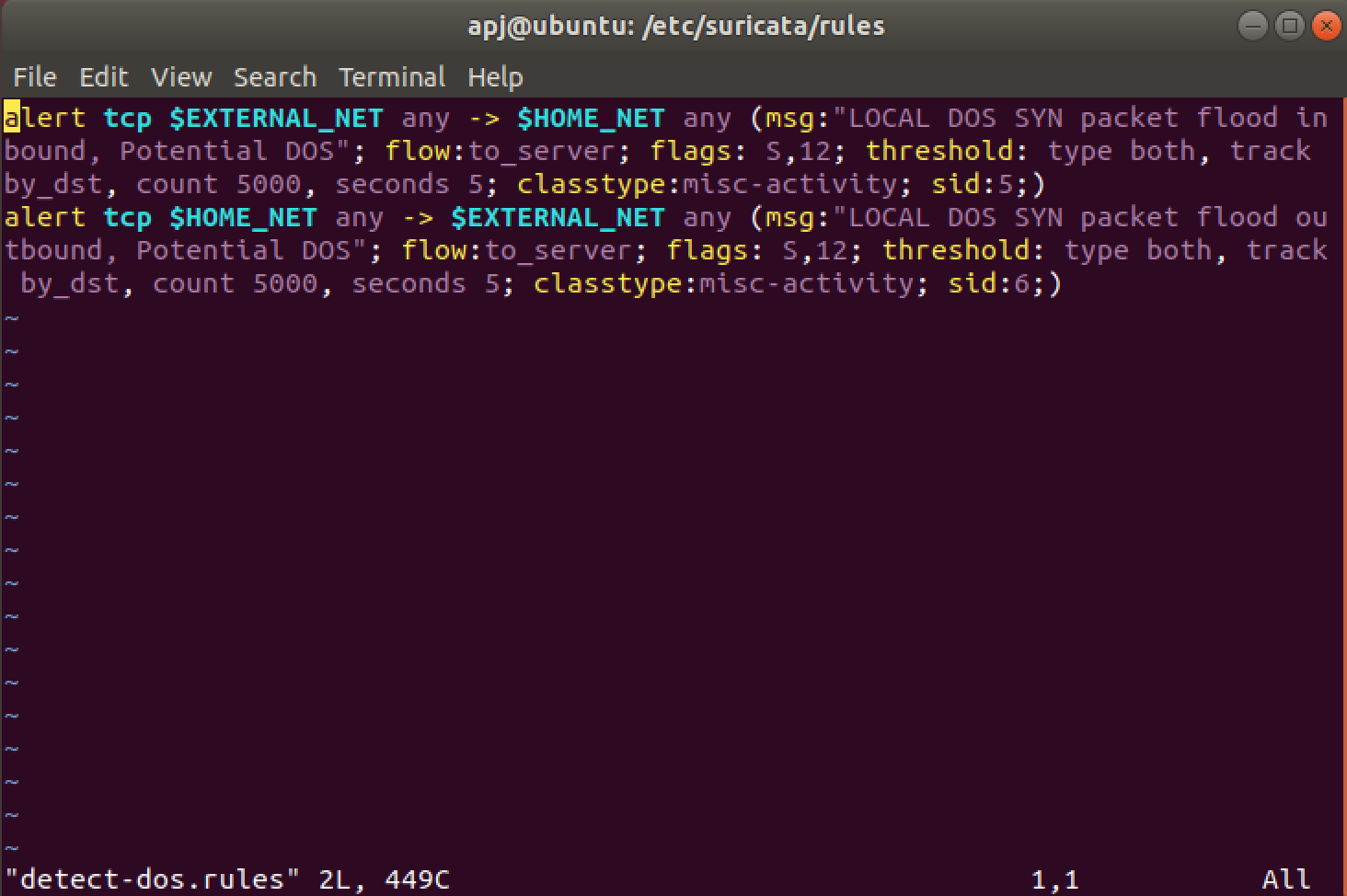
# **DOS attack**

## Step 1 :Adding DOS detection rule

Example rules:



Create new rules file with give above example

Rule file location : /etc/suricata/rules/

Create new rule file : sudo vim /etc/suricata/rules/detect-dos.rules

“detect-dos.rules” is new rule file

Step 2:

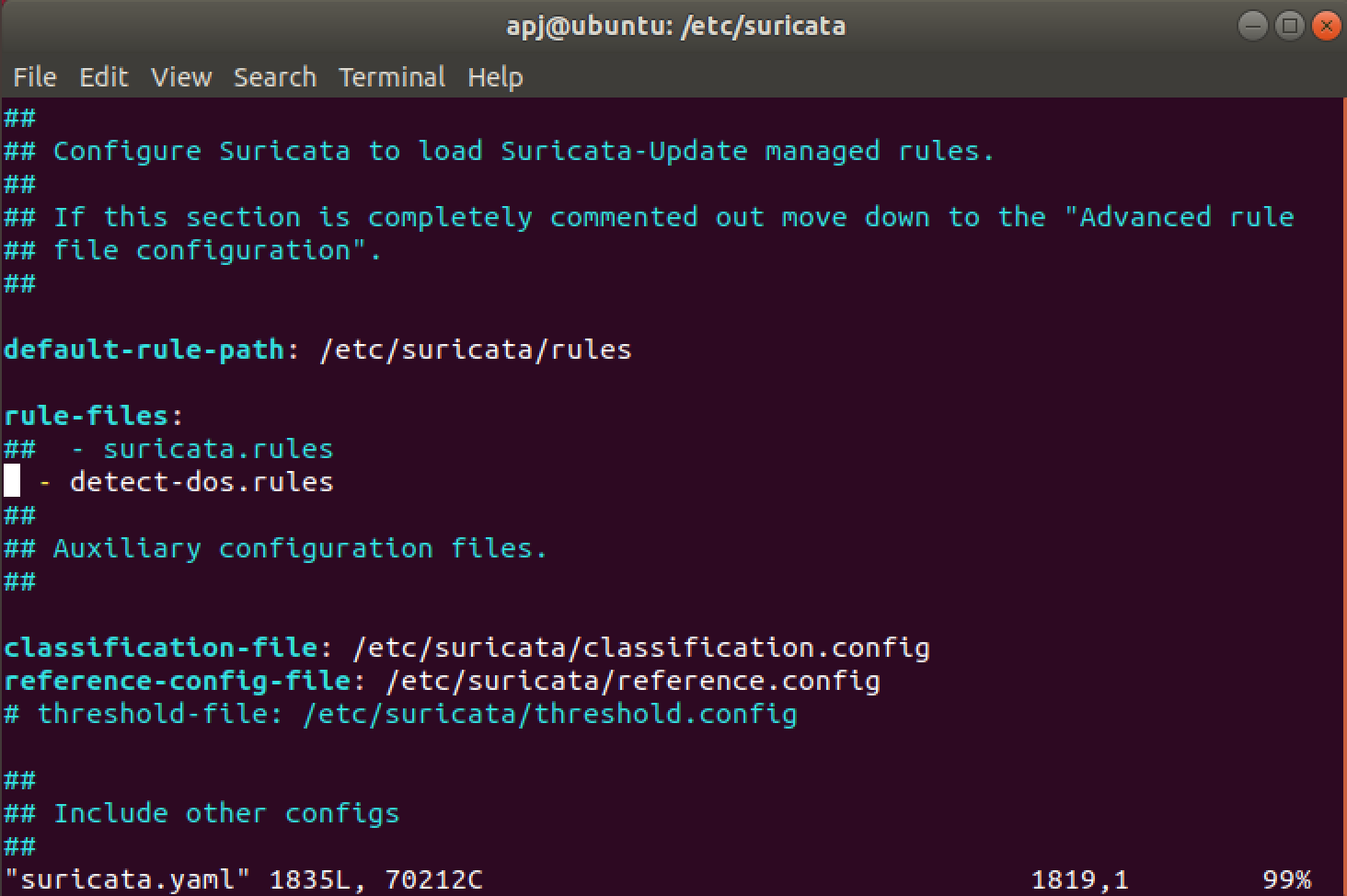
**The newly created rule file which was placed in the appropriate directory is added to the rule-files list:**

