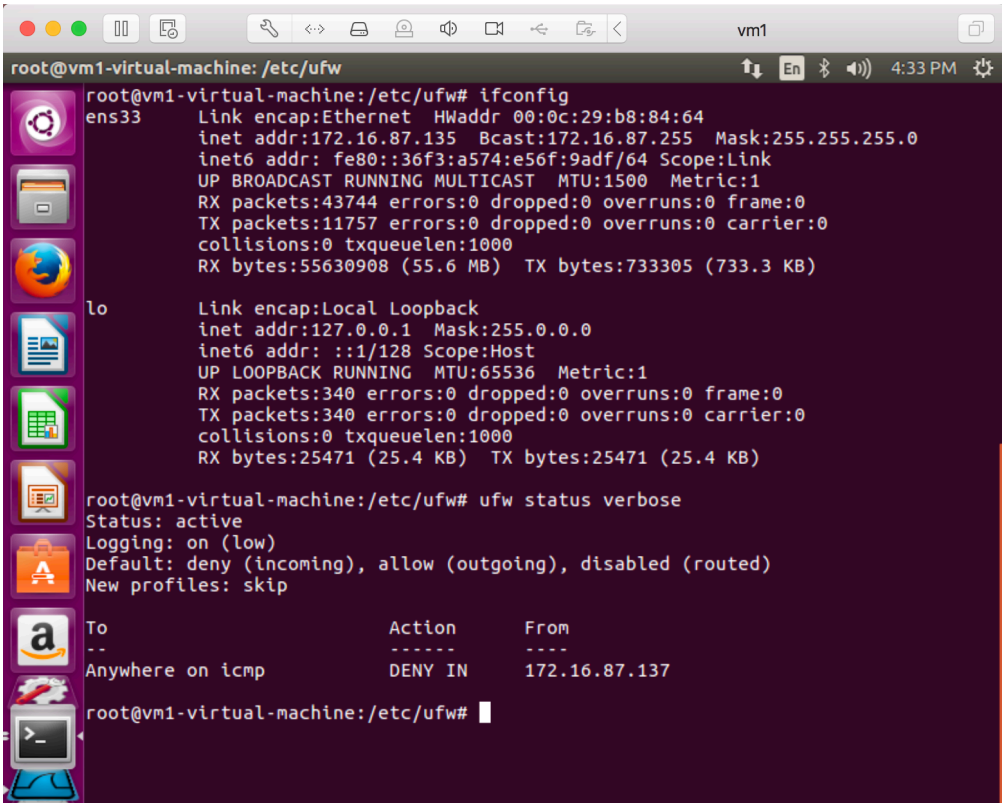
SPC-Project 2-Part 2

Yue Guan

Screenshots of Terminal showing that these services are running (or set up):

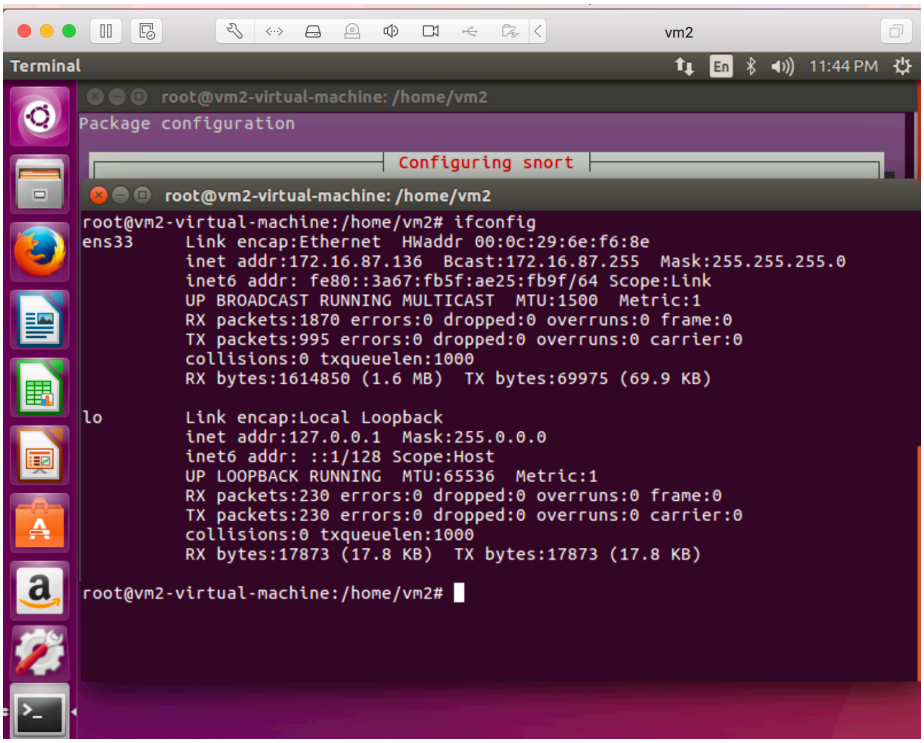
Screenshot on VM1:

1. IP Address of VM1 is 172.16.87.135
2. UFW Status on VM1

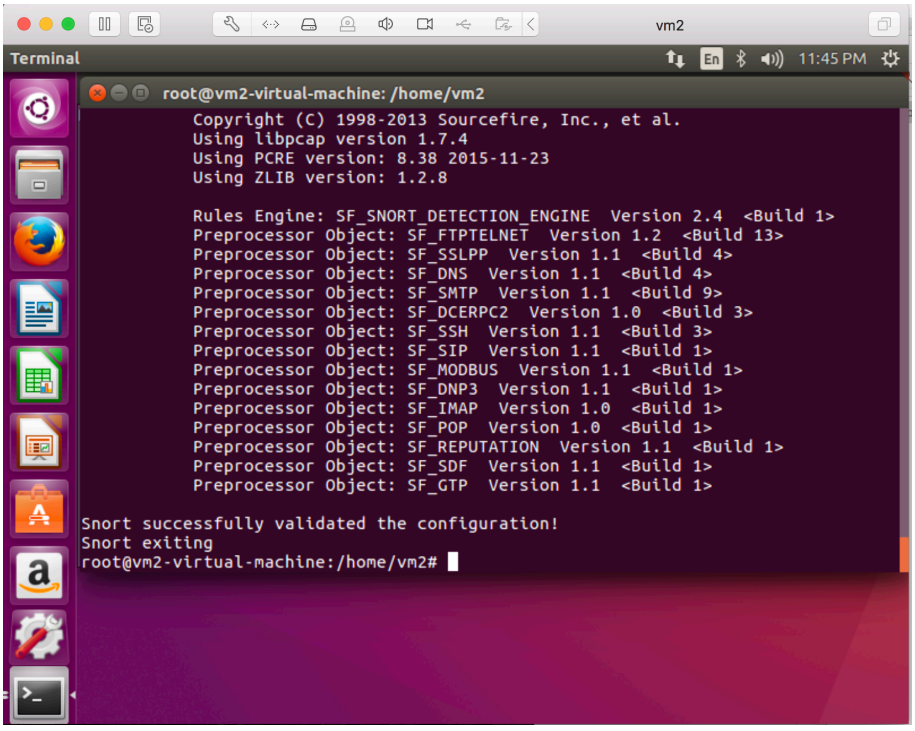


Screenshot of VM 2: Snort, HTTP, FTP

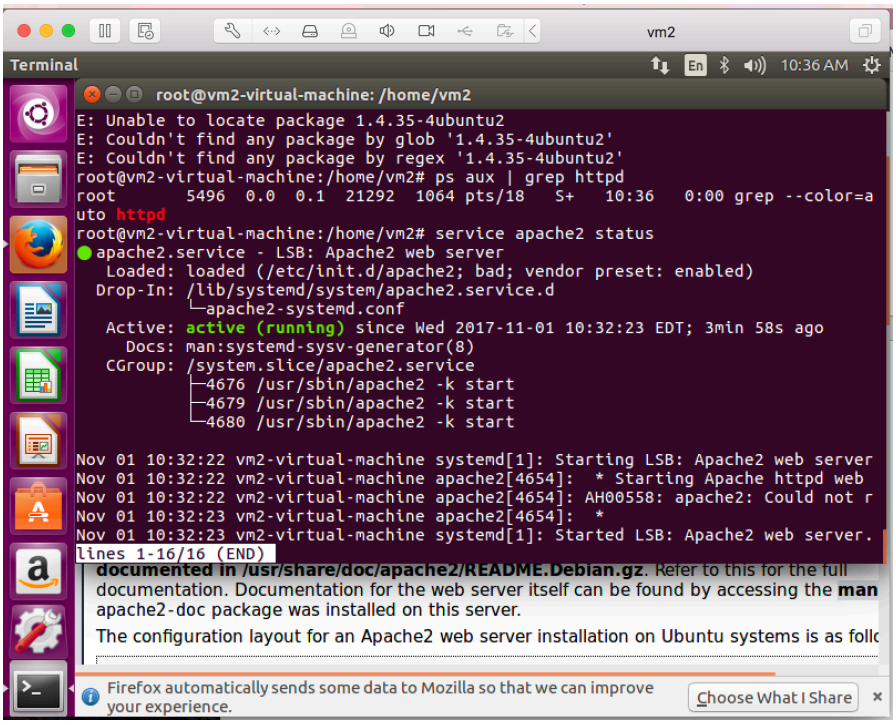
1. VM 2 IP Address: 172.16.87.136

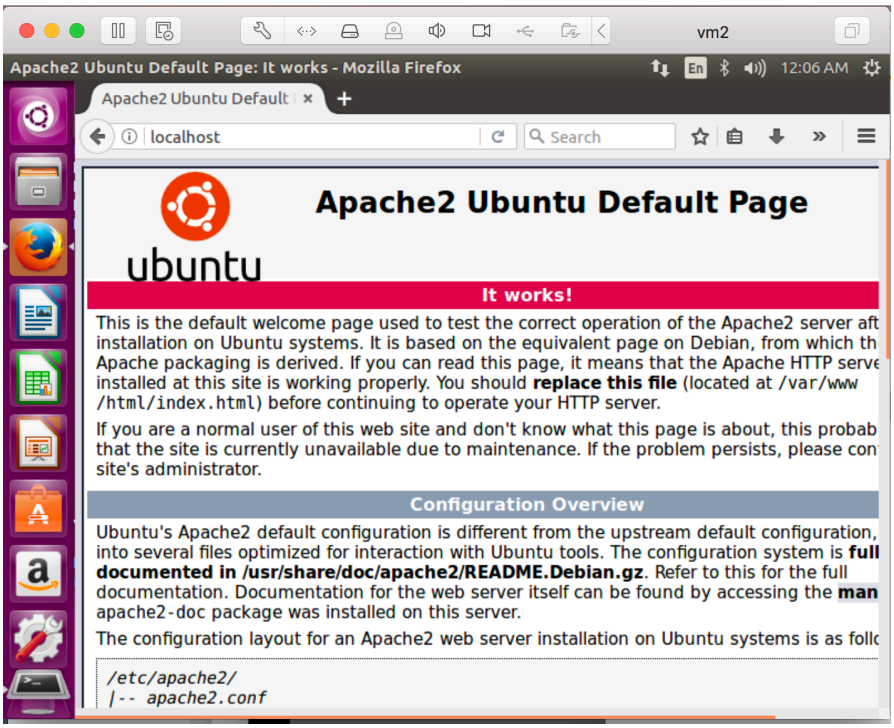


2. Snort

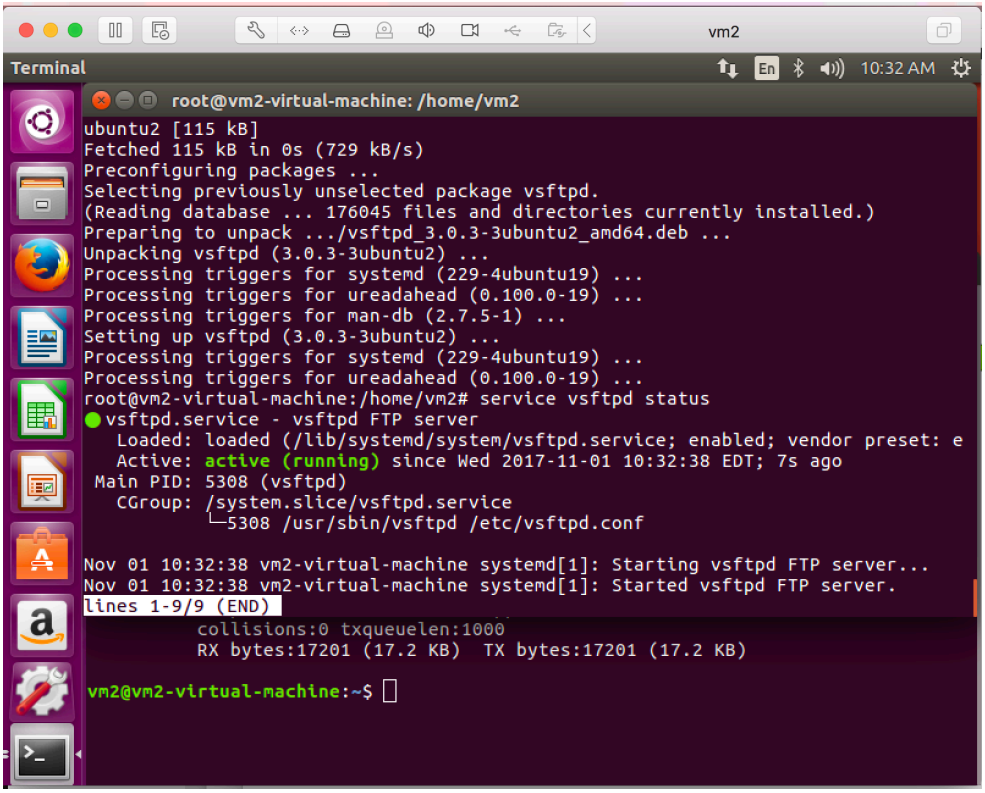


3. HTTP


vm2
Terminal
10:36 AM
root@vm2-virtual-machine: /home/vm2
E: Unable to locate package 1.4.35-4ubuntu2
E: Couldn't find any package by glob '1.4.35-4ubuntu2'
E: Couldn't find any package by regex '1.4.35-4ubuntu2'
root@vm2-virtual-machine:/home/vm2# ps aux | grep httpd
root 5496 0.0 0.1 21292 1064 pts/18 S+ 10:36 0:00 grep --color=a
uto httpd
root@vm2-virtual-machine:/home/vm2# service apache2 status
apache2.service - LSB: Apache2 web server
Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
Drop-In: /lib/systemd/system/apache2.service.d
└apache2-systemd.conf
Active: active (running) since Wed 2017-11-01 10:32:23 EDT; 3min 58s ago
Docs: man:systemd-sysv-generator(8)
CGroup: /system.slice/apache2.service
├4676 /usr/sbin/apache2 -k start
├4679 /usr/sbin/apache2 -k start
└4680 /usr/sbin/apache2 -k start
Nov 01 10:32:22 vm2-virtual-machine systemd[1]: Starting LSB: Apache2 web server
Nov 01 10:32:22 vm2-virtual-machine apache2[4654]: * Starting Apache httpd web
Nov 01 10:32:22 vm2-virtual-machine apache2[4654]: AH00558: apache2: Could not r
Nov 01 10:32:23 vm2-virtual-machine apache2[4654]: *
Nov 01 10:32:23 vm2-virtual-machine systemd[1]: Started LSB: Apache2 web server.
lines 1-16/16 (END)
documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full
documentation. Documentation for the web server itself can be found by accessing the man
apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follc
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share

