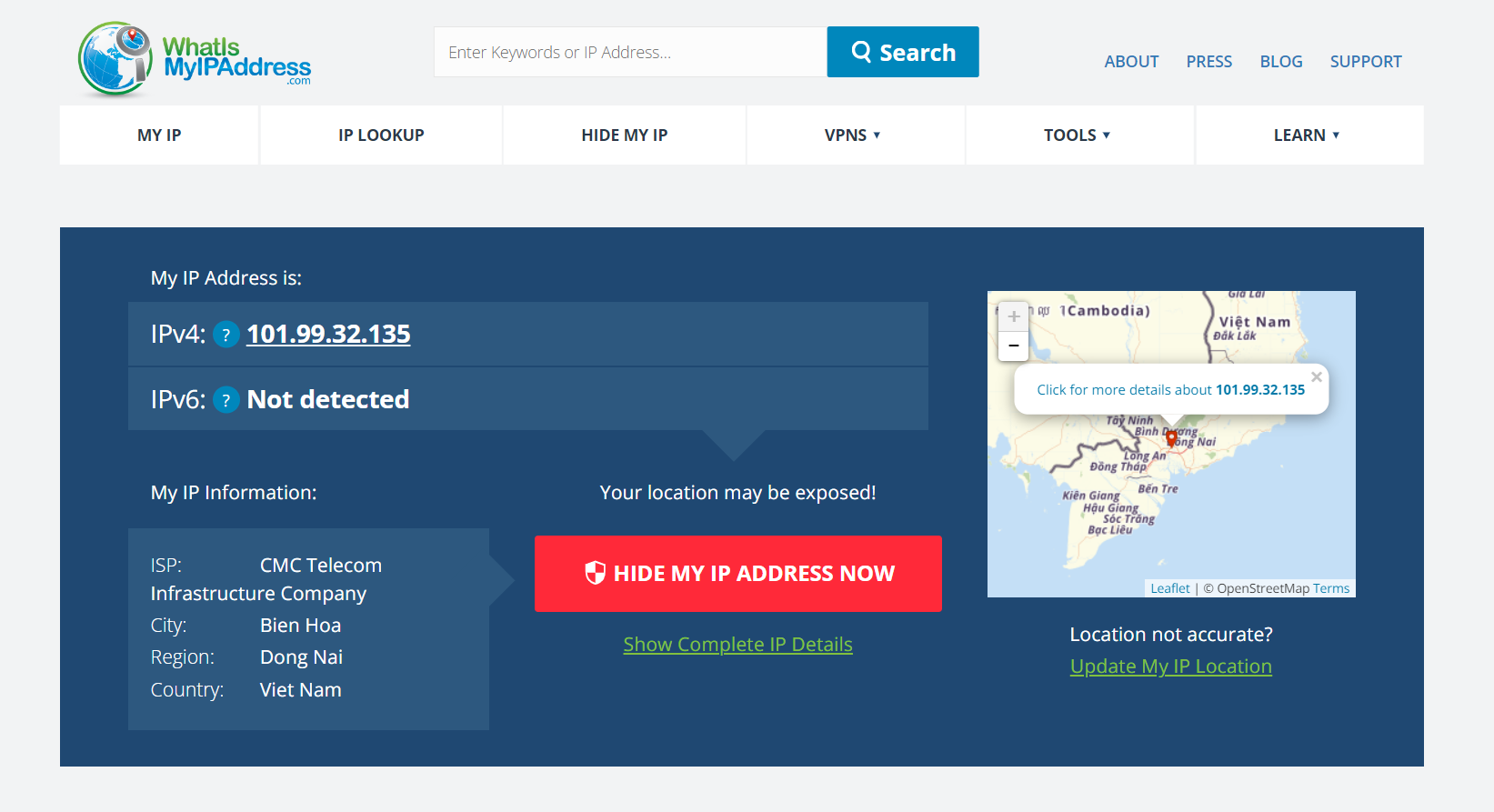
Report\_Week\_02

Họ và tên: Trần Hân Nhi

MSSV: 2011770131 Lớp: 20DATA1

**Ex\_01:**

****

Trước khi sử dụng công cụ giả mạo, thông tin địa chỉ IP của máy hiển thị như sau:

