**Security Onion**

DCOIDM Buck Shot Yankee uses a freeware Linux toolbox know as Security Onion (*SO*) to aggregate and analyze network traffic flow in target environments. Pending approval by local network administration, a SO server will be installed alongside the main server cluster of the target environment and configured to listen for network traffic. This guide assumes the target environment will be using VSphere as their VMware manger.

1. Security Onion Instillation:
2. Acquiring Installation Media:

https://Securityonion.net is the primary source for ***SO*** media and online documentation. The “Downloads” tab on the home page of the website redirects to a *Github* portal containing the most current version of the ***SO*** .ISO file (Version 16.04.6.3 at the time this guide was written).

The ISO file should be downloaded and verified on local media prior to any live application. An external harddrive containing this file, as well as any additional tools required by the team, is recommended bearing in mind that all tools and media will need to be replicated across both NIPR and SIPR enclaves. Additionally, forward deployed networks and many target environments will be operating on minimal bandwidth without access to a standard white-line. Attempting to update currently running services in these environments is not recommended and all steps should be taken to ensure that all software taken to the target environment is already configured with any and all recent changes.

https://Securityonion.net also provides a link to the manufacture’s documentation for further clarification on ***SO*** installation and capabilities.

1. Types of Deployment:

Buck Shot Yankee uses ***SO*** in one of two configurations depending on the target environment, Standalone and Master Sensor.

A standalone deployment of security onion is the standard light weight deployment for small to moderately sized networks. The entire system is contained in one virtual server, collecting packets and preforming analytics at the same time. To provide a measure of scope and scale, a single standalone server, when adequately provisioned with network resources, proved entirely capable of mission requirements on the NIPR enclave of MWX 2019.

The master sensor deployment provides a wider base for packet collection than the standalone option. A master server is established alongside the main server cluster of the target environments which collects network analytics from any number of sensor servers deployed throughout the network. This method of deployment allows the team to forward traffic from multiple network locations, but is subject to network limitations and interruptions. A master sensor deployment is best suited for a wide spread target environment or large-scale enterprises.

1. Hardware Requirements:

Hardware requirements are as follows for both anticipated set ups:

* Standalone: A minimum of 4 CPU cores and 8 GB RAM. Storage is based on network traffic but is recommended between 2-4T B for a 5 day operation.
* Master Server: A minimum of 8 CPU cores and between 16-32 GB RAM. Storage should be modeled after network requirements. 3-6 TB is recommended.
* Sensor: A minimum of 6 CPU cores and between 8 GB RAM. Storage should be modeled after network requirements. 3 TB is recommended.

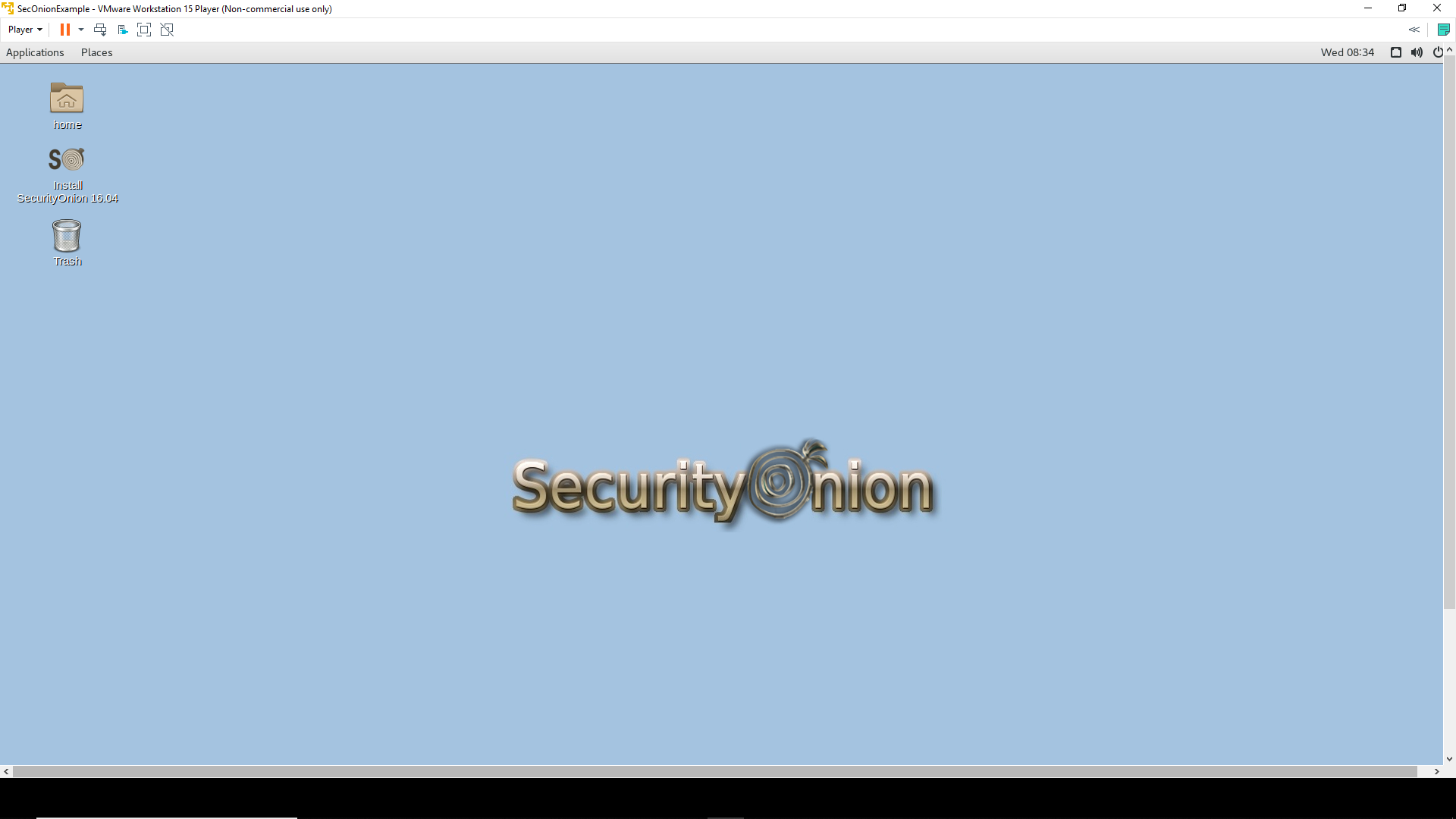
These storage requirements are manufacturer recommendations and best practices, but they can be scaled down to limit the resource footprint of the team in target environments via configuration found on then image after installation.

