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.

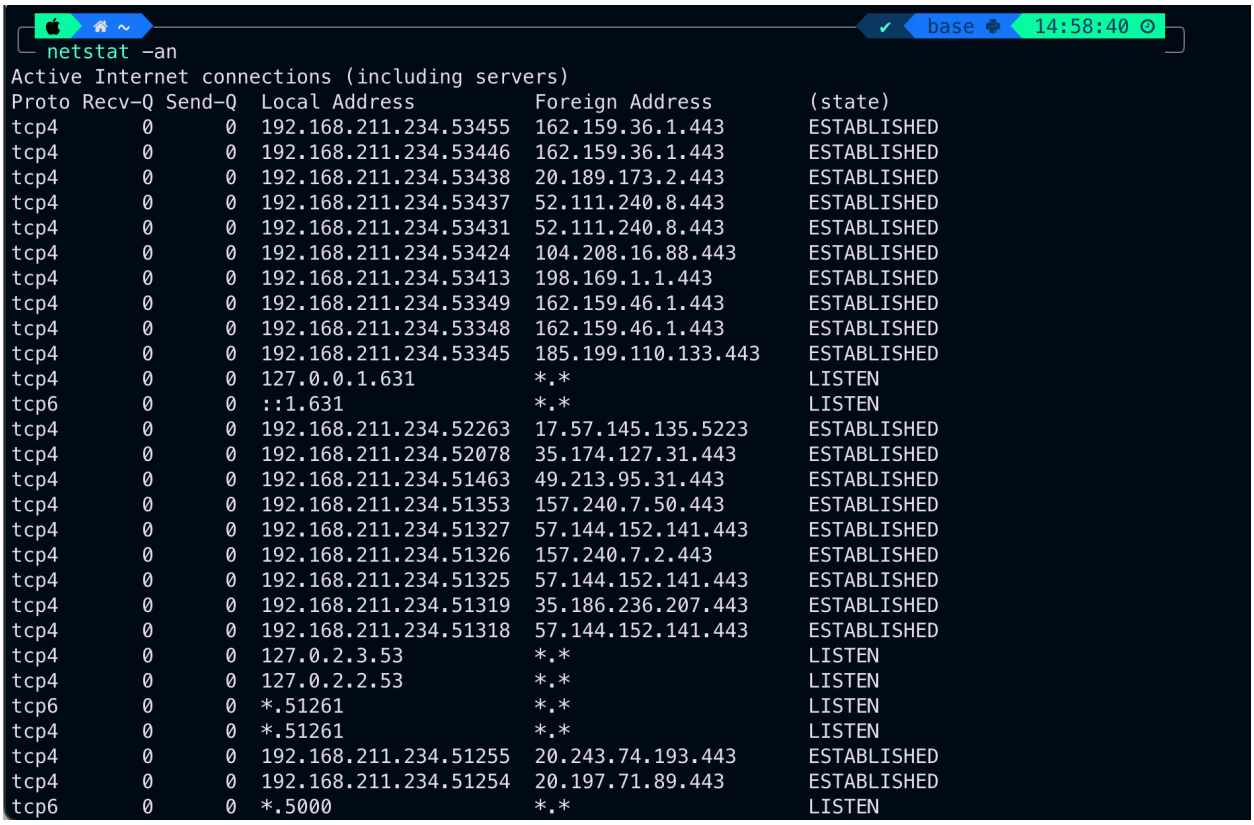
`netstat -n` : Hiển thị địa chỉ IP thay vì tên miền.

`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.



