Network Intrusion Detection & Prevention with Snort

1) Summary about the lab:

Role:

- You are responsible for monitoring, detecting, and preventing malicious network activities on an internal server using Snort IDS/IPS in a controlled environment with an attacker machine.

Environment:

- Defender VM: Cybersec-Server (Snort installed)
- Attacker VM: Cybersec-Attacker
- Network: Internal subnet 10.0.2.0/24
- Tool: Snort (IDS & IPS modes)

Task 1: Baseline IDS Configuration & ICMP Detection

Scenario

Unmonitored ICMP traffic may indicate **network scanning or reconnaissance**. You are tasked with ensuring that all ICMP packets are detected and logged.

Requirements to Achieve

- Configure Snort to correctly identify the **protected internal network**
- Modify HOME_NET to the local subnet (10.0.2.0/24)
- Verify Snort installation and version
- Create a **custom ICMP alert rule** in local.rules
- Assign a valid **SID (>1000000)** and revision number
- Restart Snort without configuration errors
- Trigger ICMP traffic from the attacker (ping)
- Confirm alerts are generated and logged in /var/log/snort

- Inspect alert and log files to validate detection

Task 2: Real-Time Detection Using IDS Console Mode

Scenario

Security operations require **real-time visibility** of threats. You must monitor live traffic and immediately detect suspicious ICMP activity.

Requirements to Achieve

- Run Snort in **IDS console mode**
- Suppress banners and non-essential output
- Observe alerts printed directly to the terminal
- Generate ICMP traffic from attacker VM
- Confirm alerts appear in real time
- Demonstrate ability to stop monitoring safely

Task 3: Detecting Unauthorized Web Access Attempts

Scenario

The server hosts a web service that should be monitored for **unauthorized access attempts**.

Requirements to Achieve

- Write a Snort rule to detect **HTTP/web traffic** to the server
- Target the correct **destination IP and port**
- Restart Snort and validate rule syntax
- Access the web server from the attacker VM
- Confirm alerts are generated in the Snort alert file
- Verify detection using log inspection

Task 4: Detecting ICMP Source Quench Attacks

Scenario

An attacker attempts to exploit **ICMP Source Quench packets**, a known attack technique used to manipulate traffic flow.

Requirements to Achieve

- Understand ICMP **type and code fields**
- Write a Snort rule specifically matching:
    - ICMP Type 4 (Source Quench)
    - ICMP Code 0
- Assign a unique SID and revision
- Restart Snort successfully
- Launch a Source Quench attack using **Netwag**
- Trigger traffic from the client VM
- Confirm alerts are generated for the attack

Task 5: Active Defense – Blocking SSH Attacks (IPS Mode)

Scenario

The attacker attempts to gain **remote shell access** via SSH. Detection alone is not enough , so the connection must be blocked.

Requirements to Achieve

- Configure Snort to run in **Intrusion Prevention System (IPS) mode**
- Write a rule using the **reject** action
- Target SSH traffic on **TCP port 22**
- Restart Snort and confirm IPS functionality
- Attempt SSH login from attacker VM
- Verify:
    - Alert is generated
    - SSH connection is **successfully blocked**

Task 6: Detecting & Blocking Telnet Connections

Scenario

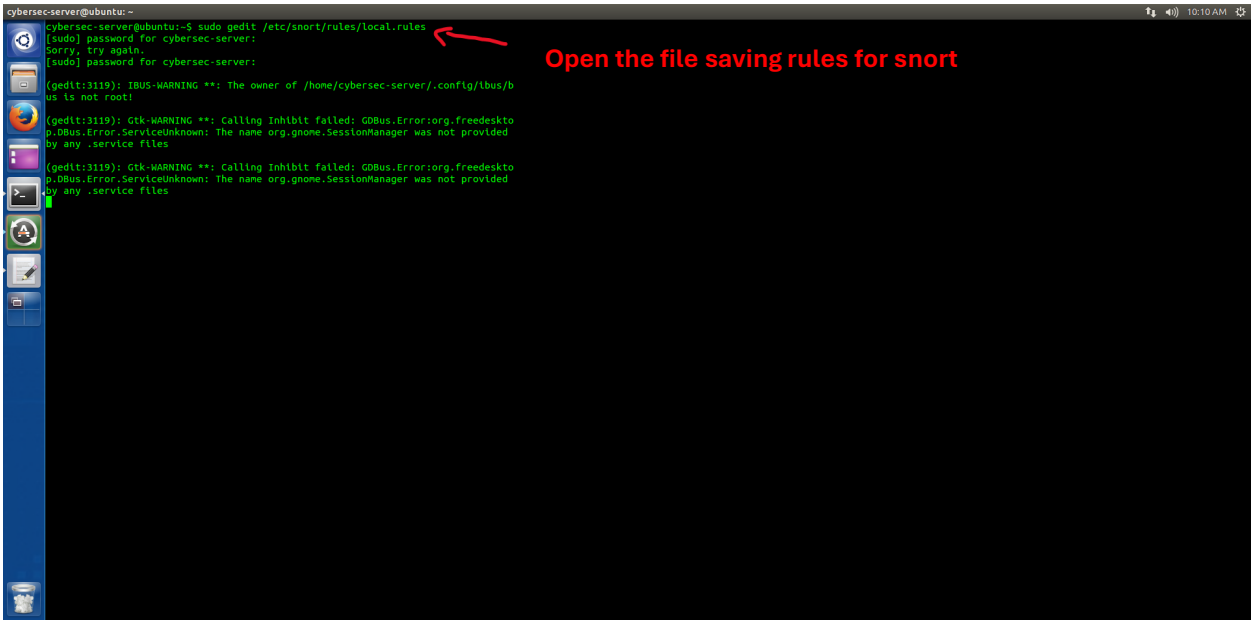
Telnet is insecure and should never be allowed. You must both **detect and prevent** Telnet access attempts.

Requirements to Achieve

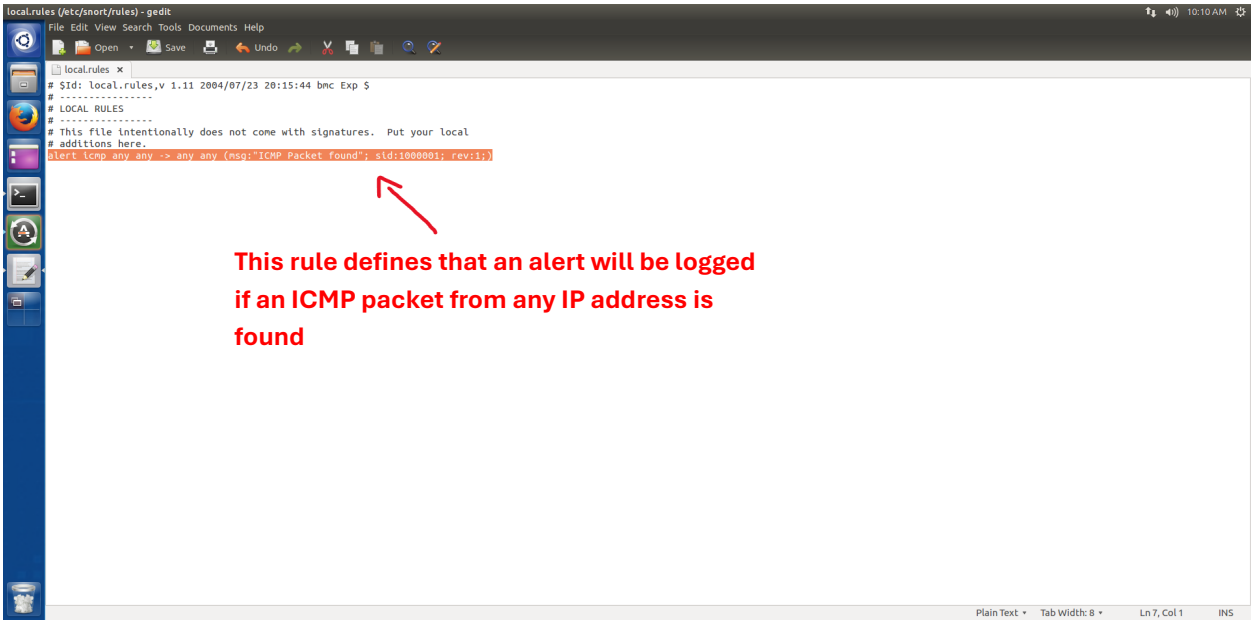
- Identify Telnet protocol characteristics:
    - TCP-based
    - Runs on **port 23**
- Create custom Snort rules to:
    - Generate alerts for Telnet attempts
    - Reject Telnet connections
- Restart Snort and validate rule syntax
- Attempt Telnet connection from attacker VM
- Confirm:
    - Alert is logged
    - Connection attempt fails
- Clearly document the rule used