1. Networking Requirements:

The Master server must be able to communicate directly with any sensors deployed on the environment. A stand alone ***SO*** server and any sensors must have a **Promiscuous Mode** interface, referred to as a **Sniffing Interface** during ***SO*** installation, on a switch configured to pass mass network traffic. The interface will be configured during installation of the image, but the surrounding environment will, in most cases, need to be adapted to enable packet capture. Ensure that the sniffing interface is on a virtual switch with promiscuous settings enabled and that all Vlan traffic is being successfully routed to the port group.

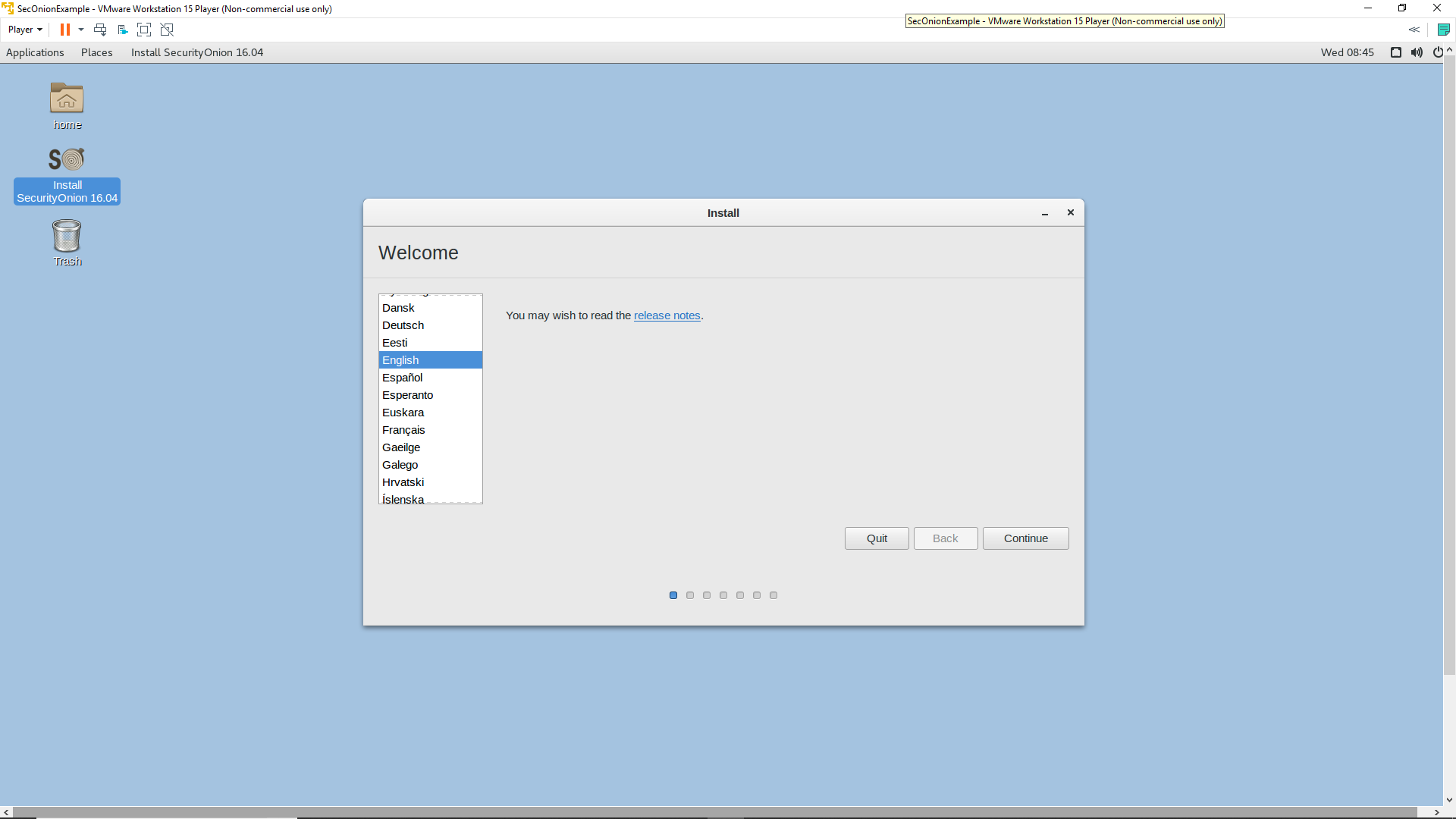
1. Basic Installation:
2. Create the virtual machine and upload the image:

* Security Onion is an Ubuntu based Linux deployment. The virtual disk should be configured for multiple files. Master Servers require 1 network interface. Standalone deployments and Sensors require 2 network interfaces, a management interface and at least one sniffing interface.



