

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

```
root@vm1-virtual-machine:/etc/ufw# ifconfig
ens3      Link encap:Ethernet HWaddr 00:0c:29:b8:84:64
          inet addr:172.16.87.135 Bcast:172.16.87.255 Mask:255.255.255.0
          inet6 addr: fe80::36f3:a574:e56f:9adf/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:43744 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:11757 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:55630908 (55.6 MB) TX bytes:733305 (733.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:65536 Metric:1
                  RX packets:340 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:340 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:25471 (25.4 KB) TX bytes:25471 (25.4 KB)

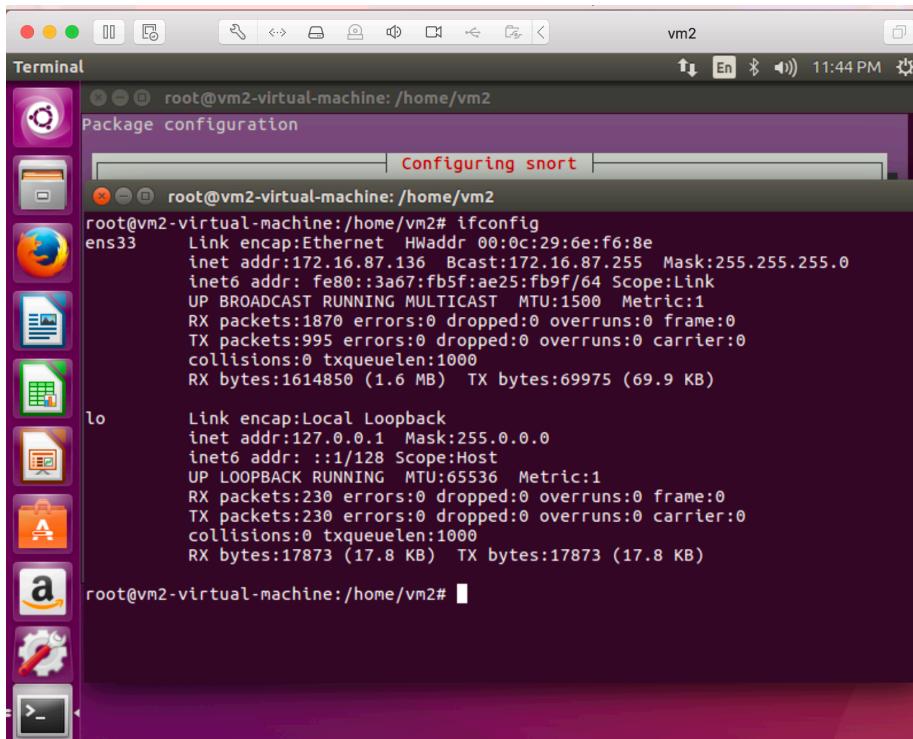
root@vm1-virtual-machine:/etc/ufw# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                      Action    From
--                      ----     ---
Anywhere on icmp        DENY IN   172.16.87.137

root@vm1-virtual-machine:/etc/ufw#
```

Screenshot of VM 2: Snort, HTTP, FTP

1. VM 2 IP Address: 172.16.87.136



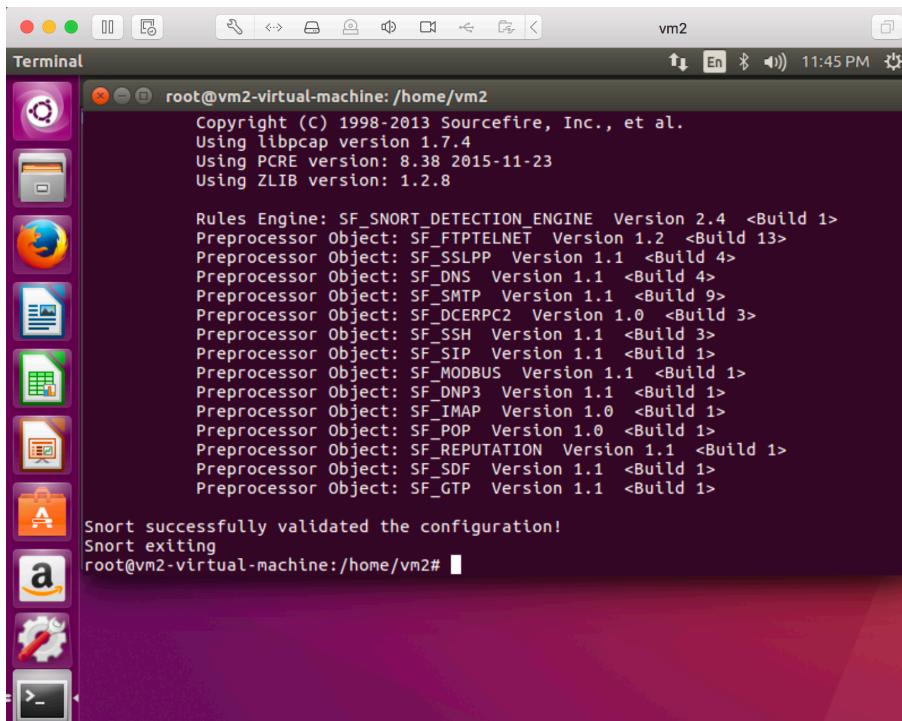
A screenshot of a Ubuntu desktop environment. The terminal window shows the output of the 'ifconfig' command. The output includes details for the ens33 interface (Link encap:Ethernet, HWaddr 00:0c:29:6e:f6:8e) and the lo interface (Link encap:Local Loopback). The IP address 172.16.87.136 is listed under the ens33 interface.

```
root@vm2-virtual-machine:/home/vm2# ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:6e:f6:8e
           inet addr:172.16.87.136 Bcast:172.16.87.255 Mask:255.255.255.0
           inet6 addr: fe80::3a67:fb5f:ae25:fb9f/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:1870 errors:0 dropped:0 overruns:0 frame:0
             TX packets:995 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:1614850 (1.6 MB) TX bytes:69975 (69.9 KB)

lo         Link encap:Local Loopback
           inet addr:127.0.0.1 Mask:255.0.0.0
           inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:65536 Metric:1
             RX packets:230 errors:0 dropped:0 overruns:0 frame:0
             TX packets:230 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:17873 (17.8 KB) TX bytes:17873 (17.8 KB)

root@vm2-virtual-machine:/home/vm2#
```

