**SARA SALEEM**

**CA/AP1/7683**

**Domain: Cyber security**

**Task 4: network intrusion detection and prevention by using Snort IDS Configuration and Testing**

**Objective**

**In this Task , you will:**

**∙ Install and configure Snort IDS**

**∙ Create and test custom Snort rules**

**∙ Perform network scanning and intrusion attempts to verify Snort alerts**

**Task Requirements**

**∙ Ubuntu/Linux machine**

**∙ Internet connectivity**

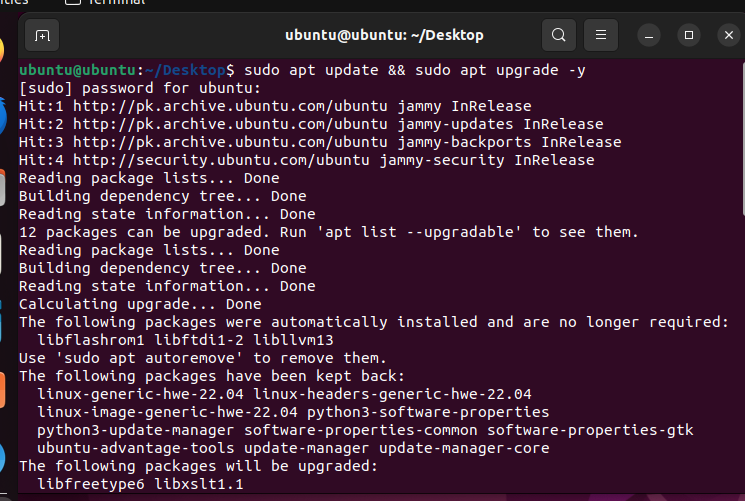
**∙ nmap installed (if not, install with sudo apt install nmap –y on linux)**

**Task Breakdown**

**Task 1: Update System and Install Snort**

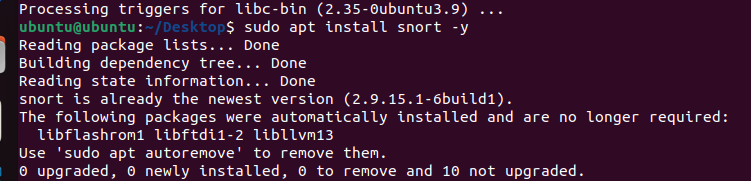
**1. Update the package lists and upgrade the system:**

**sudo apt update && sudo apt upgrade -y**

****

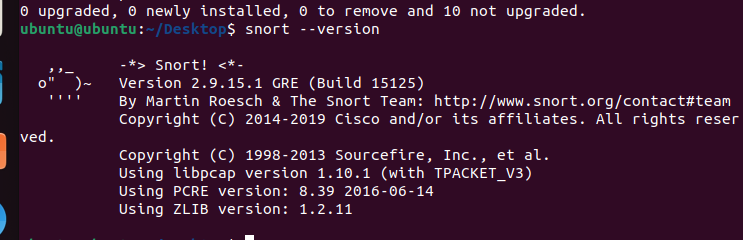
**2. Install Snort:**

**sudo apt install snort -y**

****

**3. Verify installation:**

**snort --version**

****

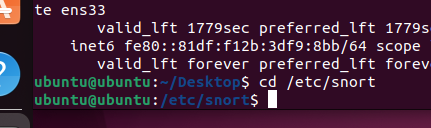
**Network Interface and Snort Configuration**

**1. Check your network IP address:**

**ip a**

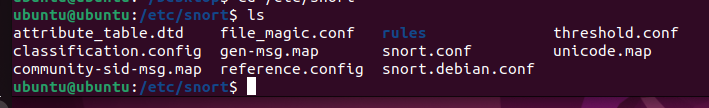
**2. Navigate to Snort configuration directory:**

