



CS 3339 Cyber Security Lab

Lab 6: Firewall & Intrusion Detection Systems

Introduction

In this lab students will explore the Snort Intrusion Detection Systems. The students will study Snort IDS, a signature based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger. For the purpose of this lab the students will use snort as a packet sniffer and write their own IDS rules.

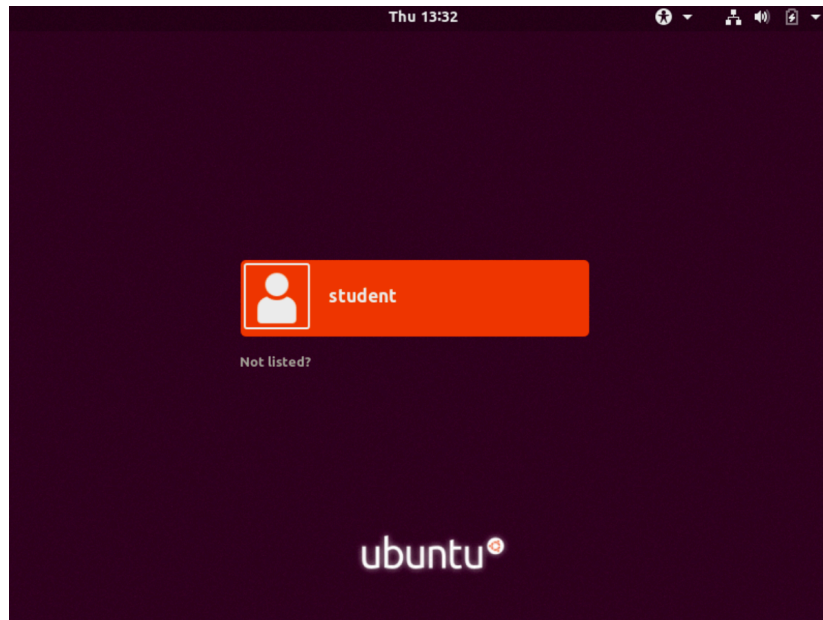
Software Requirements

All required files are packed and configured in the provided virtual machine image.

- VirtualBox
<https://www.virtualbox.org/wiki/Downloads>
- The Ubuntu 18.04 Long Term Support (LTS) Version
<https://s2.smu.edu/~rtumac/cs3339/spring2020/Lab6/>
<https://ubuntu.com/download/desktop>
- Snort: A signature-based Intrusion Detection System
<https://www.snort.org/#get-started>

Starting the Lab 9 Virtual Machine

In this lab, we use Ubuntu as our VM image. Select the VM named Ubuntu CS3339.



Login the Ubuntu image with username student, and password CS3339ubnt. Below is the screen snapshot after login.



Installing Snort into the Operating System

In our Lab 6 Ubuntu VM image, the snort has been installed and setup for you. If you want to use your own version of the image, you need to install snort into the operating system. To install the latest version of the snort, you can follow the installation instruction from the snort website. Note that installation instructions are vary from OSes. The instruction below shows how to install snort from its source code on Linux.

Find the appropriate package for your operating system and install.

Source Fedora Centos FreeBSD Windows

```
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz  
wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
```

```
tar xvzf daq-2.0.6.tar.gz  
  
cd daq-2.0.6  
./configure && make && sudo make install
```

```
tar xvzf snort-2.9.15.tar.gz  
  
cd snort-2.9.15  
./configure --enable-sourcefire && make && sudo make install
```

You can find more information here:

<https://www.snort.org/#get-started>

While you install the snort, your system may miss some libraries. You need to install the required libraries, too.

Configuring and Starting the Snort IDS

After installing the Snort, we need to configure it. The configuration file of snort is stored at `/etc/snort/snort.conf`. The screenshot below shows the commands to configure the Snort. You need to switch to root to gain the permission to read the snort configurations file.

```
root@student-VirtualBox: /home/student

File Edit View Search Terminal Help
student@student-VirtualBox:~$ sudo su
[sudo] password for student:
root@student-VirtualBox:/home/student# vim /etc/snort/snort.conf
```

