Security Onion Installation

SO Configuration Guide

Created by

Harish. R

NOTE

Security Onion 2.3.110 (SO) Operating system has been installed in the system as a Production standalone setup. This document is to record the configurations made during the initial setup on 6th April 2022 for future verifications. Further changes in the setup will be updated under this section.

User Roles:

- The user-created during installation will be considered as a "superuser" by default.
- Other users that are created manually after installation will be added as an "analyst".

Pre-requisites:

- ***A bootable device with the latest SO iso image:***
  We have downloaded the latest version of security onion from their official site (https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md) and formatted the Pendrive as a bootable device with this iso image using the tool "Etcher"
  [Note: Formatting the Pendrive using the Rufus tool gives an error "Invalid signature check" during booting the image].
- ***16 Gb RAM and 2 TB Hard disks are used for this installation***

Installation Screenshots:

After mounting the USB device, the following configurations are performed.

Figure 1

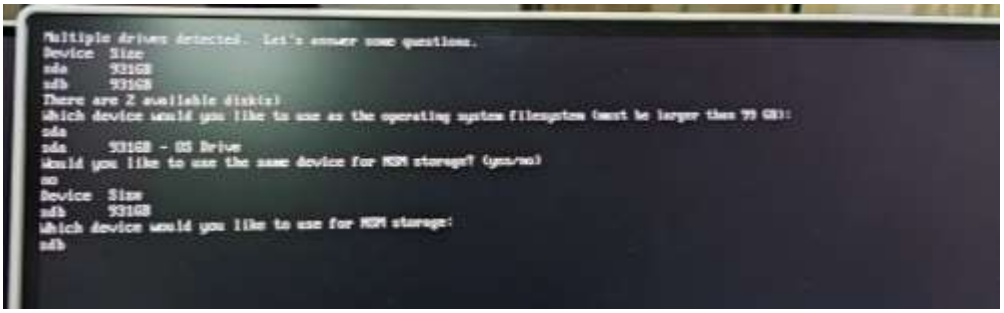

Figure 2

Figure 3

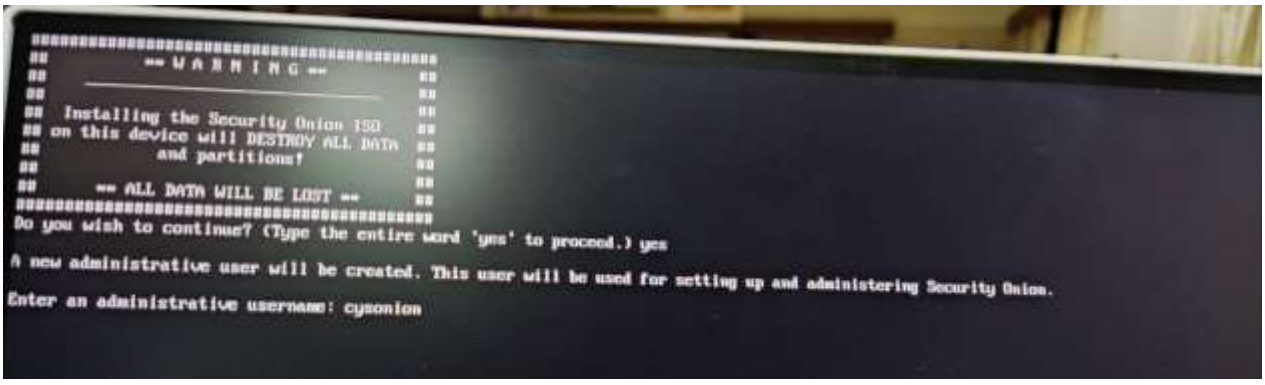

Figure 4

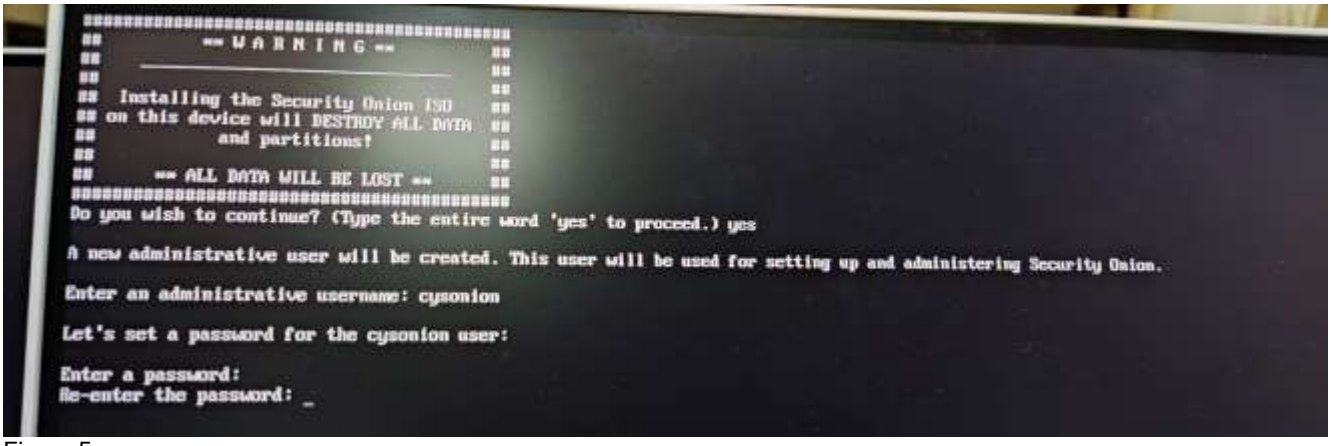

Figure 5

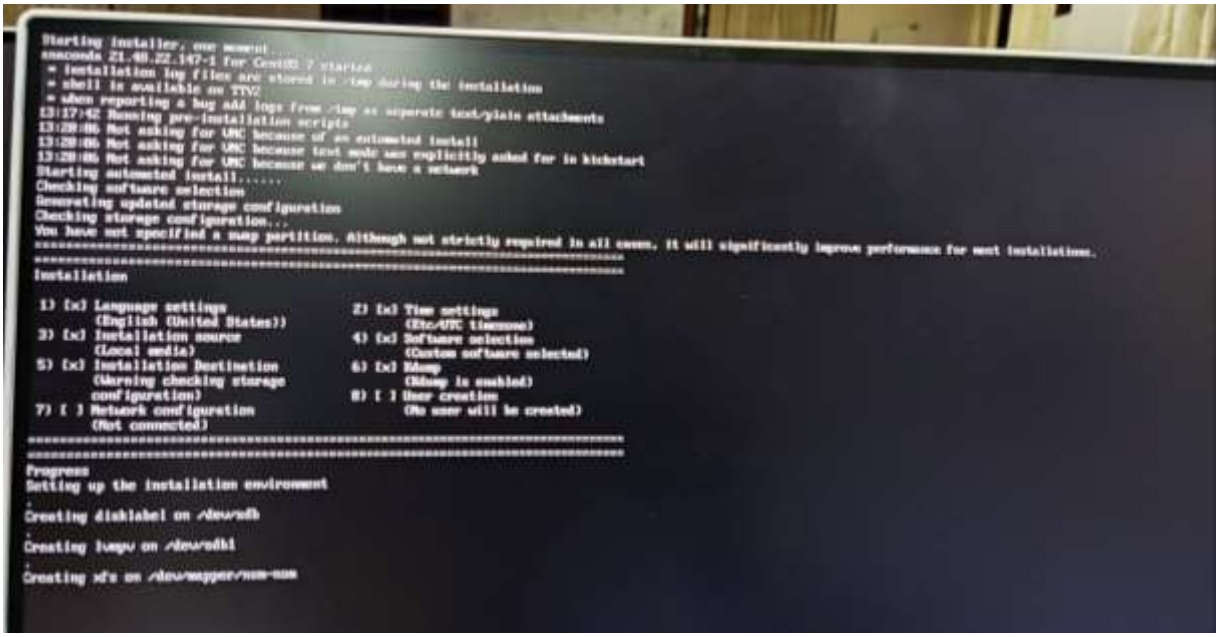

Figure 6

Figure 7

Figure 8

Figure 9

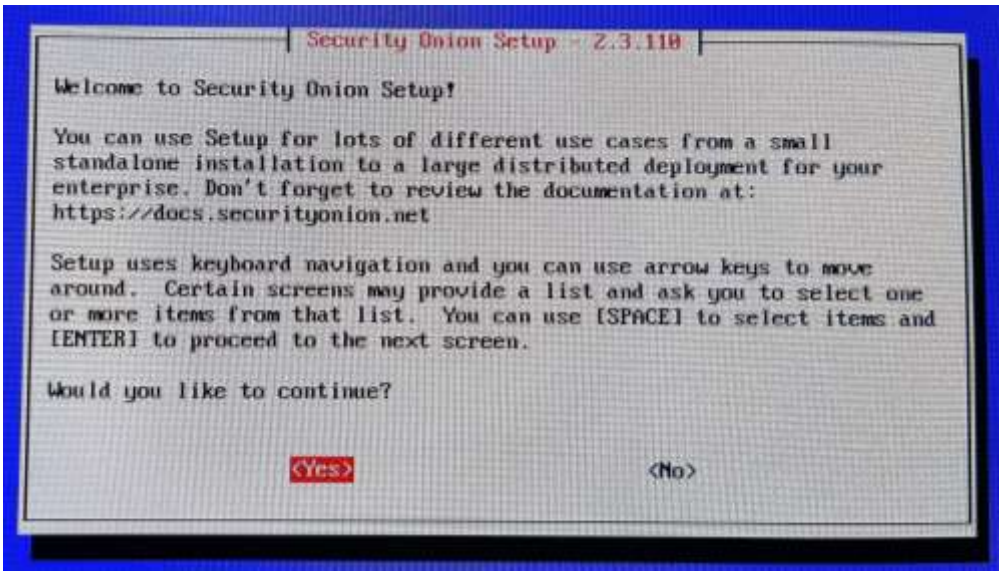

Figure 10

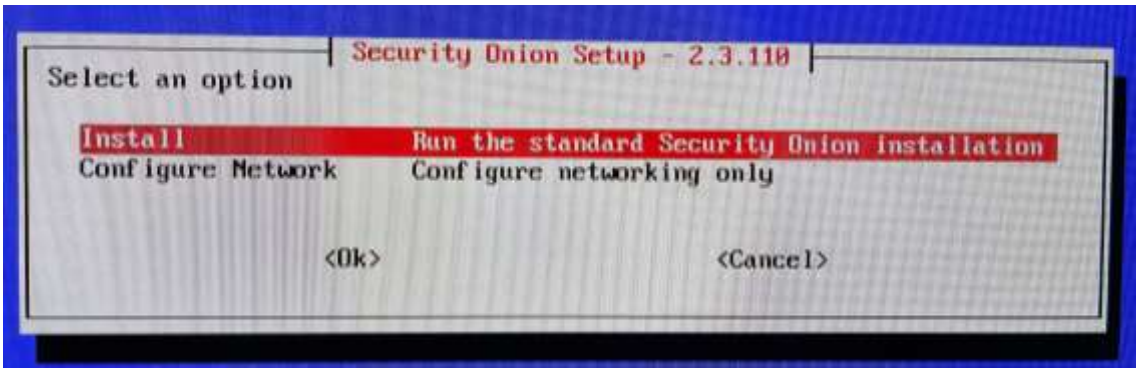

Figure 11

Figure 12 - Standalone mode was selected

