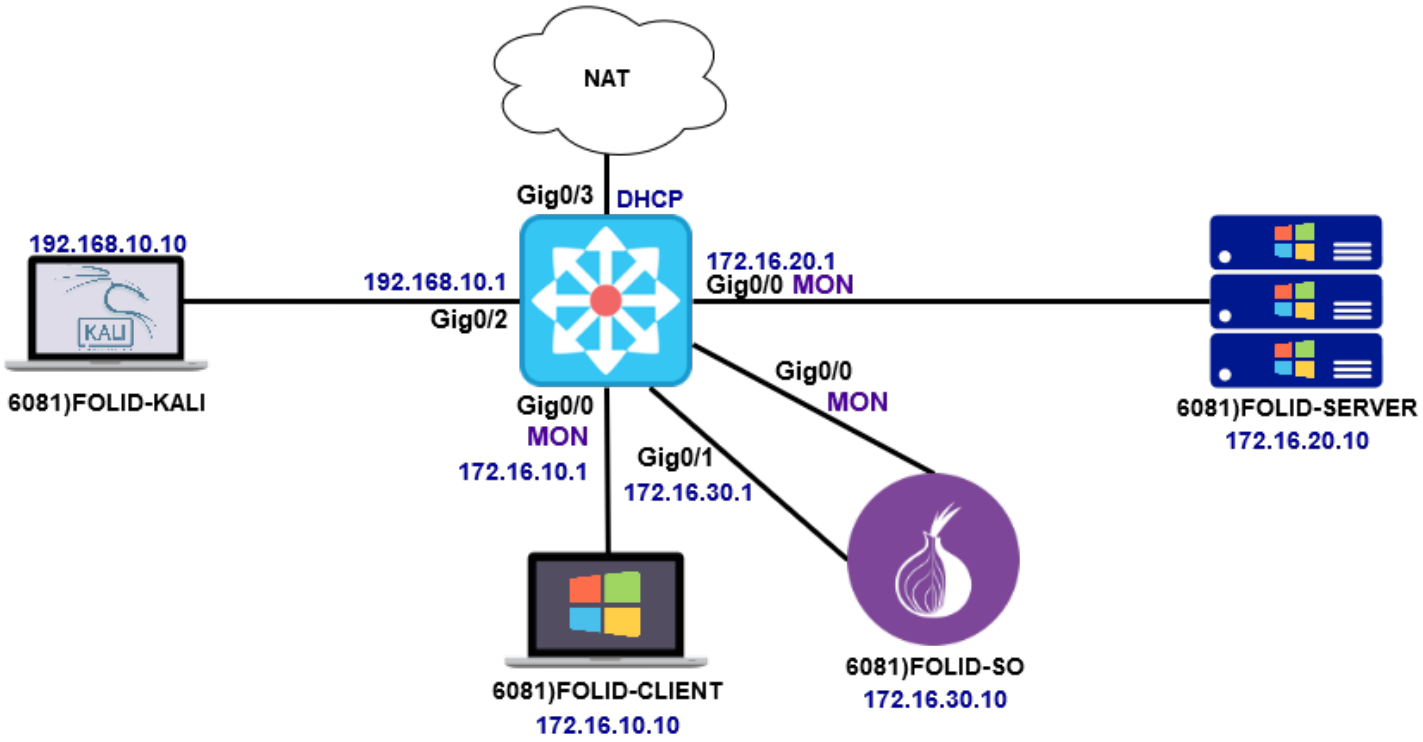
Lab 2 – Installing Security Onion

Lab Topology and Learning Goals



In this lab you will setup your lab environment to simulate and monitor networks attacks

