

Bài Thực hành 1A

Bài 1

1. Netstat

Chức năng: Netstat (Network Statistics) là công cụ dòng lệnh có sẵn trên Windows, dùng để hiển thị thông tin về các kết nối mạng, bảng định tuyến, thống kê giao thức mạng TCP/IP.

Cách sử dụng: Thực hiện trong cmd (Command Prompt). Một số tham số phổ biến:

`netstat /?` : Hiển thị hướng dẫn sử dụng.

`netstat` : Hiển thị các kết nối TCP/IP đang hoạt động.

`netstat -a` : Hiển thị tất cả kết nối và các cổng đang lắng nghe.

`netstat -n` : Hiển thị địa chỉ IP thay vì tên miền.

`netstat -o` : Hiển thị ID tiến trình (PID) của mỗi kết nối.

`netstat -b` : Hiển thị tên chương trình đang tạo kết nối (cần quyền Admin).

Thực hiện:

`netstat -an` : Hiển thị tất cả kết nối đang mở với PID.

```
netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 0 192.168.211.234.53455 162.159.36.1.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53446 162.159.36.1.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53438 20.189.173.2.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53437 52.111.240.8.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53431 52.111.240.8.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53424 104.208.16.88.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53413 198.169.1.1.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53349 162.159.46.1.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53348 162.159.46.1.443 ESTABLISHED
tcp4 0 0 192.168.211.234.53345 185.199.110.133.443 ESTABLISHED
tcp4 0 0 127.0.0.1.631 *,* LISTEN
tcp6 0 0 ::1.631 *,* LISTEN
tcp4 0 0 192.168.211.234.52263 17.57.145.135.5223 ESTABLISHED
tcp4 0 0 192.168.211.234.52078 35.174.127.31.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51463 49.213.95.31.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51353 157.240.7.50.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51327 57.144.152.141.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51326 157.240.7.2.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51325 57.144.152.141.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51319 35.186.236.207.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51318 57.144.152.141.443 ESTABLISHED
tcp4 0 0 127.0.2.3.53 *,* LISTEN
tcp4 0 0 127.0.2.2.53 *,* LISTEN
tcp6 0 0 *.51261 *,* LISTEN
tcp4 0 0 *.51261 *,* LISTEN
tcp4 0 0 192.168.211.234.51255 20.243.74.193.443 ESTABLISHED
tcp4 0 0 192.168.211.234.51254 20.197.71.89.443 ESTABLISHED
tcp6 0 0 *.5000 *,* LISTEN
```

2. TCPView

Chức năng: TCPView là công cụ giao diện đồ họa của Microsoft (Sysinternals) dùng để hiển thị chi tiết các kết nối TCP và UDP theo thời gian thực, bao gồm cả tên tiến trình.

Cách sử dụng:

- Tải từ link chính thức: <https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview>
- Giải nén và chạy file TCPView.exe (không cần cài đặt).
- Giao diện liệt kê danh sách các tiến trình, địa chỉ IP, cổng, trạng thái kết nối (Established, Listening,...).

Điểm mạnh:

- Giao diện trực quan.
- Có thể kết thúc tiến trình hoặc đóng kết nối ngay trên giao diện.
- Xem nhanh quá trình kết nối theo thời gian thực.

Process Name	Process ID	Protocol	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets
svchost.exe	1136	TCP	LAPTOP-1D8FE6IP	135	0.0.0.0	0	22.1.2023.23:26:46	RpcEptMapper		
System	4	TCP	192.168.1.6	139	0.0.0.0	0	28.1.2023.21:41:57	System		
expressvpn.exe	5280	TCP	127.0.0.1	2015	0.0.0.0	0	22.1.2023.23:26:51	expressvpn.exe		
svchost.exe	7656	TCP	LAPTOP-1D8FE6IP	5040	0.0.0.0	0	28.1.2023.21:41:52	CDPSvc		
svchost.exe	10356	UDPv6	fe80:2d44:5301:8f68:778	1900	*	0	28.1.2023.21:41:54	SSDPSRV		
lsass.exe	964	TCP	LAPTOP-1D8FE6IP	49664	0.0.0.0	0	22.1.2023.23:26:46	lsass.exe		
wininit.exe	812	TCP	LAPTOP-1D8FE6IP	49665	0.0.0.0	0	22.1.2023.23:26:46	wininit.exe		
svchost.exe	1776	TCP	LAPTOP-1D8FE6IP	49666	0.0.0.0	0	22.1.2023.23:26:46	Schedule		
spoolsv.exe	3612	TCP	LAPTOP-1D8FE6IP	49667	0.0.0.0	0	22.1.2023.23:26:47	Eventlog		
services.exe	4200	TCP	LAPTOP-1D8FE6IP	49668	0.0.0.0	0	22.1.2023.23:26:47	Spooler		
msedge.exe	952	TCP	LAPTOP-1D8FE6IP	49670	0.0.0.0	0	22.1.2023.23:26:52	services.exe		
msedge.exe	6364	UDPv6	⋮	5353	*	0	28.1.2023.21:57:29	msedge.exe		
svchost.exe	2512	UDPv6	⋮	5353	*	0	28.1.2023.21:41:57	Dnscache		
ExpressVPNNotificationService.exe	2420	TCP	127.0.0.1	52155	0.0.0.0	0	24.1.2023.18:40:54	ExpressVPNNotificationService.exe		
svchost.exe	2512	UDPv6	⋮	5355	*	0	28.1.2023.21:41:57	Dnscache		
svchost.exe	2512	UDPv6	⋮	49214	*	0	28.1.2023.21:53:15	Dnscache		
svchost.exe	2512	UDPv6	⋮	50440	*	0	28.1.2023.22:02:47	Dnscache		
svchost.exe	2512	UDPv6	⋮	54692	*	0	28.1.2023.22:05:04	Dnscache		
svchost.exe	10356	UDPv6	fe80:2d44:5301:8f68:778	60973	*	0	28.1.2023.21:41:54	SSDPSRV		
svchost.exe	10356	UDPv6	⋮	60974	*	0	28.1.2023.21:41:54	SSDPSRV		
svchost.exe	2512	UDPv6	⋮	63188	*	0	28.1.2023.22:04:11	Dnscache		
svchost.exe	2512	UDPv6	⋮	64858	*	0	28.1.2023.22:05:04	Dnscache		
System	4	TCP	LAPTOP-1D8FE6IP	445	0.0.0.0	0	22.1.2023.23:26:49	System		
svchost.exe	1136	TCPv6	LAPTOP-1D8FE6IP	135	⋮	0	22.1.2023.23:26:46	RpcEptMapper		
System	4	TCPv6	LAPTOP-1D8FE6IP	445	⋮	0	22.1.2023.23:26:49	System		
lsass.exe	964	TCPv6	LAPTOP-1D8FE6IP	49664	⋮	0	22.1.2023.23:26:46	lsass.exe		
wininit.exe	812	TCPv6	LAPTOP-1D8FE6IP	49665	⋮	0	22.1.2023.23:26:46	wininit.exe		
svchost.exe	1776	TCPv6	LAPTOP-1D8FE6IP	49666	⋮	0	22.1.2023.23:26:46	Schedule		
spoolsv.exe	3612	TCPv6	LAPTOP-1D8FE6IP	49667	⋮	0	22.1.2023.23:26:47	Eventlog		
services.exe	4200	TCPv6	LAPTOP-1D8FE6IP	49668	⋮	0	22.1.2023.23:26:47	Spooler		
jhj_service.exe	5544	TCPv6	LAPTOP-1D8FE6IP	49669	⋮	0	22.1.2023.23:26:48	jhj_service		
services.exe	952	TCPv6	LAPTOP-1D8FE6IP	49670	⋮	0	22.1.2023.23:26:52	services.exe		
svchost.exe	10788	UDP	LAPTOP-1D8FE6IP	123	*	0	28.1.2023.21:42:38	W32Time		
System	4	UDP	192.168.1.6	137	*	0	28.1.2023.21:41:57	System		
System	4	UDP	192.168.1.6	138	*	0	28.1.2023.21:41:57	System		

3. Process Explorer

Chức năng: Process Explorer là công cụ thay thế Task Manager nâng cao, hiển thị chi tiết các tiến trình đang chạy, bao gồm:

- Cấu trúc cây tiến trình.
- Tài nguyên (CPU, RAM, GPU) mà tiến trình sử dụng.
- Thư viện (DLL) mà tiến trình gọi.
- Các kết nối mạng mà tiến trình sử dụng.

Cách sử dụng:

- Tải từ Microsoft Sysinternals: <https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer>
- Chạy file procexp.exe.

Chức năng:

- Tìm tiến trình mở một file hoặc cổng mạng cụ thể.
- Kill tiến trình hoặc Suspend (tạm dừng).
- Tra cứu thông tin chi tiết về tiến trình, như nhà phát triển, đường dẫn file chạy,...

