

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

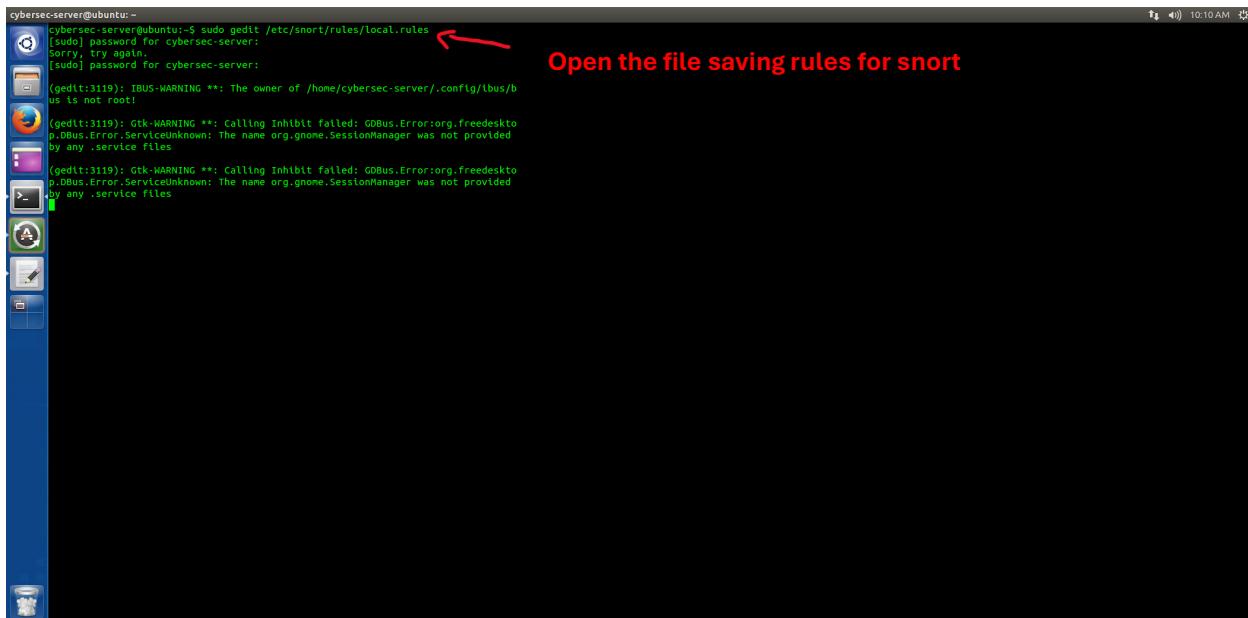
Telnet is insecure and should never be allowed. You must both **detect and prevent** Telnet access attempts.

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:

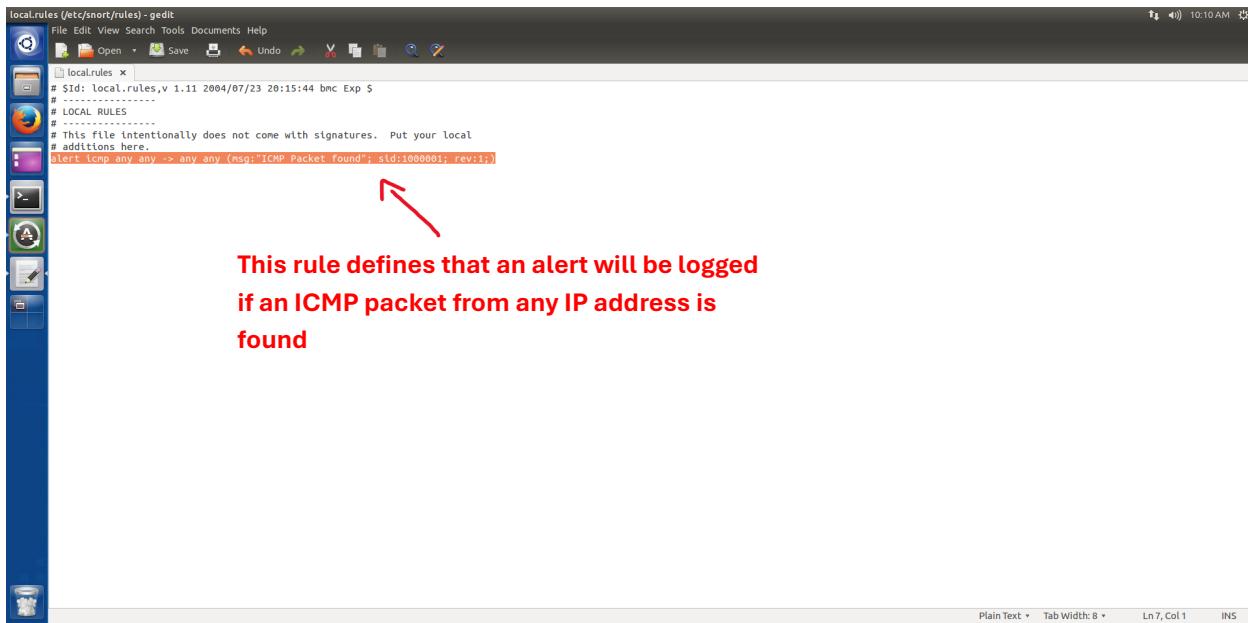
Task 1: Adding a Rule for ICMP packets



```
cybersec-server@ubuntu:~$ sudo gedit /etc/snort/rules/local.rules
[sudo] password for cybersec-server: Sorry, try again.
[sudo] password for cybersec-server:
(gedit:3119): IBUS-WARNING **: The owner of /home/cybersec-server/.config/gibus/bus is not root!
(gedit:3119): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
(gedit:3119): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
```

Open the file saving rules for snort

Inside the rules file:



```
localRules (/etc/snort/rules) - gedit
File Edit View Search Tools Documents Help
Open Save Undo Redo Cut Copy Paste Find Replace Select All
local.rules x
# $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;}
```

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:~$ 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=0.601 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.841 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=0.740 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.327 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.120 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
```

