# Notes from Exploring OSSEC and Bro

## Instructions

Make a copy of this document, rename it to “exploring-ossec-and-bro-notes” and move it to your CSE 523 Google Docs collection. If at any point in this exercise you feel stuck, raise your hand and get some guidance. When you reach each GATE below, switch over to the Tracking Progress document and update your position. Try to be efficient with your time.

## Overview

Today we will explore two programs: Ossec and Bro. They are designed to help defend against some of the attacks we’ve discussed previously in the semester. Both programs are classified as “Intrusion Detection Systems” or IDS. Keep detailed notes below (place your comments in between the provided horizontal lines); you will be referring to these in the future to do your work.

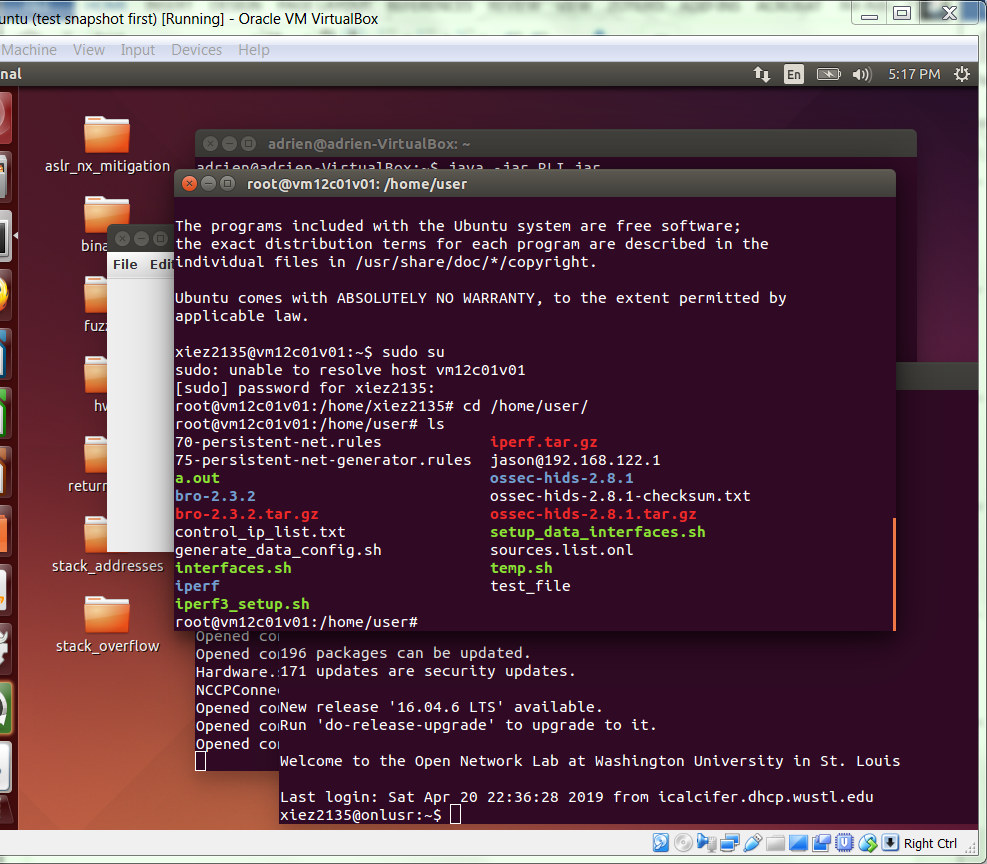
**GATE 1**

Similar to previous exercises, you need to start two virtual machines (VM1 and VM2) inside of ONL. You can reference the ONL connection setup instructions from Section 4 of [HW2](https://docs.google.com/document/d/1stg8-AAEh8Nx9om4FC_bUrtpkIRgbBVHDi8_jO1ixqE/edit?usp=sharing). For this in-class assignment, we will use a slightly different topology called cse523\_ids.onl, which you can download [here](https://drive.google.com/file/d/1MaFcywzvYvwUV2VWHSnqLbiq8_kWIH2R/view?usp=sharing). After downloading the topology file, open it in the RLI and follow the usual process. At this point, your experiment should have committed successfully.

