

SNORT

- Most popular open-source intrusion prevention system: does traffic analysis + packet logging on IP networks
- Defines malicious network activity
- Finds packets that match against them, generating alerts
- Three primary uses: packet sniffer, packet logger for network traffic debugging, full-blown network intrusion prevention system

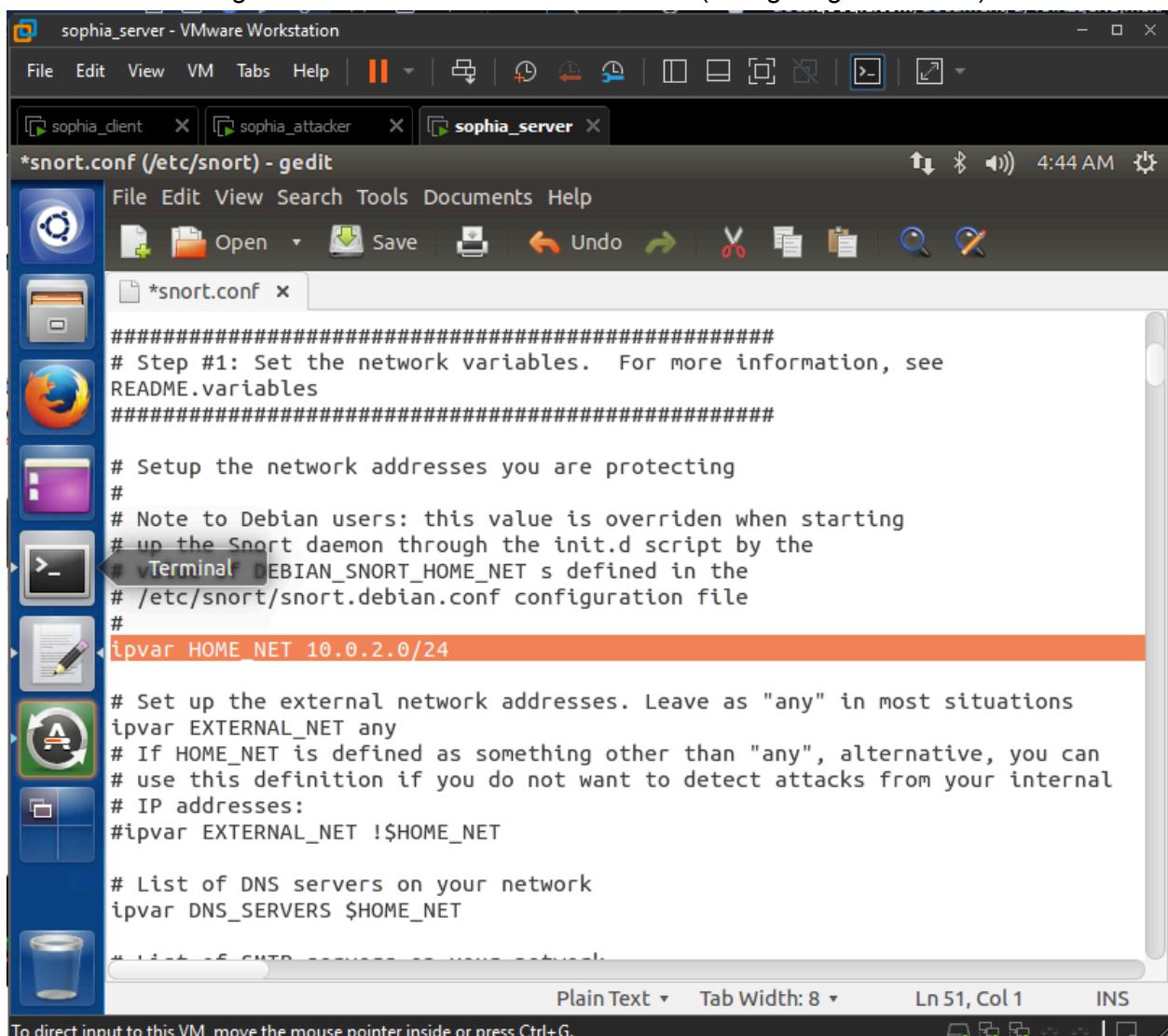
LAB ENVIRONMENT

- Server, Attacker VM
- 10.0.2.6 is server, 10.0.2.7 is attacker and 10.0.2.8 client

