

First Install Snort

```
-----[event-filter-config]-----
| memory-cap : 1048576 bytes
|-----[event-filter-global]-----
|-----[event-filter-local]-----
| none
|-----[suppression]-----
| none
|-----
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations:
[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]
pcap bpf configured to passive.
Acquiring network traffic from "ens33".

--== Initialization Complete ==--

--> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.9.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SOF Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_PIPELINER Version 1.2 <Build 13>
Preprocessor Object: SF_DCEPPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MQMBUS Version 1.1 <Build 1>

Snort successfully validated the configuration!
***
Snort exiting
nfsu@ubuntu:/etc/snort$
```

Create Some Rules

```
GNU nano 4.8 /etc/snort/rules/local.rules
# sid: 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 udp any any -> any any (msg:"Chirag, udp being attacked"; sid:100001; rev:1;)
alert tcp any any -> any any (msg:"Chirag, tcp being attacked"; sid:100002; rev:2;)
alert icmp any any -> any any (msg:"Chirag, icmp being attacked"; sid:100003; rev:3;)

Wrote 11 lines
```

Check IP Address

```
o* ~- Version 2.9.7.0 GRE (Build 149)
.... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.9.1 (with TPACKET_V3)
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SDP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DCEMRP2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MQMBUS Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
nfsu@ubuntu:/etc/snort$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.84.131 netmask 255.255.255.0 broadcast 192.168.84.255
    inet6 fe80::f123:94ad:b31:a995 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:59:c5:81 txqueuelen 1000 (Ethernet)
    RX packets 12671 bytes 9876085 (9.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7275 bytes 781126 (781.1 KB)
    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 13675 bytes 1177587 (1.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13675 bytes 1177587 (1.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

nfsu@ubuntu:/etc/snort$
```

Getting Response

```
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MQMBUS Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
nfsu@ubuntu:/etc/snort$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.84.131 netmask 255.255.255.0 broadcast 192.168.84.255
    inet6 fe80::f123:94ad:b31:a995 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:59:c5:81 txqueuelen 1000 (Ethernet)
    RX packets 12671 bytes 9876085 (9.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7275 bytes 781126 (781.1 KB)
    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 13675 bytes 1177587 (1.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13675 bytes 1177587 (1.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

nfsu@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -t ens33
03/14-15:03:00.846213 ** [1:100001:1] Chirag, udp being attacked ** [Priority: 0] [UDP] 192.168.84.1:55488 -> 239.255.255.250:1900
03/14-15:03:01.853444 ** [1:100001:1] Chirag, udp being attacked ** [Priority: 0] [UDP] 192.168.84.1:55488 -> 239.255.255.250:1900
03/14-15:03:02.855711 ** [1:100001:1] Chirag, udp being attacked ** [Priority: 0] [UDP] 192.168.84.1:55488 -> 239.255.255.250:1900
03/14-15:03:03.860388 ** [1:100001:1] Chirag, udp being attacked ** [Priority: 0] [UDP] 192.168.84.1:55488 -> 239.255.255.250:1900
03/14-15:03:11.690210 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:11.690229 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:03:12.716907 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:12.716922 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:03:13.740830 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:13.740851 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:03:14.741924 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:14.741939 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:03:15.756622 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:15.756638 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:03:16.780722 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:16.780738 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:03:17.804592 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:17.804607 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:03:18.828614 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:03:18.828629 ** [1:100003:3] Chirag, tcp being attacked ** [Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
```

Ping from Another OS

The image shows a Kali Linux virtual machine interface. At the top, there are tabs for 'Home', 'Libvirt (44-bit 2)', and 'kali-linux-2024.1-vmu...'. Below the tabs is a taskbar with icons for Firefox ESR and a file manager. The main window is a terminal titled 'kali@kali ~'. The terminal shows a command prompt '(kali@kali) ~' followed by a user typing 'ping 192.168.84.131'. The output of the command is a series of 34 ping results, each showing '64 bytes from 192.168.84.131: icmp_seq=1-34 ttl=64 time=0.XXX ms', where XXX represents a value between 537 and 558. The terminal background has a dark theme with a faint, large watermark of a cat's face. At the bottom of the terminal window, there is a small status bar that reads 'To direct input to this VM, click inside or press Ctrl+G.'

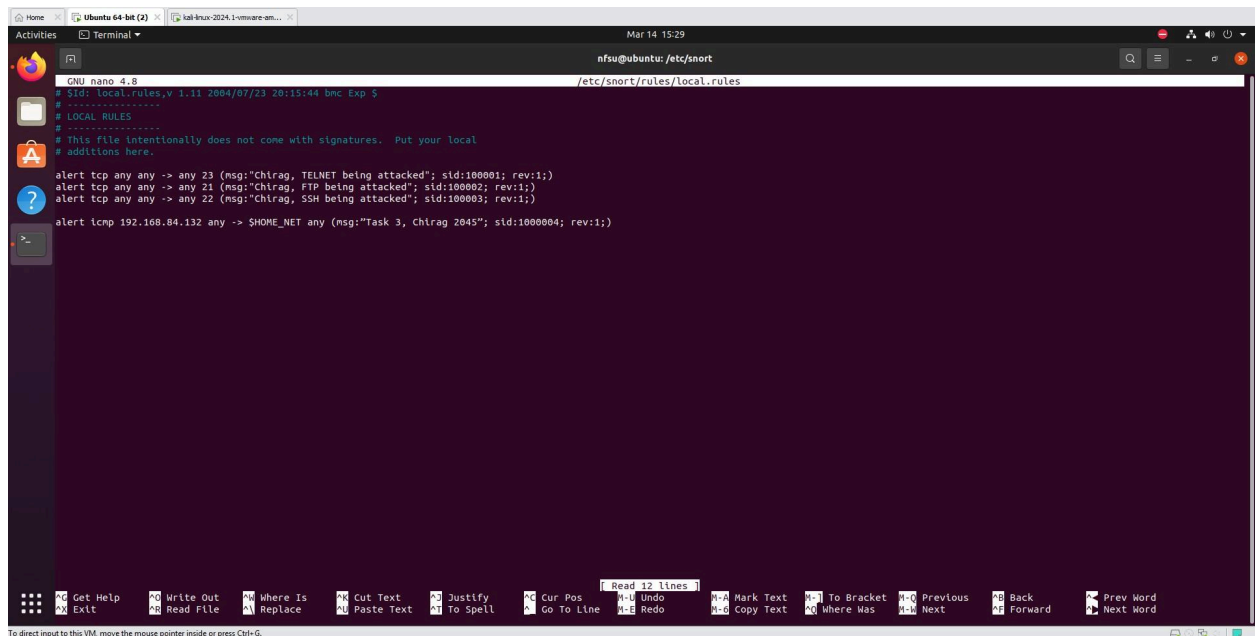
Getting Response from Ping

```
Home | Ubuntu 64-bit (2) | kali-kali-2024.1-console-amd64... Mar 14 15:25
Activities Terminal nfsu@ubuntu:/etc/snort

03/14-15:04:04.812243 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:04.812259 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:04:05.836181 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:05.836197 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:04:06.860815 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:06.860820 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:04:07.884157 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:07.884173 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:04:08.908185 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:08.908201 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:04:09.932126 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:09.932191 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:04:10.956135 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:10.956151 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132
03/14-15:04:11.980170 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
03/14-15:04:11.980186 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.131 -> 192.168.84.132

^C** Caught Int-Signal
03/14-15:04:13.004222 **[] 11:000003:3 Chirrag, tcp being attacked **[Priority: 0] [ICMP] 192.168.84.132 -> 192.168.84.131
nfsu@ubuntu:/etc/snort$ ^C
nfsu@ubuntu:/etc/snort$ sudo nano /etc/snort/rules/local.rules
nfsu@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -t ens33
ERROR: /etc/snort/rules/local.rules(8) Bad protocol: telnet.
