
SNORT®
Abegail Jakop and Minh Le Hoang

Reminder: Snort

- Network intrusion detection and prevention service
- 3 modes
  - Sniffing, logging and intrusion detection
- Rules consist of a header and options

Header

- action
- protocol
- IP+netmask and port

action protocol IP+netmask port
DIRECTION IP+netmask port

Options

- message
- sd_pattern

(option: ...; option2: ...; ...)

Credit Card Numbers

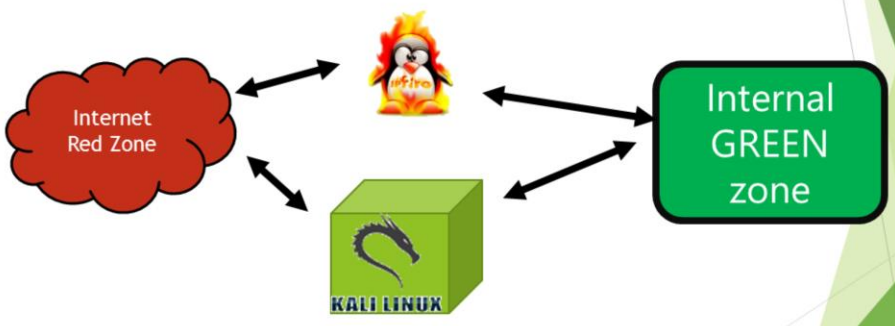
```
alert tcp $HOME_NET any
-> $EXTERNAL_NET [80,20,25,143,110]
(msg:"SENSITIVE-DATA Credit Card Numbers";
sd_pattern:2,credit_card; )
```

Guardian + Snort

- Guardian is part of IPFire
- Guardian blocks IP based on Snort logs
  - Blocks by adding a rule in the firewall (IPFire)
- Detection -> Prevention


New content!

Topology



Configuration Files

- Include rules and other files
- Declare variables
  - ipvar, portvar, var
  - VARTYPE VARNAME VARVALUE
  - ipvar HOME_NET [192.168.1.0/24, 10.1.1.0/24]
- Specify when running snort

- alert - generate an alert using the selected alert method, and then log the packet
- log - log the packet
- pass - ignore the packet
- drop - block and log the packet
- reject - block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
- sdrop - block the packet but do not log it.

Option Types

- General
  - message, metadata
- Payload detection
  - content, length, ssl_version
- Non-payload detection
  - id, ttl, flow
- Post-detection
  - activates, activated_by, count

More about Rules

- Static rules
  - Have an immediate and consistent action
- Dynamic rules
  - Events differ based on what other rules are triggered

Dynamic Rules

- actions
  - dynamic
    - remain idle until activated by an activate rule , then act as a log rule
    - (…; activated_by: id; count: ##)
  - activate
    - alert and then turn on another dynamic rule
    - (…; activates: id)

Dynamic Rules

- non-payload detection option
  - flow bits
    - sets "states" and avoid logging
      - flowbits:set,logged_in; flowbits:noalert;
    - checks state, and logs if it matches
      - flowbits:isset,logged_in;

Dynamic Rules

- post-detection option
  - tags
    - once a rule is triggered, all subsequent traffic from the same host or session is logged for a specified period