**TRƯỜNG ĐẠI HỌC BÁCH KHOA**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO MÔN HỌC**

**AN TOÀN HỆ THỐNG THÔNG TIN**

**GVHD : TS Nguyễn Tấn Khôi**

**SVTH : Lê Trọng Hiếu**

**MSSV : 102150274**

**Đà Nẵng, 4/2019**

**Ý KIẾN ĐÁNH GIÁ CỦA GIẢNG VIÊN**

# MỤC LỤC

[MỤC LỤC 1](#_Toc5809579)

[DANH SÁCH HÌNH ẢNH 2](#_Toc5809580)

[LAB 1: XEM THÔNG TIN MẠNG TRÊN HỆ ĐIỀU HÀNH WINDOW 4](#_Toc5809581)

[1.1 Chuẩn bị 4](#_Toc5809582)

[1.2 Lệnh ipconfig 4](#_Toc5809583)

[1.3 Lệnh ping 7](#_Toc5809584)

[1.4 Lệnh route 9](#_Toc5809585)

[1.5 Lệnh netstat 10](#_Toc5809586)

[1.6 Lệnh nslookup 14](#_Toc5809587)

[1.7 Lệnh net 14](#_Toc5809588)

[LAB 2. SỬ DỤNG CÔNG CỤ](#_Toc5809589)  [QUÉT & DÒ TÌM LỖ HỖNG TRÊN MẠNG 17](#_Toc5809590)

[2.1 Công cụ quét mạng NMAP 17](#_Toc5809591)

[LAB 3. SỬ DỤNG CÔNG CỤ SNORT 20](#_Toc5809592)

[3.1 Chuẩn bị 20](#_Toc5809593)

[3.2 Xem thông tin dịch vụ Snort 21](#_Toc5809594)

[3.3 Xem kết quả bắt gói tin 21](#_Toc5809595)

[LAB 3. THỰC HÀNH PHÂN TÍCH MÃ MÁY 25](#_Toc5809596)

[4.1 Công cụ Process Explorer 25](#_Toc5809597)

[4.2 Công cụ TCPView 26](#_Toc5809598)

[4.3 Phân tích mã độc với OllyDbg 26](#_Toc5809599)

# DANH SÁCH HÌNH ẢNH

[Hình 1. Xem tất cả các lệnh ipconfig 4](#_Toc5809633)

[Hình 2. Hiển thị tất cả cấu hình IP của PC đang sử dụng : IP Address , Subnet Mask , Default Gateway , .... 5](#_Toc5809634)

[Hình 3. Cập nhật lại tất cả cấu hình IP trên card mạng 6](#_Toc5809635)

[Hình 4. Xoá bộ nhớ đệm trên chương trình DNS Resolver Cache 6](#_Toc5809636)

[Hình 5. Đăng ký mới DNS với DNS Server, đồng thời Refresh quá trình cấp IP từ DHCP Server 6](#_Toc5809637)

[Hình 6. Thông báo Reply khi ping đến địa chỉ 192.168.1.10 7](#_Toc5809638)

[Hình 7. Thông báo request timed out khi ping đến đại chi 8.8.8.8 8](#_Toc5809639)

[Hình 8. Thông báo Reply khi ping đến địa chỉ google.com 8](#_Toc5809640)

[Hình 9. Lệnh ping có xác định số gói tin sẽ gửi đi. 8](#_Toc5809641)

[Hình 10. Xem thông tin các Adapter trên máy và IPv4 Route Table 9](#_Toc5809642)

[Hình 11. Thông tin IPv6 Route Table 10](#_Toc5809643)

[Hình 12. Hiển thị thông tin số cổng đang kết nối và lắng nghe, số process ID của mỗi chương trình với lệnh -nao 11](#_Toc5809644)

[Hình 13. Xem tên file EXE đang sử dụng trên mỗi cổng 12](#_Toc5809645)

[Hình 14. Xem cổng TCP 884 bắt đầu được sử dụng trên máy tính, cùng với process ID đang sử dụng trên cổng. 13](#_Toc5809646)

[Hình 15. Thống kê gói tin TCP. 13](#_Toc5809647)

[Hình 16. Truy vấn thông tin DNS được phân giải trong tên miền 14](#_Toc5809648)

[Hình 17. Liệt kê các bản ghi MX của domain gmail.com 14](#_Toc5809649)

[Hình 18. Xem danh sách các tài nguyên chia sẻ trên máy với lệnh net share 14](#_Toc5809650)

[Hình 19. Tạo một ổ đĩa ánh xạ kết nối đến thư mục chia sẽ PUBLIC trên máy Linux 192.168.1.10 15](#_Toc5809651)

[Hình 20. Xem danh sách các kết nối trên hệ thống vớ lệnh net session 15](#_Toc5809652)

[Hình 21. Tạo một tài khoản mới với tên masv(102150274), mật khẩu: 123456 16](#_Toc5809653)

[Hình 22. Xem các cổng dịch vụ và hệ điều hành của máy ở xa với lệnh nmap (1) 17](#_Toc5809654)

[Hình 23. Xem các cổng dịch vụ và hệ điều hành của máy ở xa với lệnh nmap (2) 18](#_Toc5809655)

[Hình 24. Xem thông tin về hệ điều hành trên máy đích 19](#_Toc5809656)

[Hình 25. Xem danh sách các máy chủ với các cổng 80 được mở: 19](#_Toc5809657)

[Hình 26. Cài đặt Snort vào thư mục C:\SNORT 20](#_Toc5809658)

[Hình 27. Cấu hình dịch vụ snort trên snort.conf 20](#_Toc5809659)

[Hình 28. Xem số hiệu card mạng với lệnh :\Snort\bin>snort –W 21](#_Toc5809660)

[Hình 29. Hiển thị IP và TCP/UDP/ICMP header (1) 21](#_Toc5809661)

[Hình 30. Hiển thị thêm các header của gói tin với tùy chọn -dev 22](#_Toc5809662)

[Hình 31. Bắt gói tin và lưu vào tập tin trong thư mục C:\Snort\log (1) 23](#_Toc5809663)

[Hình 32. Bắt gói tin và lưu vào tập tin trong thư mục C:\Snort\log (2) 24](#_Toc5809664)

[Hình 33. Theo dõi các tiến trình bằng Process Explorer 25](#_Toc5809665)

[Hình 34. Thông tin các tiến trình trên TCPView 26](#_Toc5809666)

[Hình 35. Giao diện OllyDbg 26](#_Toc5809667)

[Hình 36. Chạy file crackme.exe và thử password 12345 27](#_Toc5809668)

[Hình 38. Tìm kiếm chuỗi “Incorrect Password” 27](#_Toc5809669)

[Hình 39. Các thông báo “Congratulation” & “Incorrect Password” và địa chỉ 28](#_Toc5809670)

[Hình 40. Nhảy đến địa chỉ 0x004010B5 28](#_Toc5809671)

[Hình 42. Xác định lệnh có ghi chú “getDlgItemTextA” 29](#_Toc5809672)

[Hình 43. Ấn F8 để chạy qua hàm getDlgItemTextA 29](#_Toc5809673)

[Hình 44. Đặt lại giá trị cờ Z=1 để tiếp tục 30](#_Toc5809674)

[Hình 45. Quan sát Stack ở câu lệnh 0x004010C3 30](#_Toc5809675)

[Hình 46. 2 chuỗi “345”, “5y” và giá trị 0x02 được đẩy vào stack 31](#_Toc5809676)

[Hình 47.Tiếp tục so sánh các kí tự từ thứ 5 trở đi với chuỗi “R3versing” 31](#_Toc5809677)

[Hình 48. Restart chương trình và nhập vào password “xa5yR3versing” 32](#_Toc5809678)

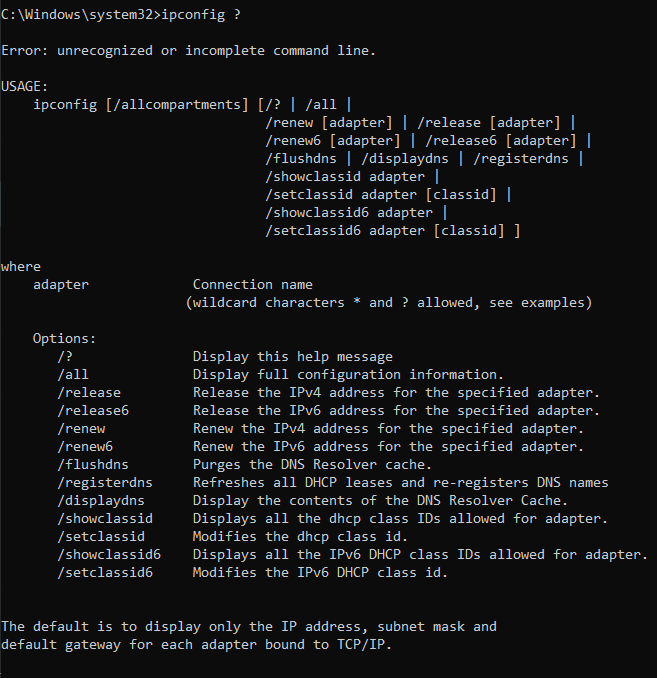
# LAB 1: XEM THÔNG TIN MẠNG TRÊN HỆ ĐIỀU HÀNH WINDOW

