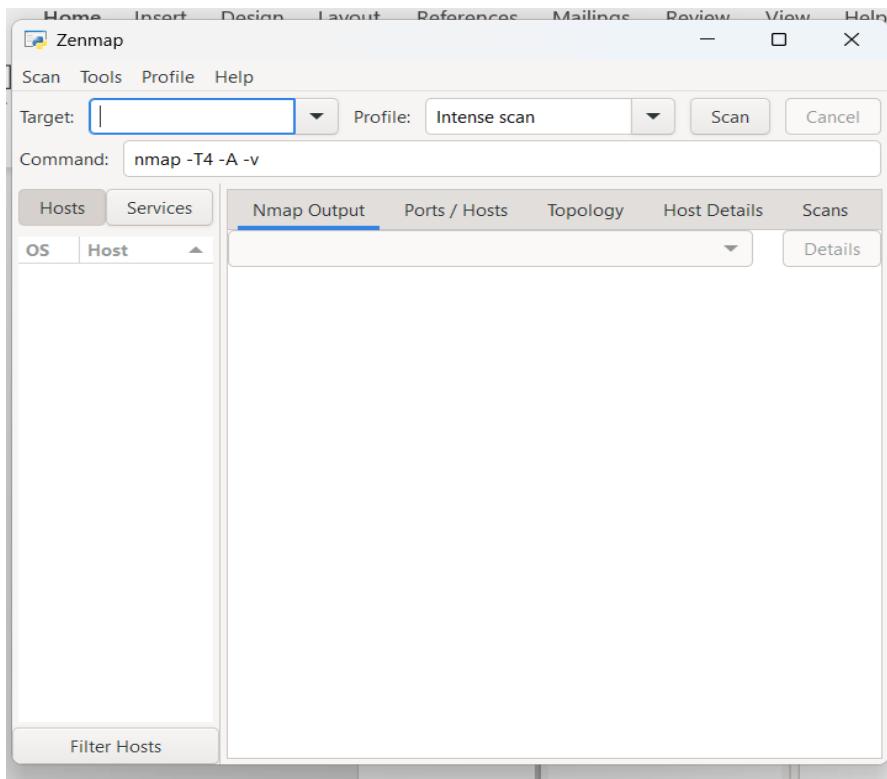


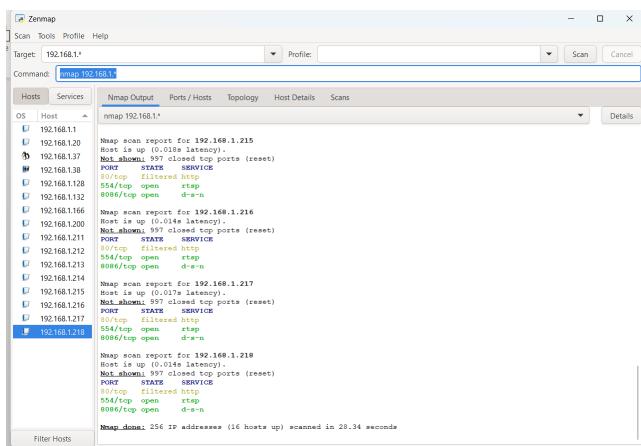
Bài Thực hành 1B

Bài 3: Quét mạng sử dụng Nmap

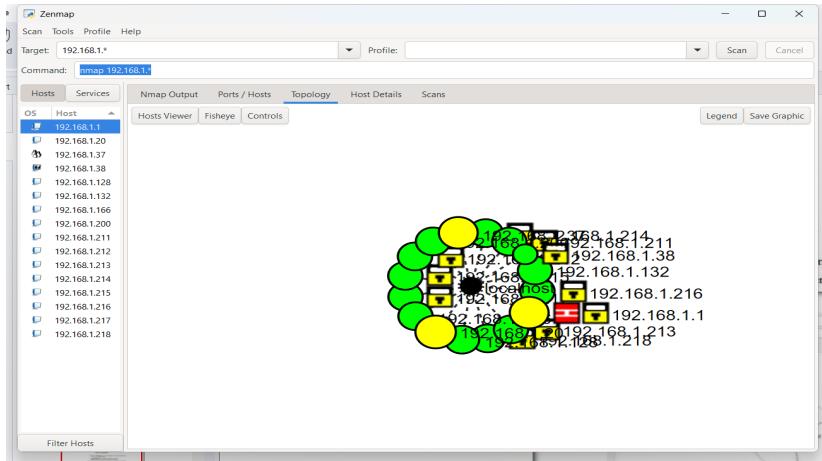
Bước 1: Setup Nmap



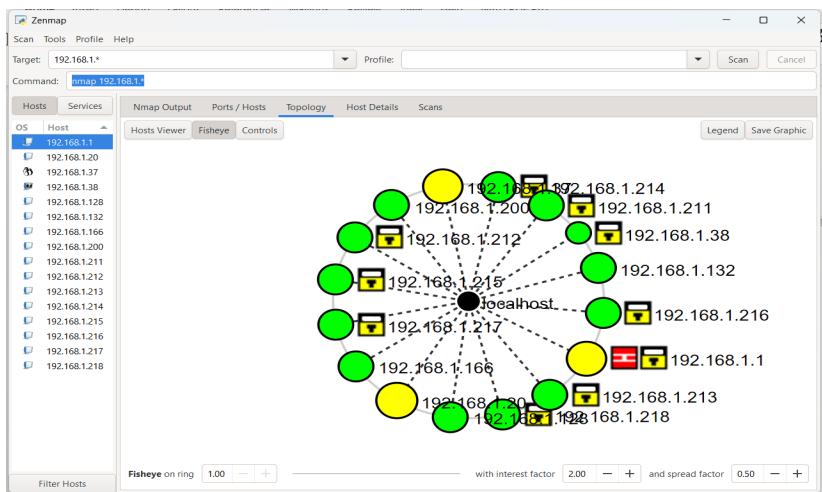
Bước 2: Nhập Nmap 192.168.1.* vào ô command và nhấn scan để quét các máy ảo trong mạng



