# Switch to root (if not using sudo)

su -

# Update and upgrade the system

apt update && apt upgrade -y

# Install Snort

apt install snort -y

# (Optional) Check your network interfaces (replace eth0 below if needed)

ip a

# Create a custom local rule for ICMP detection

echo 'alert icmp any any -> any any (msg:"ICMP Detected!"; sid:1000001; rev:1;)' > /etc/snort/rules/local.rules

# Edit snort.conf to include the local.rules file

sed -i '/^# include \$RULE\_PATH\/local.rules/s/^# //' /etc/snort/snort.conf

# Run Snort with custom rule (replace eth0 if needed)

snort -i eth0 -A console -c /etc/snort/snort.conf