Abhishek Chopra | Lab 6: Firewall & Intrusion Detection System | 2019130009 | TE COMPS

# 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

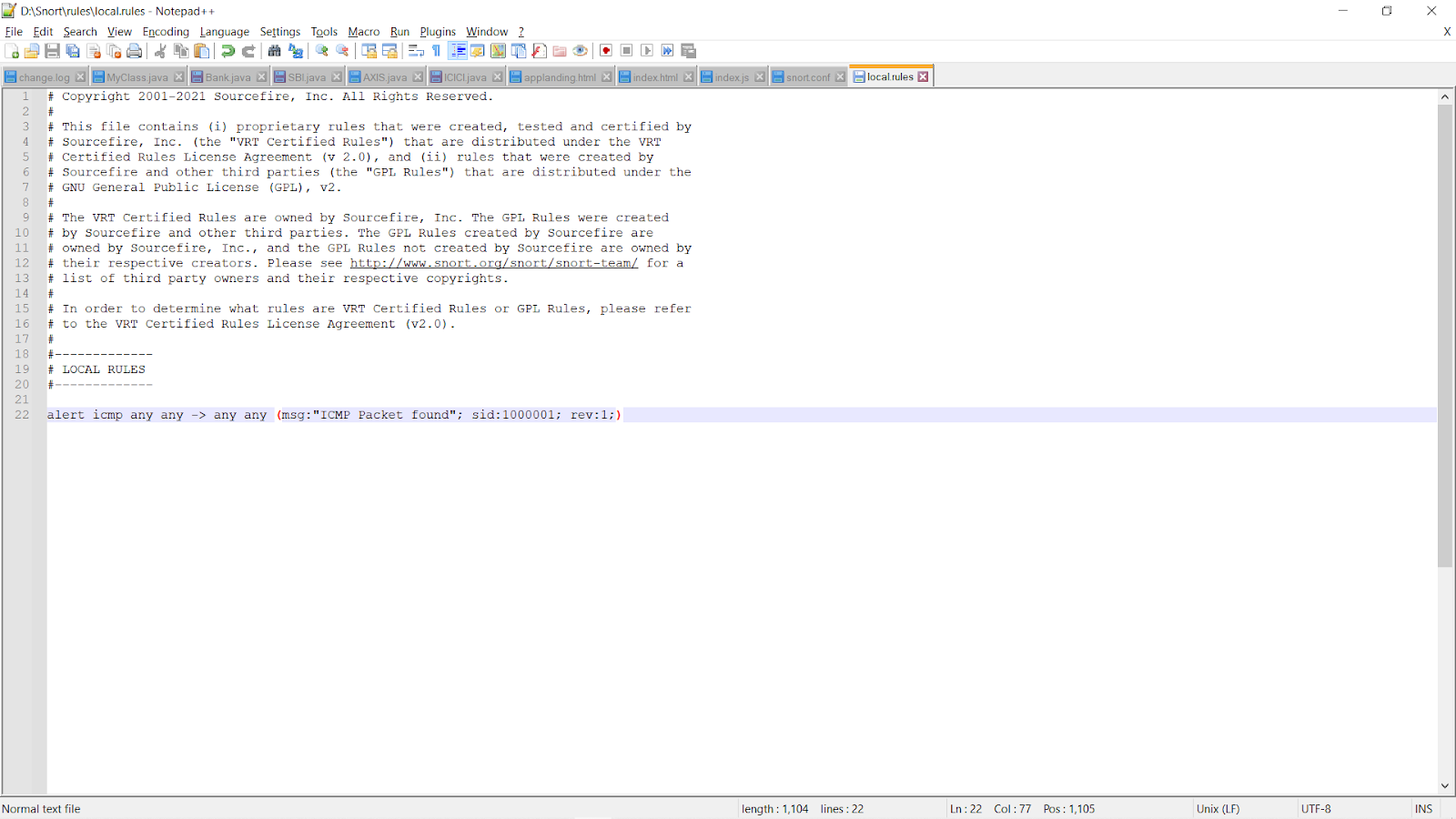
# Writing and Adding a Snort Rule

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.



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.