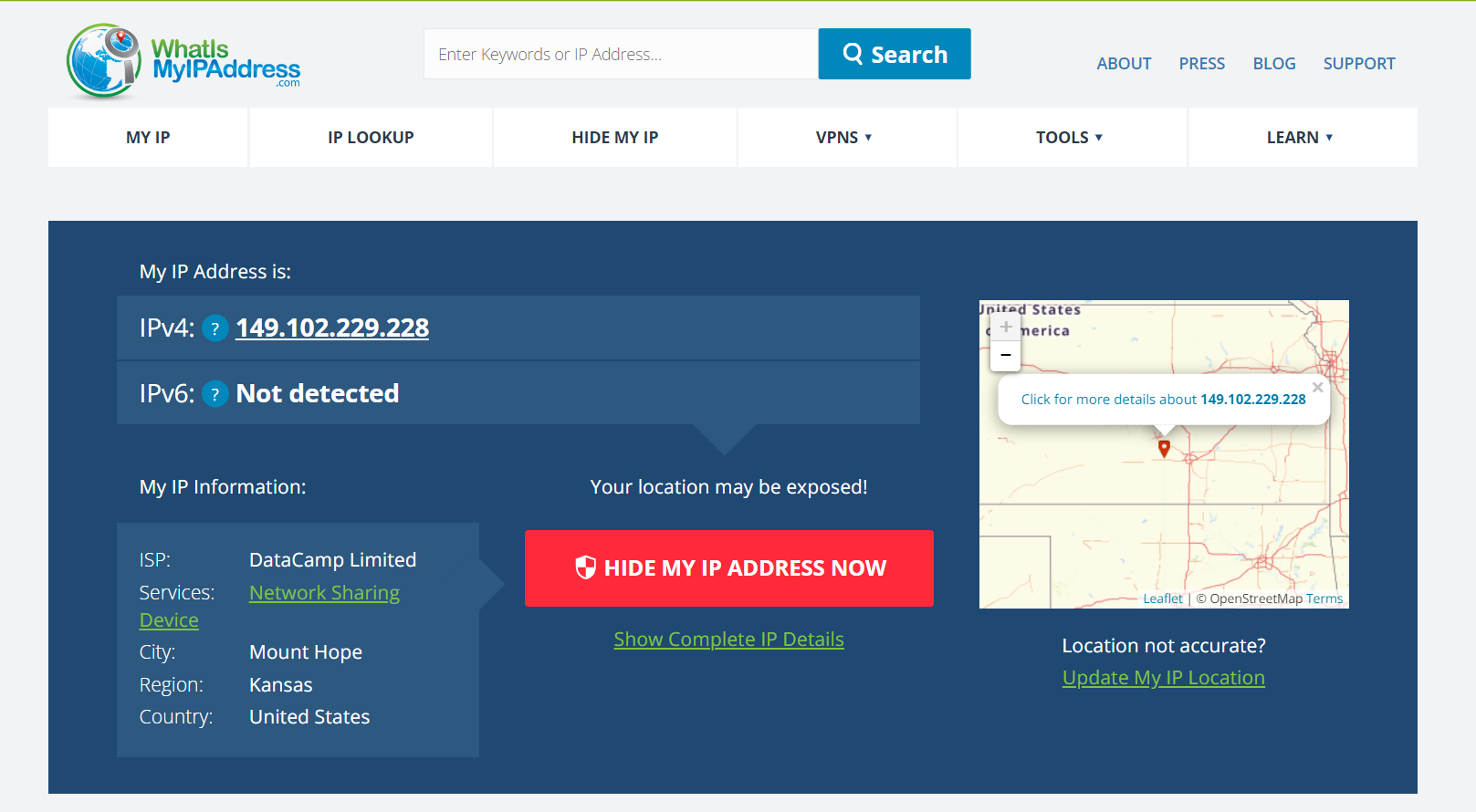
Địa chỉ IPv4: 101.99.32.135

Nhà cung cấp dịch vụ (ISP): CMC Telecom Infrastructure Company

Thành phố: Biên Hoà

Tỉnh: Đồng Nai

Quốc gia: Việt Nam



Sau khi sử dụng công cụ, các thông số về nhà cung cấp dịch vụ, thành phố, dịch vụ, tỉnh, thành phố và quốc gia đều thay đổi:

Địa chỉ IPv4: 149.102.229.228

Nhà cung cấp dịch vụ (ISP): DataCamp Limited

Dịch vụ: Network Sharing Device

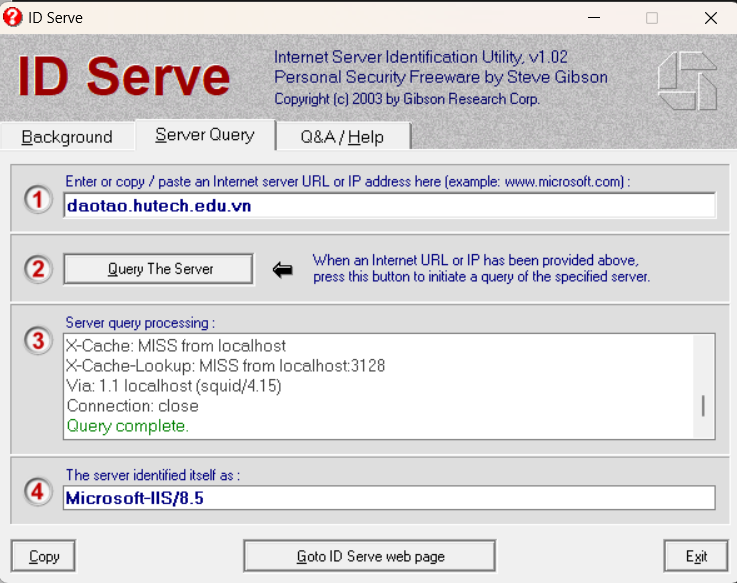
Thành phố: Mount Hope

Tỉnh: Kansas

Quốc gia: US

**Ex\_02:**

* ***Công cụ ID Serve***



* **Những thông tin lấy được khi sử dụng công cụ ID Serve**

Domain: daotao.hutech.edu.vn

Địa chỉ IP: 103.63.115.6

Port: 80

The server returned the following response headers:

HTTP/1.1 200 OK

Cache-Control: private, max-age=10

Content-Type: text/html; charset=utf-8

Expires: Thu, 14 Sep 2023 07:02:04 GMT

Last-Modified: Thu, 14 Sep 2023 07:01:54 GMT

Server: Microsoft-IIS/8.5

X-AspNet-Version: 2.0.50727

Set-Cookie: ASP.NET\_SessionId=qk1r0sb1xp0ulr55ezt0oq45; path=/; HttpOnly

X-Powered-By: ASP.NET

Date: Thu, 14 Sep 2023 07:01:54 GMT

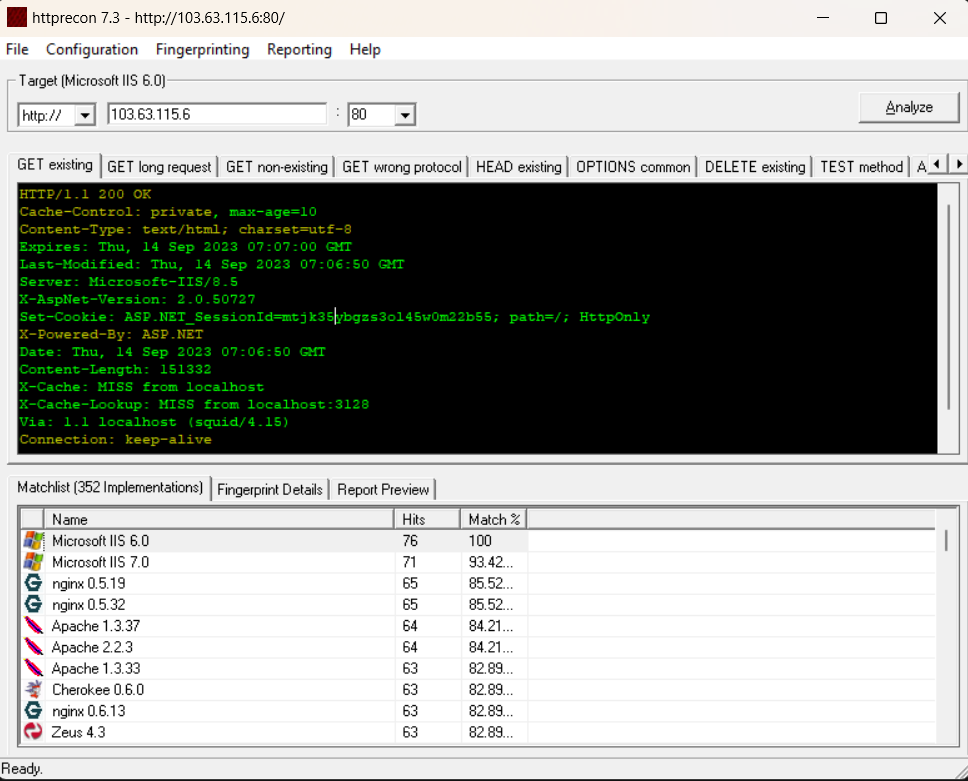
Content-Length: 151332

X-Cache: MISS from localhost

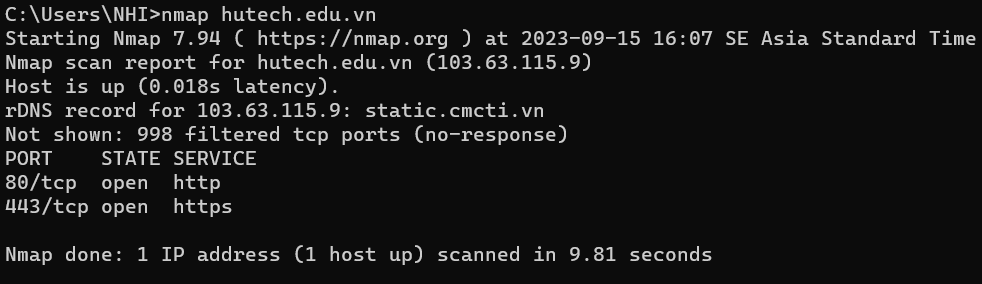
X-Cache-Lookup: MISS from localhost:3128

Via: 1.1 localhost (squid/4.15)

* ***Công cụ Httprecon***

****

**Ex\_03:**

****

* Đối với trang web có địa chỉ IP 103.63.115.6 có 2 port đang mở là:

Port 80 – Dùng cho việc truy cập các trang web và dịch vụ web.

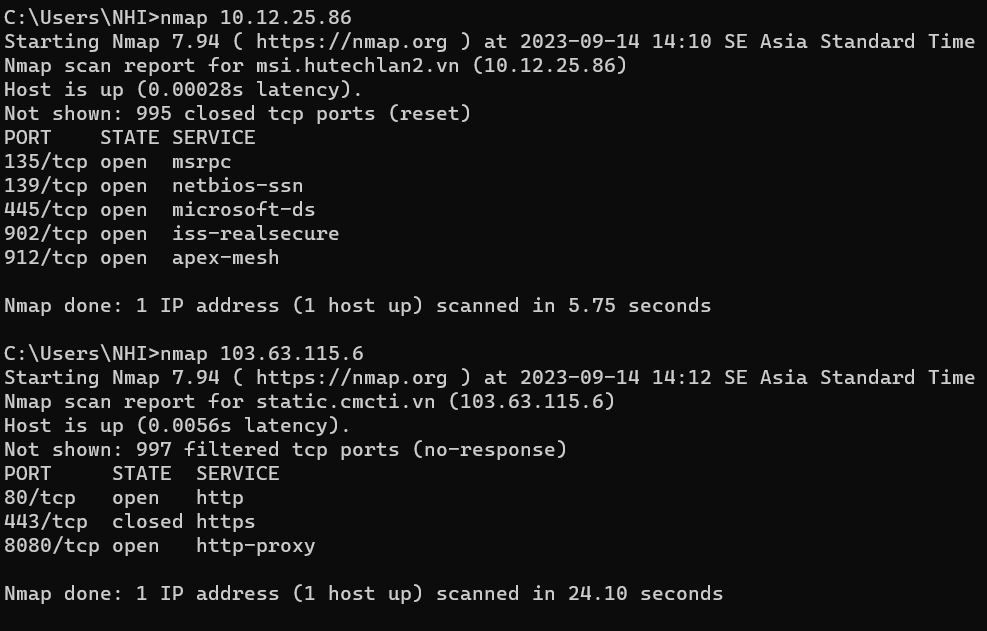
Giao thức: TCP (Transmission Control Protocol)

Dịch vụ: HTTP (Hypertext Transfer Protocol)

Port 443 – Tương tư như port 80 nhưng port 80 không mã hóa dữ liệu, trong khi port 443 sử dụng mã hóa SSL/TLS để đảm bảo tính bảo mật của dữ liệu.