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	User Name	Protection	Integrity
System	Suspended	152 K	222,150 K	4	System	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
System Idle Process	0.00	60 K	8 K	0	System Idle Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
System	0.36	258 K	30,680 K	4	System	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
smss.exe	0.62	0 K	0 K	n/a	Hardware Interrupts and DPCs	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
csrss.exe	1.152 K	1,172 K	1,172 K	1004	Windows Session Manager	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
Memory Compression	1.480 K	59,444 K	4,404 K	4404	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
smss.exe	2.972 K	4,732 K	4,732 K	1112	Windows Start-Up Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
csrss.exe	1.620 K	4,908 K	1,224 K	1224	Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
services.exe	10,392 K	13,776 K	1,300 K	1300	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
svchost.exe	31,396 K	47,908 K	1444 K	1444	WMI Surrogate	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
WsmProvSE.exe	55,800 K	70,512 K	5092 K	5092	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
svchost.exe	4,952 K	10,576 K	1,1420 K	11420	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	22,132 K	32,864 K	1,5040 K	15040	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	7,548 K	26,460 K	14472 K	14472	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	19,420 K	50,854 K	14776 K	14776	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
SettingSyncHost.exe	11,488 K	7,736 K	10344 K	10344	Host Process for Setting Synchron...	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
explorer.exe	153,452 K	187,060 K	13448 K	13448	Windows Explorer	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	8,896 K	27,476 K	1,5368 K	15368	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
svchost.exe	16,032 K	23,108 K	1,7412 K	17412	COM Surrogate	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
YourPhoneServer.exe	68,896 K	78,544 K	1,8612 K	18612	Sink to receive asynchronous call...	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
unsecapp.exe	1,956 K	8,056 K	1,8632 K	18632	Sink to receive asynchronous call...	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
FileCoAuth.exe	8,976 K	24,892 K	24296 K	24296	Microsoft OneDriveFile Co-Author...	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
BackgroundTaskHost.exe	15,112 K	13,844 K	2,8584 K	28584	Background Task Host	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
ghcnth.exe	3,944 K	9,584 K	2,7892 K	27892	ghcnth Module	Intel Corporation	PAVEL7760\Pavel	Medium	Medium
unsecapp.exe	1,856 K	8,492 K	2,8052 K	28052	Sink to receive asynchronous call...	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
ApplicationFrameHost.exe	26,236 K	38,204 K	4,092 K	4092	Application Frame Host	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
Outlook.exe	Suspended	38,548 K	3,044 K	30396	Microsoft Outlook	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	3,872 K	16,156 K	22344	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
HiTar.exe	Suspended	23,960 K	22,464 K	26152	Microsoft Outlook Communications	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	6,824 K	15,508 K	14964	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
WinStoreApp.exe	Suspended	82,220 K	3,032 K	29176	Store	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
GameBar.exe	Suspended	43,756 K	4,472 K	37264	Xbox Game Bar	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
GameBarTServer.exe	Suspended	3,304 K	8,420 K	37564	Xbox Game Bar Full Trust COM Se...	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	3,276 K	10,240 K	38056	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
Microsoft Photos.exe	Suspended	71,796 K	50,848 K	36408	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	5,760 K	16,212 K	12380	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	2,360 K	7,340 K	34208	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
WsmProvSE.exe	Suspended	4,680 K	10,488 K	35364	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
WsmProvSE.exe	Suspended	4,352 K	10,784 K	41212	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
Calculator.exe	Suspended	49,888 K	57,324 K	45940	Calculator	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	1,808 K	5,400 K	29040	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
YourPhone.exe	Suspended	75,540 K	79,492 K	6480	YourPhone	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	6,816 K	20,800 K	37464	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
WsmProvSE.exe	Suspended	15,336 K	27,276 K	17772	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	System	System
RuntimeBroker.exe	Suspended	10,976 K	35,148 K	45402	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
GoVpnApp.exe	Suspended	50,428 K	62,452 K	45000	GoVpnApp	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium
RuntimeBroker.exe	Suspended	708,112 K	766,768 K	17600	Runtime Broker	Microsoft Corporation	PAVEL7760\Pavel	Medium	Medium

Bài 2

Bước 1: Kiểm tra kết nối cơ bản

ping www.certifiedhacker.com

Chức năng:

- Gửi các gói ICMP tới địa chỉ đích để kiểm tra độ phản hồi (latency).
- Hiển thị số lượng gói gửi, nhận, mất, và thời gian phản hồi trung bình.

```

base 13:53:38
ping www.certifiedhacker.com
PING certifiedhacker.com (162.241.216.11): 56 data bytes
64 bytes from 162.241.216.11: icmp_seq=0 ttl=48 time=214.314 ms
64 bytes from 162.241.216.11: icmp_seq=1 ttl=48 time=212.936 ms
64 bytes from 162.241.216.11: icmp_seq=2 ttl=48 time=212.354 ms
64 bytes from 162.241.216.11: icmp_seq=3 ttl=48 time=212.505 ms
64 bytes from 162.241.216.11: icmp_seq=4 ttl=48 time=212.431 ms
64 bytes from 162.241.216.11: icmp_seq=5 ttl=48 time=212.648 ms
64 bytes from 162.241.216.11: icmp_seq=6 ttl=48 time=269.285 ms
64 bytes from 162.241.216.11: icmp_seq=7 ttl=48 time=215.312 ms
64 bytes from 162.241.216.11: icmp_seq=8 ttl=48 time=212.689 ms

```

Nhận xét:

- Nếu ping thành công → mạng đích hoạt động bình thường.
- Nếu timeout hoặc Request Timed Out → có thể bị chặn ICMP hoặc lỗi mạng.
- Địa chỉ IP trả về giúp xác định server đang hosting website (có thể dùng để kiểm tra geolocation hoặc cấu hình firewall).

Bước 2: Tìm kích thước tối đa của gói tin (MTU - Maximum Transmission Unit)

ping www.certifiedhacker.com -f -l 1500

Chức năng:

- Thử gửi gói tin có kích thước 1500 bytes với cờ -f (không cho phân mảnh).
- Dùng để xác định giới hạn MTU (Maximum Transmission Unit) của kết nối mạng.
- Nếu gói tin quá lớn, hệ thống sẽ báo lỗi “Packet needs to be fragmented but DF set”.

```
Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Nhận xét:

- Nếu gói tin bị lỗi phân mảnh, bạn sẽ thấy thông báo "Packet needs to be fragmented" → gói quá lớn.
- Tiếp tục thử với giá trị nhỏ hơn (ví dụ -l 1400, -l 1472) để tìm ra ngưỡng tối đa không bị lỗi.
- MTU chuẩn của đa số mạng Internet là 1500 bytes, trong đó phần dữ liệu có thể là 1472 bytes (1500 - 28 bytes header IP + ICMP).

Bước 3: Gửi gói tin với TTL cụ thể

ping www.certifiedhacker.com -i 3

Chức năng:

- Gửi gói tin với TTL (Time To Live) = 3.
- Giới hạn số hop (router) mà gói tin được phép đi qua.

```
ping www.certifiedhacker.com -i 3
PING certifiedhacker.com (162.241.216.11): 56 data bytes
64 bytes from 162.241.216.11: icmp_seq=0 ttl=48 time=202.177 ms
64 bytes from 162.241.216.11: icmp_seq=1 ttl=48 time=205.042 ms
64 bytes from 162.241.216.11: icmp_seq=2 ttl=48 time=206.480 ms
```

Nhận xét:

- Nếu TTL < số hop tới đích → sẽ timeout tại hop thứ 3.
- Có thể dùng để xác định từng router trung gian.

Bước 4: Theo dõi đường đi gói tin

tracert www.certifiedhacker.com

Chức năng:

- Hiện thị danh sách các router mà gói tin đi qua từ máy bạn tới đích.
- Mỗi dòng thể hiện 1 hop.

```
Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1      1 ms      1 ms      1 ms  192.168.1.1
 2      5 ms      3 ms      4 ms  static.vnpt.vn [123.29.12.52]
 3     33 ms     32 ms     32 ms  static.vnpt.vn [113.171.44.225]
 4     43 ms     31 ms     32 ms  static.vnpt.vn [113.171.46.5]
 5     37 ms     32 ms     33 ms  static.vnpt.vn [113.171.143.26]
 6     34 ms     31 ms     32 ms  static.vnpt.vn [113.171.31.33]
 7      *        *        30 ms  ix-ge-400-0-0-27.qcore2.hk2-hongkong.as6453.net [180.87.168.110]
 8      *        30 ms     31 ms  if-bundle-5-2.qcore1.hk2-hongkong.as6453.net [180.87.168.96]
 9     34 ms     36 ms     31 ms  if-ae-65-2.tcore1.hk2-hongkong.as6453.net [180.87.168.114]
10     29 ms     32 ms     32 ms  ae-15.a00.chwahk03.hk.bb.gin.ntt.net [129.250.8.25]
11      *        *        *      Request timed out.
12      *        *        *      Request timed out.
13      *        78 ms     *      ae-1.r33.tokyjp05.jp.bb.gin.ntt.net [129.250.5.54]
14    188 ms    191 ms    189 ms  ae-4.r27.lsanca07.us.bb.gin.ntt.net [129.250.3.193]
15    186 ms    183 ms    184 ms  ae-3.a03.lsanca07.us.bb.gin.ntt.net [129.250.3.245]
16    188 ms    185 ms    188 ms  ce-3-0-1.a03.lsanca07.us.ce.gin.ntt.net [168.143.228.173]
17    201 ms    200 ms    209 ms  162-215-195-144.unifiedlayer.com [162.215.195.144]
18    208 ms    208 ms    207 ms  69-195-64-111.unifiedlayer.com [69.195.64.111]
19    200 ms    203 ms    204 ms  po97.prv-leaf1b.net.unifiedlayer.com [162.144.240.131]
20    208 ms    202 ms    204 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.
```

Nhận xét:

- Dùng để phân tích tuyến đường mạng, xác định chậm trễ hoặc sự cố tại hop nào.
- Rất hữu ích trong việc khắc phục sự cố kết nối mạng.

Bước 5: Kiểm tra phản hồi theo TTL

```
ping www.certifiedhacker.com -i 2 -n 1
```

```
ping www.certifiedhacker.com -i 3 -n 1
```

```
ping www.certifiedhacker.com -i 4 -n 1
```

Chức năng:

- Gửi 1 gói tin với TTL lần lượt là 2, 3, 4.
- Quan sát phản hồi để xác định tại hop nào gói tới được.

Nhận xét:

- Dùng TTL tăng dần giống như tracer, nhưng có thể kiểm soát từng bước.
- Có thể xác định hop nào là router cuối cùng trước khi đến đích.

```
PING certifiedhacker.com (162.241.216.11): 56 data bytes
64 bytes from 162.241.216.11: icmp_seq=0 ttl=48 time=296.172 ms

--- certifiedhacker.com ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 296.172/296.172/296.172/nan ms
```



```
ping -c 1 -i 3 www.certifiedhacker.com

PING certifiedhacker.com (162.241.216.11): 56 data bytes
64 bytes from 162.241.216.11: icmp_seq=0 ttl=48 time=211.259 ms

--- certifiedhacker.com ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 211.259/211.259/211.259/0.000 ms

ping -c 1 -i 4 www.certifiedhacker.com

PING certifiedhacker.com (162.241.216.11): 56 data bytes
64 bytes from 162.241.216.11: icmp_seq=0 ttl=48 time=225.303 ms

--- certifiedhacker.com ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 225.303/225.303/225.303/nan ms
```

Bước 6: Truy vấn DNS

Nslookup

Chức năng:

- Truy cập công cụ dòng lệnh để tra cứu thông tin DNS.
- Hỗ trợ nhiều loại truy vấn: A, CNAME, MX, NS,...

```
Nslookup
> www.certifiedhacker.com
Server:      127.0.2.2
Address:     127.0.2.2#53

** server can't find www.certifiedhacker.com: NXDOMAIN
>
```

Nhận xét:

- Công cụ mạnh để phân tích tên miền và DNS server.
- Có thể đổi DNS server truy vấn nếu cần.

Bước 7: Tra bản ghi A

set type=a

www.certifiedhacker.com

Chức năng:

- Truy vấn bản ghi A → trả về địa chỉ IPv4 của tên miền.

```
nslookup
> set type=A
> www.certifiedhacker.com
Server:          127.0.2.2
Address:         127.0.2.2#53

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Name:   certifiedhacker.com
Address: 162.241.216.11
```

Nhận xét:

- Biết được IP chính xác của server để sử dụng trong các truy vấn khác.
- Cần thiết khi cần chặn IP, kiểm tra geolocation hoặc dùng cho tường lửa.

Bước 8: Tra bản ghi CNAME

set type=cname

www.certifiedhacker.com

Chức năng:

- Truy vấn xem tên miền có trỏ đến một tên miền khác không.

```
nslookup -type=CNAME www.certifiedhacker.com

Server:          127.0.2.2
Address:         127.0.2.2#53

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.

Authoritative answers can be found from:
```

Nhận xét:

- Phát hiện các tên miền phụ, dịch vụ CDN, hoặc server redirect.
- Giúp hiểu kiến trúc phân phối tên miền.