Steps to install Secured Onion OS and ELK Stack

The primary purpose of using security onion is Setting up

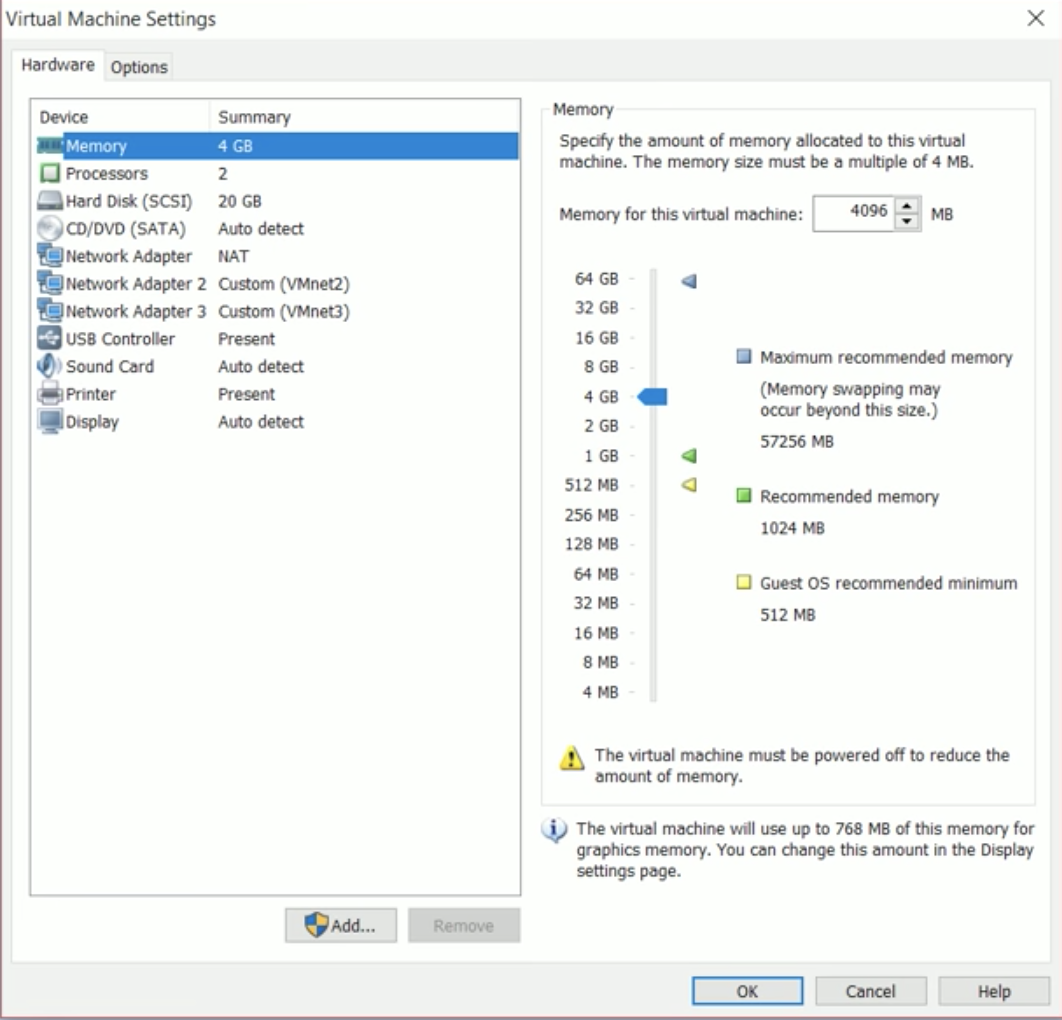
1. Intrusion detection environment
2. Network security tools
3. Log management

Operating System Installation:

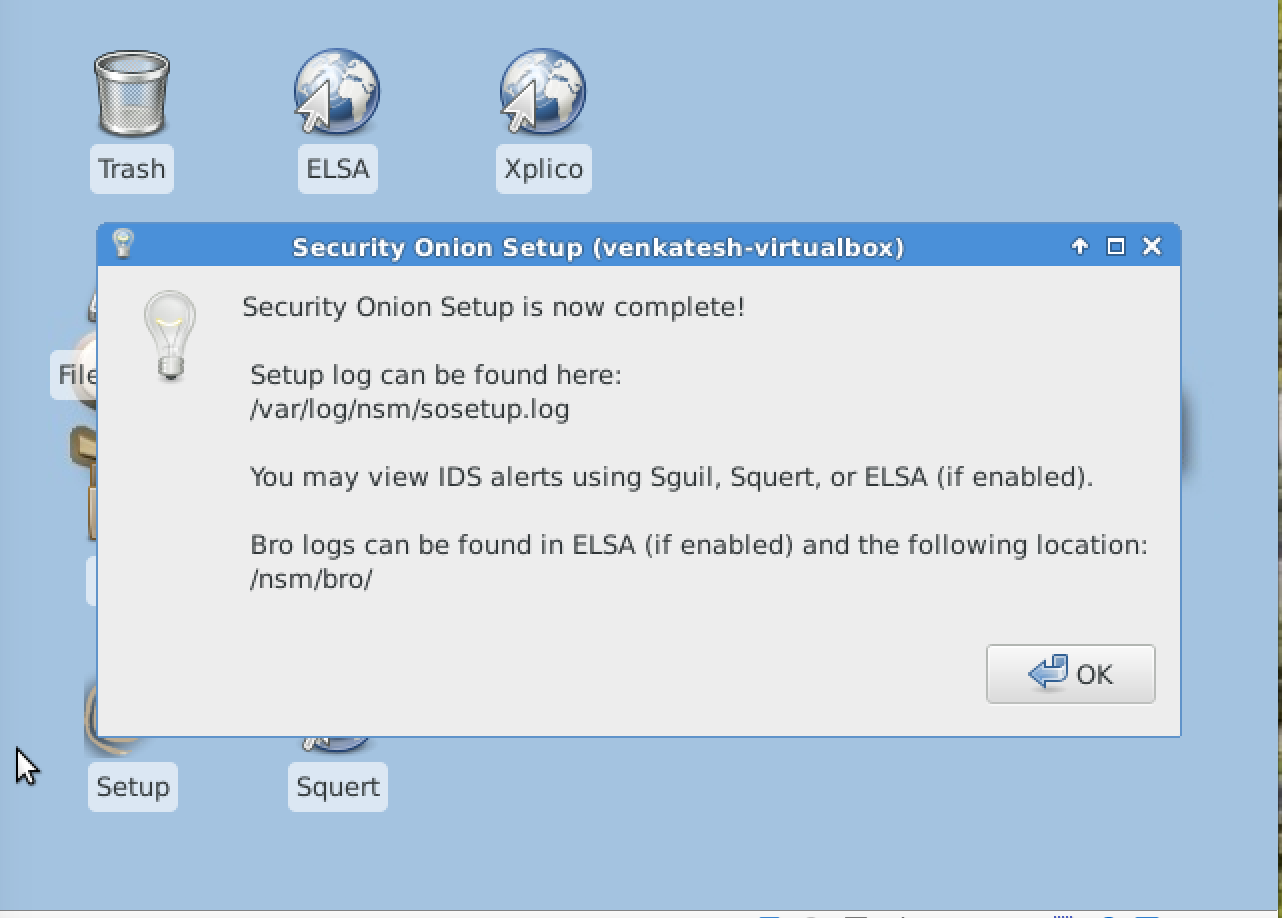
1. Download the iso file of operating system using below URL

<https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md>

1. RAM: 3 GB
2. Memory: 10 GB
3. Set up a Secured Onion VM using Virtual Box/VM Ware software

***Note: Make sure to you enter number of processors as 2 while configuring VM***

1. Click setup application on the desktop and give password to perform installation task.
2. Select DHCP, since it is evaluation mode and it will ask for reboot. At this point go ahead and reboot the machine.
3. After reboot, again click on setup application and select evaluation mode.
4. Then it will prompt to create username and password for Sguil.
5. After creation of Sguil you will get below image.