Giao thức: TCP (Transmission Control Protocol)

Dịch vụ: HTTPS (Hypertext Transfer Protocol Secure)

****

* Đối với máy có địa chỉ IP 10.12.25.86

Port 135 - Cho phép các ứng dụng và dịch vụ chạy trên các máy tính trong mạng chia sẻ thông tin và truyền tải dữ liệu.

Giao thức: TCP (Transmission Control Protocol)

Dịch vụ: MSRPC (Microsoft Remote Procedure Call)

Port 139 - Sử dụng cho dịch vụ NetBIOS Session Service, một giao thức cũ thường được sử dụng trong mạng Windows để chia sẻ tệp và máy in, cũng như quản lý tài nguyên trên mạng.

Giao thức: TCP (Transmission Control Protocol)

Dịch vụ: NetBIOS Session Service (NetBIOS-ssn)

Port 445 - Cung cấp dịch vụ Microsoft-DS, được sử dụng để truy cập tệp và máy chủ in trên mạng. Nó là phiên bản tiếp theo của NetBIOS và thường được sử dụng trong các môi trường Windows.

Giao thức: TCP (Transmission Control Protocol)

Dịch vụ: Microsoft-DS (Microsoft Directory Services)

Port 902 - Sử dụng cho dịch vụ ISS RealSecure, một ứng dụng dùng để giám sát và bảo mật mạng.

Giao thức: TCP (Transmission Control Protocol)

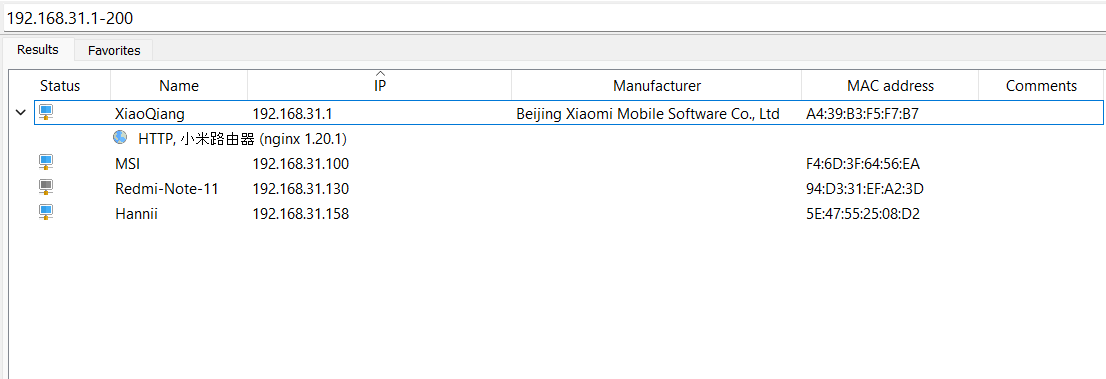
Dịch vụ: ISS RealSecure

Port 912 - Sử dụng cho dịch vụ APEX Mesh, một ứng dụng có thể liên quan đến quản lý mạng hoặc truyền tải dữ liệu.

Giao thức: TCP (Transmission Control Protocol)

Dịch vụ: APEX Mesh

**Ex\_04:**



Sử dụng Advanced IP Scanner để quét dãy địa chỉ IP 192.168.31.1-200:

* Router (XiaoQuiang)

Địa chỉ IP: 192.168.31.1

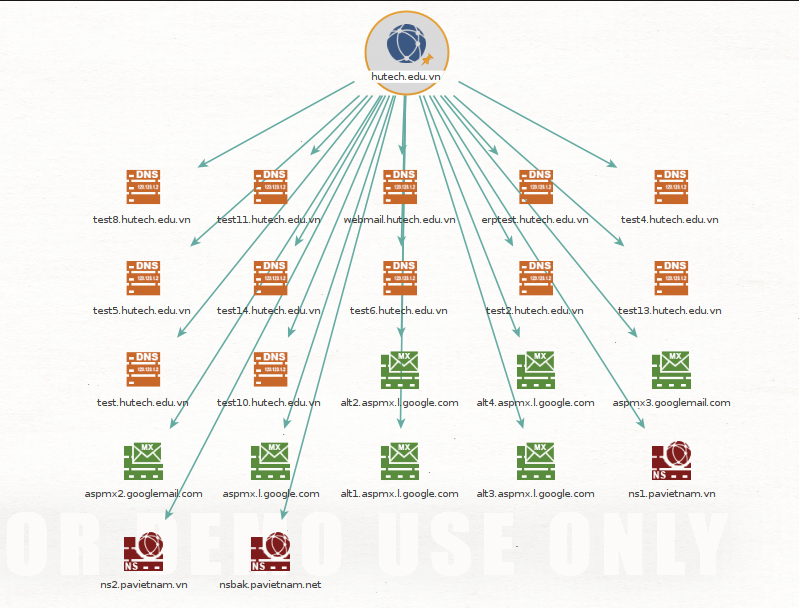
Nhà sản xuất: Beijing Xiaomi Mobile Software Co., Ltd

