

# 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	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets
svchost.exe	1136	LAPTOP-1DBFE6IP	135	0.0.0	0	22.1.2023 23:26:46	RpcEptMapper		
System	4	192.168.1.6	139	0.0.0	0	28.1.2023 21:41:57	System		
expressvpnd.exe	5280	127.0.1.1	2015	0.0.0	0	22.1.2023 23:26:51	expressvpnd.exe		
svchost.exe	7056	LAPTOP-1DBFE6IP	5040	0.0.0	0	28.1.2023 21:41:52	CDPSvc		
svchost.exe	10356	fe80:2d44:5301:8f68:778	1900	*		28.1.2023 21:41:54	SSDP_SRV		
lsass.exe	964	TCP	Listen	LAPTOP-1DBFE6IP	49664	0.0.0		22.1.2023 23:26:46	
wininit.exe	812	TCP	Listen	LAPTOP-1DBFE6IP	49665	0.0.0		22.1.2023 23:26:46	wininit.exe
svchost.exe	1776	TCP	Listen	LAPTOP-1DBFE6IP	49666	0.0.0		22.1.2023 23:26:46	Schedule
svchost.exe	3612	TCP	Listen	LAPTOP-1DBFE6IP	49667	0.0.0		22.1.2023 23:26:47	EventLog
spoolsv.exe	4200	TCP	Listen	LAPTOP-1DBFE6IP	49668	0.0.0		22.1.2023 23:26:47	Spooler
services.exe	952	TCP	Listen	LAPTOP-1DBFE6IP	49670	0.0.0		22.1.2023 23:26:52	services.exe
msedge.exe	6364	UDPv6			5353	*		28.1.2023 21:57:29	msedge.exe
svchost.exe	2512	UDPv6			5353	*		28.1.2023 21:41:57	DnsCache
ExpressVPNNotification...	2420	TCP	Listen	127.0.0.1	52155	0.0.0	0	24.1.2023 18:04:04	ExpressVPNNotificationService...
svchost.exe	2512	UDPv6			5355	*		28.1.2023 21:41:57	DnsCache
svchost.exe	2512	UDPv6			49214	*		28.1.2023 21:53:15	DnsCache
svchost.exe	2512	UDPv6			50440	*		28.1.2023 22:02:47	DnsCache
svchost.exe	2512	UDPv6			54692	*		28.1.2023 22:05:04	DnsCache
svchost.exe	10356	UDPv6			60973	*		28.1.2023 21:41:54	SSDP_SRV
svchost.exe	10356	UDPv6	:1		60974	*		28.1.2023 21:41:54	SSDP_SRV
svchost.exe	2512	UDPv6			63188	*		28.1.2023 22:04:11	DnsCache
svchost.exe	2512	UDPv6			64858	*		28.1.2023 22:05:04	DnsCache
System	4	TCP	Listen	LAPTOP-1DBFE6IP	445	0.0.0	0	22.1.2023 23:26:49	System
svchost.exe	1136	TCPIP	Listen	LAPTOP-1DBFE6IP	135	:	0	22.1.2023 23:26:46	RpcEptMapper
System	4	TCPIP	Listen	LAPTOP-1DBFE6IP	445	:	0	22.1.2023 23:26:49	System
lsass.exe	964	TCPIP	Listen	LAPTOP-1DBFE6IP	49664	:	0	22.1.2023 23:26:46	lsass.exe
wininit.exe	812	TCPIP	Listen	LAPTOP-1DBFE6IP	49665	:	0	22.1.2023 23:26:46	wininit.exe
svchost.exe	1776	TCPIP	Listen	LAPTOP-1DBFE6IP	49666	:	0	22.1.2023 23:26:46	Schedule
svchost.exe	3612	TCPIP	Listen	LAPTOP-1DBFE6IP	49667	:	0	22.1.2023 23:26:47	EventLog
spoolsv.exe	4200	TCPIP	Listen	LAPTOP-1DBFE6IP	49668	:	0	22.1.2023 23:26:47	Spooler
jh_service.exe	5544	TCPIP	Listen	LAPTOP-1DBFE6IP	49669	:	0	22.1.2023 23:26:48	jh_service
services.exe	952	TCPIP	Listen	LAPTOP-1DBFE6IP	49670	:	0	22.1.2023 23:26:52	services.exe
svchost.exe	10788	UDP			123	*		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 procepx.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	Select Column...	Company Name	User Name	Protection	Integrity
Secure System	Suspended	184 K	272,160 K	104			NT AUTHORITY\SYSTEM		System	
Regsvr		33,768 K	105,608 K	180			NT AUTHORITY\SYSTEM		System	
System Idle Process	96.05	60 K	8 K	0			NT AUTHORITY\SYSTEM		System	
System		224 K	224 K	4			NT AUTHORITY\SYSTEM		System	
