Objectives

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 Reequirment

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

-The VMWare Software - http://apps.eng.wayne.edu/MPStudents/Dreamspark.aspx

- The ubantu 14.04 or Ubantu Long Term Support (LTS) versionor Kali linux image
- The ubantu 14.04 or Ubuntu 14.04 Long Term Support (LTS) Version
- Snort: A signature-based Intrusion Detection System https://www.snort.org/#get-started

Implementation

Starting the Lab 1 Virtual Machine

In this lab, we use Ubuntu as our VM image.

Login the Ubuntu image with username and password

Installing 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.

You can find more information here:

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

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

Snort is software created by Martin Roesch, which is widely used as Intrusion Prevention System [IPS] and Intrusion Detection System [IDS] in the network. It is separated into the five most important mechanisms for instance: Detection engine, Logging, and alerting system, a Packet decoder, Preprocessor, and Output modules.

The program is quite famous to carry out real-time traffic analysis, also used to detect query or attacks, packet logging on Internet Protocol networks, to detect malicious activity, denial of service attacks and port scans by monitoring network traffic, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes:

Sniffer mode: it will observe network packets and present them on the console.

Packet logger mode: it will record packets to the disk.

Intrusion detection mode: the program will monitor network traffic and analyze it against a rule set defined by the user.

After that, the application will execute a precise action depend upon what has been identified.

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.

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

```
$ service snort start
```

or

```
$ /etc/init.d/


snort start
```

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.

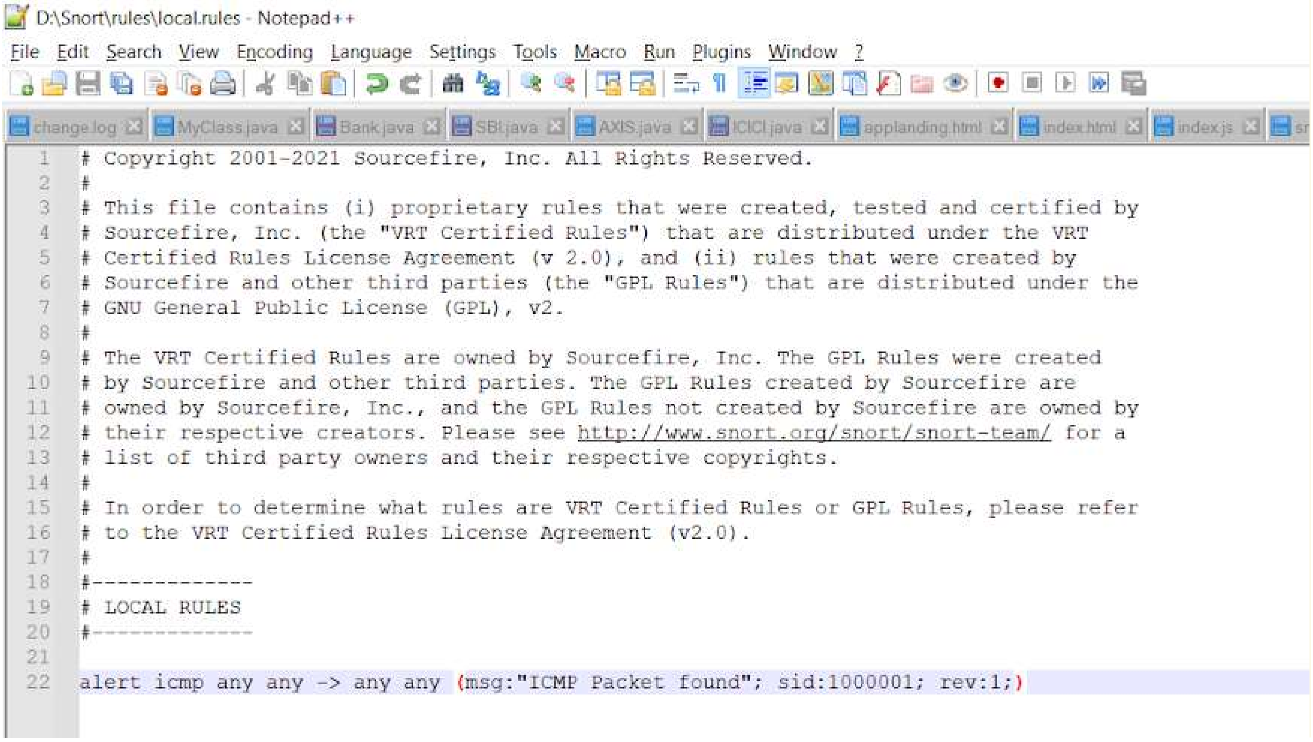
```
$ ls /etc/snort/rules
```

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. e.g. Make sure to pick a SID greater 1000000 for your own rules.


D:\Snort\rules\local.rules - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
MyClass.java
Bank.java
SBI.java
AXIS.java
ICICI.java
applanding.html
index.html
index.js

```
# Copyright 2001-2021 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------

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

To make the rule become effective, you need to restart the snort service by typing the following command.