Required Resources

- **VMware Workstation 15**

Active Hosts

- **6081)Router**
- **6081)FOLID-SO**
- **6081)FOLID-SERVER**
- **6081)FOLID-CLIENT**

Submission Instructions

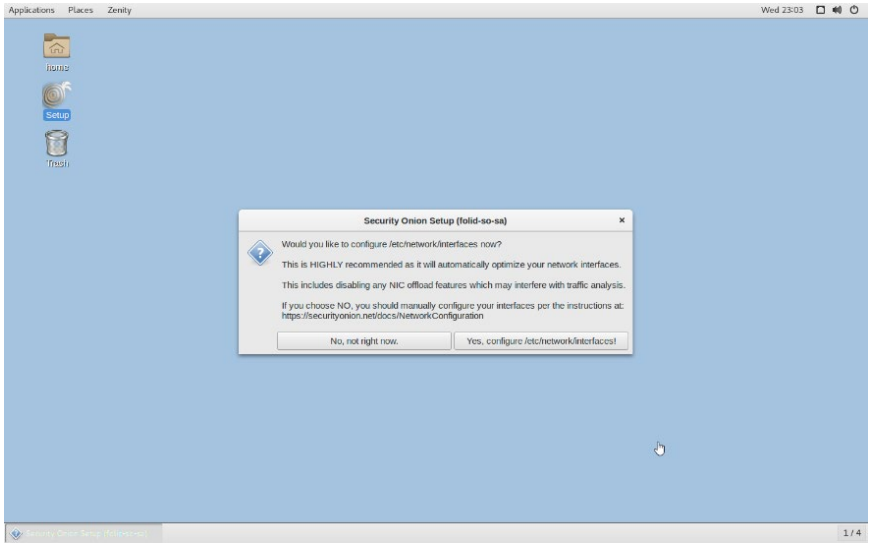
Submit your completed lab to the appropriate lab quiz on FOL

- You can attempt the quiz multiple time, but only the last attempt will be graded
- Submissions are accepted until 11:59 PM of the same day
- Submissions by email will not be accepted
- All screenshots must include you FOLID (where FOLID is your FOL username)

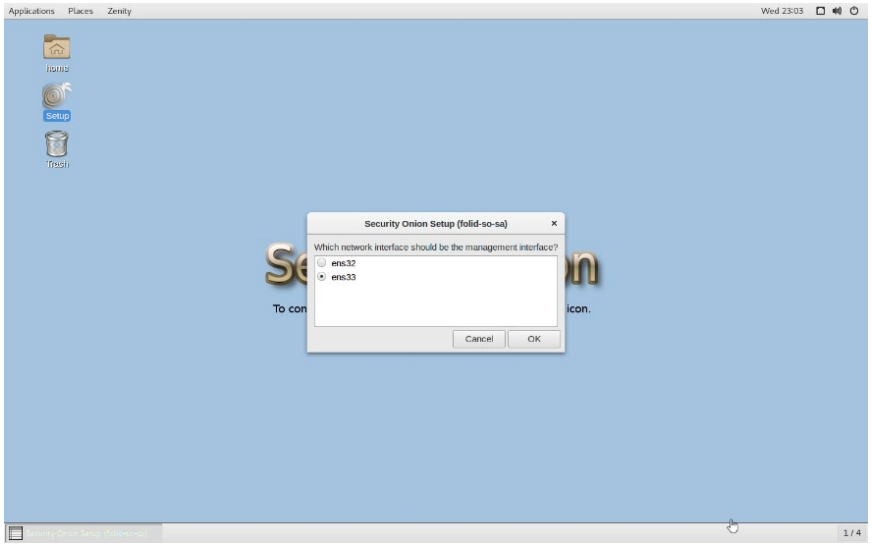
Lab 2 – Installing Security Onion

Configuring Security Onion – Stage 1

Power on the SO host; when loaded to the desktop, double click the **Setup** icon to begin the first stage of the configuration process

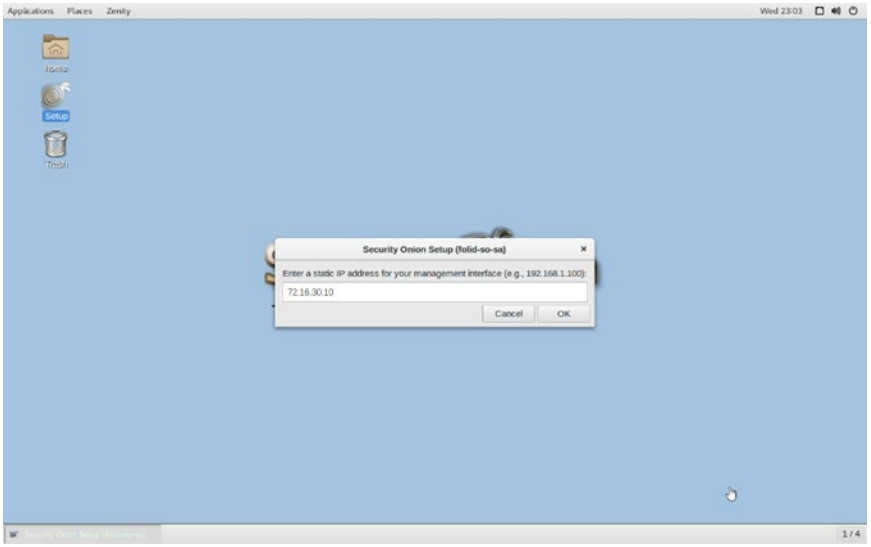


When prompted, select **Yes** to configure network interfaces



Select the interface that will be configured as the **management** interface, in this case, select **ens32**

