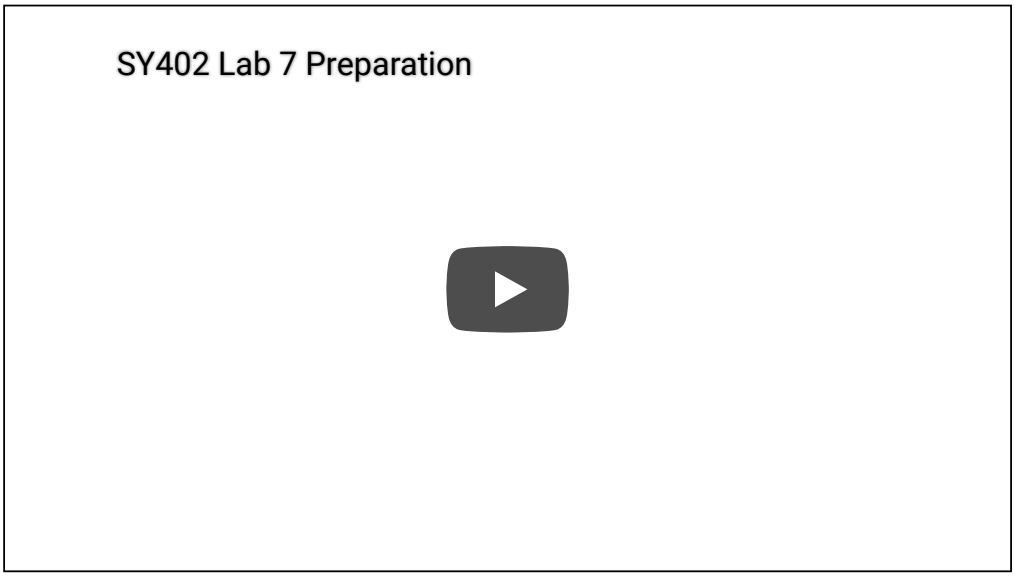
Instructor Note:



Lab 7 - Ensuring Host Integrity

NIST SP 800-92 specifically discusses Host-Based Intrusion Detection Systems (IDS). Defining them as follows. A host-based IDS monitors the characteristics of a single host and the events occurring within the host for suspicious activity. Many host-based IDS products monitor hosts' OS, security software, and application logs. Some host-based IDS products use logs as only one of several sources of data in detecting suspicious activity, while other host-based IDS products monitor logs only. Generally, a host-based IDS that uses log data has signatures for known malicious activity that it matches against log entries to identify events of interest. However, such products often focus on the OS logs and the most common security software and applications, and offer little or no support for less common software.

The purpose of this lab is to install and work with OSSEC, and to begin to understand the power of pooling data.

Part 1. Initial install of OSSEC

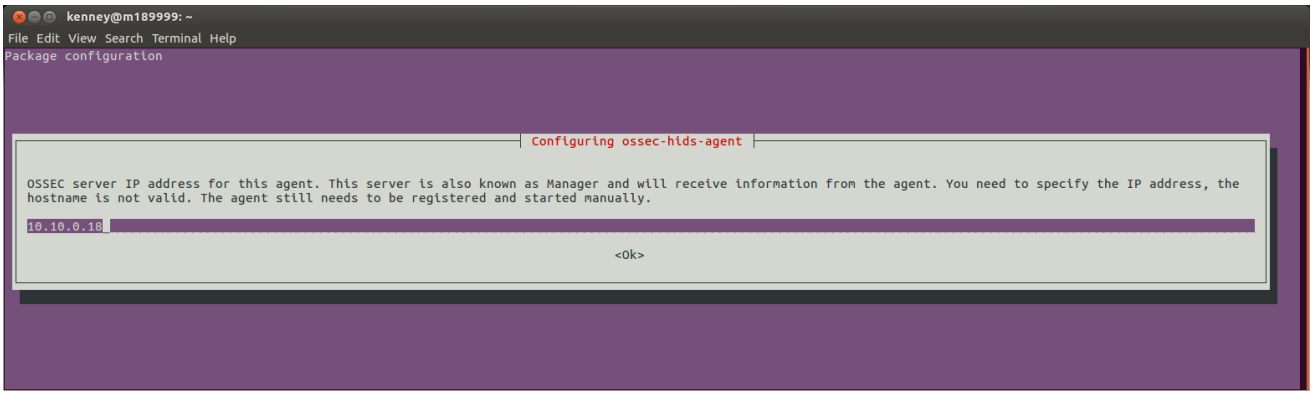
The following installation steps *should* guide you through the initial install of OSSEC on your Virtual Machine, assuming that your configuration is as expected.