Begin by logging into VM1. Begin by going to the directory /home/user/ after becoming root:

sudo su

cd /home/user/



In this directory, you should see multiple files, but the only ones that are relevant to the exercise are the ones that begin with either “bro” or “ossec”. The other files are used by the ONL for setting up the VM automatically and can be safely ignored. Our next step is to setup ossec. To begin, cd into the directory:

cd ossec-hids-2.8.1

Installing ossec is relatively easy, and can be done with it’s “install.sh” script:

./install.sh

You will be guided along the installation process with several questions. For these questions, you should enter the following answers:

Question: What you should select:

Language? en

Installation type? local

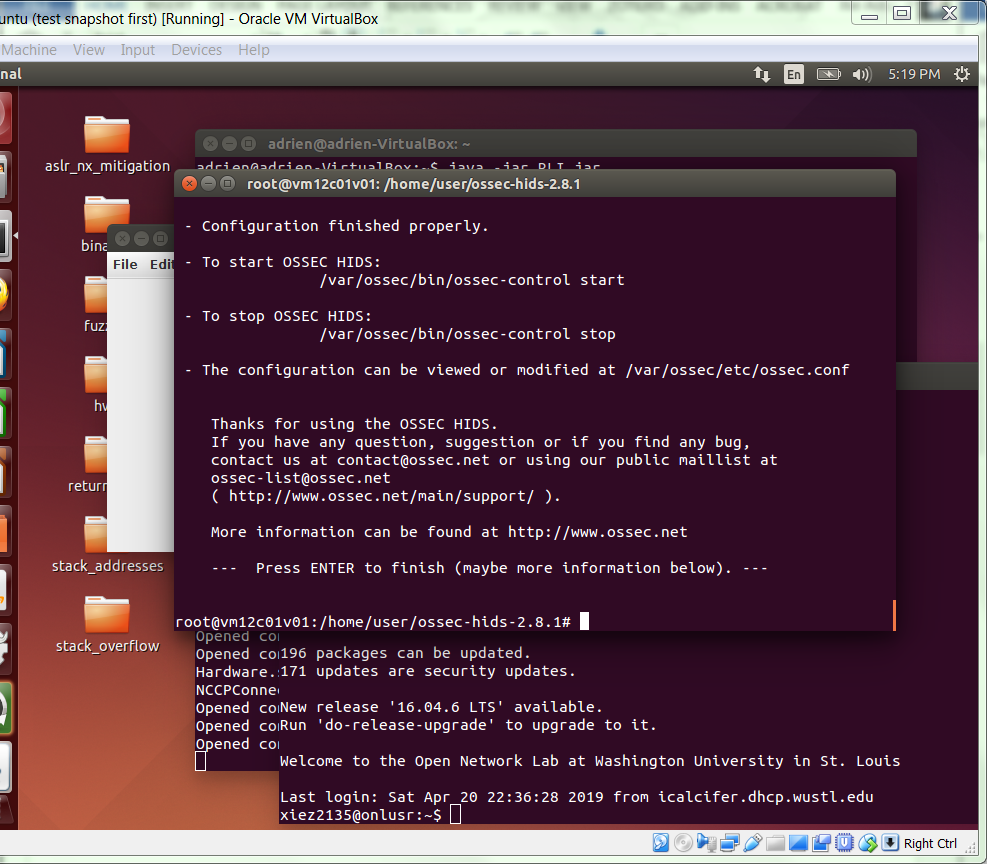
Install Directory? /var/ossec

Email address? n

Run integrity check daemon? y

Run rootkit detection engine? y

Enable active response? n



To finish up, we need to start ossec:

cd /var/ossec/bin

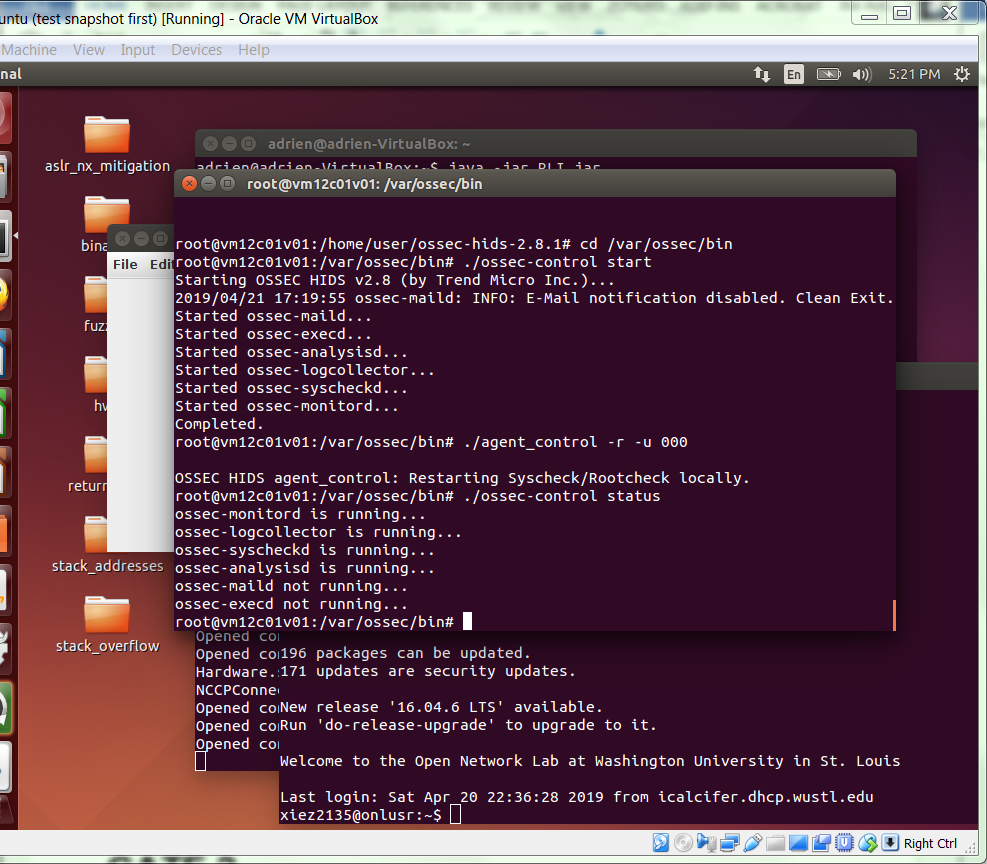
./ossec-control start

./agent\_control -r -u 000

These commands start the ossec daemon and then tell it to check the integrity of the system’s OS files. One of ossec’s main functions is to report whenever system files are modified, since many malicious programs operate by changing system files in some way. When ossec is started for the first time, it must build a database of checksums for all of the monitored system files on the disk (and in the case of Windows, all of the registry files as well). This process should take between 5 and 10 minutes, so we will come back to ossec later in the exercise. For now, verify that ossec is up and running by using the following command and recording its output:

./ossec-control status

.



.

**GATE 2**

While we wait for ossec to finish building its integrity checking database, we will move on to setting up Bro. First, we must change directories to bro:

cd /home/user/bro-2.3.2

Normally, the first step in installing bro is to install all of bro’s dependencies through apt-get, and then to build bro with a “make” command. However, this takes over 30 minutes to do, so your VM has already completed these steps for you. We will continue the installation process with:

make install

This command will take about a minute to finish. Afterwards, we must configure bro to work with our VMs by editing one file. First, we have to change directories to bro’s configuration files:

cd /usr/local/bro/etc/

Now, open the file “node.cfg” with your favorite command line text editor. If you do not normally use command line text editors, I recommend nano for this exercise since it is the easiest to start using:

nano node.cfg

Use nano to change the interface setting from “eth0” to “data1”. You can then close nano and save your changes with the <ctrl-x> key combination. Since we are using bro on a local network, we do not have to do any more configuration. To finish this gate and start bro, change directories to bro’s bin folder and start bro, and record your output below:

cd /usr/local/bro/bin/

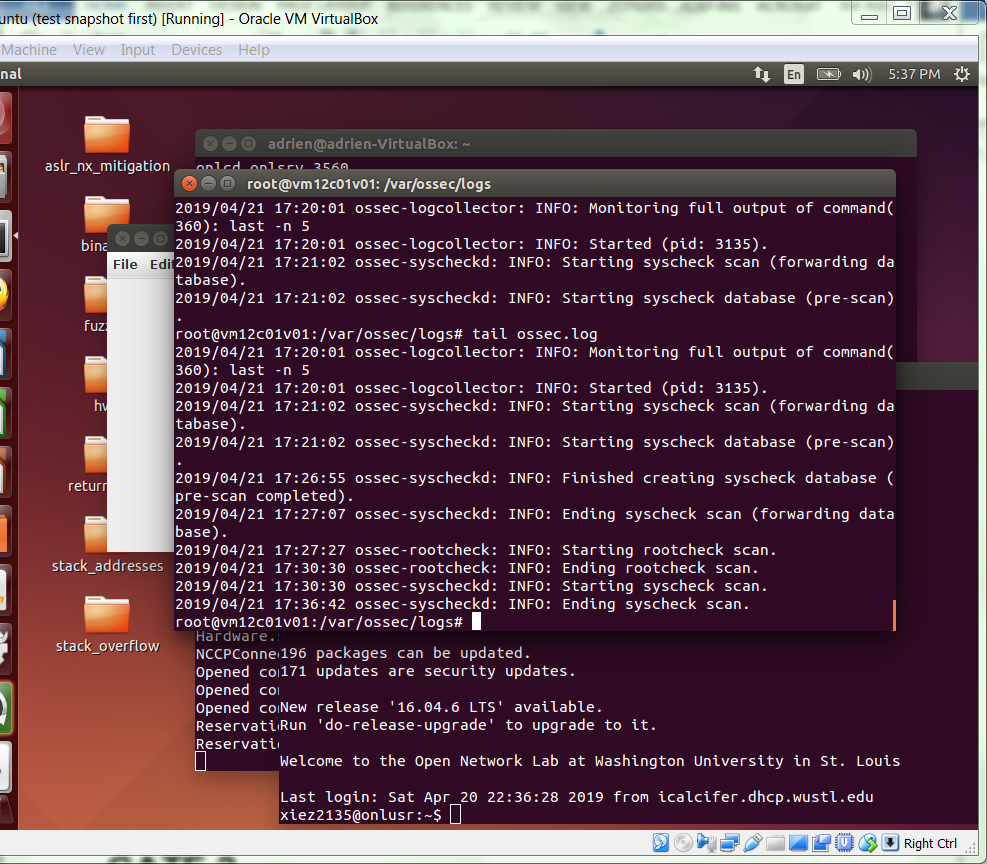
./broctl

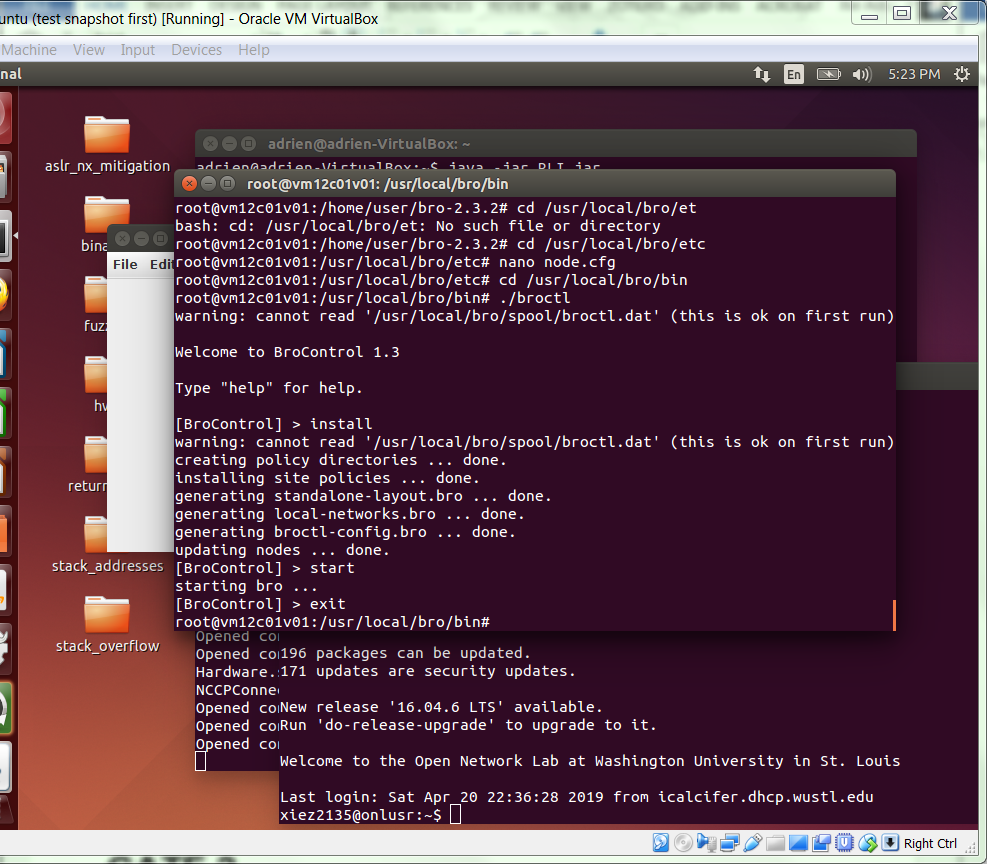
install

start

exit

.





.

**GATE 3**

By now, enough time should have passed for ossec to finish its initial scans. To check to see if ossec is finished, use the following command:

cd /var/ossec/logs/

tail ossec.log

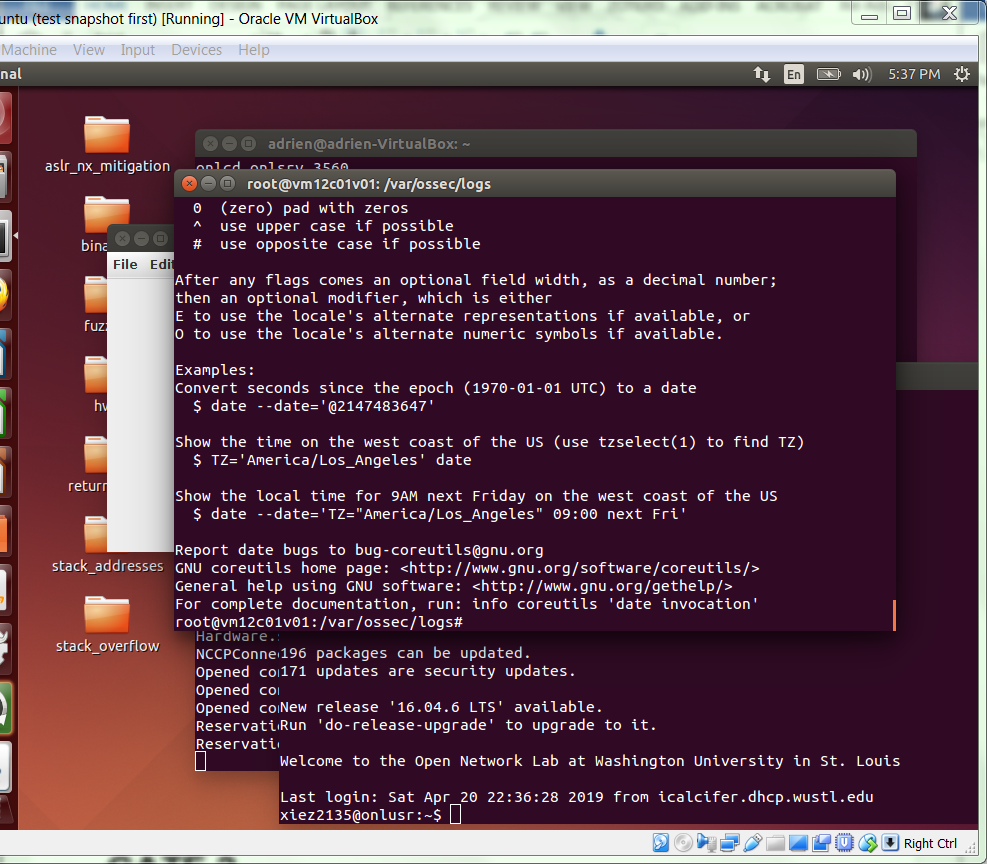
If the scan is finished, you should see a line that says “Ending syscheck scan”. If you do not see this line, then you should at least see a line that says “Starting syscheck scan”. If you see the “Starting syscheck scan” line, then you should wait a minute or two and repeat the “tail ossec.log” command until you see “Ending syscheck scan”. If you see neither of these lines, tell the TA and he will assist you. You can ignore the progress of the subsequent “rootcheck” scan.

At this point, ossec is running and configured properly. One of ossec’s features is determining whether any system files have been changed by malicious programs. To test this feature, we are going to redo part of the first lab of the semester: Changing the program “date”.

Like the first lab, start by recording date’s help information below:

date --help

.



.

Now, we will make a change to the binary with the following commands. Type each line exactly as it appears:

vi /bin/date

:%s/bug/rug/g

:wq

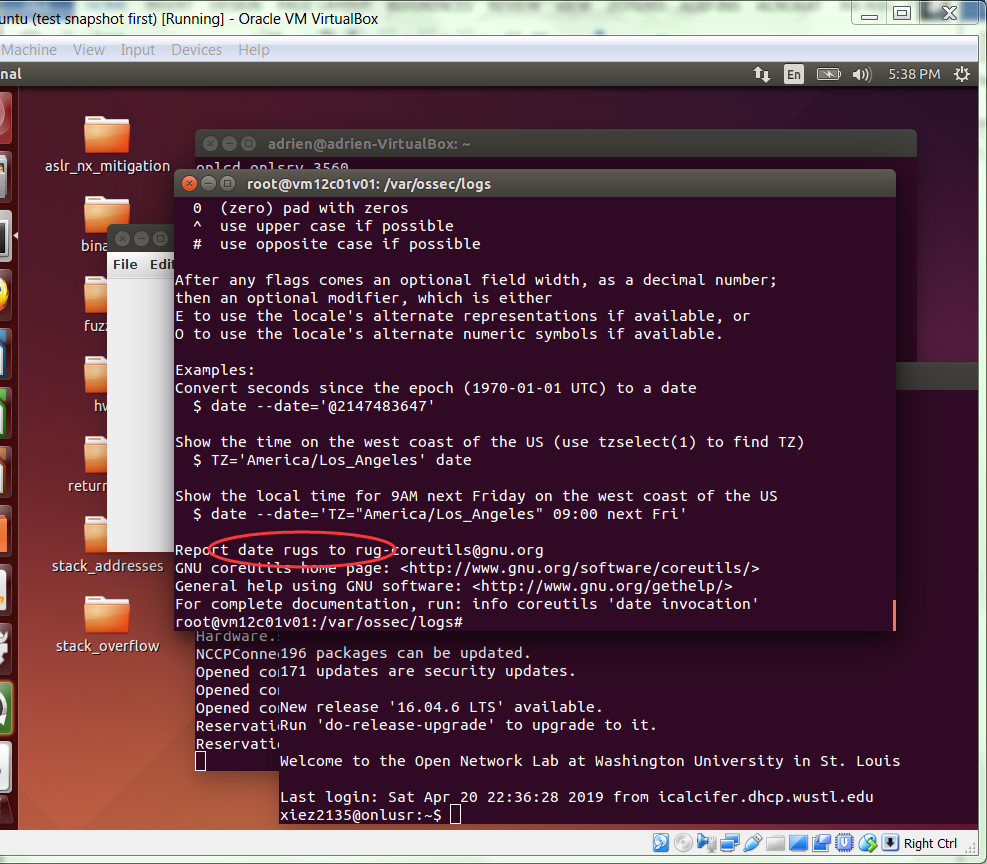
You can see what our change did with another help command to date:

date --help

After observing the output, briefly describe what change we made to date:

.

Bugs are changed to rugs



.

By default, ossec will run an integrity check on the system files every 10 minutes. To speed things along, we will force an integrity check with the following commands:

cd /var/ossec/bin

./agent\_control -r -u 000

Again, this will take about 10 minutes to finish, so we will temporarily move on to bro while we wait.

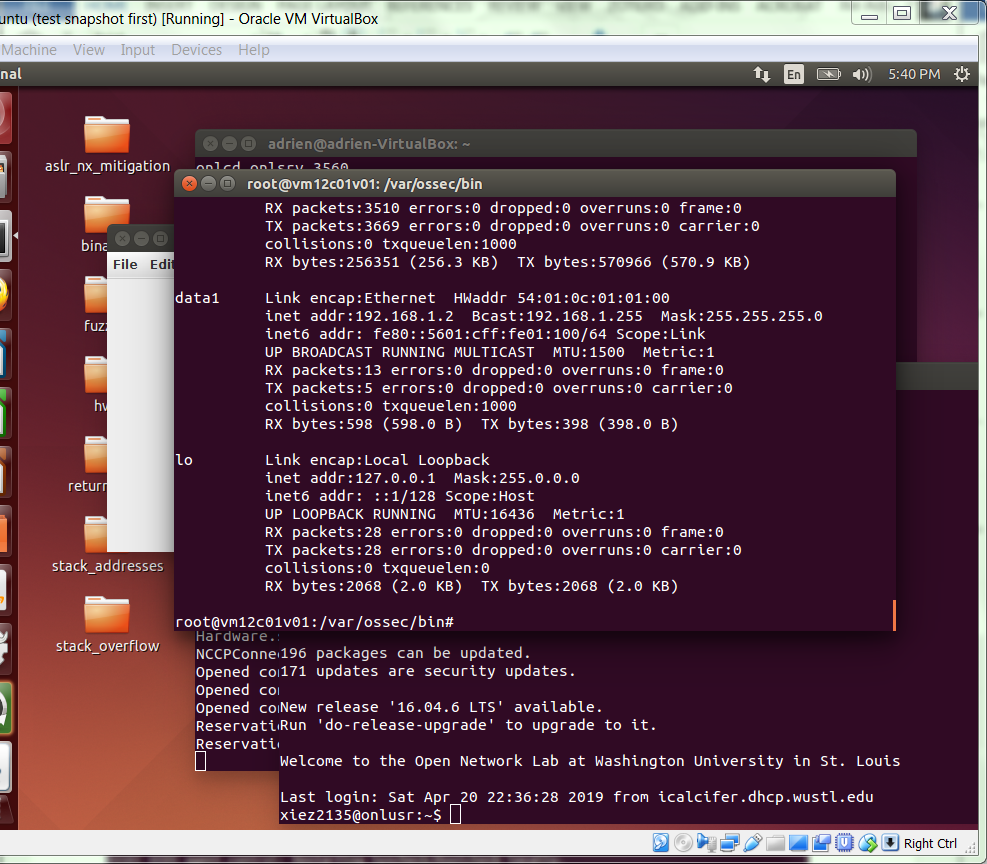
**GATE 4**

While ossec is designed to detect changes made to the host system, bro is designed to sniff network traffic and detect suspicious connections. To test out bro, we will perform an nmap scan on our machine using VM2. Before we begin, note the IP address of VM1’s data1 interface after using ifconfig:

ifconfig

.