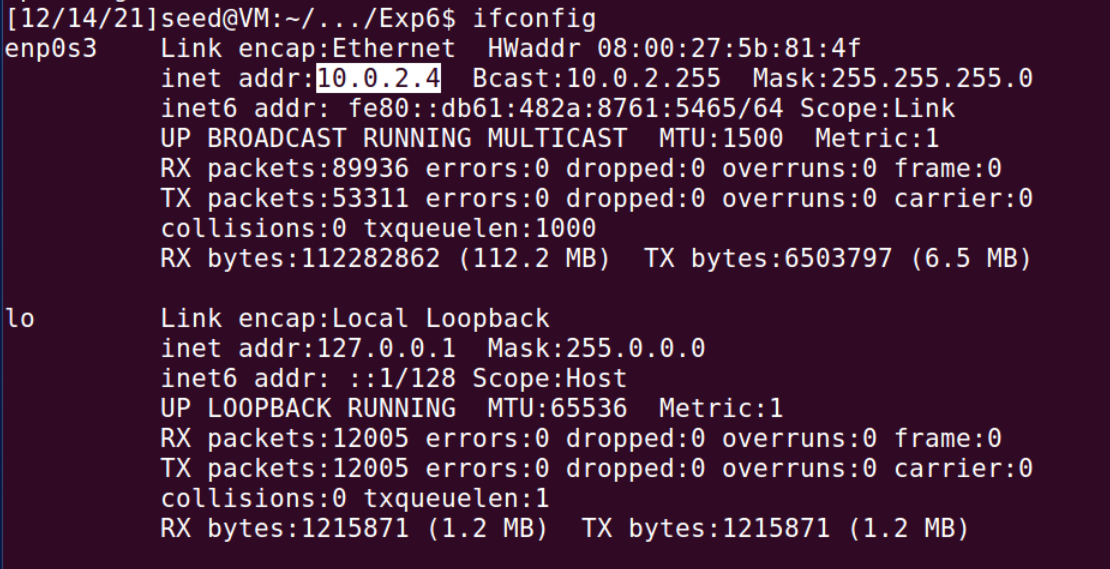
$ ifconfig

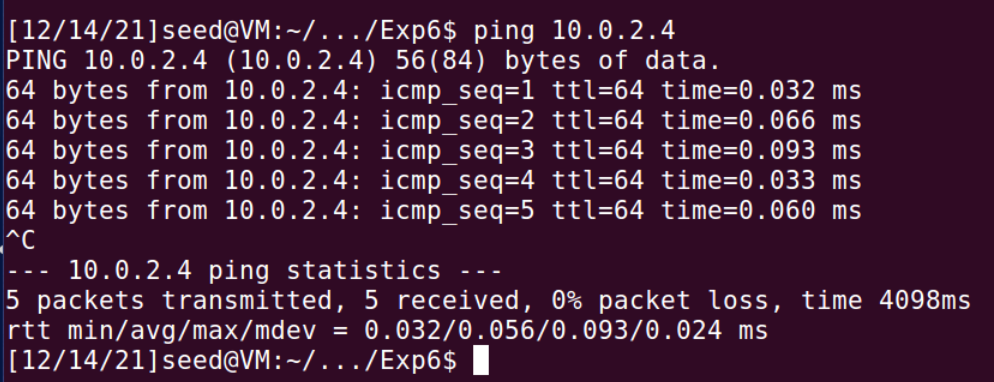
For instance, the screenshot shows the execution result on my VM image, and the IP address is e.g. 172.16.108.242

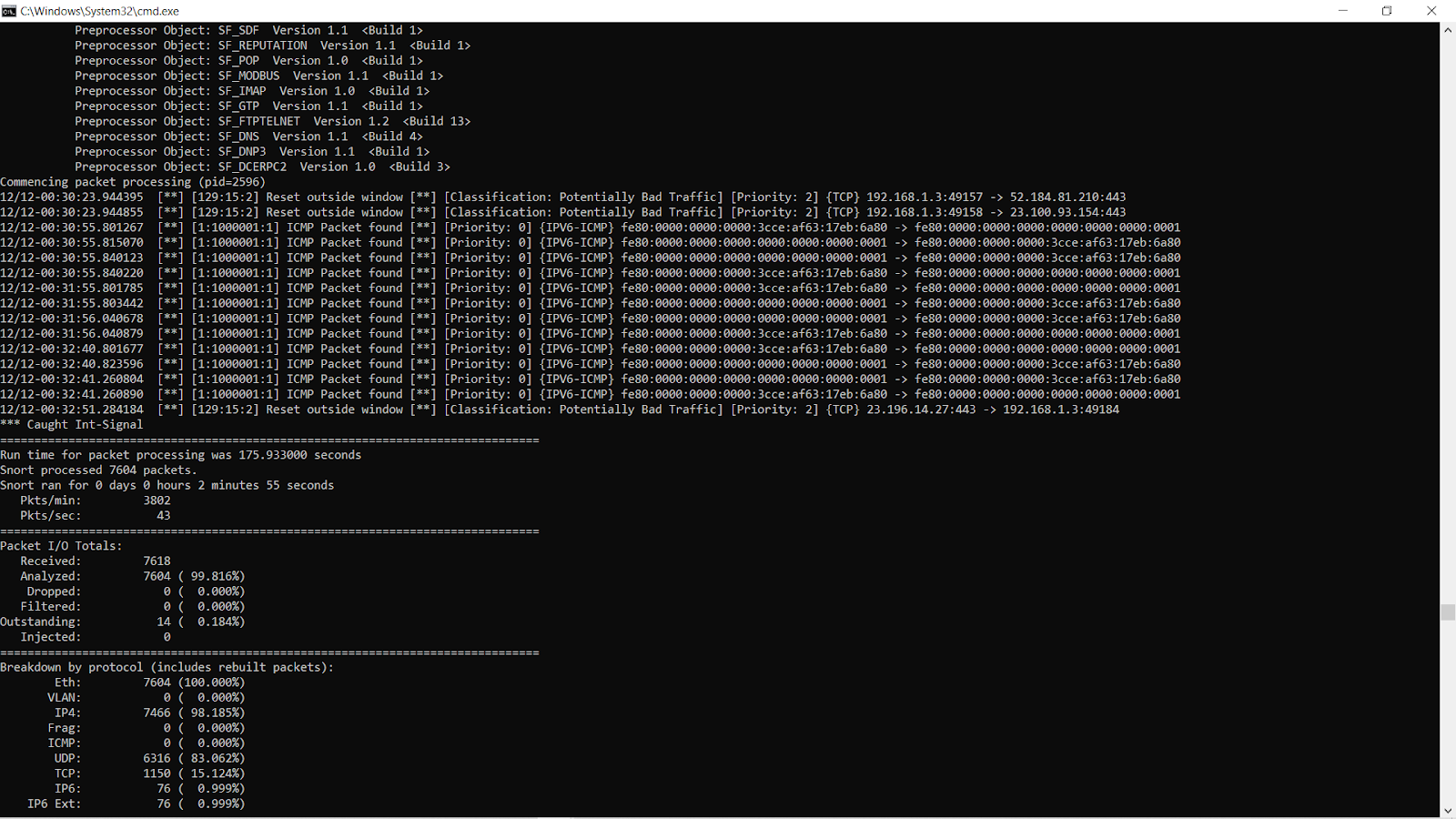
After you have a terminal, you can just type the following command to send ping messages to the VM.