Interrupts	0.62	0 K	0 K	n/a	Hardware Interrupts and DPCs	0 K				
Input.exe		1,182 K	1,172 K	1004	Windows Session Manager	490,384 K	Microsoft Corporation	NT AUTHORITY\SYSTEM	PaProtectedSigner	System
Memory Compression		1,460 K	59,444 K	4404			NT AUTHORITY\SYSTEM		System	
Power.exe	< 0.01	2,972 K	4,732 K	1112	Client Server Runtime Process	2,151,708,100 K	Microsoft Corporation	NT AUTHORITY\SYSTEM	PaProtectedSigner	System
Wininit.exe		1,620 K	4,908 K	1224	Windows Start-Up Application	2,151,747,656 K	Microsoft Corporation	NT AUTHORITY\SYSTEM	PaProtectedSigner	System
services.exe		10,392 K	13,776 K	1300	Services and Controller app	2,151,758,960 K	Microsoft Corporation	NT AUTHORITY\SYSTEM	PaProtectedSigner	System
svchost.exe		31,396 K	47,908 K	1444	Host Process for Windows Services	2,151,889,488 K	Microsoft Corporation	NT AUTHORITY\SYSTEM		System
WmiPrvSE.exe	< 0.01	55,800 K	70,512 K	5092	WMI Provider Host	2,151,862,200 K	Microsoft Corporation	NT AUTHORITY\SYSTEM		System
dhcpcsvc.exe		4,952 K	10,576 K	11420	COM Surrogate	2,152,824,084 K	Microsoft Corporation	NT AUTHORITY\SYSTEM		System
RuntimeBroker.exe		22,132 K	32,864 K	15248	Runtime Broker	2,151,921,376 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
RuntimeBroker.exe		7,648 K	26,460 K	14472	Runtime Broker	2,151,834,504 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
RuntimeBroker.exe		19,420 K	50,864 K	14776	Runtime Broker	2,152,000,048 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
SettingSyncHost.exe		11,488 K	7,736 K	10344	Host Process for Setting Synchronization	2,151,875,840 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
explorer.exe		153,452 K	187,060 K	13448	Windows Explorer	2,152,444,240 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
RuntimeBroker.exe		8,836 K	27,476 K	15658	Runtime Broker	2,151,887,612 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
dhcpcsvc.exe		16,032 K	23,108 K	17412	COM Surrogate	2,152,863,700 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
YourPhoneServer.exe	< 0.01	68,896 K	78,544 K	18612		2,152,456,612 K		PAVEL760\PAVEL	Medium	
Unsecapp.exe		1,956 K	8,056 K	18652	Sink to receive asynchronous call...	2,151,768,024 K	Microsoft Corporation	NT AUTHORITY\SYSTEM		System
FileCoAuth.exe		8,976 K	24,892 K	24296	Microsoft OneDrive File Co-Auth...	2,151,831,288 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
BackgroundTaskHost.exe		19,848 K	18,848 K	25256	Background Task Host	2,151,863,700 K	Microsoft Corporation	PAVEL760\PAVEL	AppContainer	
ghost11.exe		3,944 K	9,584 K	27892	ghost Module	2,151,768,444 K	Intel Corporation	PAVEL760\PAVEL	Medium	
ghost11.exe		1,850 K	8,492 K	29052	Service to receive asynchronous call...	2,151,767,000 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
ApplicationFrameHost.exe		26,236 K	36,204 K	4092	Application Frame Host	2,152,660,832 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
HDIconHost.exe	Suspended	58,548 K	3,044 K	30396		2,151,967,532 K	Microsoft Corporation	PAVEL760\PAVEL	AppContainer	
RuntimeBroker.exe		3,372 K	16,156 K	22344	Runtime Broker	2,151,768,268 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
Hitler.exe	Suspended	23,960 K	22,454 K	26152	Microsoft Outlook Communications	2,151,972,272 K	Microsoft Corporation	PAVEL760\PAVEL	AppContainer	
RuntimeBroker.exe		6,824 K	15,508 K	14964	Runtime Broker	2,151,836,700 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
WinStoreApp.exe	Suspended	82,220 K	3,032 K	29176	Store	5,299,200 K	Microsoft Corporation	PAVEL760\PAVEL	AppContainer	
GameBar.exe	Suspended	43,756 K	4,472 K	37264	Xbox Game Bar	2,152,238,504 K	Microsoft Corporation	PAVEL760\PAVEL	AppContainer	
GameBarITServer.exe		3,304 K	8,420 K	37964	Xbox Game Bar Full Trust COM Se...	2,151,807,992 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
RuntimeBroker.exe		3,276 K	10,240 K	38056	Runtime Broker	2,151,804,244 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
Microsoft.Photos.exe	Suspended	71,796 K	50,848 K	36408		5,279,880 K		PAVEL760\PAVEL	AppContainer	
RuntimeBroker.exe		5,760 K	16,212 K	12380	Runtime Broker	2,151,833,444 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
RuntimeBroker.exe		2,308 K	7,740 K	34208	Runtime Broker	2,151,777,200 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
WmiPrvSE.exe		4,680 K	10,488 K	35364	WMI Provider Host	75,160 K	Microsoft Corporation	NT AUTHORITY\NET...	System	
WmiPrvSE.exe		4,352 K	10,784 K	41212	WMI Provider Host	2,151,760,880 K	Microsoft Corporation	NT AUTHORITY\NET...	System	
Calculator.exe	Suspended	49,888 K	57,324 K	45940		4,771,832 K		PAVEL760\PAVEL	AppContainer	
RuntimeBroker.exe		1,808 K	5,480 K	29040	Runtime Broker	2,151,760,732 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
YourPhone.exe	Suspended	75,548 K	79,492 K	6480	YourPhone	5,282,680 K	Microsoft Corporation	PAVEL760\PAVEL	AppContainer	
RuntimeBroker.exe		6,816 K	20,900 K	37454	Runtime Broker	2,151,816,112 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
WmiPrvSE.exe		15,336 K	27,276 K	17772	WMI Provider Host	2,151,787,788 K	Microsoft Corporation	NT AUTHORITY\NET...	System	
RuntimeBroker.exe		70,976 K	35,148 K	45492	Runtime Broker	2,151,873,288 K	Microsoft Corporation	PAVEL760\PAVEL	Medium	
GpVpnApp.exe	Suspended	50,428 K	62,452 K	45000		4,764,768 K		PAVEL760\PAVEL	AppContainer	
ResourceHost.exe		206,152 K	206,152 K	37623	Resource Host	3,167,609,072 K	Microsoft Corporation	PAVEL760\PAVEL	AppContainer	

## Bài 2

### Bước 1: Kiểm tra kết nối cơ bản

ping [www.certifiedhacker.com](http://www.certifiedhacker.com)

```
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:**

- Thủ 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.

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](http://www.certifiedhacker.com)

## Chức năng:

- Hiển 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 tracert, 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](http://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](http://www.certifiedhacker.com)

### Chức năng:

- Truy vấn xem tên miền có trả 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.