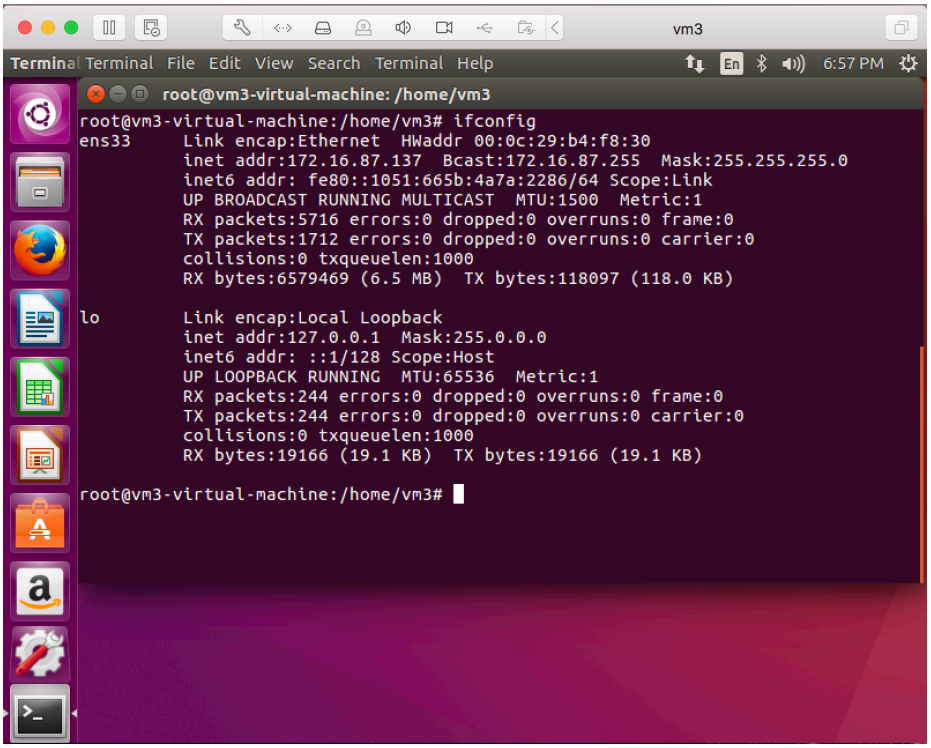

vm2
Apache2 Ubuntu Default Page: It works - Mozilla Firefox
12:06 AM
Apache2 Ubuntu Default
localhost
Search
Apache2 Ubuntu Default Page
ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server aft
installation on Ubuntu systems. It is based on the equivalent page on Debian, from which th
Apache packaging is derived. If you can read this page, it means that the Apache HTTP serve
installed at this site is working properly. You should replace this file (located at /var/www
/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probab
that the site is currently unavailable due to maintenance. If the problem persists, please con
site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration,
into several files optimized for interaction with Ubuntu tools. The configuration system is full
documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full
documentation. Documentation for the web server itself can be found by accessing the man
apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follc
/etc/apache2/
|-- apache2.conf

4. FTP

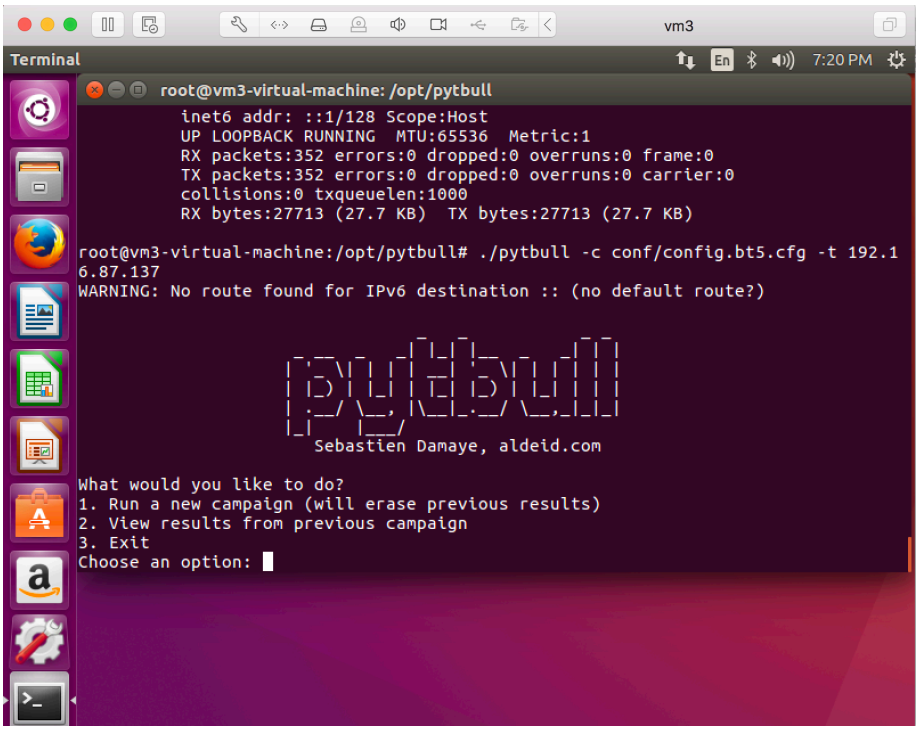

vm2
Terminal
En
10:32 AM
root@vm2-virtual-machine: /home/vm2
ubuntu2 [115 kB]
Fetched 115 kB in 0s (729 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 176045 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-3ubuntu2_amd64.deb ...
Unpacking vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for systemd (229-4ubuntu19) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for systemd (229-4ubuntu19) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@vm2-virtual-machine:/home/vm2# service vsftpd status
vsftpd.service - vsftpd FTP server
Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
Active: active (running) since Wed 2017-11-01 10:32:38 EDT; 7s ago
Main PID: 5308 (vsftpd)
CGroup: /system.slice/vsftpd.service
└─5308 /usr/sbin/vsftpd /etc/vsftpd.conf
Nov 01 10:32:38 vm2-virtual-machine systemd[1]: Starting vsftpd FTP server...
Nov 01 10:32:38 vm2-virtual-machine systemd[1]: Started vsftpd FTP server.
lines 1-9/9 (END)
collisions:0 txqueuelen:1000
RX bytes:17201 (17.2 KB) TX bytes:17201 (17.2 KB)
vm2@vm2-virtual-machine:~$