**Go to suricata configuration file edit “rule-file:”section (suricata.yaml)**

**rule-files:**

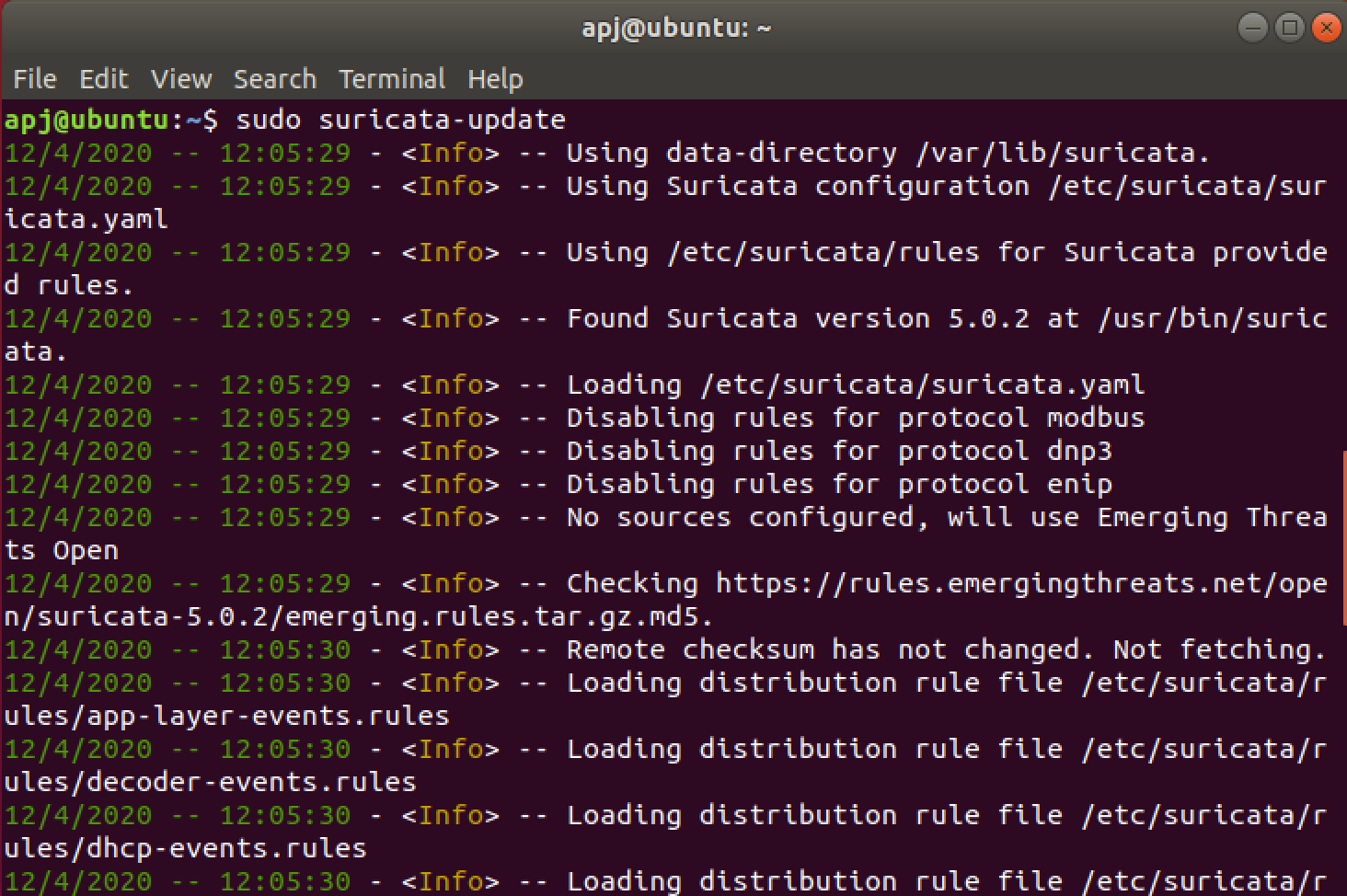
**- detect-dos.rules**

**Disable existing suricata.rules**

****

**Step 3:**

**suricata-update**

****

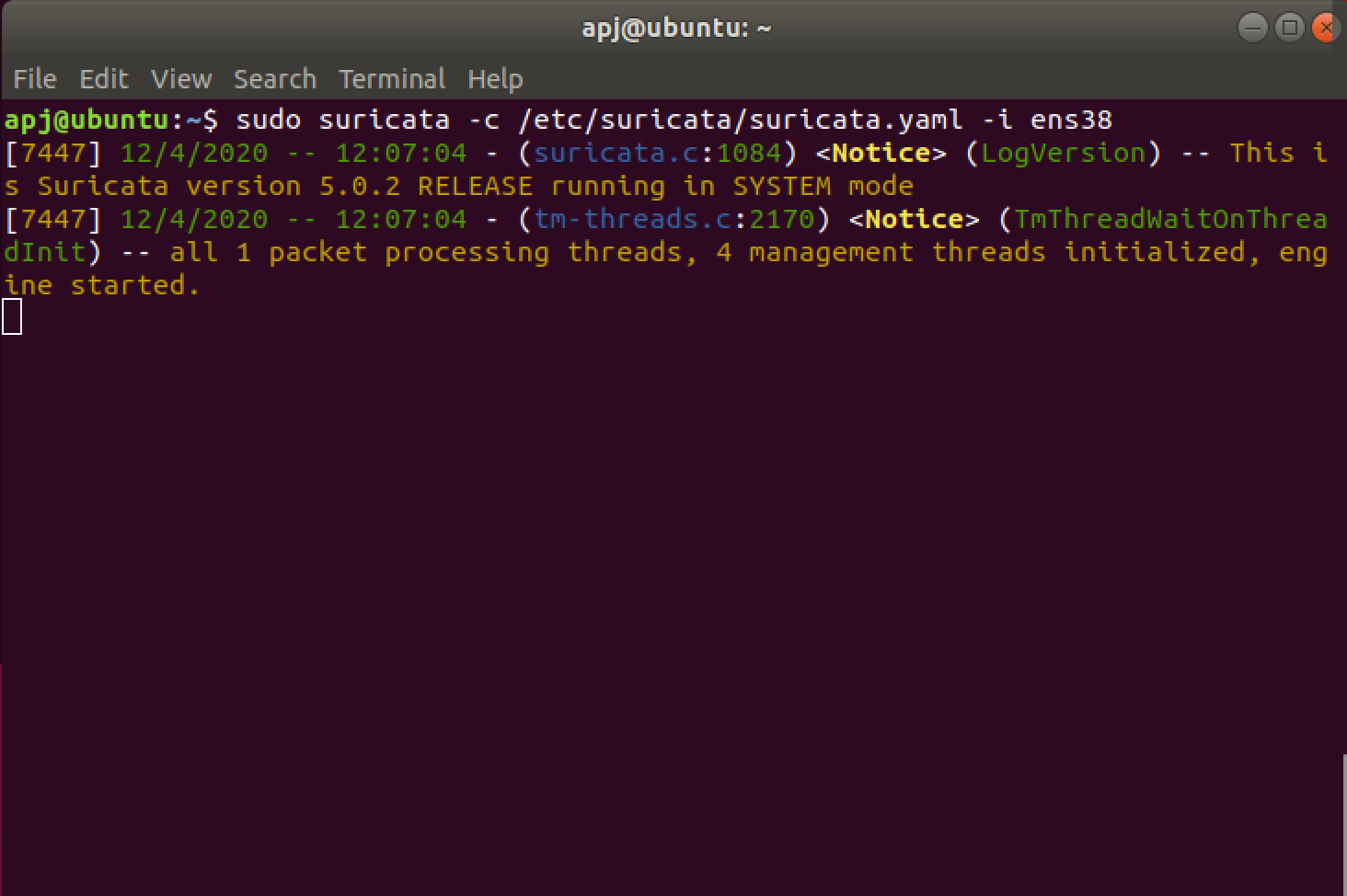
