DDoS (Distributed Denial of Service) là một loại tấn công mạng nhằm làm gián đoạn hoạt động bình thường của một dịch vụ, máy chủ, hoặc mạng bằng cách làm quá tải tài nguyên của mục tiêu.

Trong bài lab đang thực hiện cụ thể một dạng của DDoS là **TCP SYN Flood**, một loại tấn công tầng giao thức (Protocol Attack) nhắm vào cơ chế bắt tay 3 bước của giao thức TCP.

Sử dụng công cụ hping 3

Cơ chế bắt tay 3 bước :

Client gửi gói SYN yêu cầu kết nối tới server

Server nhận gói và phản hồi với gói SYN-AcK và chừa slot kết nối trong hàng đợi và chờ phản hồi từ client

Client sẽ nhận gói và phản hồi với gói ACK cho server

TCP SYN Flood :

Máy tấn công gửi hàng loạt nhiều gói SYN cho server, ở đây là máy kali gửi với ip giả.

Máy server ( ubuntu ) nhận và gửi SYN-ACK và chừa slot trong hàng đợi kết nối tương ứng với mỗi gói SYN.

Nhưng vì ip giả nên server không nhận được phản hồi, làm cho hàng đợi kết nối đầy và không thể xử lý được nữa.

Snort : Hệ thống giám sát lưu lượng kết nối và phát hiện những hành vi bất thường tại lưu lượng từ đó gửi cảnh báo đến máy.

HYDRA

FTP

FTP (File Transfer Protocol) là giao thức dùng để truyền tải file giữa các máy tính qua mạng.

Brute Force là một kỹ thuật tấn công mật khẩu, trong đó kẻ tấn công thử nhiều tổ hợp username/password cho đến khi tìm ra thông tin đăng nhập hợp lệ.

FTP Brute Force là quá trình sử dụng công cụ (như Hydra) để thử hàng loạt tổ hợp username/password nhằm đăng nhập trái phép vào một FTP server.

Cách hoạt động :

* Kẻ tấn công (ở đây là Máy Kali) sử dụng Hydra để gửi liên tục các yêu cầu đăng nhập FTP đến server (Máy Ubuntu) trên cổng 21.
* Hydra thử từng tổ hợp username/password từ một danh sách (wordlist) cho đến khi tìm ra thông tin đăng nhập hợp lệ hoặc hết danh sách.
* Mỗi lần thử đăng nhập, Hydra gửi các lệnh FTP,
* Nếu thông tin đăng nhập đúng, Hydra sẽ thông báo; nếu không, nó tiếp tục thử với mật khẩu tiếp theo trong danh sách.

SQL

SQL Injection là một kỹ thuật tấn công vào ứng dụng web, trong đó kẻ tấn công chèn các câu lệnh SQL độc hại vào dữ liệu đầu vào (như form, URL, hoặc tham số) để thao túng cơ sở dữ liệu của ứng dụng.

**Cách hoạt động của sqlmap**:

* sqlmap gửi các yêu cầu HTTP đến URL mục tiêu, chèn các payload SQL Injection (như ' OR '1'='1, ' AND '1'='1, ...) để kiểm tra xem ứng dụng có bị lỗi SQL Injection không.
* Nếu phát hiện lỗ hổng, sqlmap sẽ khai thác sâu hơn để:
  + Xác định loại cơ sở dữ liệu (ví dụ: MySQL).
  + Lấy thông tin như tên database, bảng, cột, và dữ liệu.

sqlmap -u "http://192.168.1.135/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=u9kn07k3ildkqvouc90siclbd3; security=low" –batch

trong đó :

-u "http://192.168.1.135/vulnerabilities/sqli/?id=1&Submit=Submit": URL của trang SQL Injection trên DVWA.

--cookie="PHPSESSID=...; security=low": Cookie để xác thực phiên làm việc với DVWA.

--batch: Tự động chọn các tùy chọn mặc định, không hỏi người dùng.