```
cybersec-server@ubuntu:~  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:32.615524 10.0.2.7 -> 10.0.2.6  
ICMP TTL:64 TOS:0x0 ID:15970 Iplen:28 DgmLen:84 DF  
Type:8 Code:0 ID:3981 Seq:11 ECHO  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:32.615547 10.0.2.6 -> 10.0.2.7  
ICMP TTL:64 TOS:0x0 ID:136723 Iplen:28 DgmLen:84 DF  
Type:0 Code:0 ID:3981 Seq:11 ECHO REPLY  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:33.616006 10.0.2.7 -> 10.0.2.6  
ICMP TTL:64 TOS:0x0 ID:15116 Iplen:28 DgmLen:84 DF  
Type:8 Code:0 ID:3981 Seq:12 ECHO  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:33.616041 10.0.2.6 -> 10.0.2.7  
ICMP TTL:64 TOS:0x0 ID:136924 Iplen:28 DgmLen:84 DF  
Type:0 Code:0 ID:3981 Seq:12 ECHO REPLY  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:34.616041 10.0.2.6 -> 10.0.2.6  
ICMP TTL:64 TOS:0x0 ID:15156 Iplen:28 DgmLen:84 DF  
Type:8 Code:0 ID:3981 Seq:13 ECHO  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:34.616057 10.0.2.6 -> 10.0.2.7  
ICMP TTL:64 TOS:0x0 ID:136980 Iplen:28 DgmLen:84 DF  
Type:0 Code:0 ID:3981 Seq:13 ECHO REPLY  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:35.616057 10.0.2.7 -> 10.0.2.6  
ICMP TTL:64 TOS:0x0 ID:15218 Iplen:28 DgmLen:84 DF  
Type:8 Code:0 ID:3981 Seq:14 ECHO  
[**] [1:1000001:1] ICMP Packet found [**]  
04/07 06:45:35.616059 10.0.2.6 -> 10.0.2.7  
ICMP TTL:64 TOS:0x0 ID:17048 Iplen:28 DgmLen:84 DF  
Type:0 Code:0 ID:3981 Seq:14 ECHO REPLY  
cybersec-server@ubuntu:~
```

The alert ICMP packet saved

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

```
cybersec-server@ubuntu:~  
cybersec-server@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -l eth0  
[sudo] password for cybersec-server:  
sorry, try again.  
[sudo] password for cybersec-server:
```

This command starts Snort in IDS mode

Ping the server from attacker

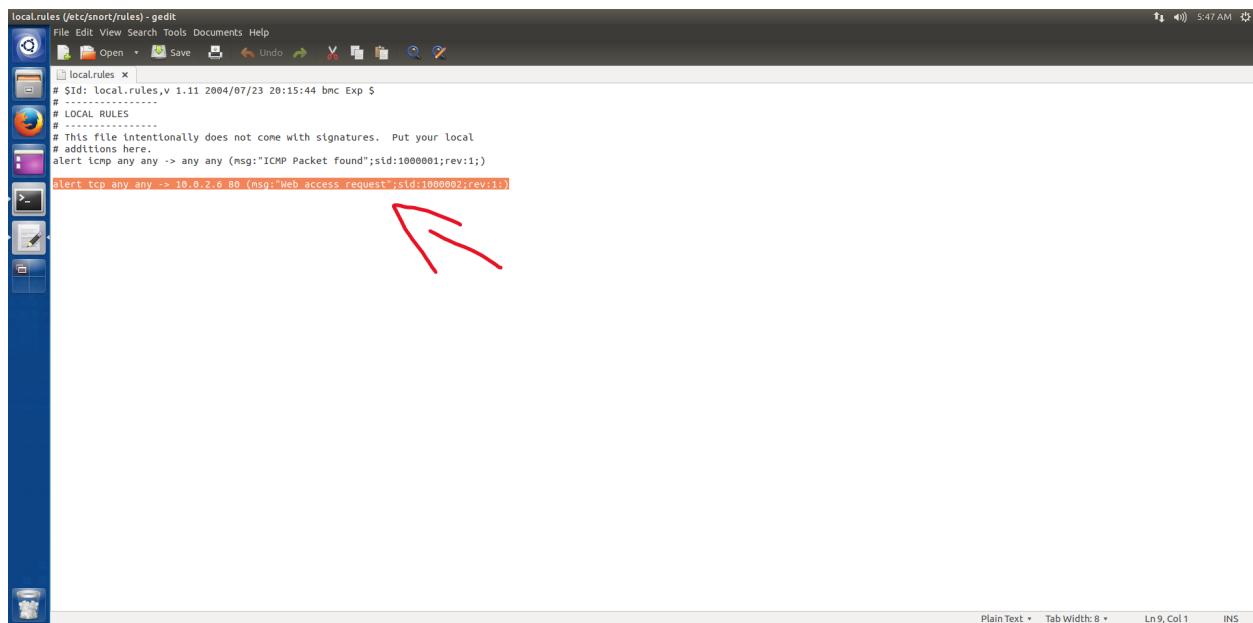
The image shows a Linux desktop environment with a blue-themed background featuring a digital network or cloud-like pattern. In the center is a large white shield icon with a silver padlock inside. Overlaid on the desktop is a terminal window with a dark gray title bar containing the text "cybersec-attacker@ubuntu: ~". The main area of the terminal displays the results of a "ping" command to the IP address 10.0.2.6. The output is as follows:

```
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=0.277 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=0.472 ms  
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.117 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=0.488 ms  
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.04 ms  
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.260 ms  
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.202 ms  
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=0.308 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=0.392 ms  
64 bytes from 10.0.2.6: icmp_seq=13 ttl=64 time=0.334 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=0.269 ms  
64 bytes from 10.0.2.6: icmp_seq=16 ttl=64 time=0.262 ms  
64 bytes from 10.0.2.6: icmp_seq=17 ttl=64 time=0.286 ms  
64 bytes from 10.0.2.6: icmp_seq=18 ttl=64 time=0.289 ms  
64 bytes from 10.0.2.6: icmp_seq=19 ttl=64 time=0.211 ms  
64 bytes from 10.0.2.6: icmp_seq=20 ttl=64 time=0.371 ms  
64 bytes from 10.0.2.6: icmp_seq=21 ttl=64 time=0.244 ms  
64 bytes from 10.0.2.6: icmp_seq=22 ttl=64 time=0.294 ms  
64 bytes from 10.0.2.6: icmp_seq=23 ttl=64 time=0.087 ms
```

The alert messages displayed in the IDS mode

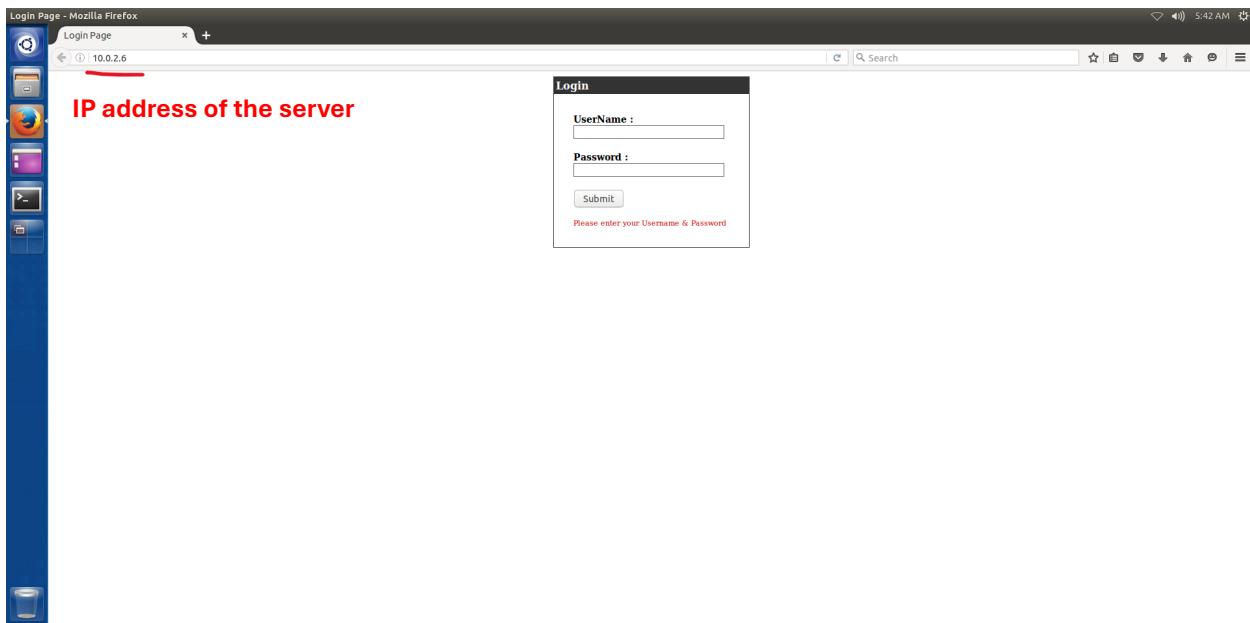
Task 3: Generating alert for web service

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



```
local.rules (/etc/snort/rules) - gedit
File Edit View Search Tools Documents Help
Open Save Undo Redo Cut Copy Paste Find Go
local.rules x
# $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:

```

cybersec-server@ubuntu:~ [**] [:1:1000002:1] Web access request [**]
[Priority: 0] 04/07/06:43:51.076976 10.0.2.7:51868 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:58614 Iplen:20 DgLen:394 DF
***AP*** Seq: 0x20080518 ACK: 0xE7034181 Winc: 0x10A TcpLen: 32
[TCP Options (3) == NOP NOP TS: 2603258 2611152

[**] [:1:1000002:1] Web access request [**]
[Priority: 0] 04/07/06:43:51.076976 10.0.2.7:51868 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:58615 Iplen:20 DgLen:394 DF
***AP*** Seq: 0x20080519 ACK: 0xE7034181 Winc: 0x10A TcpLen: 32
[TCP Options (3) == NOP NOP TS: 2603258 2611152

[**] [:1:1000002:1] Web access request [**]
[Priority: 0] 04/07/06:43:51.076976 10.0.2.7:51868 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:58616 Iplen:20 DgLen:394 DF
***AP*** Seq: 0x20080571 ACK: 0xE7034181 Winc: 0x116 TcpLen: 32
[TCP Options (3) == NOP NOP TS: 2603258 2611152

[**] [:1:1000002:1] Web access request [**]
[Priority: 0] 04/07/06:43:52.223768 10.0.2.7:51868 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:58616 Iplen:20 DgLen:394 DF
***AP*** Seq: 0x20080571 ACK: 0xE7034181 Winc: 0x116 TcpLen: 32
[TCP Options (3) == NOP NOP TS: 2603544 2611137

[**] [:1:1000002:1] Web access request [**]
[Priority: 0] 04/07/06:43:52.223768 10.0.2.7:51868 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:58617 Iplen:20 DgLen:394 DF
***AP*** Seq: 0x20080572 ACK: 0xE7034181 Winc: 0x116 TcpLen: 32
[TCP Options (3) == NOP NOP TS: 2603544 2611137

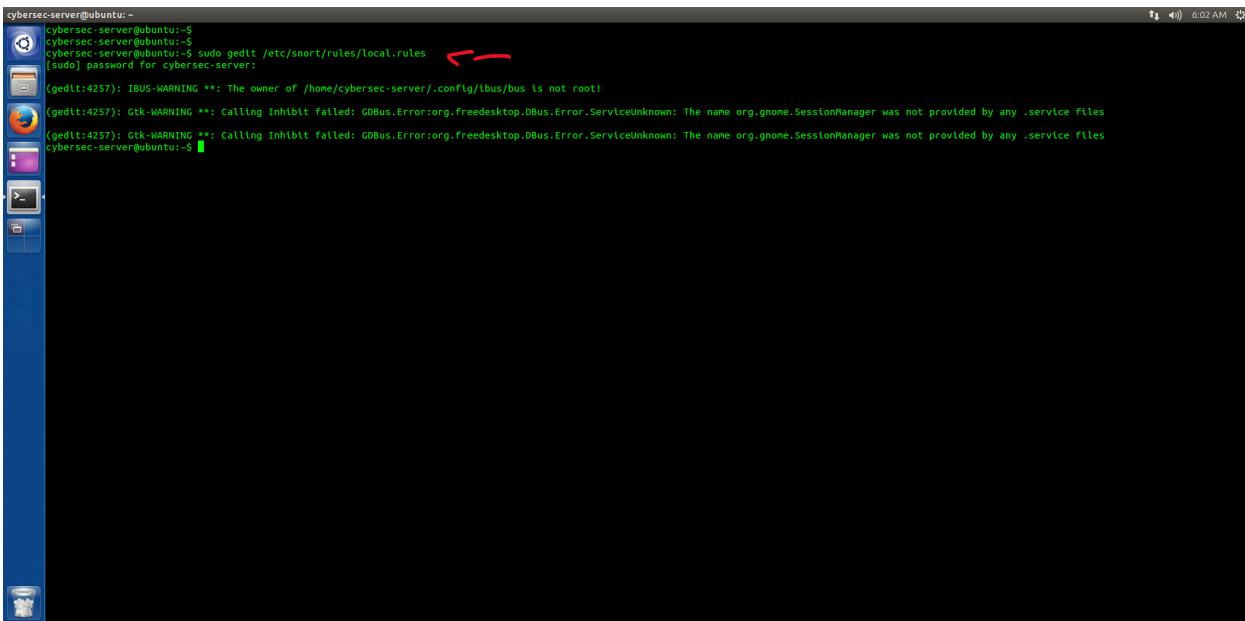
[**] [:1:1000002:1] Web access request [**]
[Priority: 0] 04/07/06:43:52.223768 10.0.2.7:51868 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:58618 Iplen:20 DgLen:394 DF
***AP*** Seq: 0x20080573 ACK: 0xE7034181 Winc: 0x116 TcpLen: 32
[TCP Options (3) == NOP NOP TS: 2603544 2611137

[**] [:1:1000002:1] ICMP Packet found [**]
[Priority: 0] 04/07/06:43:57.223256 10.0.2.7:51868 -> 10.0.2.6:80
ICMP TTL:64 TOS:0x0 ID:58619 Iplen:20 DgLen:52 DF
***TYPE3*** Code: 0x00000000 REASON: PORT UNREACHABLE: PORT UNREACHABLE
***ORIGIN*** DATAGRAM DUMP:
10.0.2.6:53 -> 10.0.2.7:54039

```

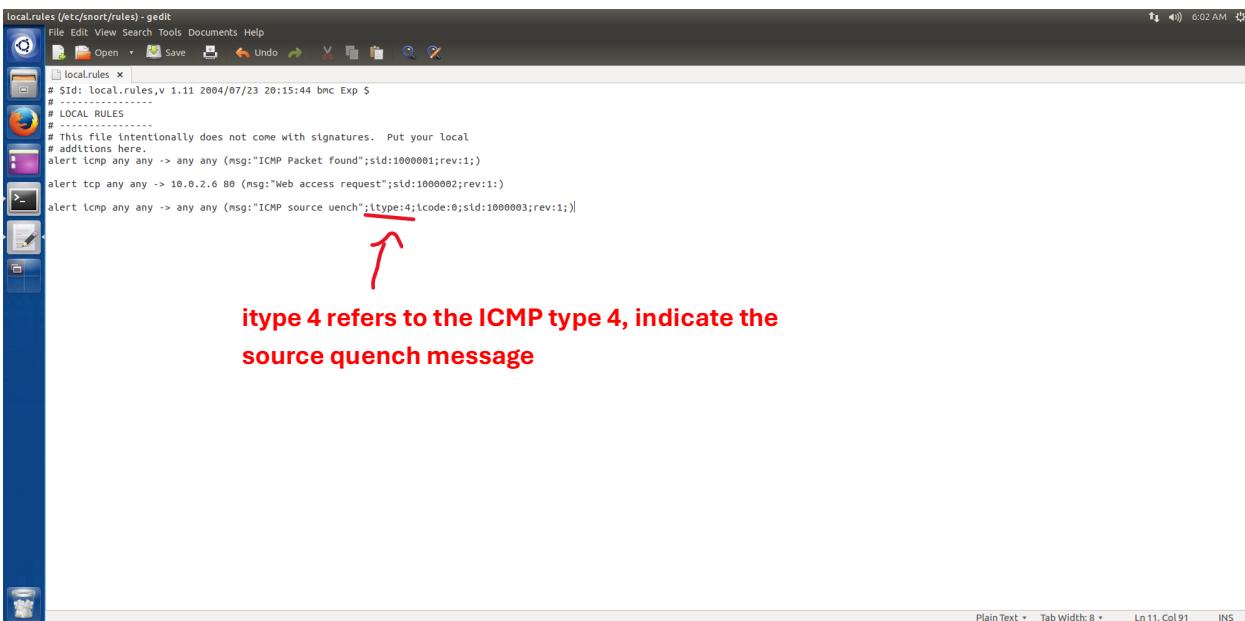
Task 4: Generating alerts for ICMP source quench packets:

Open the rules file:



```
cybersecserver@ubuntu:~\n[cybersec-server@ubuntu:~$ \n[cybersec-server@ubuntu:~$ sudo gedit /etc/snort/rules/local.rules \n[sudo] password for cybersec-server:\n(gedit:4257): IBUS-WARNING **: The owner of /home/cybersec-server/.config/ibus/bus is not root\n(gedit:4257): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files\n(gedit:4257): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files\n[cybersec-server@ubuntu:~$ ]
```

The alert command for ICMP Source Quench Packets



```
local.rules (/etc/snort/rules) - gedit\nFile Edit View Search Tools Documents Help\nlocal.rules x | \n# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $\n# -----\n# LOCAL RULES\n# -----\n# This file intentionally does not come with signatures. Put your local\n# additions here.\nalert icmp any any -> any any (msg:"ICMP Packet found";sid:1000001;rev:1;)\nalert tcp any any -> 10.0.2.6 80 (msg:"Web access request";sid:1000002;rev:1;)\nalert icmp any any -> any any (msg:"ICMP source quench";itype:4;lcode:0;sid:1000003;rev:1;)
```

itype 4 refers to the ICMP type 4, indicate the source quench message

Using netwag to send ICMP source quench message



Ping the server from the client

The terminal window shows the command 'ping 10.0.2.6' being run. The output displays multiple ICMP echo requests and responses. A red arrow points from the terminal window to the text 'Source quench message being sent' located below the terminal window.

```

cybersec-client@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
From 10.0.2.6: icmp_seq=1 ttl=64 time=0.379 ms
From 10.0.2.6: icmp_seq=2 ttl=64 time=0.394 ms
From 10.0.2.6: icmp_seq=3 ttl=64 time=0.394 ms
From 10.0.2.6: icmp_seq=4 ttl=64 time=0.371 ms
From 10.0.2.6: icmp_seq=5 ttl=64 time=0.664 ms
From 10.0.2.6: icmp_seq=6 ttl=64 time=0.536 ms
From 10.0.2.6: icmp_seq=7 ttl=64 time=0.539 ms
From 10.0.2.6: icmp_seq=8 ttl=64 time=0.777 ms
From 10.0.2.6: icmp_seq=9 ttl=64 time=0.348 ms
From 10.0.2.6: icmp_seq=10 ttl=64 time=0.438 ms
From 10.0.2.6: icmp_seq=11 ttl=64 time=0.286 ms
From 10.0.2.6: icmp_seq=12 ttl=64 time=0.308 ms
From 10.0.2.6: icmp_seq=13 ttl=64 time=0.315 ms
From 10.0.2.6: icmp_seq=14 ttl=64 time=1.04 ms
From 10.0.2.6: icmp_seq=15 ttl=64 time=0.530 ms
From 10.0.2.6: icmp_seq=16 ttl=64 time=0.39 ms
From 10.0.2.6: icmp_seq=17 ttl=64 time=0.547 ms
From 10.0.2.6: icmp_seq=18 ttl=64 time=0.697 ms
From 10.0.2.6: icmp_seq=19 ttl=64 time=0.344 ms
From 10.0.2.6: icmp_seq=20 ttl=64 time=0.673 ms
From 10.0.2.6: icmp_seq=21 ttl=64 time=0.770 ms
From 10.0.2.6: icmp_seq=22 ttl=64 time=0.15 ms
From 10.0.2.6: icmp_seq=23 ttl=64 time=0.429 ms
From 10.0.2.6: icmp_seq=24 ttl=64 time=0.432 ms
From 10.0.2.6: icmp_seq=25 ttl=64 time=0.266 ms

```

Source quench message being sent

```

cybersec-server@ubuntu:~ 
[*] 1:0.2.8 > 10.0.2.6 
[IP/ICMP] 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 -> 10.0.2.6 
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 quench [*] 
[Priority: 0] 
04/07/07:21:41.071560 10.0.2.6 -> 10.0.2.6 
ICMP TTL:255 TOS:0x0 ID:1674 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 DF 
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:1674 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 DF 
Type: 0 Code: 0 Csum: 49780 Id: 5766 SeqNo: 15 
** END OF DUMP 

[*] [1:527:8] 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:1674 Iplen:20 DgmLen:56 
Type:8 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 DF 
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=i999-0016][Xref => http://www.securityfocus.com/bid/2666] 
cybersec-server@ubuntu:~ 

```

Task 5: Running Snort as Intrusion Prevention System

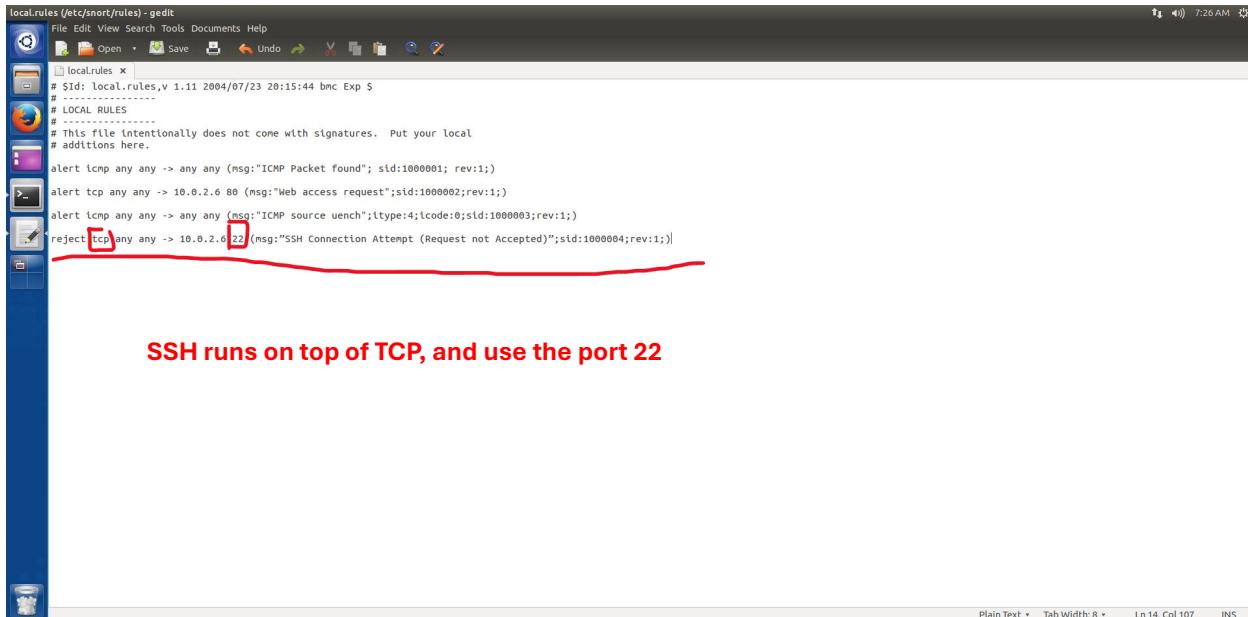
Open the rules file

```

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! 

