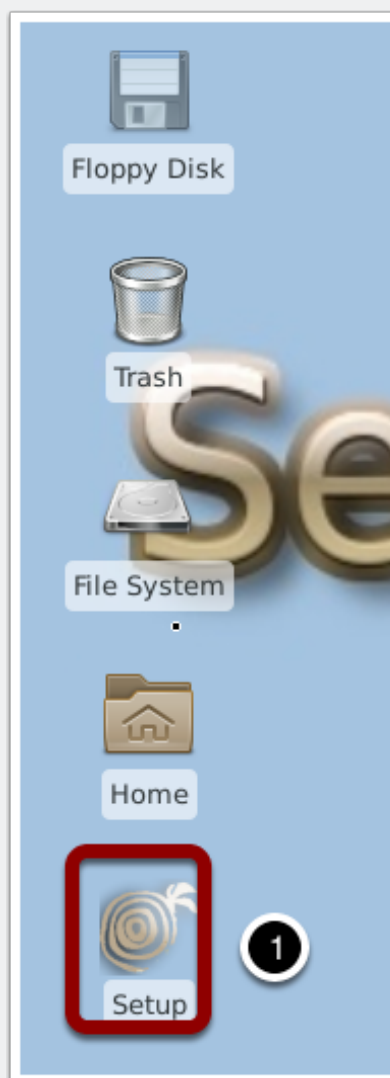


Security Onion Set Up Script

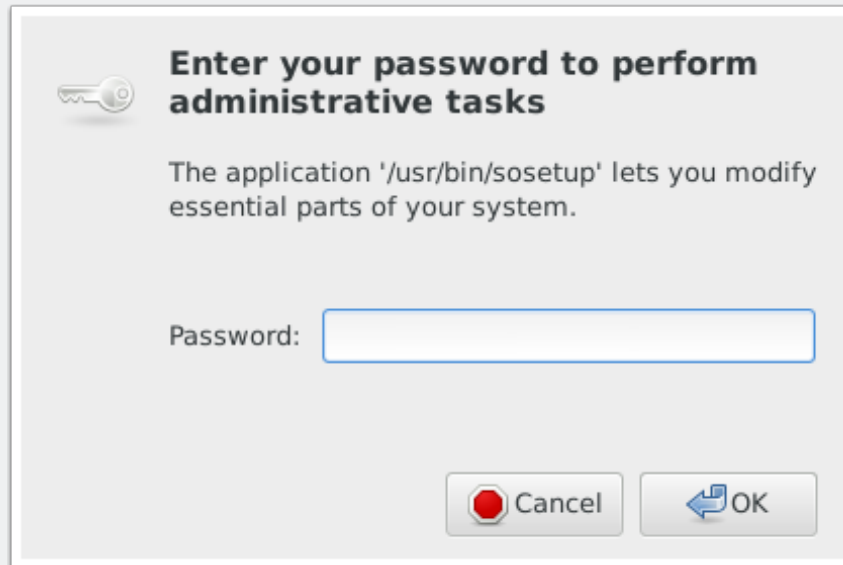
Login to your assigned Security Onion VM.

