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:

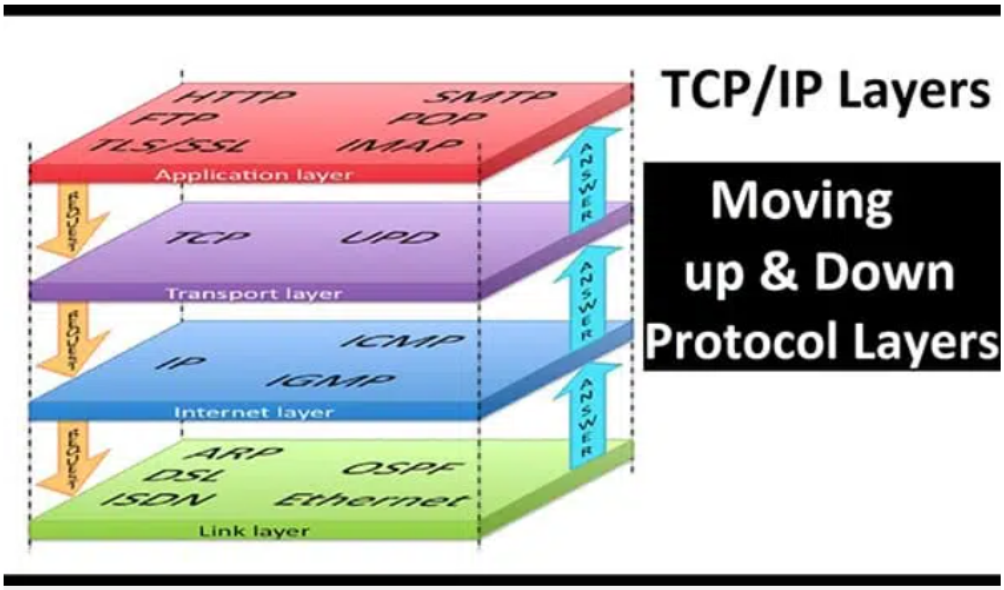
    - Tcpdump: là một công cụ dòng lệnh để bắt và phân tích các gói tin trên mạng.

      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

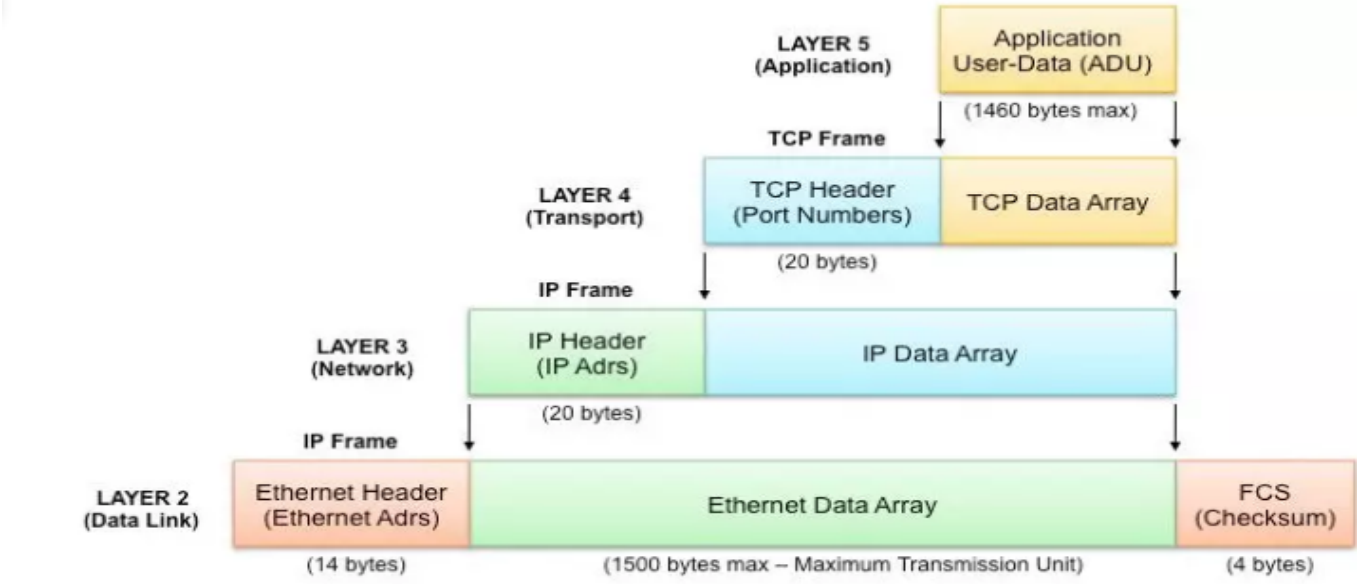


Mô hình phân tầng của TCP/IP

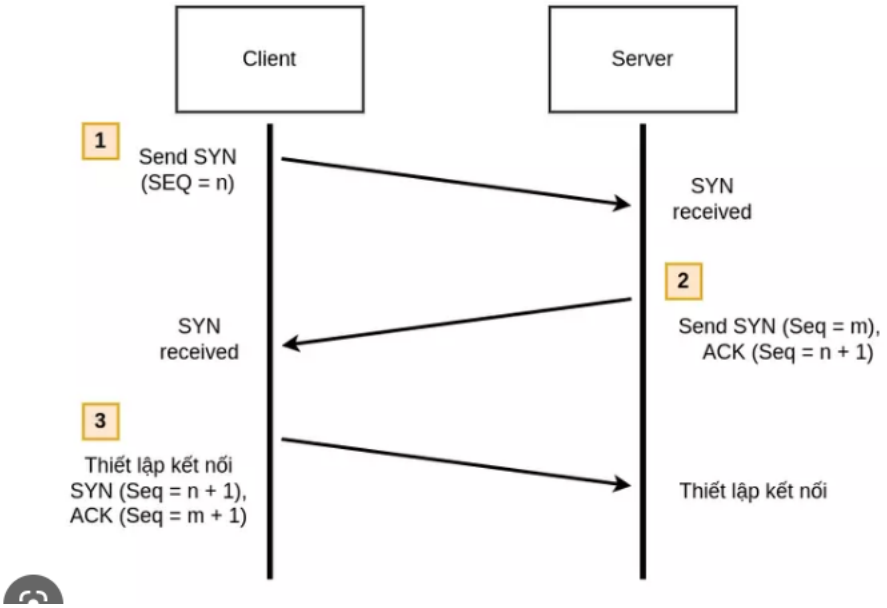
1. Mô hình phân tầng TCP/IP, các giao thức trên từng tầng

- **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 ko nhận được gói tin thì sẽ được gửi lại) và User Datagram Protocol (UDP, nó giống với TCP, tuy nhiên nó ko 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)

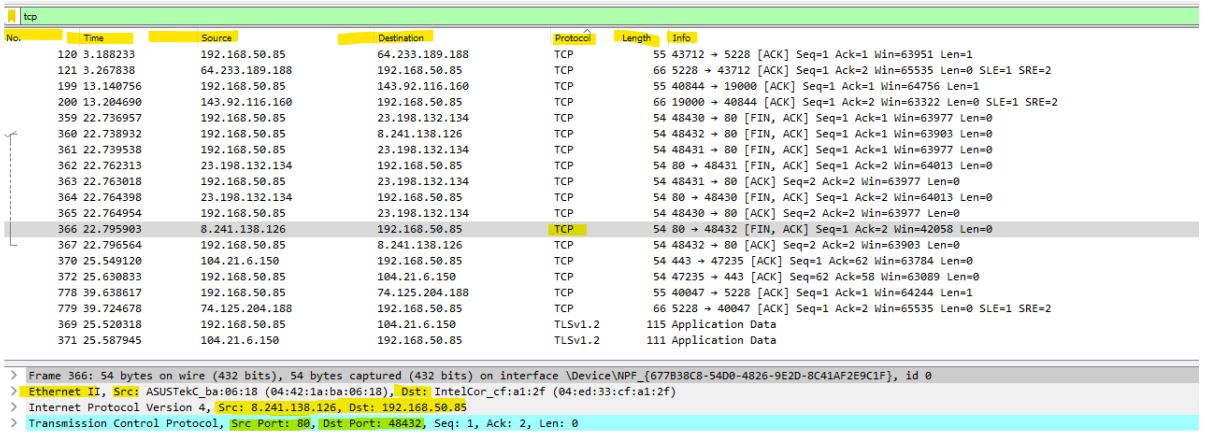
Sau khi thiết bị A nhận được phản hồi SYN-ACK từ thiết bị B, nó sẽ gửi một thông điệp xác nhận (ACK) đến thiết bị B để hoàn tất quy trình thiết lập kết nối. Gói tin ACK này chứa số thứ tự của thiết bị A (ACK), và số thứ tự của thiết bị B mà nó đã nhận được (ACK).

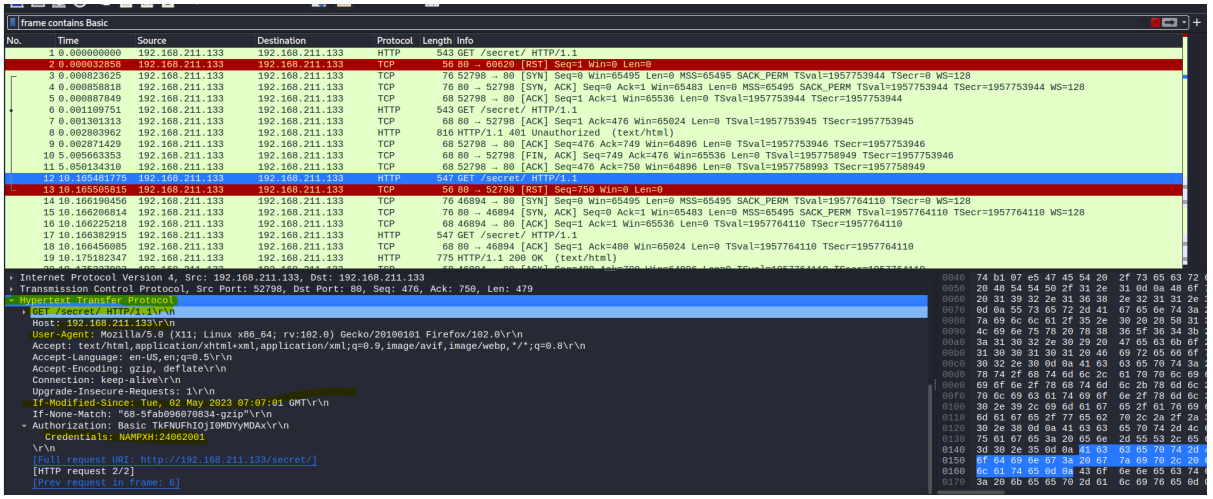
=> Sau khi quá trình bắt tay ba bước hoàn tất, kết nối giữa hai thiết bị sẽ được thiết lập và dữ liệu có thể được truyền tải giữa chúng. Nếu trong quá trình này có bất kỳ lỗi nào xảy ra hoặc thiết bị

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:** 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)
```

```
┌──(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

┌──(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

┌──(root㉿nampxhhe151338)-[~]
└─#
```

- Quét mạng và xác định các dịch vụ đang chạy trên các thiết bị: **nmap -sS -sV -O <target>**

```
┌──(root㉿nampxhhe151338)-[~]
└─# nmap -sS -sV -O 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 22:21 EDT
Nmap scan report for RT-AX55-0618 (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
49152/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=7.93%E=4%D=5/2%OT=80%CT=1%CU=40312%PV=Y%DS=1%DC=D%G=Y%M=04421A%TM
OS:=6451C5EF%P=x86_64-pc-linux-gnu)SEQ(SP=10A%GCD=1%ISR=10C%TI=Z%CI=I%TS=A)
OS:SEQ(SP=10A%GCD=1%ISR=10C%TI=Z%II=I%TS=A)SEQ(SP=10A%GCD=1%ISR=10C%TI=Z%CI
OS:=I%II=I%TS=A)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST
OS:11NW5%O5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=
OS:7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW5%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=
OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=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/teradataordbms?
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Nmap NSE cho phép người dùng tạo hoặc chạy các script để thực hiện các hoạt động khai thác khác nhau. Có nhiều script lắm.

```
┌──(root㉿nampxhhe151338)-[~]
└─# 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  7001 Oct  6  2022 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 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 amqp-info.nse
-rw-r--r-- 1 root root 15024 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 bitcoinrpc-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  3866 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-discoveryd.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
```

- Một số danh mục chính của 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.

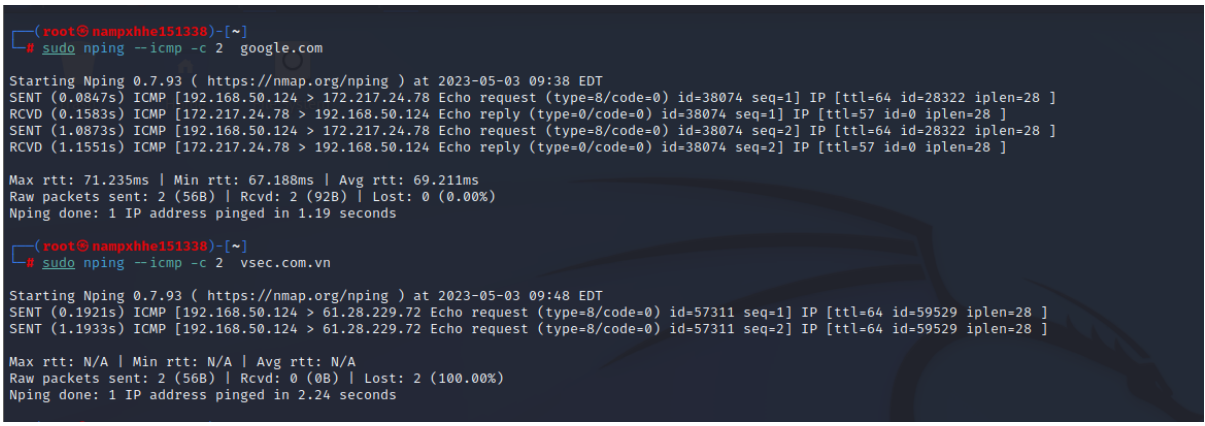
7. Web: Các script trong danh mục này được sử dụng để phát hiện các lỗ hổng bảo mật trên các ứng dụng web.

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.

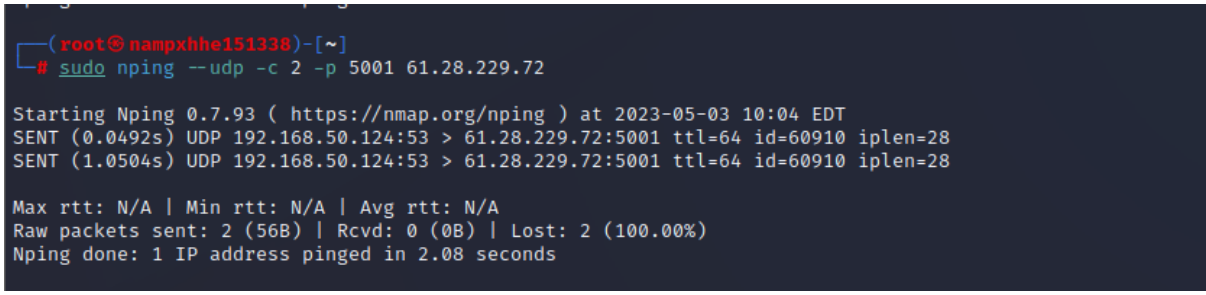
1. ICMP Mode:

   sudo nping --icmp -c 2 google.com



2. TCP Mode:
   nping --tcp-connect -c 2 -p 80 google.com

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**)**



-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.