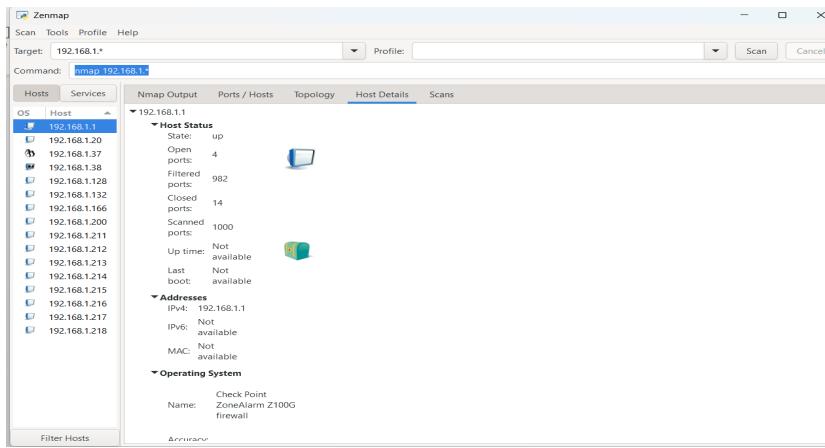
Bước 3: Sơ đồ mạng



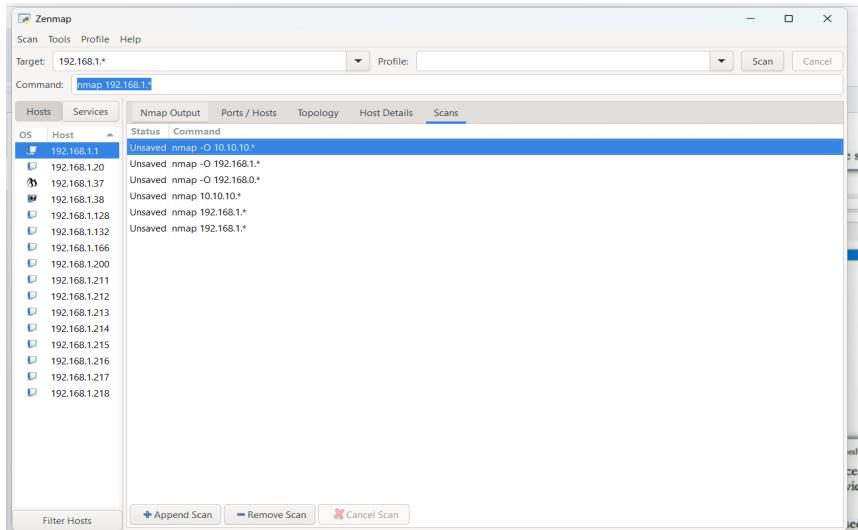
Bước 4: Ché độ fisheye



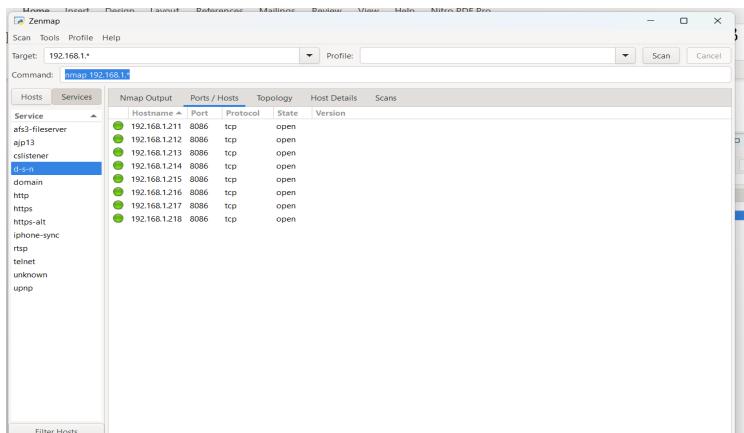
Bước 5: Host detail