SNORT RULES

STEPS

1. Enter sudo gedit /etc/snort/snort.conf in serverVM (configuring snort rules)



```
File Edit View Tools Documents Help
  Open Save Undo Redo Cut Copy Paste Find Replace
  *snort.conf x

#####
# 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 overridden when starting
# up the Snort daemon through the init.d script by the
# vTerminal DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 10.0.2.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
```

2. Enter sudo service snort start
3. Enter snort -V
4. Enter ls /etc/snort/rules (checks snort rules)

The screenshot shows a VMware Workstation interface with a window titled "sophia_server - VMware Workstation". Inside, there are three terminal tabs:

- sophia_client**: Shows the desktop environment with icons for the terminal, file manager, browser, and others.
- sophia_attacker**: Shows a terminal session with the command `ls /etc/snort/rules` outputting several files like `snort.conf`, `local.rules`, etc.
- sophia_server**: Shows a terminal session with the following commands and output:

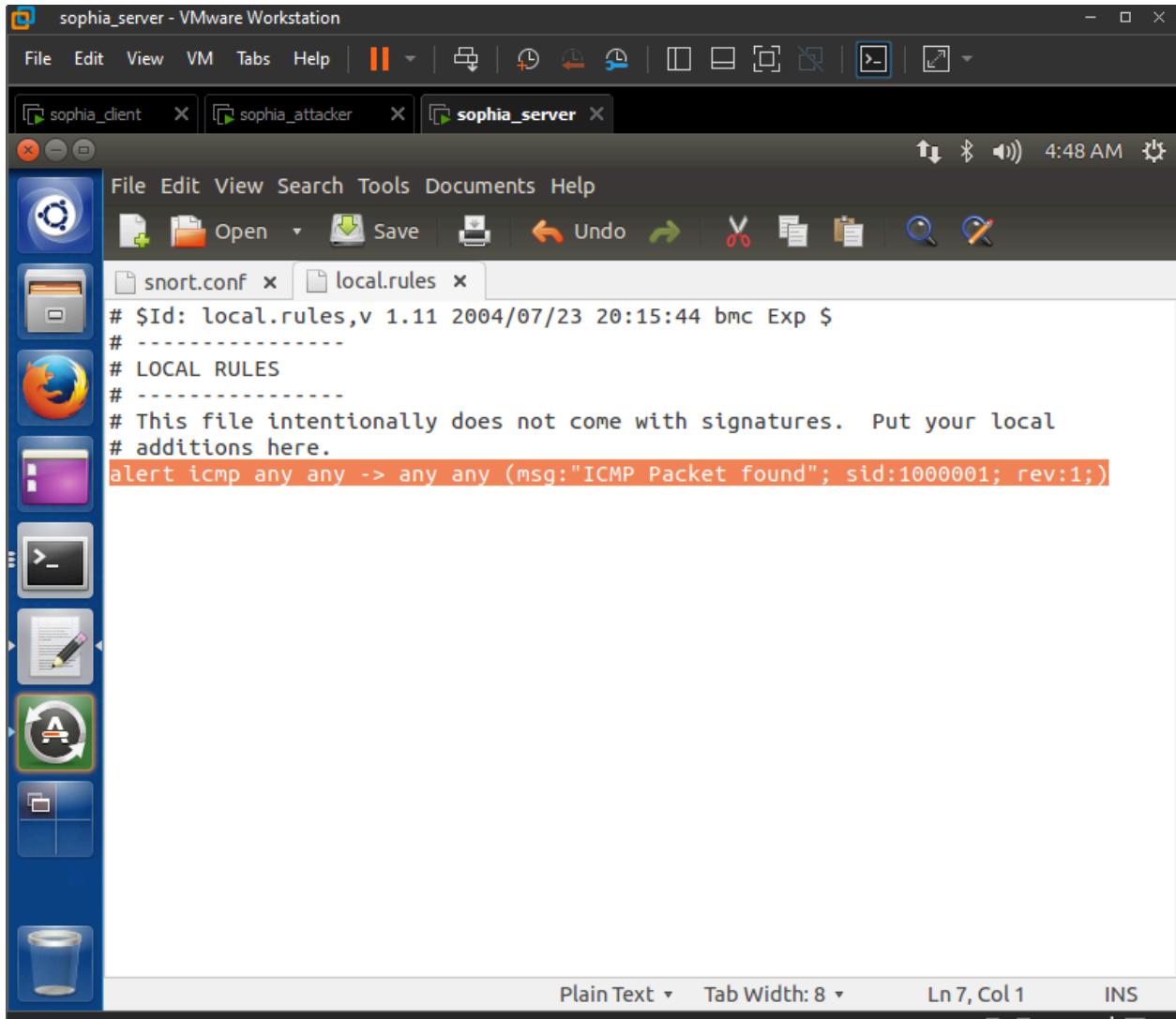

```
cybersec-server@ubuntu:~$ sudo gedit /etc/snort/snort.conf
[sudo] password for cybersec-server:
(gedit:3293): IBUS-WARNING **: The owner of /home/cybersec-server/.config/ibus/bus is not root!
cybersec-server@ubuntu:~$ sudo service snort start
[sudo] password for cybersec-server:
* Starting Network Intrusion Detection System snort [ OK ]
cybersec-server@ubuntu:~$ snort -V
[...]
--> Snort! <-
Version 2.9.6.0 GRE (Build 47)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
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
```

