PROJECT : Snort on Ubuntu

Name : Vaishnavi Madhav Shinde

Roll No : MH-JM-24-07-0103

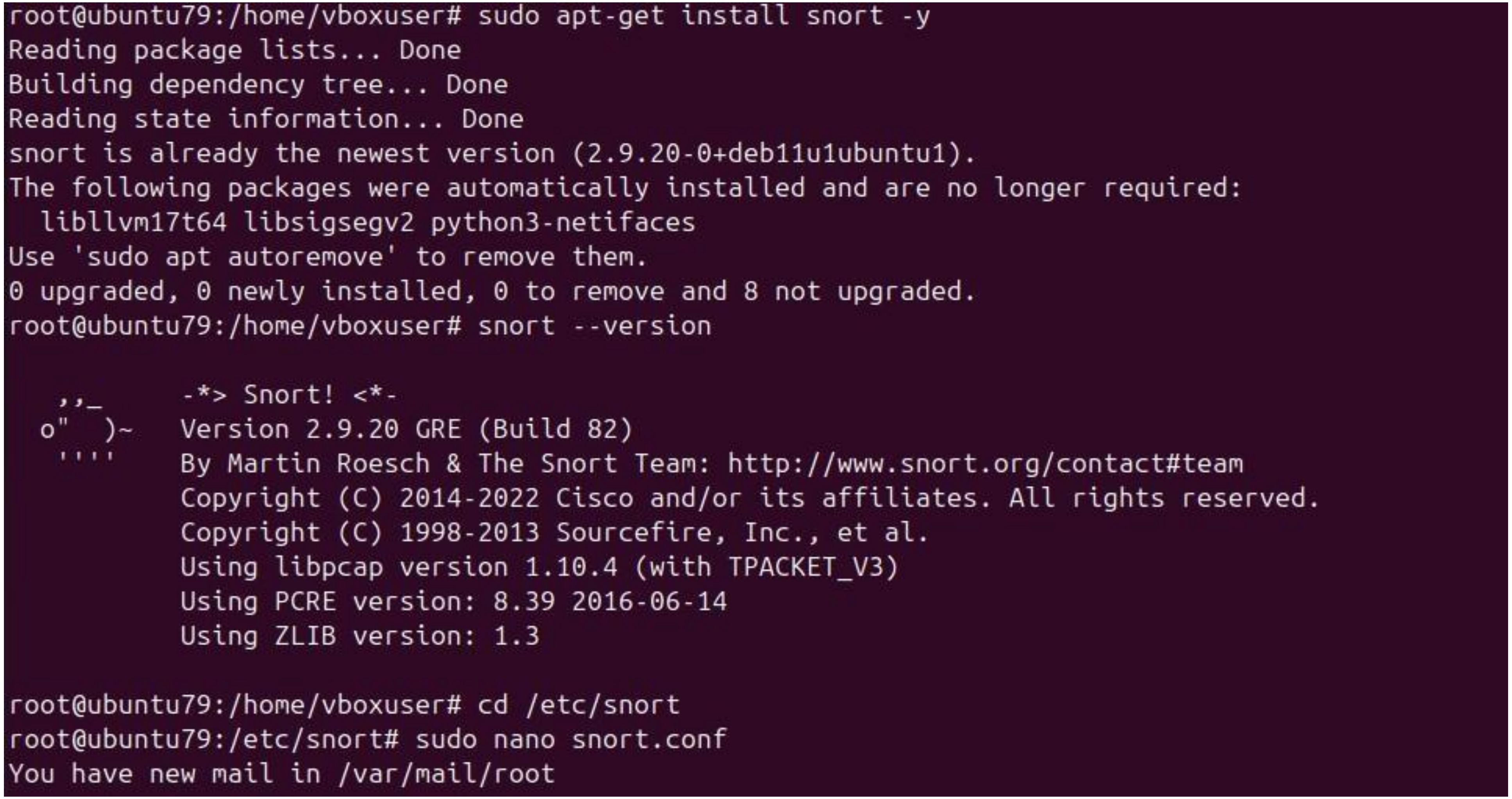
Course : Cyber Security Specialist

Guided By : Deepyesh Sir.

Snort on Ubuntu

Snort is an **open-source IDS/IPS** that monitors network traffic for threats using predefined rules. It can **detect, log, and block** malicious activity in real-time. It’s widely used for **network security, forensics, and threat detection**. You can customize rules to identify specific attacks.