2. Snort



A screenshot of a Ubuntu desktop environment. The terminal window shows the output of the Snort configuration validation command. It lists various engine and preprocessor versions, followed by a success message indicating the configuration was validated.

```
root@vm2-virtual-machine:/home/vm2#
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
root@vm2-virtual-machine:/home/vm2#
```

3. HTTP

The screenshot shows a Linux desktop environment with a terminal window open in the foreground and a Firefox browser window in the background.

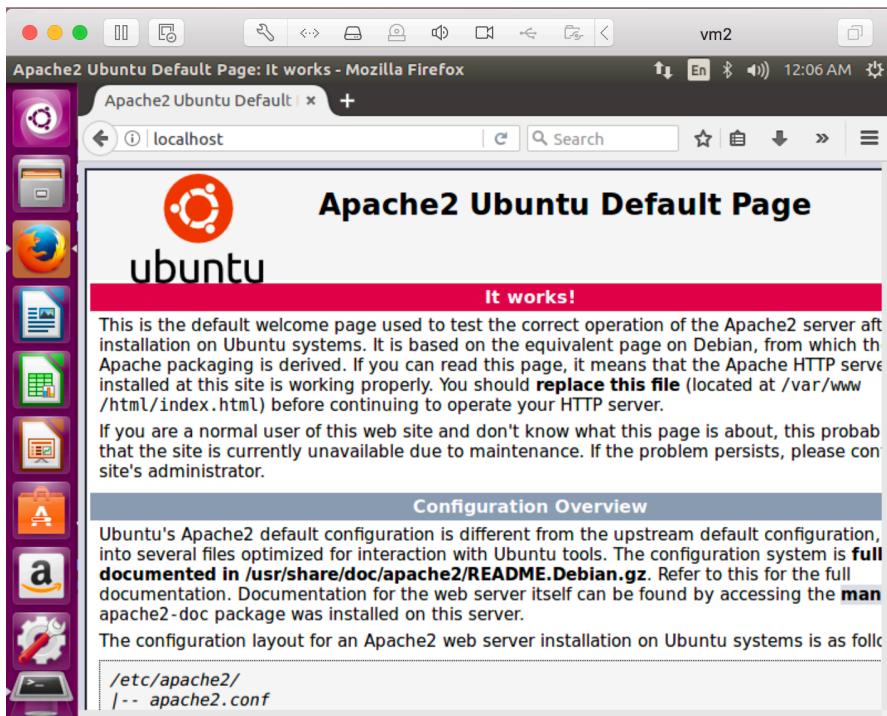
Terminal Window Content:

```
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=auto
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

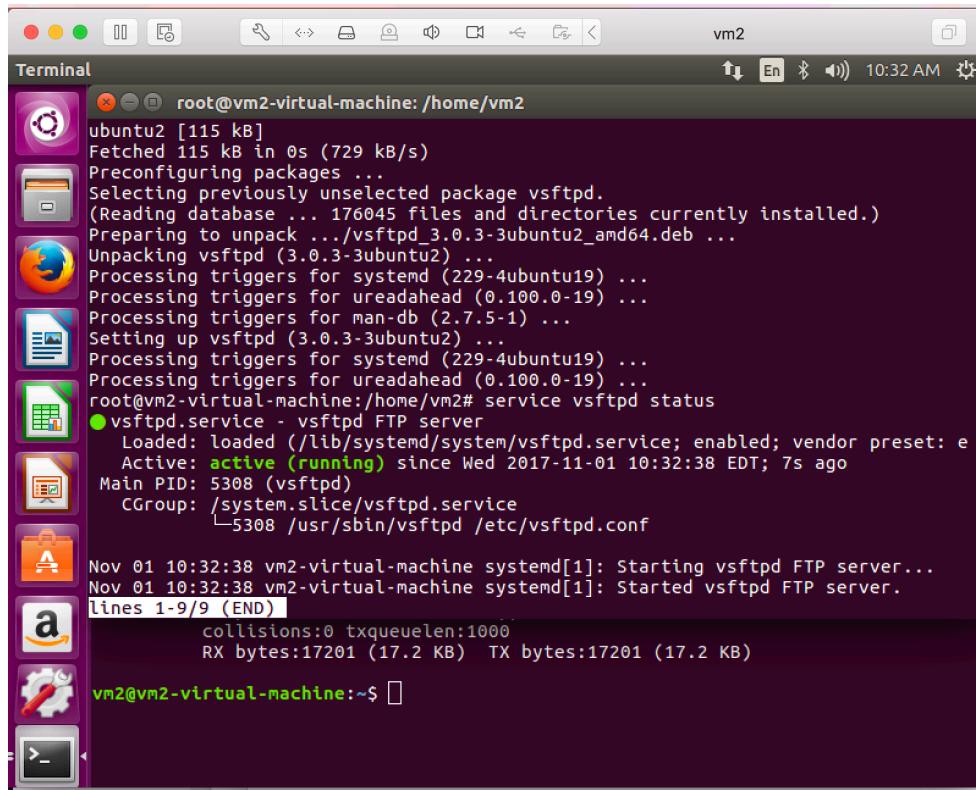
Nov 01 10:32:22 vm2-virtual-machine systemd[1]: Starting LSB: Apache2 web server
Nov 01 10:32:22 vm2-virtual-machine apache2[4654]: * Starting Apache httpd web
Nov 01 10:32:22 vm2-virtual-machine apache2[4654]: AH00558: apache2: Could not r
Nov 01 10:32:23 vm2-virtual-machine apache2[4654]: *
Nov 01 10:32:23 vm2-virtual-machine systemd[1]: Started LSB: Apache2 web server.
lines 1-16/16 (END)
```