2) Step-by-step solution for each task:

Task 1: Adding a Rule for ICMP packets

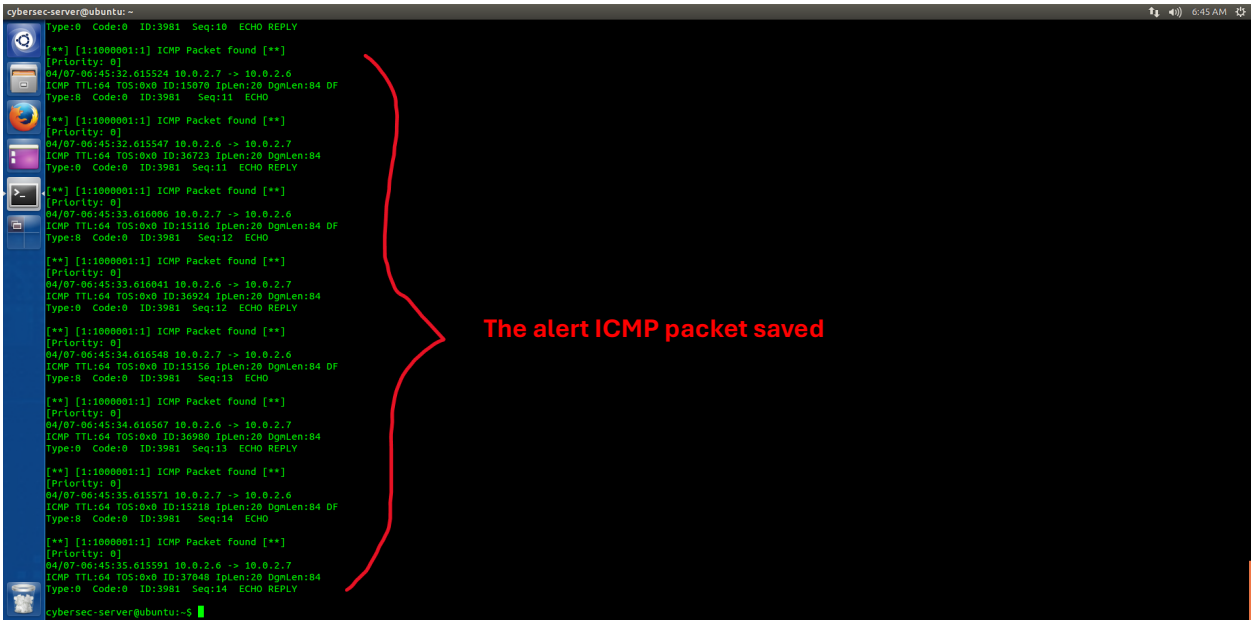


Inside the rules file:

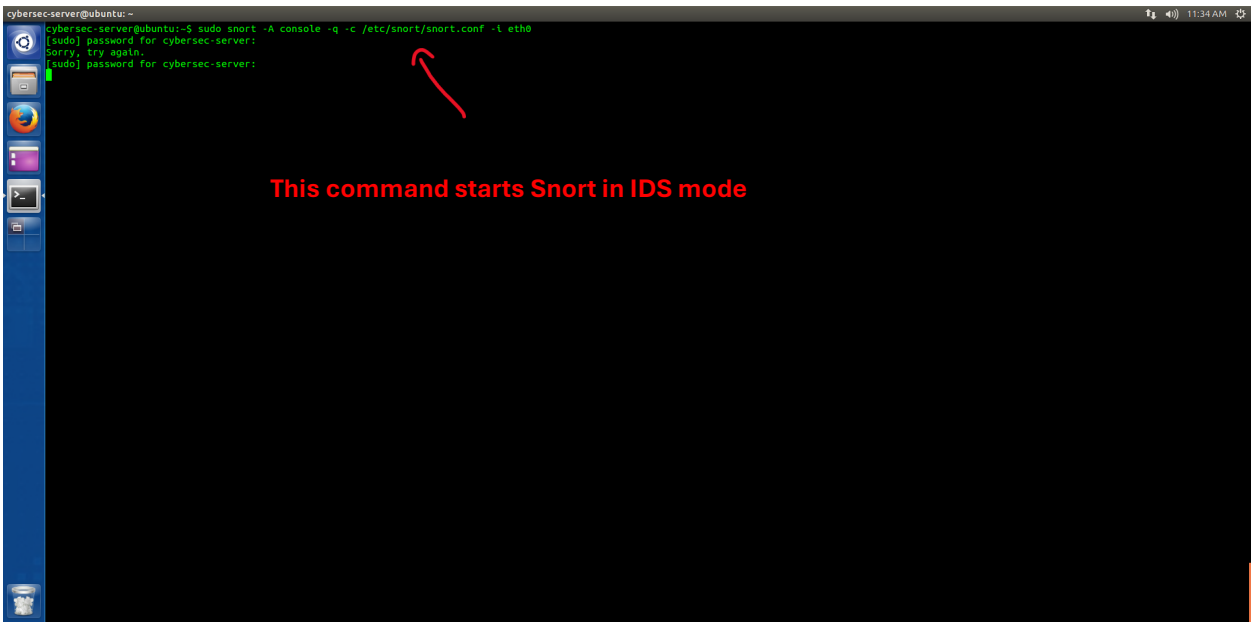


*The sid value is greater than 1000000 means that an self-defined rule by the users.

Ping the server from the attacker to trigger the alert for the new rule:

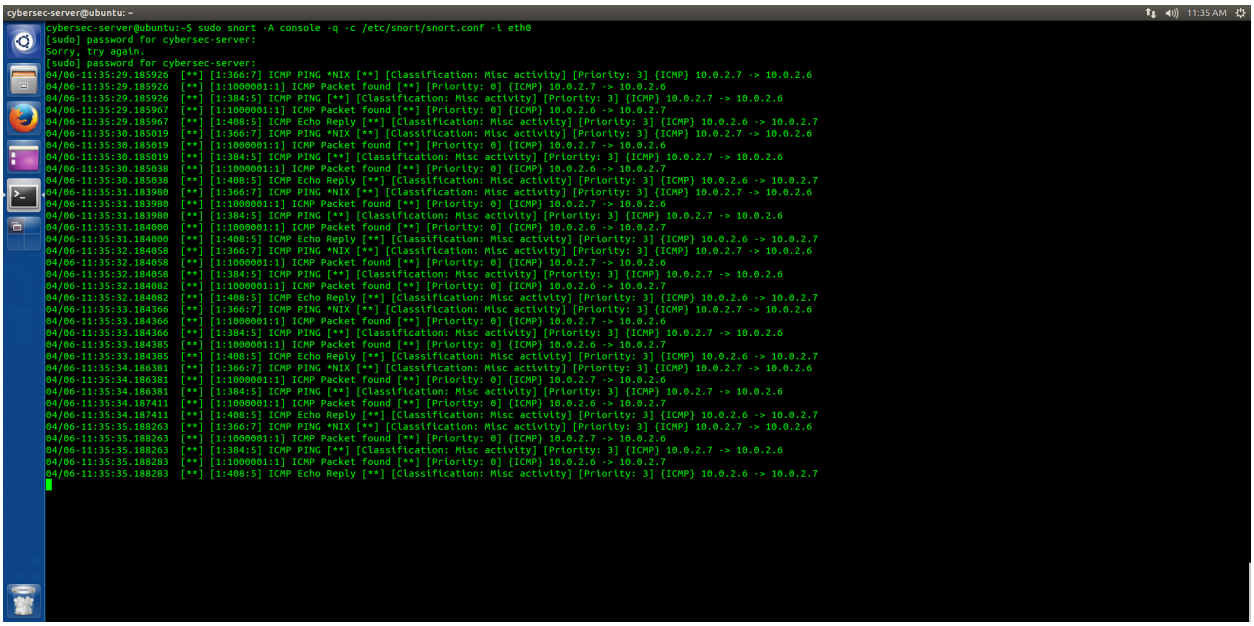


Task 2: Snort in IDS mode and displaying alerts to the console



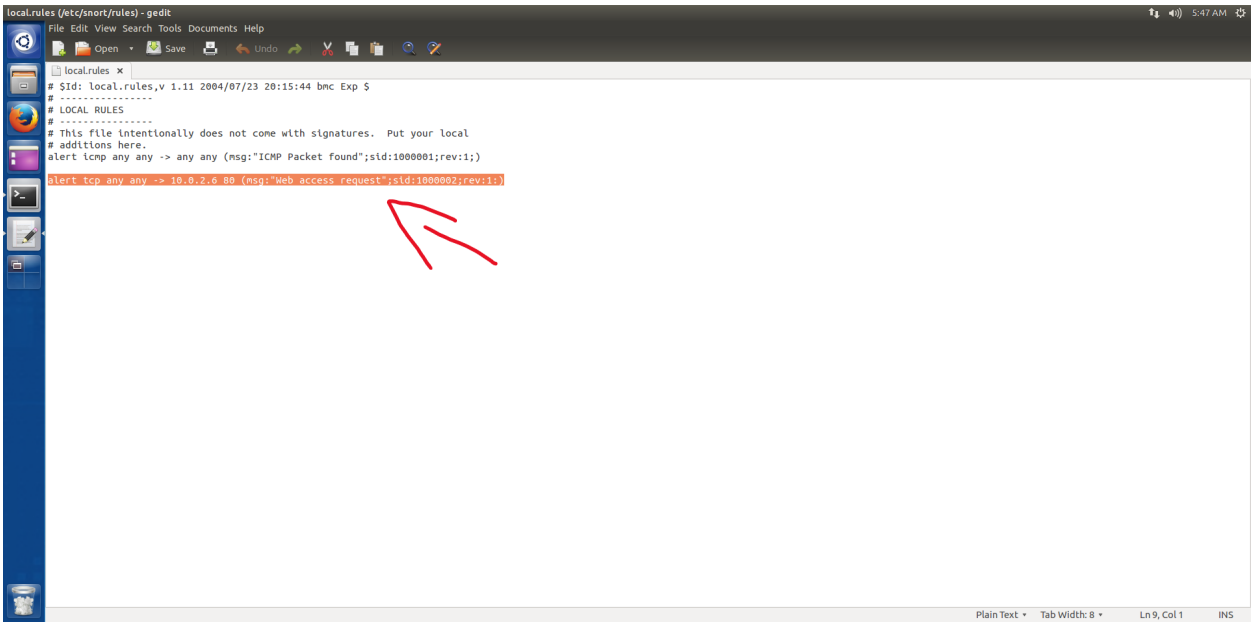
Ping the server from attacker

The alert messages displayed in the IDS mode

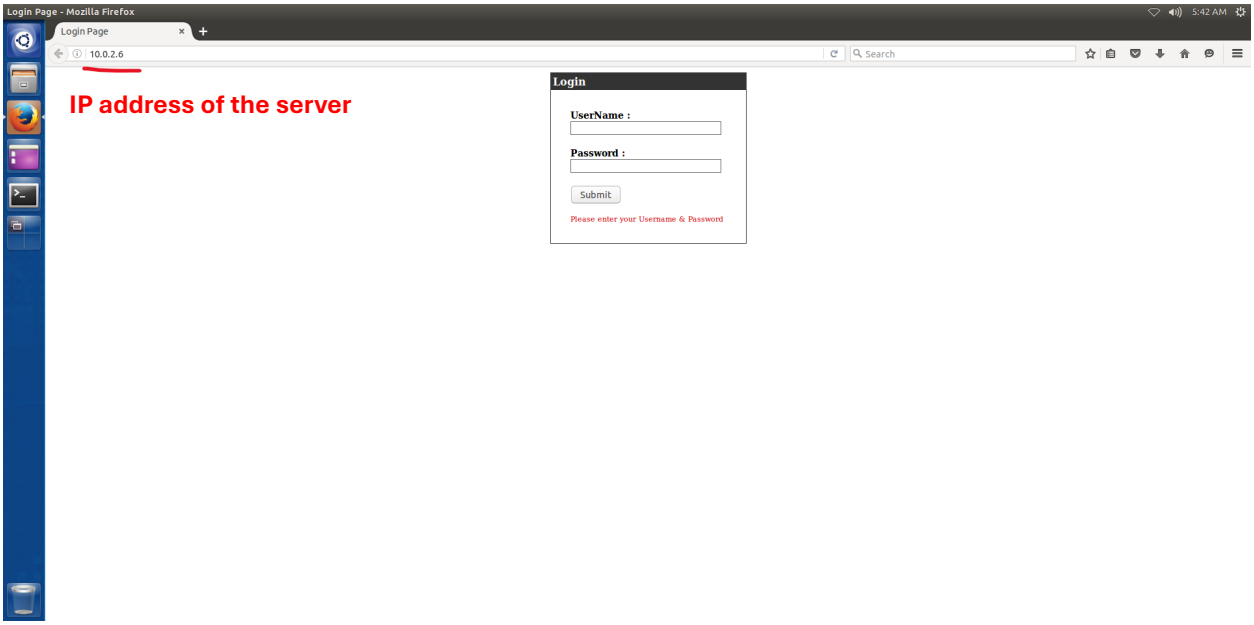