After configuring the Snort, you need to start the Snort. You can simply type the following command to start the service.

```
$ snort -c /etc/snort/snort.conf -l /var/log/snort/
```

```
root@student-VirtualBox: /home/student

File Edit View Search Terminal Help
root@student-VirtualBox:/home/student# snort -c /etc/snort/snort.conf -l /var/log/snort/
Running in IDS mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort/

+++++
Initializing rule chains...
0 Snort rules read
  0 detection rules
  0 decoder rules
  0 preprocessor rules
0 Option Chains linked into 0 Chain Headers
+++++

+-----[Rule Port Counts]-----+
|      tcp      udp      icmp      ip      |
|  src      0      0      0      0      |
|  dst      0      0      0      0      |
|  any      0      0      0      0      |
|  nc       0      0      0      0      |
|  s+d      0      0      0      0      |
+-----+

+-----[detection-filter-config]-----+
| memory-cap : 1048576 bytes |
+-----[detection-filter-rules]-----+
| none |
+-----+

+-----[rate-filter-config]-----+
| memory-cap : 1048576 bytes |
+-----[rate-filter-rules]-----+
| none |
+-----+
```

Snort Rules

Snort is a signature-based IDS, and it defines rules to detect the intrusions. All rules of Snort are stored under `/etc/snort/rules` directory. The screenshot below shows the files that contain rules of Snort.

```
root@student-VirtualBox: /home/student
File Edit View Search Terminal Help
root@student-VirtualBox:/home/student# ls /etc/snort/rules/
community.rules  local.rules  web-misc.rules
root@student-VirtualBox:/home/student#
```

The screenshot below shows a rule in the `/etc/snort/rules/web-misc.rules`

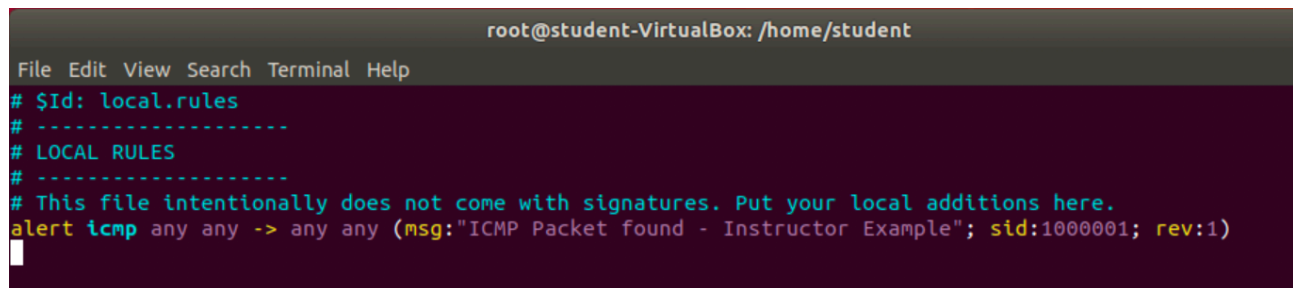
```
# NOTES: this signature looks for someone accessing the file "active.log" via
# a web server. By allowing anyone on the internet to view the web access
# logs, attackers can gain information about your customers that probably
# should not be made public.
#
# This logfile is made available from the WebActive webserver. This webserver
# is no longer maintained and should be replaced with an actively maintained
# webserver. If converting to another webserver is not possible, remove read
# access to this file.
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC active.log access"; flow:to_s
erver,established; uricontent: "/active.log"; nocase; reference:bugtraq,1497; reference:cve,2000-0642;
reference:nessus,10470; classtype:web-application-activity; sid:1851; rev:6;)
```

Writing and Adding a Snort Rule

Next, we are going to add a simple snort rule. You should add your own rules at /etc/snort/rules/local.rules. Add the following line into the local.rules file

alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)

Basically, this rule defines that an alert will be logged if an ICMP packet is found. The ICMP packet could be from any IP address and the rule ID is 1000001. Make sure to pick a SID greater 1000000 for your own rules. The screenshot below shows the contents of the local.rules file after adding the rule.



```
root@student-VirtualBox: /home/student
File Edit View Search Terminal Help
# $Id: local.rules
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local additions here.
alert icmp any any -> any any (msg:"ICMP Packet found - Instructor Example"; sid:1000001; rev:1)
```

To make the rule become effective, you need to restart the snort service. To accomplish this you can run the following two commands to stop and restart snort respectively.

```
$ kill -9 $(pidof snort)
```