Firefox Browser Window Content:

The Firefox browser is displaying the Apache2 Ubuntu Default Page. The page title is "Apache2 Ubuntu Default Page". It features the Ubuntu logo and the text "It works!". Below this, there is a detailed explanation of the default welcome page and a "Configuration Overview" section. A note at the bottom of the page states: "The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows: /etc/apache2/ -- apache2.conf".



4. FTP

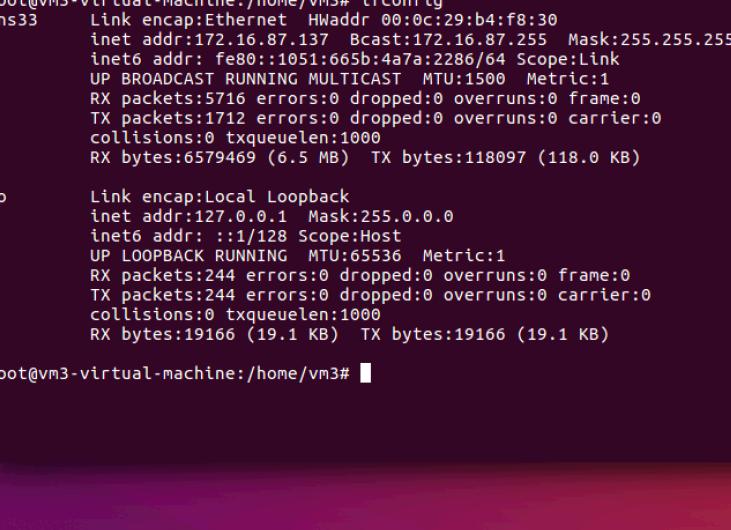


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and the window title is "vm2". The terminal output shows the following steps:

- Uploading a file named "ubuntu2" (115 kB) from the current directory.
- 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