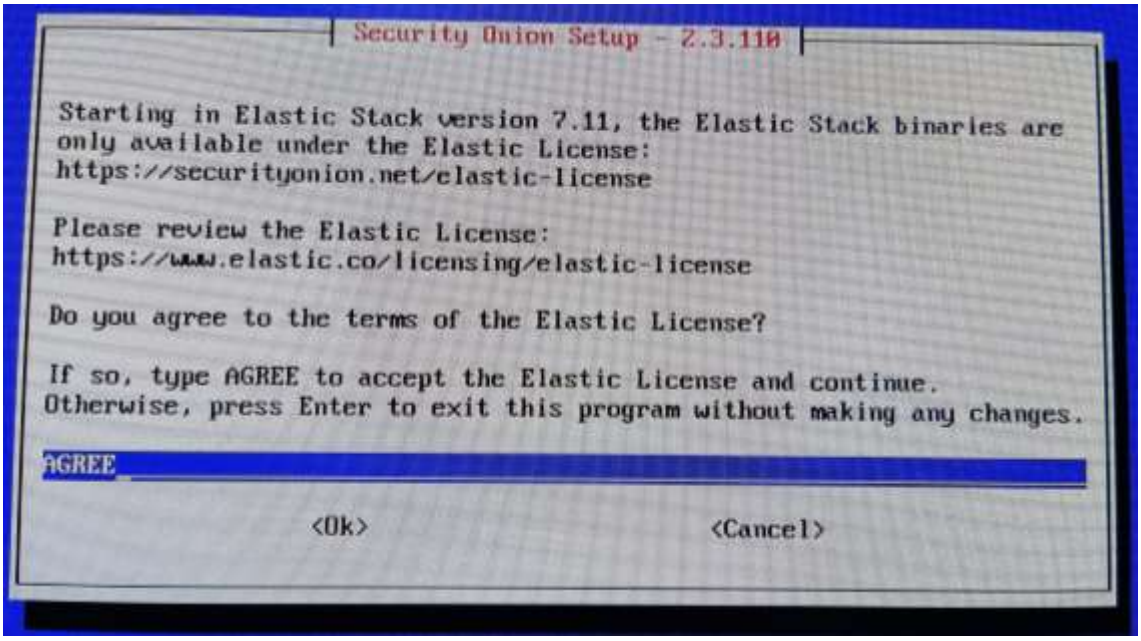

Figure 13

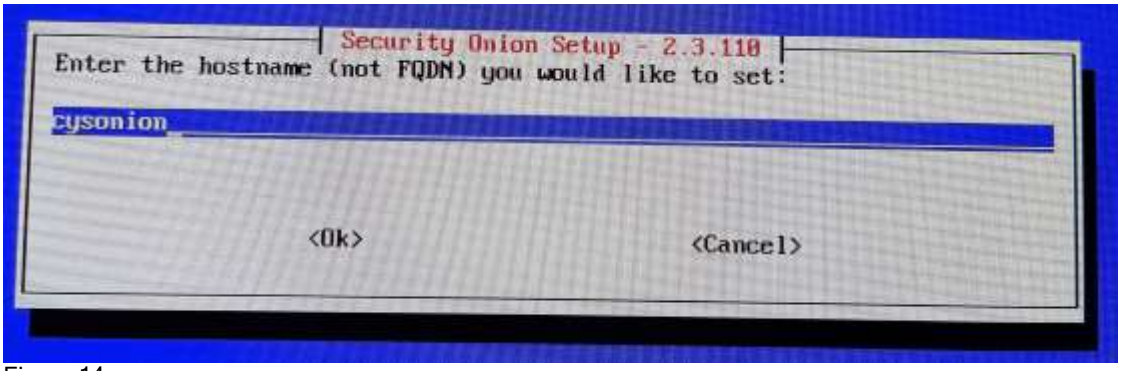

Figure 14

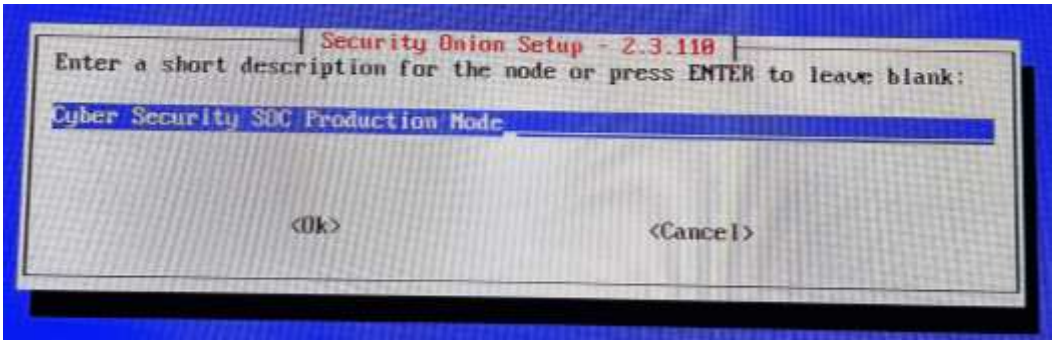

Figure 15

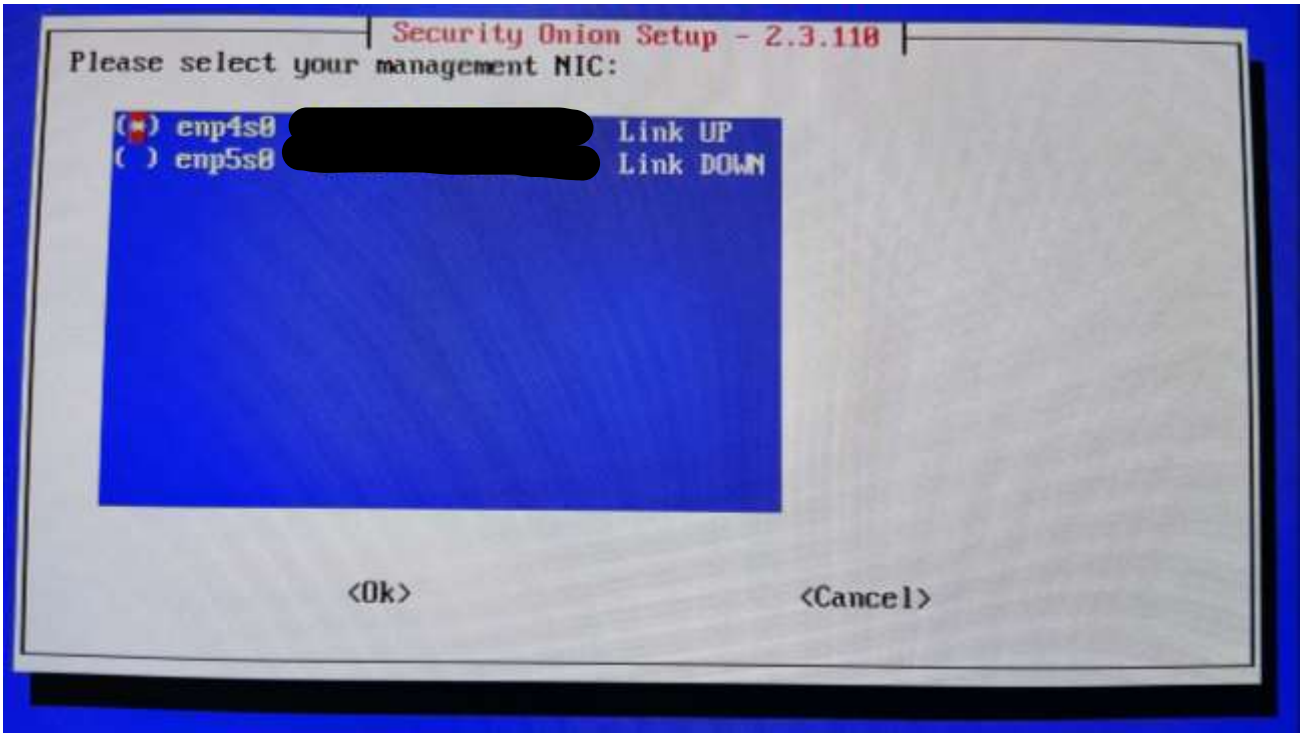

Figure 16

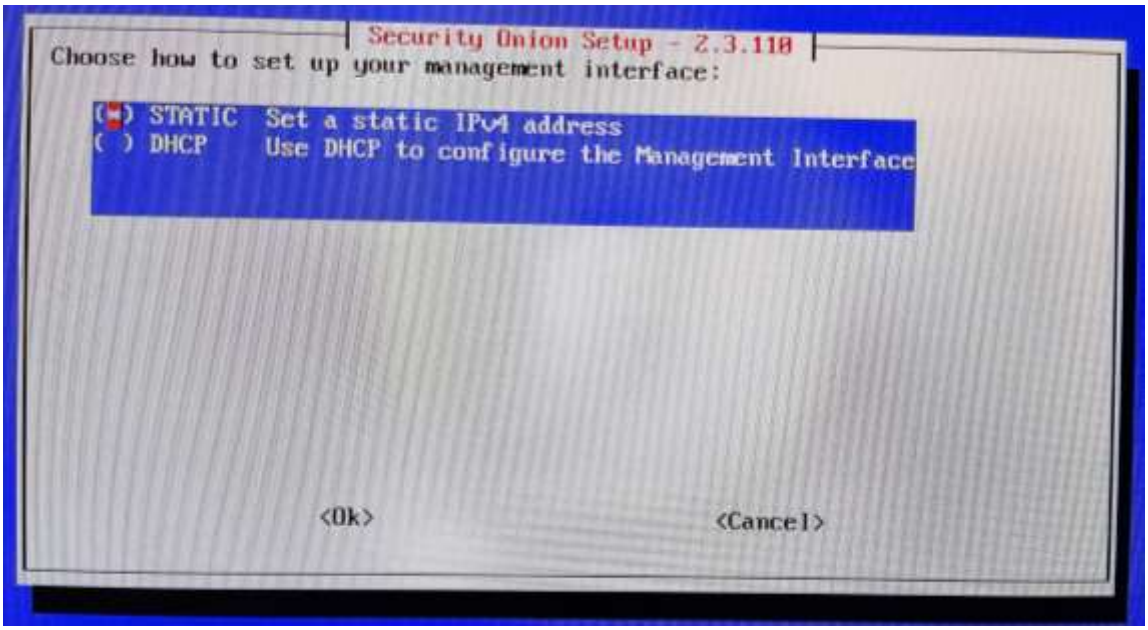

Figure 17

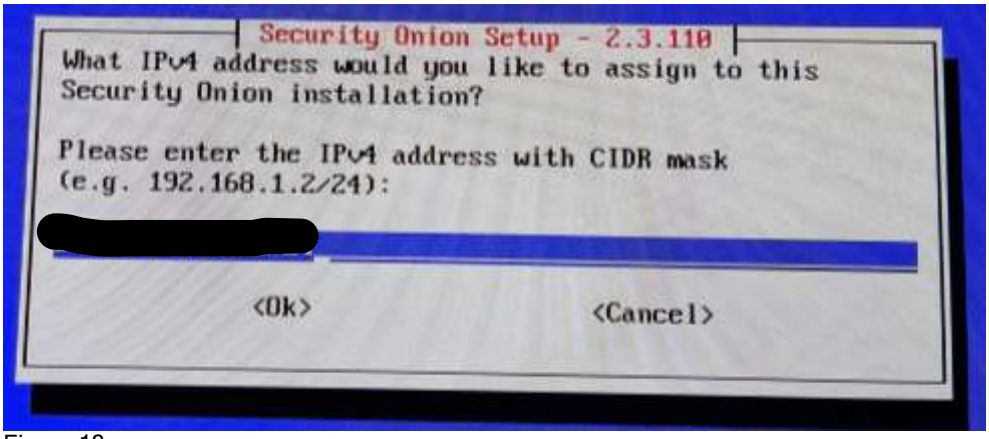

Figure 18

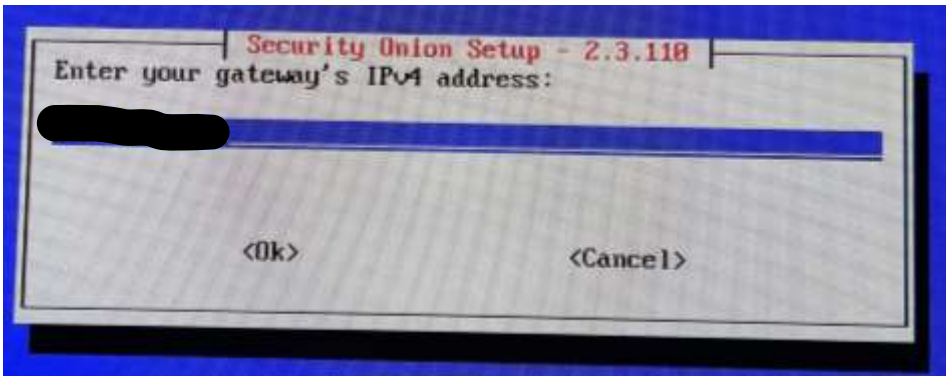

Figure 19

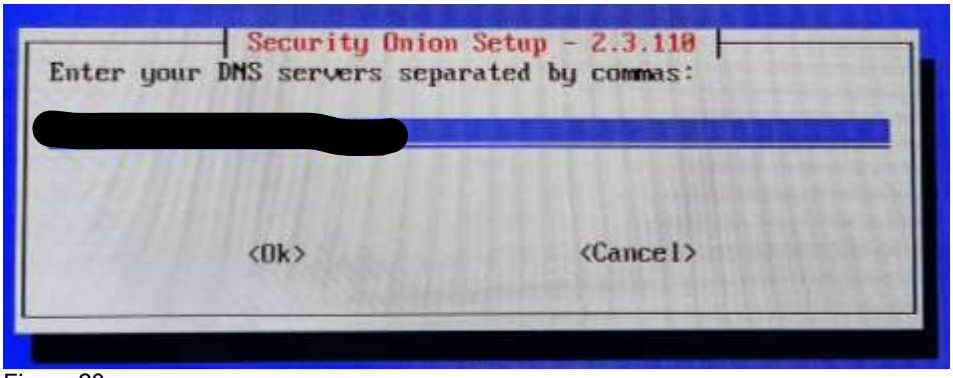

Figure 20

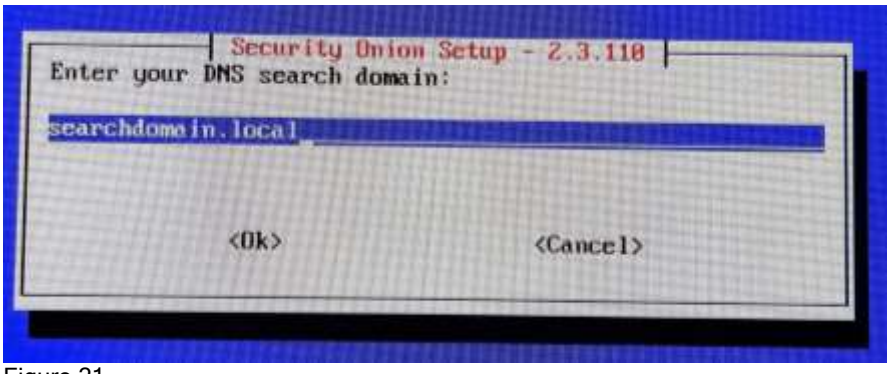

Figure 21

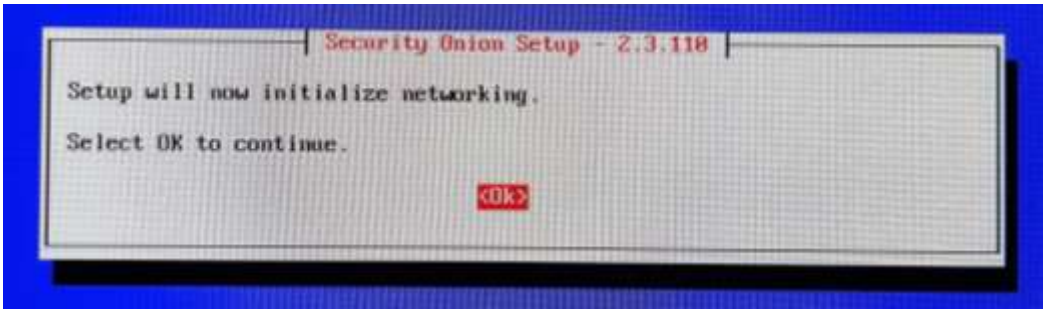

Figure 22

