

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

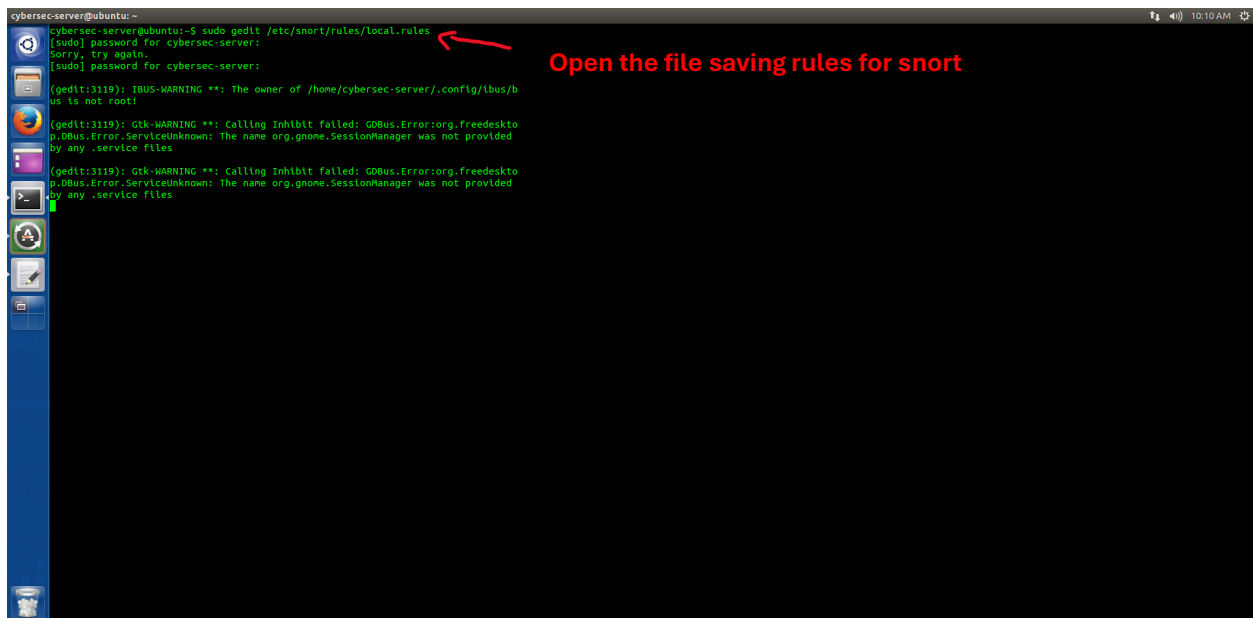
Telnet is insecure and should never be allowed. You must both **detect and prevent** Telnet access attempts.

Requirements to Achieve

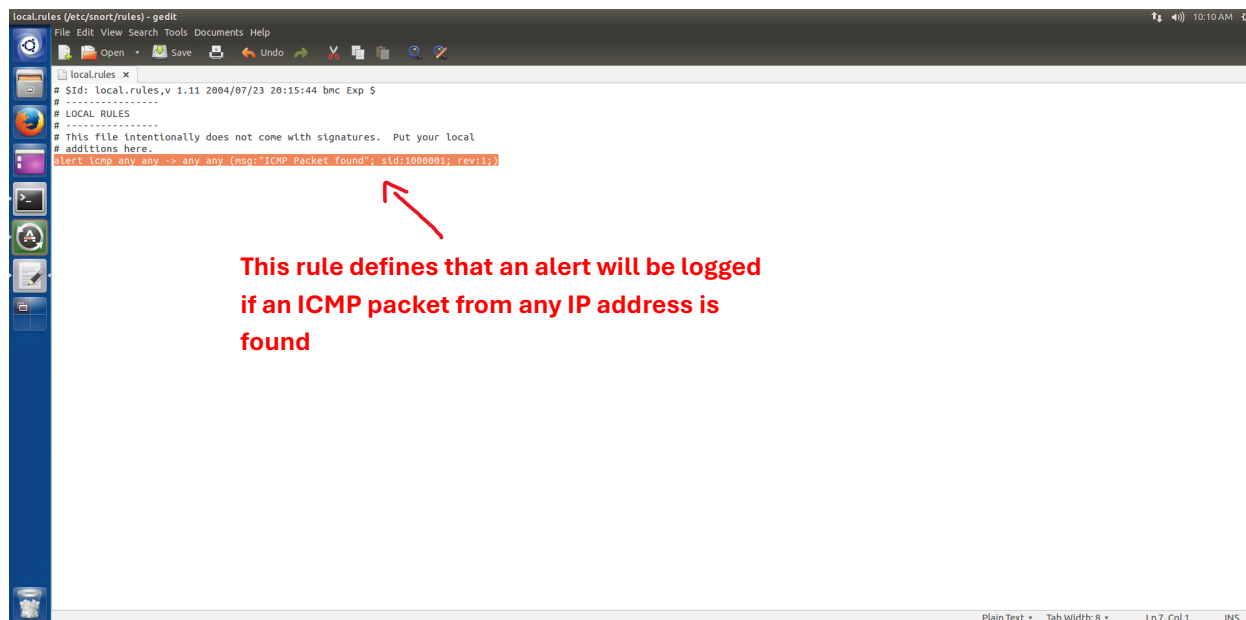
- Identify Telnet protocol characteristics:
 - TCP-based
 - Runs on **port 23**
- Create custom Snort rules to:
 - Generate alerts for Telnet attempts
 - Reject Telnet connections
- Restart Snort and validate rule syntax
- Attempt Telnet connection from attacker VM
- Confirm:
 - Alert is logged
 - Connection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



```
local.rules (/etc/snort/rules) - gedit
# Sid: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any -> any any (msg:'ICMP Packet found'; sid:1000001; rev:1)
```

This rule defines that an alert will be logged if an ICMP packet from any IP address is found

*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:



```
cybersec-attacker@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data:
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.661 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.661 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.745 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.381 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.323 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.128 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.241 ms
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.327 ms
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.352 ms
```

