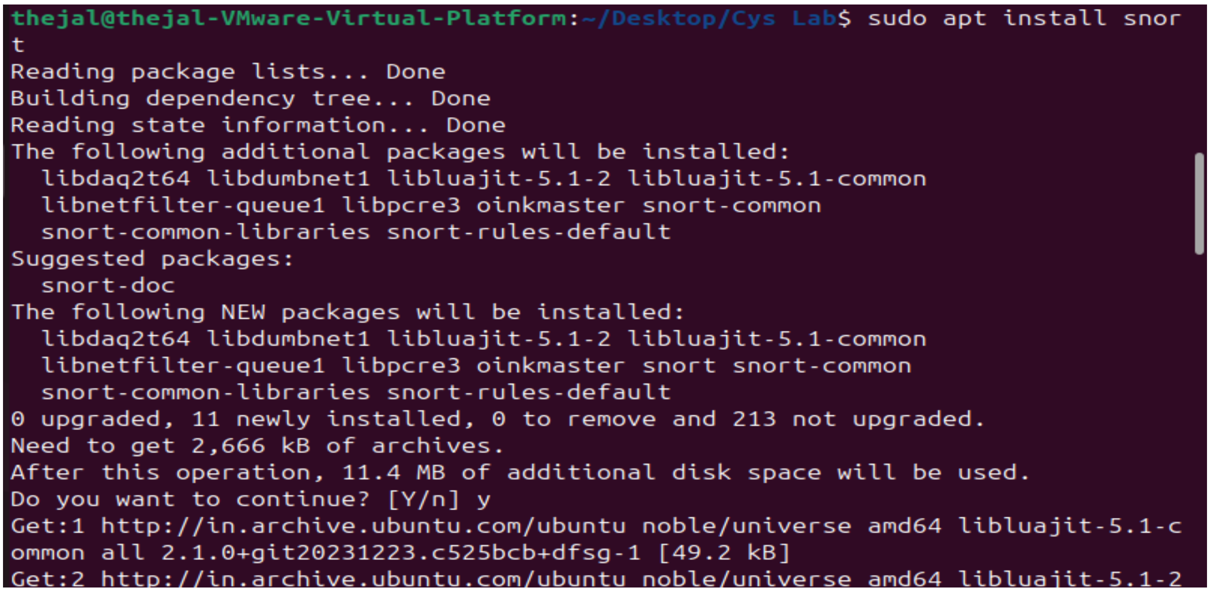
SNORT ASSIGNMENT

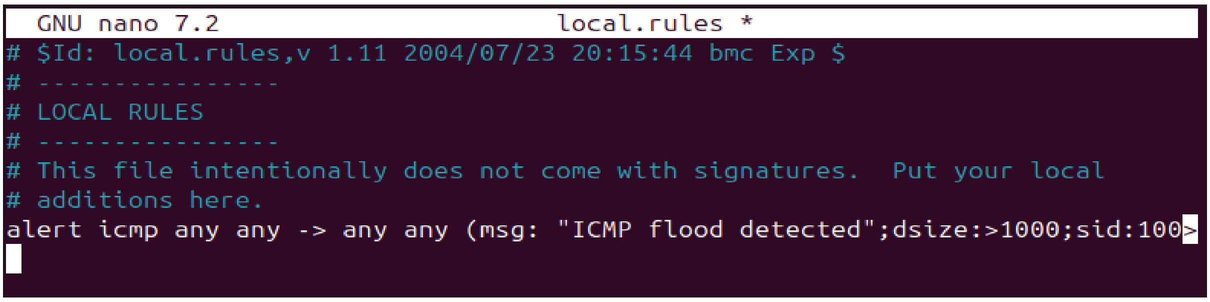
- Snort is an open – source IDS and IPS developed by Cisco.
- Used for real – time network traffic analysis and packet logging to detect and prevent potential threats.

1. Install snort in ubuntu.



```
thejal@thejal-VMware-Virtual-Platform:~/Desktop/Cys Lab$ sudo apt install snor
t
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 oinkmaster snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 oinkmaster snort snort-common
  snort-common-libraries snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 213 not upgraded.
Need to get 2,666 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://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-c
ommon all 2.1.0+git20231223.c525bcb+dfsg-1 [49.2 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-2
```

