

Report_Week_02

Họ và tên: Trần Hân Nhi

MSSV: 2011770131 Lớp: 20DATA1

Ex_01:

The screenshot shows the homepage of WhatIsMyIPAddress.com. The main content area displays the following information:

- My IP Address is:**
 - IPv4: [101.99.32.135](#)
 - IPv6: **Not detected**
- My IP Information:**
 - ISP: CMC Telecom Infrastructure Company
 - City: Biên Hòa
 - Region: Đồng Nai
 - Country: Viet Nam
- Location:** A map of Vietnam with a red pin indicating the location. A tooltip says "Click for more details about 101.99.32.135".
- Warning:** "Your location may be exposed!" with a red button labeled "HIDE MY IP ADDRESS NOW".
- Links:** [Show Complete IP Details](#) and [Update My IP Location](#).

The top navigation bar includes links for ABOUT, PRESS, BLOG, and SUPPORT. The bottom of the page has a footer with "Leaflet | © OpenStreetMap Terms".

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

The screenshot shows the homepage of WhatIsMyIPAddress.com. The header includes the logo, a search bar, and navigation links (ABOUT, PRESS, BLOG, SUPPORT). Below the header is a menu with links: MY IP, IP LOOKUP, HIDE MY IP, VPNs, TOOLS, and LEARN. The main content area displays the user's IP address (149.102.229.228) and IPv6 status (Not detected). It also shows 'My IP Information' including ISP (DataCamp Limited), Services (Network Sharing Device), City (Mount Hope), Region (Kansas), and Country (United States). A red button labeled 'HIDE MY IP ADDRESS NOW' is prominent. To the right, a map shows the location in the United States, with a warning 'Your location may be exposed!' and a link to 'Show Complete IP Details'. A 'Location not accurate?' message with a link to 'Update My IP Location' is also present.

My IP Address is:

IPv4: [149.102.229.228](#)

IPv6: [Not detected](#)

My IP Information:

ISP: DataCamp Limited

Services: [Network Sharing Device](#)

City: Mount Hope

Region: Kansas

Country: United States

Your location may be exposed!

[HIDE MY IP ADDRESS NOW](#)

[Show Complete IP Details](#)

Location not accurate? [Update My IP Location](#)

