Lab - Snort

Introduction

Snort is the world’s most popular Open Source Intrusion Prevention System (IPS), capable of performing real-time traffic analysis and packet logging on IP networks. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger for network traffic debugging, or it can be used as a full-blown network intrusion prevention system.

Required resources

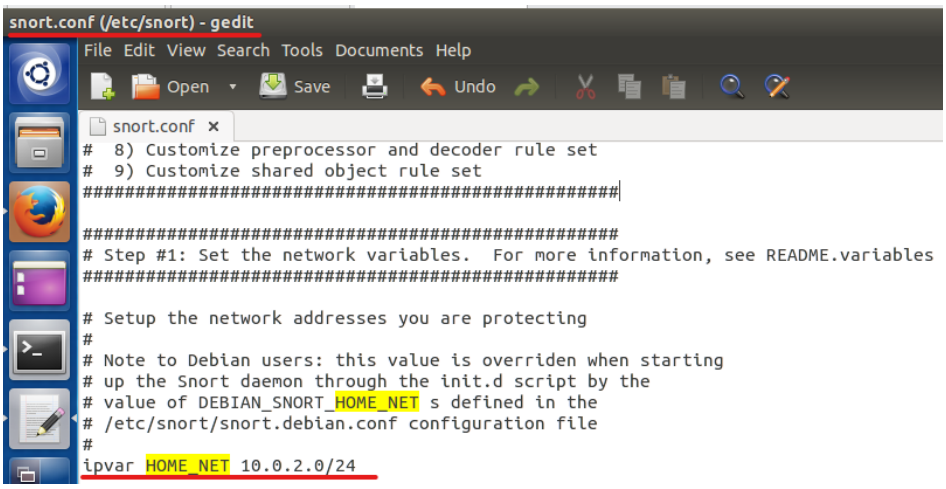
We are going to use Cybersec-Server, Cybersec-Attacker VM for this lab

Task

Configure Snort rules

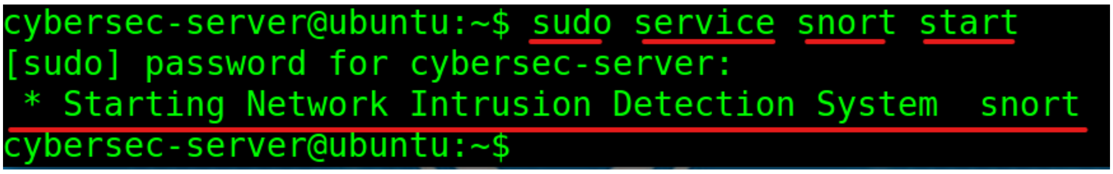
Step 1 start Snort on **Cybersec-Server**

1) Snort is already installed in our system, Snort configuration file is /etc/snort/snort.conf, this is a big configuration file, we will change the ipvar **HOME_NET** from “any” to our local network “10.0.2.0/24”
   sudo gedit /etc/snort/snort.conf


snort.conf (/etc/snort) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
snort.conf ×

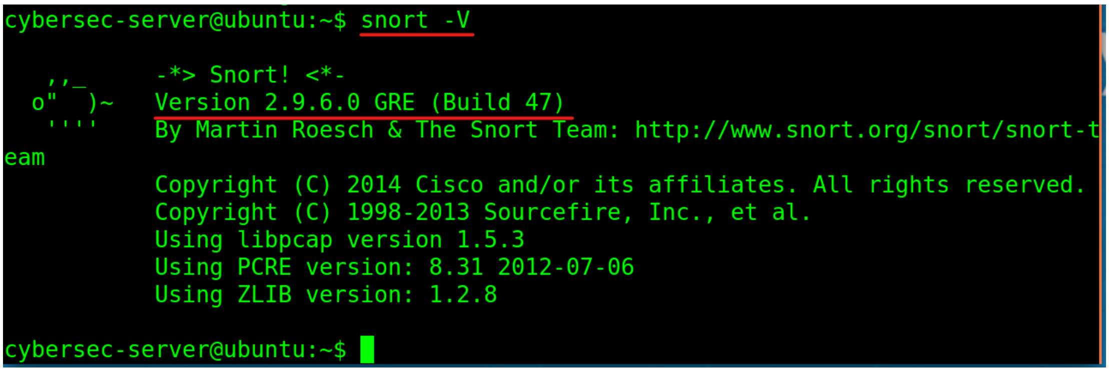
```
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 10.0.2.0/24
```

2) To start Snort:



```
cybersec-server@ubuntu:~$ sudo service snort start
[sudo] password for cybersec-server:
 * Starting Network Intrusion Detection System  snort
cybersec-server@ubuntu:~$
```

3) Check the version of Snort installed

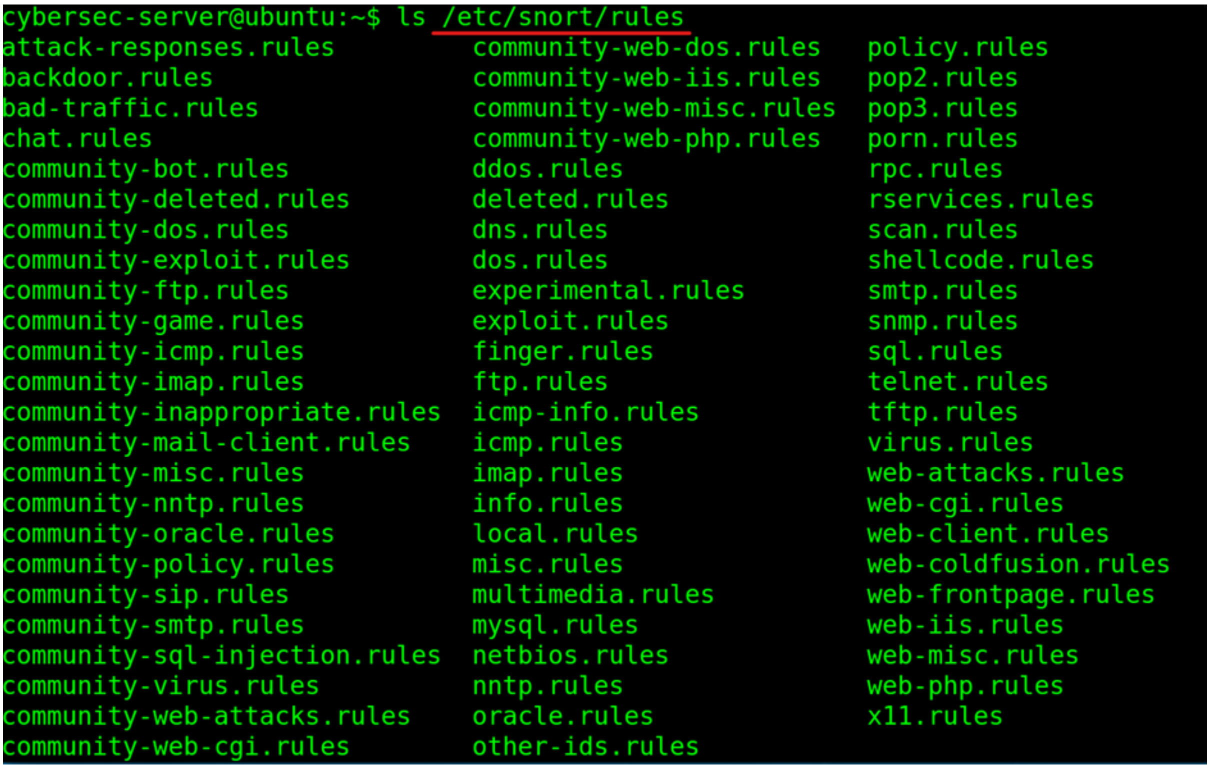


```
cybersec-server@ubuntu:~$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.5.3
           Using PCRE version: 8.31 2012-07-06
           Using ZLIB version: 1.2.8

cybersec-server@ubuntu:~$
```

