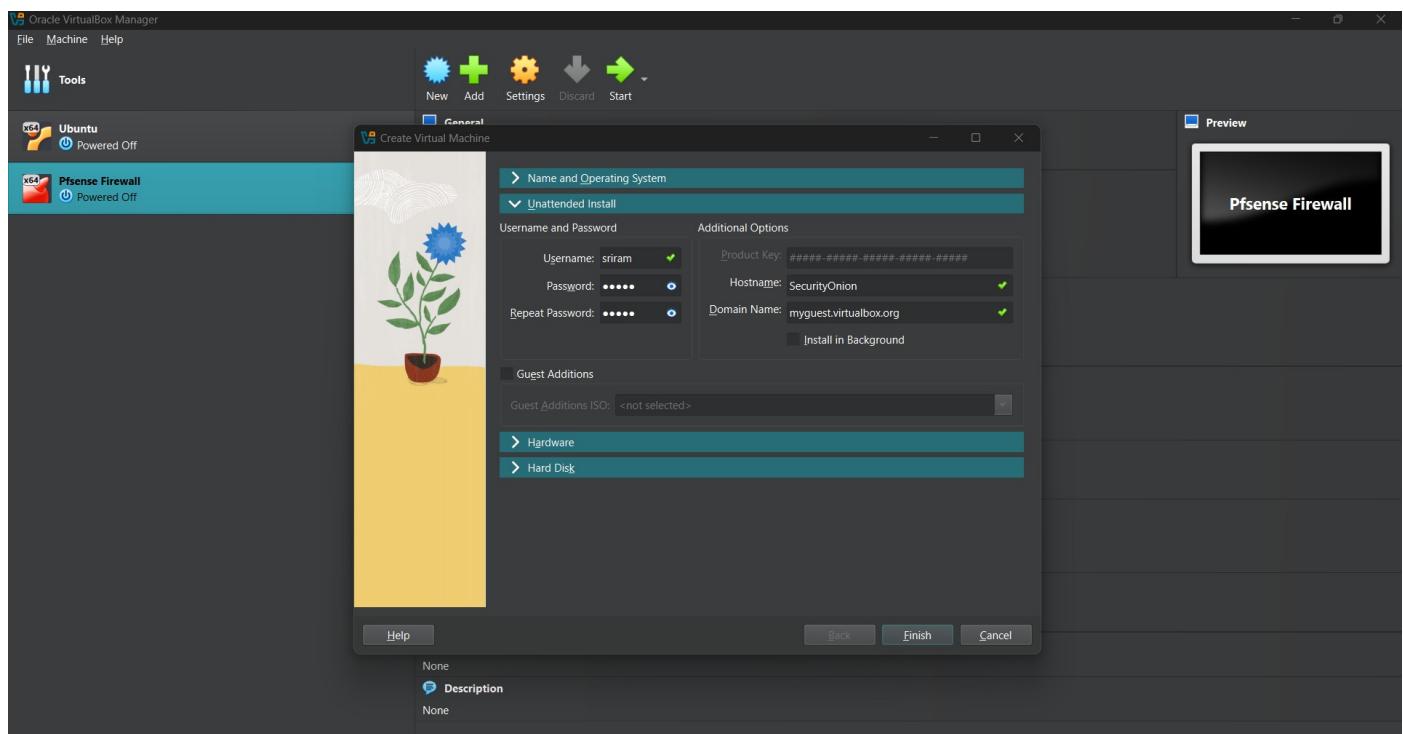
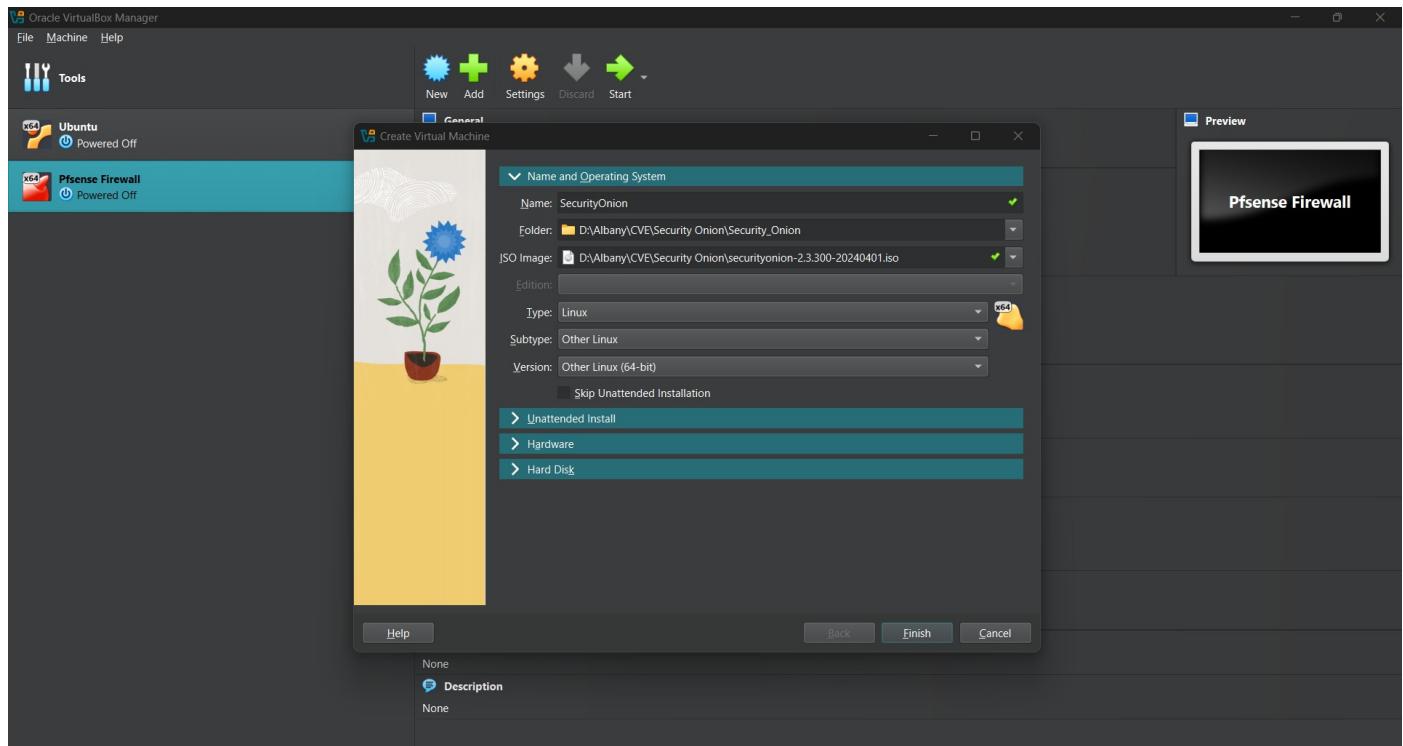
INTERNAL NETWORK : 192.168.10.0/24

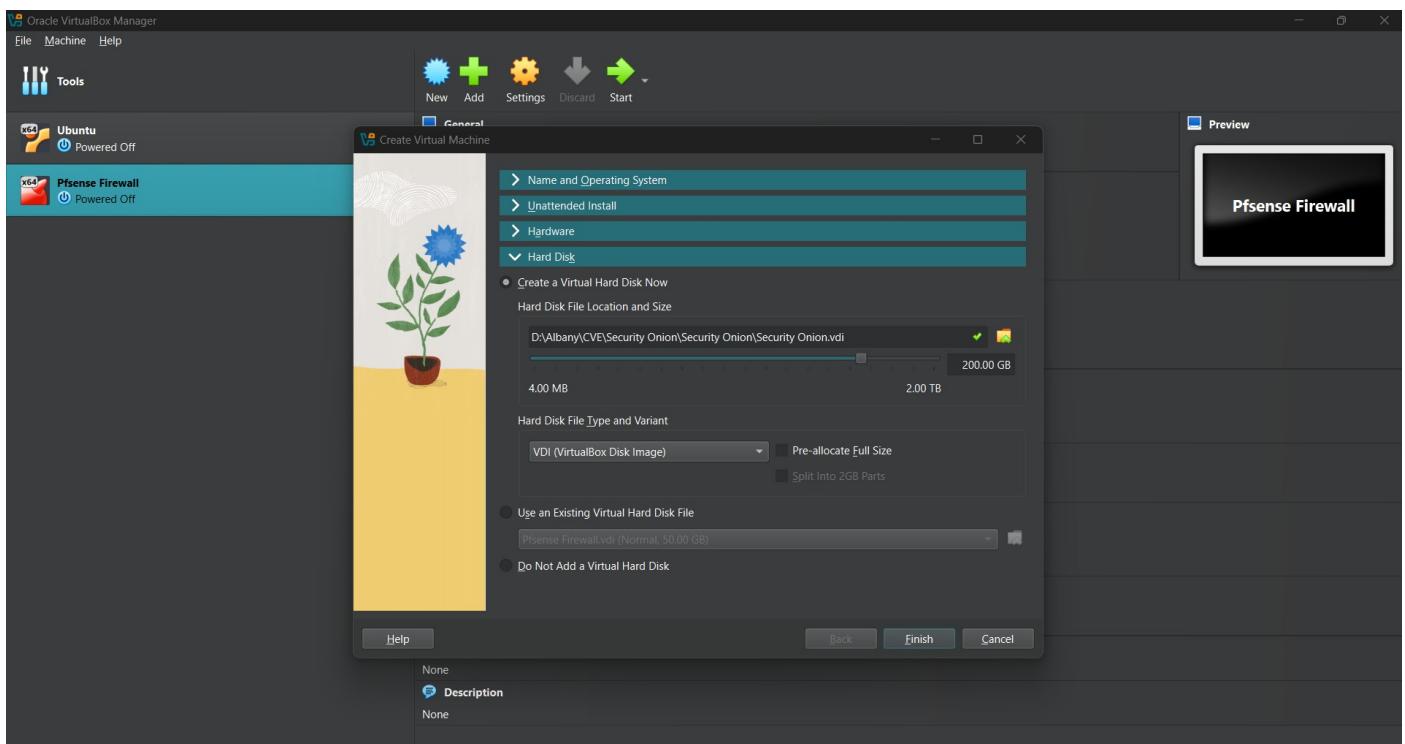
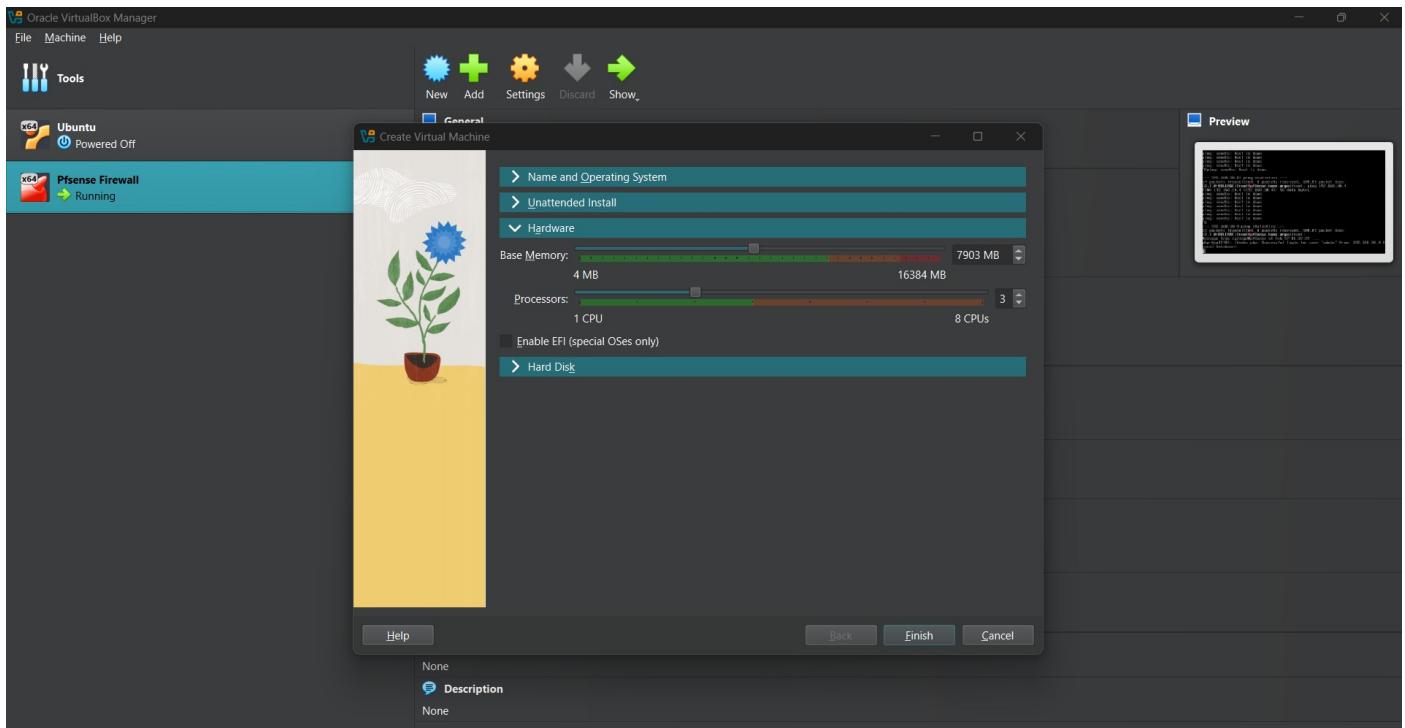
EXTERNAL ZONE: 192.168.20.0/24

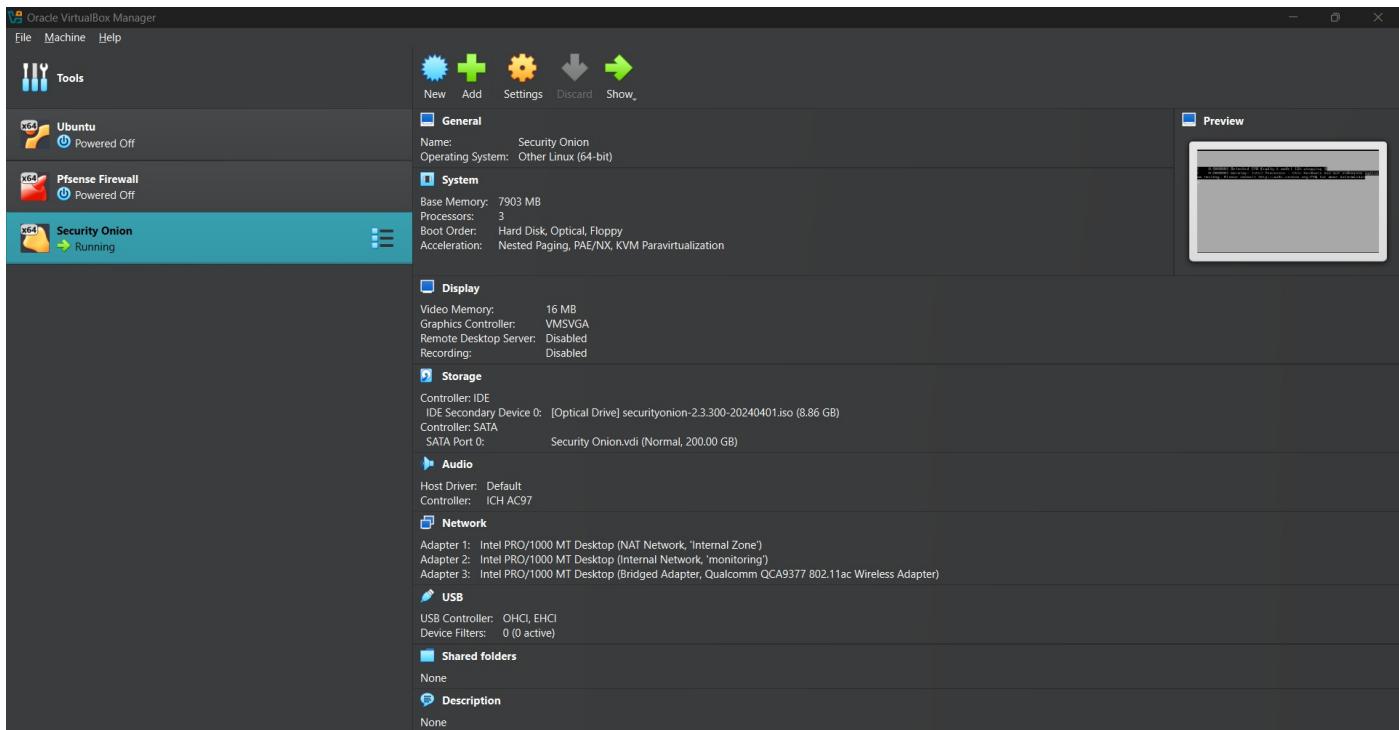


Now I opened Virtualbox and selected *File* → *New Virtual Machine*. I chose the *Typical* configuration option and clicked *Next*. I selected the *Installer disc* option on the next screen, clicked *Browse*, and found the ISO file for Security Onion I had just downloaded. I clicked *Open* and then *Next*. I specified the operating system as *Linux*, subtype as *other-linux* and version is *Other Linux 64-bit*, and clicked *Next*. I named the VM *Security Onion* and clicked *Next*. I specified the size of the virtual disk to 200 GB and clicked *Next*. I clicked

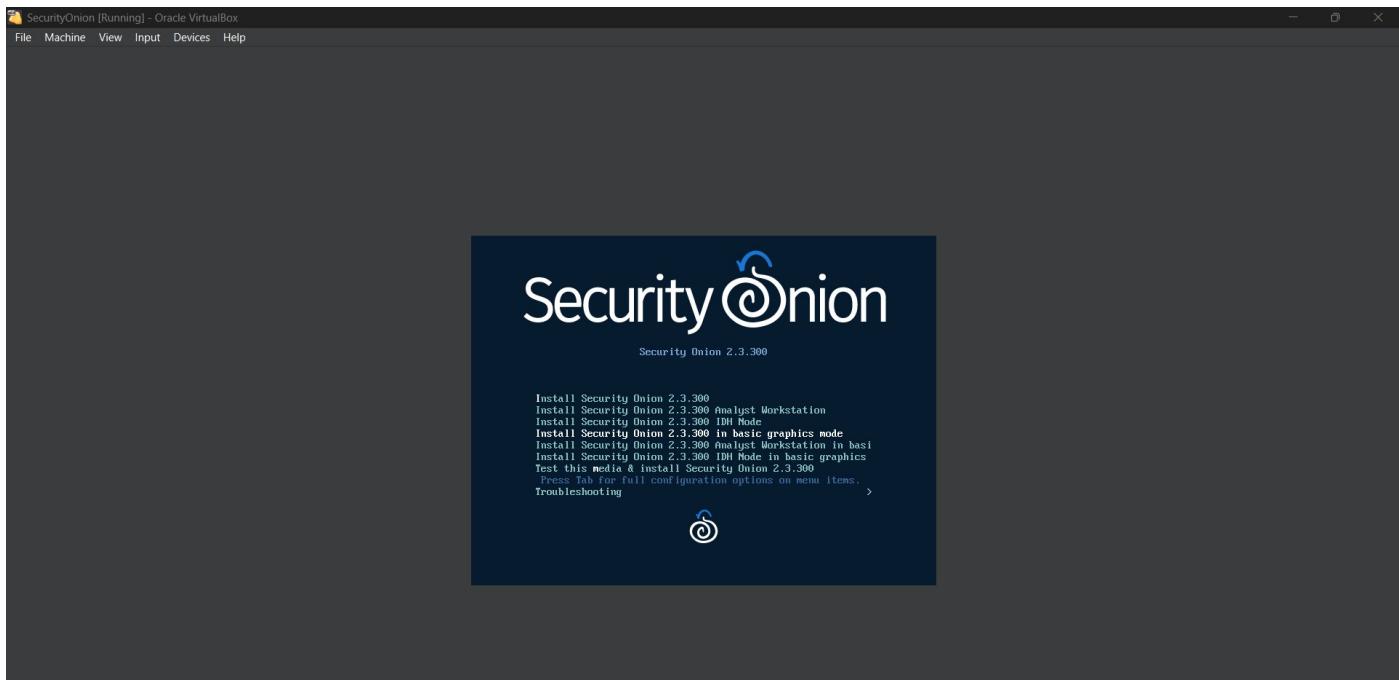
Customize Hardware on the summary screen and configured the hardware resources for the VM. I powered on the Security Onion VM and waited for it to boot into the installation screen.