The terminal window has a dark theme, and the status bar at the bottom indicates "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

TASK 1: ADDING A RULE FOR ICMP PACKETS

STEPS

1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM
2. Add "alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)" in file



The screenshot shows a Linux desktop environment within a VMware Workstation window titled "sophia_server - VMware Workstation". The desktop has a dark theme with a dock on the left containing icons for various applications like a terminal, file manager, and browser. A terminal window is open, showing the following Snort configuration code:

```
# $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;)
```

3. Enter sudo service snort restart

4. Enter ping 10.0.2.6 in attackerVM

5. Enter cat /var/log/snort/alert in serverVM

```
[Priority: 0]
09/23/04:50:34.043217 10.0.2.7 -> 10.0.2.6
#ICMP TTL:64 TOS:0x0 ID:20560 IpLen:20 DgmLen:84 DF
#Type:8 Code:0 ID:3215 Seq:63 ECHO
#
#[**] [1:1000001:1] ICMP Packet found [**]
#[Priority: 0]
#09/23/04:50:34.043234 10.0.2.6 -> 10.0.2.7
#ICMP TTL:64 TOS:0x0 ID:20498 IpLen:20 DgmLen:84
#Type:0 Code:0 ID:3215 Seq:63 ECHO REPLY
a

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/23/04:50:35.043208 10.0.2.7 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:20607 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:3215 Seq:64 ECHO
#
#[**] [1:1000001:1] ICMP Packet found [**]
#[Priority: 0]
#09/23/04:50:35.043225 10.0.2.6 -> 10.0.2.7
#ICMP TTL:64 TOS:0x0 ID:20564 IpLen:20 DgmLen:84
#Type:0 Code:0 ID:3215 Seq:64 ECHO REPLY
cybersec-server@ubuntu:~$
```

QUESTION 1. Have you received alert messages for ICMP Packets? Please provide screenshot to support your answer

- Ls /var/log/snort/ in serverVM
- Enter sudo snort -r /var/log/snort/snort.log.1663555616" in server VM