Cyber Security

Ping the server from attacker

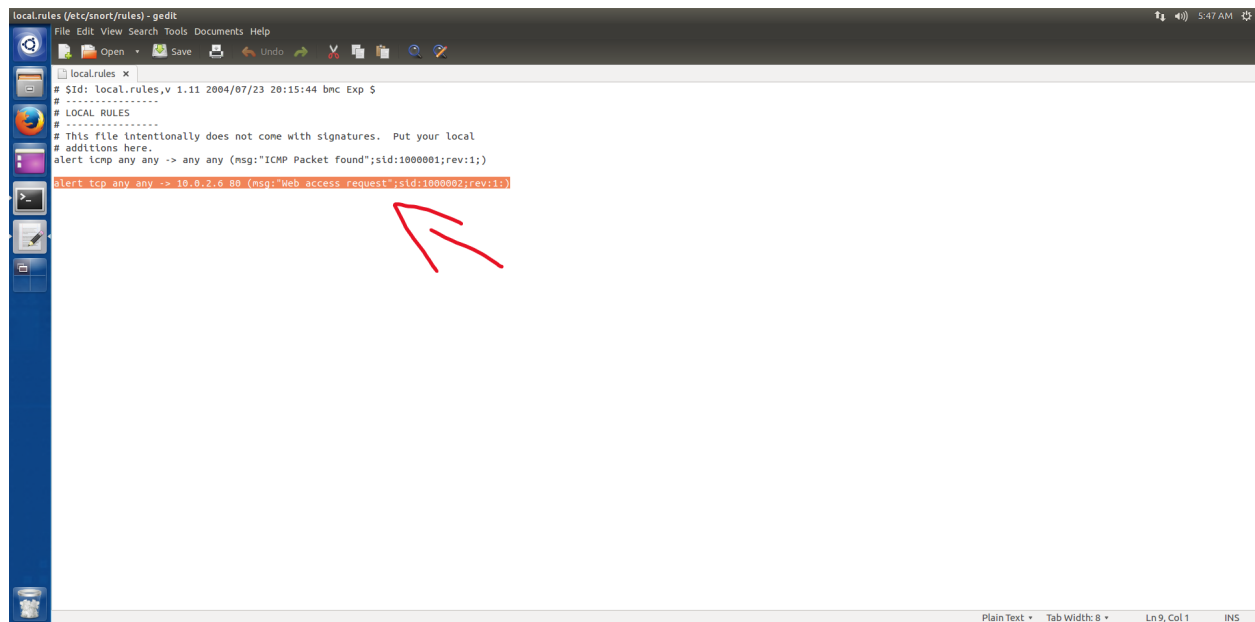
```
cybersec-attacker@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data:
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.377 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.461 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.372 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=1.18 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.379 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=4.06 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=3.04 ms
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.268 ms
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.268 ms
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=0.365 ms
64 bytes from 10.0.2.6: icmp_seq=11 ttl=64 time=0.321 ms
64 bytes from 10.0.2.6: icmp_seq=12 ttl=64 time=0.292 ms
64 bytes from 10.0.2.6: icmp_seq=13 ttl=64 time=0.447 ms
64 bytes from 10.0.2.6: icmp_seq=14 ttl=64 time=0.394 ms
64 bytes from 10.0.2.6: icmp_seq=15 ttl=64 time=0.375 ms
64 bytes from 10.0.2.6: icmp_seq=16 ttl=64 time=0.455 ms
64 bytes from 10.0.2.6: icmp_seq=17 ttl=64 time=0.262 ms
64 bytes from 10.0.2.6: icmp_seq=18 ttl=64 time=0.286 ms
64 bytes from 10.0.2.6: icmp_seq=19 ttl=64 time=0.311 ms
64 bytes from 10.0.2.6: icmp_seq=20 ttl=64 time=0.471 ms
64 bytes from 10.0.2.6: icmp_seq=21 ttl=64 time=0.336 ms
64 bytes from 10.0.2.6: icmp_seq=22 ttl=64 time=0.286 ms
64 bytes from 10.0.2.6: icmp_seq=23 ttl=64 time=0.311 ms
64 bytes from 10.0.2.6: icmp_seq=24 ttl=64 time=0.311 ms
64 bytes from 10.0.2.6: icmp_seq=25 ttl=64 time=0.311 ms
```

The alert messages displayed in the IDS mode

```
cybersec-server@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
[sudo] password for cybersec-server:
Sorry, try again.
[sudo] password for cybersec-server:
04/06-11:35:29.185926 ** [1:366:7] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:29.185926 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:29.185926 ** [1:384:5] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:29.185967 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:29.185967 ** [1:408:5] ICMP Echo Reply ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:30.185019 ** [1:366:7] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:30.185019 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:30.185019 ** [1:384:5] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:30.185038 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:30.185038 ** [1:408:5] ICMP Echo Reply ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:31.183980 ** [1:366:7] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:31.183980 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:31.183980 ** [1:384:5] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:31.184000 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:31.184000 ** [1:408:5] ICMP Echo Reply ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:32.184058 ** [1:366:7] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:32.184058 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:32.184058 ** [1:384:5] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:32.184082 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:32.184082 ** [1:408:5] ICMP Echo Reply ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:33.184366 ** [1:366:7] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:33.184366 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:33.184366 ** [1:384:5] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:33.184385 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:33.184385 ** [1:408:5] ICMP Echo Reply ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:34.186381 ** [1:366:7] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:34.186381 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:34.186381 ** [1:384:5] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:34.187411 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:34.187411 ** [1:408:5] ICMP Echo Reply ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:35.188263 ** [1:366:7] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:35.188263 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:35.188263 ** [1:384:5] ICMP PING *NIX ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.7 -> 10.0.2.6
04/06-11:35:35.188283 ** [1:1000001:1] ICMP Packet found ** [Priority: 0] (ICMP) 10.0.2.6 -> 10.0.2.7
04/06-11:35:35.188283 ** [1:408:5] ICMP Echo Reply ** [Classification: MISC activity] [Priority: 3] (ICMP) 10.0.2.6 -> 10.0.2.7
```