## Chuẩn bị

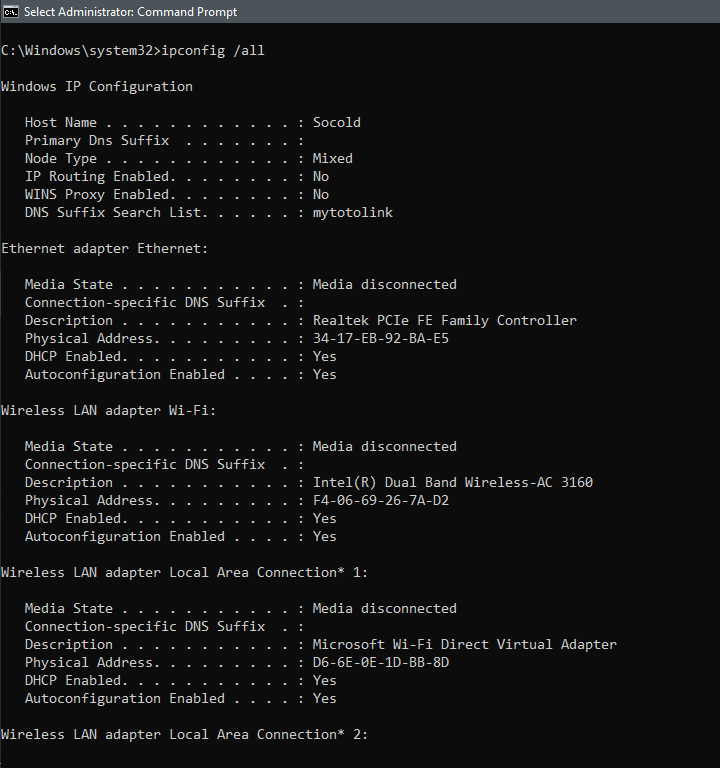
- Kết nối máy tính vào mạng

- Trên Windows, vào menu Start\Windows System\CommandPrompt, nháy nút phải chọm More\Run as administrator

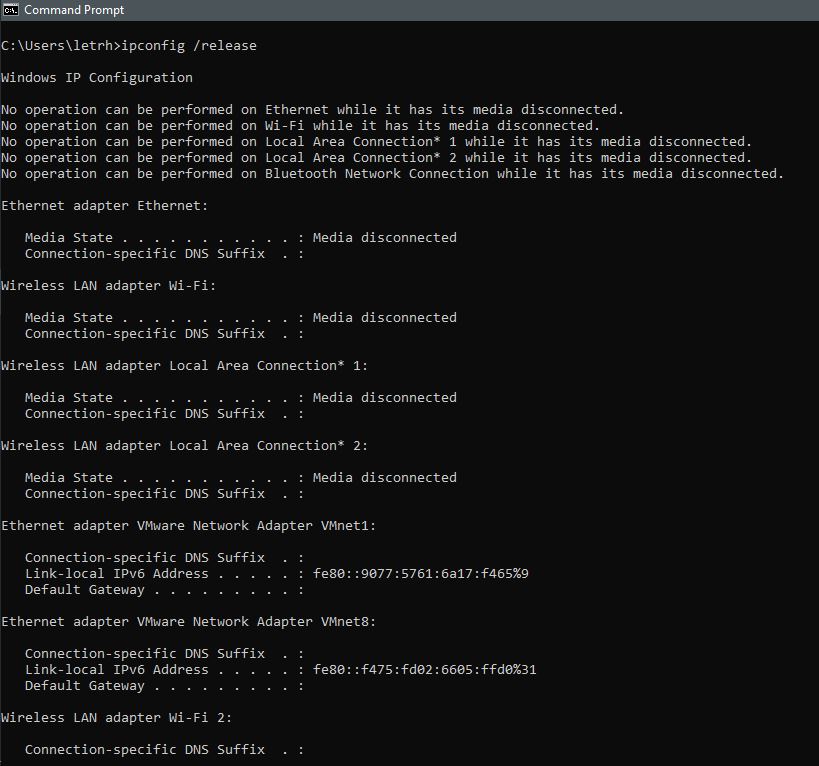
## Lệnh ipconfig



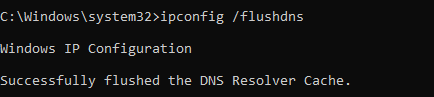
Hình . Xem tất cả các lệnh ipconfig



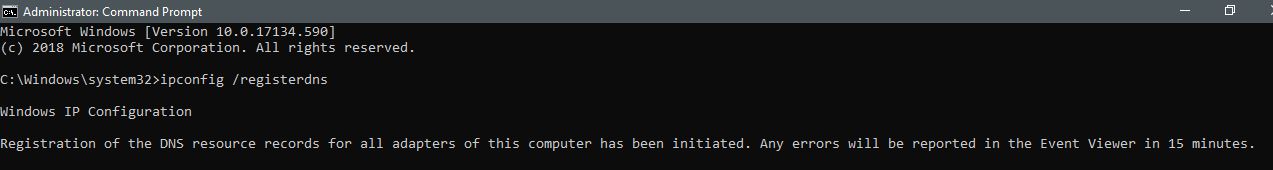
Hình . Hiển thị tất cả cấu hình IP của PC đang sử dụng : IP Address , Subnet Mask , Default Gateway , ....



Hình . Cập nhật lại tất cả cấu hình IP trên card mạng



Hình . Xoá bộ nhớ đệm trên chương trình DNS Resolver Cache



Hình . Đăng ký mới DNS với DNS Server, đồng thời Refresh quá trình cấp IP từ DHCP Server

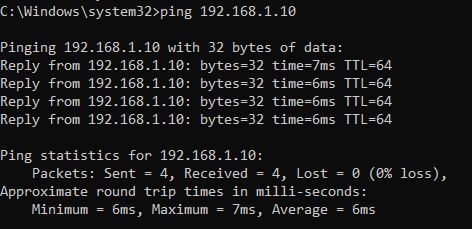
## Lệnh ping

Lệnh Ping (Packet Internet Groper) cho phép kiểm tra xem một máy tính có thể kết nối tới một máy chủ cụ thể nào đó hay không, và ước lượng khoảng thời gian trễ trọn vòng đi và về của gói dữ liệu cũng như tỉ lệ các gói dữ liệu có thể bị mất giữa hai máy.

**Các dạng thông báo sau khi thực hiện lệnh ping:**

1. Thông báo: Reply from 192.168.1.10: bytes=32 time=7ms TTL=64

* Lệnh ping đã thực hiện thành công và không có lỗi trên mạng.
* Địa chỉ IP 192.168.1.10 cho biết máy nào đang gửi thông điệp trả lời.
* bytes=32 là kích thước của gói tin ICMP được gửi đi.
* time=7ms thời gian của quá trình hồi đáp
* TTL=64 là giá trị “time to live” (thời gian sống) của gói tin ICMP. Hết thời gian này thì gói tin sẽ bị hủy.

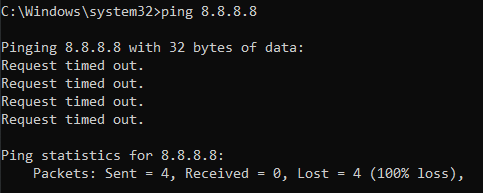


Hình . Thông báo Reply khi ping đến địa chỉ 192.168.1.10

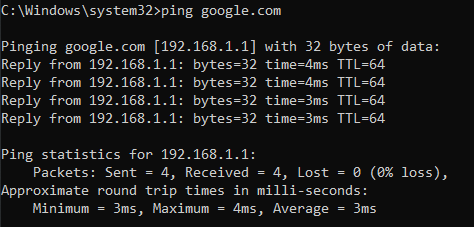
1. Thông báo: Request timed out

Xảy ra khi không kết nối được với máy đích, không có hồi đáp trả về. Nguyên nhân:

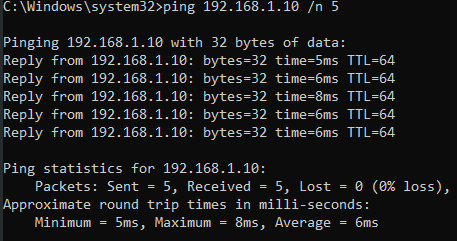
* Thiết bị định tuyến Router bị tắt.
* Địa chỉ máy đích không có thật hoặc máy đích đang bị tắt, hoặc cấm ping.
* Nếu máy đích khác đường mạng với máy nguồn thì nguyên nhân có thể do không có định tuyến ngược trở lại máy nguồn. Lúc này, nếu máy đích đang chạy, có thể kiểm tra đường đi về của gói tin bằng cách xem lại thông số Default Gateway trên máy đích, máy nguồn và router kết nối các đường mạng
* Thông báo: Destination host unreachable: Thông báo cho biết không thể kết nối đến máy đích. Nguyên nhân gây ra lỗi này có thể là do kết nối vật lý của máy tính như cáp mạng bị đứt, không gắn cáp vào card mạng, card mạng bị tắt, Driver card mạng bị hỏng, chưa bật wifi, …