**cd /etc/snort**

****

**3. List available files:**

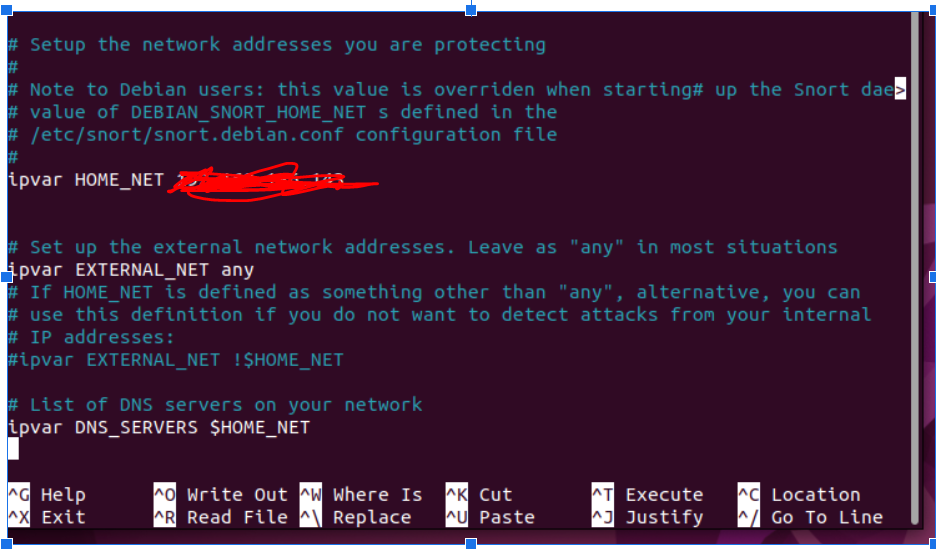
**ls**

****

**4. Open snort.conf for editing:**

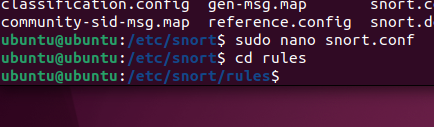
**sudo nano snort.conf**

**o Ensure HOME\_NET is set correctly**

** Adding Custom Rules**

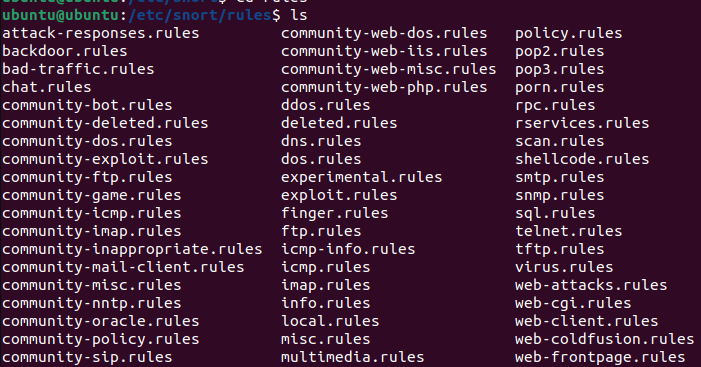
**1. Go to the rules directory:**

**cd rules**

****

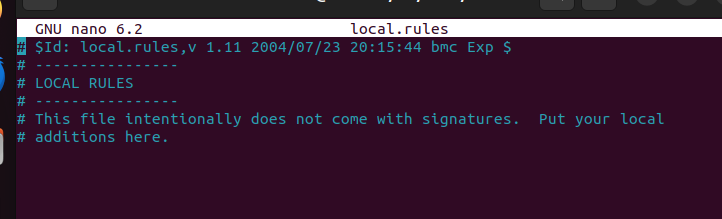
**2. List available rule files:**

**ls**

****

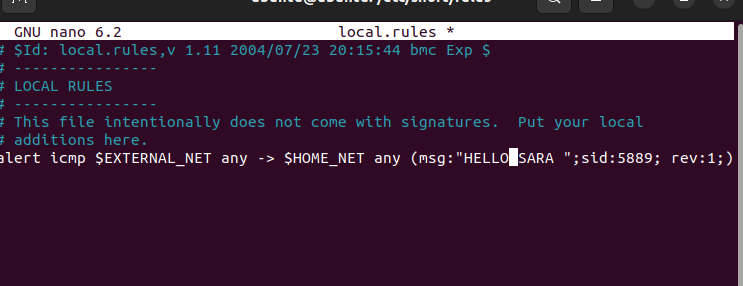
**3. Open local.rules for editing:**

**sudo nano local.rules**

****

**4. Add the following custom rules:**

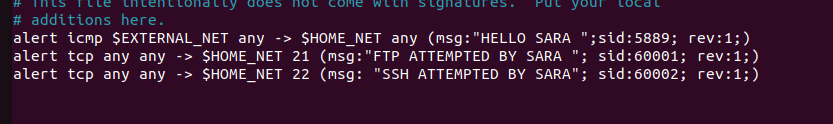
**alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"Hello World"; sid:5889; rev:1;)**