Lab 2 – Installing Security Onion



Configure the interface with the following settings:

Address Type: **static**

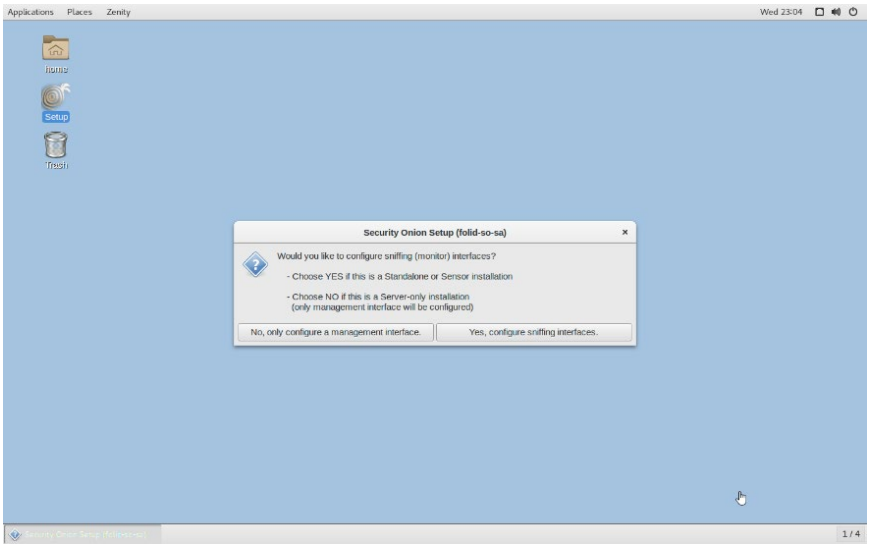
IP Address: **172.16.30.10**

Subnet Mask: **255.255.255.0**

Gateway: **172.16.30.1**

DNS Server: **1.1.1.1**

Local Domain: **fanco.com**



When prompted, select **Yes** to configure a **sniffing** interface

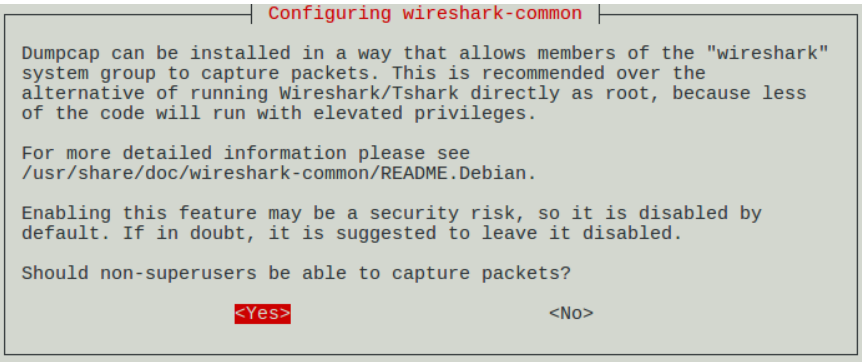
On the next screen, **ens33** should be the only available option