Địa chỉ MAC: A4:39:B3:F5:F7:B7

Web server: Nginx 1.20.1

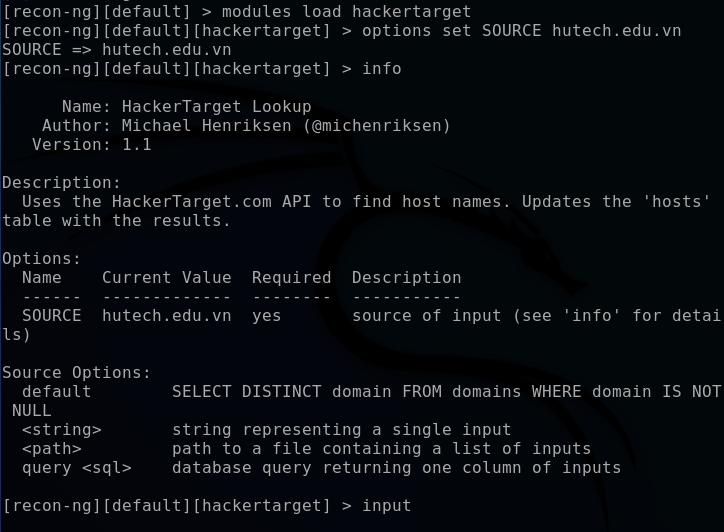
* Cùng với các thiết bị sử dụng mạng như laptop, điện thoại với các thông tin như tên thiết bị, địa chỉ IP và địa chỉ MAC.