Step2 Check Snort rules.

Snort is a signature-based IPS, and it defines rules to detect the intrusions. All rules of Snort are stored under /etc/snort/rules directory. All the rules are generally about one line in length and follow the same format.

The screenshot below shows all the rule files Snort has; you can download the latest rules at https://www.snort.org/downloads .



```
cybersec-server@ubuntu:~$ ls /etc/snort/rules
attack-responses.rules          community-web-dos.rules   policy.rules
backdoor.rules                  community-web-iis.rules   pop2.rules
bad-traffic.rules               community-web-misc.rules  pop3.rules
chat.rules                      community-web-php.rules   porn.rules
community-bot.rules             ddos.rules                rpc.rules
community-deleted.rules         deleted.rules             rservices.rules
community-dos.rules             dns.rules                 scan.rules
community-exploit.rules         dos.rules                 shellcode.rules
community-ftp.rules             experimental.rules        smtp.rules
community-game.rules            exploit.rules             snmp.rules
community-icmp.rules            finger.rules              sql.rules
community-imap.rules            ftp.rules                 telnet.rules
community-inappropriate.rules   icmp-info.rules           tftp.rules
community-mail-client.rules     icmp.rules                virus.rules
community-misc.rules            imap.rules                web-attacks.rules
community-nntp.rules            info.rules                web-cgi.rules
community-oracle.rules          local.rules               web-client.rules
community-policy.rules          misc.rules                web-coldfusion.rules
community-sip.rules             multimedia.rules          web-frontpage.rules
community-smtp.rules            mysql.rules               web-iis.rules
community-sql-injection.rules   netbios.rules             web-misc.rules
community-virus.rules           nntp.rules                web-php.rules
community-web-attacks.rules     oracle.rules              x11.rules
community-web-cgi.rules         other-ids.rules
```

Step 3 Add Snort rule.

Snort rules are divided into two logical sections:

1. Rule Header: The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, the source and destination ports information, and the direction of the flow. The direction operators <> and -> show traffic direction which to watch. Traffic can either flow in one direction or bi-directionally. The action can be alert, log, pass, drop etc.

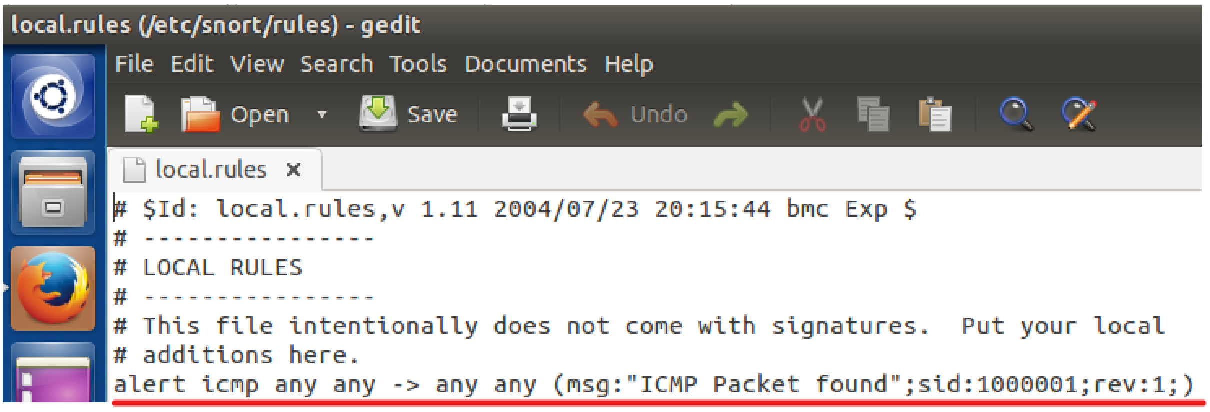
2. Rule Options: The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken. The rule options are separated using a semicolon “;”. Rule option keywords are separated from arguments using a colon “:”.

a) Use your favourite editor to add a rule to /etc/snort/rules/local.rules.

Add the following line into the local.rules file.

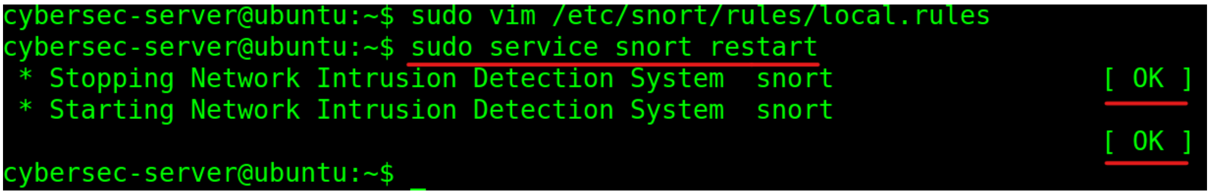
```
alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
```

This rule defines that an alert will be logged if an ICMP packet from any IP address is found. The signature ID(sid) should be greater than 1000000 for your own rules, here we use rule ID 1000001. Rev:1 is the revision number; this option allows for easier rule organization.


local.rules (/etc/snort/rules) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
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;)
```

b) Restart the snort service after adding the rule.



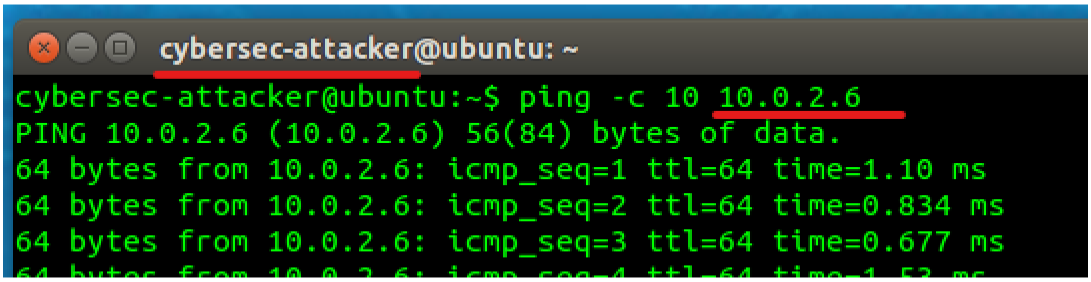
```
cybersec-server@ubuntu:~$ sudo vim /etc/snort/rules/local.rules
cybersec-server@ubuntu:~$ sudo service snort restart
 * Stopping Network Intrusion Detection System  snort                 [ OK ]
 * Starting Network Intrusion Detection System  snort
                                                                      [ OK ]
cybersec-server@ubuntu:~$ _
```

Note: You may receive [fail] message if there is error in the rule file, modify the rule file then restart the service.

You can use `sudo snort -T -i eth0 -c /etc/snort/snort.conf` to check the configuration file to find out the details of the error.

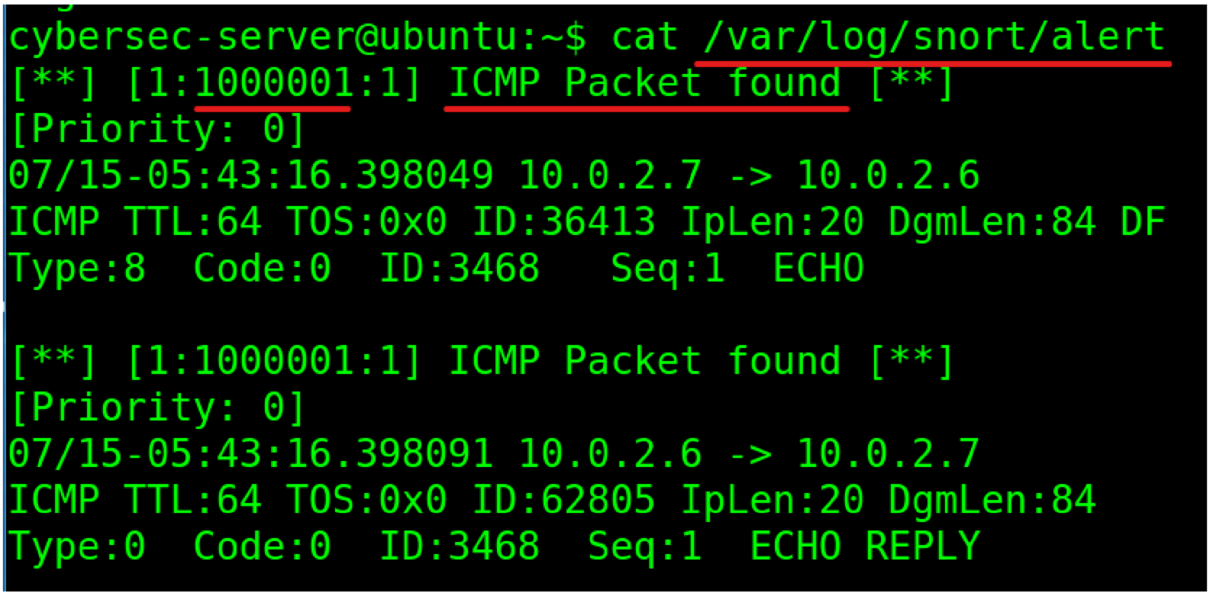
Step 4 Triggering an alert for the new rule.

Ping from attacker VM to the server.



```
cybersec-attacker@ubuntu:~$ ping -c 10 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=1.10 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.834 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.677 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=1.53 ms
```

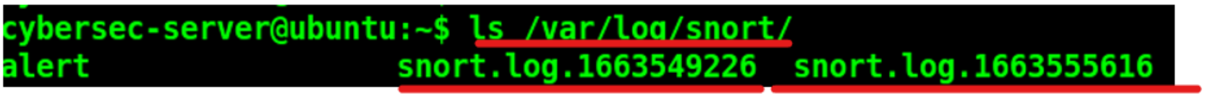
This ping will trigger alerts, the alerts are saved in /var/log/snort, read the alert.



```
cybersec-server@ubuntu:~$ cat /var/log/snort/alert
[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
07/15-05:43:16.398049 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:36413 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:3468   Seq:1  ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
07/15-05:43:16.398091 10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:62805 IpLen:20 DgmLen:84
Type:0  Code:0  ID:3468  Seq:1  ECHO REPLY
```

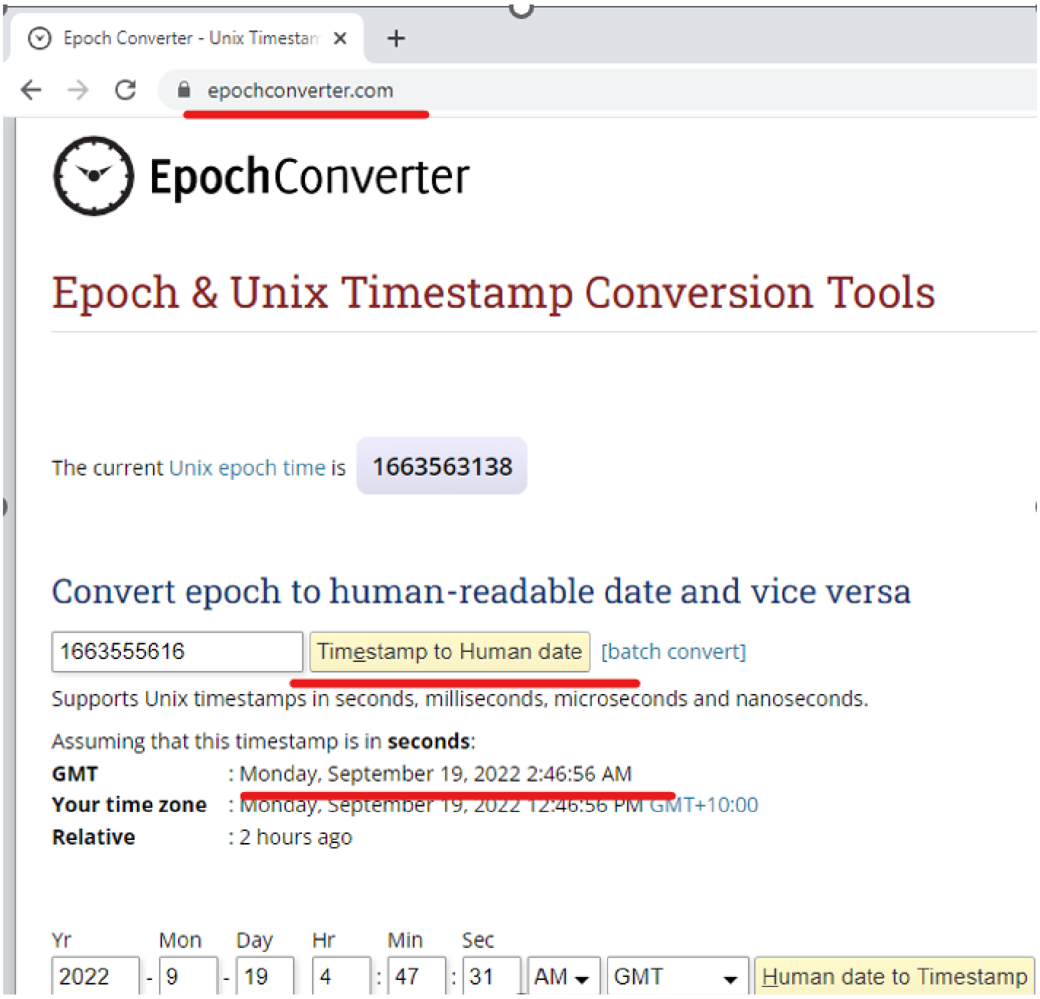
We can see the alert message is “ICMP Packet found” as we defined.

We can also verify the log file of the alert. The difference between log and alert is that each IP address gets its own log file for later analysis, while all alerts are stored in one common file.