```

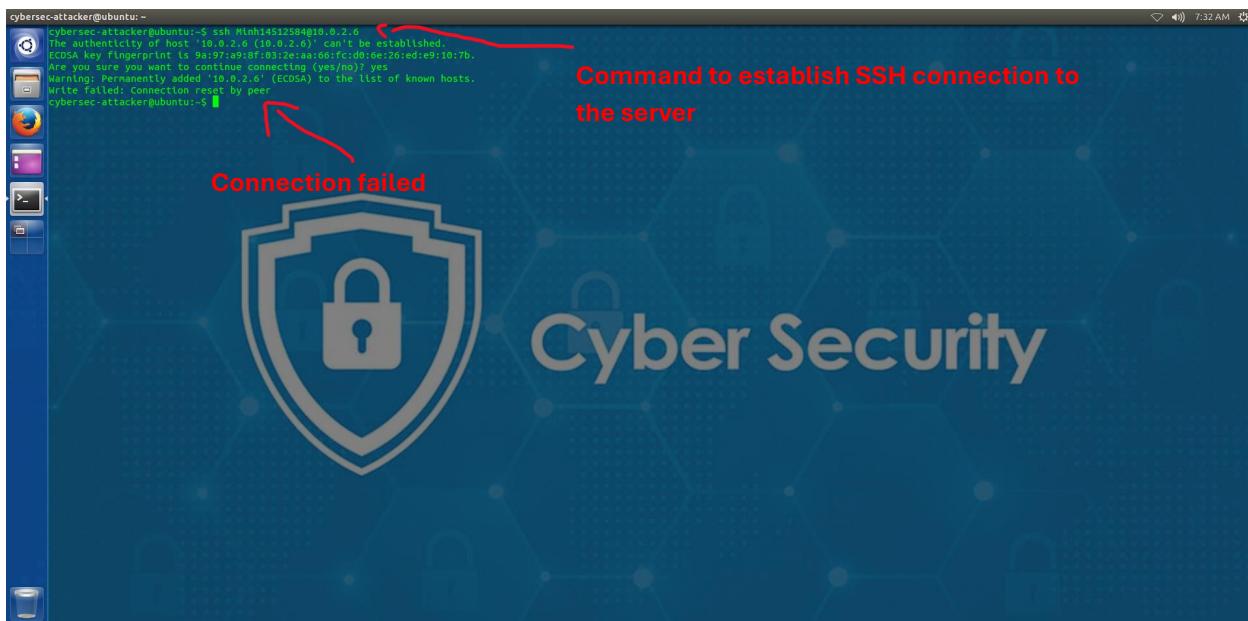
The reject rule for SSH connection being added



```
# 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;)  
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 uench";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



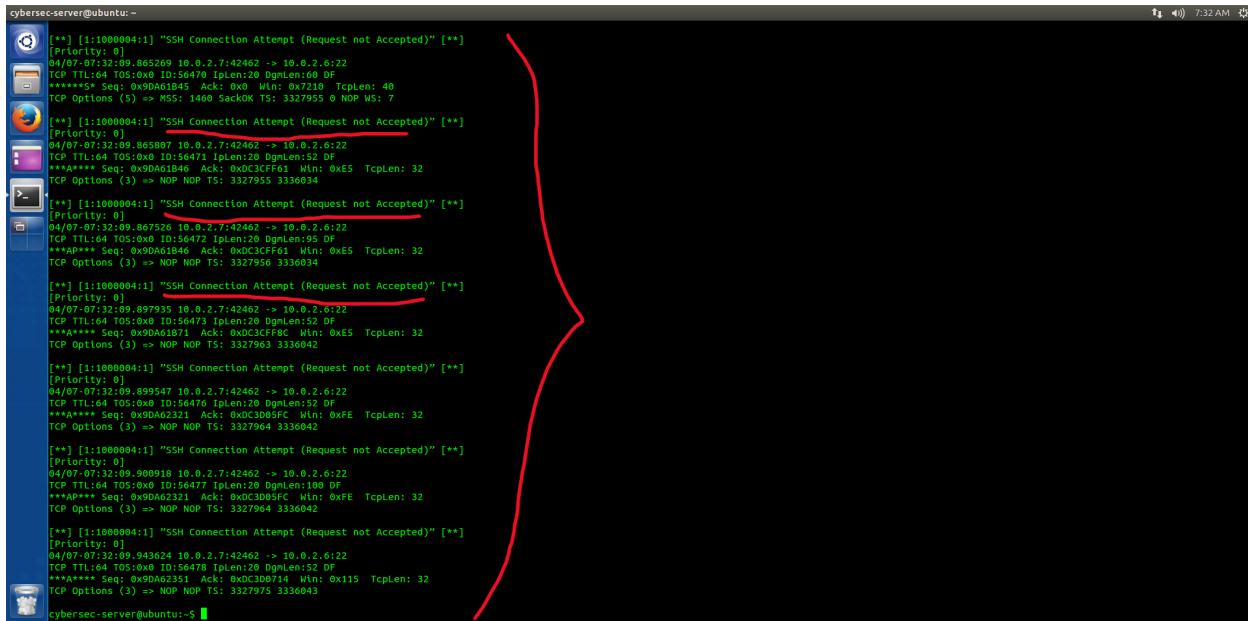
```
cybersec-attacker@ubuntu:~$ ssh Mihai4512584@10.0.2.6  
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.  
ECDSA key fingerprint is 9a:97:a9:9af1:03:2e:a1:66:fc:dd:6:26:ed:e9:10:7b.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known hosts.  
Write failed: Connection reset by peer  
cybersec-attacker@ubuntu:~$
```

Command to establish SSH connection to the server

Connection failed

Cyber Security

The alerts messages for SSH connection attempt:

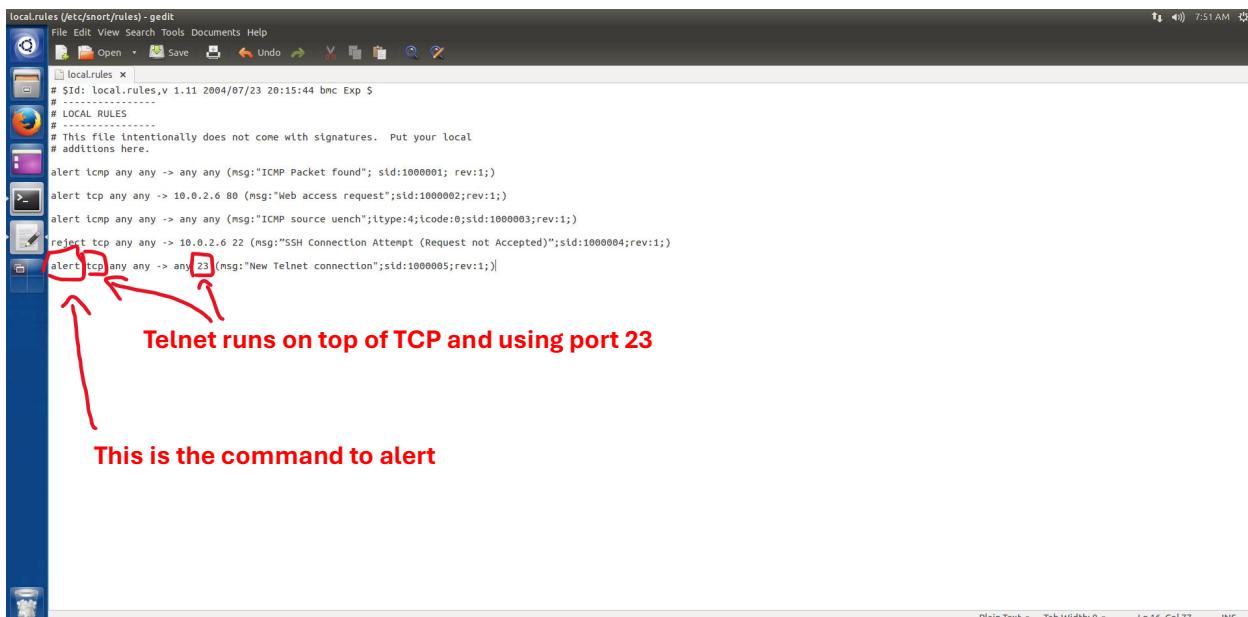


