Lab8 – Snort

Document your commands or take screenshots. Answer questions in english or finnish.

Virtual machines can be found at: \\ghost\virtuaalikoneet\TTKS\Snort

Kali: root/root66, Ubuntu: student/tietoturva, Pfsense: admin/pfsense

The labs use the following topology :

Kali (Attacker) ---- PFSense ---- Victim (Centos-Desktop)

Attacker – 200.0.0.2/24 (intnet)

Victim – 192.168.1.2/24 (intnet) check that CABLE is CONNECTED on adapters -> advanced

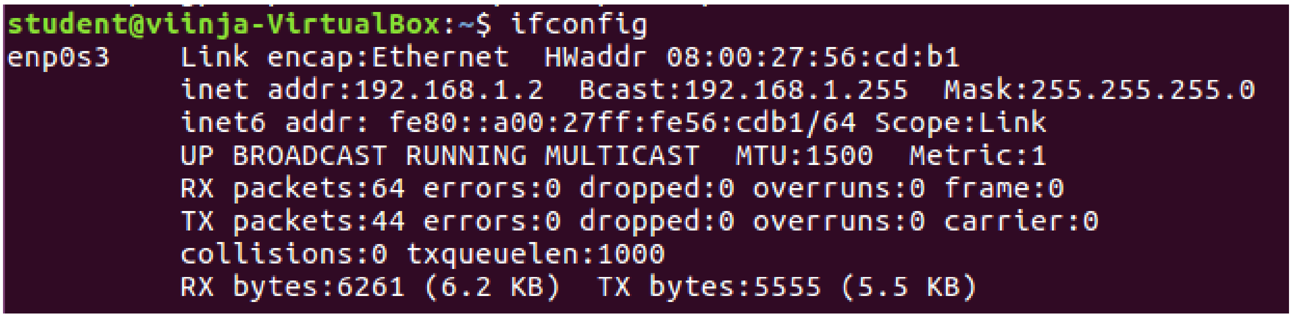
PFsense interfaces:

Adapter1: intnet

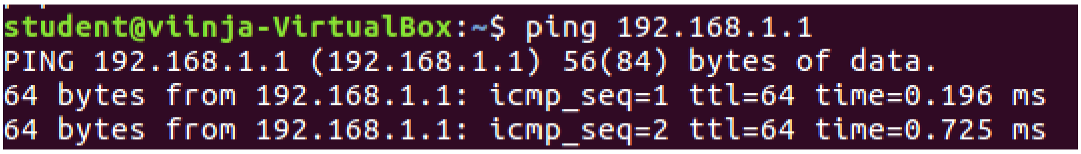
Adapter2: intnet

em0: 200.0.0.1/24

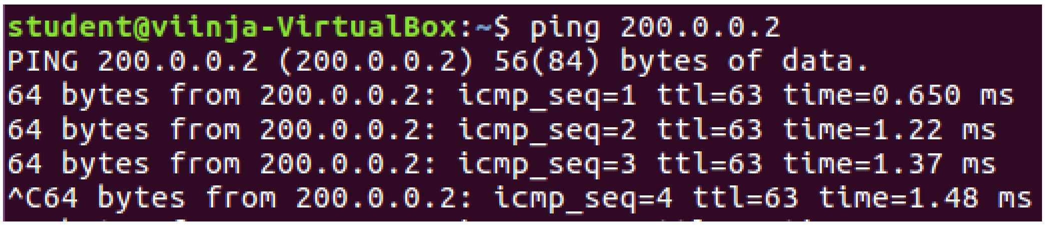
em1:192.168.1.1/24



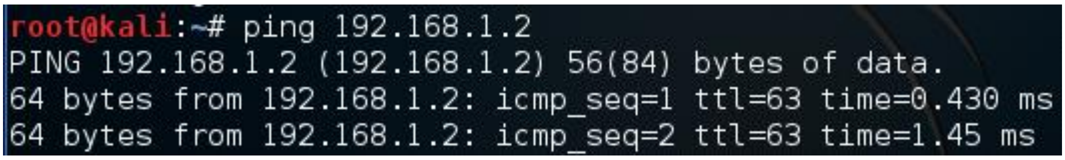
```
student@viinja-VirtualBox:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:56:cd:b1
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe56:cdb1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6261 (6.2 KB)  TX bytes:5555 (5.5 KB)
```