```
cybersec-server@ubuntu:~$ ls /var/log/snort/
alert                  snort.log.1663549226  snort.log.1663555616
```

The number in the log file name indicate the time when the alert be generated, it is epoch time, it indicates the number of seconds that have elapsed since January1,1970. We can use epoch converter(like https://www.epochconverter.com/) to convert it to human readable time. (**Note:** your time will be different than the above screenshot)



Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is 1663563138

Convert epoch to human-readable date and vice versa

1663555616 | Timestamp to Human date | [batch convert]

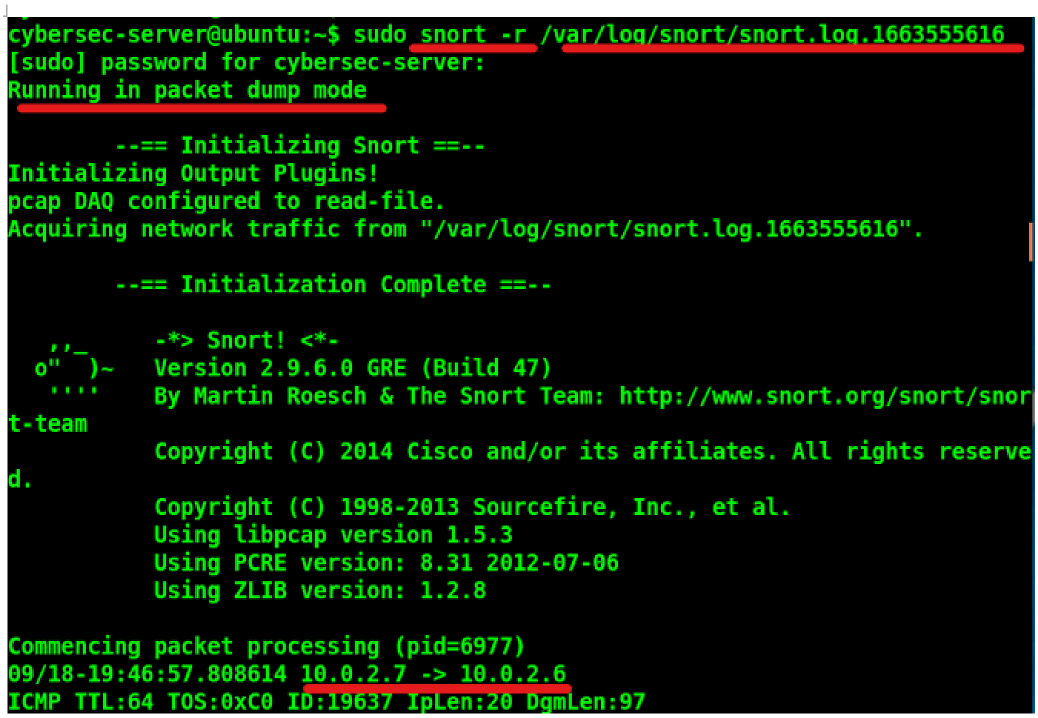
Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Monday, September 19, 2022 2:46:56 AM
Your time zone : Monday, September 19, 2022 12:46:56 PM GMT+10:00
Relative : 2 hours ago

Yr 2022 - Mon 9 - Day 19 Hr 4 : Min 47 : Sec 31 AM GMT | Human date to Timestamp

To read the log file, use “sudo snort -r /var/log/snort/snort.log.1663555616”



```
cybersec-server@ubuntu:~$ sudo snort -r /var/log/snort/snort.log.1663555616
[sudo] password for cybersec-server:
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to read-file.
Acquiring network traffic from "/var/log/snort/snort.log.1663555616".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snor
t-team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserve
d.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.5.3
           Using PCRE version: 8.31 2012-07-06
           Using ZLIB version: 1.2.8