2. TCPView

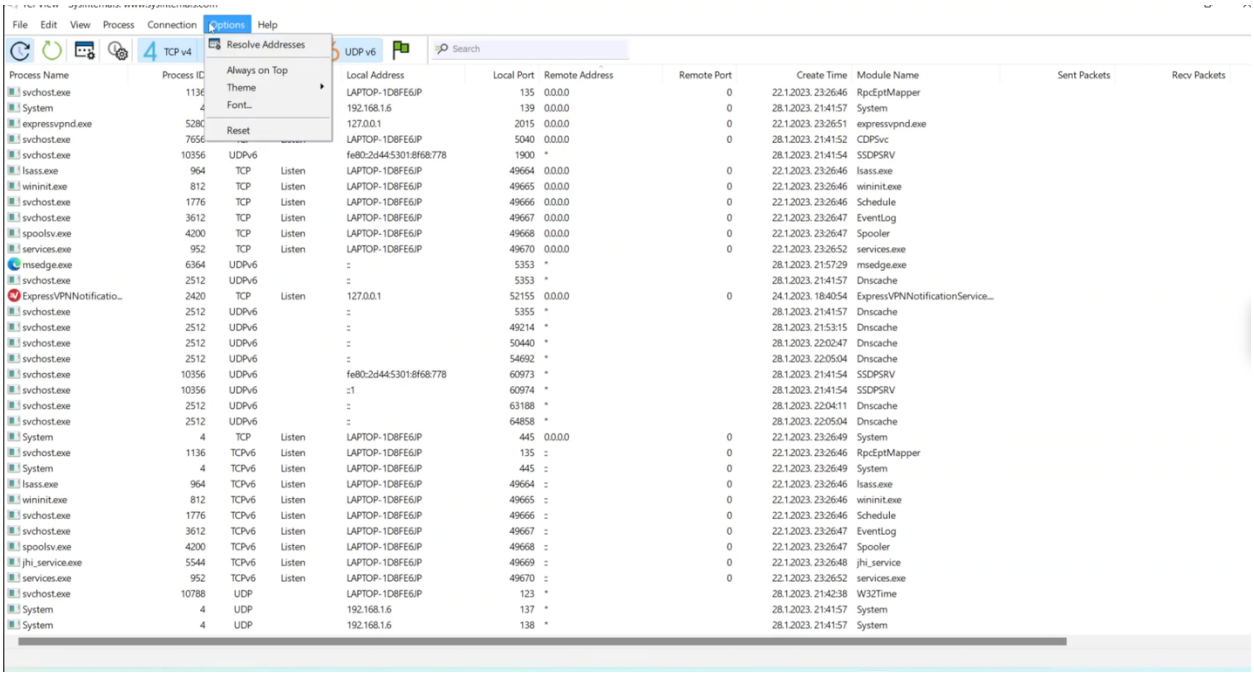
Chức năng: TCPView là công cụ giao diện đồ họa của Microsoft (Sysinternals) dùng để hiển thị chi tiết các kết nối TCP và UDP theo thời gian thực, bao gồm cả tên tiến trình.

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.



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:

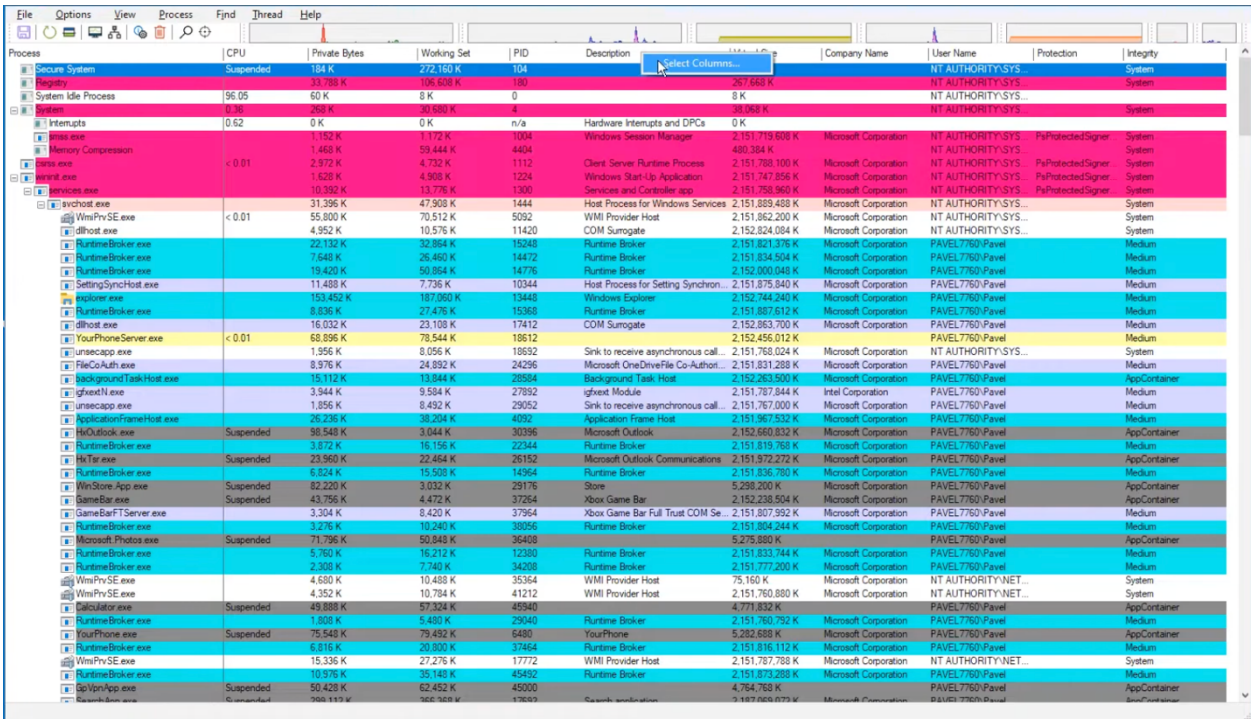
- Cấu trúc cây tiến trình.
- Tài nguyên (CPU, RAM, GPU) mà tiến trình sử dụng.
- Thư viện (DLL) mà tiến trình gọi.
- Các kết nối mạng mà tiến trình sử dụng.

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,…



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:

- 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                                                    64 ✘  base  14:32:46
> www.certiifiedhacker.com
Server:         127.0.2.2
Address:        127.0.2.2#53

** server can't find www.certiifiedhacker.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.