SECURITY ONION

GROUP-2
SRIRAM RAYALA

Lab 1: Setting up and Configuring Security Onion

Introduction

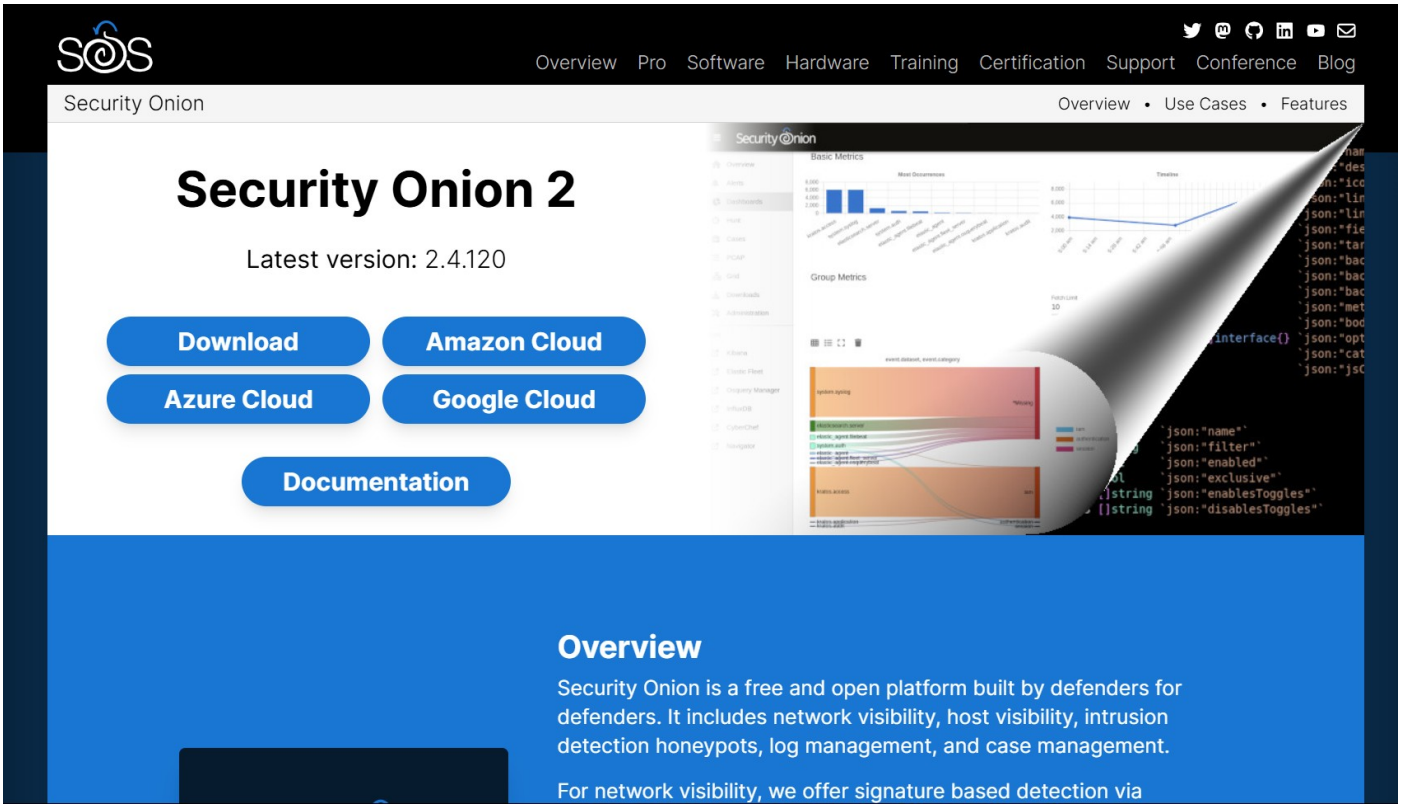
In this lab, I deployed and configured a Security Onion VM. This lab covered the following topics:

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:

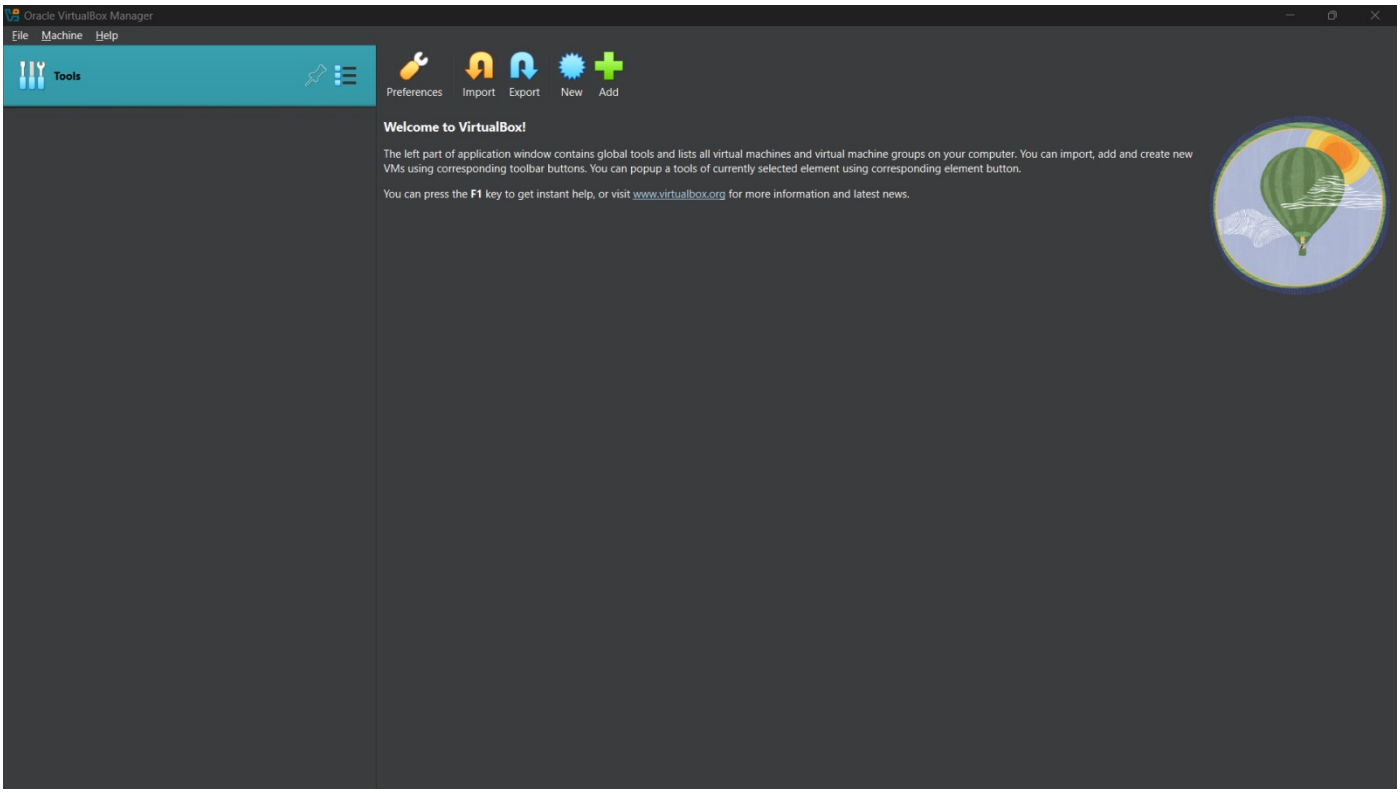
I downloaded the latest version of the Security Onion appliance from https://securityonionsolutions.com/software/.

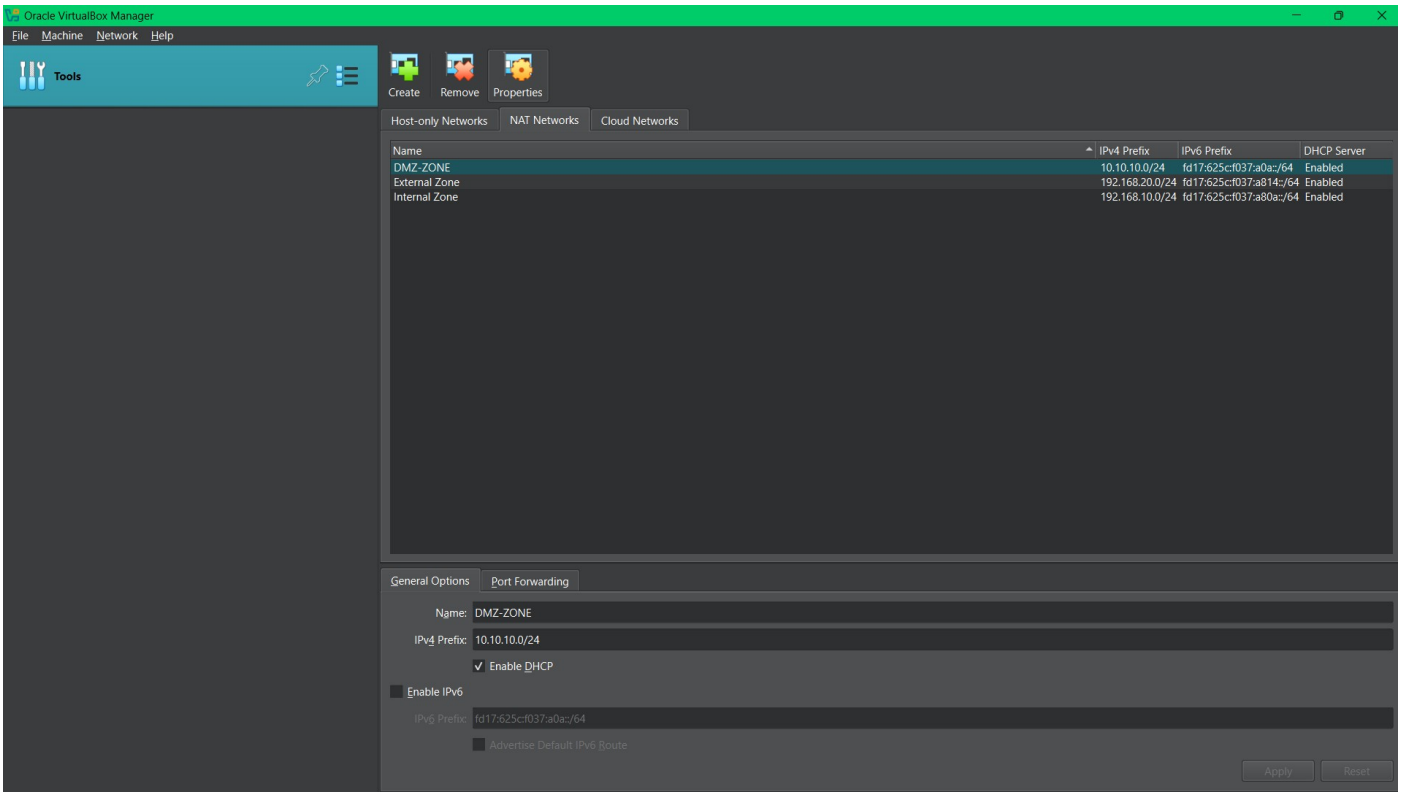


I have also downloaded VirtualBox and added 3 NAT networks to VirtualBox to be assigned to Virtual Machines. The 3 NAT networks include:

DMZ ZONE : 10.10.10.0/24
INTERNAL NETWORK : 192.168.10.0/24

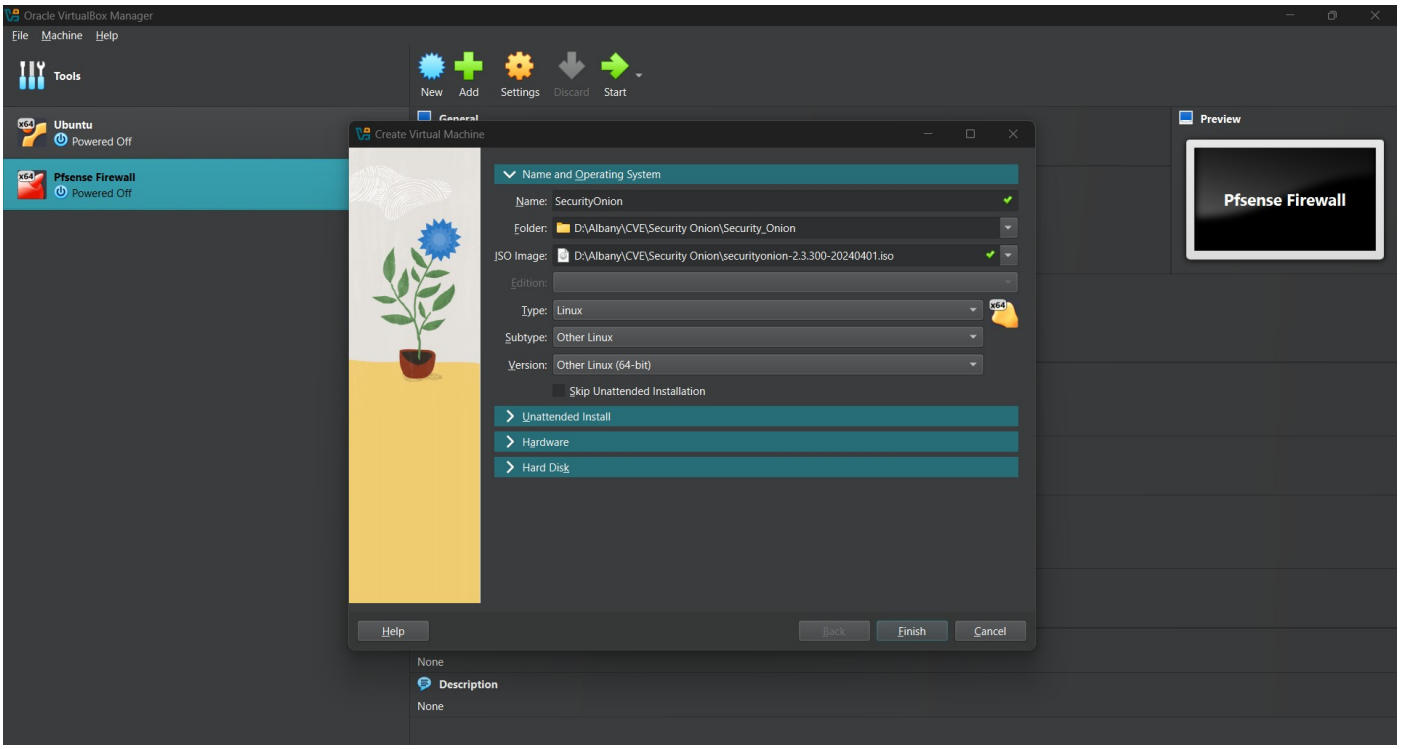
EXTERNAL ZONE: 192.168.20.0/24

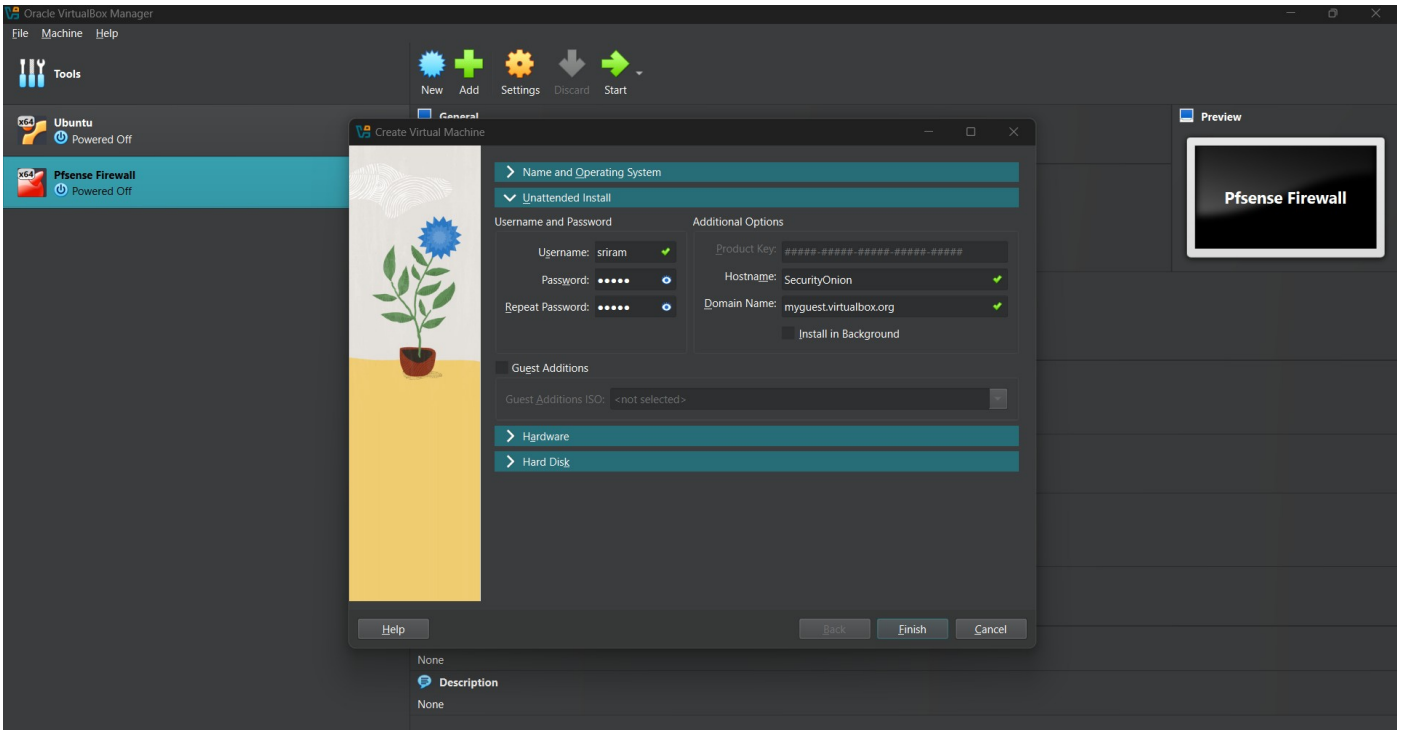


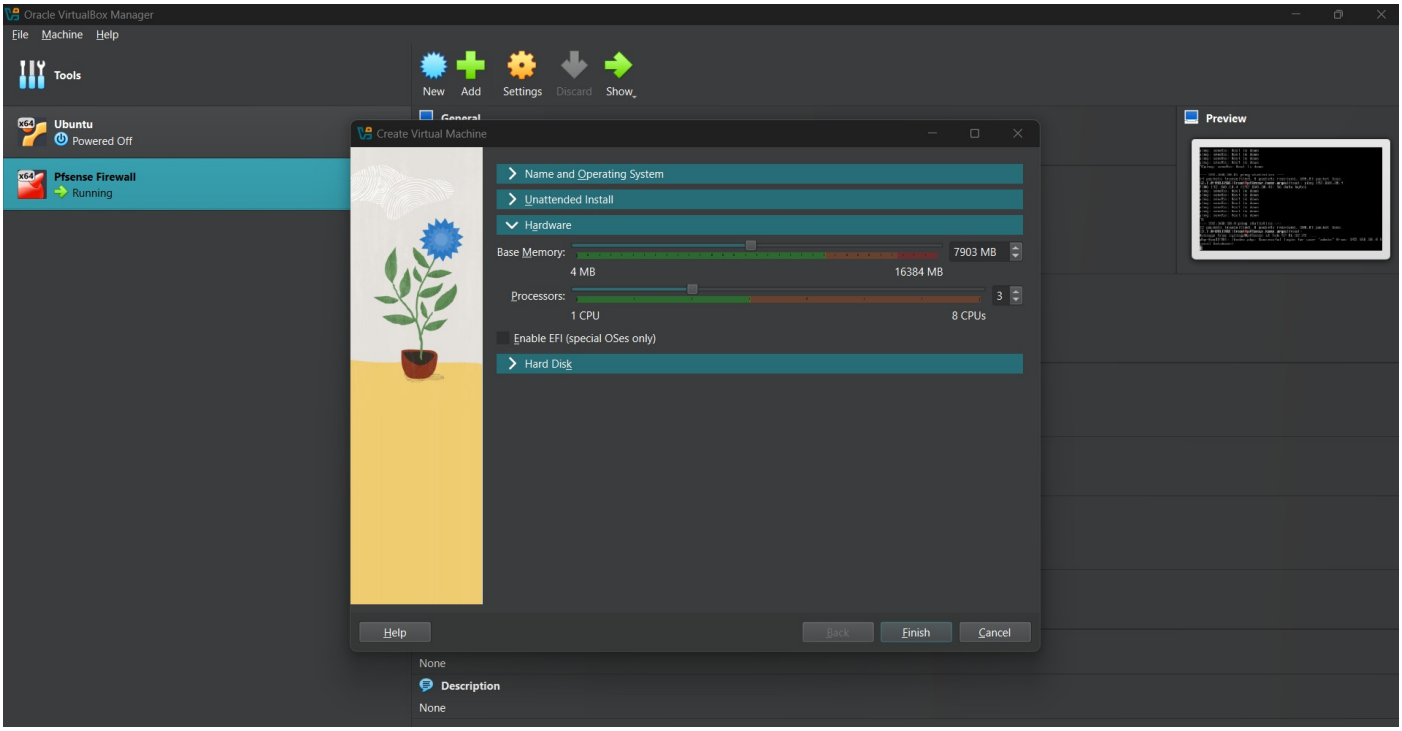


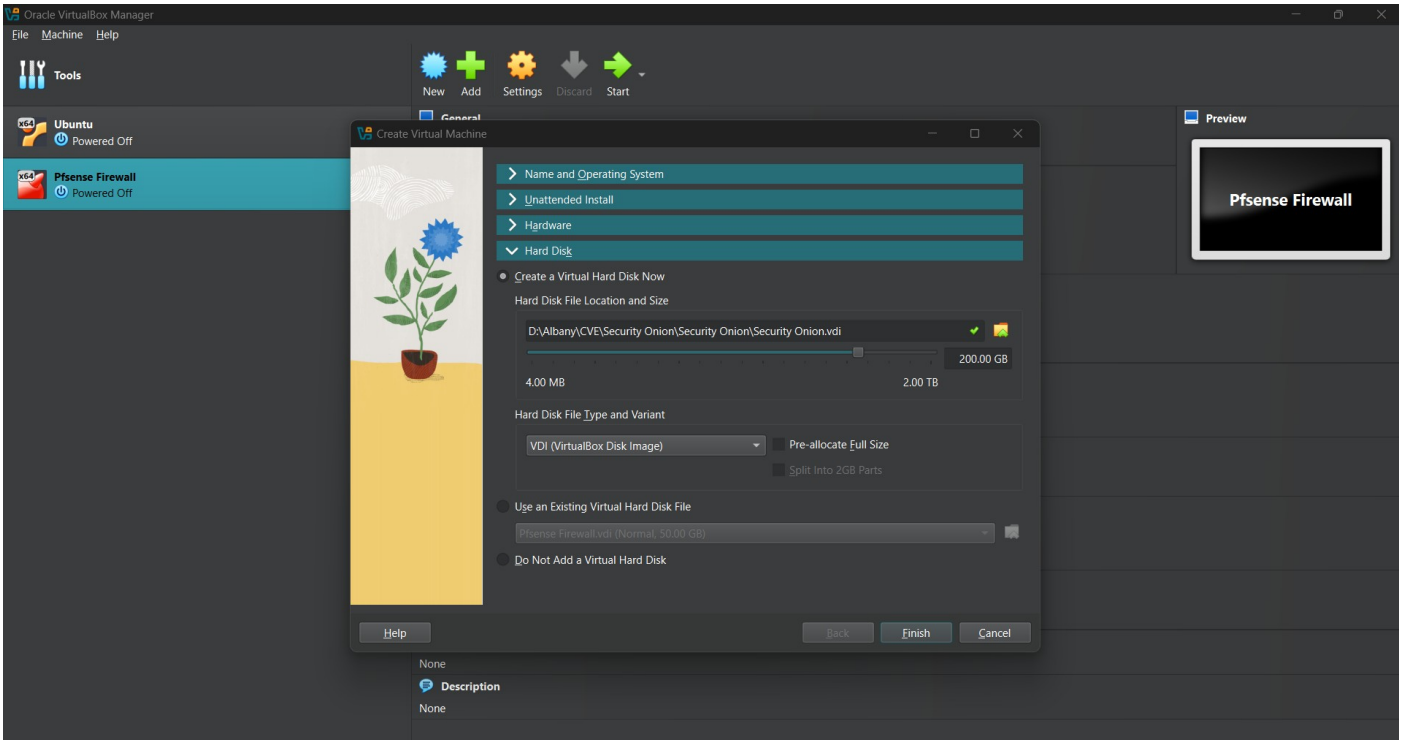
Now I opened Virtualbox and selected *File → New Virtual Machine*. I chose the *Typical* configuration option and clicked *Next*. I selected the *Installer disc* option on the next screen, clicked *Browse*, and found the ISO file for Security Onion I had just downloaded. I clicked *Open* and then *Next*. 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

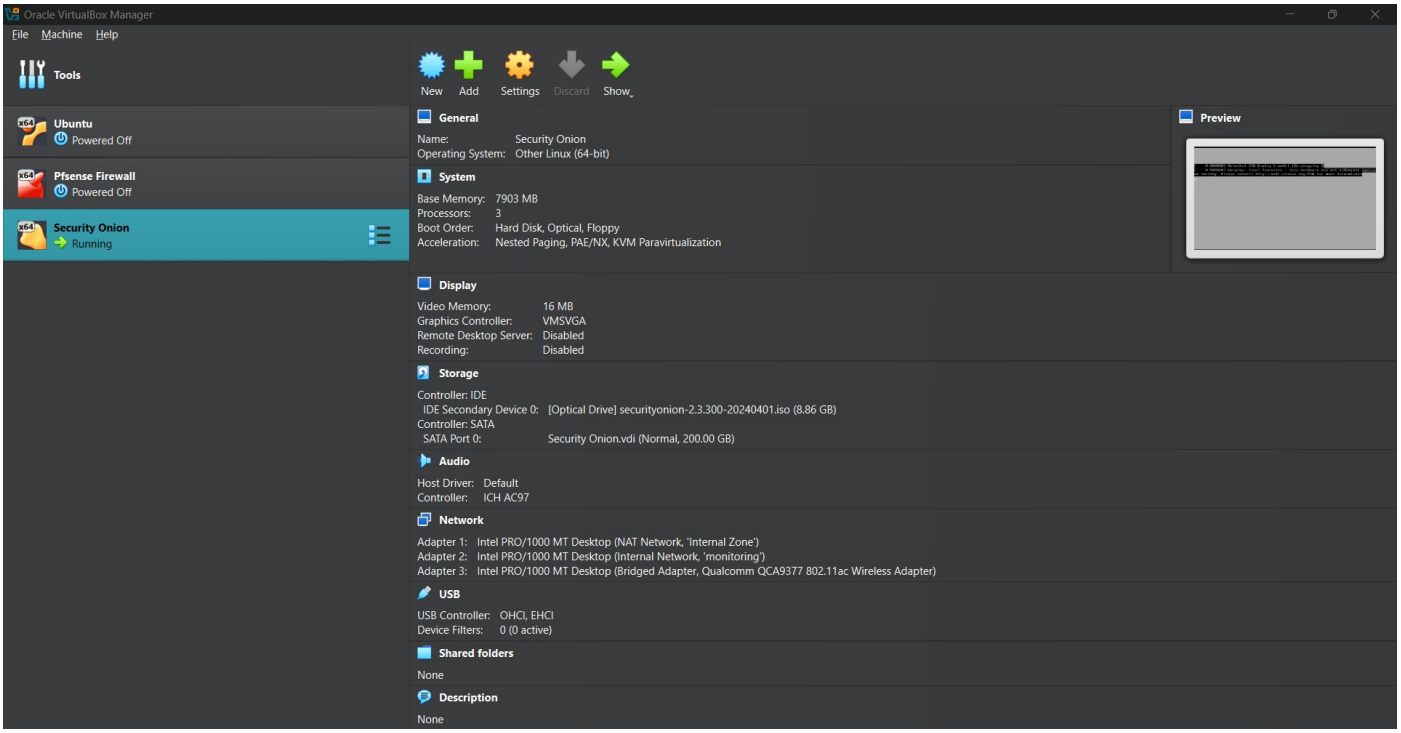
Customize Hardware on the summary screen and configured the hardware resources for the VM. I powered on the Security Onion VM and waited for it to boot into the installation screen.