TASK 2: SNORT IN IDS MODE AND DISPLAYING ALERTS TO CONSOLE

WISHLIST STEPS

1. Enter sudo snort -A console -q -c /etc/snort/snort.conf -i eth0 in severVM
 2. Enter ping 10.0.2.6 in attackerVM

```
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=0.359 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.281 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.324 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.300 ms
64 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.253 ms
64 bytes from 10.0.2.6: icmp_seq=6 ttl=64 time=0.286 ms
64 bytes from 10.0.2.6: icmp_seq=7 ttl=64 time=0.329 ms
64 bytes from 10.0.2.6: icmp_seq=8 ttl=64 time=0.303 ms
64 bytes from 10.0.2.6: icmp_seq=9 ttl=64 time=0.266 ms
64 bytes from 10.0.2.6: icmp_seq=10 ttl=64 time=0.253 ms
64 bytes from 10.0.2.6: icmp_seq=11 ttl=64 time=0.299 ms
64 bytes from 10.0.2.6: icmp_seq=12 ttl=64 time=0.239 ms
64 bytes from 10.0.2.6: icmp_seq=13 ttl=64 time=0.276 ms
64 bytes from 10.0.2.6: icmp_seq=14 ttl=64 time=0.303 ms
64 bytes from 10.0.2.6: icmp_seq=15 ttl=64 time=0.280 ms
```

QUESTION 2. Have you received alert messages for ICMP Packets in IDS Mode? Please provide a screenshot to support your answer.

```
ICMP] 10.0.2.6 -> 10.0.2.7
09/23-05:03:22.031068  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.2.6 -> 10.0.2.7
09/23-05:03:23.031196  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.2.7 -> 10.0.2.6
09/23-05:03:23.031196  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 10.0.2.7 -> 10.0.2.6
09/23-05:03:23.031196  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.2.7 -> 10.0.2.6
[Show Desktop].031217  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 10.0.2.7 -> 10.0.2.7
09/23-05:03:23.031217  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.2.6 -> 10.0.2.7
09/23-05:03:24.031408  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.2.7 -> 10.0.2.6
09/23-05:03:24.031408  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 10.0.2.7 -> 10.0.2.6
09/23-05:03:24.031408  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.2.7 -> 10.0.2.6
09/23-05:03:24.031431  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 10.0.2.6 -> 10.0.2.7
09/23-05:03:24.031431  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.2.6 -> 10.0.2.7
```