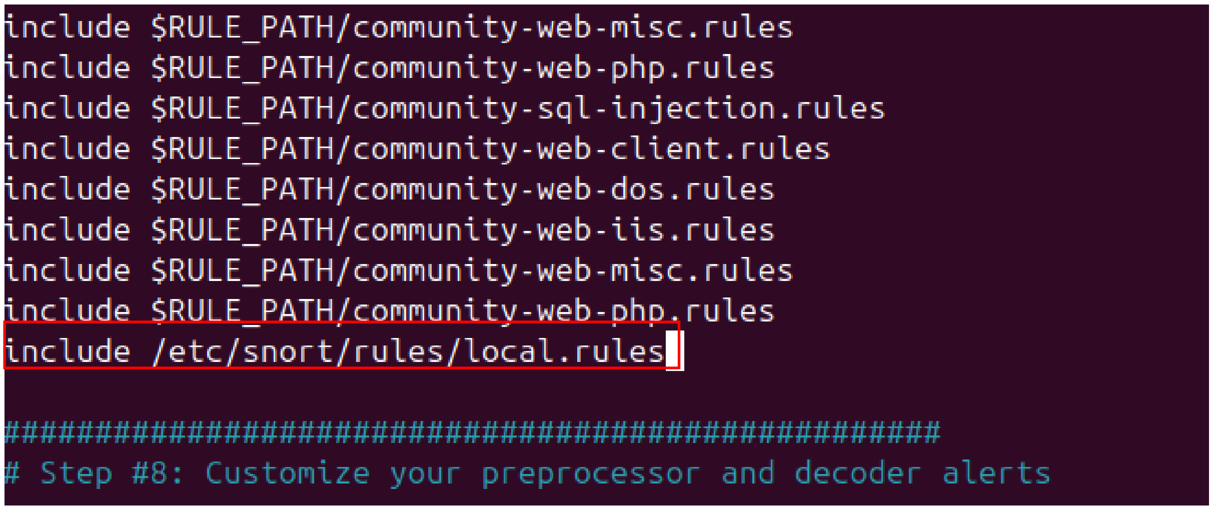
2. Navigate to snort's configuration directory and create a rule file and then add a rule to generate an alert.



```
 GNU nano 7.2                           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 icmp any any -> any any (msg: "ICMP flood detected";dsize:>1000;sid:100>
```

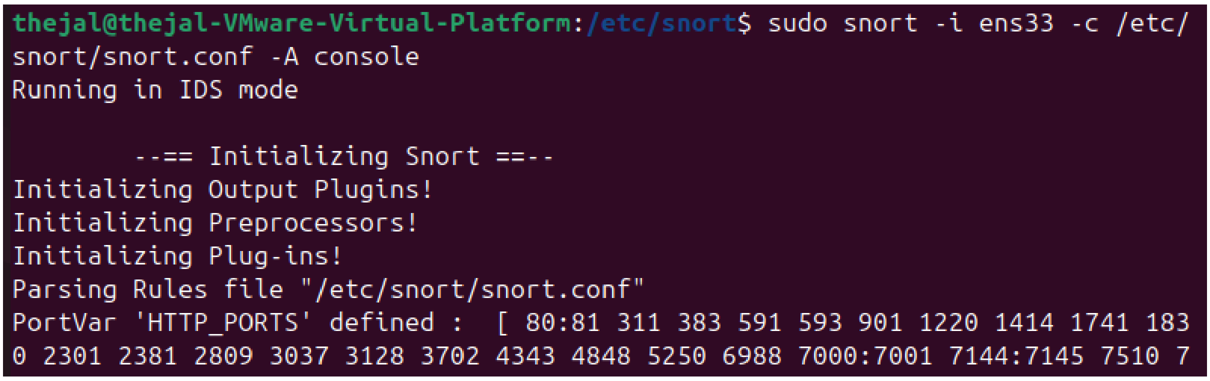
- alert – action to take.
- Icmp – protocol
- Any any – any source IP and port, destination IP and port.
- Msg – custom message.

3. Edit the snort.conf file to include the local.rules file.
   Sudo nano snort.conf



```
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include /etc/snort/rules/local.rules

###################################################
# Step #8: Customize your preprocessor and decoder alerts
```

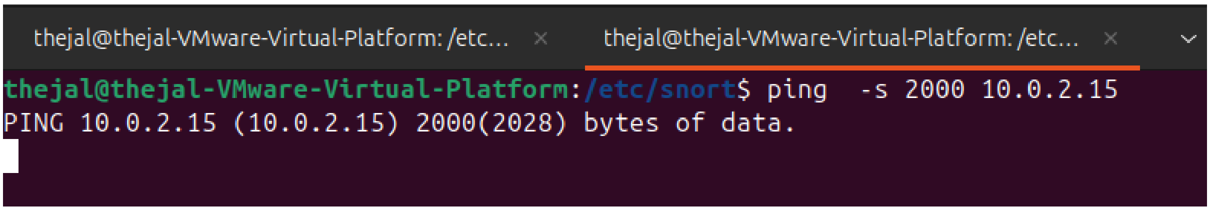
4. Run snort in NIDS mode to activate the alert.



