**EX NO: 10**

**DATE:**

**PERFORM REAL-TIME NETWORK TRAFFIC ANALYSIS AND DATA POCKET LOGGING USING SNORT**

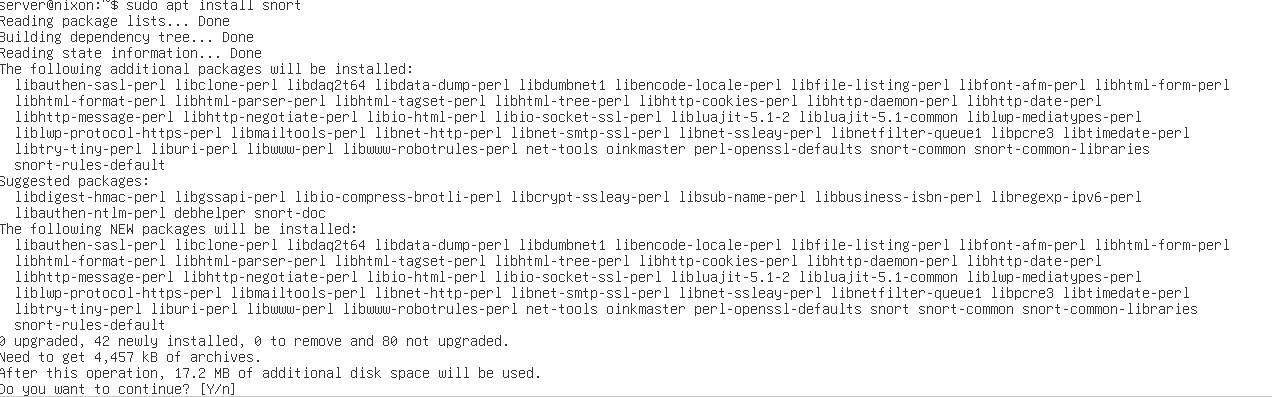
**AIM:**

To perform real-time network traffic analysis and data pocket logging using Snort.

**PROCEDURE:**

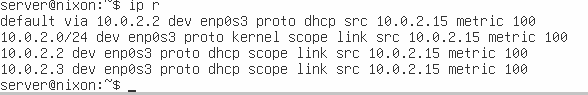
**Step1:** Install the snort tool by using the following command

**$sudo apt install snort**



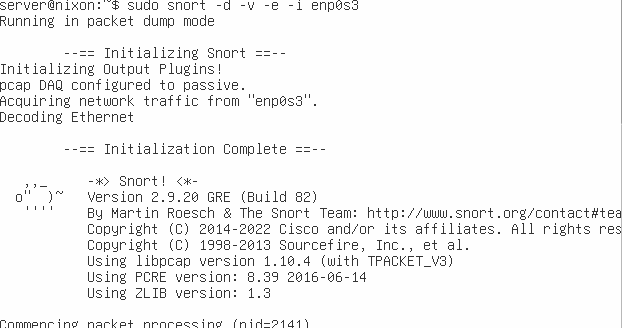
**Step2:** Note the IP of the ubuntu server

**$ ip r**



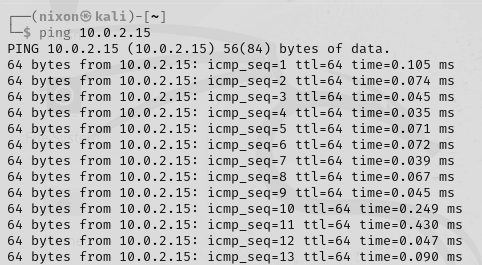
**Step3:**To run the snort in sniffer mode (capture packets)

**$ sudo snort -d -v -e -i enp0s3**



**Step4:**Open the kali linux and ping the ubuntu server

**$ ping 10.0.2.15**



**Step5**: In the ubuntu server we can see the ICMP ECHO messages.



**RESULT:**

Thus the real-time network traffic analysis and data pocket logging using Snort has been done successfully.