Double Click the Set Up Icon



Security Onion Set Up Script

Enter password

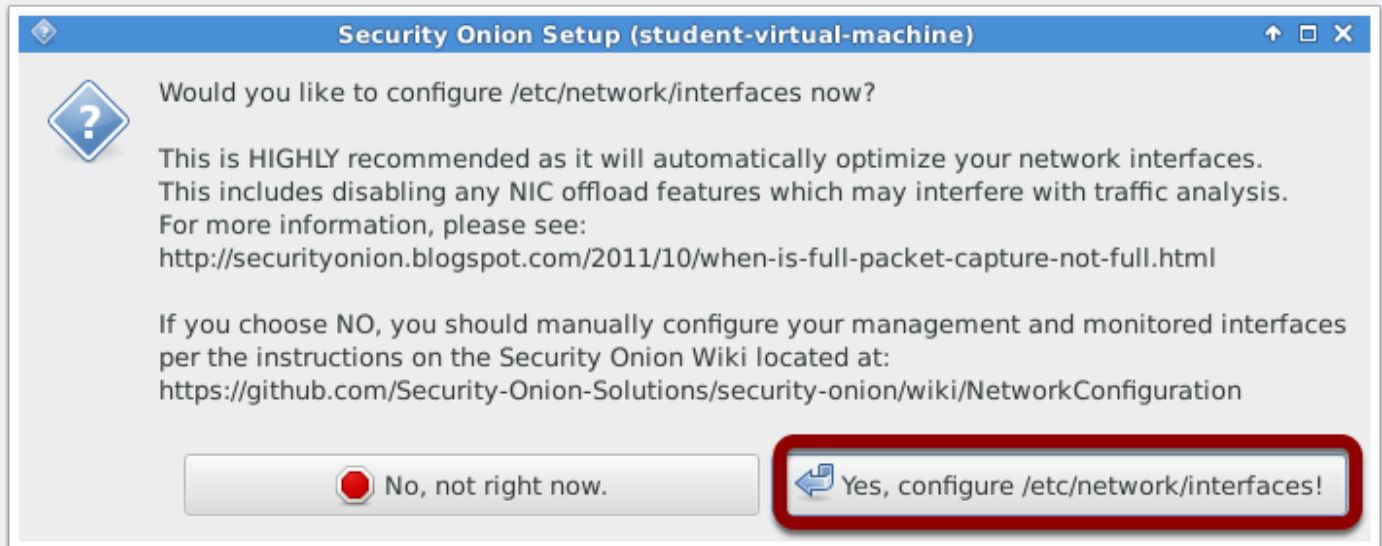


Click Yes

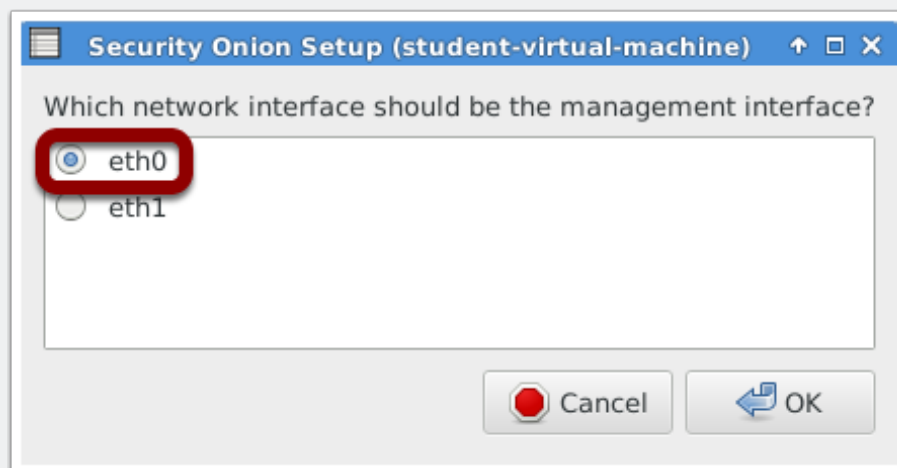


Security Onion Set Up Script

Click Yes

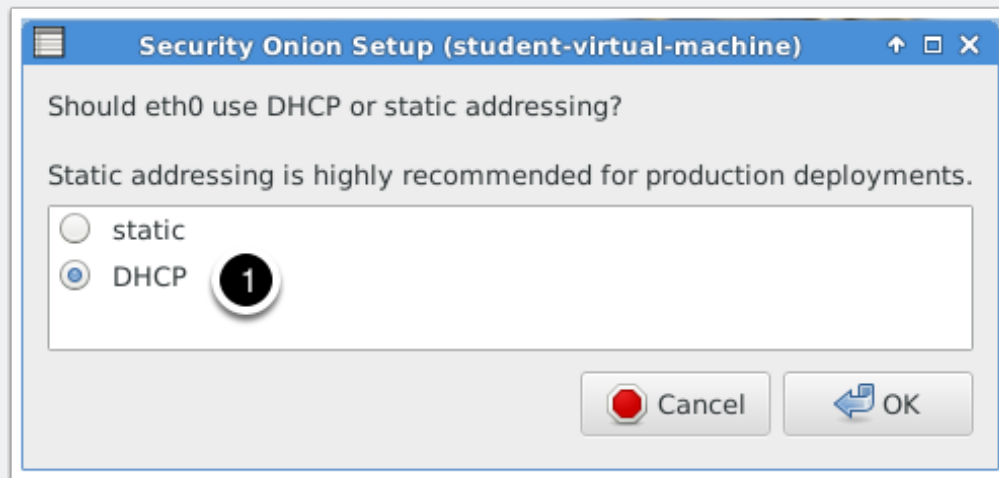


Select eth0

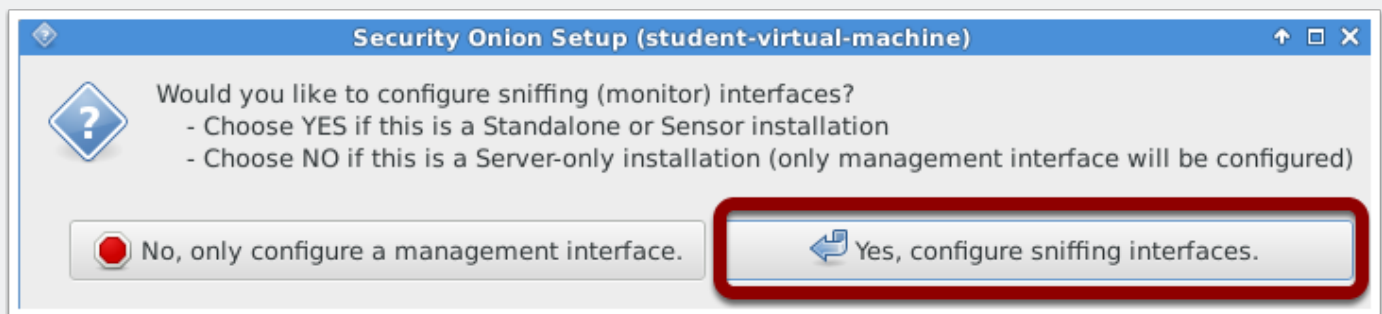


Security Onion Set Up Script

DHCP

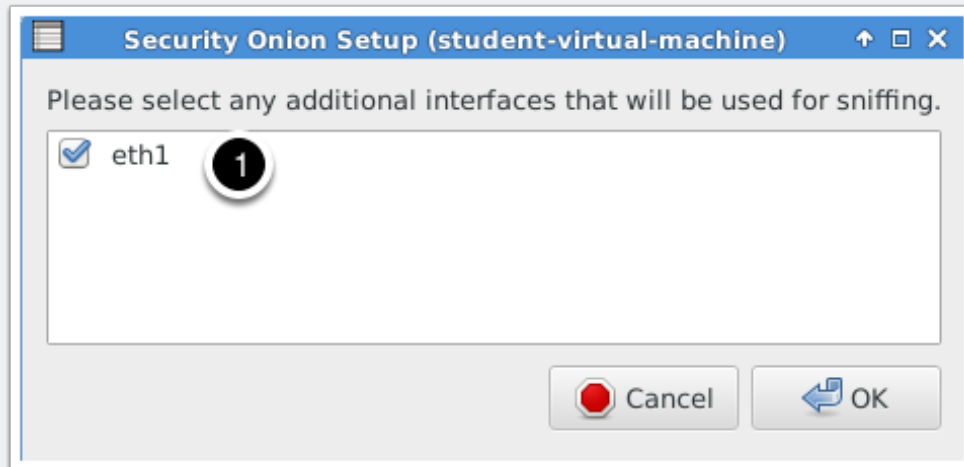


Click Yes

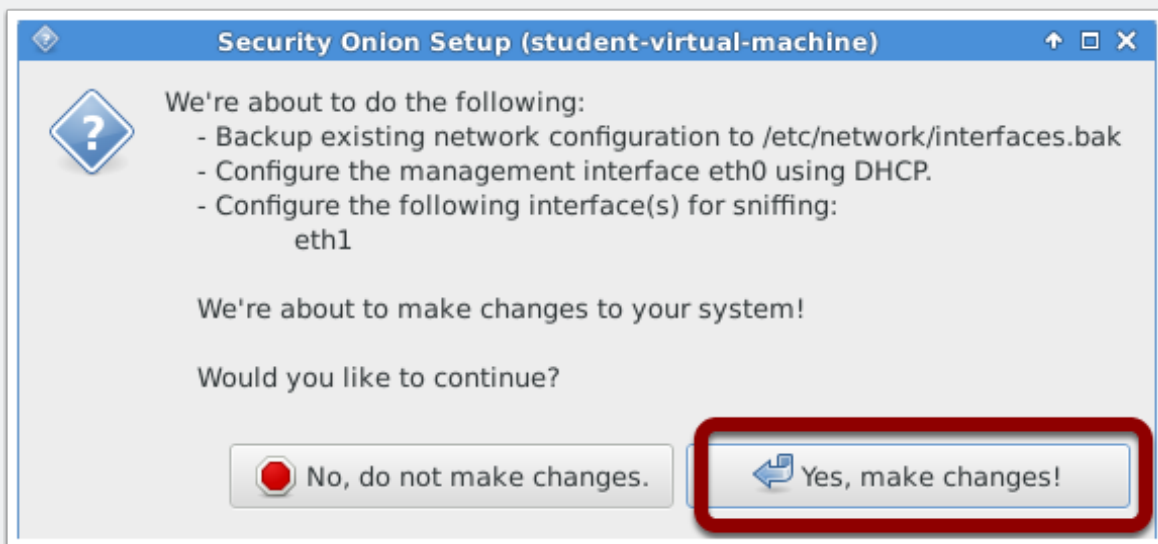


Security Onion Set Up Script

Select eth1

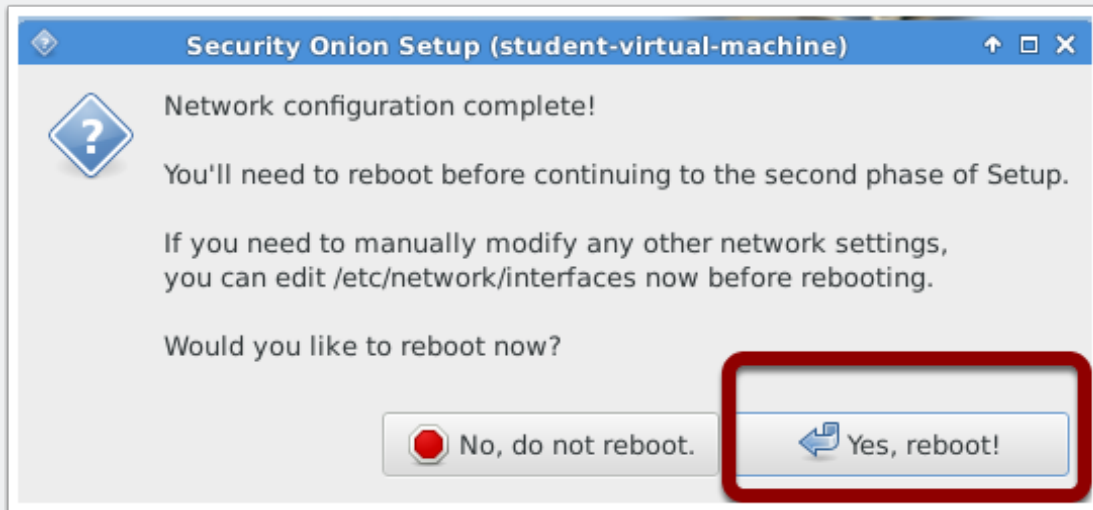


Click Yes

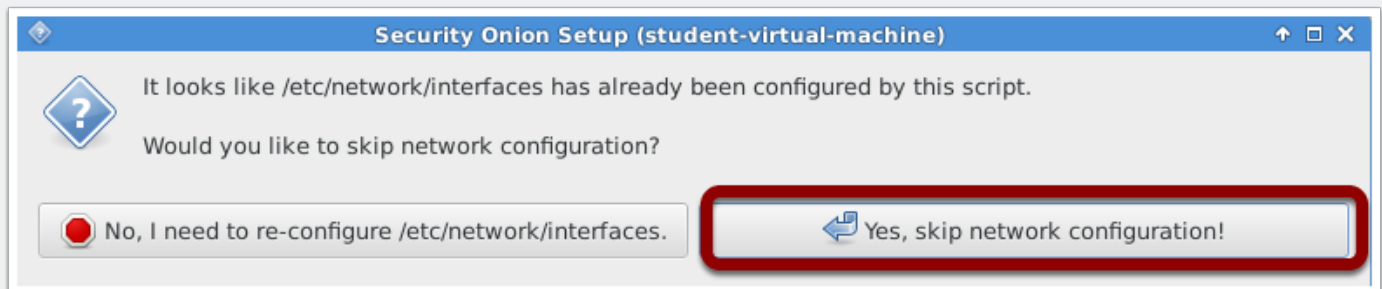


Security Onion Set Up Script

Reboot

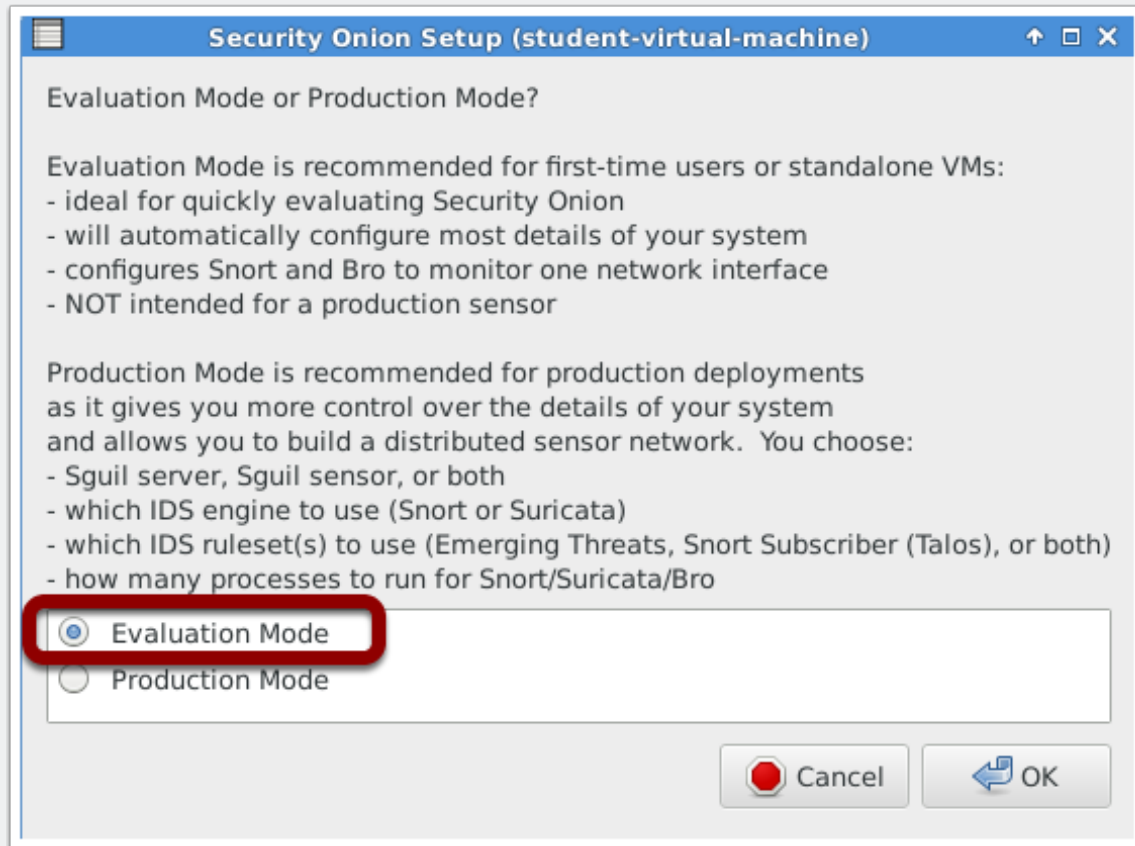


Run setup again but skip network config



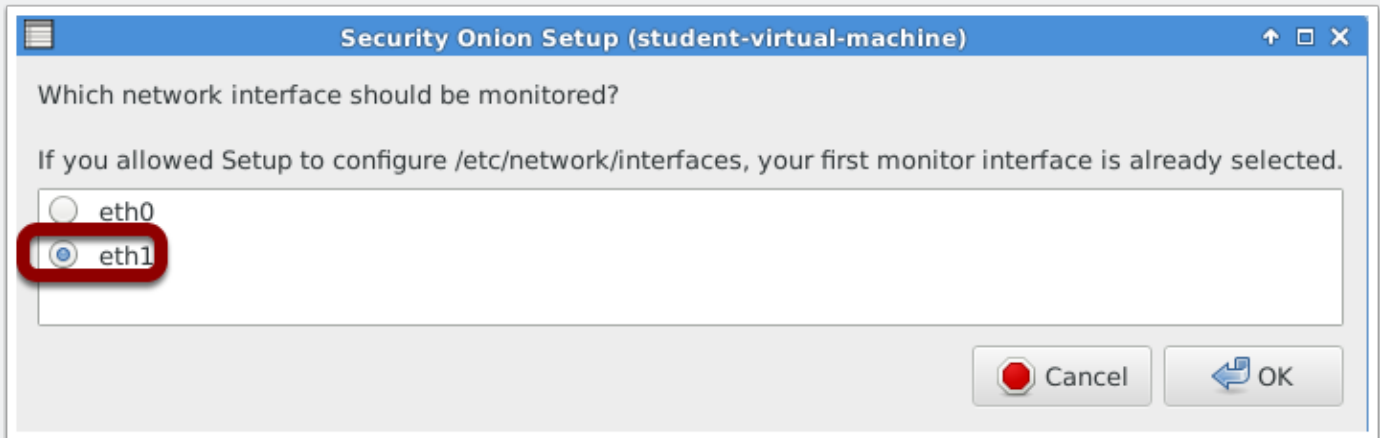
Security Onion Set Up Script

Evaluation Mode



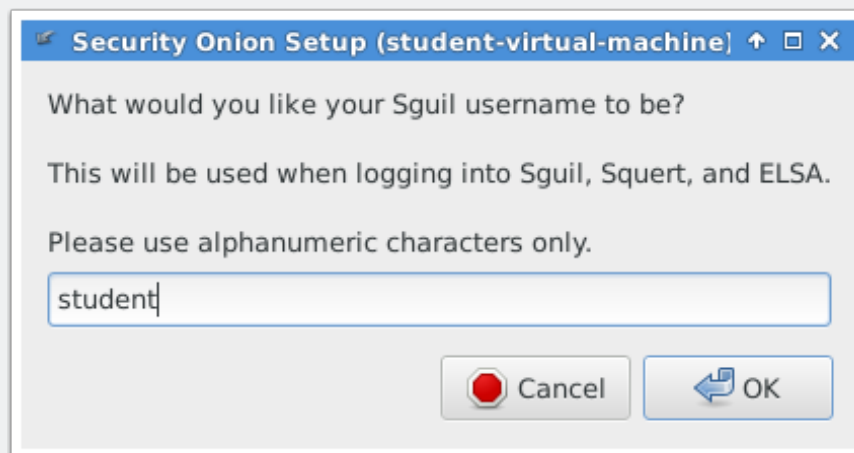
Security Onion Set Up Script

Select eth1



Select a username (Don't forget it)