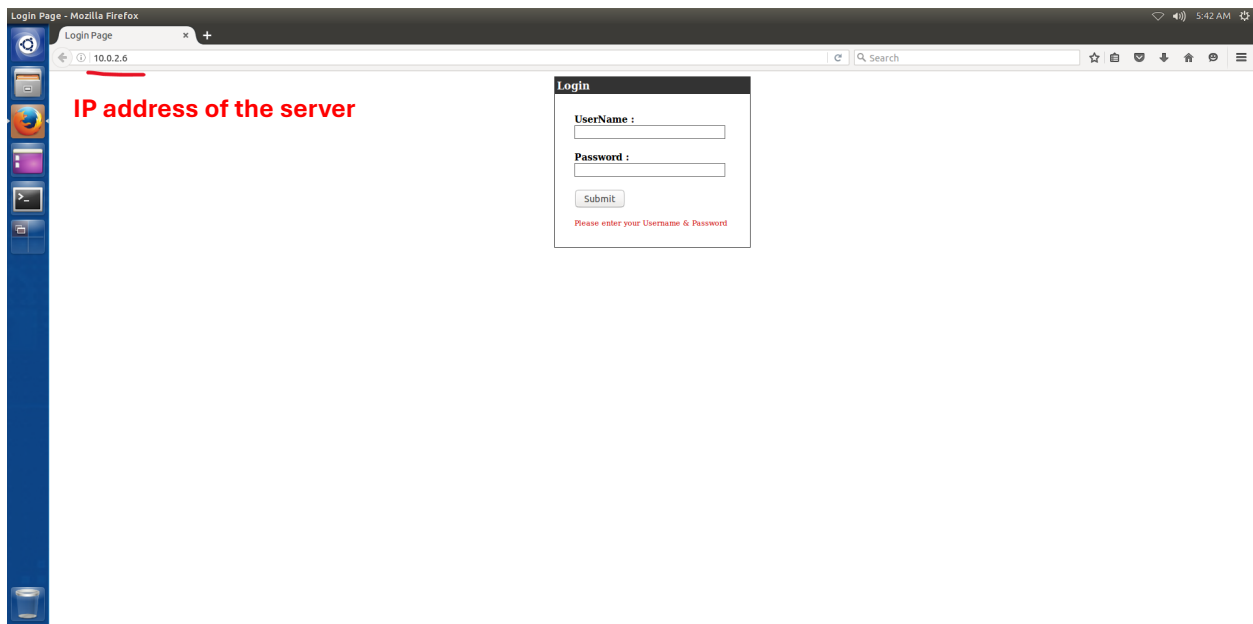
Task 3: Generating alert for web service

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

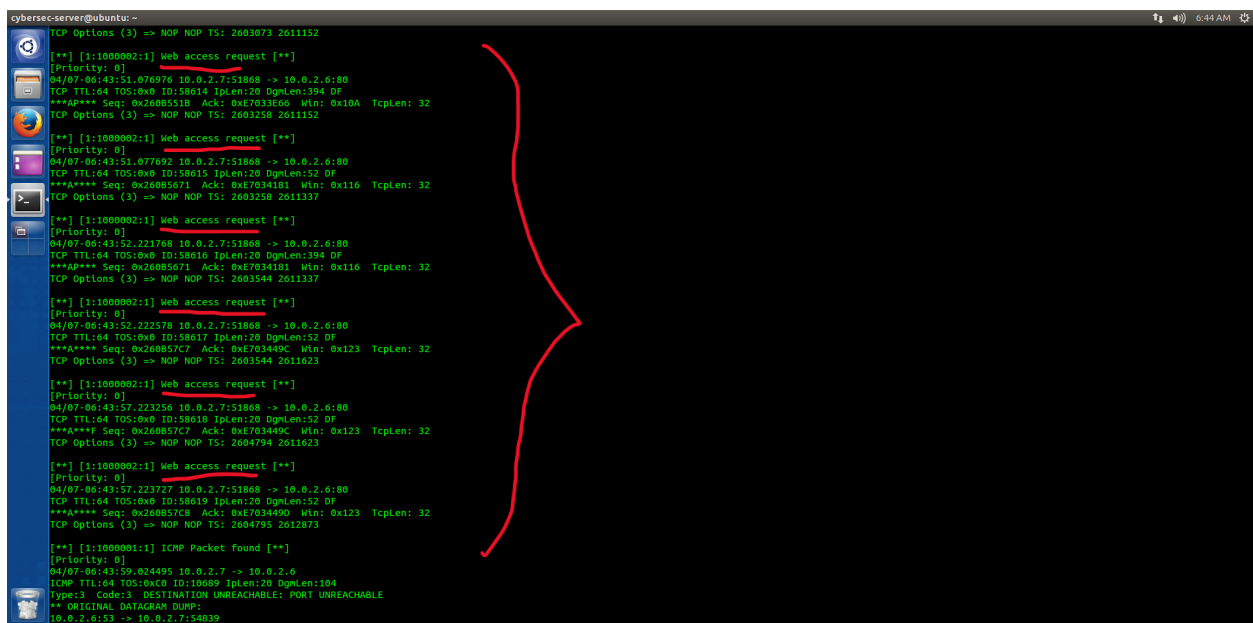


```
local.rules (/etc/snort/rules) - gedit
File Edit View Search Tools Documents Help
local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> any any (msg:"ICMP Packet found";sid:1000001;rev:1;)
alert tcp any any -> 10.0.2.6 80 (msg:'Web access request';sid:1000002;rev:1;)
```

