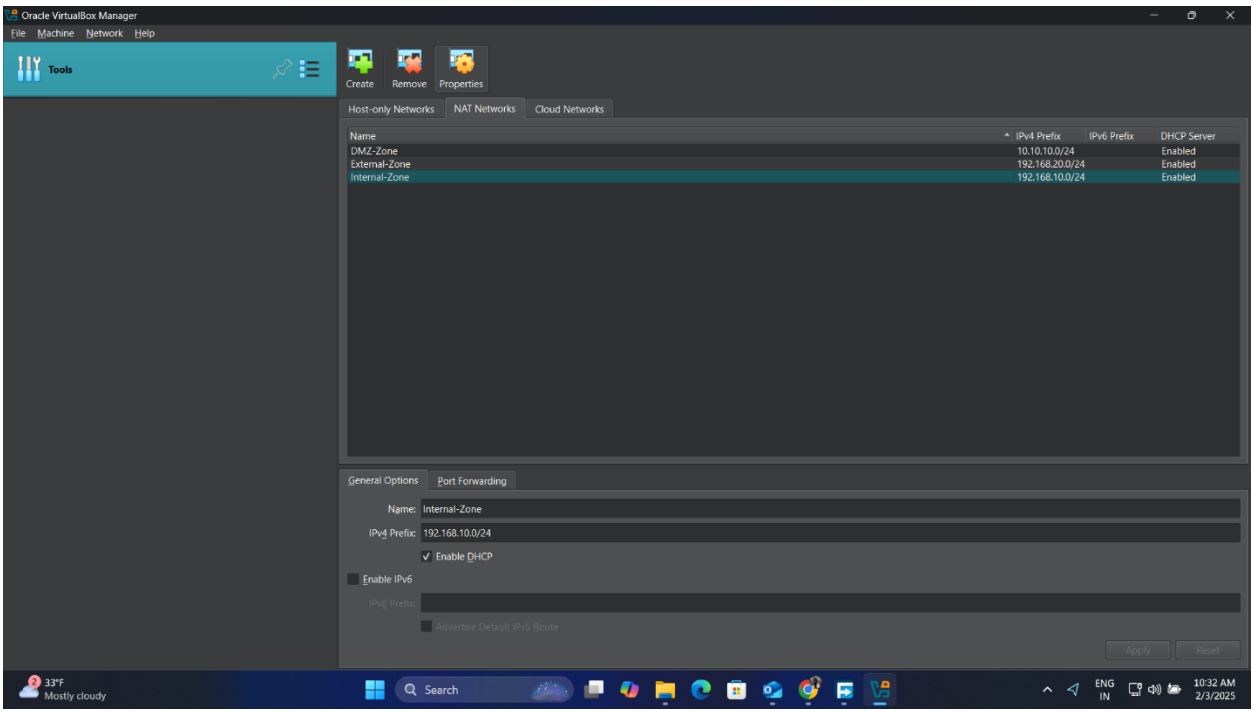
Name : Phanindhar Reddy Karnati **Reg.no**: 001667635

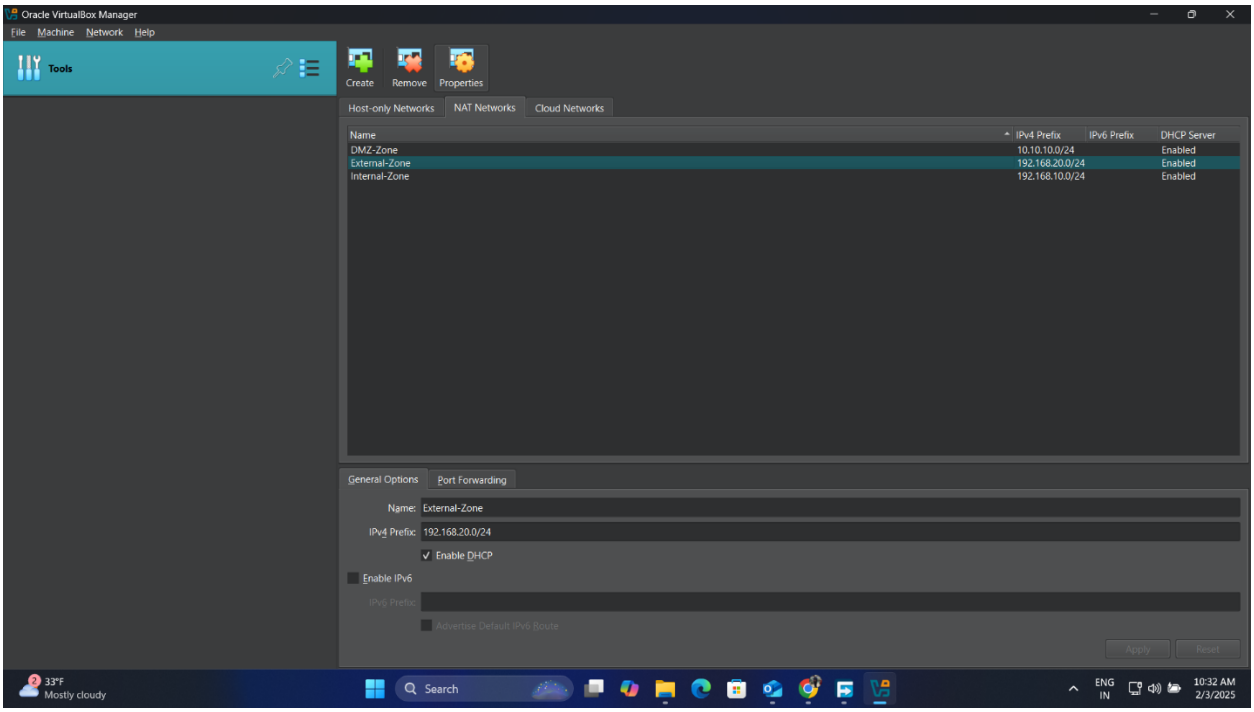
LAB -0, Virtual Box Lab Setup

- I have Created **NAT Networks** in Virtual Machines.

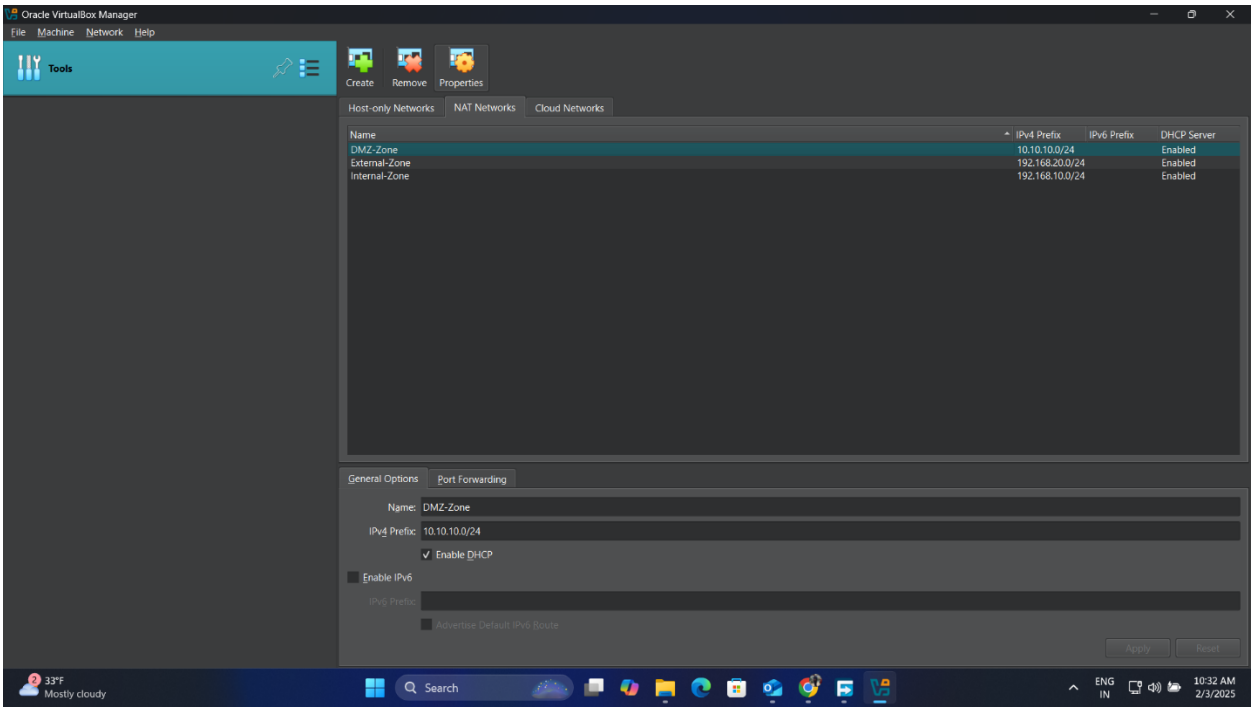
- Internal Zone:



External Zone:



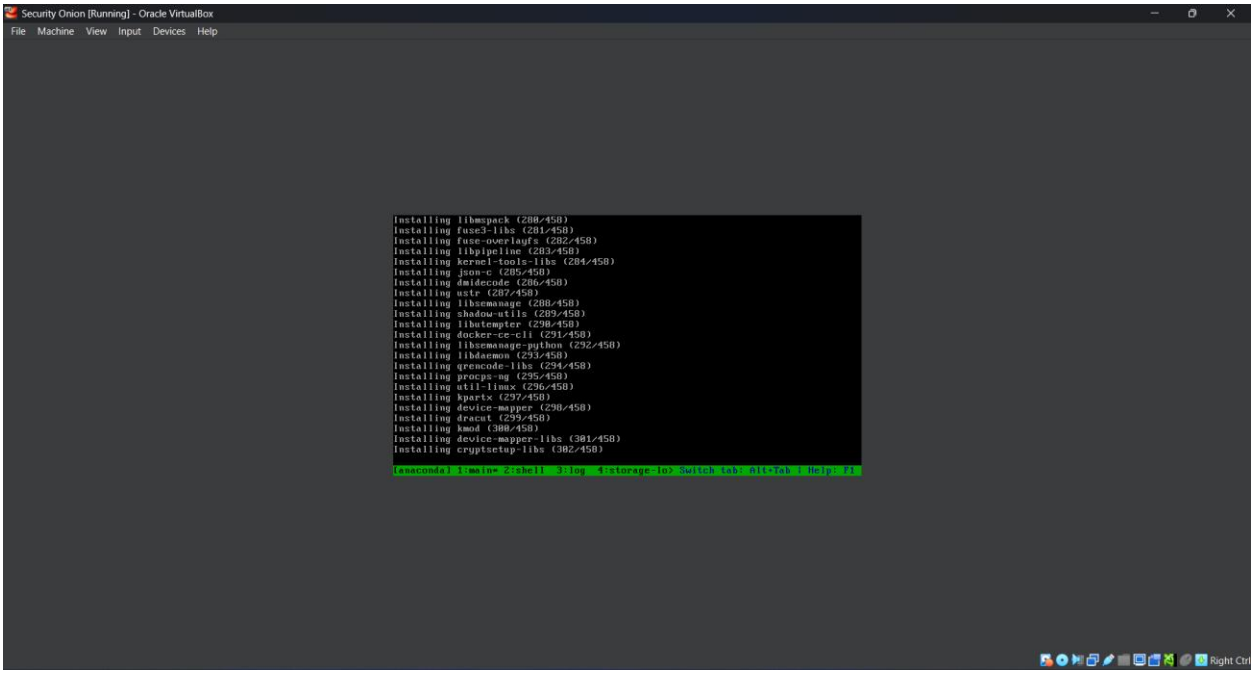
DMZ Zone:

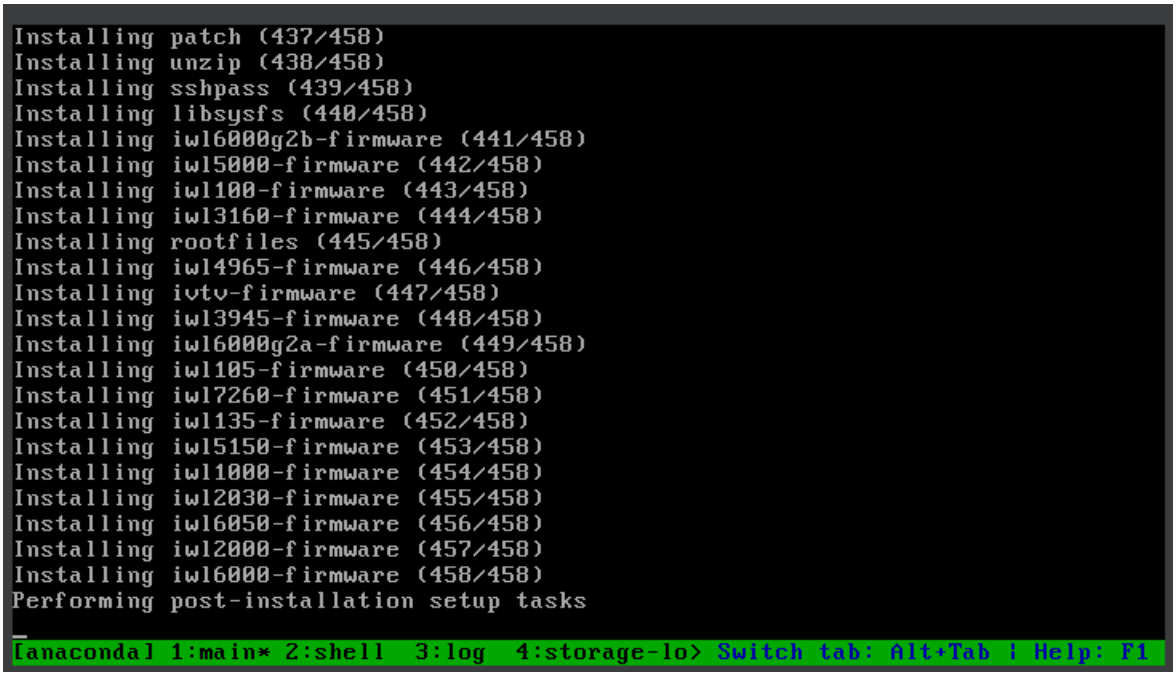


LAB 1: Setting up and Configuring Security Onion:

Introduction

I deployed and installed a Security Onion VM for this lab. The setup is the foundation for security monitoring, and I will be greatly dependent on its analytics and search functionality throughout the semester for threat-hunting labs.





Objective 1: Installing the Security Onion VM

I downloaded the latest version of the Security Onion appliance from the official website to start with. After downloading the ISO file, I began with creating a brand new virtual machine inside VMware Workstation, doing the following adjustments:

Selected Linux (**CentOS 7 64-bit**) as the Operating System

.Named the VM

Allocated at least 100GB for the virtual disk

.Altered hardware settings for high performance

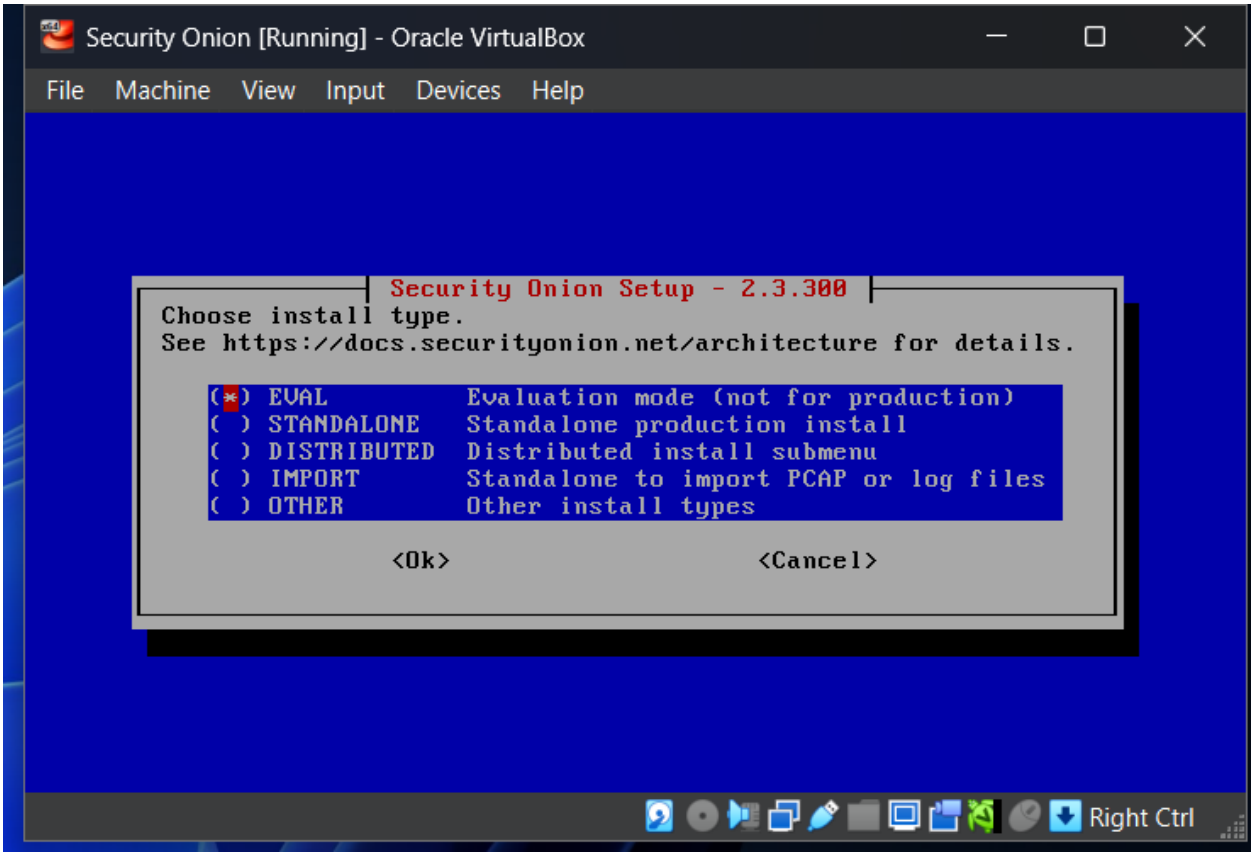
After I finished setting up the VM settings, I proceeded with the installation:

Powered on VM and clicked Install **Security Onion 2.3.21**.

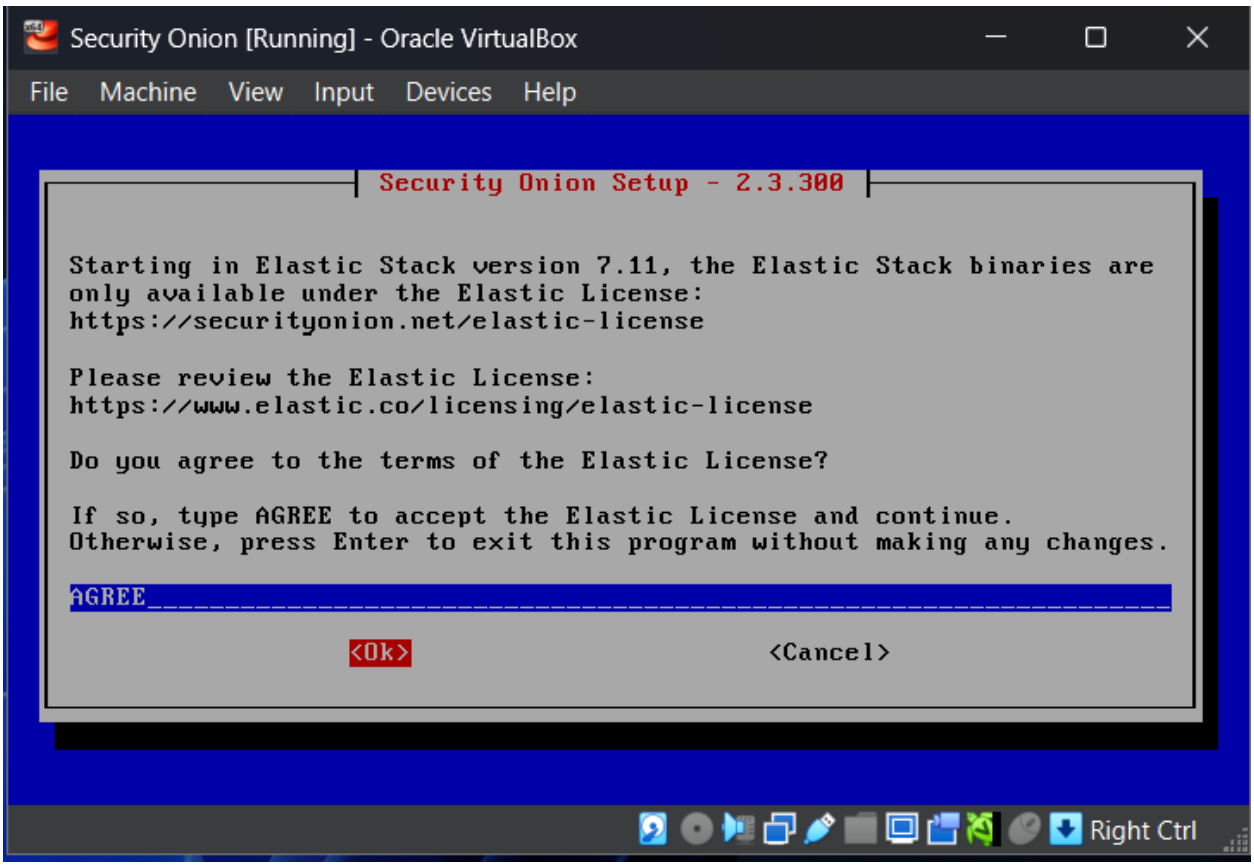
Confirmed that by typing yes, it will install OS and format the disk.

Set admin username and password.

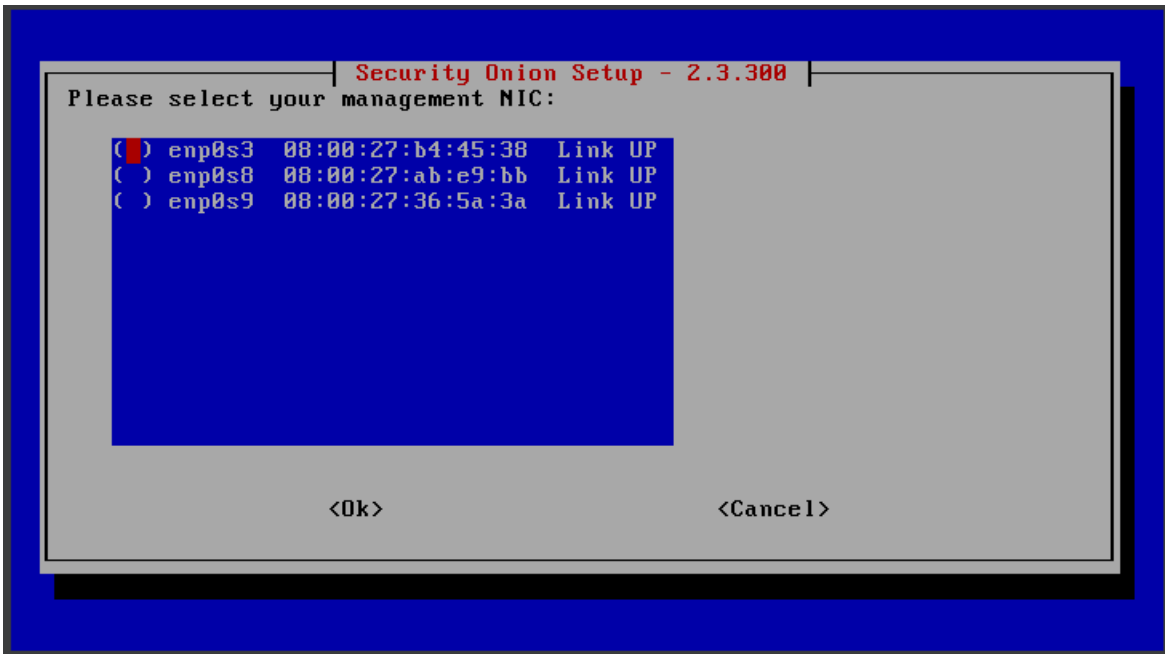
Installed, then r**ebooted** system.

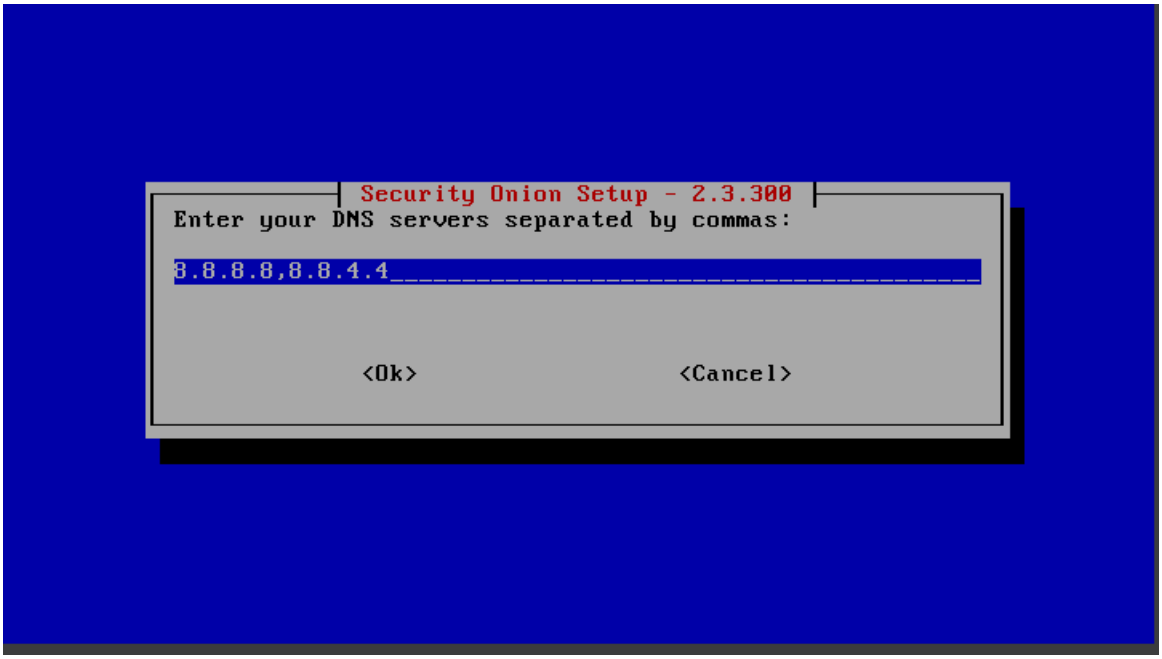


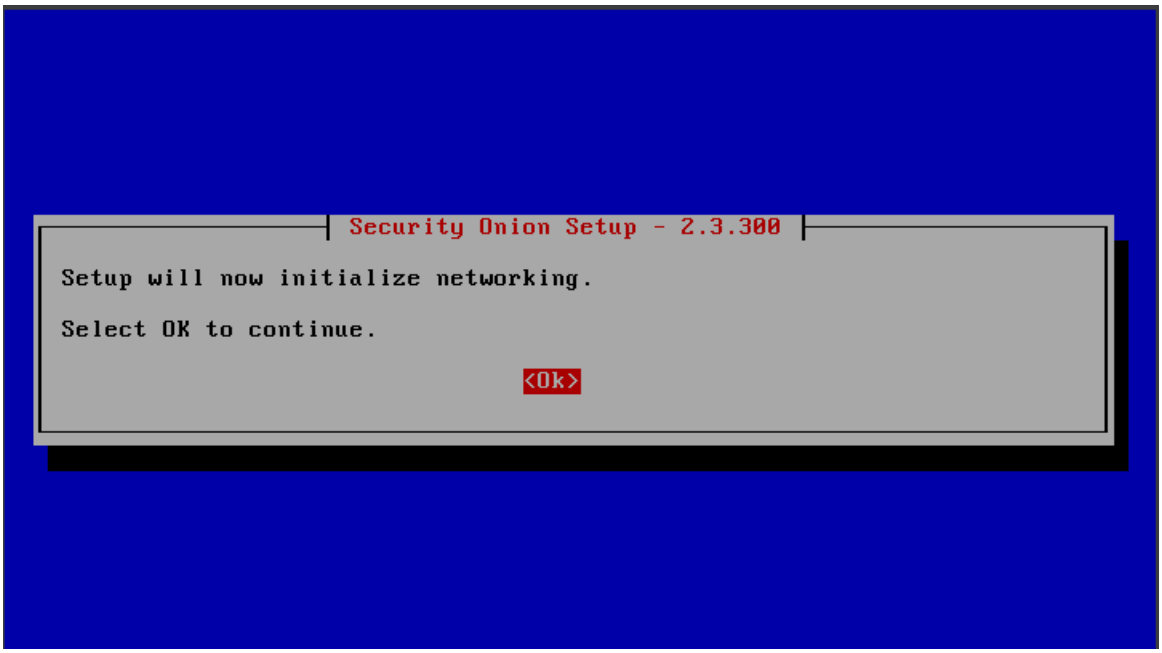
- Following **system reboot**, I installed Security Onion with **EVAL mode** for testing and a STANDARD install to allow updates. I have established a static IP address and configured network adapters: one for management and the other for monitoring the network.



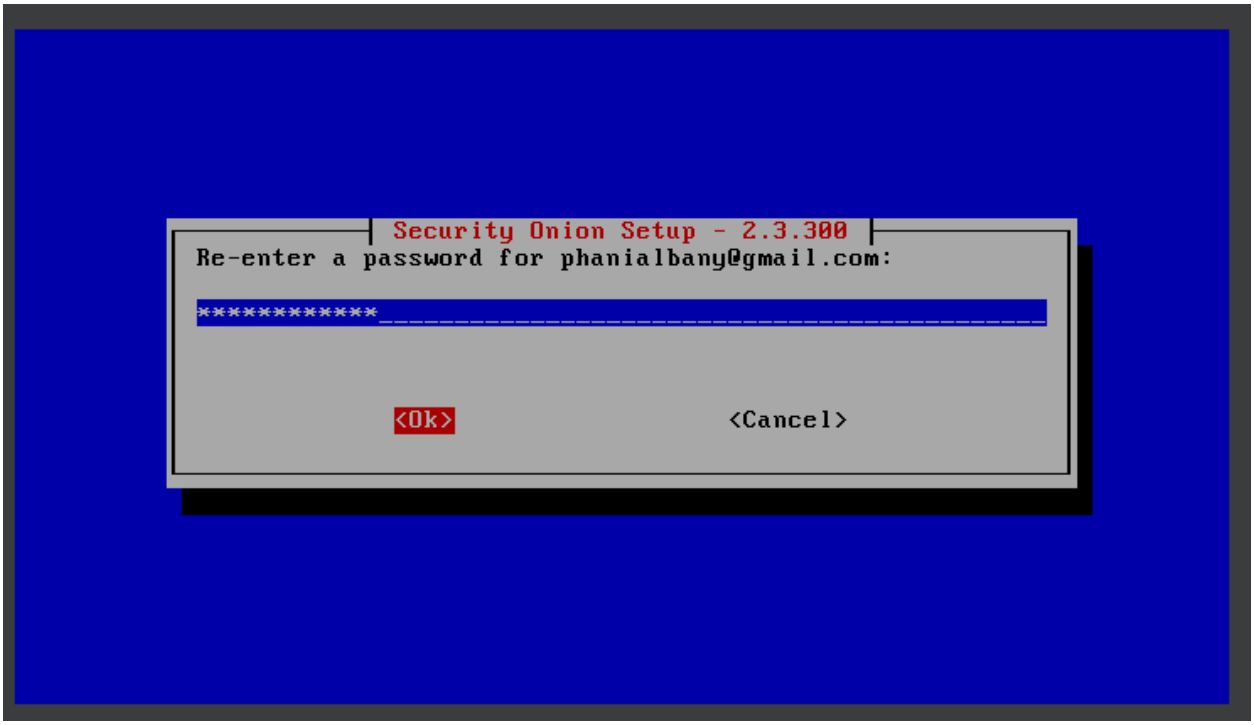
Finally, I set **HOME_NET** to define the range of the internal network **(192.168.10.0/24)** and selected default components to install. The system was completely ready for use after a final restart.


Security Onion Setup - 2.3.300
Please select your management NIC:
( ) enp0s3 08:00:27:b4:45:38 Link UP
( ) enp0s8 08:00:27:ab:e9:bb Link UP
( ) enp0s9 08:00:27:36:5a:3a Link UP
<Ok>
<Cancel>


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 Setup - 2.3.300
Setup will now initialize networking.
Select OK to continue.
<Ok>


Security Onion Setup - 2.3.300
The management IP could not be determined. Please check the log at /root/sosetup.log and verify the network configuration. Press OK to exit.
<Ok>

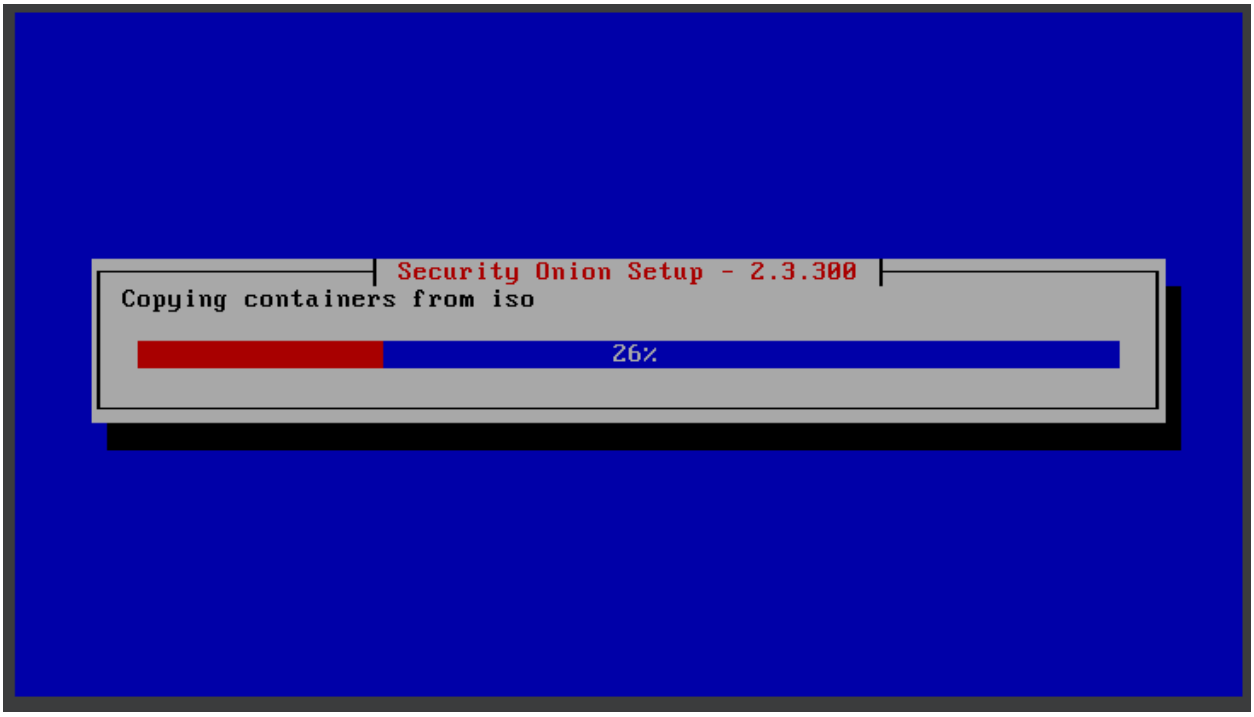

Security Onion Setup - 2.3.300
Re-enter a password for phanialbany@gmail.com:
****
<Ok>
<Cancel>

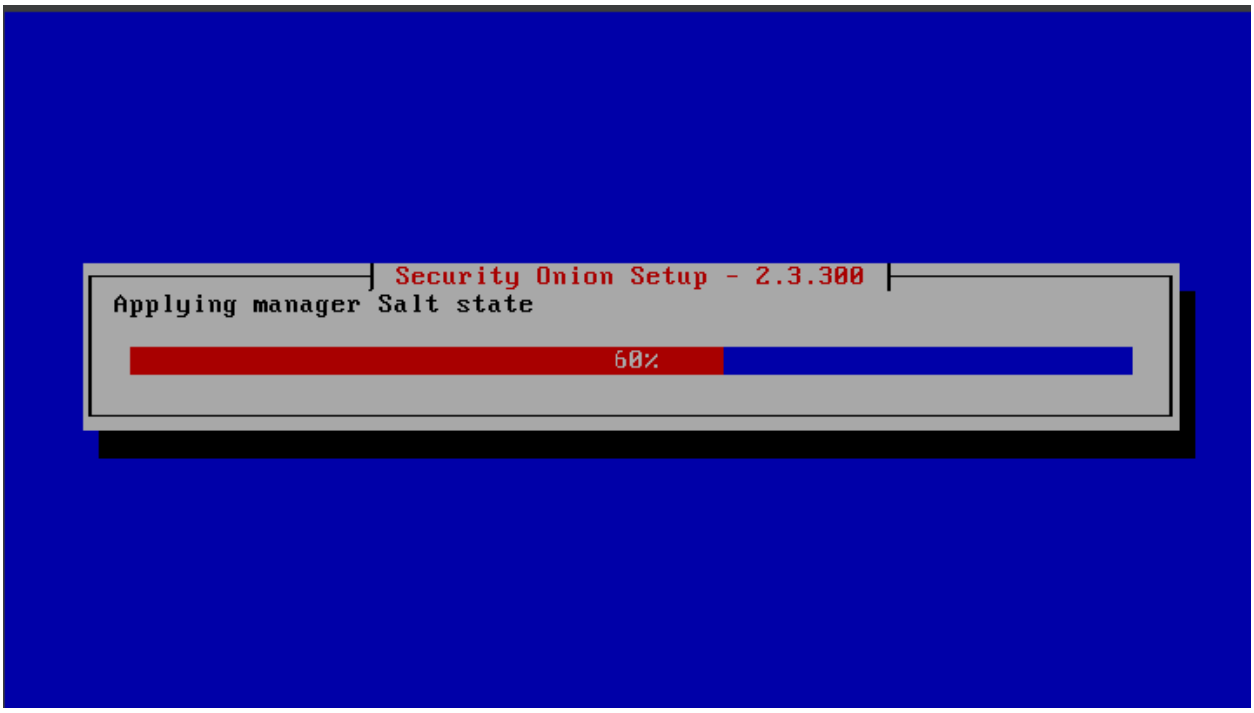
```
The following options have been set, would you like to proceed?

Security Onion Version: 2.3.300
Node Type: EVAL
Hostname: securityonionphani
Network: STATIC
Management NIC: enp0s3
Management IP: 192.168.10.1
Gateway: 192.168.10.2
DNS: 8.8.8.8 8.8.4.4
DNS Domain: searchdomain.local
Proxy: N/A
Bond NIC(s):
Home Network(s):
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/12
Access URL: https://192.168.10.1
Allowed IP or Subnet: 192.168.10.0/24
Web User: phanialbany@gmail.com

                    <Yes>                    <No>
```

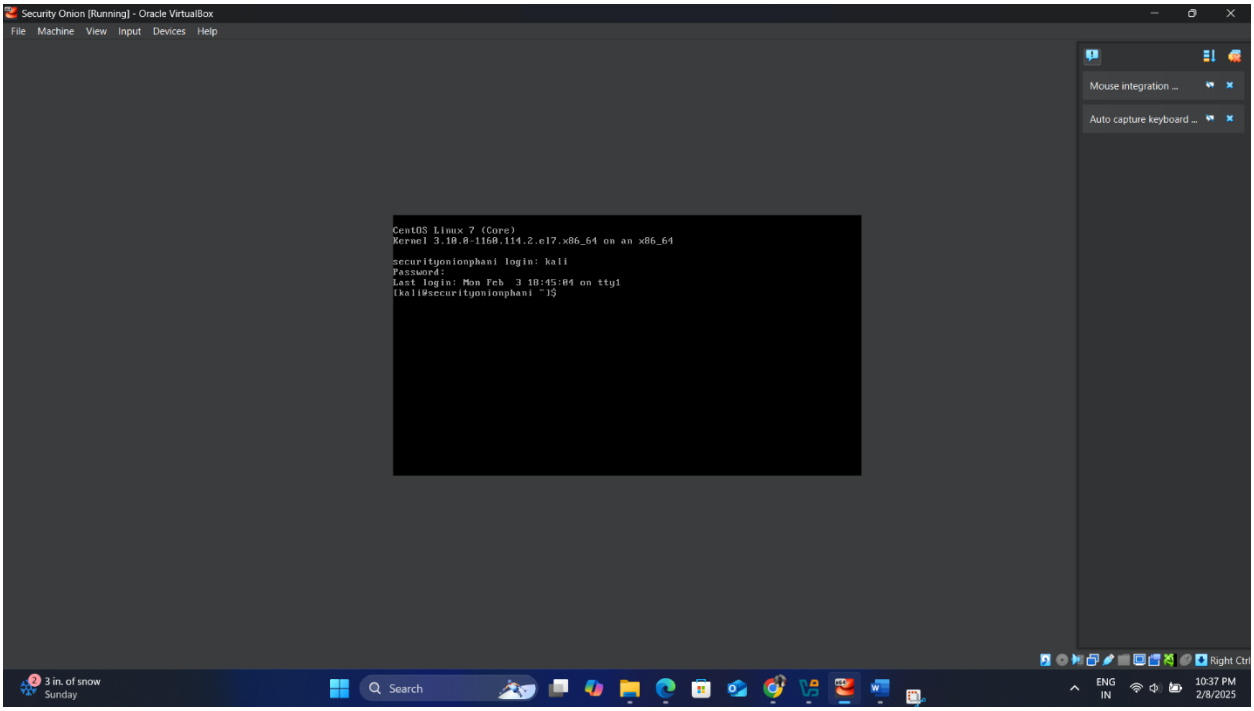
```
The following options have been set, would you like to proceed?

Web User: phanialbany@gmail.com
Fleet User: phanialbany@gmail.com
Enabled Optional Components:
  - GRAFANA
  - OSQUERY
  - WAZUH
  - PLAYBOOK
  - STRELKA
Metadata Tool: ZEEK
IDS Ruleset: ETOPEN
Patch Schedule:
  Type: auto
OS Package Updates: Open
NTP Servers:
  - 0.pool.ntp.org
  - 1.pool.ntp.org
Elasticsearch Heap Size: 2669m
Elasticsearch Storage Space: 35GB

                    <Yes>                    <No>
```

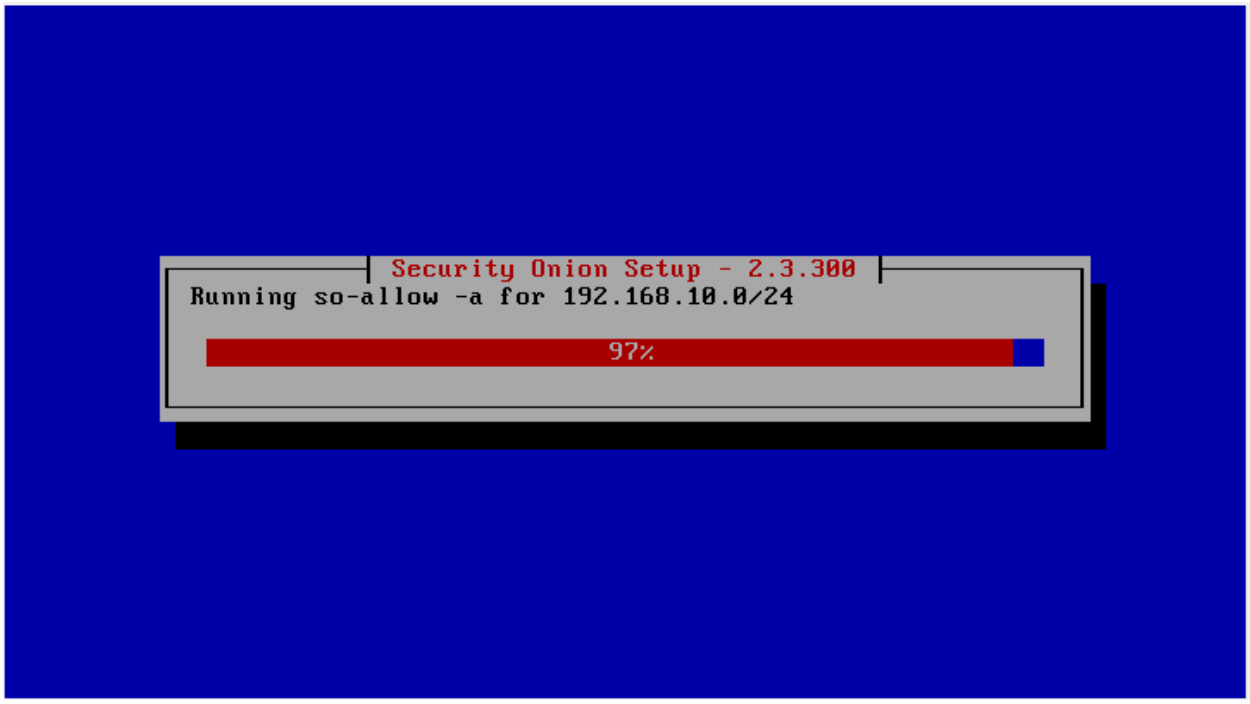
```
The following options have been set, would you like to proceed?

  - PLAYBOOK
  - STRELKA
Metadata Tool: ZEEK
IDS Ruleset: ETOPEN
Patch Schedule:
  Type: auto
OS Package Updates: Open
NTP Servers:
  - 0.pool.ntp.org
  - 1.pool.ntp.org
Elasticsearch Heap Size: 2669m
Elasticsearch Storage Space: 35GB
Logstash Heap Size: 700m
Logstash Worker Count: 125
Logstash Batch Size: 125
Logstash Input Threads: 1

Press TAB to select yes or no.

                <Yes>                    <No>
```