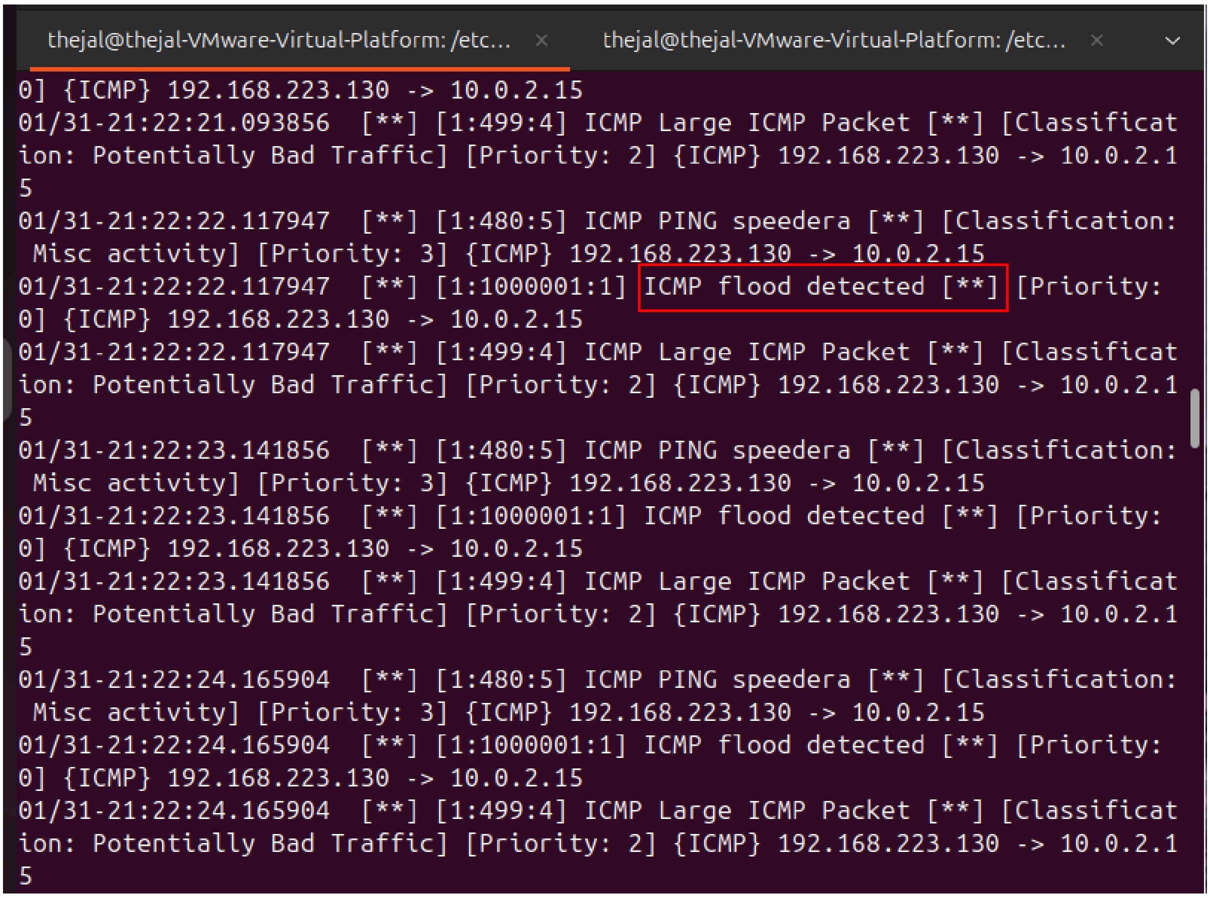
```
thejal@thejal-VMware-Virtual-Platform:/etc/snort$ sudo snort -i ens33 -c /etc/
snort/snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 183
0 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7
```

NIDS (Newtwork IDS) mode actively monitors network traffic, detects suspicious activities, and alerts users based on predefined rules. This mode is commonly used to identify attacks like port scans, DoS attacks, malware traffic, and unauthorized access attempts.