Open the browser and access the server

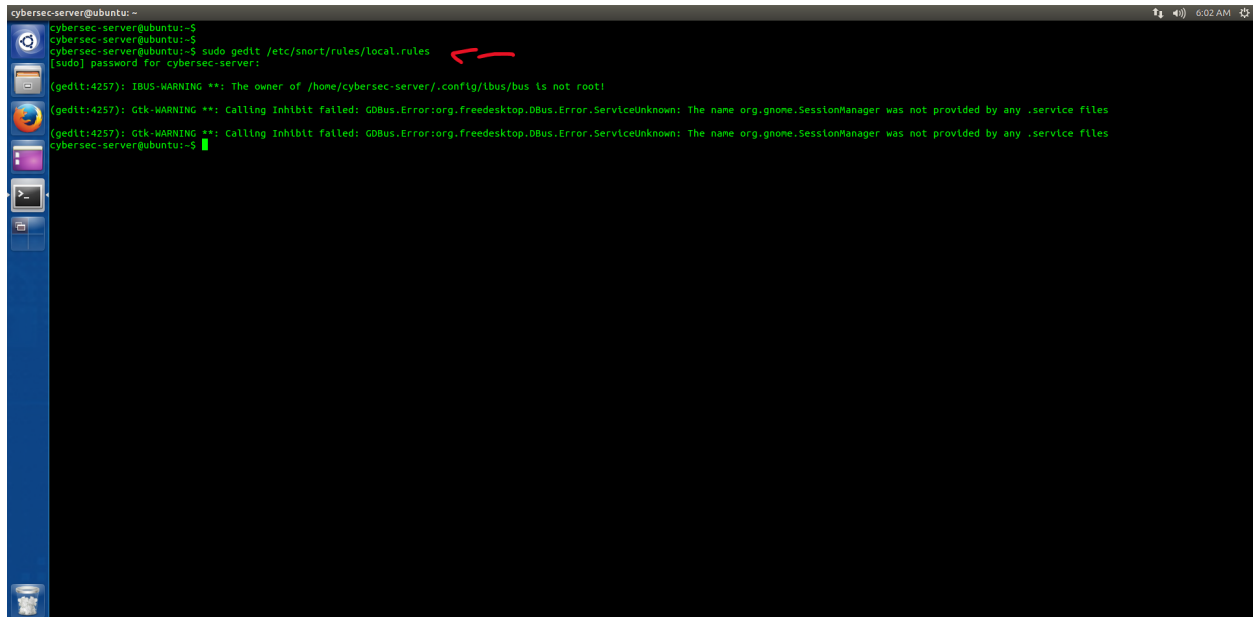


Alert “Web access request” are logged:



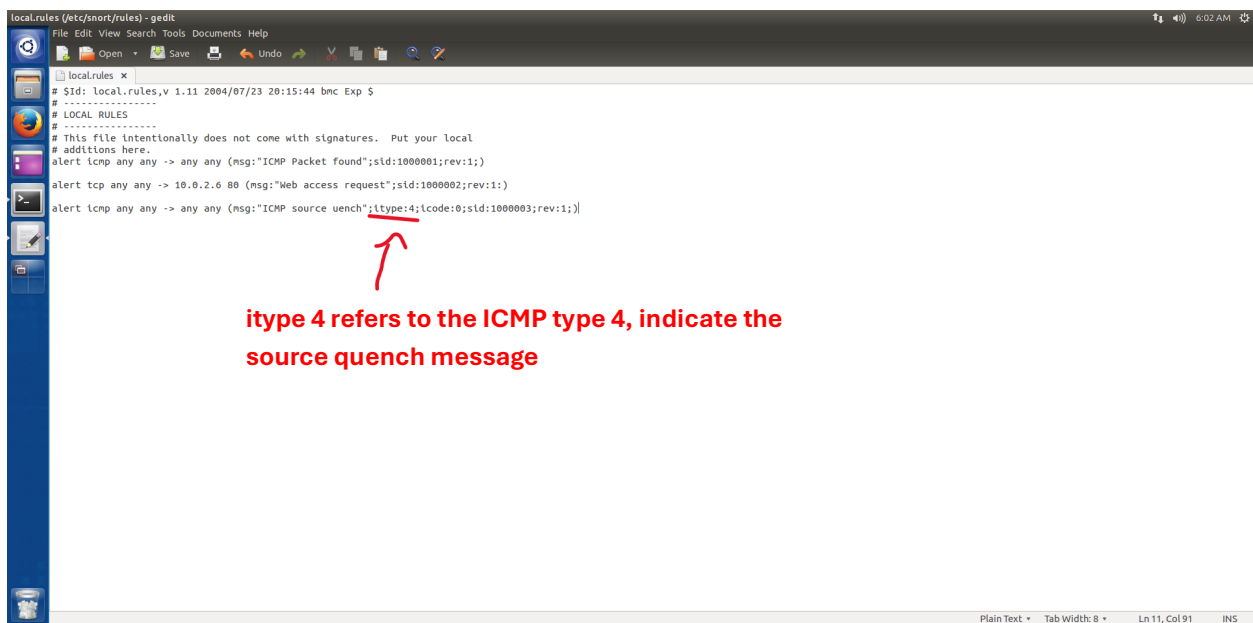
Task 4: Generating alerts for ICMP source quench packets:

Open the rules file:



A terminal window on a Linux system. The user is at the prompt `cybersec-server@ubuntu:~`. They enter `cybersec-server@ubuntu:~$ sudo gedit /etc/snort/rules/local.rules`. A red arrow points to the `local.rules` file path. The terminal shows the password prompt and then the `gedit` application starts. There are some warning messages from `ibus` and `gtk` about session manager services.

The alert command for ICMP Source Quench Packets



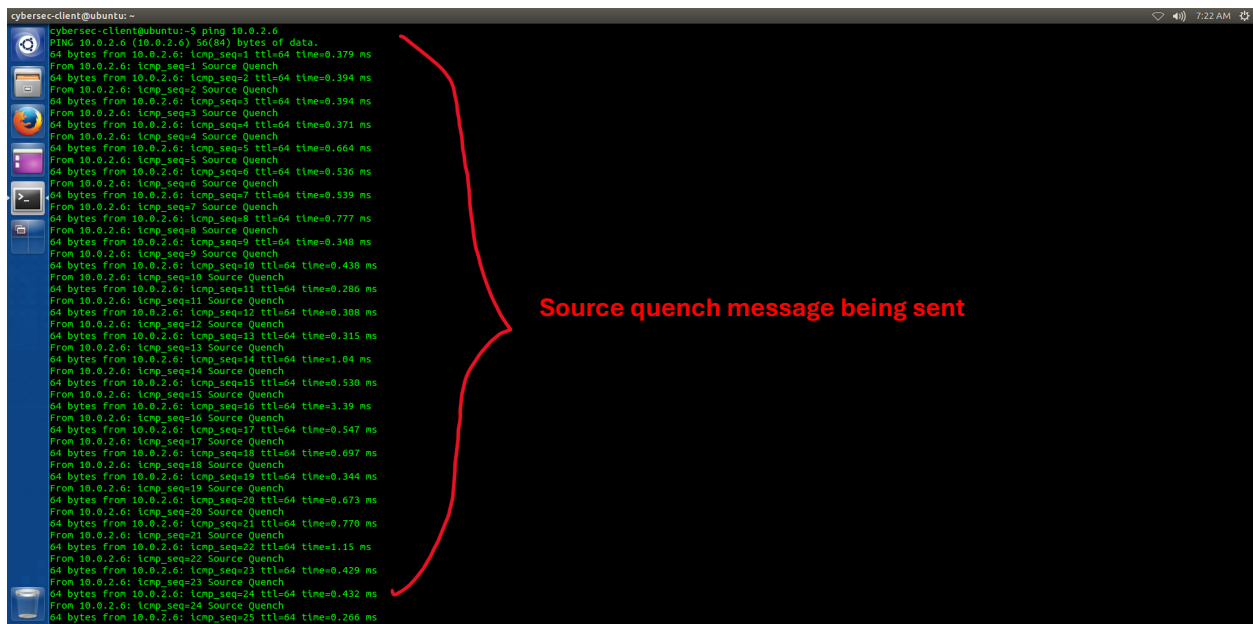
A screenshot of the `local.rules` file in the `gedit` editor. The file contains several alert rules. The last rule is highlighted with a red arrow pointing to the `ltype:4` part of the rule signature. Below the screenshot, a red arrow points to the text: **itype 4 refers to the ICMP type 4, indicate the source quench message**.