Hình . Thông báo request timed out khi ping đến đại chi 8.8.8.8

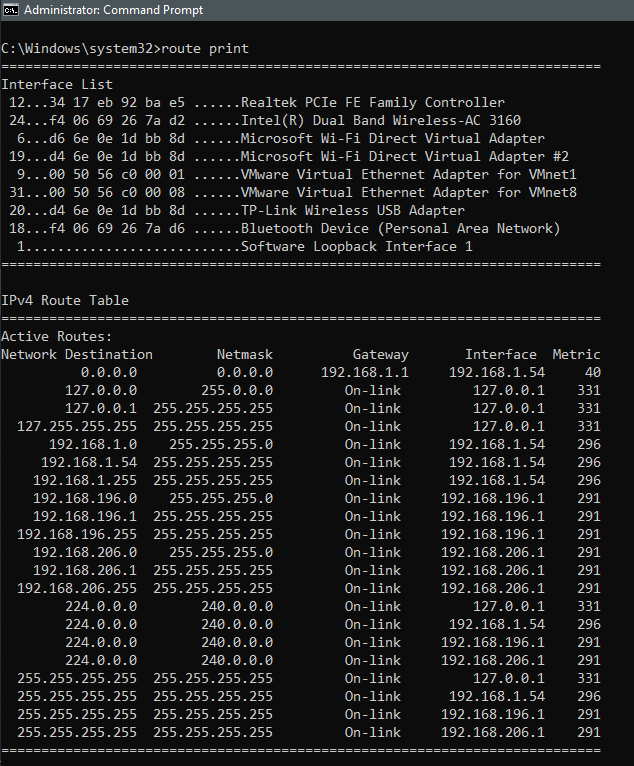


Hình . Thông báo Reply khi ping đến địa chỉ google.com

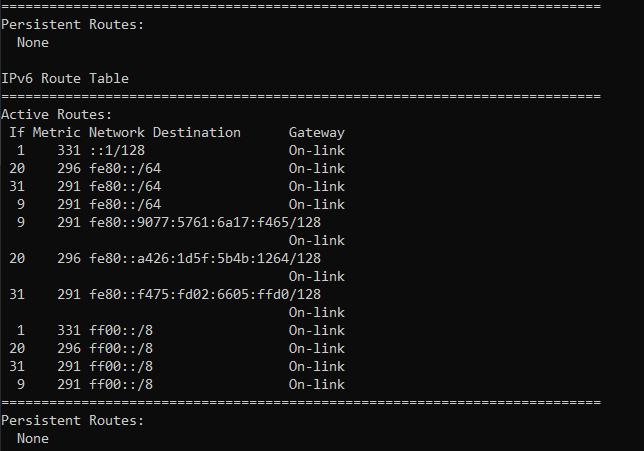


Hình . Lệnh ping có xác định số gói tin sẽ gửi đi.

## Lệnh route



Hình . Xem thông tin các Adapter trên máy và IPv4 Route Table



Hình . Thông tin IPv6 Route Table

## Lệnh netstat

Lệnh netstat cho phép xem thông tin hoạt động của mạng TCP/IP.

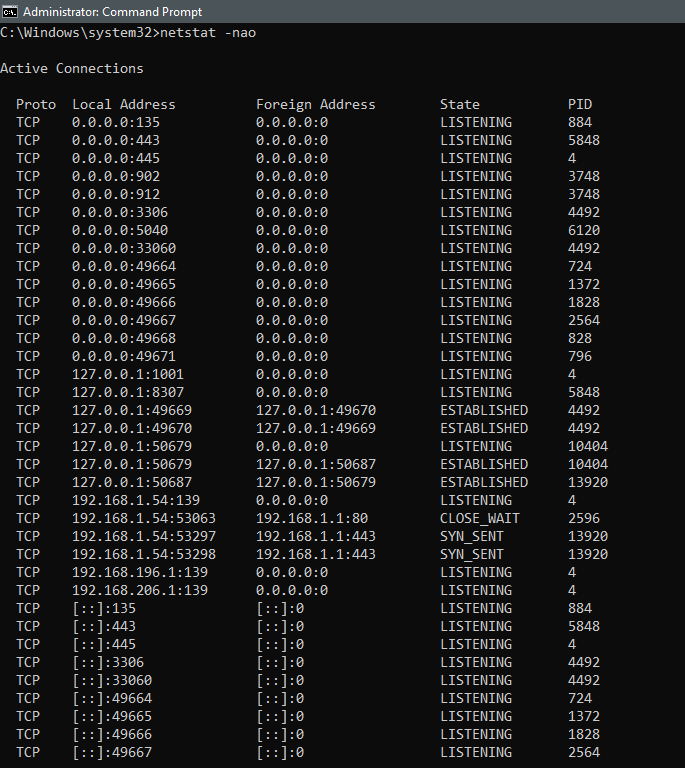
Cú pháp: Netstat [-a][-e][-n]

- Tham số -a: Hiển thị tất cả các kết nối và các cổng đang lắng nghe (listening)

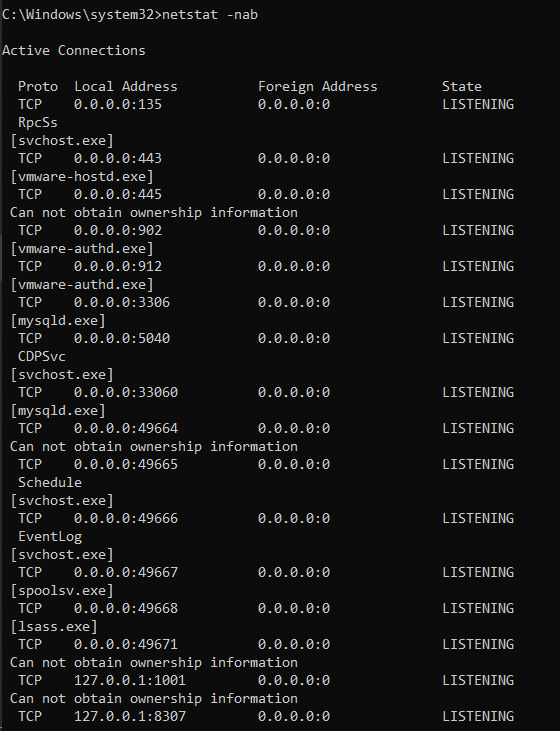
- Tham số -e: hiển thị các thông tin thống kê Ethernet

- Tham số -n: Hiển thị các địa chỉ và các số cổng kết nối...

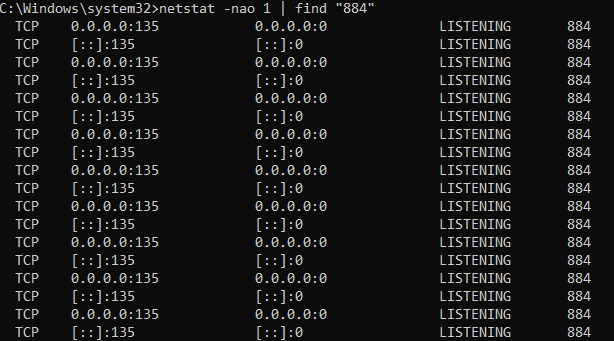
- Tham số -o thông báo cho netstat hiển thị số processID của mỗi chương trình đang tương tác với cổng TCP hoặc UDP.



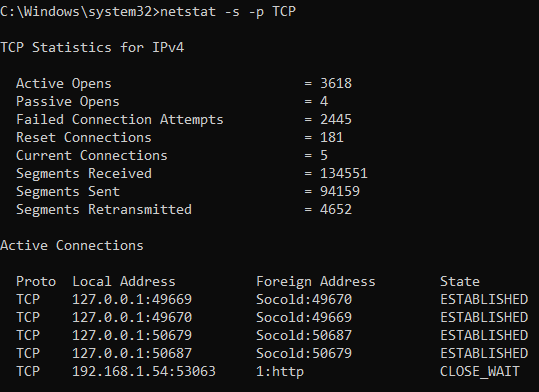
Hình . Hiển thị thông tin số cổng đang kết nối và lắng nghe, số process ID của mỗi chương trình với lệnh –nao



Hình . Xem tên file EXE đang sử dụng trên mỗi cổng



Hình . Xem cổng TCP 884 bắt đầu được sử dụng trên máy tính, cùng với process ID đang sử dụng trên cổng.



Hình . Thống kê gói tin TCP.

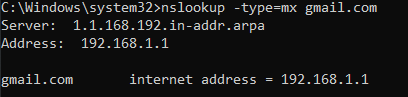
## Lệnh nslookup

* Dùng để truy vấn thông tin DNS trong phân giải tên miền.
* Hiển thị thông tin có thể được dùng để chẩn đoán cấu trúc của DNS.
* Giúp tìm kiếm thêm địa chỉ IP nếu DNS biết được whois.
* Bản ghi MX cho biết địa chỉ IP của mail server.

Kết quả xuất hiện thông tin hostname và địa chỉ IP của DNS server được cấu hình.