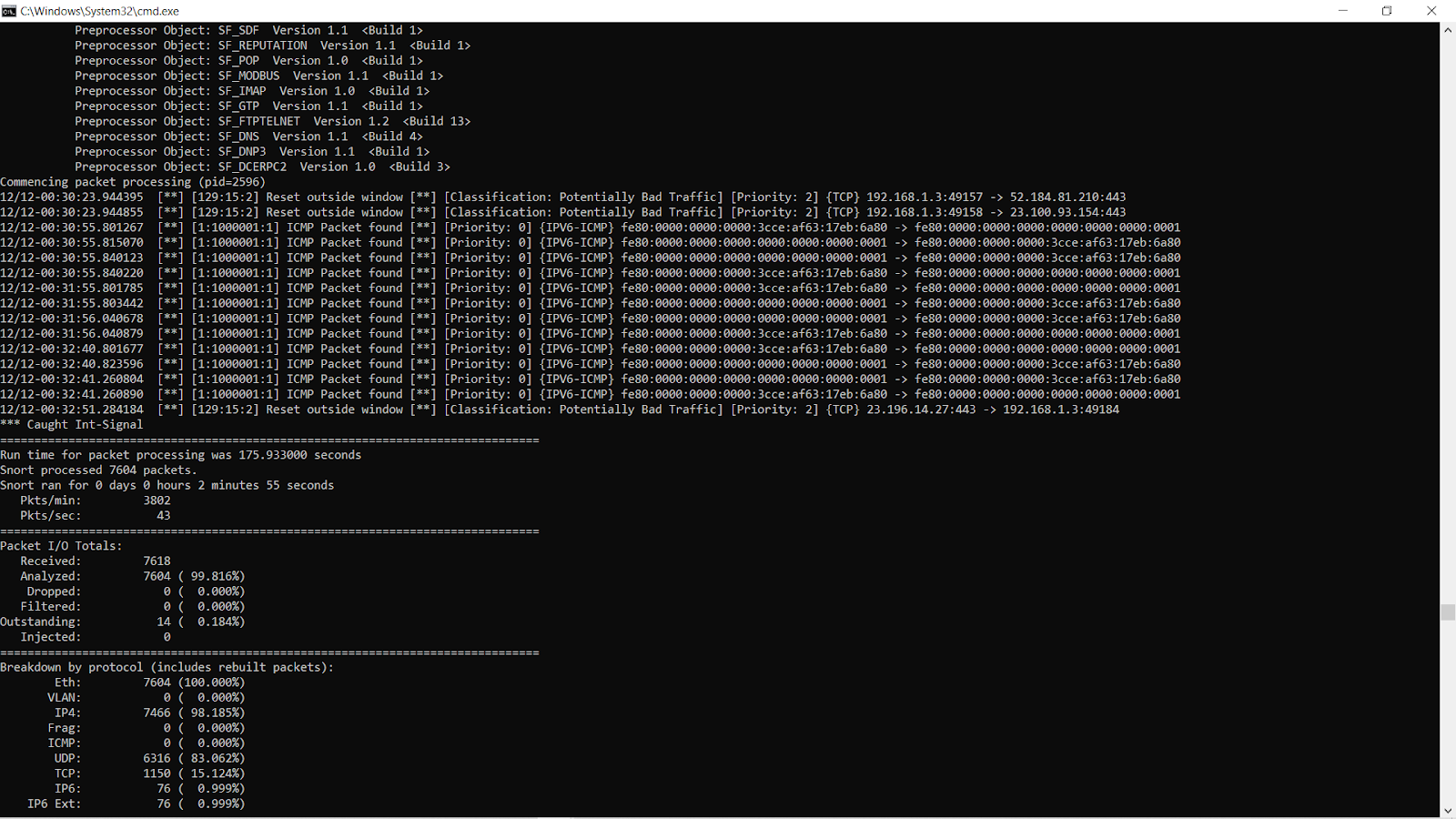
$ ping 172.16.108.242

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.









# 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.
   1. 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.

* 1. 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.

* 1. 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.

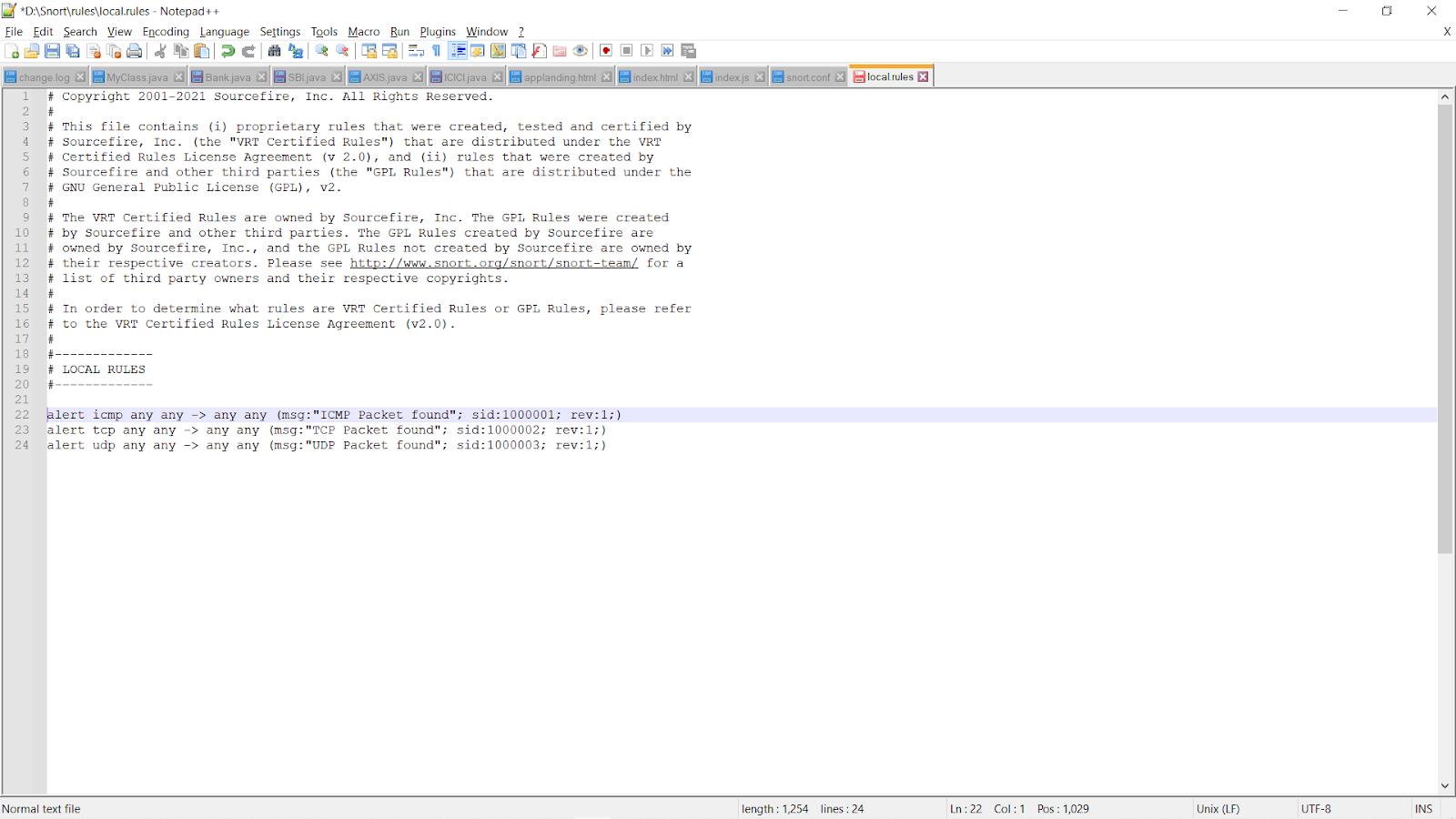
Number of total alarms = (100\*950)/95 = 1000 alarms.

Number of false alarms = 50 alarms.