```
$ service snort restart
```

or

```
$ /etc/init.d/snort restart
```

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.

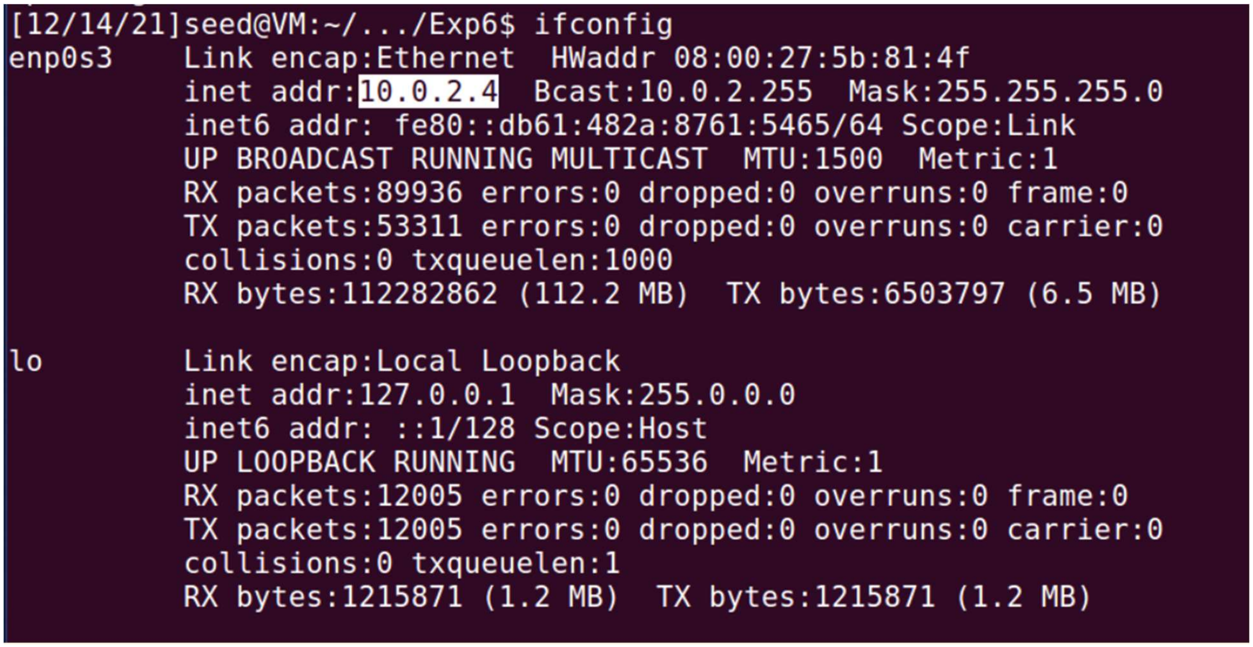
$ ifconfig

For instance, the screenshot shows the execution result on my VM image, and the IP address is e.g. 172.16.108.242

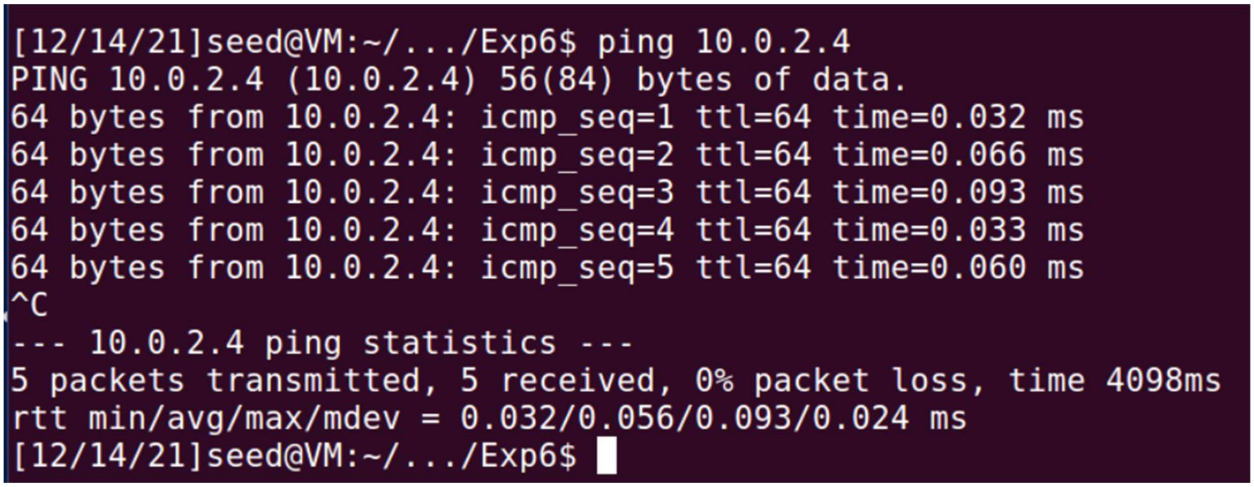
After you have a terminal, you can just type the following command to send ping messages to the VM.

$ ping 172.16.108.242

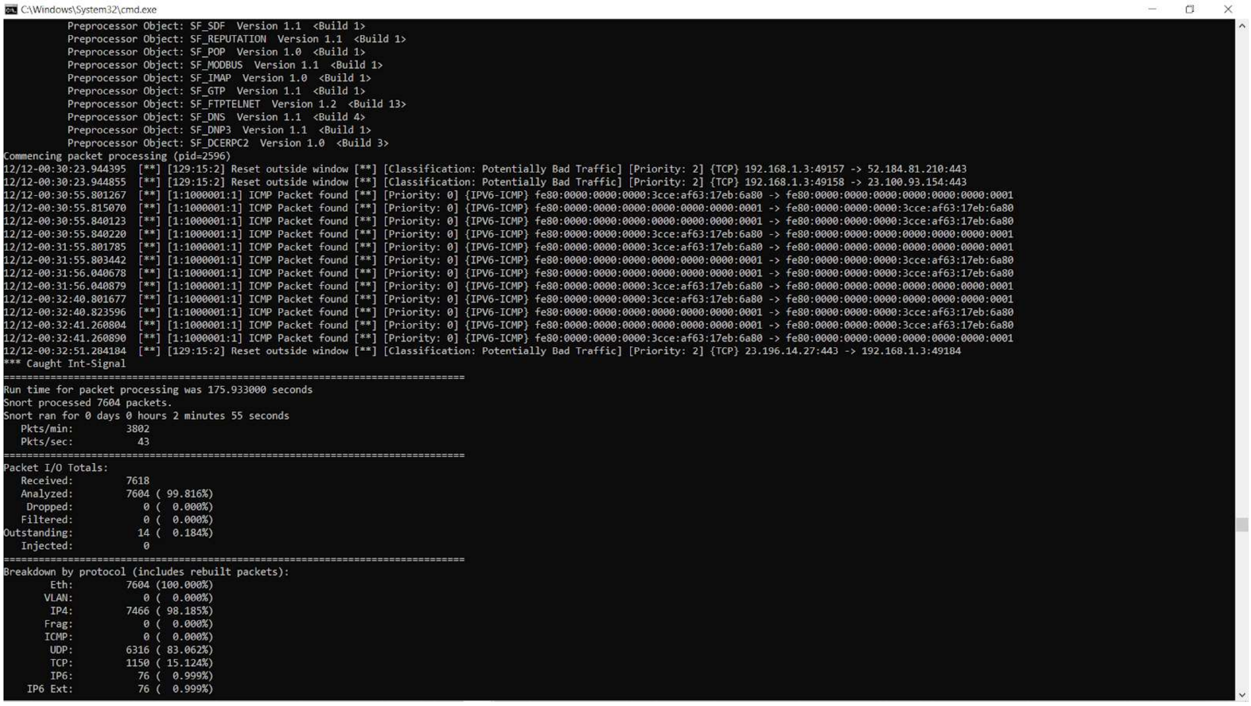
After you send the ping messages, the alerts should be triggered and you can find the log messages in /var/log/snort/snort.log. However, the snort.log file will be binary format. You need to use a tool, called u2spewfoo, to read it. Observer terminal on screen with log where you can see that the SID is 1000001, and the alerts are generated by the ICMP messages.



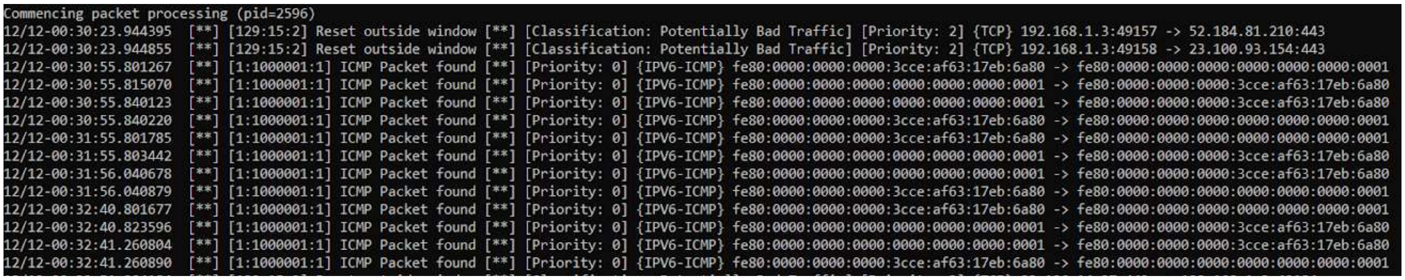
```
[12/14/21]seed@VM:~/.../Exp6$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:5b:81:4f
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::db61:482a:8761:5465/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:89936 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112282862 (112.2 MB)  TX bytes:6503797 (6.5 MB)