The screenshot shows a terminal window running as root on a virtual machine named vm3. The terminal displays the output of the 'ifconfig' command, listing network interfaces ens33 and lo. The interface 'ens33' is an Ethernet adapter with an IP address of 172.16.87.137 and a MAC address of 00:0c:29:b4:f8:30. The interface 'lo' is a loopback adapter with an IP address of 127.0.0.1. Both interfaces show no errors or dropped packets.

```
root@vm3-virtual-machine:/home/vm3# ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:b4:f8:30
           inet addr:172.16.87.137 Bcast:172.16.87.255 Mask:255.255.255.0
             inet6 addr: fe80::1051:665b:4a7a:2286/64 Scope:Link
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
               RX packets:5716 errors:0 dropped:0 overruns:0 frame:0
               TX packets:1712 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:1000
               RX bytes:6579469 (6.5 MB)  TX bytes:118097 (118.0 KB)

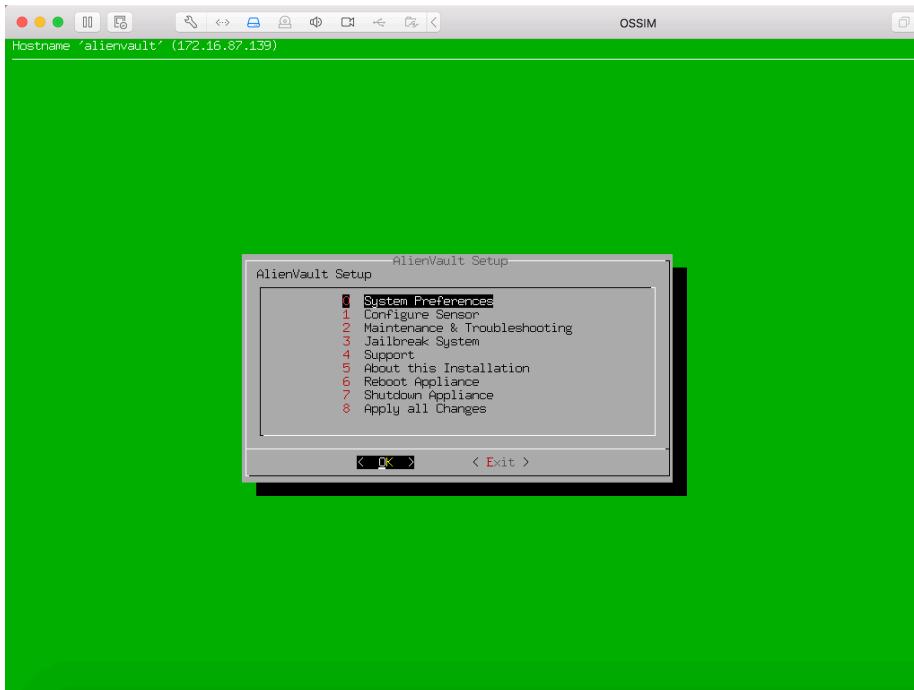
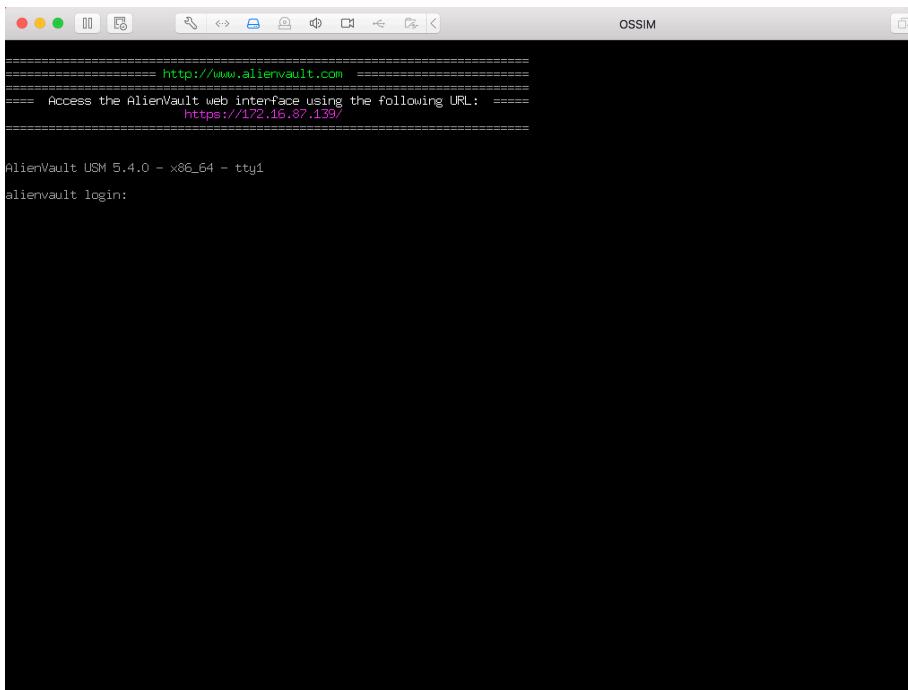
lo         Link encap:Local Loopback
           inet addr:127.0.0.1 Mask:255.0.0.0
             inet6 addr: ::1/128 Scope:Host
               UP LOOPBACK RUNNING MTU:65536 Metric:1
               RX packets:244 errors:0 dropped:0 overruns:0 frame:0
               TX packets:244 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:1000
               RX bytes:19166 (19.1 KB)  TX bytes:19166 (19.1 KB)

root@vm3-virtual-machine:/home/vm3#
```