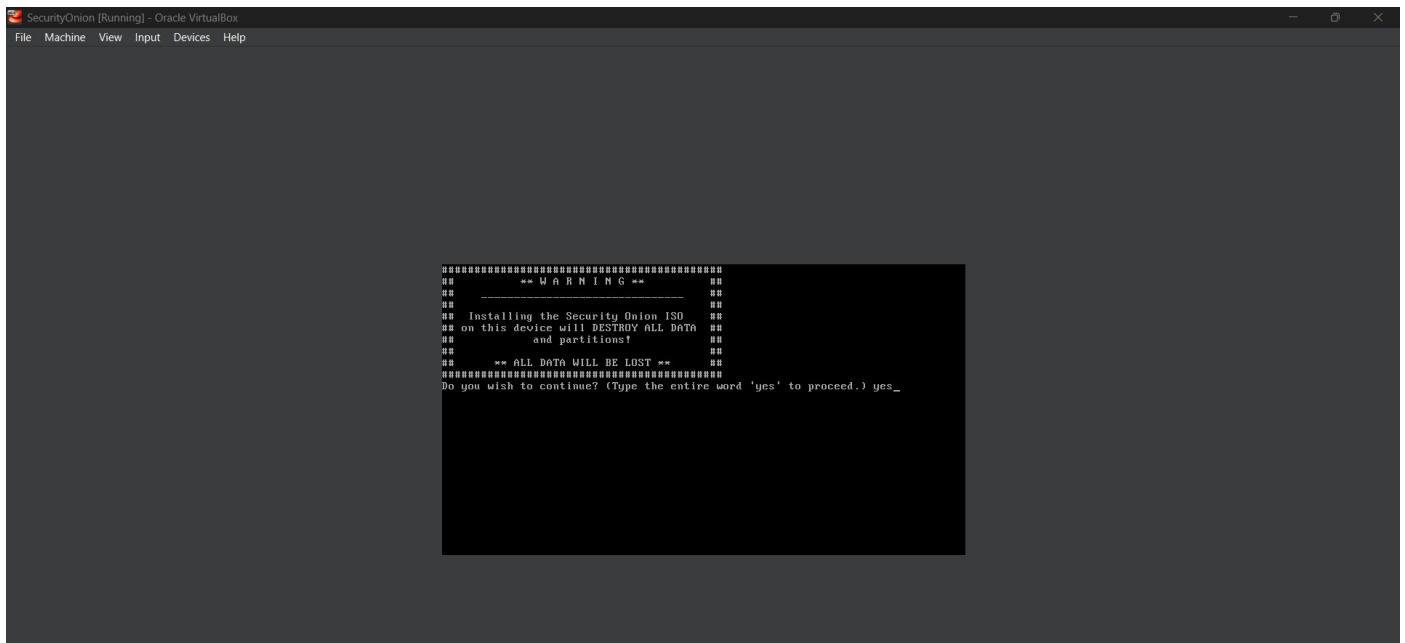




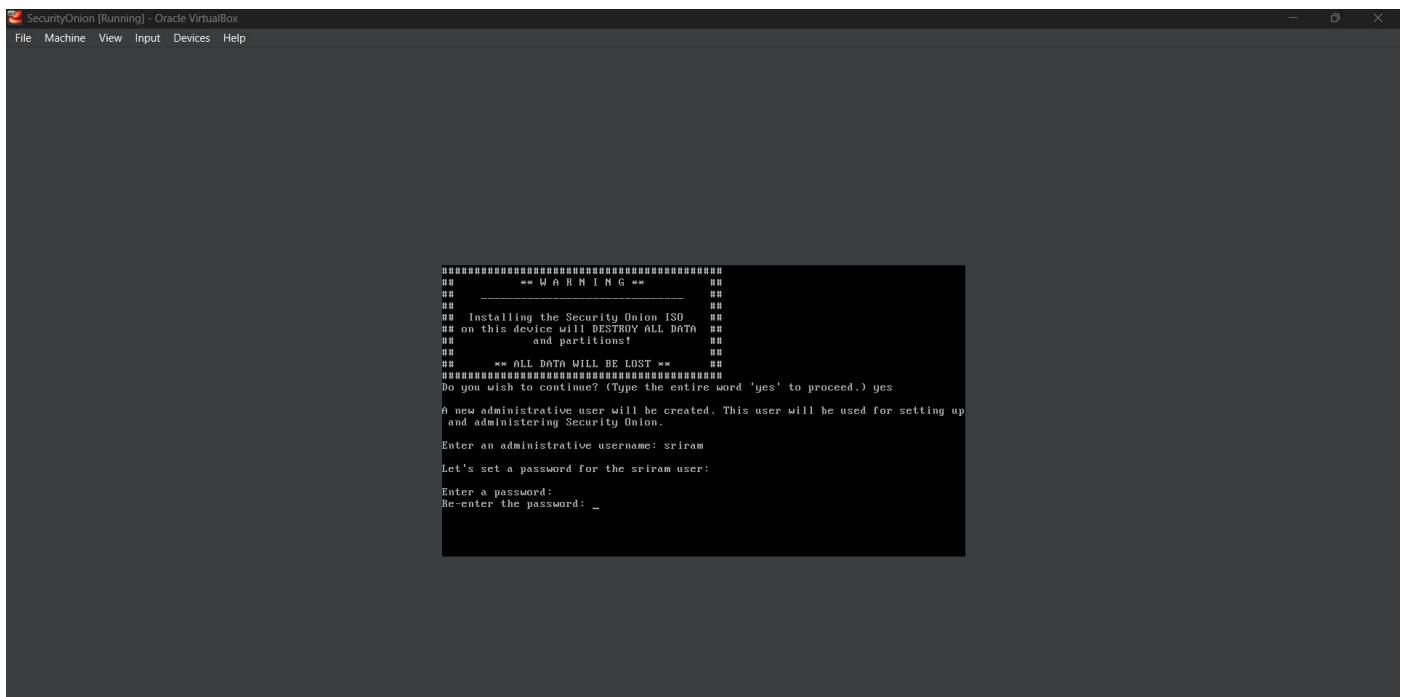
I highlighted *Install Security Onion 2.3.300 in basic graphics mode* and hit *Enter* to start the installation process.



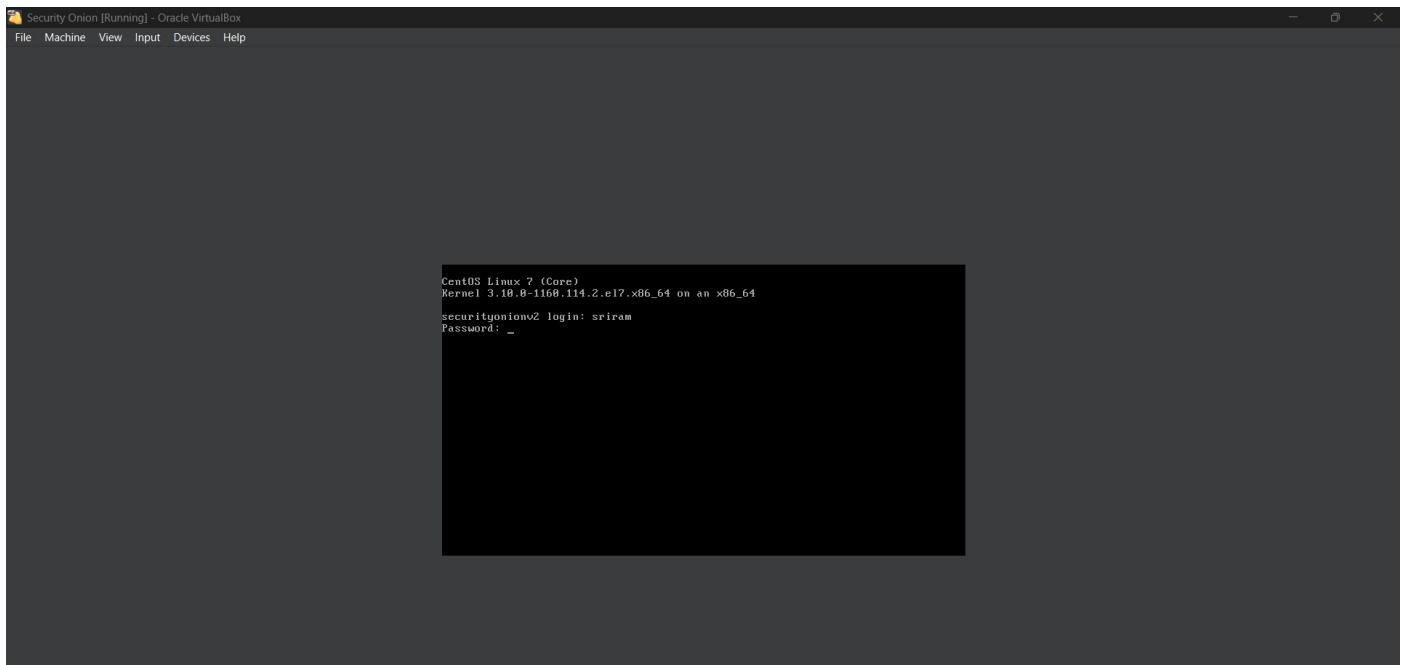
I typed yes to confirm that I wanted to wipe the hard drive and install the Security Onion operating system.



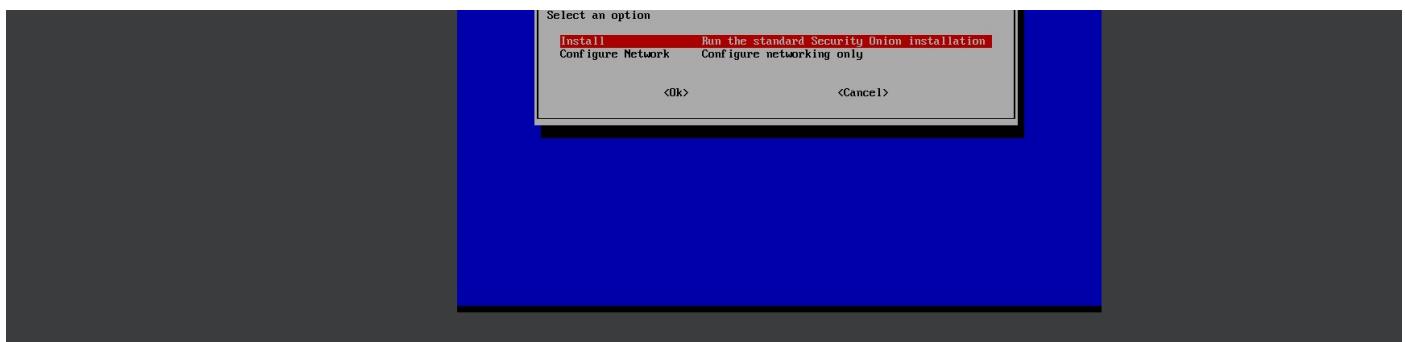
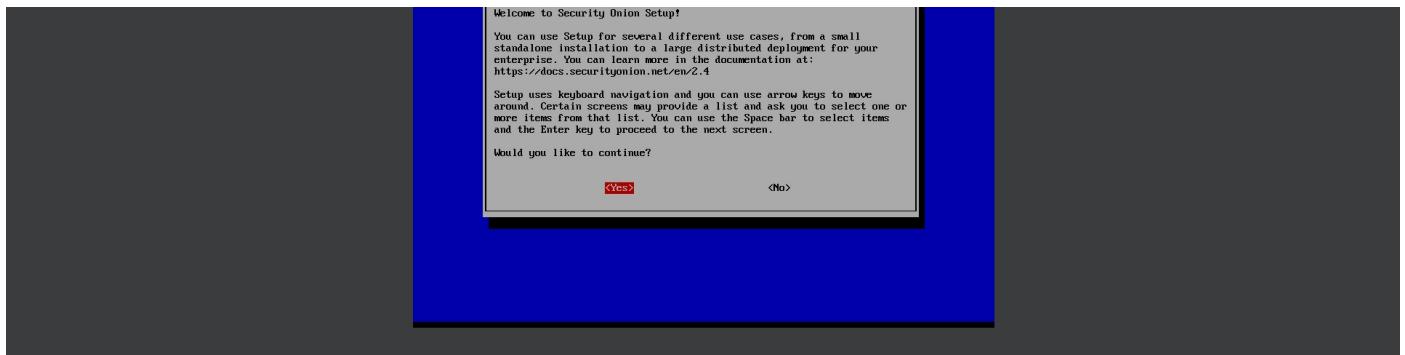
I set up the administrative username and password for the installation.



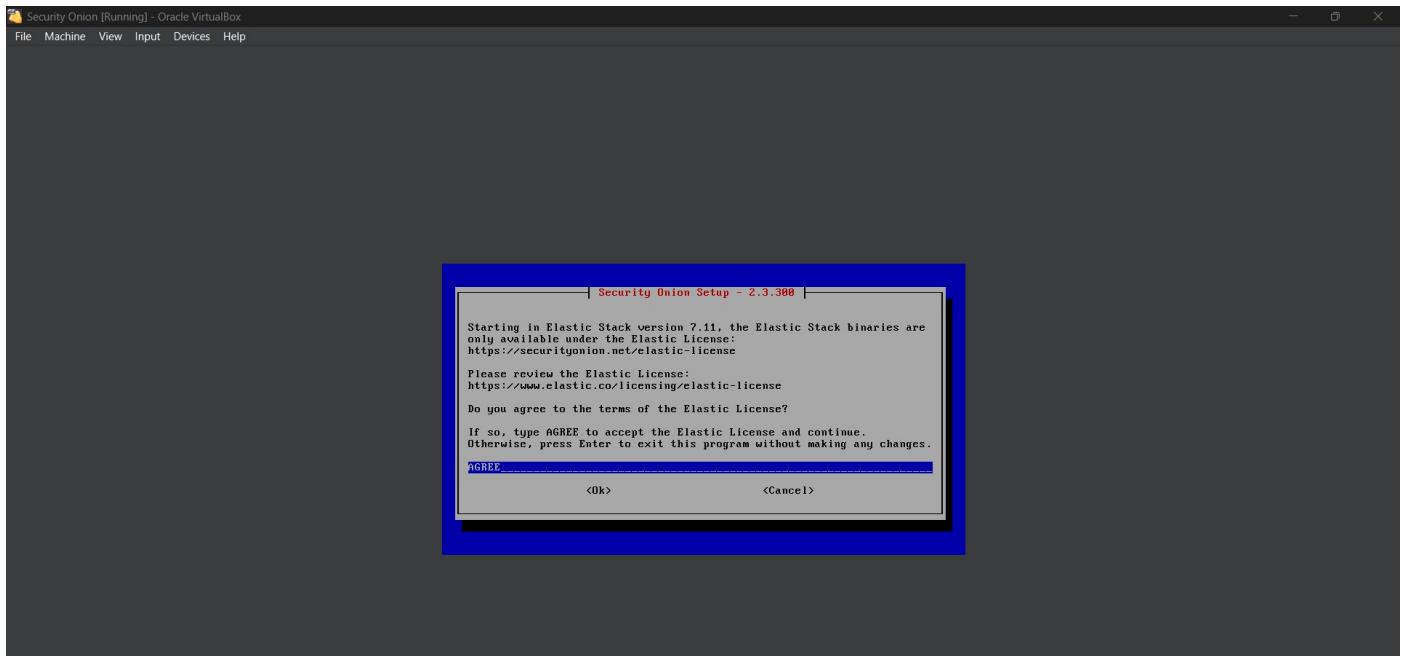
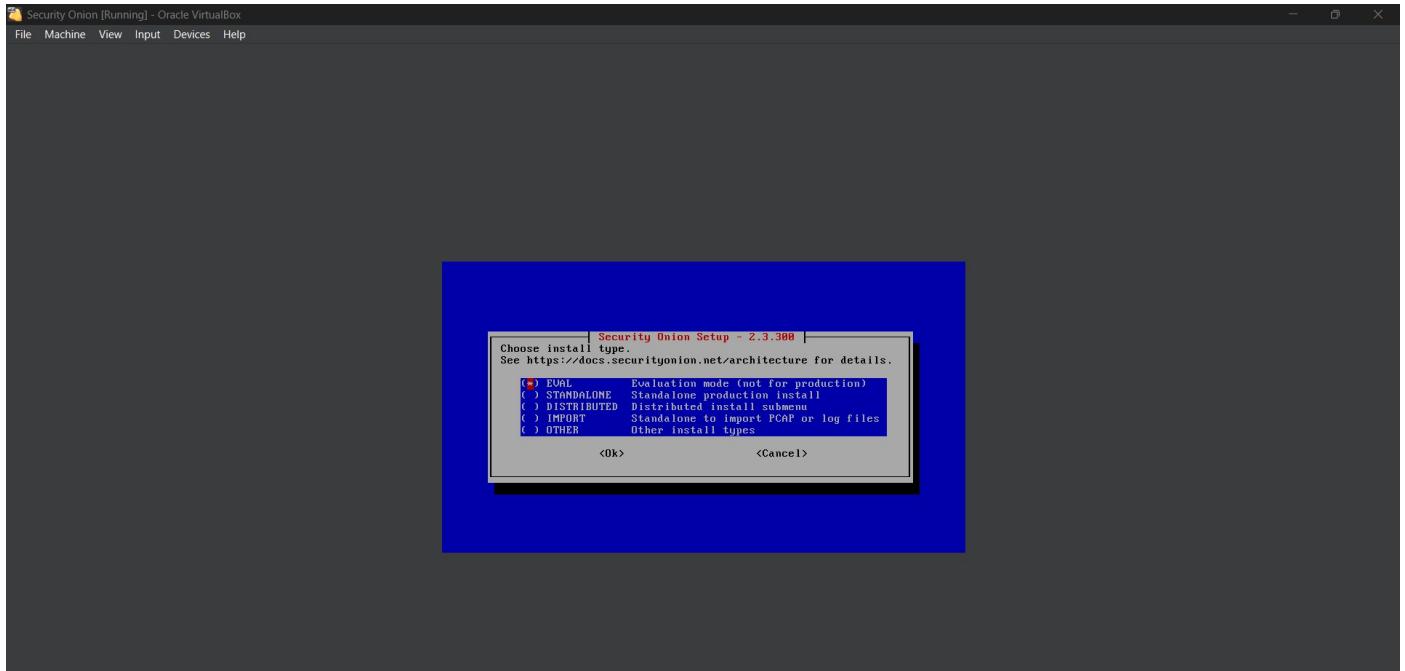
The installer formatted the hard drive and installed the Security Onion operating system. After the installation, I logged into the newly installed operating system with the credentials I had set up.



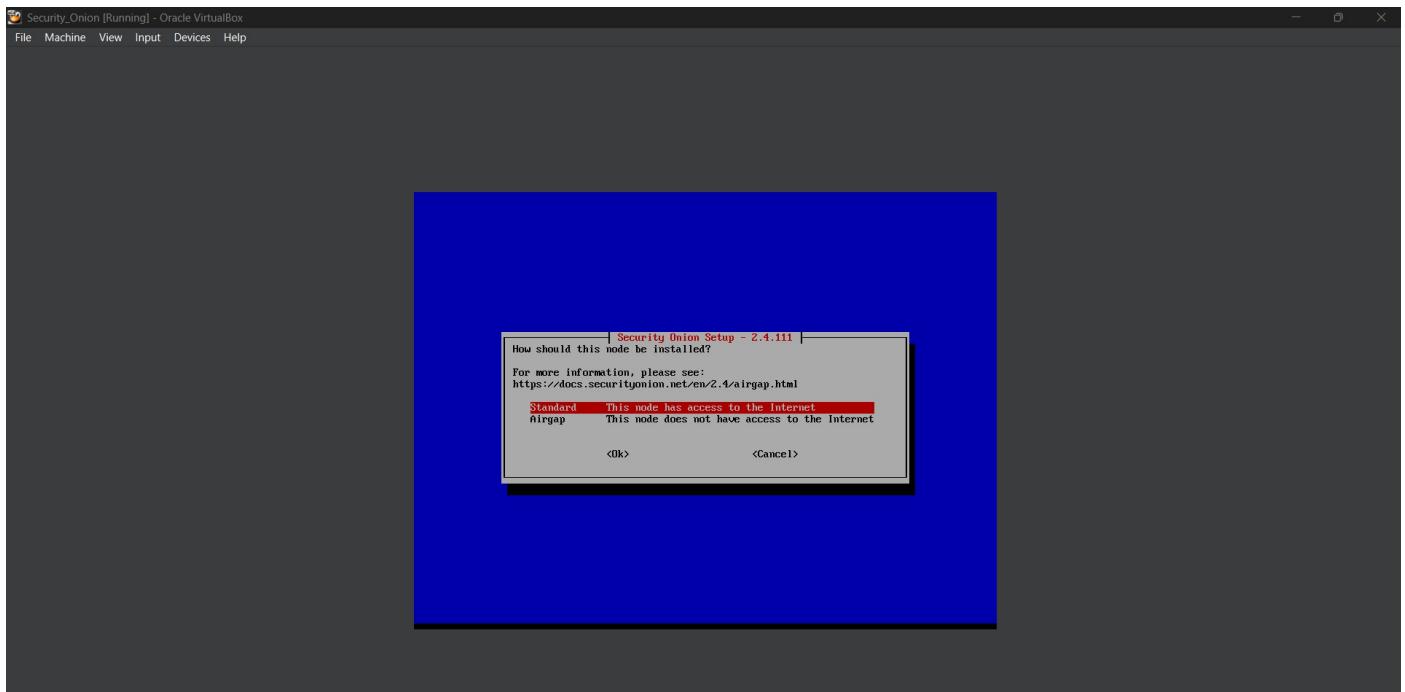
I confirmed that I wanted to continue with the setup.