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any -> any any (msg:"ICMP Packet found";sid:1000001;rev:1;)
alert tcp any any -> 10.0.2.6 80 (msg:"Web access request";sid:1000002;rev:1;)
alert icmp any any -> any any (msg:"ICMP source quench";ltype:4;lcode:0;sid:1000003;rev:1;)
```

Using netwag to send ICMP source quench message



Ping the server from the client



```
cybersec-server@ubuntu: ~
10.0.2.8 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:4181 Iplen:20 Dgmlen:84 DF
Type: 8 Code: 0 Csum: 47732 Id: 5766 SeqNo: 15
** END OF DUMP

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
04/07-07:21:41.071554 10.0.2.6 -> 10.0.2.8
ICMP TTL:255 TOS:0x0 ID:41832 Iplen:20 Dgmlen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.8 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:4181 Iplen:20 Dgmlen:84 DF
Type: 8 Code: 0 Csum: 47732 Id: 5766 SeqNo: 15
** END OF DUMP

[**] [1:1000003:1] ICMP source unench [**]
[Priority: 0]
04/07-07:21:41.071566 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:61674 Iplen:20 Dgmlen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:35666 Iplen:20 Dgmlen:84
Type: 0 Code: 0 Csum: 49780 Id: 5766 SeqNo: 15
** END OF DUMP

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
04/07-07:21:41.071566 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:61674 Iplen:20 Dgmlen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:35666 Iplen:20 Dgmlen:84
Type: 0 Code: 0 Csum: 49780 Id: 5766 SeqNo: 15
** END OF DUMP

[**] [1:527:0] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
04/07-07:21:41.071566 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:61674 Iplen:20 Dgmlen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:35666 Iplen:20 Dgmlen:84
Type: 0 Code: 0 Csum: 49780 Id: 5766 SeqNo: 15
** END OF DUMP

[Xref => http://www.cert.org/advisories/CA-1997-28.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref => http://www.securityfocus.com/bid/2666]

cybersec-server@ubuntu: ~
```

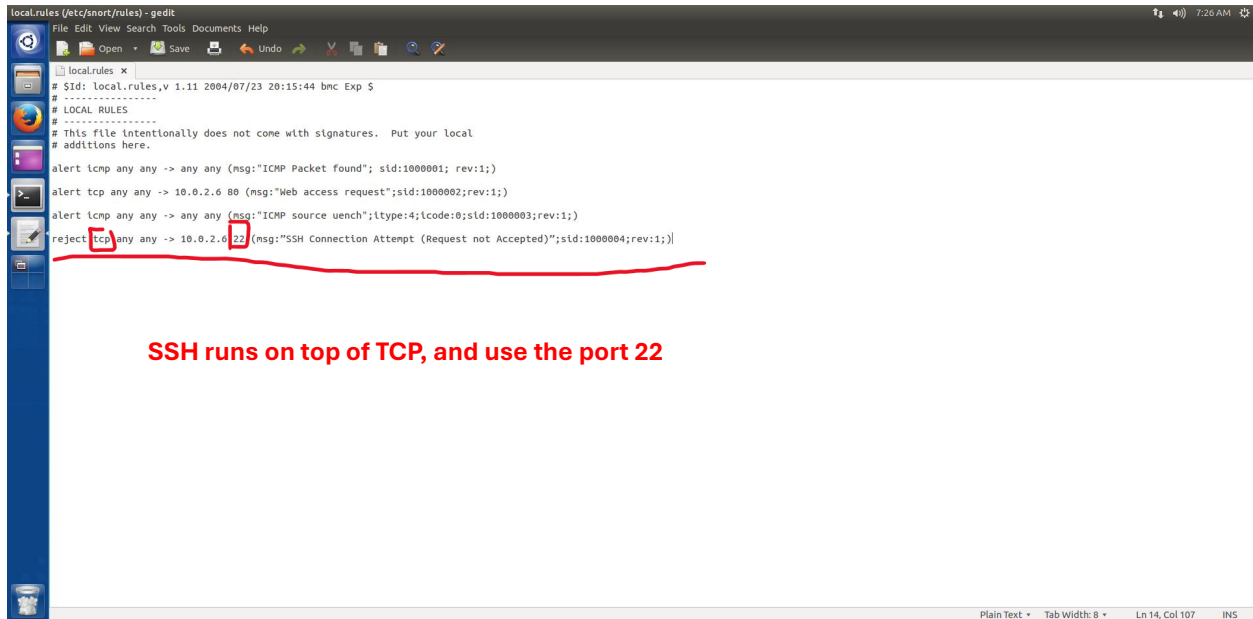
ICMP source quence alert

Task 5: Running Snort as Intrusion Prevention System

Open the rules file

```
cybersec-server@ubuntu: ~
cybersec-server@ubuntu:~$ sudo gedit /etc/snort/rules/local.rules
[sudo] password for cybersec-server:
(gedit:4663): IBUS-WARNING **: The owner of /home/cybersec-server/.config/ibus/bus is not root!
```

The reject rule for SSH connection being added