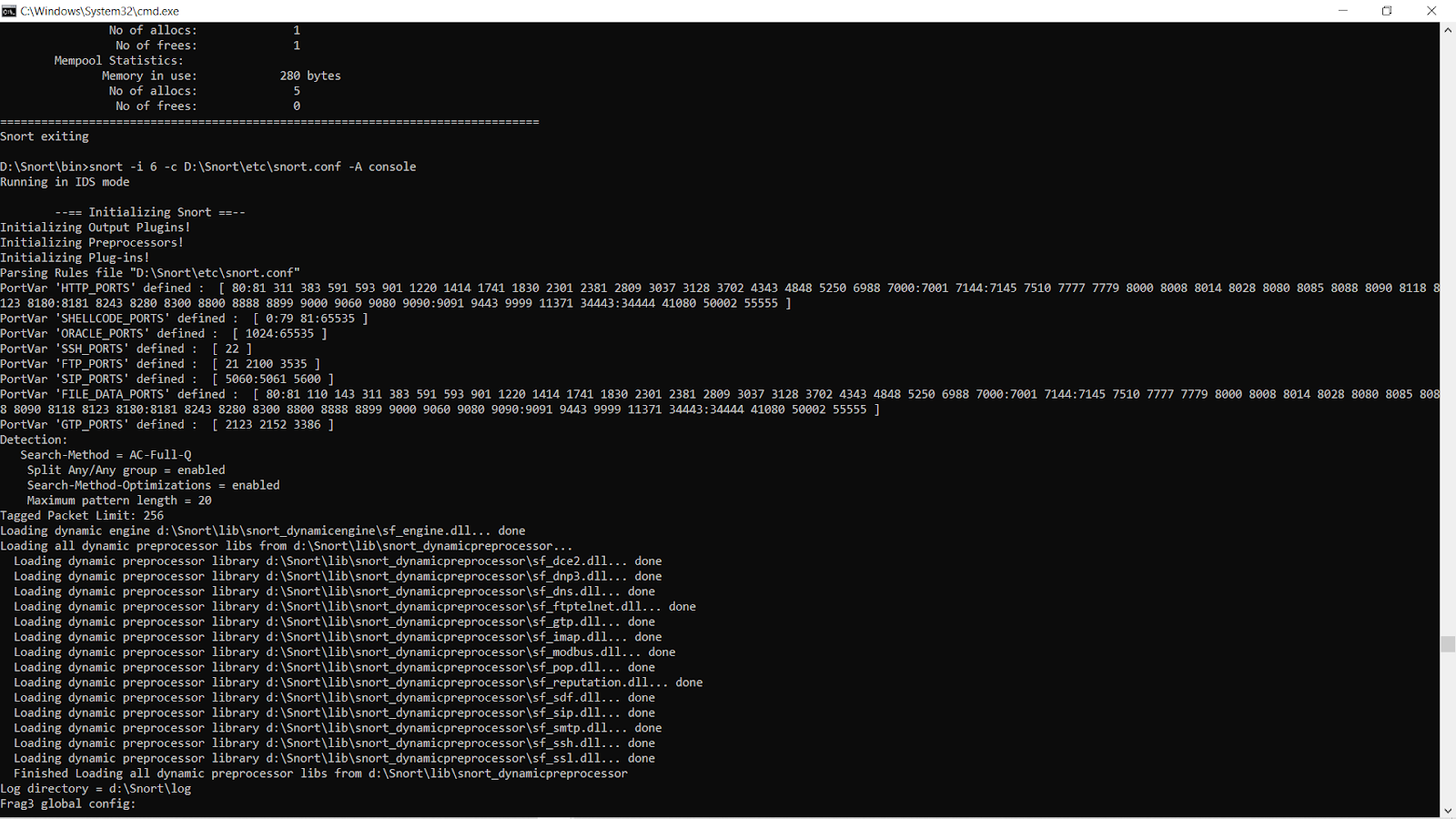
False Alarm Rate = (Number of false alarms / Total Events) \* 100 = (50 / 999000) \* 100 = **0.005%**