**Step 4:**

## Execute Suricata IDS

**Now the IDS is executed with the following command:**

**suricata -c /etc/suricata/suricata.yaml -i enp0s3**

**“enp0s3” is interface of system**

****

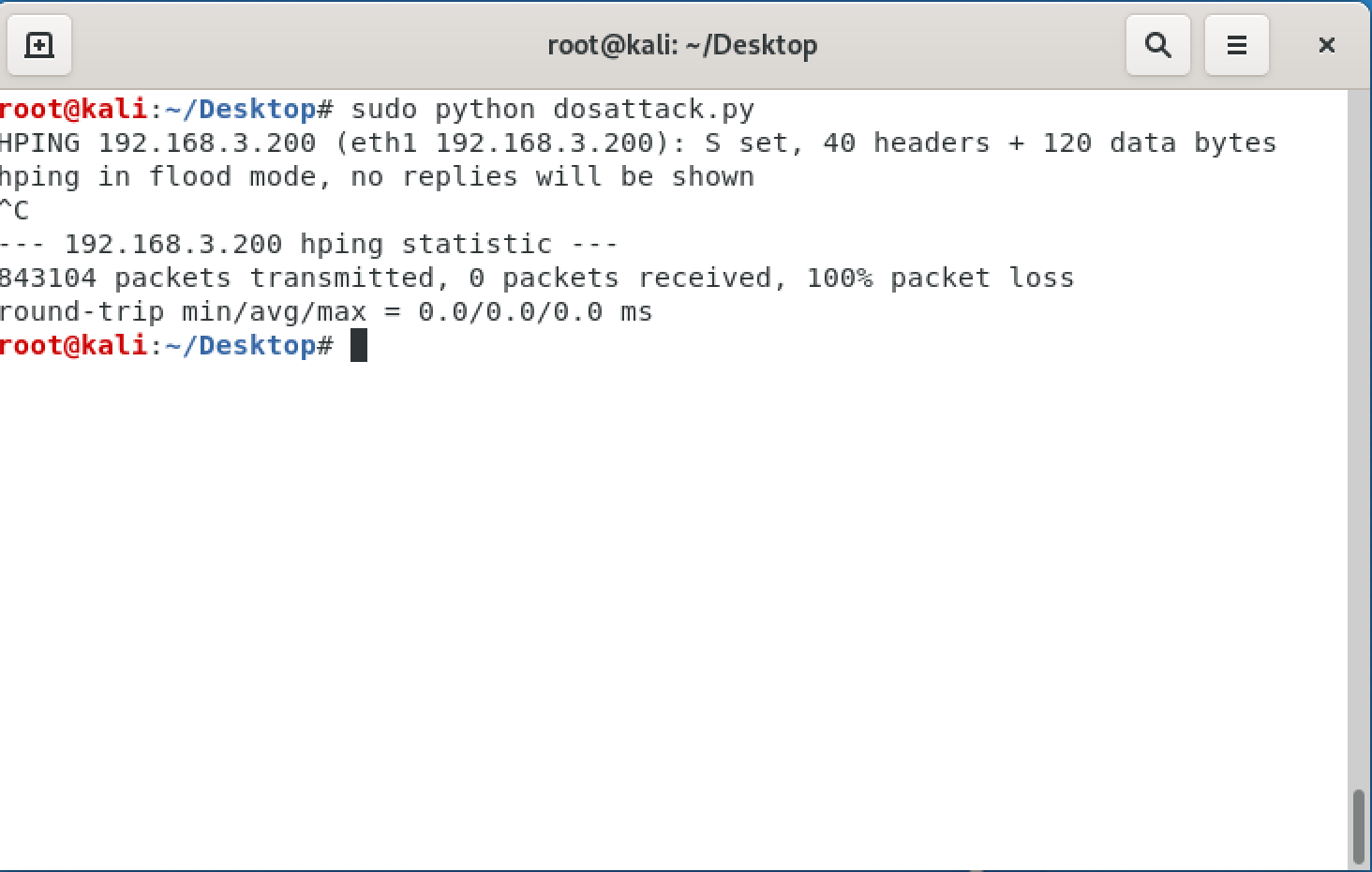
**Now , Suricata Started**

**Step 5:**

**Now the DOS attack is conducted from the Kali Vm using the python script dos\_attack.py which utilizes the hping3 network utlity to generate and flood TCP SYN packet to the target IP address (the IP address can be updated by changing the file contents).**