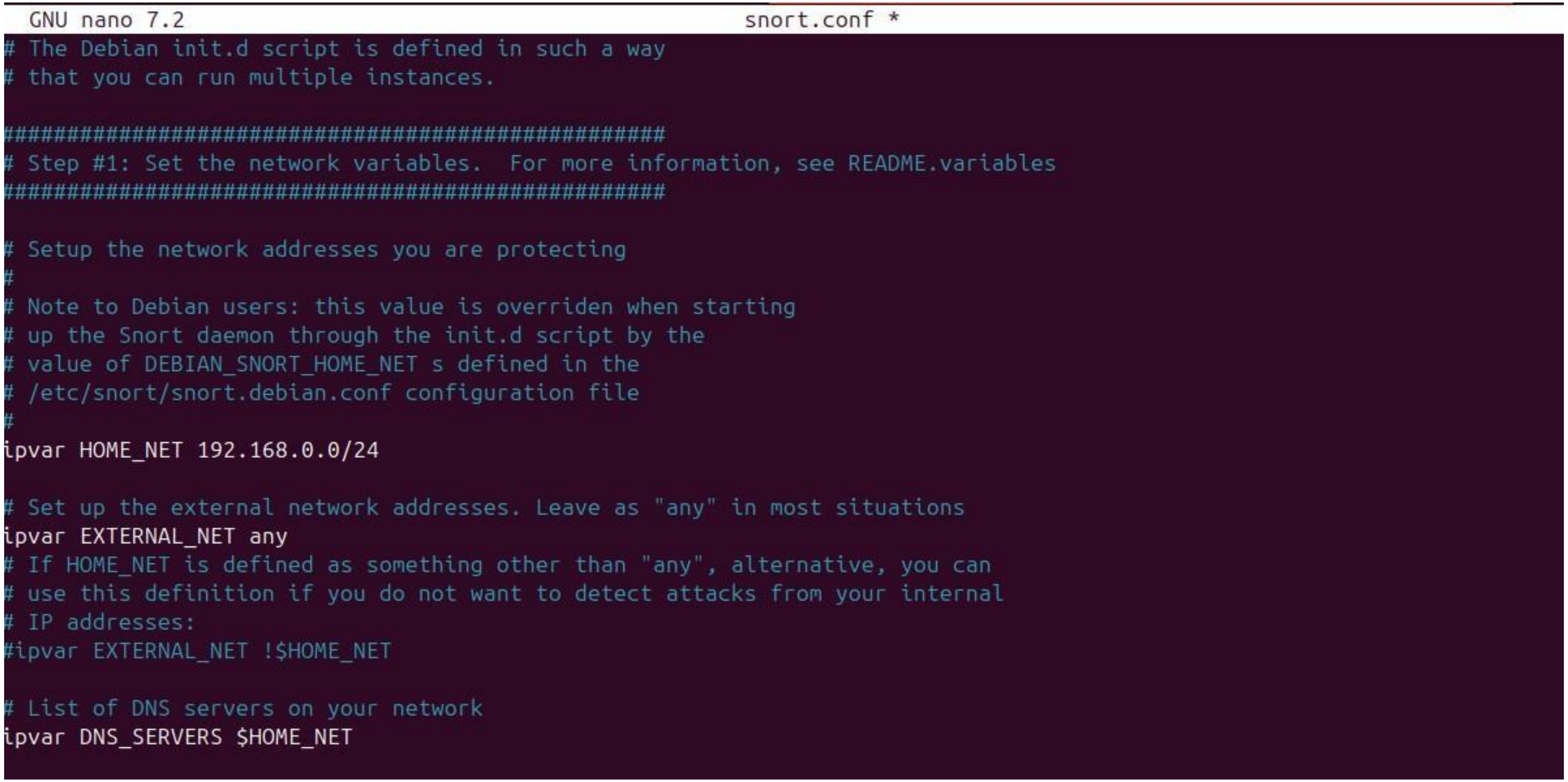
```
>sudo apt-get install snort -y

 >snort --version

 >cd /etc/snort

 >open the snort.conf file for editing

 >sudo nano snort.conf
```



```
root@ubuntu79:/home/vboxuser# sudo apt-get install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.20-0+deb11u1ubuntu1).
The following packages were automatically installed and are no longer required:
  libllvm17t64 libsigsegv2 python3-netifaces
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
root@ubuntu79:/home/vboxuser# snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

root@ubuntu79:/home/vboxuser# cd /etc/snort
root@ubuntu79:/etc/snort# sudo nano snort.conf
You have new mail in /var/mail/root
```