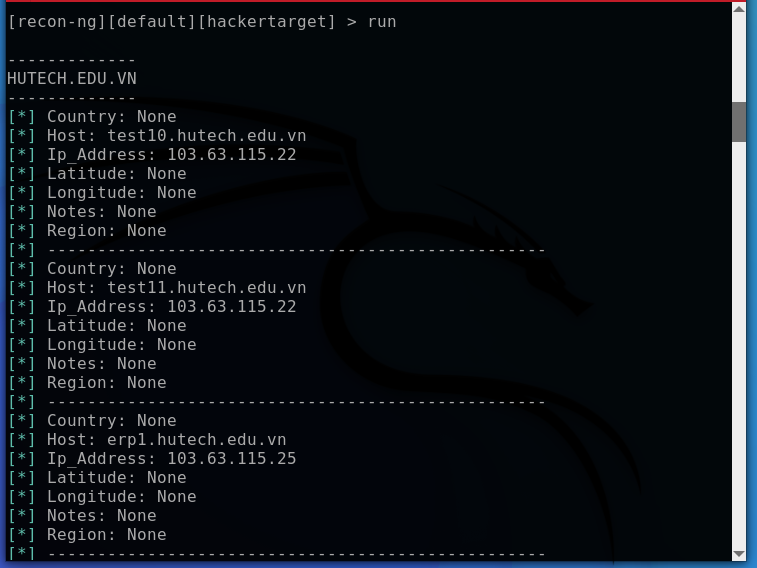
**Ex\_05: Sử dụng công cụ Maltego**

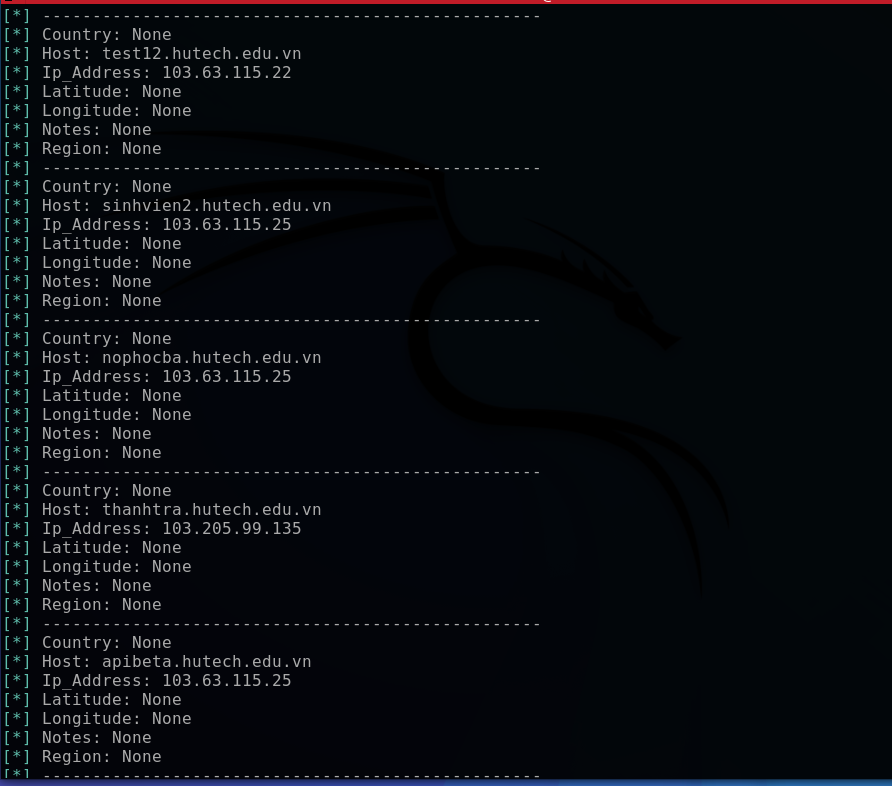
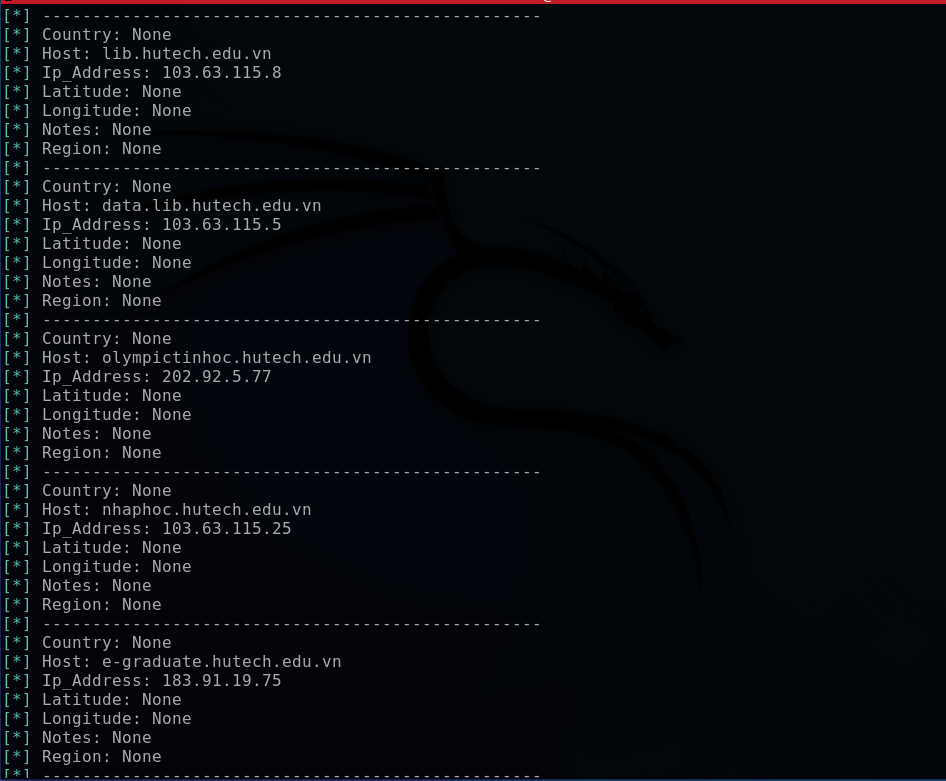
****

Tên miền: hutech.edu.vn. Từ domain name tìm MX records, NS records và DNS.