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

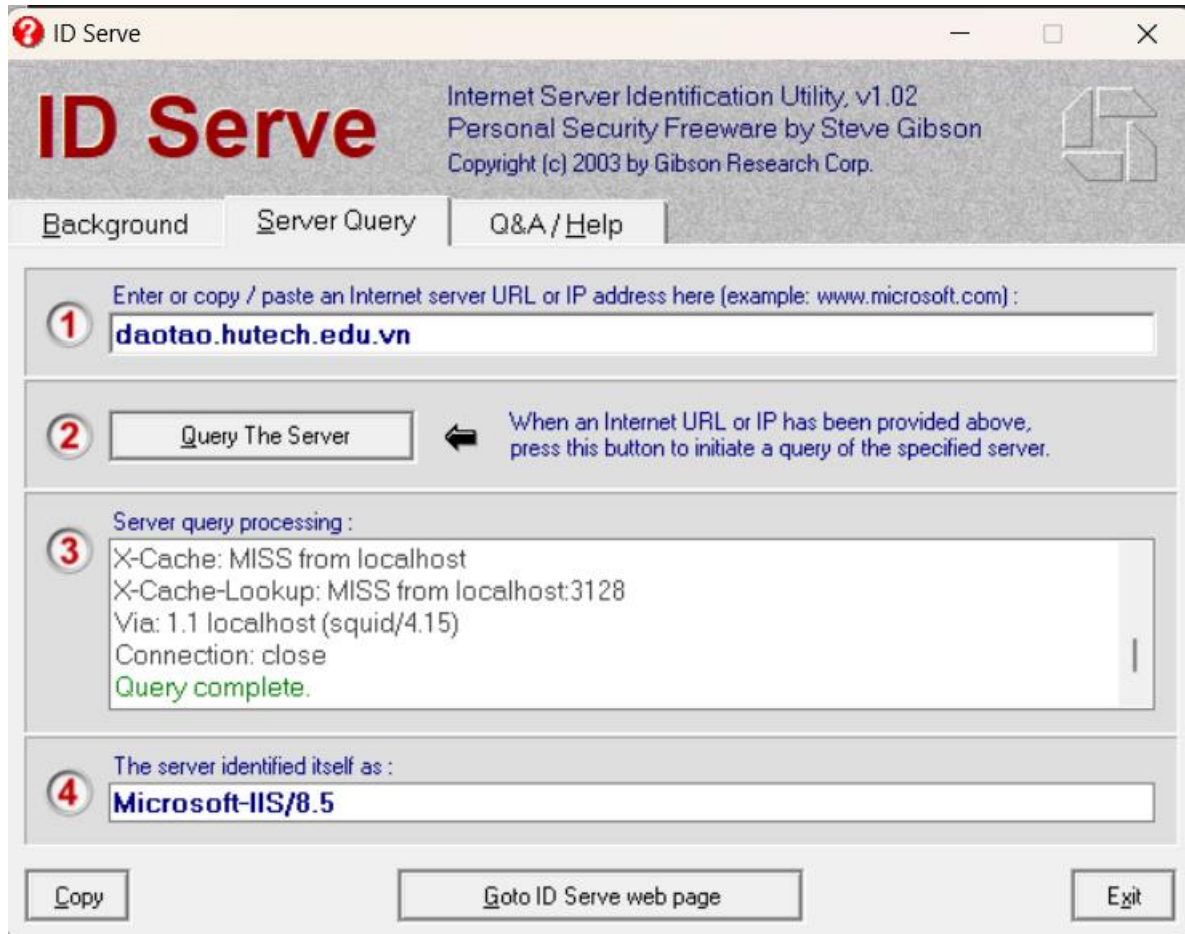
Thành phố: Mount Hope

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*

The screenshot shows the Httprecon 7.3 application window. The title bar indicates the target is `http://103.63.115.6:80/`. The interface includes a menu bar (File, Configuration, Fingerprinting, Reporting, Help) and a toolbar with an 'Analyze' button. The main display area shows the results of an HTTP request, including the status line `HTTP/1.1 200 OK` and various headers. Below the main display, there is a 'Matchlist (352 Implementations)' section with a table showing the results of the fingerprinting process.

Name	Hits	Match %
Microsoft IIS 6.0	76	100
Microsoft IIS 7.0	71	93.42...
nginx 0.5.19	65	85.52...
nginx 0.5.32	65	85.52...
Apache 1.3.37	64	84.21...
Apache 2.2.3	64	84.21...
Apache 1.3.33	63	82.89...
Cherokee 0.6.0	63	82.89...
nginx 0.6.13	63	82.89...
Zeus 4.3	63	82.89...

Ex_03:

```
C:\Users\NHI>nmap hutech.edu.vn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-15 16:07 SE Asia Standard Time
Nmap scan report for hutech.edu.vn (103.63.115.9)
Host is up (0.018s latency).
rDNS record for 103.63.115.9: static.cmcti.vn
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 9.81 seconds
```

- 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 tự 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)

```
C:\Users\NHI>nmap 10.12.25.86
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 14:10 SE Asia Standard Time
Nmap scan report for msi.hutechlan2.vn (10.12.25.86)
Host is up (0.00028s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsure
912/tcp   open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 5.75 seconds
```

- 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:

192.168.31.1-200					
Results Favorites					
Status	Name	IP	Manufacturer	MAC address	Comments
✓	XiaoQiang	192.168.31.1	Beijing Xiaomi Mobile Software Co., Ltd	A4:39:B3:F5:F7:B7	
	HTTP, 小米路由器 (nginx 1.20.1)				
	MSI	192.168.31.100		F4:6D:3F:64:56:EA	
	Redmi-Note-11	192.168.31.130		94:D3:31:EF:A2:3D	
	Hannii	192.168.31.158		5E:47:55:25:08:D2	