1. Click ok to complete Security Onion setup.

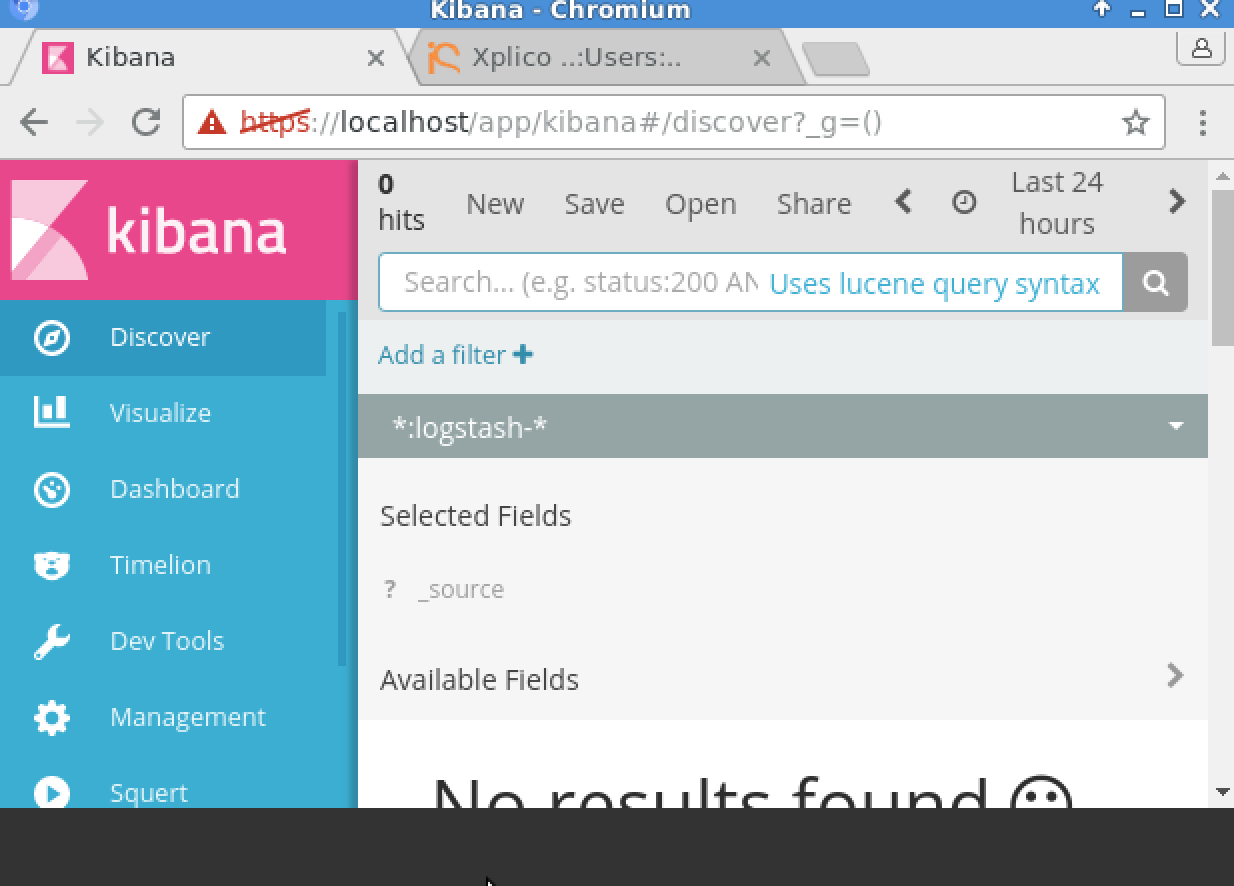
**ELK Stack Setup:**

1. Open the terminal and type below command to download setup files.

wget <https://raw.githubusercontent.com/Security-Onion-Solutions/elastic-test/master/>

securityonion\_elastic.sh

1. sudo bash securityonion\_elastic.sh
2. It will take around 20 to 30 minutes to complete the setup.
3. Once setup is done enter-<https://localhost/app/kibana> in the browser.

****