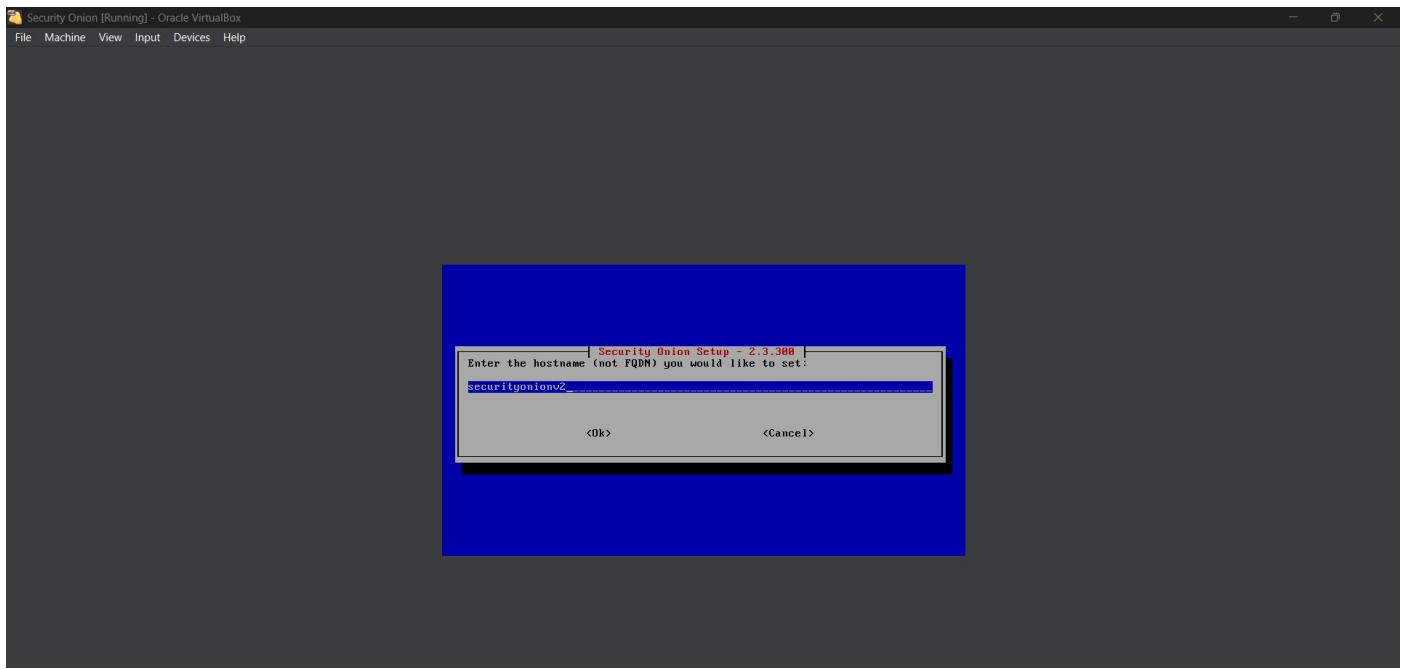
I chose the *EVAL* installation mode to evaluate all aspects of Security Onion.



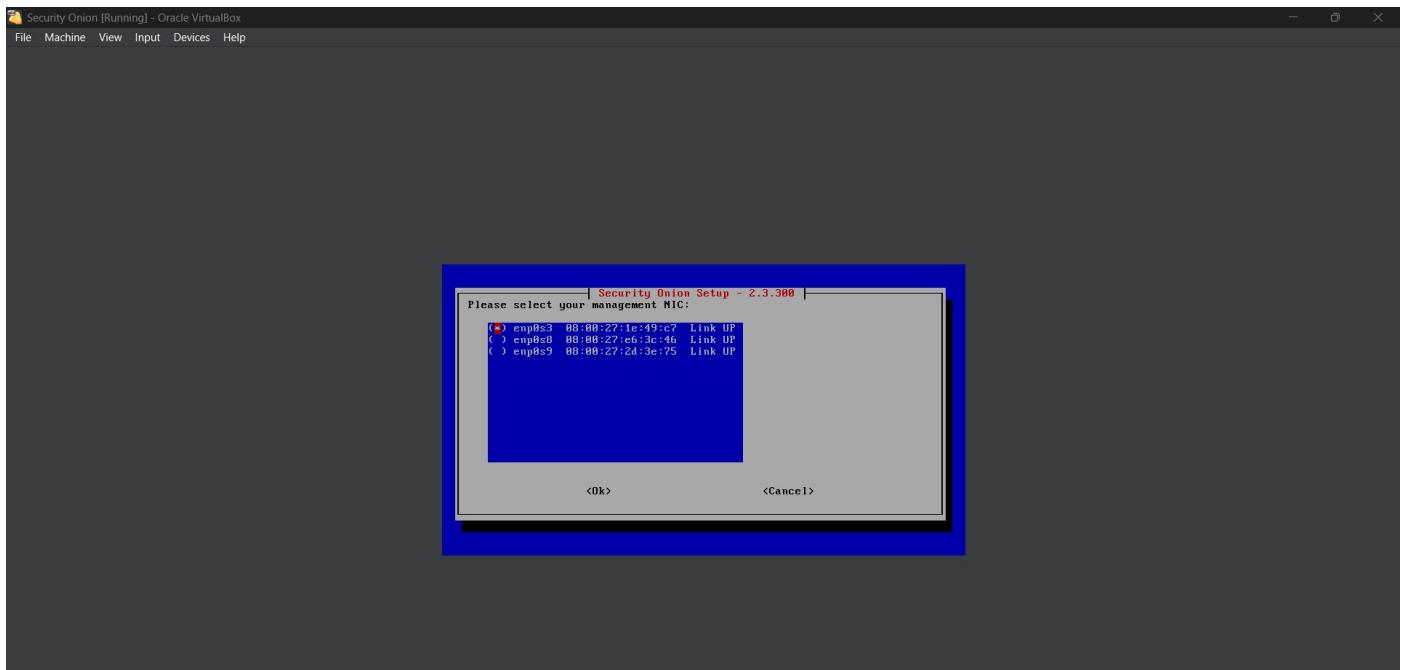
I selected the *STANDARD* install option to allow Security Onion to retrieve updates over the internet.



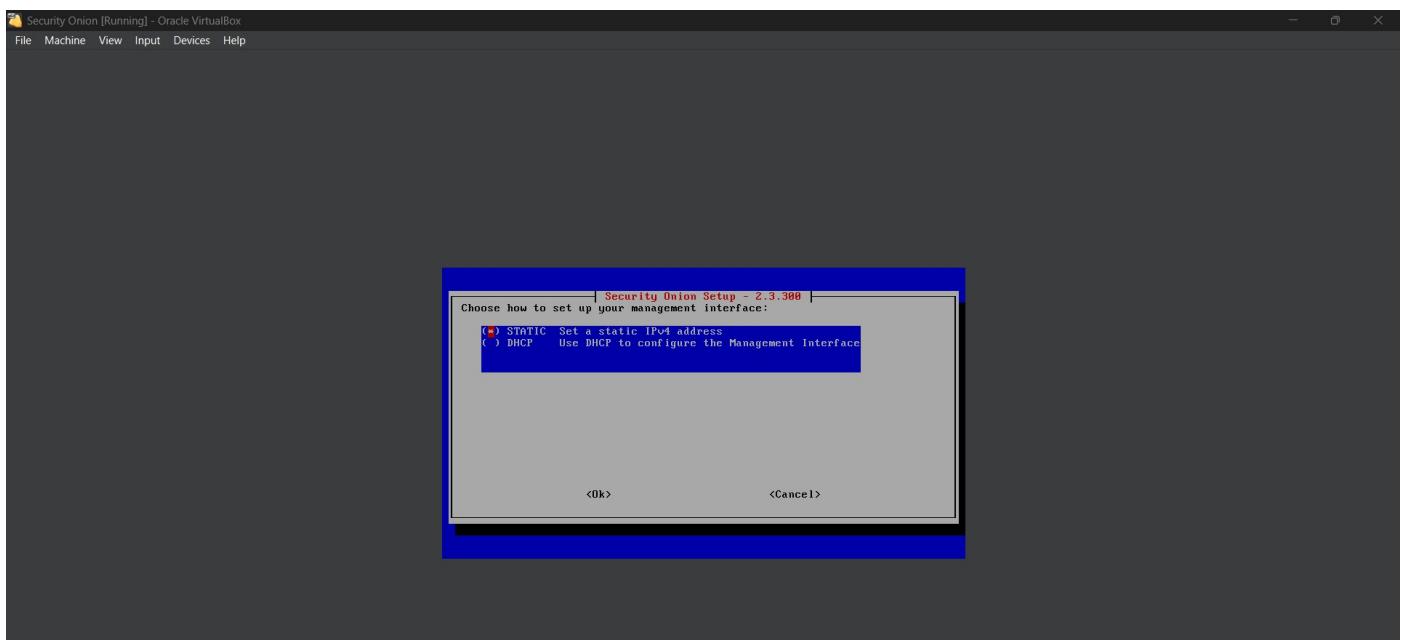
I named the Security Onion appliance *securityonionv2*.

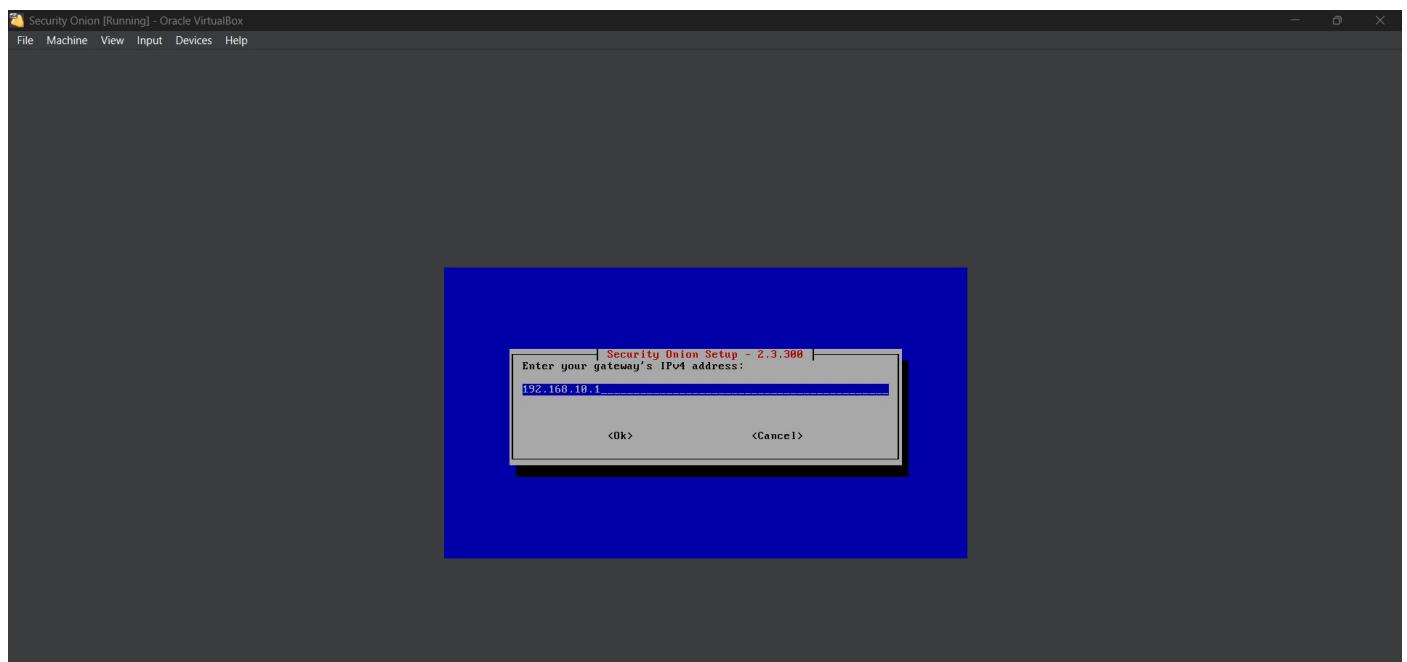
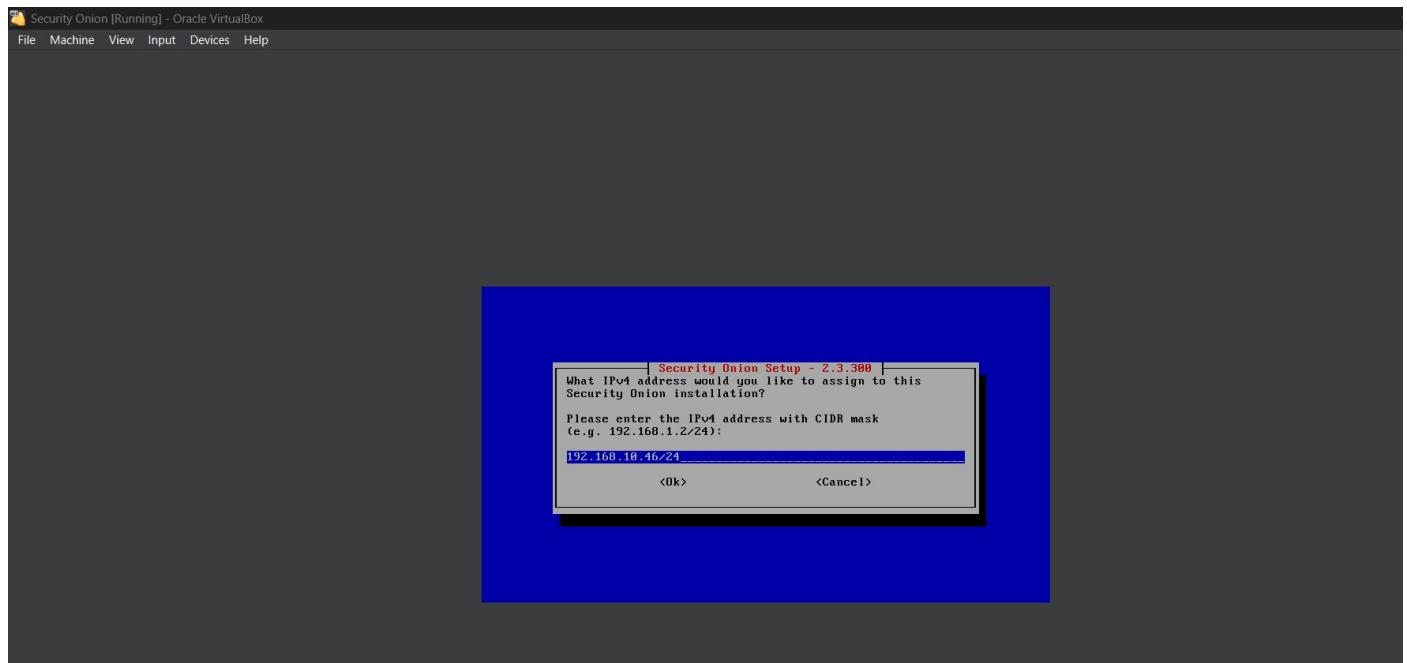


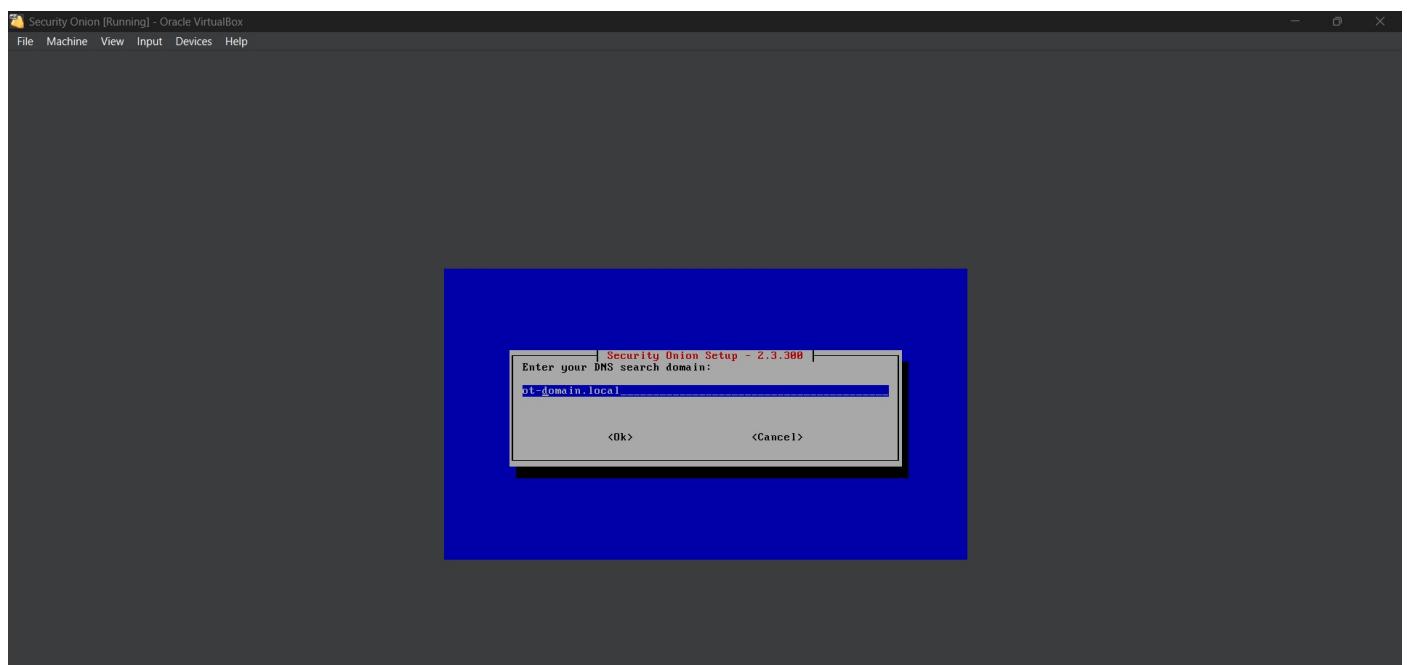
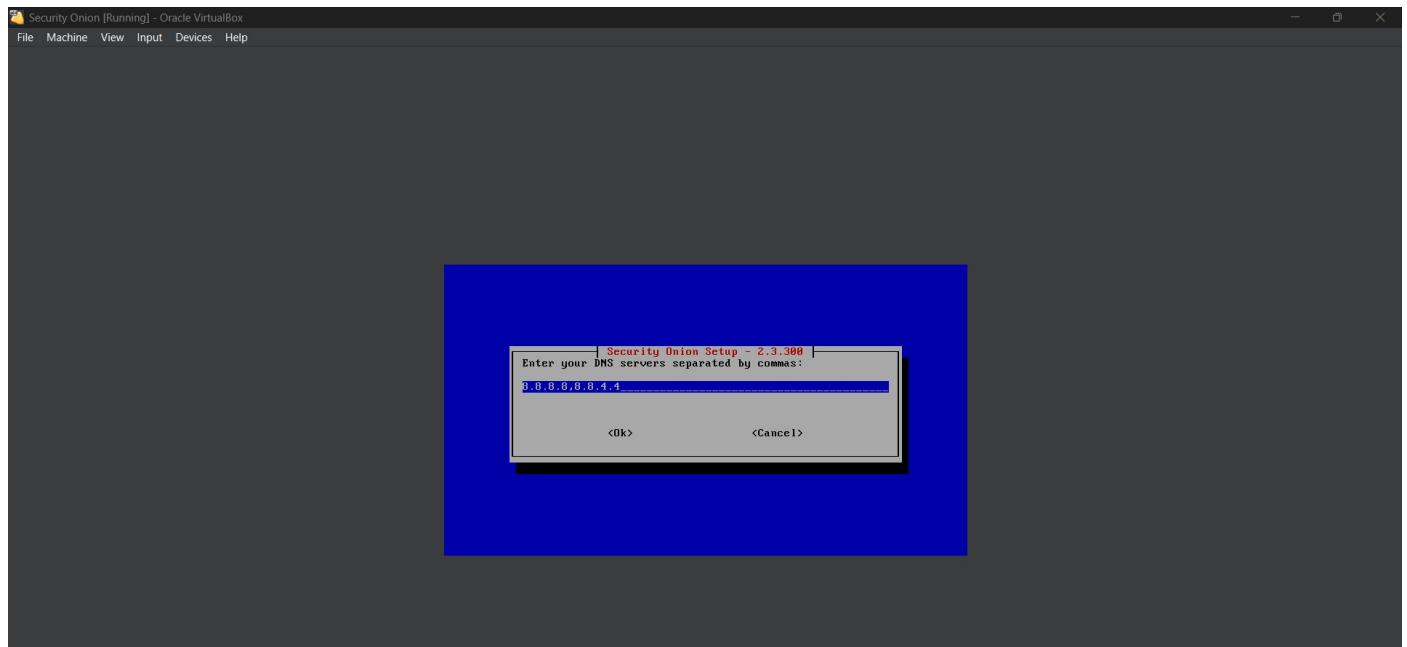
I selected the first interface enp0s3(NAT-Internal Network) for the management NIC.

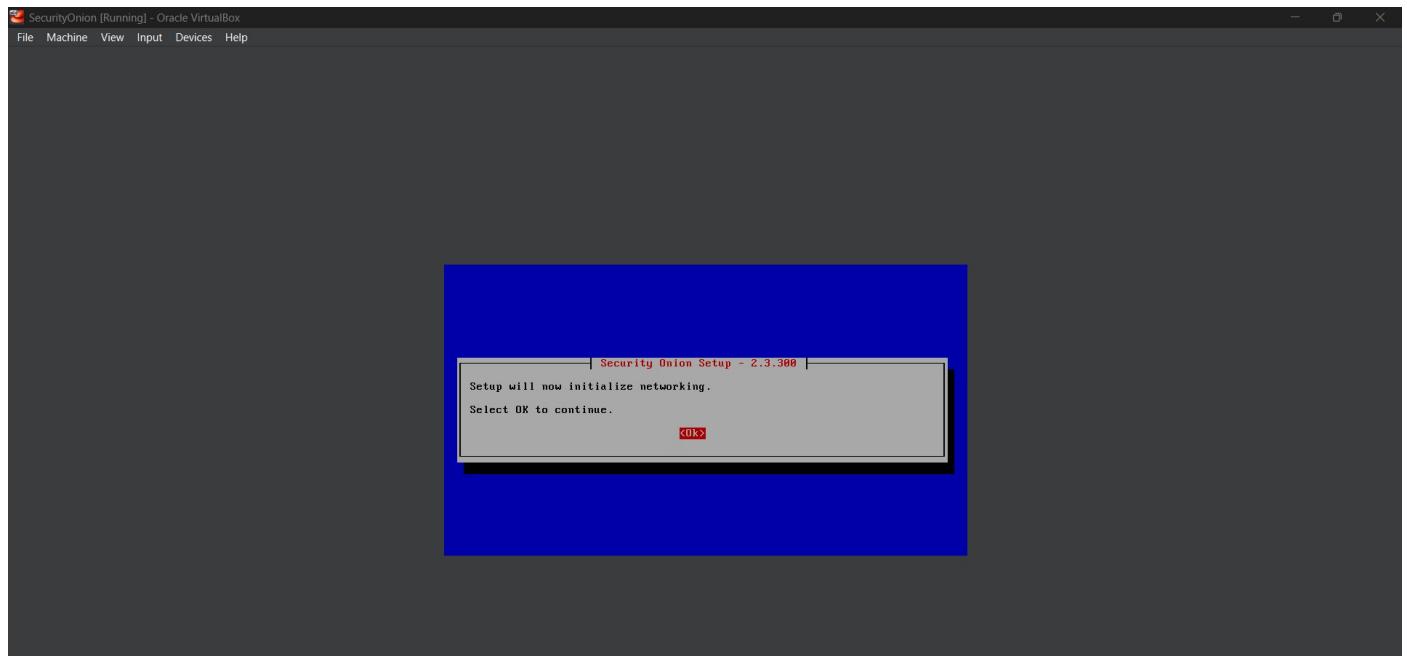


I configured the IP address details, including static IP, netmask, gateway, and DNS server.