Task 3: Generating alert for web service

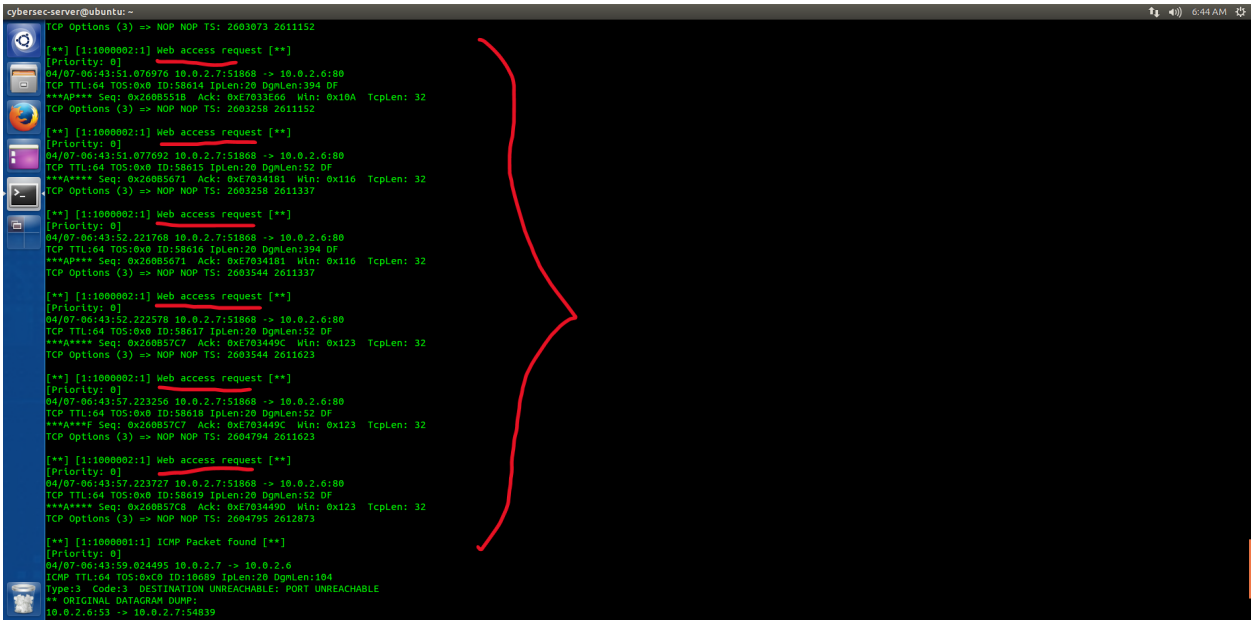
Add the rule to alert the tcp connection from browsers to the server:



Open the browser and access the server

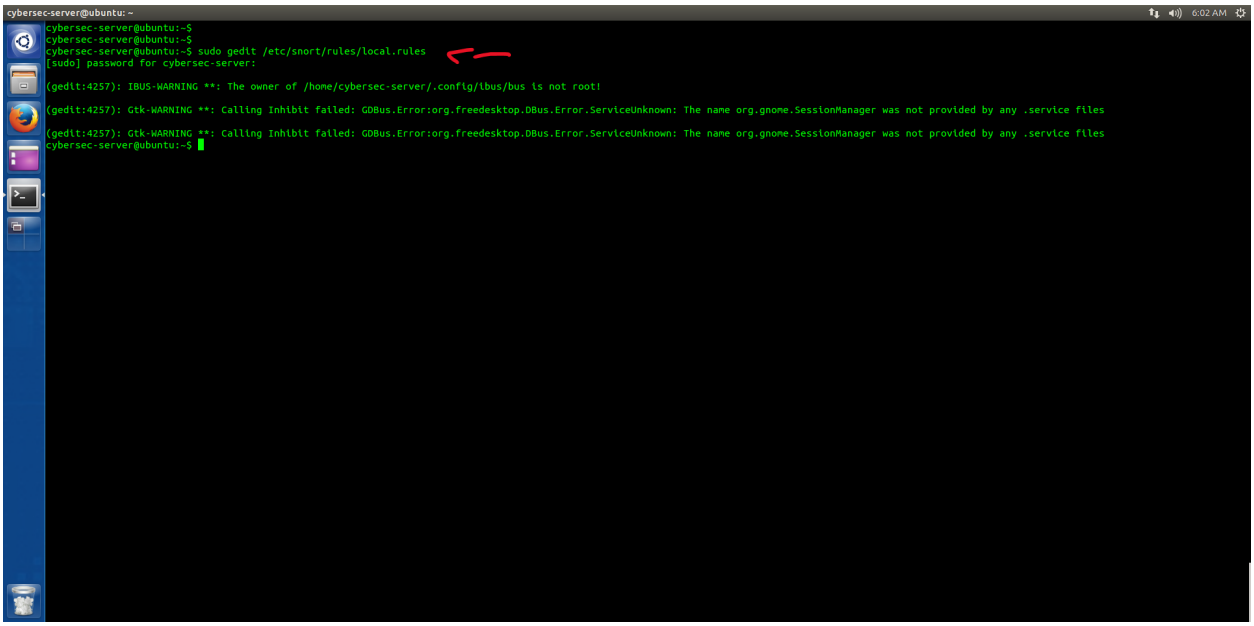


Alert “Web access request” are logged:

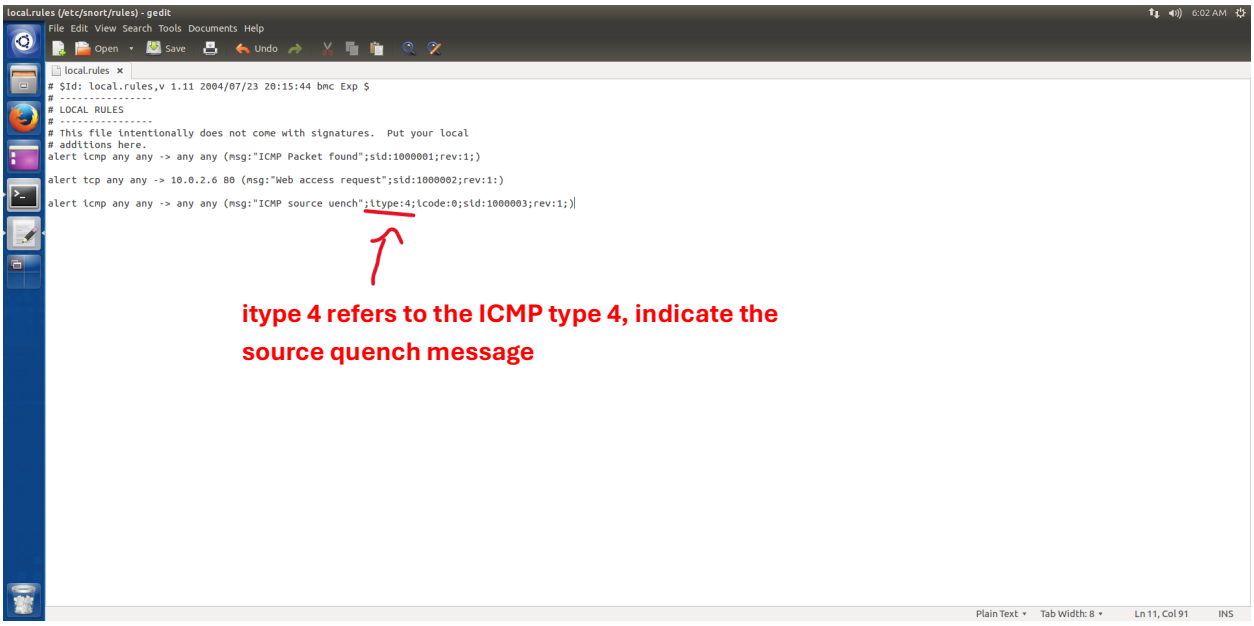


Task 4: Generating alerts for ICMP source quench packets:

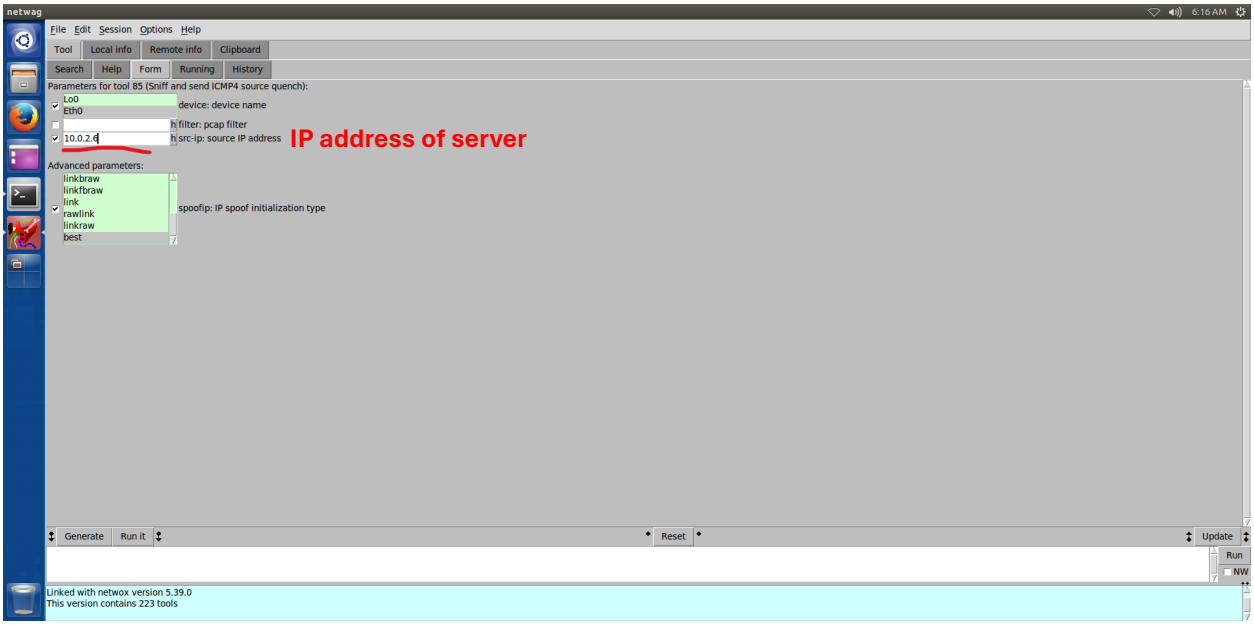
Open the rules file:



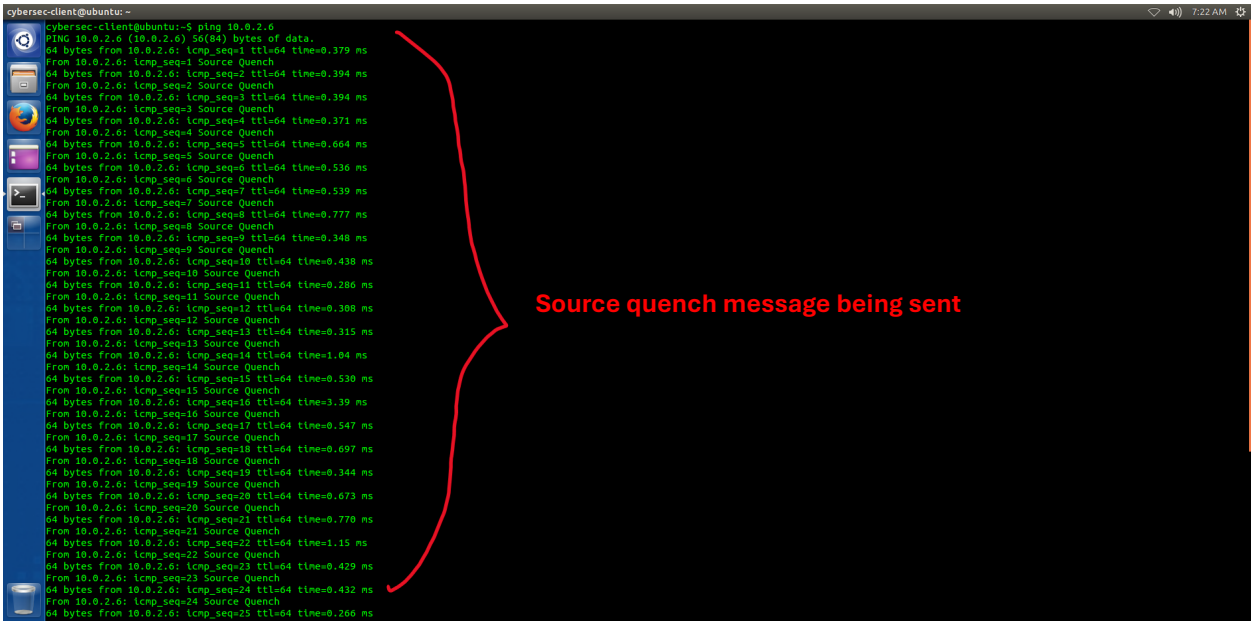
The alert command for ICMP Source Quench Packets