Inside the Nano editor, find the line:

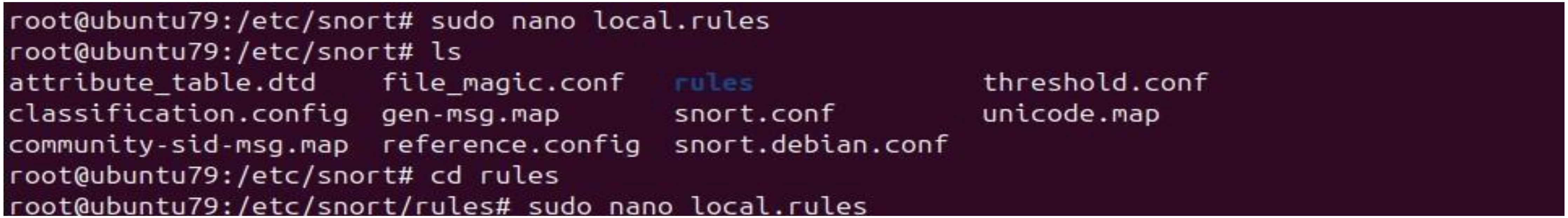
> ipvar HOME_NET 192.168.0.0/24



```
# The Debian init.d script is defined in such a way
# that you can run multiple instances.

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.0.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
```

Create a new rule file for ICMP traffic:

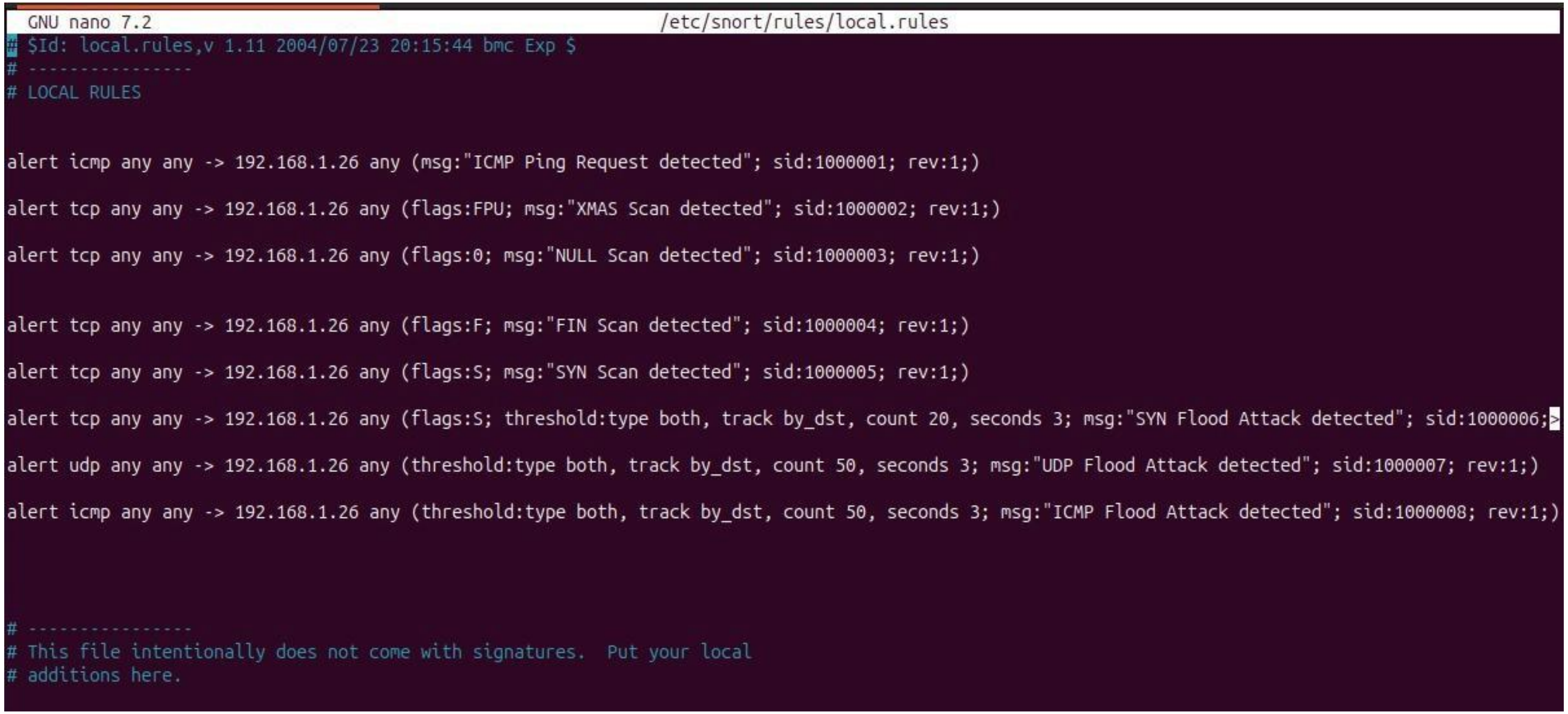
c>sudo nano local.rules



```
root@ubuntu79:/etc/snort# sudo nano local.rules
root@ubuntu79:/etc/snort# ls
attribute_table.dtd    file_magic.conf   rules              threshold.conf
classification.config  gen-msg.map       snort.conf         unicode.map
community-sid-msg.map  reference.config  snort.debian.conf
root@ubuntu79:/etc/snort# cd rules
root@ubuntu79:/etc/snort/rules# sudo nano local.rules
```

