**BÁO CÁO LAB 6**

*Môn: An toàn mạng máy tính nâng cao*

*GVTH: Đỗ Thị Phương Uyên*

|  |  |
| --- | --- |
| Sinh viên thực hiện | **Sinh viên 1**  MSSV: 21521520  Họ tên: Huỳnh Minh Tân Tiến  **Sinh viên 2**  MSSV: 21521817  Họ tên: Bùi Hoàng Trúc Anh  **Sinh viên 3**  MSSV: 21521253  Họ tên: Lê Hoàng Oanh  **Sinh viên 4**  MSSV: 21520353  Họ tên: Nguyễn Ngọc Trà My |
| Lớp | **NT534.O21.ATCL** |
| Tổng thời gian thực hiện Lab trung bình |  |
| Phân chia công việc  *(nếu là nhóm)* | **[Sinh viên 1]**:  **[Sinh viên 2]**: |
| Link Video thực hiện *(nếu có yêu cầu)* |  |
| Ý kiến *(nếu có)*  *+ Khó khăn gặp phải + Đề xuất, góp ý…* |  |
| Điểm tự đánh giá *(bắt buộc)* | 10/**10** |

*[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]*

1. **SYN Flooding một Target Host bằng Metasploit**

Máy victim: Windows 10 – IP: 192.168.30.137

A screenshot of a computer

Description automatically generated

Máy attacker: Kali Linux – IP: 192.168.30.132

A computer screen shot of a program

Description automatically generated

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 192.168.30.137/24

A computer screen shot of a computer program

Description automatically generated

Bước 2: Xác định cổng 4444 đóng hay mở. Dùng nmap để kiểm tra tình trạng của cổng này. Gõ lệnh: nmap –p 4444 192.168.30.137

A computer screen shot of a computer program

Description automatically generated

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:



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

Bước 5: Gõ lệ̂nh 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.

Chúng ta sẽ thiết lập:

set RHOST 192.168.30.137

set RPORT 4444

A screen shot of a computer screen

Description automatically generated

Buớc 7: Gõ lệnh exploit để tấn công DoS

A screen shot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **SYN Flooding bằng Hping 3**

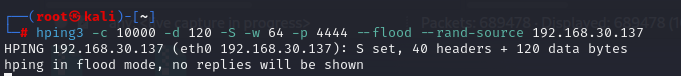
Bước 1: Tại máy Victim, bật công cụ bắt gói tin Wireshark

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

hping3 -c 10000 -d 120 -S -w 64 -p 4444 --flood --rand-source 192.168.30.137

Trong đó:

* -c 1000 là số packet sẽ gửi đi
* -d 120 là kích thuớc 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 tam tới replies của target
* --rand-source là tùy chọn nhằm random địa chỉ IP giả mạo đê tấn công



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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **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

A screenshot of a computer program

Description automatically generated

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

A screenshot of a computer screen

Description automatically generated

* Nhập email gửi nhận thông báo

A screenshot of a computer

Description automatically generated

* 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

A screenshot of a computer program

Description automatically generated

* Giữ nguyên các thiết lập còn lại.

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

A screenshot of a computer

Description automatically generated

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

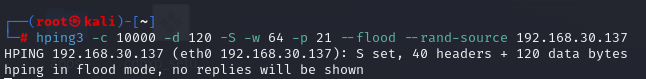
• Dùng công cụ nmap trên máy Kali Linux để scan cổng FTP trên máy nạn nhân có mở hay không

A screen shot of a computer

Description automatically generated

• Tiếp theo chúng ta sẽ dùng hping3 để tấn công DoS cổng 21 trên máy tính nạn nhân

hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.30.137



Bước 5: Quan sát kết quả của KFSensor.

A screenshot of a computer

Description automatically generated

KFSensor có khả năng nhận biết các cuộc tấn công và gửi email thông báo cho người dùng. Cụ thể hơn, khi KFSensor phát hiện hoạt động đáng ngờ hoặc tấn công vào hệ thống của bạn, nó có thể được cấu hình để gửi các cảnh báo qua email hoặc các phương thức thông báo khác, tùy thuộc vào thiết lập của bạn.