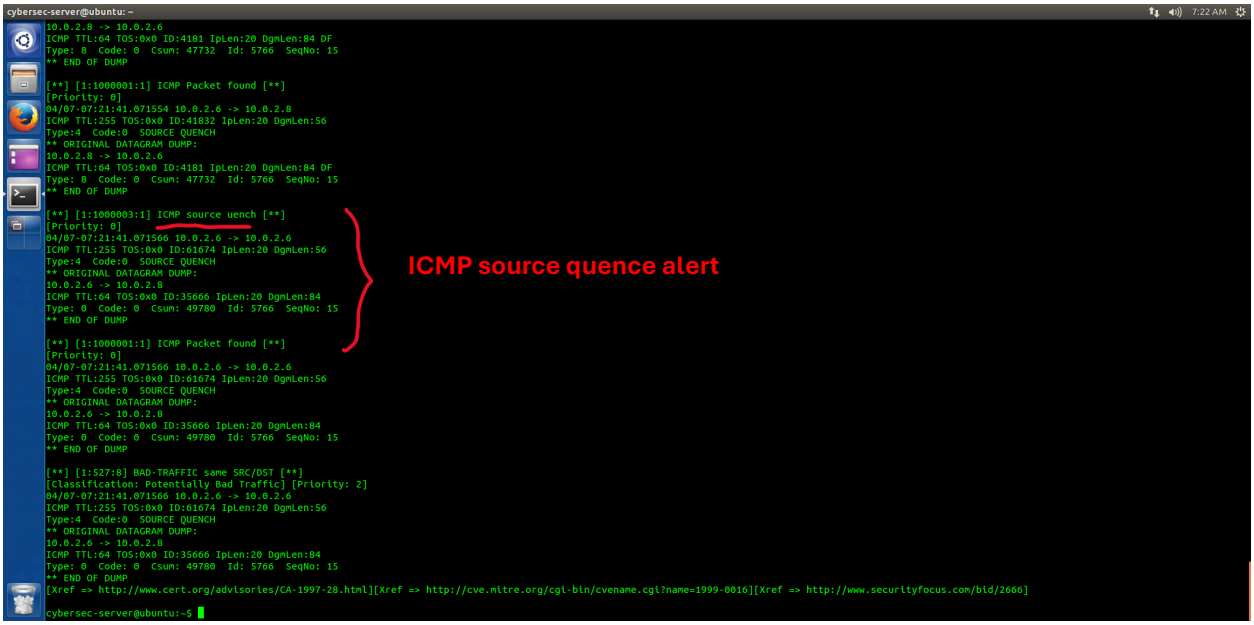


Using netwag to send ICMP source quench message



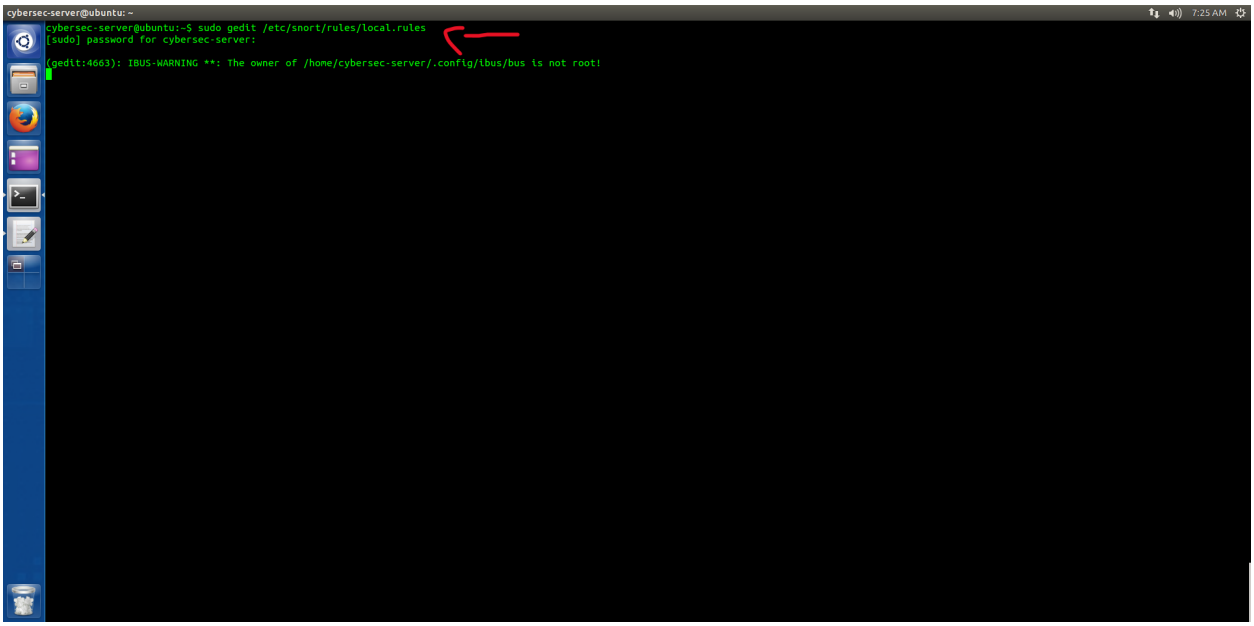
Ping the server from the client



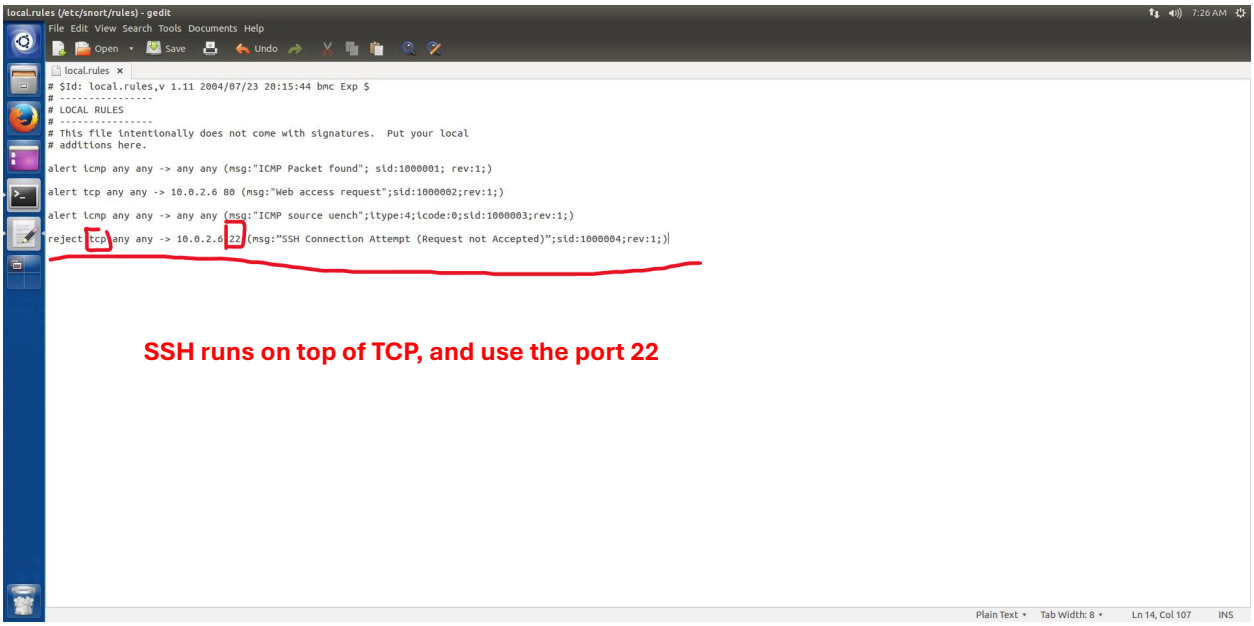


Task 5: Running Snort as Intrusion Prevention System

Open the rules file

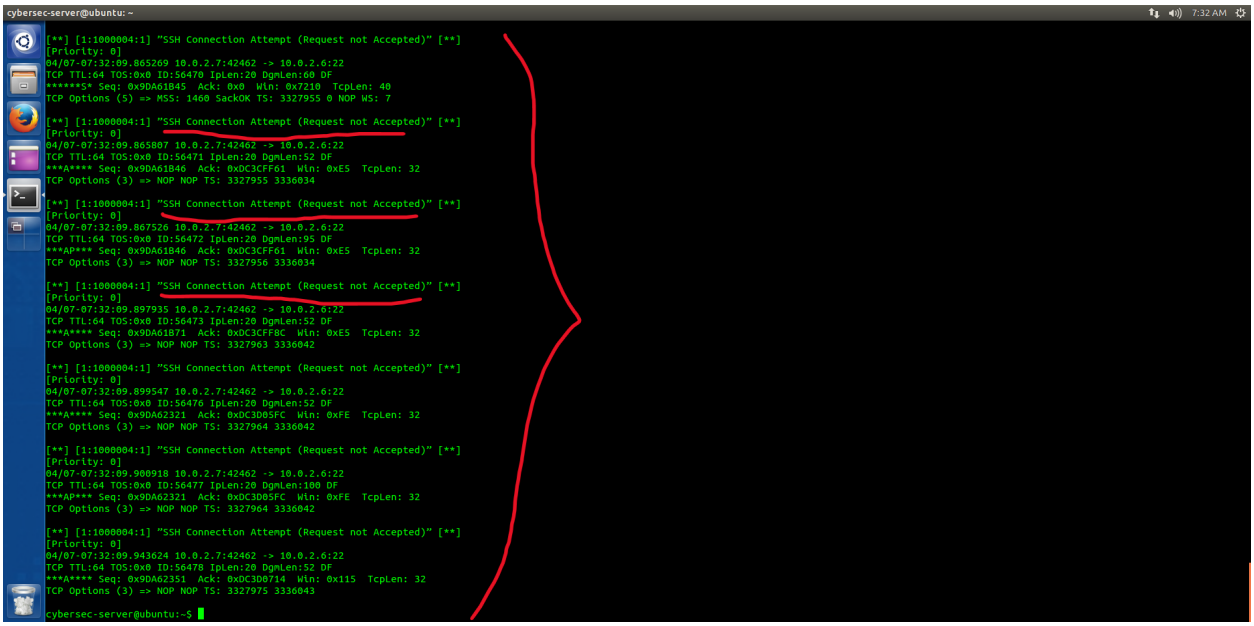


The reject rule for SSH connection being added