Commencing packet processing (pid=6977)
09/18-19:46:57.808614 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0xC0 ID:19637 IpLen:20 DgmLen:97
```

Step 5: Now let's start Snort in IDS mode and tell it to display alerts to the console, then ping from Cybersec-Attacker VM again, you will see the message on the console.

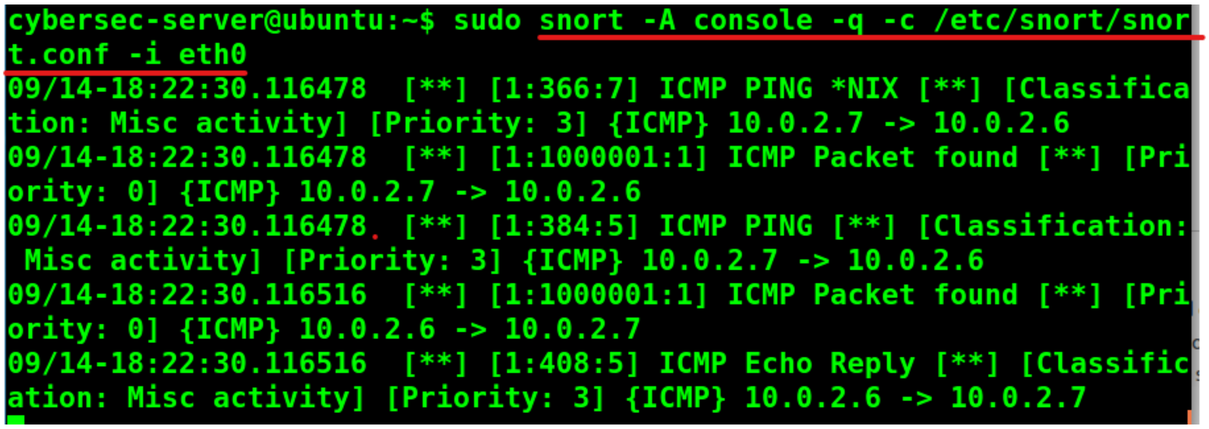
```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

-c point Snort to the configuration file

-A print alerts to standard output

-q is for "quiet" mode (not showing banner and status report).

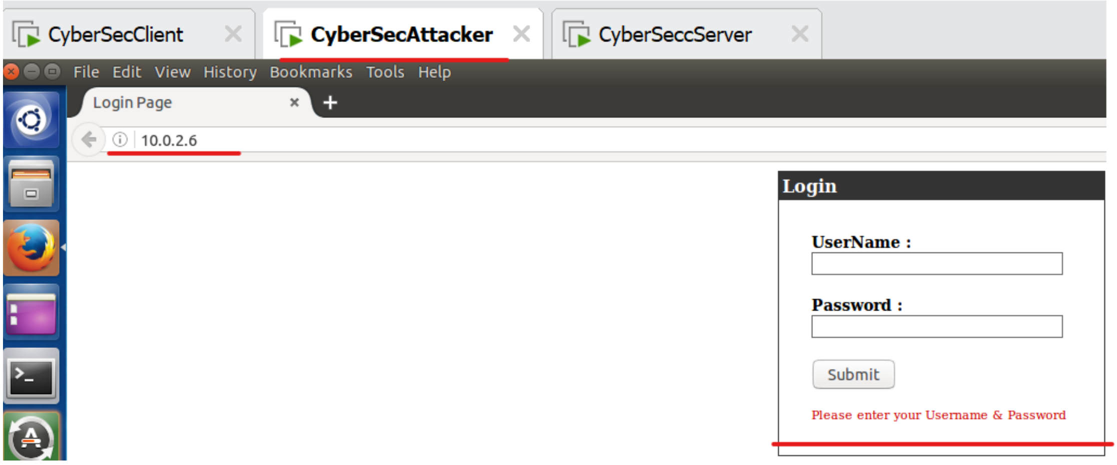
You shouldn't see any output when you enter the command because Snort hasn't detected any activity specified in the rule we wrote. Now ping from Cybersec-Attack VM to server, you will see the massages are displayed to console. Ctrl+c to stop it.



```
cybersec-server@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snor
t.conf -i eth0
09/14-18:22:30.116478  [**] [1:366:7] ICMP PING *NIX [**] [Classifica
tion: Misc activity] [Priority: 3] {ICMP} 10.0.2.7 -> 10.0.2.6
09/14-18:22:30.116478  [**] [1:1000001:1] ICMP Packet found [**] [Pri
ority: 0] {ICMP} 10.0.2.7 -> 10.0.2.6
09/14-18:22:30.116478  [**] [1:384:5] ICMP PING [**] [Classification:
 Misc activity] [Priority: 3] {ICMP} 10.0.2.7 -> 10.0.2.6
09/14-18:22:30.116516  [**] [1:1000001:1] ICMP Packet found [**] [Pri
ority: 0] {ICMP} 10.0.2.6 -> 10.0.2.7
09/14-18:22:30.116516  [**] [1:408:5] ICMP Echo Reply [**] [Classific
ation: Misc activity] [Priority: 3] {ICMP} 10.0.2.6 -> 10.0.2.7
```

Step6: let's write a more specific rule to generate alert for web service

a) Start web browser in attacker VM to access 10.0.2.6



Login

UserName :

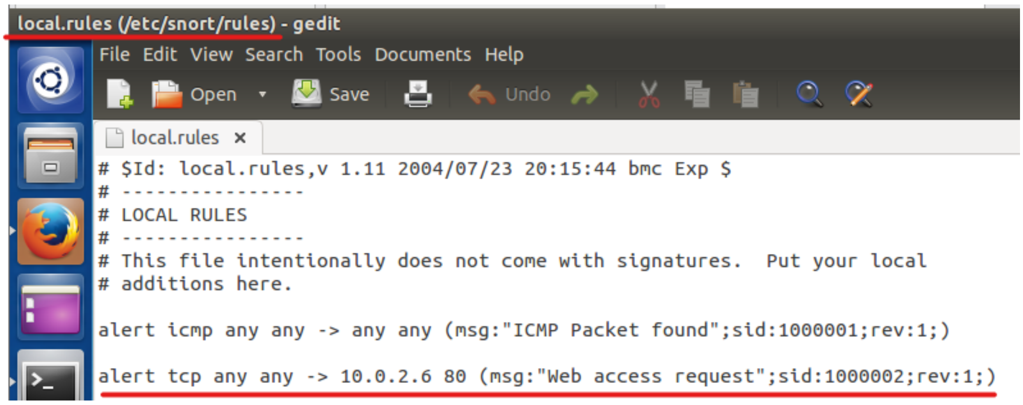
Password :

Submit

Please enter your Username & Password

b) Open our local.rules file in a text editor and add new rule to generate alert when there is web access reqest

```
sudo gedit /etc/snort/rules/local.rules
```

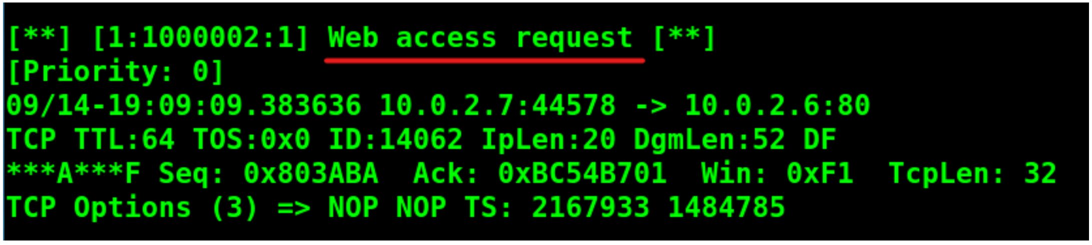

local.rules (/etc/snort/rules) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
local.rules

```
# $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;)
```

c) Restart the snort service
sudo service snort restart

d) Refresh the webpage in attacker VM

e) Check the alert file, you will see the alert message “Web access request”
cat /var/log/snort/alert