TASK 3: GENERATING ALERTS FOR WEB SERVICE

STEPS

1. Enter 10.0.2.6 in web browser of attackerVM
2. Enter sudo gedit /etc/snort/rules/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 tcp any any -> 10.0.2.6 80 (msg:"Web access request";sid:1000002;rev:1;)
```

3. Enter sudo service snort restart
4. Refresh the webpage in Attacker VM
5. Enter cat /var/log/snort/alert

QUESTION 3. Have you received alert messages for Web access? Please provide a screenshot to support your answer.

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
#  
# sophiapineda - cybersec-server@ubuntu: ~  
# TCP Options (3) => NOP NOP TS: 801846 802577  
#  
# [**] [1:1000002:1] Web access request [**]  
a[Priority: 0]  
09/23-05:09:30.973689 10.0.2.7:56856 -> 10.0.2.6:80  
TCP TTL:64 TOS:0x0 ID:37017 Iplen:20 DgmLen:394 DF  
***AP*** Seq: 0xA6EFAF34 Ack: 0x7565B69E Win: 0x116 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 802016 802577  
  
[**] [1:1000002:1] Web access request [**]  
[Priority: 0]  
09/23-05:09:30.974545 10.0.2.7:56856 -> 10.0.2.6:80  
TCP TTL:64 TOS:0x0 ID:37018 Iplen:20 DgmLen:52 DF  
***A*** Seq: 0xA6EFB08A Ack: 0x7565B9B9 Win: 0x123 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 802016 802747  
  
[**] [1:1000002:1] Web access request [**]  
[Priority: 0]  
09/23-05:09:35.976380 10.0.2.7:56856 -> 10.0.2.6:80  
TCP TTL:64 TOS:0x0 ID:37019 Iplen:20 DgmLen:52 DF  
***A***F Seq: 0xA6EFB08A Ack: 0x7565B9BA Win: 0x123 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 803267 803998  
  
cybersec-server@ubuntu:~$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

TASK 4: GENERATING ALERTS FOR ICMP SOURCE QUENCH PACKETS

STEPS

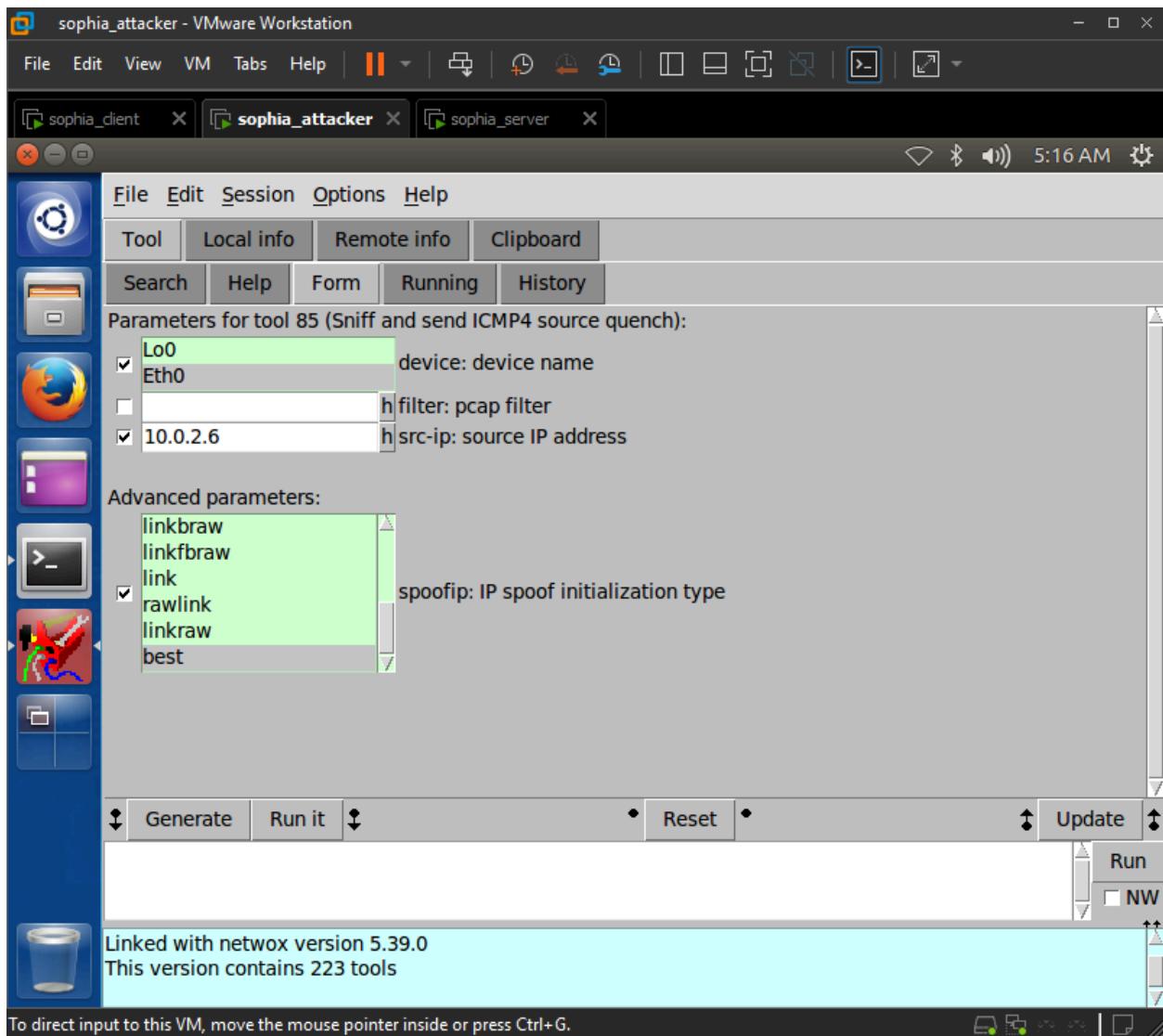
1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM
2. Add "alert icmp any any -> any any (msg:"ICMP source uench"; itype:4; icode:0; sid:1000003; rev:1;)"

The screenshot shows a Linux desktop environment within a VMware Workstation window. The desktop has a blue theme with various icons on the left. A terminal window titled 'sophia_server' is open, displaying a configuration file named 'local.rules'. The file content is as follows:

```
# $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 source
quench";itype:4;icode:0;sid:1000003;rev:1;)
```

The terminal window also shows status information at the bottom: 'Plain Text', 'Tab Width: 8', 'Ln 7, Col 1', and 'INS'. A status bar at the very bottom indicates: 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G'.

3. Enter sudo netwoq in attackerVM. tool 85. 10.0.2.6



4. Ping 10.0.2.6 in clientVM

5. Enter cat /var/log/snort/alert in serverVM

QUESTION 4. Have you received alert messages for Source Quench packets? Please provide a screenshot to support your answer.

The screenshot shows a VMware Workstation window with several open tabs at the top: "sophia_client", "sophia_attacker", and "sophia_server". The "sophia_server" tab is active, displaying a terminal session. The terminal window title is "sophiapineda - cybersec-server@ubuntu: ~". The session output is as follows:

```
cybersec-server@ubuntu:~$ sudo gedit /etc/snort/rules/local.rules
[sudo] password for cybersec-server:
(gedit:3967): IBUS-WARNING **: The owner of /home/cybersec-server/.config/ibus/bus is not root!
sophiapineda - cybersec-server@ubuntu: ~
(** ORIGINAL DATAGRAM DUMP:
P 10.0.2.6 -> 10.0.2.8
b) ICMP TTL:64 TOS:0x0 ID:35668 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 32396 Id: 3076 SeqNo: 65
(** END OF DUMP
P [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/id/2666]

[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
09/23-05:17:12.107124 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:61006 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:35898 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 11657 Id: 3076 SeqNo: 66
** 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/id/2666]

cybersec-server@ubuntu:~$
```

TASK 5: RUNNING SNORT AS INTRUSION PREVENTION SYSTEM

WORKS

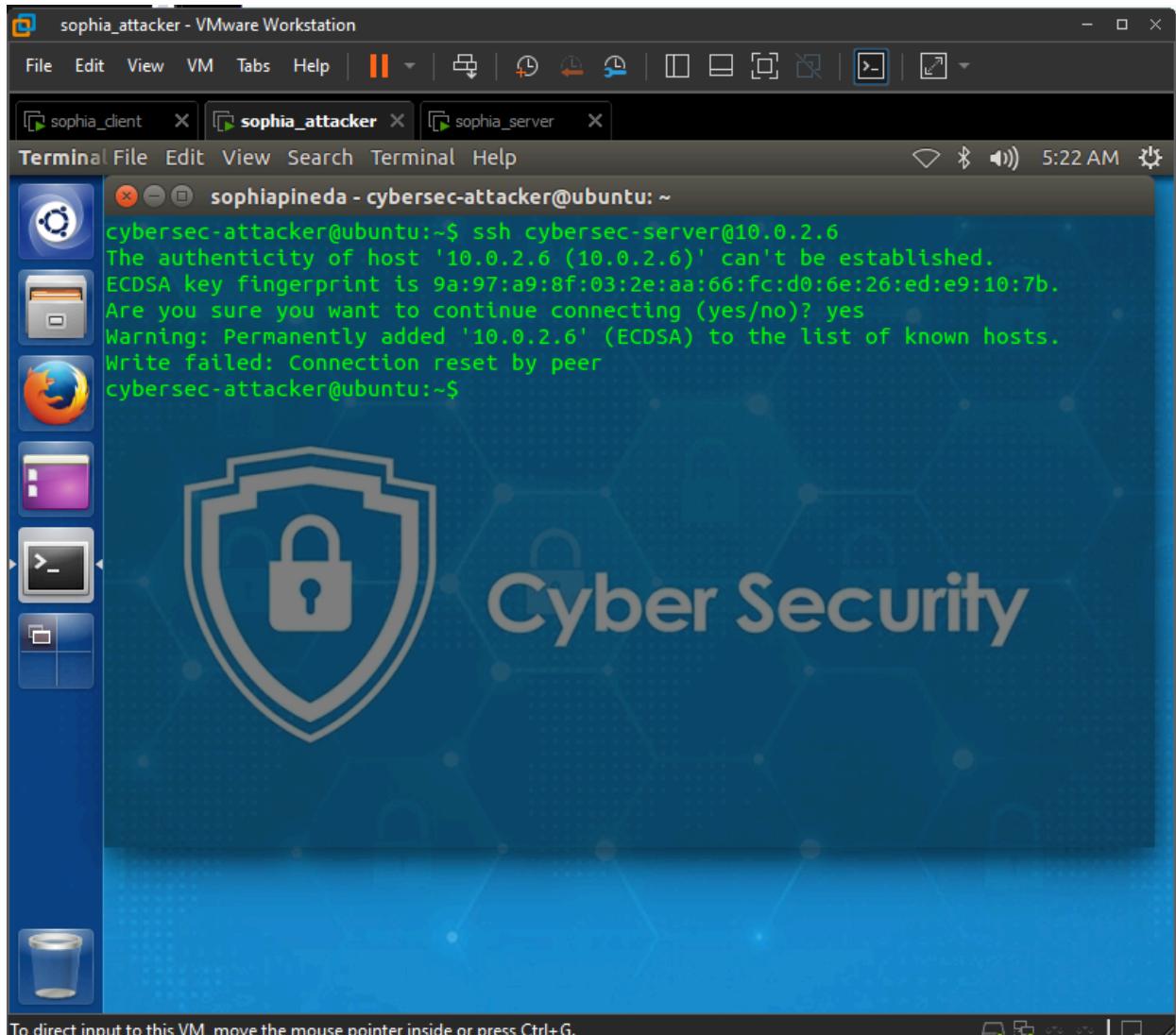
1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM
 2. Add “reject tcp any any -> 10.0.2.6 22 (msg:”SSH Connection Attempt(Request not Accepted)”;sid:1000004;rev:1;)” in file

The screenshot shows a Linux desktop environment with several open windows. At the top, there's a VMware Workstation toolbar with icons for file operations, tabs, and system status. Below it is a window manager toolbar with icons for window control and system status. The main window is a terminal titled "gedit" showing the contents of "/etc/snort/rules/local.rules". The terminal window has a dark theme with light-colored text. The terminal content includes a header, a section for local rules, and a note about not including signatures. A specific rule is highlighted in orange:

```
# $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.  
ShowDesktop / any -> 10.0.2.6 22 (msg:"SSH Connection Attempt(Request not  
Accepted)";sid:1000004;rev:1;)
```

The desktop background is blue, and the taskbar on the left shows icons for various applications like a terminal, file manager, and browser.

3. Enter sudo service snort restart
 4. Enter ssh cybersec-server@10.0.2.6 in attackerVM



5. Enter cat /var/log/snort/alert in serverVM

QUESTION 5. Have you received alert messages for SSH connection Attempt? Did the connection attempt succeed? Please provide a screenshot to support your answer.

TASK 6: GENERATE ALERTS FOR TELNET CONNECTION ATTEMPTS FROM ATTACKER TO SERVER AND REJECT TELNET CONNECTION ATTEMPTS FROM ATTACKER STEPS

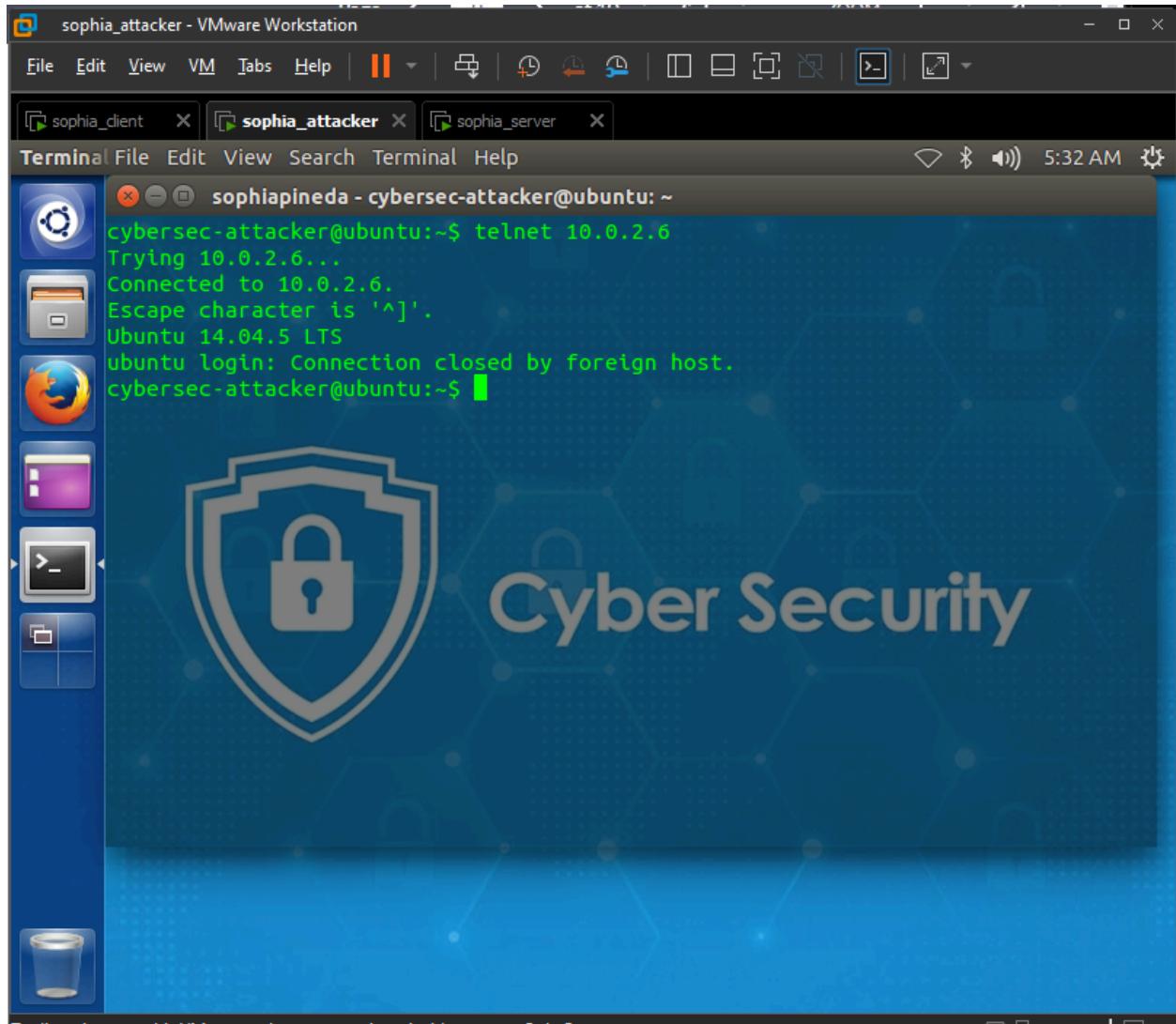
1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM
reject tcp any any -> 10.0.2.6 23 (msg:"Telnet Connection Attempt(Request not Accepted)":sid:1000004;rev:1;)

The screenshot shows a Linux desktop environment with several windows open. The main window is a terminal titled "local.rules (/etc/snort/rules) - gedit" displaying Snort configuration rules. The terminal content includes:

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
Firefox Web Browser.
# This file intentionally does not come with signatures. Put your local
# additions here.
reject tcp any any -> 10.0.2.6 23 (msg:"Telnet Connection Attempt(Request not
Accepted)";sid:1000004;rev:1;)
```

The desktop interface includes a dock on the left with icons for various applications like a terminal, file manager, and browser. The top bar shows the title "sophia_server - VMware Workstation" and standard window controls. The status bar at the bottom indicates "Plain Text" mode, a tab width of 8, and the current position as "Ln 7, Col 1".

2. Enter sudo service snort restart
 3. Enter telnet 10.0.2.6 from attackerVM



4. Enter cat /var/log/snort/alert in serverVM

QUESTION 6. Have you received alert messages for Telnet connection established from Attacker to Server? Did the telnet connection attempt from Attacker to Server succeed? Please provide a screenshot to support your answer. Also, mention the rule that was added to "local.rules" to create this alert.