5. Generate ICMP traffic and verify that the alert is triggered.

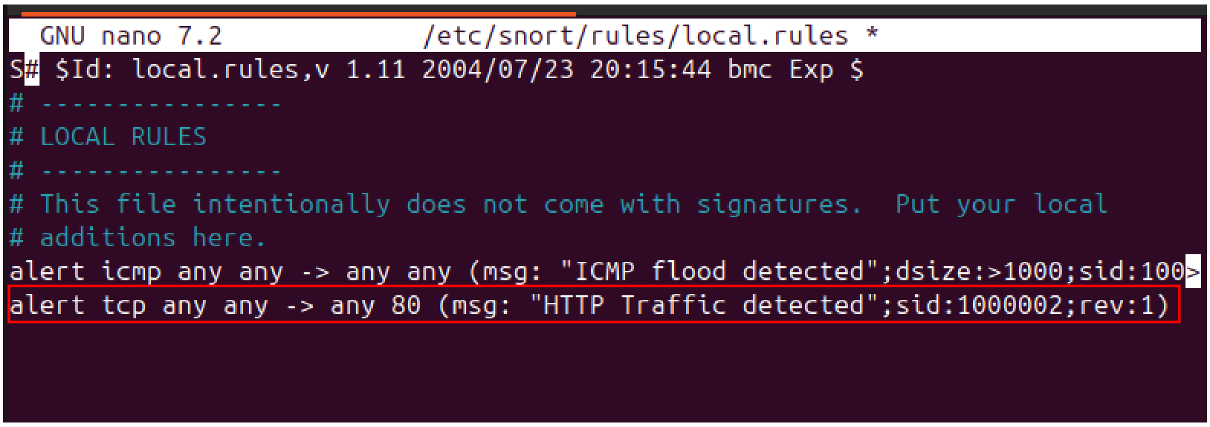

thejal@thejal-VMware-Virtual-Platform: /etc...
thejal@thejal-VMware-Virtual-Platform: /etc...

```
thejal@thejal-VMware-Virtual-Platform:/etc/snort$ ping  -s 2000 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 2000(2028) bytes of data.
```


thejal@thejal-VMware-Virtual-Platform: /etc...
thejal@thejal-VMware-Virtual-Platform: /etc...

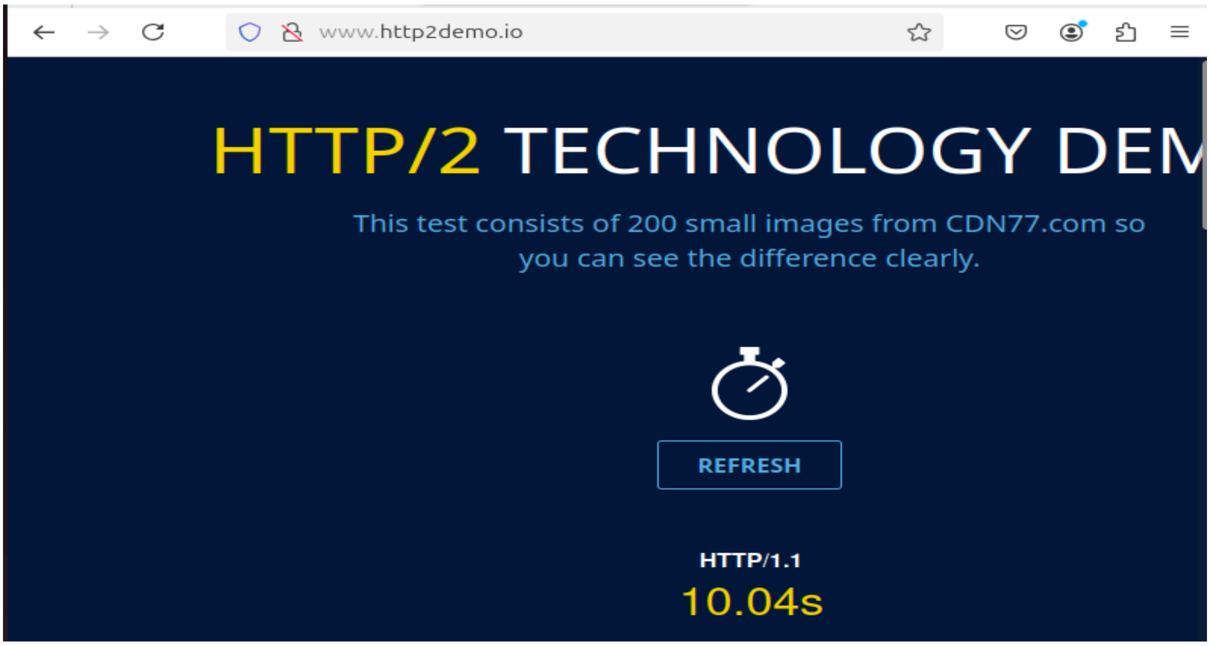
```
0] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-21:22:21.093856  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.223.130 -> 10.0.2.1
5
01/31-21:22:22.117947  [**] [1:480:5] ICMP PING speedera [**] [Classification:
 Misc activity] [Priority: 3] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-21:22:22.117947  [**] [1:1000001:1] ICMP flood detected [**] [Priority:
0] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-21:22:22.117947  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.223.130 -> 10.0.2.1
5
01/31-21:22:23.141856  [**] [1:480:5] ICMP PING speedera [**] [Classification:
 Misc activity] [Priority: 3] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-21:22:23.141856  [**] [1:1000001:1] ICMP flood detected [**] [Priority:
0] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-21:22:23.141856  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.223.130 -> 10.0.2.1
5
01/31-21:22:24.165904  [**] [1:480:5] ICMP PING speedera [**] [Classification:
 Misc activity] [Priority: 3] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-21:22:24.165904  [**] [1:1000001:1] ICMP flood detected [**] [Priority:
0] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-21:22:24.165904  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.223.130 -> 10.0.2.1
5
```