**Ex\_06: Sử dụng công cụ Footprinting Recon-ng**

****

****

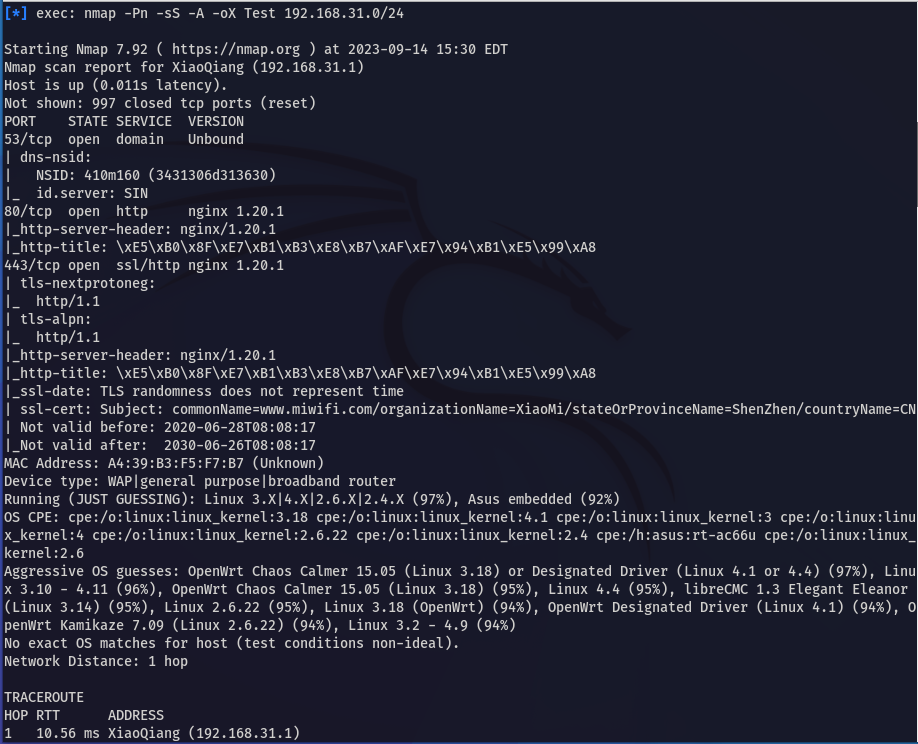
**** ****

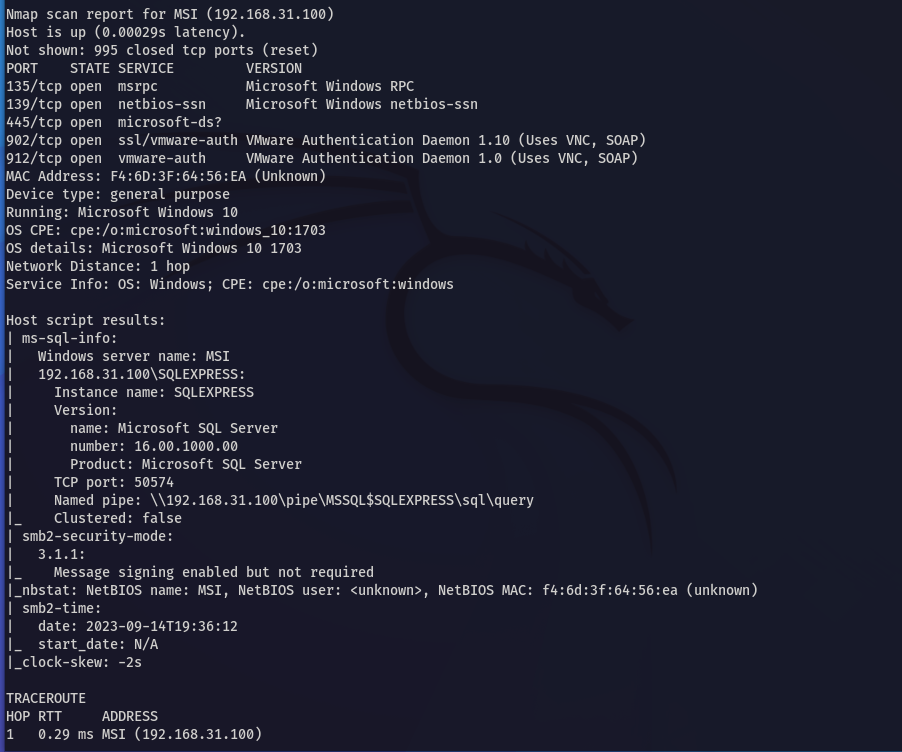
…

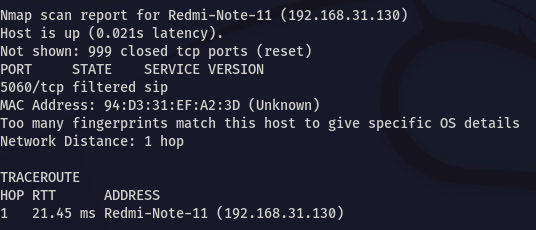
****

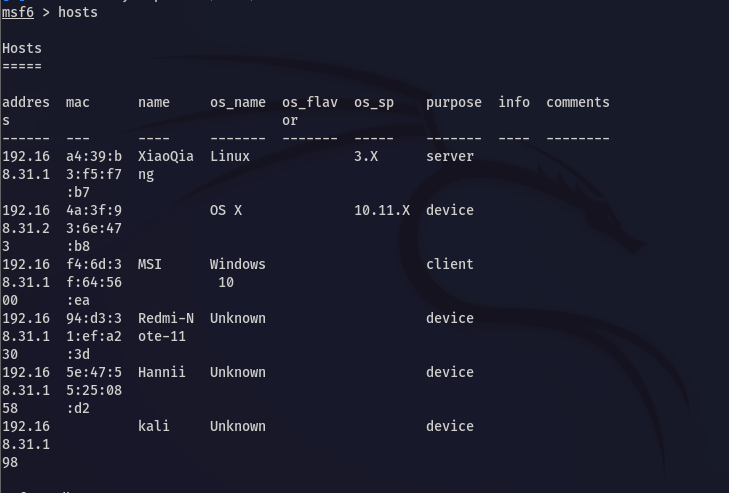
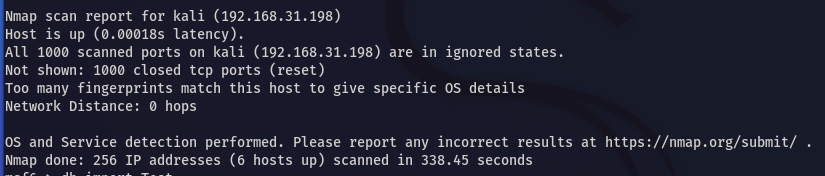
Thu thập được tổng cộng 47 host với các địa chỉ IP, tên miền và những thông tin có liên quan tới mục tiêu.

