

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÁO CÁO BÀI TẬP TRÊN LỚP**  
**MÔN KỸ THUẬT THEO DÕI VÀ**  
**GIÁM SÁT AN TOÀN MẠNG**

**Giảng viên: Ninh Thị Thu Trang**

**Nhóm lớp: 02**

**Sinh viên: Hoàng Trung Kiên**

**Mã sinh viên: B20DCAT098**

**Hà Nội – 2024**

## **Mục lục**

<b>I. Tổng quan về Bộ tiền xử lý danh tiếng.....</b>	<b>3</b>
<b>II. Cài đặt snort .....</b>	<b>3</b>
<b>III. Cấu hình Bộ tiền xử lý danh tiếng (reputation preprocessor) .....</b>	<b>3</b>
<b>IV. Thêm mục nhập vào danh sách IP theo cách thủ công.....</b>	<b>5</b>
<b>V. Chạy snort.....</b>	<b>6</b>

## **I. Tổng quan về Bộ tiền xử lý danh tiếng**

- Bộ tiền xử lý danh tiếng được tạo ra để cho phép Snort sử dụng một tệp chỉ có địa chỉ IP để xác định các máy chủ xấu và máy chủ đáng tin cậy. Địa chỉ IP độc hại được lưu trữ trong danh sách đen và địa chỉ IP đáng tin cậy được lưu trữ trong danh sách trắng. Bộ tiền xử lý danh tiếng tải các danh sách này khi Snort khởi động và so sánh tất cả lưu lượng truy cập với các danh sách đó. Snort kiểm tra cả địa chỉ IP gửi và nhận trong mỗi gói đối với mọi mục trong danh sách IP và nếu địa chỉ IP trong gói khớp với địa chỉ IP trong danh sách đen, danh sách trắng hoặc cả hai danh sách, Snort có thể thực hiện một số hành động khác nhau: Snort có thể tạo cảnh báo, chặn gói, cho phép gói mà không cần xử lý nào khác (bỏ qua tất cả các quy tắc khác) hoặc để gói tiếp tục vượt qua phần còn lại của quá trình kiểm tra quy tắc thông thường. Hành động mà Snort thực hiện tùy thuộc vào cách chúng ta định cấu hình bộ tiền xử lý danh tiếng và nếu Snort đang chạy ở chế độ IDS hoặc IPS (Snort chỉ có thể loại bỏ các gói khi chạy ở chế độ IPS, vì những lý do rõ ràng).
- Bộ tiền xử lý danh tiếng là bộ tiền xử lý đầu tiên mà một gói gặp phải trong Snort (sau khi được bộ giải mã tập hợp). Lý do cho điều này là vì bộ tiền xử lý danh tiếng có thể đánh dấu các gói tin cậy để bỏ qua phần còn lại của bộ tiền xử lý và công cụ quy tắc hoặc có thể loại bỏ gói, điều đó có thể giúp giảm tải cho hệ thống Snort.

## **II. Cài đặt snort**

- Cài đặt snort với câu lệnh *sudo apt install snort* .
- Nếu cài đặt thành công, sử dụng lệnh *snort -version* sẽ hiển thị phiên bản của snort.

```
kienat098@kienat098-virtual-machine: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kienat098@kienat098-virtual-machine:~/Desktop$ cd
kienat098@kienat098-virtual-machine:~$ sudo apt-get install snort
[sudo] password for kienat098:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1
  net-tools oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1
  net-tools oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 12 not upgraded.
Need to get 2.554 kB of archives.
After this operation, 11,4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 liblua5.1-common all 5.1.0-beta2-1dfc
kienat098@kienat098-virtual-machine:~$ snort --version

  ,,-
o" )~
  ' '

-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

kienat098@kienat098-virtual-machine:~$
```

### III. Cấu hình Bộ tiền xử lý danh tiếng (reputation preprocessor)

- Bộ tiền xử lý danh tiếng được cấu hình trong snort.conf .
- Nếu Nhiều cài đặt Snort tiêu chuẩn đặt tệp này tại **/etc/snort/snort.conf**. Mở tệp cấu hình snort này và tìm phần dành cho bộ tiền xử lý danh tiếng. bộ tiền xử lý bị vô hiệu hóa với ký hiệu băm (#) ở đầu mỗi dòng cho bộ tiền xử lý, có thể bật nó bằng cách xóa ký hiệu băm khỏi đầu mỗi dòng. Cấu hình tiền xử lý sẽ trông giống như sau khi được bật:

```

kienat098@kienat098-virtual-machine: ~
GNU nano 6.2 /etc/snort/snort.conf
#
# Note to Debian users: this is disabled since it is an experimental
# preprocessor. If you want to use it you have to create the rules files
# referenced below in the /etc/snort/rules directory
#
# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
    memcap 500, \
    priority whitelist, \
    nested_ip inner, \
    scan_local, \
    # whitelist $WHITE_LIST_PATH/white_list.rules, \
    blacklist $BLACK_LIST_PATH/black_list.rules
#####
# Step #6: Configure output plugins
# For more information, see Snort Manual: Configuring Snort: Output Modules

```

- Có một vài dòng khác trong snort.conf cũng liên quan đến danh sách IP. Hai dòng sau đây cho Snort biết thư mục chứa white\_list và black\_list:

```

kienat098@kienat098-virtual-machine: ~
GNU nano 6.2 /etc/snort/snort.conf *
# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0]

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules

```

- Sử dụng lệnh sau để tạo blacklist và whitelist.

*sudo nano /etc/snort/rules/black\_list.rules*

*sudo nano /etc/snort/rules/white\_list.rules*

```
kienat098@kienat098-virtual-machine: ~  
kienat098@kienat098-virtual-machine:~$ sudo nano /etc/snort/rules/black_list.rules  
kienat098@kienat098-virtual-machine:~$ sudo nano /etc/snort/rules/white_list.rules  
kienat098@kienat098-virtual-machine:~$
```

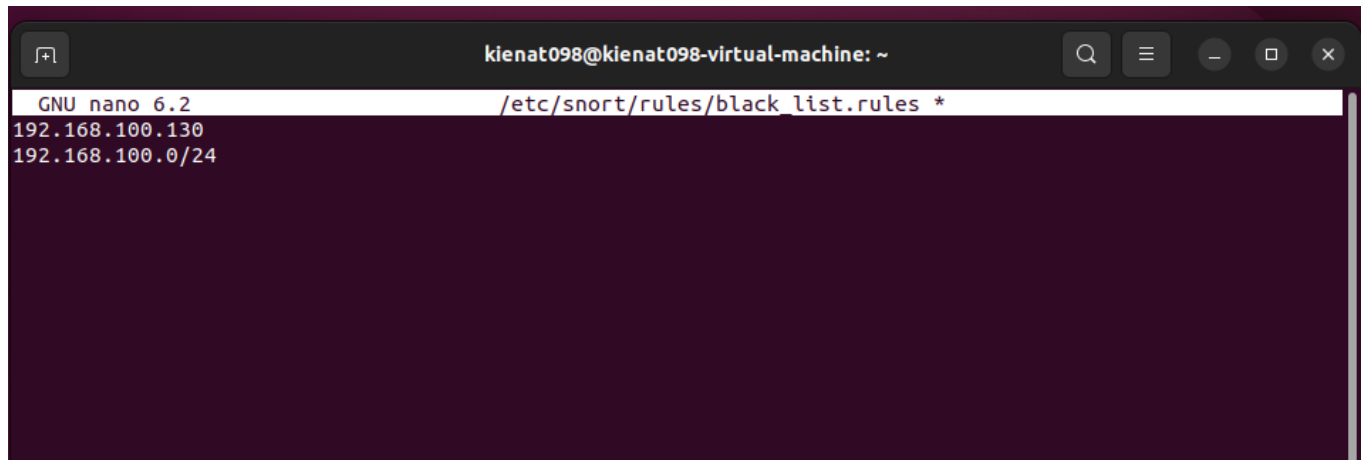
- Sau khi cấu hình xong, kiểm tra xem file snort.config có lỗi không.

```
sudo snort -T -c /etc/snort/snort.conf -i ens33
```

```
kienat098@kienat098-virtual-machine: ~  
o")~  
'''  
-*> Snort! <*-  
Version 2.9.15.1 GRE (Build 15125)  
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.10.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>  
Preprocessor Object: SF_SSH Version 1.1 <Build 3>  
Preprocessor Object: appid Version 1.1 <Build 5>  
Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>  
Preprocessor Object: SF_SDF Version 1.1 <Build 1>  
Preprocessor Object: SF_SIP Version 1.1 <Build 1>  
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>  
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
Preprocessor Object: SF_POP Version 1.0 <Build 1>  
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>  
  
Snort successfully validated the configuration!  
Snort exiting  
kienat098@kienat098-virtual-machine:~$ sudo nano /etc/snort/rules/black_list.rules  
kienat098@kienat098-virtual-machine:~$
```

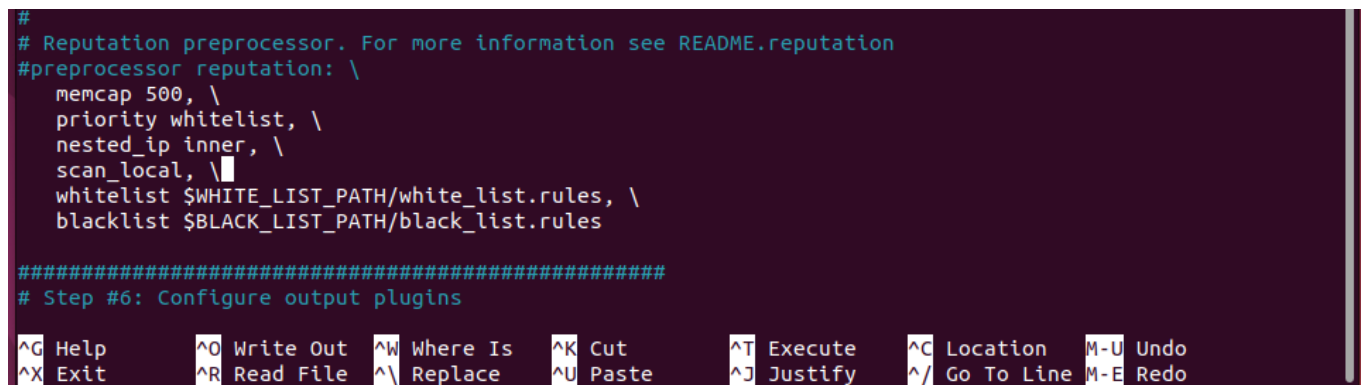
#### IV. Thêm mục nhập vào danh sách IP theo cách thủ công

- Snort có thể dễ dàng tải nhiều whitelist và blacklist. Danh sách phải là tài liệu văn bản có địa chỉ IP đơn giản (chỉ định một máy chủ) hoặc địa chỉ IP ở định dạng CIDR, với một mục nhập trên mỗi dòng. Có thể có nhận xét đầy đủ và nội tuyến bằng cách sử dụng ký hiệu băm (#).



```
kienat098@kienat098-virtual-machine: ~
GNU nano 6.2 /etc/snort/rules/black_list.rules *
192.168.100.130
192.168.100.0/24
```

- Sau đó thêm tùy chọn scan\_local vào bộ tiền xử lý danh tiếng.



```
#
# Reputation preprocessor. For more information see README.reputation
#preprocessor reputation: \
  memcap 500, \
  priority whitelist, \
  nested_ip inner, \
  scan_local, \
  whitelist $WHITE_LIST_PATH/white_list.rules, \
  blacklist $BLACK_LIST_PATH/black_list.rules

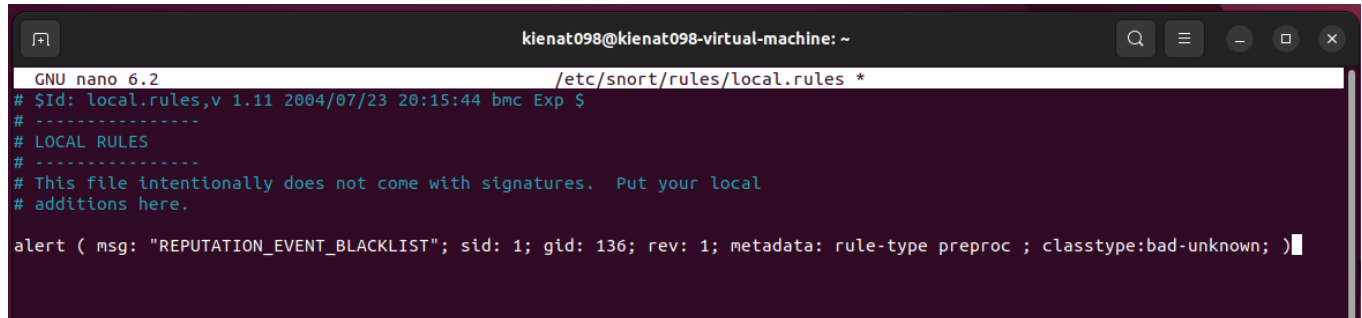
#####
# Step #6: Configure output plugins

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

- Thiết lập local.rules để tạo cảnh báo cho các sự kiện trong blacklist.

```
alert ( msg: "REPUTATION_EVENT_BLACKLIST"; sid: 1; gid: 136;  
rev: 1; metadata: rule-type preproc ; classtype:bad-unknown; )
```

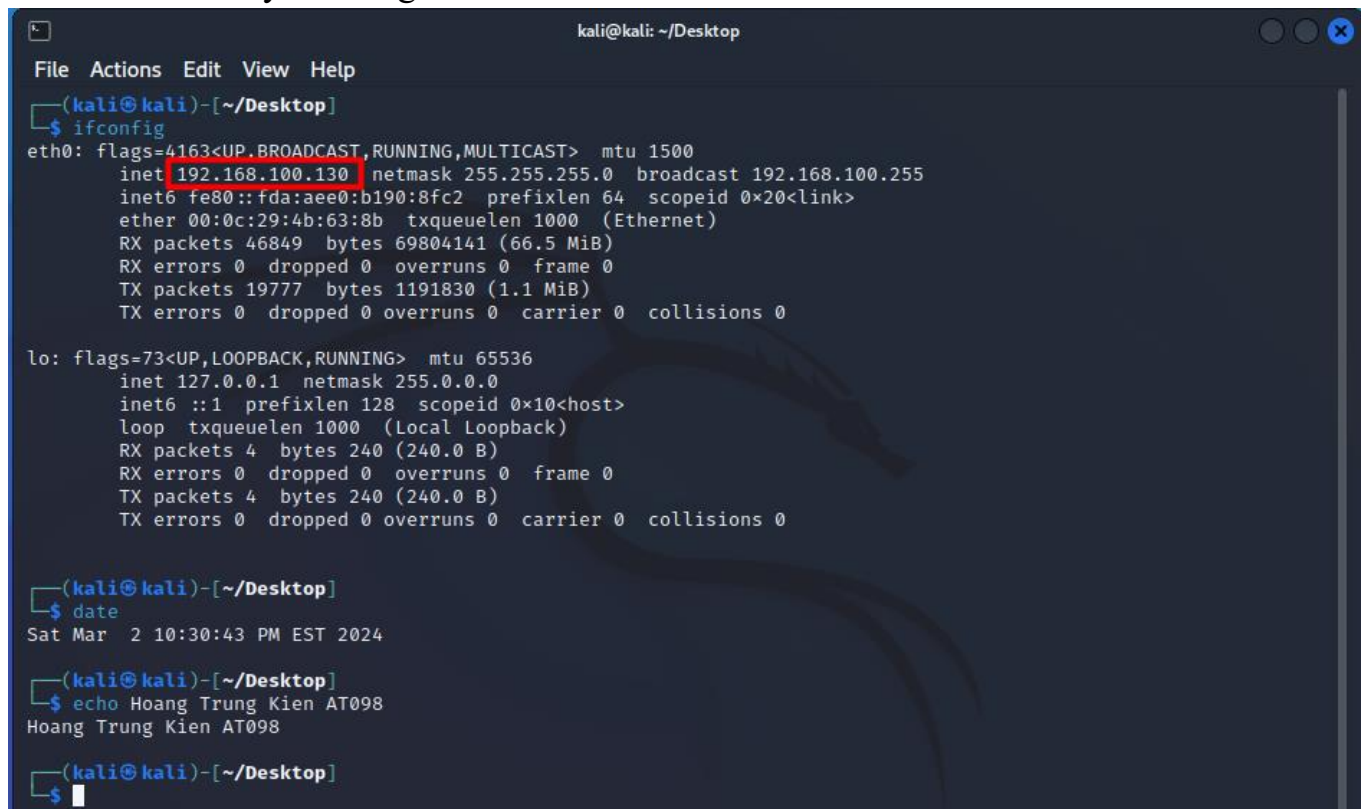
- Các quy tắc có GID 136 là các quy tắc được kích hoạt bởi bộ tiền xử lý danh tiếng.