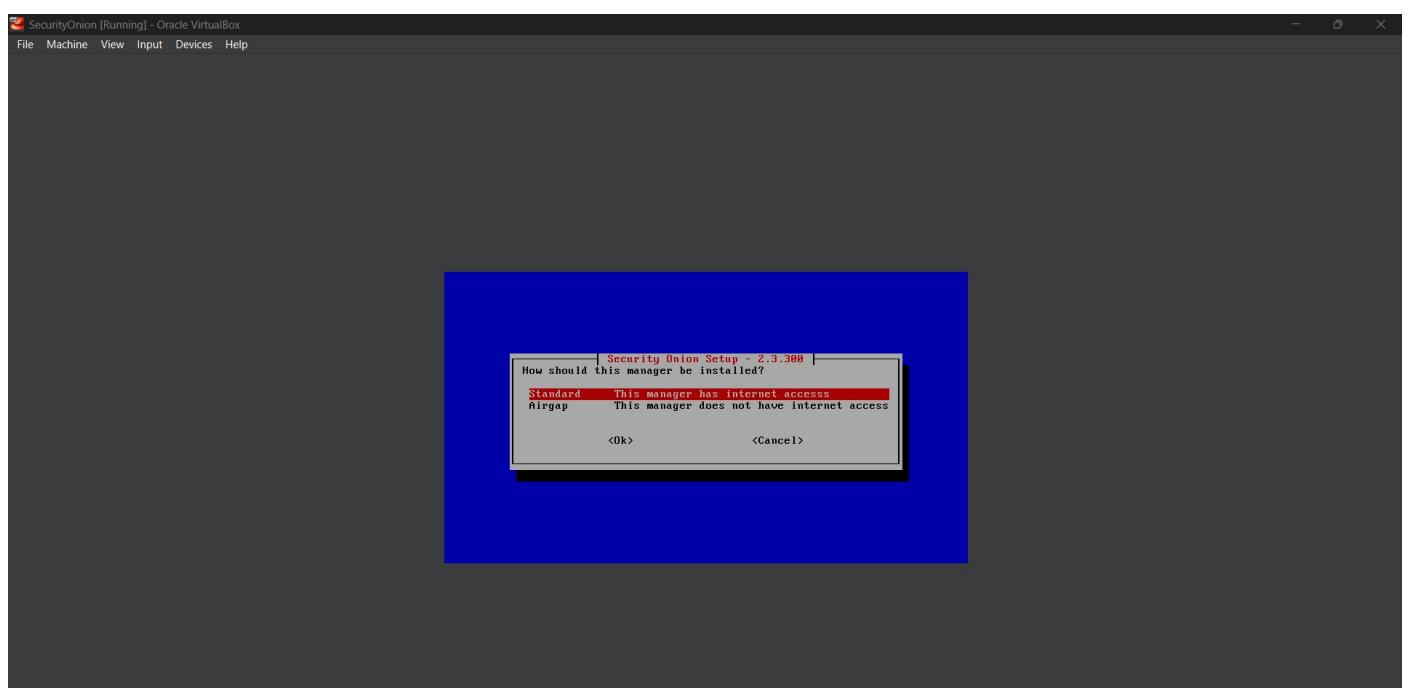


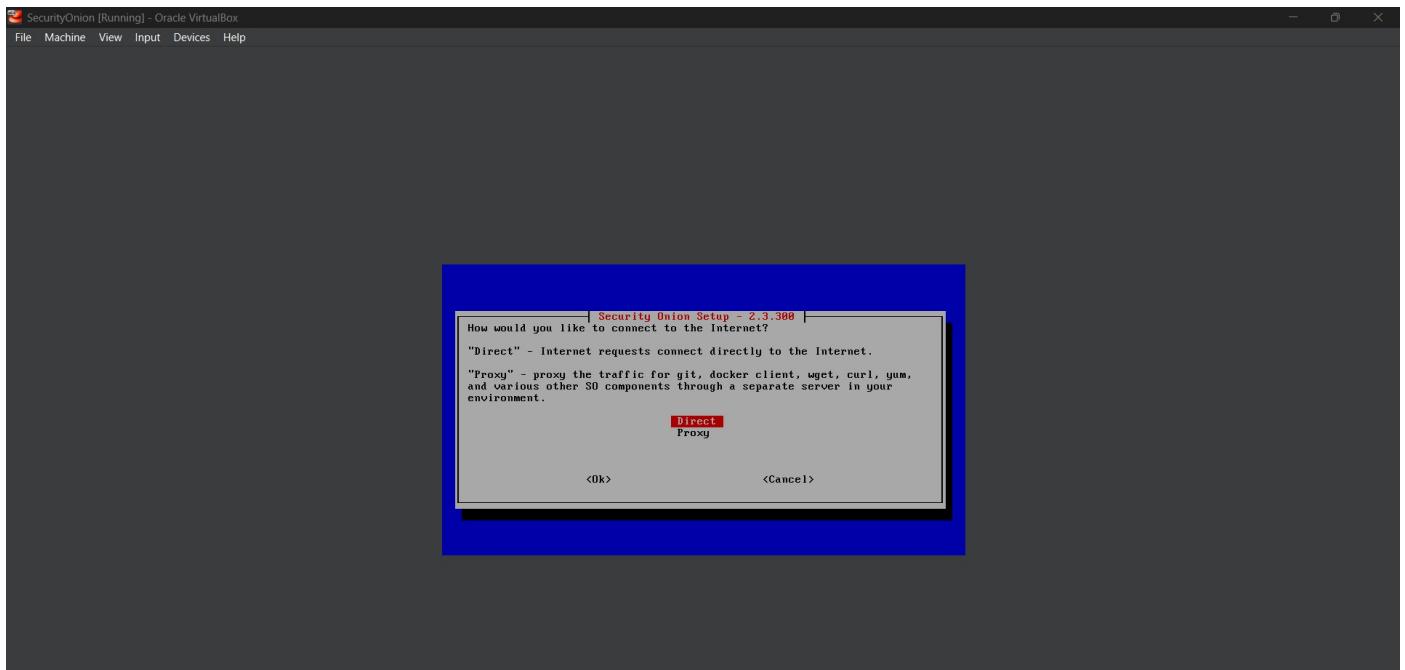




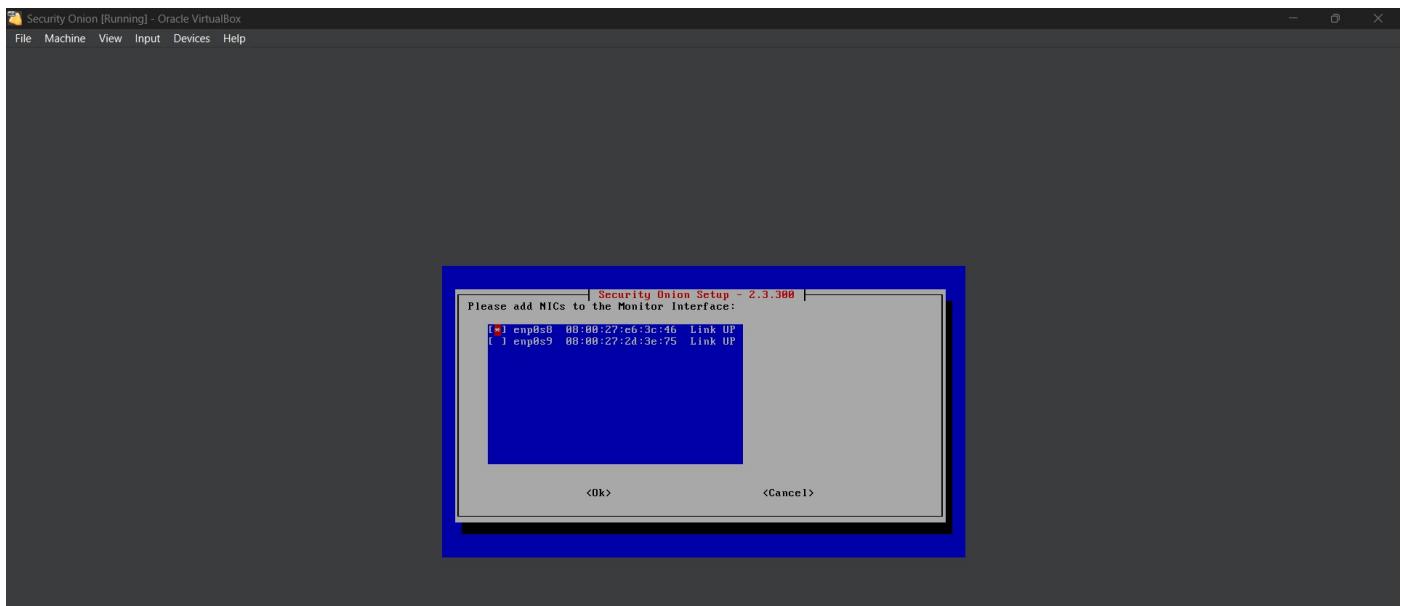


I Installed the manager in Standard mode so that I will have Internet Access

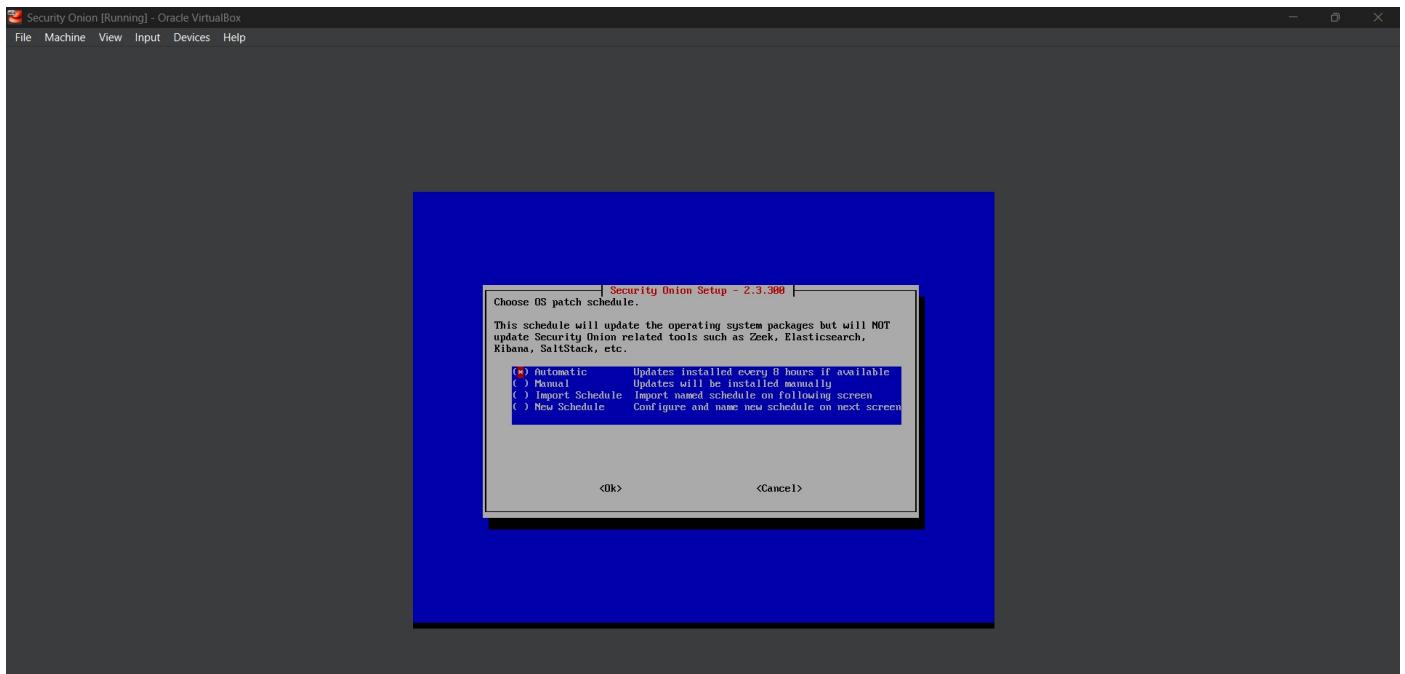




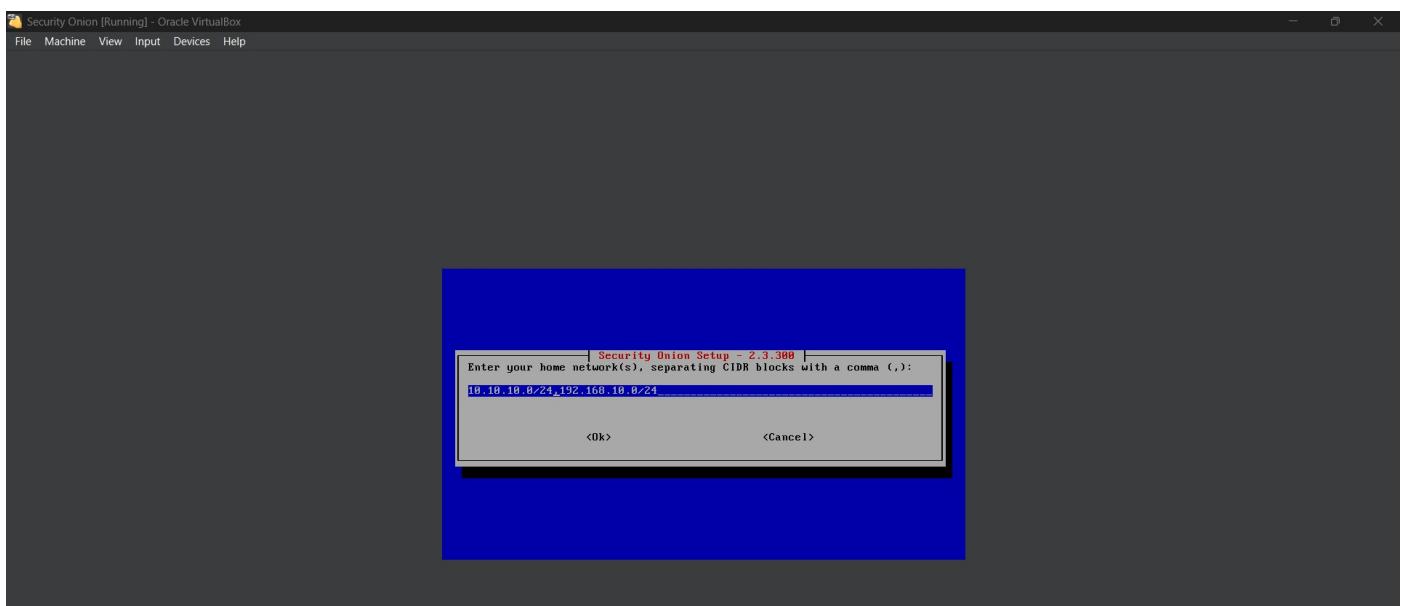
I selected the second interface as the monitoring(enp0s8) as (sniffing) interface.



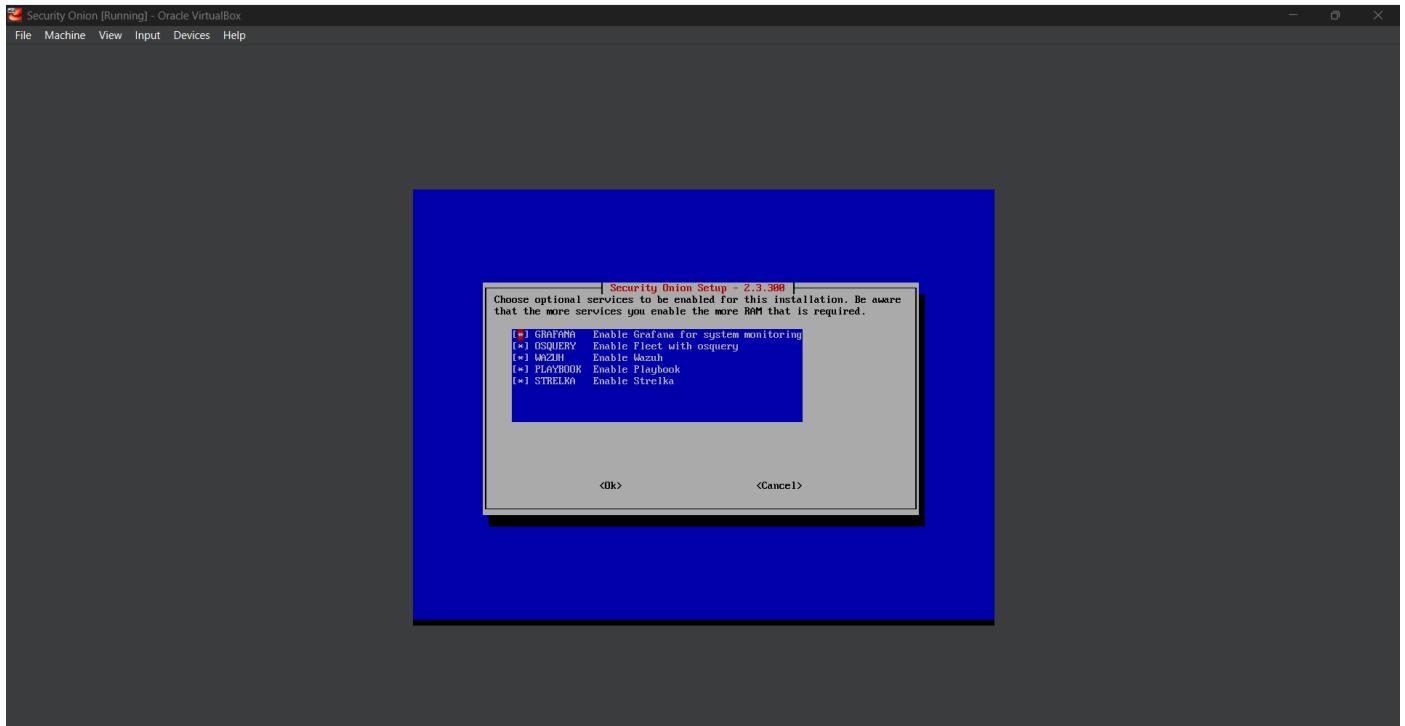
I chose *Automatic* for the operating system patch schedule.