Confirm the changes to the interfaces and reboot the system

Lab 2 – Installing Security Onion

Configure Wireshark to Allow Non-Sudo Access and Test Monitored Interface

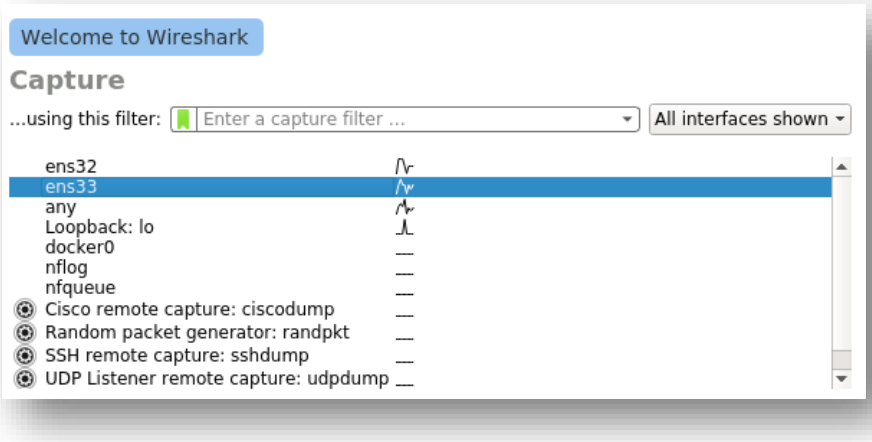
Open the terminal, and run the command: **sudo dpkg-reconfigure wireshark-common**



When prompted, allow non-superusers to be able to capture packets

Next, run the command: **sudo adduser administrator wireshark**

Reboot the host



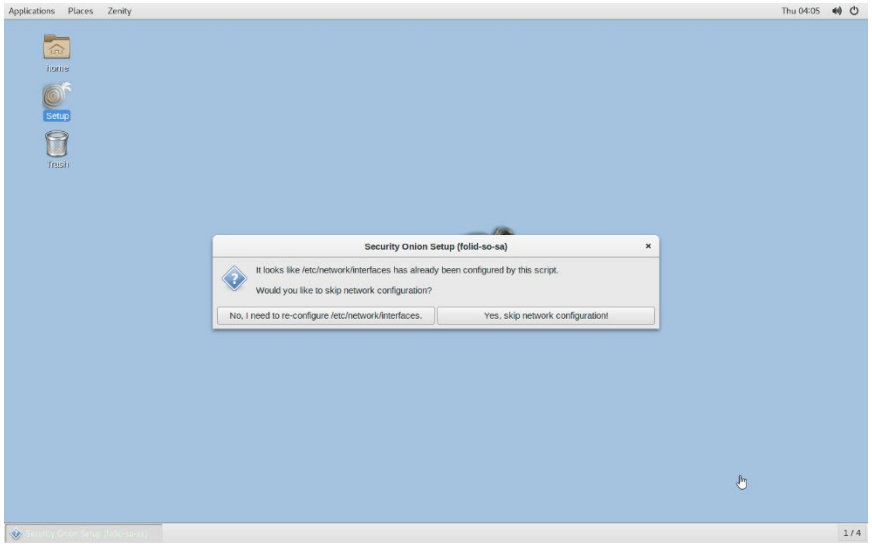
Confirm that the correct interface is set to monitored by opening Wireshark and starting a capture of the **ens33** interface

Generate some traffic by sending a ping from the **Windows Server to 1.1.1.1**, you should see both **Echo Request** and **Echo Reply** packets in the output.

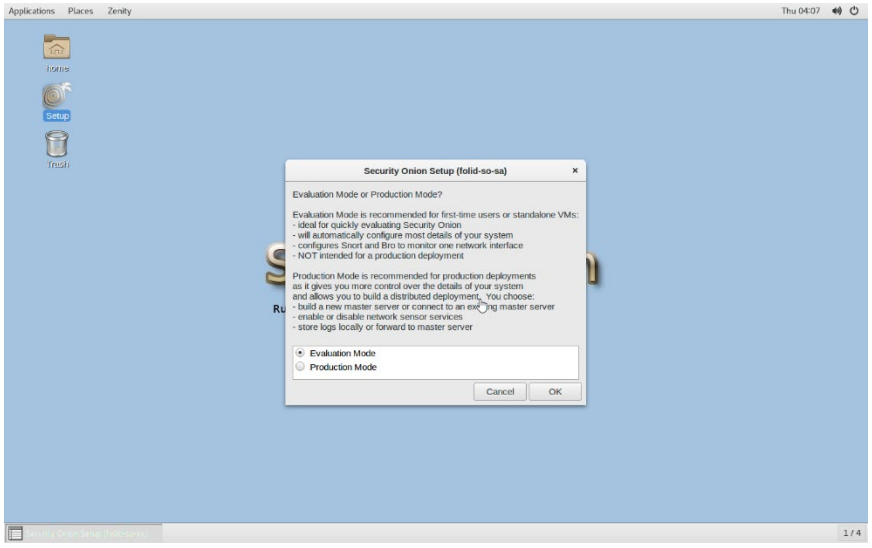
Lab 2 – Installing Security Onion

Configuring Security Onion – Stage 2

Begin the second stage of the setup by double clicking on the **Setup** icon once more