This will be your username and password for Squert and Sguil

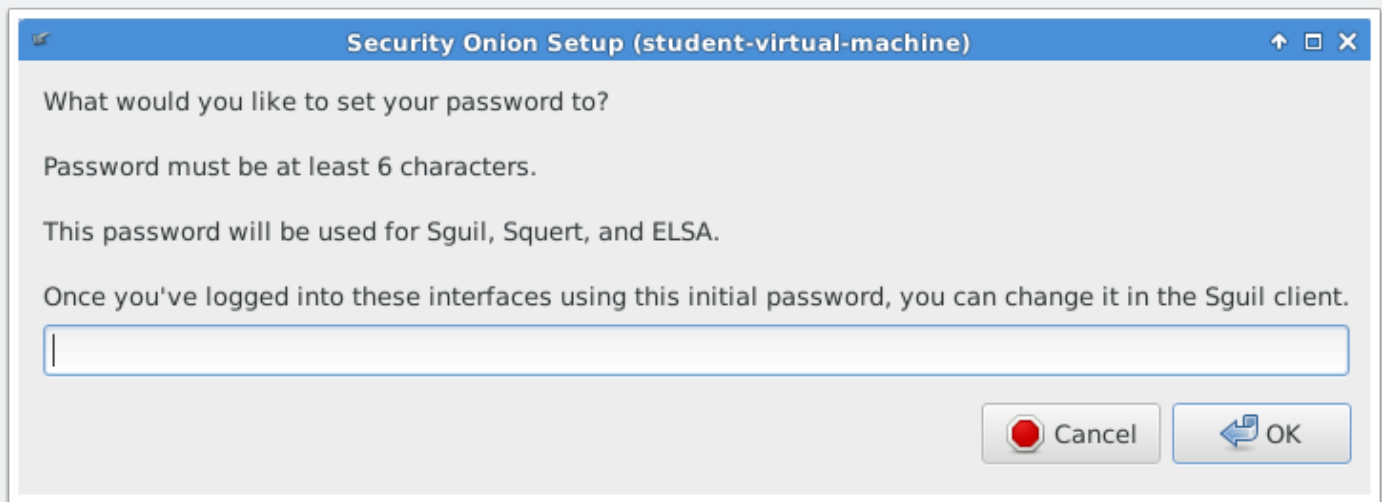


Security Onion Set Up Script

Set Password (Don't forget it)

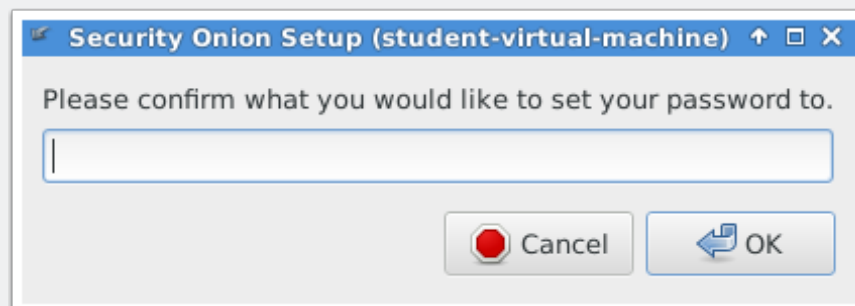
For the lab environment recommend a standard password.

If you forget the username and password you will need to redo the setup script.



The screenshot shows a Windows-style dialog box titled "Security Onion Setup (student-virtual-machine)". The text inside reads: "What would you like to set your password to?", "Password must be at least 6 characters.", "This password will be used for Sguil, Squert, and ELSA.", and "Once you've logged into these interfaces using this initial password, you can change it in the Sguil client." Below the text is a single-line text input field. At the bottom right are two buttons: "Cancel" with a red stop icon and "OK" with a blue arrow icon.