6. Edit the local.rules file to add a rule for capturing HTTP traffic.



```
  GNU nano 7.2            /etc/snort/rules/local.rules *
S# $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 flood detected";dsize:>1000;sid:100>
alert tcp any any -> any 80 (msg: "HTTP Traffic detected";sid:1000002;rev:1)
```

7. Open a browser and visit an HTTP website.



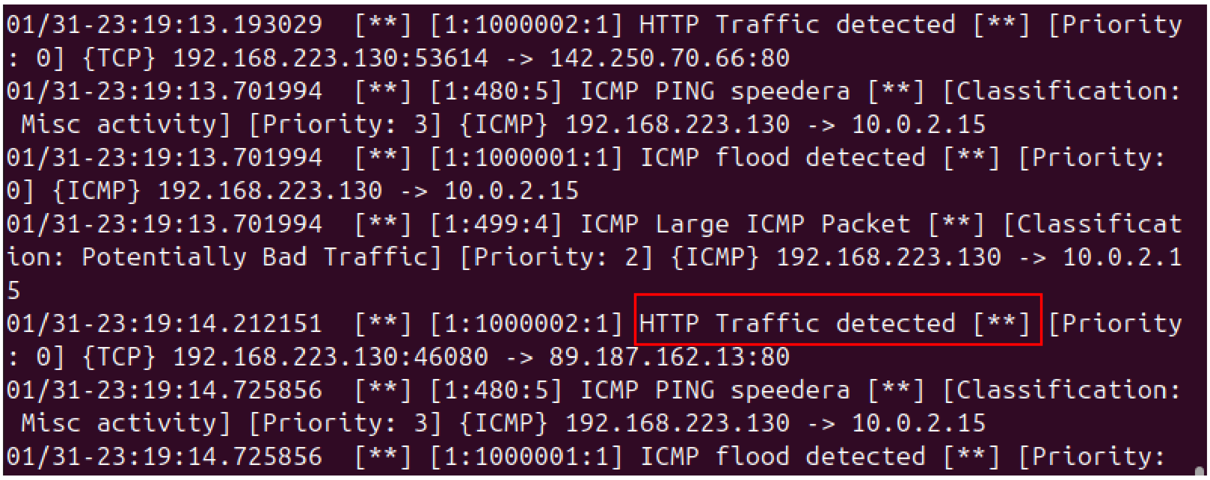
HTTP/2 TECHNOLOGY DEM

This test consists of 200 small images from CDN77.com so you can see the difference clearly.

HTTP/1.1

10.04s

8. Again run snort in NIDS mode.
9. Observe the alert.



```
01/31-23:19:13.193029  [**] [1:1000002:1] HTTP Traffic detected [**] [Priority
: 0] {TCP} 192.168.223.130:53614 -> 142.250.70.66:80
01/31-23:19:13.701994  [**] [1:480:5] ICMP PING speedera [**] [Classification:
 Misc activity] [Priority: 3] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-23:19:13.701994  [**] [1:1000001:1] ICMP flood detected [**] [Priority:
0] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-23:19:13.701994  [**] [1:499:4] ICMP Large ICMP Packet [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.223.130 -> 10.0.2.1
5
01/31-23:19:14.212151  [**] [1:1000002:1] HTTP Traffic detected [**] [Priority
: 0] {TCP} 192.168.223.130:46080 -> 89.187.162.13:80
01/31-23:19:14.725856  [**] [1:480:5] ICMP PING speedera [**] [Classification:
 Misc activity] [Priority: 3] {ICMP} 192.168.223.130 -> 10.0.2.15
01/31-23:19:14.725856  [**] [1:1000001:1] ICMP flood detected [**] [Priority:
```