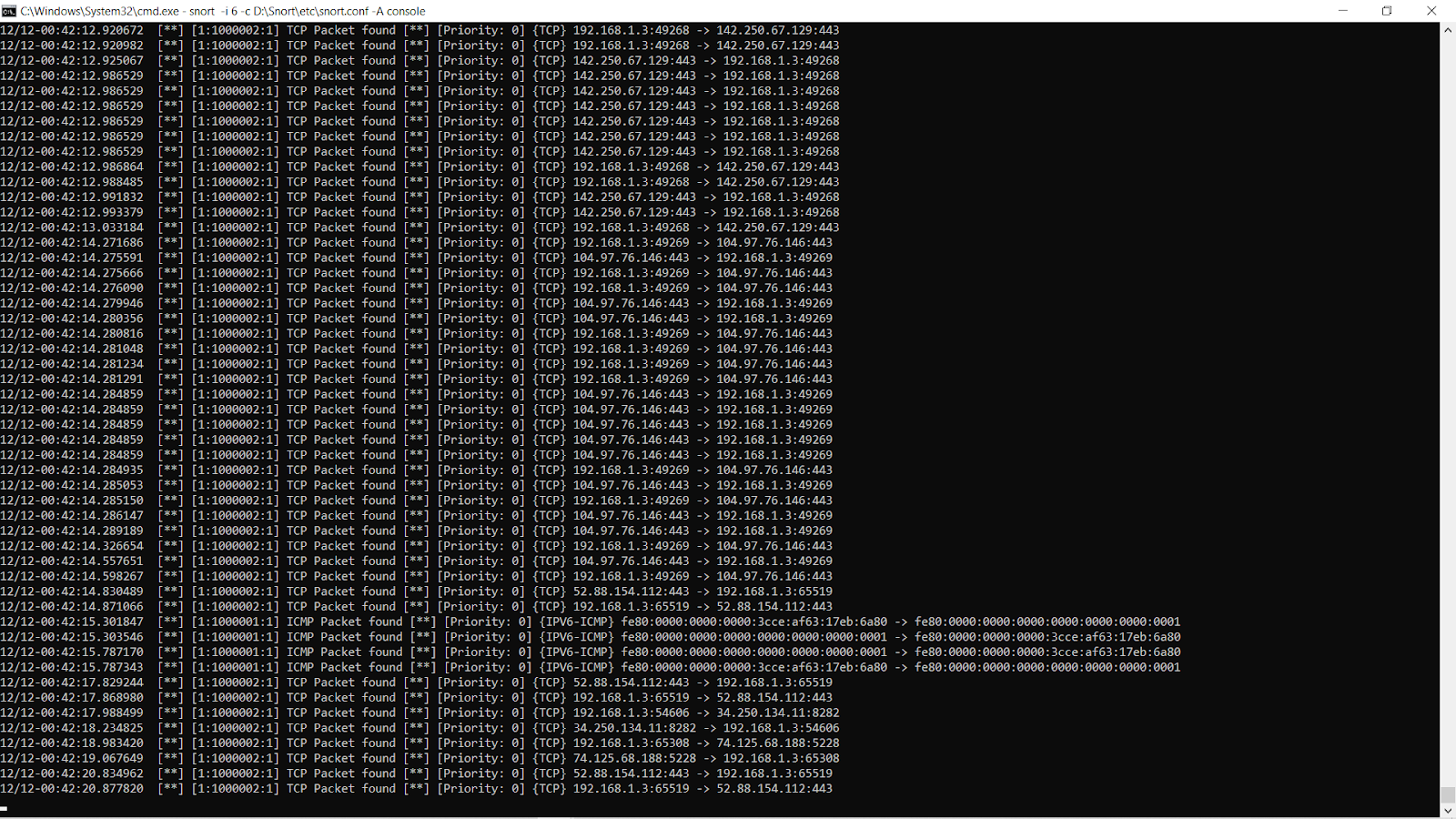
1. Write and add another snort rule and show me you trigger it.

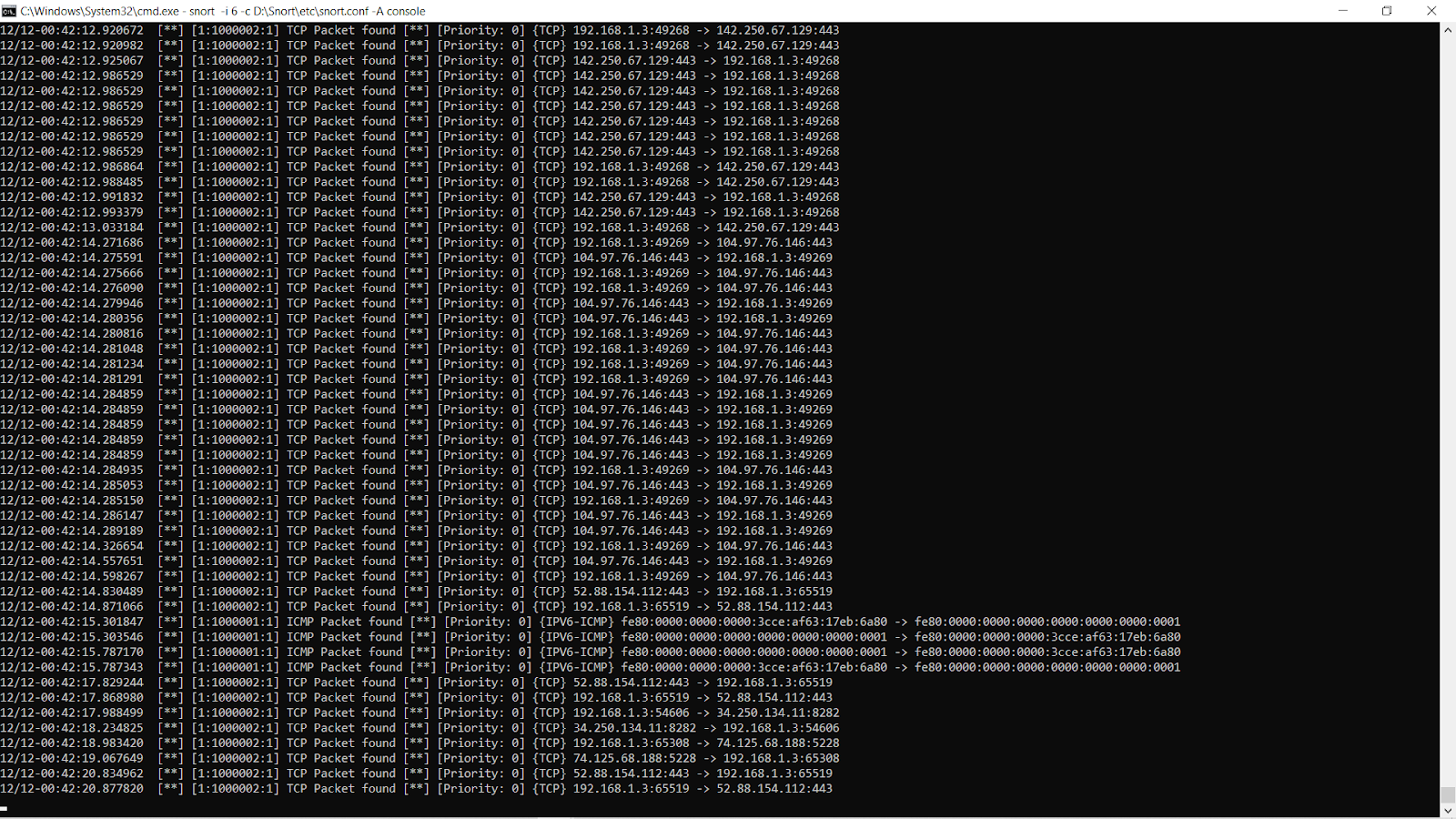
* 1. The rule you added (from the rules file)



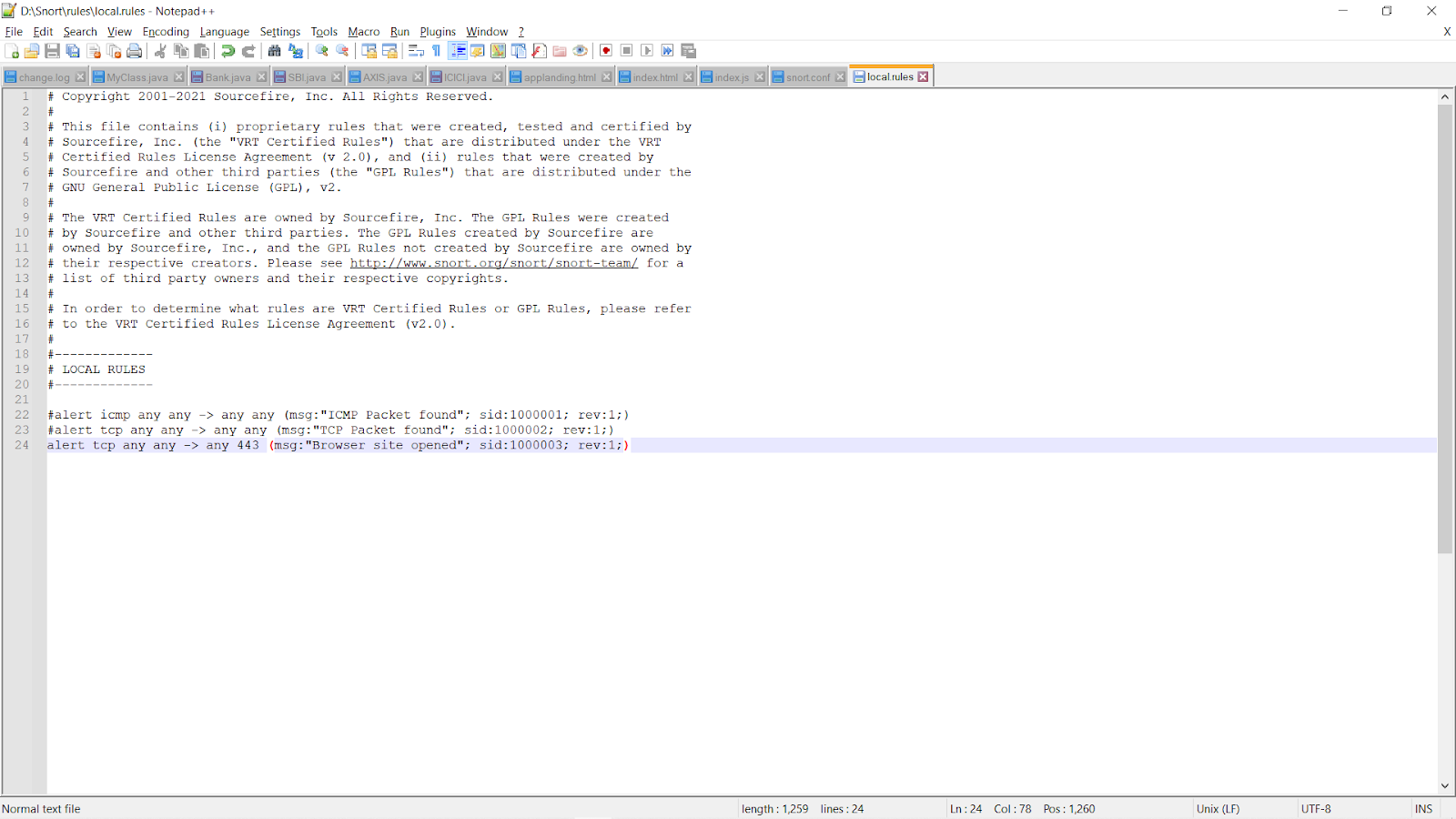
* 1. A description of how you triggered the alert. The alert itself from the log file (after converting it to readable text)