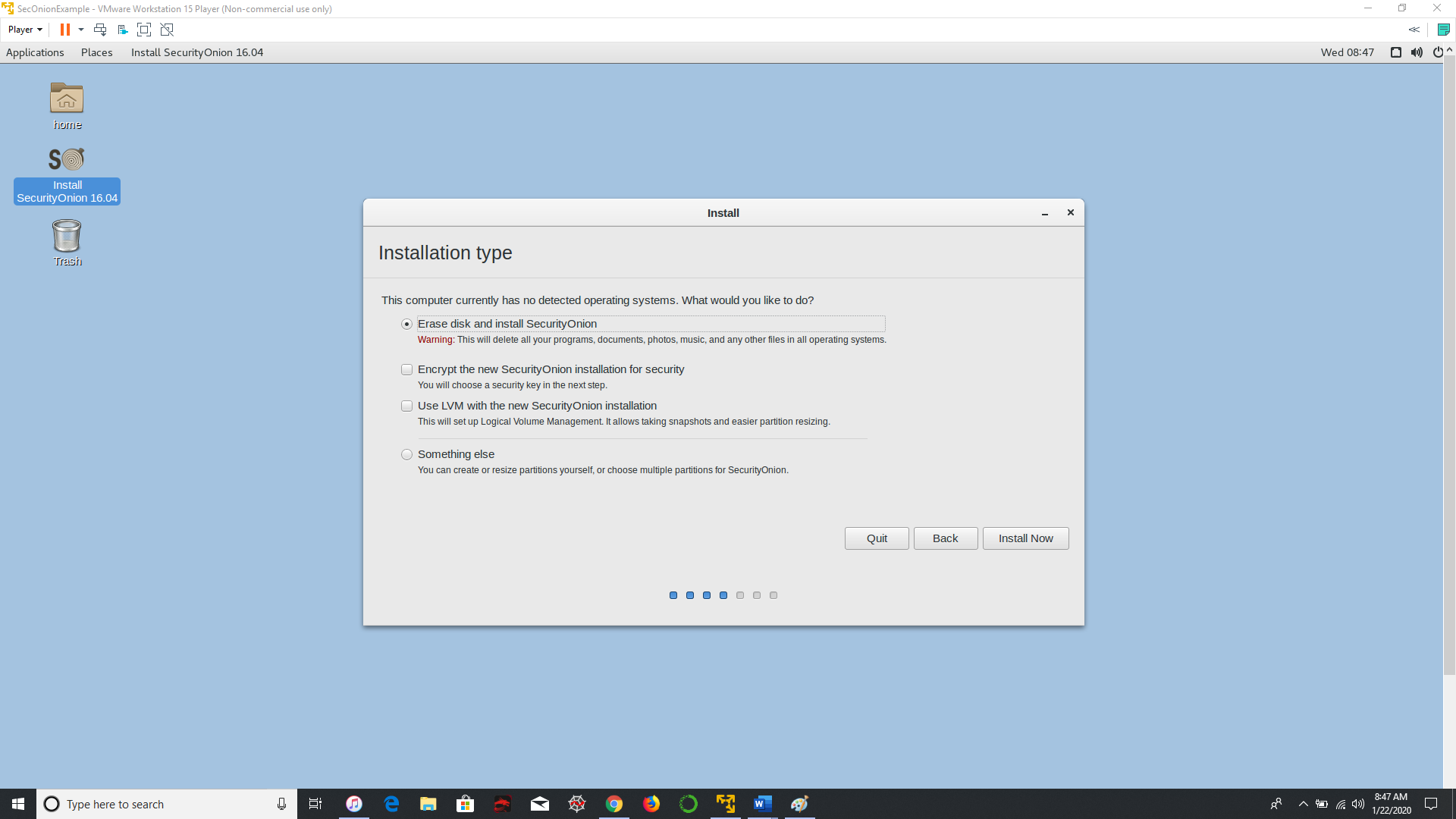
1. Double Click the Install SecurityOnion Icon on the Desktop.

* For further clarification on this, consult your MOS monitor.



1. Follow on Screen Prompts.

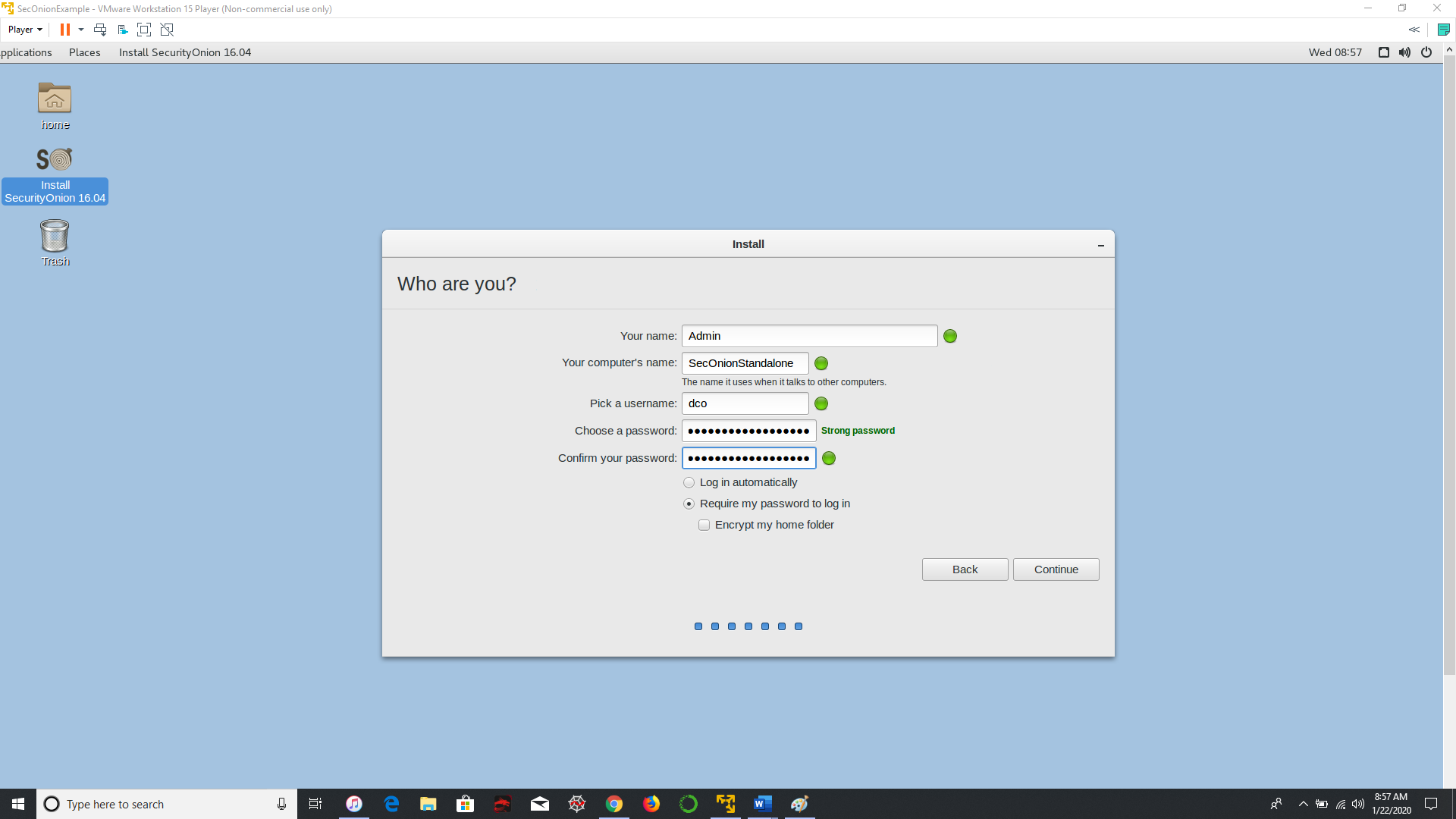
* The install wizard will begin to run, presenting standard configuration options. The options used by Buckshotyankee will be listed to prevent confusion during installation:
* When prompted, do not select either options for updating or drivers. These attempts will most likely be impossible during installation in tactical environments.
* At the “Installation Type” screen ensure “Erase Disk and Install Security Onion.” Is selected.



* Select the most relevant time zone to reflect mission requirements.
* Keyboard layout will be English (US), aka moonlanding enslish.

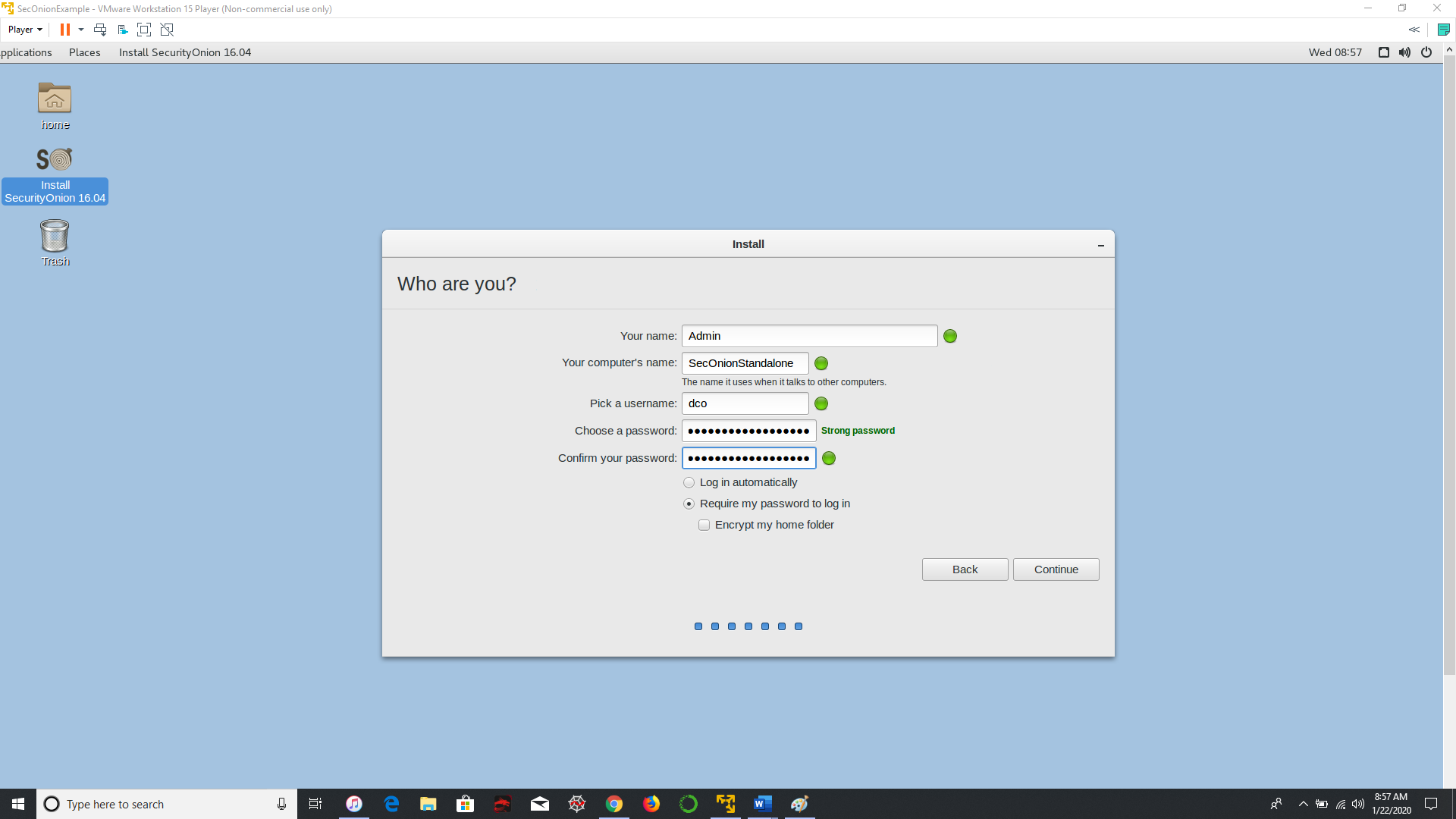
1. Configure Initial Account and Computer Name.

* Your Name = Admin
* Computers Name = SecOnion+Master/Sensor/Standalone, depending on deployment.
* Username = dco
* Password = dcoidm1721DCOIDM!&!@
* This password should be changed/kept secure to fit mission requirements. This is the standard installation build.



1. Installation Completes and System Restarts.
2. Begin Setup.
3. Configure Network Interfaces.

* Set up will prompt network interfaces before progressing to granular settings.



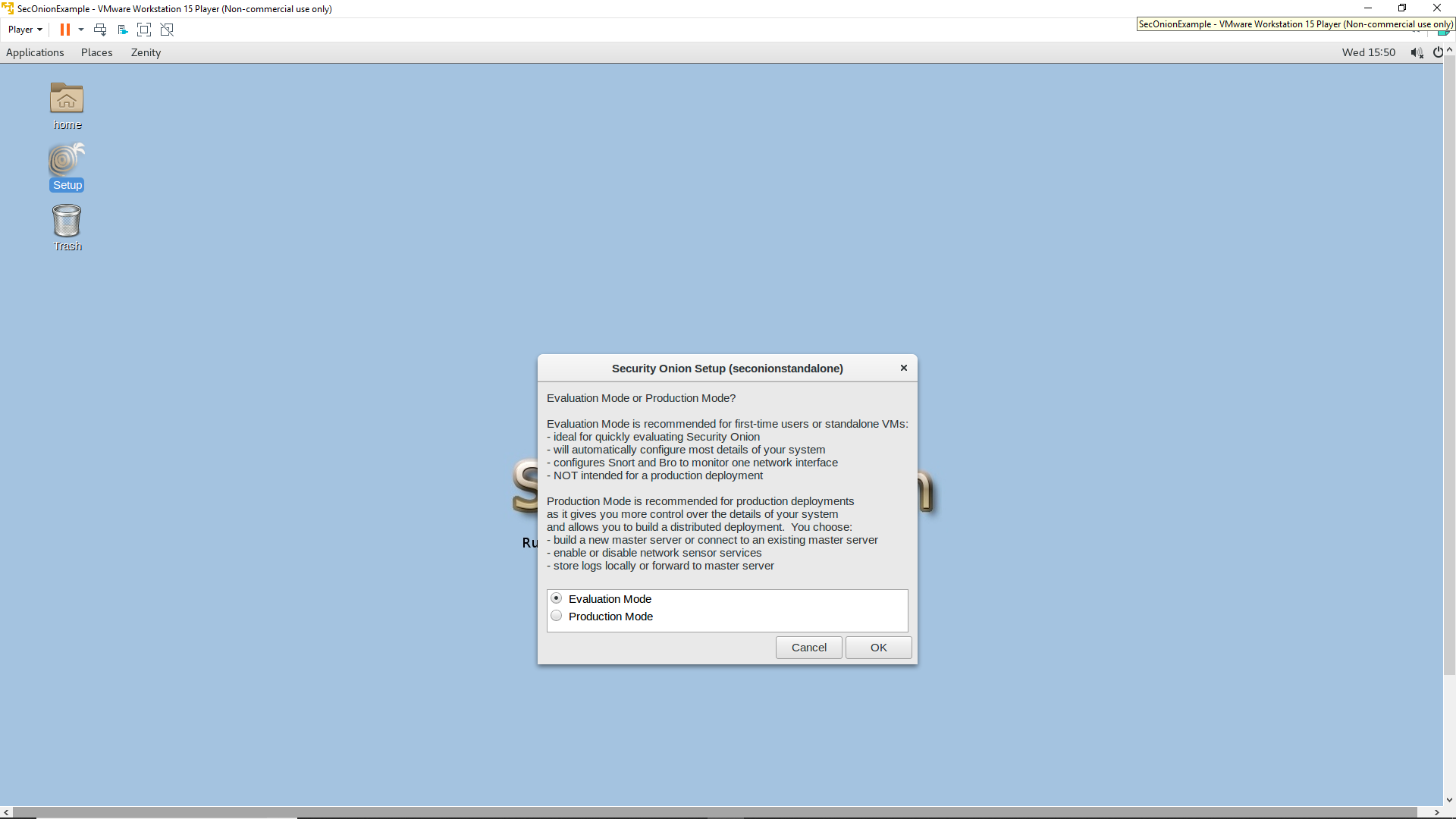
* Configure management interface, static addressing is strongly recommended.
* Follow on screen prompts to enter networking information and domain.

**\*A Master Server will only configure a management interface. For both Sensors and Standalone deployments continue to configure sniffing interfaces. \***

* In most cases only one interface will be selected and placed on the network as a sniffing interface. Cases requiring separate sniffing interfaces are rare and are more easily solved by implementing another sensor on any disparate network segments.
* The image will reboot after network interface configuration.

1. Continue Setup.

* When prompted this time select ‘Yes, skip network configuration.’
* Proceed to the Evaluation VS Production screen.



**\*At this point in installation Master/Sensor and Standalone deployments begin to diverge. Production Mode is used for both deployments. Sensors will be added to an existing build, all others will start a new instance of Security Onion. Return to this point in the guide to configure different permutations of *SO* servers. \***

1. Standalone or Master server configuration:
2. Select Production Mode and continue.

* Indicate a New build for Master Servers and Standalone deployments.

1. Create the first user.

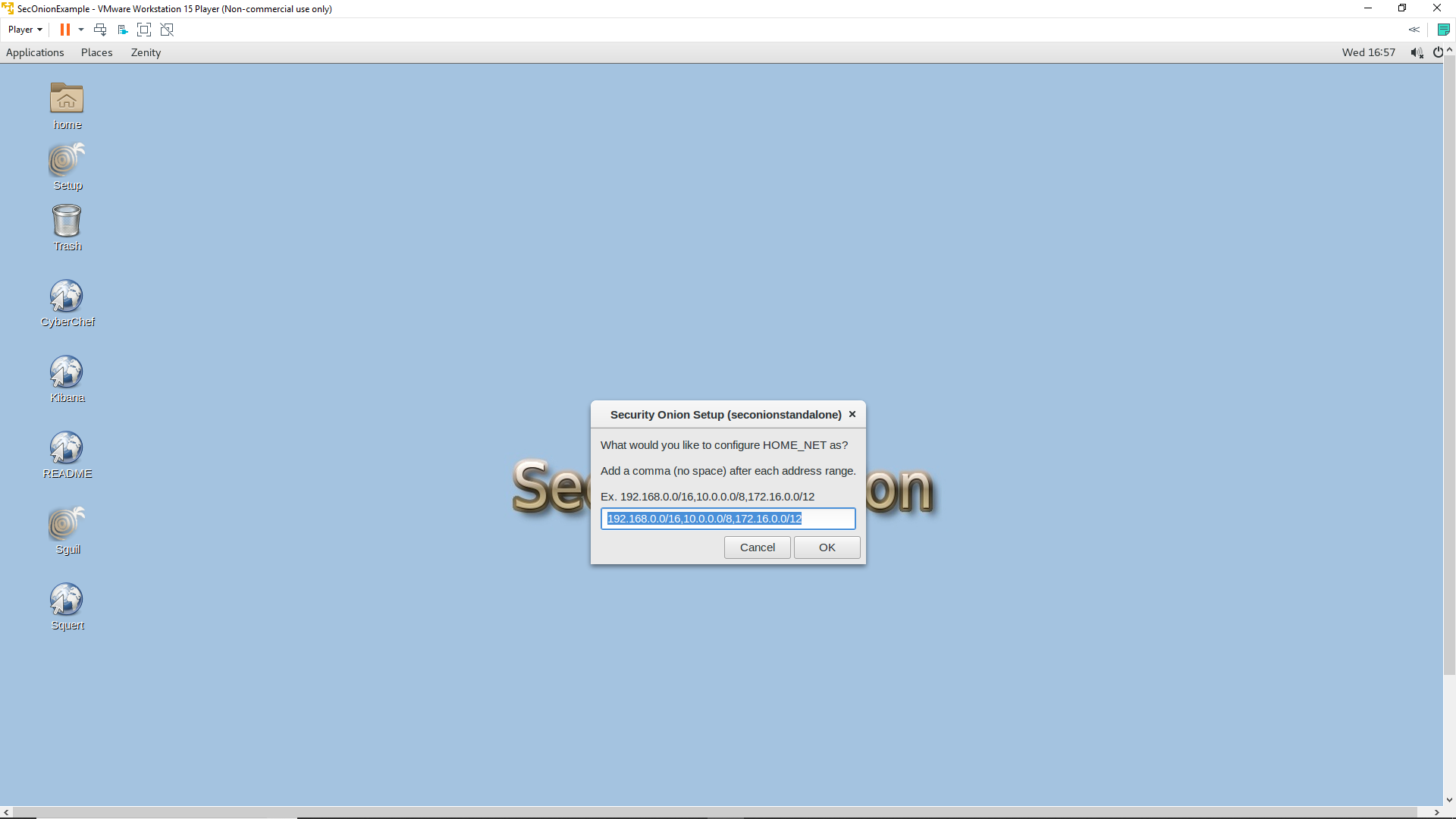
* Username = dco
* Password = dcoidm1721DCOIDM!&!@
* This password should be changed/kept secure to fit mission requirements. This is the standard installation build.

1. Select Custom.

* Days of Alerts = 30
* Days of data for Squil = 7
* IDS ruleset = Emerging Threats Open
* IDS Engine = Snort
* Enable network sensor services
* PF\_RING min\_num\_slots = 4096
* Sniffing interface should be monitored. \***Master Servers will *not have* a sniffing interface. \***
* Enable the IDS Engine

1. Establish the Home\_net.

* The Home\_net is the network range the sensor will be covering, which includes every subnet specified by the mission. Ranges will be added to the input box as shown, separated by commas.



1. Enable Bro.

* Yes, enable file extraction.

1. Enable full packet capture.

* Packet captures will be 768 MB
* Enable mmap I/O.

1. Set PCAP ring buffer to 128 MB.
2. Set disk usage percent to 90
3. Enable Salt
4. Enable Elastic Stack.
5. Yes, store logs locally.
6. Set disk space for Elasticsearch logs equal to 1024 GB.

- This assumes total disk space is multiple Terabytes. Do not exceed 90% of total disk space.

1. Proceed with changes. Setup is complete after the host restarts.

**\*At this point a standalone or Master server is completely configured. \***

1. Sensor Configuration:

Ensure that a Master server is active and running in the intended environment before configuring the sensor. Before configuring a security onion sensor open a terminal on the master server.

* Use the sudo so-allow command
* Enter ‘S’ for the new selection
* Input the future IP address of the sensor.
* Press enter
* Proceed with Sensor configuration.

1. Select Production Mode

* Indicate an existing deployment.

1. Enter the IP address of the master server.

* Username = dco

1. Select Forward Node.
2. Select Custom.

* PF\_RING min\_num\_slots = 4096
* Sniffing interface should be monitored. \***Master Servers will *not have* a sniffing interface. \***
* Enable the IDS Engine.

1. Establish the Home\_net.

* The Home\_net is the network range the sensor will be covering, which includes every subnet specified by the mission. Ranges will be added to the input box as shown.

1. Enable Bro

* Yes, Enable File extraction

1. Enable full packet capture.

* Packet captures will be 768 MB
* Enable mmap I/O.

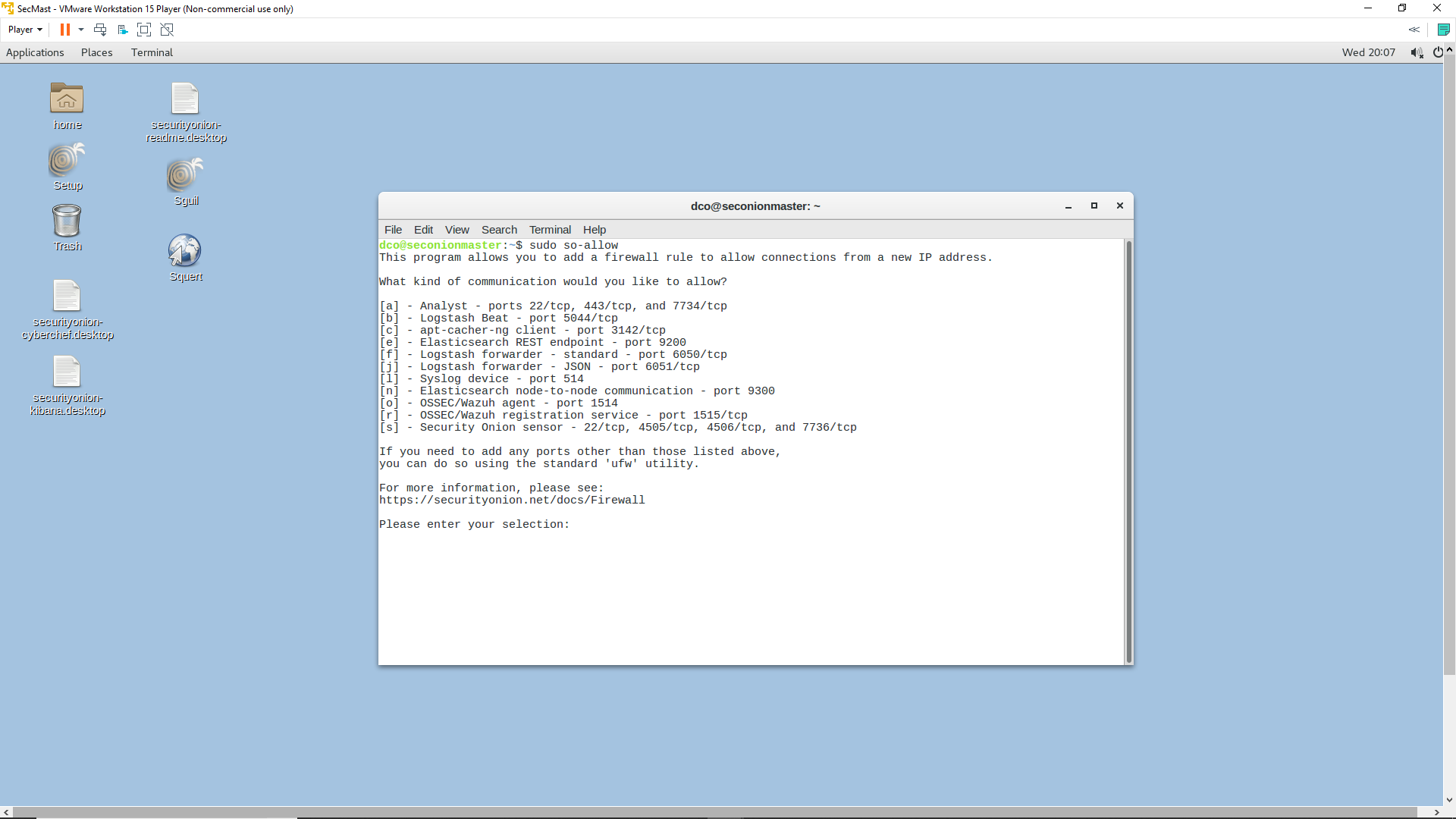
1. Set PCAP ring buffer to 128 MB.
2. Set disk usage percent to 90
3. Enable Salt
4. A console window will open. Type ‘yes’ and enter.

* Password = dcoidm1721DCOIDM!&@!
* The words ‘Skipping adding existing rule should appear.’

**\*Sensor configuration is Complete. \***

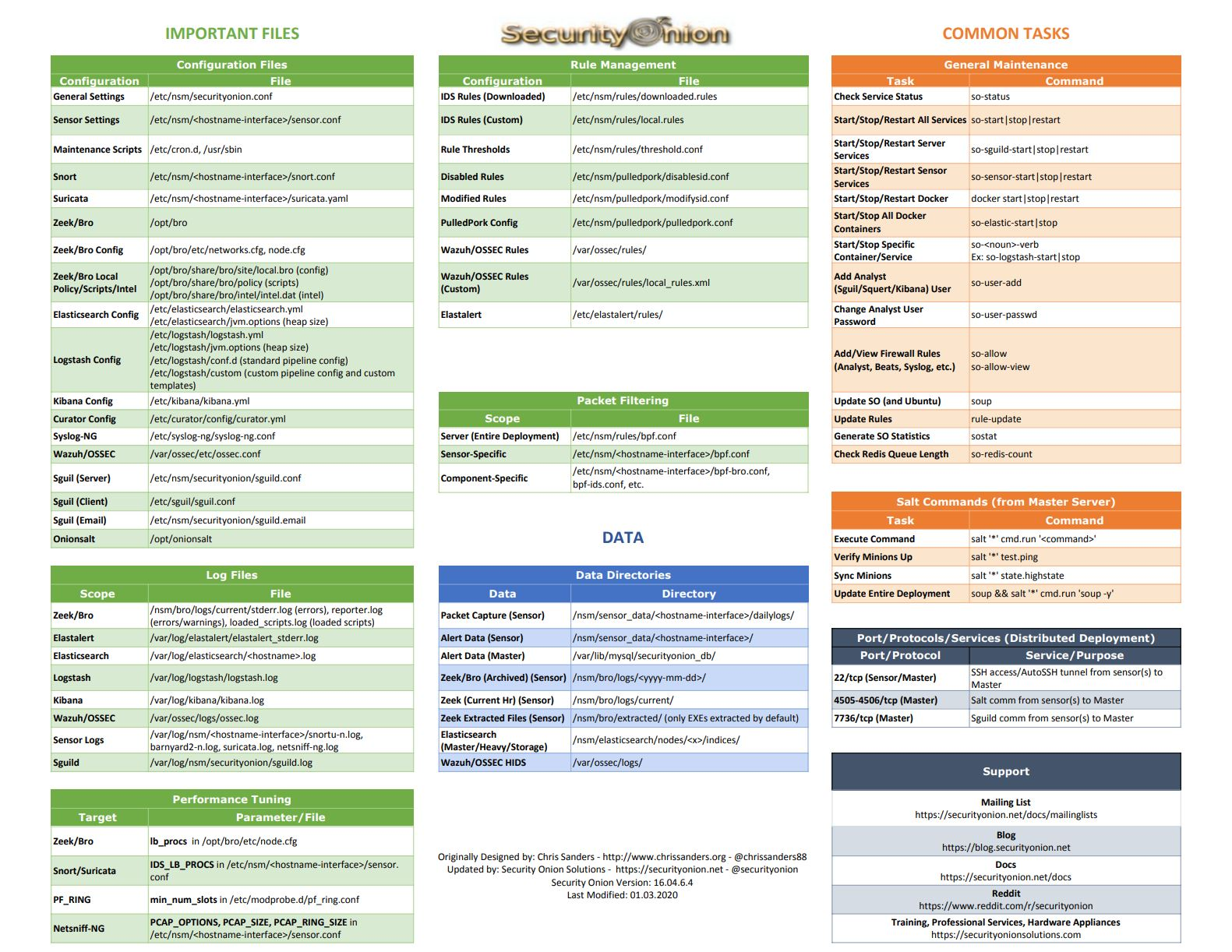
1. Console Commands and Permissions:

After configuring the server, the next priority is to get access to Kibana and begin hunting. In order to do so permissions need to be assigned to analyst boxes. In addition, expanded capabilities need to be accounted for. Many of these are enabled through the so-allow command on the Master Server.



Security onion can be navigated like any number of similar Linux systems though the terminal. Packet captures can be accessed at /nsm/sensor\_data/seconionscanner-ens34/daillogs/

A cheat sheet of useful commands has been included at the end of this guide to assist with navigation.





Credits:

Author, Creator, Sudo-Diety,

Sgt Ian McConnell.