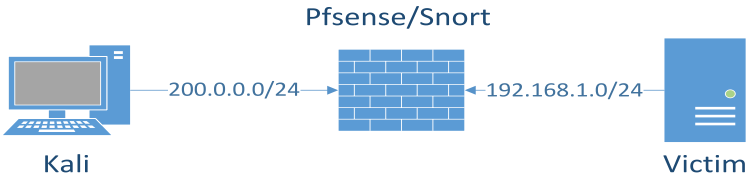
```
student@viinja-VirtualBox:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.196 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.725 ms
```



```
student@viinja-VirtualBox:~$ ping 200.0.0.2
PING 200.0.0.2 (200.0.0.2) 56(84) bytes of data.
64 bytes from 200.0.0.2: icmp_seq=1 ttl=63 time=0.650 ms
64 bytes from 200.0.0.2: icmp_seq=2 ttl=63 time=1.22 ms
64 bytes from 200.0.0.2: icmp_seq=3 ttl=63 time=1.37 ms
^C64 bytes from 200.0.0.2: icmp_seq=4 ttl=63 time=1.48 ms
```



```
root@kali:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=0.430 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=1.45 ms
```


Pfsense/Snort
200.0.0.0/24
192.168.1.0/24
Kali
Victim

- **Connect PFsense & Setup snort (1p)**

With victim pc, connect to https://192.168.1.1, log in with admin/pfsense .

Next set snort to work on WAN interface.