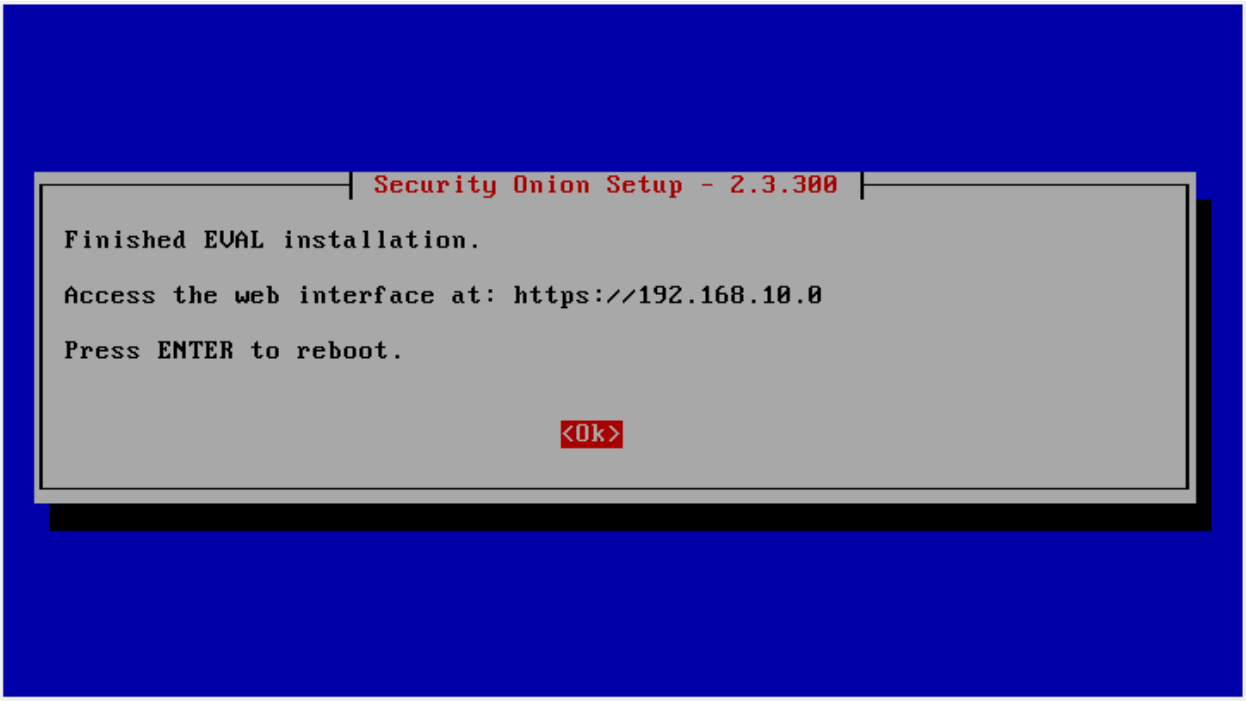
```
Security Onion Setup - 2.3.300
Running initial configuration steps

                    0%
```


Security Onion Setup - 2.3.300
Copying containers from iso
26%


Security Onion Setup - 2.3.300
Applying manager Salt state
60%


Security Onion [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.114.2.el7.x86_64 on an x86_64
securityonionphani login: kali
Password:
Last login: Mon Feb 3 10:45:04 on tty1
[kali@securityonionphani ~]$
Right Ctrl
3 in. of snow
Sunday
Search
ENG
IN
10:37 PM
2/8/2025


Security Onion Setup - 2.3.300
Running so-allow -a for 192.168.10.0/24
97%



Objective 2: Configuration of Security Onion

Installation of VMware Tools
For the purpose of increasing integration and compatibility between the VM and VMware Workstation, I installed VMware tools as follows:
commands:
- sudo yum update
- sudo yum install open-vm-tools-desktop fuse
- sudo reboot

After installation, I rebooted the VM so that the changes would take effect.

Security Onion [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
 iwl2030-firmware     noarch  18.168.6.1-83.el7_9            updates      246 k
 iwl3160-firmware     noarch  25.30.13.0-83.el7_9            updates      1.5 M
 iwl3945-firmware     noarch  15.32.2.9-83.el7_9             updates       97 k
 iwl4965-firmware     noarch  228.61.2.24-83.el7_9           updates      110 k
 iwl5000-firmware     noarch  8.83.5.1_1-83.el7_9            updates      290 k
 iwl5150-firmware     noarch  8.24.2.2-83.el7_9              updates      152 k
 iwl6000-firmware     noarch  9.221.4.1-83.el7_9             updates      172 k
 iwl6000g2a-firmware  noarch  18.168.6.1-83.el7_9            updates      305 k
 iwl6000g2b-firmware  noarch  18.168.6.1-83.el7_9            updates      305 k
 iwl6050-firmware     noarch  41.28.5.1-83.el7_9              updates      242 k
 iwl7260-firmware     noarch  25.30.13.0-83.el7_9            updates       14 M
 kernel-tools         x86_64  3.10.0-1160.119.1.el7          updates      8.2 M
 kernel-tools-libs    x86_64  3.10.0-1160.119.1.el7          updates      8.1 M
 less                 x86_64  458-10.el7_9                   updates      120 k
 linux-firmware       noarch  20200421-83.git78c0348.el7_9   updates       80 M
 python-perf          x86_64  3.10.0-1160.119.1.el7          updates      8.2 M
 wazuh-agent          x86_64  4.9.2-1                        wazuh4_repo   10 M

Transaction Summary
================================================================================
Install   1 Package
Upgrade  39 Packages

Total download size: 209 M
Is this ok [y/d/N]:
```

```
  iwl1000-firmware.noarch 1:39.31.5.1-83.el7_9
  iwl105-firmware.noarch 0:18.168.6.1-83.el7_9
  iwl135-firmware.noarch 0:18.168.6.1-83.el7_9
  iwl2000-firmware.noarch 0:18.168.6.1-83.el7_9
  iwl2030-firmware.noarch 0:18.168.6.1-83.el7_9
  iwl3160-firmware.noarch 0:25.30.13.0-83.el7_9
  iwl3945-firmware.noarch 0:15.32.2.9-83.el7_9
  iwl4965-firmware.noarch 0:228.61.2.24-83.el7_9
  iwl5000-firmware.noarch 0:8.83.5.1_1-83.el7_9
  iwl5150-firmware.noarch 0:8.24.2.2-83.el7_9
  iwl6000-firmware.noarch 0:9.221.4.1-83.el7_9
  iwl6000g2a-firmware.noarch 0:18.168.6.1-83.el7_9
  iwl6000g2b-firmware.noarch 0:18.168.6.1-83.el7_9
  iwl6050-firmware.noarch 0:41.28.5.1-83.el7_9
  iwl7260-firmware.noarch 0:25.30.13.0-83.el7_9
  kernel-tools.x86_64 0:3.10.0-1160.119.1.el7
  kernel-tools-libs.x86_64 0:3.10.0-1160.119.1.el7
  less.x86_64 0:458-10.el7_9
  linux-firmware.noarch 0:20200421-83.git78c0348.el7_9
  python-perf.x86_64 0:3.10.0-1160.119.1.el7
  wazuh-agent.x86_64 0:4.9.2-1

Complete!
[kali@securityonionphani ~]$
[kali@securityonionphani ~]$ _
```

securityonio [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
#

[base]
name=CentOS-7 - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra
baseurl=http://vault.centos.org/centos/7/os/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://vault.centos.org/centos/7/os/x86_64/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-7 - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$inf
ra
baseurl=http://vault.centos.org/centos/7/os/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://vault.centos.org/centos/7/os/x86_64/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-7 - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infr
a
baseurl=http://vault.centos.org/centos/7/os/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://vault.centos.org/centos/7/os/x86_64/RPM-GPG-KEY-CentOS-7


~
~
~
~
~
-- INSERT --                                                    11,1          Bot
```

```
 libusbx                    x86_64  1.0.21-1.el7                base       61 k
 libwayland-client          x86_64  1.15.0-1.el7                 base       33 k
 libwayland-cursor          x86_64  1.15.0-1.el7                 base       20 k
 libwayland-egl             x86_64  1.15.0-1.el7                 base       13 k
 libwayland-server          x86_64  1.15.0-1.el7                 base       39 k
 libxcb                     x86_64  1.13-1.el7                   base      214 k
 libxkbcommon               x86_64  0.7.1-3.el7                  base      108 k
 libxshmfence               x86_64  1.2-1.el7                    base      7.2 k
 mesa-libEGL                x86_64  18.3.4-12.el7_9              updates   110 k
 mesa-libGL                 x86_64  18.3.4-12.el7_9              updates   166 k
 mesa-libgbm                x86_64  18.3.4-12.el7_9              updates    39 k
 mesa-libglapi              x86_64  18.3.4-12.el7_9              updates    46 k
 pango                      x86_64  1.42.4-4.el7_7               base      280 k
 pangomm                    x86_64  2.40.1-1.el7                 base       58 k
 pixman                     x86_64  0.34.0-1.el7                 base      248 k
 rest                       x86_64  0.8.1-2.el7                  base       63 k
 xkeyboard-config           noarch  2.24-1.el7                   base      834 k

Transaction Summary
================================================================================
Install  1 Package (+76 Dependent packages)

Total download size: 29 M
Installed size: 92 M
Is this ok [y/d/N]: y_
```

```
  libproxy.x86_64 0:0.4.11-11.el7
  libsigc++20.x86_64 0:2.10.0-1.el7
  libsoup.x86_64 0:2.62.2-2.el7
  libthai.x86_64 0:0.1.14-9.el7
  libtiff.x86_64 0:4.0.3-35.el7
  libusbx.x86_64 0:1.0.21-1.el7
  libwayland-client.x86_64 0:1.15.0-1.el7
  libwayland-cursor.x86_64 0:1.15.0-1.el7
  libwayland-egl.x86_64 0:1.15.0-1.el7
  libwayland-server.x86_64 0:1.15.0-1.el7
  libxcb.x86_64 0:1.13-1.el7
  libxkbcommon.x86_64 0:0.7.1-3.el7
  libxshmfence.x86_64 0:1.2-1.el7
  mesa-libEGL.x86_64 0:18.3.4-12.el7_9
  mesa-libGL.x86_64 0:18.3.4-12.el7_9
  mesa-libgbm.x86_64 0:18.3.4-12.el7_9
  mesa-libglapi.x86_64 0:18.3.4-12.el7_9
  pango.x86_64 0:1.42.4-4.el7_7
  pangomm.x86_64 0:2.40.1-1.el7
  pixman.x86_64 0:0.34.0-1.el7
  rest.x86_64 0:0.8.1-2.el7
  xkeyboard-config.noarch 0:2.24-1.el7

Complete!
[kali@securityonionphani ~]$
```

```
  libsoup.x86_64 0:2.62.2-2.el7
  libthai.x86_64 0:0.1.14-9.el7
  libtiff.x86_64 0:4.0.3-35.el7
  libusbx.x86_64 0:1.0.21-1.el7
  libwayland-client.x86_64 0:1.15.0-1.el7
  libwayland-cursor.x86_64 0:1.15.0-1.el7
  libwayland-egl.x86_64 0:1.15.0-1.el7
  libwayland-server.x86_64 0:1.15.0-1.el7
  libxcb.x86_64 0:1.13-1.el7
  libxkbcommon.x86_64 0:0.7.1-3.el7
  libxshmfence.x86_64 0:1.2-1.el7
  mesa-libEGL.x86_64 0:18.3.4-12.el7_9
  mesa-libGL.x86_64 0:18.3.4-12.el7_9
  mesa-libgbm.x86_64 0:18.3.4-12.el7_9
  mesa-libglapi.x86_64 0:18.3.4-12.el7_9
  pango.x86_64 0:1.42.4-4.el7_7
  pangomm.x86_64 0:2.40.1-1.el7
  pixman.x86_64 0:0.34.0-1.el7
  rest.x86_64 0:0.8.1-2.el7
  xkeyboard-config.noarch 0:2.24-1.el7

Complete!
[kali@securityonionphani ~]$
[kali@securityonionphani ~]$ sudo reboot
[sudo] password for kali:
```

- Updating Suricata Rulesets

For current threat protection, I updated the Suricata rules using:

bash

Copy

Edit

sudo so-rule-update

This updated the ruleset and automatically restarted the Suricata engine.

```
  pango.x86_64 0:1.42.4-4.el7_7
  pangomm.x86_64 0:2.40.1-1.el7
  pixman.x86_64 0:0.34.0-1.el7
  rest.x86_64 0:0.8.1-2.el7
  xkeyboard-config.noarch 0:2.24-1.el7

Complete!
[kali@securityonion ~]$ sudo so-rule-update
[sudo] password for kali:
2025-02-14 21:46:32,566 - <INFO> - Loading ./rulecat.conf.
2025-02-14 21:46:32,610 - <INFO> - Forcing Suricata version to 6.0.
2025-02-14 21:46:32,648 - <INFO> - Fetching https://rules.emergingthreats.net/op
en/suricata-6.0.0/emerging.rules.tar.gz.
 100% - 4788642/4788642
2025-02-14 21:46:33,996 - <INFO> - Done.
2025-02-14 21:46:34,692 - <INFO> - Ignoring file rules/emerging-deleted.rules
2025-02-14 21:46:34,693 - <INFO> - Loading local file /opt/so/rules/nids/local.r
ules
2025-02-14 21:47:01,733 - <INFO> - Loaded 56315 rules.
2025-02-14 21:47:02,132 - <INFO> - Disabled 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Enabled 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Modified 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Dropped 0 rules.
2025-02-14 21:47:03,754 - <INFO> - Enabled 136 rules for flowbit dependencies.
_
```

```
  rest.x86_64 0:0.8.1-2.el7
  xkeyboard-config.noarch 0:2.24-1.el7

Complete!
[kali@securityonion ~]$ sudo so-rule-update
[sudo] password for kali:
2025-02-14 21:46:32,566 - <INFO> - Loading ./rulecat.conf.
2025-02-14 21:46:32,610 - <INFO> - Forcing Suricata version to 6.0.
2025-02-14 21:46:32,648 - <INFO> - Fetching https://rules.emergingthreats.net/op
en/suricata-6.0.0/emerging.rules.tar.gz.
 100% - 4788642/4788642
2025-02-14 21:46:33,996 - <INFO> - Done.
2025-02-14 21:46:34,692 - <INFO> - Ignoring file rules/emerging-deleted.rules
2025-02-14 21:46:34,693 - <INFO> - Loading local file /opt/so/rules/nids/local.r
ules
2025-02-14 21:47:01,733 - <INFO> - Loaded 56315 rules.
2025-02-14 21:47:02,132 - <INFO> - Disabled 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Enabled 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Modified 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Dropped 0 rules.
2025-02-14 21:47:03,754 - <INFO> - Enabled 136 rules for flowbit dependencies.
2025-02-14 21:48:07,621 - <INFO> - Writing rules to /opt/so/rules/nids/all.rules
: total: 56315; enabled: 42054; added: 31; removed 0; modified: 1163
2025-02-14 21:48:08,413 - <INFO> - Done.
[kali@securityonion ~]$ _
```

Sudo so-rule-update:

```
2025-02-14 21:46:34,693 - <INFO> - Loading local file /opt/so/rules/nids/local.r
ules
2025-02-14 21:47:01,733 - <INFO> - Loaded 56315 rules.
2025-02-14 21:47:02,132 - <INFO> - Disabled 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Enabled 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Modified 0 rules.
2025-02-14 21:47:02,132 - <INFO> - Dropped 0 rules.
2025-02-14 21:47:03,754 - <INFO> - Enabled 136 rules for flowbit dependencies.
2025-02-14 21:48:07,621 - <INFO> - Writing rules to /opt/so/rules/nids/all.rules
: total: 56315; enabled: 42054; added: 31; removed 0; modified: 1163
2025-02-14 21:48:08,413 - <INFO> - Done.
[kali@securityonion ~]$ sudo so-user-add web-pac@ot-domain.local
Enter new password:
Password does not meet the minimum requirements
[kali@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 minu
tes...
Successfully added new user to SOC
Successfully added user to Fleet
Successfully updated Fleet user password
[kali@securityonion ~]$
[kali@securityonion ~]$
```

web-pac@ot-domain.local

```
Migrating roles to new file: /opt/so/conf/soc/soc_users_roles
The following users have all been migrated with the super user role:
superuser:5dda9f81-9d2f-44d2-ba46-b3c0ce81a793
Syncing users and roles between SOC and Elastic...
Elastic state will be re-applied to affected minions. This may take several minu
tes...
/sbin/so-user: line 290: /opt/so/log/soc/sync.log: No such file or directory
/sbin/so-user: line 291: /opt/so/log/soc/sync.log: No such file or directory
Successfully added new user to SOC
[kali@securityonionphani ~]$ sudo so-allow
[sudo] password for kali:

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

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

Please enter your selection:
```

- Adding a Web Portal User

For managing the Security Onion web page, I created a web portal user using:

bash

Copy

Edit

Command:

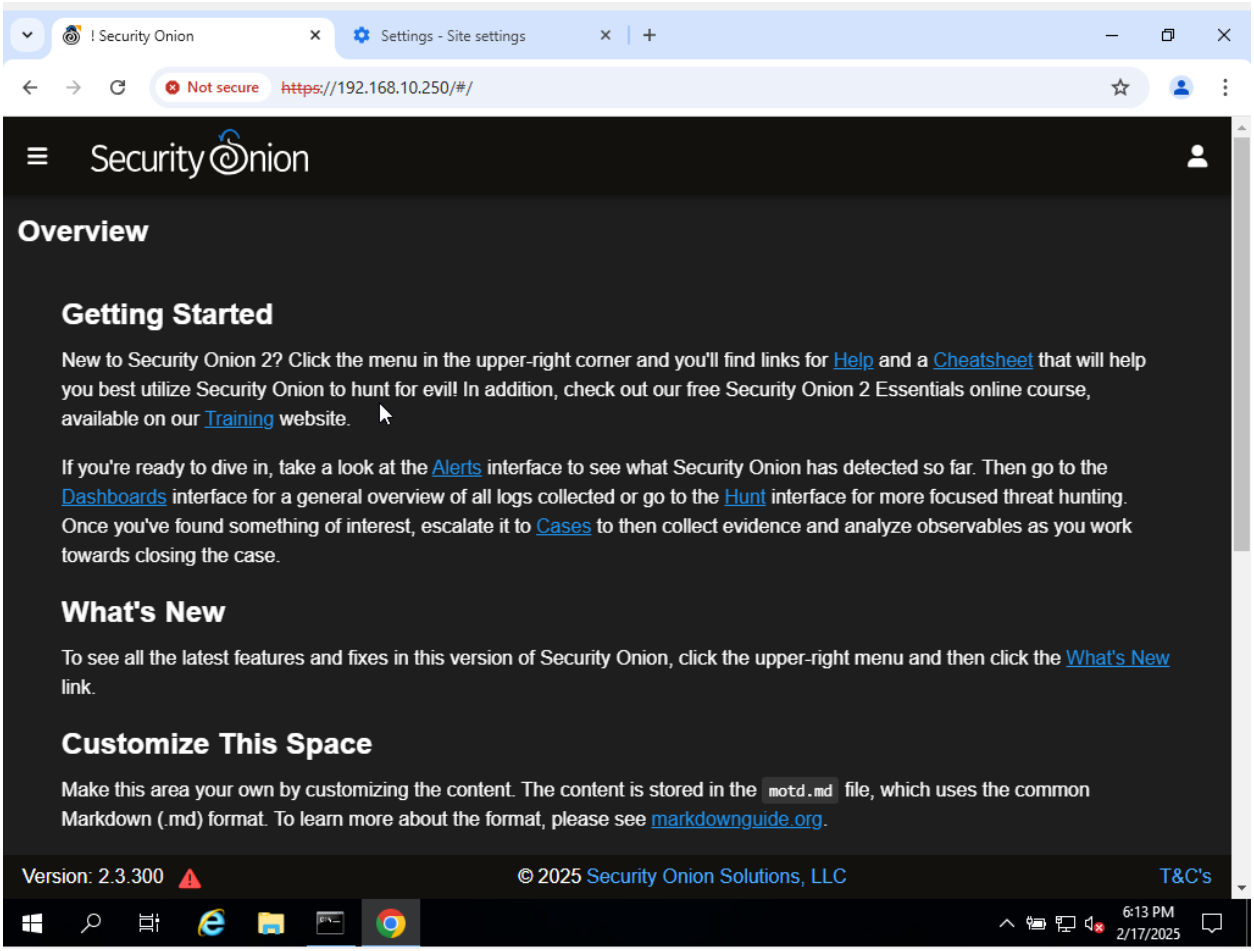
- sudo so-user-add web-pac@ot-domain.local

Once I've entered the needed credentials, I was successfully able to add the user and access the Security Onion web portal.

```
Elastic state will be re-applied to affected minions. This may take several minu
tes...
/sbin/so-user: line 290: /opt/so/log/soc/sync.log: No such file or directory
/sbin/so-user: line 291: /opt/so/log/soc/sync.log: No such file or directory
Successfully added new user to SOC
[kali@securityonionphani ~]$ sudo so-allow
[sudo] password for kali:

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

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

Please enter your selection: w
Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 1
72.25.100.0/24
Adding 172.25.100.0/24 to the wazuh_agent role. This can take a few seconds...
[kali@securityonionphani ~]$ _
```

```
     Changes:
              ----------
              new:
                  /opt/so/rules/hids/local_rules.xml
----------
          ID: /opt/so/rules/hids/ruleset
    Function: file.symlink
      Result: True
     Comment: Created new symlink /opt/so/rules/hids/ruleset -> /nsm/wazuh/rules
et
     Started: 05:53:16.718977
    Duration: 1.505 ms
     Changes:
              ----------
              new:
                  /opt/so/rules/hids/ruleset

Summary for local
------------
Succeeded: 19 (changed=19)
Failed:     1
------------
Total states run:     20
Total run time:  172.080 s
[kali@securityonionphani ~]$ _
```

```
              ----------
              new:
                  /opt/so/rules/hids/ruleset

Summary for local
------------
Succeeded: 19 (changed=19)
Failed:     1
------------
Total states run:     20
Total run time:  172.080 s
[kali@securityonionphani ~]$ sudo so-wazuh-agent-manage
[sudo] password for kali:


****************************************
* 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).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```



Objective 3: Installing Wazuh Agents

Activating Wazuh Agent Communication

To activate communication of the Wazuh agents with the Security Onion appliance,

I entered:

- **sudo so-allow**

Then I selected the **Wazuh agent** – **Port 1514/tcp/udp** option and typed in network range **192.168.10.0/24** for giving access.

```
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R 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: HMI-2
   * The IP Address of the new agent: 172.25.100.220
Confirm adding it?(y/n): y
Agent added with ID 001.