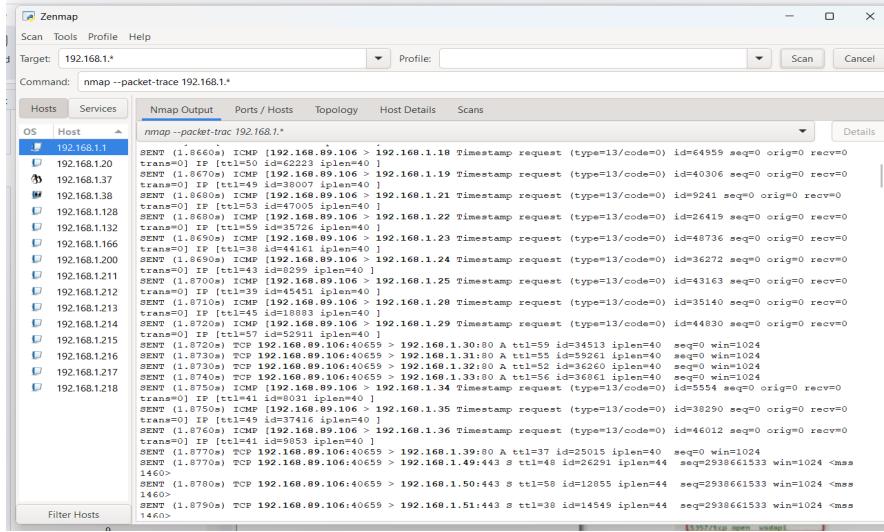
Bước 6: Trạng thái quét



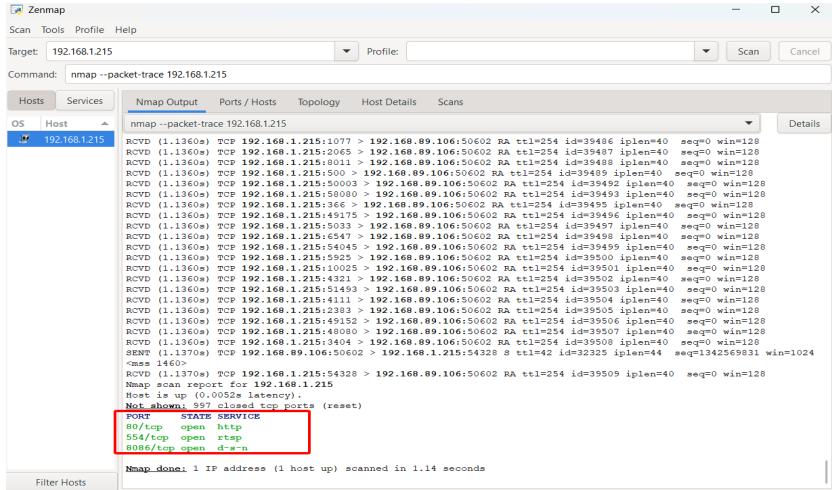
Bước 7: Chi tiết dịch vụ theo cổng



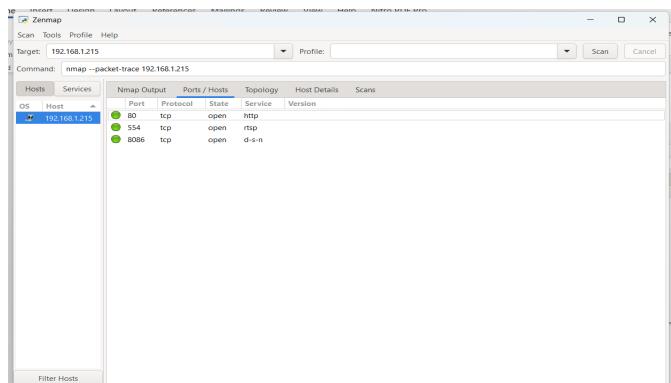
Bước 8: Dùng nmap --packet-trace 192.168.1.