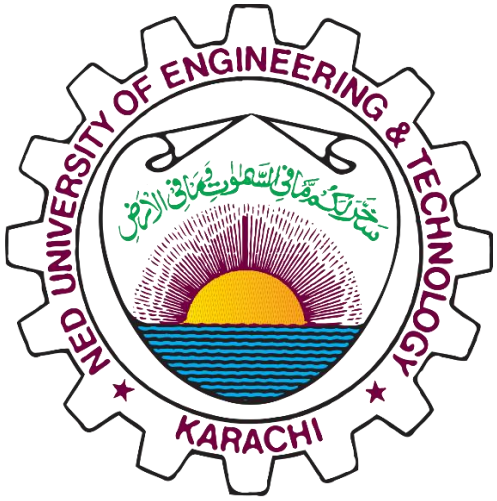
Intrusion Detection & Prevention System Using Snort on Ubuntu



Group Members	**Uzma Haneef** **Sarah Zafar** **Hashem Al-Sakkaf**
Course Instructor	**Prof. Dr. Muhammad Mubashir**
Course Title	**Information Security**
Course Code	**CT-355**

Introduction:

Snort is a widely used open-source intrusion detection system (IDS) designed to analyze network traffic in real-time and identify potential threats by matching traffic patterns against predefined rules. For this project, we installed and configured Snort on Ubuntu, a user-friendly Linux distribution, to serve as the platform for implementing a basic IDS and IPS. The setup involved configuring Snort rules to specifically detect ICMP packets, such as ping requests, and SSH login attempts, which are common in network reconnaissance and unauthorized access attempts. By customizing Snort's rule set and optimizing its configuration on Ubuntu, the system was fine-tuned to monitor network activity effectively and log potential security events for analysis.

Commands used:

To install snort:

sudo apt-get install snort

Change snort.conf home_net directory to:

ipvar HOME_NET 192.168.0.0/24

To configure Snort:

cd/ etc/snort

ls

sudo cp snort.conf snort.conf.backup

ls

sudo nano snort.conf

sudo snort –T –I enp0s8 –c etc/snort/snort.conf

Setting up custom rules on Snort:

sudo nano local.rules

alert icmp any any -> $HOME_NET any (msg: "ICMP Detected"; sid: 1000001; rev: 1)

alert tcp any any -> any443 (msg: “SSH Detected”; sid: 1000002; rev: 1)

ls

sudo snort –A console –q –i enp0s8 –c etc/snort/snort.conf –K ascii

On new terminal: -For ICMP packet detection

sudo nano /var/log/snort/snort.alert.fast

ping google.com

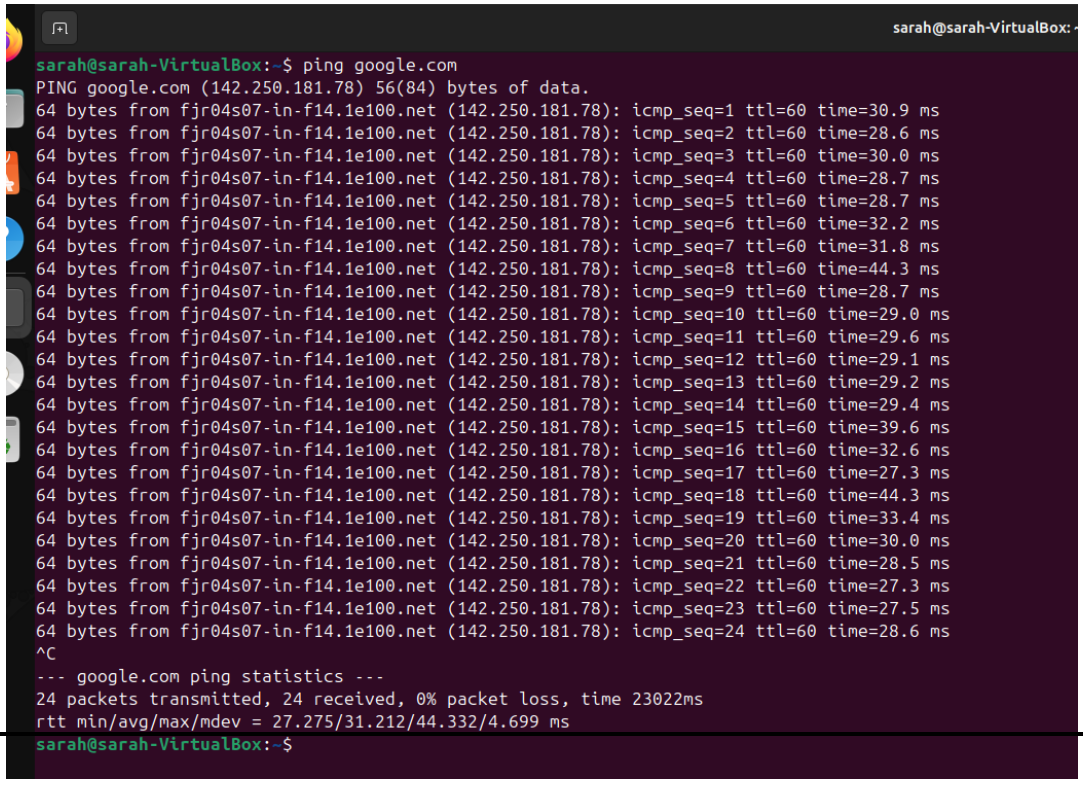
On new terminal: -For SSH login attempt detection

sudo su

sudo nano /var/log/snort/snort.alert.fast

sudo snort –A console –q –i enp0s8 –c etc/snort/snort.conf –K ascii

Ping google.com results:



ICMP packet & SSH login attempt detection: