1. **Dos attack với syn flood**
2. **DoS là gì?**

DoS viết tắt của cụm từ Denial of Service, là một kiểu tấn công từ chối dịch vụ khi đó máy tính của bạn sẽ bị tấn công bởi lưu lượng truy cập từ hệ thống của hacker. DoS là một cuộc tấn công trực tuyến thường nhắm vào một trang web hoặc máy chủ điển hình. Bằng cách làm quá tải tài nguyên hệ thống, tốc độ hệ thống của máy tính sẽ bị chậm lại đáng kể.

Cuộc tấn công này có thể khiến máy tính của bạn ngừng hoạt động hoặc tắt đột ngột. Khi hiện tượng này xảy ra sẽ ảnh hưởng nghiêm trọng đến hệ thống của máy tính và buộc máy tính phải tắt nguồn.

1. **Cuộc tấn công SYN Flood là gì?**

SYN flood (half-open attack) là một kiểu tấn công từ chối dịch vụ (Dos). Tấn công này với mục đích làm cho Server không có lưu lượng để truy cập hợp pháp. Bằng cách tiêu thụ tất cả tài nguyên server đang có sẵn. Người tấn công có thể áp đảo tất cả các cổng trên [Server](https://vnso.vn/thue-may-chu-rieng/). Làm cho thiết bị Client đáp ứng lưu lượng hợp pháp một cách chậm chạp.

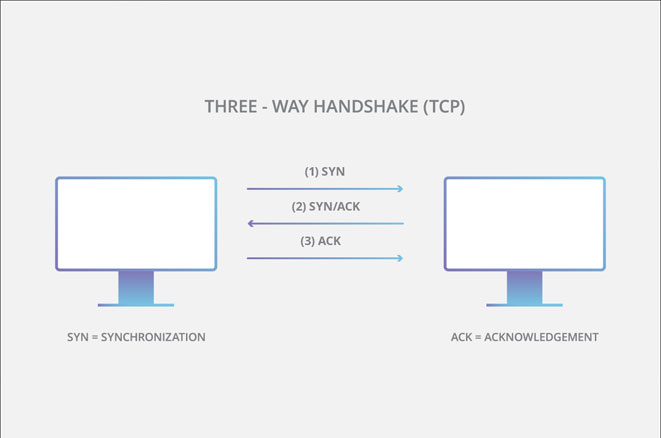
1. **Làm thế nào tấn công SYN Flood ?**

Một cuộc tấn công DDoS SYN-flood tận dụng quy trình bắt tay ba chiều TCP. Trong điều kiện bình thường, kết nối TCP được thể hiện quy trình 3 bước riêng biệt để tạo được sự kết nối như sau:

**Bước 1**: Đầu tiên, máy tấn công gửi 1 packet tin SYN đến Server để yêu cầu kết nối.

**Bước 2:** Sau khi tiếp nhận packet SYN, Server phản hồi lại máy khách bằng một packet SYN/ACK, để xác nhận thông tin từ Client.

**Bước 3:** Cuối cùng, Client nhận được packet tin SYN/ACK thì sẽ trả lời server bằng packet tin ACK báo với server biết rằng nó đã nhận được packet tin SYN/ACK, kết nối đã được thiết lập và sẵn sàng trao đổi dữ liệu.



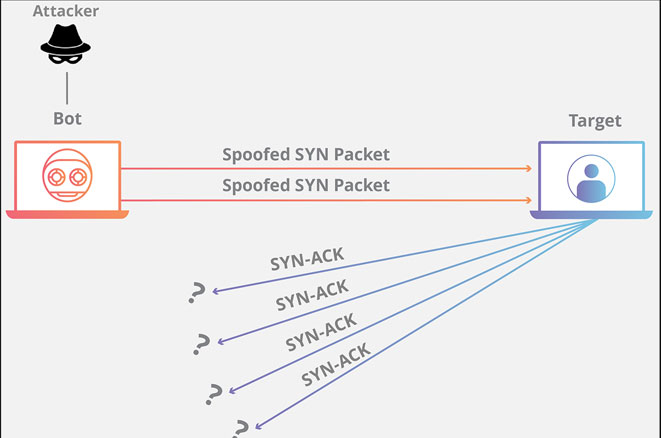
Để tạo từ chối dịch vụ (DOS), thực tế kẻ tấn công sẽ khai thác sau khi nhận được packet SYN ban đầu từ Client. Server sẽ phản hồi lại 1 hoặc nhiều packet SYN/ACK và chờ đến bước cuối cùng trong quá trình Handshake. Ở đây, cách thức thực hiện của nó như sau:

**Bước 1:** Kẻ tấn công sẽ gửi một khối lượng lớn các packet tin SYN đến Server. Được nhắm là mục tiêu và thường là các địa chỉ IP giả mạo.

**Bước 2:** Sau đó Server sẽ phản hồi lại từng yêu cầu kết nối. Để lại 1 cổng mở sẵn sàng tiếp nhận và phản hồi.

**Bước 3:** Trong khi Server chờ packet ACK ở bước cuối cùng từ Client, packet mà không bao giờ đến. Kẻ tấn công tiếp tục gửi thêm các packet SYN. Sự xuất hiện các packet SYN mới khiến [máy chủ](https://vnso.vn/thue-may-chu-rieng/) tạm thời duy trì kết nối cổng mở mới trong một thời gian nhất định. Một khi các cổng có sẵn được sử dụng thì Server không thể hoạt động như bình thường.

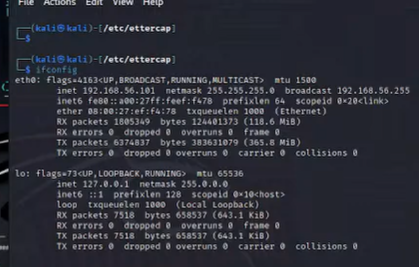
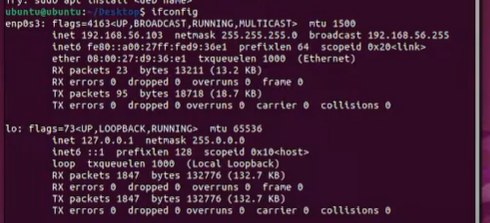
Trong kết nối mạng, khi Server bên này kết nối mở nhưng máy bên kia không kết nối thì được coi là half-open. Trong kiểu tấn công DDos, sau khi server gửi gói tin SYN/ACK nó sẽ phải đợi cho đến khi client trả lời. Đến khi các port trở lại bình thường. Kết quả của kiểu tấn công này được coi là cuộc tấn công half-open.



DEMO

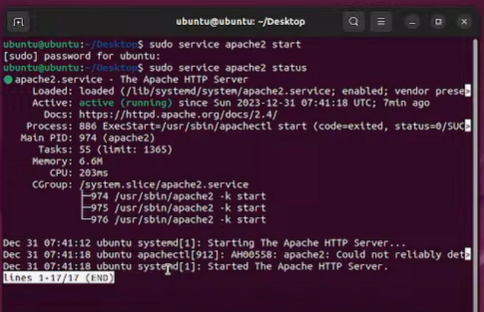
Link demo đã làm sẵn: <https://www.youtube.com/watch?v=3NZDCaBzqQg>

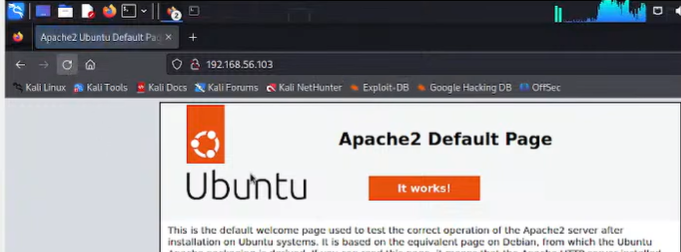
B1: Check IP attacker and victim

* Dùng lệnh ifconfig
* IP victim Ubuntu 192.168.56.103 và ip attacker Kali-linux 192.168.56.101
* 
* 

B2: Run apache server trên victim computer

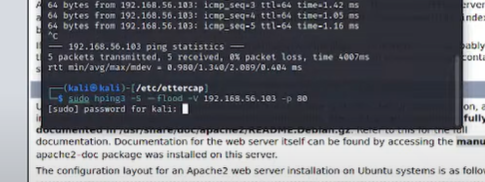
* Dùng lệnh sudo service apache2 start để bật apache server, sudo service apache2 status để kiểm tra trạng thái của apache server.



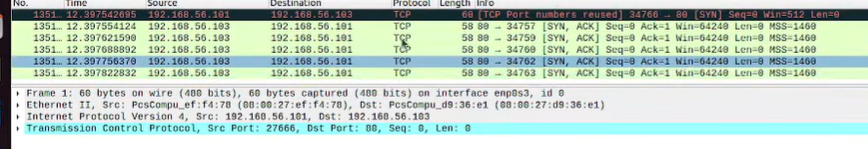


B3: Syn flood attack với hping 3 trên attacker computer

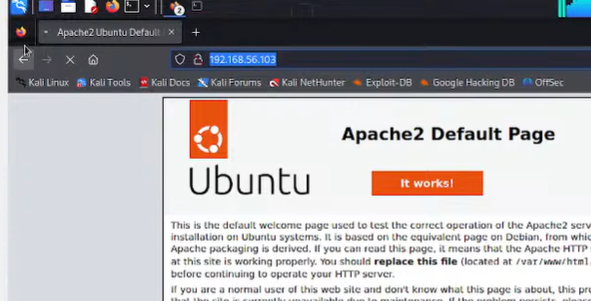
* Cú pháp : sudo hping3 –s –flood –V 192.5168.67.103 –p 80



* Bắt gói tin với wireshark thấy rằng có rất nhiều ip syn từ máy attacker đên victim và ip ask từ máy victim đến attacker



B4: Nạn nhân đã bị tấn công, lúc này truy cập vào apache server vô cùng chậm.



## ARP Poisoning Attack với ARP spoofing

## Tấn công ARP Poisoning là gì?

Address Resolution Protocol (ARP) là một quy trình kết nối liên kết địa chỉ IP với địa chỉ vật lý tĩnh của Media Access Control (MAC) qua mạng LAN. Vì địa chỉ của IP và MAC có các thành phần khác nhau nên chúng không tương thích. ARP dung hòa sự khác biệt này để đảm bảo rằng cả hai phần tử đều đồng bộ. Nếu không, chúng sẽ không nhận ra nhau.

Tấn công ARP Poisoning là một quá trình theo đó kẻ xâm nhập gửi nội dung độc hại qua mạng cục bộ (LAN) để chuyển hướng kết nối của một địa chỉ IP hợp pháp đến địa chỉ MAC của chúng. Trong quá trình này, kẻ tấn công thay thế địa chỉ MAC ban đầu sẽ kết nối với địa chỉ IP, cho phép chúng truy cập những tin nhắn mà mọi người gửi đến địa chỉ MAC xác thực.

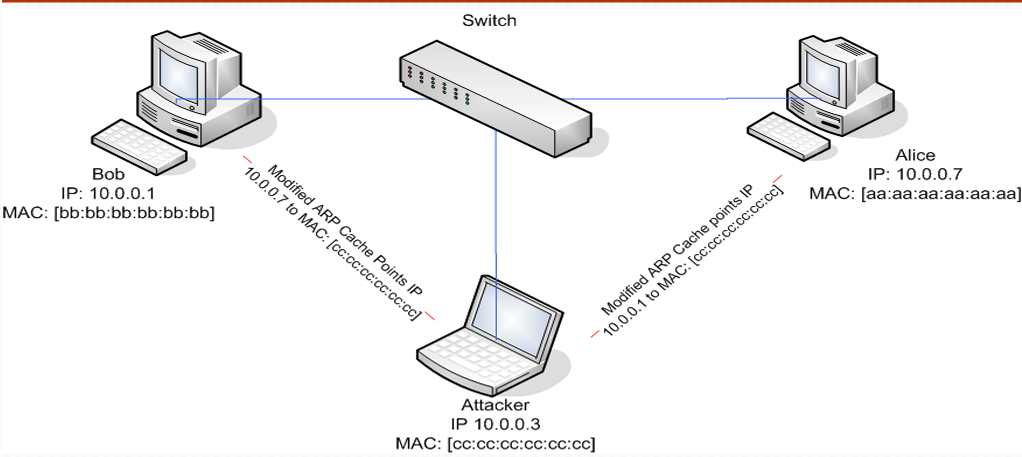
## Tấn công ARP Poisoning hoạt động như thế nào?

Một số mạng có thể hoạt động trên mạng cục bộ (LAN) cùng một lúc. Mỗi mạng đang hoạt động có một địa chỉ IP cụ thể dùng làm phương tiện nhận dạng và phân biệt nó với các mạng khác. Khi dữ liệu từ các mạng khác nhau đến cổng, ARP sẽ sắp xếp chúng cho phù hợp, vì vậy mỗi mạng sẽ đi thẳng đến đích đã định.

Kẻ tấn công tạo và gửi một thông báo ARP sai đến hệ thống được định hình. Chúng thêm địa chỉ MAC của mình và địa chỉ IP của mục tiêu trong tin nhắn. Khi nhận và xử lý thông báo ARP sai, hệ thống sẽ đồng bộ địa chỉ MAC của kẻ tấn công với địa chỉ IP.

Khi mạng LAN kết nối địa chỉ IP với địa chỉ MAC của kẻ xâm nhập, kẻ xâm nhập bắt đầu nhận tất cả các thông báo dành cho địa chỉ MAC hợp pháp. Chúng có thể nghe trộm thông tin liên lạc để truy xuất dữ liệu nhạy cảm khi trao đổi, sửa đổi thông tin liên lạc bằng cách chèn nội dung độc hại hoặc thậm chí xóa dữ liệu trong khi truyền để người nhận không nhận được.

1. **Tấn công ARP spoofing**

**ARP spoofing là gì?** 

ARP spoofing là gì? ARP spoofing còn được gọi là ARP poisoning, là một cuộc tấn công Man in the Middle (MitM) cho phép những kẻ tấn công chặn giao tiếp giữa các thiết bị mạng. Cuộc tấn công sẽ diễn ra như sau:

1. Kẻ tấn công phải có quyền truy cập vào mạng. Chúng quét mạng để xác định địa chỉ IP của ít nhất hai thiết bị⁠ — giả sử đây là một máy trạm và một bộ định tuyến.

2. Kẻ tấn công sử dụng một công cụ giả mạo, chẳng hạn như Arpspoof hoặc Driftnet, để gửi phản hồi ARP giả mạo.

3. Các phản hồi giả mạo thông báo rằng địa chỉ MAC chính xác cho cả hai địa chỉ IP, thuộc bộ định tuyến và máy trạm (workstation), là địa chỉ MAC của kẻ tấn công. Điều này đánh lừa cả bộ định tuyến và máy trạm kết nối với máy của kẻ tấn công, thay vì kết nối với nhau.

4. Hai thiết bị cập nhật các mục bộ nhớ cache ARP của chúng và từ thời điểm đó trở đi, giao tiếp với kẻ tấn công thay vì trực tiếp với nhau.

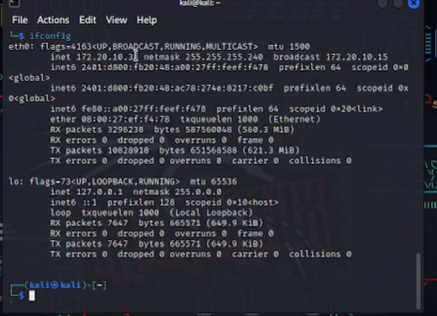
5. Kẻ tấn công hiện đang bí mật đứng giữa mọi liên lạc.

DEMO

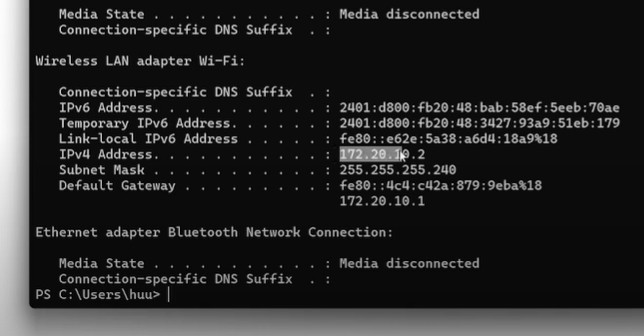
Link demo đã làm: <https://www.youtube.com/watch?v=Go1_cmqTVRM>

B1: Check IP attacker ,victim và router

Attacker: Kali-linux , IP: 172.20.10.3



Victim: Window , IP: 172.20.10.2



Router: IP: 172.20.10.1

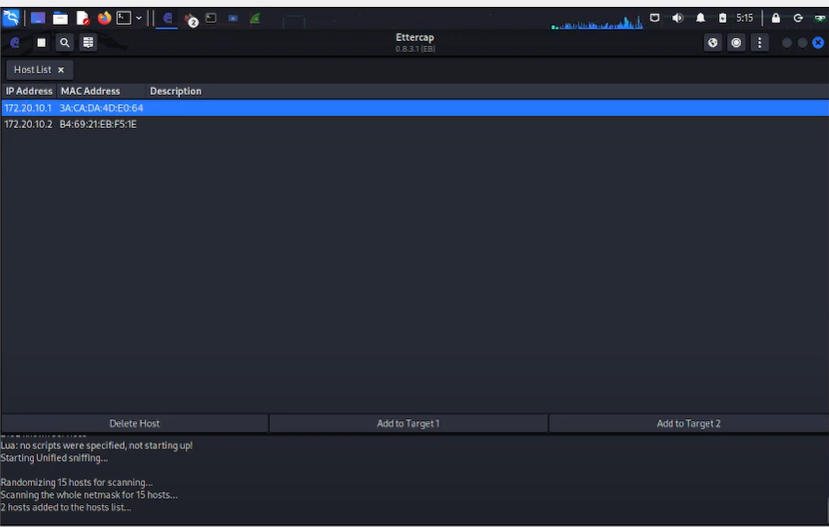


B2: Tiến hành tấn công với Ettercap

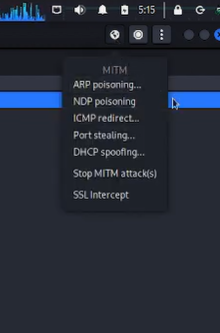
* Thực hiện chọn ip cho target:

IP: 172.20.10.2 -> target 1: Victim

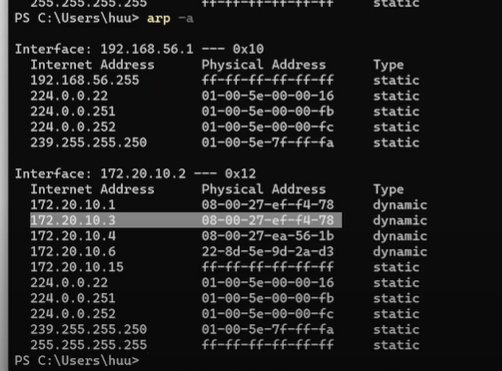
IP: 172.20.10.1 -> target 2: router



* Tiến hành đầu độc bảng ARP của máy nạn nhân và router

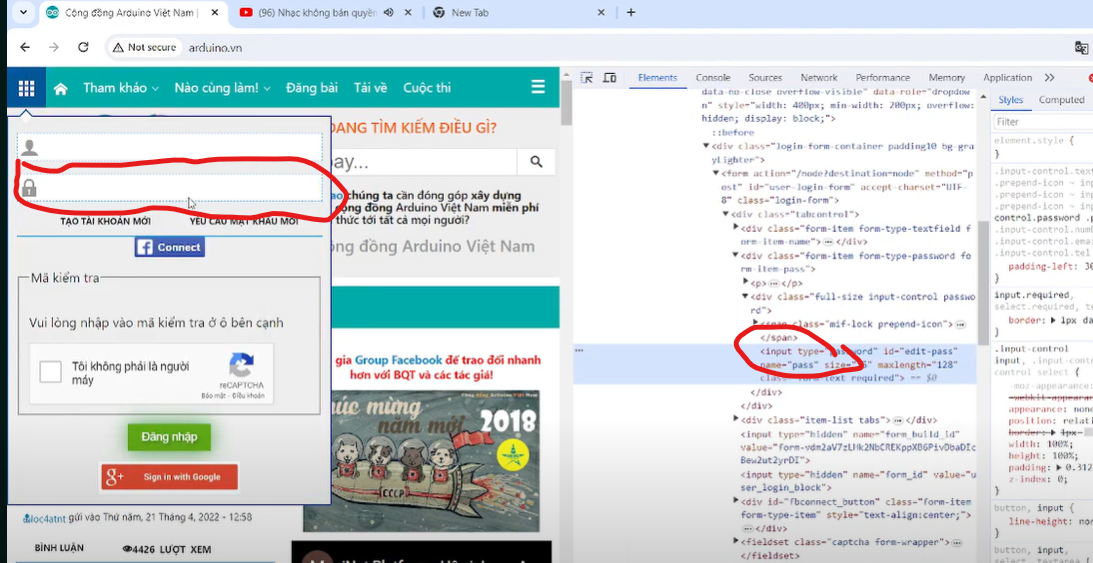


* Router gw ip 172.20.10.1, Mac: 08-00-27-ef-f4-78 -> Trùng với Mac của attacker -> Thành công



B3. Lấy trộm thông tin đăng nhập của victim

- Vào trang http://arduino.vn/ -> Tiến hành đăng nhậpp -> Ví dụ lấy thông password của người dùng-> Ta check thẻ html thấy form đăng nhập input password có name là "pass"



-> Mở wireshark để bắt gói tin-> filter gói tin chứa pass với lệnh frame contains "pass" -> Như vậy thấy được pass vừa nhap : "abc" -> Thành công.