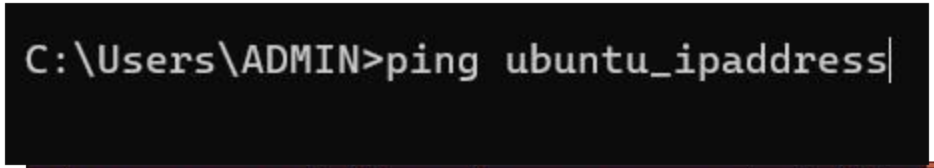
Add the following rule to detect ICMP traffic:

alert icmp any any -> $HOME_NET any (msg: “ICMP PING DETECTED”; sid:1000011; rev:1;

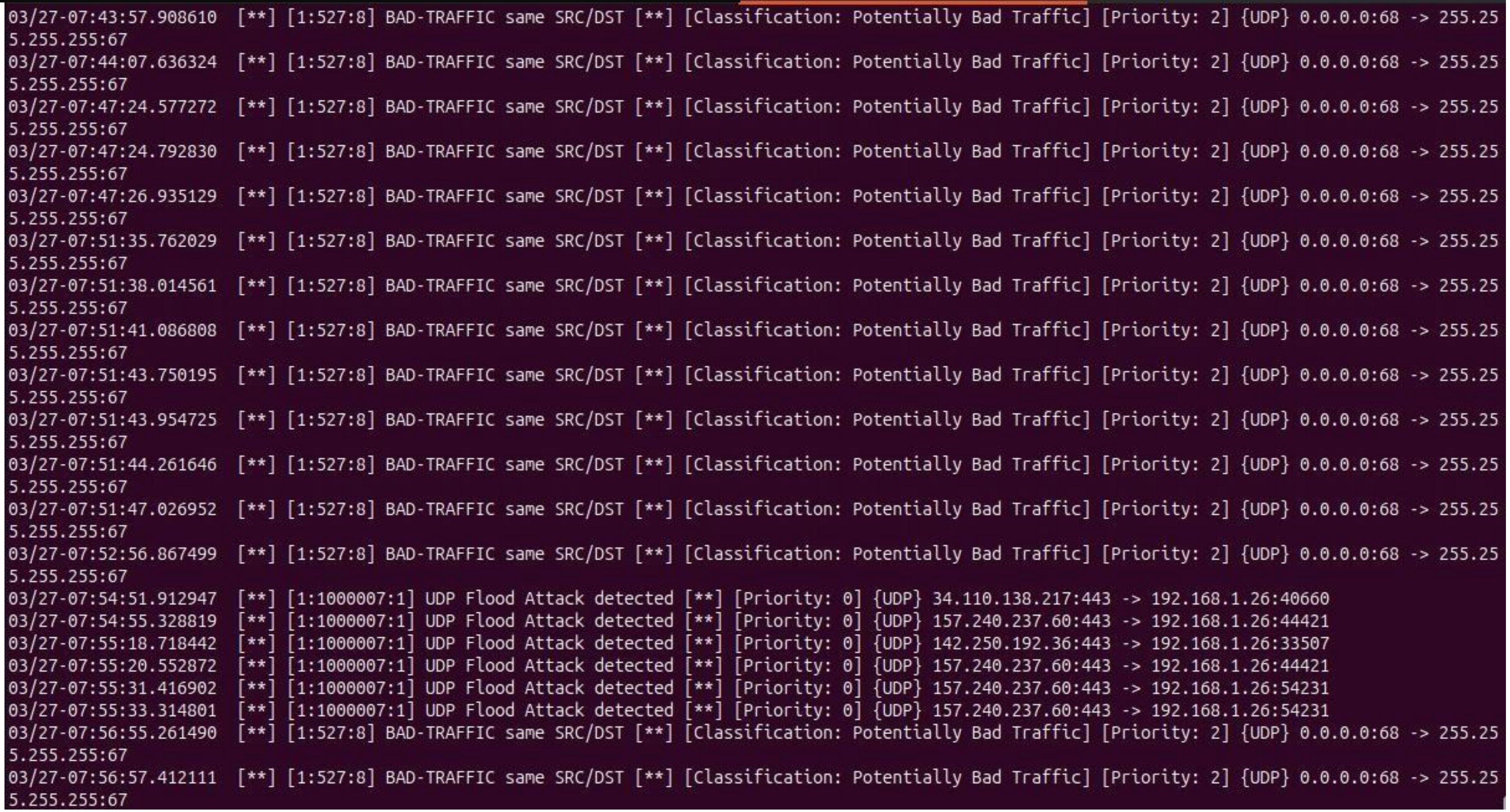


```
  GNU nano 7.2                                        /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES


alert icmp any any -> 192.168.1.26 any (msg:"ICMP Ping Request detected"; sid:1000001; rev:1;)

alert tcp any any -> 192.168.1.26 any (flags:FPU; msg:"XMAS Scan detected"; sid:1000002; rev:1;)

alert tcp any any -> 192.168.1.26 any (flags:0; msg:"NULL Scan detected"; sid:1000003; rev:1;)


alert tcp any any -> 192.168.1.26 any (flags:F; msg:"FIN Scan detected"; sid:1000004; rev:1;)

alert tcp any any -> 192.168.1.26 any (flags:S; msg:"SYN Scan detected"; sid:1000005; rev:1;)

alert tcp any any -> 192.168.1.26 any (flags:S; threshold:type both, track by_dst, count 20, seconds 3; msg:"SYN Flood Attack detected"; sid:1000006;>

alert udp any any -> 192.168.1.26 any (threshold:type both, track by_dst, count 50, seconds 3; msg:"UDP Flood Attack detected"; sid:1000007; rev:1;)

alert icmp any any -> 192.168.1.26 any (threshold:type both, track by_dst, count 50, seconds 3; msg:"ICMP Flood Attack detected"; sid:1000008; rev:1;)




# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
```

