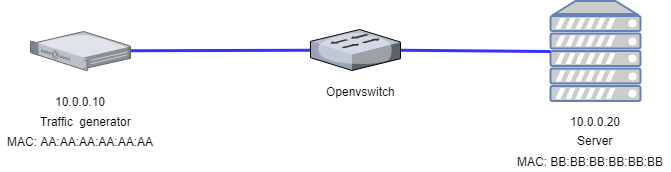
# 1 Hướng dẫn sử dụng tấn công bonesi và tcpreplay



* 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 moo 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

1.2. 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,chúng em 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*

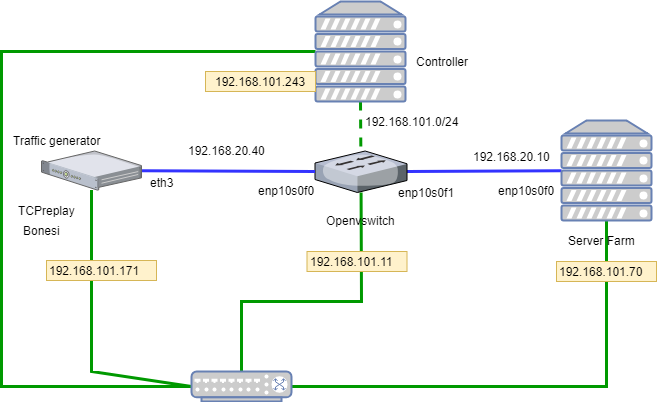
*r=$(( $RANDOM % 1000 + 5000 ))*

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

*sleep 5*

**done**

2. Phát lưu lượng trên testbed:



Bước 1: Truy cập ssh vào 192.168.101.171 vào quyền root

$sudo –i

$ cd traffic\_testbed

Bước 2 : Thực hiện tấn công và phát traffic thường

Traffic normal

Tcpreplay –i eth3 traffic\_normal.pcap

Tấn công tcpsyn

./bonesi-tcp.sh 1000 192.168.20.10

Tấn công ICMP

./ multi-bonesi-icmp.sh 192.168.20.10

Tấn công DNS

./multi-tcpreplay-dns.sh

Vào giao diện sflow :

Khởi động sflow :

$cd sflow-rt/

$ ./start.sh

* Vào trang web

<http://192.168.101.243:8008/>

chọn [dashboard-example-master](http://192.168.101.243:8008/app/dashboard-example-master/html/)

Khởi động fpga

Ssh vào máy fpga

Chạy lệnh

$ sudo -i

$ ./nic1.sh

$reboot

$./nic2.sh

Gắn card FPGA vào openvswitch

$ ./start-ovs.sh 192.168.101.243:6653

Tên tài khoản và đăng nhập các máy :

Controller :

User :fil

Password:1

NetFpga:

User :super-switch

Password:1

Traffic generator:

User :traffic

Password:1

Server Farm:

User :admin123

Password:abc123-+