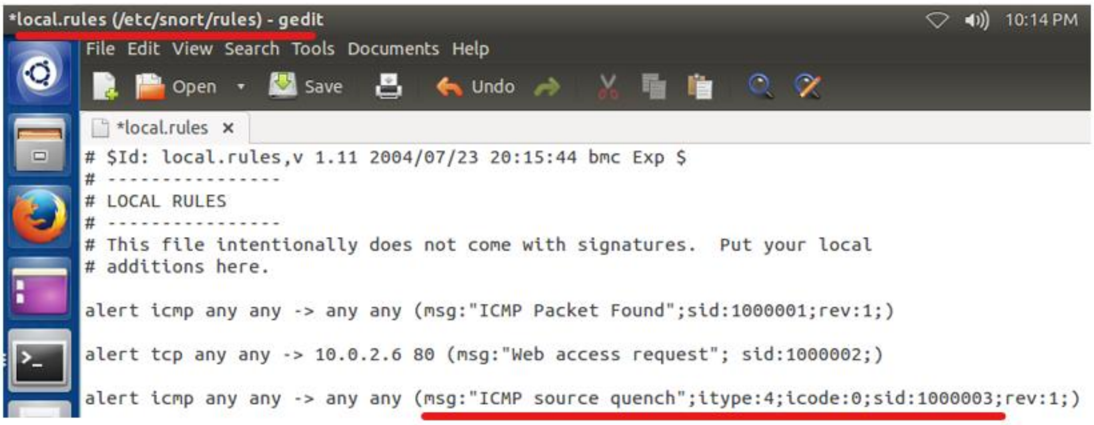


```
[**] [1:1000002:1] Web access request [**]
[Priority: 0]
09/14-19:09:09.383636 10.0.2.7:44578 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:14062 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x803ABA  Ack: 0xBC54B701  Win: 0xF1  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2167933 1484785
```

Step7: Add another rule to generate alert for ICMP source quench packet.

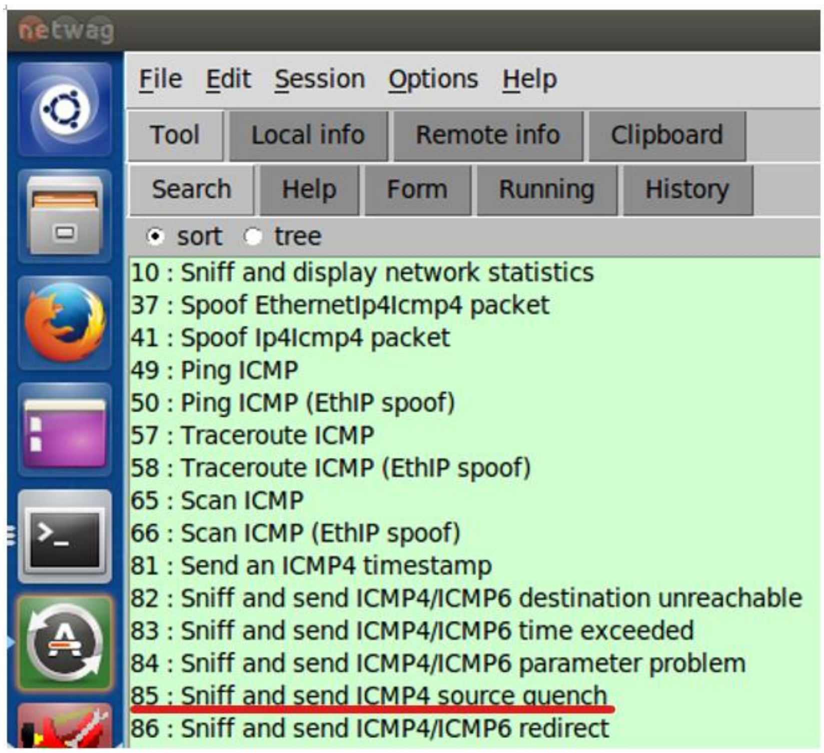
Recall the ICMP attack lab we did last week, we used **netwag** to launch ICMP Source Quench attack. ICMP packet has “type” and “code” filed, type 4 is for Source Quench, the code field is not used for Source Quench message and this filed is set to 0.

Add the following rule to the local rule file then restart snort.
alert icmp any any -> any any (msg:"ICMP source uench"; itype:4; icode:0; sid:1000003; rev:1;)


*local.rules (/etc/snort/rules) - gedit
10:14 PM
File Edit View Search Tools Documents Help
Open
Save
Undo
*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;)

alert icmp any any -> any any (msg:"ICMP source quench";itype:4;icode:0;sid:1000003;rev:1;)
```

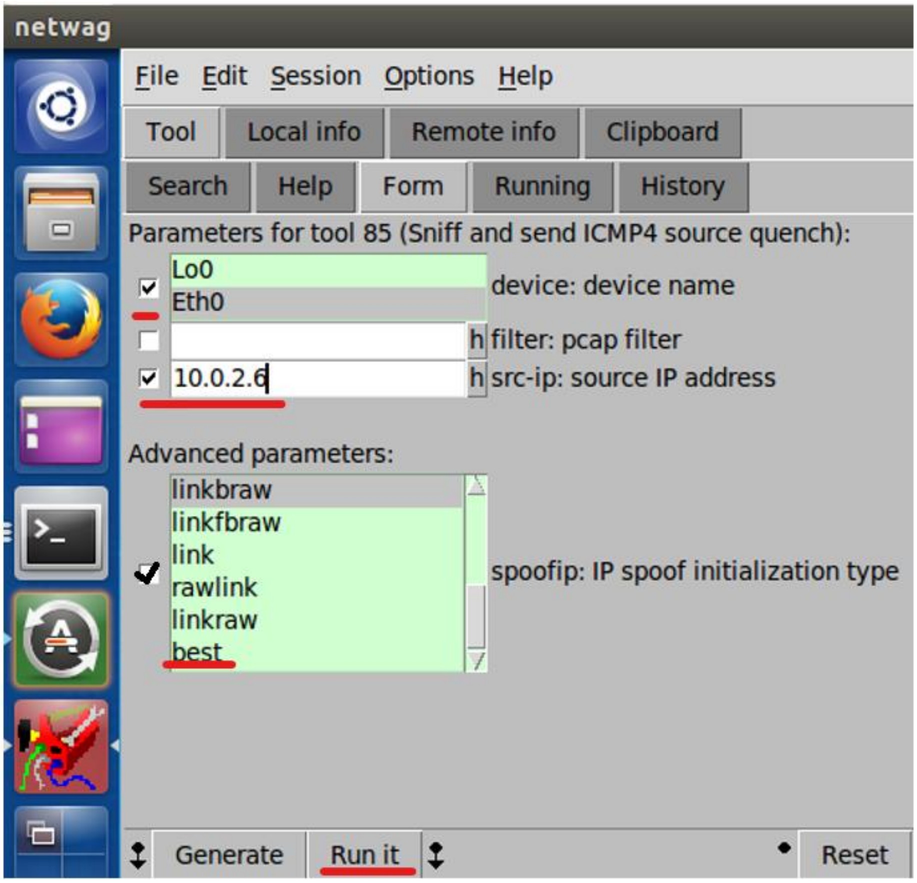
Now start the **netwag** on attacker’s VM, search for ICMP source quench.


netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History

● sort ○ tree

10 : Sniff and display network statistics
37 : Spoof EthernetIp4Icmp4 packet
41 : Spoof Ip4Icmp4 packet
49 : Ping ICMP
50 : Ping ICMP (EthIP spoof)
57 : Traceroute ICMP
58 : Traceroute ICMP (EthIP spoof)
65 : Scan ICMP
66 : Scan ICMP (EthIP spoof)
81 : Send an ICMP4 timestamp
82 : Sniff and send ICMP4/ICMP6 destination unreachable
83 : Sniff and send ICMP4/ICMP6 time exceeded
84 : Sniff and send ICMP4/ICMP6 parameter problem
85 : Sniff and send ICMP4 source quench
86 : Sniff and send ICMP4/ICMP6 redirect

Fill in the source quench form, change the source IP address to 10.0.2.6 and run it.


netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Generate
Run it
Reset

Parameters for tool 85 (Sniff and send ICMP4 source quench):

☑ Lo0 / Eth0 — device: device name

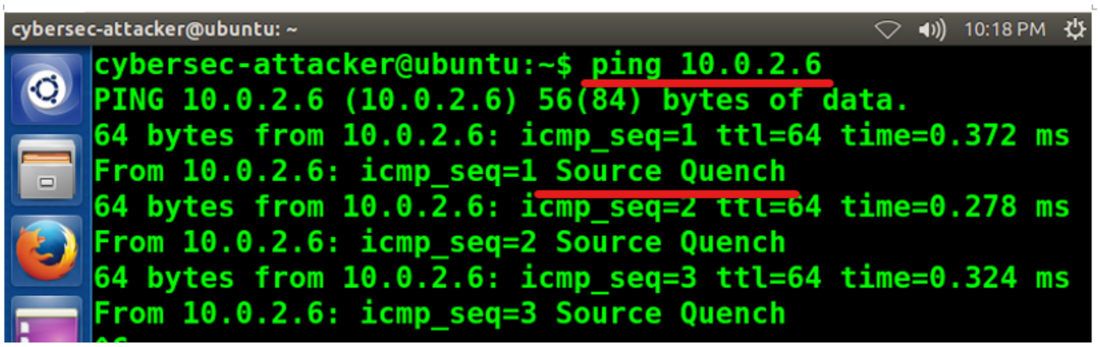
□ h filter: pcap filter

☑ 10.0.2.6 h src-ip: source IP address

Advanced parameters:

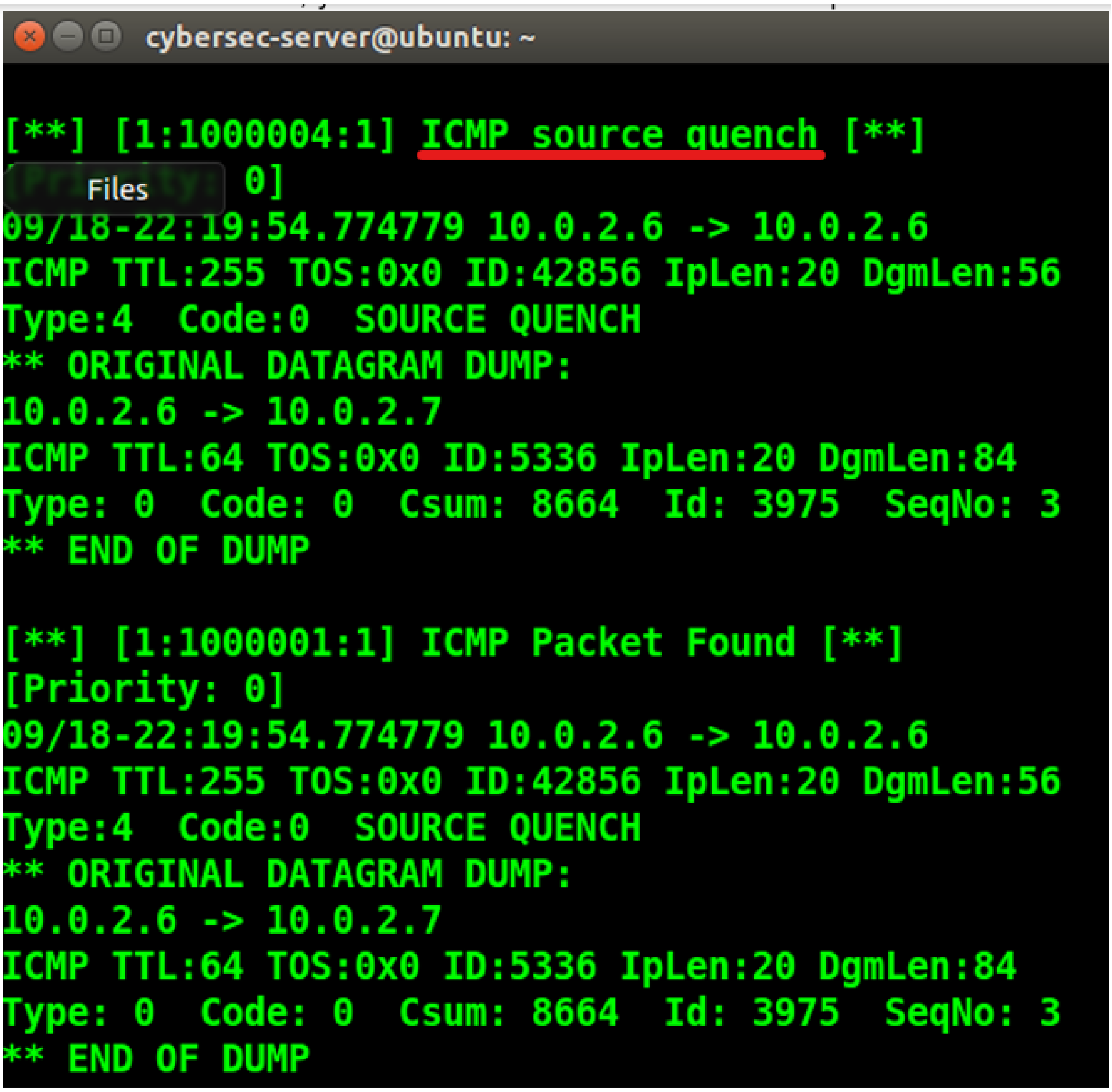
✓ linkbraw / linkfbraw / link / rawlink / linkraw / best — spoofip: IP spoof initialization type

Open another terminal in the attacker’s VM to ping the server.



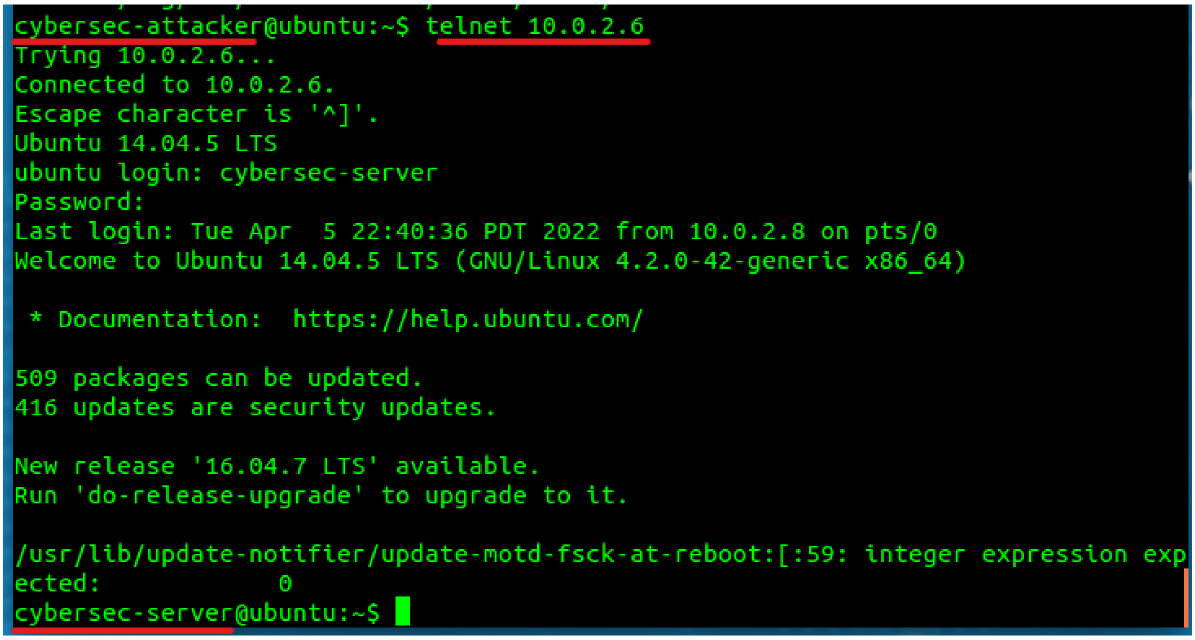
```
cybersec-attacker@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.372 ms
From 10.0.2.6: icmp_seq=1 Source Quench
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.278 ms
From 10.0.2.6: icmp_seq=2 Source Quench
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.324 ms
From 10.0.2.6: icmp_seq=3 Source Quench
```

Check the snort alert, you should see the alert for source quench attack.



```
[**] [1:1000004:1] ICMP source quench [**]
[Priority: 0]
09/18-22:19:54.774779 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:42856 IpLen:20 DgmLen:56
Type:4  Code:0  SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:5336 IpLen:20 DgmLen:84
Type: 0  Code: 0  Csum: 8664  Id: 3975  SeqNo: 3
** END OF DUMP

[**] [1:1000001:1] ICMP Packet Found [**]
[Priority: 0]
09/18-22:19:54.774779 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:42856 IpLen:20 DgmLen:56
Type:4  Code:0  SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.7
ICMP TTL:64 TOS:0x0 ID:5336 IpLen:20 DgmLen:84
Type: 0  Code: 0  Csum: 8664  Id: 3975  SeqNo: 3
** END OF DUMP
```

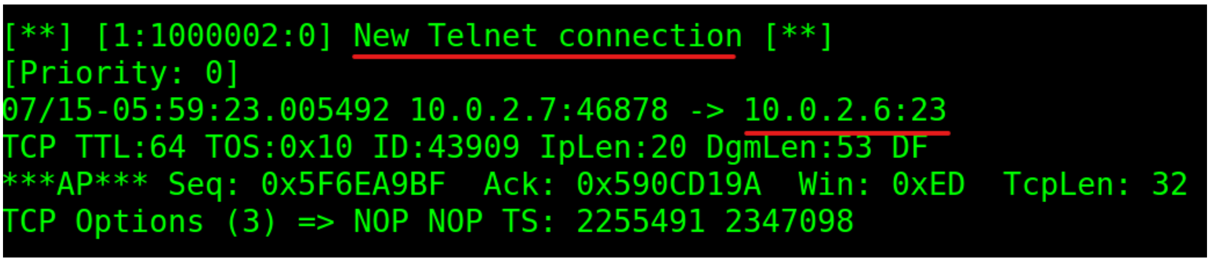
Challenge: test telnet from Attacker VM to Server VM.



```
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: Tue Apr  5 22:40:36 PDT 2022 from 10.0.2.8 on pts/0
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.2.0-42-generic x86_64)

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

509 packages can be updated.
416 updates are security updates.

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

/usr/lib/update-notifier/update-motd-fsck-at-reboot:[:59: integer expression exp
ected:             0
cybersec-server@ubuntu:~$ 
```

Now add a rule so that Snort will generate an alert with the message “new telnet connection” if someone tries to Telnet to Cybersec-Server through port 23. (Hint: telnet runs on top of tcp).

The alert should include the information for the telnet connection like below.



```
[**] [1:1000002:0] New Telnet connection [**]
[Priority: 0]
07/15-05:59:23.005492 10.0.2.7:46878 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:43909 IpLen:20 DgmLen:53 DF
***AP*** Seq: 0x5F6EA9BF  Ack: 0x590CD19A  Win: 0xED  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2255491 2347098
```

Hint: Snort’s rule syntax and configuration: http://manual.snort.org/node27.html