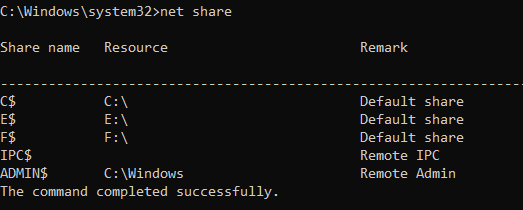


Hình . Truy vấn thông tin DNS được phân giải trong tên miền

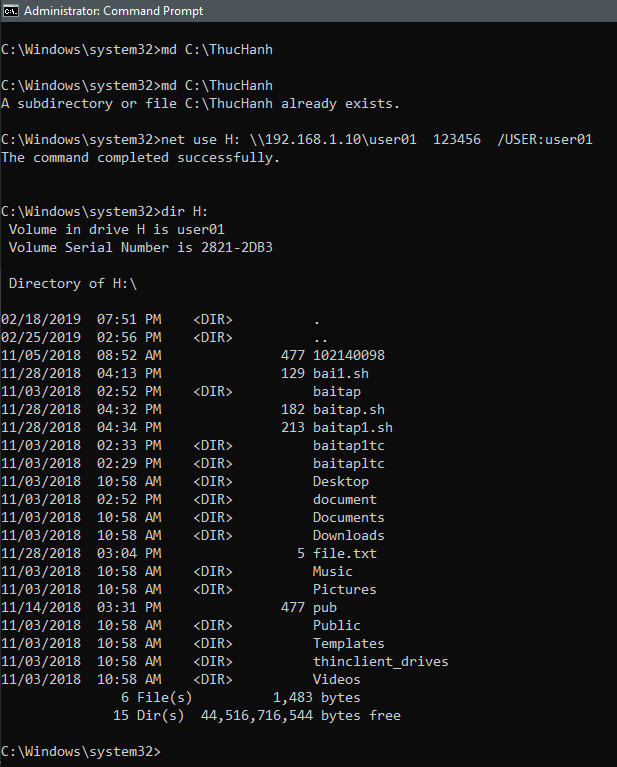


Hình . Liệt kê các bản ghi MX của domain gmail.com

## Lệnh net



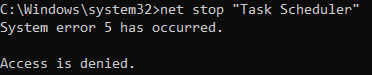
Hình . Xem danh sách các tài nguyên chia sẻ trên máy với lệnh net share

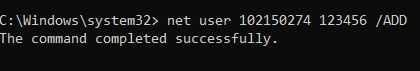


Hình . Tạo một ổ đĩa ánh xạ kết nối đến thư mục chia sẽ PUBLIC trên máy Linux 192.168.1.10



Hình . Xem danh sách các kết nối trên hệ thống vớ lệnh net session





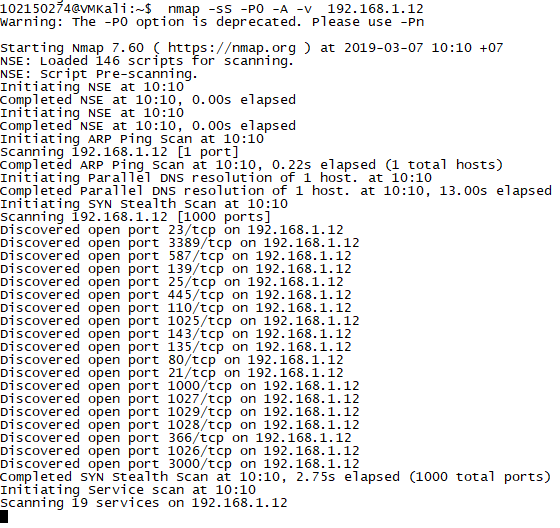
Hình . Tạo một tài khoản mới với tên masv(102150274), mật khẩu: 123456

# LAB 2. SỬ DỤNG CÁC CÔNG CỤ

# QUÉT & DÒ TÌM LỖ HỖNG TRÊN MẠNG

## Công cụ quét mạng NMAP

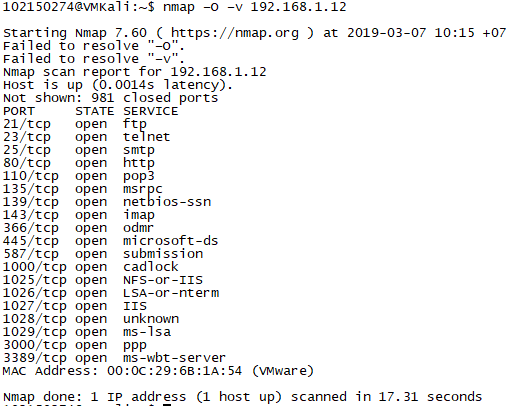
Nmap (Network Mapper) là một công cụ quét, theo dõi và đánh giá bảo mật một hệ thống mạng. Các chức năng chính của nmap: Liệt kê các port đang mở trên một host, xác định các dịch vụ chạy trên các port đang mở cùng với phần mềm và phiên bản đang dùng, xác định hệ điều hành của thiết bị, chạy các script đặc biệt…



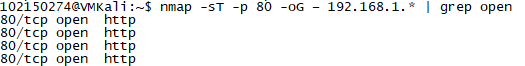
Hình . Xem các cổng dịch vụ và hệ điều hành của máy ở xa với lệnh nmap (1)



Hình . Xem các cổng dịch vụ và hệ điều hành của máy ở xa với lệnh nmap (2)



Hình . Xem thông tin về hệ điều hành trên máy đích



Hình . Xem danh sách các máy chủ với các cổng 80 được mở:

# LAB 3. SỬ DỤNG CÔNG CỤ SNORT

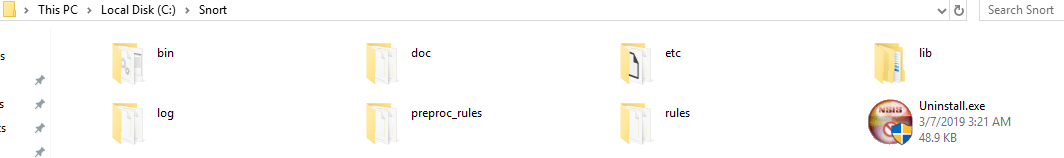
## 3.1 Chuẩn bị

Thực hành trên hệ điều hành Windows.

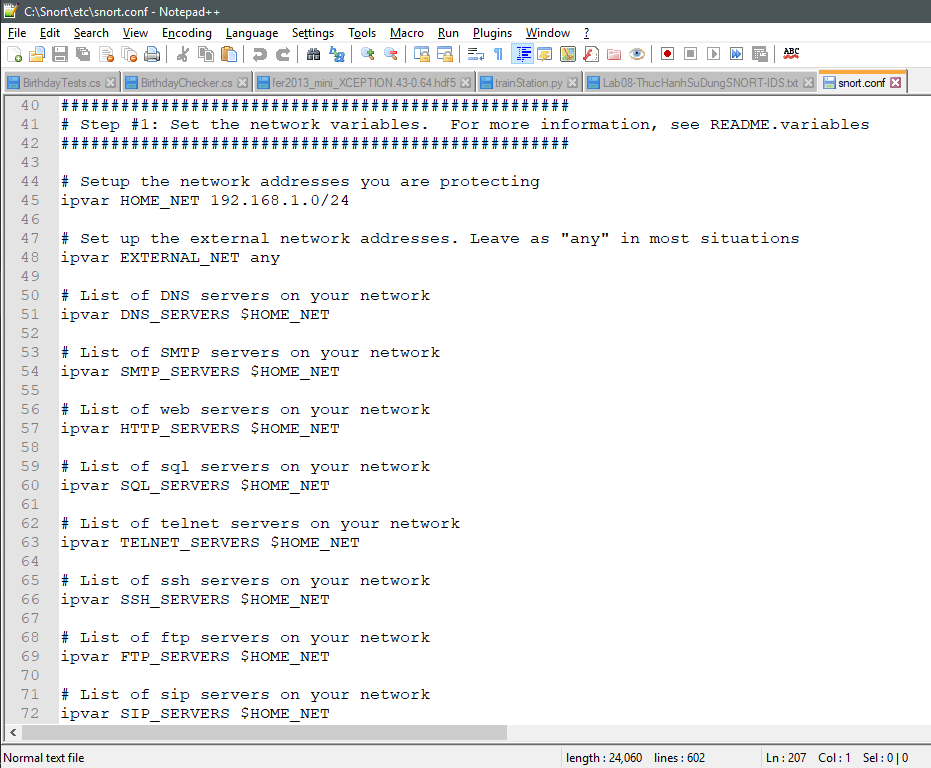
Vào ftp://192.168.1.10/ToolSnortIDS/ tải các file:

• Snort v2.9.11.1 Installer.exe

• WinPcap v4.1.3.exe



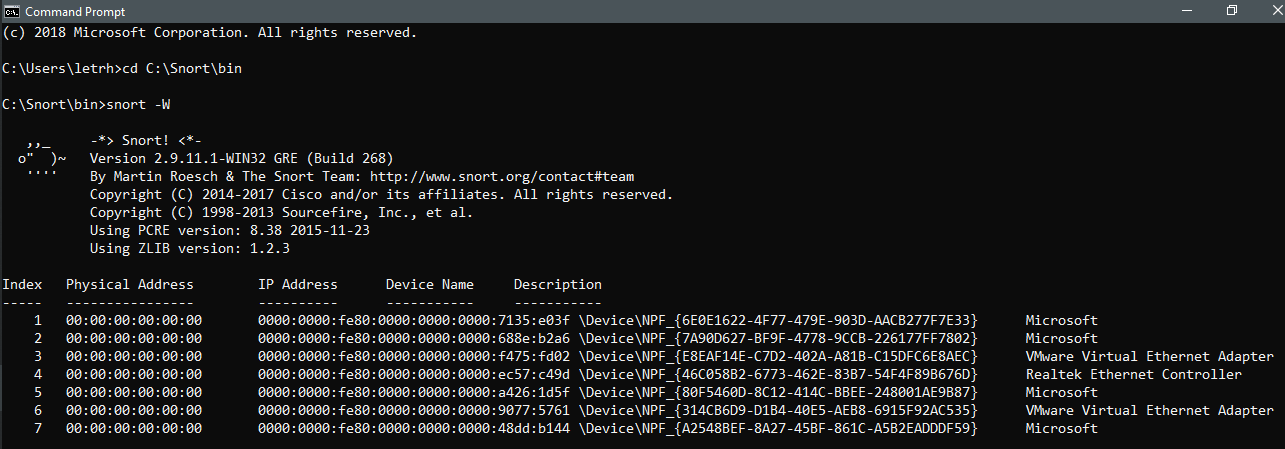
Hình . Cài đặt Snort vào thư mục C:\SNORT