```
local.rules (etc/snort/rules) - gedit
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
alert tcp any any -> 10.0.2.6 80 (msg:"Web access request";sid:1000002;rev:1;)
alert icmp any any -> any any (msg:"ICMP source unch";ltype:4;lcode:0;sid:1000003;rev:1;)
reject tcp any any -> 10.0.2.6 22 (msg:"SSH Connection Attempt (Request not Accepted)";sid:1000004;rev:1;)
```

SSH runs on top of TCP, and use the port 22

Establish SSH connection from the attacker

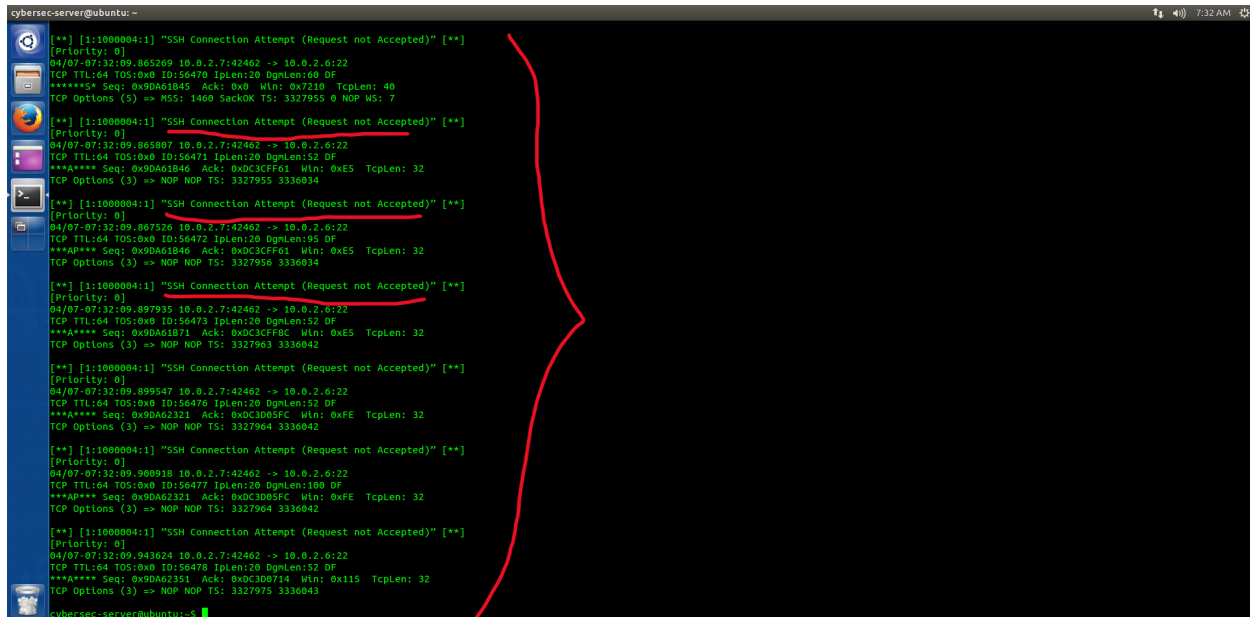


```
cybersec-attacker@ubuntu:~$ ssh MinH4512594810.0.2.6
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known hosts.
cybersec-attacker@ubuntu:~$
```

Connection failed

Command to establish SSH connection to the server

The alerts messages for SSH connection attempt:

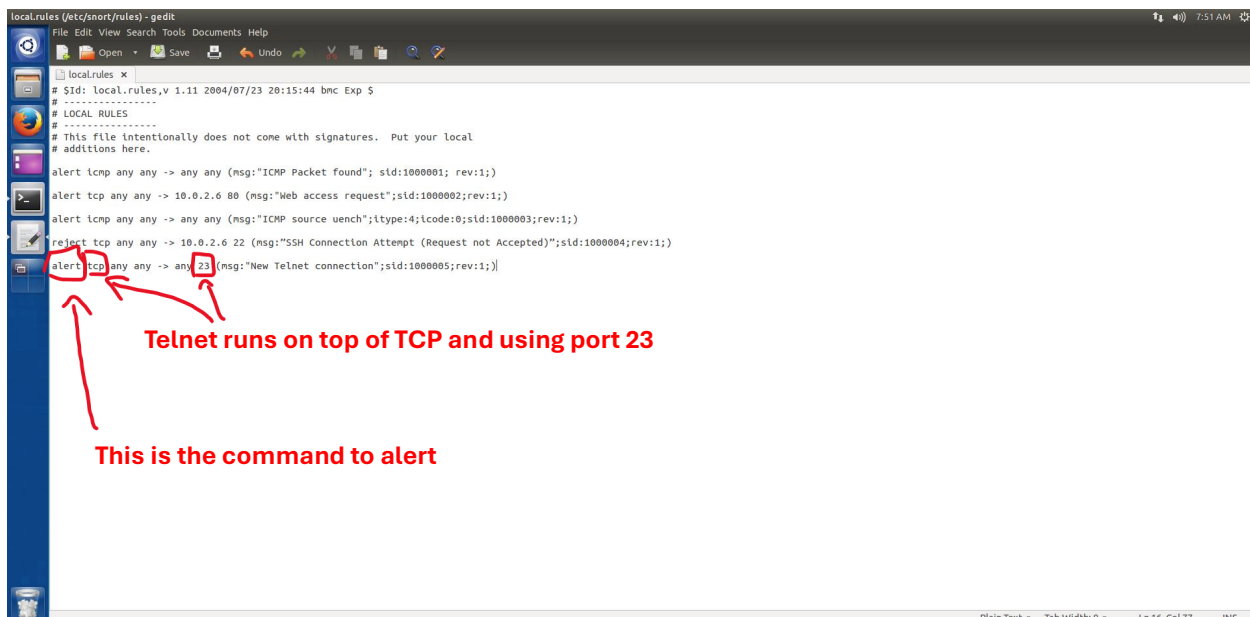


