

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.

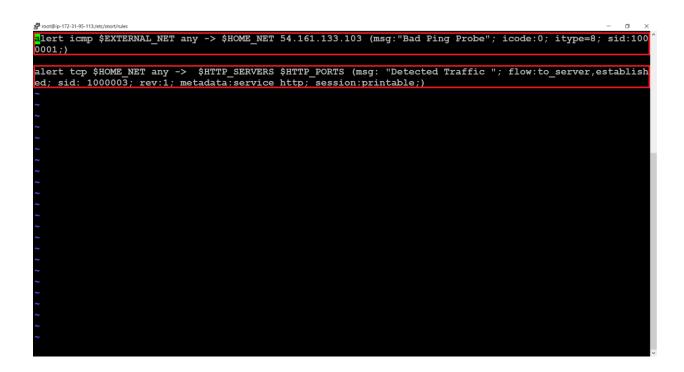
INSTALLING SNORT REPOSITORIES AND PACKAGES

CONFIGURING SNORT

```
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/sno
                                                                                                                                                                                                    П
#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



INSTALLING AND CONFIGURING HONEYPOT

>>PentBox

```
0
[root@ip-172-31-95-113 pentbox-1.8]# ./pentbox.rb
PenTBox 1.8
       U00U|.'@@@@@`.
       | (@@@@@@@@@)
             (000000000)
             YY~~~YY
                       ruby2.5.3 @ x86_64-linux
 ----- Menu
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
```

```
// 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
-> ■
```

>>After implementing honeypot