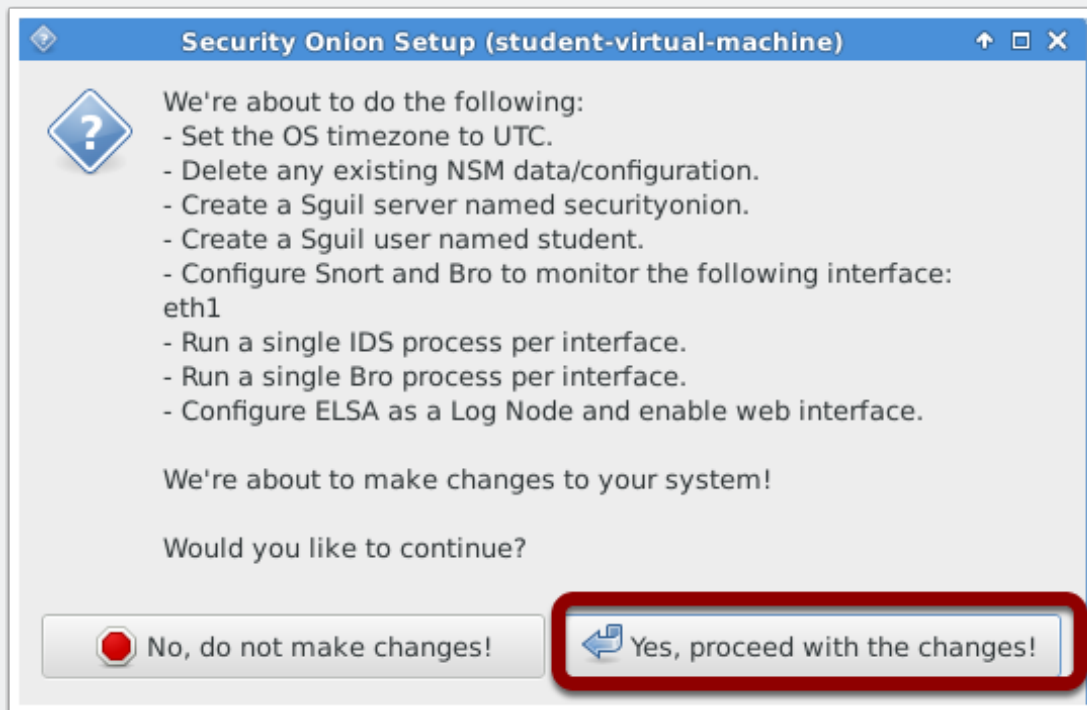
Confirm password



The screenshot shows the same dialog box as before, but the text now reads: "Please confirm what you would like to set your password to." Below the text is a single-line text input field. At the bottom right are the same two buttons: "Cancel" and "OK".

