|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| HỌC PHẦN  **ĐÁNH GIÁ VÀ KIỂM ĐỊNH**  **AN TOÀN HỆ THỐNG THÔNG TIN** |
| BÀI THỰC HÀNH  **THU THẬP THÔNG TIN VÀ XÁC ĐỊNH**  **CỔNG, DỊCH VỤ MẠNG** |
| **Sinh viên thực hiện: HOÀNG NGUYÊN THÁI - AT14C** |
| **Hà Nội, 2021** |

MỤC LỤC

[MỤC LỤC 2](#_Toc75971341)

[*Phần 1. Thu thập thông tin* 2](#_Toc75971342)

[Giới thiệu 2](#_Toc75971343)

[Chuẩn bị 3](#_Toc75971344)

[Các bước thực hiện 3](#_Toc75971345)

[*Phần 2. Sử dụng Nmap để dò quét cổng, dịch vụ mạng* 8](#_Toc75971347)

[Giới thiệu 8](#_Toc75971348)

[Chuẩn bị 9](#_Toc75971349)

[Các bước thực hiện 10](#_Toc75971350)

# *Thu thập thông tin*

## Giới thiệu

Thu thập thông tin là công việc đầu tiên cần thực hiện khi tiến hành một dự án đánh giá. Theo EC-Council, thu thập thông tin có thể chiếm tới 80% khả năng thành công của dự án bởi lẽ đây là tiền đề cho tất cả cac bước đánh giá tiếp theo.

Trên Internet, có rất nhiều trang web cho phép người dùng tìm kiếm và trích xuất thông tin. Một số trang web điển hình là: Google.com, Whois.com, Alexa.com. Bài thực hành này sẽ sử dụng các trang Web và công cụ để thu thập thông tin.

## Chuẩn bị

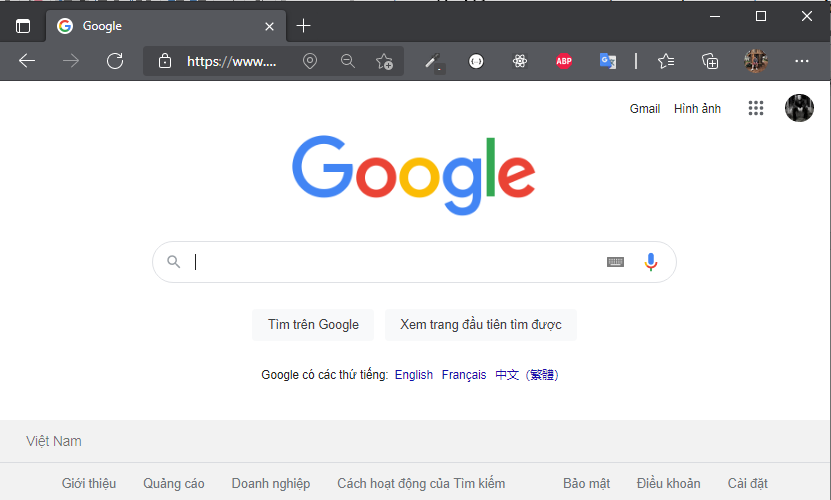


* 01 máy tính có thể kết nối mạng Internet, trong đó:
* Cài đặt HĐH Windows hoặc Linux (Ubuntu)
* Cài đặt trình duyệt Web: Firefox, hoặc Google Chorome
* Cài đặt công cụ Maltego

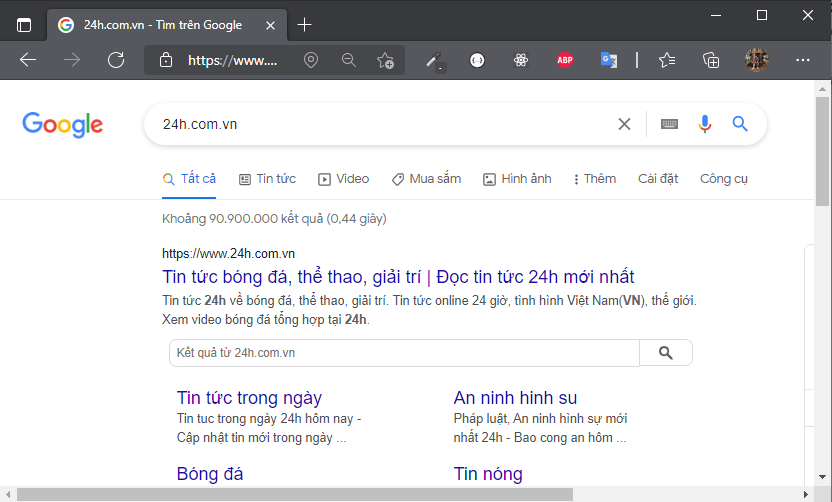
## Các bước thực hiện

### Sử dụng trình duyệt Web để thu thập thông tin

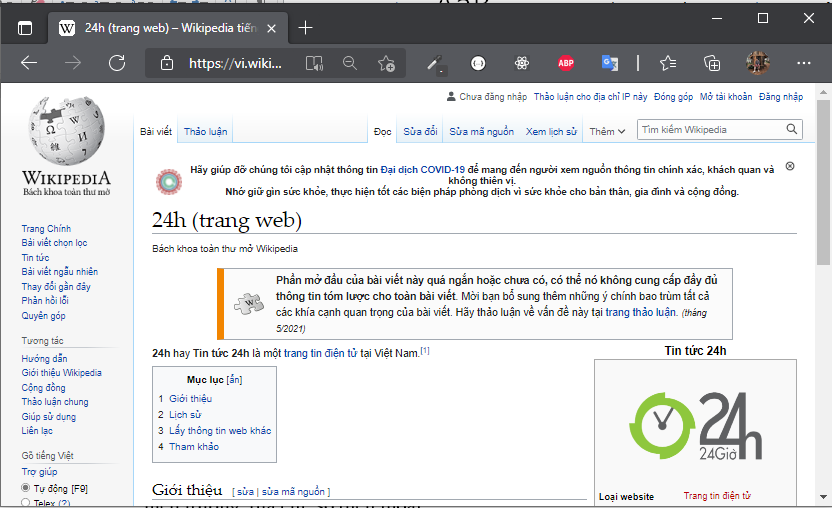
* Sử dụng trình duyệt web truy cập vào địa chỉ [www.google.com](http://www.google.com)



* Nhập từ khóa cần thu thập thông tin (ví dụ: “24h.com.vn”) vào ô tìm kiếm của google và nhấn Enter.
* Theo dõi các kết quả hiển thị tìm kiếm



* Click vào 1 liên kết từ kết quả tìm kiếm của Google, ví dụ liên kết Wikipedia



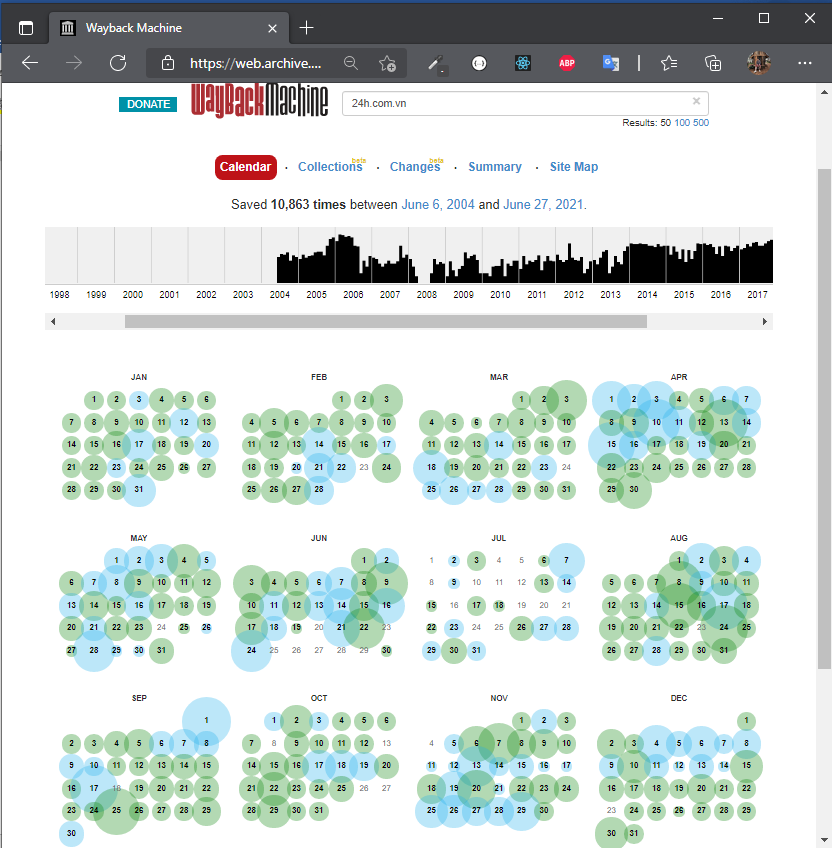
* Thu thập các thông tin liên quan từ Wikipedia về: ngày thành lập, loại hình, hiệu trưởng, địa chỉ, số điện thoại,...

Trang 24h.com.vn được thành lập chính thức vào ngày 25 tháng 06 năm 2004. Từ giai đoạn 2005 đến năm 2012, trang thông tin điện tử này có trụ sở ở tòa nhà HITTC của Sở thông tin và truyền thông Hà Nội 185 Giảng Võ, Đống Đa, Hà Nội. Sau đó, chuyển về tòa nhà Geleximco 36 Hoàng Cầu, Đống Đa, Hà Nội.

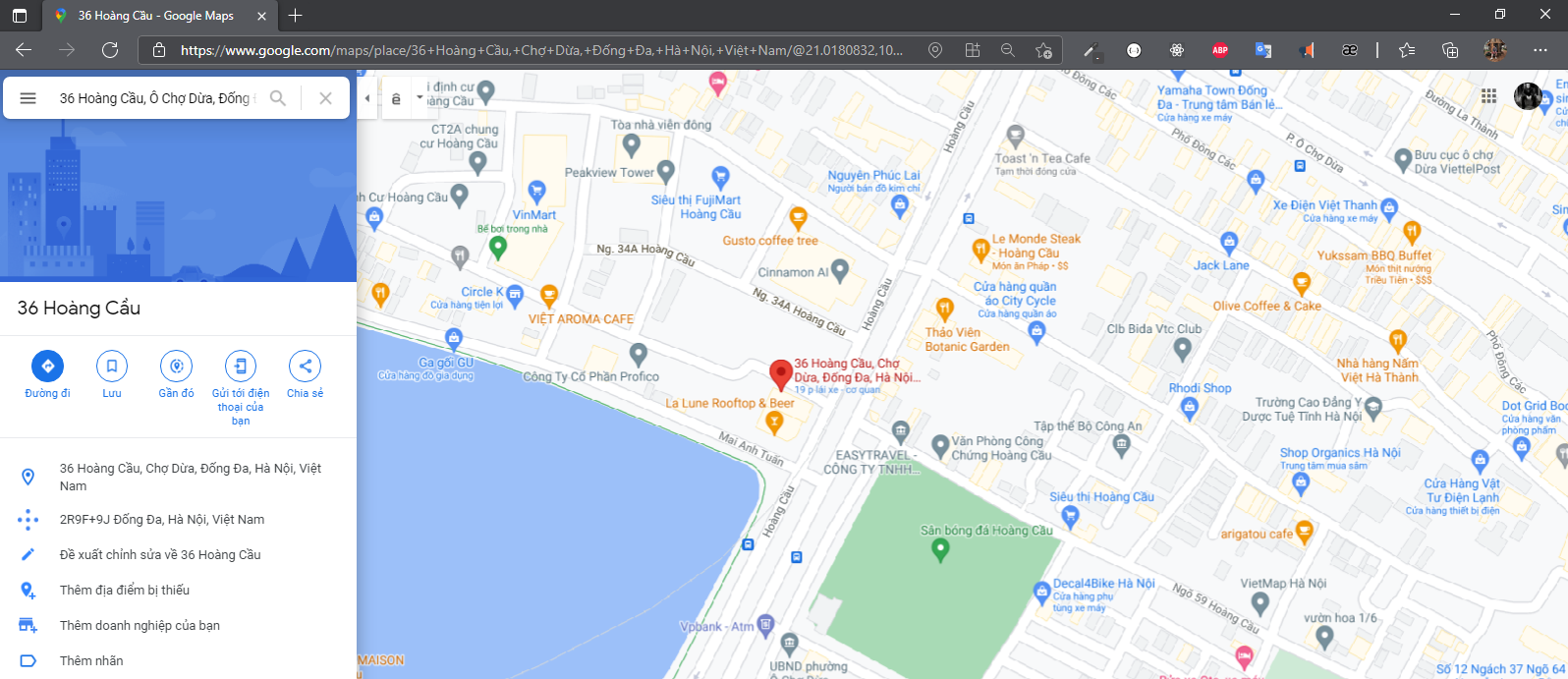
* Truy cập vào địa chỉ: whois.net.vn và thực hiện tìm kiếm thông tin về 24h.com.vn



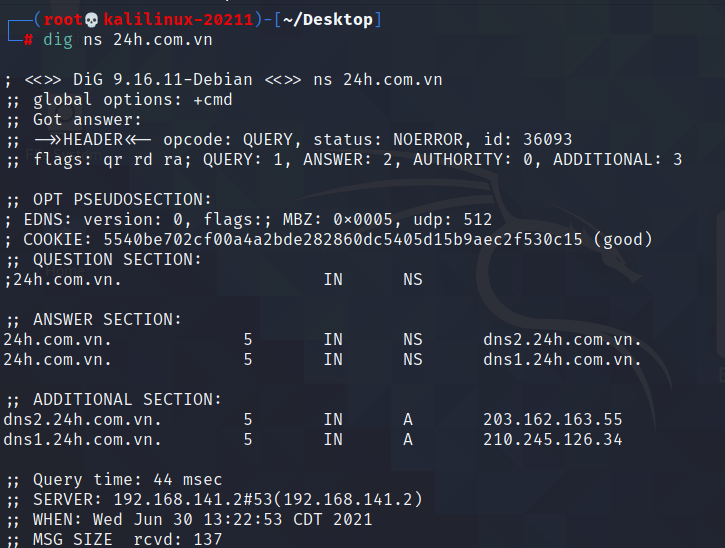
* Thu thập các thông tin liên quan đến địa điểm của 24h.com.vn
* Cơ quan chủ quản: Công ty Cổ phần Quảng cáo Trực tuyến 24h
* Giấy phép số 332/GP – TT ĐT này cấp 22/01/2018 SỞ THÔNG TIN VÀ TRUYỀN THÔNG HÀ NỘI
* Chịu trách nhiệm xuất bản: Phan Minh Tâm
* Hotline: 0965082424
* Truy cập vào địa chỉ: archive.org và lựa chọn một mốc thời điểm của năm 2018



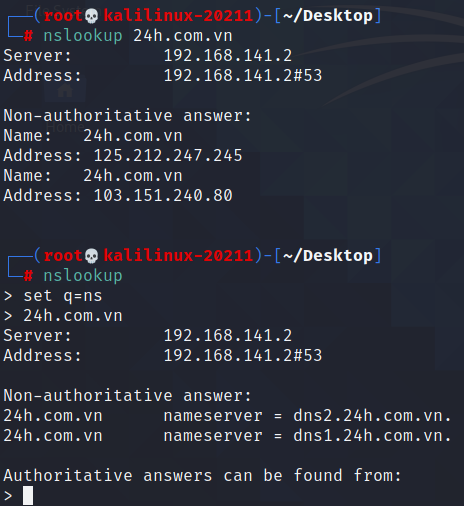
* Truy cập vào địa chỉ: maps.google.com và tìm kiếm vị trí của Học viện Kỹ thuật Mật mã.



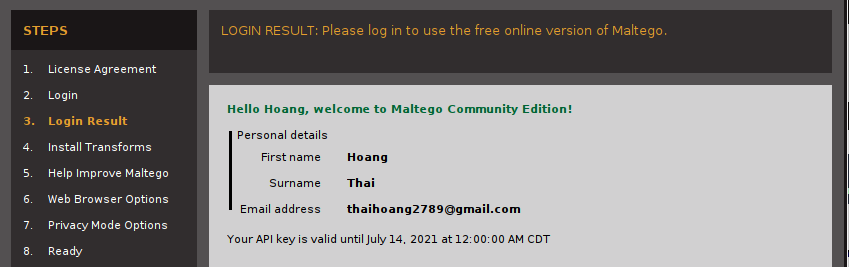
* Sử dụng công cụ để thu thập thông tin
* Khởi chạy máy ảo Kali Linux và mở công cụ Terminal
* Sử dụng công cụ dig để tìm kiếm các thông tin liên quan đến DNS của 24h.com.vn



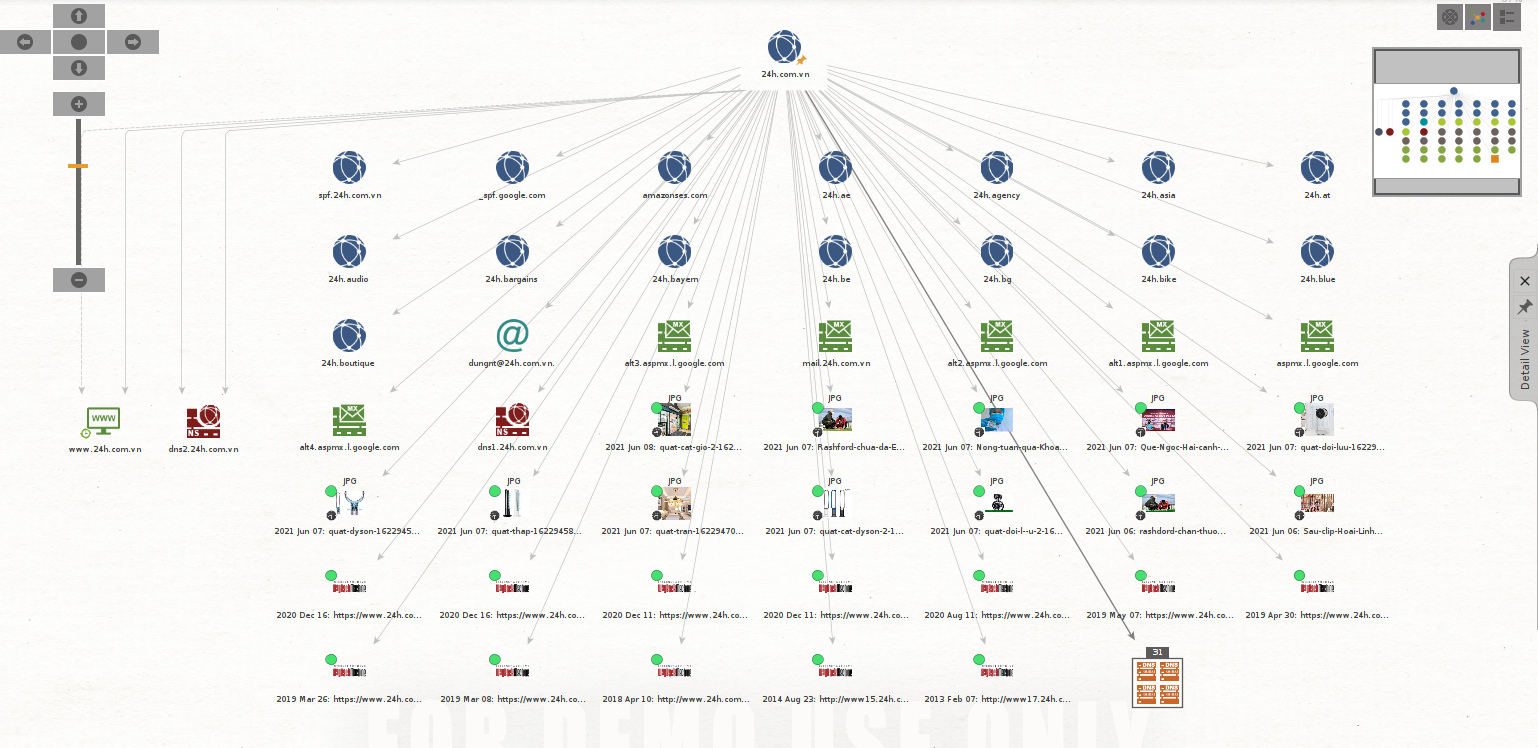
* Sử dụng công cụ nslookup để tìm kiếm thông tin về địa chỉ IP, tên miền của 24h.com.vn



* Khởi chạy công cụ Maltego từ Kali Linux
* Đăng nhập (hoặc đăng ký nếu chưa có tài khoản) để truy nhập vào Maltego.



* Từ công cụ Maltego lựa chọn New Graph để tạo 1 Graph mới.
* Từ thanh Pallette lựa chọn 1 Domain hoặc URL, Website,...đưa ra ngoài Graph.
* Nhập tên Domain (hoặc tên Website, địa chỉ URL) vào phần Domain name (hoặc Website name, URL...), ví dụ: 24.com.vn
* Click phải chuột vào Domain (hoặc Website, URL...) lựa chọn RunTransform và thu thập các thông tin về:



# *Sử dụng Nmap để dò quét cổng, dịch vụ mạng*

## Giới thiệu

Nmap (Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap có mã nguồn mở, miễn phí, dùng để quét cổng và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

Nmap sử dụng các giao thức tầng bao gồm TCP (giao thức điều khiển truyền), UDP (giao thức truy vấn người dùng), SCTP (giao thức truyền dẫn điều khiển luồng) và ICMP (giao thức tin nhắn điều khiển Internet, được sử dụng để gửi thông báo lỗi). Các giao thức khác nhau phục vụ cho các các mục đích và các cổng hệ thống khác nhau.

Nmap có thể được sử dụng được trên rất nhiều hệ điều hành khác nhau. Nó chạy được trên Windows, macOS, các bản phân phối của Linux bao gồm Red Hat, Mandrake, SUSE và Fedora. Nó cũng hoạt động tốt trên các hệ điều hành khác bao gồm BSD, Solaris, AIX và AmigaOS.

Ngoài chức năng cơ bản của Nmap là quét cổng, nó cũng cung cấp cho người dùng một loạt các tính năng liên quan bao gồm:

+ Lập bản đồ mạng (Network mapping)

+ Phát hiện hệ điều hành(OS detection)

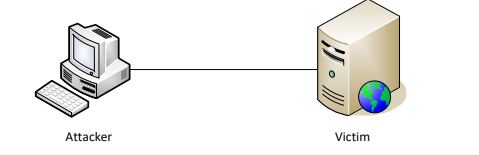
+ Dò tìm dịch vụ (Service discovery)

+ Kiểm tra bảo mật (Security auditing)

Cú pháp lệnh nmap:

**nmap [Scan Type(s)] [Options] {target specification}**

## Chuẩn bị



* 01 Máy tính đóng vai trò là máy tấn công (Attacker)
* 01 Máy tính đóng vai trò là Victim
* Công cụ Nmap

Trong đó:

Máy Victim:

+ Cài đặt HĐH Windows 7 hoặc Windows Server 2008.

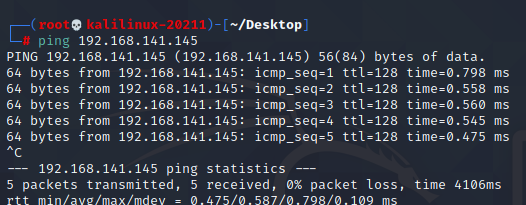
+ Cài đặt dịch vụ WebServer Apache hoặc IIS.

Máy Attacker:

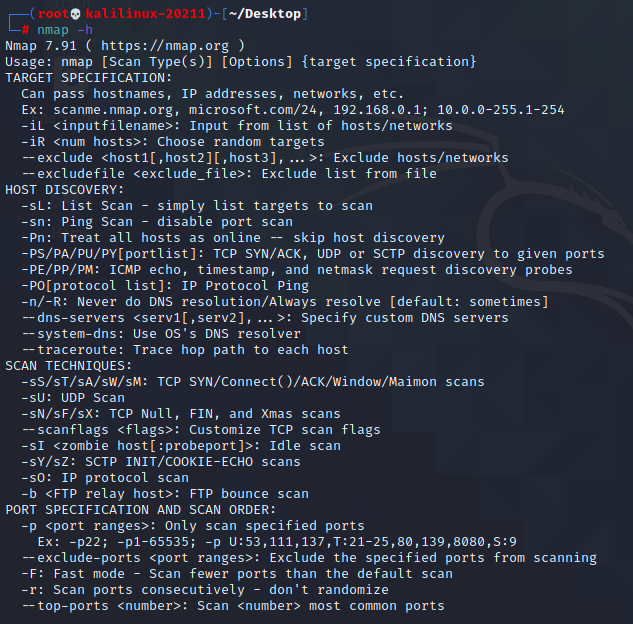
+ Sử dụng máy ảo Kali Linux

## Các bước thực hiện

* Từ máy Attacker ping tới địa chỉ Ip của Victim để kiểm tra tình trạng kết nối



* Mở máy Kali Linux, khởi chạy Terminal
* Nhập lệnh: nmap –h để hiển thị lệnh hỗ trợ



* Thực hiện dò quét cổng, dịch vụ và hệ điều hành với các kiểu quét: SYN Scan, TCP Connect Scan, ACK Scan, XMAS Scan,…