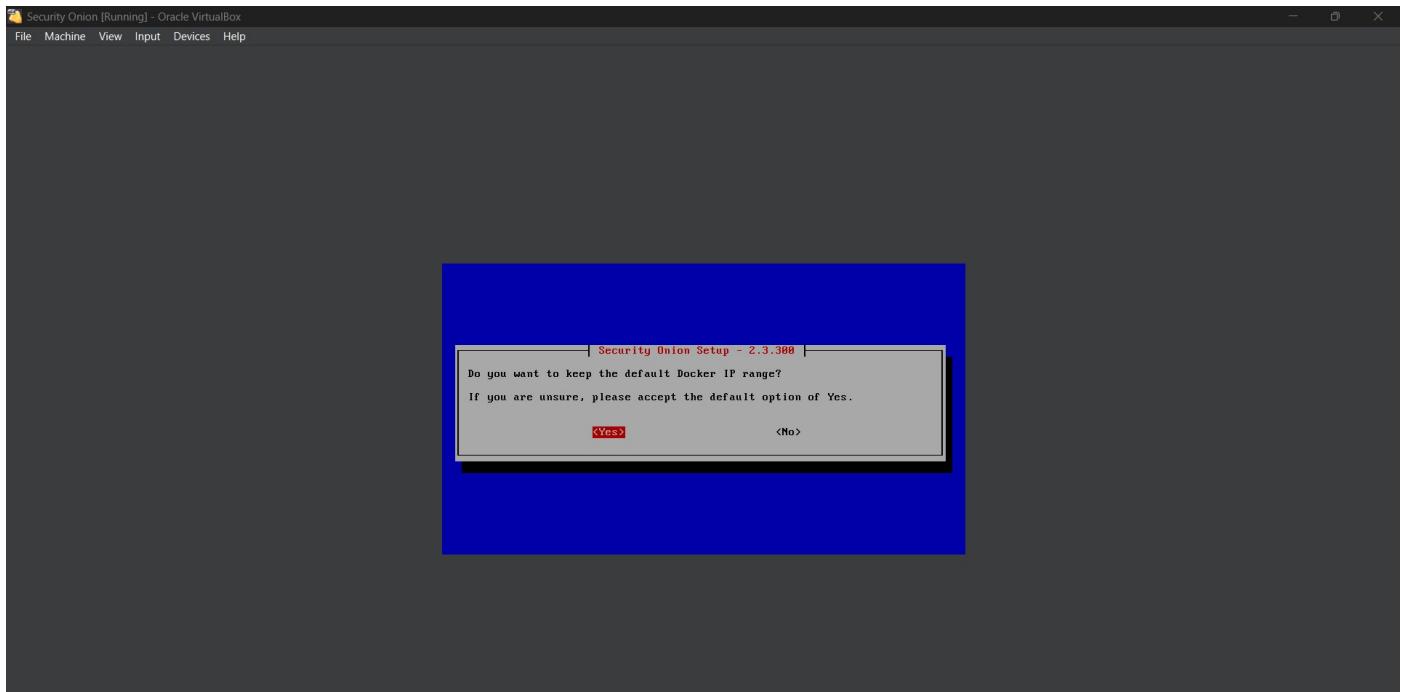
I set the *HOME_NET* IP address range to *10.10.10.0/24, 192.168.10.0/24*



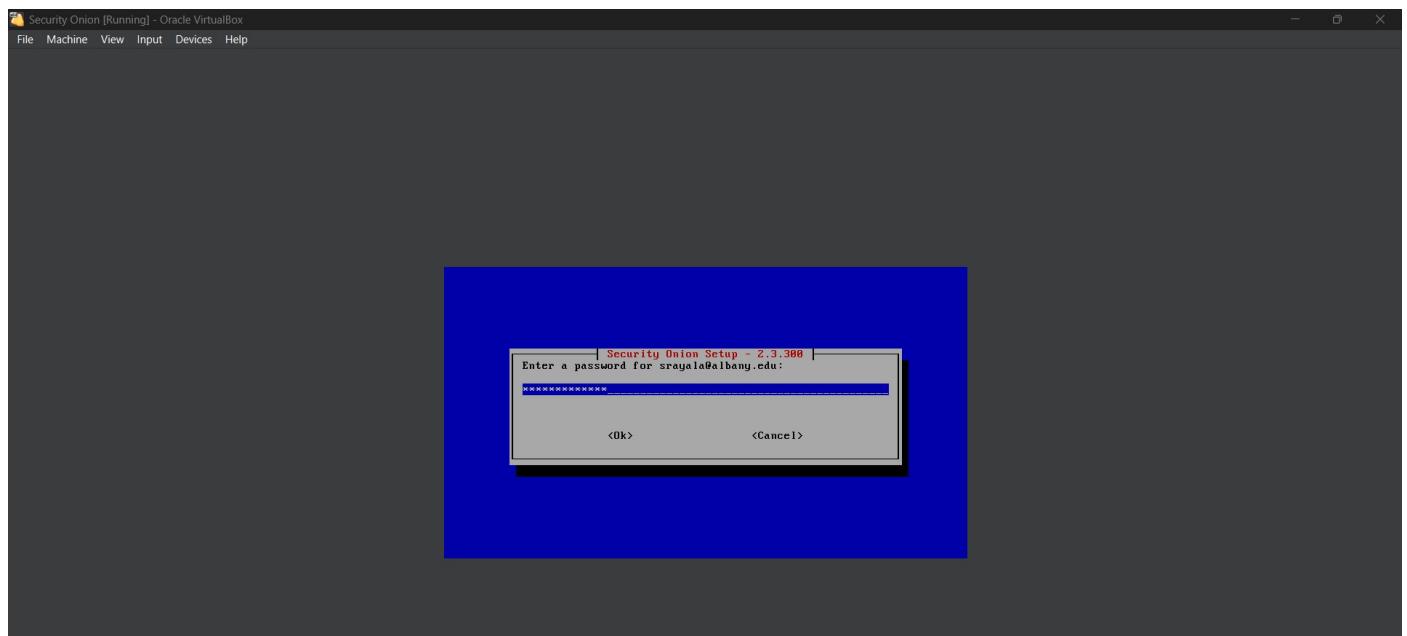
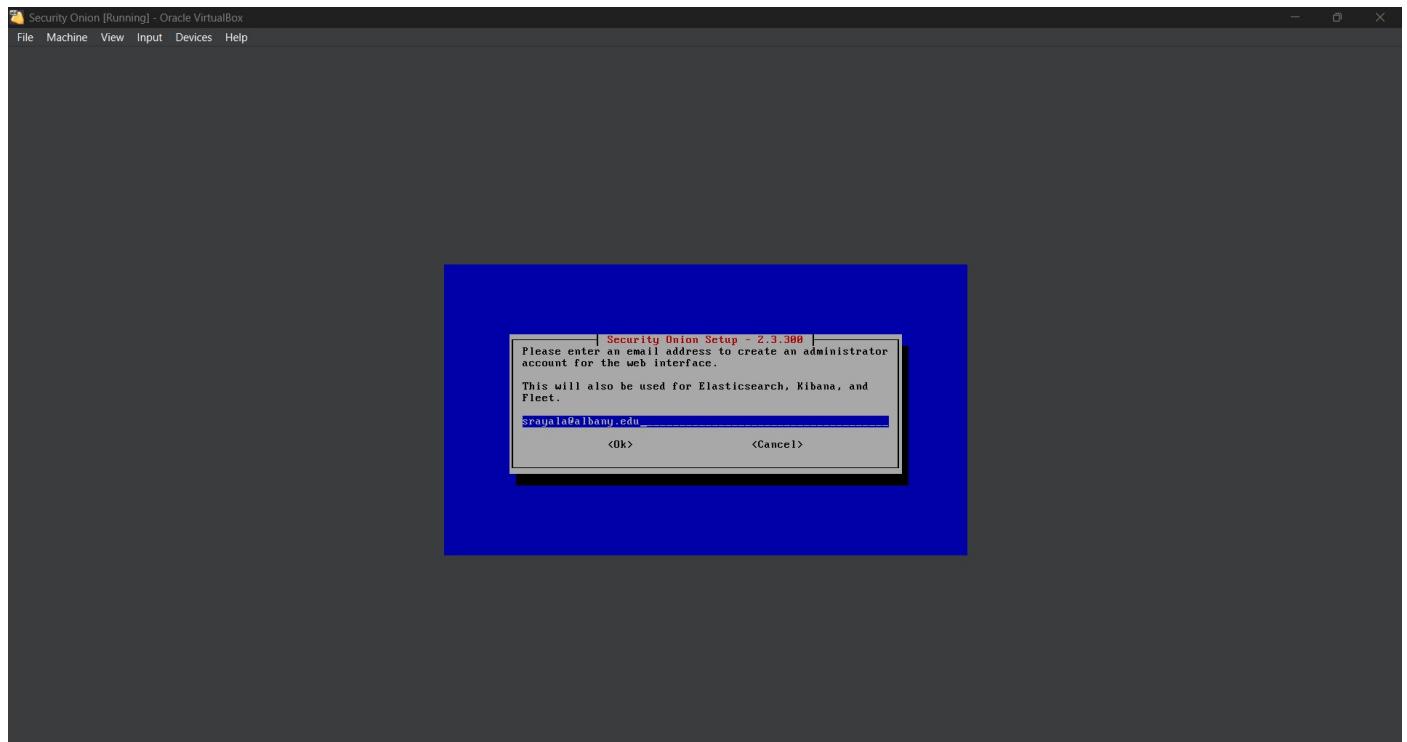
I selected the default components to install for the Security Onion services.



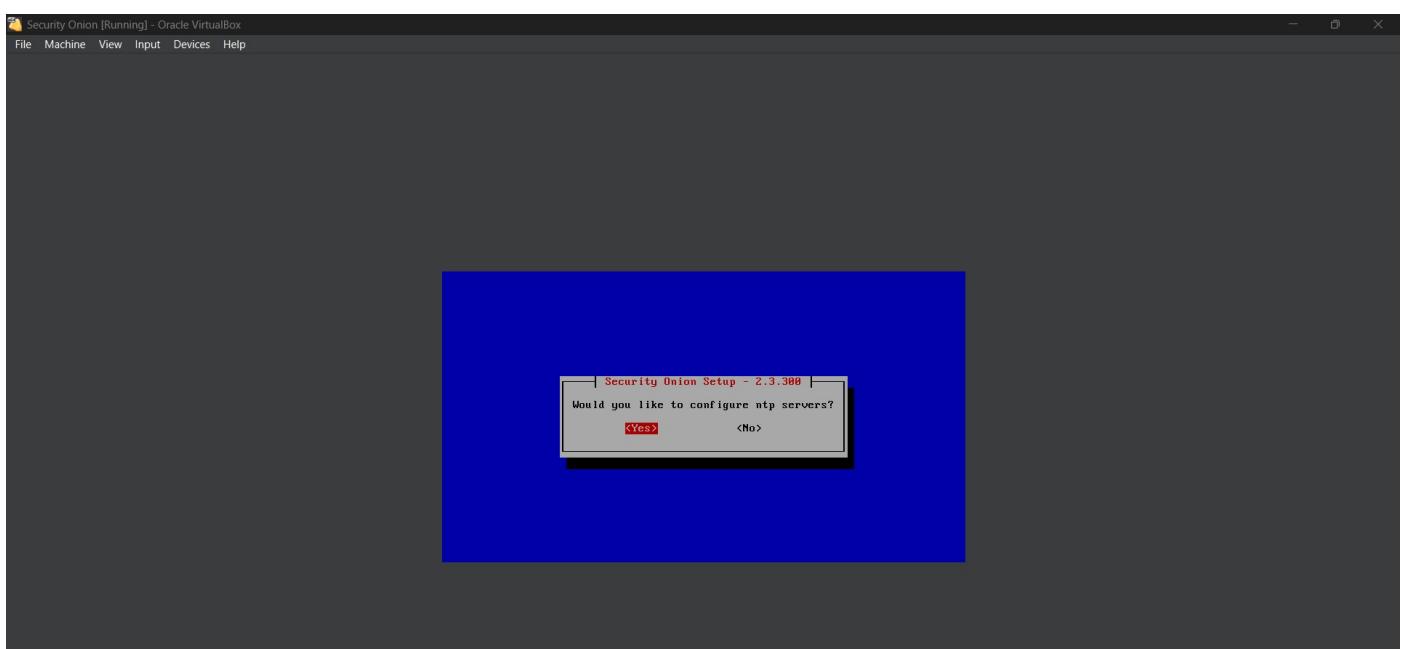
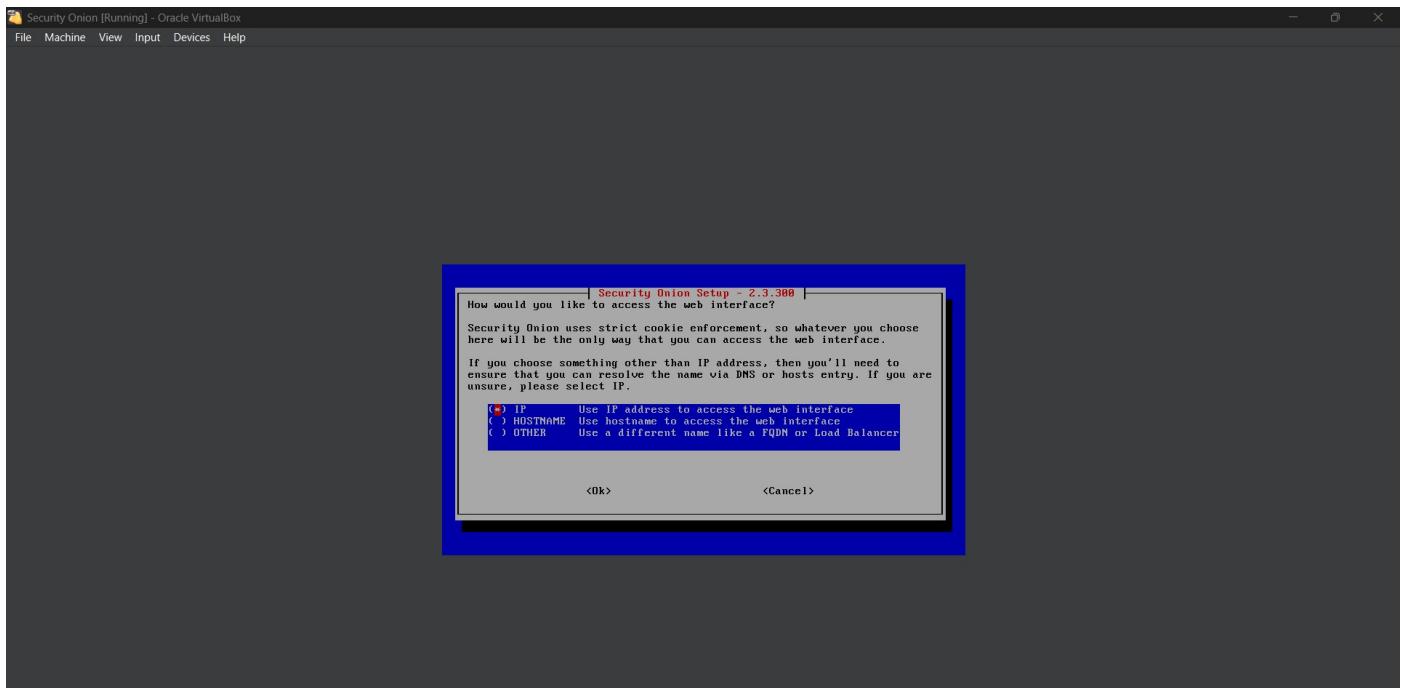
I confirmed that I wanted Security Onion to use the default Docker IP range.

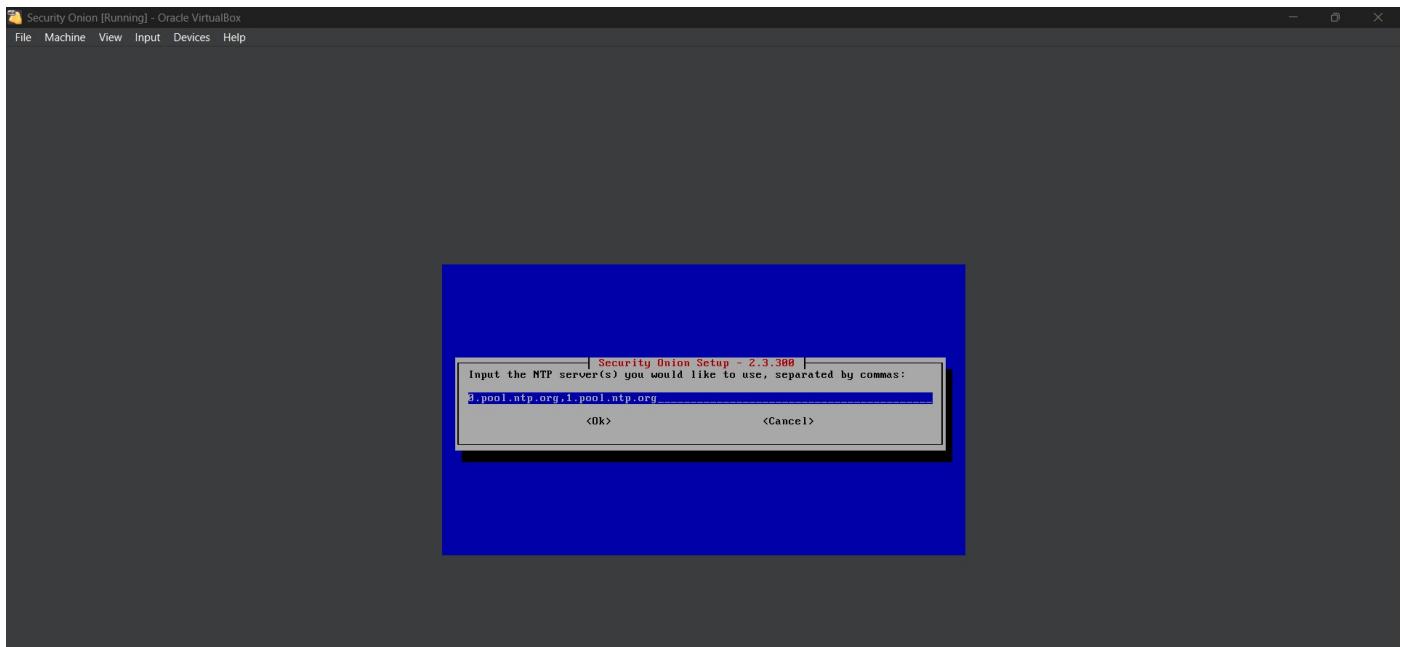


I specified an email address and password for the administrator of the web interface.