****

**alert tcp any any -> $HOME\_NET 21 (msg:"FTP Attempted"; sid:60001; rev:1;)**

**alert tcp any any -> $HOME\_NET 22 (msg:"SSH Attempted"; sid:60002; rev:1;)**

**5. Save the file (Ctrl + X, then Y, then Enter).**

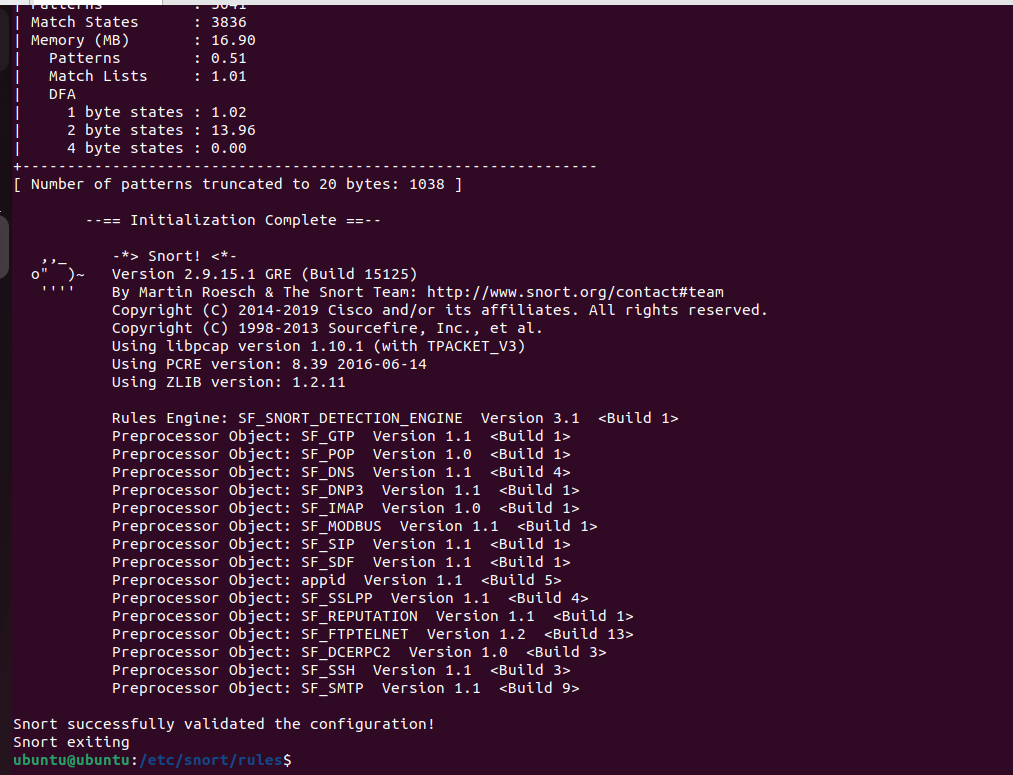
****

**Task 4: Testing Snort Configuration (4 Marks)**

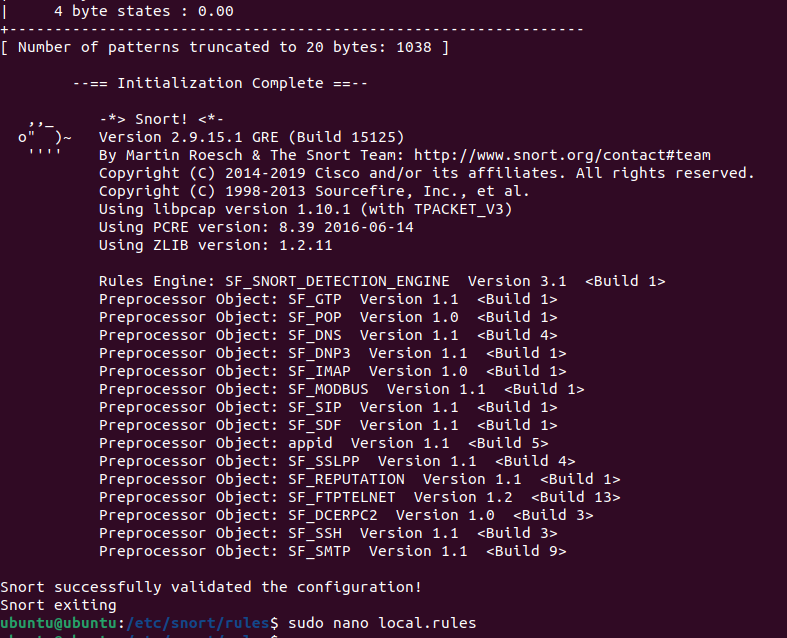
**1. Test Snort for configuration errors:**

