BÁO CÁO THỰC HÀNH

**Môn học: Tấn Công Mạng**

**Lab 1:**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT522.N11.ATCL.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Quang Huy | 20520546 | 20520546@gm.uit.edu.vn |
| 2 | Bùi Đức Hoàng | 20520514 | 20520514@gm.uit.edu.vn |
| 3 | Triệu Quốc Minh | 18521110 | 18521110@gm.uit.edu.vn |
| 4 | Nguyễn Quốc Huy | 18520847 | 18520847@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Tấn công DoS/DDoS với Scapy | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Tấn công Dos bằng Scapy

### UDP Flooding

Các cuộc tấn công UDP Flooding là một loại tấn công từ chối dịch vụ (DoS) khai thác Giao thức gói dữ liệu người dùng (UDP). Các cuộc tấn công này nhằm mục đích áp đảo một hệ thống mục tiêu bằng cách gửi một số lượng lớn các gói UDP đến các cổng ngẫu nhiên trên máy chủ.

Để thực hiện tấn công UDP Flooding bằng scapy, nhóm sử dụng đoạn code sau :

A black background with colorful text

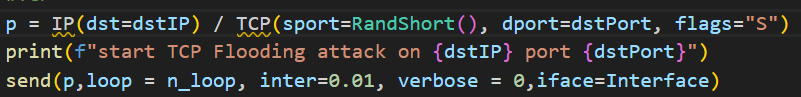
Description automatically generated

Đầu tiên, ta cần tạo một gói tin UDP sử dụng thư viện Scapy với địa chỉ IP đích (dstIP) là địa chỉ máy nạn nhân, cổng đích (dstPort) là cổng kết nối của nạn nhân cần tấn công và dữ liệu (payload) cho gói tin. Sau đó, sử dụng send để gửi gói tin UDP (p) tới địa chỉ IP và cổng mục tiêu với chỉ định loop = True (n\_loop), thời gian chờ giữa các gói tin (inter) được set với thời gian trong 0.01s và interface mạng sử dụng (iface) để tấn công.

### TCP Flooding

Tấn công TCP Flooding, còn được gọi là TCP SYN Flooding, là một loại tấn công từ chối dịch vụ (DoS) khai thác cơ chế bắt tay ba chiều TCP để áp đảo máy chủ và khiến nó không phản hồi các yêu cầu hợp lệ. Kẻ tấn công gửi một loạt các yêu cầu SYN đến một máy chủ mục tiêu nhưng cố tình tránh gửi ACK cuối cùng. Điều này khiến máy chủ phải chờ phản hồi không bao giờ đến, tiêu tốn tài nguyên cho mỗi kết nối nửa mở này.

Để thực hiện tấn công TCP Flooding bằng scapy, nhóm sử dụng đoạn code sau :

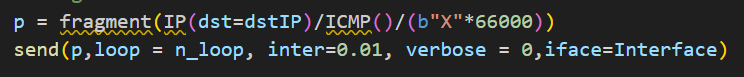


Tương tự như đoạn code được sử dụng để tấn công UDP flooding, tuy nhiên ở gói tin được tạo, ta cần set giao thức TCP với cổng nguồn (sport) ngẫu nhiên với hàm RandShort và flags được set ở chế độ “SYN” (S)

### Ping of Death attack

Tấn công Ping of Death (PoD) là một hình thức tấn công từ chối dịch vụ (DoS) khai thác lỗ hổng trong Giao thức thông báo điều khiển Internet (ICMP) và phân mảnh IP. Bằng cách gửi các gói ICMP quá khổ hoặc không đúng định dạng, kẻ tấn công có thể gây ra sự cố hệ thống, đóng băng hoặc khởi động lại trên thiết bị mục tiêu. Ở đây, nhóm sử dụng trường hợp sử dụng gói tin ICMP có kích thước lớn hơn 65,535 để tấn công

Đoạn code để khai thác như sau :



Ta tạo một gói tin ICMP với payload ngẫu nhiên nhưng với kích thước 66000, sau đó sử dụng hàm fragment để chia nhỏ gói tin này ra trước khi gửi và sử dụng hàm send tương tự 2 cuộc tấn công trên

### DNS amplication attack

Tấn công DNS amplication là một loại tấn công từ chối dịch vụ phân tán (DDoS) khai thác các máy chủ DNS mở có thể truy cập công khai để áp đảo hệ thống đích với lưu lượng phản hồi DNS tràn ngập. Cuộc tấn công này dựa trên hiệu ứng khuếch đại, trong đó kẻ tấn công gửi yêu cầu tra cứu tên DNS đến máy chủ DNS mở với địa chỉ nguồn giả mạo là địa chỉ của mục tiêu. Khi máy chủ DNS phản hồi, nó sẽ gửi phản hồi đến mục tiêu, dẫn đến sự gia tăng đáng kể lưu lượng truy cập hướng vào nạn nhân.

Đoạn code sử dụng cho tấn công này như sau :

A black screen with colorful lights

Description automatically generated with medium confidence

Đầu tiên, ta cần set các địa chỉ DNS server đã biết bằng dns\_destination, 1 tên miền cần phân giải ngẫu nhiên và các loại record cần query, sau đó sử dụng giao thức UDP với DNS và set địa chỉ nguồn là địa chỉ máy nạn nhân để gửi đến tất cả các DNS server. Khi đó, các DNS server sẽ trả về số lượng lớn các respone đến máy nạn nhân.

### File tổng hợp

Nhóm đã gom tất cả các kiểu tấn công trên vào 1 file Dos\_scapy.py. Để sử dụng, cần gọi theo “python Dos\_scapy.py [Kiểu tấn công(UDP/TCP/PingDeath/DNS) [Địa chỉ máy cần tấn công] [Cổng để gửi các gói tin tấn công(Với DNS mặc định là 53)]”

## Tấn công DDos

Trong trường hợp ta có thể tạo ra các botnet đã có file Dos\_scapy.py và các máy bot đều có thể khai thác điểm yếu ở port Telnet (Tấn công Mirai), ta có thể tạo thành tấn công DDos với các máy bot thông qua một server trung tâm C2.

Nhóm sử dụng đoạn code sau để thực thi tấn công DDos

A screen shot of a computer program

Description automatically generated

Bằng thư viện telnetlib và threading, ta lần lượt mở kết nối telnet trên mỗi thread đến toàn bộ máy bot và thực thi lệnh chạy file Dos\_scapy với các option tấn công, ta có thể tạo ra được tấn công DDos đến máy nạn nhân.

## Video Demo

<https://drive.google.com/drive/folders/1shcNS3K3veVDDqvs3jSP-wesRDPhDMFp?usp=sharing>

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

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

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)