```
cybersec-server@ubuntu:~  
[**] [i:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07/07:32:09.865269 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x00 ID:56470 Iplen:20 DgmLen:68 DF  
***AP*** Seq: 0x90A0A1B45 ACK: 0x0  Win: 0x7210 TcpLen: 48  
TCP Options (3) == MSS: 1460 SackOK TS: 5327955 0 NOP MS: 7  
[**] [i: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:0x00 ID:56471 Iplen:20 DgmLen:62 DF  
***AP*** Seq: 0x90A0A1B45 ACK: 0x0C3CFE61 Win: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 5327955 3336034  
[**] [i: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:0x00 ID:56472 Iplen:20 DgmLen:95 DF  
***AP*** Seq: 0x90A0A1B46 ACK: 0x0C3CFE61 Win: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 5327956 3336034  
[**] [i:1000004:1] "SSH Connection Attempt (Request not Accepted)" [**]  
[Priority: 0]  
04/07/07:32:09.887935 10.0.2.7:42462 -> 10.0.2.6:22  
TCP TTL:64 TOS:0x00 ID:56473 Iplen:20 DgmLen:52 DF  
***AP*** Seq: 0x90A0A1B71 ACK: 0x0C3CF8C Win: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 5327963 3336042  
[**] [i: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:0x00 ID:56476 Iplen:20 DgmLen:52 DF  
***AP*** Seq: 0x90A0A2321 ACK: 0x0C3D05FC Win: 0xF E TcpLen: 32  
TCP Options (3) == NOP NOP TS: 5327964 3336042  
[**] [i: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:0x00 ID:56477 Iplen:20 DgmLen:100 DF  
***AP*** Seq: 0x90A0A2321 ACK: 0x0C3D05FC Win: 0xF E TcpLen: 32  
TCP Options (3) == NOP NOP TS: 5327964 3336042  
[**] [i: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:0x00 ID:56478 Iplen:20 DgmLen:52 DF  
***AP*** Seq: 0x90A0A2351 ACK: 0x0C3D0714 Win: 0x115 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 5327975 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  
File Open Save Undo Redo Cut Copy Paste Find  
localrules x  
# $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 unreach";itype:4;icode: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

```
cybersec-server@ubuntu:~\n[Login Incorrect\nUbuntu login: Connection closed by foreign host.\n[cybersec-attacker@ubuntu:~$ telnet "10.0.2.6"\n[Trying 10.0.2.6...\nConnected to 10.0.2.6.\nEscape character is '^A'.\nUbuntu 14.04.5 LTS\nUbuntu login: Minh14512584\nPassword:\n[Login Incorrect\nubuntu login:\npassword:\n[Login timed out after 60 seconds.\nConnection closed by foreign host.\n[cybersec-attacker@ubuntu:~$ clear\n[cybersec-attacker@ubuntu:~$ telnet 10.0.2.6\n[Trying 10.0.2.6...\nConnected to 10.0.2.6.\nEscape character is '^A'.\nUbuntu 14.04.5 LTS\nUbuntu login: Minh14512584\nPassword:\n[Login Incorrect\nubuntu login: cybersec-connection closed by foreign host.\n[cybersec-attacker@ubuntu:~$ telnet 10.0.2.6\n[Trying 10.0.2.6...\nConnected to 10.0.2.6.\nEscape character is '^A'.\nUbuntu 14.04.5 LTS\nUbuntu login: cybersec-server\nPassword:\n[Welcome to Ubuntu 17.22:04:33 PDT 2016 from 10.0.2.0 on pts/6\n[Documentation: https://help.ubuntu.com/\n588 packages can be updated,\n416 updates are security updates.\ncybersec-server@ubuntu:~$ ]\n
```

Alert messages showed in the alert file of the server:

```
[**] [1:1000005:1] New Telnet connection [**]\n[Priority: 0]\n04/07/07:57:55.525083 10.0.2.7:42394 -> 10.0.2.6:23\nTCP TTL:64 TOS:0x10 ID:52658 Iplen:20 DgmLen:52 DF\n***+*** Seq: 0xE5C66A23 ACK: 0xB8BBB0239 Win: 0xE5 TcpLen: 32\nTCP Options (3) => NOP NOP TS: 3714370 3722469\n\n[**] [1:1000005:1] New Telnet connection [**]\n[Priority: 0]\n04/07/07:57:55.529339 10.0.2.7:42394 -> 10.0.2.6:23\nTCP TTL:64 TOS:0x10 ID:52659 Iplen:20 DgmLen:52 DF\n***+*** Seq: 0xE5C66A23 ACK: 0xB8BBB0278 Win: 0xE5 TcpLen: 32\nTCP Options (3) => NOP NOP TS: 3714371 3722458\n\n[**] [1:1000005:1] New Telnet connection [**]\n[Priority: 0]\n04/07/07:57:55.530564 10.0.2.7:42394 -> 10.0.2.6:23\nTCP TTL:64 TOS:0x10 ID:52660 Iplen:20 DgmLen:52 DF\n***+*** Seq: 0xE5C66A23 ACK: 0xB8BBB027A Win: 0xE5 TcpLen: 32\nTCP Options (3) => NOP NOP TS: 3714371 3722458\n\n[**] [1:1000005:1] New Telnet connection [**]\n[Priority: 0]\n04/07/07:57:55.530697 10.0.2.7:42394 -> 10.0.2.6:23\nTCP TTL:64 TOS:0x10 ID:52661 Iplen:20 DgmLen:52 DF\n***+*** Seq: 0xE5C66A23 ACK: 0xB8BBB0288 Win: 0xE5 TcpLen: 32\nTCP Options (3) => NOP NOP TS: 3714371 3722458\n\n[**] [1:1000005:1] New Telnet connection [**]\n[Priority: 0]\n04/07/07:57:55.529770 10.0.2.7:42394 -> 10.0.2.6:23\nTCP TTL:64 TOS:0x10 ID:52662 Iplen:20 DgmLen:52 DF\n***+*** Seq: 0xE5C66A23 ACK: 0xB8BBB0331 Win: 0xE5 TcpLen: 32\nTCP Options (3) => NOP NOP TS: 3714431 3722491\n\n[**] [1:1000005:1] New Telnet connection [**]\n[Priority: 0]\n04/07/07:57:55.696880 10.0.2.7:42394 -> 10.0.2.6:23\nTCP TTL:64 TOS:0x10 ID:52663 Iplen:20 DgmLen:52 DF\n***+*** Seq: 0xE5C66A23 ACK: 0xB8BBB0369 Win: 0xE5 TcpLen: 32\nTCP Options (3) => NOP NOP TS: 3714431 3722491\n\n[**] [1:1000005:1] New Telnet connection [**]\n[Priority: 0]\n04/07/07:58:22.194273 10.0.2.7:42394 -> 10.0.2.6:23\nTCP TTL:64 TOS:0x10 ID:52664 Iplen:20 DgmLen:61 DF\n***+*** Seq: 0xE5C66A23 ACK: 0xB8BBB0369 Win: 0xE5 TcpLen: 32\nTCP Options (3) => NOP NOP TS: 3721037 3722491\ncybersec-server@ubuntu:~$ ]\n
```

In this case, the telnet connection is established successfully.

2) Reject

```
# $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 uench";itype:4;icode: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;)  
reject tcp any any -> 10.0.2.6 23 (msg:"Telnet Connection Attempt (Request not Accepted)";sid:1000005;rev:1;)
```

Telnet runs on top of TCP and using port 23

This command is to reject

>Loading file '/etc/snort/rules/local.rules'... Plain Text Tab Width: 8 Ln 1, Col 1 INS

Establish telnet connection from the attacker:

```
cybersec-attacker@ubuntu:~$ telnet 10.0.2.6  
Trying 10.0.2.6...  
Connected to 10.0.2.6.  
Escape character is '^]'.  
Ubuntu Login: Connection closed by foreign-host.  
cybersec-attacker@ubuntu:~$ cybersec-server  
cybersec-server: command not found  
cybersec-attacker@ubuntu:~$ cybersec  
cybersec: command not found  
cybersec-attacker@ubuntu:~$
```

IP address of the server

This connection was not successful

Cyber Security

The alerts being logged:

```
cybersec-server@ubuntu:~  
[**] [i: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 Iplen:20 DgmLen:79 DF  
***AP*** Seq: 0xB0DE2B88 ACK: 0xE571D01 WIn: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 3903636 3911705  
[**] [i:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07/08:10:32.565508 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48120 Iplen:20 DgmLen:52 DF  
***AP*** Seq: 0xB0DE2B88 ACK: 0xE571D01 WIn: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 3903636 3911709  
[**] [i: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 Iplen:20 DgmLen:52 DF  
***AP*** Seq: 0xB0DE2B88 ACK: 0xE571D04 WIn: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 3903636 3911709  
[**] [i: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 Iplen:20 DgmLen:126 DF  
***AP*** Seq: 0xB0DE2B88 ACK: 0xE571D04 WIn: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 3903636 3911709  
[**] [i:1000005:1] Telnet Connection Attempt (Request not Accepted) [**]  
[Priority: 0]  
04/07/08:10:32.566440 10.0.2.7:42406 -> 10.0.2.6:23  
TCP TTL:64 TOS:0x10 ID:48123 Iplen:20 DgmLen:55 DF  
***AP*** Seq: 0xB0DE2B88 ACK: 0xE571D04 WIn: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 3903636 3911709  
[**] [i: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 Iplen:20 DgmLen:55 DF  
***AP*** Seq: 0xB0DE2B88 ACK: 0xE571D04 WIn: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 3903636 3911709  
[**] [i: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 Iplen:20 DgmLen:52 DF  
***AP*** Seq: 0xB0DE2B88 ACK: 0xE571D05 WIn: 0xE5 TcpLen: 32  
TCP Options (3) == NOP NOP TS: 3903636 3911709
```

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