2. Pytbull

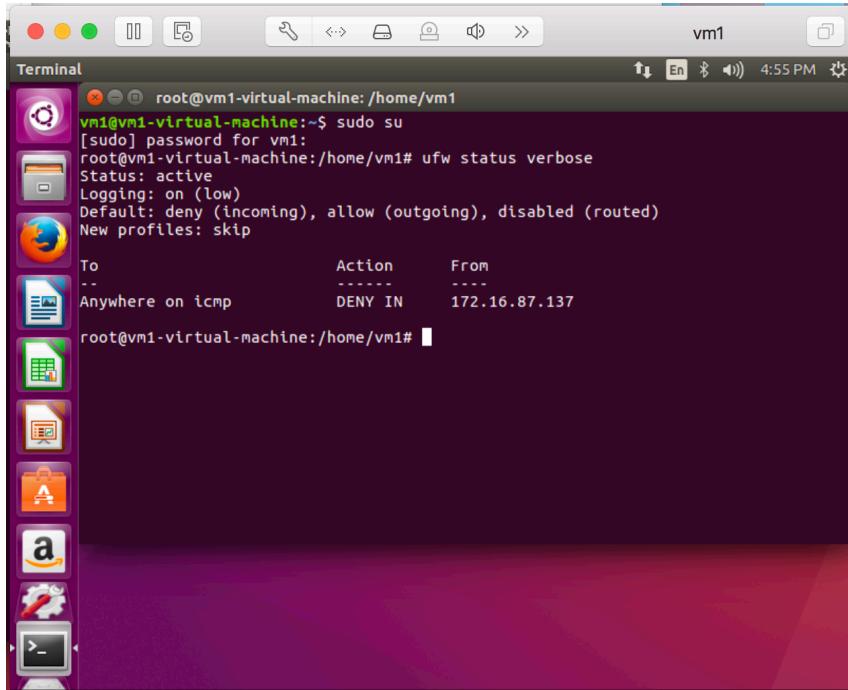
Screenshot on VM 4:

1. OSSIM



Logs from FW:

1. Firewall rules on VM1, deny icmp from VM3



The screenshot shows a Linux desktop environment with a terminal window titled "vm1". The terminal window contains the following command and its output:

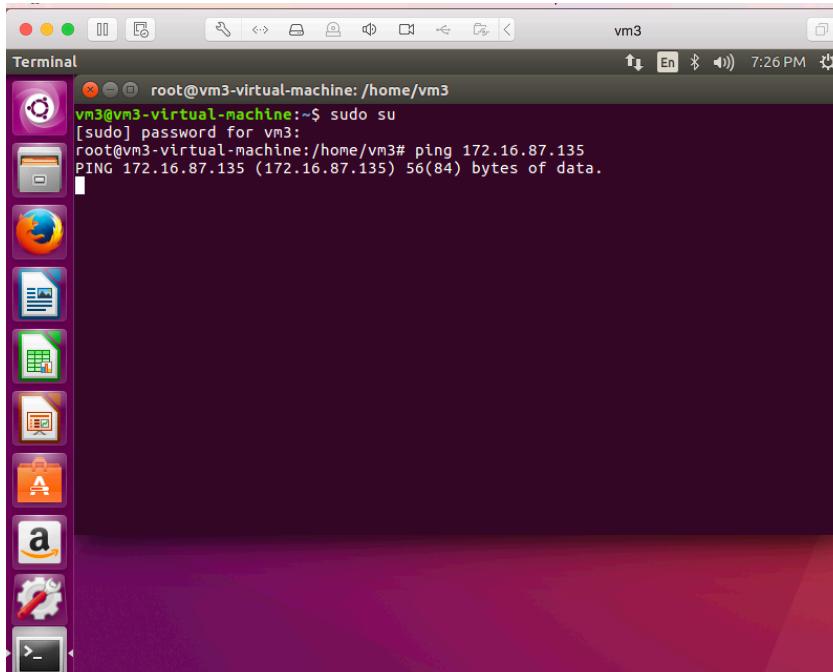
```
root@vm1-virtual-machine:~$ sudo su
[sudo] password for vm1:
root@vm1-virtual-machine:/home/vm1# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ----      ---
Anywhere on icmp          DENY IN    172.16.87.137

root@vm1-virtual-machine:/home/vm1#
```