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

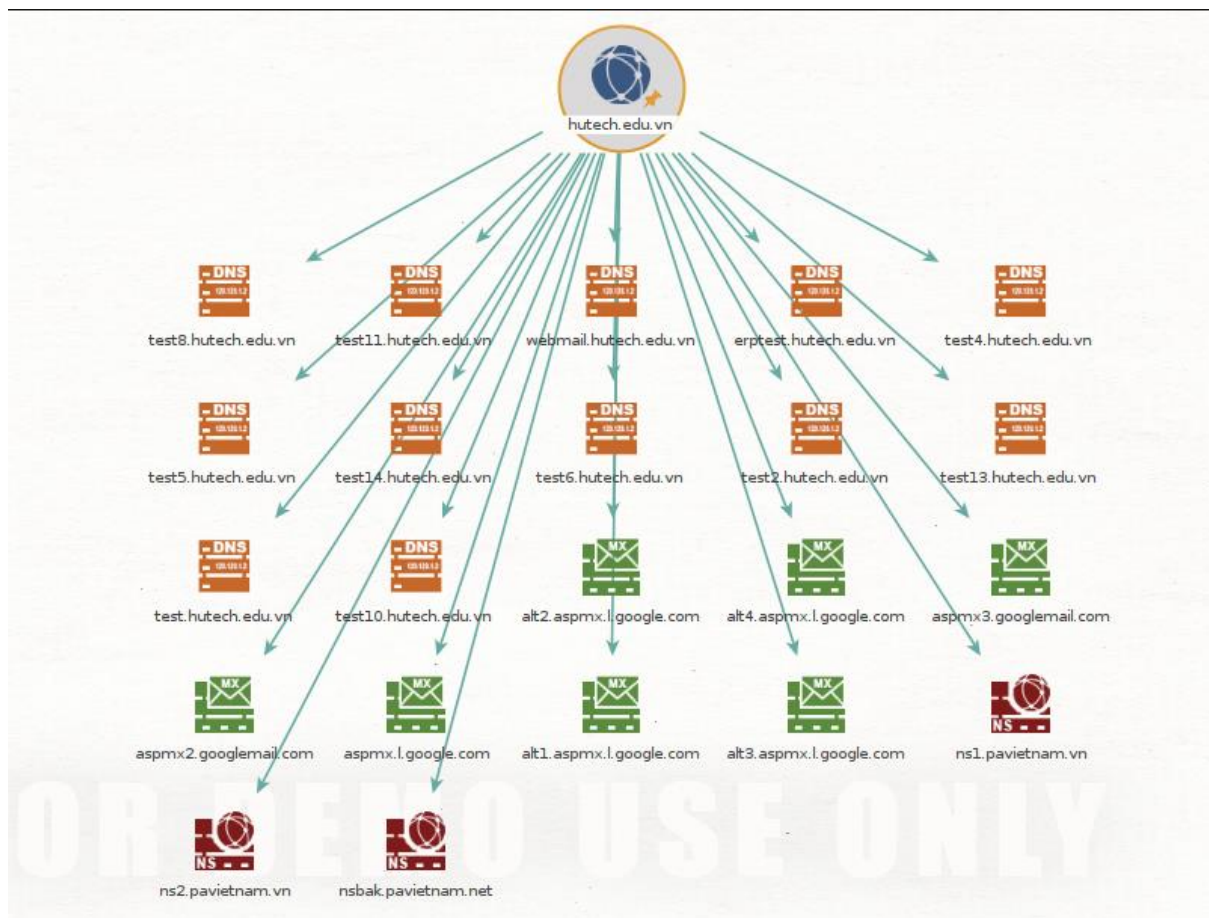
Nhà sản xuất: Beijing Xiaomi Mobile Software Co., Ltd

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

```
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > options set SOURCE hutech.edu.vn
SOURCE => hutech.edu.vn
[recon-ng][default][hackertarget] > info

    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts'
    table with the results.

Options:
    Name      Current Value  Required  Description
    -----
    SOURCE    hutech.edu.vn    yes       source of input (see 'info' for details)

Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT
    NULL
    <string>      string representing a single input
    <path>        path to a file containing a list of inputs
    query <sql>  database query returning one column of inputs

[recon-ng][default][hackertarget] > input
```

```
[recon-ng][default][hackertarget] > run

-----
HUTECH.EDU.VN
-----
[*] Country: None
[*] Host: test10.hutech.edu.vn
[*] Ip_Address: 103.63.115.22
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: test11.hutech.edu.vn
[*] Ip_Address: 103.63.115.22
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: erp1.hutech.edu.vn
[*] Ip_Address: 103.63.115.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
```



```
[*] -----
[*] Country: None
[*] Host: test12.hutech.edu.vn
[*] Ip_Address: 103.63.115.22
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: sinhvien2.hutech.edu.vn
[*] Ip_Address: 103.63.115.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: nophocba.hutech.edu.vn
[*] Ip_Address: 103.63.115.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: thanhtra.hutech.edu.vn
[*] Ip_Address: 103.205.99.135
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: apibeta.hutech.edu.vn
[*] Ip_Address: 103.63.115.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
```

```
[*] -----
[*] Country: None
[*] Host: lib.hutech.edu.vn
[*] Ip_Address: 103.63.115.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: data.lib.hutech.edu.vn
[*] Ip_Address: 103.63.115.5
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: olympictinhoc.hutech.edu.vn
[*] Ip_Address: 202.92.5.77
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: nhaphoc.hutech.edu.vn
[*] Ip_Address: 103.63.115.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: e-graduate.hutech.edu.vn
[*] Ip_Address: 183.91.19.75
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
```

...

```
[*] 47 total (47 new) hosts found.
```

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

```
[*] exec: nmap -Pn -sS -A -oX Test 192.168.31.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 15:30 EDT
Nmap scan report for XiaoQiang (192.168.31.1)
Host is up (0.011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain Unbound
| dns-nsid:
|   NSID: 410m160 (3431306d313630)
|_ id.server: SIN
80/tcp    open  http    nginx 1.20.1
|_ http-server-header: nginx/1.20.1
|_ http-title: \xE5\xB0\x8F\xE7\xB1\xB3\xE8\xB7\xAF\xE7\x94\xB1\xE5\x99\xA8
443/tcp    open  ssl/http nginx 1.20.1
|_ tls-nextprotoneg:
|_   http/1.1
|_ tls-alpn:
|_   http/1.1
|_ http-server-header: nginx/1.20.1
|_ http-title: \xE5\xB0\x8F\xE7\xB1\xB3\xE8\xB7\xAF\xE7\x94\xB1\xE5\x99\xA8
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=www.miwifi.com/organizationName=XiaoMi/stateOrProvinceName=ShenZhen/countryName=CN
|_ Not valid before: 2020-06-28T08:08:17
|_ Not valid after: 2030-06-26T08:08:17
MAC Address: A4:39:B3:F5:F7:B7 (Unknown)
Device type: WAP|general purpose|broadband router
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X|2.4.X (97%), Asus embedded (92%)
OS CPE: cpe:/o:linux:linux_kernel:3.18 cpe:/o:linux:linux_kernel:4.1 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linu
x_kernel:4 cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:linux:linux_kernel:2.4 cpe:/h:asus:rt-ac66u cpe:/o:linux:linux_
kernel:2.6
Aggressive OS guesses: OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (97%), Linu
x 3.10 - 4.11 (96%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) (95%), Linux 4.4 (95%), libreCMC 1.3 Elegant Eleanor
(Linux 3.14) (95%), Linux 2.6.22 (95%), Linux 3.18 (OpenWrt) (94%), OpenWrt Designated Driver (Linux 4.1) (94%), O
penWrt Kamikaze 7.09 (Linux 2.6.22) (94%), Linux 3.2 - 4.9 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1 10.56 ms XiaoQiang (192.168.31.1)
```

```
Nmap scan report for MSI (192.168.31.100)
Host is up (0.00029s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: F4:6D:3F:64:56:EA (Unknown)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ ms-sql-info:
|   Windows server name: MSI
|   192.168.31.100\SQLEXPRESS:
|     Instance name: SQLEXPRESS
|     Version:
|       name: Microsoft SQL Server
|       number: 16.00.1000.00
|       Product: Microsoft SQL Server
|     TCP port: 50574
|     Named pipe: \\192.168.31.100\pipe\MSSQL$SQLEXPRESS\sql\query
|_   Clustered: false
|_ smb2-security-mode:
|   3.1.1:
|_   Message signing enabled but not required
|_ nbstat: NetBIOS name: MSI, NetBIOS user: <unknown>, NetBIOS MAC: f4:6d:3f:64:56:ea (unknown)
|_ smb2-time:
|   date: 2023-09-14T19:36:12
|_   start_date: N/A
|_ clock-skew: -2s

TRACEROUTE
HOP RTT      ADDRESS
1   0.29 ms  MSI (192.168.31.100)
```

```
Nmap scan report for Redmi-Note-11 (192.168.31.130)
Host is up (0.021s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5060/tcp   filtered sip
MAC Address: 94:D3:31:EF:A2:3D (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   21.45 ms  Redmi-Note-11 (192.168.31.130)
```

```

Nmap scan report for kali (192.168.31.198)
Host is up (0.00018s latency).
All 1000 scanned ports on kali (192.168.31.198) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 338.45 seconds

```

```
msf6 > hosts
```

```
Hosts
```

```
=====
```

addresses	mac	name	os_name	os_flav or	os_sp	purpose	info	comments
192.168.31.1	a4:39:b3:f5:f7:b7	XiaoQiang	Linux		3.X	server		
192.168.31.2	4a:3f:93:6e:47:b8		OS X		10.11.X	device		
192.168.31.00	f4:6d:3f:64:56:ea	MSI	Windows 10			client		
192.168.31.30	94:d3:31:ef:a2:3d	Redmi-Note-11	Unknown			device		
192.168.31.58	5e:47:55:25:08:d2	Hannii	Unknown			device		
192.168.31.98		kali	Unknown			device		

```
msf6 > db_nmap -sS -S 192.168.31.158
```

```

[*] Nmap: 'WARNING: If -S is being used to fake your source address, you may also have to use -e <interface> and -Pn . If you are using it to specify your real source address, you can ignore this warning.'
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 15:43 EDT
[*] Nmap: 'Could not figure out what device to send the packet out on with the source address you gave me! If you are trying to spoof your scan, this is normal, just give the -e eth0 or -e ppp0 or whatever. Otherwise you can still use -e, but I find it kind of fishy.'
[*] Nmap: 'QUITTING!'

