

sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -A INPUT -p tcp --dport s
sh -j ACCEPT
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables
iptables v1.6.1: no command specified
Try `iptables -h' or 'iptables --help' for more information.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

sudo iptables -A INPUT -p tcp --dport http -j ACCEPT

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -A INPUT -p tcp --dport h
ttp -j ACCEPT
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ssh
ACCEPT    tcp  --  anywhere              anywhere               tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

sudo iptables -A INPUT -p tcp --dport https -j ACCEPT

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -A INPUT -p tcp --dport h
ttps -j ACCEPT
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ssh
ACCEPT    tcp  --  anywhere              anywhere               tcp dpt:http
ACCEPT    tcp  --  anywhere              anywhere               tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

sudo iptables -D INPUT 1

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -D INPUT 1
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http
ACCEPT    tcp  --  anywhere              anywhere               tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

sudo iptables -A INPUT -j DROP

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -A INPUT -j DROP
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http
ACCEPT     tcp  --  anywhere               anywhere               tcp dpt:https
ACCEPT     tcp  --  anywhere               anywhere
ACCEPT     all  --  anywhere               anywhere
DROP       all  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

sudo iptables -I INPUT -p icmp -j ACCEPT

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -I INPUT -p icmp -j ACCEPT
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http
ACCEPT     icmp --  anywhere               anywhere
ACCEPT     tcp  --  anywhere               anywhere               tcp dpt:https
ACCEPT     tcp  --  anywhere               anywhere
ACCEPT     icmp --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

sudo iptables -I INPUT 2 -p icmp -j ACCEPT

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -I INPUT 2 -p icmp -j ACCEPT
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http
ACCEPT     tcp  --  anywhere               anywhere               tcp dpt:https
ACCEPT     icmp --  anywhere               anywhere
ACCEPT     tcp  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Activities Terminal Tue 14:54

Lab1006@lab1006-HP-280-G4-MT-Business-PC: ~

```
File Edit View Search Terminal Help
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

Send Anywhere - File tra... Lab Assignment 11 Short ID: X Lab Assignment 11 Firewall: X

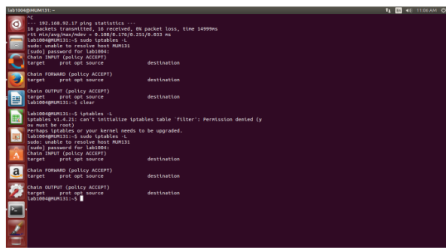
file:///home/lab1006/Downloads/Lab Assignment 11 Firewall: X

3. REJECT ignores the packet, but responds to the request with a packet denied message.

### Basic commands

Typing

```
sudo iptables -L
(-L - List the current filter rules.)
```



As you can see, we have our three default chains (INPUT, OUTPUT, and FORWARD). We also can see each chain's default policy (each chain has ACCEPT as its default policy). We

Find in page Highlight All Match Case Match Diacritics X

Activities Terminal Tue 15:03

Lab1006@lab1006-HP-280-G4-MT-Business-PC: ~

```
File Edit View Search Terminal Help
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables
iptables v1.6.1: no command specified
Try 'iptables -h' or 'iptables --help' for more information.
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

Send Anywhere - File tra... Lab Assignment 11 Short ID: X Lab Assignment 11 Firewall: X google docs - Google X

file:///home/lab1006/Downloads/Lab Assignment 11 Firewall: X

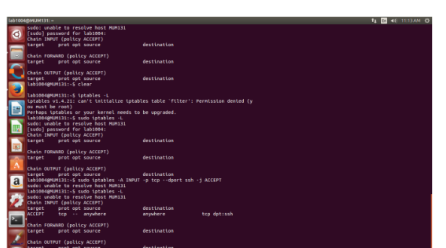
4 of 12 Automatic Zoom

TCP traffic on that port to come in.

```
sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
```

Referring back to the list above, you can see that this tells iptables:

- append this rule to the input chain (-A INPUT) so we look at incoming traffic
- check to see if it is TCP (-p tcp).
- If so, check to see if the input goes to the SSH port (--dport ssh).
- If so, accept the input (-j ACCEPT).