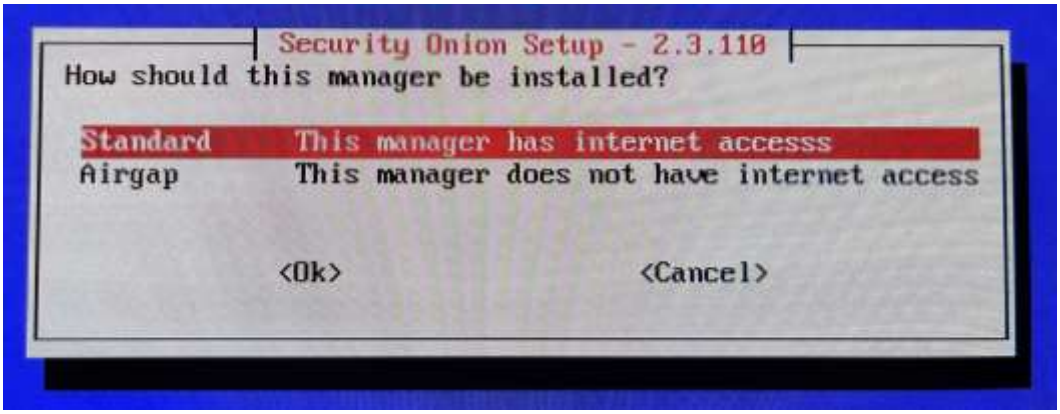

Figure 23

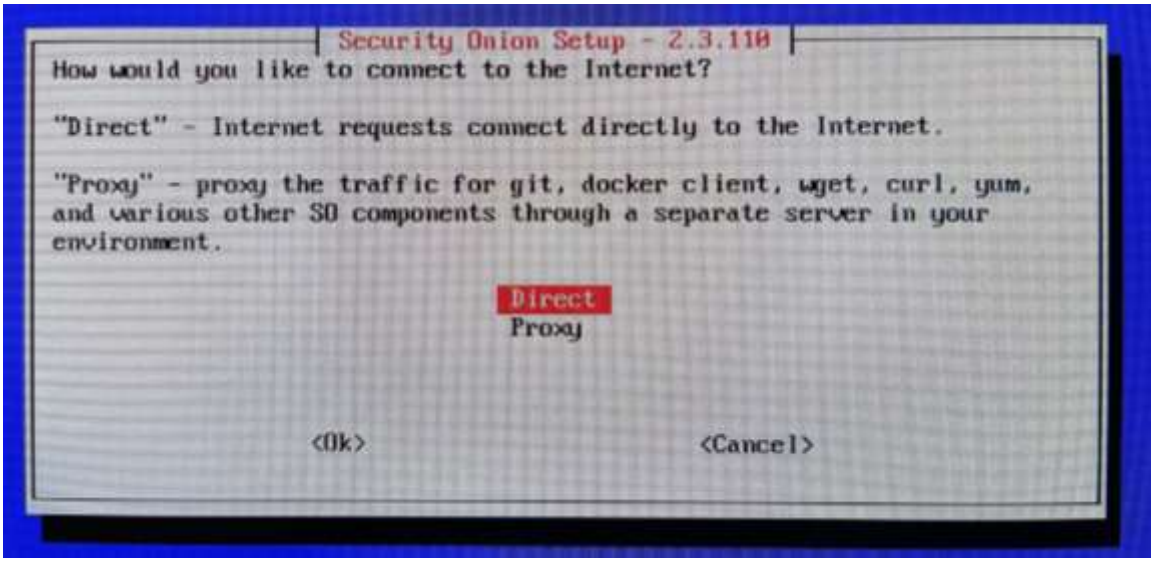

Figure 24

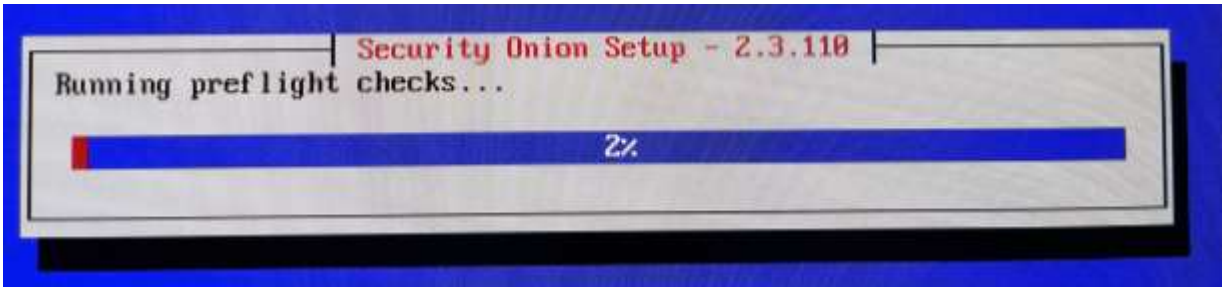

Figure 25

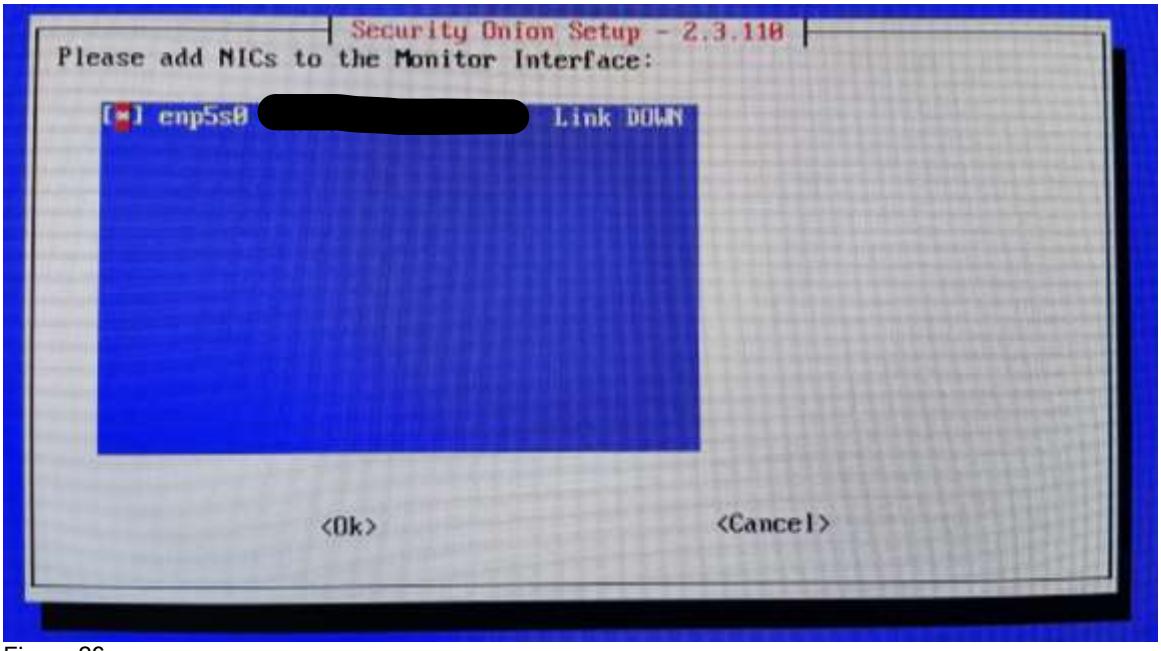

Figure 26

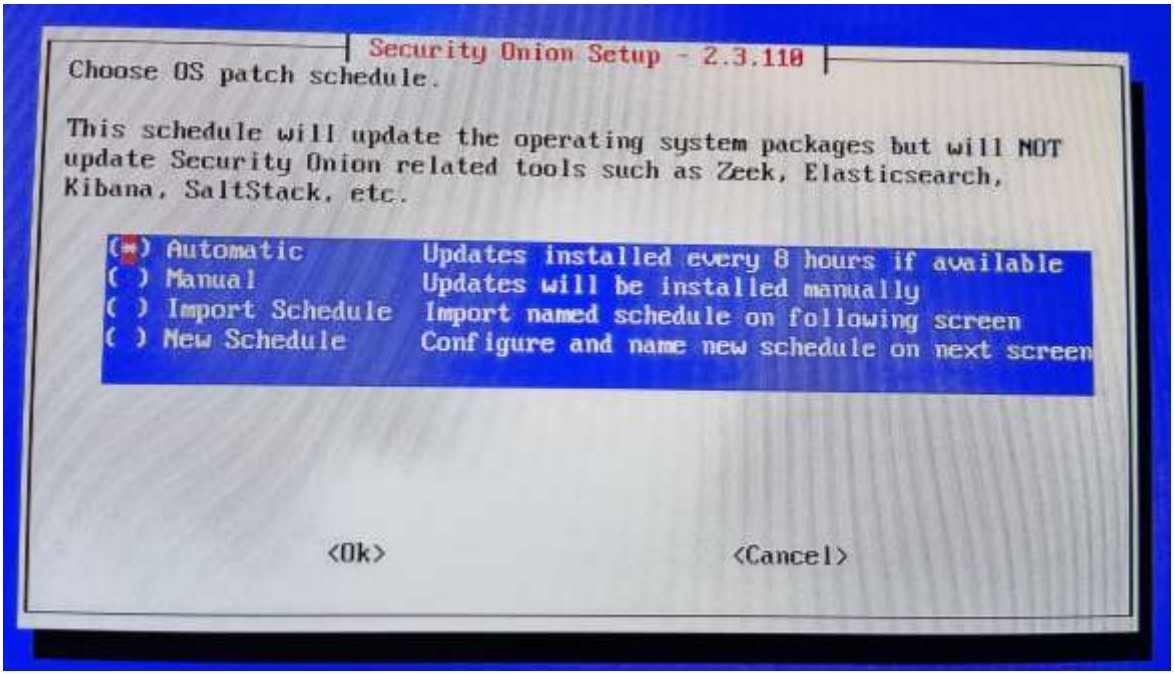

Figure 27

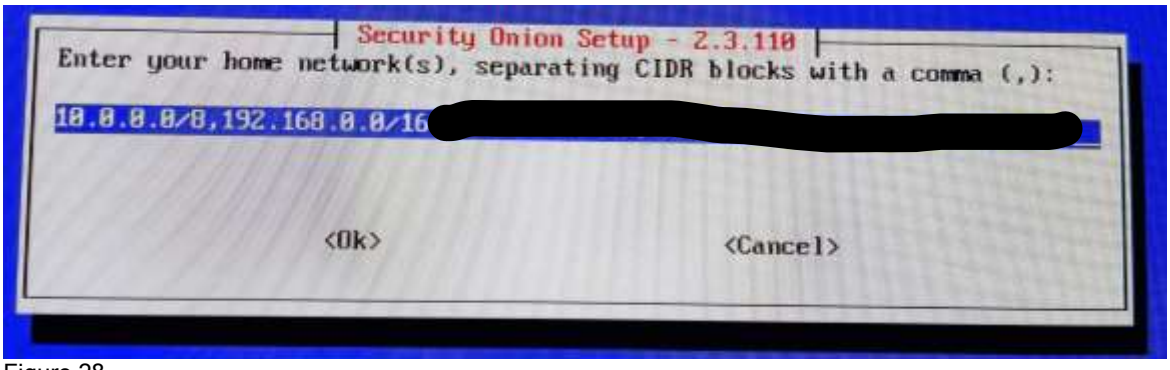

Figure 28

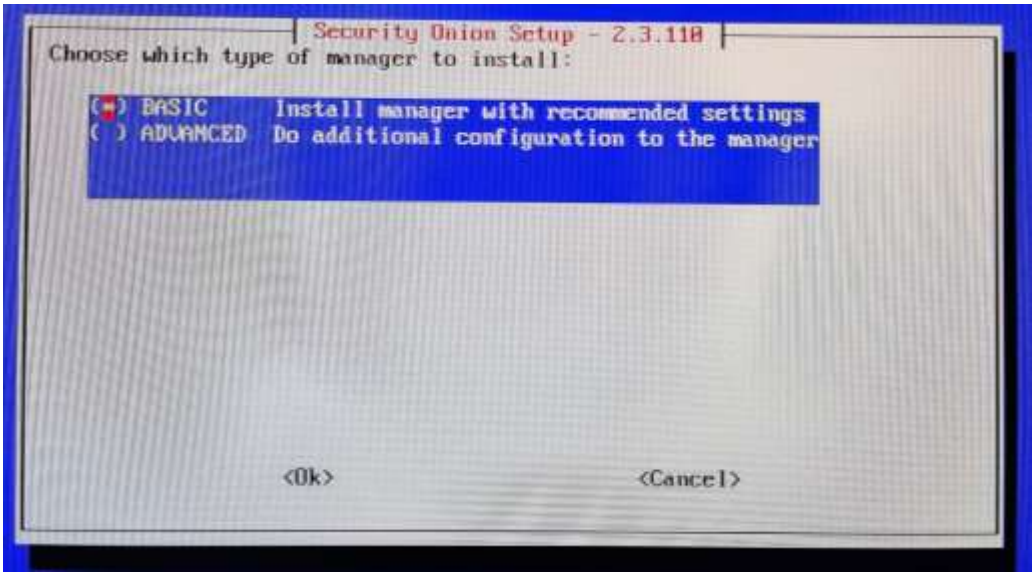

Figure 29

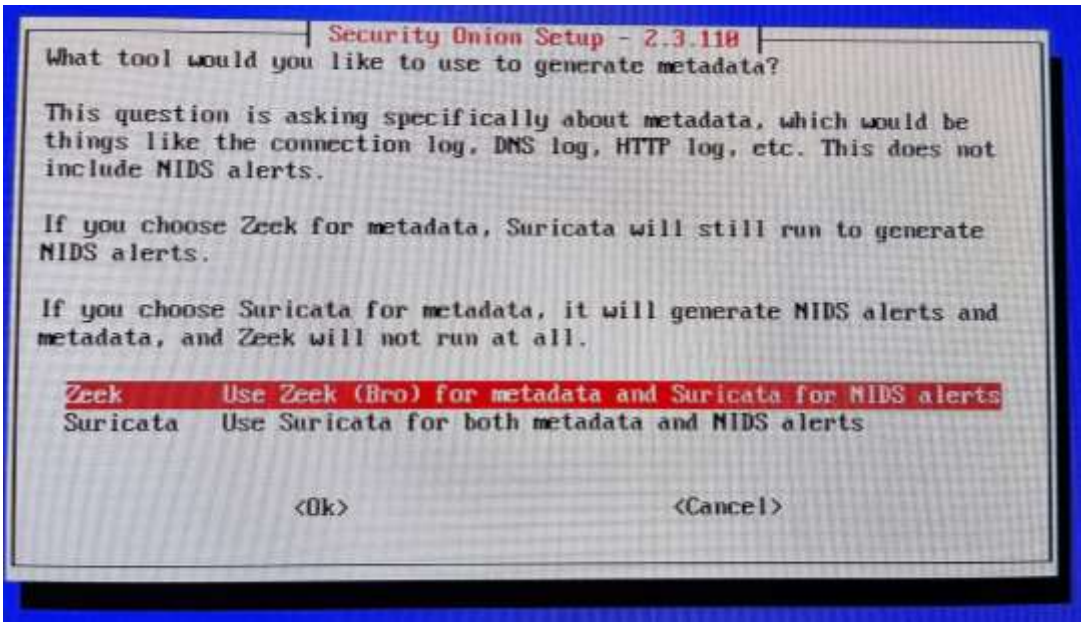

Figure 30

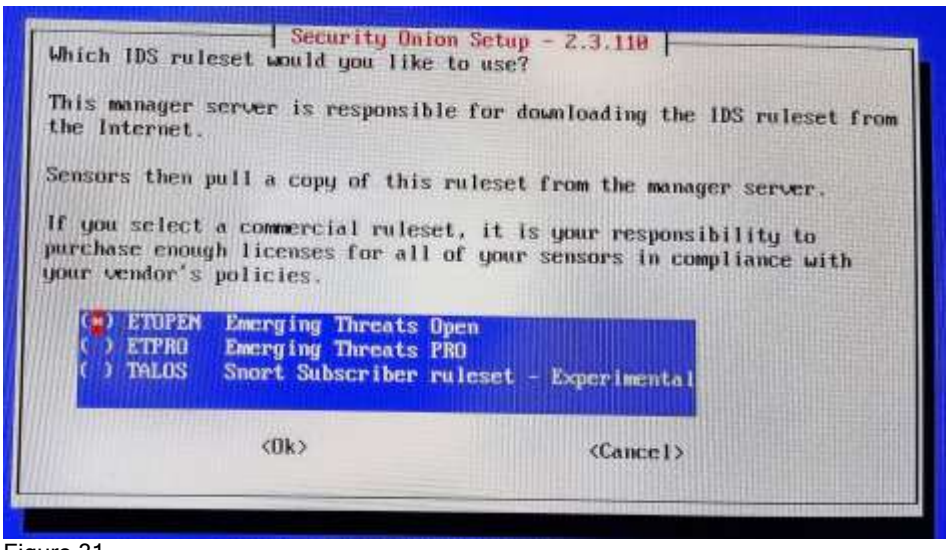

Figure 31

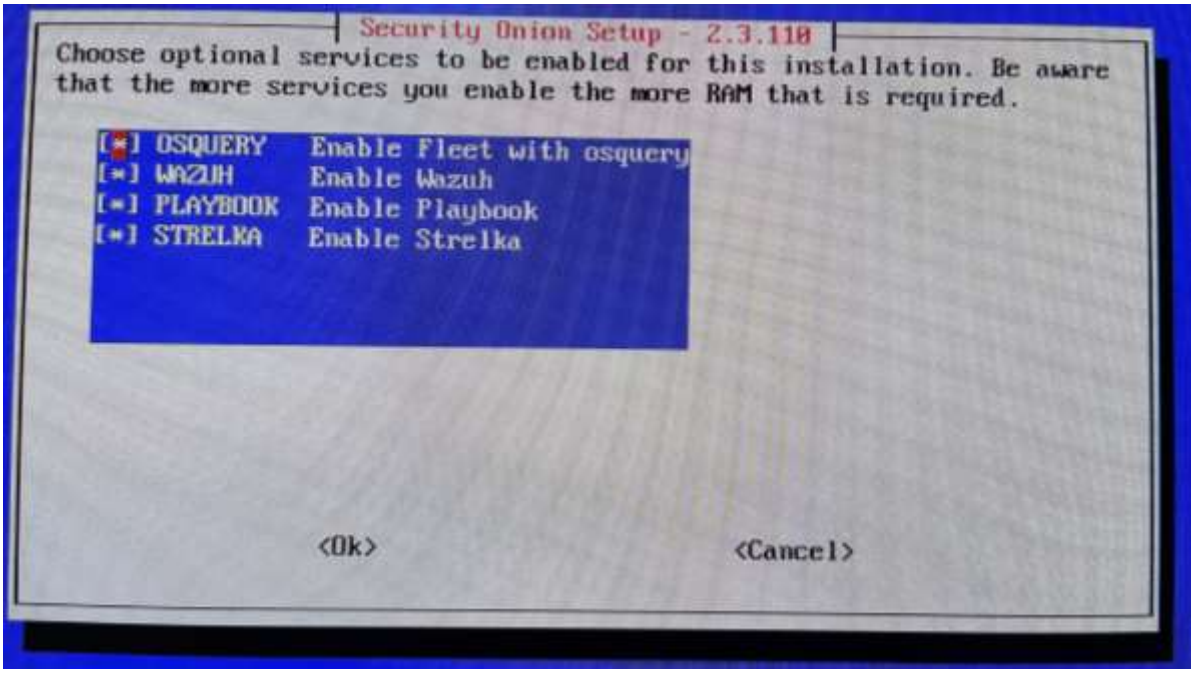

Figure 32

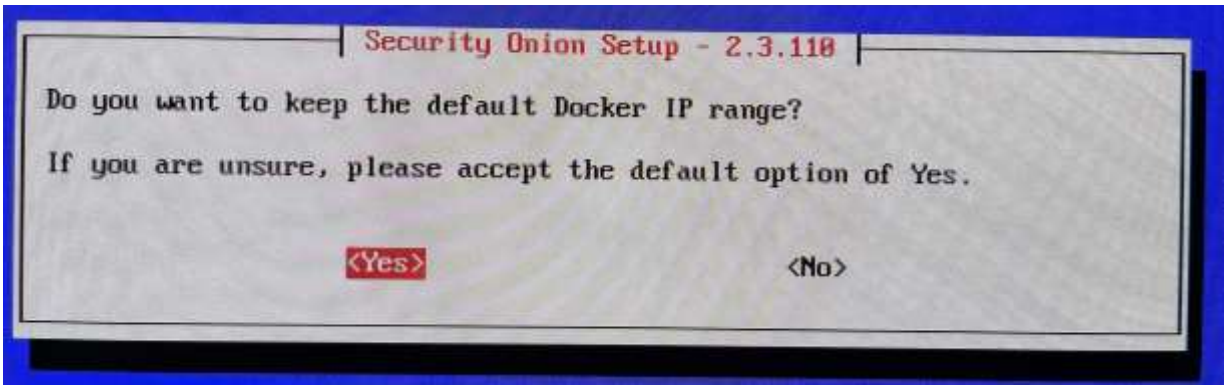

Figure 33

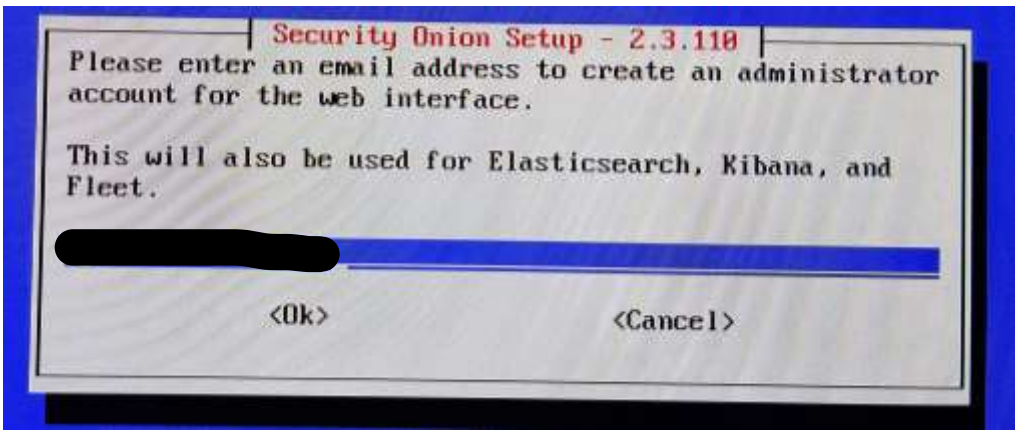

Figure 34

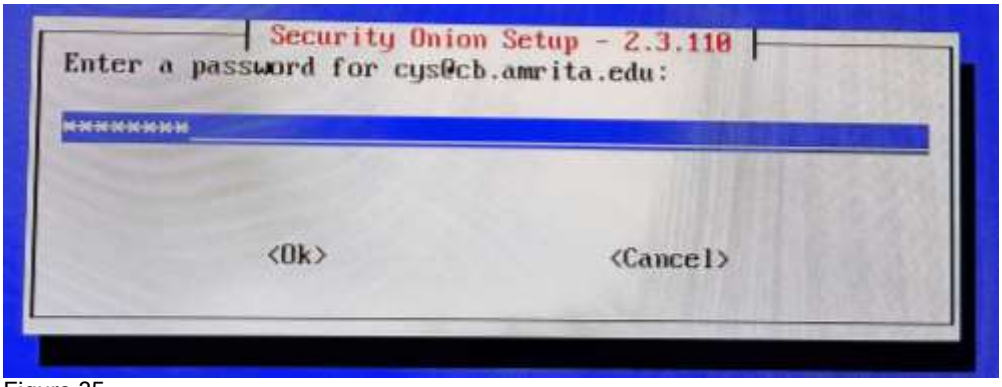

Figure 35

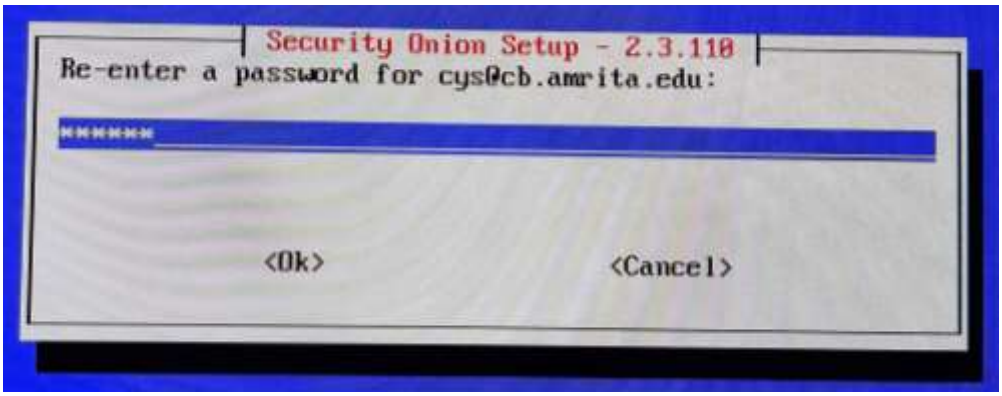

Figure 36

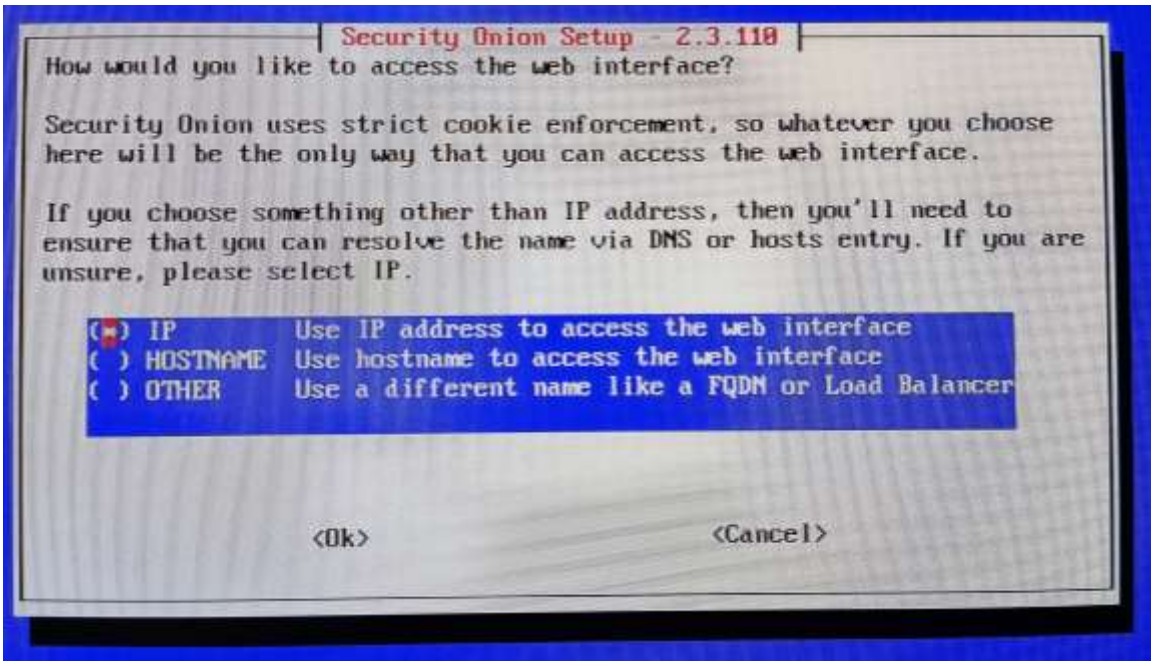

Figure 37

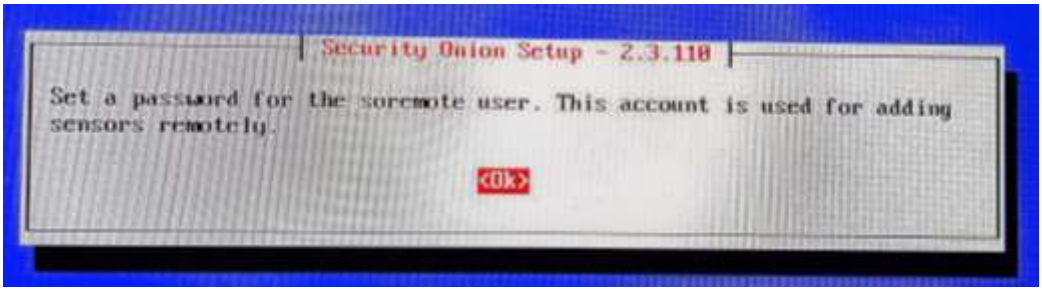

Figure 38

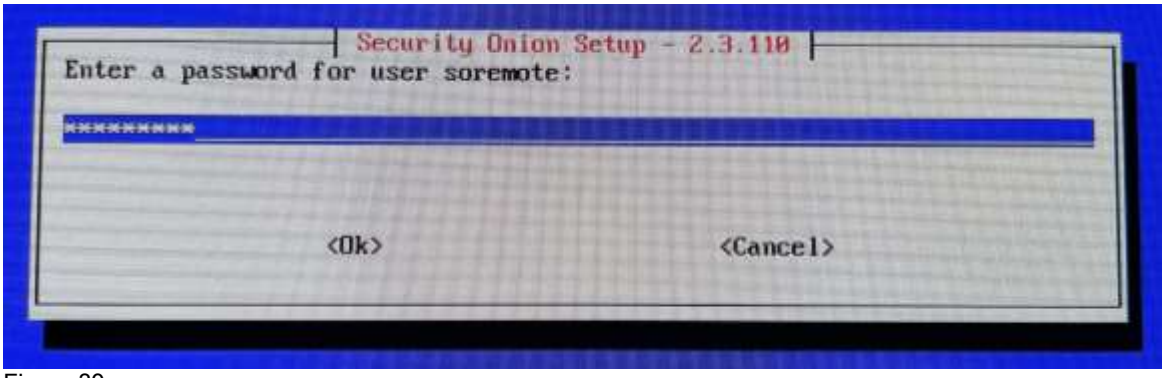

Figure 39

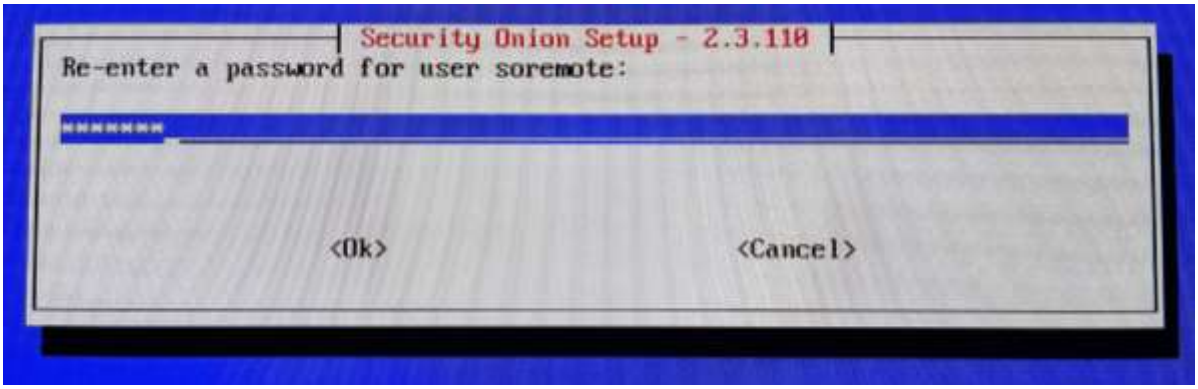

Figure 40

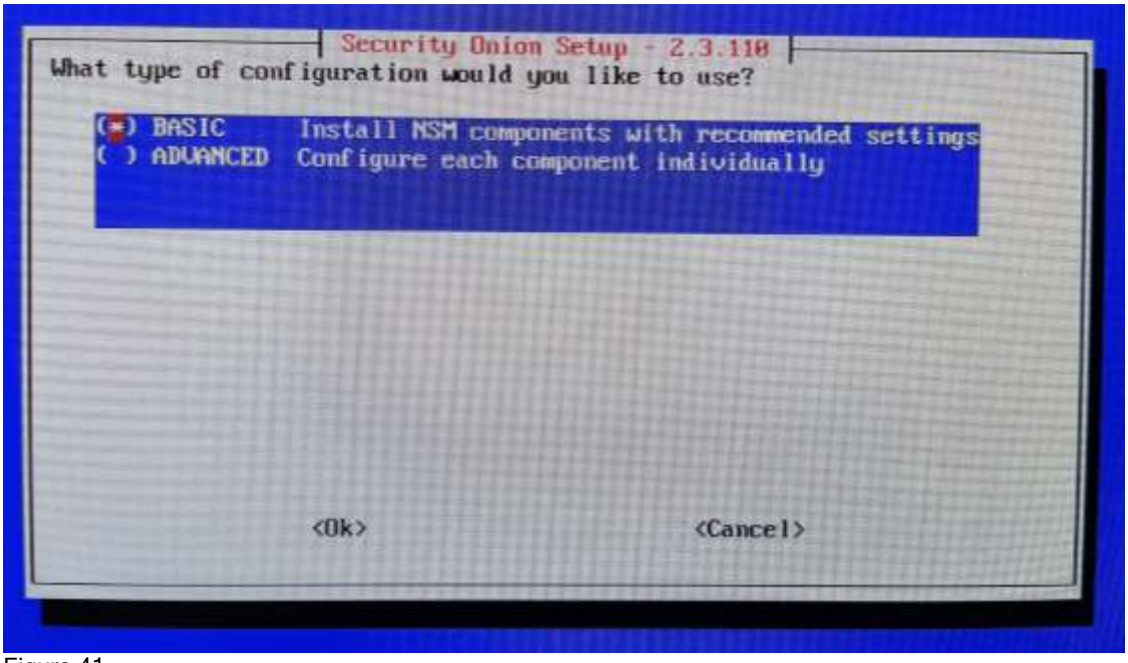

Figure 41

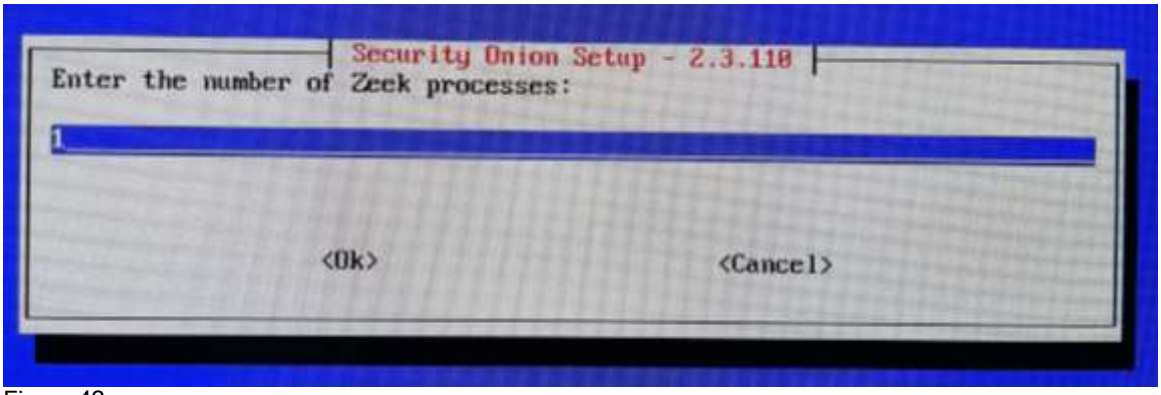

Figure 42

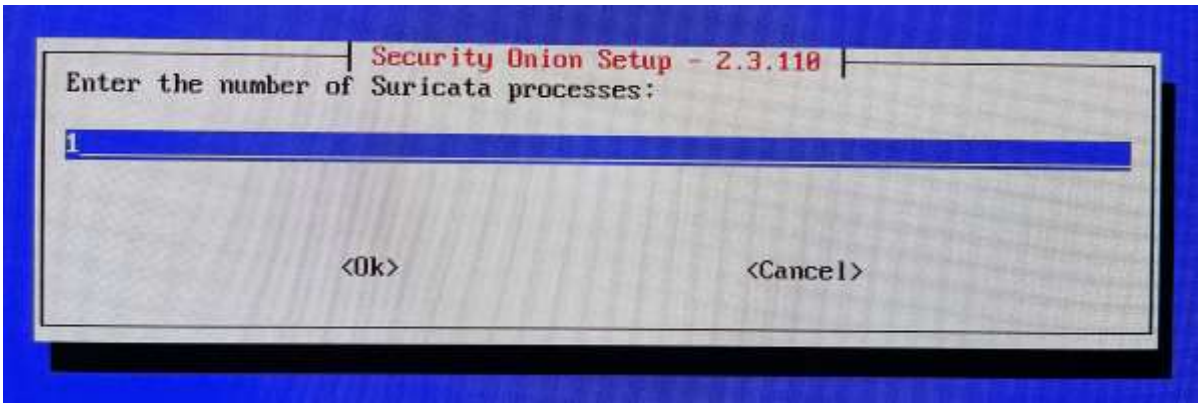

Figure 43

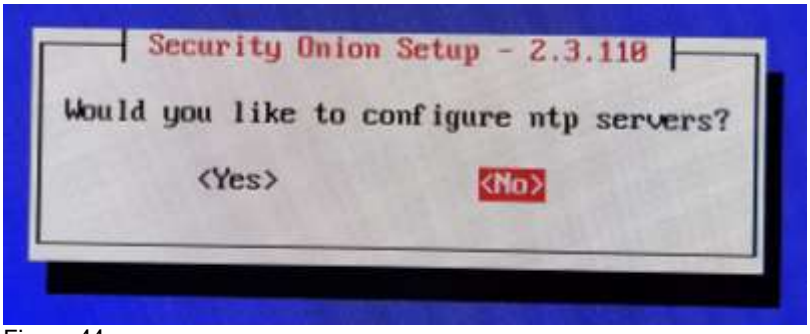

Figure 44

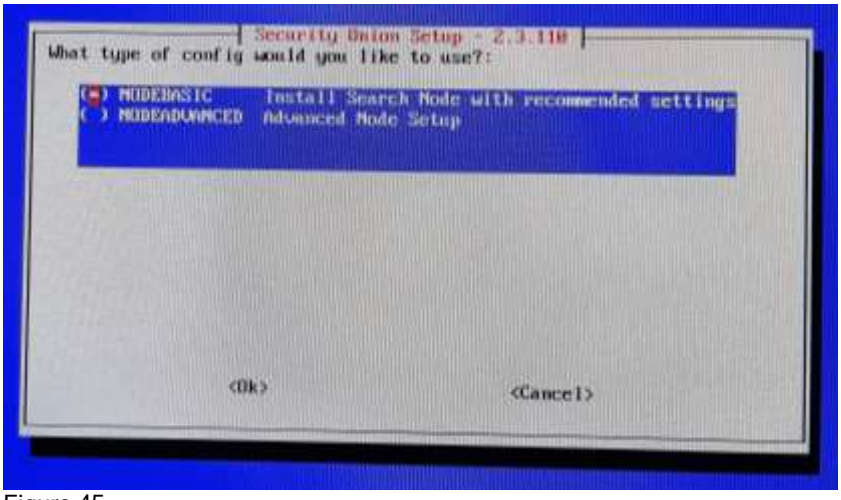

Figure 45

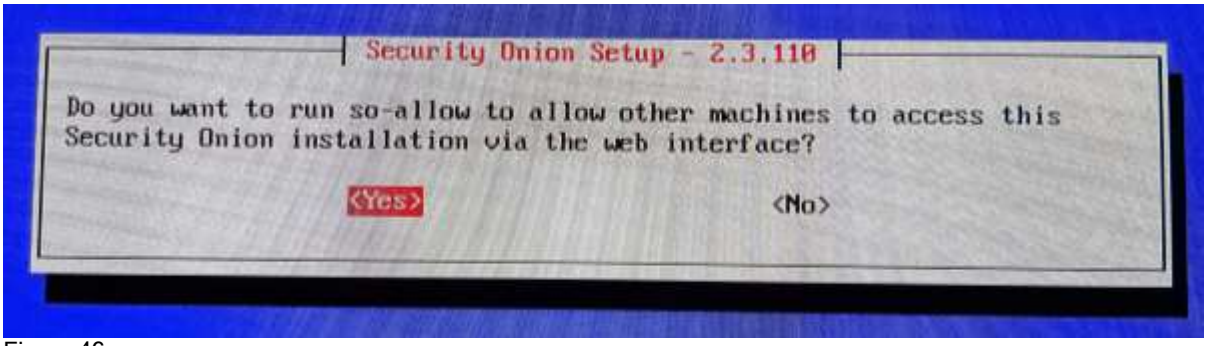

Figure 46

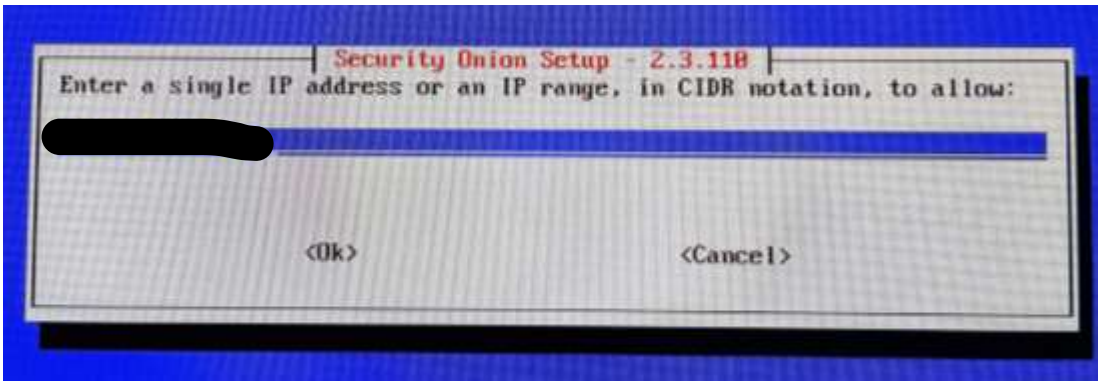

Figure 47

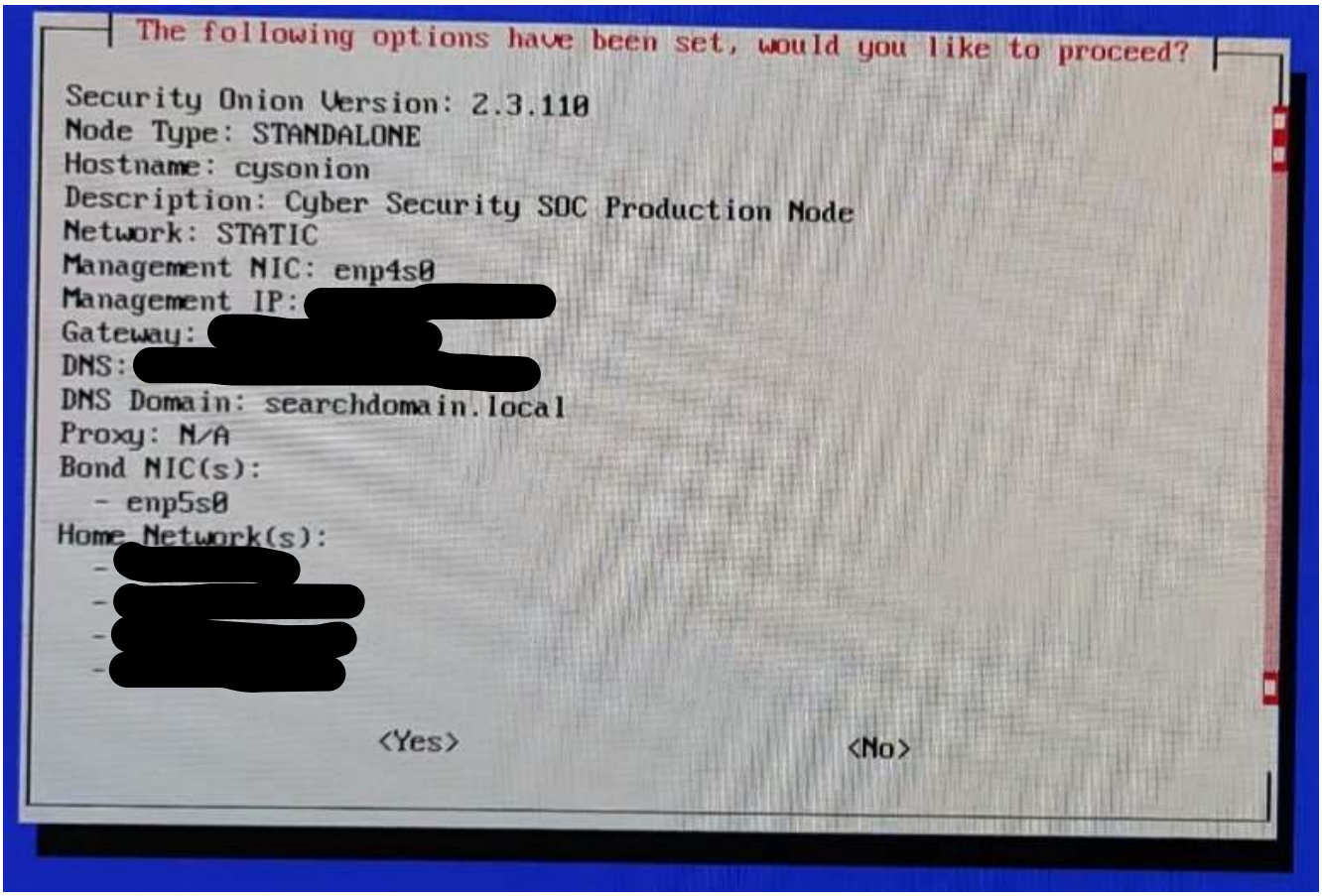

Figure 48

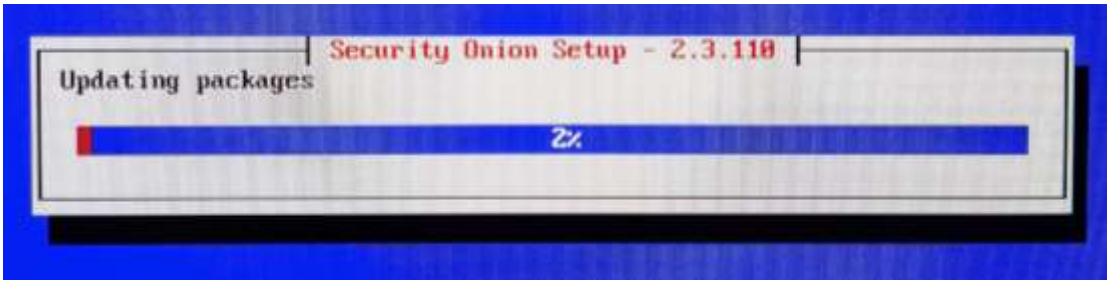

Figure 49

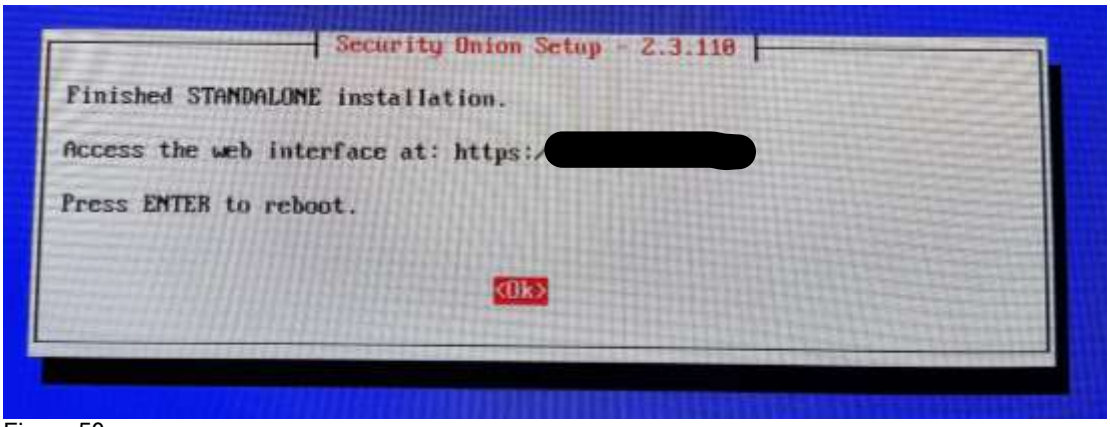

Figure 50

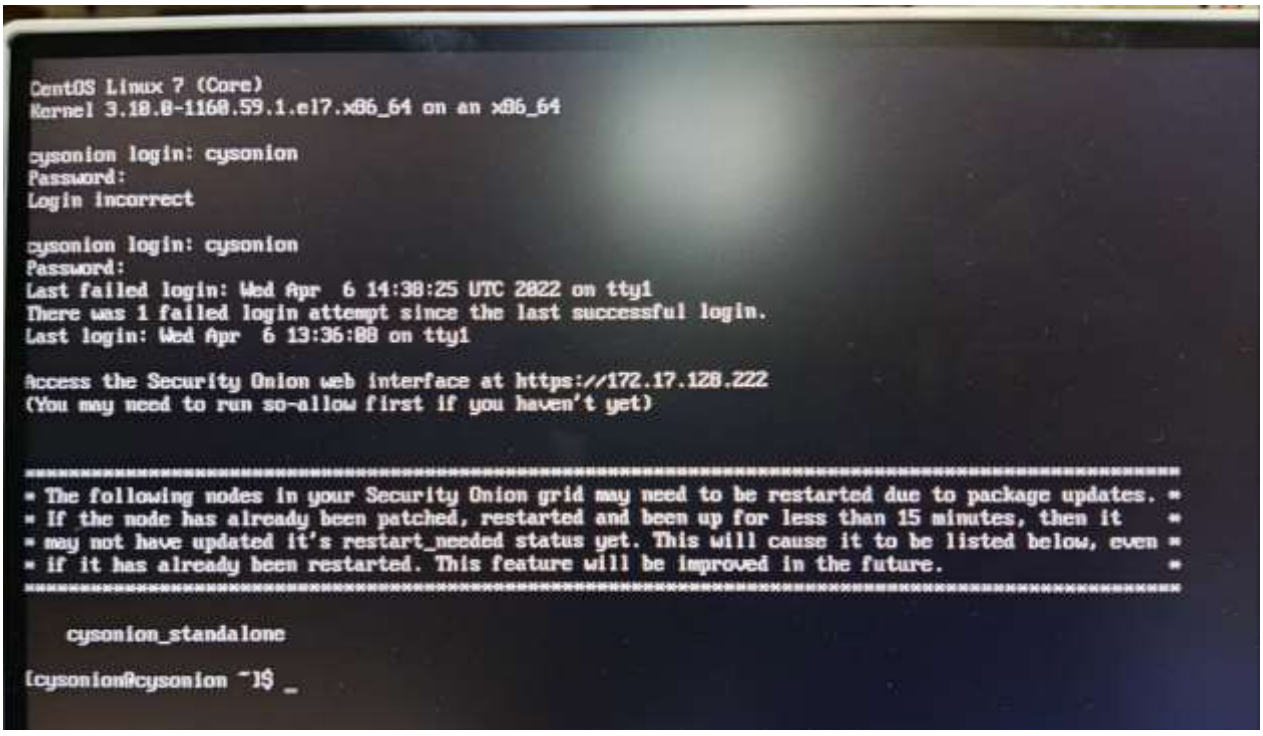

Figure 51

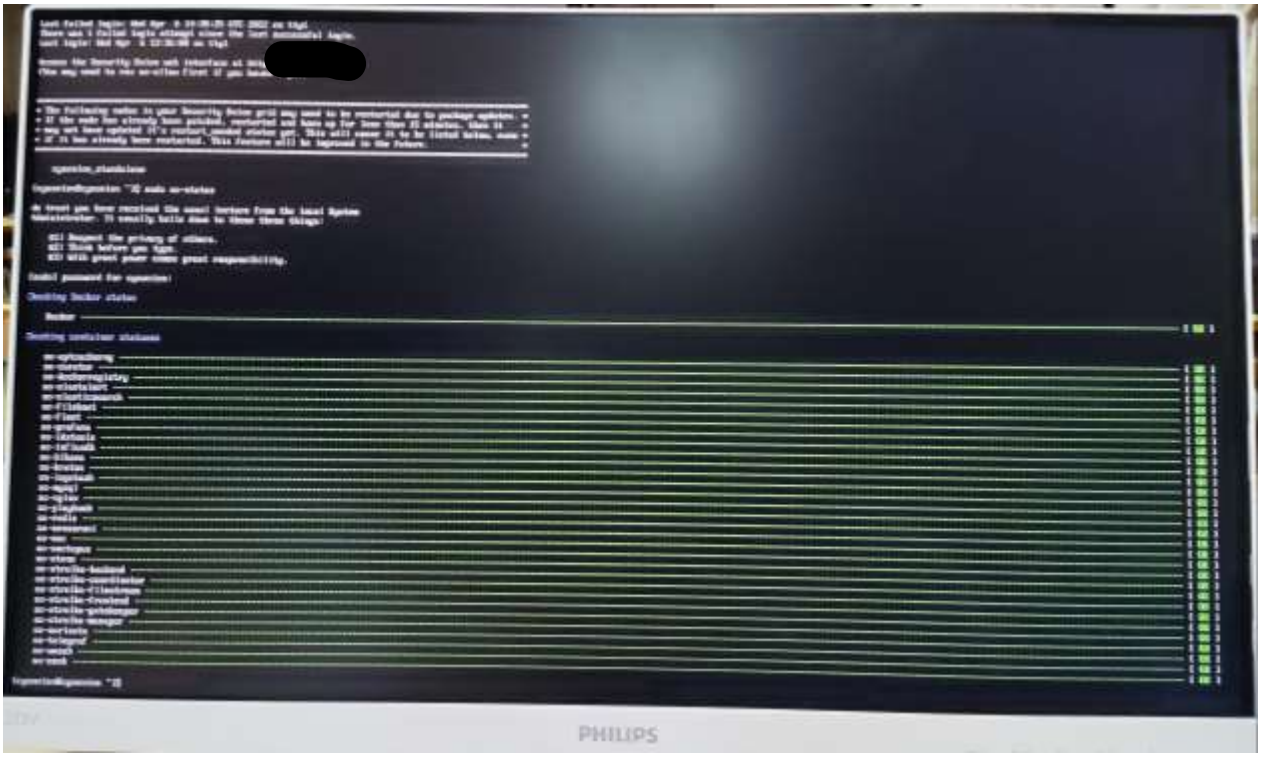

Figure 52

FINAL SUMMARY

After this installation and configuration, the GUI of security Onion can be accessed by typing “configured ip/hostname” on the browsers of any system in the same LAN. So, these are the configurations performed to install the security onion successfully in standalone mode.

References

- https://securityonionsolutions.com/software/
- https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md
- https://docs.securityonion.net/en/2.3/
- https://chrissanders.org/2017/06/security-onion-cheat-sheet/