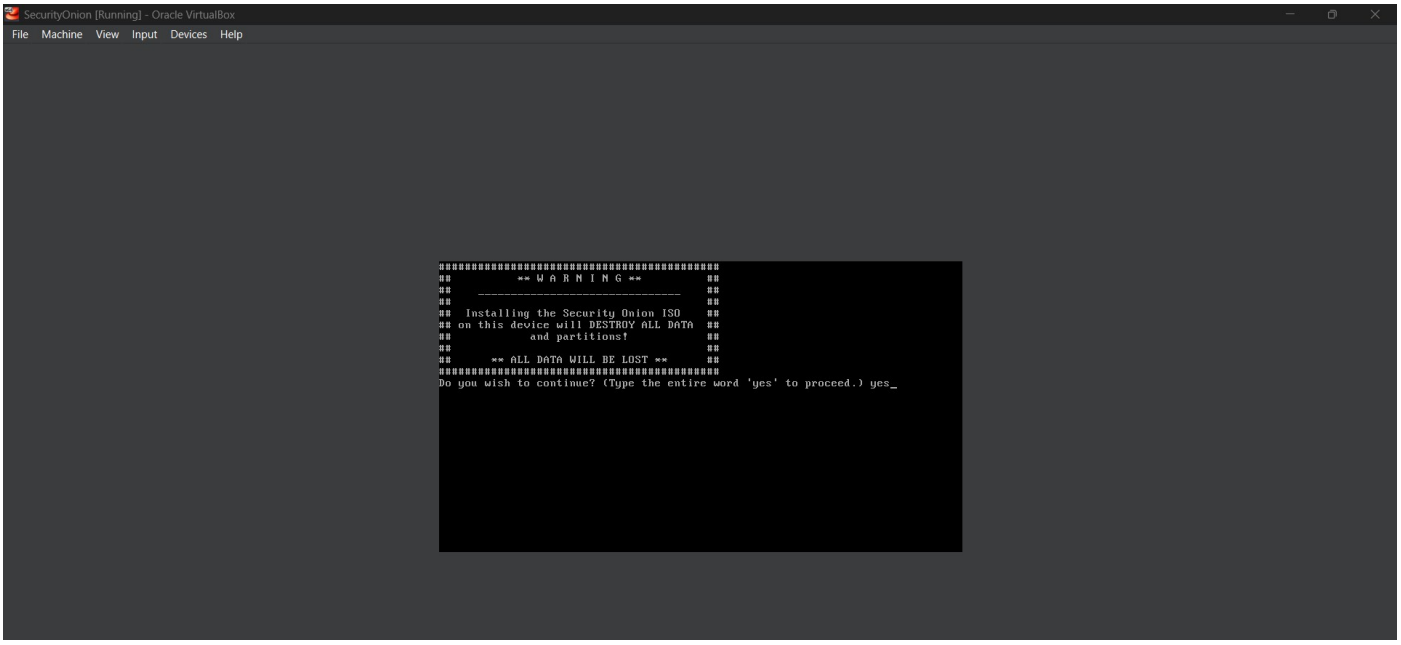

Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Show
Ubuntu
Powered Off
Pfsense Firewall
Running
Preview
Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Base Memory:
7903 MB
4 MB
16384 MB
Processors:
3
1 CPU
8 CPUs
Enable EFI (special OSes only)
Hard Disk
Help
Back
Finish
Cancel
None
Description
None


Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
Ubuntu
Powered Off
Pfsense Firewall
Powered Off
Preview
Pfsense Firewall
Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
D:\Albany\CVE\Security Onion\Security Onion\Security Onion.vdi
200.00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split Into 2GB Parts
Use an Existing Virtual Hard Disk File
Pfsense Firewall.vdi (Normal, 50.00 GB)
Do Not Add a Virtual Hard Disk
Help
Back
Finish
Cancel
None
Description
None

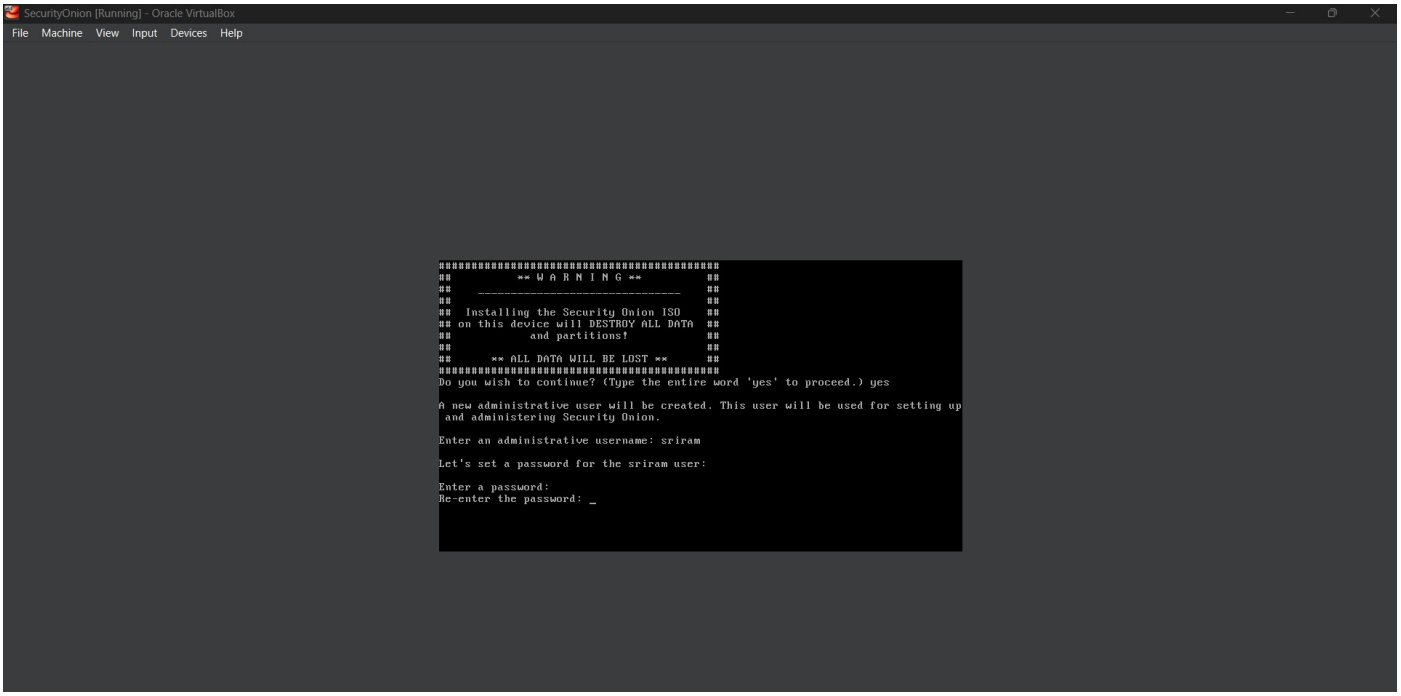


I highlighted *Install Security Onion 2.3.300 in basic graphics mode* and hit *Enter* to start the installation process.

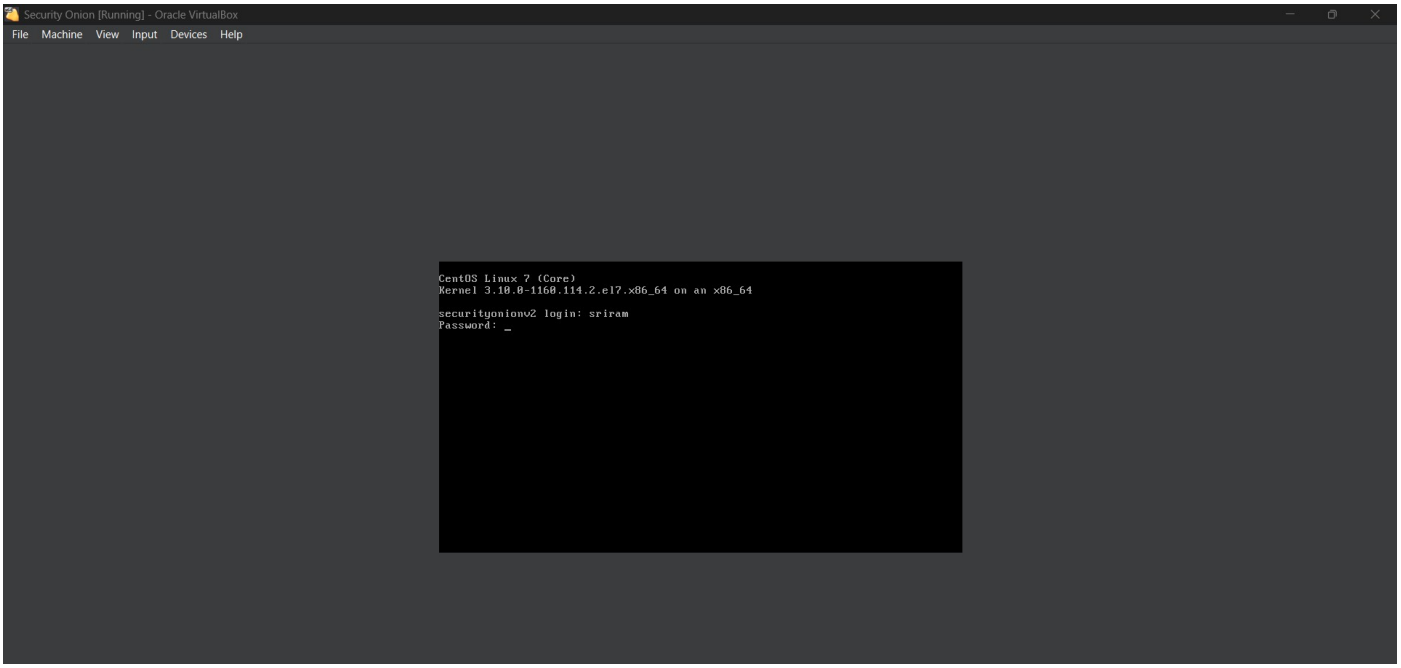
I typed *yes* to confirm that I wanted to wipe the hard drive and install the Security Onion operating system.



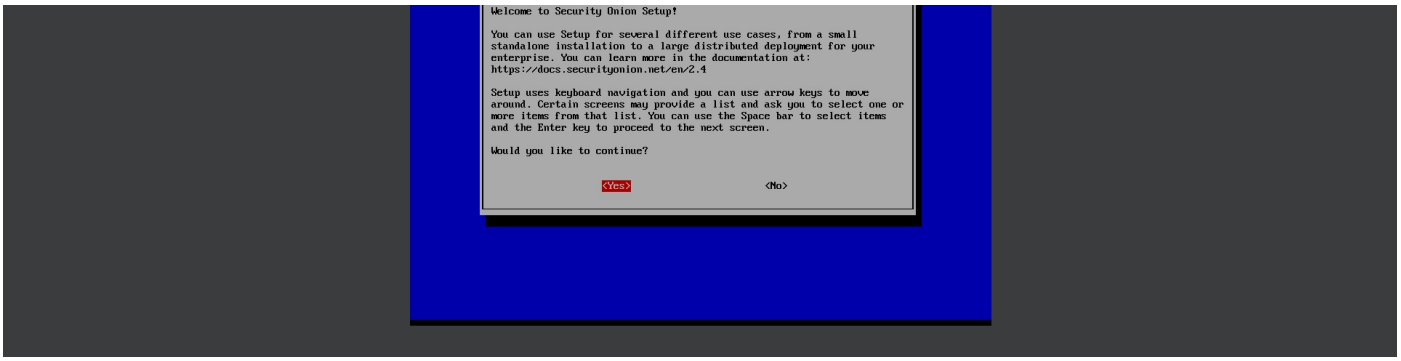
I set up the administrative username and password for the installation.

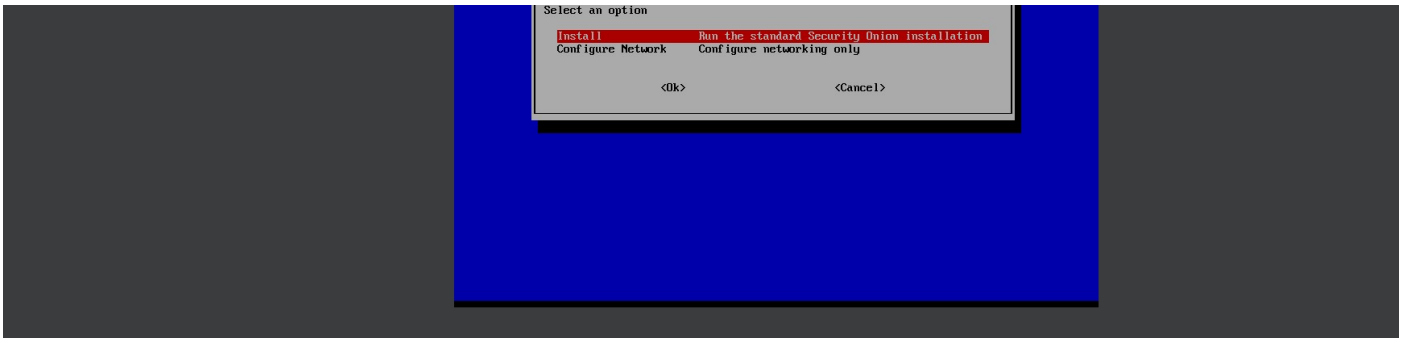


The installer formatted the hard drive and installed the Security Onion operating system. After the installation, I logged into the newly installed operating system with the credentials I had set up.

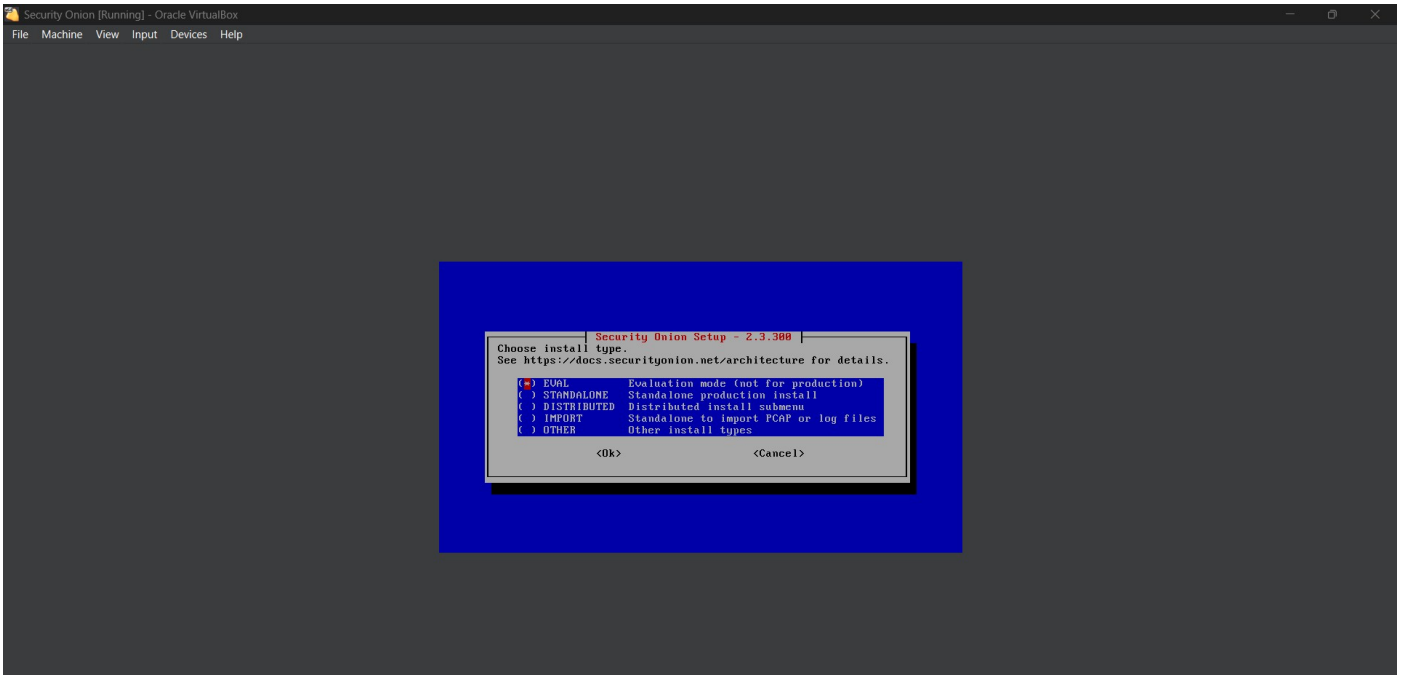


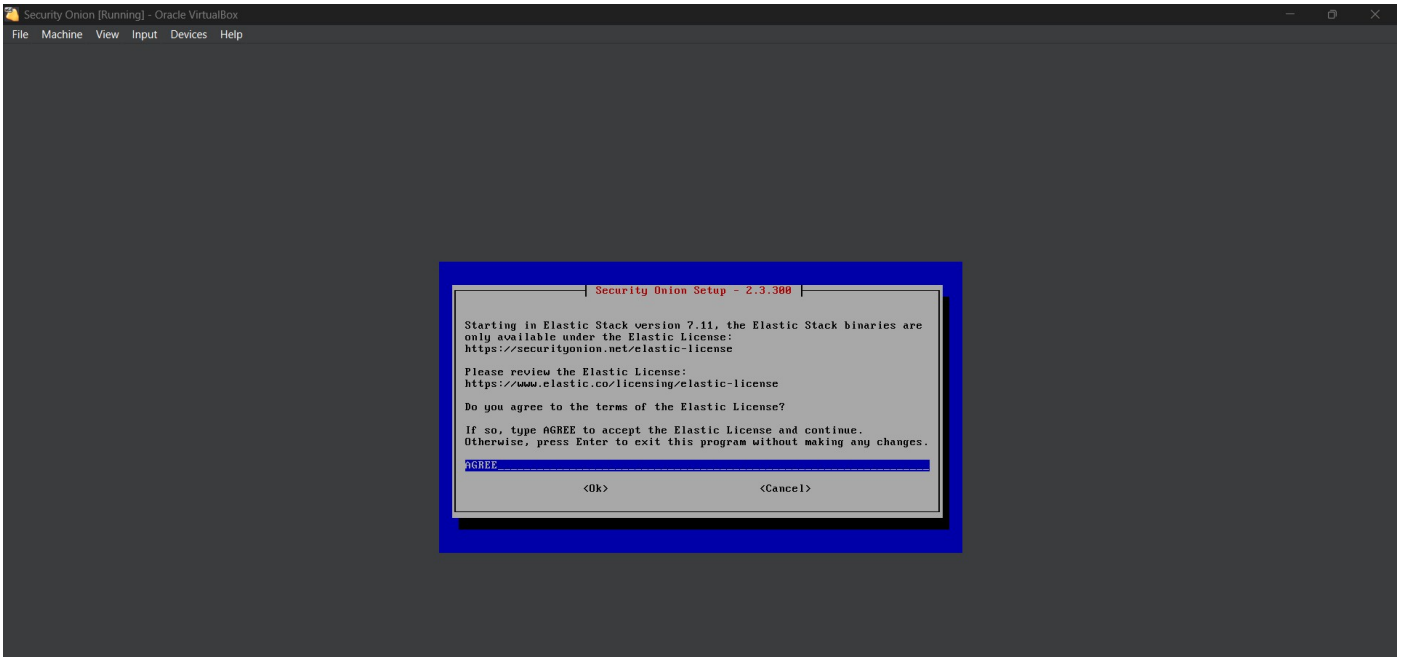
I confirmed that I wanted to continue with the setup.



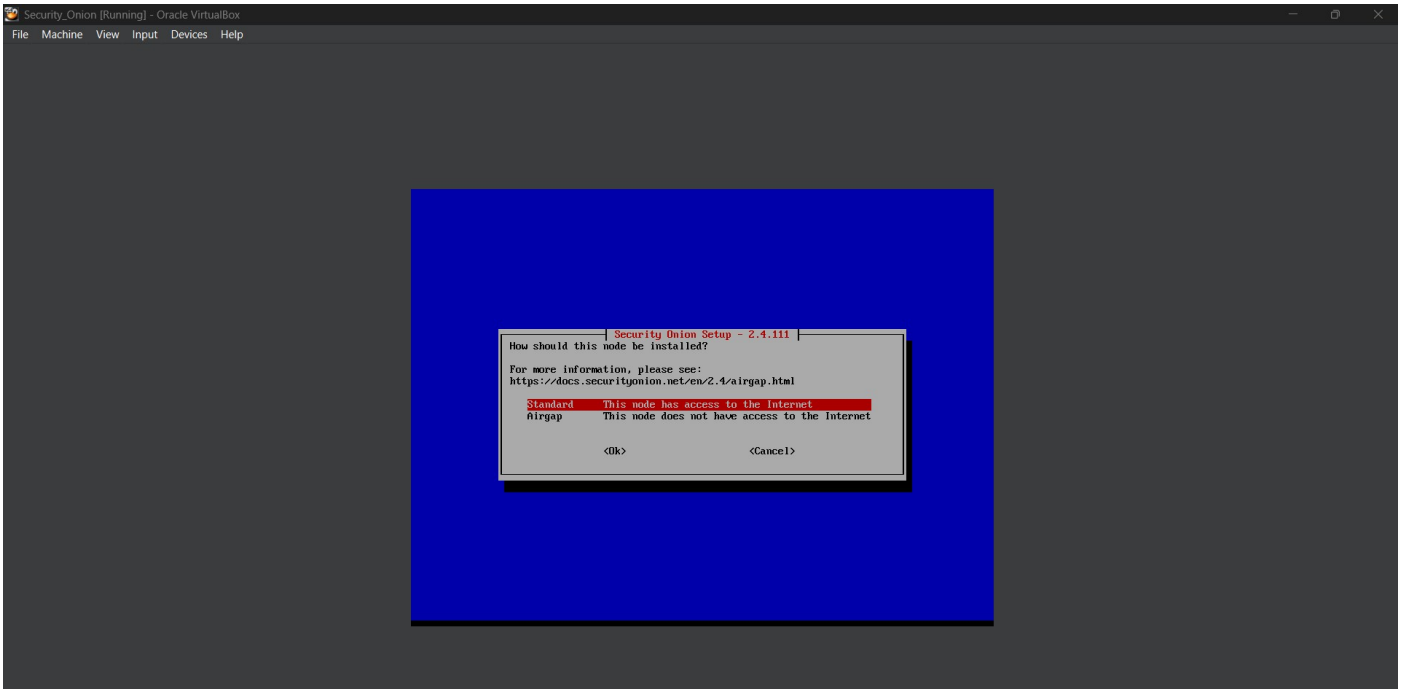


I chose the *EVAL* installation mode to evaluate all aspects of Security Onion.

