BoNeSi

MỤC LỤC

1.Tổng quan

1.1.Giới thiệu

- BoNeSi, DDoS Botnet Simulator là tool để mô phỏng Botnet Traffic trong môi trường testved trên wire. Nó được thiết kết để nghiên cứu ảnh hưởng của cả các cuộc tấn công DDoS.

- Traffic nào có thể được tạo?

BoNeSi tạo ra các cuộc tấn công flooding ICMP, UDP và TCP (HTTP) từ một kích thước botnet đã xác định (các địa chỉ IP khác nhau). **BoNeSi có** highly configurable và rates, data volume, source IP addresses, URLs và một số parameters có thể được cấu hình.

- Điều gì làm cho nó khác với các công cụ khác?

Có rất nhiều công cụ khác ngoài đó để giả mạo địa chỉ IP với UDP và ICMP, nhưng đối với giả mạo TCP, không có giải pháp. BoNeSi là công cụ đầu tiên để mô phỏng HTTP-GET floods từ các mạng bot quy mô lớn. **BoNeSi** cũng cố gắng tránh tạo các packets với các mẫu có thể nhận dạng dễ dàng (có thể lọc ra dễ dàng).

- Tôi có thể chạy **BoNeSi** ở đâu?

Chúng tôi khuyên bạn nên chạy **BoNeSi** trong môi trường testbed kín. Tuy nhiên, các cuộc tấn công UDP và ICMP có thể chạy trên internet, nhưng bạn nên cẩn thận. Các cuộc tấn công HTTP-Flooding không thể được mô phỏng trên internet, bởi vì các câu trả lời từ webserver phải được chuyển trở lại host chạy **BoNeSi**.

- TCP Spoofing hoạt động như thế nào?

BoNeSi tìm kiếm các TCP packets trên network interface và responds tất cả các packets để thiết lập các kết nối TCP. Đối với tính năng này, nó là cần thiết, rằng tất cả lưu lượng truy cập từ target webserver được chuyển trở lại host chạy **BoNeSi**.

- Làm thế nào để performance của **BoNeSi** được tốt?

Chúng tôi tập trung rất nhiều vào performance để mô phỏng các botnet lớn. Trên AMD Opteron với 2Ghz, chúng tôi có thể tạo ra tới 150.000 packets/s. Trên một chiếc AMD Phenom II X6 1100T gần đây hơn với 3.3Ghz, bạn có thể tạo ra 300.000 pps (chạy trên 2 lõi).

- Có phải **BoNeSi** tấn công thành công?

Có, họ rất thành công. Các cuộc tấn công UDP / ICMP có thể dễ dàng lấp đầy băng thông và các cuộc tấn công HTTP-Flooding loại bỏ các webserver nhanh chóng. Chúng tôi cũng đã thử nghiệm **BoNeSi** chống lại các hệ thống giảm thiểu DDoS thương mại hiện đại và có thể làm hỏng chúng hoặc ẩn các cuộc tấn công khỏi bị phát hiện.

1.2.Chi tiết

- BoNeSi là network traffic generator cho các loại protocols khác nhau. Các attributes của các packets và kết nối được tạo ra có thể được kiểm soát bởi một số parameters như rate hoặc payload size hoặc chúng được xác định một cách tình cờ. Nó giả mạo source ip addresses ngay cả khi tạo tcp traffic. Nó bao gồm một tcp-stack đơn giản để xử lý các kết nối TCP ở chế độ promiscuous. Đối với công việc chính xác, người ta phải đảm bảo rằng

các response packets được định tuyến đến hosts mà BoNeSi đang chạy. Do đó BoNeSi không thể sử dụng trong cơ sở hạ tầng mạng tùy ý. Loại lưu lượng truy cập tiên tiến nhất có thể được tạo là các http requests.

- **TCP HTTP** Để làm cho các http requests thực tế hơn, một số điều được xác định bởi cơ hội:

- source port
- ttl: 3..255
- tcp options: out of seven different real life options with different lengths and probabilities
- user agent for http header: out of a by file given list (an example file is included, see below)

2.Cài đặt và sử dụng

2.1.Cài đặt trên Ubuntu Server 14.04

- Lưu ý: Các command sau đây sử dụng user root.

- Update và upgrade:

```
apt update -y && apt upgrade -y
```

- Cài đặt các packets liên quan:

```
apt install make
apt install build-essential
apt install libpcap-dev libnet-dev autoconf gcc automake
```

- Clone repo BoNeSi:

```
apt install git
git clone https://github.com/Markus-Go/bonesi
```

- Cài đặt:

```
cd bonesi
```

```
autoreconf
./configure
automake --add-missing
make
make install
```

- Chú ý:

BoNeSi dùng automake 1.14 nên chỉ cài trên Ubuntu 14.04 và các phiên bản Ubuntu sử dụng automake 1.14. Ubuntu 16.04 sử dụng automake 1.15 nên không cài được!

2.2.Sử dụng

- Cú pháp:

```
:~$ bonesi [OPTION...] <dst_ip:port>


 Options:


  -i, --ips=FILENAME               filename with ip list
  -p, --protocol=PROTO             udp (default), icmp or tcp
  -r, --send_rate=NUM              packets per second, 0 = infinite
(default)
  -s, --payload_size=SIZE          size of the paylod, (default: 32)
  -o, --stats_file=FILENAME        filename for the statistics,
(default: 'stats')
  -c, --max_packets=NUM            maximum number of packets (requests
at tcp/http), 0 = infinite (default)
      --integer                    IPs are integers in host byte order
instead of in dotted notation
  -t, --max_bots=NUM               determine max_bots in the 24bit
prefix randomly (1-256)
```

```
  -u, --url=URL                     the url (default: '/') (only for
tcp/http)
  -l, --url_list=FILENAME           filename with url list (only for
tcp/http)
  -b, --useragent_list=FILENAME     filename with useragent list (only
for tcp/http)
  -d, --device=DEVICE               network listening device (only for
tcp/http, e.g. eth1)
  -m, --mtu=NUM                     set MTU, (default 1500). Currently
only when using TCP.
  -f, --frag=NUM                    set fragmentation mode (0=IP,
1=TCP, default: 0). Currently only when using TCP.
  -v, --verbose                     print additional debug messages
  -h, --help                        print help message and exit
```

- VD1: Sử dụng địa chỉ IP nguồn trong file 50-bots, interface eth0, giao thức eth0, 50000 packets/s, payload size (chính là data) của packet là 30B, địa chỉ IP đích là 10.0.0.2 và port đích là 29

```
bonesi -i 50k-bots -d eth0 -p icmp -r 50000 -s 30 172.16.69.11:29
```

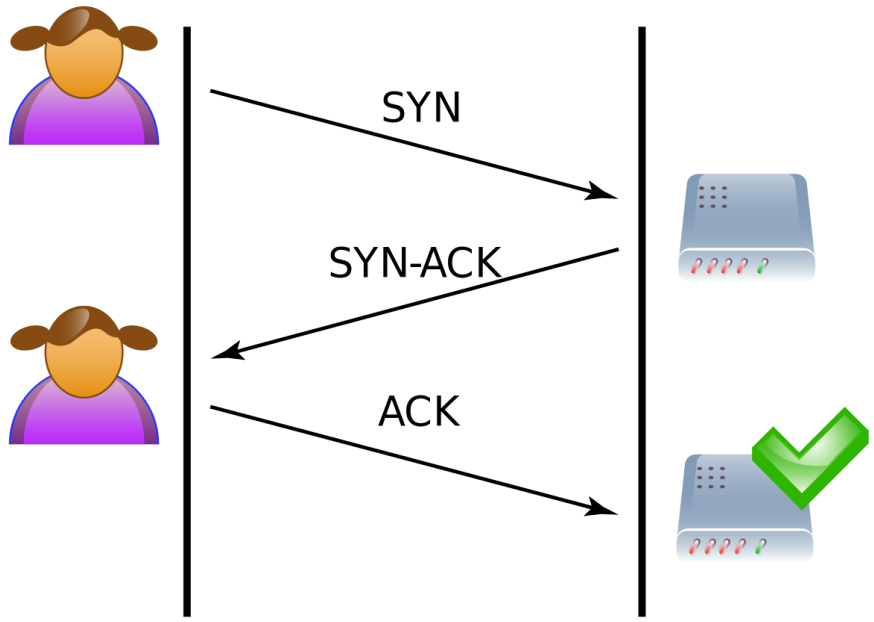
- VD2: Sử dụng giao thức UDP

```
bonesi -i 50k-bots -d eth0 -p udp -r 50000 -s 30 172.16.69.11:29
```

- VD3: Sử dụng giao thức TCP

```
bonesi -i 50k-bots -d eth0 -p tcp -r 50000 -s 30 172.16.69.11:29
```

BoNeSi sẽ gửi TCP SYN đến 172.16.69.11:29.


SYN
SYN-ACK
ACK

THAM KHẢO