Find in page Highlight All Match Case Match Diacritics X

```
Activities Terminal
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -l enp3s0
09/27-16:06:52.536751 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:52.536751 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:52.536792 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.147
09/27-16:06:52.536792 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:53.565476 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:53.565476 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:53.565514 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.46 -> 192.168.100.147
09/27-16:06:54.589481 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:54.589481 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:54.589520 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.46 -> 192.168.100.147
09/27-16:06:55.613429 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:55.613429 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:55.613467 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.46 -> 192.168.100.147
09/27-16:06:56.637434 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:56.637434 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:56.637472 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.46 -> 192.168.100.147
09/27-16:06:57.661341 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:57.661341 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:57.661379 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.46 -> 192.168.100.147
09/27-16:06:58.685434 ** [1:366:7] ICMP PING *NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:58.685434 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.147 -> 192.168.100.46
09/27-16:06:58.685472 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.100.46 -> 192.168.100.147
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf
Unpacking snort-rules-default (2.9.7.0-5build1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../2-snort-common_2.9.7.0-5build1_all.deb ...
Unpacking snort-common (2.9.7.0-5build1) ...
Selecting previously unselected package libdaq2.
Preparing to unpack .../3-libdaq2_2.0.4-3build2_and64.deb ...
Unpacking libdaq2 (2.0.4-3build2) ...
Selecting previously unselected package libdumbnet1:amd64.
Preparing to unpack .../4-libdumbnet1_1.12-7build1_and64.deb ...
Unpacking libdumbnet1:amd64 (1.12-7build1) ...
Selecting previously unselected package snort.
Preparing to unpack .../5-snort_2.9.7.0-5build1_and64.deb ...
Unpacking snort (2.9.7.0-5build1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../6-oinkmaster_2.0-4_all.deb ...
Unpacking oinkmaster (2.0-4) ...
Setting up snort-common-libraries (2.9.7.0-5build1) ...
Setting up snort-rules-default (2.9.7.0-5build1) ...
Setting up libdaq2 (2.0.4-3build2) ...
Setting up libdumbnet1:amd64 (1.12-7build1) ...
Setting up snort (2.9.7.0-5build1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-20) ...
ureadahead will be reprofiled on next reboot
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
Processing triggers for systemd (237-3ubuntu10.56) ...
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo gedit /etc/snort/snort.conf
** (gedit:12656): WARNING **: 16:01:19.525: Set document metadata failed: Setting a ttribute metadata:gedit-spell-language not supported
** (gedit:12656): WARNING **: 16:01:19.525: Set document metadata failed: Setting a ttribute metadata:gedit-encoding not supported
** (gedit:12656): WARNING **: 16:01:21.482: Set document metadata failed: Setting a ttribute metadata:gedit-spell-language not supported
** (gedit:12656): WARNING **: 16:01:21.482: Set document metadata failed: Setting a ttribute metadata:gedit-encoding not supported
** (gedit:12656): WARNING **: 16:01:26.013: Set document metadata failed: Setting a ttribute metadata:gedit-position not supported
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
Activities Terminal Tue 16:11 lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
(Reading database ... 294521 files and directories currently installed.)
Preparing to unpack .../0-snort-common-libraries_2.9.7.0-5build1_and64.deb ...
Unpacking snort-common-libraries (2.9.7.0-5build1) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../1-snort-rules-default_2.9.7.0-5build1_all.deb ...
Unpacking snort-rules-default (2.9.7.0-5build1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../2-snort-common_2.9.7.0-5build1_all.deb ...
Unpacking snort-common (2.9.7.0-5build1) ...
Selecting previously unselected package libdaq2.
Preparing to unpack .../3-libdaq2_2.0.4-3build2_and64.deb ...
Unpacking libdaq2 (2.0.4-3build2) ...
Selecting previously unselected package libdumbnet1:amd64.
Preparing to unpack .../4-libdumbnet1_1.12-7build1_and64.deb ...
Unpacking libdumbnet1:amd64 (1.12-7build1) ...
Selecting previously unselected package snort.
Preparing to unpack .../5-snort_2.9.7.0-5build1_and64.deb ...
Unpacking snort (2.9.7.0-5build1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../6-oinkmaster_2.0.4_all.deb ...
Unpacking oinkmaster (2.0.4) ...
Setting up oinkmaster (2.0.4) ...
Setting up snort-common-libraries (2.9.7.0-5build1) ...
Setting up snort-rules-default (2.9.7.0-5build1) ...
Setting up libdaq2 (2.0.4-3build2) ...
Setting up libdumbnet1:amd64 (1.12-7build1) ...
Setting up snort (2.9.7.0-5build1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-20) ...
ureadahead will be reprofiled on next reboot
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
Processing triggers for systemd (237-3ubuntu10.50) ...
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo gedit /etc/snort/snort.conf

** (gedit:12656): WARNING **: 16:01:19.525: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:12656): WARNING **: 16:01:19.525: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:12656): WARNING **: 16:01:21.482: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:12656): WARNING **: 16:01:21.482: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:12656): WARNING **: 16:01:26.013: Set document metadata failed: Setting attribute metadata::gedit-position not supported
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
Activities Terminal Tue 16:11 lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -l enp3s0
09/27-16:06:52.536751 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:52.536751 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:52.536792 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.147
09/27-16:06:53.565476 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:53.565476 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:53.565514 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.147
09/27-16:06:54.589481 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:54.589481 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:54.589520 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.147
09/27-16:06:55.613429 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:55.613429 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:55.613467 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.147
09/27-16:06:56.637434 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:56.637434 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:56.637472 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.147
09/27-16:06:57.661341 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:57.661341 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:57.661379 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.147
09/27-16:06:58.685434 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:58.685434 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.147 -> 192.168.100.46
09/27-16:06:58.685472 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.147
09/27-16:08:13.354549 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-NONXT} 2001:0:348b:fb58:3cf4:f3e:9896:
d2ce -> ff02::1
09/27-16:09:37.085518 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.147:49480 -> 192.168.100.46:1
61
09/27-16:09:37.090970 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.147:49480 -> 192.168.1
00.46:705
09/27-16:10:04.910634 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:04.910634 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:04.910665 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.89
09/27-16:10:05.911362 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:05.911362 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:05.911400 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.89
09/27-16:10:06.919659 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:06.919659 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:06.919697 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.89
09/27-16:10:07.943567 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:07.943567 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.89 -> 192.168.100.46
09/27-16:10:07.943604 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.100.89
09/27-16:10:26.203916 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
09/27-16:10:26.213794 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ffe2:9163
09/27-16:10:42.583773 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.46 -> 192.168.
100.100
```