Establish SSH connection from the attacker

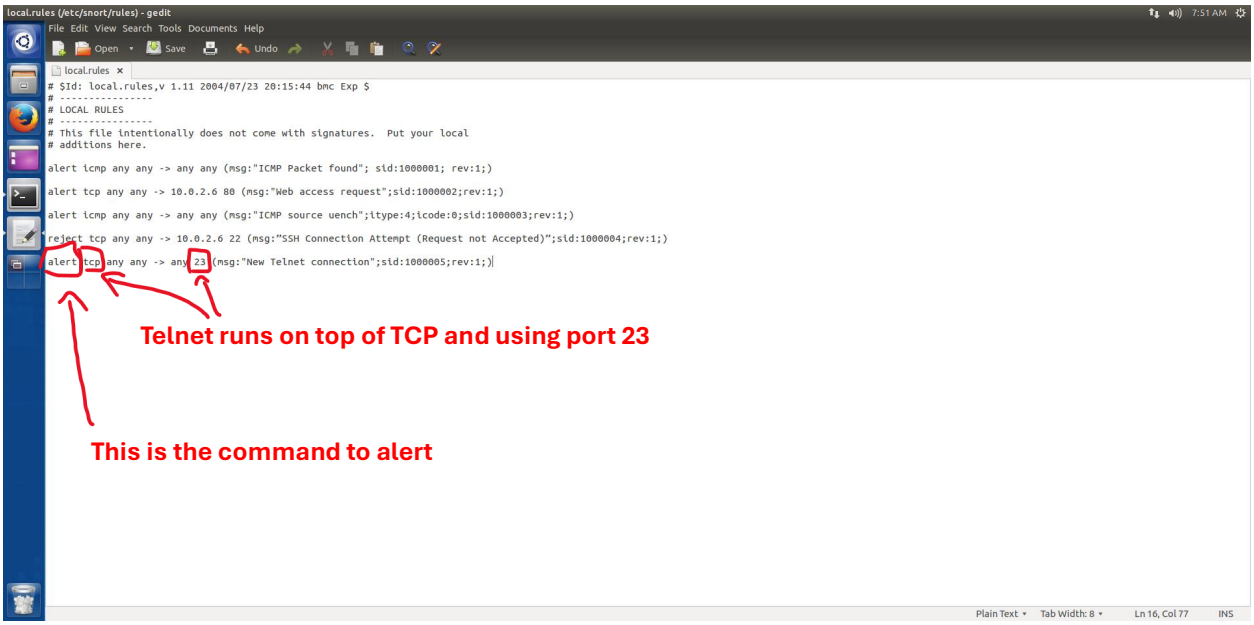
The alerts messages for SSH connection attempt:



*The connection attempts were unsuccessful

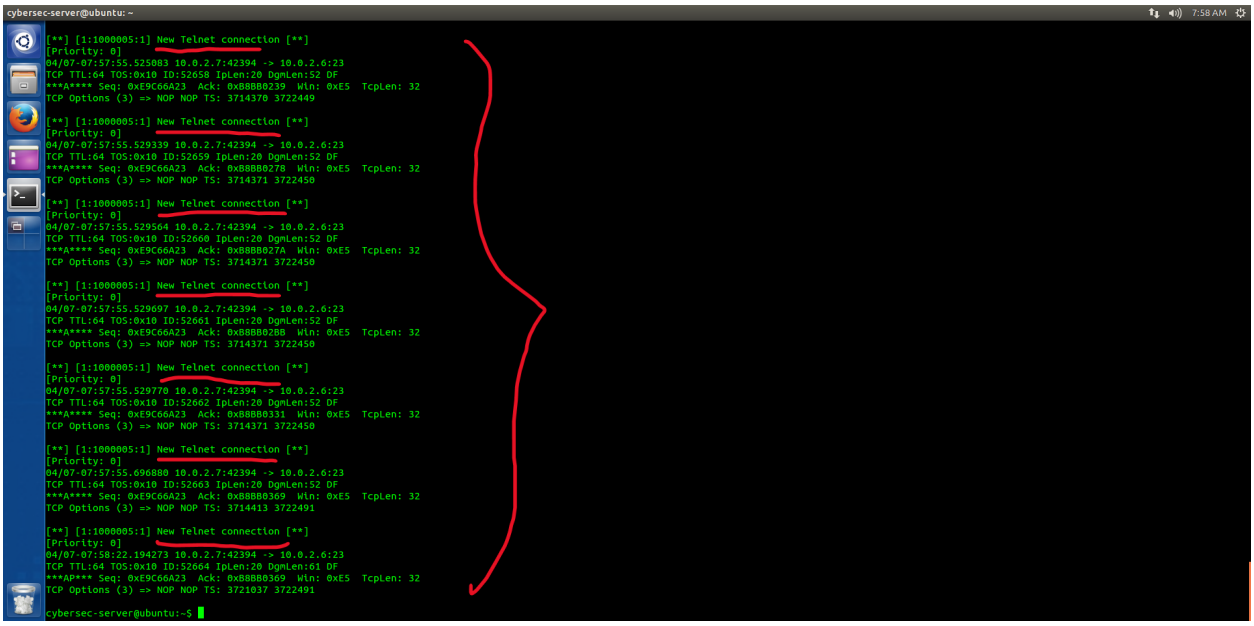
Task 6: Generate Alerts for Telnet connection attempts from Attacker to Server and Reject Telnet connection attempts from Attacker to Server.