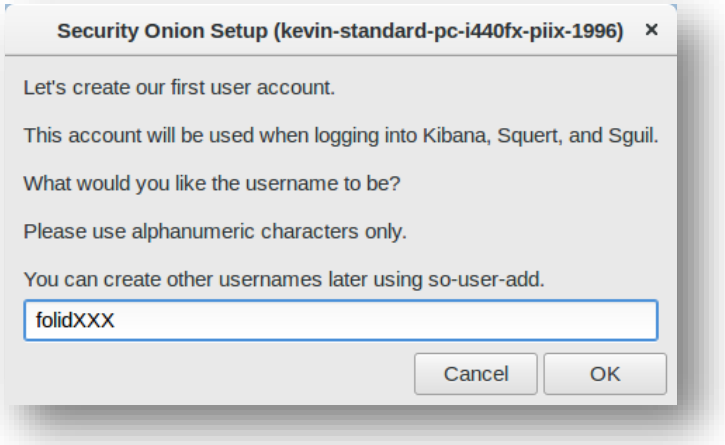
If your test concluded that you correctly configured the management and monitoring interfaces, you can skip the network configuration; otherwise, reconfigure the interfaces and correct the error



When prompted, select the option to install SO in **Evaluation Mode**

Continue with **ens33** as the **monitored** interface

Lab 2 – Installing Security Onion



Create a user with the name **folidXXX** (where folid represents your FOL username, and XXX represents the current semester code [Summer 2020 would be S20])

NOTE: The Security Onion SSO account is limited to 16 characters, if your FOL username and the semester code is longer than 16 characters, shorten your FOL username appropriately

Enter **Windows1** as the password, and wait for the configuration process to complete

Lab 2 – Installing Security Onion

Confirm Configuration Operation

When the install process is complete, open a terminal and issue the command: **ifconfig ens32 | grep 172.16.30.10.**

Then, issue the command **ifconfig ens33 | grep PROMISC.**

Add a screenshot of the output to the Lab 2 quiz, make sure you include your FOLID in the output.

Managing Security Onion Services

To manage the service states, run the following commands in the terminal:

To verify the state of services: **sudo so-status** (if any services show FAIL, you need to add more RAM). Logstash will take some time to fully start and may appear in a WARN state. Wait until all services are in an [OK] state.

Add a screenshot of the output to the Lab 2 quiz, make sure you include your FOLID in the output.

To start services: **sudo so-start**

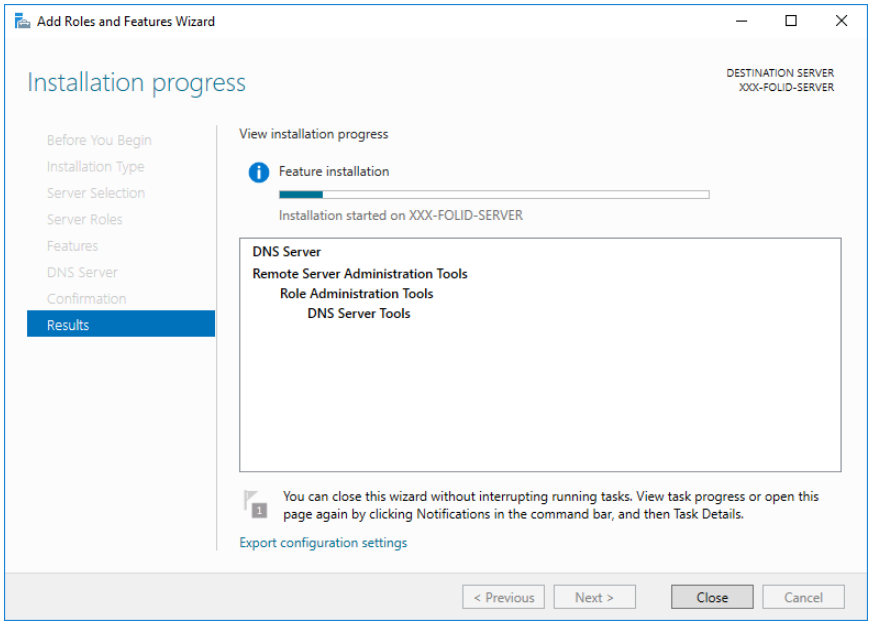
To restart sensor services: **sudo so-sensor-restart**

To view detailed statistics for services: **sudo sostat | less**

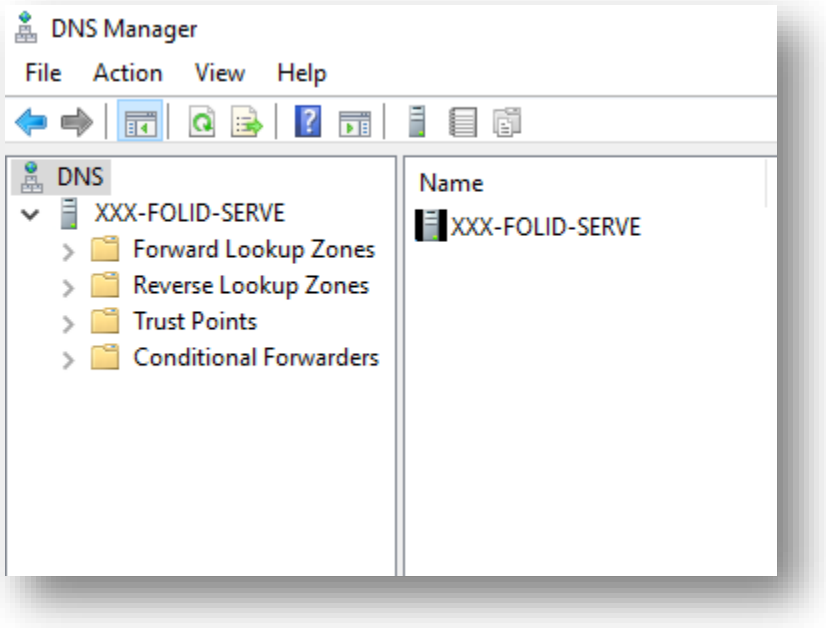
NOTE: Some of the management commands provided in the textbook have been depreciated

Configure DNS Services

If not already running, power on the **6081)FOLID-SERVER** host



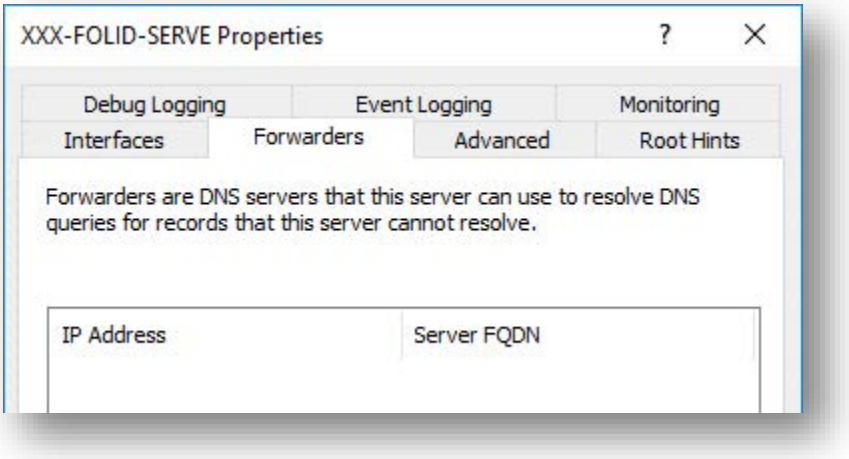
Add the **DNS Server** role to the host



Open the **DNS Manager**

Add a new Primary **Forward Lookup Zone** for the domain **fanco.com**

Lab 2 – Installing Security Onion



Edit the server properties, and add a **Forwarder** configuration, pointing towards the DNS servers located at **172.16.100.11** and **1.1.1.1**

Test DNS Resolution

On the **6081)FOLID-CLIENT** host, open the terminal and ping **google.ca**

Add a screenshot of the output to the Lab 2 quiz, make sure you include your FOLID in the output

In future labs, the **SO** host will take a long time to power on if you do a cold boot. The solution to this is to take a snapshot of the VM while it is still running. At the start of the next lab, instead of powering on the VM, simply restore the snapshot the running VM. While running, take a snapshot on the SO host called **Lab 2 complete**

Shutdown the **SO** host

Shutdown the other hosts and take a snapshot called **Lab 2 complete**

Submit your completed **Lab 2** quiz