**snort -T -c /etc/snort/snort.conf**

**For rule no 1**

****

**For all**

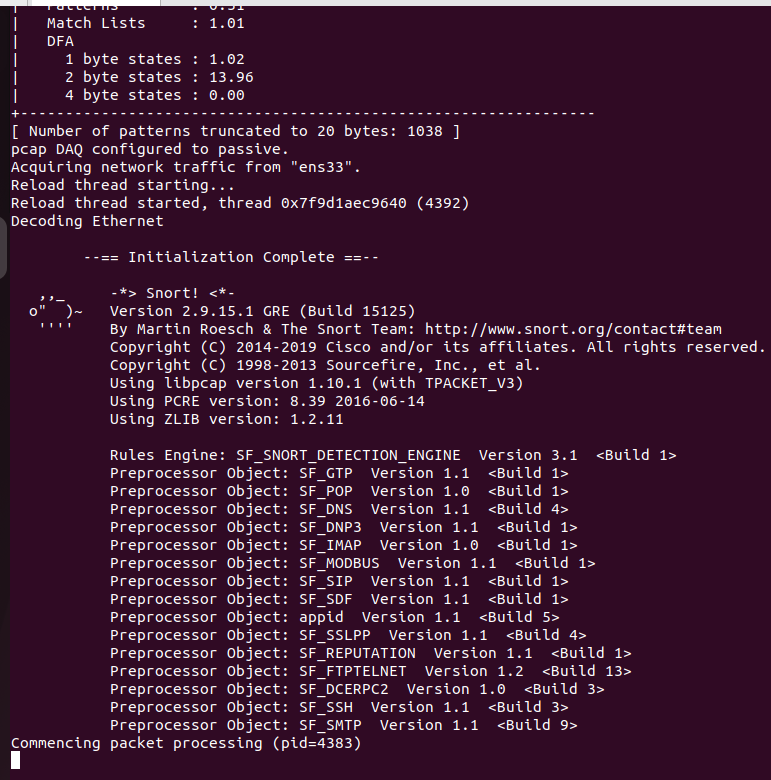
****

**o If there are errors, troubleshoot and fix them.**

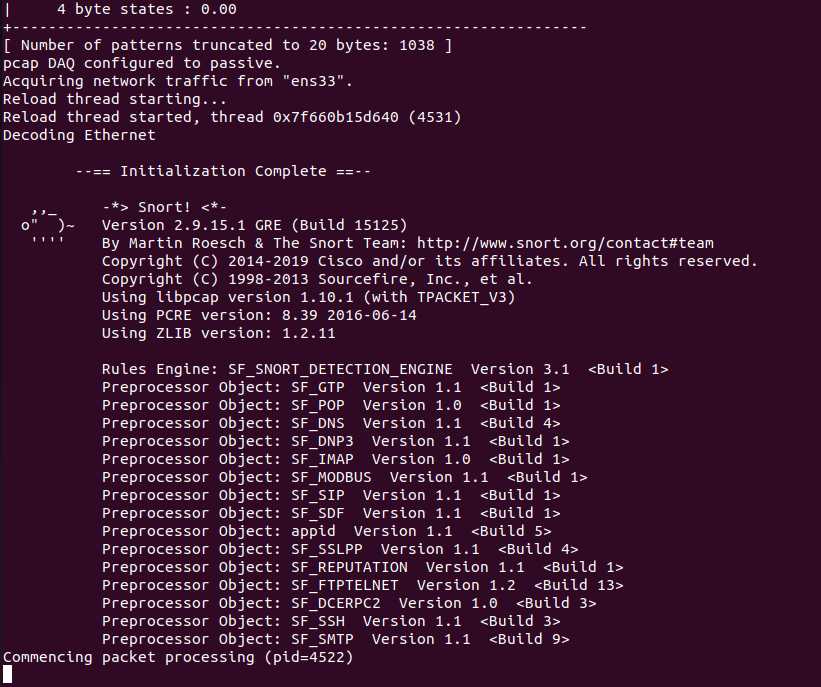
**2. Run Snort in alert mode (console output):**

**snort -A console -c /etc/snort/snort.conf**

**For rule no 1**

****

**For all**

****

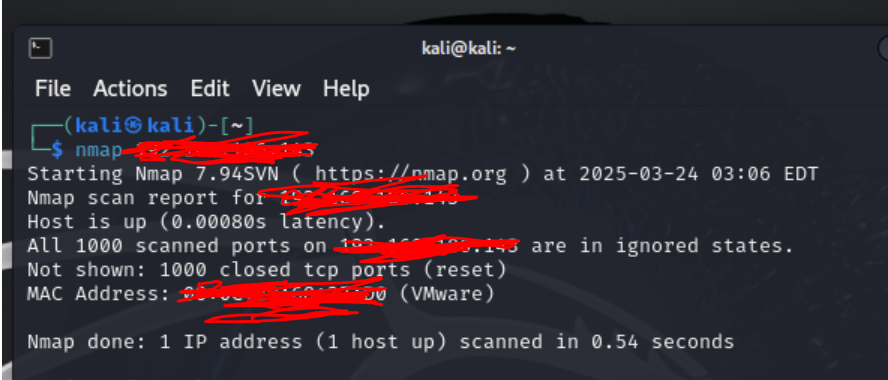
**Task 5: Attack Simulation and Detection (6 Marks)**