Test that Victim can ping Attacker and vice versa

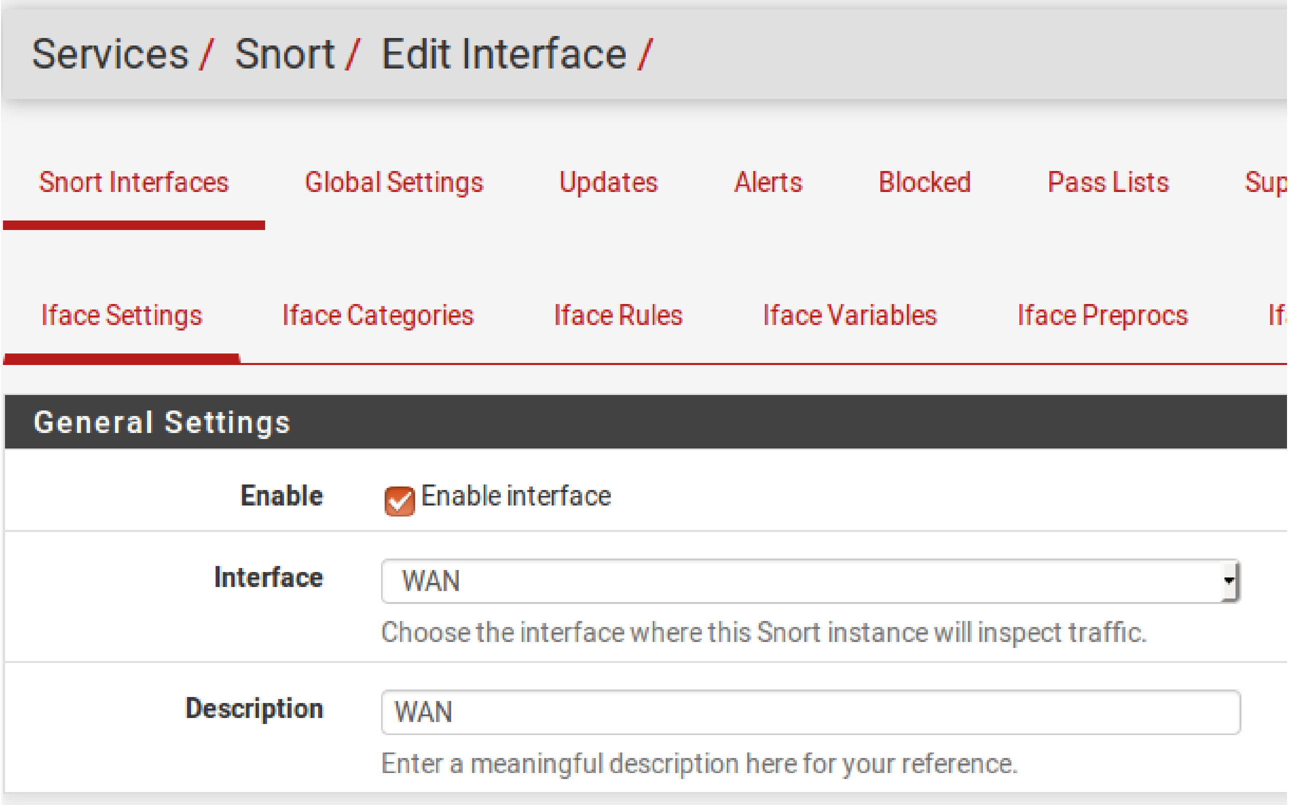
- **Setting up snort & rules (1p)**

Select services → snort

add

Enable on interface WAN

Save



General Settings

Enable ☑ Enable interface

Interface: WAN

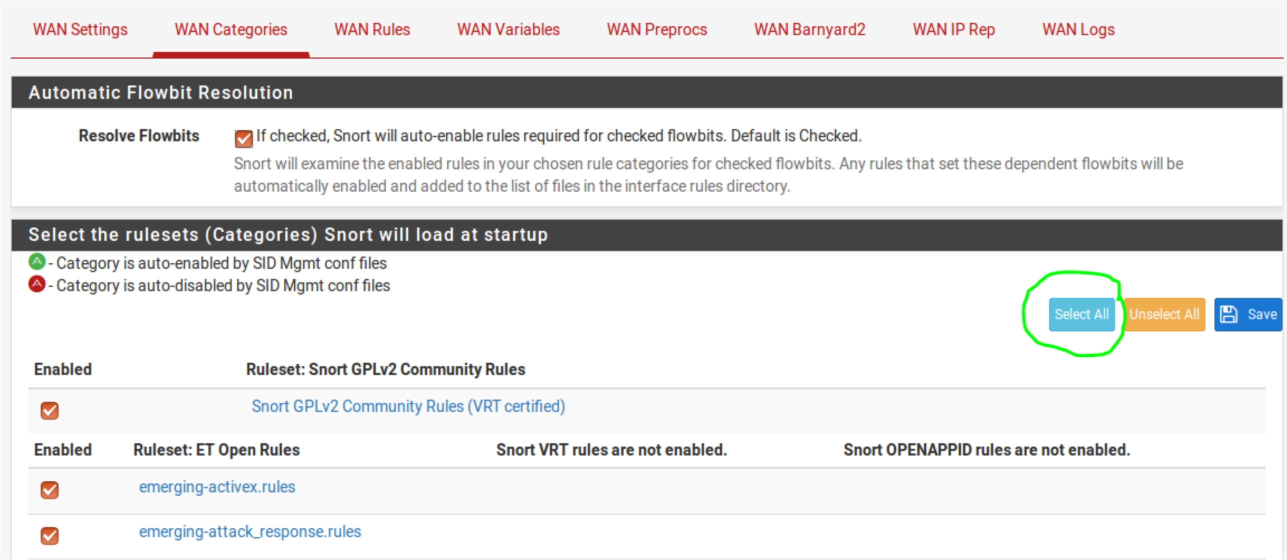
Choose the interface where this Snort instance will inspect traffic.

Description: WAN

Enter a meaningful description here for your reference.

Edit

WAN Categories Select All (To make sure we can detect attacks, lets select all rulesets!)



Automatic Flowbit Resolution

Resolve Flowbits ☑ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.

Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Select the rulesets (Categories) Snort will load at startup

🟩 - Category is auto-enabled by SID Mgmt conf files

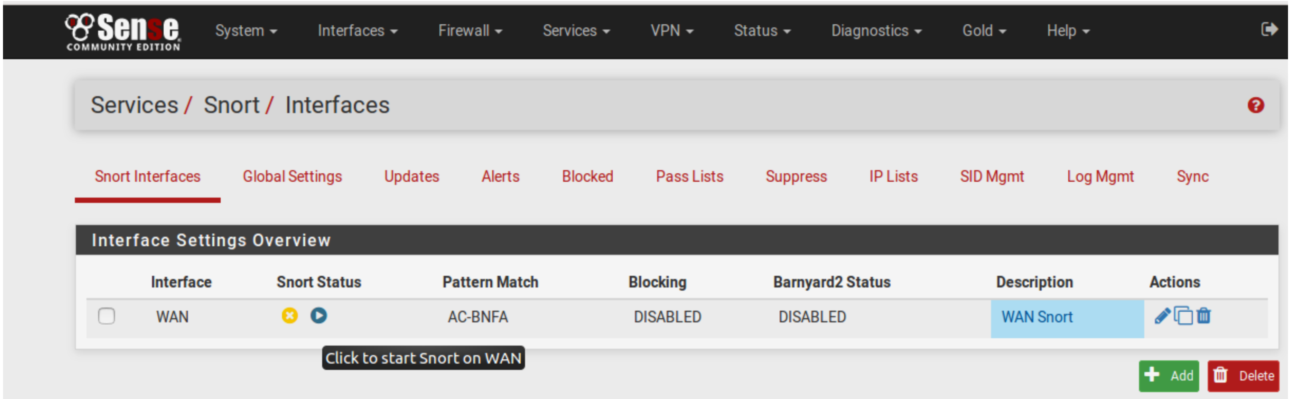
🟥 - Category is auto-disabled by SID Mgmt conf files

Enabled	Ruleset: Snort GPLv2 Community Rules
☑	Snort GPLv2 Community Rules (VRT certified)

Enabled	Ruleset: ET Open Rules	Snort VRT rules are not enabled.	Snort OPENAPPID rules are not enabled.
☑	emerging-activex.rules		
☑	emerging-attack_response.rules		

Save

Go back to snort interfaces and start snort on WAN

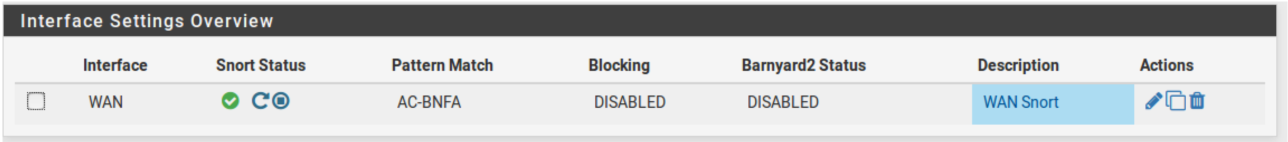


Services / Snort / Interfaces

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
☐	WAN	✖ ▶	AC-BNFA	DISABLED	DISABLED	WAN Snort	