```
kienat098@kienat098-virtual-machine: ~  
GNU nano 6.2 /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 ( msg: "REPUTATION_EVENT_BLACKLIST"; sid: 1; gid: 136; rev: 1; metadata: rule-type preproc ; classtype:bad-unknown; )
```

## V. Chạy snort

- Máy tấn công



```
kali@kali: ~/Desktop  
File Actions Edit View Help  
(kali@kali)-[~/Desktop]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.100.130 netmask 255.255.255.0 broadcast 192.168.100.255  
    inet6 fe80::fda:aee0:b190:8fc2 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:4b:63:8b txqueuelen 1000 (Ethernet)  
    RX packets 46849 bytes 69804141 (66.5 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 19777 bytes 1191830 (1.1 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~/Desktop]  
$ date  
Sat Mar  2 10:30:43 PM EST 2024  
  
(kali@kali)-[~/Desktop]  
$ echo Hoang Trung Kien AT098  
Hoang Trung Kien AT098  
  
(kali@kali)-[~/Desktop]  
$
```

- Bắt đầu Snort bằng lệnh sẽ tạo cảnh báo cho bảng điều khiển:  
*sudo snort -i ens33 -q -A console -c /etc/snort/snort.conf*
- Từ máy có địa chỉ 192.168.150.128 ping đến máy snort sẽ hiện cảnh báo.



```
Activities Terminal Thg 3 3 10:55

kienat098@kienat098-virtual-machine: ~
kienat098@kienat098-virtual-machine: ~$ sudo snort -t ens33 -n -A console -c /etc/snort/snort.conf
03/03-10:55:22.977527 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.130 -> 192.168.100.135
03/03-10:55:22.977548 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.135 -> 192.168.100.130
03/03-10:55:23.997608 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.130 -> 192.168.100.135
03/03-10:55:23.997626 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.135 -> 192.168.100.130
03/03-10:55:25.021898 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.130 -> 192.168.100.135
03/03-10:55:25.021916 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.135 -> 192.168.100.130
03/03-10:55:26.045735 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.130 -> 192.168.100.135
03/03-10:55:26.045753 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.135 -> 192.168.100.130
03/03-10:55:27.069997 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.130 -> 192.168.100.135
03/03-10:55:27.070018 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.135 -> 192.168.100.130
03/03-10:55:28.093900 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.130 -> 192.168.100.135
03/03-10:55:28.093917 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.135 -> 192.168.100.130
03/03-10:55:29.117266 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.130 -> 192.168.100.135
03/03-10:55:29.117282 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
[Priority: 2] [ICMP] 192.168.100.135 -> 192.168.100.130
03/03-10:55:30.141572 ** [136:1:1] (spp_reputation) packets blacklisted ** [Classification: Potentially Bad Traffic]
```

```
kali@kali: ~/Desktop

File Actions Edit View Help
rtt min/avg/max/mdev = 0.156/0.416/1.304/0.139 ms

(kali@kali)~[~/Desktop]
$ ping 192.168.100.135
PING 192.168.100.135 (192.168.100.135) 56(84) bytes of data.
64 bytes from 192.168.100.135: icmp_seq=1 ttl=64 time=0.390 ms
64 bytes from 192.168.100.135: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 192.168.100.135: icmp_seq=3 ttl=64 time=0.425 ms
64 bytes from 192.168.100.135: icmp_seq=4 ttl=64 time=0.405 ms
64 bytes from 192.168.100.135: icmp_seq=5 ttl=64 time=0.400 ms
64 bytes from 192.168.100.135: icmp_seq=6 ttl=64 time=0.366 ms
64 bytes from 192.168.100.135: icmp_seq=7 ttl=64 time=0.394 ms
64 bytes from 192.168.100.135: icmp_seq=8 ttl=64 time=0.390 ms
64 bytes from 192.168.100.135: icmp_seq=9 ttl=64 time=0.172 ms
64 bytes from 192.168.100.135: icmp_seq=10 ttl=64 time=0.295 ms
64 bytes from 192.168.100.135: icmp_seq=11 ttl=64 time=0.362 ms
64 bytes from 192.168.100.135: icmp_seq=12 ttl=64 time=0.405 ms
64 bytes from 192.168.100.135: icmp_seq=13 ttl=64 time=0.177 ms
64 bytes from 192.168.100.135: icmp_seq=14 ttl=64 time=0.339 ms
64 bytes from 192.168.100.135: icmp_seq=15 ttl=64 time=0.339 ms
64 bytes from 192.168.100.135: icmp_seq=16 ttl=64 time=0.351 ms
```