TÀI LIỆU HƯỚNG DẪN XÂY DỰNG TESTBED

MỤC LỤC

Sơ đồ kiến trúc SDN chống tấn công chung 3

Đồ hình testbed 3

Các module phát triển trên controller và Openflow switch 4

Hướng dẫn chạy controller Floodlight 6

Hướng dẫn chạy module Analyzer 10

Hướng dẫn các cách phát kịch bản tấn công 12

DANH MỤC HÌNH VẼ

Figure 1. Kiến trúc mạng SDN chống tấn công 3

Figure 2. Đồ hình mạng doanh nghiệp thử nghiệm 4

Figure 3. Các module phát triển trên Gateway và controller 4

# Sơ đồ kiến trúc SDN chống tấn công chung

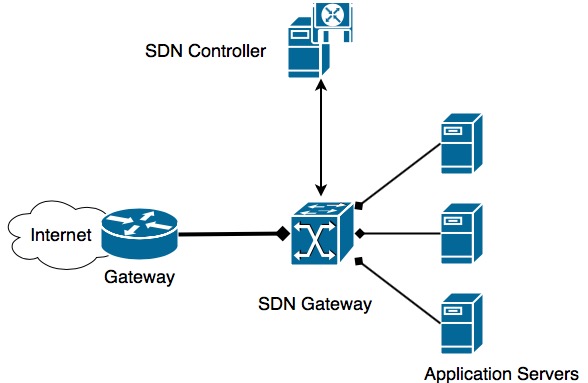


Figure 1. Kiến trúc mạng SDN chống tấn công

Trong kiến trúc này, chúng ta đặt bộ SDN gateway, tại vị trí cửa ngõ đầu vào để bảo vệ các application server tại mạng doanh nghiệp bên trong. Bộ gateway này sẽ chịu sự chỉ đoạ của SDN controller để điều phối lưu lượng đi vào từ Internet. Tại bộ gateway này, hệ thống tiền hành giám sát, phân tích lưu lượng đi vào theo các chỉ số đặt ra. Sau một khoảng thời gian giám sát và phân tích lưu lượng, bộ controller sẽ đưa ra cảnh báo nếu có dấu hiệu bất thường và tiến hành các chính sách giảm thiểu tấn công khác nhau.

# Đồ hình testbed

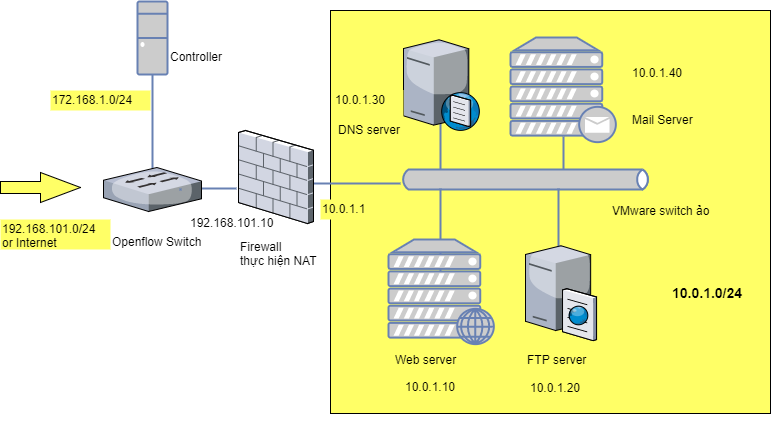


Figure 2. Đồ hình mạng doanh nghiệp thử nghiệm

# Các module phát triển trên controller và Openflow switch

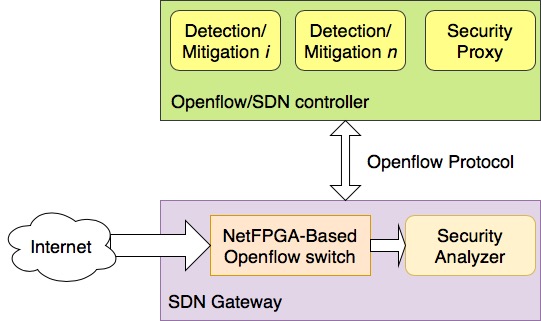


Figure 3. Các module phát triển trên Gateway và controller

Trong đó, các module hiện nay đang phát triển trên controller gồm:

* Module phát hiện và đưa chính sách chống tấn công dùng Fuzzy Logic --> dùng cho TCP SYN
  + Chính sách giảm thiểu: xoá tỷ lệ Z các flow trên toàn bộ flow, xoá các flow TCP có 1 packet đầu tiên.
* Module phát hiện tấn công dựa vào One class support vector machine --> dùng cho cả ICMP và TCP
  + Chính sách giảm thiểu: cài 1 flow entry với action: đánh rớt toàn bộ gói tin ICMP
  + Chính sách giảm thiểu: xoá toàn bộ các TCP flow có 1 gói tin
* Module phát hiện tấn công DNS amplification dùng ngưỡng xác định
  + Đóng port 53 chặn các bản tin DNS response trong vòng 5s ( idle time out của 1 flow entry). Trong vòng 5s từ lúc bắt đầu đóng port, nếu có bản tin DNS response tới thì chu kỳ 5s này lại được reset lại từ đầu.

# Hướng dẫn chạy controller Floodlight

* B1: cài git cho Ubuntu

$sudo apt-get install git

* B2 : Tải floodlight Controller trên github

$git clone <https://github.com/VuongBaNam/floodlight.git>

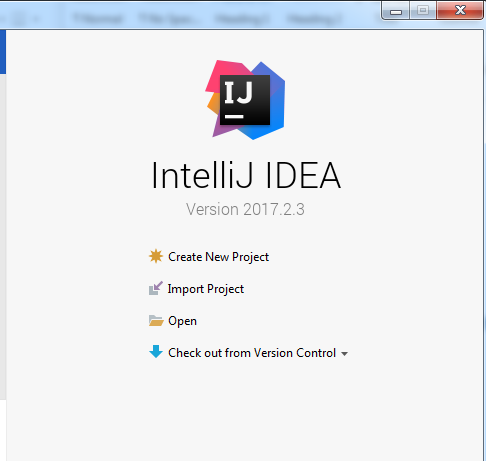
* B3 : build floodlight trên phần mềm intellij
* Tải Intellij trên trang chủ <https://www.jetbrains.com/idea/download/#section=linux>
* Chạy Intellij :

$ cd /<Thư mục vừa giải nén từ file tải về>/bin

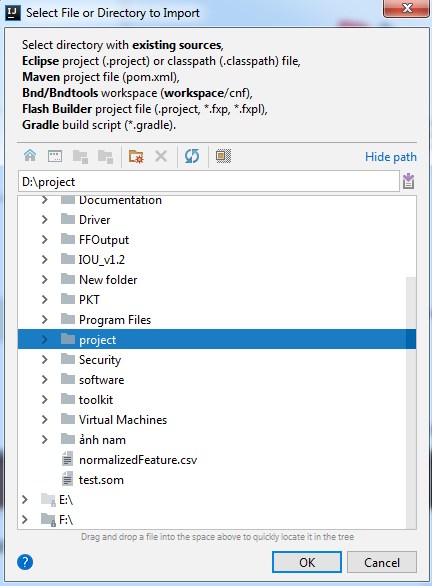
$./idea.sh

* Import floodlight:

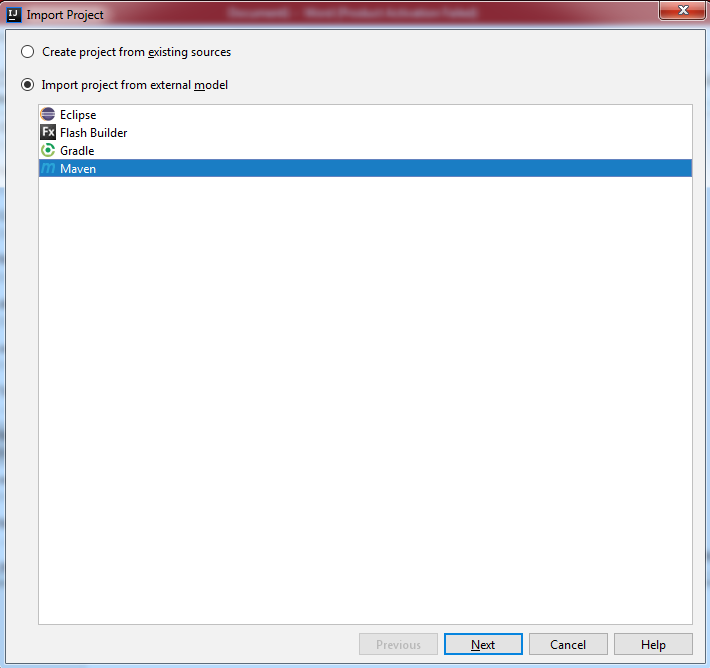
Chọn Import project



Chọn đường dẫn đến project Floodlight rồi ấn OK



Chọn Import project from external module -> Maven



Sau đó chọn Next-> Next->Next->Next -> Finish

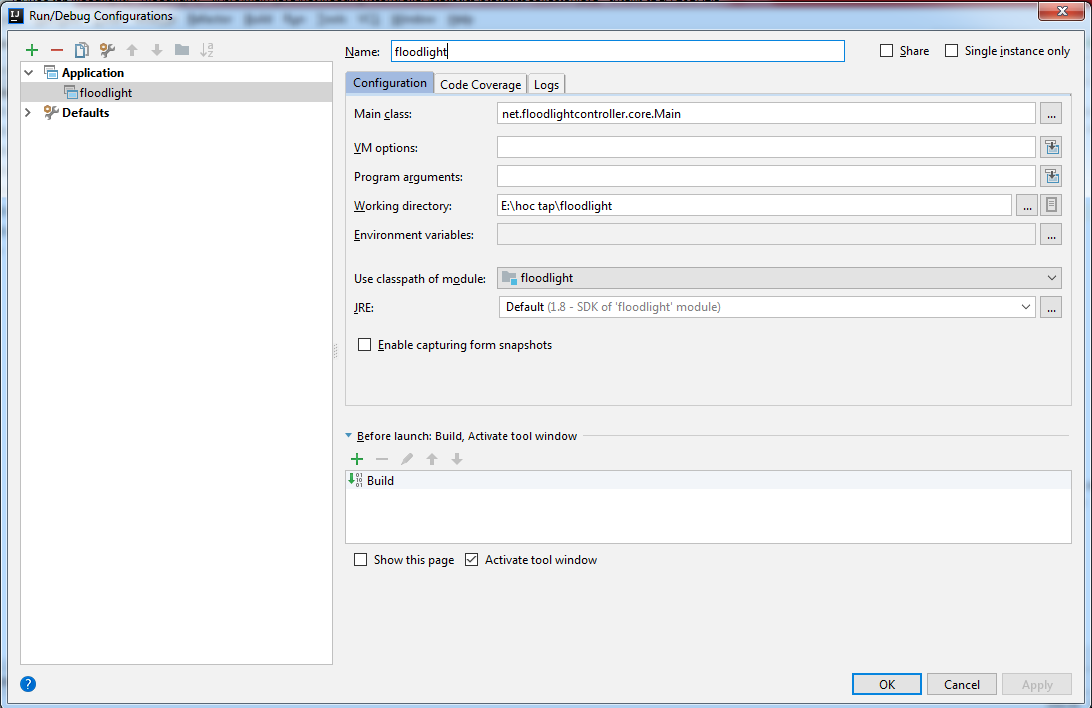
* B4 : Chạy Floodlight Controlller

Sau khi build xong project Chọn Run -> Edit Confìgurations

Trong cửa sổ Run/Debug Confìgurations chon dấu [+] -> Application

Trong Main class chọn class net.floodlightcontroller.core.Main

Chọn OK



Các module phát hiện và giảm thiểu tấn công đã được xây dựng trong Floodlight Controller



Như hình trên thì ta đang chạy tất cả các module. Nếu muốn chạy module nào thì ta comment các module còn lại.