****************************************
* 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).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: _
```

Registration of a Wazuh Agent

In order to register a Wazuh agent, I entered:

Command:

sudo so-wazuh-agent-manage

Within the agent management terminal, I:

Selected A (Add an agent)

Entered the agent's hostname and IP address

Confirmed the addition

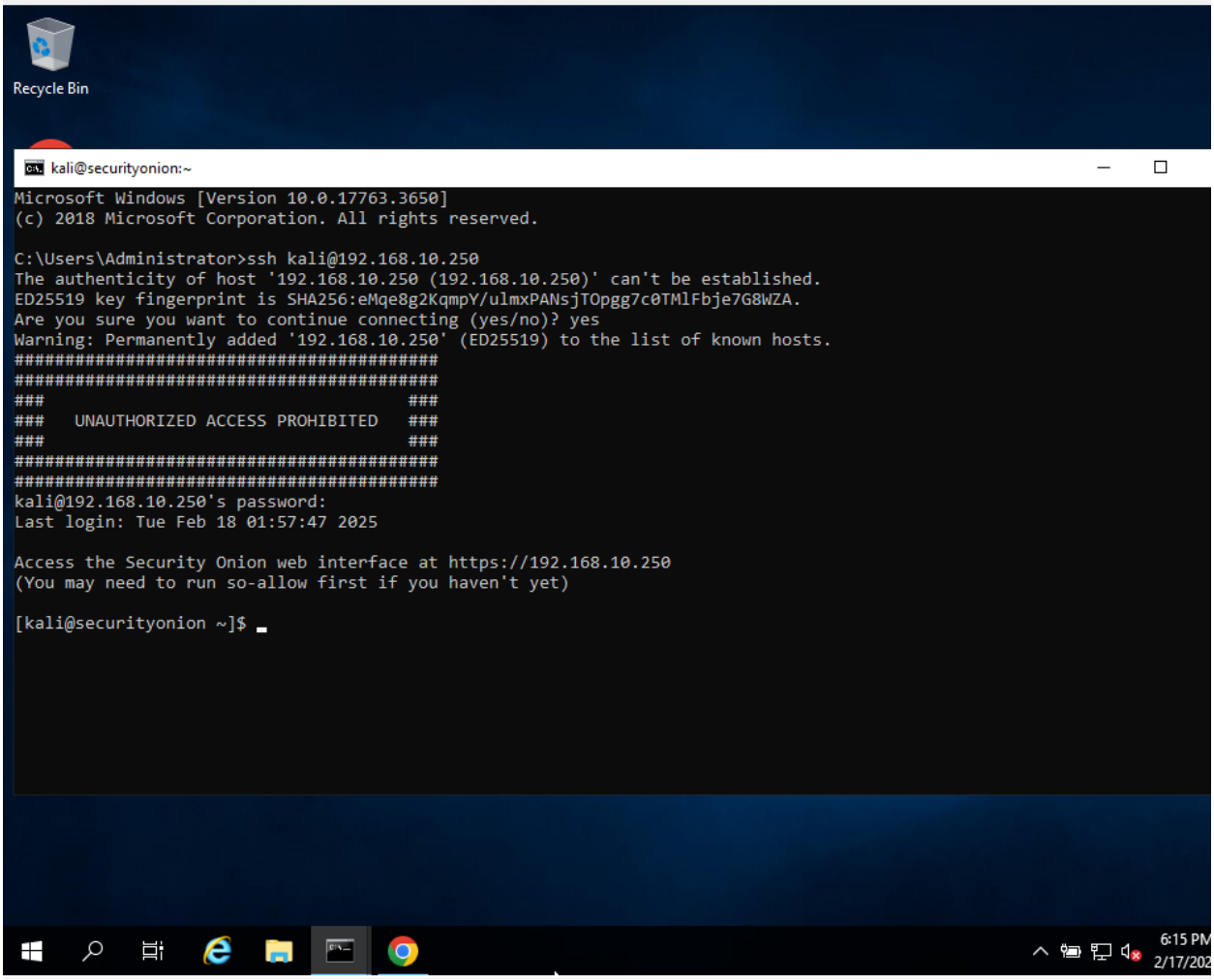
I then extracted the agent key using:

Command- **sudo so-wazuh-agent-manage**

I selected E (Extract key for an agent) and recorded the generated key for later use.

```
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R 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: IND-SecurityOnionv2
   * The IP Address of the new agent: 172.25.100.250
Confirm adding it?(y/n): y
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).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

```
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: HMI-2, IP: 172.25.100.220
   ID: 002, Name: IND-SecurityOnionv2, IP: 172.25.100.250
Provide the ID of the agent to extract the key (or '\q' to quit): 2

Agent key information for '002' is:
MDAyIE1ORC1TZWN1cml0eU9uaW9udjIgMTcyLjI1LjEwMC4yNTAgNzM5OWYyNTAxNGZkZWI3ODFiOWQy
YjY1ZjVkMmM2ZDU5ZTI4OTc4ZmQ1ZTZkY2E3YTljOTJkYjMzZWRkNTY5Yg==

** Press ENTER to return to the main menu.



****************************************
* 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).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: _
```


Recycle Bin
kali@securityonion:~
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ssh kali@192.168.10.250
The authenticity of host '192.168.10.250 (192.168.10.250)' can't be established.
ED25519 key fingerprint is SHA256:eMqe8g2KqmpY/ulmxPANsjTOpgg7c0TMlFbje7G8WZA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.250' (ED25519) to the list of known hosts.
##
##
###
UNAUTHORIZED ACCESS PROHIBITED
###
##
##
kali@192.168.10.250's password:
Last login: Tue Feb 18 01:57:47 2025
Access the Security Onion web interface at https://192.168.10.250
(You may need to run so-allow first if you haven't yet)
[kali@securityonion ~]$
6:15 PM
2/17/202

```
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R 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: windowsserver 2019

** Invalid name 'windowsserver 2019' given. Name must contain only alphanumeric characters (min=2, m
ax=32).

   * A name for the new agent: windowsserver2019
   * The IP Address of the new agent: 192.168.10.9
Confirm adding it?(y/n): y
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).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: securityonion, IP: 192.168.10.250
   ID: 002, Name: windowsserver2019, IP: 192.168.10.9
Provide the ID of the agent to extract the key (or '\q' to quit):
```

Installing and Configuring Wazuh Agent

After downloading the Windows installer for Wazuh,

Installed the agent on the target endpoint

Entered the Security Onion server IP **(192.168.10.250)** and agent key

Replaced the default configuration file with a custom one that includes event-forwarding rules for Sysmon logs and PowerShell script logging.

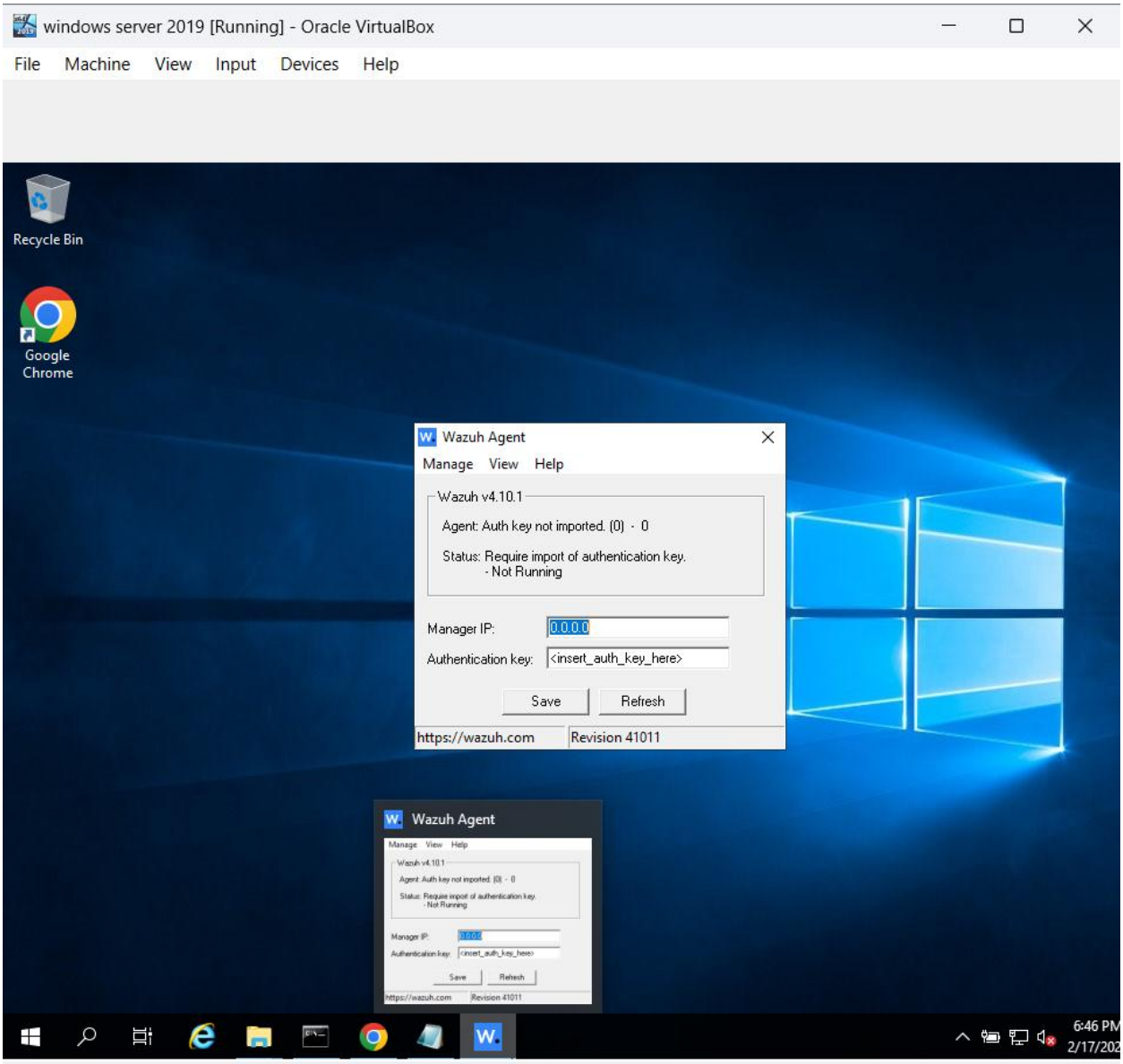
- Restarted the **Wazuh agent** to apply the changes

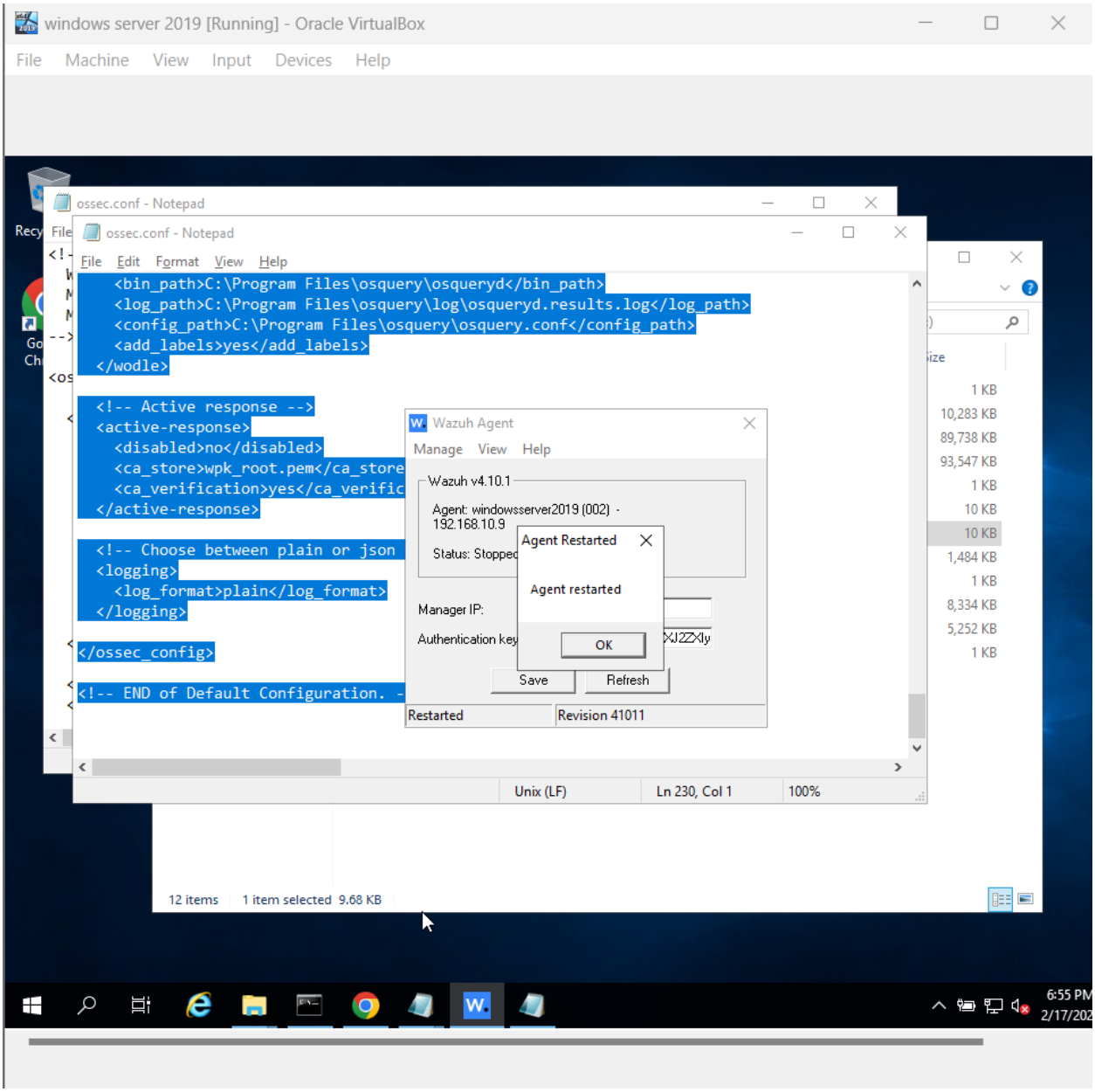
Upon verifying the **log files**, I confirmed that the agent was properly communicating with the **Wazuh manager**, offering event forwarding and **host-based** intrusion detection features.