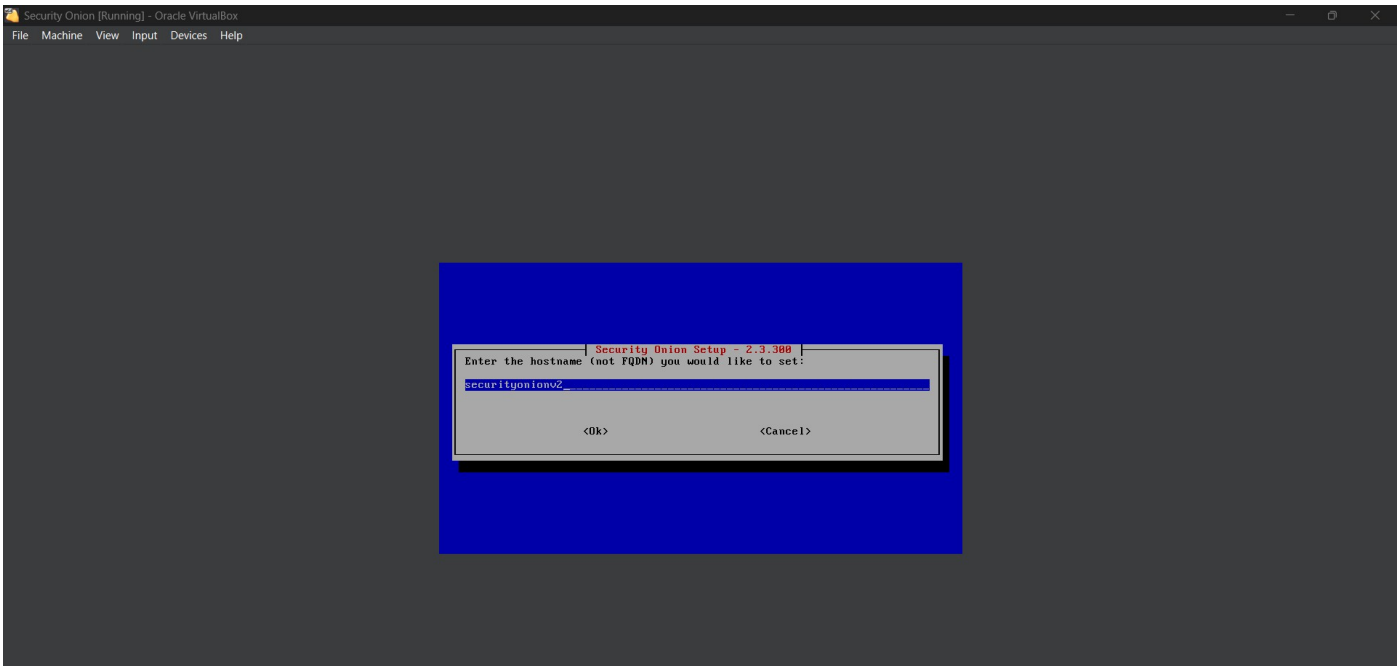




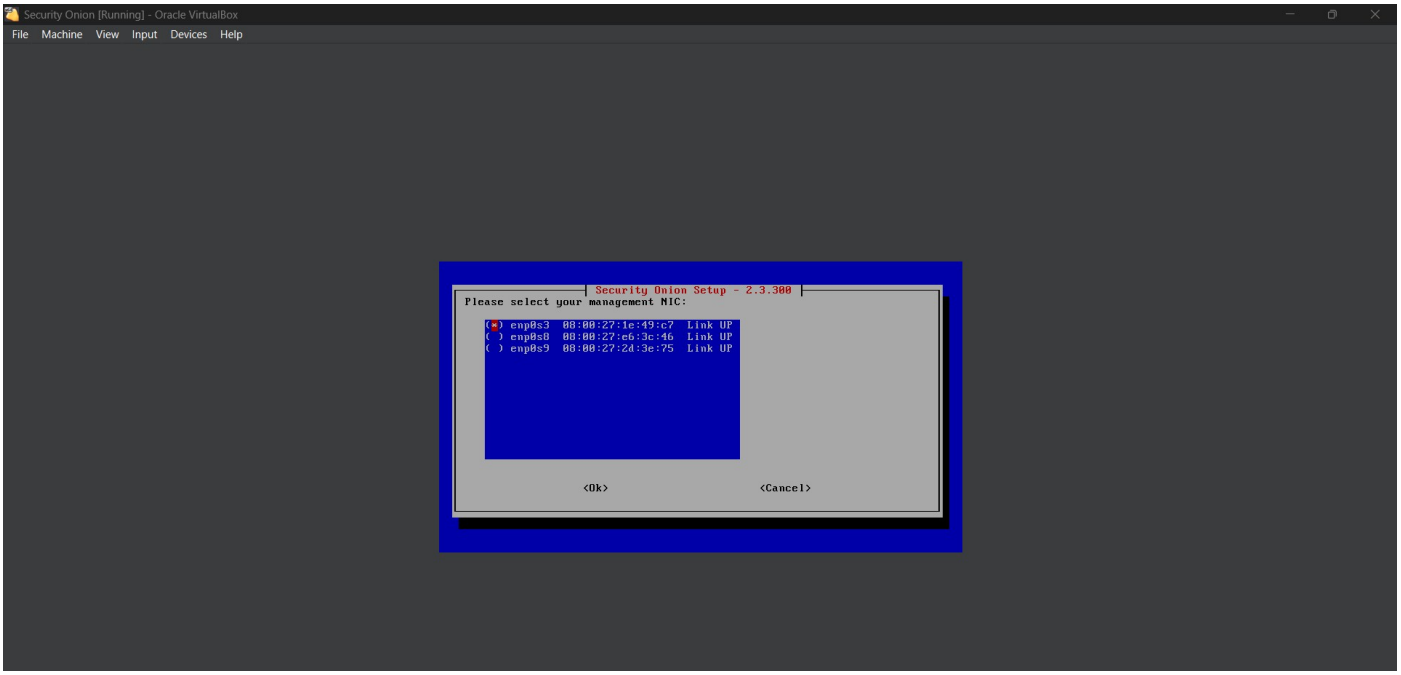
I selected the *STANDARD* install option to allow Security Onion to retrieve updates over the internet.



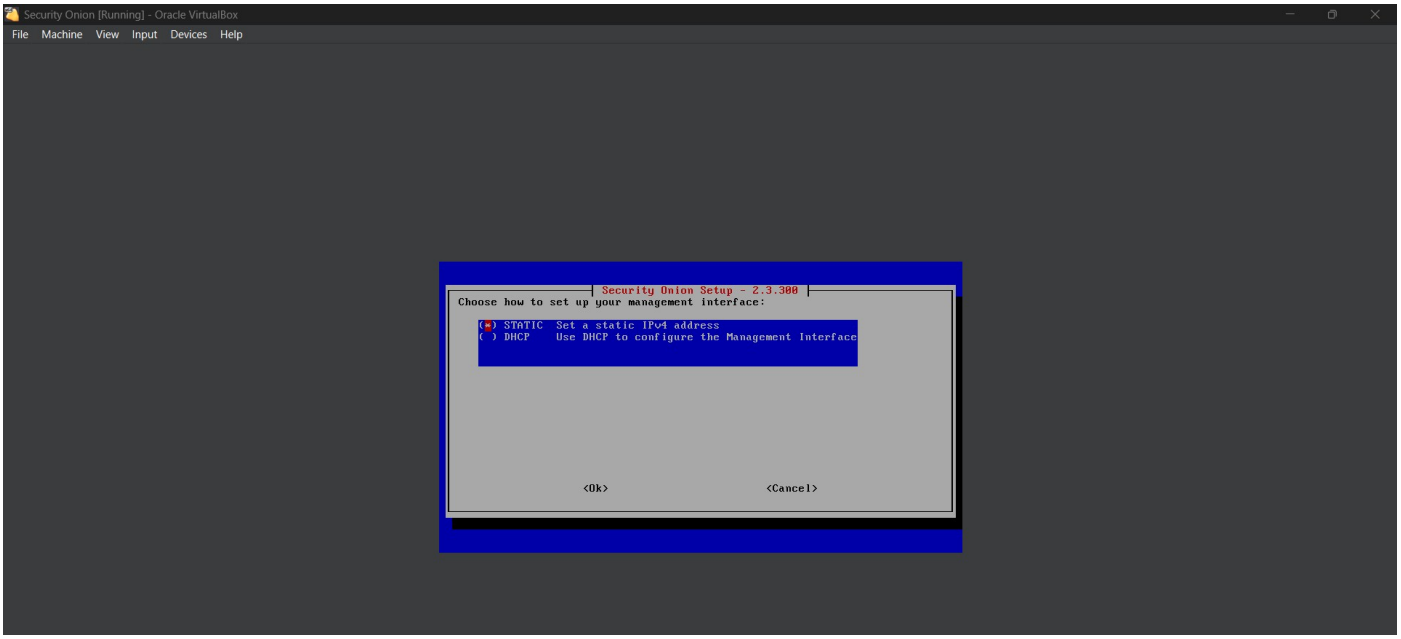
I named the Security Onion appliance s*ecurityonionv2*.

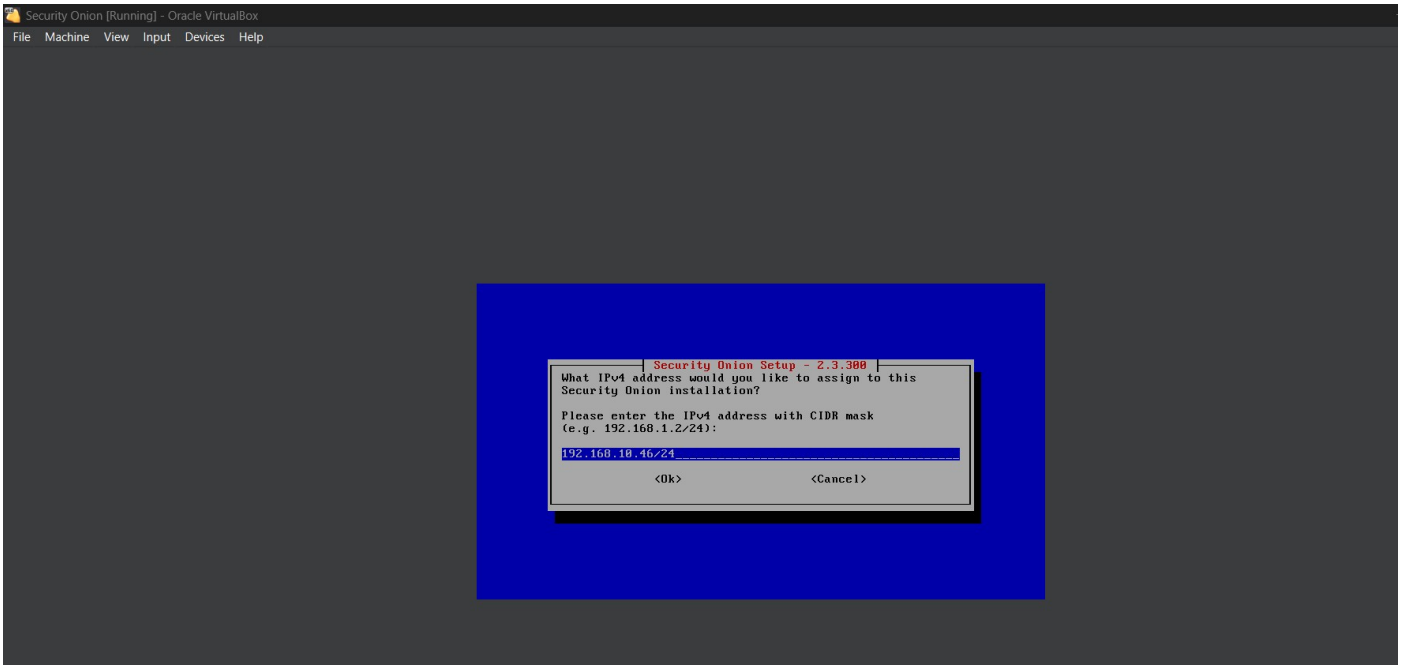


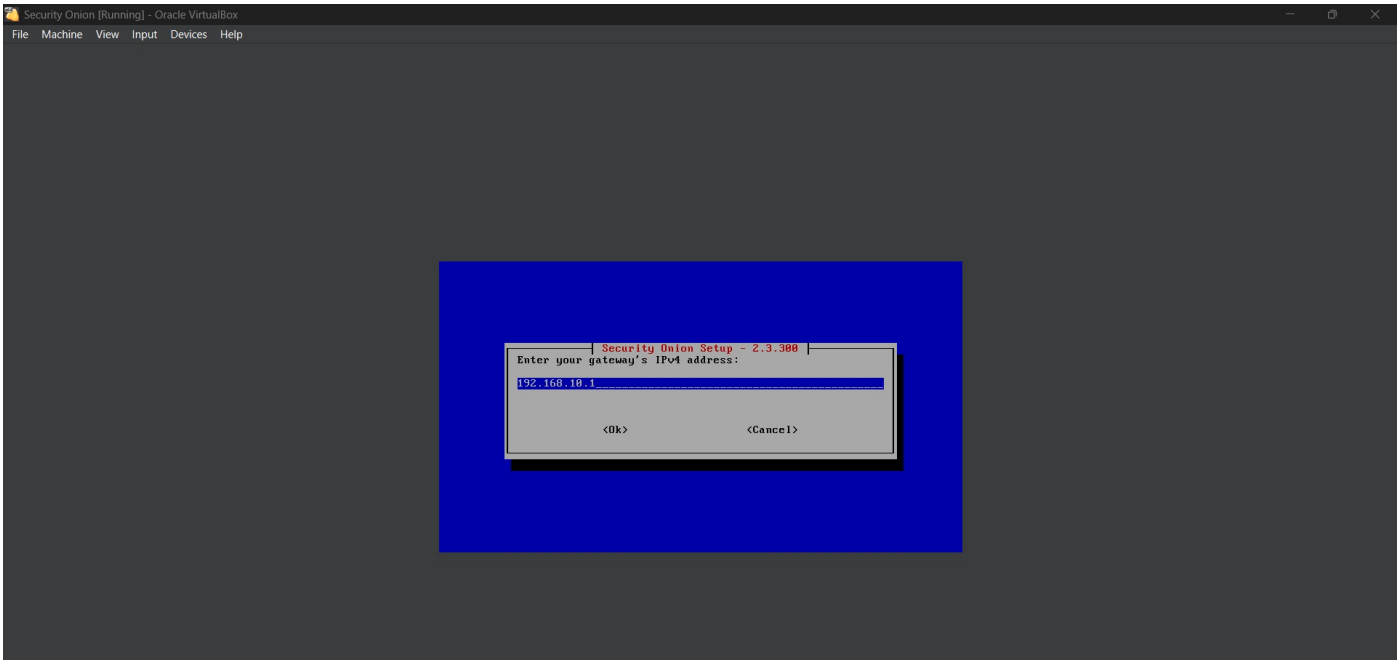
I selected the first interface enp0s3(NAT-Internal Network) for the management NIC.

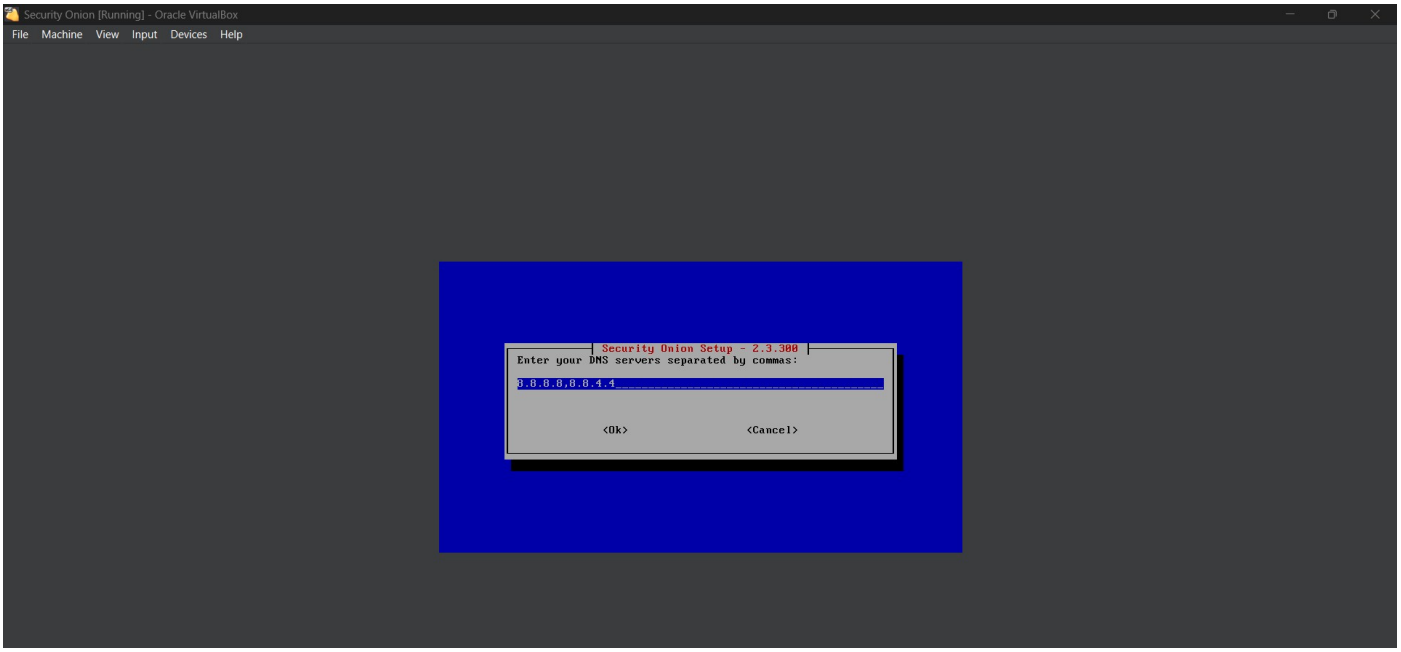


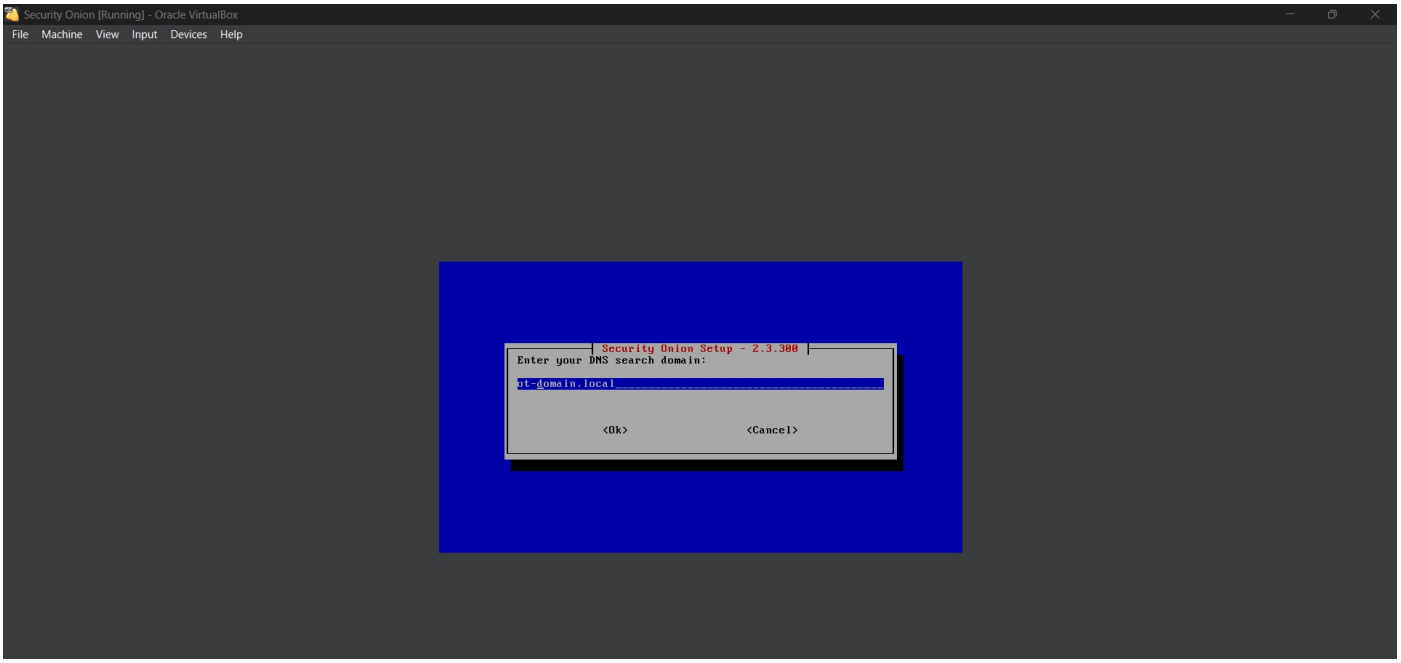
I configured the IP address details, including static IP, netmask, gateway, and DNS server.

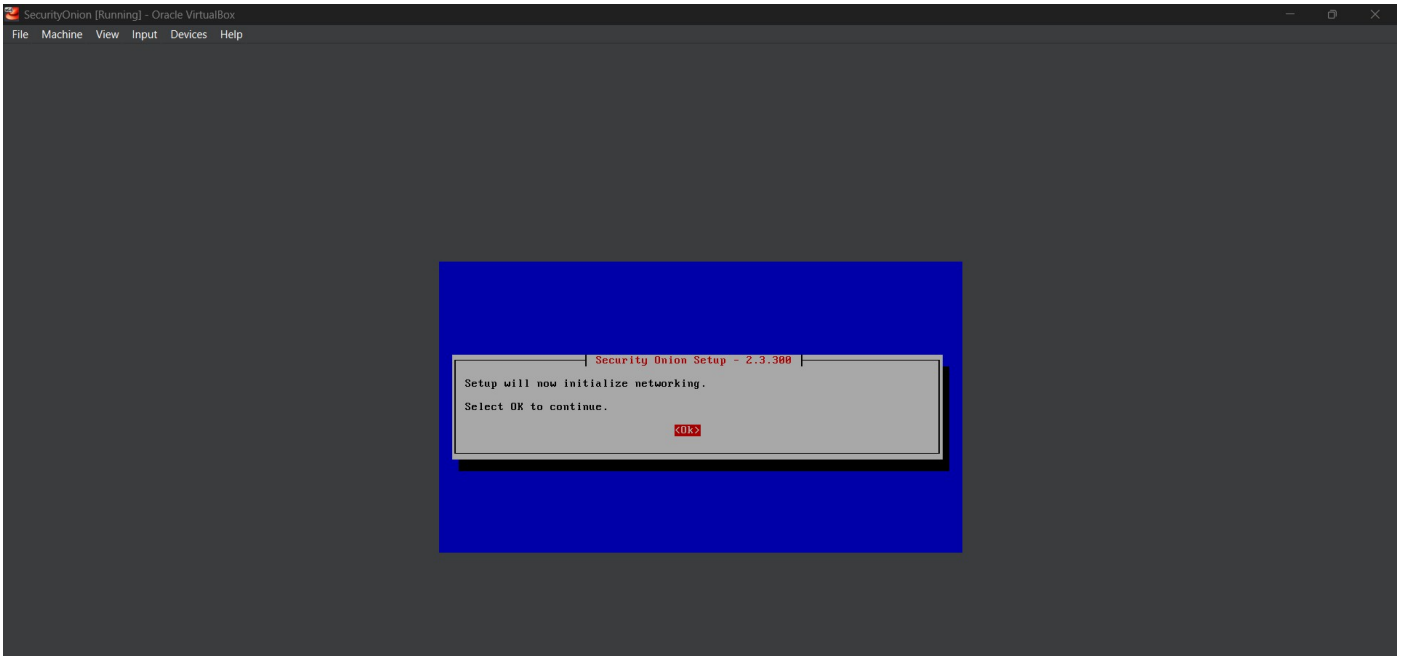



Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Security Onion Setup - 2.3.300
What IPv4 address would you like to assign to this
Security Onion installation?
Please enter the IPv4 address with CIDR mask
(e.g. 192.168.1.2/24):
192.168.10.46/24
<Ok>
<Cancel>

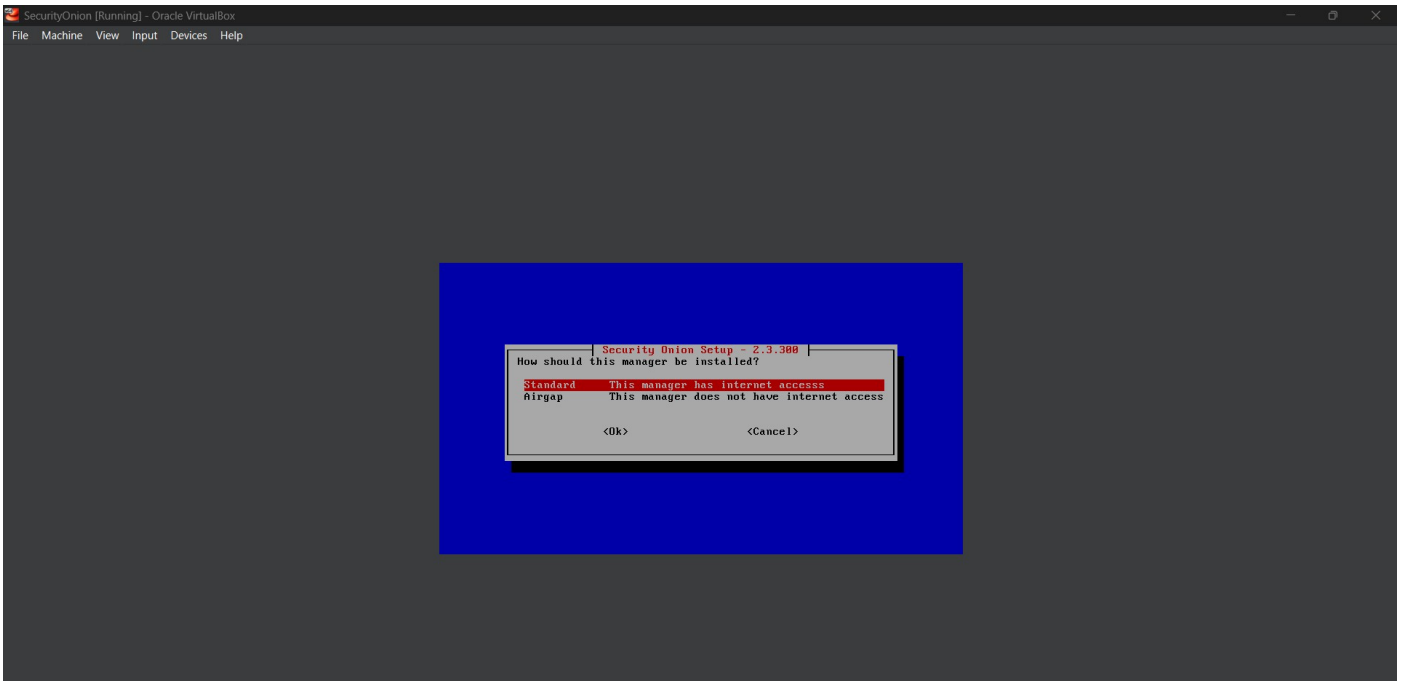

Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Security Onion Setup - 2.3.300
Enter your gateway's IPv4 address:
192.168.10.1
<Ok>
<Cancel>

