Snort Sniffing

Introduction and/or Background

What happens when you mix an olfactory professional with a crossing guard and a programmer? You get Snort: an Intrusion Protection and Detection System that blocks malicious packets and logs their details when detected. Able to match packets to a wide variety of different included rulesets, as well as apply custom rulesets, Snort is used to protect against a wide variety of attacks in the business world.

Objectives

In this project/lab the student will:

- Gain familiarity with Snort

Equipment/Supplies Needed

- As specified in Lab 0.0.1.

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

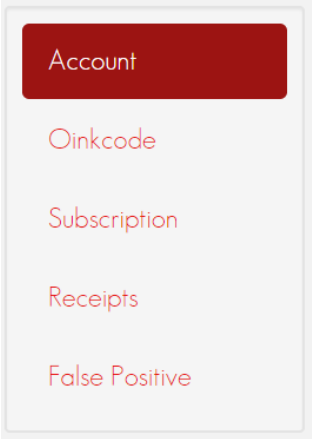
Assignment

1. Register an account on https://snort.org

2. Obtain an Oinkcode
   a. Click your account name in the upper-right corner of the page.

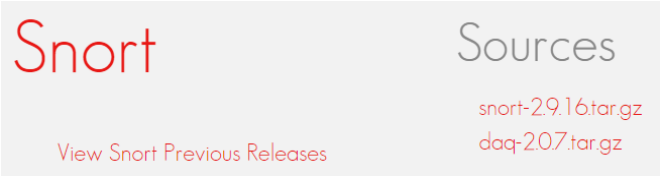
   

   b. Click Oinkcode on the menu.



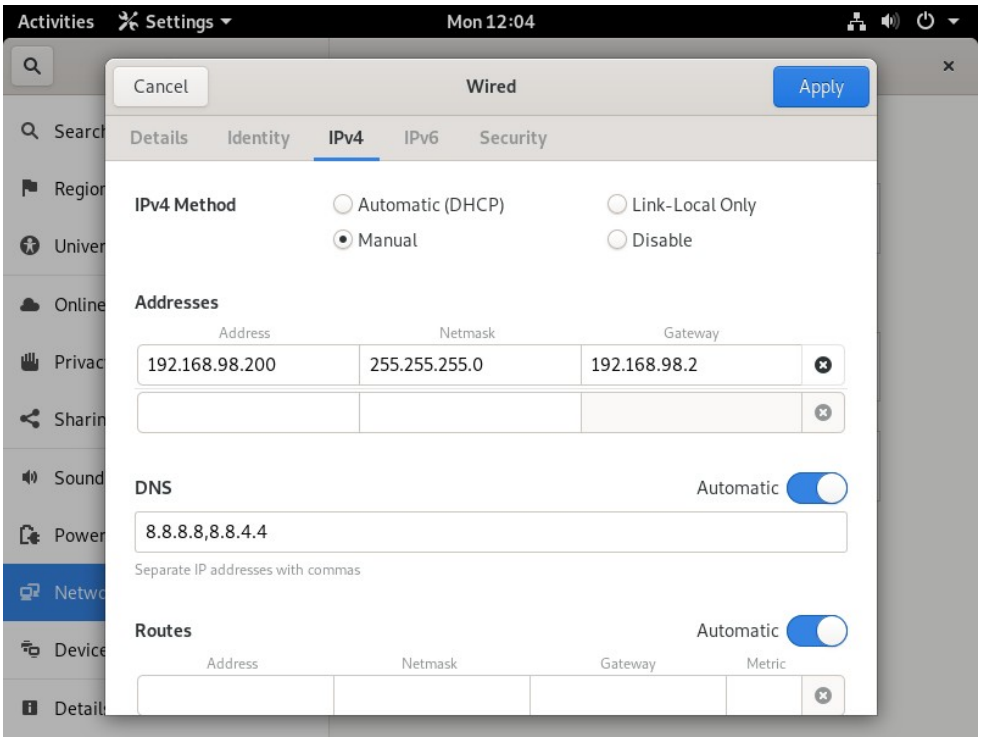
c. Copy the oinkcode to a text file for later use.