Để chạy Floodlight Controller thì ta nhấn Shift+F10

# Hướng dẫn chạy module Analyzer

sudo setcap cap\_net\_raw,cap\_net\_admin,cap\_dac\_override+eip <Đường dẫn đến máy ảo java>

* B1 : Tải project CMD trên github

$git clone <https://github.com/VuongBaNam/CMD.git>

* B2 : Làm tương tự với project floodlight như trên nhưng với thư mục CMD
* B3 : Chỉnh các thông số cần thiết trong Utils.java

**public class** Utils {

// IP của controller  
 **public static final** String ***IP\_CONTROLLER*** = **"127.0.0.1"**;

// Port socket được mở trên controller

//Mặc định là port 5000  
 **public static final int *PORT*** = 5000;

//   
 **public static final double *THRESHOLD\_IAT*** = 0.2;  
}

* B4 : Chạy Project CMD

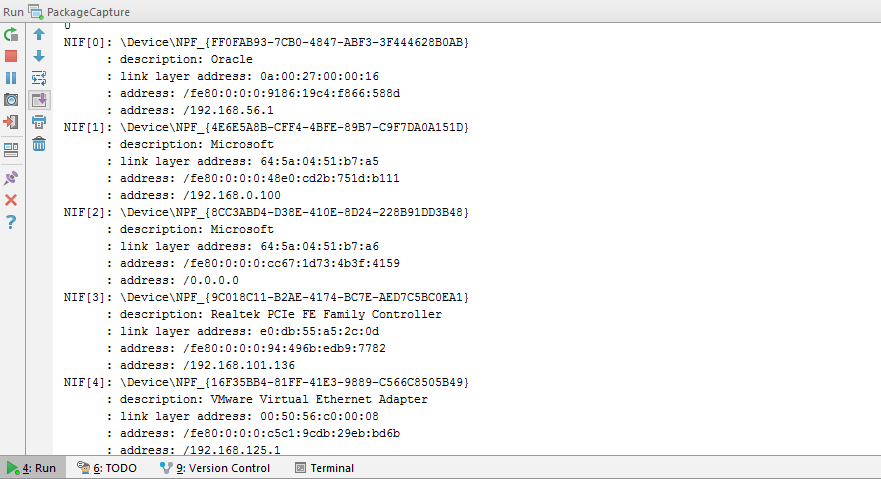
Sau khi build xong project Chọn Run -> Edit Confìgurations

Trong cửa sổ Run/Debug Confìgurations chon dấu [+] -> Application

Trong Main class chọn class capture.PackageCapture

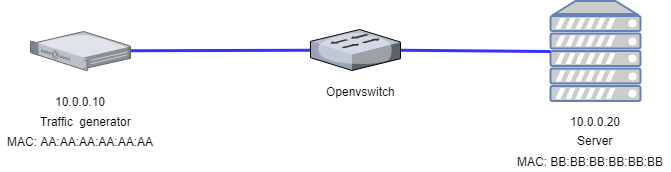
Chọn OK

Để chạy nhận Shift+F10



Nhập số tương ứng với Network Interface Card - chính là port được kết nối với victim mà ta muốn thống kê thông tin.

# Hướng dẫn các cách phát kịch bản tấn công



1. Sử dụng TCP-Replay phát các loại tấn công NTP,SNMP,DNS:

Mô hình test tấn công NTP,SNMP,DNS như hình trên:

|  |  |  |
| --- | --- | --- |
| Tên | Chức năng | Công cụ |
| Traffic Generator | Phát lại file pcap | TcpReplay |
| Openvswitch | Chuyển tiếp gói tin | Openvswicth |
| Server | Nạn nhân | Web Server |

Sau khi thu được các file pcap NTP, SNMP, DNS ta thực hiện các bước sau để thay đổi IP và Mac các file pcap.

Các file pcap hiện tại được để trên máy traffic generator địa chỉ ip 192.168.101.171

Để truy nhập vào sử dụng các file pcap ta làm các bước sau:

Bước 1:Thực hiện ssh vào traffic

$ssh [traffic@192.168.101.171](mailto:traffic@192.168.101.171)

password là 1

Bước 2: Vào thư mục root

$sudo –i

Với password là 1

Tiếp theo là phát lại các file pcap sử dụng TcpReplay xem mô hình phía trên tham khảo

Bước 1: Thay đổi ip đích

**$** tcprewrite --endpoints=192.168.1.10:10.0.0.20 --infile=input.pcap --outfile=output.pcap –skipbroadcast

Trong đó:

* --endpoint=ip\_ban\_đầu:ip\_muốn\_đổi\_thành
* --infile=tên\_file\_pcap\_muốn\_đổi
* --outfile=tên\_file\_pcap\_ghi\_vào

Bước 2: Thay đổi mac nguồn , mac đích

$ tcprewrite --enet-dmac= BB:BB:BB:BB:BB:BB --enet-smac= AA:AA:AA:AA:AA:AA --infile=input.pcap --outfile=output.pcap –dlt=enet

* --enet-dmac =mac\_đích\_muốn\_đổi\_thành
* --enet-smac =mac\_nguồn\_muốn\_đổi\_thành
* --infile=tên\_file\_pcap\_muốn\_đổi
* --outfile=tên\_file\_pcap\_ghi\_vào

Bước 3: Phát lại file pcap với tốc độ nhanh hơn

$ sudo tcpreplay -i enp10s0f0 -l 10000 -M 1000.0 dns.pcap

Trong đó :

* -i tên cổng mạng muốn phát traffic vào
* -l số lần phát lặp lại
* -M số lần muốn tốc độ phát tăng lên
* Dns.pcap tên file muốn phát

Trên máy traffic generator đã có các file snmp.pcap và ntp.pcap là các file tấn công của snmp attack và ntp attack sử dụng câu lệnh này để phát các file đó.

$ sudo tcpreplay -i enp10s0f0 -l 10000 -M 1000.0 snmp.pcap

$ sudo tcpreplay -i enp10s0f0 -l 10000 -M 1000.0 ntp.pcap

2. Sử dụng Bonesi tạo các loại tấn công ICMP,UDP,TCP SYN,HTTP GET

Cách sử dụng:

**Tấn công icmp**

*$bonesi -i 50k-bots -d lo -r 50000 -s 1400 -p icmp ip\_đích:22*

**Tấn công tcp syn**

*$bonesi -i 50k-bots -d lo -r 50000 -s 1400 -p tcp ip\_đích:22*

**Tấn công udp**

*$bonesi -i 50k-bots -d lo -r 50000 -s 1400 -p udp ip\_đích:22*

**Tấn công http get (chú ý port 80 là port dịch vụ web và cần thực hiện thêm route)**

**Bước 1: Tạo route cho gói tin trả về**

***$sudo route add default gw ip\_gateway\_trỏ\_đến dev tên\_cổngmạng\_đến\_gateway\_đó***

**Vd : Trong mô hình trên**

***$sudo route add default gw 10.0.0.10 dev eth0***

**Các gói tin sẽ trả về phía traffic generator qua cổng eth0 của nạn nhân**

**Bước 2: Phát tấn công http get**

*$bonesi -i 50k-bots -d lo -r 50000 -s 1400 -p tcp ip\_đích:80*

Trong đó:

* -i : tên file chứa địa chỉ IP mô phỏng mạng botnet
* -d : tên cổng mạng muốn phát gói qua
* -r : số lượng gói tin muốn phát trong 1 giây
* -s : kích thước gói tin bytes (đối với tấn công udp, icmp )
* -p : giao thức tấn công muốn thực hiện có tcp(bản chất là tcpsyn) , http (vẫn sử dụng tcp cần cấu hình thêm route), udp,icmp.

Do nhược điểm chỉ phát được một lượng gói tin cố định và địa chỉ IP cụ thể mỗi giây, ta đã phát triển công cụ Bonesi lên để có khả năng với gói tăng liên tục với lượng địa chỉ IP cũng gia tăng theo. Giải pháp sử dụng đó là chạy nhiều tiến trình song song dưới mức hệ điều hành sao cho mỗi tiến trình sẽ thực thi một tiến trình phát gói sử dụng bonesi với tương ứng một file IP botnet khác nhau để số lượng botnet và gói có thể tăng tuyến tính theo thời gian.

*max=30*

*for i in `seq 1 $max`*

*do*

*r=$(( $RANDOM % 1000 + 5000 ))*

*screen -dmS mutilbonesi bonesi -i $i -d lo -r $r -s 1400 -p icmp 127.0.0.1:22*

*sleep 5*

**done**