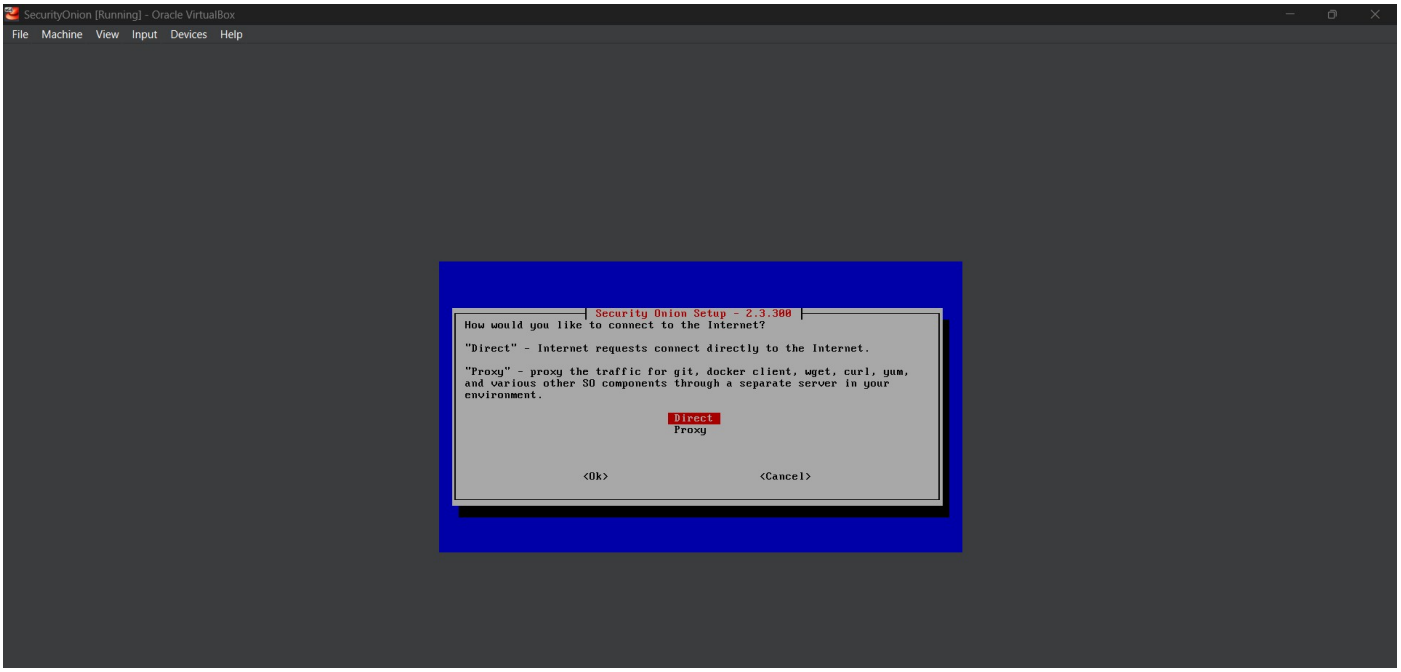

Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Security Onion Setup - 2.3.300
Enter your DNS servers separated by commas:
8.8.8.8,8.8.4.4
<Ok>
<Cancel>


Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Security Onion Setup - 2.3.300
Enter your DNS search domain:
ot-domain.local
<Ok>
<Cancel>

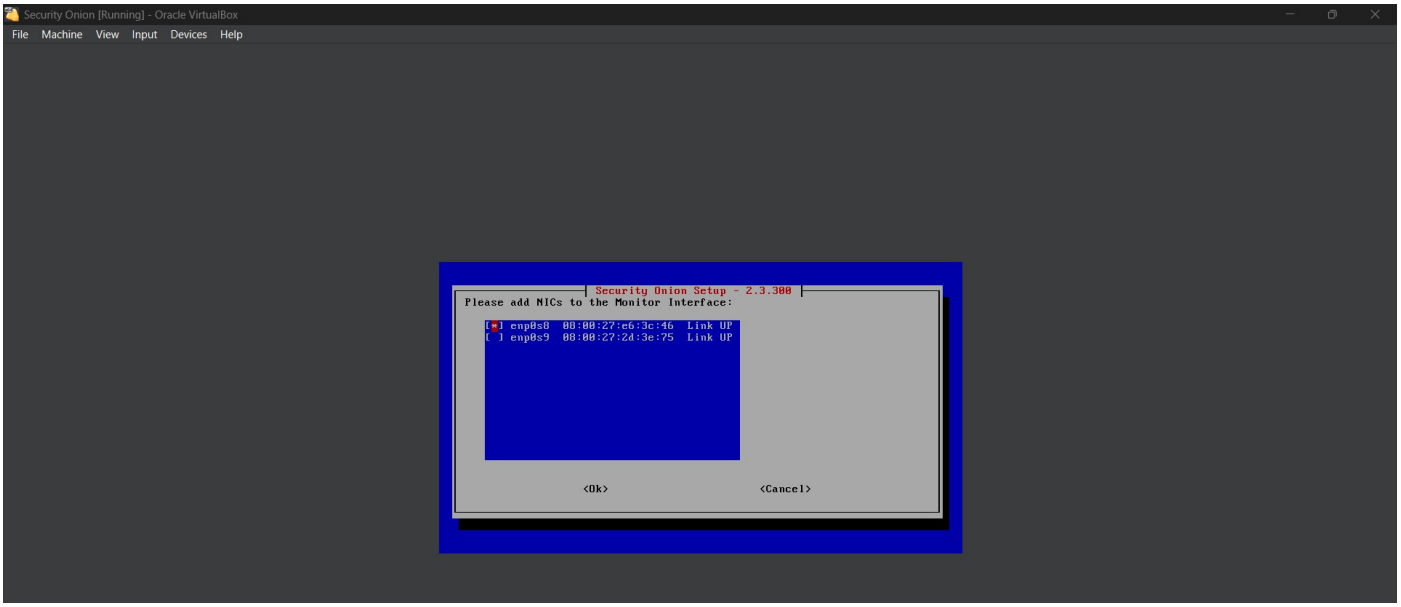


I Installed the manager in Standard mode so that I will have Internet Access

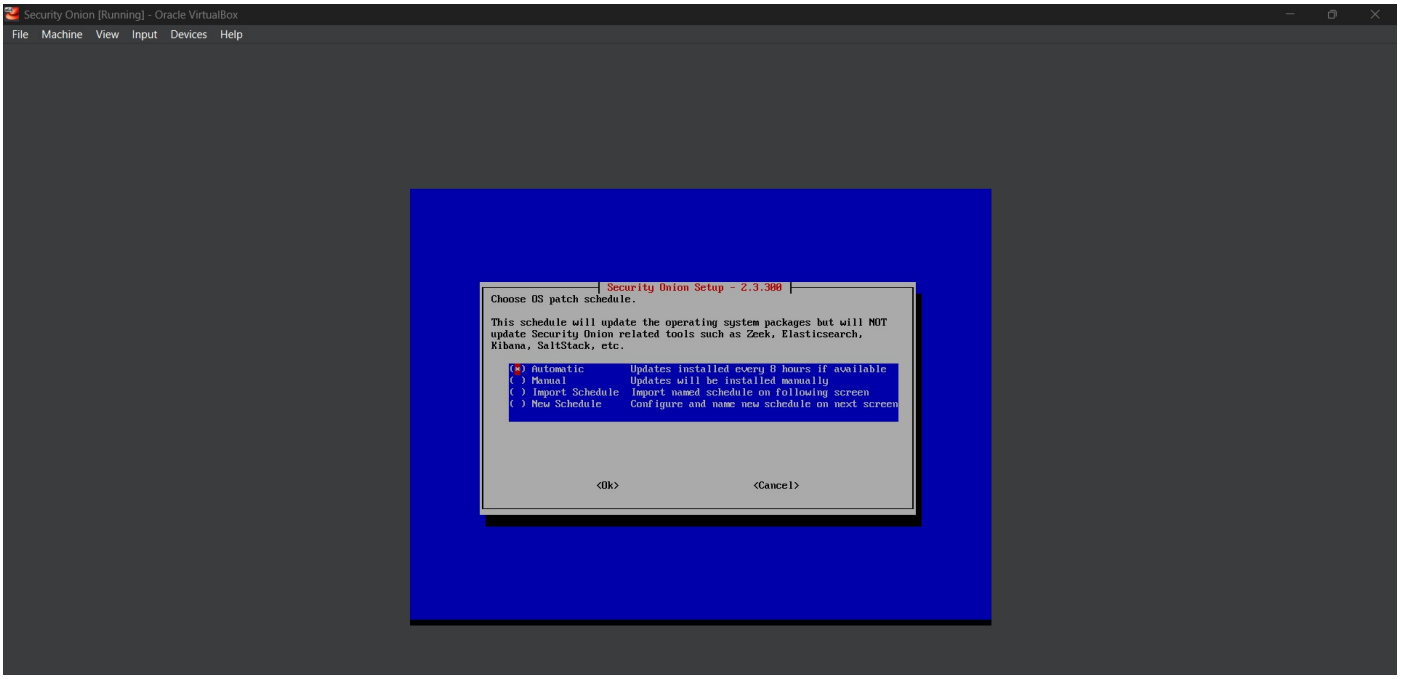




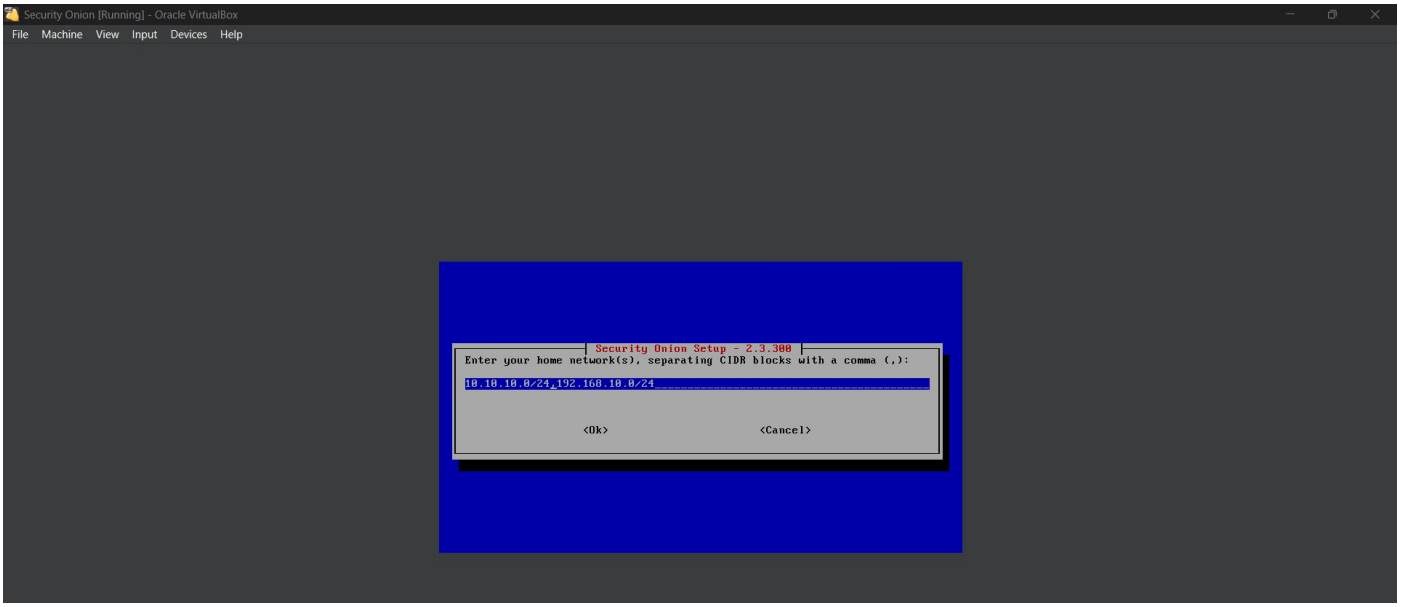
I selected the second interface as the monitoring(enp0s8) as (sniffing) interface.



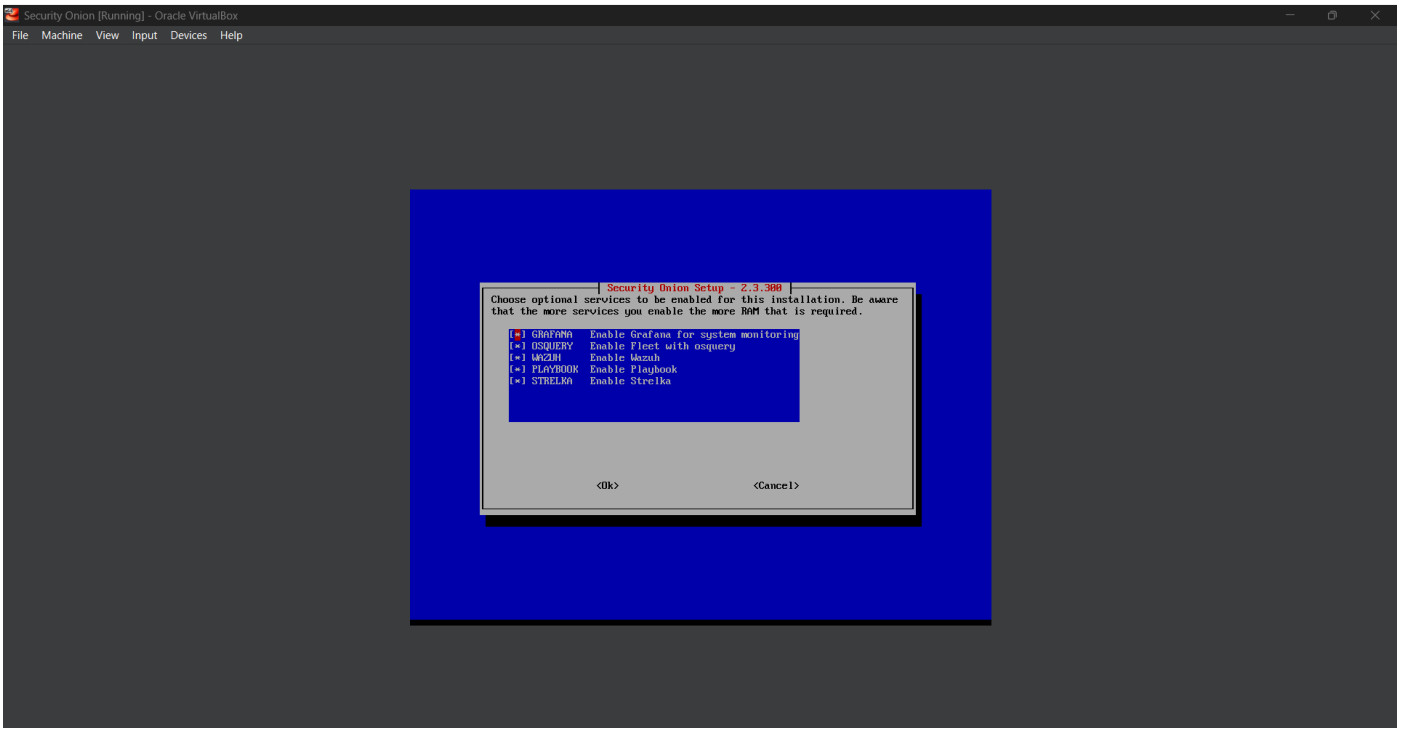
I chose *Automatic* for the operating system patch schedule.



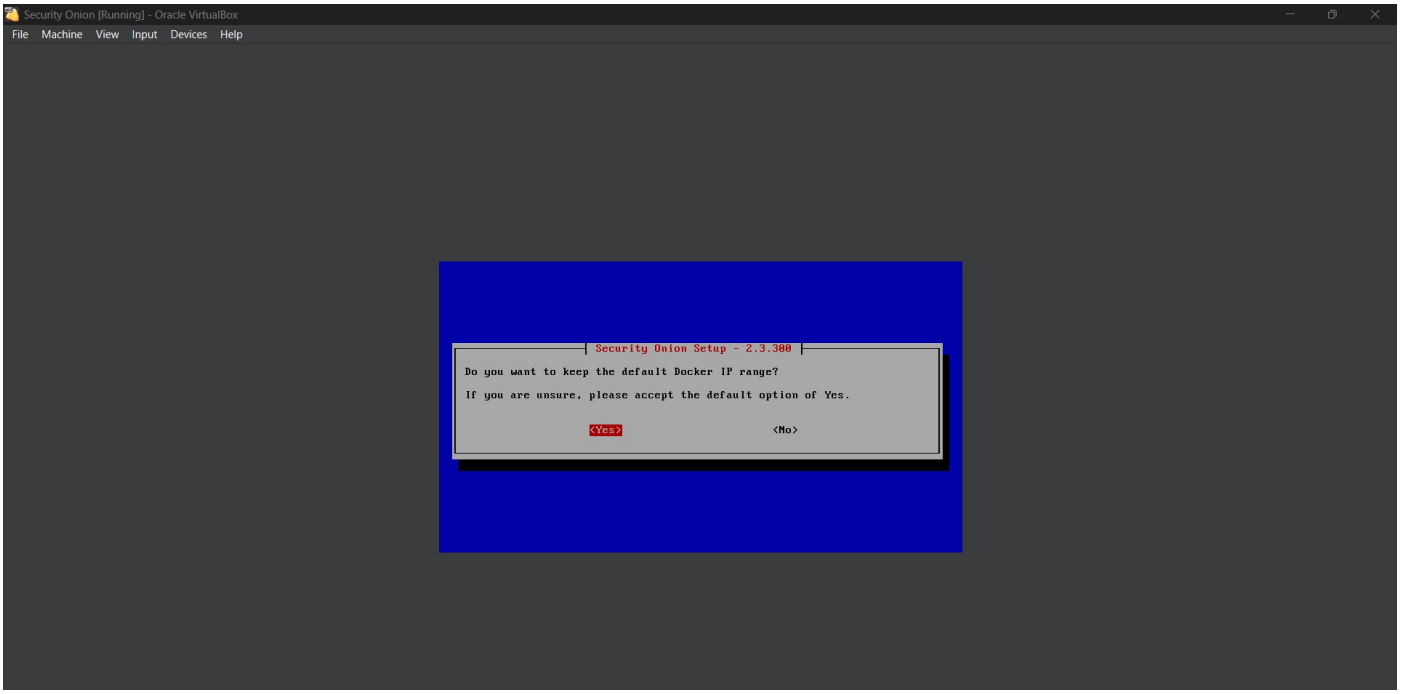
I set the *HOME_NET* IP address range to *10.10.10.0/24, 192.168.10.0/24*



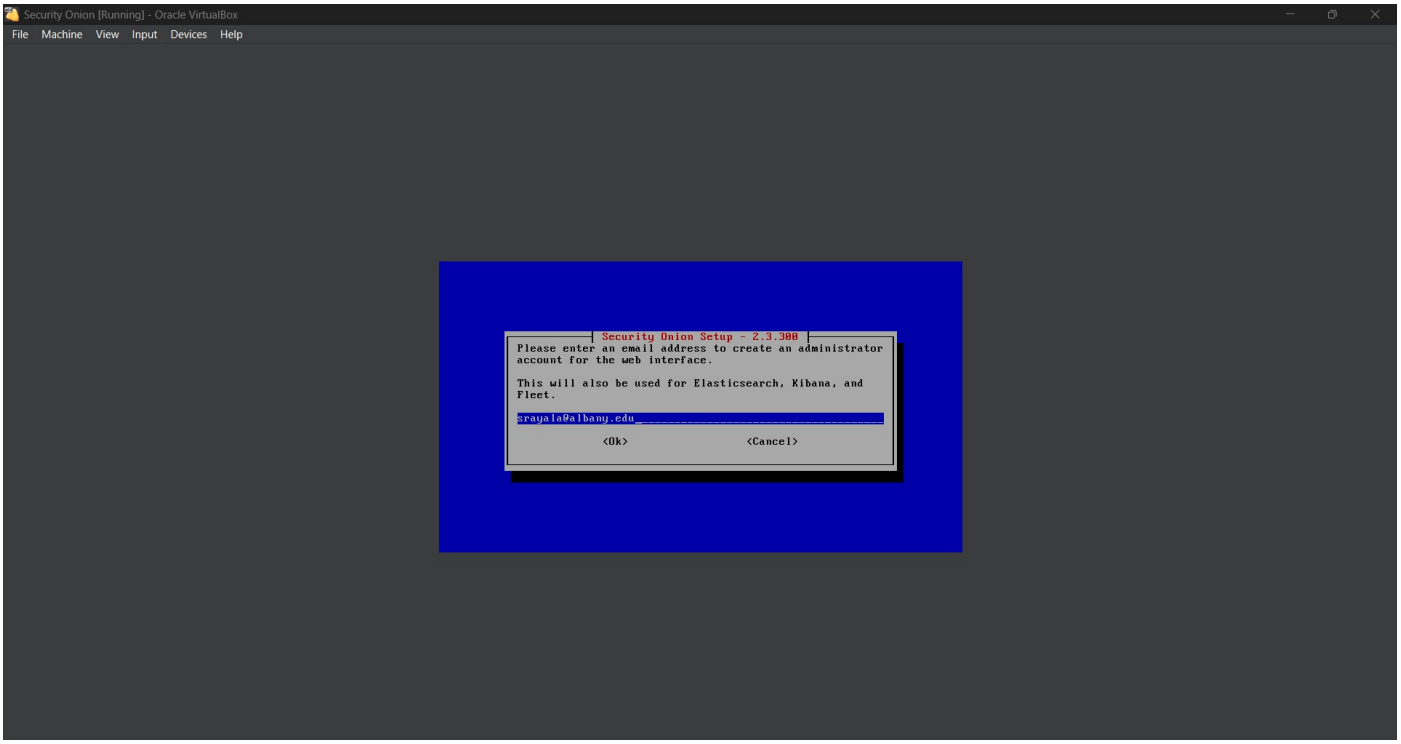
I selected the default components to install for the Security Onion services.

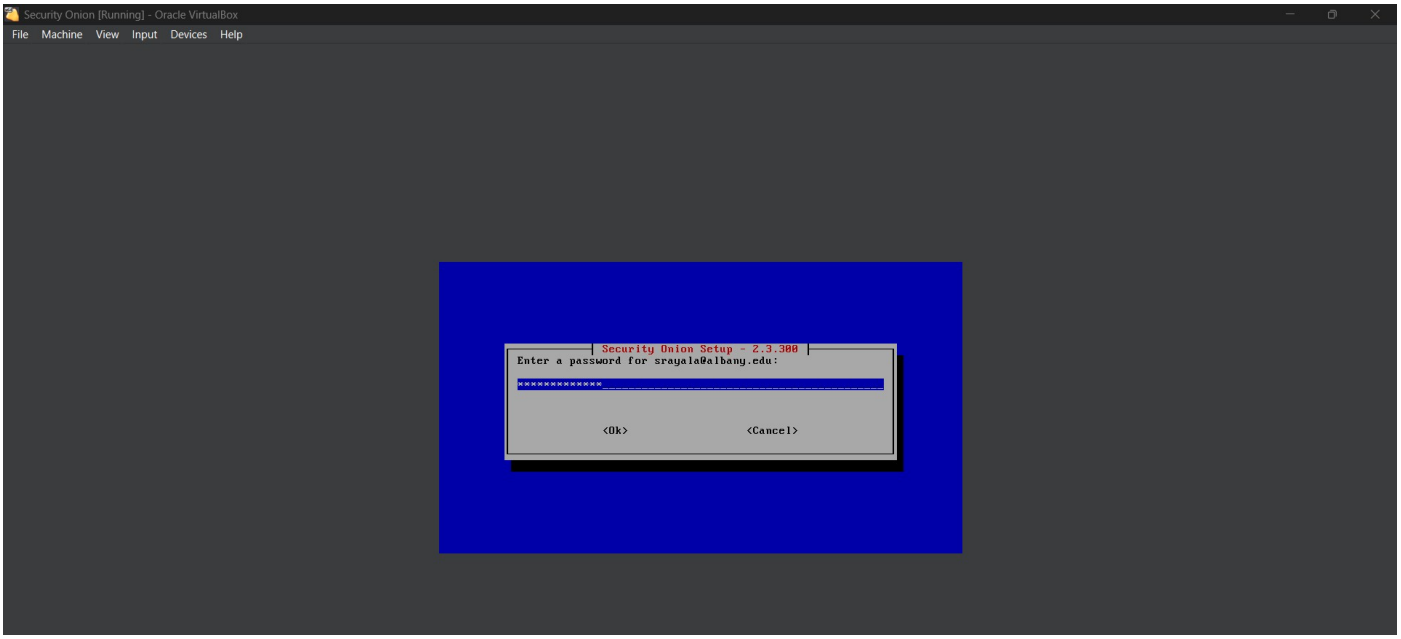


I confirmed that I wanted Security Onion to use the default Docker IP range.