3. Note the most recent version of snort and its daq at https://www.snort.org/downloads



Pre-Installation Steps

1. Prepare the server for installation
   a. If necessary, assign it a static private IP address.
      i. Note the address, subnet, and gateway it was assigned via DHCP: ip addr
      ii. Edit its address information:



        iii. Restart the VM.
    b. Update the operating system: sudo apt-get update

2. Install Snort's prerequisites:
   sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet autoconf libtool build-essential tcpdump

Installation Instructions

1. Create a user and group for snort's files:
   a. sudo groupadd snort
   b. sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort

2. Create an installation directory for Snort:
   a. sudo mkdir /home/snort/
   b. sudo mkdir /home/snort/snort_src

3. Change the working directory to snort_src

4. Prepare the DAQ:
   a. Download the latest version: sudo wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
      i. Note: The latest version is located at https://www.snort.org/downloads
   b. Install the DAQ:
      i. Decompress it: sudo tar -xvf daq-2.0.7.tar.gz
      ii. Change to its directory: cd daq-2.0.7
      iii. Prepare the configuration script: sudo autoreconf -f -i
      iv. Run its compilation scripts: sudo ./configure && sudo make && sudo make install

5. Install Snort:
   a. Return to the snort_src directory.
   b. Obtain the latest version: sudo wget https://www.snort.org/downloads/snort/snort-2.9.16.tar.gz
   c. Extract it: sudo tar -xvf snort-2.9.16.tar.gz
   d. Change to its directory: cd snort-2.9.16
   e. Prepare its configuration script: sudo autoreconf -f -i
   f. Compile and install it: ./configure --enable-sourcefire && sudo make && sudo make install
   g. Configure its library directories: sudo ldconfig

6. Prepare Snort for use:
   a. Create a soft link for its binary file: sudo ln -s /usr/local/bin/snort /usr/sbin/snort
   b. Verify its installation: sudo snort -V

```
administrator@VMSVR1:/home/snort/snort_src/snort-2.9.16$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.16 GRE (Build 118)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

c. **Take a screenshot** for later submission.

7. Prepare its NIDS component
   a. Create Snort's /etc structure.
      i. Create its basic directory structure:
         1. sudo mkdir /etc/snort
         2. sudo mkdir /etc/snort/rules
         3. sudo mkdir /etc/snort/preproc_rules
         4. sudo mkdir /var/log/snort
      ii. Create its rule files
         1. sudo touch /etc/snort/rules/white_list.rules
         2. sudo touch /etc/snort/rules/black_list.rules
         3. sudo touch /etc/snort/rules/local.rules
         4. sudo touch /var/log/snort/snort.log
   b. Create a directory for snort Dynamics rules: sudo mkdir /usr/local/lib/snort_dynamicrules
   c. Set the appropriate directory permissions
      i. sudo chmod -R 5775 /etc/snort
      ii. sudo chmod -R 5775 /var/log/snort
      iii. sudo chmod -R 5775 /usr/local/lib/snort
      iv. sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
   d. Set the appropriate ownership permissions
      i. sudo chown -R snort:snort /etc/snort
      ii. sudo chown -R snort:snort /var/log/snort
      iii. sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
   e. Copy *.conf and *.map files from snort download directory to /etc/snort. Change snort-2.9.16 to the directory containing snort's installation files.
      i. sudo cp /home/snort/snort_src/snort-2.9.16/etc/*.conf* /etc/snort/
      ii. sudo cp -v /home/snort/snort_src/snort-2.9.16/etc/*.map* /etc/snort/
   f. Configure /etc/snort/snort.conf
      i. Before editing snort.conf get the backup of that file first: sudo cp /etc/snort/snort.conf /etc/snort/snort_orig.conf
   g. Copy all of the rules into their their proper locations (copy and paste the command):
      sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf

8. Configure Snort's configuration settings
   a. Edit the HOME_NET and EXTERNAL_NET variables

i. Open the /etc/snort/snort.conf file for editing and go to line 45.
ii. Change the ip variable HOME_NET from any to the server's ip address. For example: ipvar HOME_NET 192.168.98.200/24
iii. Change the ip variable EXTERNAL_NET from any to !HOME_NET. Example: ipvar EXTERNAL_NET !$HOME_NET

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.98.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
```

b. Update its ruleset directory locations.
   i. Go to line 104 and modify the section's current variables.
      1. var RULE_PATH /etc/snort/rules
      2. var SO_RULE_PATH /etc/snort/so_rules
      3. var PREPROC_RULE_PATH /etc/snort/preproc_rules