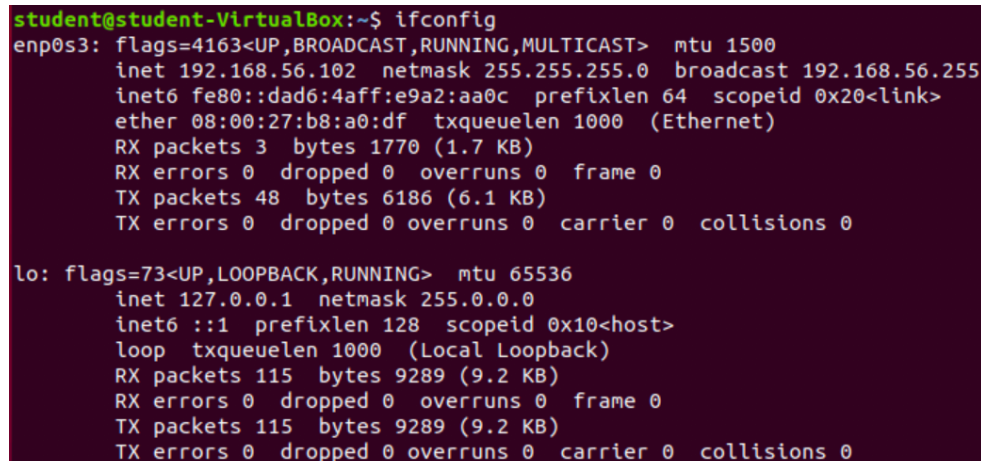
```
$ snort -c /etc/snort/snort.conf -l /var/log/snort/
```

Triggering an Alert for the New Rule

To trigger an alert for the new rule, you only need to send an ICMP message to the VM image where snort runs. First, you need to find the IP address of the VM by typing the following command.

```
$ ifconfig
```

For instance, the screenshot shows the execution result on my VM image, and the IP address is 192.168.56.102



```
student@student-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
    inet6 fe80::dad6:4aff:e9a2:aa0c  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:b8:a0:df  txqueuelen 1000  (Ethernet)
    RX packets 3  bytes 1770 (1.7 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 48  bytes 6186 (6.1 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 115  bytes 9289 (9.2 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 115  bytes 9289 (9.2 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Next, you can open a terminal in your host. If you host is a Windows OS, you can use one of the following two ways to open a terminal

1. Press "Win-R," type "cmd" and press "Enter" to open a Command Prompt session using just your keyboard.
2. Click the "Start | Program Files | Accessories | Command Prompt" to open a Command Prompt session using just your mouse.

After you have a terminal, you can just type the following command to send ping messages to the VM.

```
$ ping 192.168.56.102
```

After you send the ping messages, the alerts should be triggered, and you can find the log messages in `/var/log/snort/alert`. The screenshot below shows the result of reading the snort alerts.

```
student@student-VirtualBox: ~  
File Edit View Search Terminal Help  
student@student-VirtualBox:~$ cat /var/log/snort/alert  
[**] [1:1000001:1] ICMP Packet found - Instructor Example [**]  
[Priority: 0]  
11/14-12:02:52.537690 192.168.56.1 -> 192.168.56.102  
ICMP TTL:64 TOS:0x0 ID:10389 IpLen:20 DgmLen:84  
Type:8 Code:0 ID:4633 Seq:0 ECHO  
  
[**] [1:1000001:1] ICMP Packet found - Instructor Example [**]  
[Priority: 0]  
11/14-12:02:52.537705 192.168.56.102 -> 192.168.56.1  
ICMP TTL:64 TOS:0x0 ID:45546 IpLen:20 DgmLen:84  
Type:0 Code:0 ID:4633 Seq:0 ECHO REPLY  
  
[**] [1:1000001:1] ICMP Packet found - Instructor Example [**]  
[Priority: 0]  
11/14-12:02:53.542892 192.168.56.1 -> 192.168.56.102  
ICMP TTL:64 TOS:0x0 ID:46416 IpLen:20 DgmLen:84  
Type:8 Code:0 ID:4633 Seq:1 ECHO  
  
[**] [1:1000001:1] ICMP Packet found - Instructor Example [**]  
[Priority: 0]  
11/14-12:02:53.542935 192.168.56.102 -> 192.168.56.1  
ICMP TTL:64 TOS:0x0 ID:45639 IpLen:20 DgmLen:84  
Type:0 Code:0 ID:4633 Seq:1 ECHO REPLY  
  
[**] [1:1000001:1] ICMP Packet found - Instructor Example [**]  
[Priority: 0]  
11/14-12:02:54.546332 192.168.56.1 -> 192.168.56.102  
ICMP TTL:64 TOS:0x0 ID:26363 IpLen:20 DgmLen:84  
Type:8 Code:0 ID:4633 Seq:2 ECHO
```

You can see that the SID is 1000001, and the alerts are generated by the ICMP messages.

Assignments for Lab 6

1. Read the lab instructions above and finish all the tasks.
2. Answer the following questions and justify your answers. Simple yes or no answer will not get any credits.
 - a. What is a zero-day attack?
 - b. Can Snort catch zero-day network attacks? If not, why not? If yes, how?
3. Write and add another snort rule and show me you trigger it.
 - a. The rule you added (from the rules file)
 - b. A description of how you triggered the alert
 - c. The alert itself from the log file

Happy Hacking!