Hình . Cấu hình dịch vụ snort trên snort.conf

## 3.2 Xem thông tin dịch vụ Snort

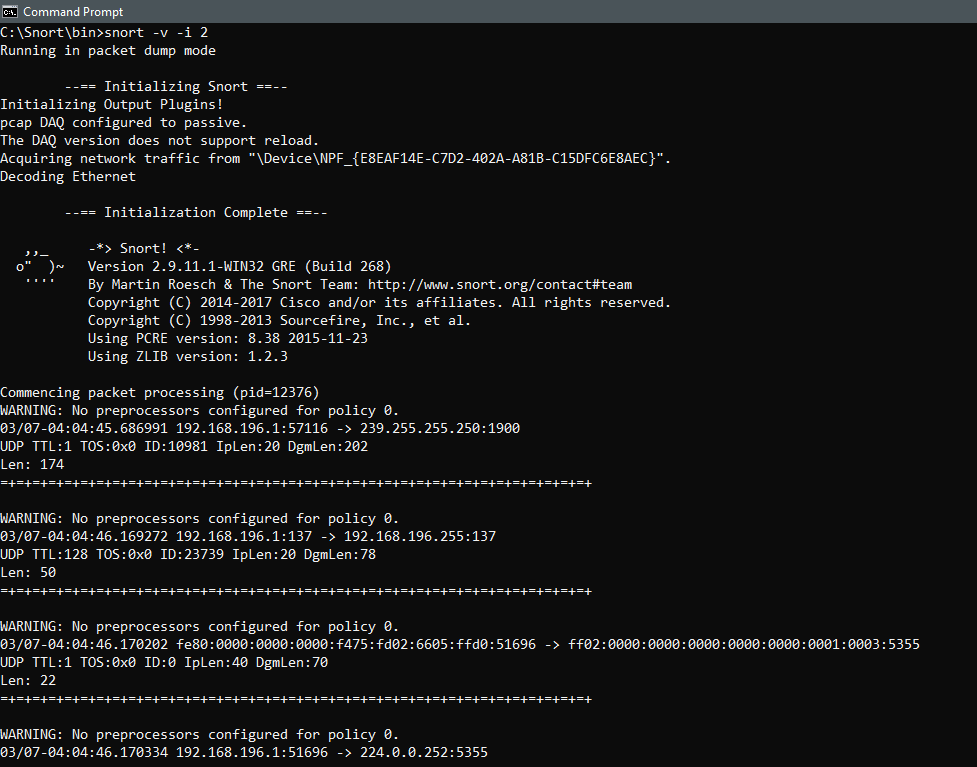
* Mở cửa sổ lệnh và chuyển đổi thư mục hiện hành là C:\Snort\bin
* Xem thư mục cài đặt: C:\Snort\bin>dir
* Xem nội dung tập tin cấu hình: C:\Snort\bin>type C:\Snort\etc\snort.conf
* Xem số hiệu card mạng để chọn bắt gói tin: Cần xác định card mạng để snort bắt gói tin ở chế độ promicous:



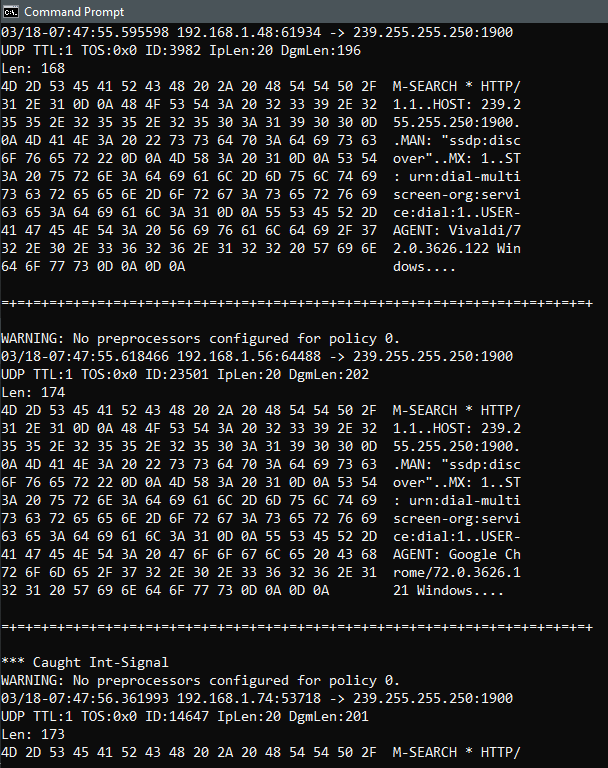
Hình . Xem số hiệu card mạng với lệnh :\Snort\bin>snort –W

## 3.3 Xem kết quả bắt gói tin

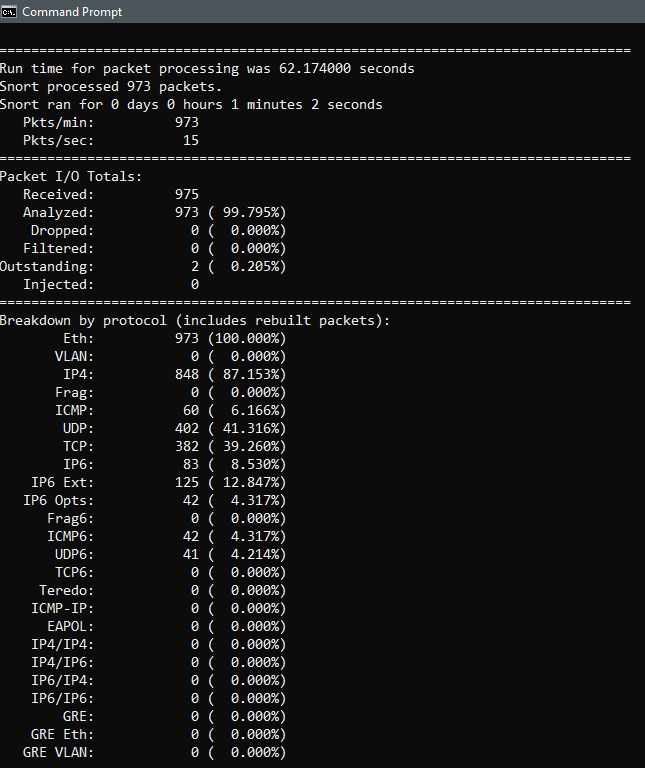
Thực hiện bắt gói tin với card mạng có số hiệu 2



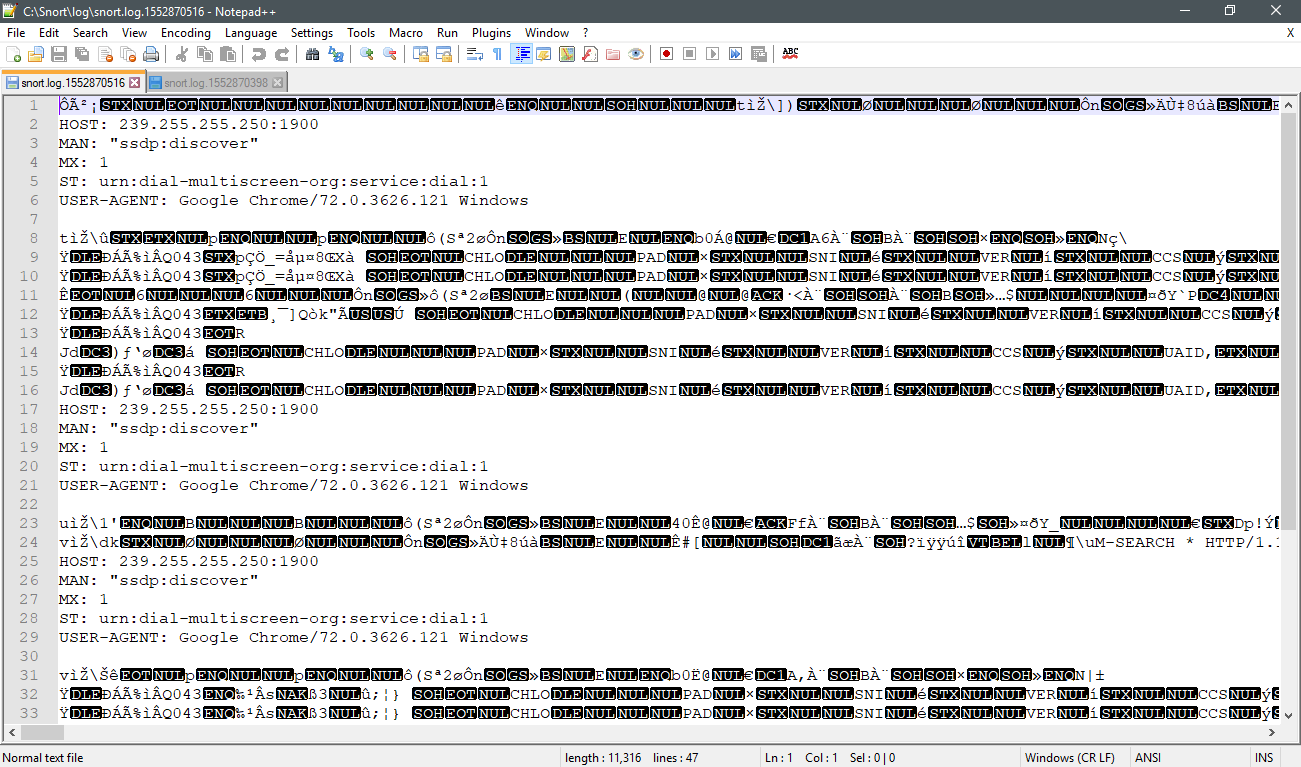
Hình . Hiển thị IP và TCP/UDP/ICMP header (1)



Hình . Hiển thị thêm các header của gói tin với tùy chọn -dev



Hình . Bắt gói tin và lưu vào tập tin trong thư mục C:\Snort\log (1)