You will probably want to disable the unix firewall from previous labs, as OSSEC uses iptables instead.

```
sudo ufw disable
```

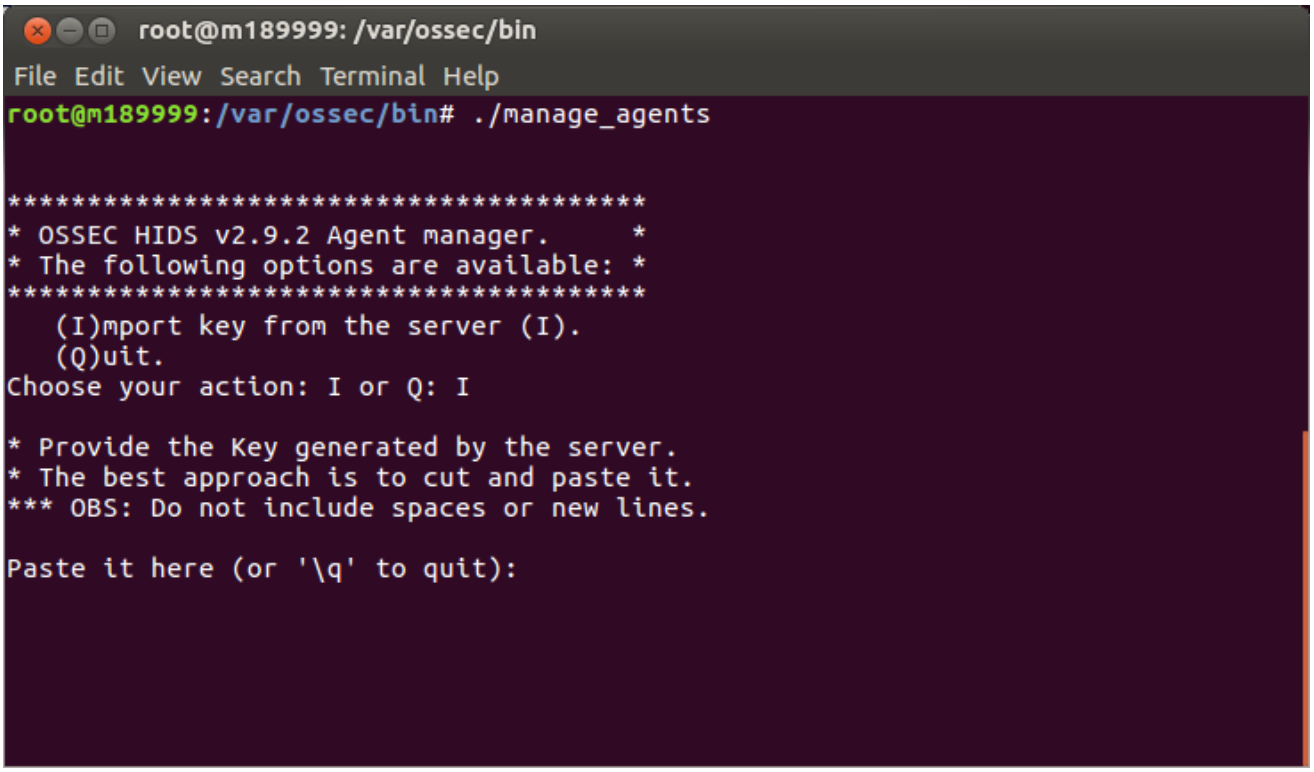
Download and install OSSEC.

```
# Download Required Repo Files
wget -q -O - https://updates.atomicorp.com/installers/atomic | sudo bash

# Update
sudo apt-get update

# Install OSSEC Agent (see picture below, use 10.10.0.18 as the OSSEC server address)
sudo apt-get install -y inotify-tools ossec-hids-agent
```



Add the OSSEC server key and link to the server.

```
sudo /var/ossec/bin/manage_agents
```



you will be cutting and pasting the key provided to you on the calendar into this window

```
sudo /var/ossec/bin/ossec-control start
sudo service ossec start
sudo cat /var/ossec/logs/ossec.log
```

What did inotify-tools provide?

Part 2. Review Setup

Spend a few minutes and read through the following older tutorials on OSSEC:

- http://danscourses.com/?s=ossec
- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-ossec-security-notifications-on-ubuntu-14-04

After reading the tutorials, review the configuration files in /var/ossec/etc.

What files/directories does the system ignore, and are there any that it specifically tracks?

Part 3. Questions

1. By default, for how long does OSSEC block traffic that triggers a firewall rule?

Answer or Discussion: By default, OSSEC will block for 600 seconds.

2. By default, How often does OSSEC check for new files? Can OSSEC detect file changes in realtime? If so, how do you configure OSSEC to set the important directories?

Answer or Discussion: The default time to search for files is 22 hours or 79200 seconds (as defined in the configuration files). OSSEC tracks important directories by marking them as realtime within the config file. Example:

```
<directories report_changes="yes" realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</
```

3. How do levels work with OSSEC rules?

Answer or Discussion:

4. Review the rootkit_trojans.txt file in /var/ossec/etc/shared. Why is OSSEC looking for antivirus sites in /etc/hosts?

Answer or Discussion: If there are antivirus definition sites listed in the hosts file, then your computer will not query DNS but will go directly to the IP address defined in the host file, if your computer has been compromised these changes will prevent your system from getting updated AV signatures.

5. After OSSEC is running on your machine for a few hours/days, what kind of alerts are you experiencing?

What to submit

When you have completed the lab **post all requested materials to your webpage**. Then, submit the link via email to your Professor.

The email subject line should be SY402 [Section Number] Lab [X]: Title of Lab (e.g., SY402 1111 Lab 7: Ensuring Host Integrity). Email sent with a different subject line will reduce the overall grade by 5 points.