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:12005 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12005 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1215871 (1.2 MB)  TX bytes:1215871 (1.2 MB)
```



```
[12/14/21]seed@VM:~/.../Exp6$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.066 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.093 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.033 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.060 ms
^C
--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4098ms
rtt min/avg/max/mdev = 0.032/0.056/0.093/0.024 ms
[12/14/21]seed@VM:~/.../Exp6$ 
```



```
         Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
         Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
         Preprocessor Object: SF_POP  Version 1.0  <Build 1>
         Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
         Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
         Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
         Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
         Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
         Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
         Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=2596)
12/12-00:30:23.944395  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.3:49157 -> 52.184.81.210:443
12/12-00:30:23.944855  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.3:49158 -> 23.100.93.154:443
12/12-00:30:55.801267  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:30:55.815070  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:30:55.840123  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:30:55.840220  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:31:55.801785  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:31:55.803442  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:31:56.040678  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:31:56.040879  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:32:40.801677  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:32:40.823596  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:32:41.260804  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:32:41.260890  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:32:51.284184  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 23.196.14.27:443 -> 192.168.1.3:49184
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 175.933000 seconds
Snort processed 7604 packets.
Snort ran for 0 days 0 hours 2 minutes 55 seconds
   Pkts/min:         3802
   Pkts/sec:           43
===============================================================================
Packet I/O Totals:
   Received:         7618
   Analyzed:         7604 ( 99.816%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:           14 (  0.184%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         7604 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         7466 ( 98.185%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:         6316 ( 83.062%)
        TCP:         1150 ( 15.124%)
        IP6:           76 (  0.999%)
    IP6 Ext:           76 (  0.999%)
```



