**Cryptography & Network Security Lab**

**PRN/ Roll No: 2019BTECS00018**

**Full name: Rushikesh Kedarnath Patange**

**Batch: B1**

**Assignment No. 15**

**Title: Snort Intrusion Detection System (IDS)**

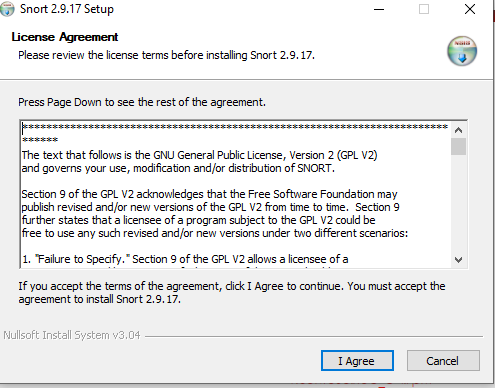
**Aim: To demonstrate installation,configuration and testing of Snort**

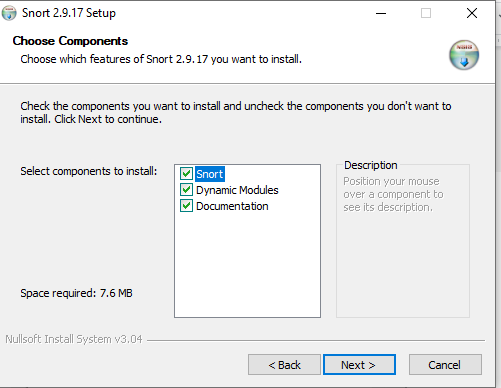
**Theory:**

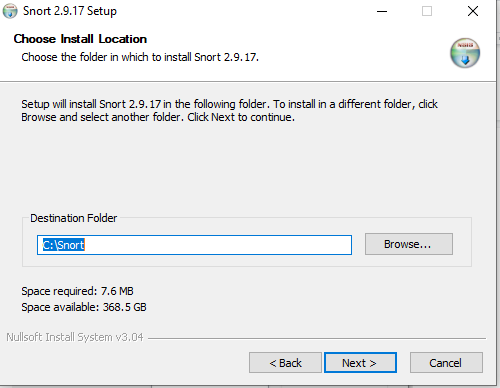
**Snort is an open source and popular Intrusion Detection System (IDS). It works by actively monitoring of network traffic parsing each packet and alerting system administrator of any anomalous behaviour that goes against the snort rules configured by the administrator according to the security policies of an organization.**

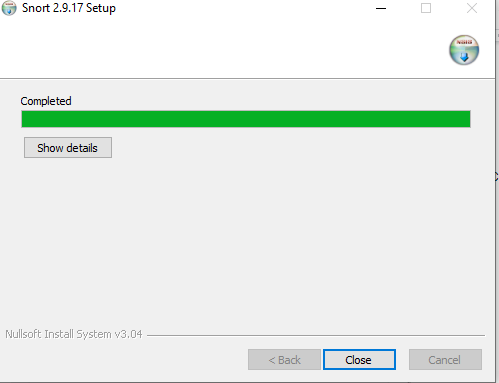
**Screenshots:**

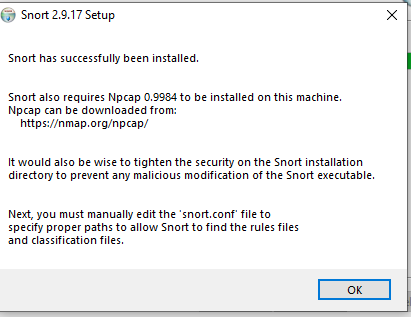
**Installation:**

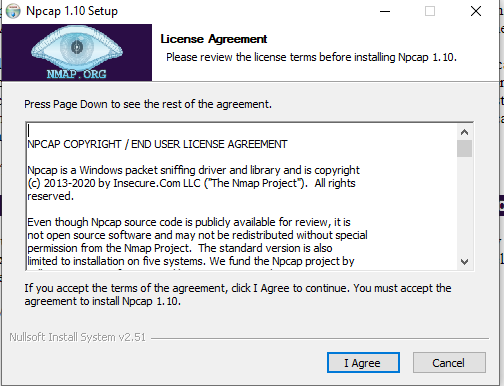


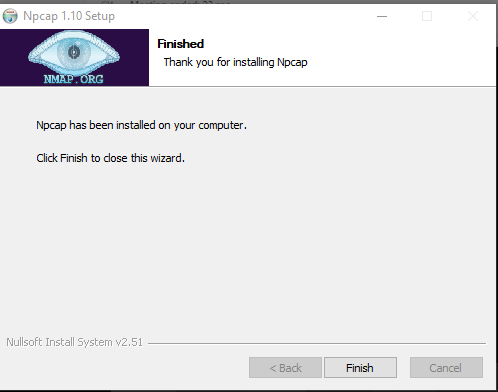












**Configuration of Snort**

1. Go to this[**link**](https://www.snort.org/downloads/#rule-downloads) and download latest snort rule file.
2. Extract 3 folders from the downloaded snortrules-snapshot-29170.tar folder into the Snorts corresponding folders in C drive.

**Folders to be extracted are**: **rules , preproc\_rules , etc**

* **rules folder** contains the rules files and the most important**local.rules** file. Which we will use to enter all our rules.
* **etc folder**contains all configuration files and the most important file is **snort.conf** file which we will use for configuration

**3**. Now open the **snort.conf** file through the notepad++ editor or any other text editor to edit configurations of snort to make it work like we want it to.

**4.** Setup the network addresses you are protecting

ipvar HOME\_NET any

**Note: Mention your own host IP addresses that you want to protect.**



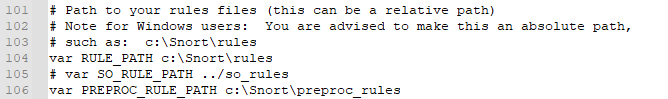
**5.** Setup the external network into anything that is not the home network. That is why ! is used in the command it denotes ‘not’.

# Set up the external network addresses. Leave as “any” in most situationsipvar EXTERNAL\_NET any



**6.** Now we have to define the directory for our rules and preproc rules folder

# 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\rulesvar RULE\_PATH ../rulesvar SO\_RULE\_PATH ../so\_rulesvar PREPROC\_RULE\_PATH ../preproc\_rules



**7.**Now we have to setup our white list and black list path it will be in our snorts’ rule folder

# If you are using reputation preprocessor set thesevar WHITE\_LIST\_PATH ../rulesvar BLACK\_LIST\_PATH ../rules



**8.**Next we have to enable to log directory, so that we store logs in our log folder. Uncomment this line and set absolute path to log directory

# Configure default log directory for snort to log to. For more information see snort -h command line options (-l)## config logdir:



**9.** Now we will set the path to dynamic preprocessors and dynamic engine

# path to dynamic preprocessor libraries  
dynamic preprocessor directory/usr/local/lib/snort\_dynamicpreprocessor/



**10.**We will do same thing for dynamic preprocessor engine

# path to base preprocessor enginedynamicengine /usr/local/lib/snort\_dynamicengine/libsf\_engine.so

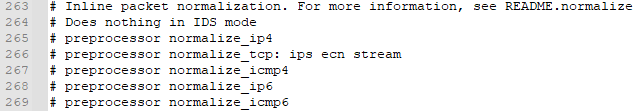


**11.** Now lets set our reputation preprocessors:

# path to dynamic rules libraries# dynamicdetection directory /usr/local/lib/snort\_dynamicrules



**12.** Just comment out these lines as shown in figure 19 in doing so we are excluding packet normalization of different packets.

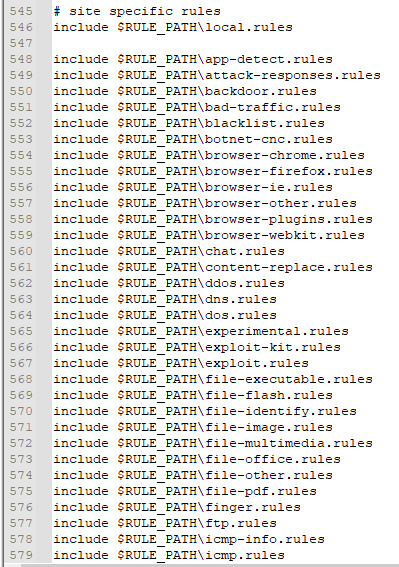


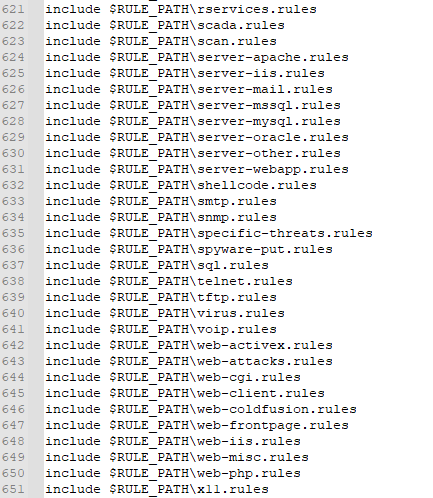
**13.**Scroll down to the reputation preprocessors. We will just change the name of the files since white list , black list are not rules they are just the list of IP addresses labelled as black or white

# Reputation preprocessor. For more information see README.reputationpreprocessor reputation: \memcap 500, \priority whitelist, \nested\_ip inner, \whitelist $WHITE\_LIST\_PATH/whitelist, \blacklist $BLACK\_LIST\_PATH\black.list



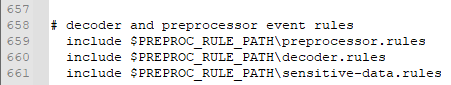
**14.**Converted back slashes to forward slashes in lines 546–651.





**15.**Again just convert forward slashes to backslashes and uncomment the lines below:

# decoder and preprocessor event rules# include $PREPROC\_RULE\_PATH/preprocessor.rules# include $PREPROC\_RULE\_PATH/decoder.rules# include $PREPROC\_RULE\_PATH/sensitive-data.rules



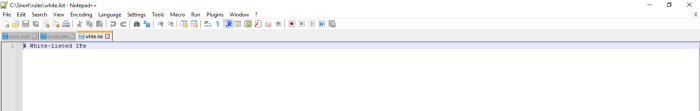
**16.**Now we just need to verify the presence of this command at the bottom of **snort.conf**file.



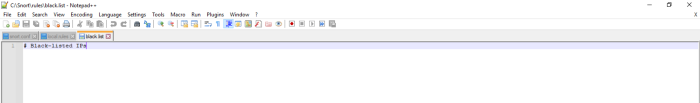
**17.**Click on Save file and save all changes to save the configuration file (**snort.conf**).

**18.**Now recalling the **Step 13** white list , black list are not rules they are just the list of IP addresses labelled as black or white right now these files don’t exist in our rule path which is why we have to create them manually , save them in this folder **C:\Snort\rules.**

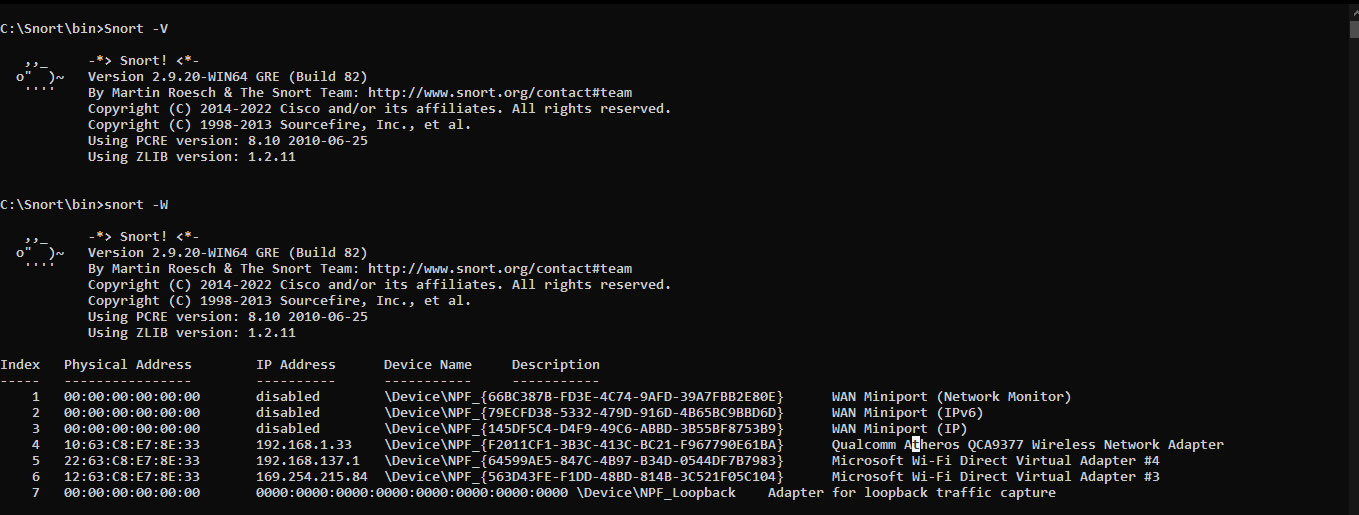
* Go to Notepad++ and create new file.
* Comment it #White-listed IPs.
* Name the file white.list and save the file.



* Create another new file.
* Comment it #Black-listed IPs.
* Name the file black.list and save the file.



**19.**Now we test snort again by running Command prompt as admin. To check if it’s running fine after all the configurations.

****

**Setting local.rules of C:\Snort\rules:**

alert icmp any any -> any any (msg: "ICMP Packet found"; sid:10000001;)

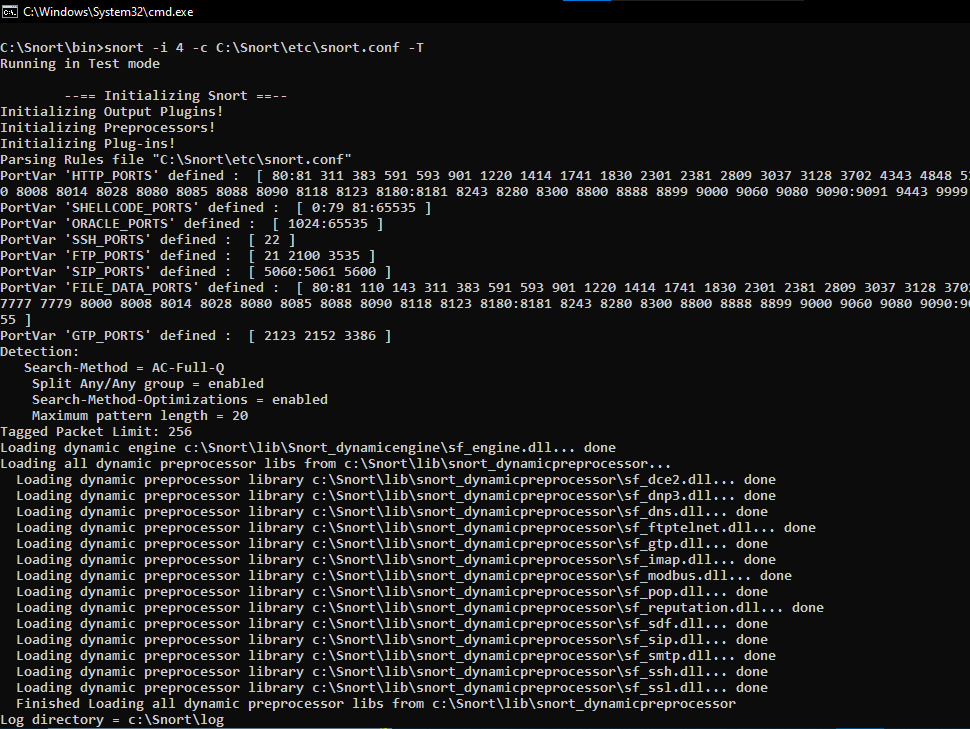
alert tcp any any -> any any (msg: "tcp Packet found"; sid:10000002;)

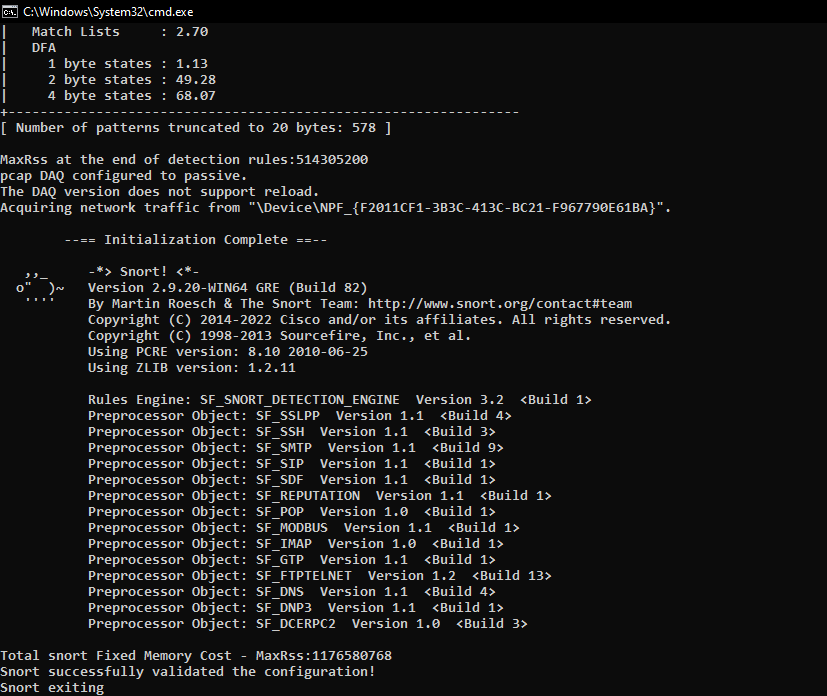
alert udp any any -> any any (msg: "udp Packet found"; sid:10000003;)

**Snort Testing:**

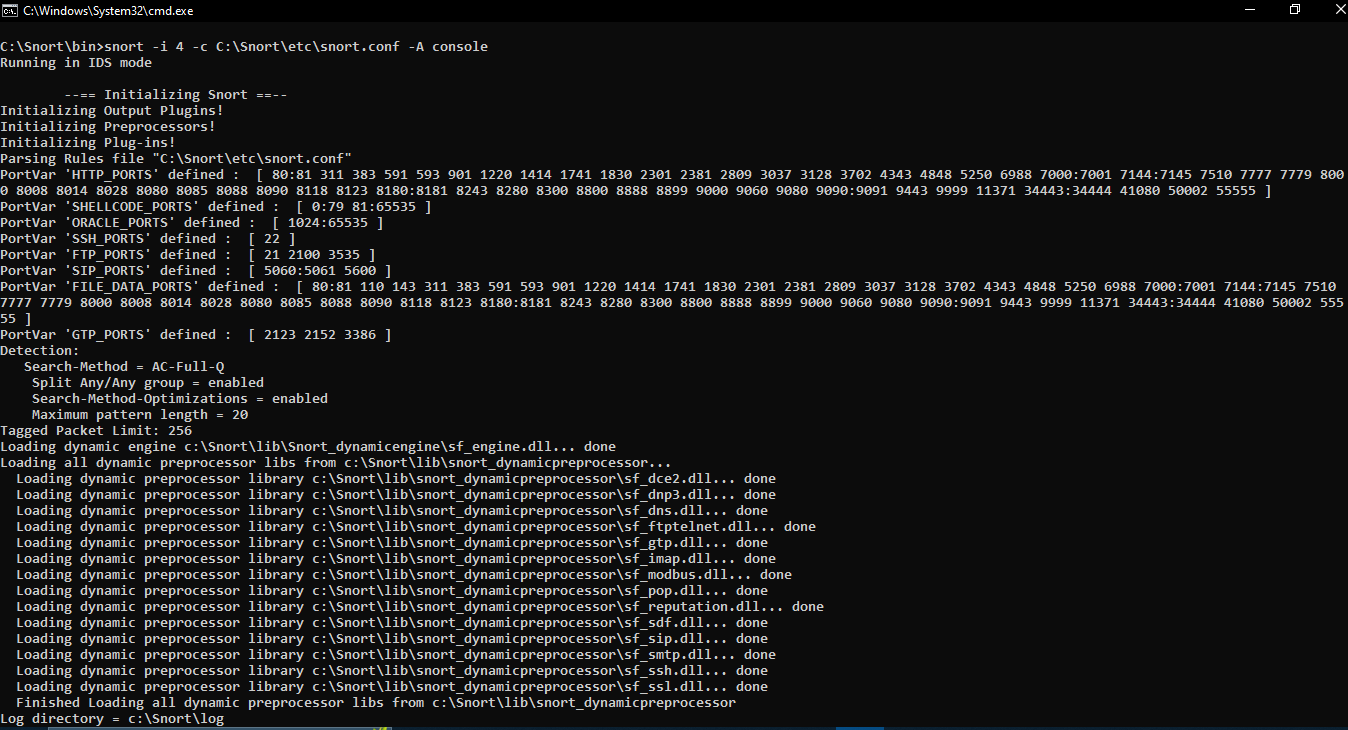
Using interface 4

snort -i 4 -c C:\Snort\etc\snort.conf -T





**Snort Console output:**

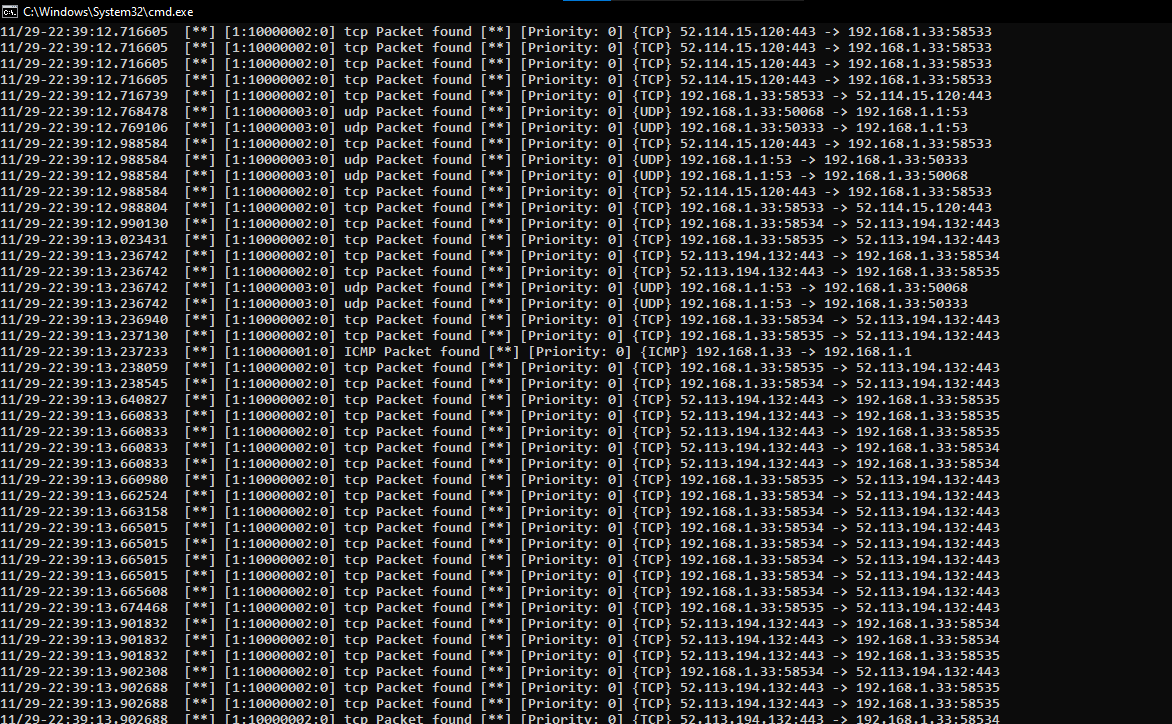
****

**Log Generation**

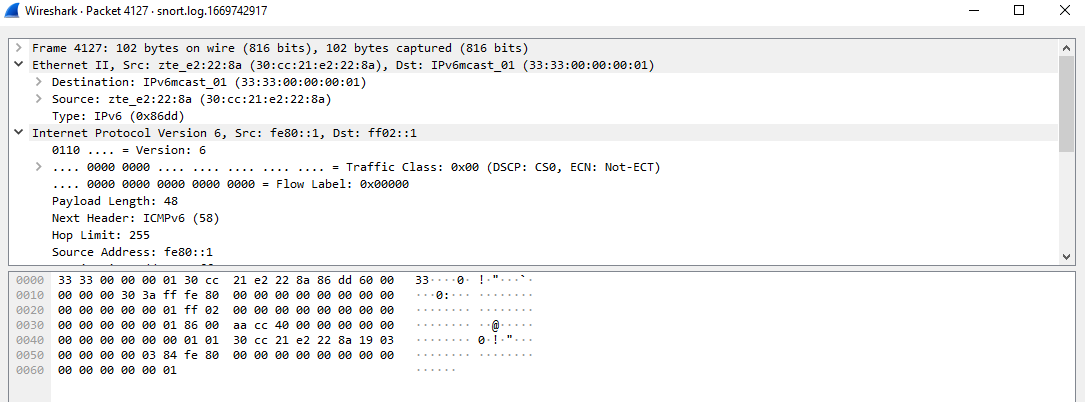
1.ICMP

2.UDP

3.TCP

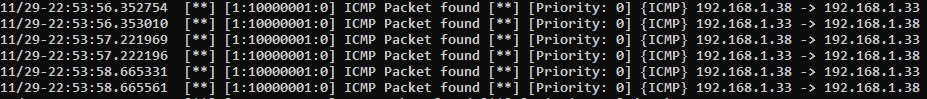


**Snort log file through wireshark:**

****

**Pinging through Intruder PC**

**Intruder IP : 192.168.1.38**

****

**Conclusion:**

Snort has multiple modes of operation, for the lab it has been used as a packet sniffer