Lab 12 Notes

TA: 江易達 ccpz@ytchiang.net

Install Snort

- Snort in some distribution don't compile with inline (ex.Ubuntu)
  - If your rule has reject, it will shows:
  - Unknown rule type: reject
- Download snort-2.8.6.tar.gz from http://www.snort.org
- ./configure --enable-inline && make
- The binary is under src/

Bridge Interface Setup

- Install bridge-utils
- Clearing IP settings of network interfaces
  - ifconfig eth0 0.0.0.0
  - ifconfig eth1 0.0.0.0
- Creating new bridge interface
  - brctl addbr br0
- Adding interfaces into bridge
  - brctl addif br0 eth0
  - brctl addif br0 eth1
- Bringing up bridge interface
  - ifconfig br0 up

Snort Rules

- You need add unique **sid** in each rule
  - alert tcp any any <> $server 80 (**sid:10001**; msg:"http connection";)
- When you write your own rules, you can:
  - String matching content:""
  - Regular expression pcre:"//"
- Official snort rules:
  - http://www.snort.org/snort-rules/?#rules
  - You need to pay for newest rules
  - You can register freely for rules released after 30 days