Screenshots on VM3:

1. IP Address: 172.16.87.137

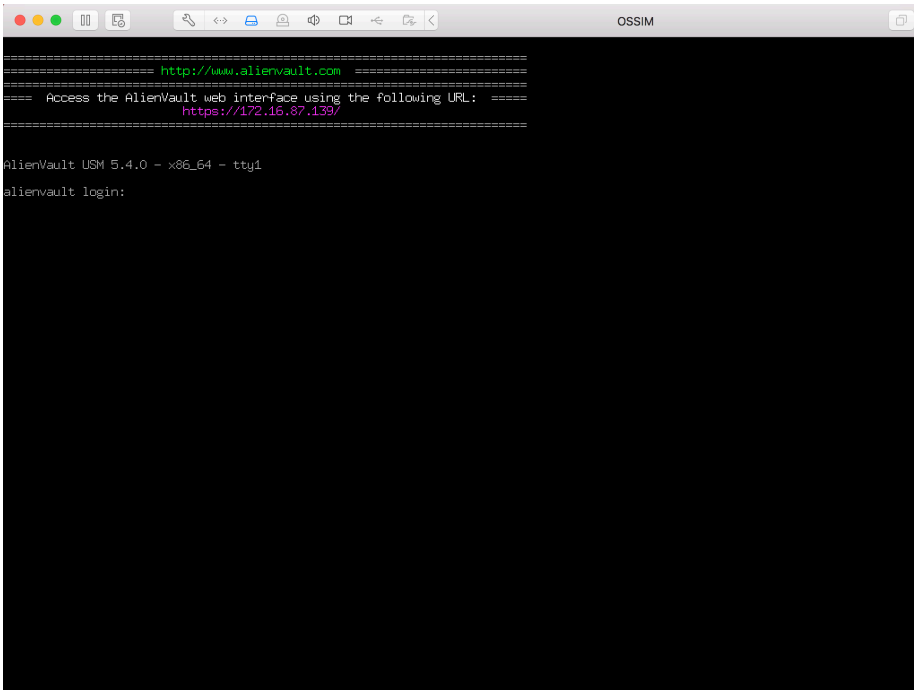


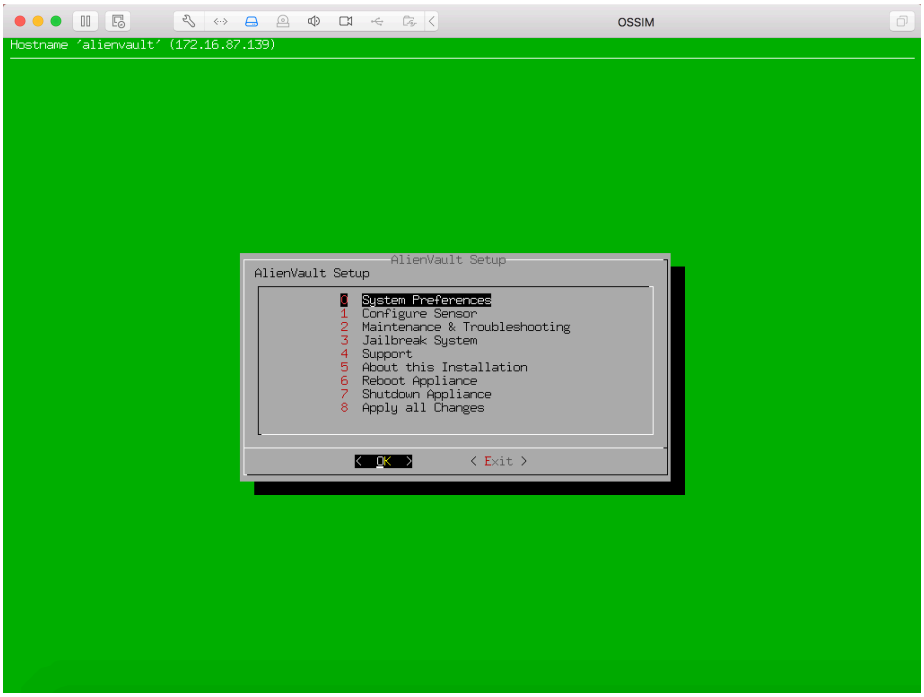
2. Pytbull



Screenshot on VM 4:

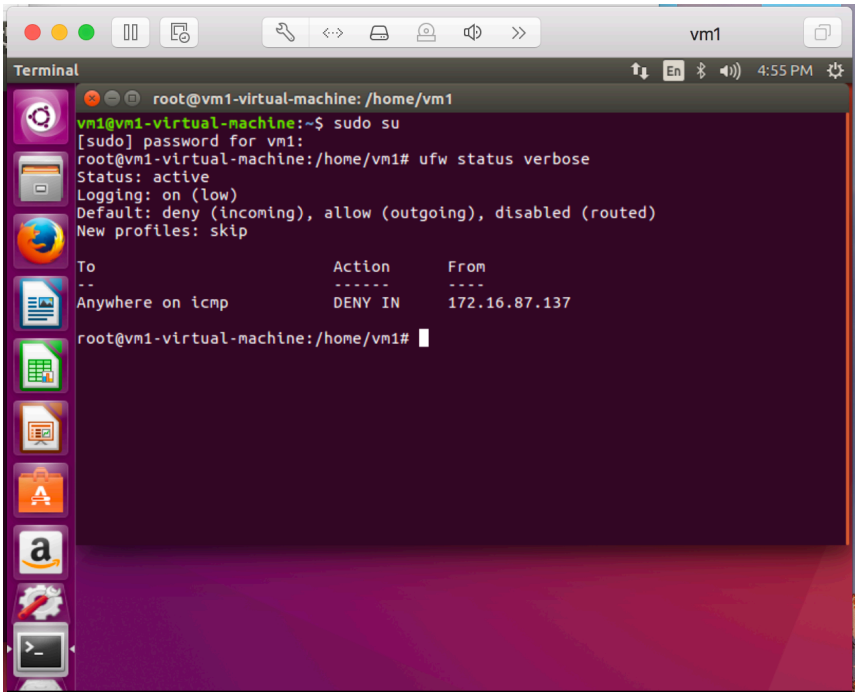
1. OSSIM





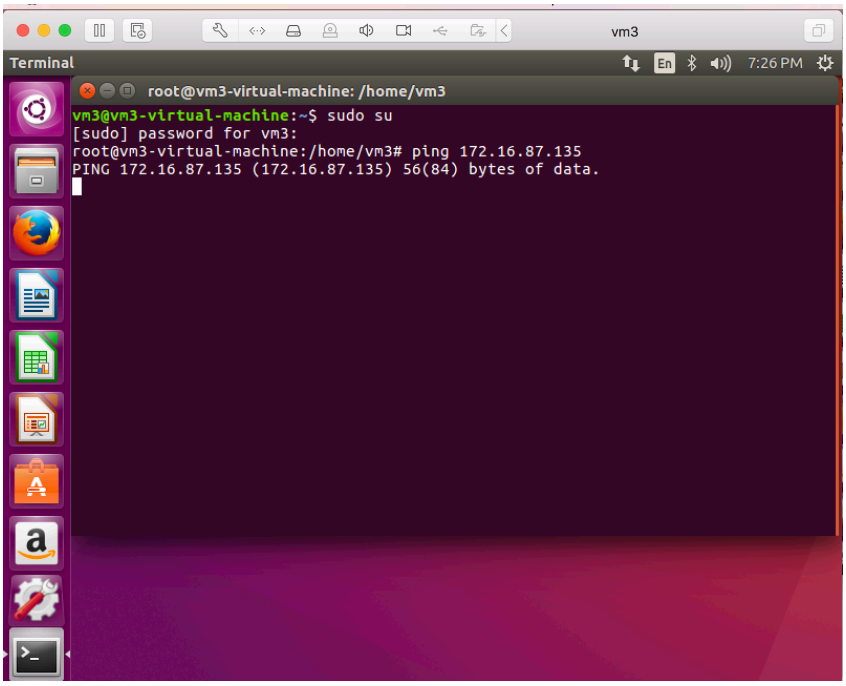
Logs from FW:

1. Firewall rules on VM1, deny icmp from VM3

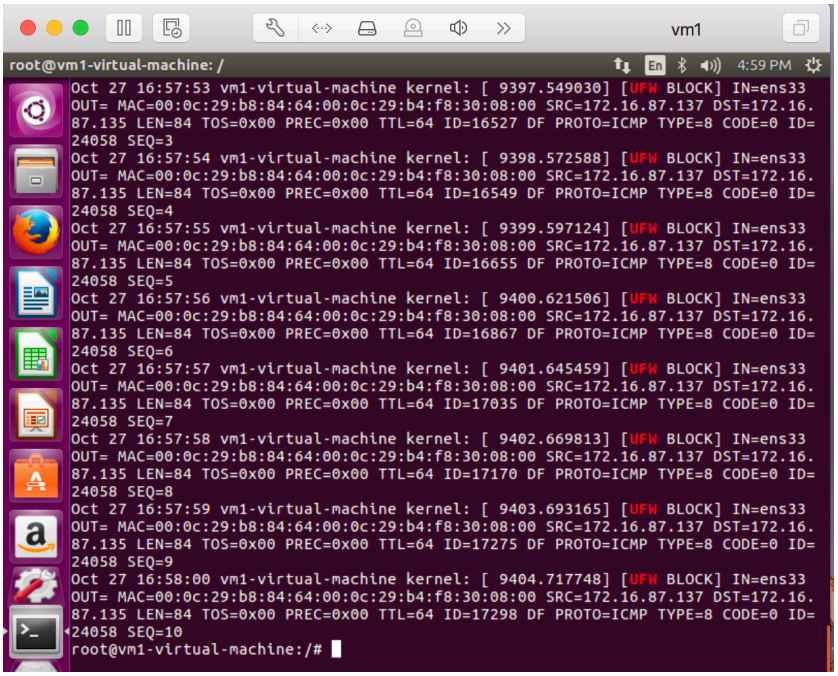


command: *ufw deny in on icmp from 172.16.87.137*

2. VM3 ping VM1

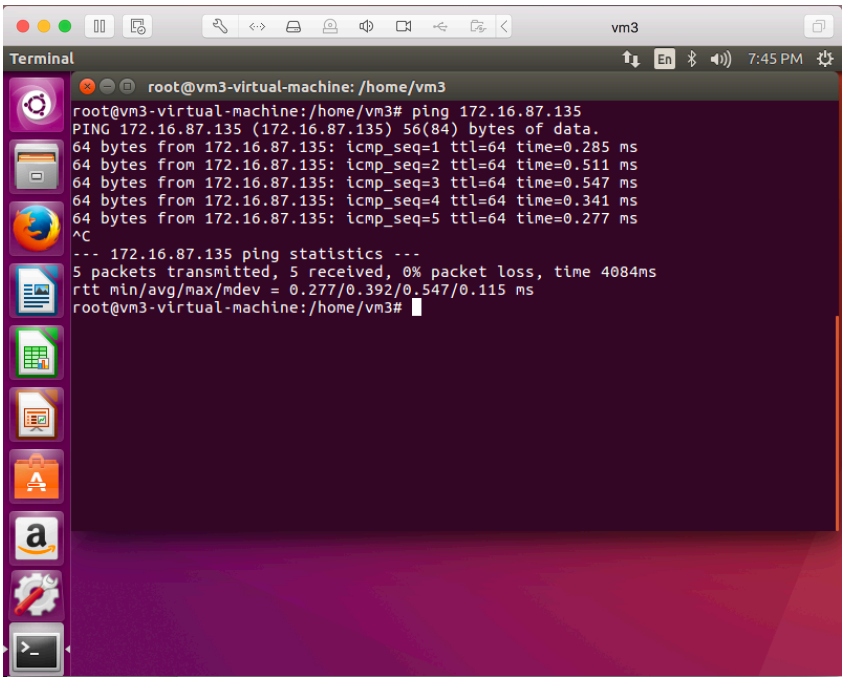


3. UFW Log:



4. When ufw Allow icmp request

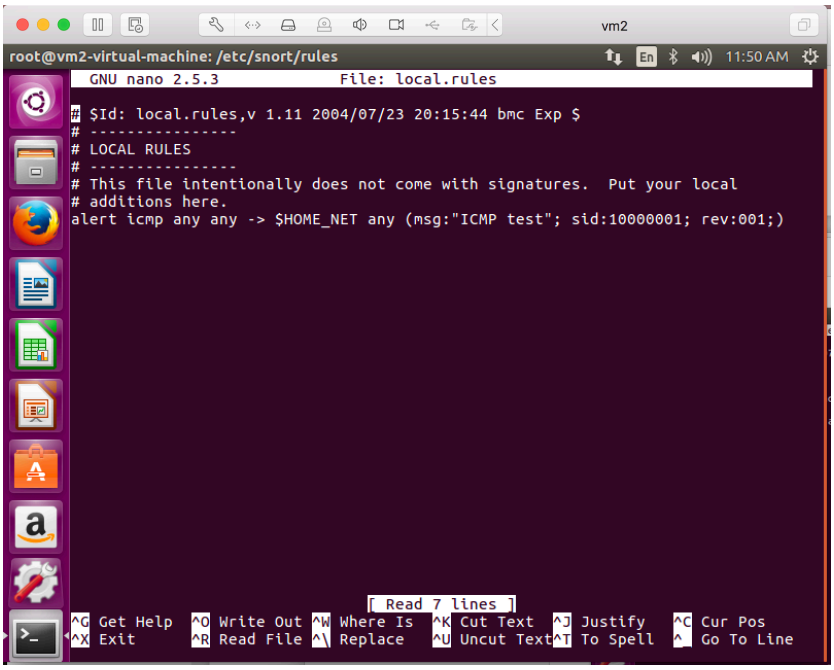
However, we just delete the rule above, because ufw allow on icmp defaultly. VM3 is pinging VM1, it succeeds.



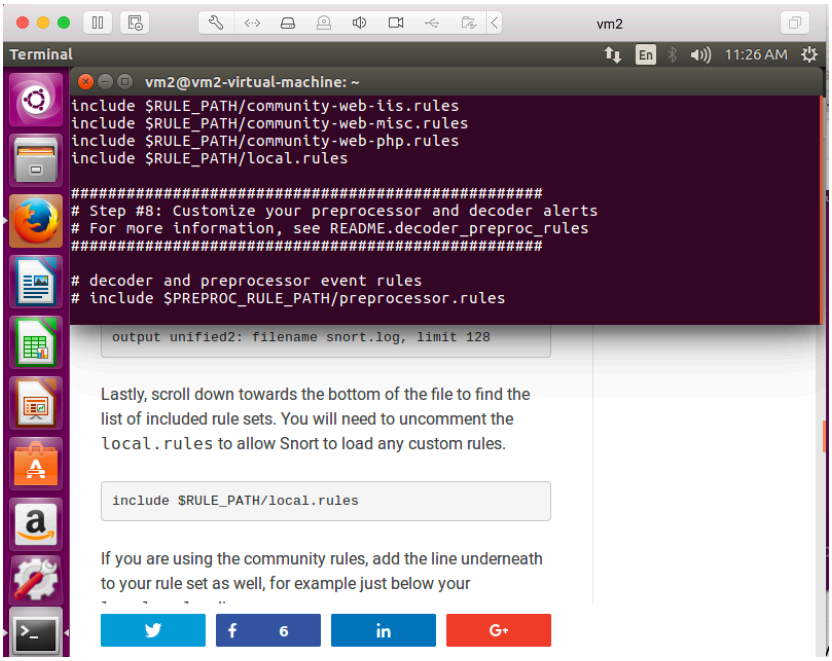
Log from IDS/IPS:

1. Setting SNORT local.rules

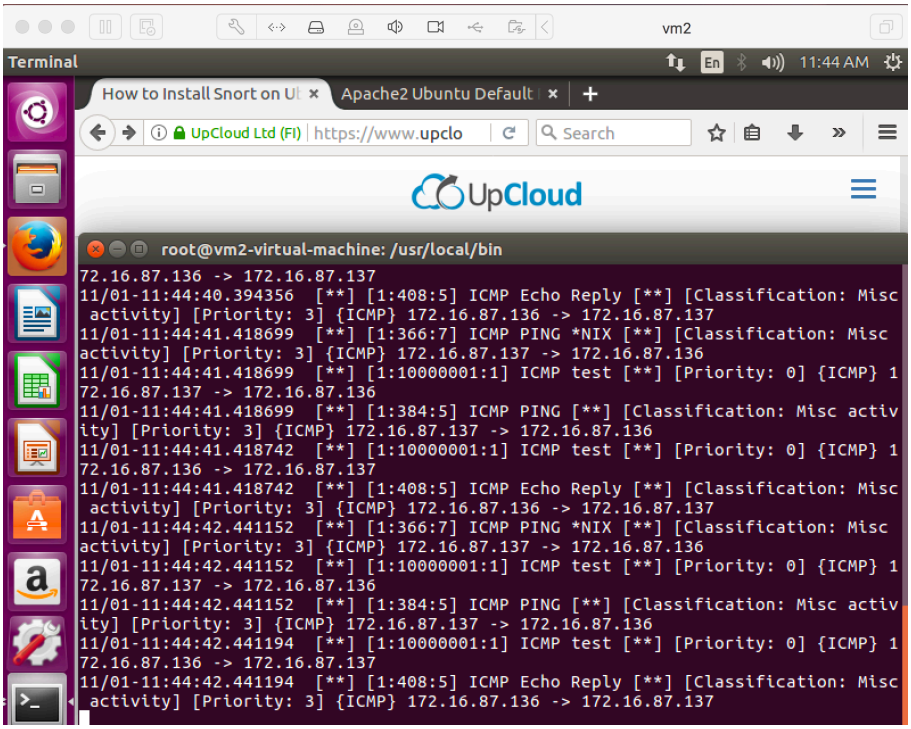
Alert icmp any any -> $HOME_NET any (msg: “ICMP test”; sid=10000001, rev:001;)

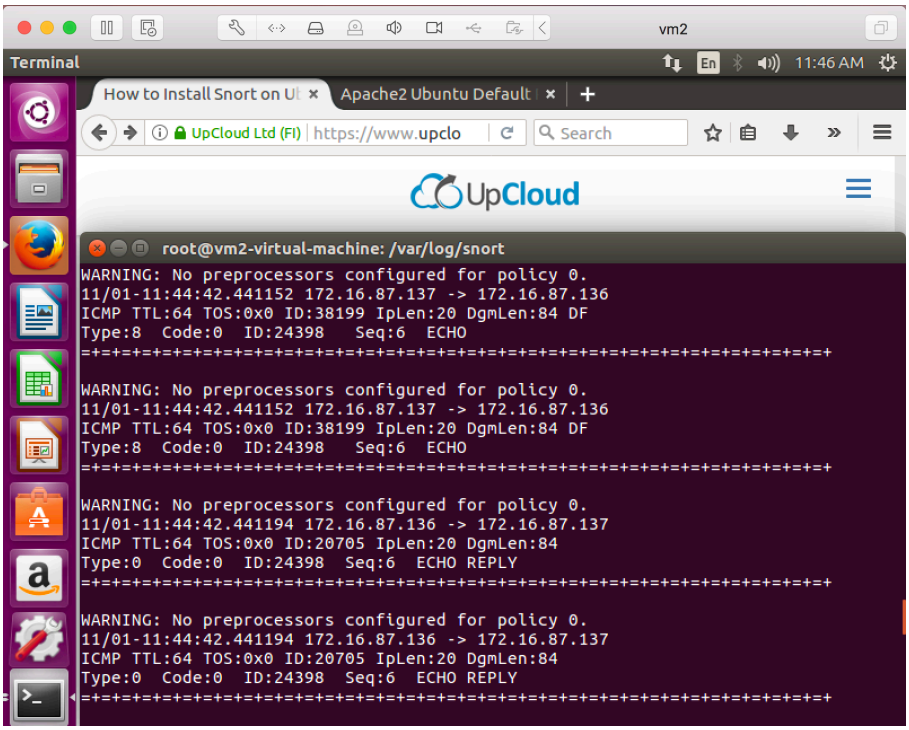


2. Include local.rules in snort.conf



3. VM3 is pinging VM2, and the snort log look like:





The architecture:

We set up the firewall on VM1 to deny icmp request from VM3 and test our UFW. Then we set up Snort IDS on VM2 and test our Snort is running. VM3 is kind of an attack VM sending Ping request to VM1 and VM2 respectively. The architecture looks like the following: