## Simulating Attack Using Pytbull-ng Framework and Testing Snort Rules

Step 1: Update your System

- : Install Docker
- : Pull the pytbull-ng image:
- : Check that the image was installed:



Step 3: Install openssh server



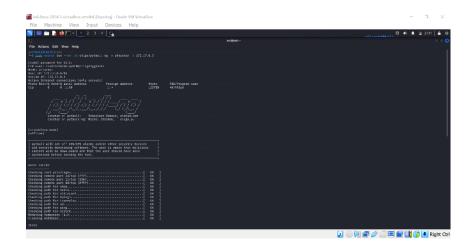
Step 3: Generating Attacks with pytbull-ng

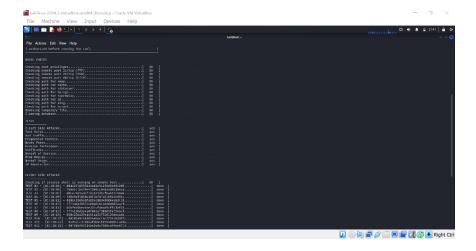




This will generate an IP, in my case IP = 172.17.0.5/16.

Open another terminal window and replace The IP generated with earlier:





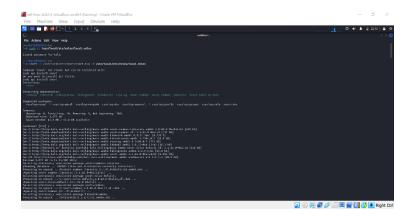
Attack is simulated on the machine

## Writing a Snort Rule to Block Google.com

Step 1 : Create folders for Snort rules and logs:



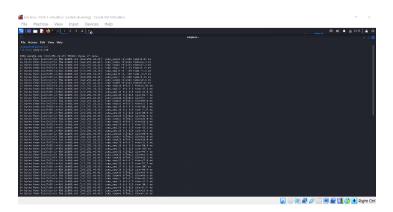
Step 2 : Edit local.rules to detect ICMP traffic: : Run Snort to validate the configuration:

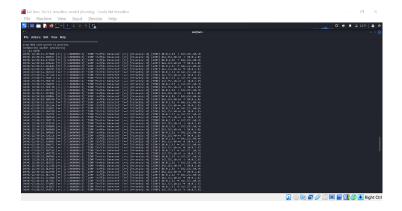


Step 3 : Run Snort in detection mode:

```
We have 1994 the large of the Manage Could Michigan Report the Section 1995 the Section 199
```

Step 5: Testing the rule with a ping command with other terminal





ICMP traffic detected is seen: detection of network traffic