SNORT BASIC PRACTICAL (DEBIAN 12)

Objective:
Install and run Snort IDS on Debian 12 and generate a basic alert.

Step 1: Backup sources.list
sudo cp /etc/apt/sources.list /etc/apt/sources.list.backup

Step 2: Edit sources.list
sudo nano /etc/apt/sources.list

Paste:
deb http://deb.debian.org/debian bullseye main
deb http://security.debian.org/debian-security bullseye-security main
deb http://deb.debian.org/debian bullseye-updates main

Step 3: Update system
sudo apt update

Step 4: Install Snort
sudo apt install snort -y

Step 5: Verify installation
snort -V

Step 6: Edit Snort config
sudo nano /etc/snort/snort.conf

Change:
ipvar HOME_NET any
To:
ipvar HOME_NET 192.168.1.0/24

Step 7: Add rule
sudo nano /etc/snort/rules/local.rules

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

Step 8: Test configuration
sudo snort -T -c /etc/snort/snort.conf

Step 9: Run Snort
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0

Step 10: Generate traffic
ping <SNORT_MACHINE_IP>

Result:
Snort generates ICMP alert on console.

Conclusion:
Snort successfully detects network traffic using signature-based rules.