command: ufw deny in on icmp from 172.16.87.137

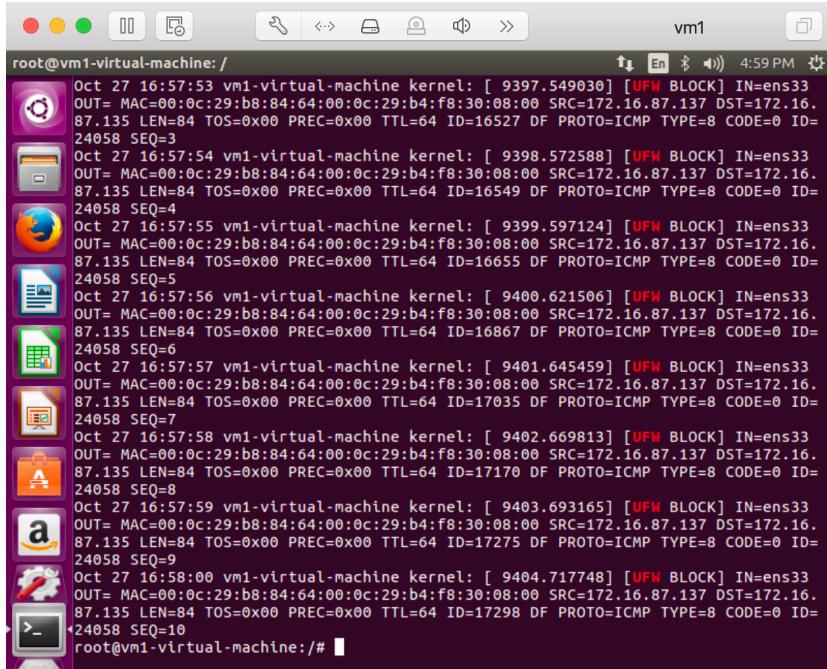
2. VM3 ping VM1



The screenshot shows a Linux desktop environment with a terminal window titled "vm3". The terminal window contains the following command and its output:

```
root@vm3-virtual-machine:~$ sudo su
[sudo] password for vm3:
root@vm3-virtual-machine:/home/vm3# ping 172.16.87.135
PING 172.16.87.135 (172.16.87.135) 56(84) bytes of data.
```

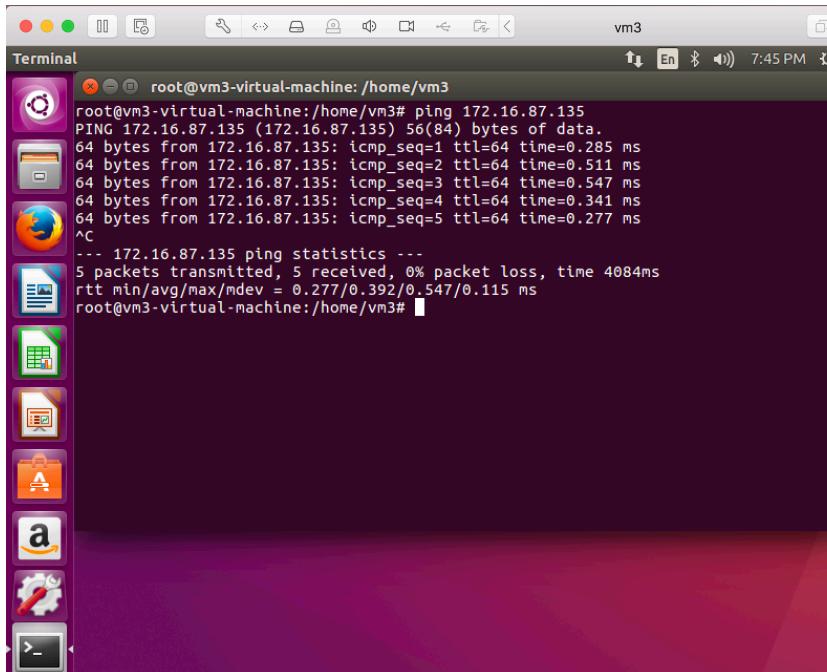
3. UFW Log:



```
root@vm1-virtual-machine: /root
Oct 27 16:57:53 vm1-virtual-machine kernel: [ 9397.549030] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=16527 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=3
Oct 27 16:57:54 vm1-virtual-machine kernel: [ 9398.572588] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=16549 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=4
Oct 27 16:57:55 vm1-virtual-machine kernel: [ 9399.597124] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=16655 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=5
Oct 27 16:57:56 vm1-virtual-machine kernel: [ 9400.621506] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=16867 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=6
Oct 27 16:57:57 vm1-virtual-machine kernel: [ 9401.645459] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=17035 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=7
Oct 27 16:57:58 vm1-virtual-machine kernel: [ 9402.669813] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=17170 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=8
Oct 27 16:57:59 vm1-virtual-machine kernel: [ 9403.693165] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=17275 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=9
Oct 27 16:58:00 vm1-virtual-machine kernel: [ 9404.717748] [UFW BLOCK] IN=ens33
OUT= MAC=00:0c:29:b8:84:64:00:0c:29:b4:f8:30:08:00 SRC=172.16.87.137 DST=172.16.
87.135 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=17298 DF PROTO=ICMP TYPE=8 CODE=0 ID=
24058 SEQ=10
root@vm1-virtual-machine:/#
```

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.