Click to start Snort on WAN



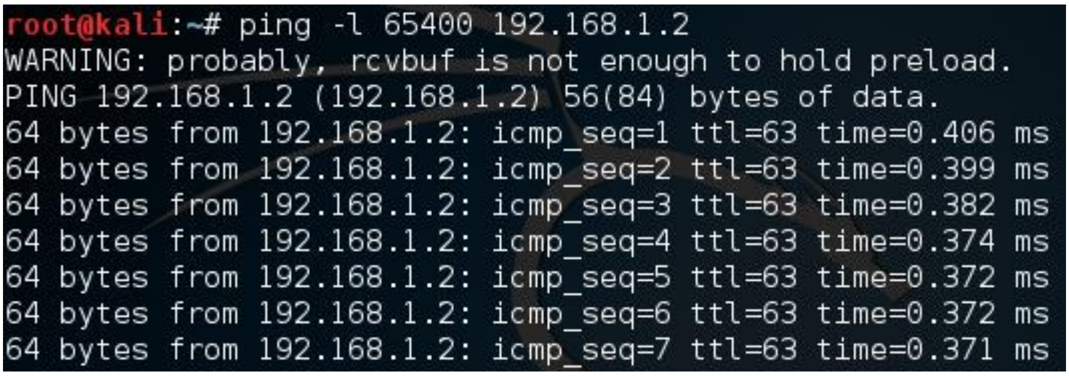
Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
☐	WAN	✓ C ●	AC-BNFA	DISABLED	DISABLED	WAN Snort	

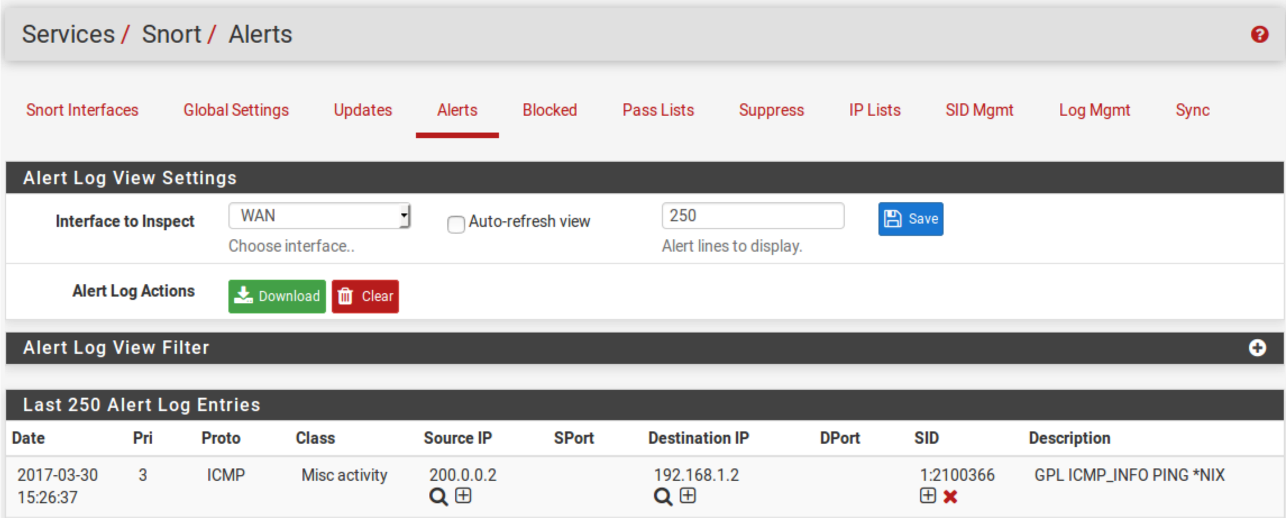
- **Snort running & detecting attacks (1p)**

With Kali generate some attacks and check that snort detects them, this should be something that snort detects:

```
ping -l 65400 192.168.1.2
```



```
root@kali:~# ping -l 65400 192.168.1.2
WARNING: probably, rcvbuf is not enough to hold preload.
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=0.406 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=0.399 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=0.382 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=0.374 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=63 time=0.372 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=63 time=0.372 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=63 time=0.371 ms
```



Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: WAN (Choose interface..) □ Auto-refresh view 250 (Alert lines to display.) Save