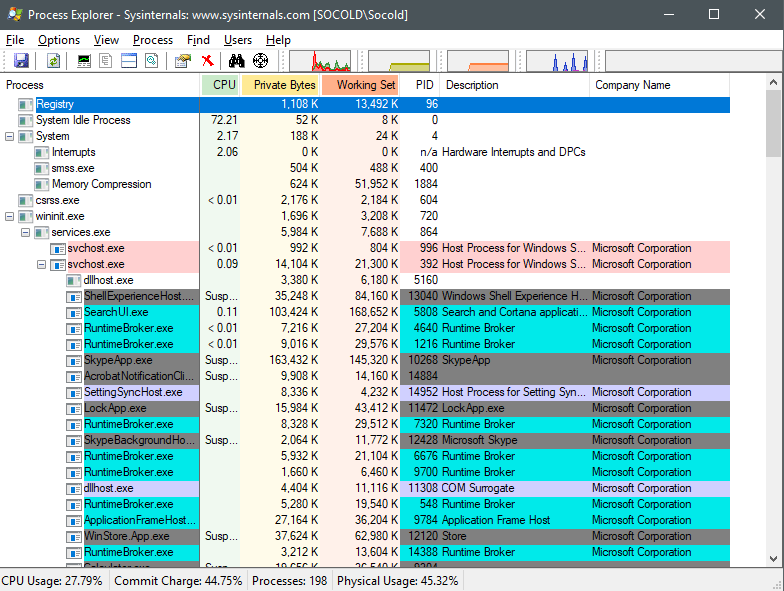


Hình . Bắt gói tin và lưu vào tập tin trong thư mục C:\Snort\log (2)

# LAB 3. THỰC HÀNH PHÂN TÍCH MÃ MÁY

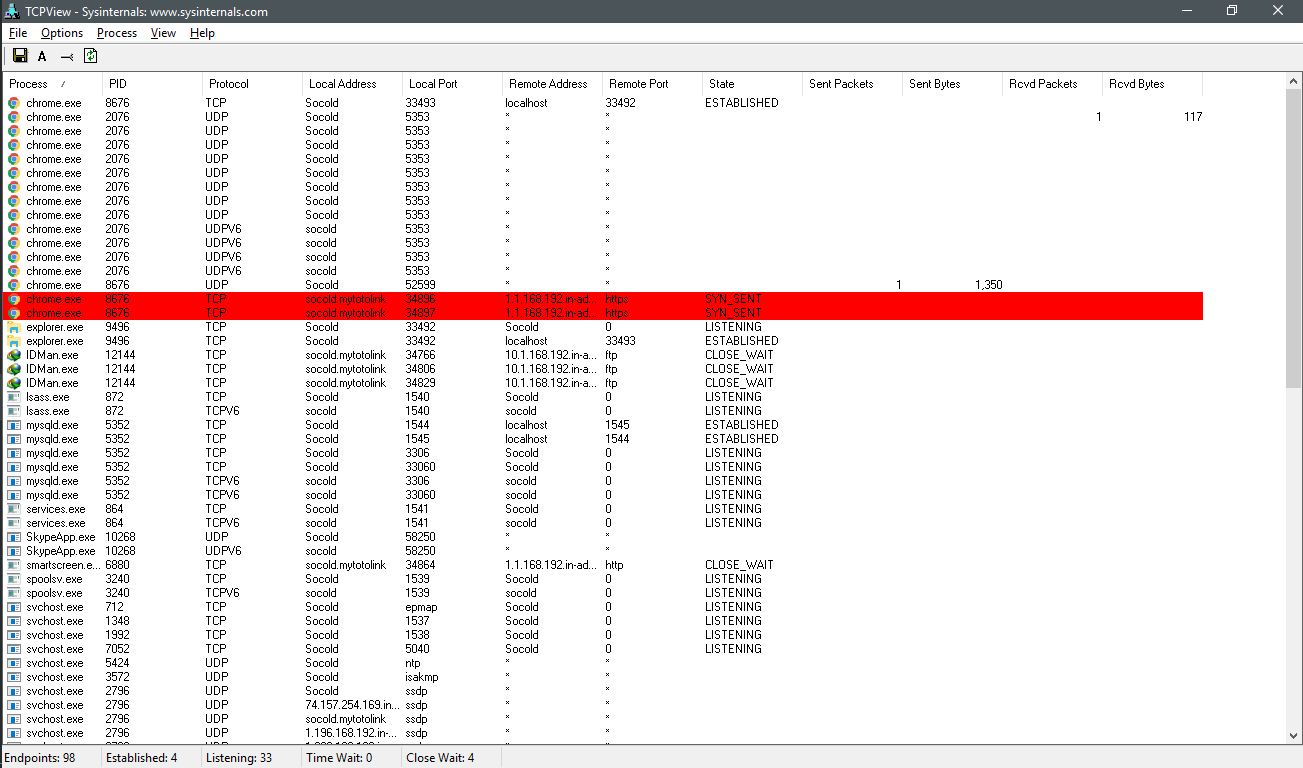
## 4.1 Công cụ Process Explorer

Dùng ProcessExplorer và TCPView v3.05 để xem chính xác một tiến trình đang mở cổng là của file nào, vị trí trên ổ đĩa cứng...



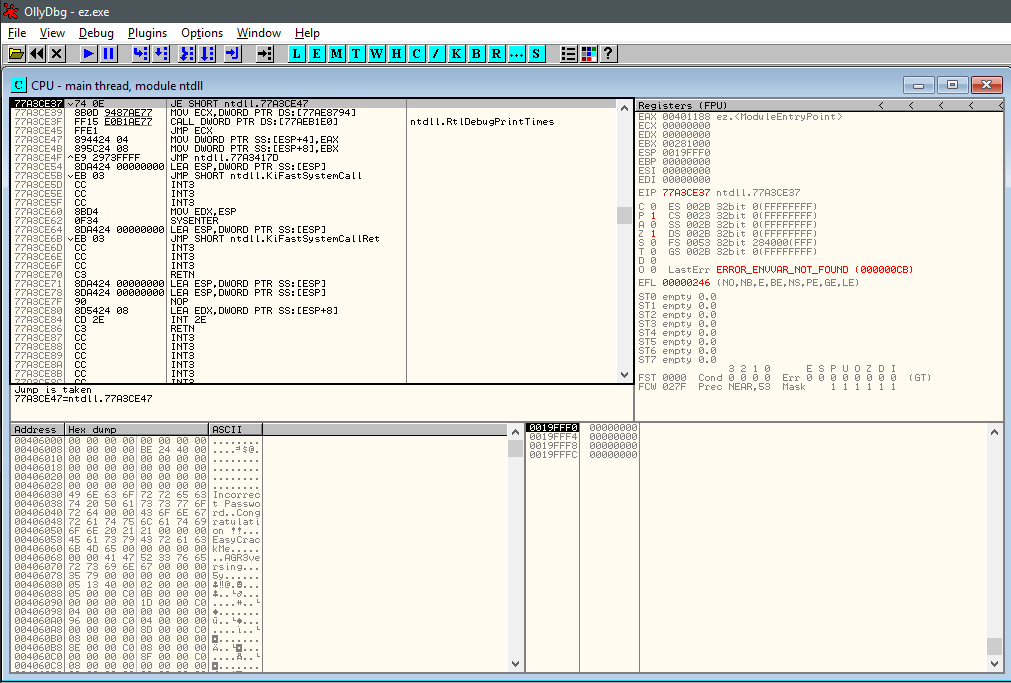
Hình . Theo dõi các tiến trình bằng Process Explorer