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

   ii. Go to line 113 and change the following:
      1. var WHITE_LIST_PATH /etc/snort/rules
      2. var BLACK_LIST_PATH /etc/snort/rules

```
# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snor$
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

c. Specify the log file's location.
   i. Go to line 186, uncomment it, and add the following: /var/log/snort

```
# Configure default log directory for snort to log to.  For more information se$
#
  config logdir: /var/log/snort
```

   ii. Go to line 522 and insert the following: output unified2: filename snort.log, limit 128

```
# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, v$
output unified2: filename snort.log, limit 128
```

d. On line 547, uncomment the site specific local.rules entry.

```
# site specific rules
include $RULE_PATH/local.rules
```

e. Save and exit the file.

9. Obtain Snort's registered user rules
   a. Navigate to the /home/snort/ directory.
   b. Download the rules, replacing oinkcode with the code obtained previously: sudo wget https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=oinkcode -O /home/snort/snort_src/registered.tar.gz

c. Extract them and copy them to the correct folder: sudo tar -xvf /home/snort/snort_src/registered.tar.gz -C /etc/snort

10. Prepare Snort's community rules
    a. If necessary, change the present working directory to snort_src
    b. Download the rules: sudo wget https://www.snort.org/downloads/community/community-rules.tar.gz
    c. Extract them: sudo tar -xvf community-rules.tar.gz
    d. Copy the community rules to the /etc/snort/rules directory: sudo cp -r /home/snort/snort_src/community-rules /etc/snort/rules

11. Copy Snort's remaining configuration files to their expected locations.
    a. sudo wget https://www.snort.org/documents/classification-config
    b. sudo wget https://www.snort.org/documents/reference-config
    c. sudo cp classification-config /etc/snort/classification.config
    d. sudo cp reference-config /etc/snort/reference.config

12. Verify the Snort configuration: sudo snort -T -i 2 -c /etc/snort/snort.conf
    a. Note: The -i option specifies the interface as listed in the "ip addr" command. Yours may be different.

13. **Take a screenshot** for later submission.

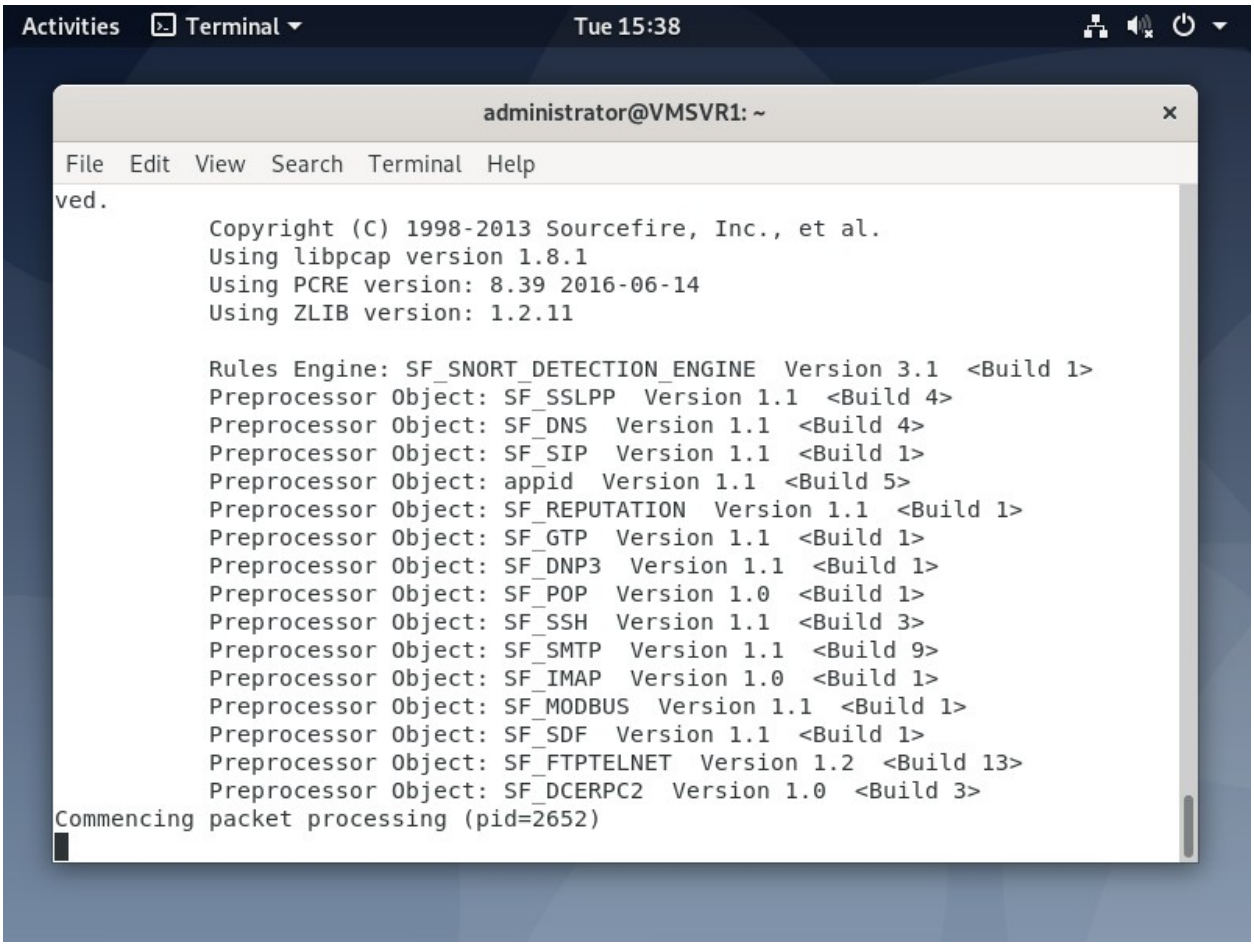
Rule Creation and Verification

1. Create a new custom rule
    a. Open the local.rules file: sudo nano /etc/snort/rules/local.rules
    b. Add the following rule to the end of the file: alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)