```
Commencing packet processing (pid=2596)
12/12-00:30:23.944395  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.3:49157 -> 52.184.81.210:443
12/12-00:30:23.944855  [**] [129:15:2] Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.3:49158 -> 23.100.93.154:443
12/12-00:30:55.801267  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:30:55.815070  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:30:55.840123  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:30:55.840220  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:31:55.801785  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:31:55.803442  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:31:56.040678  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:31:56.040879  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:32:40.801677  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:32:40.823596  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:32:41.260804  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:32:41.260890  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
```

Assignments for Lab 1

1.Read the lab instructions above and finish all the tasks.

2.Answer the questions and justify your answers. Simple yes or no answer will not get any credits.

a. What is a zero-day attack?

A zero-day attack is the use of a zero-day exploit to cause damage to or steal data from a system affected by a vulnerability. A zero-day exploit is the method hackers use to attack systems with a previously unidentified vulnerability. A zero-day vulnerability is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed. Zero day vulnerabilities can be missing authorizations, URL redirects, bugs or password security.

b. Can Snort catch zero-day network attacks? If not, why not? If yes, how?

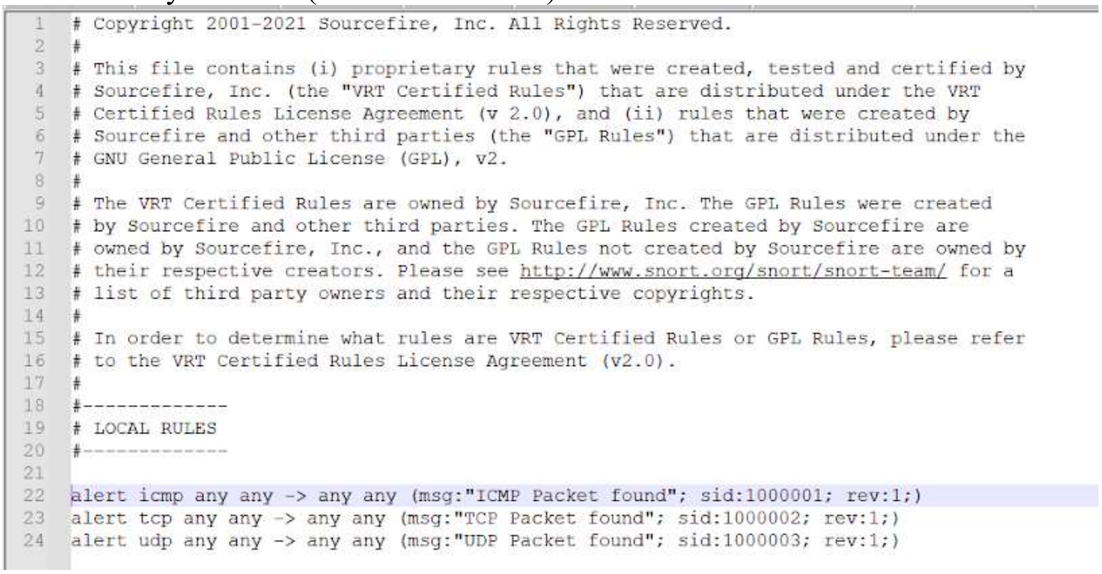
No snort cannot catch zero day network attacks because snort uses a set of predefined rules for prevention of attack but in the case of zero day attacks the vulnerabilities are unknown to the developers so these cannot be prevented.

c. Given a network that has 1 million connections daily where 0.1% (not 10%) are attacks. If the IDS has a true positive rate of 95%,and the probability that an alarm is an attack is 95%. What is the false alarm rate?

Number of attacks on network = 0.1% of 1000000 = 1000 attacks.
Remaining = 99.9% = 999000 events
IDS has a true positive rate of 95% so out of 1000, 950 will set alarms.
Number of alarms = 950.
Number of total alarms = (100*950)/95 = 1000 alarms.
Number of false alarms = 50 alarms.
False Alarm Rate = (Number of false alarms / Total Events) * 100 = (50 / 999000) * 100 =
0.005%

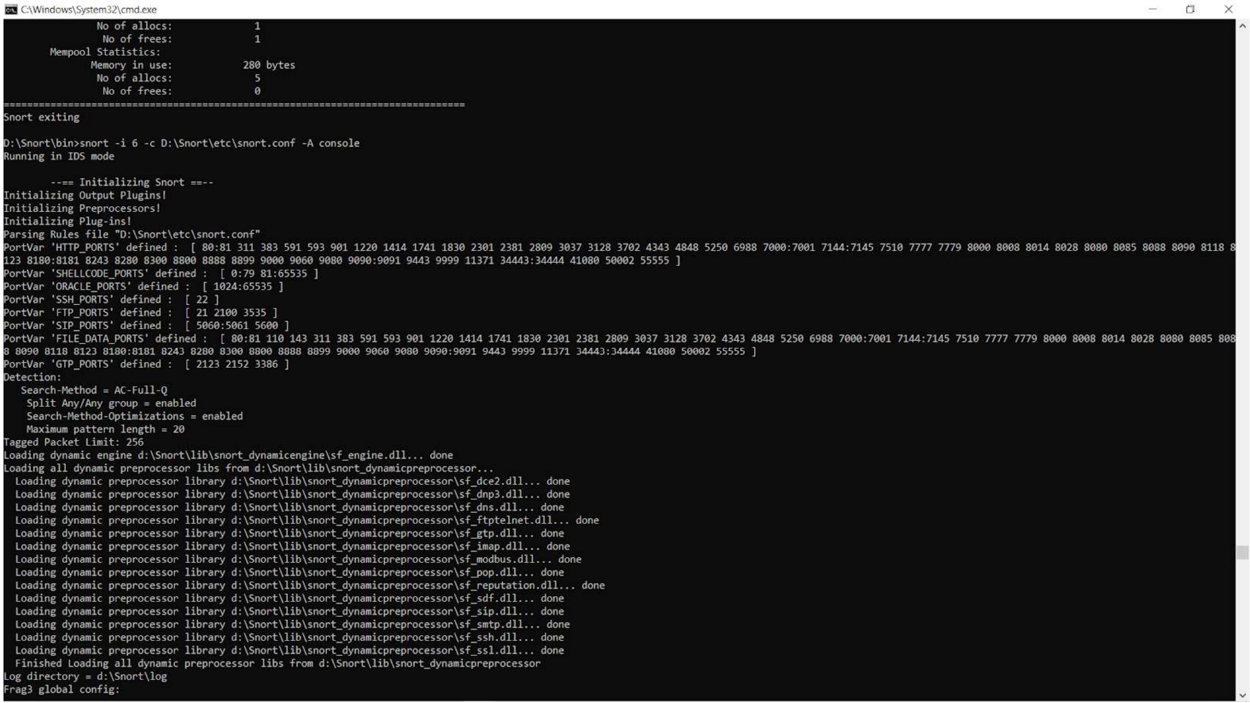
3. Write and add another snort rule and show me you trigger it.

a. The rule you added (from the rules file)

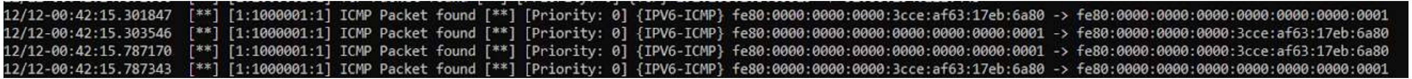


```
# Copyright 2001-2021 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------

alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
alert tcp any any -> any any (msg:"TCP Packet found"; sid:1000002; rev:1;)
alert udp any any -> any any (msg:"UDP Packet found"; sid:1000003; rev:1;)
```

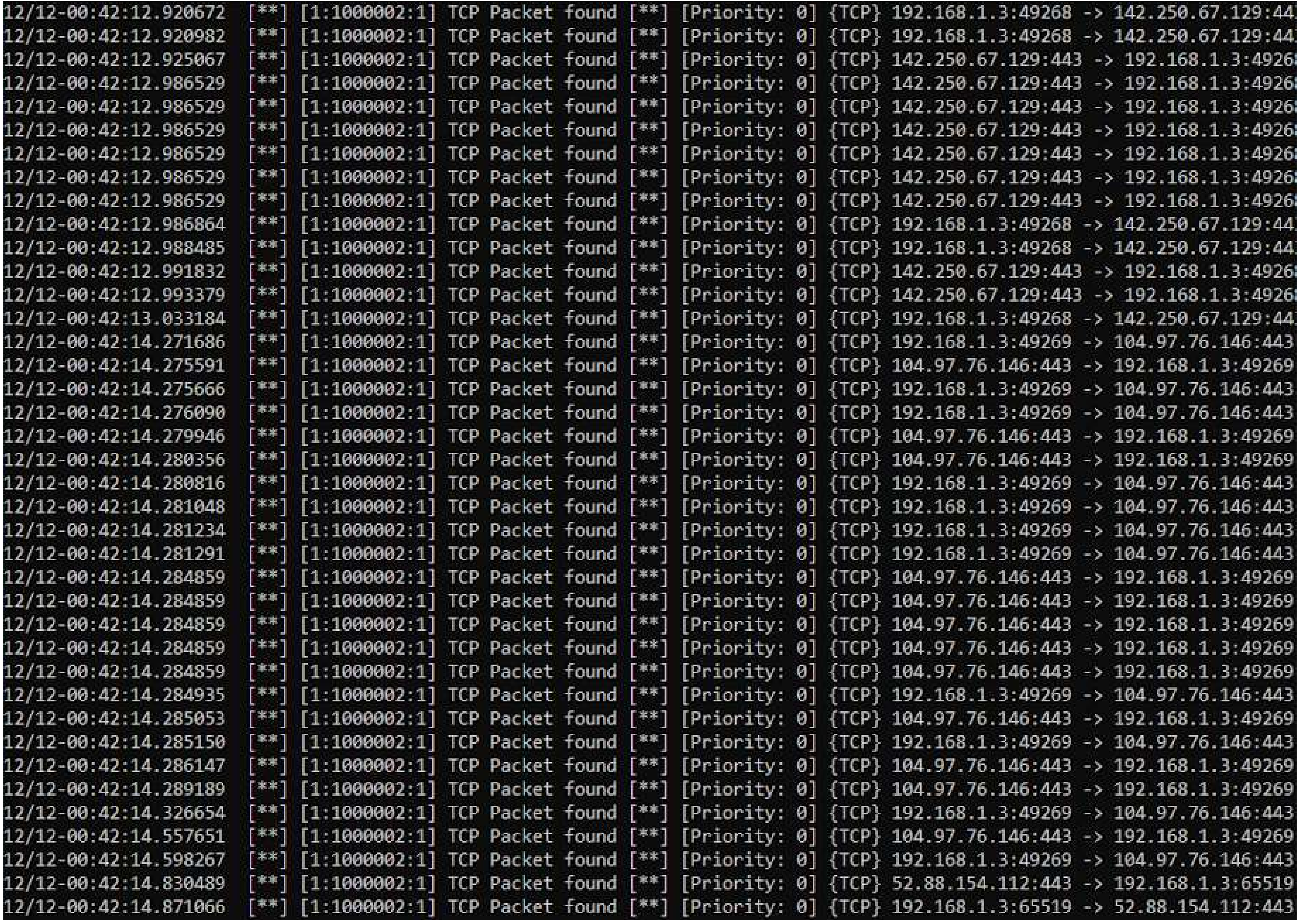
b. A description of how you triggered the alert. The alert itself from the log file (after converting it to readable text)



```
C:\Windows\System32\cmd.exe
              No of allocs:             1
               No of frees:             1
        Mempool Statistics:
             Memory in use:           280 bytes
              No of allocs:             5
               No of frees:             0
===============================================================================
Snort exiting

D:\Snort\bin>snort -i 6 -c D:\Snort\etc\snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "D:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8
123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine d:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from d:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library d:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from d:\Snort\lib\snort_dynamicpreprocessor
Log directory = d:\Snort\log
Frag3 global config:
```

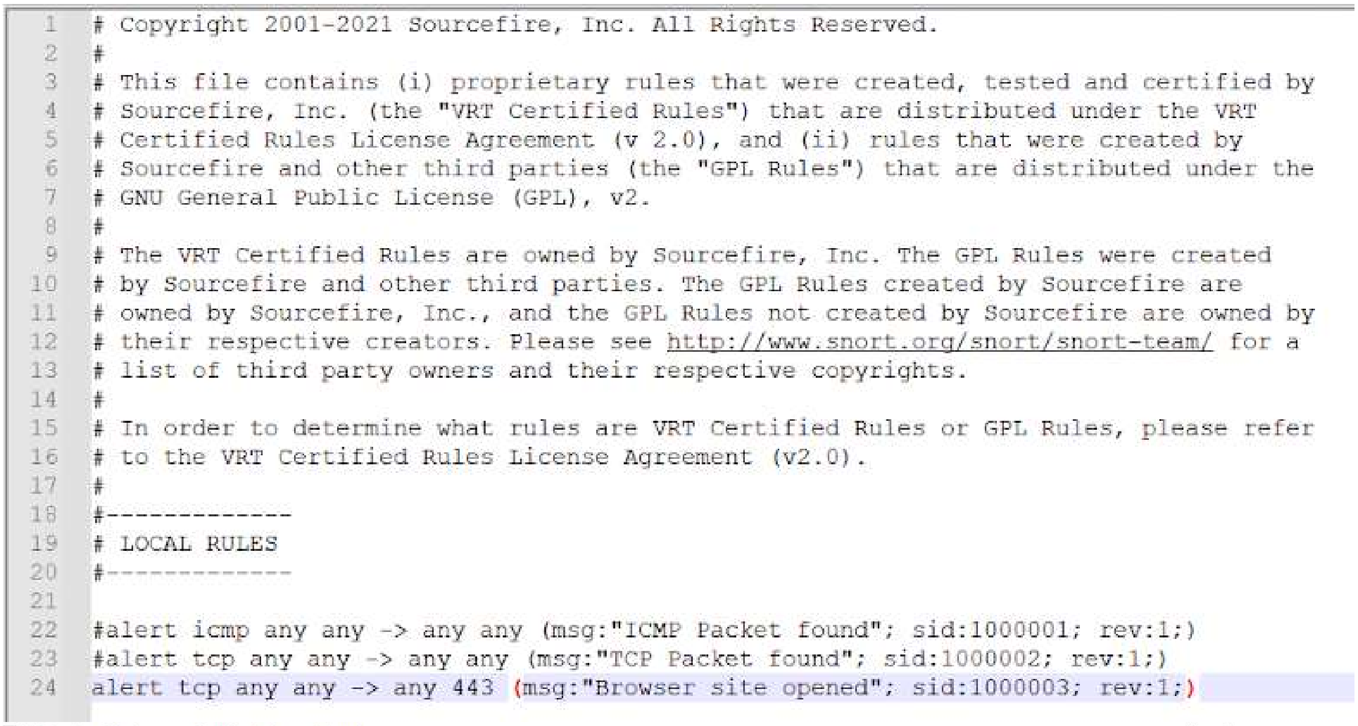