192.168.1.2



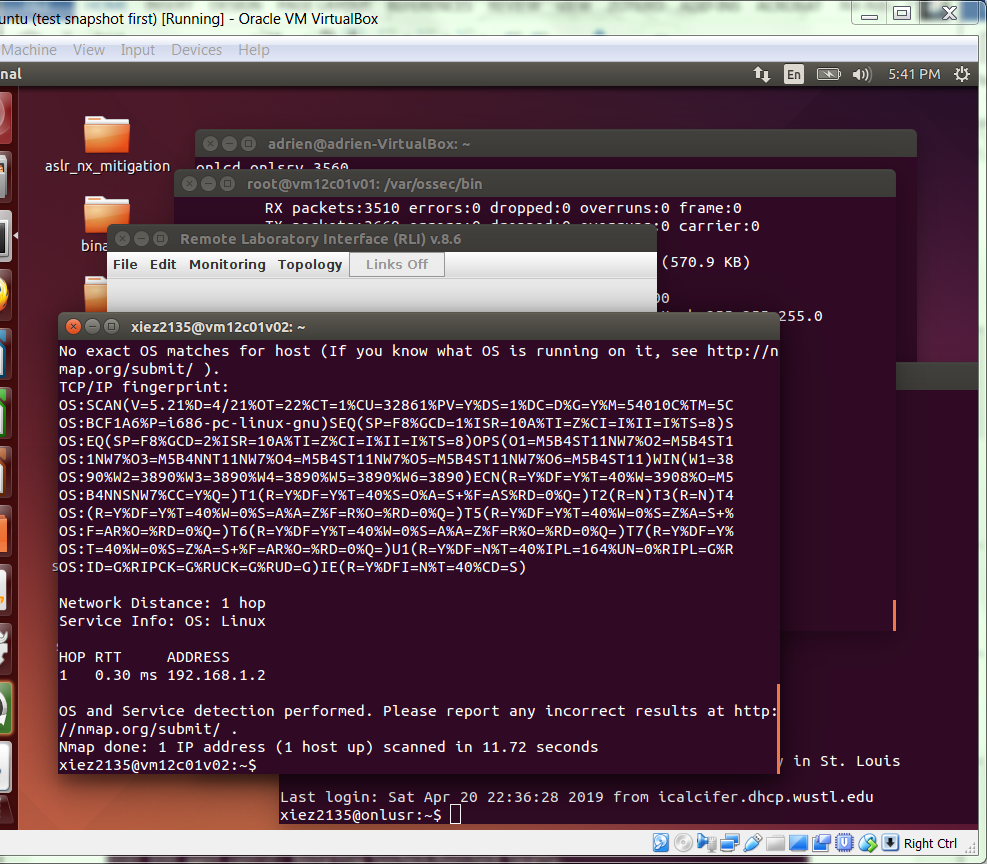
.

Log into VM2 in a different terminal window. We can perform an nmap scan of our first VM with the following command, replacing {VM1’s IP address} with the IP address found above:

sudo nmap -A {VM1’s IP address}

Place the output of the nmap command below (it will take a minute or two to complete):

.

 .

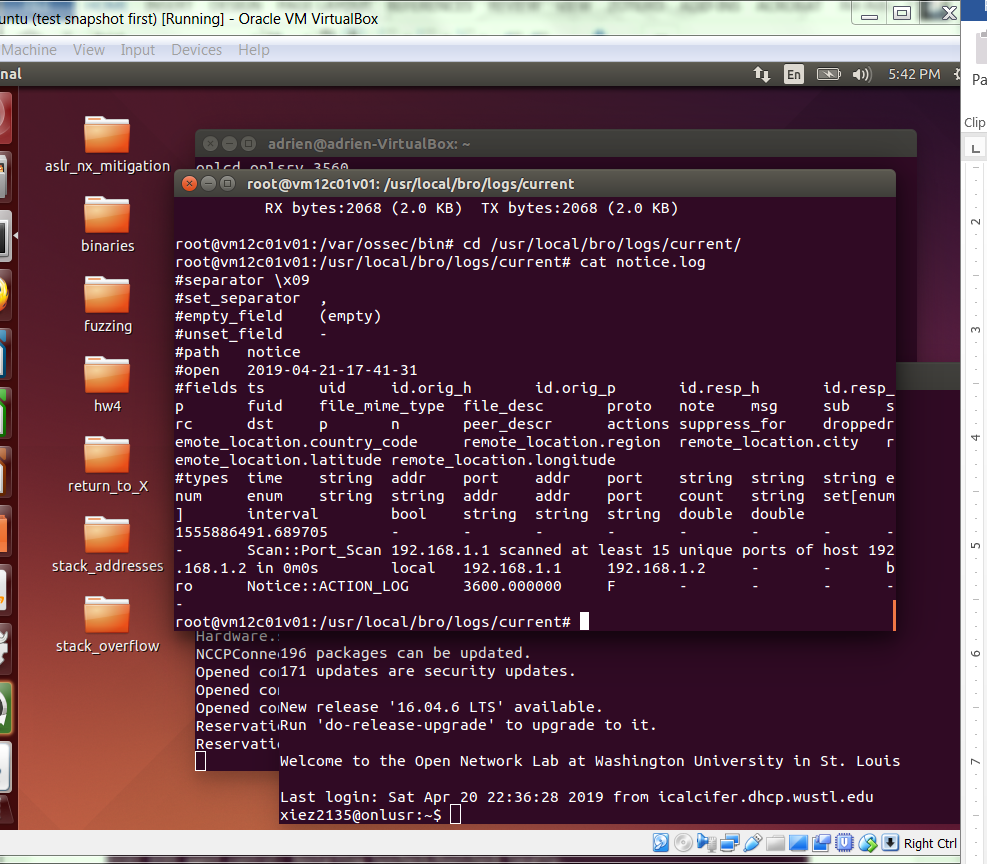
With the scan over, we are done with VM2, so return to VM1 and navigate to the bro logs at:

cd /usr/local/bro/logs/current/

To finish up our exploration of bro, output the bro logs and summarize what you see (If the logs are not there yet, wait a few minutes and try again. notice.log seems to take longer than the rest, be patient.). Was bro able to successfully raise an alarm from the nmap scan?

cat notice.log

.

 .

**GATE 5**

By now, ossec should have finished its integrity scan. Again, to see if ossec is finished, use the following command:

cd /var/ossec/logs/

tail ossec.log

If you see “Ending Syscheck Scan”, then the scan has completed. We can see all of ossec’s alerts, followed by those only involving the integrity scan, with these two sets of outputs:

cat /var/ossec/logs/alerts/alerts.log

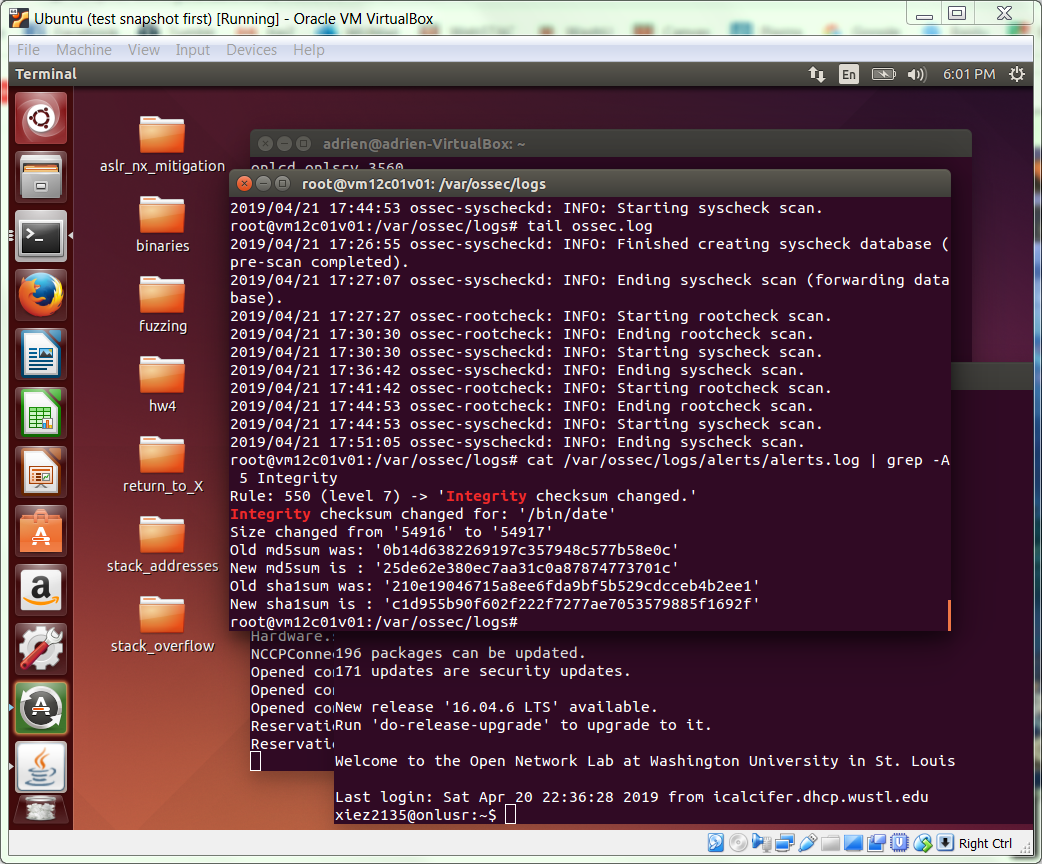
cat /var/ossec/logs/alerts/alerts.log | grep -A 5 Integrity

Looking over the entries in the log, what do you see? Was ossec able to successfully detect the change in /bin/date?

.

The change in the /bin/date is listed.

Yes, ossec successfully detect the change in /bin/date.



.

**COMPLETE**