**Save dos\_attack.py file in Desktop**

**Inside python file like**

****

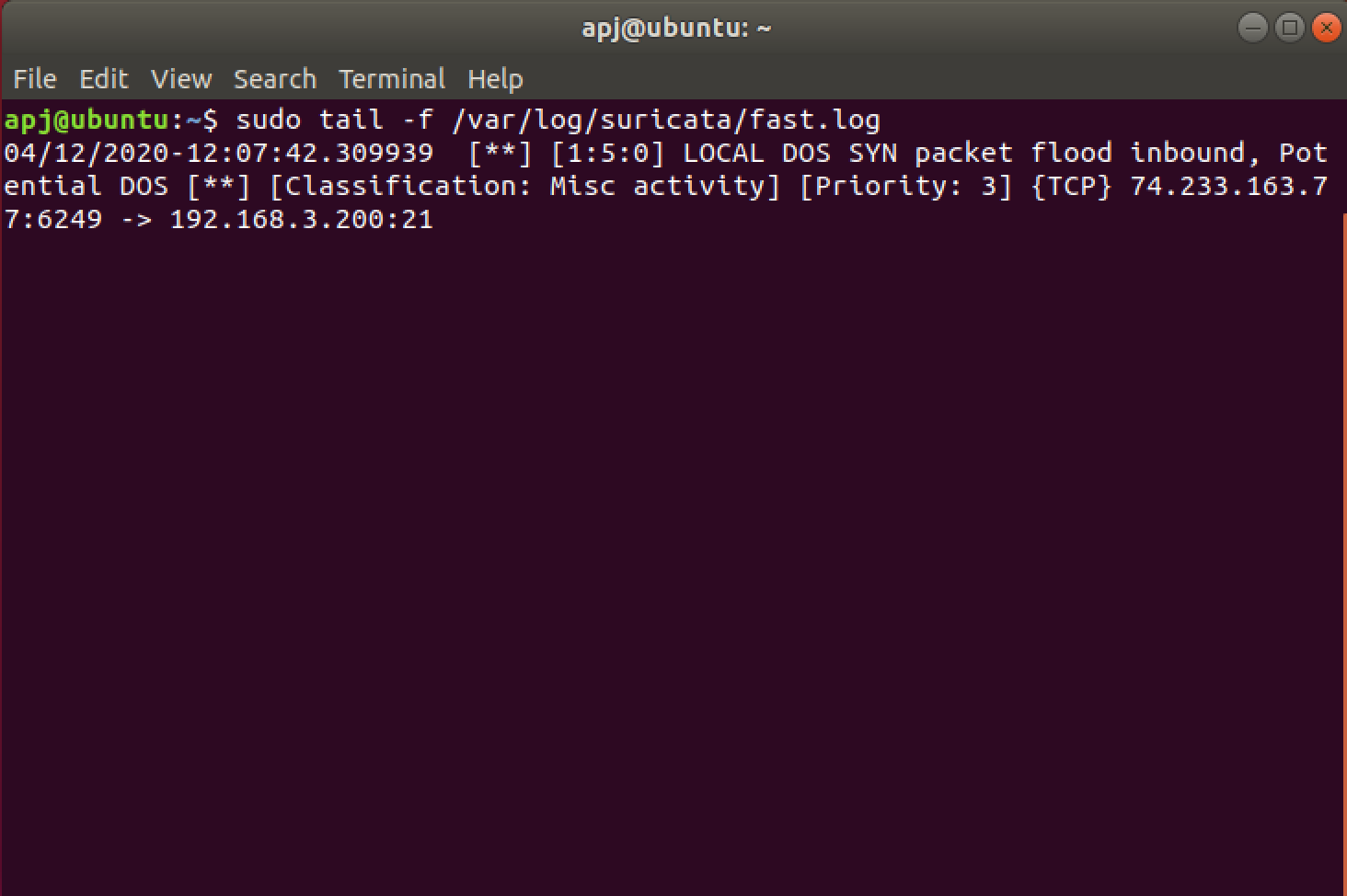
**Run python file in Kali Linux command prompt**

**Type : python dos\_attack.py**

**Step 6:**

**Now the IDS rules get triggered and suricata alerts that there is a possible DOS attack, this can be seen in the logs with the command:**

**“ sudo tail -f /var/log/suricata/fast.log “**

****

**Hence suricata acted as an IDS and detected the DoS attack.**