Fatal Error, Quitting..
nfsu@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -t ens33
ERROR: /etc/snort/rules/local.rules(8) Bad protocol: telnet.
Fatal Error, Quitting..
nfsu@ubuntu:/etc/snort$ sudo nano /etc/snort/rules/local.rules
nfsu@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -t ens33
ERROR: /etc/snort/rules/local.rules(8) Bad protocol: telnet.
Fatal Error, Quitting..
nfsu@ubuntu:/etc/snort$ sudo nano /etc/snort/rules/local.rules
nfsu@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -t ens33
^[[Anfnsu@ubuntu:/etc/snort$ shano /etc/snort/rules/local.rulessn33
nfsu@ubuntu:/etc/snort$ sudo nano /etc/snort/rules/local.rules
nfsu@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -t ens33
^C** Caught Int-Signal
^Cnfsu@ubuntu:/etc/snort$ sudnano /etc/snort/rules/local.rules
nfsu@ubuntu:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -t ens33
03/14-15:22:06.408050 **[] 11:000003:1 Chirrag, SSH being attacked **[Priority: 0] [TCP] 192.168.84.132:45600 -> 192.168.84.131:22
03/14-15:22:41.170320 **[] 11:000003:1 Chirrag, SSH being attacked **[Priority: 0] [TCP] 192.168.84.132:40748 -> 192.168.84.131:22
03/14-15:23:03.856414 **[] 11:000001:1 Chirrag, TELNET being attacked **[Priority: 0] [TCP] 192.168.84.132:42700 -> 192.168.84.131:23
03/14-15:23:14.935428 **[] 11:000001:1 Chirrag, TELNET being attacked **[Priority: 0] [TCP] 192.168.84.132:53192 -> 192.168.84.131:23
03/14-15:23:39.004129 **[] 11:000003:1 Chirrag, SSH being attacked **[Priority: 0] [TCP] 192.168.84.132:58860 -> 192.168.84.131:22
03/14-15:25:22.335432 **[] 11:000002:1 Chirrag, FTP being attacked **[Priority: 0] [TCP] 192.168.84.132:34576 -> 192.168.84.131:21
```