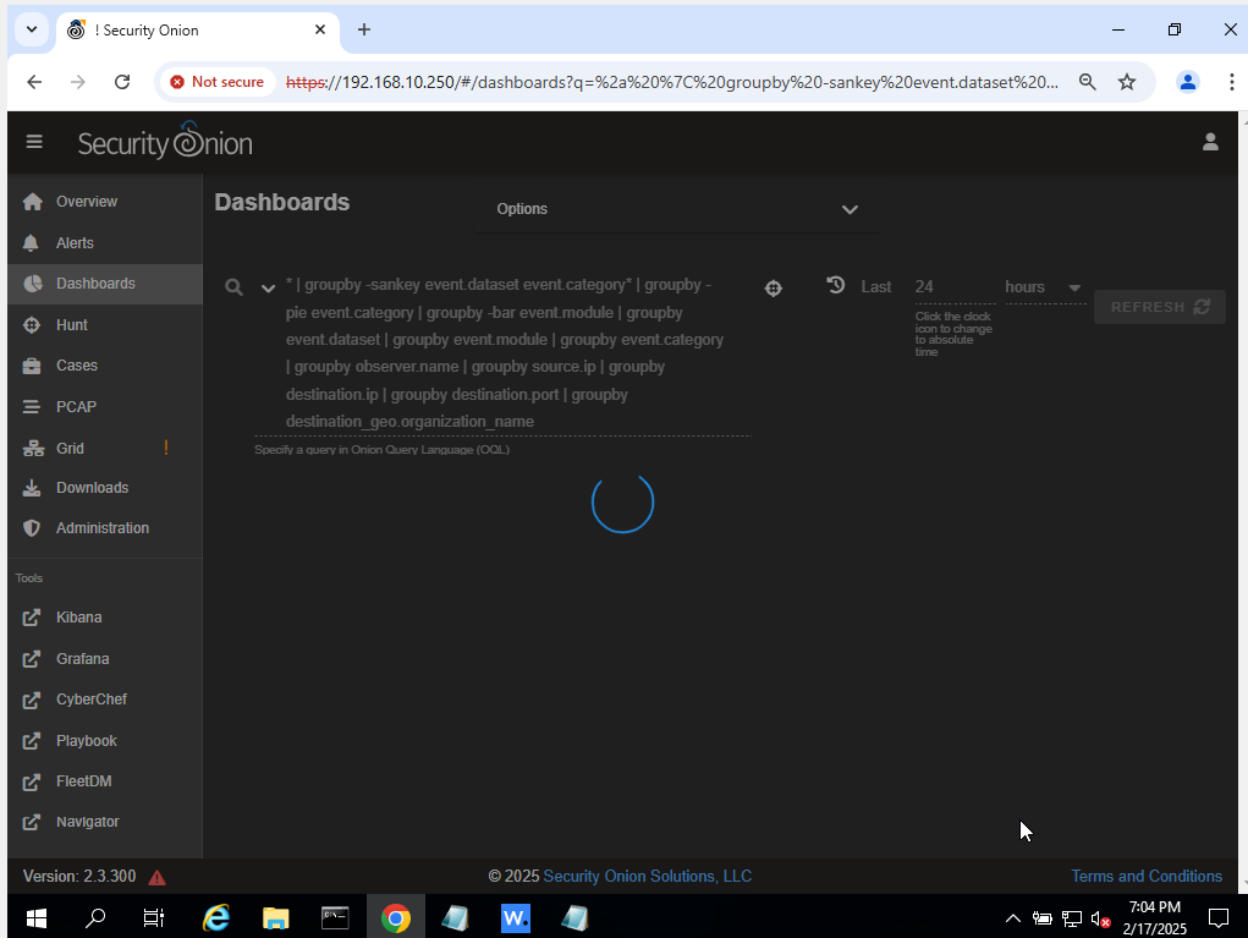
```
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: windowsserver 2019

** Invalid name 'windowsserver 2019' given. Name must contain only alphanumeric characters (min=2, m
ax=32).

   * A name for the new agent: windowsserver2019
   * The IP Address of the new agent: 192.168.10.9
Confirm adding it?(y/n): y
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).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: securityonion, IP: 192.168.10.250
   ID: 002, Name: windowsserver2019, IP: 192.168.10.9
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIHdpbmRvd3NzZXJ2ZXIyMDE5IDE5Mi4xNjguMTAuOSAwNzg1M2YyNjJjNzExZWI5ZmFlNzFkYjk2NjMzNjQwYThhMzRmZGJm
YmZkMWYxZjhmNGJhMjA2OGRjNWMxYjI3

** Press ENTER to return to the main menu.
```

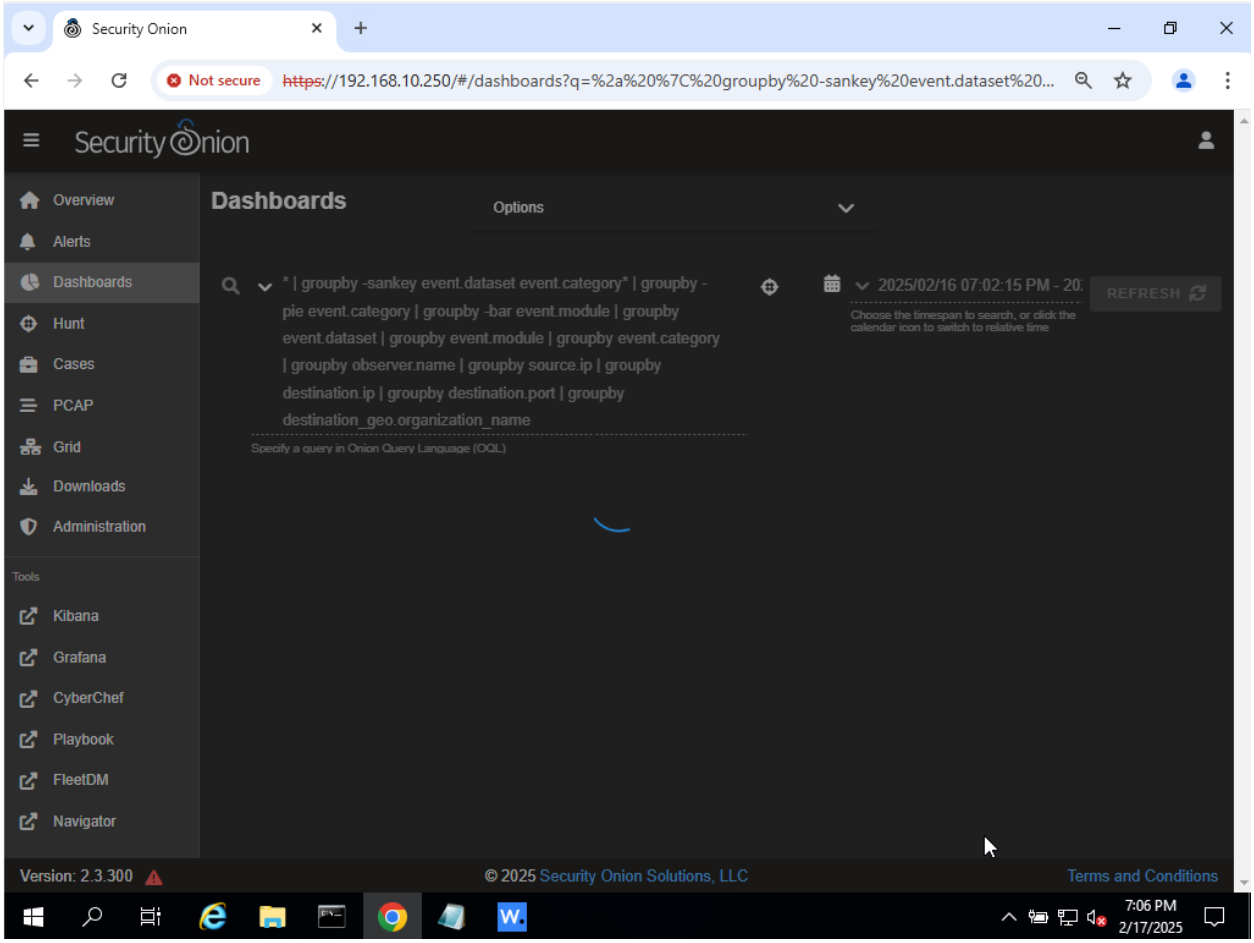
Agent Key:

```
Agent key information for '002' is:
MDAyIHdpbmRvd3NzZXJ2ZXIyMDE5IDE5Mi4xNjguMTAuOSAwNzg1M2YyNjJjNzExZWI5ZmFlNzFkYjk2NjMzNjQwYThhMzRmZGJm
YmZkMWYxZjhmNGJhMjA2OGRjNWMxYjI3
```


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Google Chrome
Wazuh Agent
Manage View Help
Wazuh v4.10.1
Agent: Auth key not imported. (0) - 0
Status: Require import of authentication key.
- Not Running
Manager IP:
0.0.0.0
Authentication key:
<insert_auth_key_here>
Save
Refresh
https://wazuh.com
Revision 41011
Wazuh Agent
6:46 PM
2/17/202


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
ossec.conf - Notepad
File Edit Format View Help
<bin_path>C:\Program Files\osquery\osqueryd</bin_path>
<log_path>C:\Program Files\osquery\log\osqueryd.results.log</log_path>
<config_path>C:\Program Files\osquery\osquery.conf</config_path>
<add_labels>yes</add_labels>
</wodle>
<!-- Active response -->
<active-response>
<disabled>no</disabled>
<ca_store>wpk_root.pem</ca_store
<ca_verification>yes</ca_verific
</active-response>
<!-- Choose between plain or json
<logging>
<log_format>plain</log_format>
</logging>
</ossec_config>
<!-- END of Default Configuration. -
Wazuh Agent
Manage View Help
Wazuh v4.10.1
Agent: windowsserver2019 (002) - 192.168.10.9
Status: Stopped
Agent Restarted
Agent restarted
OK
Manager IP:
Authentication key
Save
Refresh
Restarted
Revision 41011
Unix (LF)
Ln 230, Col 1
100%
12 items
1 item selected 9.68 KB
6:55 PM
2/17/202


! Security Onion
Not secure
https://192.168.10.250/#/dashboards?q=%2a%20%7C%20groupby%20-sankey%20event.dataset%20...
Security Onion
Overview
Alerts
Dashboards
Hunt
Cases
PCAP
Grid
Downloads
Administration
Tools
Kibana
Grafana
CyberChef
Playbook
FleetDM
Navigator
Dashboards
Options
* | groupby -sankey event.dataset event.category* | groupby -pie event.category | groupby -bar event.module | groupby event.dataset | groupby event.module | groupby event.category | groupby observer.name | groupby source.ip | groupby destination.ip | groupby destination.port | groupby destination_geo.organization_name
Specify a query in Onion Query Language (OQL)
Last
24
hours
Click the clock icon to change to absolute time
REFRESH
Version: 2.3.300
© 2025 Security Onion Solutions, LLC
Terms and Conditions
7:04 PM
2/17/2025



Conclusion

In this experiment, I was able to deploy, configure, and tune Security Onion for network security monitoring. Additionally, I integrated **Wazuh** for host-based monitoring to enhance visibility into security incidents. These configurations will allow future threat-hunting and incident response activities throughout the semester.