

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.

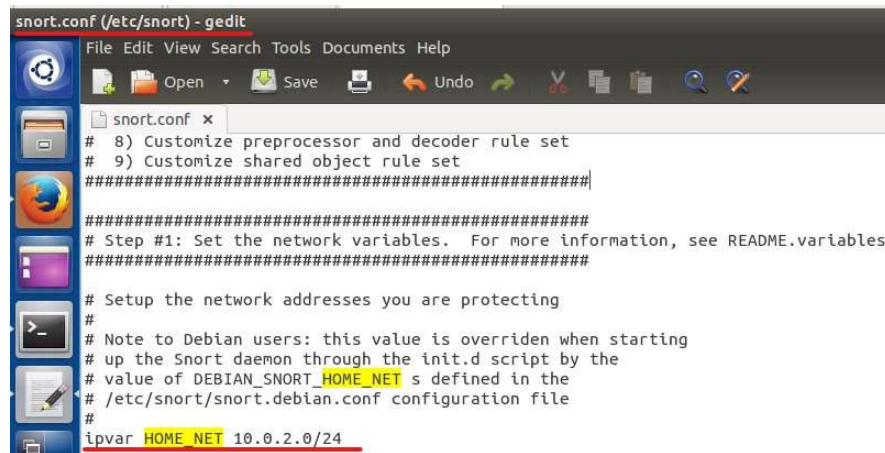
Required resources:

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

Objective: 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`



- 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

  ,,-_
 o" )~
  ' '

-*> Snort! <*-
Version 2.9.6.0 GRE (Build 47)
By Martin Roesch & The Snort Team: http://www.snort.org/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

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 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

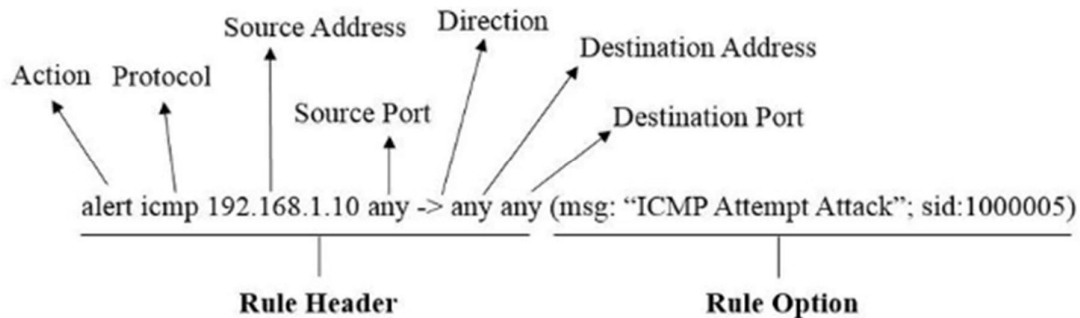
```

Step 3 Add Snort rule.

Snort rules are divided into two logical sections:

1. **Rule Header:** The rule header contains the rule's action (**e.g., alert, log, pass, drop, reject, sdrop**), 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 “:”.



Task 1: Adding a Rule for ICMP Packets.

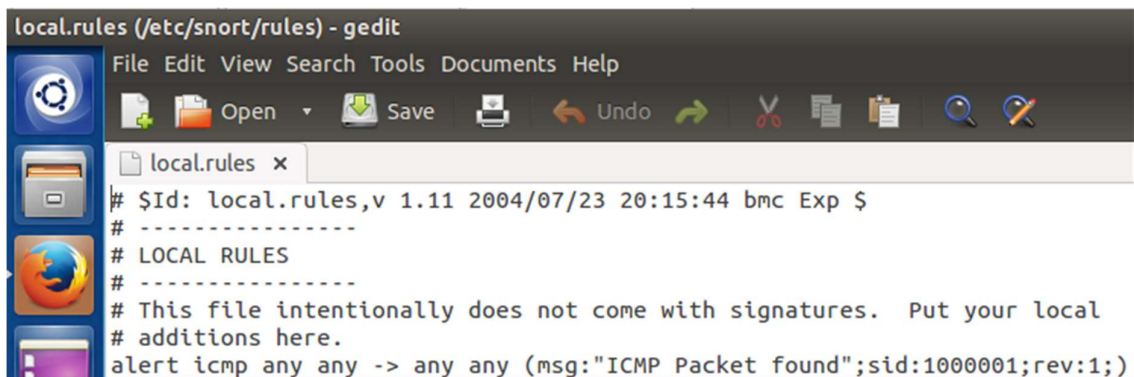
- a. Use a text editor to add a rule to `/etc/snort/rules/local.rules`.

```
cybersec-server@ubuntu:~$ sudo gedit /etc/snort/rules/local.rules
```

- b. 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.



- c. 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.

- d. Triggering an alert for the new rule. Ping Server from attacker.
- e. This ping will trigger alerts, the alerts are saved in `/var/log/snort`, read the alert.

```
cybersec-server@ubuntu:~$ cat /var/log/snort/alert
```

Q1. Have you received alert messages for ICMP Packets? Please provide screenshot to support your answer.

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 January 1, 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)

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

a. Start Snort in IDS Mode. (Server)

```
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).

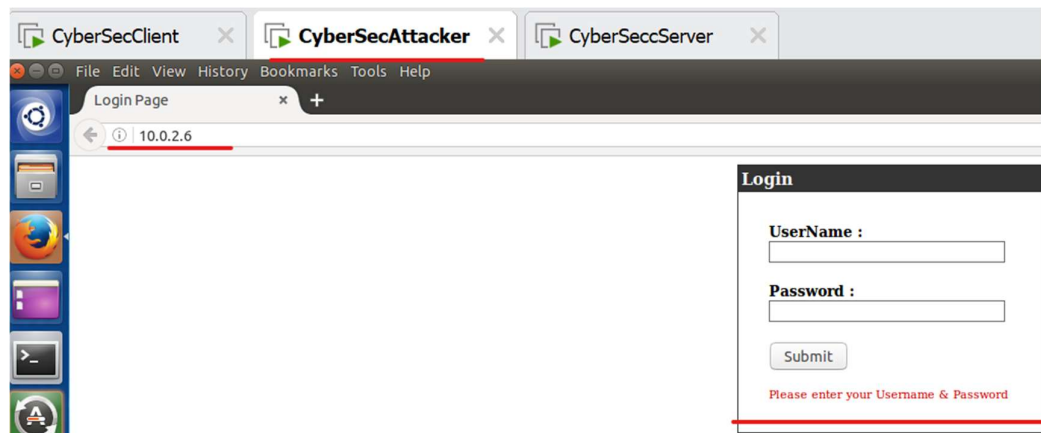
You should not see any output when you enter the command because Snort has not detected any activity specified in the rule we wrote.

b. Ping Server from Cybersec-Attack VM, Observe the messages displayed to console. **Ctrl+c** to stop it.

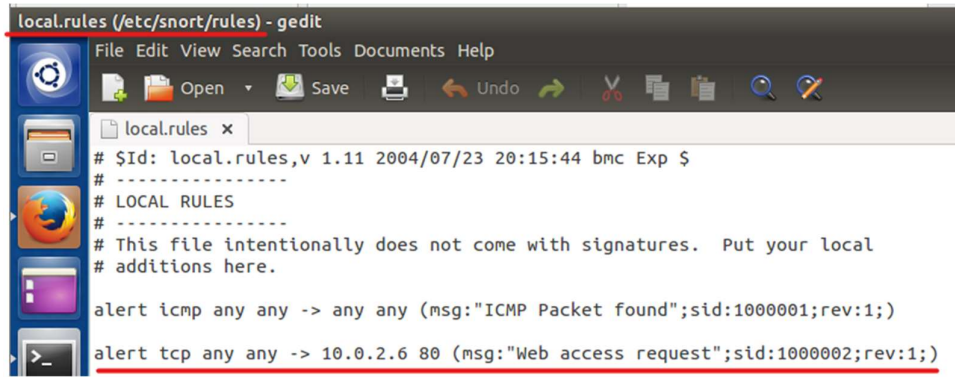
Q2. Have you received alert messages for ICMP Packets in IDS Mode? Please provide screenshot to support your answer.

Task 3: Generating alerts for web service

a) Start web browser in attacker VM to access 10.0.2.6



b) Open our local.rules file in a text editor and add new rule to generate alert when there is web access request `sudo gedit /etc/snort/rules/local.rules`



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

- 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. Use `cat /var/log/snort/alert`

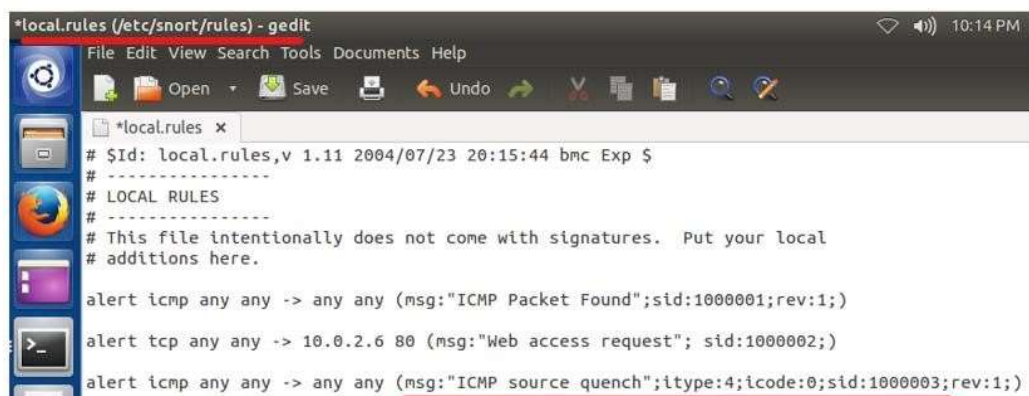
Q3. Have you received alert messages for Web access? Please provide screenshot to support your answer.

Task 4: Generating alerts for ICMP Source Quench Packets

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

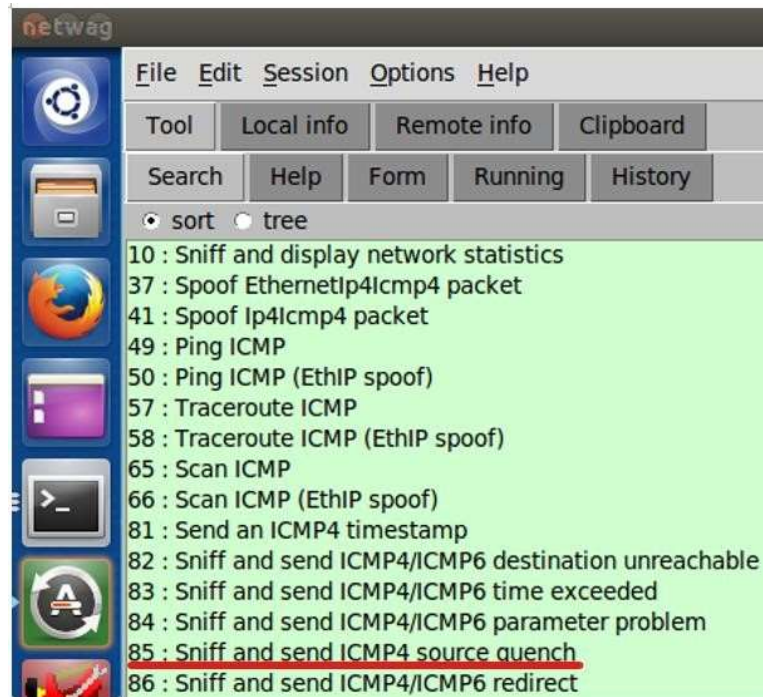
- a. Add the following rule to the local rule file then restart snort.

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



```
*local.rules (/etc/snort/rules) - gedit
File Edit View Search Tools Documents Help
*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;)
alert icmp any any -> any any (msg:"ICMP source quench";itype:4;icode:0;sid:1000003;rev:1;)
```

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



- c. Fill in the source quench form, select the interface and spoofip, change the source IP address to Server's IP address and click "Run it."
- d. Use terminal in the Client's VM to ping the server.
- e. Check the snort alert, you should see the alert for source quench packets.

Q4. Have you received alert messages for Source Quench packets? Please provide screenshot to support your answer.

Task 5: Running Snort as Intrusion Prevention System (IPS)

In this task, we will run Snort with rules to reject SSH connection attempt from Attacker to Server.

Steps:

- a. Add the following rule to the "local.rules" on Server VM and restart Snort.

reject tcp any any -> 10.0.2.6 22 (msg:"SSH Connection Attempt (Request not Accepted)";sid:1000004;rev:1;)

- b. Establish an SSH connection from Attacker VM to Server VM. (ssh username@IPAddress)
- c. Check the Alert file.

Q5. Have you received alert messages for SSH connection Attempt? Did the connection attempt succeed? Please provide screenshot to support your answer.

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

Steps:

- a. Add Rules to the “local.rules” on Server VM and restart Snort.
- b. Establish a telnet connection from Attacker VM to Server VM. (telnet “IP Address”)
- c. Check the Alert File.

Hints:

1. Telnet runs on top of TCP.
2. Telnet protocol runs on Port 23.

Q6. 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 screenshot to support your answer. Also, mention the rule that was added to “local.rules” to create this alert.