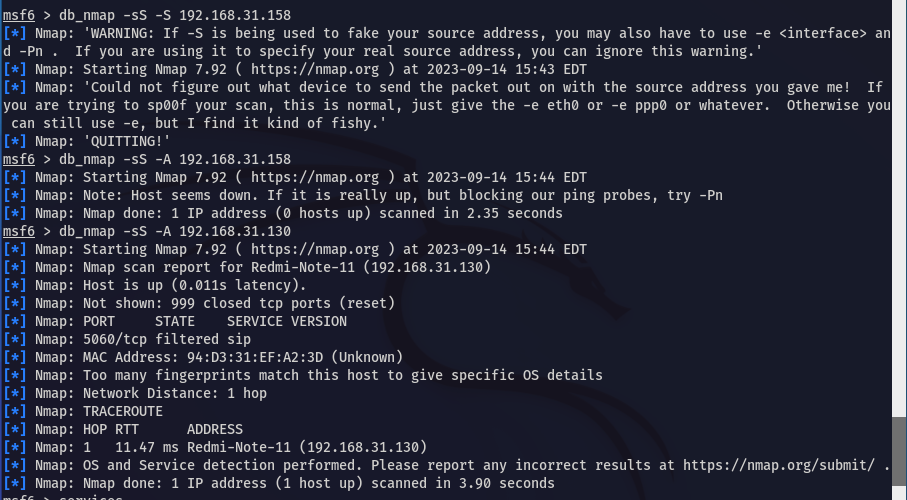
**Ex\_08:** **Sử dụng Metasploit**

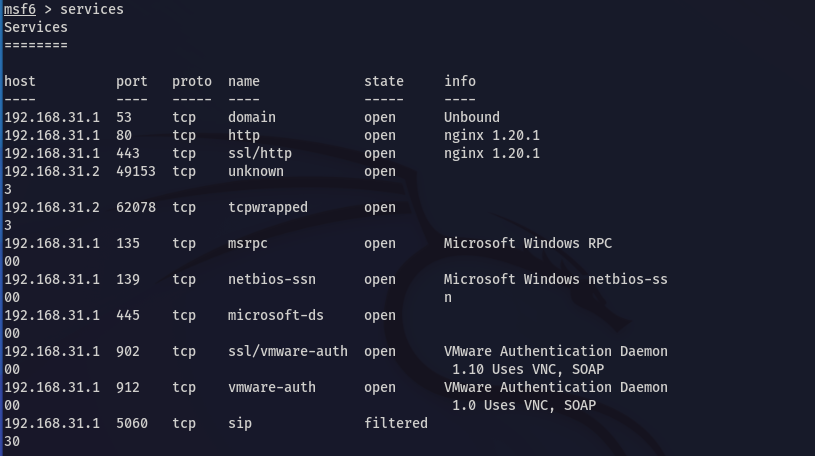
****

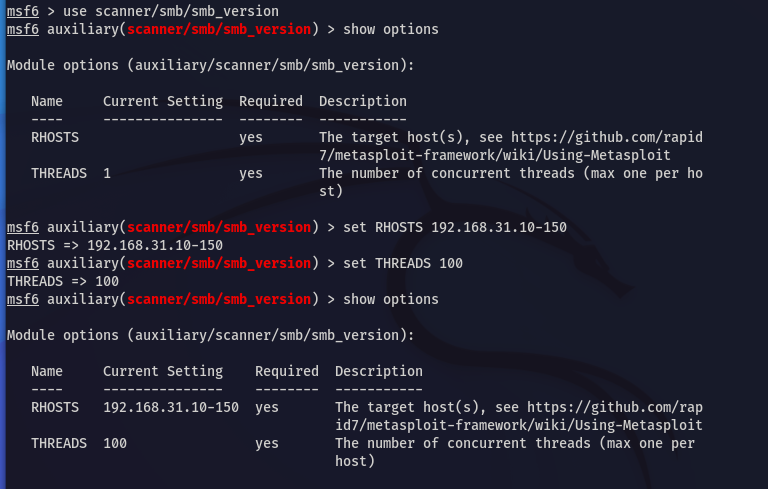
****

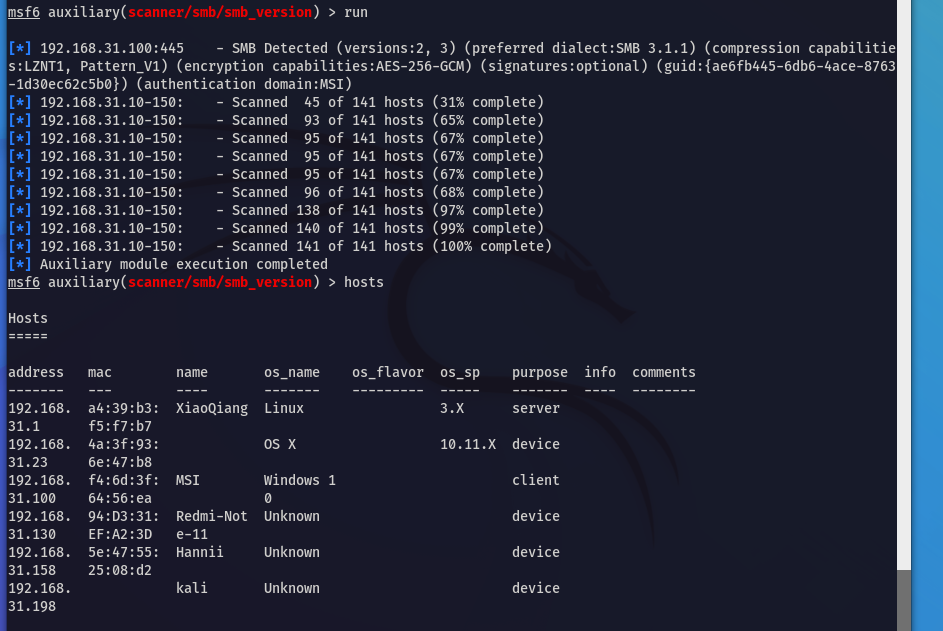
****

****

****

****

****

****

Thu thập được những thông tin như: port (80,53,135,5060,..), dịch vụ (http,ssl,msrpc,netbios-ssn,…), phiên bản (nginx 1.20.1, Microsoft Windows RPC,…), địa chỉ MAC, địa chỉ IP, traceroute, thông tin cụ thể của từng thiết bị như: thông tin hệ điều hành (Linux, OS X, Win 10,…), mssql (tên, phiên bản sử dụng,TCP port).

Hiển thị thông tin với lệnh hosts: Địa chỉ IP, MAC, tên hệ điều hành, phiên bản của hệ điều hành.

Hiển thị thông tin với lệnh services: host (địa chỉ IP), các port của host cùng với tình trạng đang mở hay đóng, tên port và thông tin phiên bản.

RHOSTS đặt dãy địa chỉ IP 192.168.31.10-150 là các máy chủ mục tiêu muốn tấn công và số lượng luồng THREADS là 100 để tăng tốc độ thực hiện.