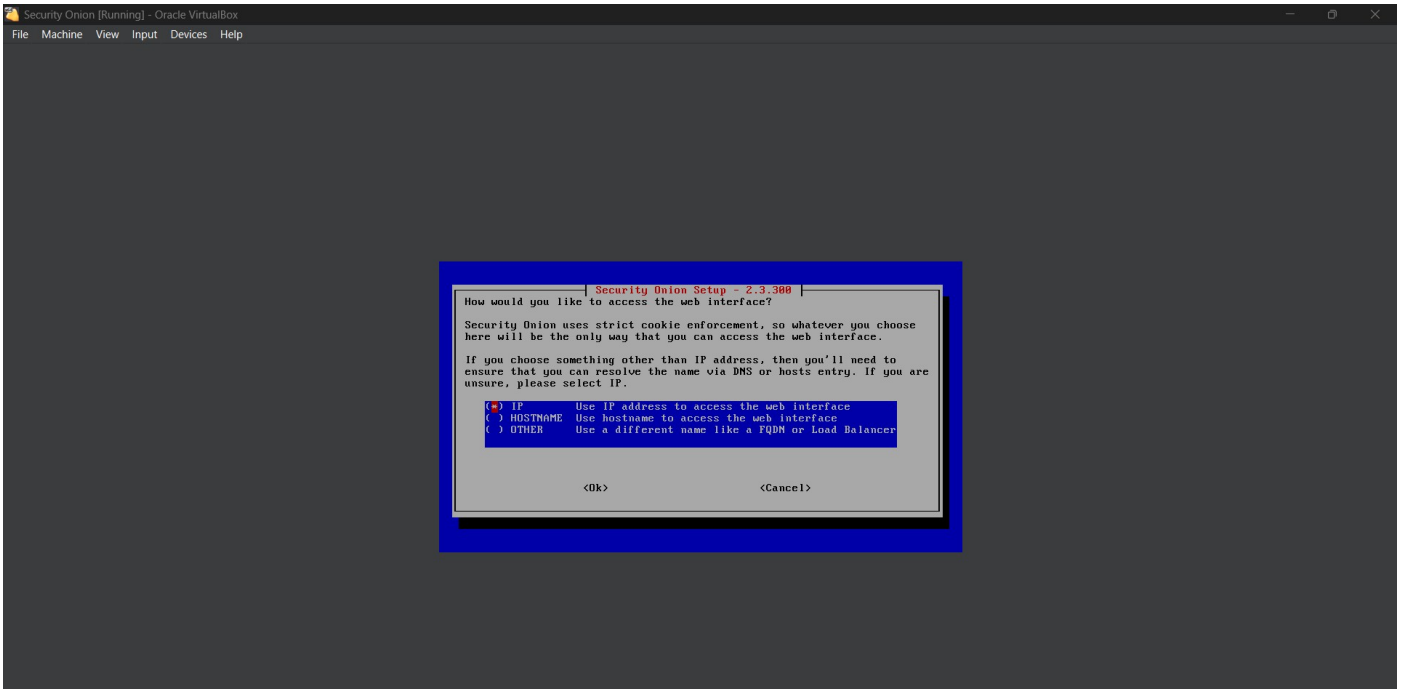


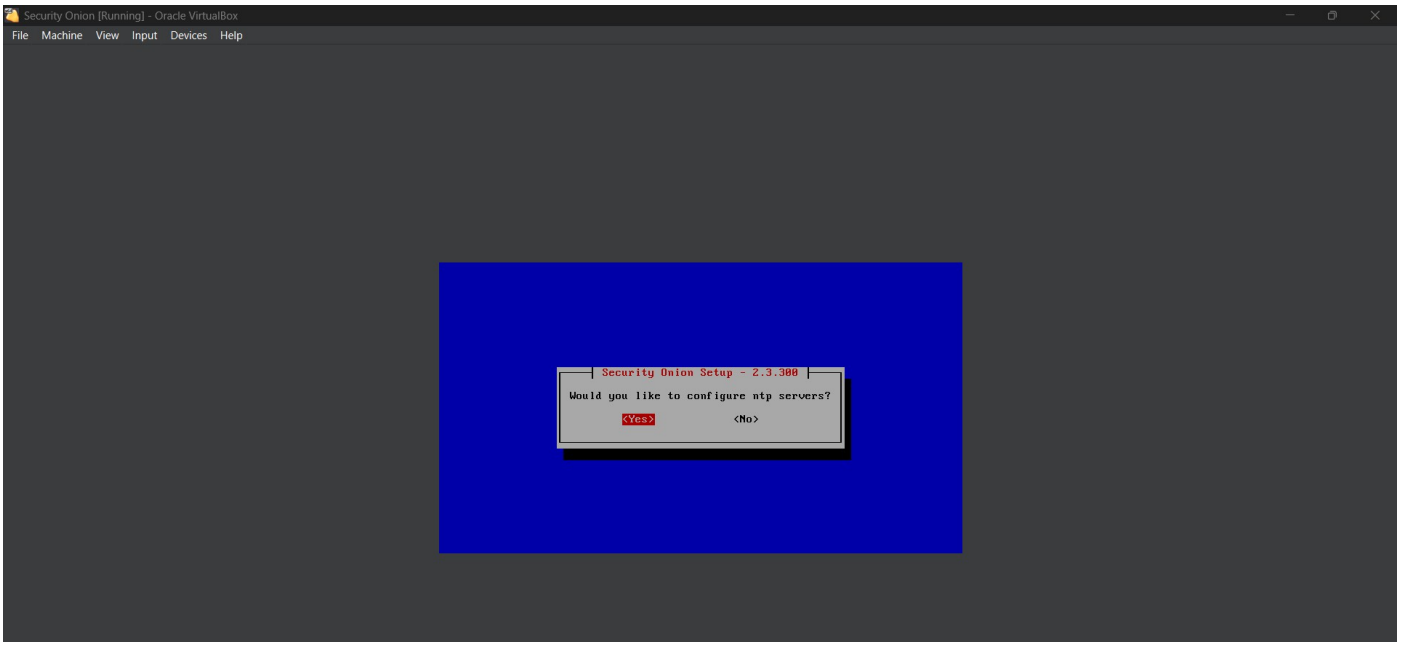
I specified an email address and password for the administrator of the web interface.

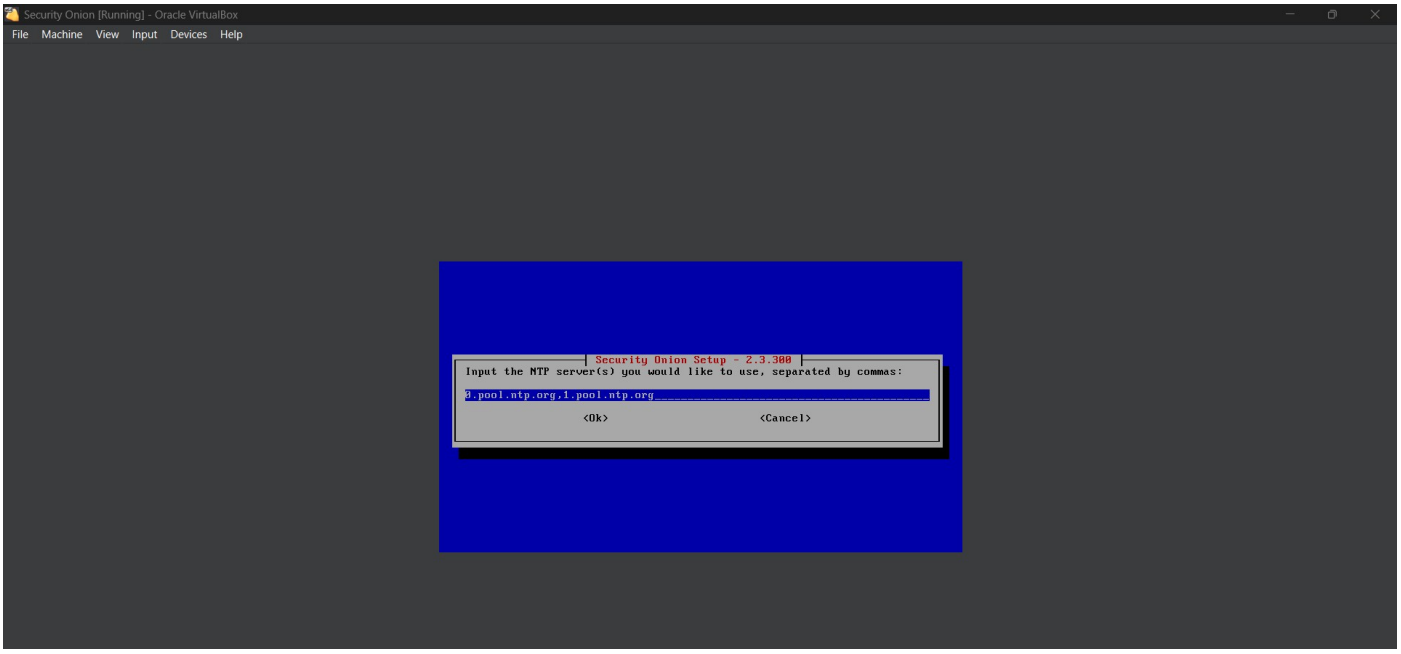




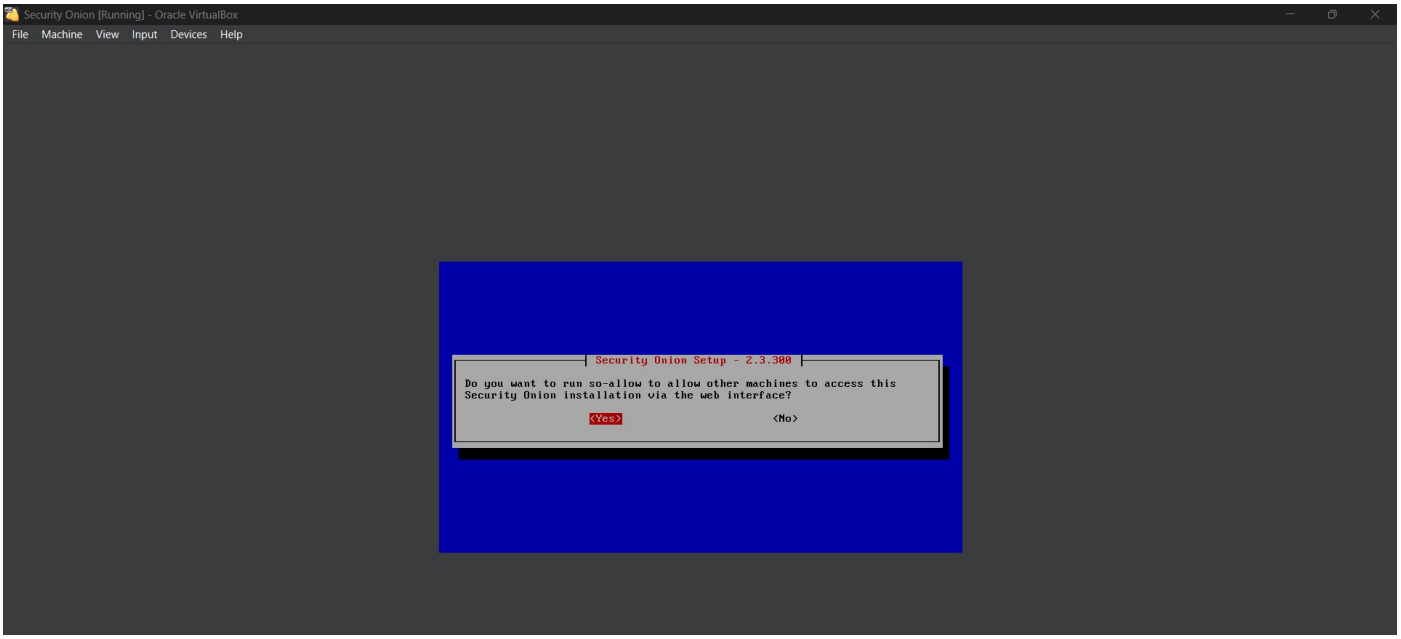
I selected *IP* for the access method and configured NTP Servers

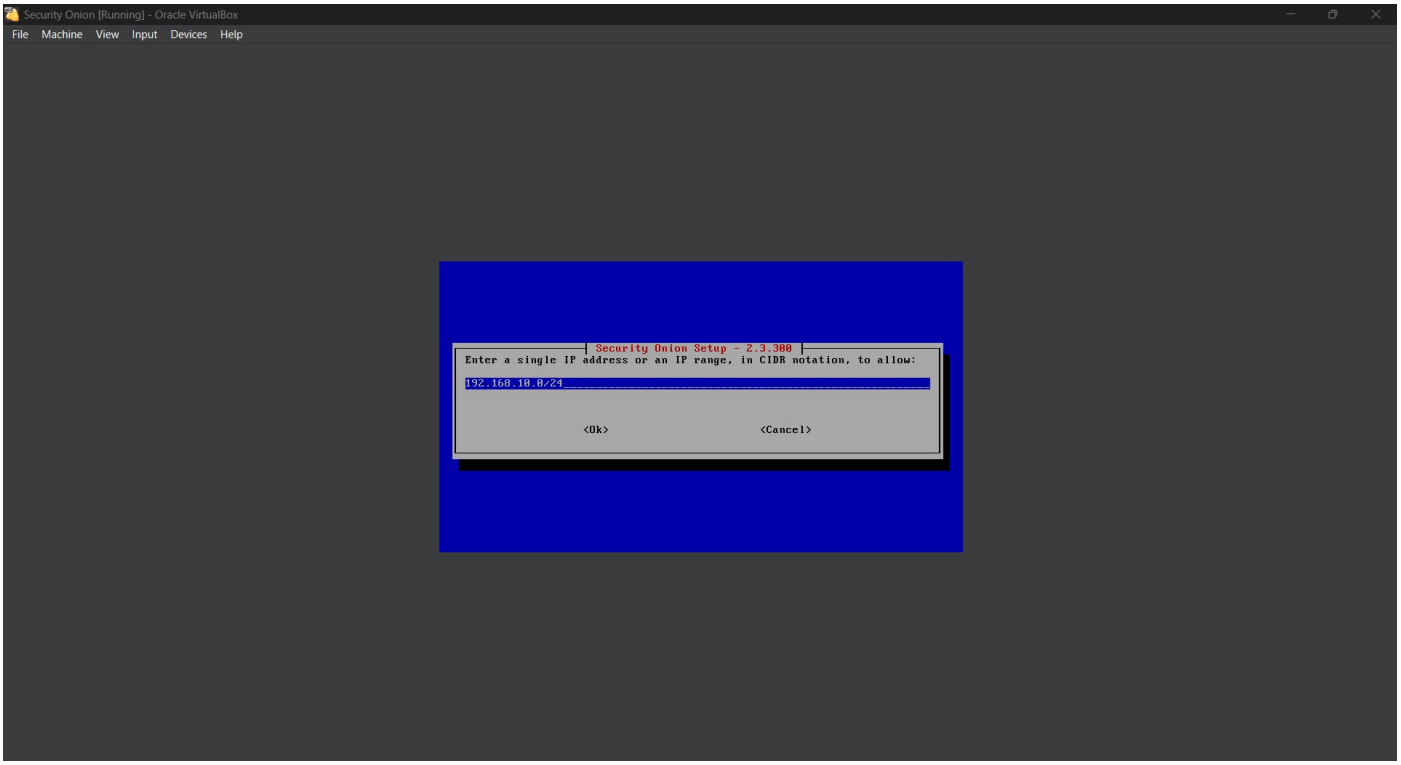

Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Security Onion Setup - 2.3.300
How would you like to access the web interface?
Security Onion uses strict cookie enforcement, so whatever you choose here will be the only way that you can access the web interface.
If you 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>

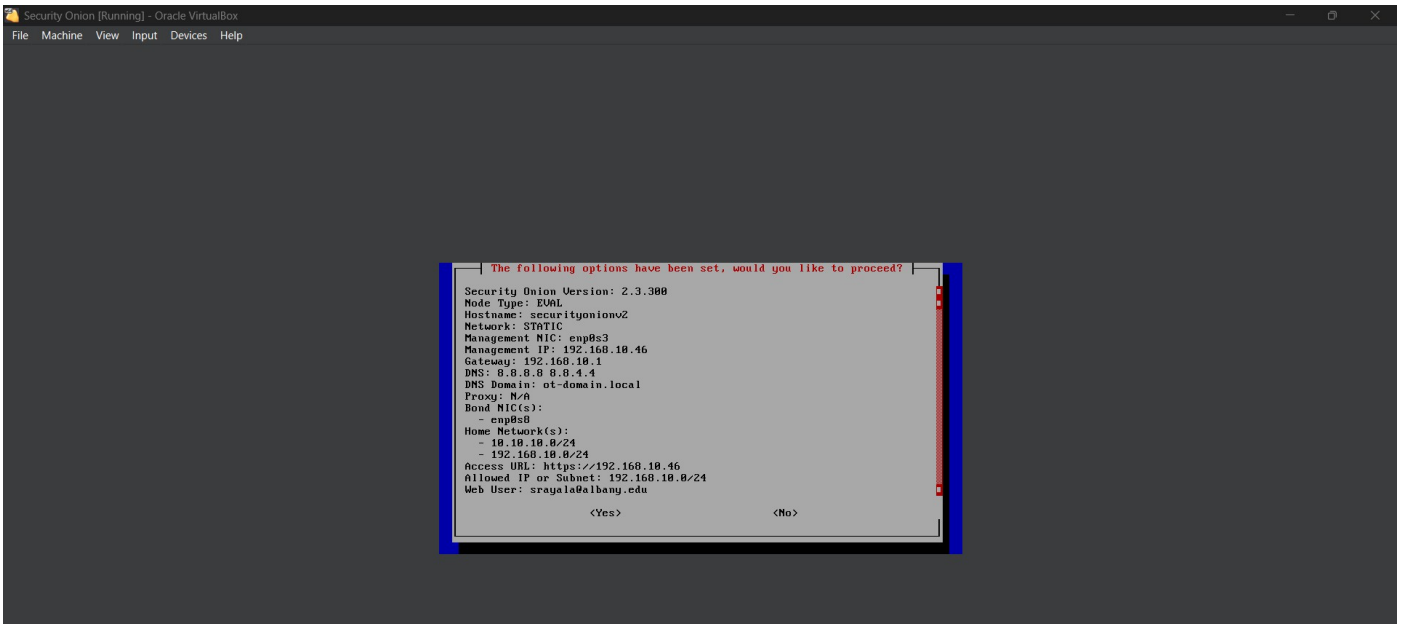

Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Security Onion Setup - 2.3.300
Would you like to configure ntp servers?
<Yes>
<No>

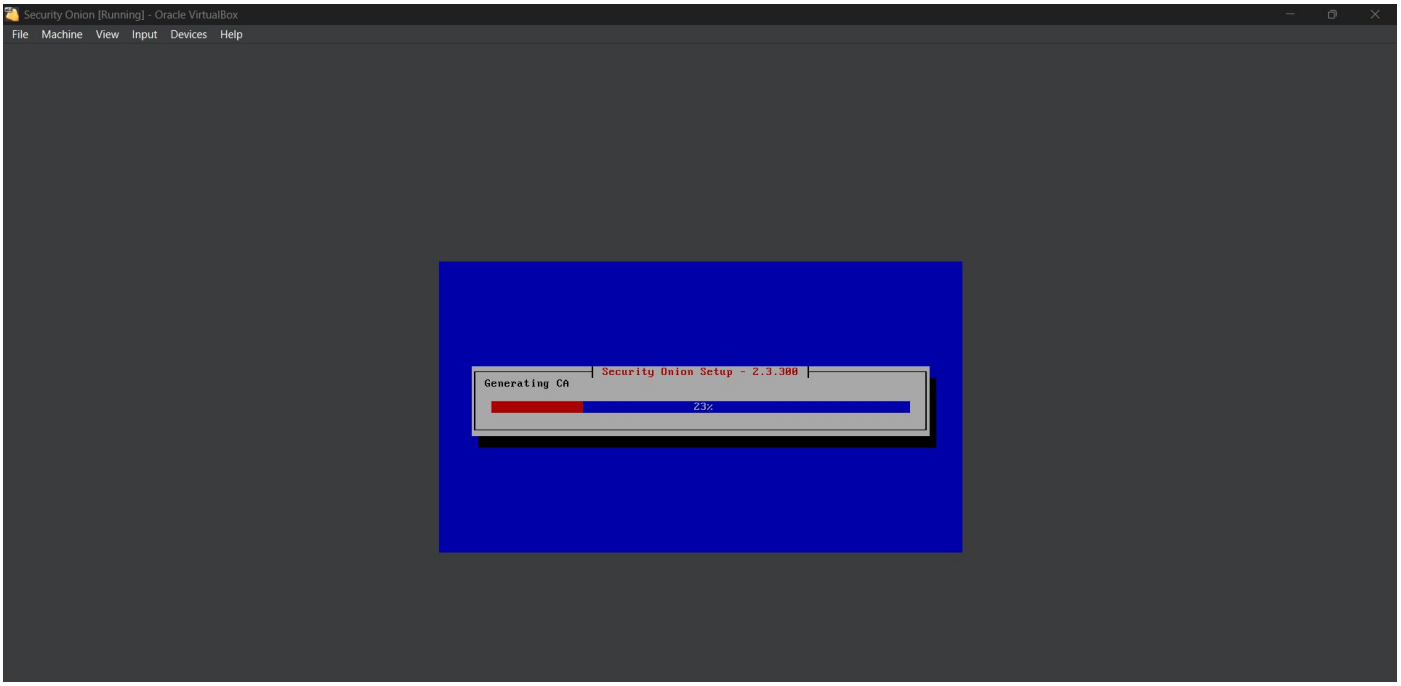


I configured the network to allow access to the Security Onion management interfaces and web portal from the lab network. I confirmed the installation process and allowed the appliance to configure.

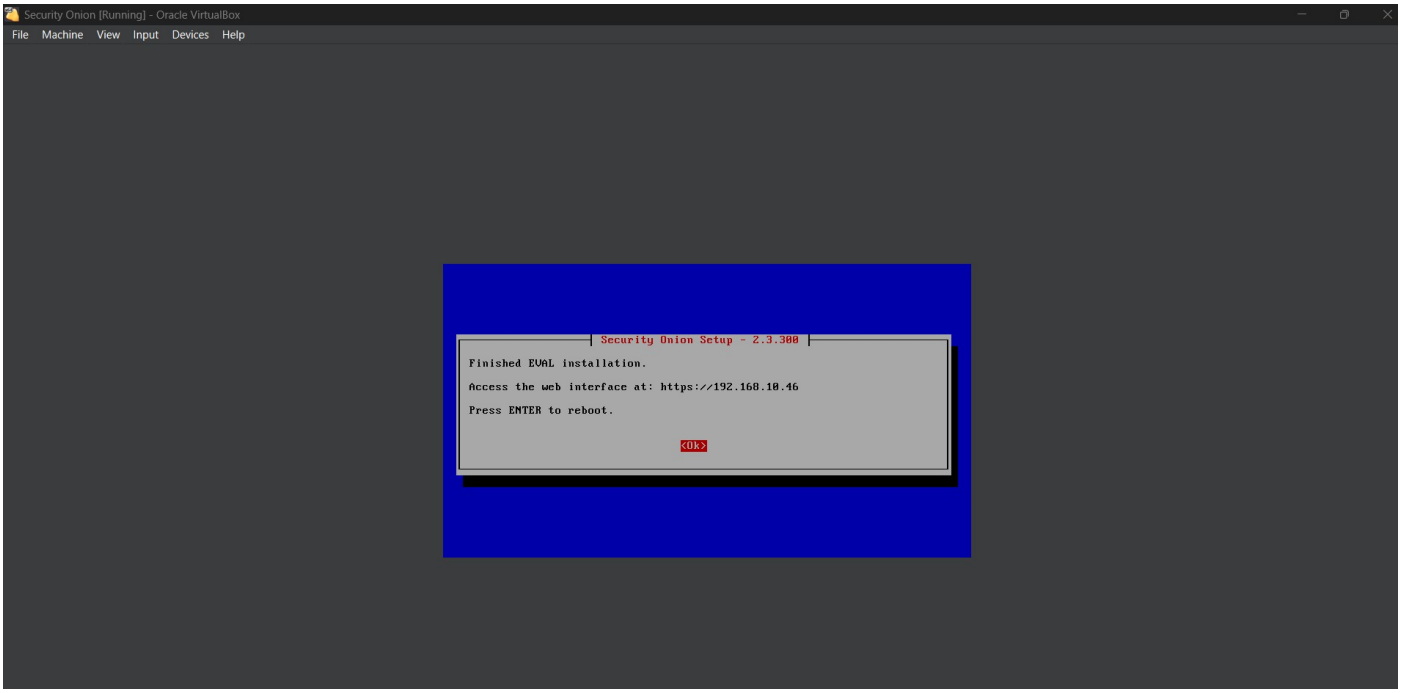



Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Security Onion Setup - 2.3.300
Enter a single IP address or an IP range, in CIDR notation, to allow:
192.168.10.0/24
<Ok>
<Cancel>

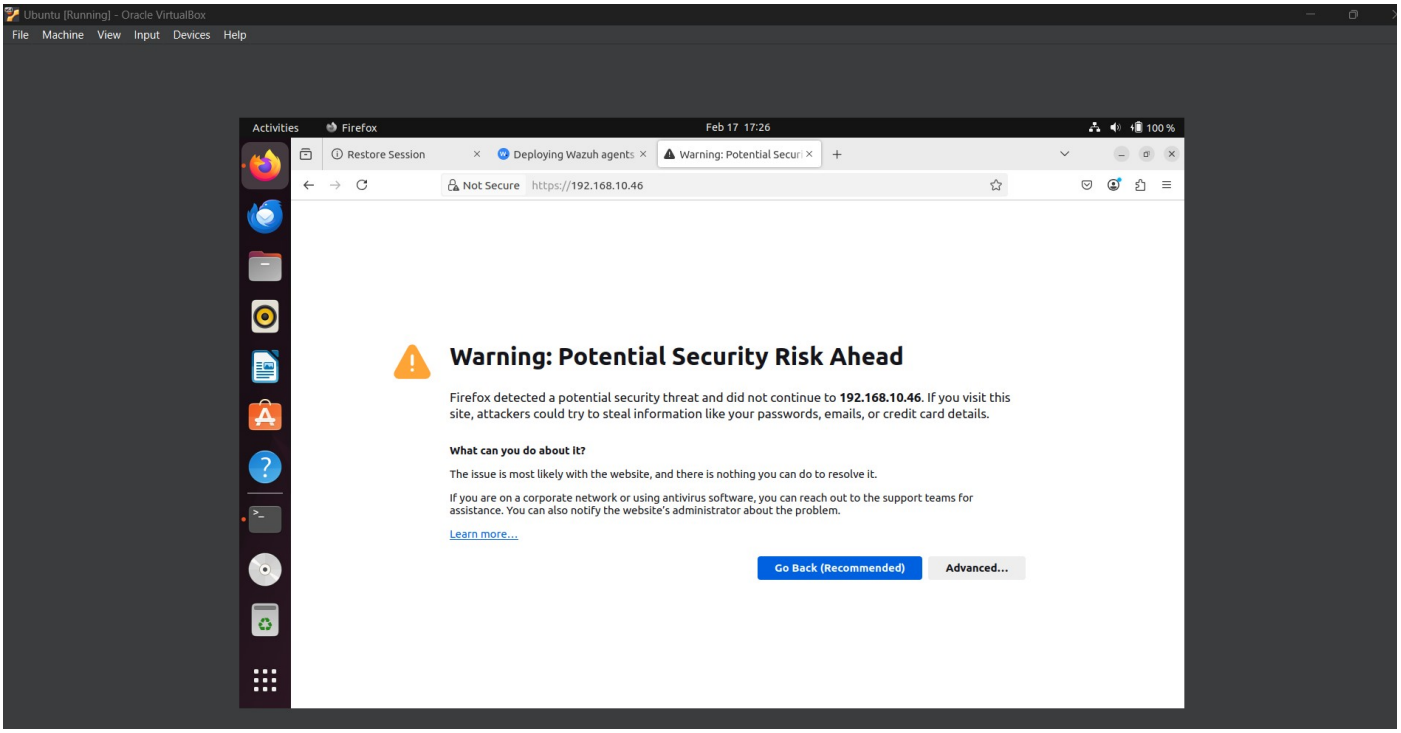

Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
The following options have been set, would you like to proceed?
Security Onion Version: 2.3.300
Mode Type: EVAL
Hostname: securityonionv2
Network: STATIC
Management NIC: enp0s3
Management IP: 192.168.10.46
Gateway: 192.168.10.1
DNS: 8.8.8.8 8.8.4.4
DNS Domain: ot-domain.local
Proxy: N/A
Bond NIC(s):
- enp0s8
Home Network(s):
- 10.10.10.0/24
- 192.168.10.0/24
Access URL: https://192.168.10.46
Allowed IP or Subnet: 192.168.10.0/24
Web User: srayala@albany.edu
<Yes>
<No>