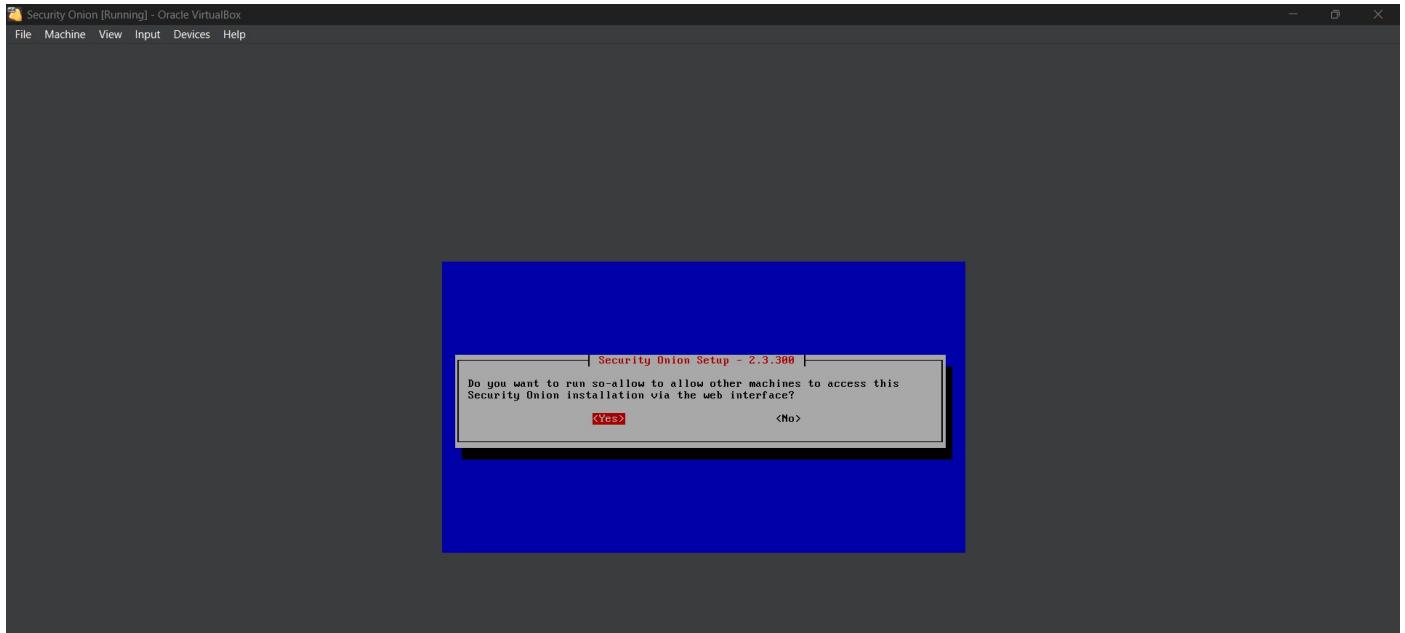


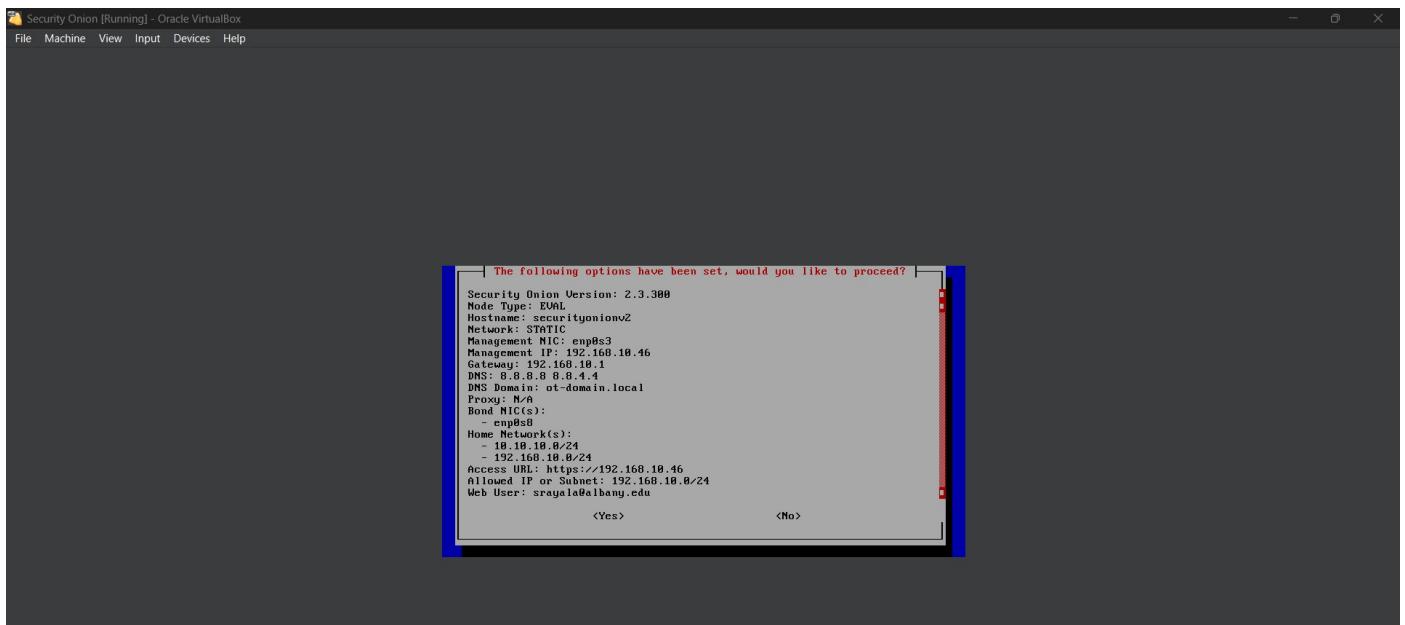
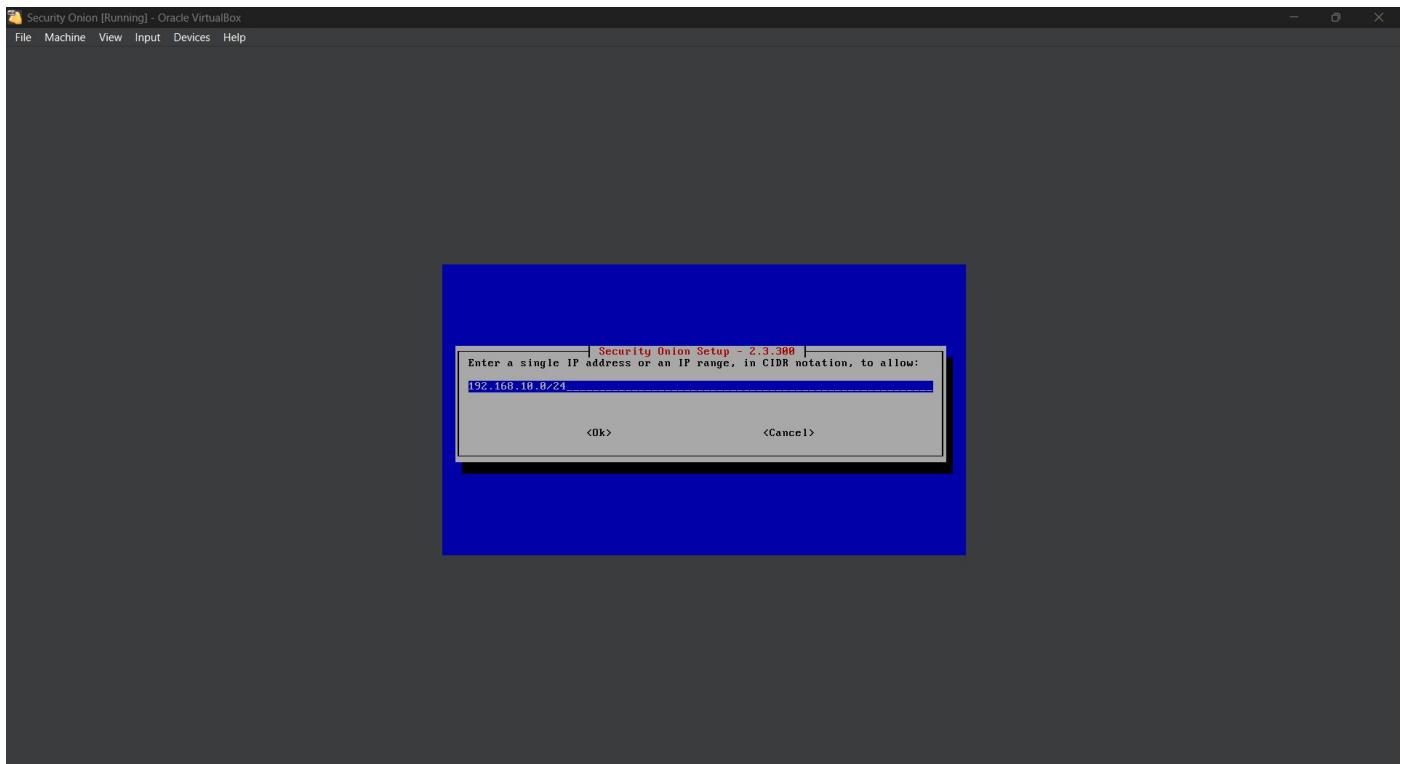
I selected *IP* for the access method and configured NTP Servers

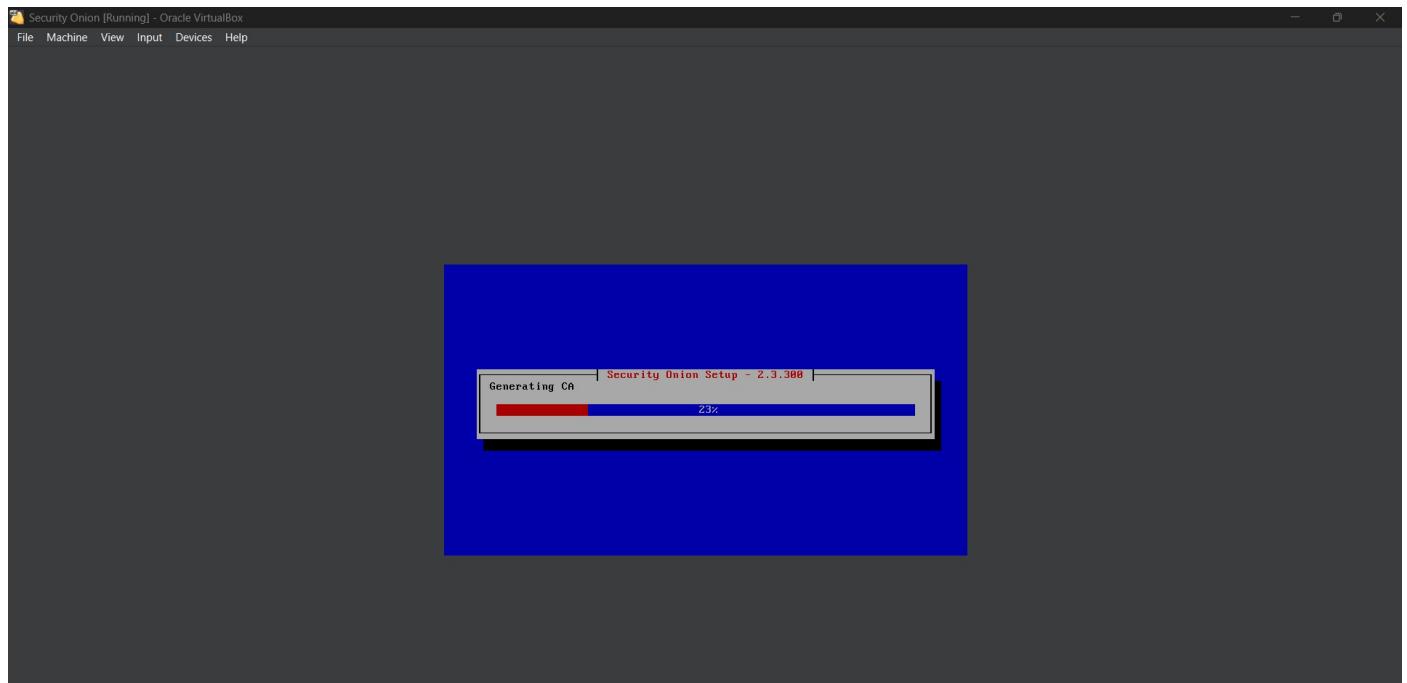




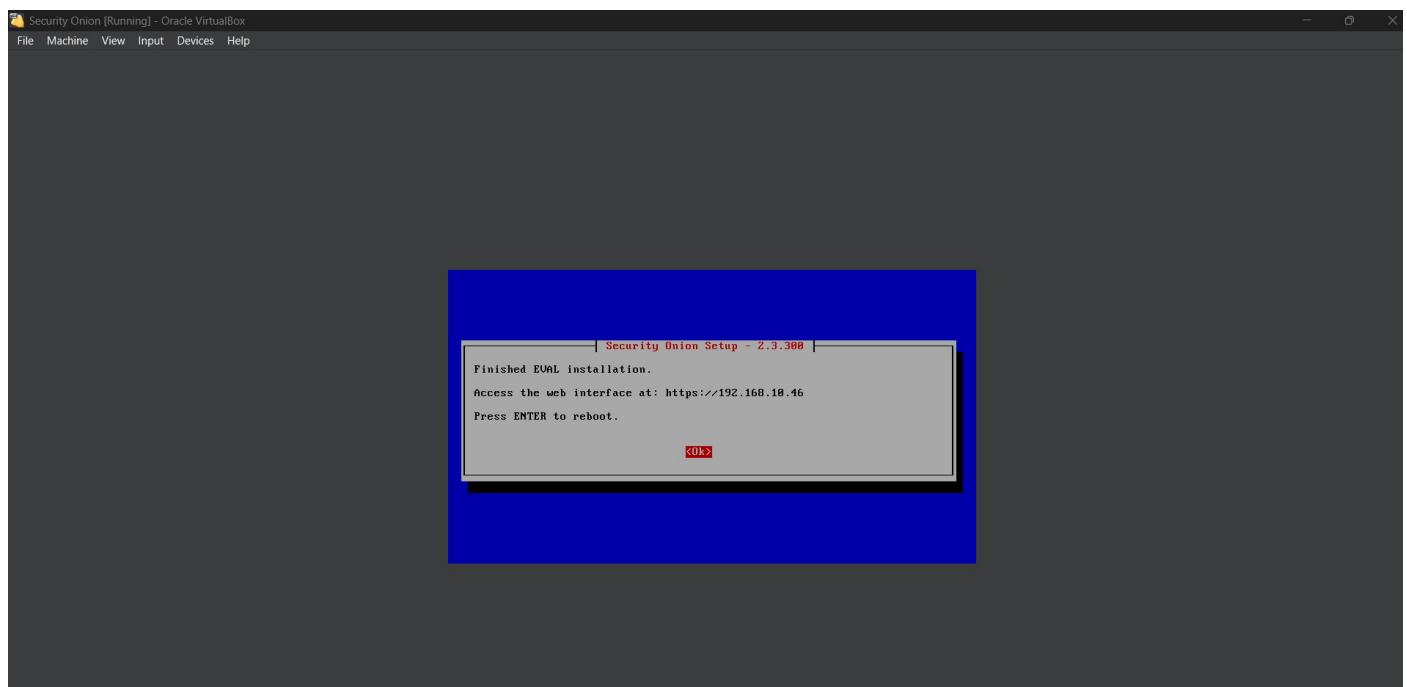
I configured the network to allow access to the Security Onion management interfaces and web portal from the lab network. I confirmed the installation process and allowed the appliance to configure.



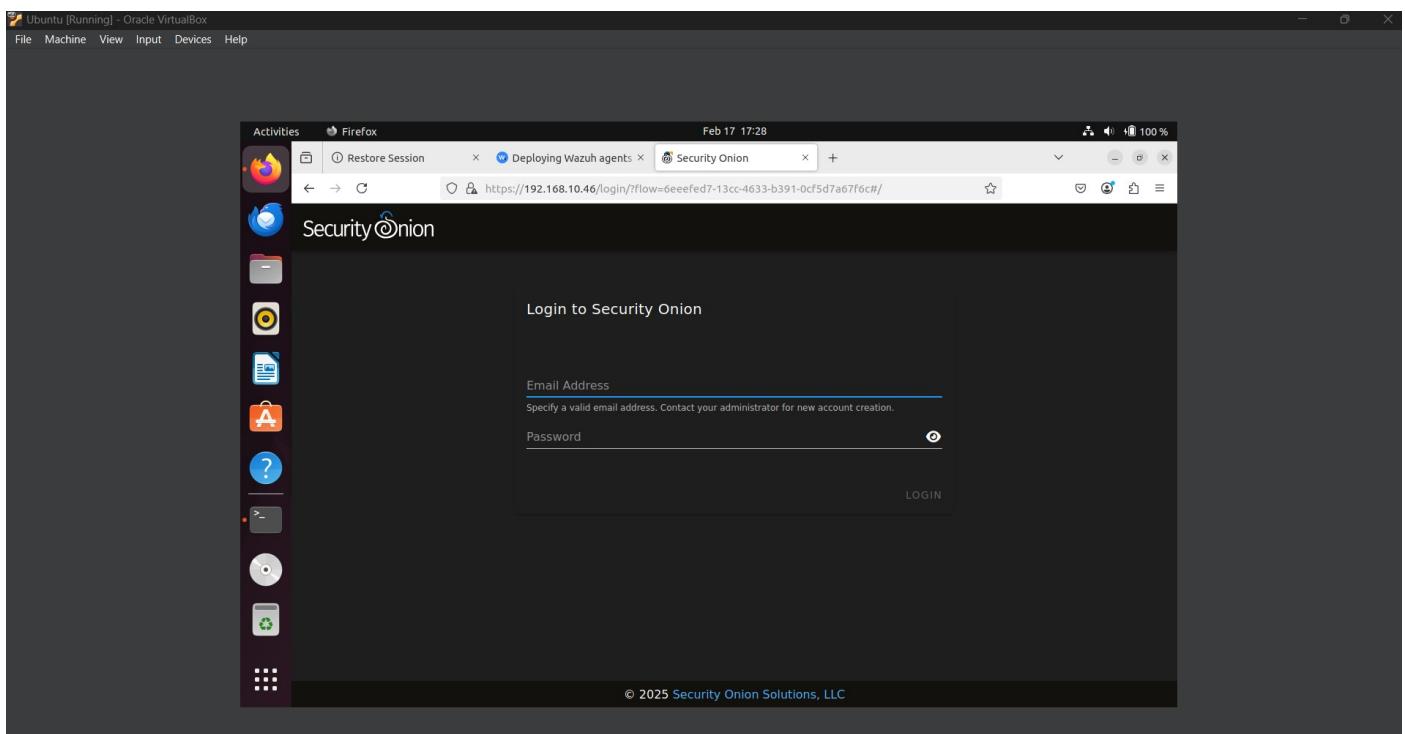
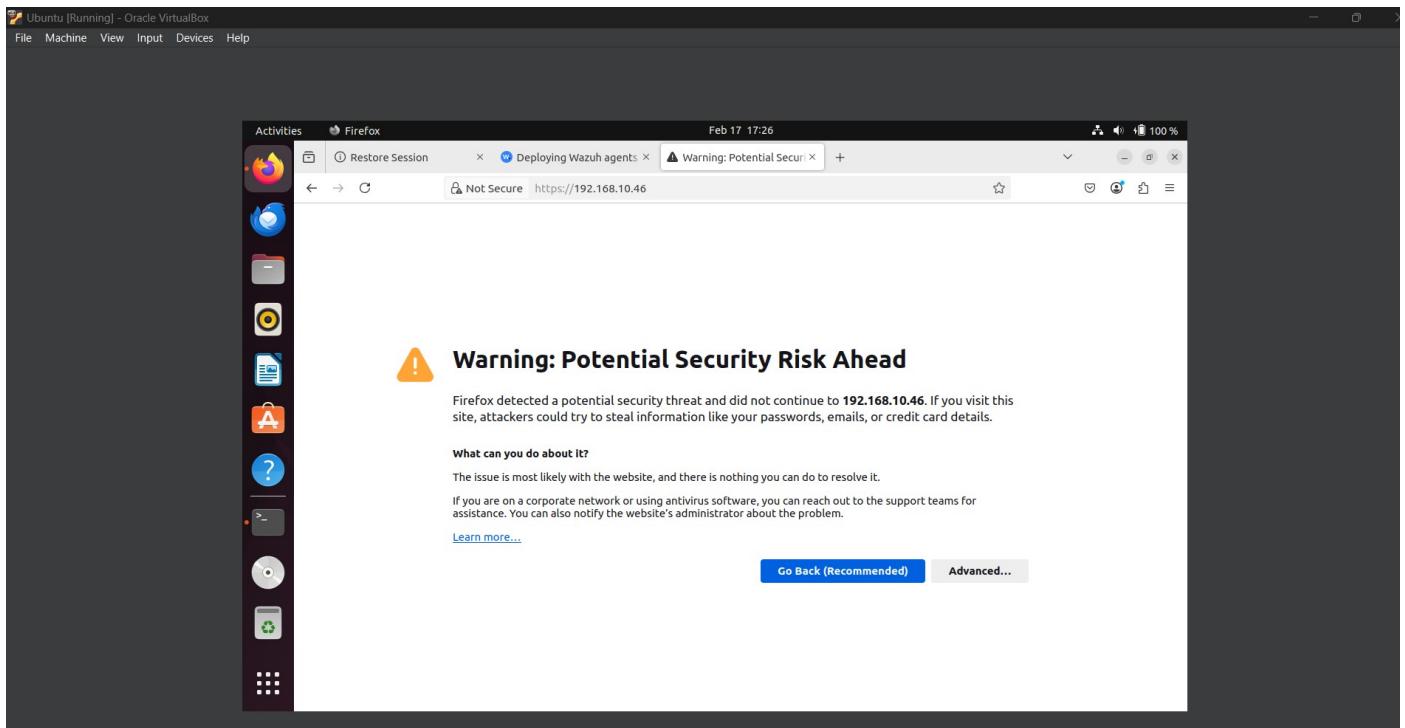




Once the installation was complete, I rebooted the system and was ready to use Security Onion.



I can access my security onion from <https://192.168.10.46>



Objective 2: Configuring Security Onion

With the Security Onion VM up and running, I proceeded with three initial configuration tasks: installing VMware tools, updating the Suricata ruleset, and adding a web interface user.

```
Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...

Dracie Linux Server 9.5
Kernel 5.15.0-305.176.4.el9uek.x86_64 on an x86_64
securityonion@ login: sriram
Password:
Login incorrect
securityonion@ login: sriram
Password:
Last failed login: Mon Feb 17 00:07:40 UTC 2025 on ttym1
There were 2 failed login attempts since the last successful login.
Last login: Sun Feb 16 20:35:43 on ttym1

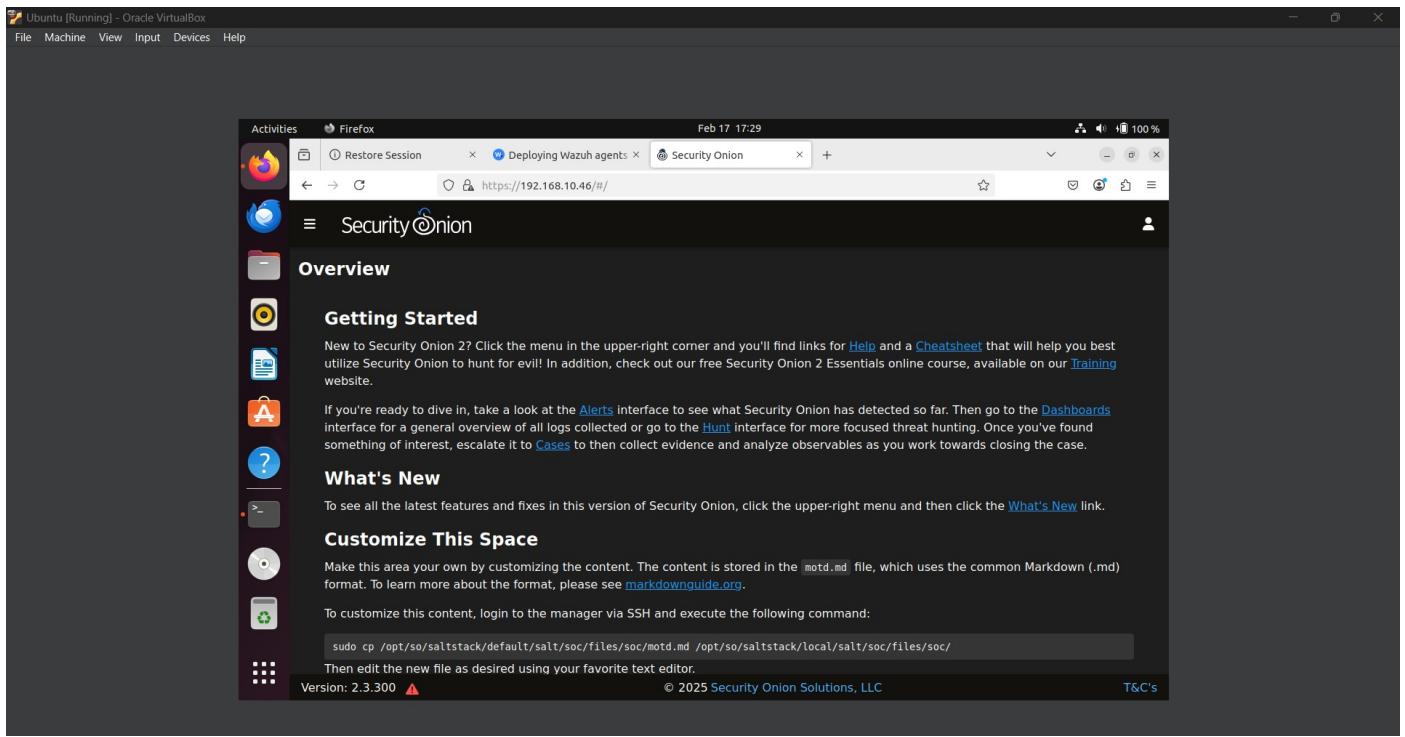
Access the Security Onion web interface at https://192.168.10.50

=====
# The following nodes in your Security Onion grid may need to be restarted due to package updates.
# If a node has already been switched and restarted but has been up for less than 15 minutes,
# then it may not have updated its status yet.
=====

securityonion@_eval
[sriram@securityonion ~]$
```

```
Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
so-grafana ----- [ STARTING ]
so-idstools ----- [ STARTING ]
so-influxdb ----- [ STARTING ]
so-kibana ----- [ STARTING ]
so-kratos ----- [ OK ]
so-mysql ----- [ OK ]
so-nginx ----- [ STARTING ]
so-playbook ----- [ STARTING ]
so-redis ----- [ STARTING ]
so-sensoroni ----- [ STARTING ]
so-soc ----- [ STARTING ]
so-splunk ----- [ STARTING ]
so-strelo ----- [ STARTING ]
so-strelka-backend ----- [ OK ]
so-strelka-coordinator ----- [ STARTING ]
so-strelka-filestream ----- [ STARTING ]
so-strelka-frontend ----- [ STARTING ]
so-strelka-gatekeeper ----- [ STARTING ]
so-strelka-manager ----- [ STARTING ]
so-suricata ----- [ STARTING ]
so-telegraf ----- [ STARTING ]
so-wazuh ----- [ STARTING ]
so-zeeb ----- [ STARTING ]

[sriram@securityonion ~]$ _
```



Objective 2.1: Installing VMware Tools

I installed VMware tools to improve the integration of the guest VM with VMware Workstation.