```
#-------------
# LOCAL RULES
#-------------

alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

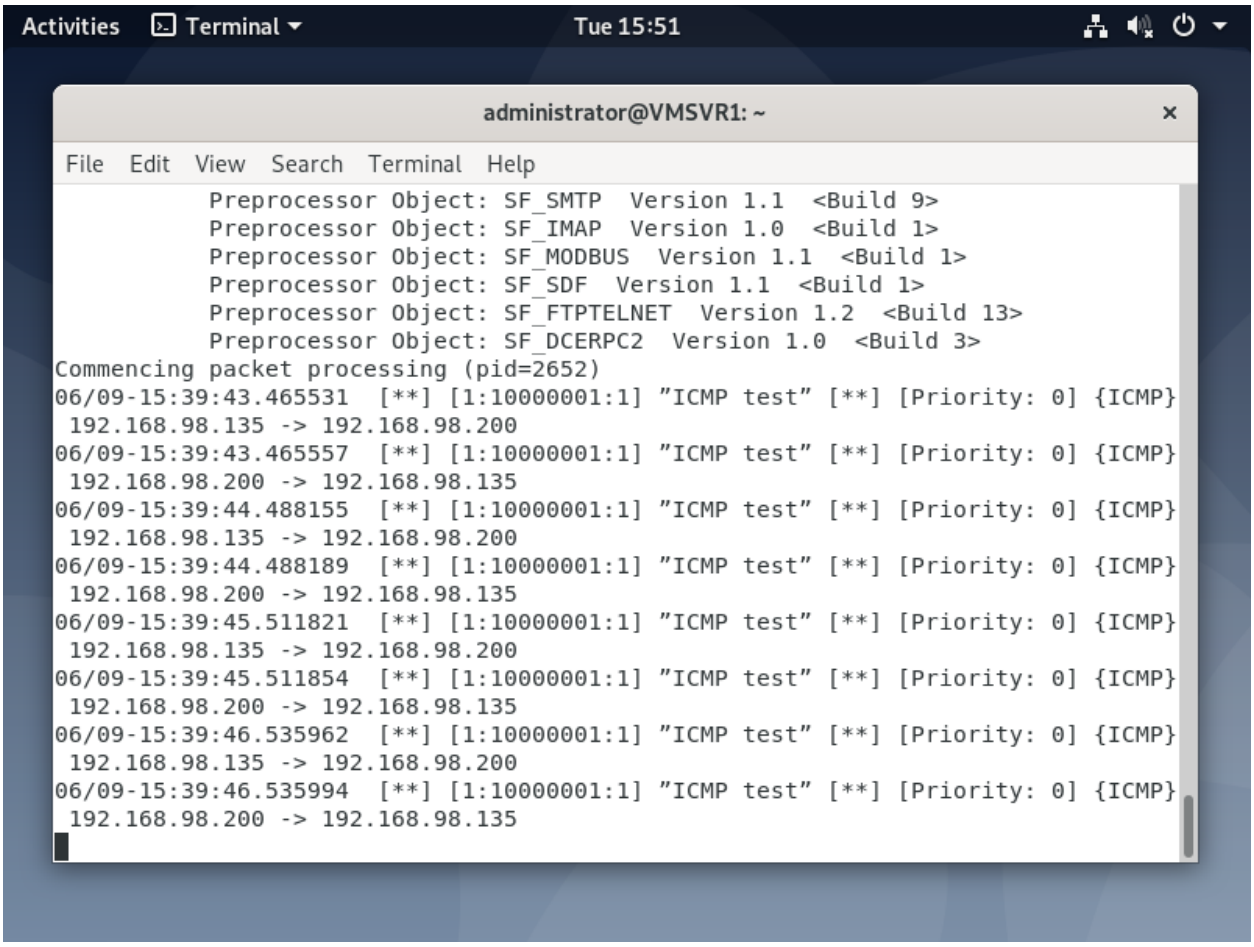
    c. Save and exit local.rules
    d. Start Snort: sudo snort -A console -i ens33 -u snort -g snort -c /etc/snort/snort.conf
    e. Take a screenshot of Snort activating successfully.