```
12/12-00:42:15.301847  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
12/12-00:42:15.303546  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:42:15.787170  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:0000:0000:0000:0001 -> fe80:0000:0000:0000:3cce:af63:17eb:6a80
12/12-00:42:15.787343  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:3cce:af63:17eb:6a80 -> fe80:0000:0000:0000:0000:0000:0000:0001
```

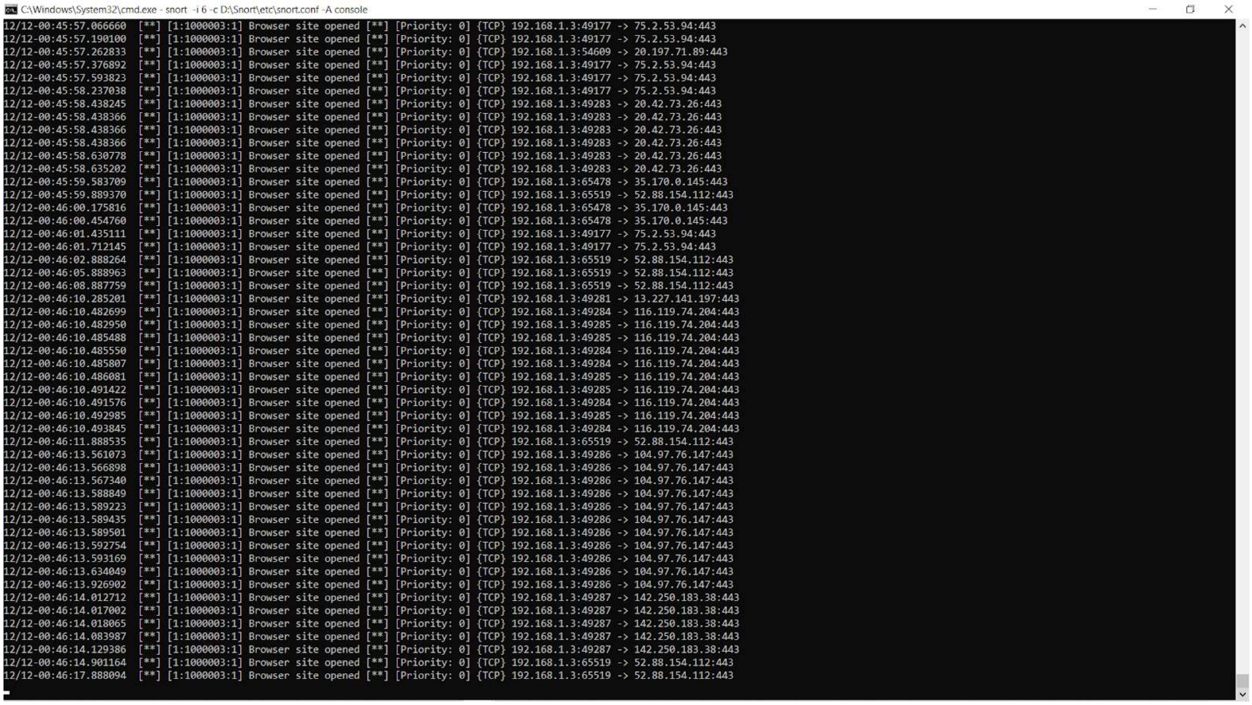