I ran the following commands to update the package repository and install VMware tools:

sudo yum update

```
Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Activities Firefox
Feb 17 17:29
Restore Session Deploying Wazuh agents Security Onion + 100 %
https://192.168.10.46/#/
Security Onion

☰ Security@onion
Overview

Getting Started
New to Security Onion 2? Click the menu in the upper-right corner and you'll find links for Help and a Cheatsheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion 2 Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. Then go to the Dashboards interface for a general overview of all logs collected or go to the Hunt interface for more focused threat hunting. Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

What's New
To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

Customize This Space
Make this area your own by customizing the content. The content is stored in the motd.md file, which uses the common Markdown (.md) format. To learn more about the format, please see markdownguide.org.

To customize this content, login to the manager via SSH and execute the following command:
sudo cp /opt/so/saltstack/default/salt/soc/files/soc/motd.md /opt/so/saltstack/local/salt/soc/files/soc/
Then edit the new file as desired using your favorite text editor.

Version: 2.3.300 ▲ © 2025 Security Onion Solutions, LLC T&C's
```

sudo yum install open-vm-tools-desktop fuse

```
grub2-tools-minimal.x86_64 1:2.02-0.07.0.e17.centos.14
iw1100-firmware.noarch 0:39.31.5.1-03.e17_9
iw1100-firmware.noarch 0:39.31.5.1-03.e17_9
iw1105-firmware.noarch 0:18.168.6.1-03.e17_9
iw1135-firmware.noarch 0:18.168.6.1-03.e17_9
iw12000-firmware.noarch 0:18.168.6.1-03.e17_9
iw12030-firmware.noarch 0:18.168.6.1-03.e17_9
iw13160-firmware.noarch 0:25.30.13.0-03.e17_9
iw14050-firmware.noarch 0:220.61.2.24-03.e17_9
iw15080-firmware.noarch 0:8.83.5.1.1-03.e17_9
iw15150-firmware.noarch 0:8.24.2.2-03.e17_9
iw16000gza-firmware.noarch 0:18.168.6.1-03.e17_9
iw16000gzb-firmware.noarch 0:18.168.6.1-03.e17_9
iw16050-firmware.noarch 0:41.28.5.1-03.e17_9
iw17260-firmware.noarch 0:25.30.13.0-03.e17_9
kernel-tools.x86_64 0:3.10.0-1160.119.1.e17
kernel-tools-libs.x86_64 0:3.10.0-1160.119.1.e17
less.x86_64 0:458-10.e17_9
linux-firmware.noarch 0:28280421-03.git78c8340.e17_9
python-perf.x86_64 0:3.10.0-1160.119.1.e17

Complete!
[sriram@securityonionv2 ~]$
```

After the installation, I rebooted the VM to apply the changes.

Objective 2.2: Updating Suricata Rulesets

To ensure that Suricata could detect the latest threats, I updated its ruleset.

sudo so-rule-update

```
iw15150-firmware.noarch 0:8.24.2.2-03.e17_9
iw16000gza-firmware.noarch 0:9.221.4.1-03.e17_9
iw16000gzb-firmware.noarch 0:18.168.6.1-03.e17_9
iw16050-firmware.noarch 0:41.28.5.1-03.e17_9
iw17260-firmware.noarch 0:25.30.13.0-03.e17_9
kernel-tools.x86_64 0:3.10.0-1160.119.1.e17
kernel-tools-libs.x86_64 0:3.10.0-1160.119.1.e17
less.x86_64 0:458-10.e17_9
linux-firmware.noarch 0:28280421-03.git78c8340.e17_9
python-perf.x86_64 0:3.10.0-1160.119.1.e17

Complete!
[sriram@securityonionv2 ~]$ sudo so-rule-update
[sudo] password for sriram:
2825-02-17 22:43:40.649 - <INFO> - Loading ./rulecat.conf.
2825-02-17 22:43:40.652 - <INFO> - Forcing Suricata version to 6.8.
2825-02-17 22:43:40.663 - <INFO> - Fetching https://rules.emergingthreats.net/open/suricata-6.8.0/emerging.rules.tar.gz.
100% - 4708642/4708642 2825-02-17 22:43:41.477 - <INFO> - Done.
2825-02-17 22:43:41.761 - <INFO> - Ignoring file rules/emerging-deleted.rules
2825-02-17 22:43:41.761 - <INFO> - Loading local file /opt/so/rules/nids/local.rules
```

The Security Onion appliance updated the ruleset and restarted the Suricata engine.

Objective 2.3: Adding a Web Portal User

To allow non-admin access to the Security Onion web portal, I added a web portal user.

I ran the following command to add a new user:

```
sudo so-user-add web-pac@ot-domain.local
```

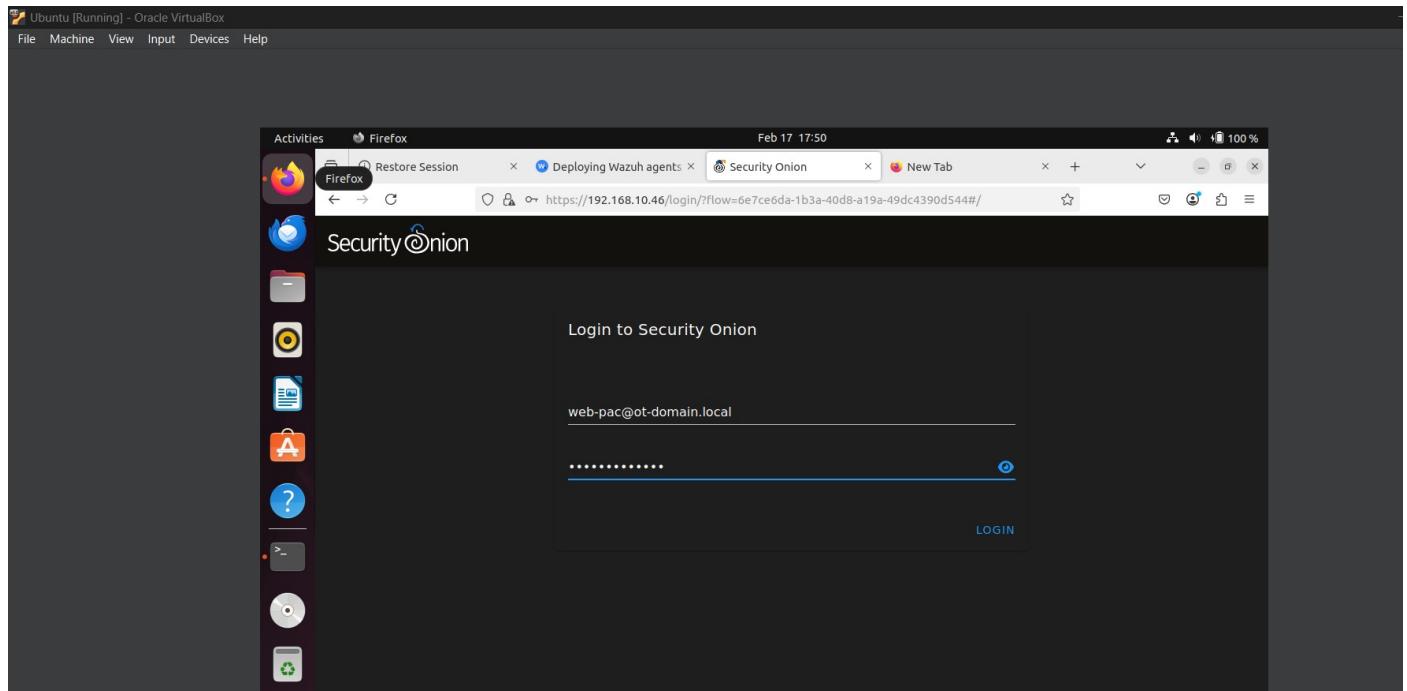
```
Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help

2025-02-17 22:43:40,003 - <INFO> - Fetching https://rules.emergingthreats.net/open/suricata-6.0.0/emerging.rules.tar.gz.
168x - 4788642/4788642 2025-02-17 22:43:41,477 - <INFO> - Done.

2025-02-17 22:43:41,761 - <INFO> - Ignoring file rules/emerging-deleted.rules
2025-02-17 22:43:41,761 - Loading local file /opt/so/rules/nids/local.rules
2025-02-17 22:43:49,367 - <INFO> - Loaded 56315 rules.
2025-02-17 22:43:49,422 - <INFO> - Disabled 0 rules.
2025-02-17 22:43:49,422 - <INFO> - Enabled 0 rules.
2025-02-17 22:43:49,422 - <INFO> - Modified 0 rules.
2025-02-17 22:43:49,422 - <INFO> - Dropped 0 rules.
2025-02-17 22:43:50,126 - <INFO> - Enabled 136 rules for flowbit dependencies.
2025-02-17 22:44:19,940 - <INFO> - Writing rules to /opt/so/rules/nids/all.rules
Total: 56315 rules added: 42344, deleted: 0, removed: 0, modified: 0
2025-02-17 22:44:23,661 - <INFO> - Done.

[lsriram@securityonionv02 ~]$ ls
[lsriram@securityonionv02 ~]$ sudo so-user-add web-pac@ot-domain.local
Enter new password:
Password does not meet the minimum requirements
[lsriram@securityonionv02 ~]$ sudo so-user-add web-pac@ot-domain.local
Enter new password:
Syncing users and roles between SOC and Elastic...
```

I entered the sudo password, followed by the new user's password, and successfully added the user to the system. I accessed the Security Onion web portal by navigating to <https://192.168.10.46> and logged in with the new user account.



Objective 3: Deploying Wazuh Agents

I deployed Wazuh agents for host-based security monitoring and event log forwarding.

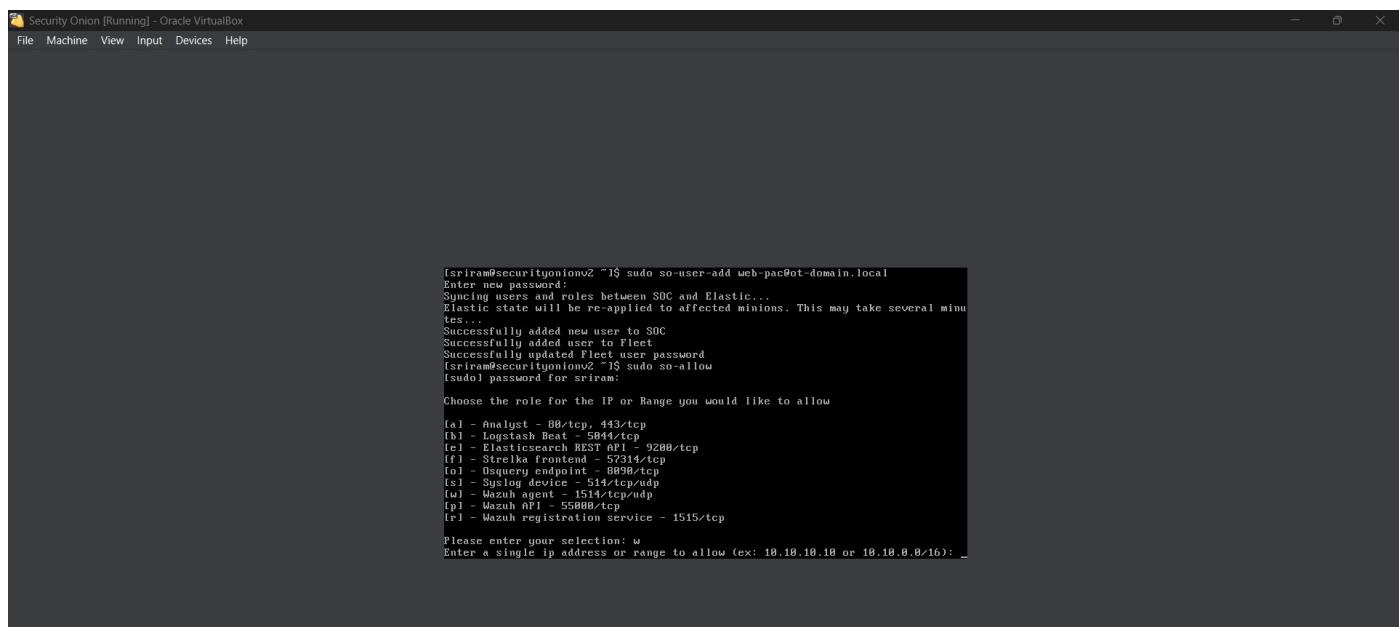
Configuring Wazuh Manager Access

1. I logged into the Security Onion appliance via SSH.

I ran the command:

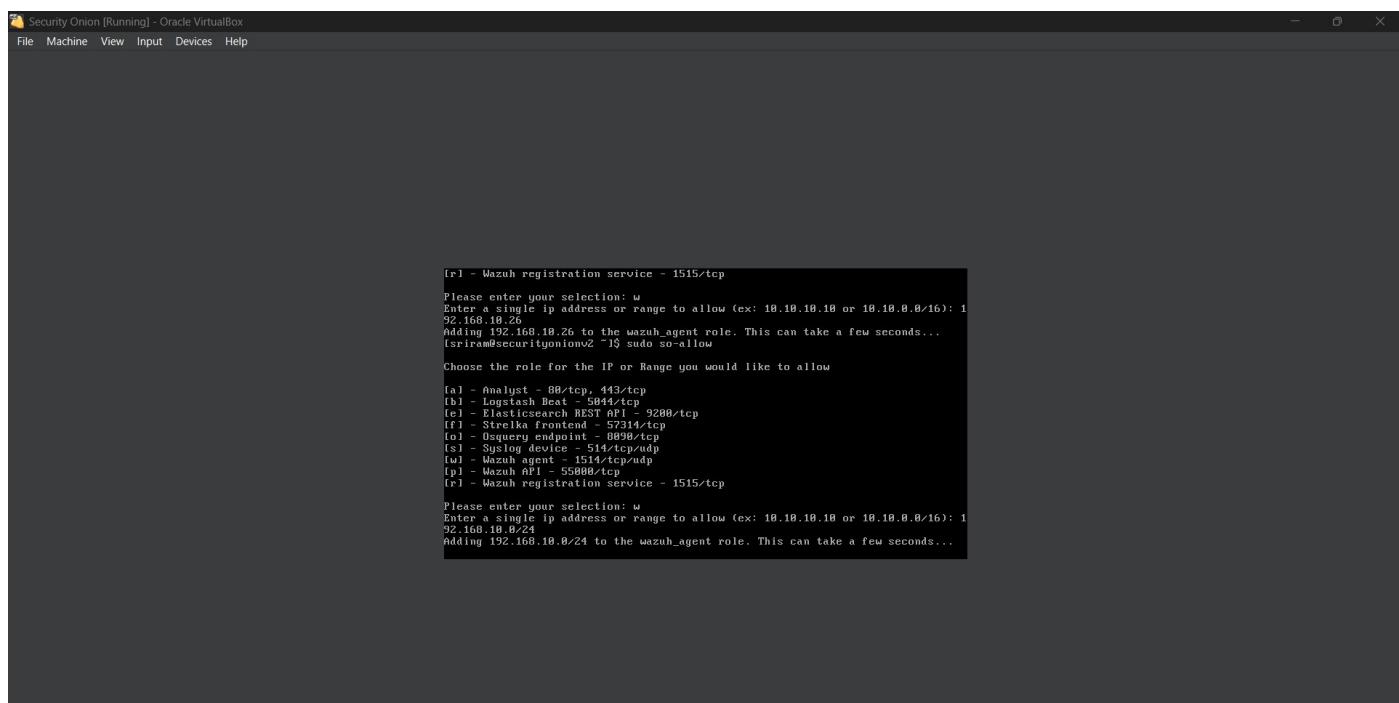
```
sudo so-allow
```

I chose the `w` option for the Wazuh agent (Port 1514/tcp/udp) and specified the lab network's IP address range `192.168.10.0/24`.



```
[sriram@securityonion ~]$ sudo so-user-add web-pac@ot-domain.local
Enter new password:
Syncing users and roles between SOC and Elastic...
Elastic state will be re-applied to affected minions. This may take several minutes.
Successfully added new user to SOC
Successfully updated Fleet user password
[sriram@securityonion ~]$ sudo so-allow
[sudo] password for sriram:
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] - Streika frontend - 57314/tcp
[o] - Osquery endpoint - 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55900/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection: w
Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 192.168.10.0/24
Adding 192.168.10.0/24 to the wazuh_agent role. This can take a few seconds...
```



```
[sriram@securityonion ~]$ sudo so-allow
[sudo] password for sriram:
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] - Streika frontend - 57314/tcp
[o] - Osquery endpoint - 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55900/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection: r
Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 192.168.10.0/24
Adding 192.168.10.0/24 to the wazuh_registration role. This can take a few seconds...
```

Registering Wazuh Agents

I ran the command to start the Wazuh agent management terminal:

sudo so-wazuh-agent-manage

I selected **A** for *Add an agent*, entered the agent's hostname and IP address, and confirmed the addition.

