

# Module 1. Tìm hiểu về Network và các công cụ phân tích mạng

- Tổng quan về TCP/IP, sử dụng các công Network traffic generation, analyzation
- Tổng quan TCP/IP stack: mô hình phân tầng TCP/IP, các giao thức trên từng tầng, Quy trình bắt tay 3 bước (3-way handshake) TCP
- Sử dụng Wireshark để phân tích gói tin TCP – chỉ rõ các trường header của gói tin và ý nghĩa của trường đó trên công cụ wireshark.
- Giới thiệu kỹ thuật scan port và các công cụ scan port Nmap, nping, hping(nmap.org)

## I. Tổng quan về TCP/IP, sử dụng các công Network traffic generation, analyzation

### 1. Network traffic generation

- Iperf: là một công cụ tạo lưu lượng mạng đơn giản, hỗ trợ nhiều giao thức như TCP, UDP và SCTP.  
Example:
- hping: là một công cụ tạo gói tin mạng và kiểm tra mạng, hỗ trợ nhiều giao thức như TCP, UDP, ICMP và RAW-IP.  
Example:

### 2. Network traffic analyzation

- Wireshark: là một công cụ phân tích lưu lượng mạng miễn phí và phổ biến, có thể hiển thị, phân tích và giải mã các giao thức mạng khác nhau.

Example:

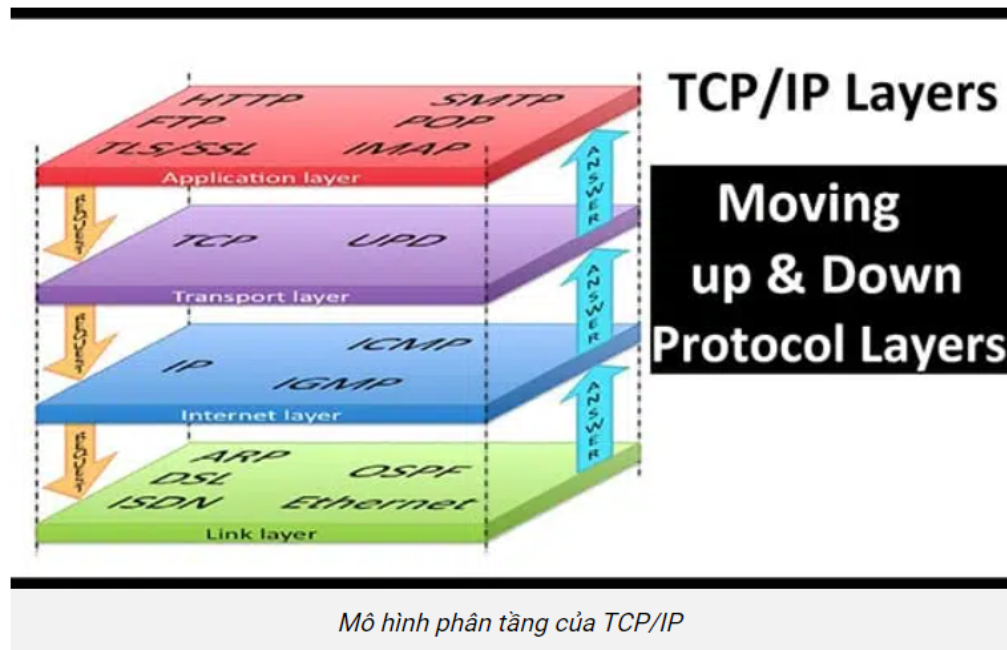
- Tcpdump: là một công cụ dòng lệnh để bắt và phân tích các gói tin trên mạng.

Example:

- tshark: là một phiên bản dòng lệnh của Wireshark, cho phép phân tích lưu lượng mạng từ xa hoặc trong một tệp lưu trữ.

Example:

## II. Tổng quan TCP/IP stack: mô hình phân tầng TCP/IP, các giao thức trên từng tầng, Quy trình bắt tay 3 bước (3-way handshake) TCP