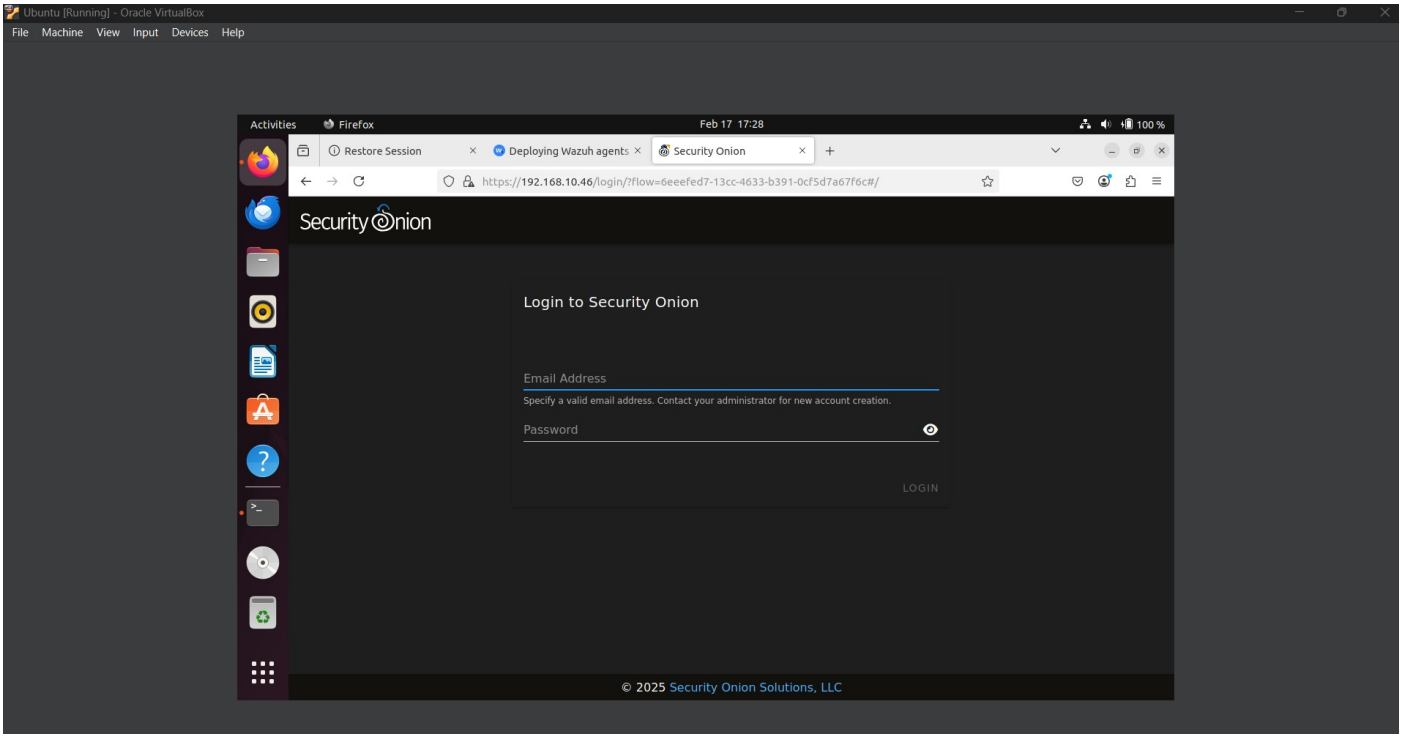


Once the installation was complete, I rebooted the system and was ready to use Security Onion.



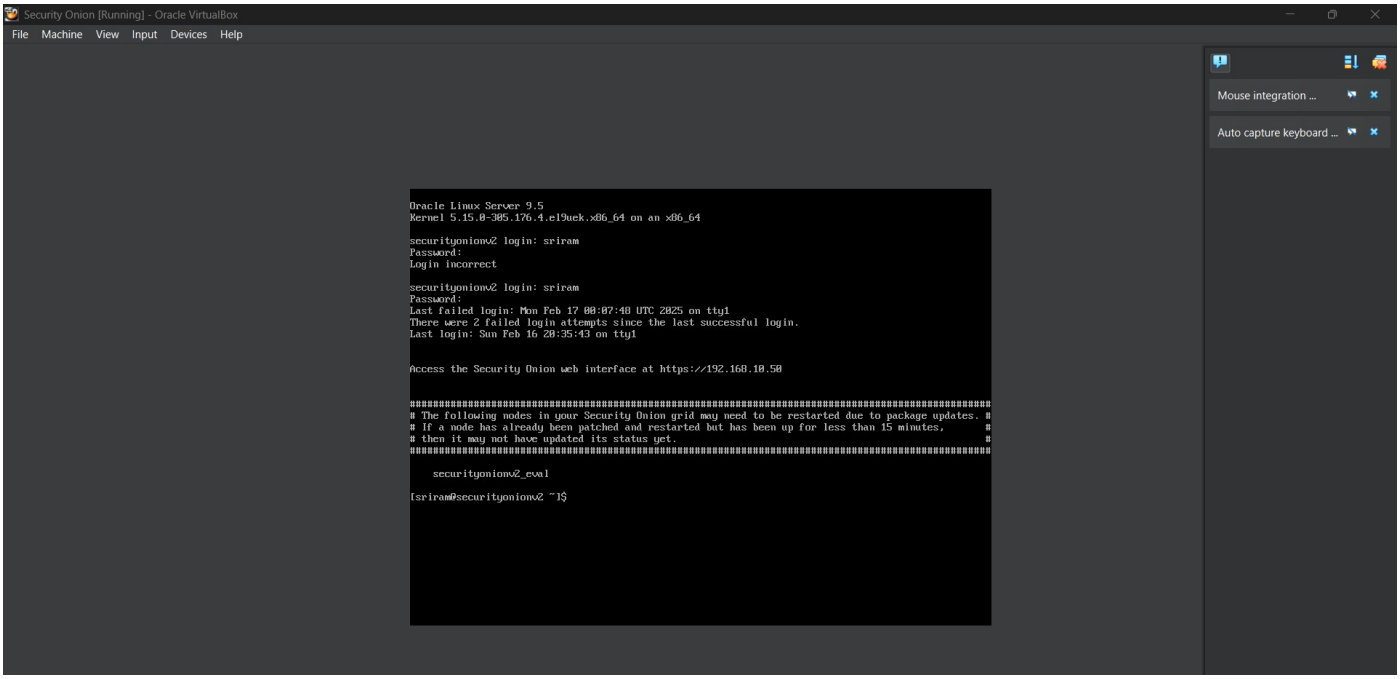
I can access my security onion from https://192.168.10.46

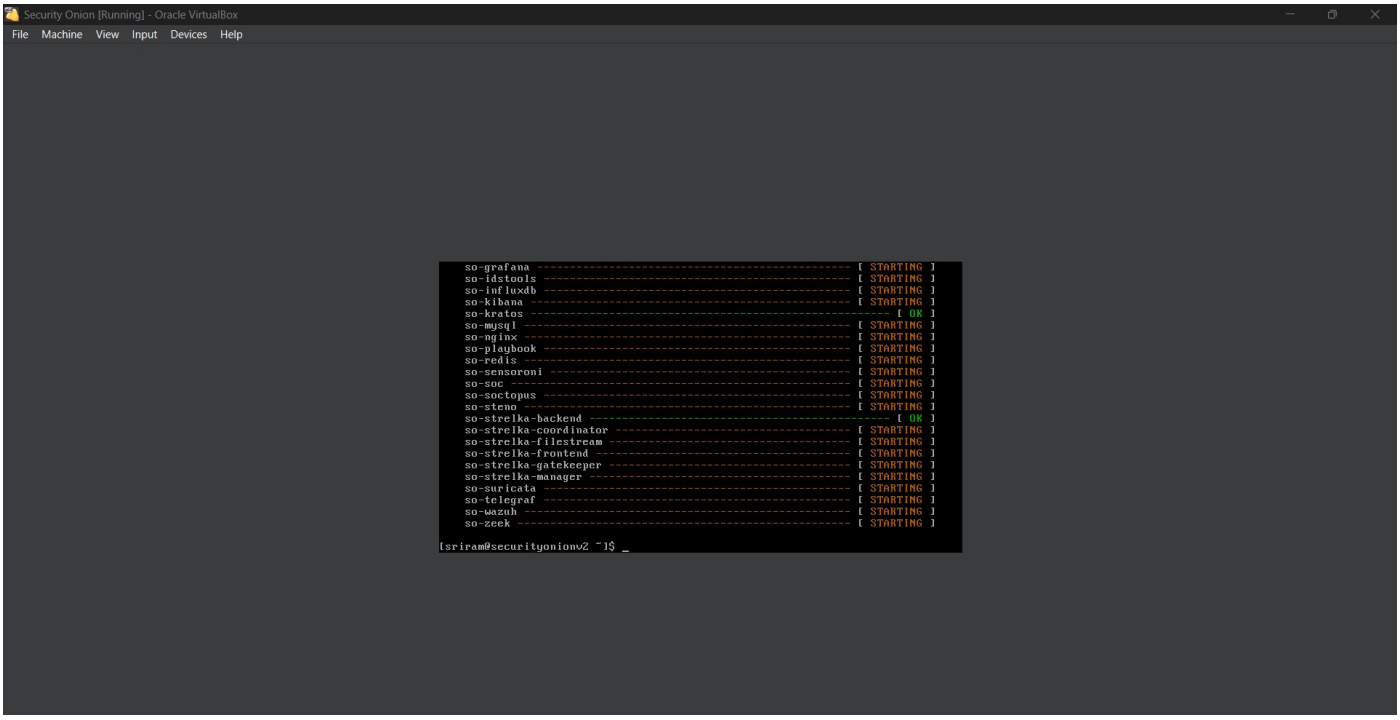


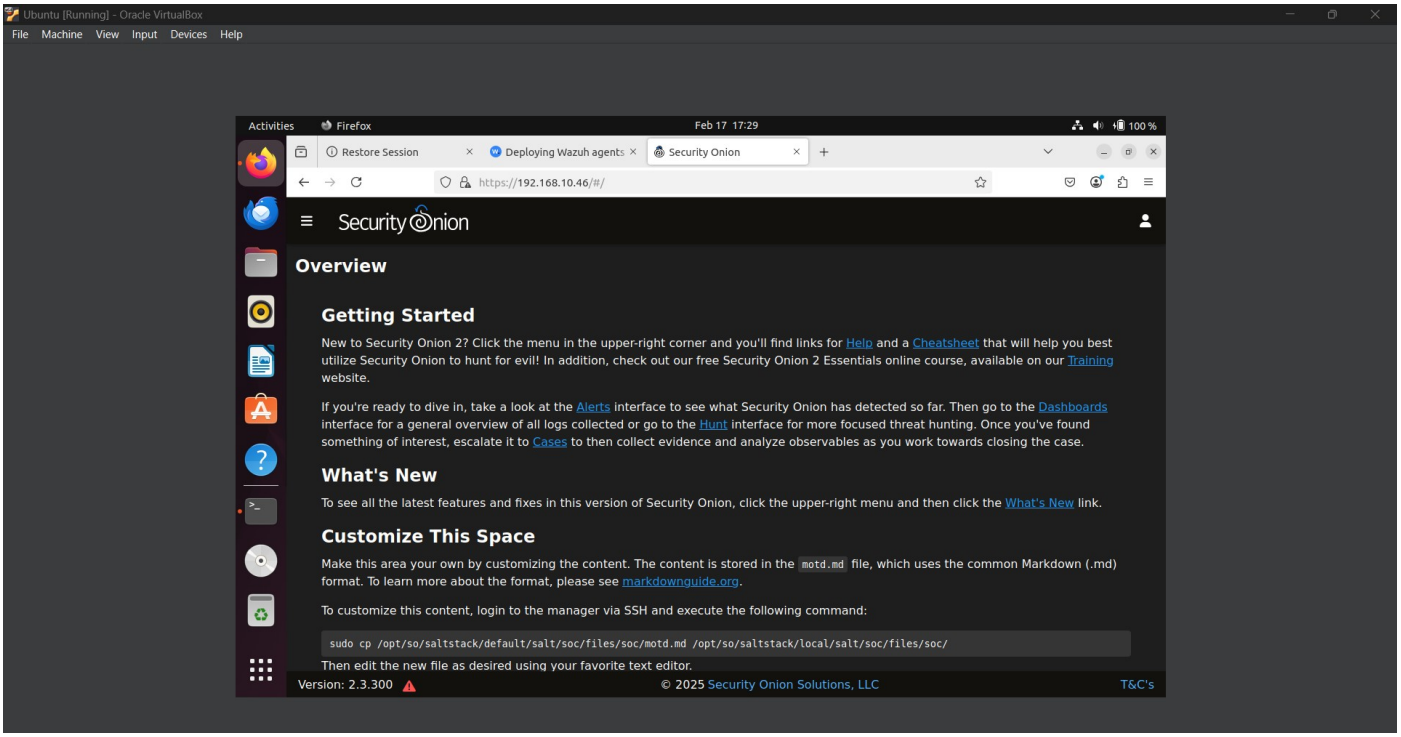


Objective 2: Configuring Security Onion

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 ...
Oracle Linux Server 9.5
Kernel 5.15.0-305.176.4.el9uek.x86_64 on an x86_64
securityonionv2 login: sriram
Password:
Login incorrect
securityonionv2 login: sriram
Password:
Last failed login: Mon Feb 17 00:07:48 UTC 2025 on tty1
There were 2 failed login attempts since the last successful login.
Last login: Sun Feb 16 20:35:43 on tty1
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 patched and restarted but has been up for less than 15 minutes,
then it may not have updated its status yet.
securityonionv2_eval
[sriram@securityonionv2 ~]$


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 [STARTING]
so-nginx [STARTING]
so-playbook [STARTING]
so-redis [STARTING]
so-sensoroni [STARTING]
so-soc [STARTING]
so-soctopus [STARTING]
so-steno [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-zeek [STARTING]
[sriram@securityonionv2 ~]$ _

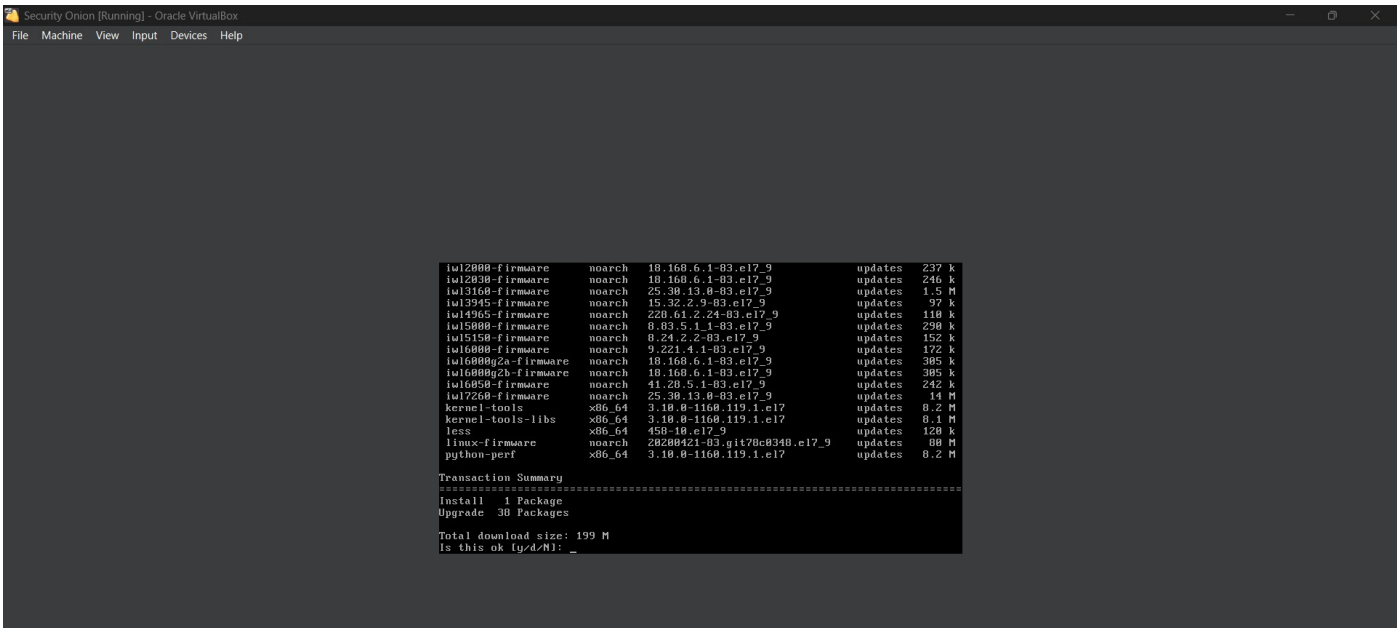


Objective 2.1: Installing VMware Tools

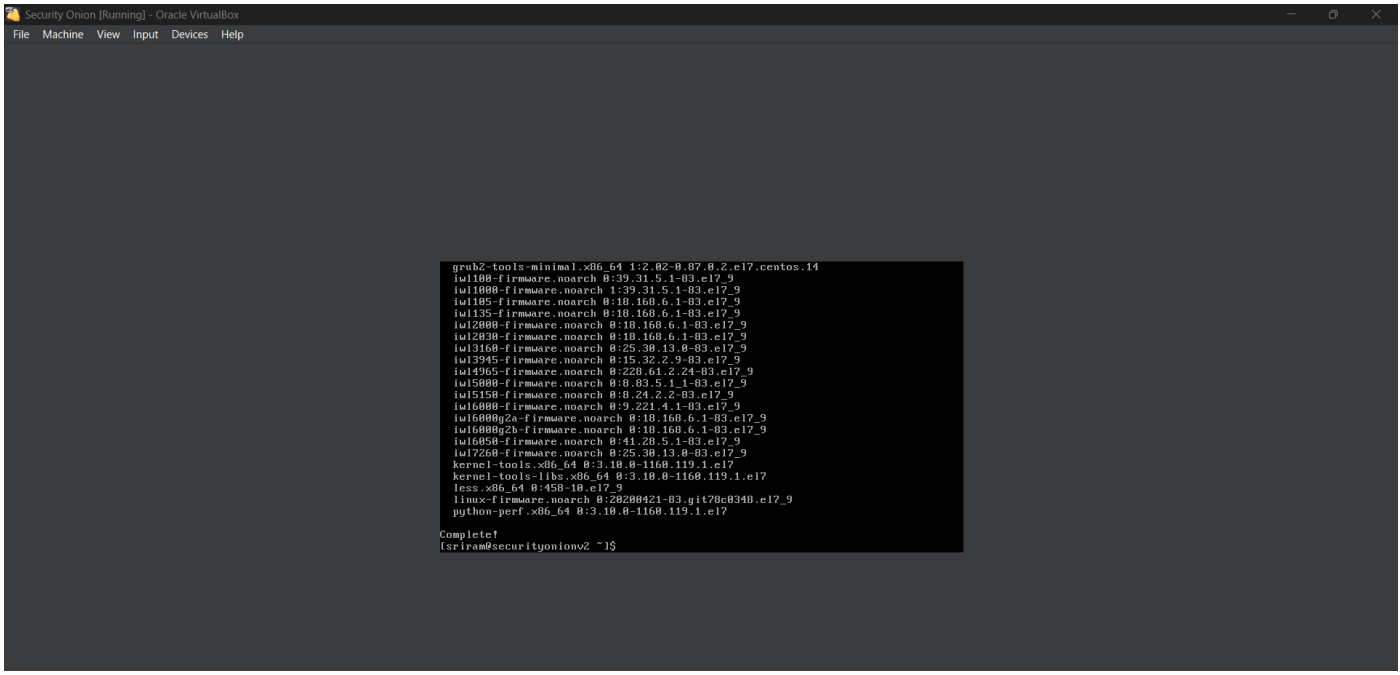
I installed VMware tools to improve the integration of the guest VM with VMware Workstation.

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

sudo yum update



sudo yum install open-vm-tools-desktop fuse

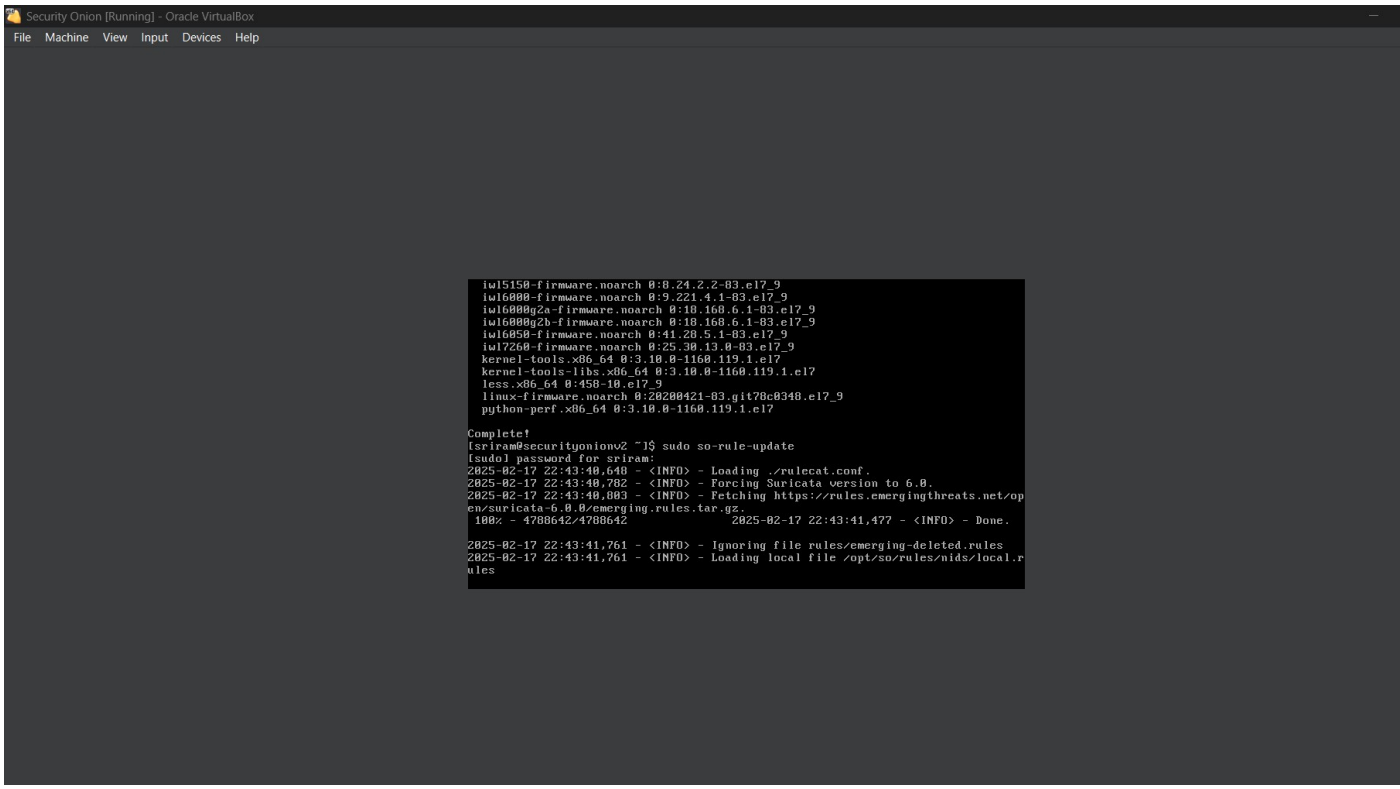


After the installation, I rebooted the VM to apply the changes.