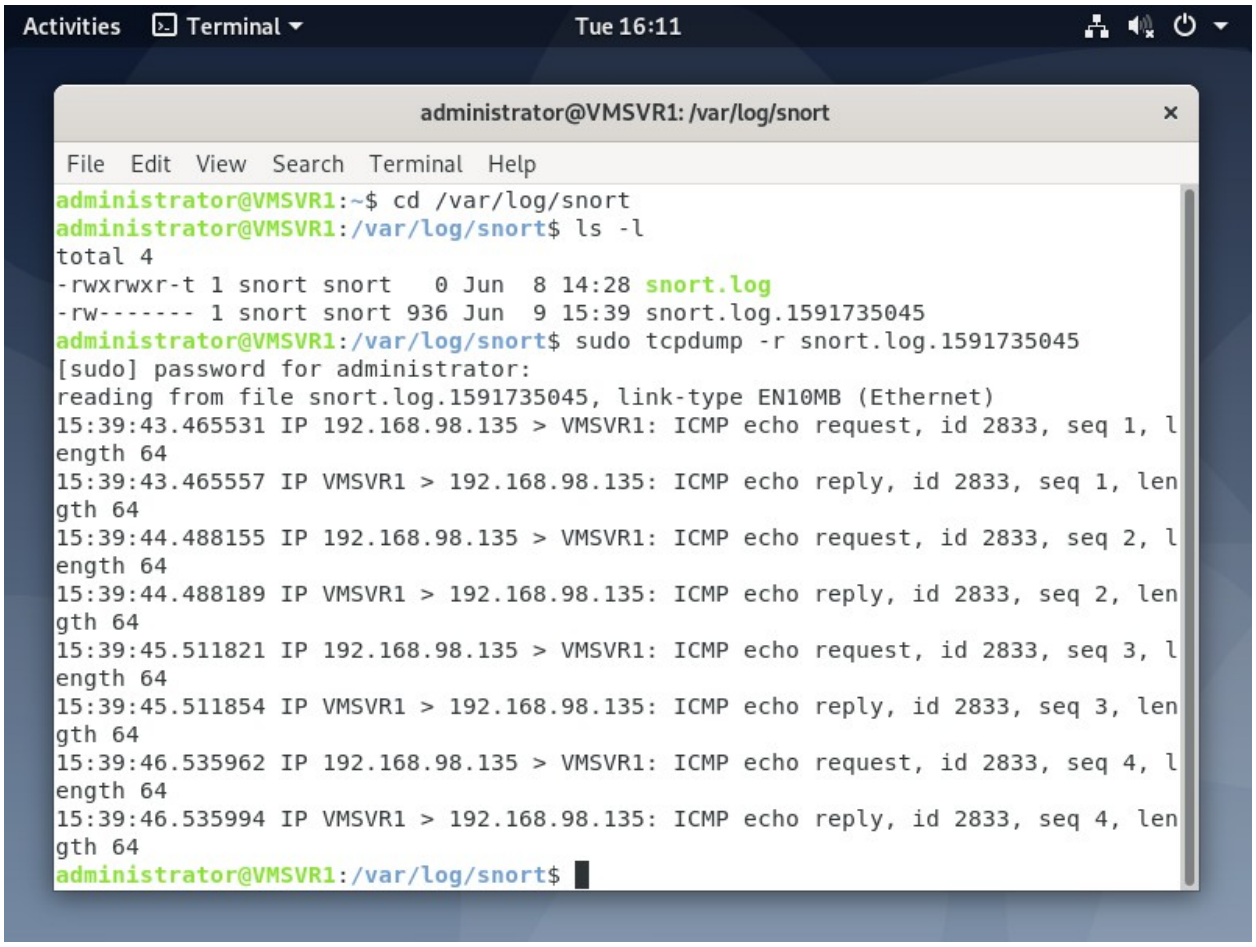
2. Verify that snort is working as intended.
   a. Turn on and log into VMPC1.
   b. Open a terminal window and ping VMSVR1's address.

```
administrator@vmpc1:~$ ping 192.168.98.200
PING 192.168.98.200 (192.168.98.200) 56(84) bytes of data.
64 bytes from 192.168.98.200: icmp_seq=1 ttl=64 time=0.176 ms
64 bytes from 192.168.98.200: icmp_seq=2 ttl=64 time=0.450 ms
64 bytes from 192.168.98.200: icmp_seq=3 ttl=64 time=0.403 ms
64 bytes from 192.168.98.200: icmp_seq=4 ttl=64 time=0.336 ms
^C
--- 192.168.98.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 73ms
rtt min/avg/max/mdev = 0.176/0.341/0.450/0.104 ms
```

   c. Switch to VMSVR1 and check for Snort output in the Terminal window.



3. Examine the snort.log file
   a. Open a new Terminal window.
   b. Switch to the /var/log/snort directory.
   c. Display the directory's contents: ls -l
   d. Decode the snort log: sudo tcpdump -r <snort log filename>



e. **Take a screenshot** of the Snort log messages in the Terminal window.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing sudo snort -V output (25 points)	
	Criteria #2: Screenshot showing sudo snort -T -i 2 -c /etc/snort/snort.conf output (25 points)	
	Criteria #3: Screenshot showing Snort activating successfully (25 points)	
	Criteria #4: Screenshot showing Snort log messages (25 points)	