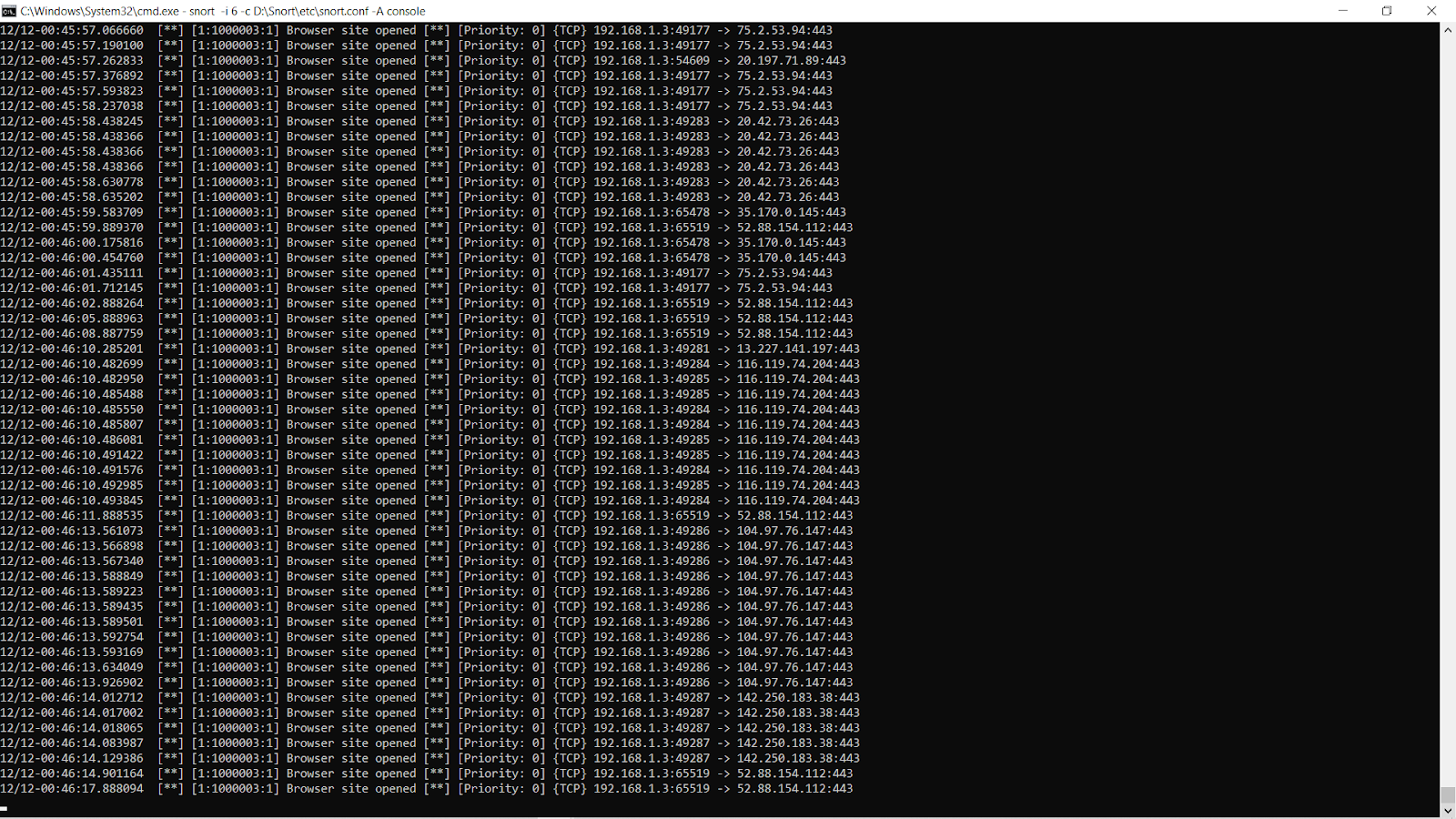






Extra Credit (10pt):Write a rule that will fire when you browse to any site from the machine Snort is running on; it should look for any outbound TCP request to the site you have considered and alert on it.





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.