**1. On Linux (Attacker Machine), run the following tests:**

**o Scan the target machine using Nmap:**

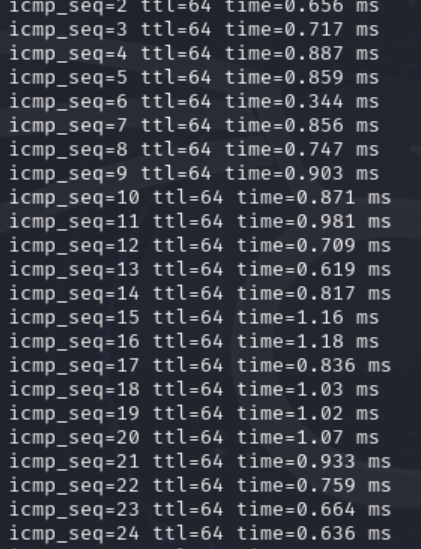
**nmap 192.168.18.131**

**For rule no 1**

****

**o Send ICMP (ping) request:**

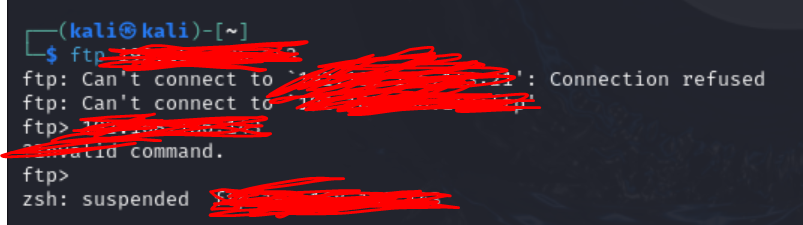
**For rule no 1**

****

**o Attempt an FTP connection:**

**ftp 192.168.18.131**

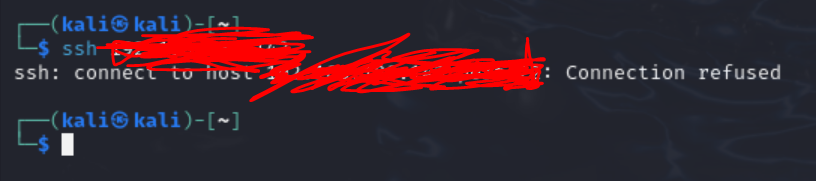
**For rule no 1**

****

**o Attempt an SSH connection:**

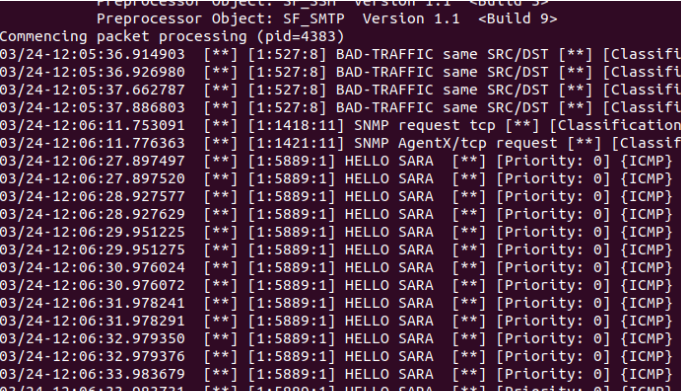
**ssh 192.168.18.131**

**For rule no 1**

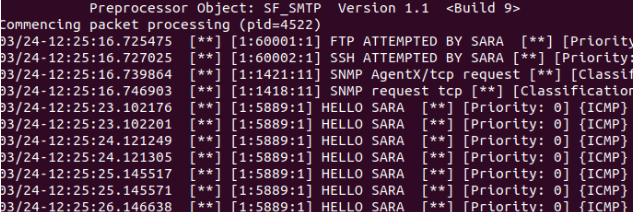
****

**2. Observe Snort console output for alerts related to the defined rules.**

**For rule no 1**

****

**For all**

****

**This lab ensures hands-on experience in Snort IDS installation, configuration, and attack simulation while following a structured sequence.**