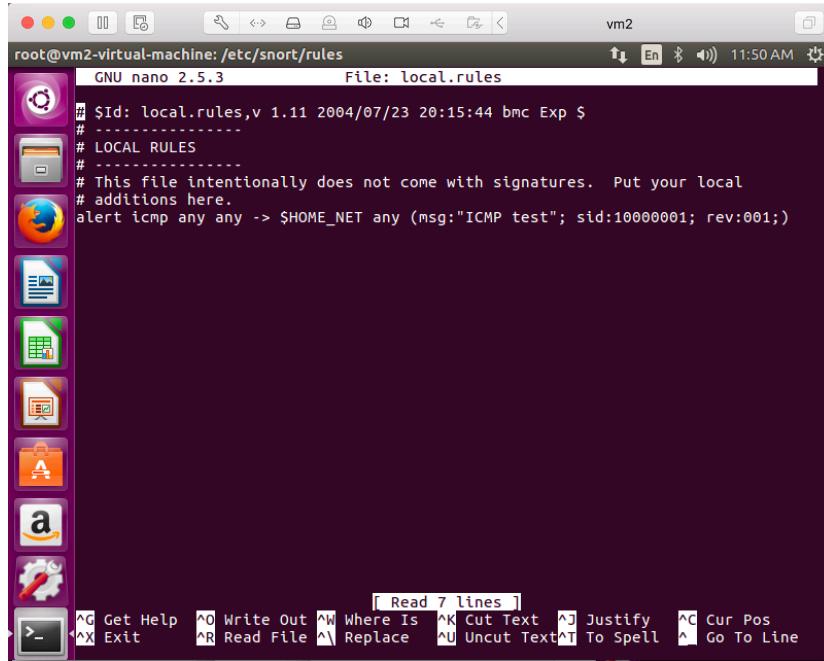


```
root@vm3-virtual-machine:/home/vm3
root@vm3-virtual-machine:/home/vm3# ping 172.16.87.135
PING 172.16.87.135 (172.16.87.135) 56(84) bytes of data.
64 bytes from 172.16.87.135: icmp_seq=1 ttl=64 time=0.285 ms
64 bytes from 172.16.87.135: icmp_seq=2 ttl=64 time=0.511 ms
64 bytes from 172.16.87.135: icmp_seq=3 ttl=64 time=0.547 ms
64 bytes from 172.16.87.135: icmp_seq=4 ttl=64 time=0.341 ms
64 bytes from 172.16.87.135: icmp_seq=5 ttl=64 time=0.277 ms
^C
--- 172.16.87.135 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4084ms
rtt min/avg/max/mdev = 0.277/0.392/0.547/0.115 ms
root@vm3-virtual-machine:/home/vm3#
```

Log from IDS/IPS:

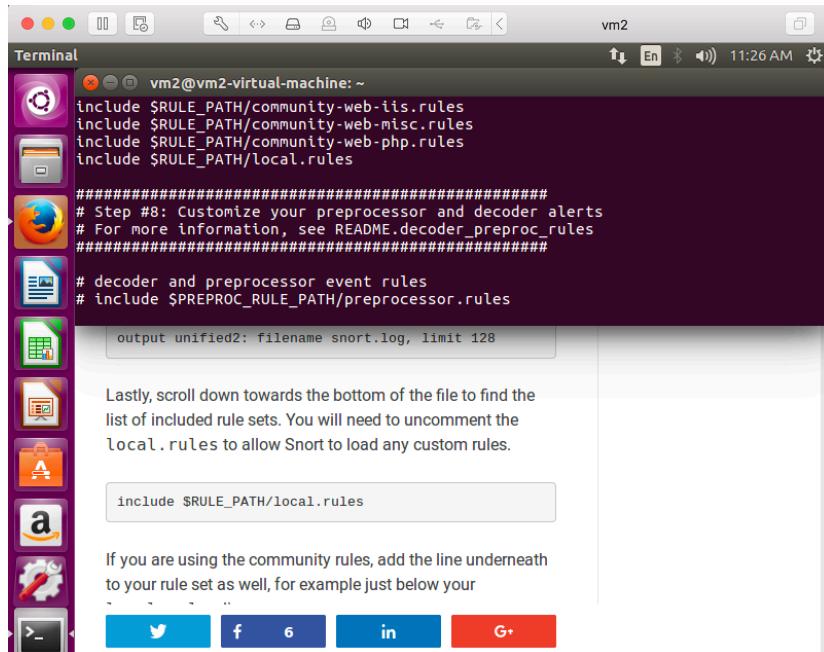
1. Setting SNORT local.rules

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



```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

2. Include local.rules in snort.conf



```
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/local.rules

#####
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
#####

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules

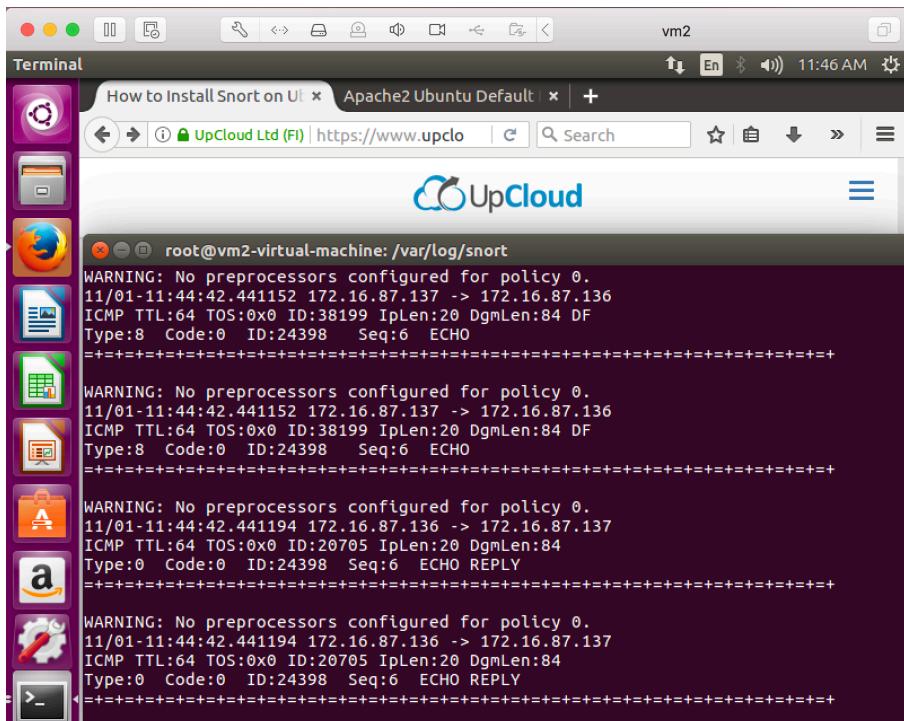
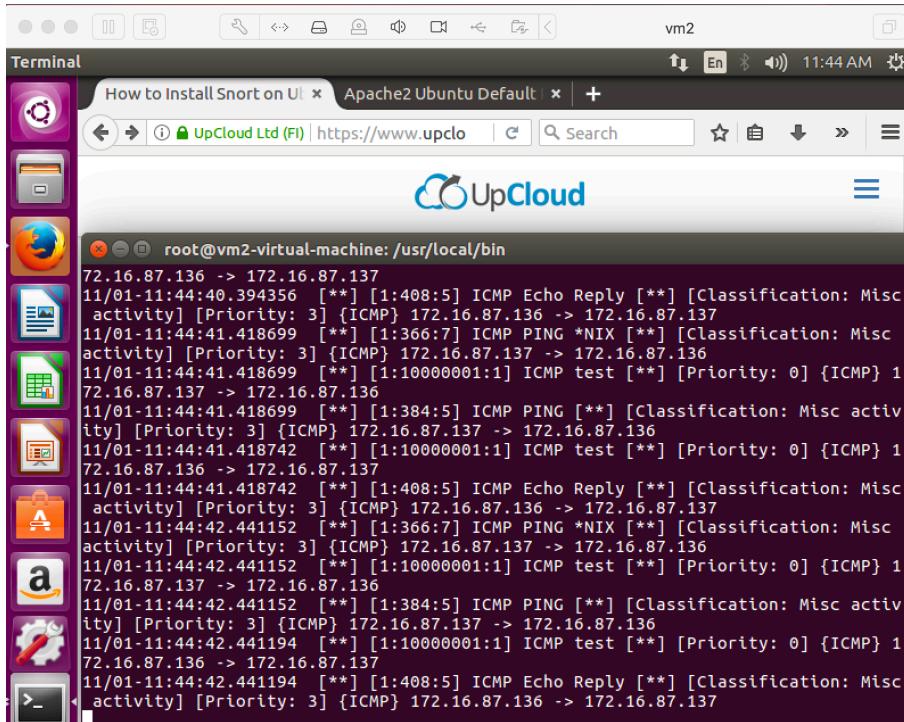
output unified2: filename snort.log, limit 128

Lastly, scroll down towards the bottom of the file to find the
list of included rule sets. You will need to uncomment the
local.rules to allow Snort to load any custom rules.

include $RULE_PATH/local.rules

If you are using the community rules, add the line underneath
to your rule set as well, for example just below your
```

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:

