

The background features a complex abstract design. On the left, there are several concentric circles in shades of blue and grey, some with dashed lines. To the right, a network of blue circuit lines with small dots and arrows extends across the page. There are also clusters of small grey squares and rectangles scattered throughout the design.

PENITRATION TESTING & SECURING CLOUD NETWORK

ROHIT GUPTA

SECURITY

SNORT



Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) created in 1998 by Martin Roesch, founder and former CTO of Sourcefire. Snort is now developed by Cisco, which purchased Sourcefire in 2013, at which Roesch is a chief security architect.

INSTALLING SNORT REPOSITORIES AND PACKAGES

```
root@ip-172-31-95-113/etc/snort
[root@ip-172-31-95-113 ec2-user]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 436
Server version: 10.3.11-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> exit
Bye
[root@ip-172-31-95-113 ec2-user]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ip-172-31-95-113 ec2-user]# service mariadb restart
Redirecting to /bin/systemctl restart mariadb.service
[root@ip-172-31-95-113 ec2-user]# cd /etc/snort
[root@ip-172-31-95-113 snort]# ls
classification.config  gen-msg.map  reference.config  rules  snort.conf  threshold.conf  unicode.map
[root@ip-172-31-95-113 snort]# vi snort.conf
[root@ip-172-31-95-113 snort]#
```

CONFIGURING SNORT

```
root@ip-172-31-95-113:/etc/snort

# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 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
ipvar HOME_NET 54.161.133.103

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

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

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
-- INSERT --
```

```
root@ip-172-31-95-113:/etc/snort

#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
#include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/experimental.rules
#include $RULE_PATH/exploit-kit.rules
#include $RULE_PATH/exploit.rules
#include $RULE_PATH/file-executable.rules
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules
#include $RULE_PATH/file-image.rules
#include $RULE_PATH/file-multimedia.rules
#include $RULE_PATH/file-office.rules
#include $RULE_PATH/file-other.rules
#include $RULE_PATH/file-pdf.rules
##include $RULE_PATH/finger.rules
#include $RULE_PATH/ftp.rules
#include $RULE_PATH/icmp-info.rules
#include $RULE_PATH/icmp.rules
#include $RULE_PATH/imap.rules
#include $RULE_PATH/indicator-compromise.rules
#include $RULE_PATH/indicator-obfuscation.rules
-- INSERT --
```

CONFIGURING THE RULES FOR ICMP AND HTTP

```
root@ip-172-31-95-113:/etc/snort
alert icmp $EXTERNAL_NET ANY -> $HOME_NET 54.161.133.103(msg:"Bad Ping Probes"; icode:0; itype:8 sid:1000001;)
-- INSERT --
```

[illegible]

INSTALLING AND CONFIGURING HONEYPOT

```
root@ip-172-31-95-113/home/ec2-user/pentbox-1.8
[root@ip-172-31-95-113 snort]# cd ..
[root@ip-172-31-95-113 etc]# cd ..
[root@ip-172-31-95-113 /]# ls
bin  data  etc  lib  media  opt  root  sbin  sys  usr
boot dev home lib64 mnt  proc run  srv  tmp  var
[root@ip-172-31-95-113 /]# cd home/ec2-user/
[root@ip-172-31-95-113 ec2-user]# ls
clamav-0.101.2  community  pentbox-1.8
[root@ip-172-31-95-113 ec2-user]# cd pentbox-1.8/
[root@ip-172-31-95-113 pentbox-1.8]# ls
changelog.txt  COPYING.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools
[root@ip-172-31-95-113 pentbox-1.8]# ./pentbox.rb
```

>>PentBox

```
root@ip-172-31-95-113/home/ec2-user/pentbox-1.8
[root@ip-172-31-95-113 pentbox-1.8]# ./pentbox.rb

PentBox 1.8

  UUUU|.'@@@@@'.
  |__| (@@@@@@@@)
      (@@@@@@@@)
  `YY~~~~YY'
    ||    ||

----- Menu                ruby2.5.3 @ x86_64-linux

1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit

-> 2
```

root@ip-172-31-95-113/home/ec2-user/pentbox-1.8

```
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit

-> 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
0- Back

-> 3
```

root@ip-172-31-95-113/home/ec2-user/pentbox-1.8

```
// Honeypot //

You must run PentBox with root privileges.

Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

-> 2

Insert port to Open.

-> 555

Insert false message to show.

-> you are in

Save a log with intrusions?

(y/n) -> y

Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

->
```

```
root@ip-172-31-95-113/home/ec2-user/pentbox-1.8
2- Manual Configuration [Advanced Users, more options]

-> 2

Insert port to Open.

-> 555

Insert false message to show.

-> you are in

Save a log with intrusions?

(y/n) -> y

Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

->

Activate beep() sound when intrusion?

(y/n) -> y

HONEYPOT ACTIVATED ON PORT 555 (2019-07-07 17:29:02 +0000)
```

>>After implementing honeypot

```
File Edit View Search Terminal Help
root@kali:~# nmap -sS 54.161.133.103
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-06 06:30 PDT
Nmap scan report for ec2-54-161-133-103.compute-1.amazonaws.com (54.161.133.103)
Host is up (0.0099s latency).

```

PORT	STATE	SERVICE
1/tcp	open	tcpmux
3/tcp	open	compressnet
4/tcp	open	unknown
5/tcp	open	unknown
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
17/tcp	open	qotd
19/tcp	open	chargen
20/tcp	open	ftp-data
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
24/tcp	open	priv-mail
25/tcp	open	smtp
26/tcp	open	rsftp
30/tcp	open	unknown
32/tcp	open	unknown
33/tcp	open	dsp
37/tcp	open	time
42/tcp	open	nameserver
43/tcp	open	whois
49/tcp	open	tacacs
53/tcp	open	domain
70/tcp	open	gopher
79/tcp	open	finger
80/tcp	open	http
81/tcp	open	hosts2-ns
82/tcp	open	xfer
83/tcp	open	mit-ml-dev
84/tcp	open	ctf
85/tcp	open	mit-ml-dev
88/tcp	open	kerberos-sec
89/tcp	open	su-mit-tg
90/tcp	open	dnsix
99/tcp	open	metagram
100/tcp	open	newacct
106/tcp	open	pop3pw
109/tcp	open	pop2
110/tcp	open	pop3
111/tcp	open	rpcbind
113/tcp	open	ident
119/tcp	open	nnntp
135/tcp	open	msrpc