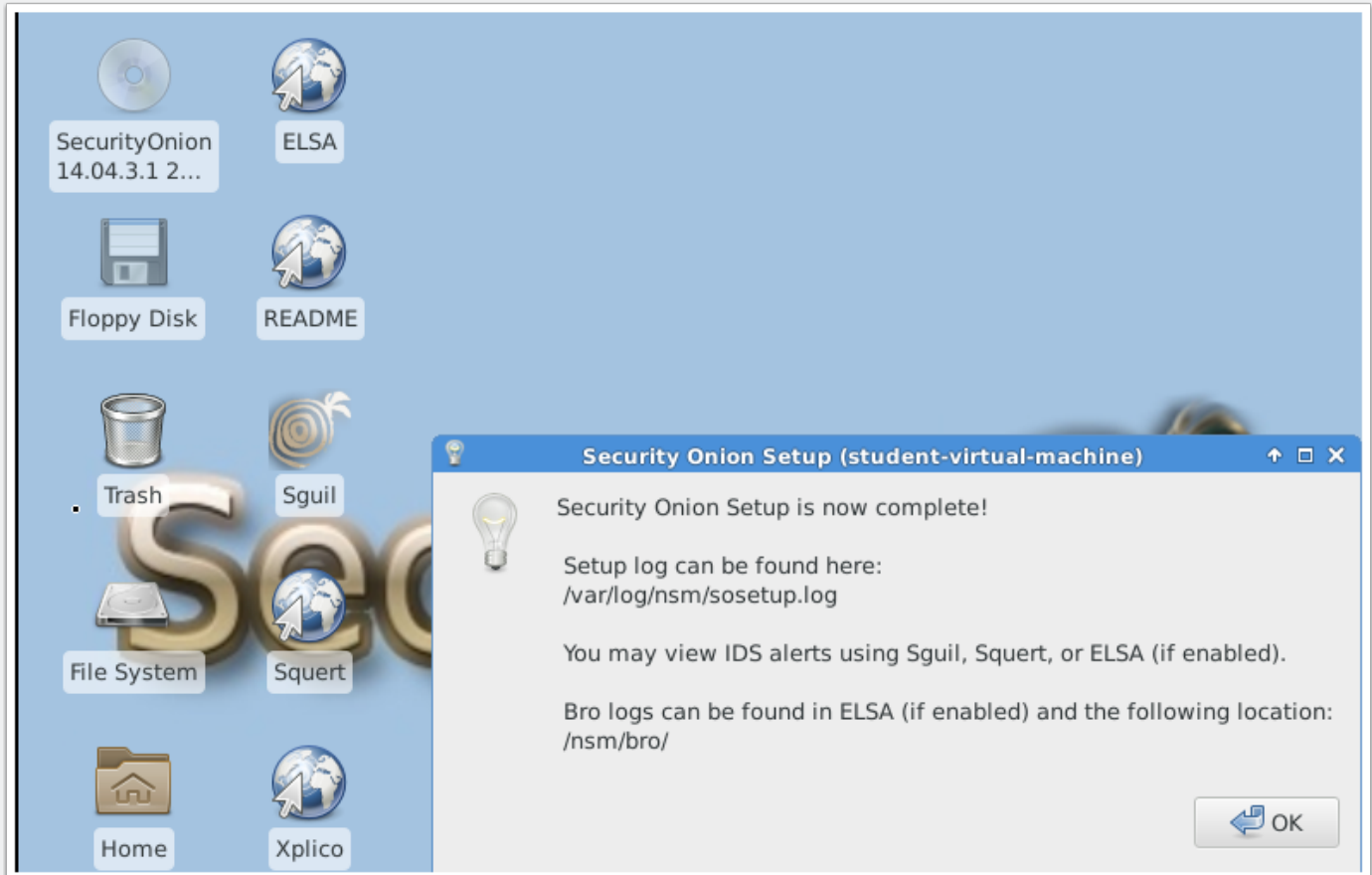
Security Onion Set Up Script

Click Yes



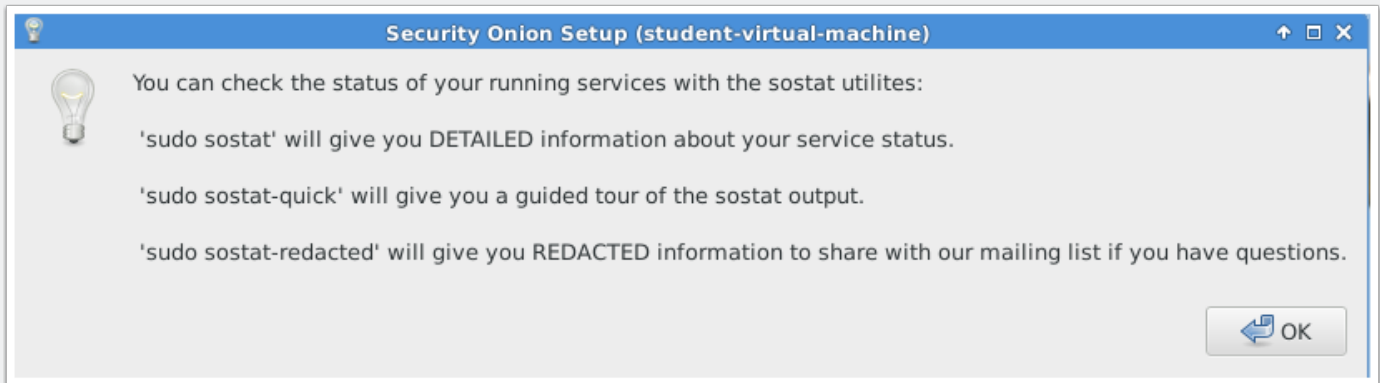
Security Onion Set Up Script

Complete

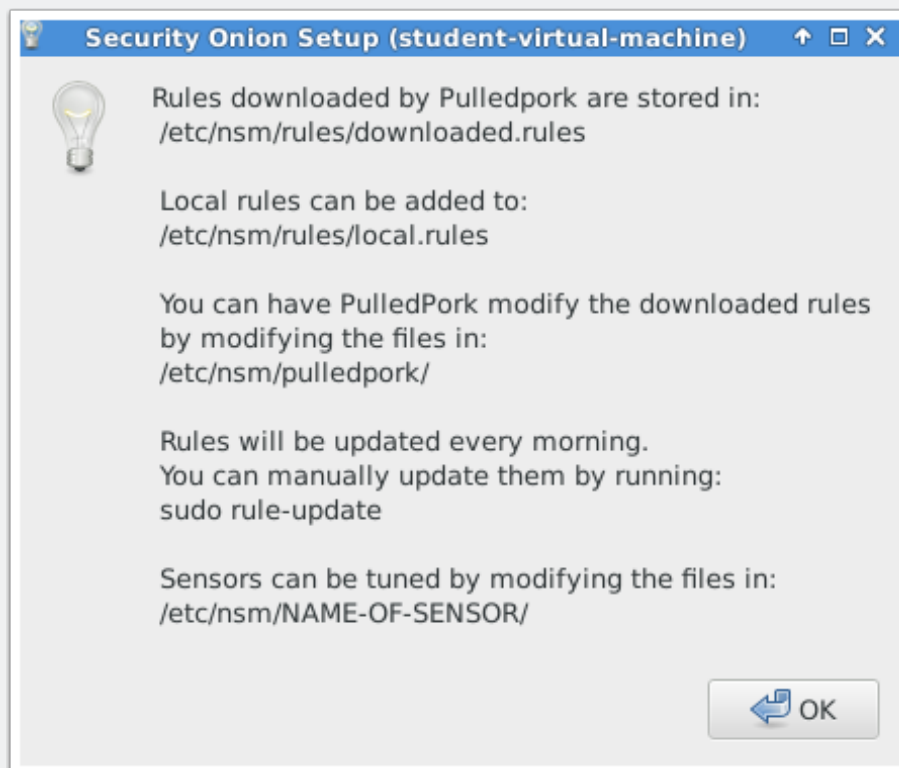


Security Onion Set Up Script

Click OK

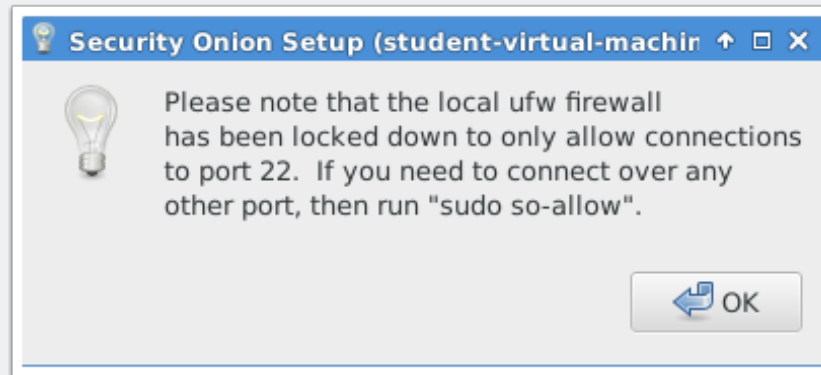


Click Ok



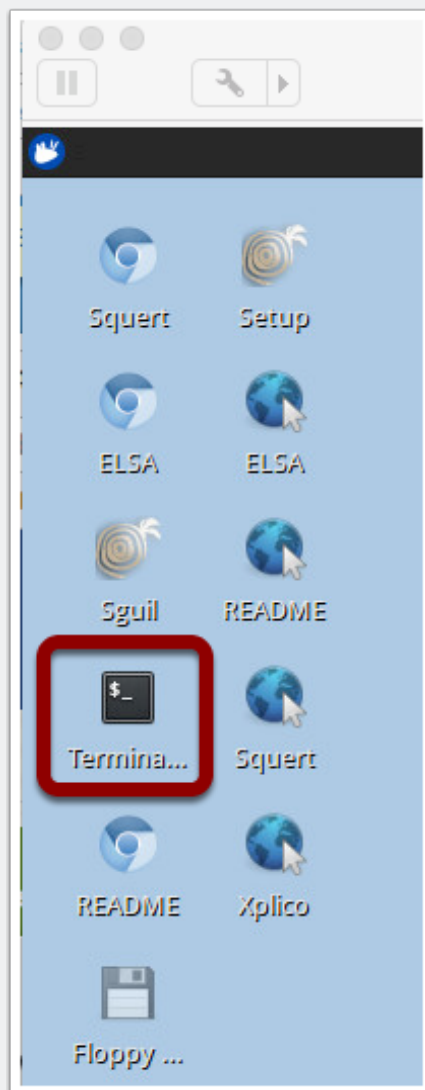
Security Onion Set Up Script

Click Ok



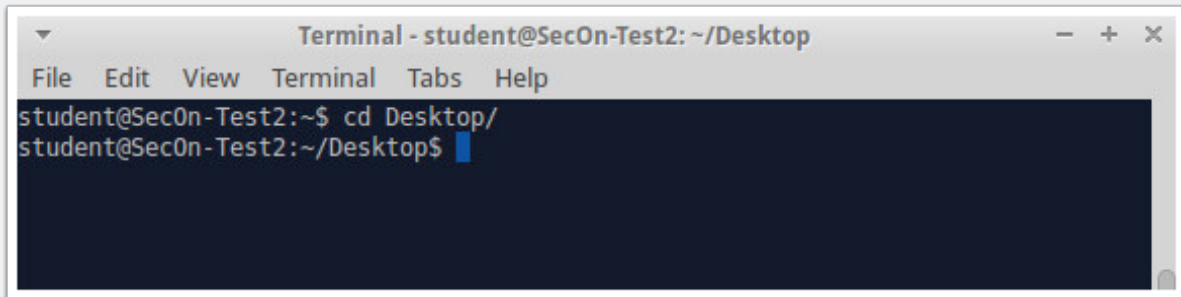
Security Onion Set Up Script

Open a terminal window



Security Onion Set Up Script

Change to the Desktop Directory

A terminal window titled "Terminal - student@SecOn-Test2: ~/Desktop" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the command "cd Desktop/" being entered and executed, resulting in the prompt "student@SecOn-Test2:~/Desktop\$".

```
Terminal - student@SecOn-Test2: ~/Desktop
File Edit View Terminal Tabs Help
student@SecOn-Test2:~$ cd Desktop/
student@SecOn-Test2:~/Desktop$
```

Security Onion Set Up Script