```
12/12-00:42:12.920672  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49268 -> 142.250.67.129:44
12/12-00:42:12.920982  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49268 -> 142.250.67.129:44
12/12-00:42:12.925067  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.986529  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.986529  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.986529  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.986529  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.986529  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.986529  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.986864  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49268 -> 142.250.67.129:44
12/12-00:42:12.988485  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49268 -> 142.250.67.129:44
12/12-00:42:12.991832  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:12.993379  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 142.250.67.129:443 -> 192.168.1.3:4926
12/12-00:42:13.033184  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49268 -> 142.250.67.129:44
12/12-00:42:14.271686  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.275591  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.275666  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.276090  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.279946  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.280356  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.280816  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.281048  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.281234  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.281291  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.284859  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.284859  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.284859  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.284859  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.284859  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.284935  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.285053  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.285150  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.286147  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.289189  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.326654  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.557651  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 104.97.76.146:443 -> 192.168.1.3:49269
12/12-00:42:14.598267  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:49269 -> 104.97.76.146:443
12/12-00:42:14.830489  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 52.88.154.112:443 -> 192.168.1.3:65519
12/12-00:42:14.871066  [**] [1:1000002:1] TCP Packet found [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
```

Extra Credit (10pt):Write a rule that will fire when you browse to any site from the machine Snort is running on; it should look for any outbound TCP request to the site you have considered and alert on it.



```
# Copyright 2001-2021 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------

#alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
#alert tcp any any -> any any (msg:"TCP Packet found"; sid:1000002; rev:1;)
alert tcp any any -> any 443 (msg:"Browser site opened"; sid:1000003; rev:1;)
```



C:\Windows\System32\cmd.exe - snort -i 6 -c D:\Snort\etc\snort.conf -A console

```
12/12-00:45:57.066660  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49177 -> 75.2.53.94:443
12/12-00:45:57.190100  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49177 -> 75.2.53.94:443
12/12-00:45:57.262833  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:54609 -> 20.197.71.89:443
12/12-00:45:57.376892  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49177 -> 75.2.53.94:443
12/12-00:45:57.593823  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49177 -> 75.2.53.94:443
12/12-00:45:58.237038  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49177 -> 75.2.53.94:443
12/12-00:45:58.438245  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49283 -> 20.42.73.26:443
12/12-00:45:58.438366  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49283 -> 20.42.73.26:443
12/12-00:45:58.438366  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49283 -> 20.42.73.26:443
12/12-00:45:58.438366  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49283 -> 20.42.73.26:443
12/12-00:45:58.630778  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49283 -> 20.42.73.26:443
12/12-00:45:58.635202  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49283 -> 20.42.73.26:443
12/12-00:45:59.583709  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65478 -> 35.170.0.145:443
12/12-00:45:59.889370  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
12/12-00:46:00.175816  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65478 -> 35.170.0.145:443
12/12-00:46:00.454760  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65478 -> 35.170.0.145:443
12/12-00:46:01.435111  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49177 -> 75.2.53.94:443
12/12-00:46:01.712145  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49177 -> 75.2.53.94:443
12/12-00:46:02.888264  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
12/12-00:46:05.888963  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
12/12-00:46:08.887759  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
12/12-00:46:10.285201  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49281 -> 13.227.141.197:443
12/12-00:46:10.482699  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49284 -> 116.119.74.204:443
12/12-00:46:10.482950  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49285 -> 116.119.74.204:443
12/12-00:46:10.485488  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49285 -> 116.119.74.204:443
12/12-00:46:10.485550  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49284 -> 116.119.74.204:443
12/12-00:46:10.485807  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49284 -> 116.119.74.204:443
12/12-00:46:10.486081  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49285 -> 116.119.74.204:443
12/12-00:46:10.491422  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49285 -> 116.119.74.204:443
12/12-00:46:10.491576  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49284 -> 116.119.74.204:443
12/12-00:46:10.492985  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49285 -> 116.119.74.204:443
12/12-00:46:10.493845  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49284 -> 116.119.74.204:443
12/12-00:46:11.888535  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
12/12-00:46:13.561073  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.566898  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.567340  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.588849  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.589223  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.589435  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.589501  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.592754  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.593169  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.634049  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:13.926902  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49286 -> 104.97.76.147:443
12/12-00:46:14.012712  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49287 -> 142.250.183.38:443
12/12-00:46:14.017002  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49287 -> 142.250.183.38:443
12/12-00:46:14.018065  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49287 -> 142.250.183.38:443
12/12-00:46:14.083987  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49287 -> 142.250.183.38:443
12/12-00:46:14.129386  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:49287 -> 142.250.183.38:443
12/12-00:46:14.901164  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
12/12-00:46:17.888094  [**] [1:1000003:1] Browser site opened [**] [Priority: 0] {TCP} 192.168.1.3:65519 -> 52.88.154.112:443
```

Conclusion:

1. Snort is used to analyze the incoming traffic and prevent any know attacks using predefined rules.
2. It uses source and destination IP address, ports and displays a message that needs to be printed if a packet matches with the predefined rule.
3. Snort cannot be used to prevent zero day attacks.