Check ICMP



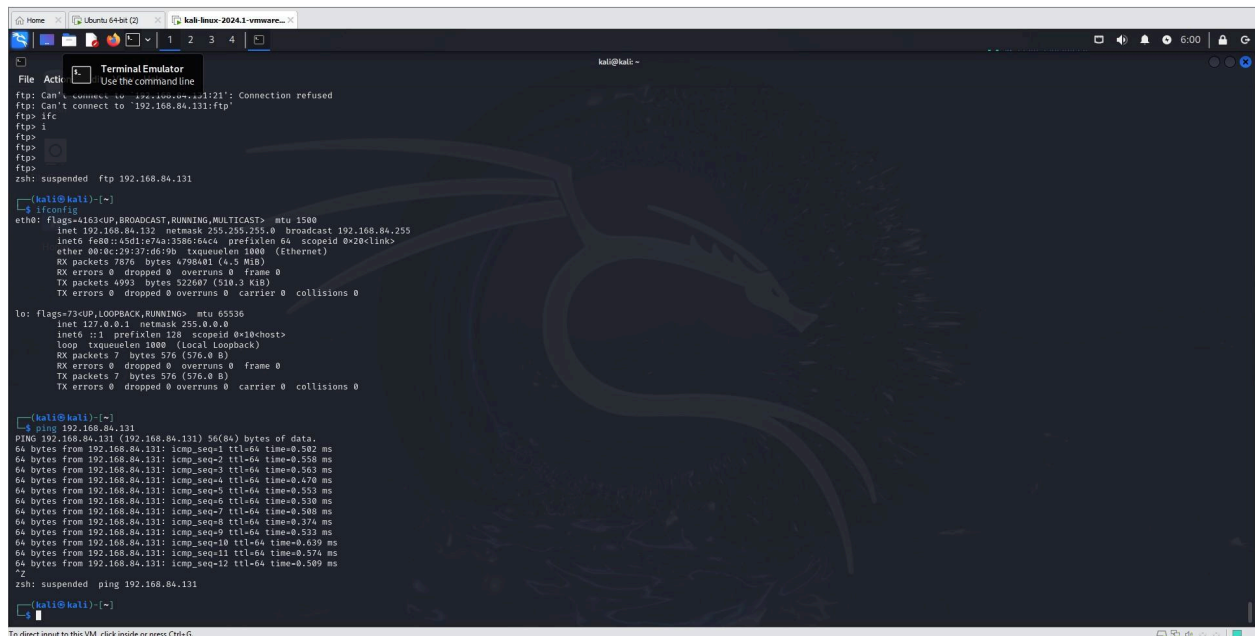
The screenshot shows a terminal window with the nano text editor open, editing the file `/etc/snort/rules/local.rules`. The file contains several Snort rules for detecting various attacks. The rules are as follows:

```
# CPU nano 4.8
# $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 -> any 23 (msg:"Chirag, TELNET being attacked"; sid:100001; rev:1;)
alert tcp any any -> any 21 (msg:"Chirag, FTP being attacked"; sid:100002; rev:1;)
alert tcp any any -> any 22 (msg:"Chirag, SSH being attacked"; sid:100003; rev:1;)

alert icmp 192.168.84.132 any -> $HOME_NET any (msg:"Task 3, Chirag 2045"; sid:1000004; rev:1;)
```

Gettin Response of Ping



The screenshot shows a terminal window with the following commands and output:

```
ftp: Can't connect to 192.168.84.131:21: Connection refused
ftp: Can't connect to 192.168.84.131:ftp
ftp> ifc
ftp> i
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
zsh: suspended ftp 192.168.84.131

(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.84.132 netmask 255.255.255.0 broadcast 192.168.84.255
    inet6 fe80::45d1:e7a3:3886:6ac4 prefixlen 64 scopeid 0<2<link>
    ether 08:00:27:37:d6:90 txqueuelen 1000 (Ethernet)
    RX packets 7876 bytes 4798401 (4.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4993 bytes 522007 (510.3 KiB)
    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 0<1<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 7 bytes 576 (576.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7 bytes 576 (576.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$ ping 192.168.84.131
PING 192.168.84.131 (192.168.84.131) 56(84) bytes of data.
64 bytes from 192.168.84.131: icmp_seq=1 ttl=64 time=0.502 ms
64 bytes from 192.168.84.131: icmp_seq=2 ttl=64 time=0.558 ms
64 bytes from 192.168.84.131: icmp_seq=3 ttl=64 time=0.470 ms
64 bytes from 192.168.84.131: icmp_seq=4 ttl=64 time=0.563 ms
64 bytes from 192.168.84.131: icmp_seq=5 ttl=64 time=0.530 ms
64 bytes from 192.168.84.131: icmp_seq=6 ttl=64 time=0.530 ms
64 bytes from 192.168.84.131: icmp_seq=7 ttl=64 time=0.508 ms
64 bytes from 192.168.84.131: icmp_seq=8 ttl=64 time=0.376 ms
64 bytes from 192.168.84.131: icmp_seq=9 ttl=64 time=0.533 ms
64 bytes from 192.168.84.131: icmp_seq=10 ttl=64 time=0.639 ms
64 bytes from 192.168.84.131: icmp_seq=11 ttl=64 time=0.576 ms
64 bytes from 192.168.84.131: icmp_seq=12 ttl=64 time=0.509 ms
^C
zsh: suspended ping 192.168.84.131

(kali@kali)~$
```