Lab Assignment – 4

- **Snort**

  Snort is an open-source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

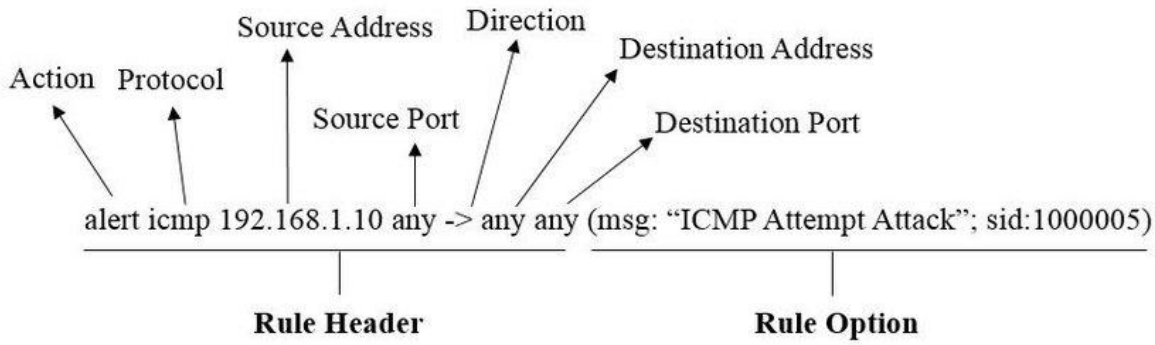
- **Snort Alert Modes**

  - **Fast:** Snort alerts include the timestamp, sending an alert message, showing the source and destination IP addresses and ports. To implement this mode, use the ***-A fast***
  - **Full:** Additionally, in the previously reported information in the fast mode, the full mode also prints the TTL, datagram length and packet headers, window size, ACK, and sequence number. To implement this mode, use the ***-A full***
  - **Console:** It shows the real time alerts in the console. This mode is enabled with the ***-A console***
  - **Cmg:** This mode is only useful for testing purposes.
  - **Unsock:** This is used to export alerts to Unix sockets.
  - **Syslog:** This mode (System Logging Protocol) instructs Snort to send a remote alert log. To run this mode, add ***-s***
  - **None:** No alerts.

- **Running snort on fast mode**

  sudo snort -A fast -c /etc/snort/snort.conf

- **Rule headers**
  - alert – Rule action. Snort will generate an alert when the set condition is met.
  - any – Source IP. Snort will look at all sources.
  - any – Source port. Snort will look at all ports.
  - -> – Direction. From source to destination.
  - $HOME_NET – Destination IP. We are using the HOME_NET value from the snort.conf file.
  - any – Destination port. Snort will look at all ports on the protected network.



Snort rule

- **Analysing incoming packet**

alert icmp any any -> $HOME_NET any (msg:"ICMP Test"; sid:1000001; rev:1)

1. sudo snort -A console -q -c /etc/snort/snort.conf -i eht0

```
stu@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
02/22-13:07:06.471944  [**] [1:1000001:1] ICMP test [**] [Classification: Generi
c ICMP event] [Priority: 3] {ICMP} 192.168.132.133 -> 192.168.132.130
02/22-13:07:06.472059  [**] [1:1000001:1] ICMP test [**] [Classification: Generi
c ICMP event] [Priority: 3] {ICMP} 192.168.132.130 -> 192.168.132.133
02/22-13:07:07.474545  [**] [1:1000001:1] ICMP test [**] [Classification: Generi
c ICMP event] [Priority: 3] {ICMP} 192.168.132.133 -> 192.168.132.130
02/22-13:07:07.474604  [**] [1:1000001:1] ICMP test [**] [Classification: Generi
c ICMP event] [Priority: 3] {ICMP} 192.168.132.130 -> 192.168.132.133
02/22-13:07:08.477023  [**] [1:1000001:1] ICMP test [**] [Classification: Generi
c ICMP event] [Priority: 3] {ICMP} 192.168.132.133 -> 192.168.132.130
```

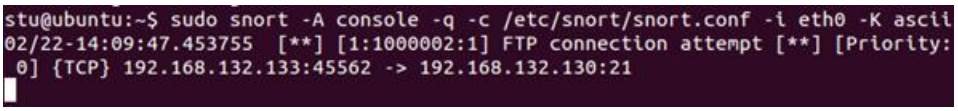
2. ping 192.168.x.x

```
root@attackserver:~# ping 192.168.132.130
PING 192.168.132.130 (192.168.132.130) 56(84) bytes of data.
64 bytes from 192.168.132.130: icmp_req=1 ttl=64 time=1.32 ms
64 bytes from 192.168.132.130: icmp_req=2 ttl=64 time=0.949 ms
64 bytes from 192.168.132.130: icmp_req=3 ttl=64 time=0.906 ms
64 bytes from 192.168.132.130: icmp_req=4 ttl=64 time=1.35 ms
64 bytes from 192.168.132.130: icmp_req=5 ttl=64 time=0.877 ms
^C
--- 192.168.132.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 0.877/1.082/1.353/0.212 ms
root@attackserver:~#
```

- **Analysing outgoing packet**

alert tcp 192.168.x.x any -> $HOME_NET 21 (msg:”FTP connection attempt”; sid:1000002; rev:1)

1. sudo snort -A console -q -c /etc/snort/snort.conf -i eht0 -K ascii



2. ftp 192.168.x.x