1) Alert:



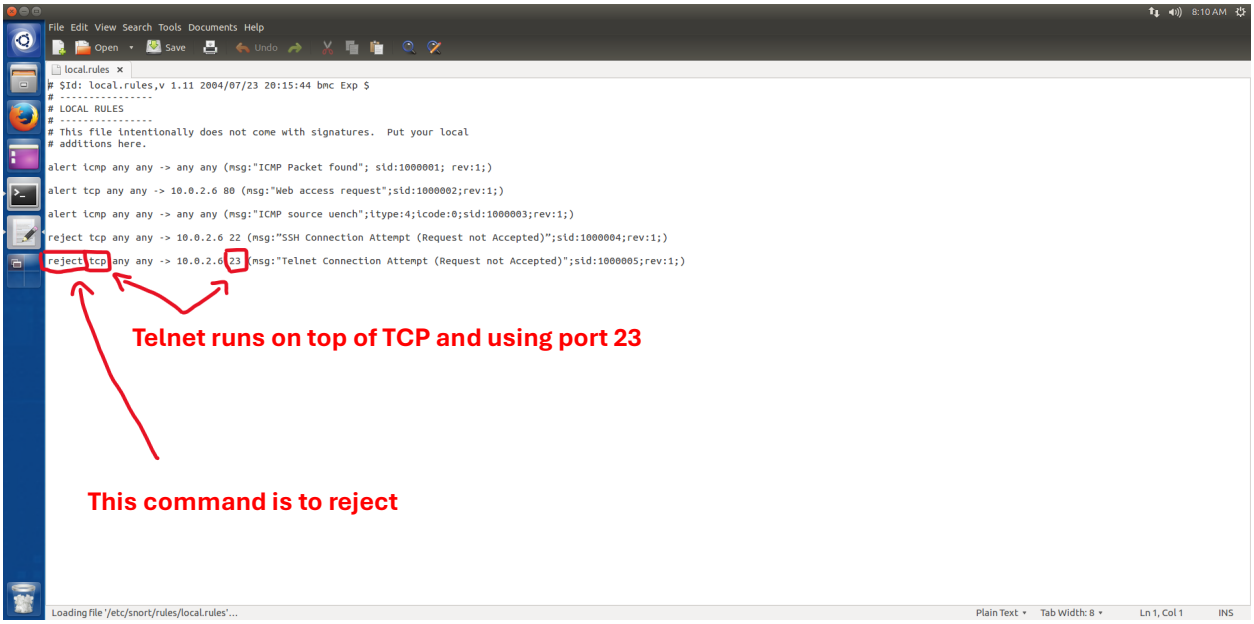
Establish telnet connection from the server

Alert messages showed in the alert file of the server:

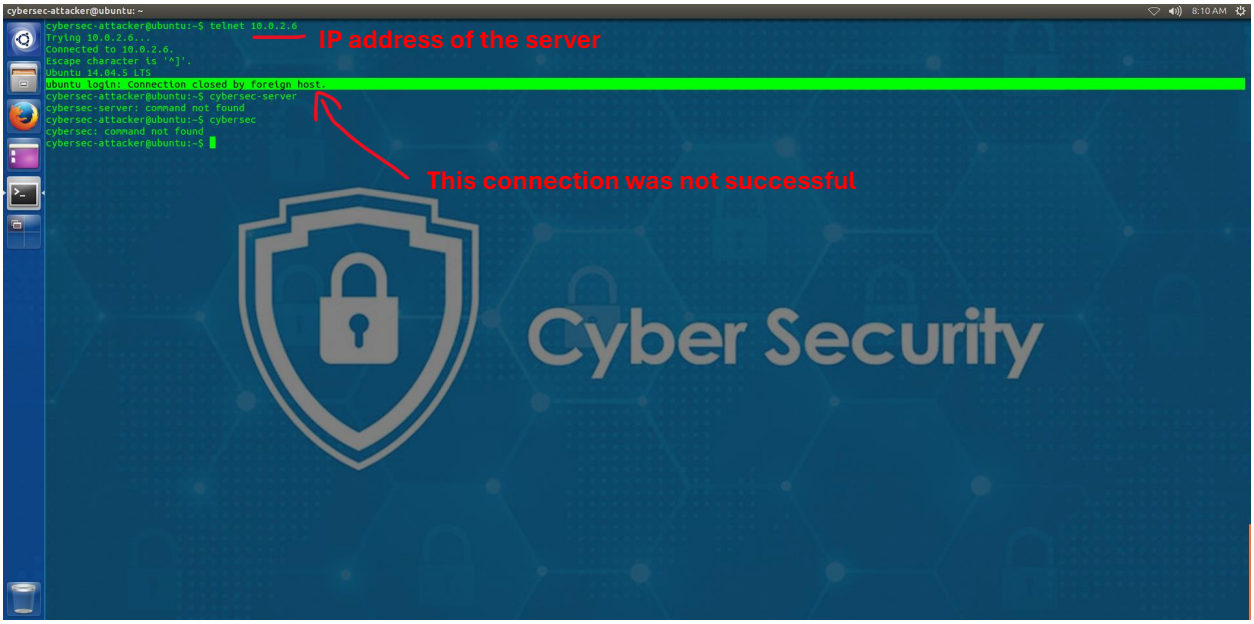


In this case, the telnet connection is established successfully.

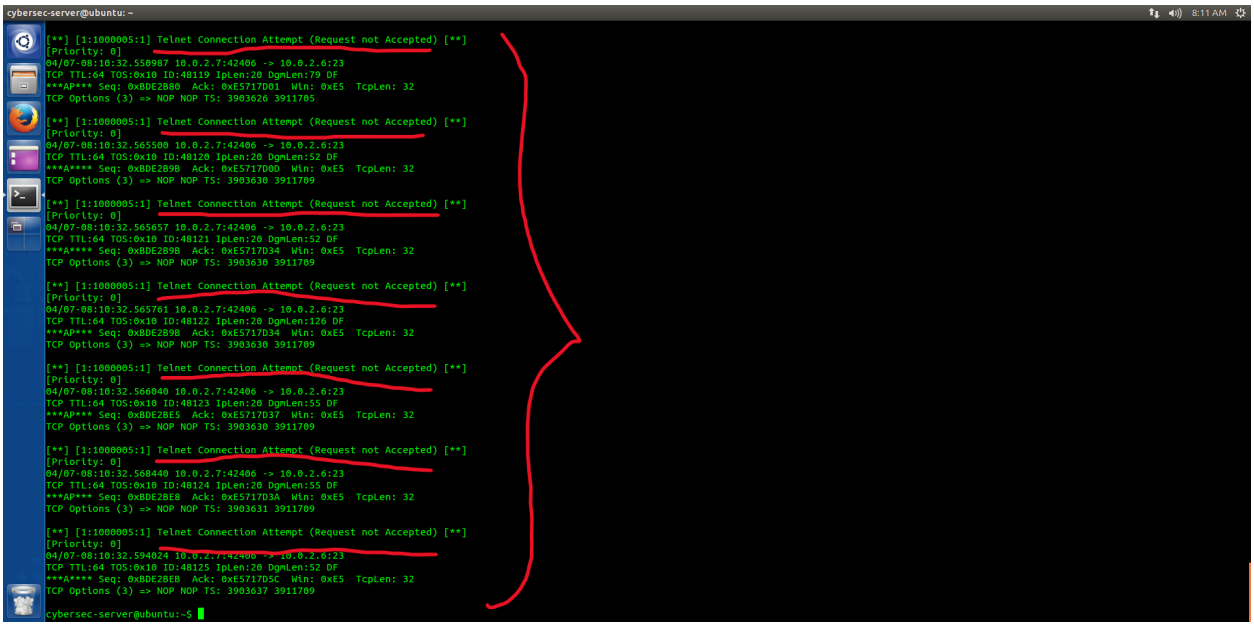
2) Reject



Establish telnet connection from the attacker:



The alerts being logged:



In this case, the telnet connection was rejected so not established successfully