Run Snort to monitor traffic in console mode: **snort -q –A CONSOLE –c /etc/snort/snort.conf -i (ip_interface)** In a Windows command prompt, ping the IP address of your Ubuntu VM to trigger ICMP traffic .



```
C:\Users\ADMIN>ping ubuntu_ipaddress
```



```
03/27-07:43:57.908610  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:44:07.636324  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:47:24.577272  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:47:24.792830  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:47:26.935129  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:51:35.762029  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:51:38.014561  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:51:41.086808  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:51:43.750195  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:51:43.954725  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:51:44.261646  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:51:47.026952  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:52:56.867499  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:54:51.912947  [**] [1:1000007:1] UDP Flood Attack detected [**] [Priority: 0] {UDP} 34.110.138.217:443 -> 192.168.1.26:40660
03/27-07:54:55.328819  [**] [1:1000007:1] UDP Flood Attack detected [**] [Priority: 0] {UDP} 157.240.237.60:443 -> 192.168.1.26:44421
03/27-07:55:18.718442  [**] [1:1000007:1] UDP Flood Attack detected [**] [Priority: 0] {UDP} 142.250.192.36:443 -> 192.168.1.26:33507
03/27-07:55:20.552872  [**] [1:1000007:1] UDP Flood Attack detected [**] [Priority: 0] {UDP} 157.240.237.60:443 -> 192.168.1.26:44421
03/27-07:55:31.416902  [**] [1:1000007:1] UDP Flood Attack detected [**] [Priority: 0] {UDP} 157.240.237.60:443 -> 192.168.1.26:54231
03/27-07:55:33.314801  [**] [1:1000007:1] UDP Flood Attack detected [**] [Priority: 0] {UDP} 157.240.237.60:443 -> 192.168.1.26:54231
03/27-07:56:55.261490  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
03/27-07:56:57.412111  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.25
5.255.255:67
```