Open the notes file on the desktop and open a terminal window



Security Onion Set Up Script

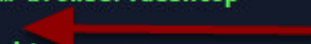
Copy this command from the notes file and paste this command in the terminal window

git clone https://github.com/csimpson4/cyb606.git

```
git clone https://github.com/csimpson4/cyb606.git
```

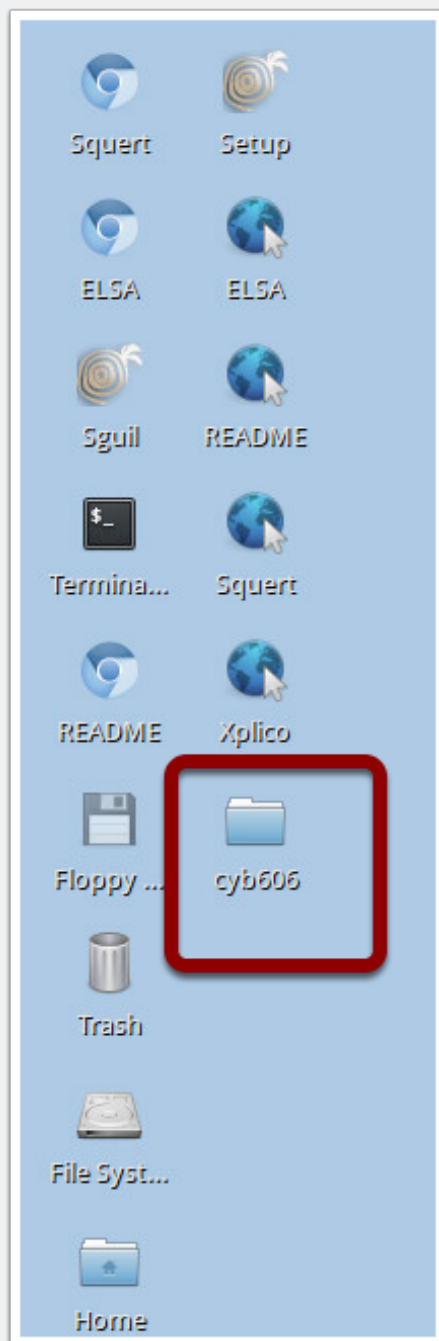
Run ls to verify that the cyb 606 folder was downloaded

```
student@Sec0n-Test2:~/Desktop$ ls
chromium-browser.desktop  securityonion-setup.desktop
cyb606                    securityonion-sguil.desktop
elsa.desktop              securityonion-squert.desktop
exo-terminal-emulator.desktop securityonion-xplico.desktop
securityonion-elsa.desktop squert.desktop
securityonion-readme.desktop
student@Sec0n-Test2:~/Desktop$
```



Security Onion Set Up Script

You can also look on the Desktop



Security Onion Set Up Script

This folder contains the lab instructions and required pcap files

Note: This is just an example, files may change over time.