```
cybersec-server@ubuntu:~$  
[**] [1:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07-07:32:09.865269 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x0 ID:56470 Iplen:20 DgmLen:80 DF  
***** Seq: 0x9DA61845 Ack: 0x0 Wln: 0x7210 TcpLen: 40  
TCP Options (5) => MSS: 1460 SackOK TS: 3327955 0 NOP WS: 7  
[**] [1:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07-07:32:09.865807 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x0 ID:56471 Iplen:20 DgmLen:82 DF  
***** Seq: 0x9DA61846 Ack: 0xDC3CFF61 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3327955 3336034  
[**] [1:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07-07:32:09.867526 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x0 ID:56472 Iplen:20 DgmLen:95 DF  
***** Seq: 0x9DA61846 Ack: 0xDC3CFF61 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3327956 3336034  
[**] [1:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07-07:32:09.867935 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x0 ID:56473 Iplen:20 DgmLen:95 DF  
***** Seq: 0x9DA61871 Ack: 0xDC3CFF61 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3327963 3336042  
[**] [1:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07-07:32:09.899547 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x0 ID:56476 Iplen:20 DgmLen:82 DF  
***** Seq: 0x9DA62321 Ack: 0xDC3D05FC Wln: 0xFE TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3327964 3336042  
[**] [1:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07-07:32:09.900918 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x0 ID:56477 Iplen:20 DgmLen:100 DF  
***** Seq: 0x9DA62321 Ack: 0xDC3D05FC Wln: 0xFE TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3327964 3336042  
[**] [1:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07-07:32:09.943624 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x0 ID:56478 Iplen:20 DgmLen:82 DF  
***** Seq: 0x9DA62321 Ack: 0xDC3D0784 Wln: 0x115 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3327975 3336043  
cybersec-server@ubuntu:~$
```

*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:



```
local.rules (etc/snort/rules) - gedit  
File Edit View Search Tools Documents Help  
local.rules *  
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
#  
# LOCAL RULES  
#  
# This file intentionally does not come with signatures. Put your local  
# additions here.  
alert icmp any any -> any any (msg:"ICMP Packet found";sid:1000001;rev:1;)  
alert tcp any any -> 10.0.2.6 80 (msg:"Web access request";sid:1000002;rev:1;)  
alert icmp any any -> any any (msg:"ICMP source unench";ltype:4;lcode:0;sid:1000003;rev:1;)  
reject tcp any any -> 10.0.2.6 22 (msg:"SSH Connection Attempt (Request not Accepted)";sid:1000004;rev:1;)  
alert tcp any any -> any 23 (msg:"New Telnet Connection";sid:1000005;rev:1;)
```

Telnet runs on top of TCP and using port 23

This is the command to alert

Establish telnet connection from the server



The terminal window shows the process of establishing a telnet connection from the 'cybersec-attacker@ubuntu' machine to the 'cybersec-server@ubuntu' machine. The attacker first tries to connect to 10.0.2.6, which fails. Then, they try to connect to 10.0.2.6, which also fails. Finally, they try to connect to 10.0.2.6, which succeeds. The terminal output is as follows:

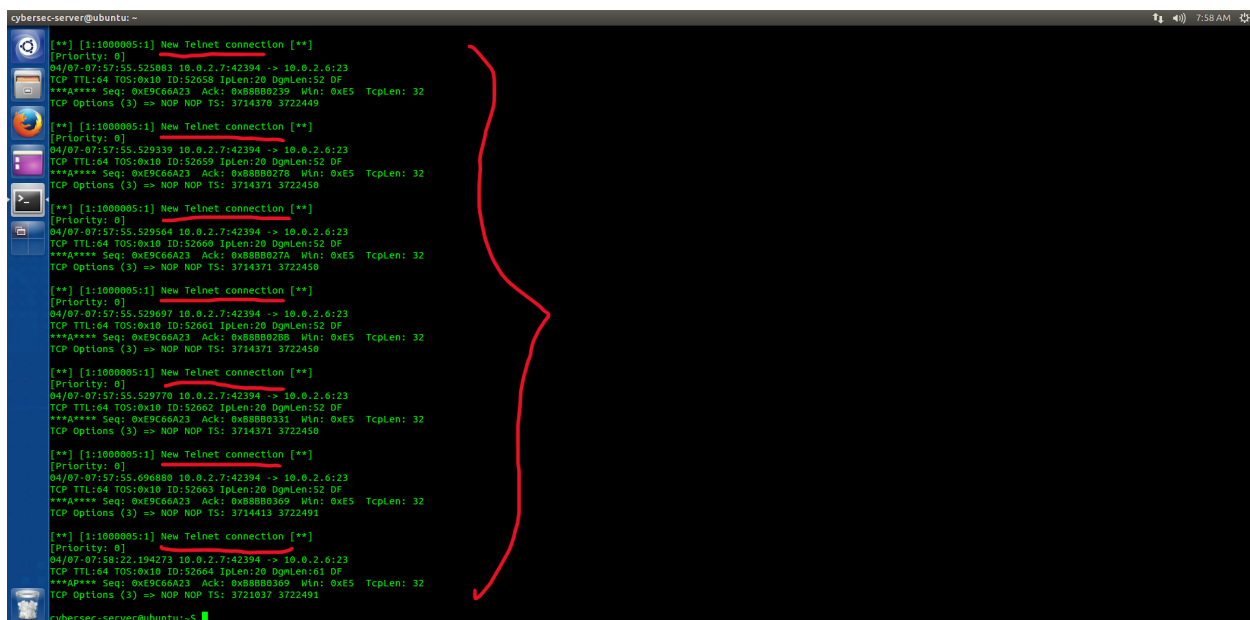
```
cybersec-server@ubuntu:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
ubuntu 14.04.5 LTS
ubuntu login: MtH14512584
Password:
Login incorrect
ubuntu login:
Password:
Login timed out after 60 seconds.
Connection closed by foreign host.
cybersec-attacker@ubuntu:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
ubuntu 14.04.5 LTS
ubuntu login: cybersec-server
Password:
Last login: Mon Oct 17 22:04:33 PDT 2016 from 10.0.2.9 on pts/0
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.2.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

288 packages can be updated.
410 updates are security updates.
cybersec-server@ubuntu:~$
```

Red annotations highlight the IP address '10.0.2.6' and the message 'Telnet connection established successfully'.

Alert messages showed in the alert file of the server:



The terminal window shows the contents of the alert file on the 'cybersec-server@ubuntu' machine. The file contains several entries indicating successful telnet connections from the 'cybersec-attacker@ubuntu' machine. The entries are as follows:

```
cybersec-server@ubuntu:~$ cat /var/log/auth.log
[11:00:00:05:1] New Telnet connection [**]
[Priority: 0]
04/07-07:57:55.525083 10.0.2.7:42394 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:52650 IPlen:20 DgLen:52 DF
***** Seq: 0xE9C66A23 Ack: 0xB8B80239 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3714370 3722449

[11:00:00:05:1] New Telnet connection [**]
[Priority: 0]
04/07-07:57:55.529339 10.0.2.7:42394 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:52659 IPlen:20 DgLen:52 DF
***** Seq: 0xE9C66A23 Ack: 0xB8B80278 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3714371 3722450

[11:00:00:05:1] New Telnet connection [**]
[Priority: 0]
04/07-07:57:55.529564 10.0.2.7:42394 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:52660 IPlen:20 DgLen:52 DF
***** Seq: 0xE9C66A23 Ack: 0xB8B80280 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3714371 3722450

[11:00:00:05:1] New Telnet connection [**]
[Priority: 0]
04/07-07:57:55.529697 10.0.2.7:42394 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:52661 IPlen:20 DgLen:52 DF
***** Seq: 0xE9C66A23 Ack: 0xB8B80280 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3714371 3722450

[11:00:00:05:1] New Telnet connection [**]
[Priority: 0]
04/07-07:57:55.529770 10.0.2.7:42394 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:52662 IPlen:20 DgLen:52 DF
***** Seq: 0xE9C66A23 Ack: 0xB8B80331 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3714371 3722450

[11:00:00:05:1] New Telnet connection [**]
[Priority: 0]
04/07-07:57:55.529880 10.0.2.7:42394 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:52663 IPlen:20 DgLen:52 DF
***** Seq: 0xE9C66A23 Ack: 0xB8B80369 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3714413 3722491

[11:00:00:05:1] New Telnet connection [**]
[Priority: 0]
04/07-07:58:22.194273 10.0.2.7:42394 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:52664 IPlen:20 DgLen:161 DF
***** Seq: 0xE9C66A23 Ack: 0xB8B80369 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3721037 3722491
cybersec-server@ubuntu:~$
```

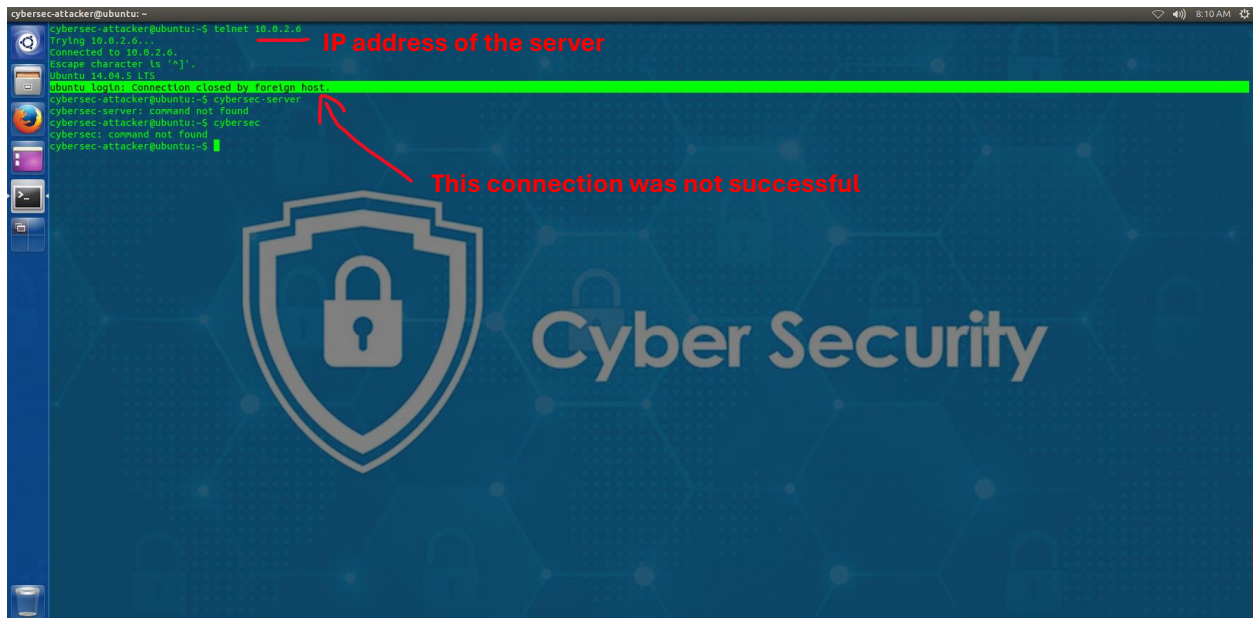
Red annotations highlight the 'New Telnet connection' messages and the IP address '10.0.2.6'.

In this case, the telnet connection is established successfully.

2) Reject



Establish telnet connection from the attacker:



The alerts being logged:

```
cybersec-server@ubuntu: ~  
[**] [1:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07-08:10:32.550987 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48119 ILen:20 DgLen:79 DF  
***A**** Seq: 0xBDE28B8 Ack: 0xE5717D01 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3983626 3911785  
[**] [1:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07-08:10:32.565500 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48120 ILen:20 DgLen:52 DF  
***A**** Seq: 0xBDE28B8 Ack: 0xE5717D00 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3983630 3911789  
[**] [1:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07-08:10:32.565657 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48121 ILen:20 DgLen:52 DF  
***A**** Seq: 0xBDE28B8 Ack: 0xE5717D34 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3983630 3911789  
[**] [1:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07-08:10:32.565761 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48122 ILen:20 DgLen:128 DF  
***A**** Seq: 0xBDE28B8 Ack: 0xE5717D34 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3983630 3911789  
[**] [1:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07-08:10:32.566040 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48123 ILen:20 DgLen:55 DF  
***A**** Seq: 0xBDE28B8 Ack: 0xE5717D37 Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3983631 3911789  
[**] [1:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07-08:10:32.568440 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48124 ILen:20 DgLen:55 DF  
***A**** Seq: 0xBDE28B8 Ack: 0xE5717D3C Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3983637 3911789  
[**] [1:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07-08:10:32.594024 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48125 ILen:20 DgLen:52 DF  
***A**** Seq: 0xBDE28B8 Ack: 0xE5717D5C Wln: 0xE5 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 3983637 3911789  
cybersec-server@ubuntu:~$
```

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