Objective 2.2: Updating Suricata Rulesets

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

sudo so-rule-update



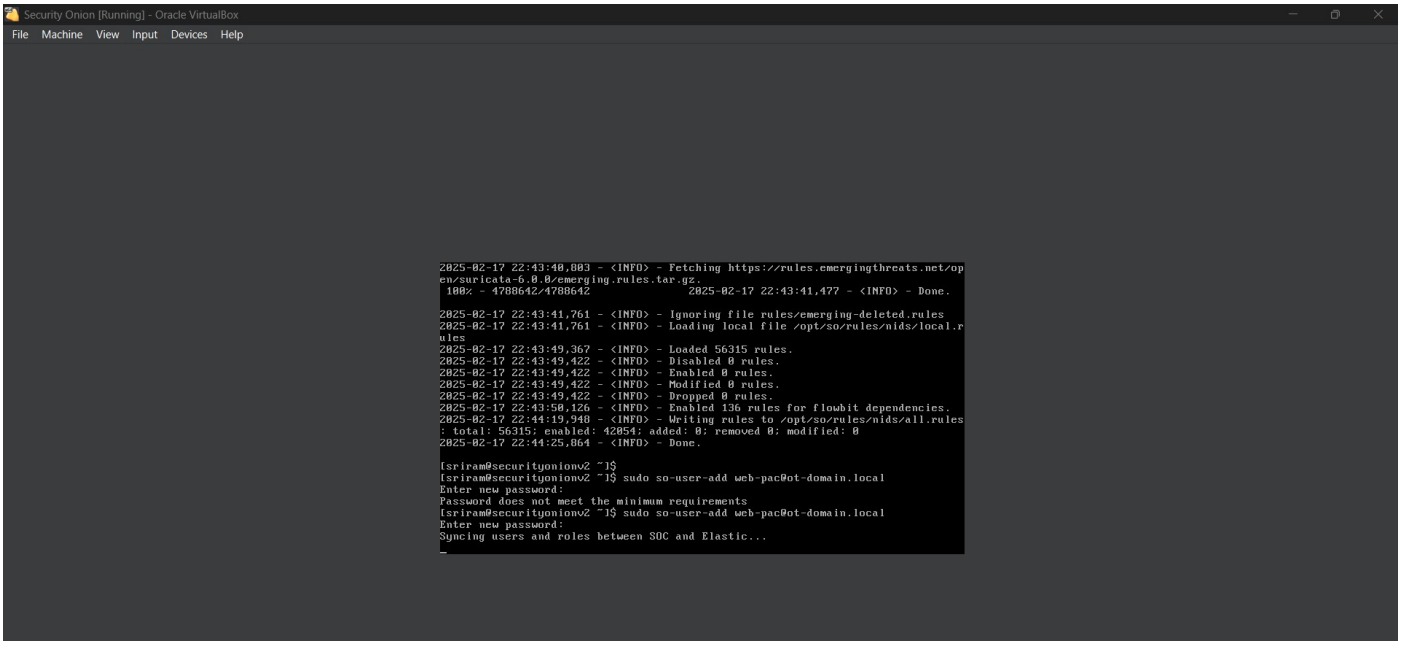
The Security Onion appliance updated the ruleset and restarted the Suricata engine.

Objective 2.3: Adding a Web Portal User

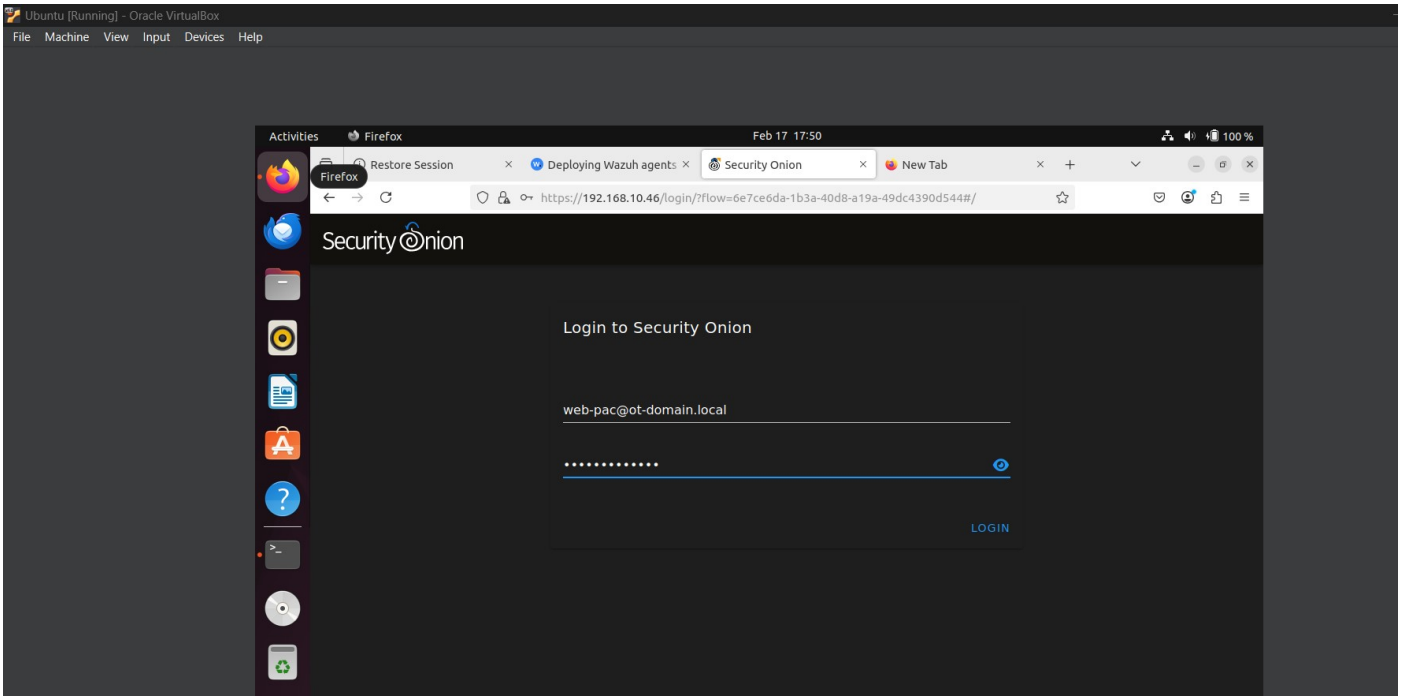
To allow non-admin access to the Security Onion web portal, I added a web portal user.

I ran the following command to add a new user:

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



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.

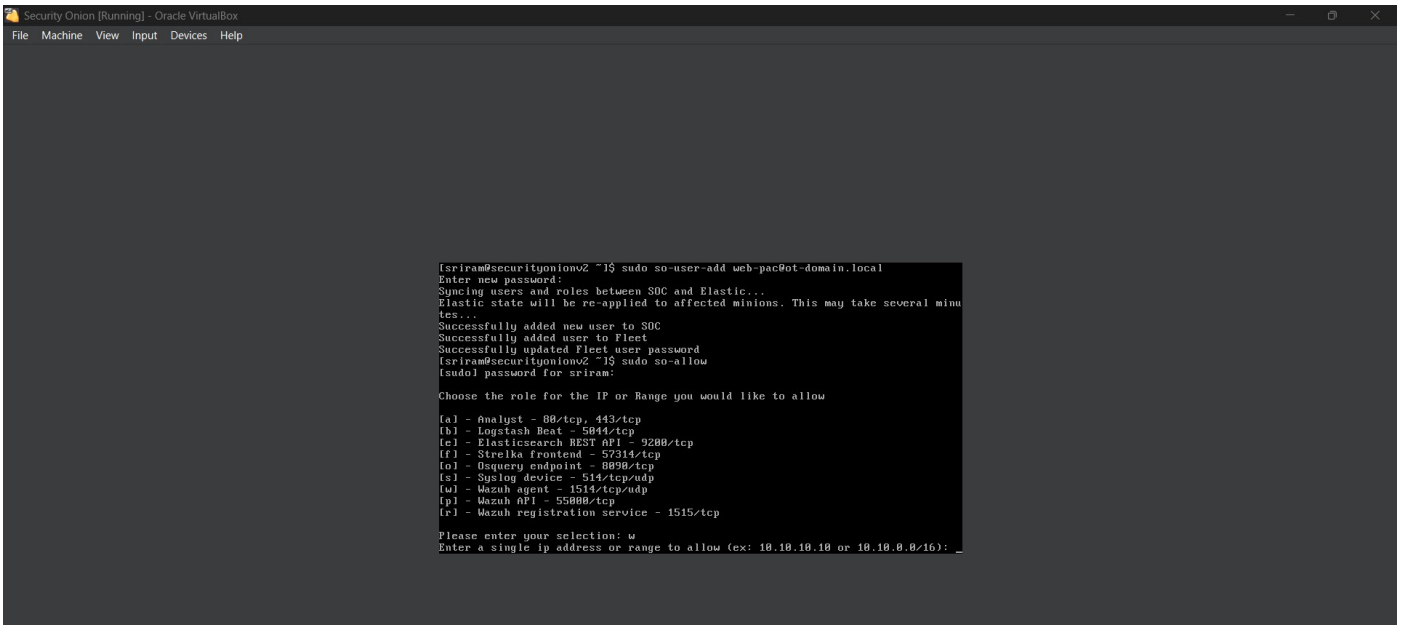
Configuring Wazuh Manager Access

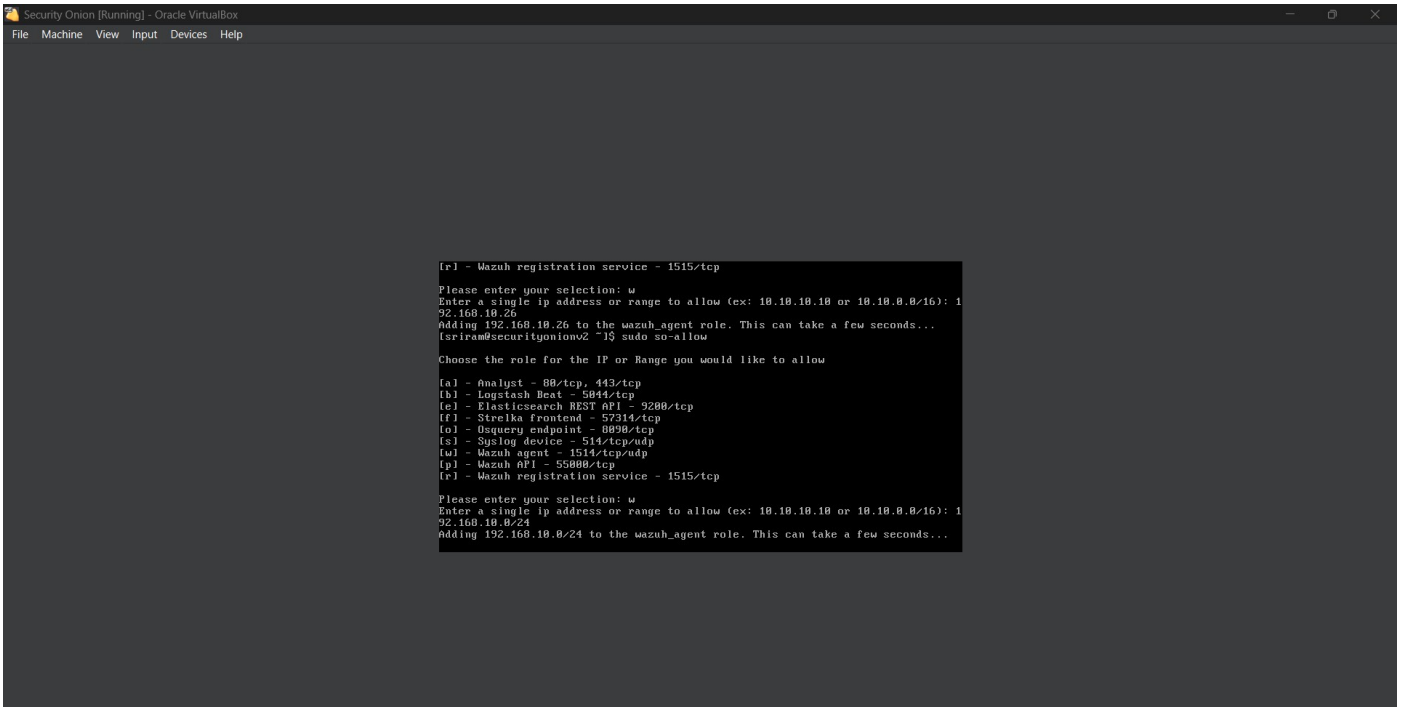
1. I logged into the Security Onion appliance via SSH.

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*.





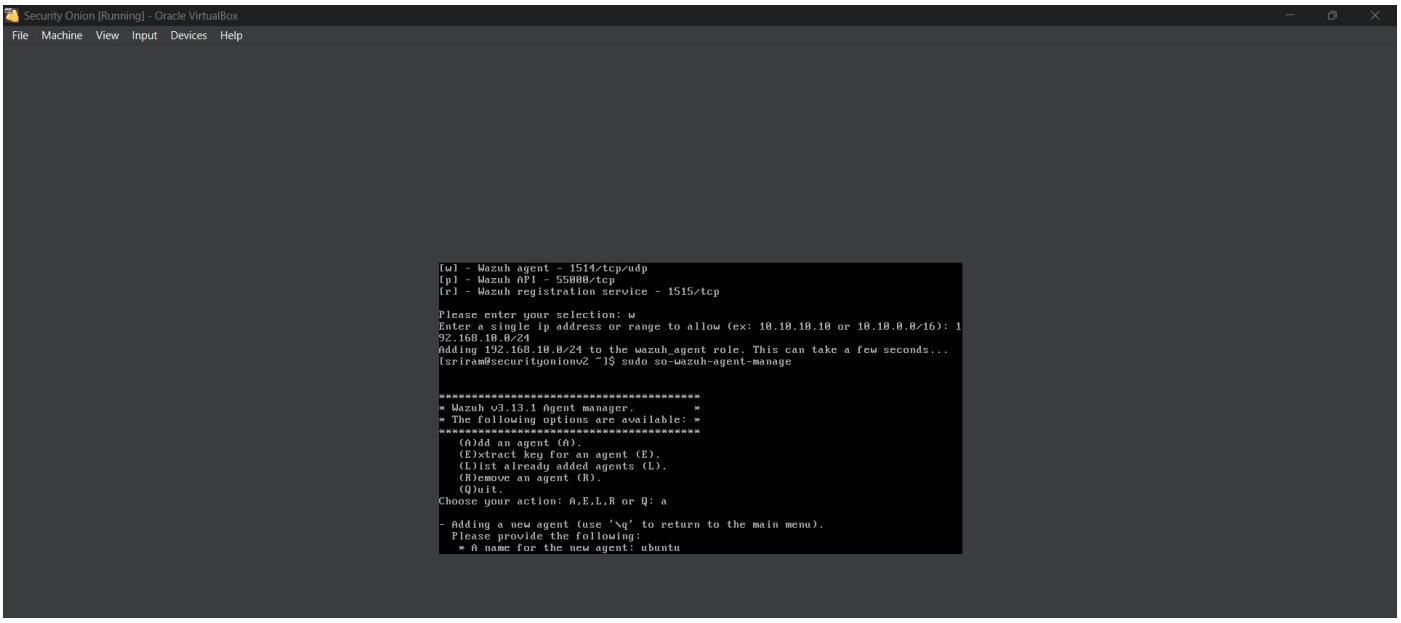
Registering Wazuh Agents

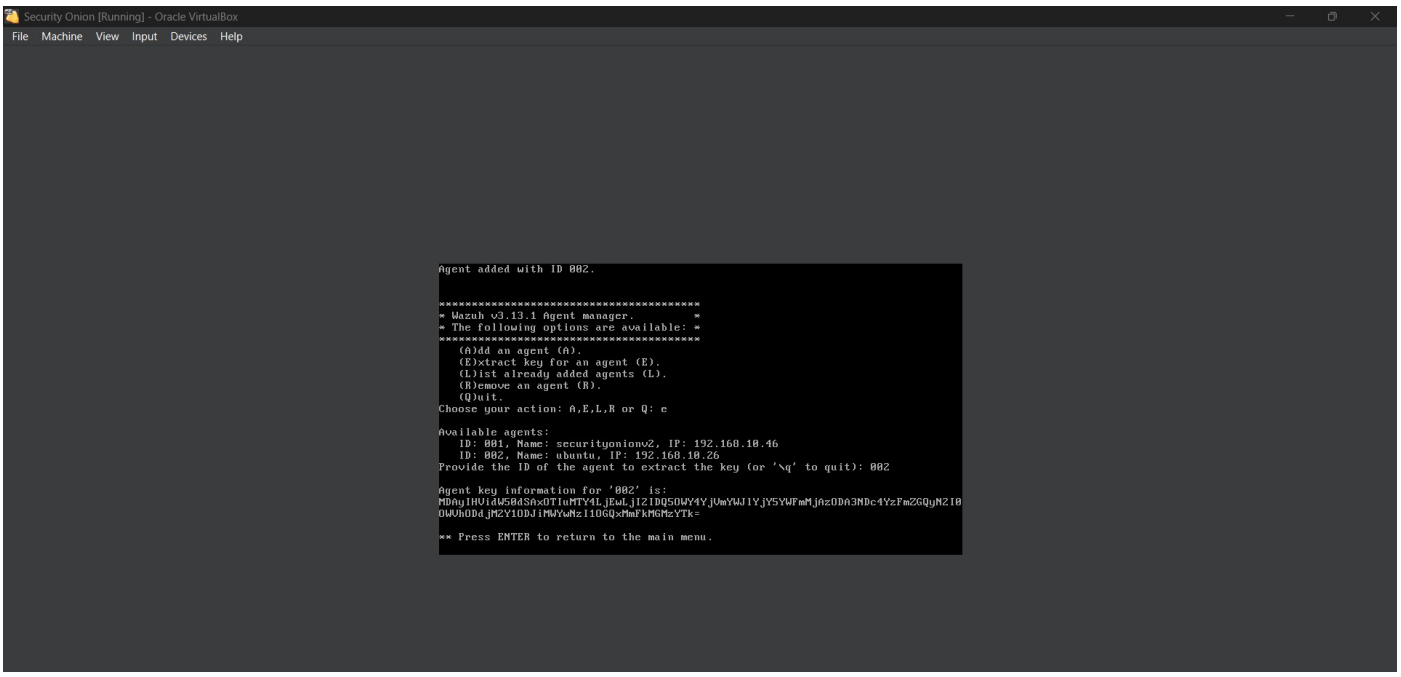
I ran the command to start the Wazuh agent management terminal:

sudo so-wazuh-agent-manage

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

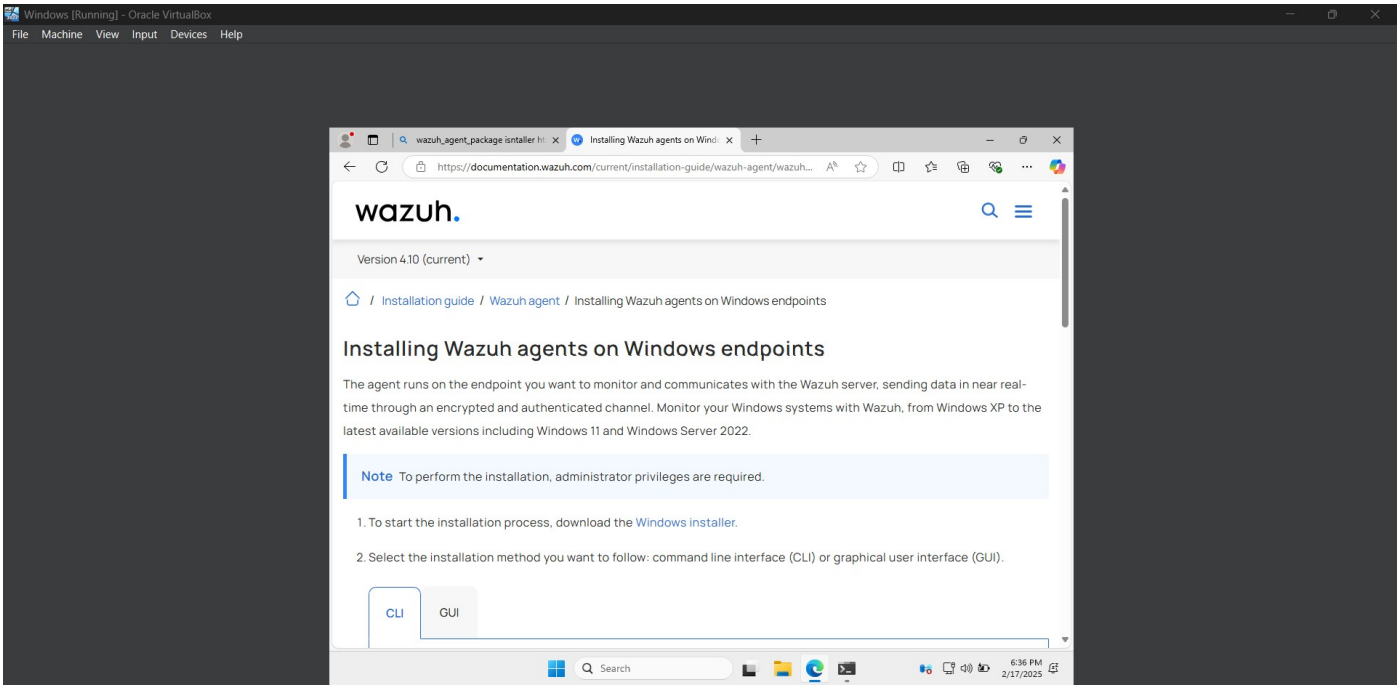
I extracted the agent key by selecting *E* for *Extract key for an agent* and recorded it for later use.

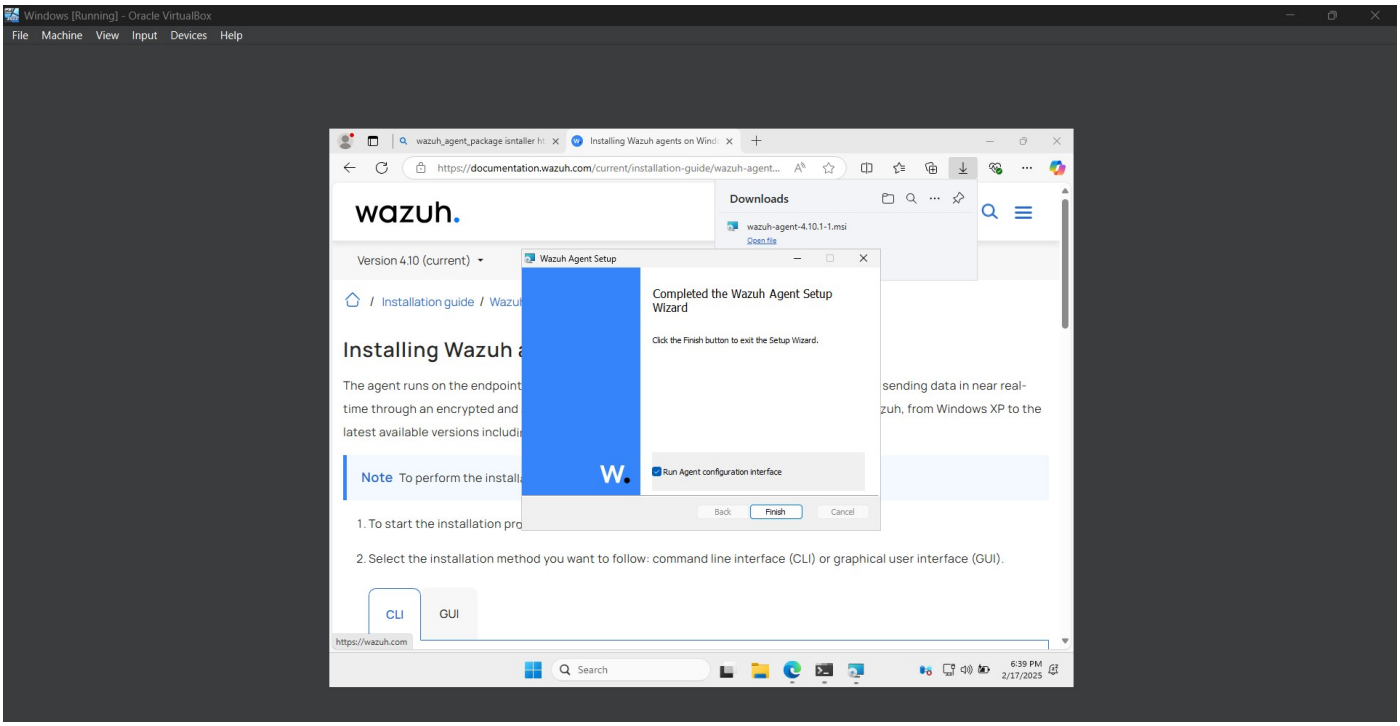




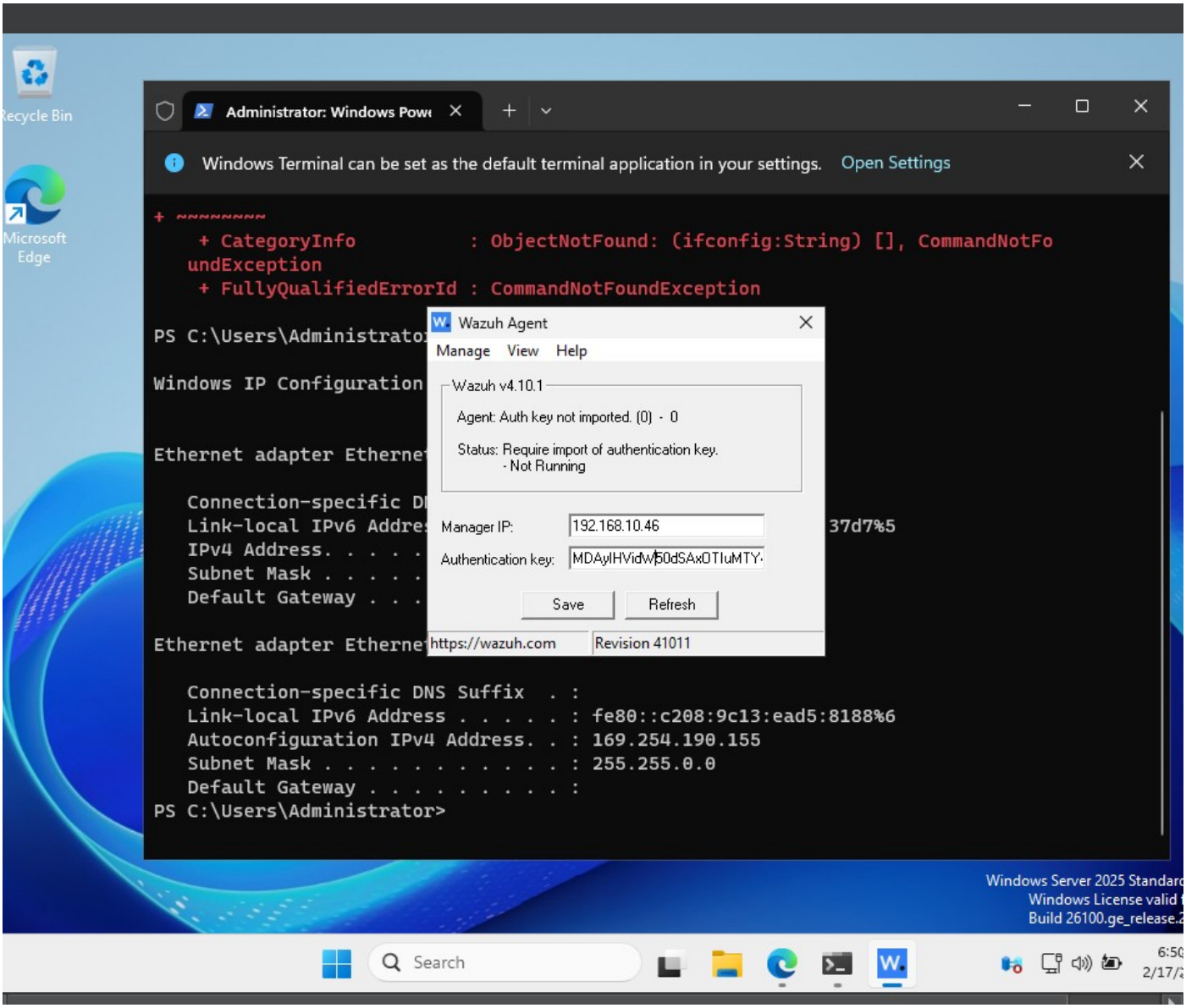
Installing the Wazuh Agent on the Endpoint