I extracted the agent key by selecting **E** for *Extract key for an agent* and recorded it for later use.

```
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection: w
Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 1
Adding 192.168.10.2/24 to the wazuh_agent role. This can take a few seconds...
(sriram@securingonionv2 ~) $ sudo so-wazuh-agent-manage

*****
* Wazuh v3.13.1 Agent manager *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(D)elete an agent (D).
(Q)uit.

Choose your action: A,E,L,D or Q: a
- Adding a new agent (use 'q' to return to the main menu).
Please provide the following:
* A name for the new agent: ubuntu
```

```
Agent added with ID 002.

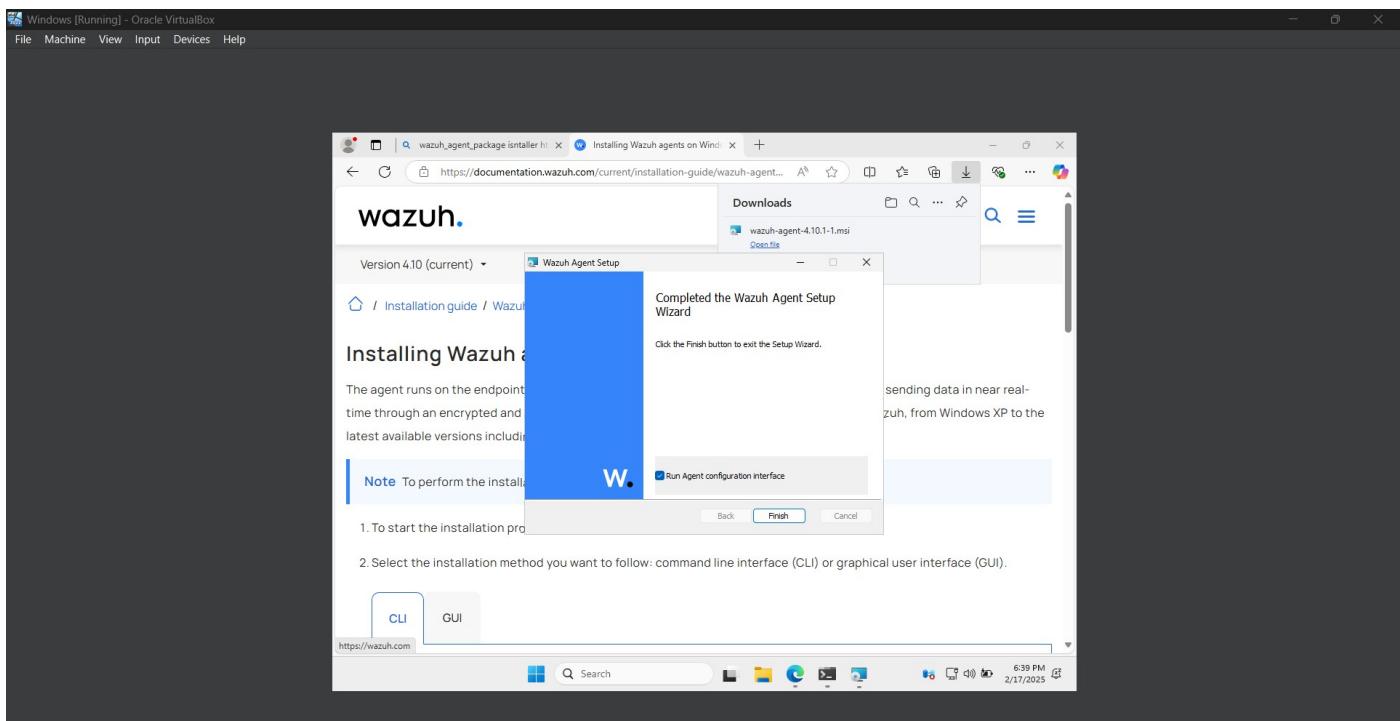
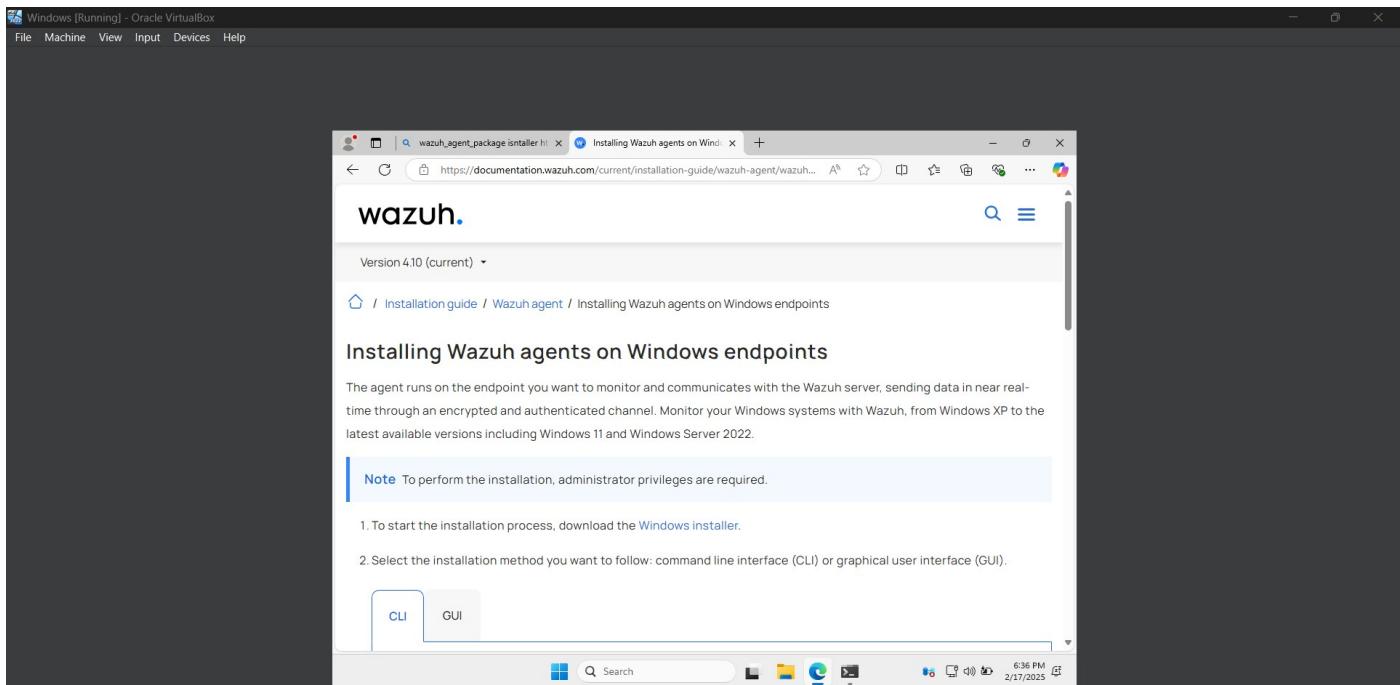
*****
* Wazuh v3.13.1 Agent manager *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(D)elete an agent (D).
(Q)uit.

Choose your action: A,E,L,D or Q: e
Available agents:
  1: ID: 001, Name: securingonionv2, IP: 192.168.10.46
  2: ID: 002, Name: ubuntu, IP: 192.168.10.26
Provide the ID of the agent to extract the key (or 'nq' to quit): 002

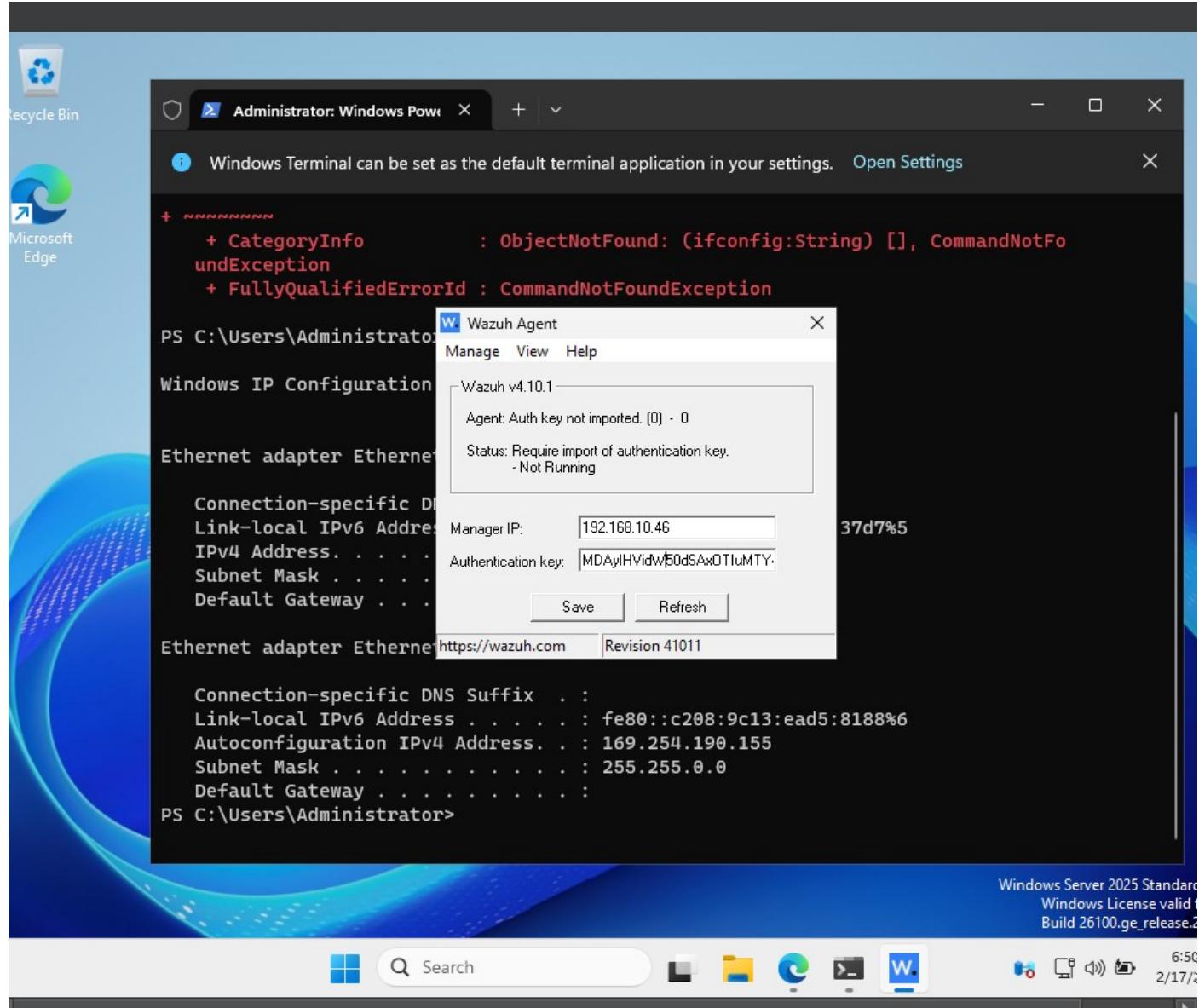
Agent key information for '002' is:
MduyIHOid4W8dSx6dTluTY4LJewLj1Z1DQ5OUY4YJUmYWJ1YjY5YMFmMj0zODA3NDc4YzFmZGQyM210
0WJhODAjM2Y1D3iWwz110GQJhmfPMGmZYTk=
** Press ENTER to return to the main menu.
```

Installing the Wazuh Agent on the Endpoint

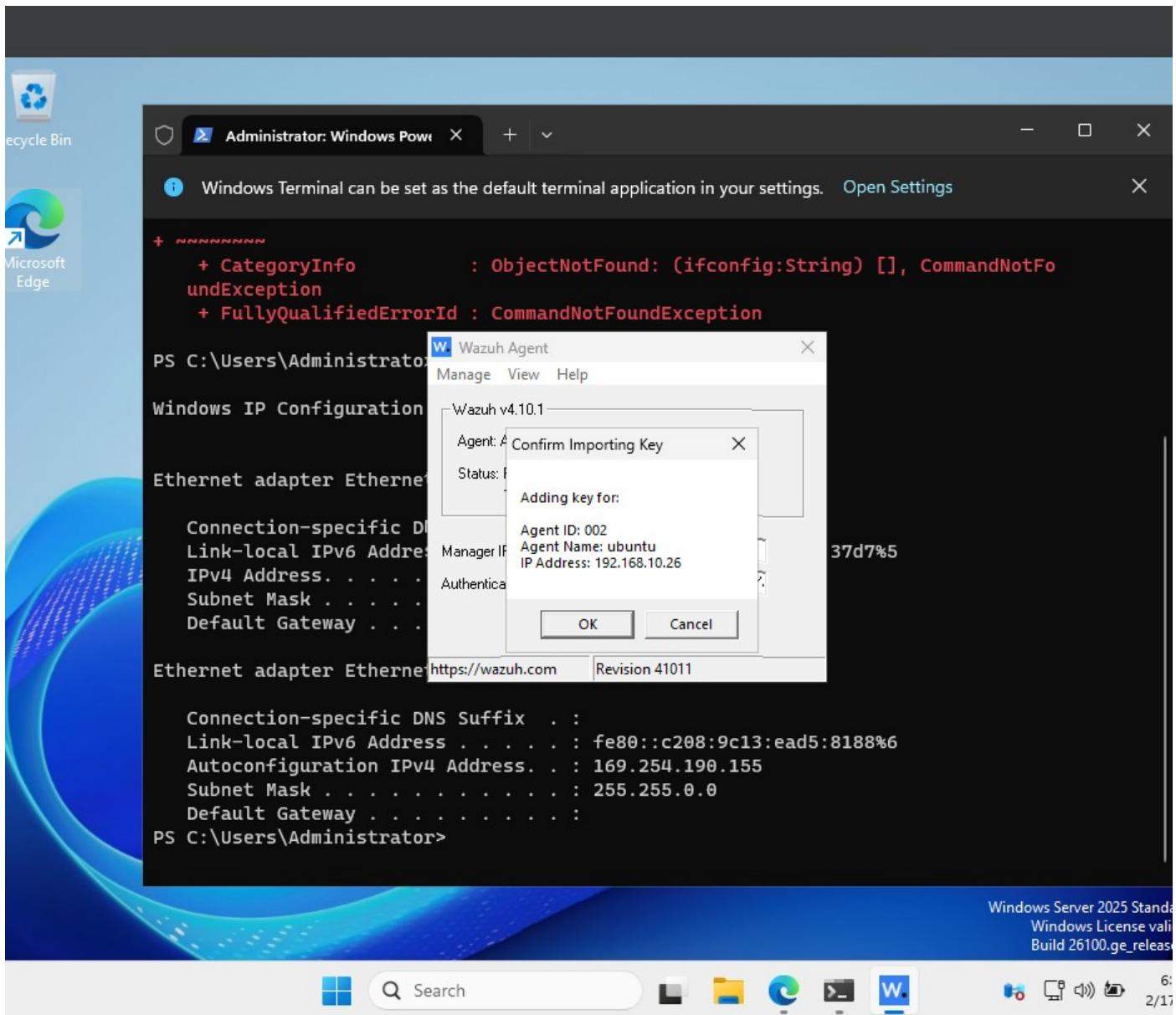
I downloaded the Wazuh agent installer for Windows from <https://documentation.wazuh.com/>



I copied the installer to the endpoint (HMI-1) and followed the instructions to install the agent. After installation, I ran the agent configuration interface, entered the Security Onion server's IP address (192.168.10.46), and pasted the agent key.



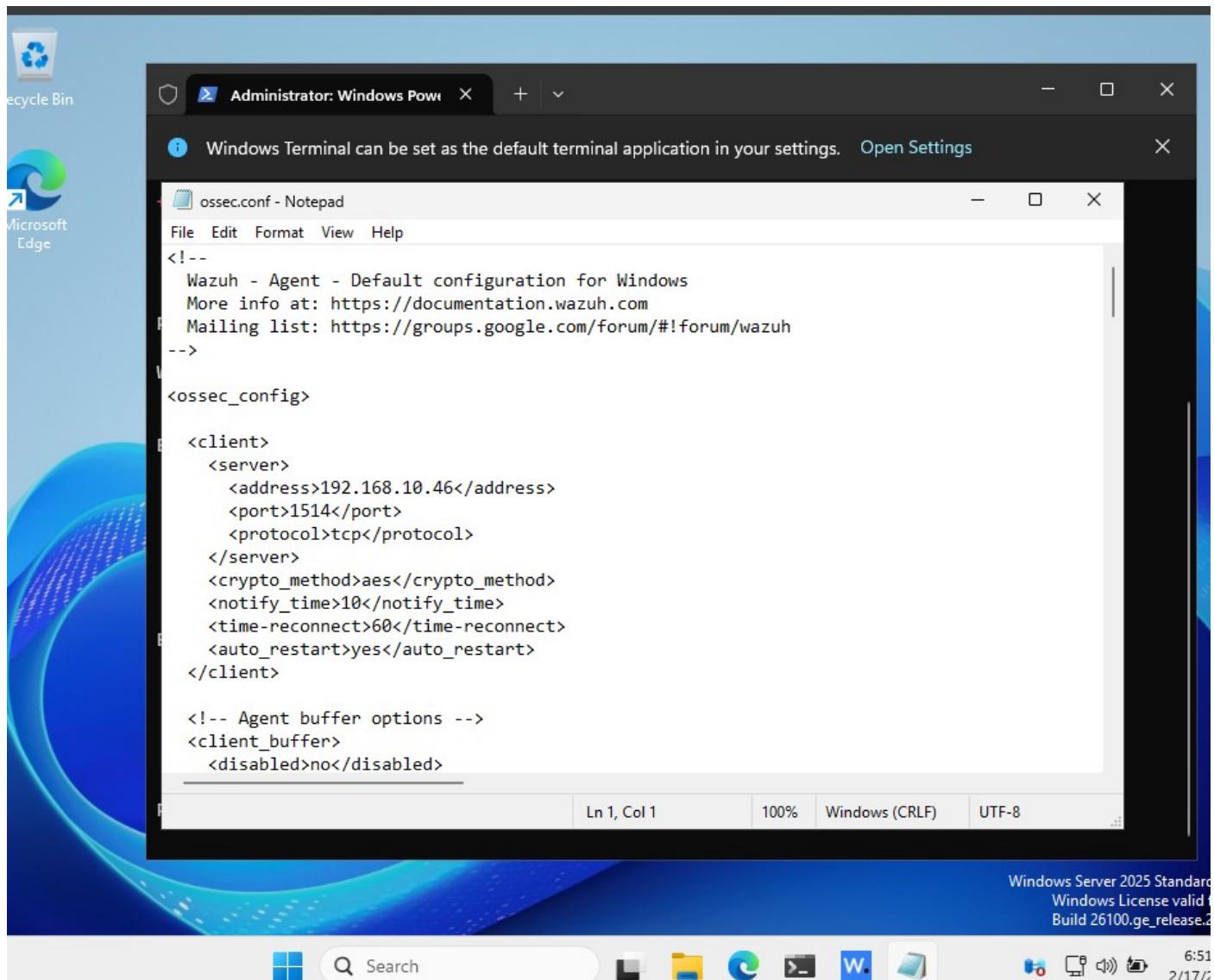
I confirmed that the agent was correctly registered and displayed the correct hostname and IP address.



Opened ossec.conf file and added the following configuration into the file

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
  <location>Microsoft-Windows-PowerShell/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
  <location>PowerShellCore/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

Saved the file and restarted the wazuh agent with new configuration



```
<localfile>
    <location>System</location>
    <log_format>eventchannel</log_format>
</localfile>

<localfile>
    <location>active-response\active-responses.log</location>
    <log_format>syslog</log_format>
</localfile>

<localfile>
    <location>Microsoft-Windows-Sysmon/Operational</location>
    <log_format>eventchannel</log_format>
</localfile>

<localfile>
    <location>Microsoft-Windows-PowerShell/Operational</location>
    <log_format>eventchannel</log_format>
</localfile>

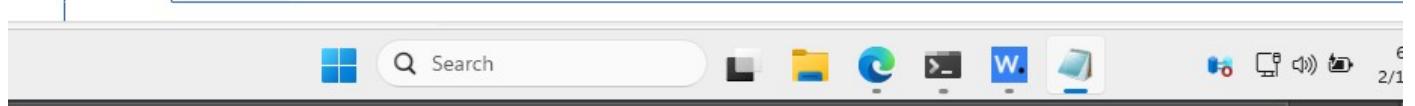
<!-- Policy monitoring --&gt;
&lt;rootcheck&gt;
    &lt;disabled&gt;no&lt;/disabled&gt;</pre>
```

1. To start the installation process, download the [Windows installer](#).

2. Select the installation method you want to follow: command line interface (CLI) or graphical user interface (GUI).

CLI

GUI



There were no errors occurred in the log file.

Windows [Running] - Oracle VirtualBox

File Machine View Input Devices Help

osses-log - Notepad

File Edit Format View Help

```
2025/02/17 18:57:47 wazuh-agent: INFO: (6003): Monitoring path: 'c:\windows\system32\windowspowershell\v1.0\' with options 's
2025/02/17 18:57:47 wazuh-agent: INFO: (6006): Ignore 'file' entry 'c:\programdata\microsoft\window\start menu\programs\star
2025/02/17 18:57:47 wazuh-agent: INFO: (6205): Ignore 'file' sregex '^log$|.htaccess$|.php$|.png$|.chm$|.pdf$|.evtx$'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\Security\Policy\Secrets'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\Security\SAM\Domains\Account\Users
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6207): Ignore 'registry' sregex '^Enum$'
2025/02/17 18:57:47 wazuh-agent: INFO: Started (pid=2948).
2025/02/17 18:57:47 wazuh-agent: INFO: Using AES as encryption method.
2025/02/17 18:57:47 wazuh-agent: INFO: Trying to connect to server ([192.168.10.46]:1514/tcp).
2025/02/17 18:57:47 wazuh-agent: INFO: Module started.
2025/02/17 18:57:47 wazuh-moduled-agent-upgrade: INFO: (153): Module Agent Upgrade started.
2025/02/17 18:57:47 wazuh-moduled-agent-upgrade: INFO: (153): Module disabled. Exiting.
2025/02/17 18:57:47 wazuh-agent: INFO: Windows version is 6.0 (Windows Server 2022) (Microsoft Windows Server 2025 Standard Evaluation [V
2025/02/17 18:57:47 wazuh-agent: INFO: (x86)\ossec-agent\ruleset\sca\cis_w2022.yml'
2025/02/17 18:57:47 wazuh-agent: INFO: Loaded policy 'C:\Program Files (x86)\ossec-agent\ruleset\sca\cis_w2022.yml'
2025/02/17 18:57:47 wazuh-agent: INFO: Starting Security Configuration Assessment scan.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Application'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Security'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'System'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1950): Analyzing event log: 'active-response/active-responses.log'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Microsoft-Windows-Sysmon/Operational'.
2025/02/17 18:57:47 wazuh-agent: ERROR: Could not EventSubscribe() for 'Microsoft-Windows-Sysmon/Operational' which returned (1
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Microsoft-Windows-PowerShell/Operational'.
2025/02/17 18:57:47 wazuh-agent: INFO: (6000): Starting daemon...
2025/02/17 18:57:47 wazuh-agent: INFO: (6010): File integrity monitoring scan frequency: 43200 seconds
2025/02/17 18:57:47 wazuh-agent: INFO: (6000): File integrity monitoring scan started.
2025/02/17 18:57:47 sca: INFO: Skipping policy 'C:\Program Files (x86)\ossec-agent\ruleset\sca\cis_w2022.yml': 'Check that
```

Ln 27, Col 105 100% Unix (LF) UTF-8

Search 7:11 PM 2/17/2025

Windows (Running) - Oracle VirtualBox

File Machine View Input Devices Help

ossec.log - Notepad

```
File Edit Format View Help
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services'
2025/02/17 18:57:47 wazuh-agent: INFO: (6206): Ignore 'registry' sregex '\Enum$'
2025/02/17 18:57:47 wazuh-agent: INFO: Started (pid: 2948).
2025/02/17 18:57:47 wazuh-agent: INFO: Using AES as encryption method.
2025/02/17 18:57:47 wazuh-agent: INFO: Trying to connect to server ([192.168.10.46]:1514/tcp).
2025/02/17 18:57:47 sca: INFO: Module started.
2025/02/17 18:57:47 wazuh-modules:agent: INFO: (8153): Module Agent Upgrade started.
2025/02/17 18:57:47 wazuh-modules:agent: INFO: Module disabled. Exiting.
2025/02/17 18:57:47 wazuh-agent: INFO: Windows version is 6.0 or newer. (Microsoft Windows Server 2025 Standard Evaluation [V
2025/02/17 18:57:47 sca: INFO: Loaded policy 'C:\Program Files (x86)\ossec-agent\ruleset\sca\cis_win2022.yml'
2025/02/17 18:57:47 sca: INFO: Starting Security Configuration Assessment scan.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Application'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Security'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'System'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1950): Analyzing file: 'active-response/active-responses.log'.
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Microsoft-Windows-Sysmon/Operational'.
2025/02/17 18:57:47 wazuh-agent: ERROR: Could not EvtSubscribe() for (Microsoft-Windows-Sysmon/Operational) which returned (1
2025/02/17 18:57:47 wazuh-agent: INFO: (1951): Analyzing event log: 'Microsoft-Windows-PowerShell/Operational'.
2025/02/17 18:57:47 wazuh-agent: INFO: (6000): Starting daemon...
2025/02/17 18:57:47 wazuh-agent: INFO: (6010): File integrity monitoring scan frequency: 43200 seconds
2025/02/17 18:57:47 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2025/02/17 18:57:47 sca: INFO: Skipping policy 'C:\Program Files (x86)\ossec-agent\ruleset\sca\cis_win2022.yml': 'Check that
2025/02/17 18:57:47 wazuh-modules:osquery: INFO: Module disabled. Exiting...
2025/02/17 18:57:47 wazuh-modules:syscollector: INFO: Module started.
2025/02/17 18:57:47 wazuh-modules:syscollector: INFO: Starting evaluation.
2025/02/17 18:57:48 wazuh-agent: INFO: Started (pid: 2948).
2025/02/17 18:57:48 wazuh-modules:syscollector: INFO: Evaluation finished.
```

Ln 27, Col 105 100% Unix (LF) UTF-8

Search

7:15 PM 2/17/2025