### 1. Mô hình phân tầng TCP/IP, các giao thức trên từng tầng

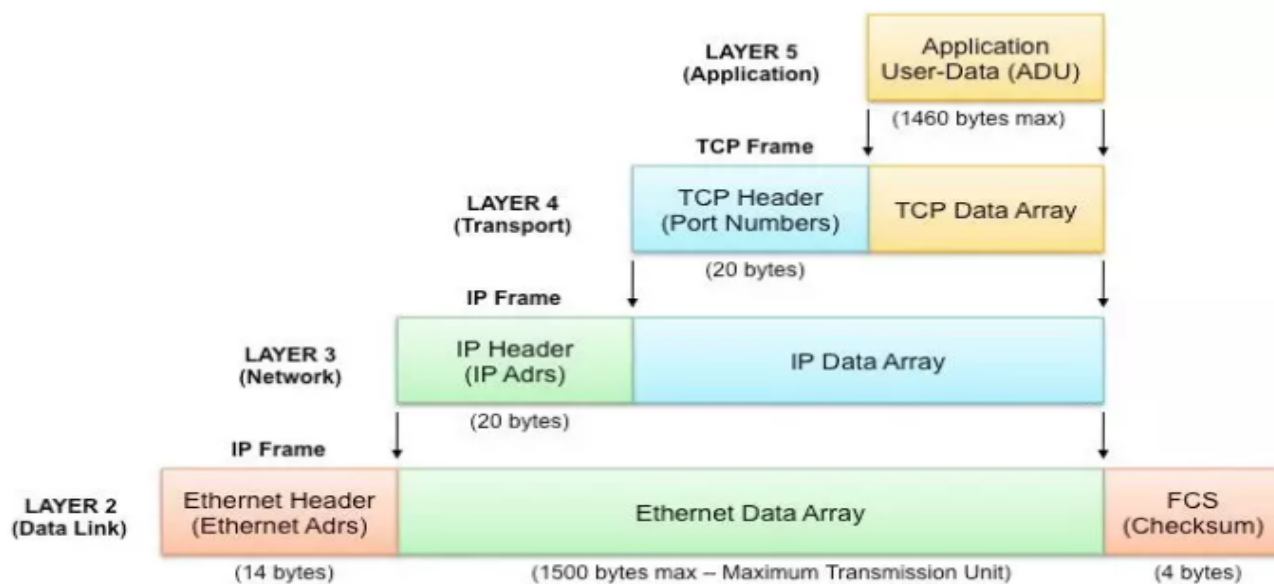
- **Application:** Xử lý các yêu cầu truy cập mạng từ các ứng dụng. Tầng này cung cấp các giao thức (HTTP, SMTP, FTP, DNS, SSH) để gửi và nhận dữ liệu giữa các ứng dụng trên các thiết bị khác nhau trên mạng. Khi dữ liệu được truyền từ ứng dụng này sang ứng dụng khác, tầng Application sẽ tạo ra các gói tin dữ liệu và chuyển giao cho tầng Transport
- **Transport:** có hai giao thức chính là Transmission Control Protocol (TCP, mỗi gói tin đều được đánh số thứ tự, nếu người nhận không nhận được gói tin thì sẽ được gửi lại) và User Datagram Protocol (UDP, nó giống với TCP, tuy nhiên nó không soát lỗi nếu gói tin nào trong quá trình truyền đi bị mất thì mất hẳn không gửi lại). Đảm bảo dữ liệu được truyền tải đến đích đến đúng và đầy đủ. Nó cũng giúp quản lý lưu lượng mạng và đảm bảo rằng các ứng dụng không xung đột với nhau trong việc sử dụng tài nguyên mạng.

- **Network:**

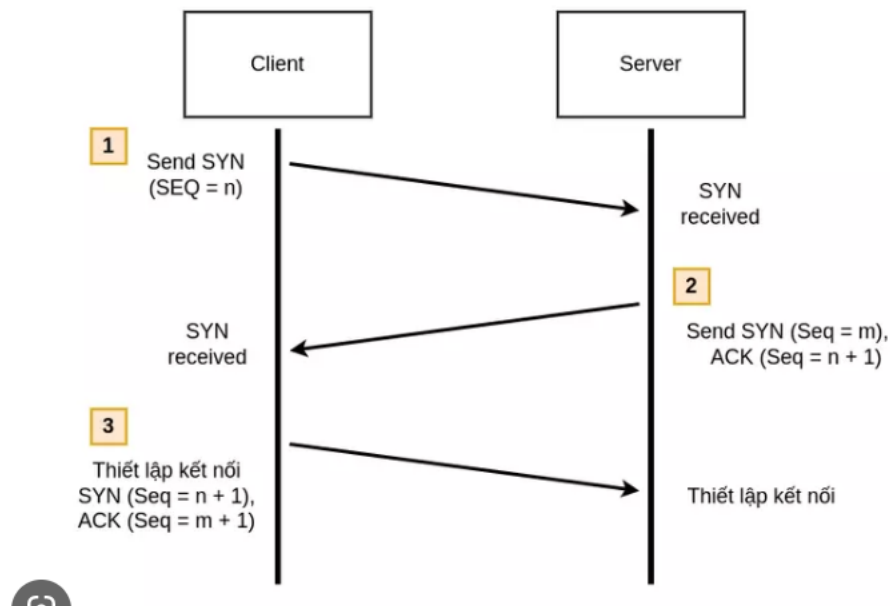
1. **Định tuyến (routing):** là quá trình xác định đường đi tối ưu để dữ liệu được truyền tải từ nguồn đến đích
2. **Chuyển đổi địa chỉ (addressing):** là quá trình chuyển đổi địa chỉ mạng và địa chỉ host để đảm bảo dữ liệu được truyền tải đến đúng đích.
3. **Phân đoạn (fragmentation):** là quá trình chia nhỏ các gói dữ liệu thành các phân đoạn nhỏ hơn để truyền tải qua các kênh truyền có dung lượng giới hạn. Quá trình này được thực hiện khi kích thước của gói dữ liệu vượt quá dung lượng tối đa cho phép của mạng
4. **Ghi nhãn (labeling):** quá trình gắn thêm thông tin nhãn vào các gói dữ liệu để hỗ trợ định tuyến trong các mạng chuyển tiếp.

- **Network Access**

1. Là tầng thấp nhất trong mô hình TCP/IP.
2. Chịu trách nhiệm truyền dữ liệu giữa các thiết bị trong cùng một mạng. Tại đây, các gói dữ liệu được đóng vào khung (Frame) và được định tuyến đi đến đích được chỉ định ban đầu.



## 2. Quy trình bắt tay 3 bước (3-way handshake) TCP\IP



- **Bước 1:** Thiết lập kết nối yêu cầu (SYN)

Trong bước này, thiết bị A muốn thiết lập kết nối với thiết bị B sẽ gửi một thông điệp yêu cầu kết nối (SYN) đến thiết bị B. Gói tin SYN này chứa số thứ tự ban đầu của thiết bị A (ISN) để xác định các gói tin sẽ được truyền theo thứ tự nào.

- **Bước 2:** Phản hồi yêu cầu kết nối (SYN-ACK)

Sau khi thiết bị B nhận được thông điệp SYN từ thiết bị A, nó sẽ gửi một thông điệp phản hồi (SYN-ACK) đến thiết bị A để xác nhận yêu cầu kết nối. Gói tin SYN-ACK này sẽ chứa số thứ tự của thiết bị B (ISN), và số thứ tự của thiết bị A mà nó đã nhận được (ACK).

- **Bước 3:** Xác nhận yêu cầu kết nối (ACK)

Sau khi thiết bị A nhận được phản hồi SYN-ACK từ thiết bị B, nó sẽ gửi một thông điệp xác nhận (ACK) đến thiết bị B để hoàn tất quy trình thiết lập kết nối. Gói tin ACK này chứa số thứ tự của thiết bị A (ACK), và số thứ tự của thiết bị B mà nó đã nhận được (ACK).

=> Sau khi quá trình bắt tay ba bước hoàn tất, kết nối giữa hai thiết bị sẽ được thiết lập và dữ liệu có thể được truyền tải giữa chúng. Nếu trong quá trình này có bất kỳ lỗi nào xảy ra hoặc thiết bị

không nhận được phản hồi nào, quá trình thiết lập kết nối sẽ thất bại và phải được thực hiện lại từ đầu.

### III. Sử dụng Wireshark để phân tích gói tin TCP – chỉ rõ các trường header của gói tin và ý nghĩa của trường đó trên công cụ wireshark.

<https://vietnix.vn/wireshark-la-gi/>

No.	Time	Source	Destination	Protocol	Length	Info
120	3.188233	192.168.50.85	64.233.189.188	TCP	55	43712 → 5228 [ACK] Seq=1 Ack=1 Win=63951 Len=1
121	3.267838	64.233.189.188	192.168.50.85	TCP	66	5228 → 43712 [ACK] Seq=1 Ack=2 Win=65535 Len=0 SLE=1 SRE=2
199	13.140756	192.168.50.85	143.92.116.160	TCP	55	40844 → 19000 [ACK] Seq=1 Ack=1 Win=64756 Len=1
200	13.204690	143.92.116.160	192.168.50.85	TCP	66	19000 → 40844 [ACK] Seq=1 Ack=2 Win=63322 Len=0 SLE=1 SRE=2
359	22.736957	192.168.50.85	23.198.132.134	TCP	54	48430 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63977 Len=0
360	22.738932	192.168.50.85	8.241.138.126	TCP	54	48432 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63903 Len=0
361	22.739538	192.168.50.85	23.198.132.134	TCP	54	48431 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63977 Len=0
362	22.762313	23.198.132.134	192.168.50.85	TCP	54	80 → 48431 [FIN, ACK] Seq=1 Ack=2 Win=64013 Len=0
363	22.763018	192.168.50.85	23.198.132.134	TCP	54	48431 → 80 [ACK] Seq=2 Ack=2 Win=63977 Len=0
364	22.764398	23.198.132.134	192.168.50.85	TCP	54	80 → 48430 [FIN, ACK] Seq=1 Ack=2 Win=63977 Len=0
365	22.764954	192.168.50.85	23.198.132.134	TCP	54	48430 → 80 [ACK] Seq=2 Ack=2 Win=63977 Len=0
366	22.795903	8.241.138.126	192.168.50.85	TCP	54	80 → 48432 [FIN, ACK] Seq=1 Ack=2 Win=42058 Len=0
367	22.796564	192.168.50.85	8.241.138.126	TCP	54	48432 → 80 [ACK] Seq=2 Ack=2 Win=63903 Len=0
370	25.549120	104.21.6.150	192.168.50.85	TCP	54	443 → 47235 [ACK] Seq=1 Ack=62 Win=63784 Len=0
372	25.630833	192.168.50.85	104.21.6.150	TCP	54	47235 → 443 [ACK] Seq=62 Ack=58 Win=63089 Len=0
778	39.638617	192.168.50.85	74.125.204.188	TCP	55	40047 → 5228 [ACK] Seq=1 Ack=1 Win=64244 Len=1
779	39.724678	74.125.204.188	192.168.50.85	TCP	66	5228 → 40047 [ACK] Seq=1 Ack=2 Win=65535 Len=0 SLE=1 SRE=2
369	25.520318	192.168.50.85	104.21.6.150	TLSv1.2	115	Application Data
371	25.587945	104.21.6.150	192.168.50.85	TLSv1.2	111	Application Data

> Frame 366: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{677838C8-54D0-4826-9E2D-8C41AF2E9C1F}, id 0

> Ethernet II, Src: ASUSTek\_ba:06:18 (04:42:1a:ba:06:18), Dst: IntelCor\_cf:af:12:f (04:ed:33:cf:af:12:f)

> Internet Protocol Version 4, Src: 8.241.138.126, Dst: 192.168.50.85

> Transmission Control Protocol, Src Port: 80, Dst Port: 48432, Seq: 1, Ack: 2, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.211.133	192.168.211.133	HTTP	543	GET /secret/ HTTP/1.1
2	0.000032850	192.168.211.133	192.168.211.133	TCP	50	80 → 8080 [RST] Seq=1 Win=0 Len=0
3	0.000023625	192.168.211.133	192.168.211.133	TCP	76	80 → 52798 [SYN, ACK] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=1957753944 TSecr=0 WS=128
4	0.000058818	192.168.211.133	192.168.211.133	TCP	76	80 → 52798 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=1957753944 TSecr=1957753944 WS=128
5	0.000087849	192.168.211.133	192.168.211.133	TCP	68	52798 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1957753944 TSecr=1957753944
6	0.001199751	192.168.211.133	192.168.211.133	HTTP	543	GET /secret/ HTTP/1.1
7	0.001391313	192.168.211.133	192.168.211.133	TCP	68	80 → 52798 [ACK] Seq=1 Ack=476 Win=65024 Len=0 TSval=1957753945 TSecr=1957753945
8	0.002893962	192.168.211.133	192.168.211.133	HTTP	816	HTTP/1.1 401 Unauthorized (text/html)
9	0.002871429	192.168.211.133	192.168.211.133	TCP	68	52798 → 80 [ACK] Seq=476 Ack=749 Win=64896 Len=0 TSval=1957753946 TSecr=1957753946
10	0.005663353	192.168.211.133	192.168.211.133	TCP	68	80 → 52798 [FIN, ACK] Seq=749 Ack=476 Win=65536 Len=0 TSval=1957758949 TSecr=1957753946
11	0.0056134310	192.168.211.133	192.168.211.133	TCP	68	52798 → 80 [ACK] Seq=476 Ack=750 Win=64896 Len=0 TSval=1957758993 TSecr=1957758949
12	0.005481775	192.168.211.133	192.168.211.133	HTTP	847	GET /secret/ HTTP/1.1
13	0.005505910	192.168.211.133	192.168.211.133	TCP	50	80 → 8080 [RST] Seq=269 Win=0 Len=0
14	0.005190450	192.168.211.133	192.168.211.133	TCP	76	46894 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=1957764110 TSecr=0 WS=128
15	0.006206814	192.168.211.133	192.168.211.133	TCP	76	80 → 46894 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=1957764110 TSecr=1957764110 WS=128
16	0.006225218	192.168.211.133	192.168.211.133	TCP	68	46894 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1957764110 TSecr=1957764110
17	0.006382915	192.168.211.133	192.168.211.133	HTTP	547	GET /secret/ HTTP/1.1
18	0.006456085	192.168.211.133	192.168.211.133	TCP	68	80 → 46894 [ACK] Seq=1 Ack=480 Win=65024 Len=0 TSval=1957764110 TSecr=1957764110
19	0.006482347	192.168.211.133	192.168.211.133	HTTP	775	HTTP/1.1 200 OK (text/html)

> Internet Protocol Version 4, Src: 192.168.211.133, Dst: 192.168.211.133

> Transmission Control Protocol, Src Port: 52798, Dst Port: 80, Seq: 476, Ack: 750, Len: 479

> Hypertext Transfer Protocol

> GET /secret/ HTTP/1.1

Host: 192.168.211.133\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20180816 Firefox/102.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

If-Modified-Since: Tue, 02 May 2023 07:07:01 GMT\r\n

If-None-Match: "63-Sfab06070634-gzip"\r\n

Authorization: Basic TFRlbnVpdjQ1bWdyYXN0\r\n

Credentials: NAMPXH:24062801

\r\n

[Full request URI: http://192.168.211.133/secret/]

[HTTP request 2/2]

[Prev request in frame: 6]

0040 74 b1 07 e5 47 45 54 20 2f 73 65 63 72  
0050 20 48 54 54 50 2f 31 2e 31 6d 0a 48 6f  
0060 20 31 30 32 2e 31 30 38 2e 32 31 31 2e  
0070 0d 0a 55 73 65 72 2d 41 67 65 de 7a 3a  
0080 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31  
0090 4c 69 6e 75 78 20 78 38 35 4f 36 3a 30  
00a0 3a 31 30 32 2e 30 29 29 47 65 63 6b 6f  
00b0 31 30 30 31 30 31 29 46 69 72 65 6b 6f  
00c0 30 32 2e 30 04 0a 41 63 65 70 74 3a  
00d0 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69  
00e0 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c  
00f0 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c  
0100 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69  
0110 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a  
0120 30 2e 38 0d 0a 41 63 65 70 74 2d 4c  
0130 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65  
0140 3d 30 2e 35 0d 0a 61 63 63 65 70 74 20  
0150 6f 64 68 6e 67 68 6f 6e 2f 7a 68 70 30  
0160 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74  
0170 3a 20 6b 65 65 70 2d 61 6c 69 76 65 6d

- **No:** Số thứ tự của gói tin trong file capture hiện tại.
- **Time:** Thời gian tương đối mà gói tin này được bắt, tính từ lúc bắt đầu quá trình bắt gói tin.
- **Source:** địa chỉ source IP của kết nối.
- **Destination:** địa chỉ destination IP của kết nối.
- **Length:** chiều dài của gói tin.
- **Protocol:** giao thức của gói tin
- **Info:** các thông tin tổng quan liên quan đến gói tin.

•

#### IV. Giới thiệu kỹ thuật scan port và các công cụ scan port Nmap, nping, hping(nmap.org)

-Scan port là phương pháp sử dụng để xác định các cổng kết nối mạng đang được sử dụng.(Cổng kết nối mạng được sử dụng để truyền thông tin giữa các thiết bị, và các ứng dụng phổ biến như web server, email server, FTP server, SSH server, và nhiều ứng dụng khác).

-Một số kỹ thuật scan port phổ biến bao gồm:

- TCP connect scan: phương pháp này sử dụng kết nối TCP đầy đủ để kiểm tra trạng thái của các cổng kết nối mạng.
- SYN scan: phương pháp này sử dụng các gói tin TCP SYN để kiểm tra trạng thái của các cổng kết nối mạng.
- UDP scan: phương pháp này sử dụng các gói tin UDP để kiểm tra trạng thái của các cổng kết nối mạng.

-Nmap:

- Để quét mạng Wi-Fi  
**nmap -sn <địa chỉ IP của mạng Wi-Fi>**

```
(root@nampxhhe151338)-[~]
# sudo nmap -sn 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 21:37 EDT
Nmap scan report for RT-AX55-0618 (192.168.50.1)
Host is up (0.0032s latency).
MAC Address: 04:42:1A:BA:06:18 (Asustek Computer)
Nmap scan report for LAPTOP-3GJTBRSD (192.168.50.85)
Host is up (0.00081s latency).
MAC Address: 04:ED:33:CF:A1:2F (Intel Corporate)
Nmap scan report for Galaxy-A02 (192.168.50.196)
Host is up (0.10s latency).
MAC Address: 42:5C:F1:1D:05:C1 (Unknown)
Nmap scan report for Samsung (192.168.50.222)
Host is up (0.0052s latency).
MAC Address: 80:47:86:CE:5A:58 (Samsung Electronics)
Nmap scan report for nampxhhe151338 (192.168.50.124)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.03 seconds
```

- Lệnh quét toàn diện. Lệnh này bao gồm quét cổng, quét dịch vụ và cung cấp thông tin chi tiết về hệ điều hành, kiến trúc, cơ sở dữ liệu và các thông tin khác của máy tính.

**nmap -A [target]**



```

(root@ nampxhhe151338)-[~]
# sudo nmap -A 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 22:08 EDT
Nmap scan report for RT-AX55-0618 (192.168.50.1)
Host is up (0.0024s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
80/tcp    open  http         ASUS WRT http admin
|_http-server-header: httpd/2.0
|_http-title: Site doesn't have a title (text/html).
8443/tcp  open  ssl/http     ASUS WRT http admin
|_http-server-header: httpd/2.0
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=router.asus.com/countryName=US
| Subject Alternative Name: DNS:router.asus.com
| Not valid before: 2018-05-05T05:05:12
|_Not valid after: 2028-05-05T05:05:12
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  upnp         Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
MAC Address: 04:42:1A:BA:06:18 (Asustek Computer)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11
Network Distance: 1 hop
Service Info: CPE: cpe:/o:asus:wrt_firmware, cpe:/h:cisco:e4200

TRACEROUTE
HOP RTT      ADDRESS
1    2.39 ms RT-AX55-0618 (192.168.50.1)

Nmap scan report for LAPTOP-3GJTBRSD (192.168.50.85)
Host is up (0.00058s latency).
All 1000 scanned ports on LAPTOP-3GJTBRSD (192.168.50.85) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 04:ED:33:CF:A1:2F (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1    0.58 ms LAPTOP-3GJTBRSD (192.168.50.85)

Nmap scan report for narzo-50i (192.168.50.198)
Host is up (0.028s latency).
All 1000 scanned ports on narzo-50i (192.168.50.198) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

```

```

^C
--- techcombank.com.vn ping statistics ---
47 packets transmitted, 0 received, 100% packet loss, time 47096ms
ping: techcombank.com.vn: connect: Connection refused (103.4.128.120): No route to host

(root@ nampxhhe151338)-[~]
# ping techcombank.com.vn
PING techcombank.com.vn (103.4.128.120) 56(84) bytes of data.

^C
--- techcombank.com.vn ping statistics ---
47 packets transmitted, 0 received, 100% packet loss, time 47096ms
ping: techcombank.com.vn: connect: Connection refused (103.4.128.120): No route to host

(root@ nampxhhe151338)-[~]
# nmap -Pn -A 103.4.128.120
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 04:03 EDT
Nmap scan report for 103.4.128.120
Host is up.
All 1000 scanned ports on 103.4.128.120 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1    7.11 ms RT-AX55-0618 (192.168.50.1)
2    8.23 ms 192.168.100.1
3    8.64 ms static.vnpt-hanoi.com.vn (203.210.148.86)
4    8.91 ms static.vnpt.vn (113.177.29.109)
5    9.17 ms static.vnpt.vn (113.171.33.149)
6    10.63 ms static.vnpt.vn (113.171.5.197)
7    10.61 ms static.vnpt.vn (113.171.33.82)
8    10.22 ms static.vnpt.vn (123.30.21.90)
9    ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.45 seconds

```

- ## **nmap -sS -sV -O <target>**

```

[root@nampshhe151338]~]
# nmap -sS -sV -O 192.168.50.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-02 22:21 EDT
Nmap scan report for RT-AX55-9618 (192.168.50.1)
Host is up (0.0025s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
80/tcp    open  http         ASUS WRT http admin
8443/tcp  open  ssl/http     ASUS WRT http admin
40152/tcp open  upnp         Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
MAC Address: 04:42:1A:BA:06:18 (Asustek Computer)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS=SCAN(V.7.9.3MFE-K4D=5/2KOT-800CT-1NCU-40312KPV-YKDS-1NDC-DWG-YVM-04421A2TH
OS=6A51SEFPK-P8=6, 04-pc-linux-gnu)SEQ(SP=10AXGCD-1KISR-10CKT1I-ZKCI1KTS=A)
OS=SEQ(SP=10AXGCD-1KISR-10CKT1I-ZKTI1KTS=A)SEQ(SP=10AXGCD-1KISR-10CKT1I-ZKCI
OS=1KTI1KTS=A)OPS(OI=1M5B4ST11NW5K02-M5B4ST11NW5K03-M5B4NNT11NW5K04-M5B4ST
OS=11NW5K05-M5B4ST11NW5K06-M5B4ST11)WIN(W1=7120XW2=7120XW3=7120XW4=7120XW5=
OS=7120XW6=7120)ECN(R=YKDF-YKT+40%W=7210X0-M5B4NNSNW5KCC-YKQ+T)I(R=YKDF-YKT
OS=40KX-010A-S+SF-AKSD0-0RQ+T)T2(R=U)T3(R=U)T4(R=YKDF-YKT+40%W-0KX-AJA-ZWf-R
OS=X02-RKD-0KQ2)T5(R=YKDF-YKT+40%W-0KX-ZKA-S+SF-AKSD0-XRD-0XQ2)T6(R=YKDF-YKT+
OS=40%W-0KX-AJA-ZWf-RKD-XRD-0XQ2)T7(R=N)U1(R=YKDF-NKT+40%IPL-164XUN=0XRIPL=
OS=GXRID0-GXRIPOCK-GXRUCK-GXRUD0X)IE7(R=YKDFI-NKT+40%CD-S)

Network Distance: 1 hop
Service Info: CPE: cpe:/o:asus:wrt_firmware, cpe:/h:cisco:e4200

Nmap scan report for LAPTOP-3GJTBRSD (192.168.50.85)
Host is up (0.00020s latency).
All 1000 scanned ports on LAPTOP-3GJTBRSD (192.168.50.85) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 04:ED:33:CF:A1:2F (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for Samsung (192.168.50.222)
Host is up (0.0040s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
8001/tcp  open  vcom-tunnel?
8002/tcp  open  ssl/teradatao

```

- hiện các hoạt động khai thác khác nhau. Có nhiều script lắm.

```

root@kali:~/size-[-]
└─# ls -al /usr/share/nmap/scripts
total 4976
drwxr-xr-x 2 root root 36864 Feb 26 19:43 .
drwxr-xr-x 4 root root 4096 Feb 26 19:43 ..
-rw-r--r-- 1 root root 3901 Oct 6 2022 acarsd-info.nse
-rw-r--r-- 1 root root 8749 Oct 6 2022 address-info.nse
-rw-r--r-- 1 root root 3345 Oct 6 2022 afp-brute.nse
-rw-r--r-- 1 root root 6463 Oct 6 2022 afp-ls.nse
-rw-r--r-- 1 root root 7081 Oct 6 2022 afp-path-vuln.nse
-rw-r--r-- 1 root root 5680 Oct 6 2022 afp-serverinfo.nse
-rw-r--r-- 1 root root 2621 Oct 6 2022 afp-showmount.nse
-rw-r--r-- 1 root root 2262 Oct 6 2022 ajp-auth.nse
-rw-r--r-- 1 root root 2983 Oct 6 2022 ajp-brute.nse
-rw-r--r-- 1 root root 1329 Oct 6 2022 ajp-headers.nse
-rw-r--r-- 1 root root 2590 Oct 6 2022 ajp-methods.nse
-rw-r--r-- 1 root root 3051 Oct 6 2022 ajp-request.nse
-rw-r--r-- 1 root root 6719 Oct 6 2022 allseeingeye-info.nse
-rw-r--r-- 1 root root 1678 Oct 6 2022 amfp-info.nse
-rw-r--r-- 1 root root 15824 Oct 6 2022 asn-query.nse
-rw-r--r-- 1 root root 2054 Oct 6 2022 auth-owners.nse
-rw-r--r-- 1 root root 870 Oct 6 2022 auth-spoof.nse
-rw-r--r-- 1 root root 9050 Oct 6 2022 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 Oct 6 2022 backorifice-info.nse
-rw-r--r-- 1 root root 53137 Oct 6 2022 bacnet-info.nse
-rw-r--r-- 1 root root 6136 Oct 6 2022 banner.nse
-rw-r--r-- 1 root root 2012 Oct 6 2022 bitcoin-getaddr.nse
-rw-r--r-- 1 root root 1812 Oct 6 2022 bitcoin-info.nse
-rw-r--r-- 1 root root 4437 Oct 6 2022 bitcoinnrpc-info.nse
-rw-r--r-- 1 root root 4079 Oct 6 2022 bittorrent-discovery.nse
-rw-r--r-- 1 root root 1344 Oct 6 2022 bjnp-discover.nse
-rw-r--r-- 1 root root 4428 Oct 6 2022 broadcast-ataoe-discover.nse
-rw-r--r-- 1 root root 2964 Oct 6 2022 broadcast-avahi-dos.nse
-rw-r--r-- 1 root root 4786 Oct 6 2022 broadcast-bjnp-discover.nse
-rw-r--r-- 1 root root 2438 Oct 6 2022 broadcast-db2-discover.nse
-rw-r--r-- 1 root root 3217 Oct 6 2022 broadcast-dhcp6-discover.nse
-rw-r--r-- 1 root root 10151 Oct 6 2022 broadcast-dhcp-discover.nse
-rw-r--r-- 1 root root 1499 Oct 6 2022 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root 12862 Oct 6 2022 broadcast-dropbox-listener.nse
-rw-r--r-- 1 root root 12202 Oct 6 2022 broadcast-eigrp-discovery.nse
-rw-r--r-- 1 root root 3472 Oct 6 2022 broadcast-hid-discovery.nse
-rw-r--r-- 1 root root 14655 Oct 6 2022 broadcast-igmp-discovery.nse
-rw-r--r-- 1 root root 3184 Oct 6 2022 broadcast-jenkins-discover.nse
-rw-r--r-- 1 root root 10449 Oct 6 2022 broadcast-listener.nse

```

1. Authentication: Các script trong danh mục này được sử dụng để kiểm tra xác thực trên các hệ thống mạng.
2. Discovery: Các script trong danh mục này được sử dụng để phát hiện các máy chủ và thiết bị mạng trong một mạng.



3. Intrusive: Các script trong danh mục này thực hiện các hoạt động quét nâng cao để tìm kiếm các lỗ hổng bảo mật trên các hệ thống mạng.
4. Malware: Các script trong danh mục này được sử dụng để phát hiện và loại bỏ các phần mềm độc hại trên các máy tính.
5. Brute force: Các script trong danh mục này được sử dụng để thực hiện tấn công Brute-force để thử các mật khẩu đăng nhập.
6. Vulnerability: Các script trong danh mục này được sử dụng để phát hiện các lỗ hổng bảo mật trên các hệ thống mạng.
7. Web: Các script trong danh mục này được sử dụng để phát hiện các lỗ hổng bảo mật trên các ứng dụng web.
8. Exploit: Các script trong danh mục này được sử dụng để tấn công các lỗ hổng bảo mật được phát hiện bằng cách sử dụng các kỹ thuật Exploit.

-Nping: có thể làm được nhiều hơn so với ping ICMP đơn giản. Nó có thể thao tác gần như bất kỳ tham số và trường nào của các gói TCP, UDP, ICMP và nó có thể được sử dụng để Denial of Service attacks, route tracing.

#### 1. ICMP Mode:

**sudo nping --icmp -c 2 google.com**

```
(root@nampxhhe151338)~#
# sudo nping --icmp -c 2 google.com

Starting Nping 0.7.93 ( https://nmap.org/nping ) at 2023-05-03 09:38 EDT
SENT (0.0847s) ICMP [192.168.50.124 > 172.217.24.78 Echo request (type=8/code=0) id=38074 seq=1] IP [ttl=64 id=28322 iplen=28 ]
RCVD (0.1583s) ICMP [172.217.24.78 > 192.168.50.124 Echo reply (type=0/code=0) id=38074 seq=1] IP [ttl=57 id=0 iplen=28 ]
SENT (1.0873s) ICMP [192.168.50.124 > 172.217.24.78 Echo request (type=8/code=0) id=38074 seq=2] IP [ttl=64 id=28322 iplen=28 ]
RCVD (1.1551s) ICMP [172.217.24.78 > 192.168.50.124 Echo reply (type=0/code=0) id=38074 seq=2] IP [ttl=57 id=0 iplen=28 ]

Max rtt: 71.235ms | Min rtt: 67.188ms | Avg rtt: 69.211ms
Raw packets sent: 2 (56B) | Rcvd: 2 (92B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.19 seconds

(root@nampxhhe151338)~#
# sudo nping --icmp -c 2 vsec.com.vn

Starting Nping 0.7.93 ( https://nmap.org/nping ) at 2023-05-03 09:48 EDT
SENT (0.1921s) ICMP [192.168.50.124 > 61.28.229.72 Echo request (type=8/code=0) id=57311 seq=1] IP [ttl=64 id=59529 iplen=28 ]
SENT (1.1933s) ICMP [192.168.50.124 > 61.28.229.72 Echo request (type=8/code=0) id=57311 seq=2] IP [ttl=64 id=59529 iplen=28 ]

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 2 (56B) | Rcvd: 0 (0B) | Lost: 2 (100.00%)
Nping done: 1 IP address pinged in 2.24 seconds
```

## 2. TCP Mode:

**nping --tcp-connect -c 2 -p 80 google.com**

```
(root@nampxhhe151338)~[~]
# nping --tcp-connect -c 2 -p 80 vsec.com.vn

Starting Nping 0.7.93 ( https://nmap.org/nping ) at 2023-05-03 09:51 EDT
SENT (0.0111s) Starting TCP Handshake > vsec.com.vn:80 (61.28.229.72:80)
SENT (1.0208s) Starting TCP Handshake > vsec.com.vn:80 (61.28.229.72:80)

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
TCP connection attempts: 2 | Successful connections: 0 | Failed: 2 (100.00%)
Nping done: 1 IP address pinged in 2.02 seconds

(root@nampxhhe151338)~[~]
# nping --tcp-connect -c 2 -p 80 google.com

Starting Nping 0.7.93 ( https://nmap.org/nping ) at 2023-05-03 09:51 EDT
SENT (0.0097s) Starting TCP Handshake > google.com:80 (172.217.24.78:80)
RCVD (0.0740s) Handshake with google.com:80 (172.217.24.78:80) completed
SENT (1.0138s) Starting TCP Handshake > google.com:80 (172.217.24.78:80)
RCVD (1.0716s) Handshake with google.com:80 (172.217.24.78:80) completed

Max rtt: 64.394ms | Min rtt: 57.958ms | Avg rtt: 61.176ms
TCP connection attempts: 2 | Successful connections: 2 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 1.07 seconds

(root@nampxhhe151338)~[~]
# nping --tcp-connect -c 2 -p 443 google.com

Starting Nping 0.7.93 ( https://nmap.org/nping ) at 2023-05-03 09:51 EDT
SENT (0.0102s) Starting TCP Handshake > google.com:443 (172.217.24.78:443)
RCVD (0.0734s) Handshake with google.com:443 (172.217.24.78:443) completed
SENT (1.0166s) Starting TCP Handshake > google.com:443 (172.217.24.78:443)
RCVD (1.0811s) Handshake with google.com:443 (172.217.24.78:443) completed

Max rtt: 64.587ms | Min rtt: 63.263ms | Avg rtt: 63.925ms
TCP connection attempts: 2 | Successful connections: 2 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 1.08 seconds

(root@nampxhhe151338)~[~]
#
```

## 3. UDP Mode:

**sudo nping --udp -c 2 -p 5001 61.28.229.72**

(Sẽ gửi hai gói tin UDP đến địa chỉ IP **61.28.229.72** trên cổng 5001 và kiểm tra xem liệu thiết bị đó có thể nhận và xử lý các gói tin UDP này hay không)

```
(root@nampxhhe151338)~[~]
# sudo nping --udp -c 2 -p 5001 61.28.229.72

Starting Nping 0.7.93 ( https://nmap.org/nping ) at 2023-05-03 10:04 EDT
SENT (0.0492s) UDP 192.168.50.124:53 > 61.28.229.72:5001 ttl=64 id=60910 iplen=28
SENT (1.0504s) UDP 192.168.50.124:53 > 61.28.229.72:5001 ttl=64 id=60910 iplen=28

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 2 (56B) | Rcvd: 0 (0B) | Lost: 2 (100.00%)
Nping done: 1 IP address pinged in 2.08 seconds
```

## -Hping:

1. công cụ hping được sử dụng như một plugin để thực hiện các cuộc tấn công mạng và kiểm tra bảo mật mạng. Hping trong Nmap có một số tính năng như:

2. Tạo gói tin TCP/IP với các thông số tùy chỉnh như địa chỉ nguồn, địa chỉ đích, cổng đích, số lượng gói tin, thời gian giữa các gói tin và nội dung dữ liệu.
3. Kiểm tra tính khả dụng của một máy chủ hoặc mạng bằng cách gửi các gói tin ICMP và TCP.
4. Phát hiện các lỗ hổng bảo mật trong hệ thống mạng bằng cách tạo ra các gói tin độc hại hoặc giả mạo để thực hiện các cuộc tấn công như SYN flood, UDP flood hoặc ICMP flood.
5. Kiểm tra tính chính xác của các bộ lọc mạng bằng cách gửi các gói tin với các tham số tùy chỉnh và quan sát phản hồi từ máy chủ mạng.

	Nping	Hping
Mục đích sử dụng	Sử dụng để kiểm tra tính khả dụng của một máy chủ hoặc mạng bằng cách gửi các gói tin ICMP hoặc TCP đến các địa chỉ IP cụ thể.	Sử dụng để kiểm tra bảo mật mạng bằng cách tạo ra các gói tin TCP/IP và tấn công vào các máy chủ mạng.
Cú pháp lệnh:	Để sử dụng Nping, bạn cần chỉ định địa chỉ IP và loại gói tin để gửi	Hping cung cấp nhiều tùy chọn để tùy chỉnh gói tin.
Tính năng:	Nó cũng có khả năng phát hiện các lỗ hổng bảo mật trong hệ thống mạng.	Có thể tạo ra các gói tin TCP/IP với các thông số tùy chỉnh, cho phép tấn công mạng một cách hiệu quả.