## 4.2 Công cụ TCPView

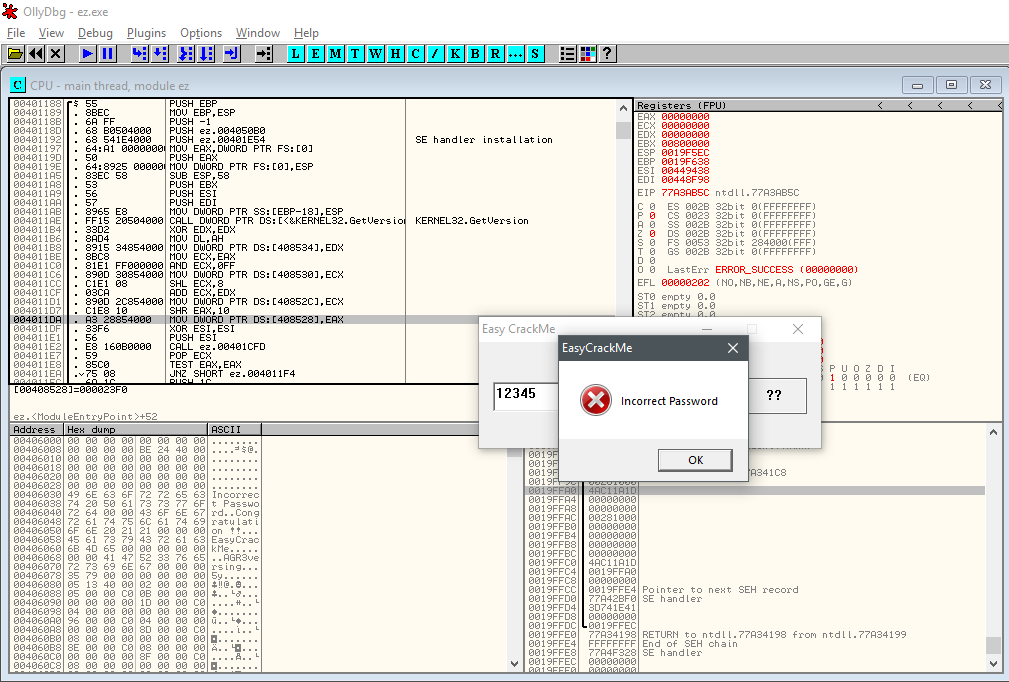


Hình . Thông tin các tiến trình trên TCPView

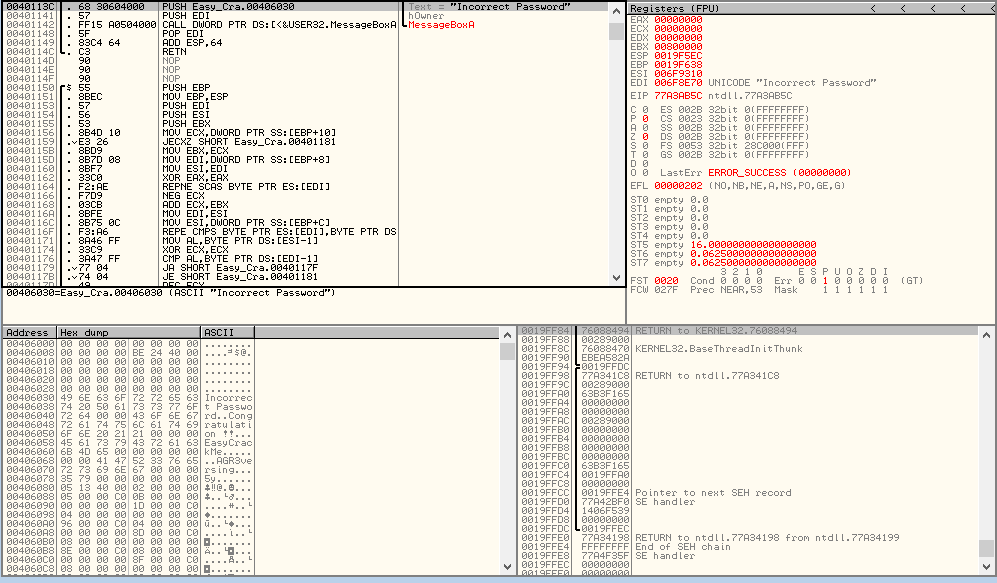
## 4.3 Phân tích mã độc với OllyDbg



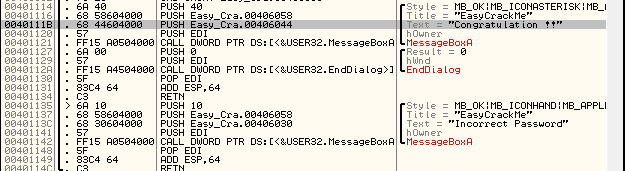
Hình . Giao diện OllyDbg



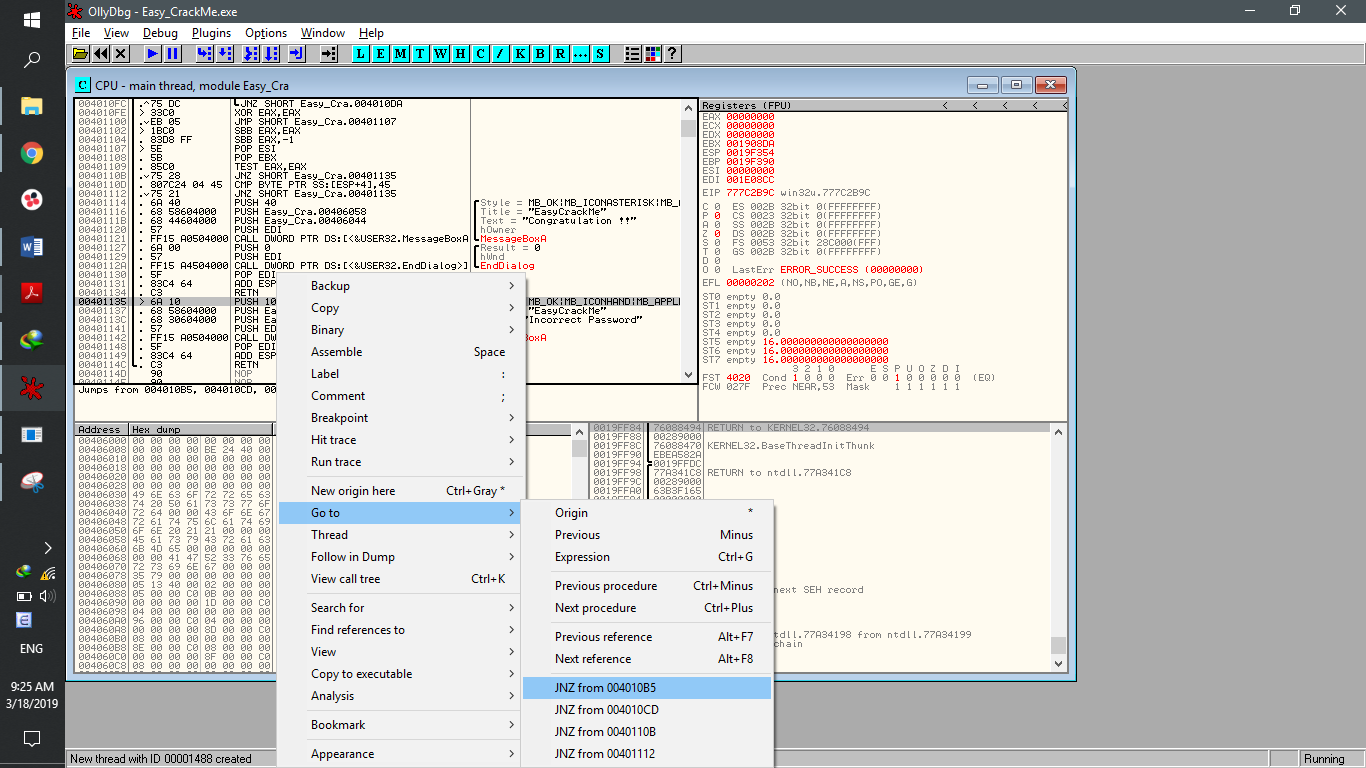
Hình . Chạy file crackme.exe và thử password 12345



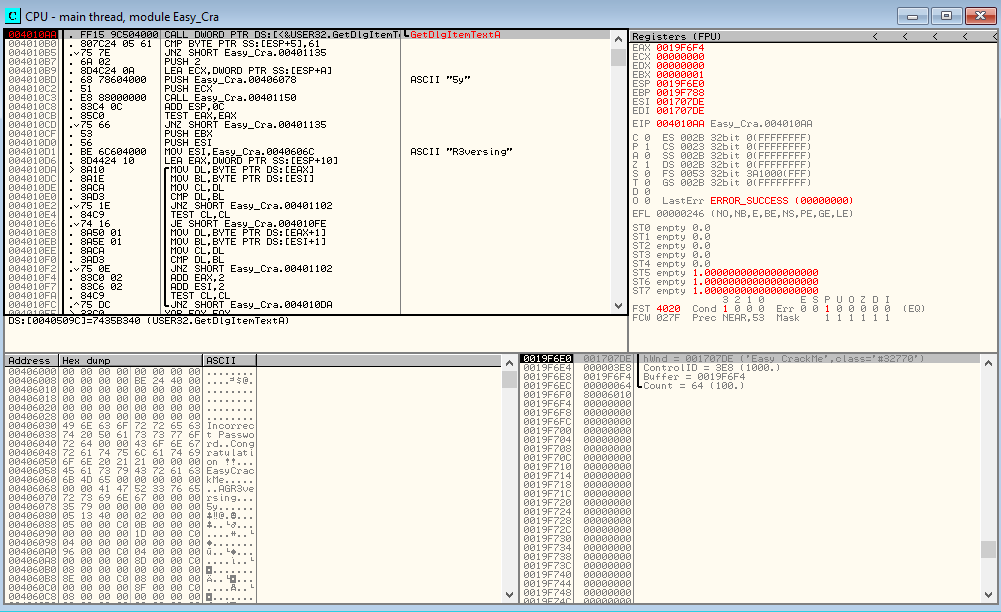
Hình . Tìm kiếm chuỗi “Incorrect Password”



Hình . Các thông báo “Congratulation” & “Incorrect Password” và địa chỉ của nó

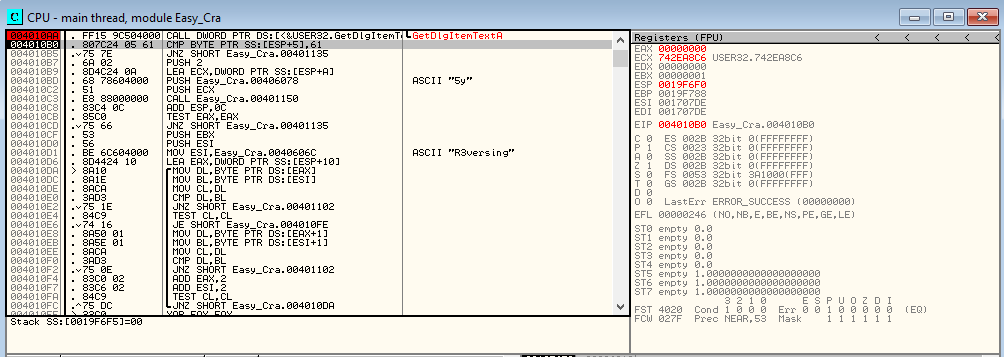


Hình . Nhảy đến địa chỉ 0x004010B5



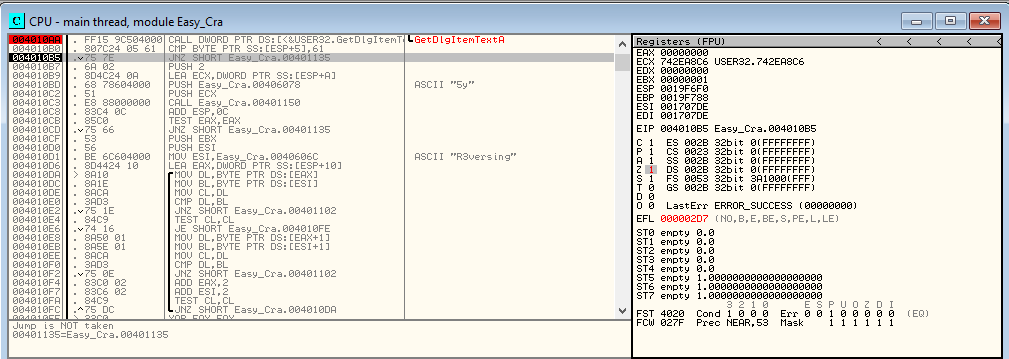
Hình . Xác định lệnh có ghi chú “getDlgItemTextA”