Alert Log Actions: Download Clear

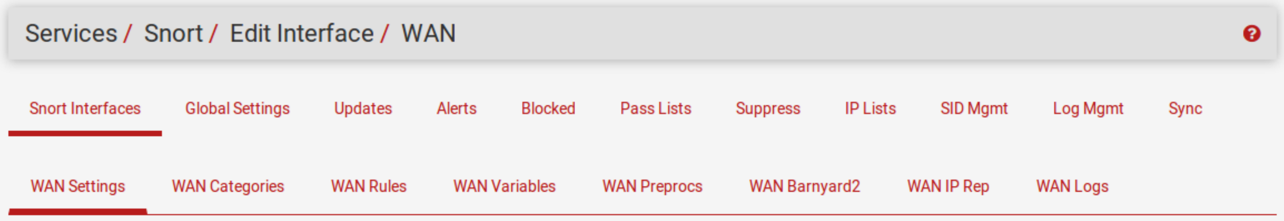
Alert Log View Filter

Last 250 Alert Log Entries

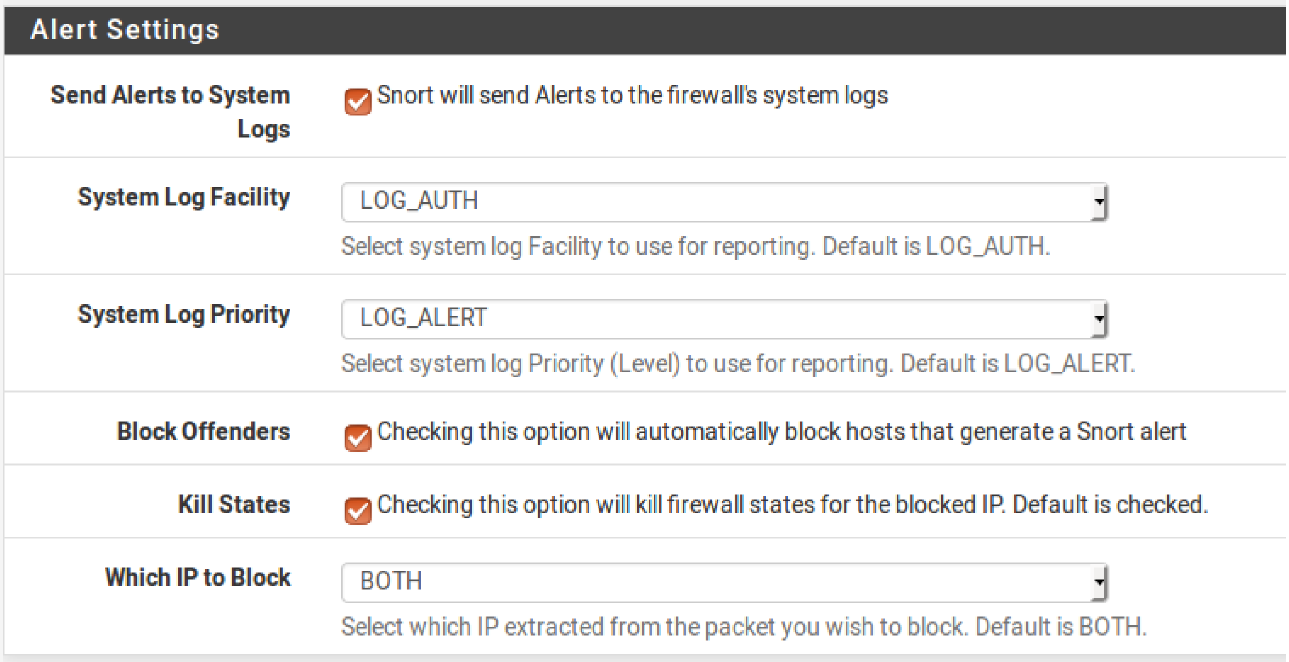
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-03-30 15:26:37	3	ICMP	Misc activity	200.0.0.2		192.168.1.2		1:2100366	GPL ICMP_INFO PING *NIX

- **Block Attacker (1p)**

Make snort to block attacker, when it detects attack



Services / Snort / Edit Interface / WAN

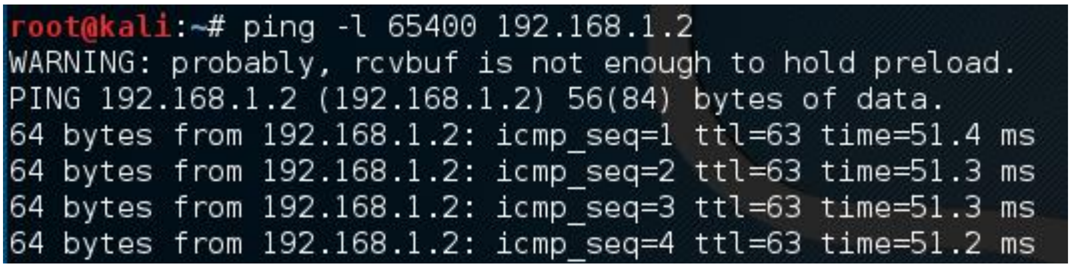


Alert Settings

Send Alerts to System Logs	☑ Snort will send Alerts to the firewall's system logs
System Log Facility	LOG_AUTH Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority	LOG_ALERT Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Block Offenders	☑ Checking this option will automatically block hosts that generate a Snort alert
Kill States	☑ Checking this option will kill firewall states for the blocked IP. Default is checked.
Which IP to Block	BOTH Select which IP extracted from the packet you wish to block. Default is BOTH.

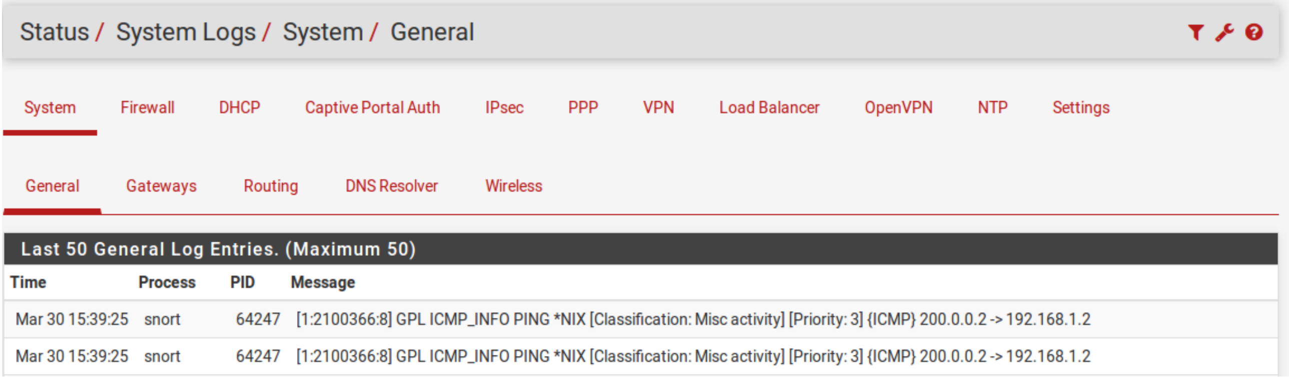
After restarting snort:

Testing the ping with kali



```
root@kali:~# ping -l 65400 192.168.1.2
WARNING: probably, rcvbuf is not enough to hold preload.
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=51.4 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=51.3 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=51.3 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=51.2 ms
```

Alerts of misc activity:

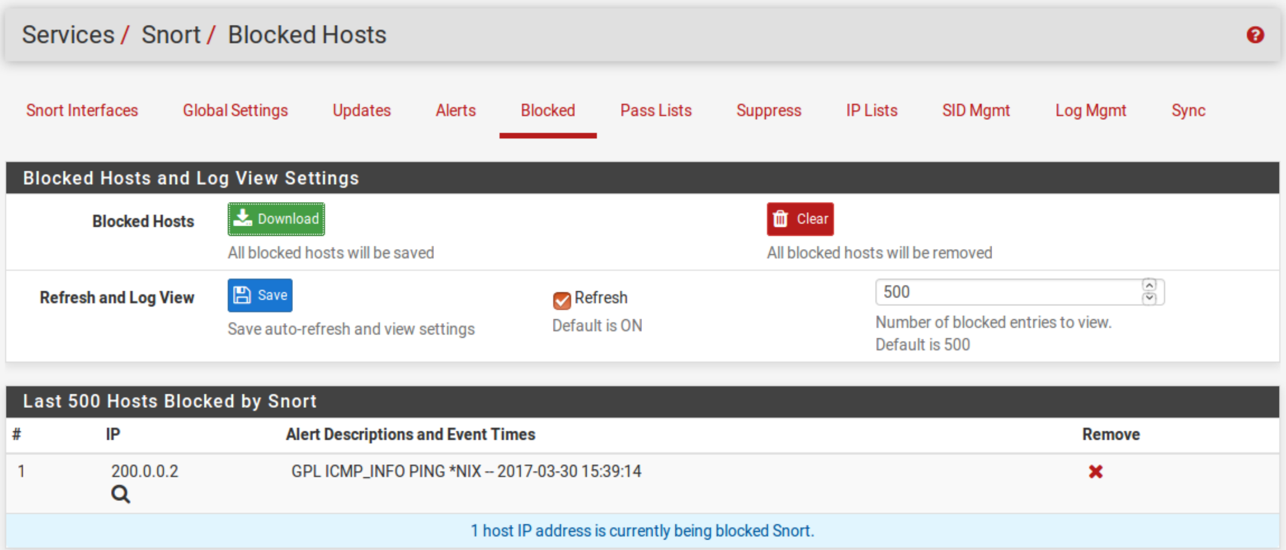


Status / System Logs / System / General

Last 50 General Log Entries. (Maximum 50)

Time	Process	PID	Message
Mar 30 15:39:25	snort	64247	[1:2100366:8] GPL ICMP_INFO PING *NIX [Classification: Misc activity] [Priority: 3] {ICMP} 200.0.0.2 -> 192.168.1.2
Mar 30 15:39:25	snort	64247	[1:2100366:8] GPL ICMP_INFO PING *NIX [Classification: Misc activity] [Priority: 3] {ICMP} 200.0.0.2 -> 192.168.1.2

The kali-VM is on the block list:



Services / Snort / Blocked Hosts

Blocked Hosts and Log View Settings

Blocked Hosts — Download — All blocked hosts will be saved — Clear — All blocked hosts will be removed

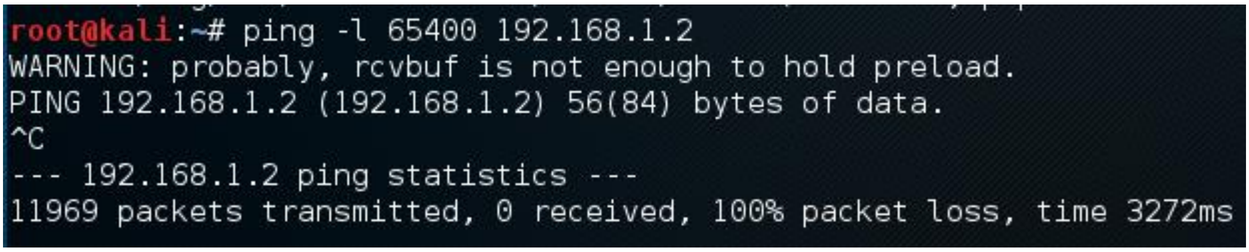
Refresh and Log View — Save — Save auto-refresh and view settings — ☑ Refresh — Default is ON — 500 — Number of blocked entries to view. Default is 500

Last 500 Hosts Blocked by Snort

#	IP	Alert Descriptions and Event Times	Remove
1	200.0.0.2	GPL ICMP_INFO PING *NIX -- 2017-03-30 15:39:14	✖

1 host IP address is currently being blocked Snort.

After the first ping the attacker cannot ping any more



```
root@kali:~# ping -l 65400 192.168.1.2
WARNING: probably, rcvbuf is not enough to hold preload.
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
11969 packets transmitted, 0 received, 100% packet loss, time 3272ms
```

- **Generate custom attack which gets detected (1p)**

Generate attack with Kali. Explain your attack, what it does, why it is bad thing etc.. And test if snort can detect it.