```

```
msf6 > db_nmap -sS -A 192.168.31.158
```

```

[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 15:44 EDT
[*] Nmap: Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 2.35 seconds

```

```
msf6 > db_nmap -sS -A 192.168.31.130
```

```

[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 15:44 EDT
[*] Nmap: Nmap scan report for Redmi-Note-11 (192.168.31.130)
[*] Nmap: Host is up (0.011s latency).
[*] Nmap: Not shown: 999 closed tcp ports (reset)
[*] Nmap: PORT      STATE      SERVICE VERSION
[*] Nmap: 5060/tcp filtered sip
[*] Nmap: MAC Address: 94:D3:31:EF:A2:3D (Unknown)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1    11.47 ms Redmi-Note-11 (192.168.31.130)
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds

```

```
msf6 > services
```

```
Services
```

```
=====
```

host	port	proto	name	state	info
192.168.31.1	53	tcp	domain	open	Unbound
192.168.31.1	80	tcp	http	open	nginx 1.20.1
192.168.31.1	443	tcp	ssl/http	open	nginx 1.20.1
192.168.31.2	49153	tcp	unknown	open	
3					
192.168.31.2	62078	tcp	tcpwrapped	open	
3					
192.168.31.1	135	tcp	msrpc	open	Microsoft Windows RPC
00					
192.168.31.1	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
00					
192.168.31.1	445	tcp	microsoft-ds	open	
00					
192.168.31.1	902	tcp	ssl/vmware-auth	open	VMware Authentication Daemon 1.10 Uses VNC, SOAP
00					
192.168.31.1	912	tcp	vmware-auth	open	VMware Authentication Daemon 1.0 Uses VNC, SOAP
00					
192.168.31.1	5060	tcp	sip	filtered	
30					

```
msf6 > use scanner/smb/smb_version
```

```
msf6 auxiliary(scanner/smb/smb_version) > show options
```

```
Module options (auxiliary/scanner/smb/smb_version):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS	1	yes	The number of concurrent threads (max one per host)

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.31.10-150
```

```
RHOSTS => 192.168.31.10-150
```

```
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
```

```
THREADS => 100
```

```
msf6 auxiliary(scanner/smb/smb_version) > show options
```

```
Module options (auxiliary/scanner/smb/smb_version):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.31.10-150	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS	100	yes	The number of concurrent threads (max one per host)

```

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.31.100:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:optional) (guid:{ae6fb445-6db6-4ace-8763-1d30ec62c5b0}) (authentication domain:MSI)
[*] 192.168.31.10-150: - Scanned 45 of 141 hosts (31% complete)
[*] 192.168.31.10-150: - Scanned 93 of 141 hosts (65% complete)
[*] 192.168.31.10-150: - Scanned 95 of 141 hosts (67% complete)
[*] 192.168.31.10-150: - Scanned 95 of 141 hosts (67% complete)
[*] 192.168.31.10-150: - Scanned 95 of 141 hosts (67% complete)
[*] 192.168.31.10-150: - Scanned 96 of 141 hosts (68% complete)
[*] 192.168.31.10-150: - Scanned 138 of 141 hosts (97% complete)
[*] 192.168.31.10-150: - Scanned 140 of 141 hosts (99% complete)
[*] 192.168.31.10-150: - Scanned 141 of 141 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====

address  mac          name      os_name  os_flavor  os_sp  purpose  info  comments
-----  ---
192.168.31.1  a4:39:b3:f5:f7:b7  XiaoQiang  Linux    3.X        server
192.168.31.23  4a:3f:93:6e:47:b8  OS X      10.11.X  device
192.168.31.100  f4:6d:3f:64:56:ea  MSI       Windows 10  client
192.168.31.130  94:D3:31:EF:A2:3D  Redmi-Not e-11      Unknown   device
192.168.31.158  5e:47:55:25:08:d2  Hannii    Unknown   device
192.168.31.198  kali          Unknown   device

```

Thu thập được những thông tin như: port (80,53,135,5060,..), dịch vụ (http,ssl,mrsrc,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.