Ấn F2 để đặt breakpoint tại địa chỉa 0x004010AA và chạy lại chương trình



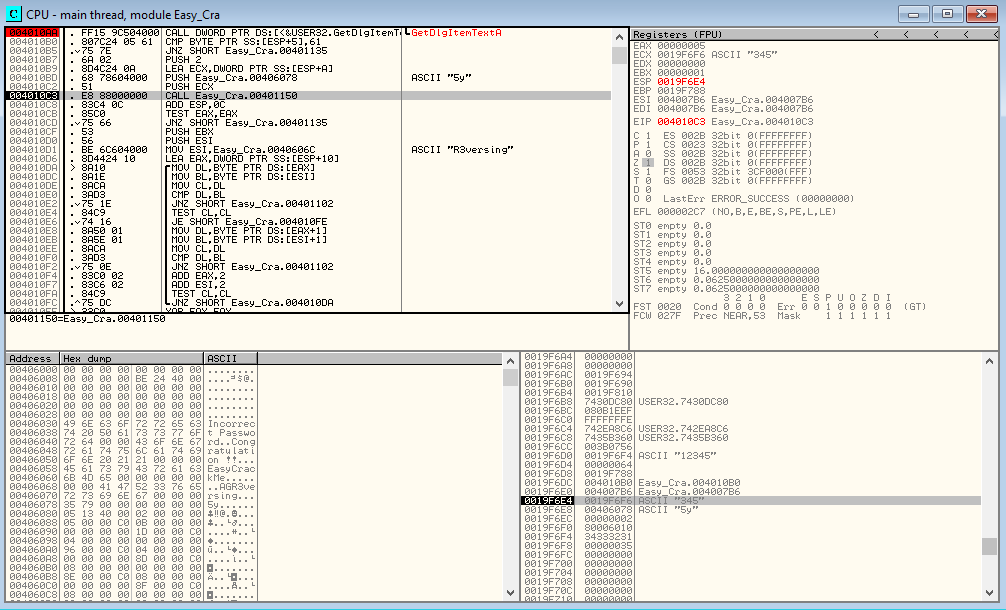
Hình . Ấn F8 để chạy qua hàm getDlgItemTextA

Câu lệnh: **004010B0 CMP BYTE PTR SS:[ESP+5], 61** thực hiện so sánh giá trị tại địa chỉ ESP+5 và 0x61. [ESP+5] là ký tự thứ 2 trong password ta vừa nhập vào.

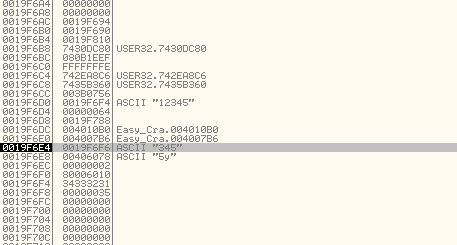


Hình . Đặt lại giá trị cờ Z=1 để tiếp tục

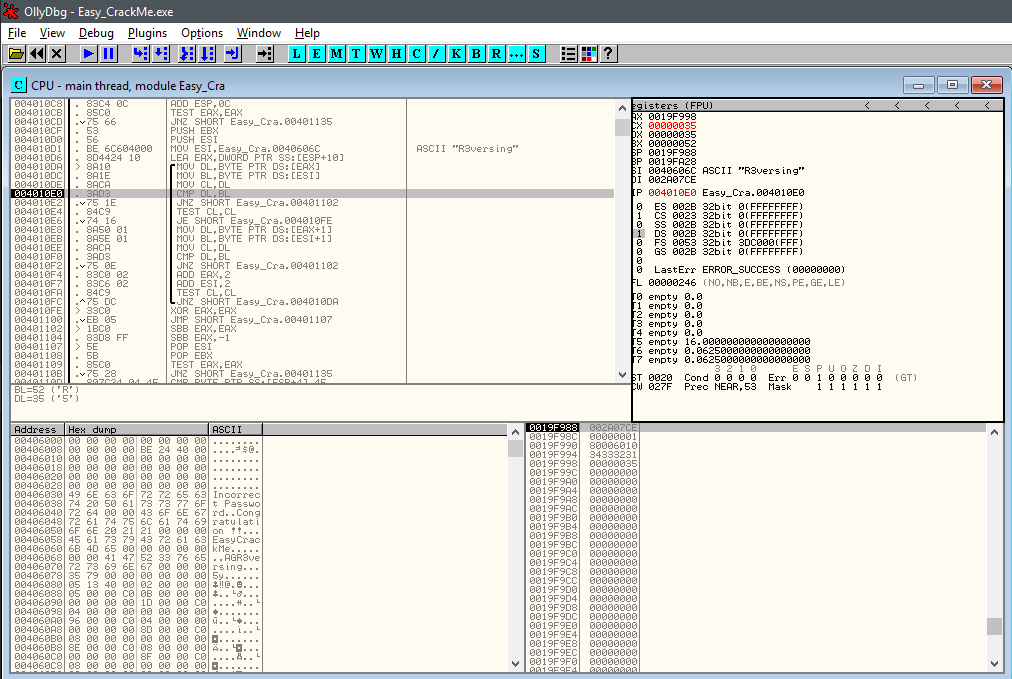
Sau câu lệnh CMP, nếu 2 giá trị được mang ra so sánh mà khác nhau, cờ ZF vẫn mang giá trị 0 và lệnh JNZ được thực hiện, đoạn code thông báo “Incorrect Password” sẽ được thực hiện và bật ra thông báo. Như vậy bước kiểm tra đầu tiên để password được chấp nhập thì thì ký tự thứ 2 của password là ký tự có mã 0x61, tức là kí tự “a”.



Hình . Quan sát Stack ở câu lệnh 0x004010C3



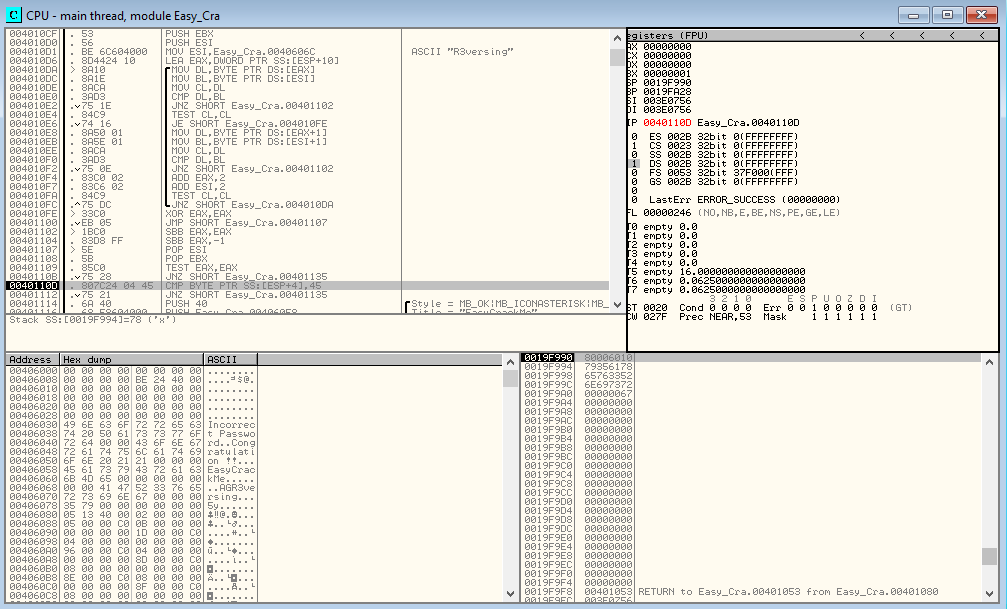
Hình . 2 chuỗi “345”, “5y” và giá trị 0x02 được đẩy vào stack



Hình .Tiếp tục so sánh các kí tự từ thứ 5 trở đi với chuỗi “R3versing”

Như vậy ta có password có dạng “xa5yR3versing” với ký tự đầu tiên chưa tìm ra. Restart lại chương trình và nhập vào password có dạng như trên. Dừng lại ở câu lệnh:

**0040110D CMP BYTE PTR SS:[ESP+4], 45**



Hình . Restart chương trình và nhập vào password “xa5yR3versing”

So sánh ký tự đầu tiên của password với ký tự “E”. Vậy password chính xác là “Ea5yR3versing”.