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

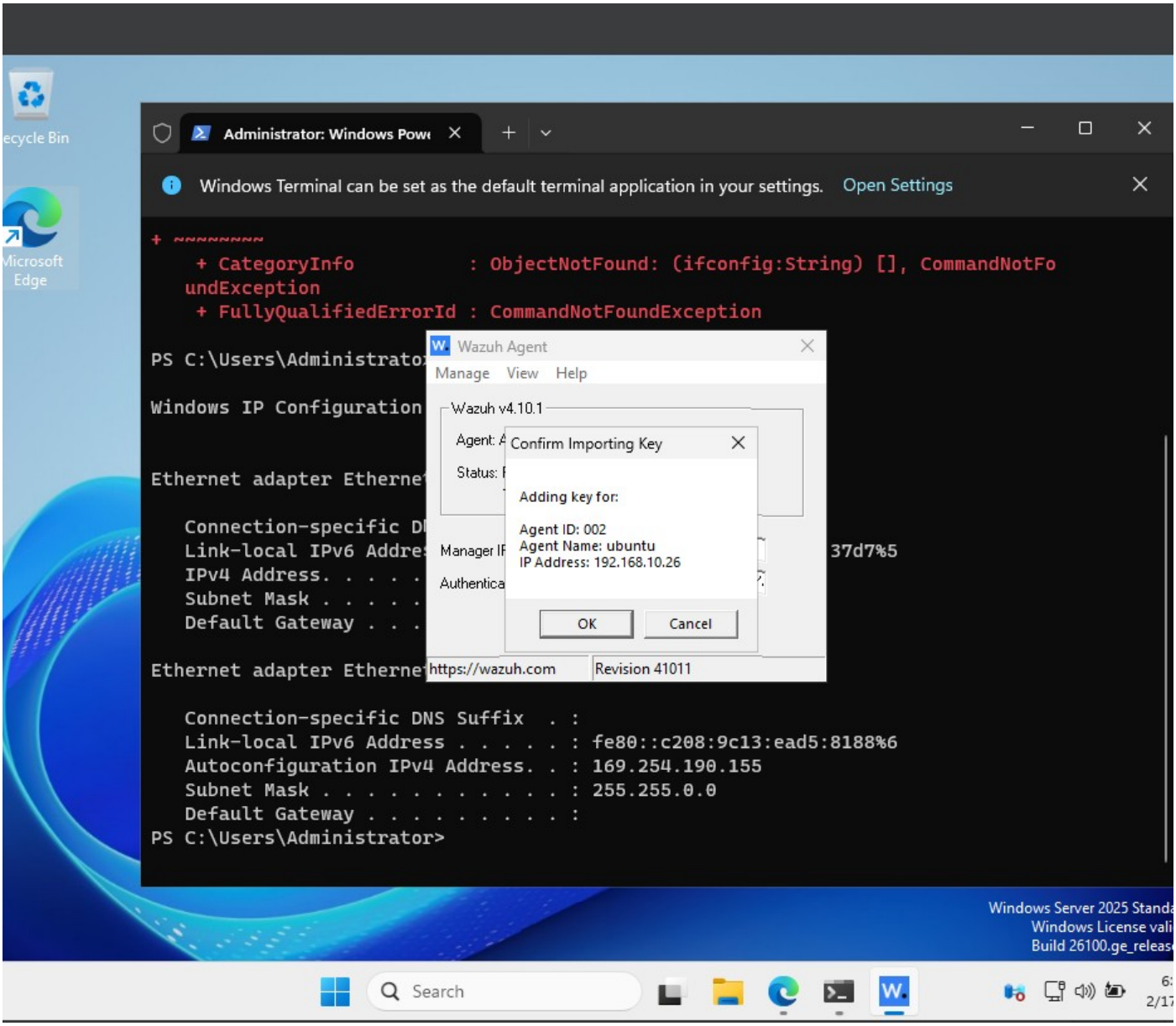




I copied the installer to the endpoint (HMI-1) and followed the instructions to install the agent. After installation, I ran the agent configuration interface, entered the Security Onion server's IP address (*192.168.10.46*), and pasted the agent key.



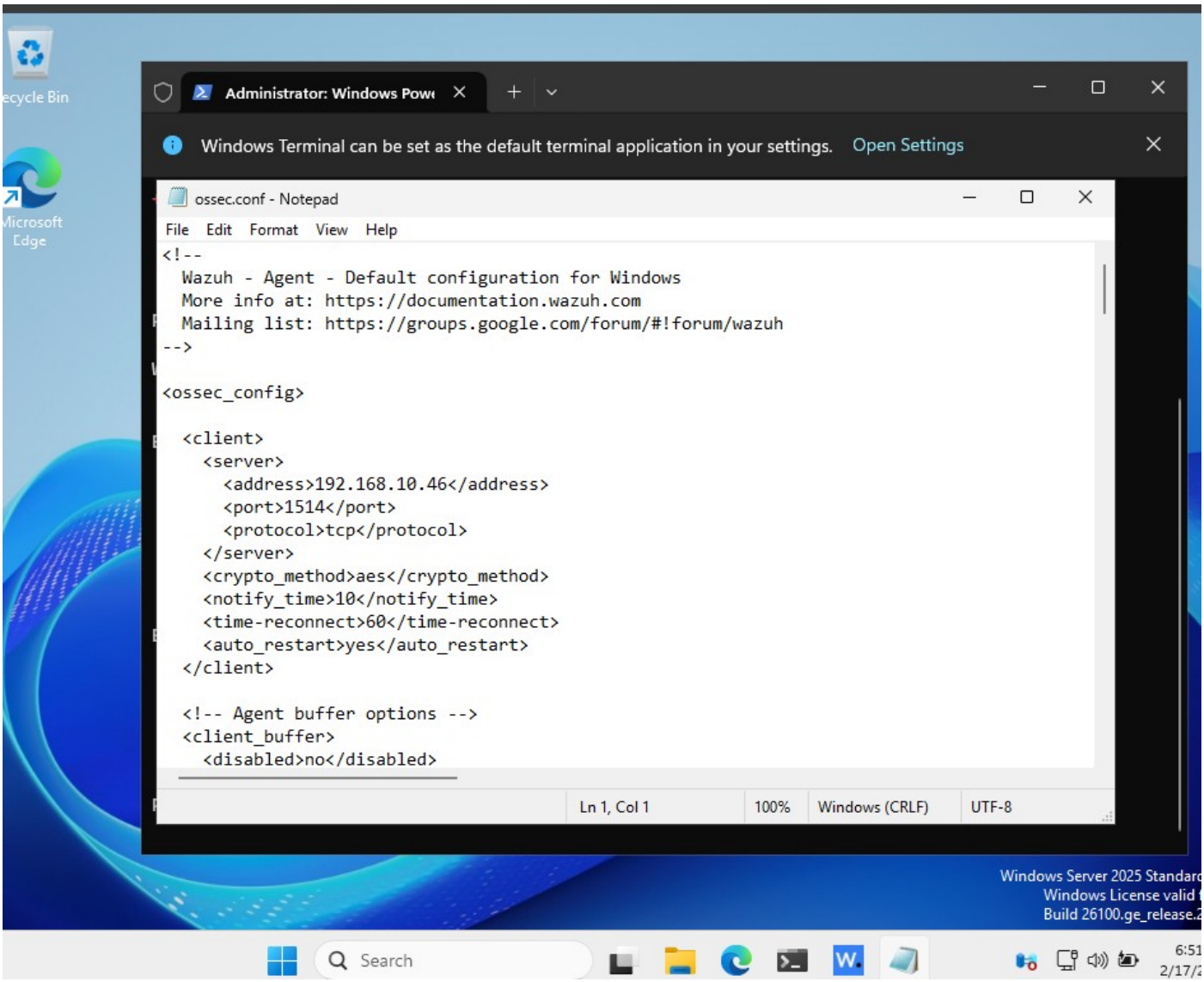
I confirmed that the agent was correctly registered and displayed the correct hostname and IP address.

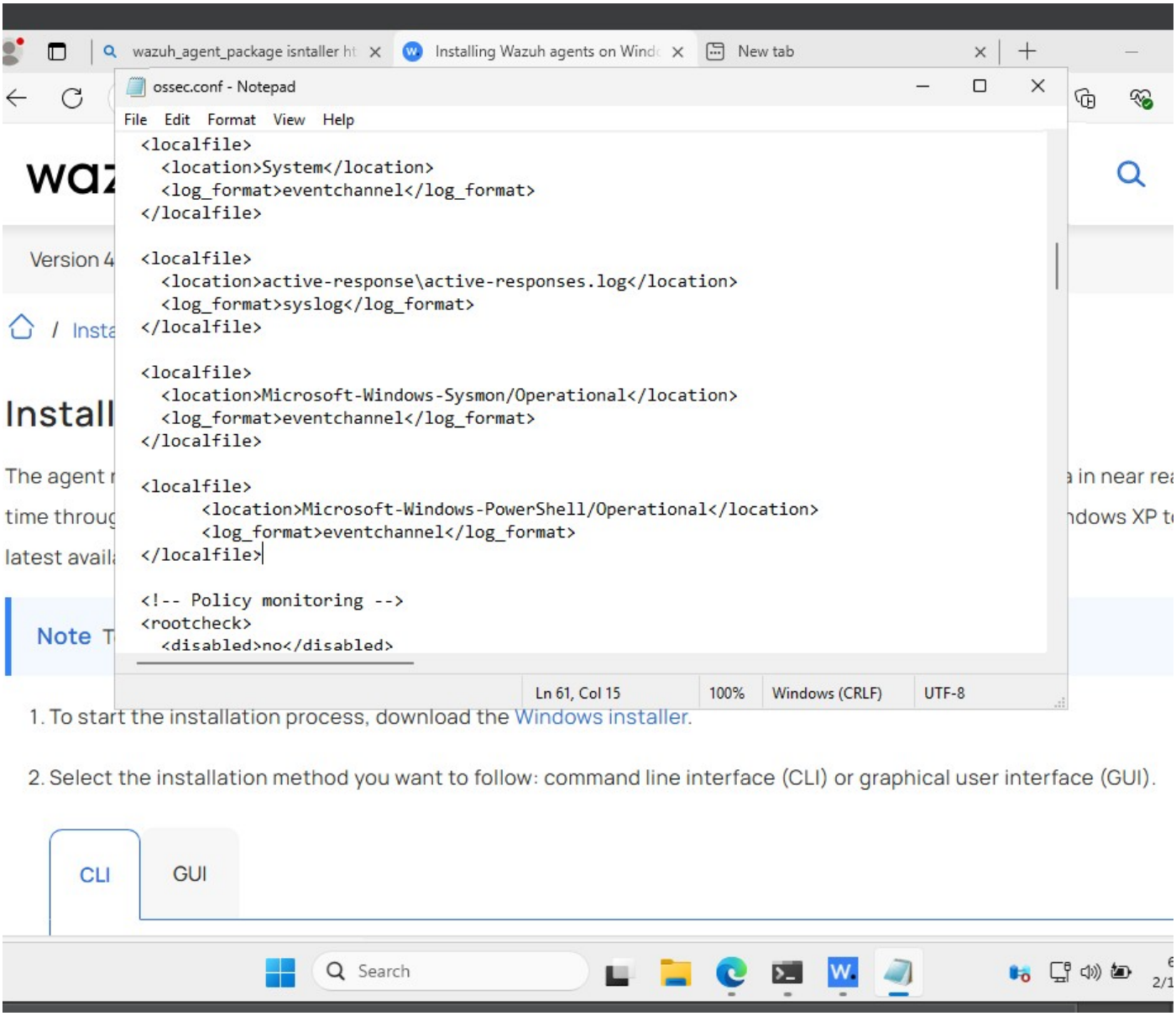


Opened ossec.conf file and added the following configuration into the file

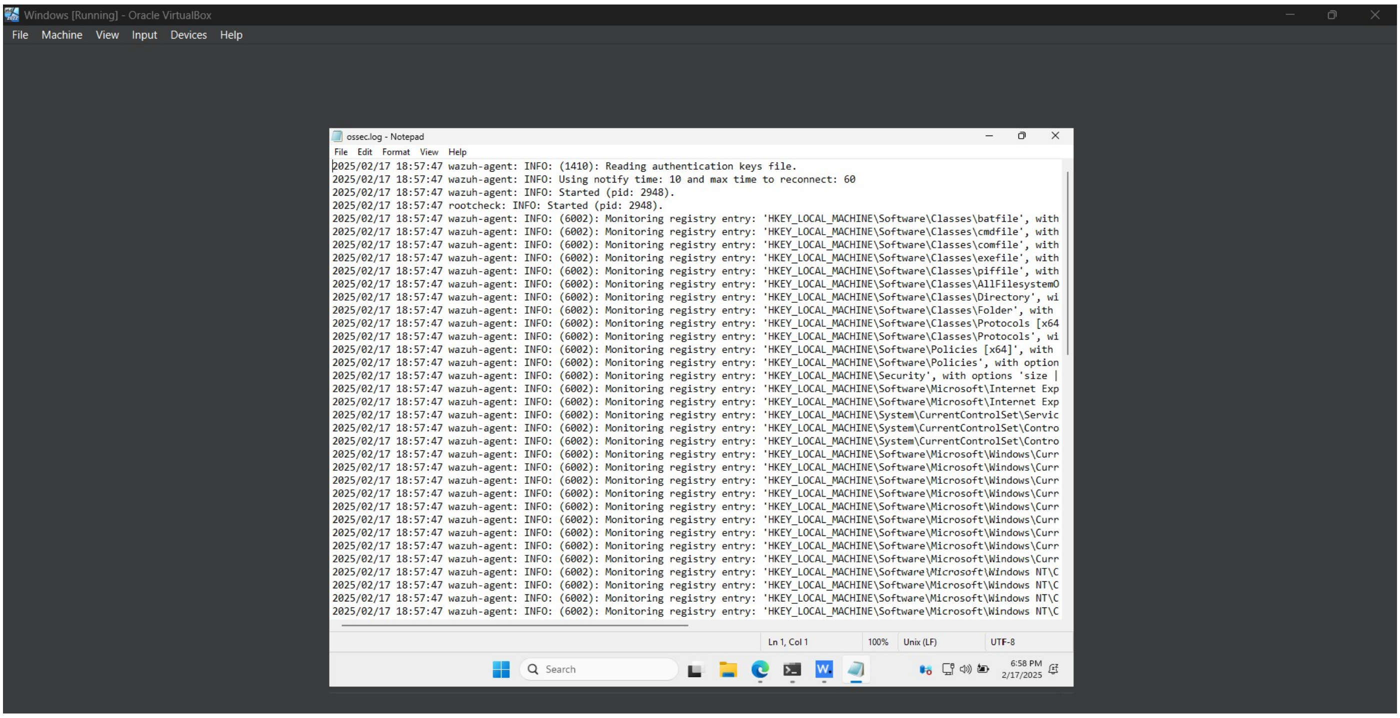
```
<localfile>
      <location>Microsoft-Windows-Sysmon/Operational</location>
      <log_format>eventchannel</log_format>
</localfile>
<localfile>
      <location>Microsoft-Windows-PowerShell/Operational</location>
      <log_format>eventchannel</log_format>
</localfile>
<localfile>
      <location>PowerShellCore/Operational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

Saved the file and restarted the wazuh agent with new configuration

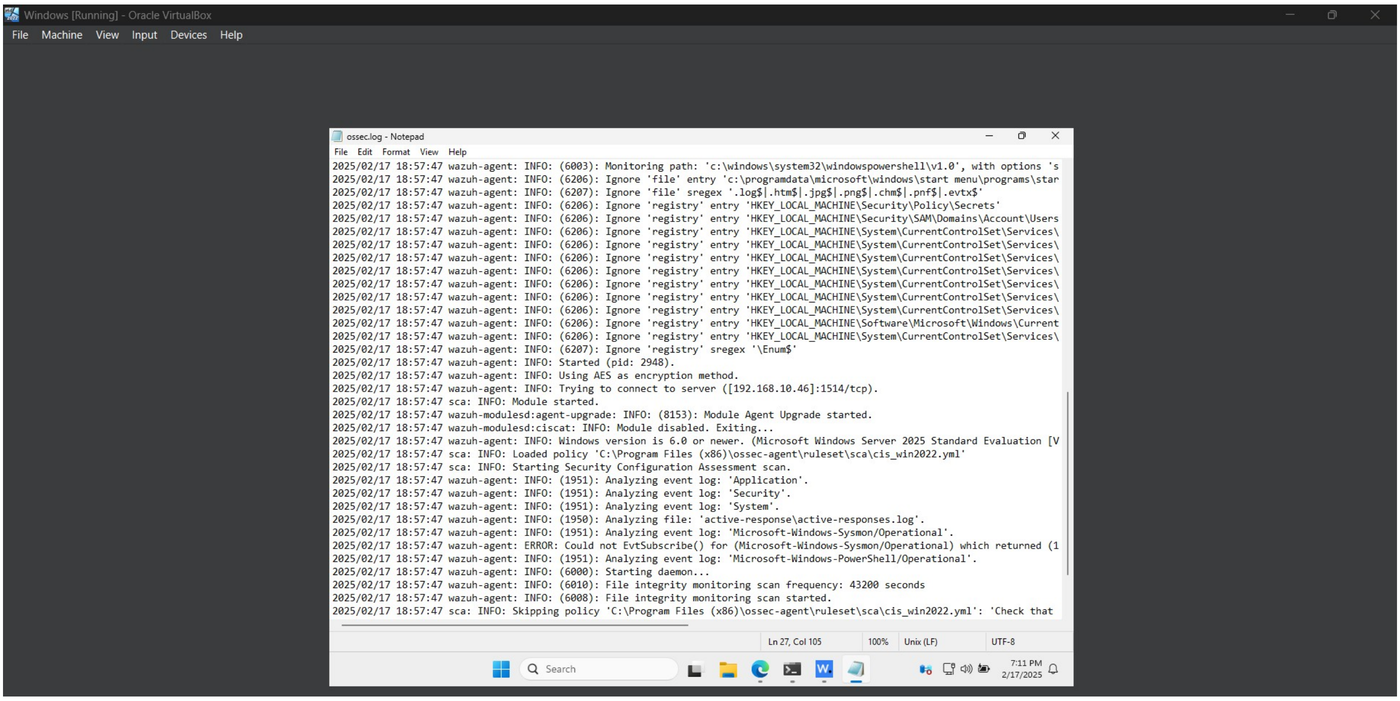

Administrator: Windows Powe
Windows Terminal can be set as the default terminal application in your settings.
Open Settings
ossec.conf - Notepad
File Edit Format View Help
<!--
Wazuh - Agent - Default configuration for Windows
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->
<ossec_config>
<client>
<server>
<address>192.168.10.46</address>
<port>1514</port>
<protocol>tcp</protocol>
</server>
<crypto_method>aes</crypto_method>
<notify_time>10</notify_time>
<time-reconnect>60</time-reconnect>
<auto_restart>yes</auto_restart>
</client>
<!-- Agent buffer options -->
<client_buffer>
<disabled>no</disabled>
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
Windows Server 2025 Standard
Windows License valid
Build 26100.ge_release.2
Search



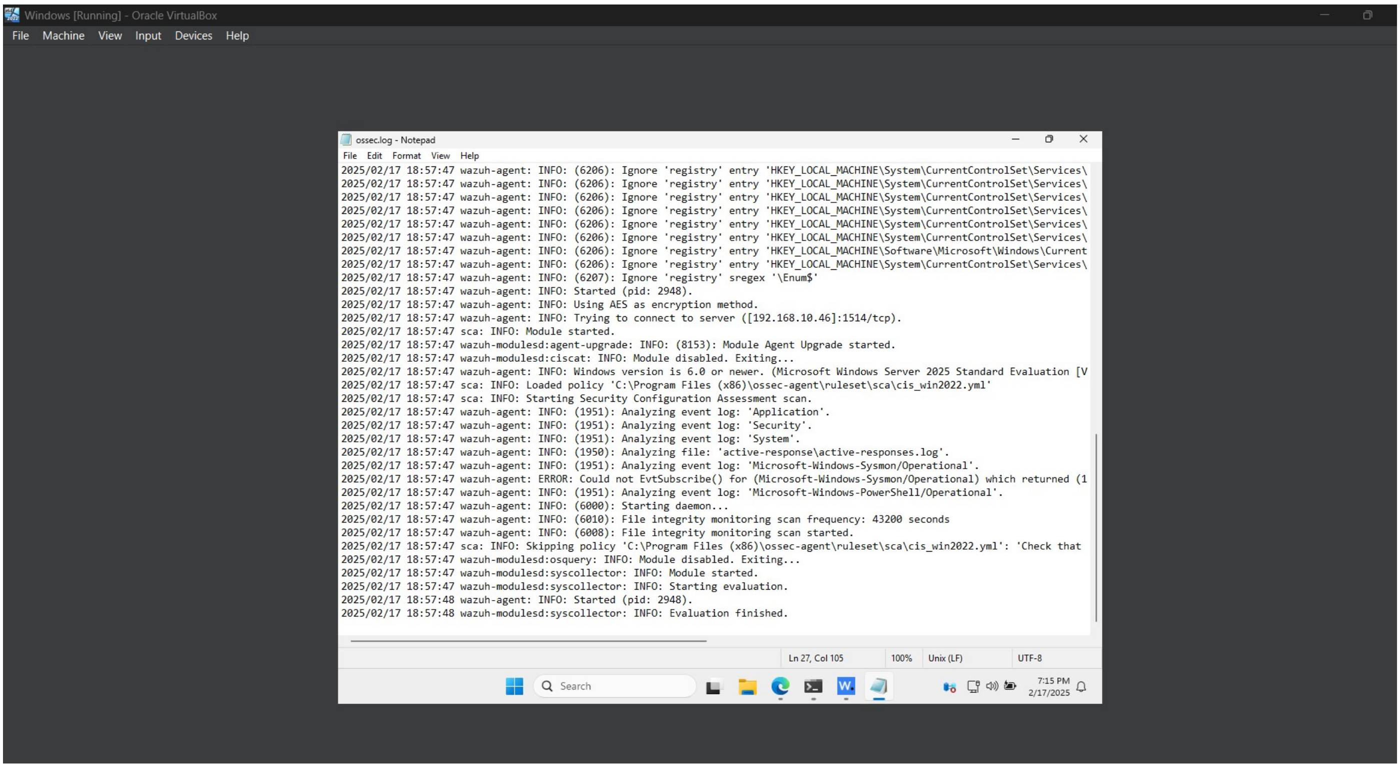
There were no errors occurred in the log file.



```
2025/02/17 18:57:47 wazuh-agent: INFO: (1410): Reading authentication keys file.
2025/02/17 18:57:47 wazuh-agent: INFO: Using notify time: 10 and max time to reconnect: 60
2025/02/17 18:57:47 wazuh-agent: INFO: Started (pid: 2948).
2025/02/17 18:57:47 rootcheck: INFO: Started (pid: 2948).
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\batfile', with
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\cmdfile', with
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\comfile', with
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\exefile', with
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\piffile', with
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\AllFilesystemO
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\Directory', wi
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\Folder', with
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\Protocols [x64
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\Protocols', wi
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Policies [x64]', with
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Policies', with option
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Security', with options 'size |
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Exp
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Exp
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Servic
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contro
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contro
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curr
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\C
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\C
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\C
2025/02/17 18:57:47 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\C
```



```
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: (6206): Ignore 'file' entry 'c:\programdata\microsoft\windows\start menu\programs\star
2025/02/17 18:57:47 wazuh-agent: INFO: (6207): Ignore 'file' sregex '.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.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 sca: INFO: Module started.
2025/02/17 18:57:47 wazuh-modulesd:agent-upgrade: INFO: (8153): Module Agent Upgrade started.
2025/02/17 18:57:47 wazuh-modulesd:ciscat: 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
```


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\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 sca: INFO: Module started.
2025/02/17 18:57:47 wazuh-modulesd:agent-upgrade: INFO: (8153): Module Agent Upgrade started.
2025/02/17 18:57:47 wazuh-modulesd:ciscat: 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-modulesd:osquery: INFO: Module disabled. Exiting...
2025/02/17 18:57:47 wazuh-modulesd:syscollector: INFO: Module started.
2025/02/17 18:57:47 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2025/02/17 18:57:48 wazuh-agent: INFO: Started (pid: 2948).
2025/02/17 18:57:48 wazuh-modulesd:syscollector: INFO: Evaluation finished.
Ln 27, Col 105
100%
Unix (LF)
UTF-8
Search
7:15 PM
2/17/2025