* để theo dõi mọi gói tin được gửi và nhận bởi Nmap



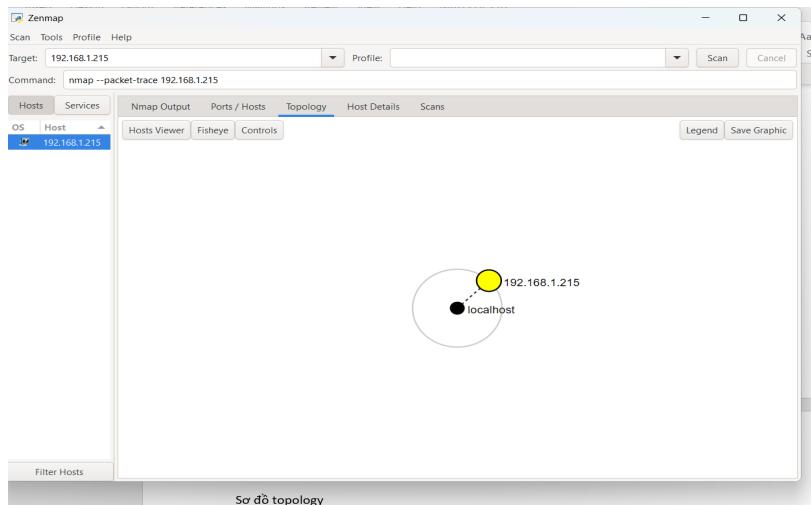
Bước 9: Các cổng đã quét



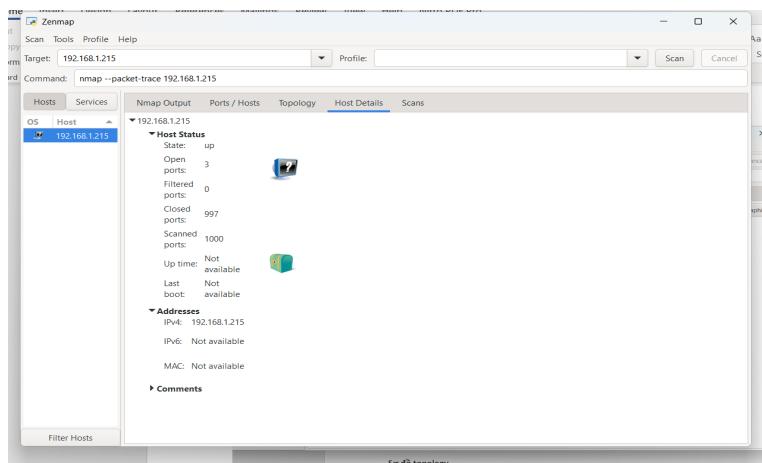
Bước 10: Có thể thấy nhiều cổng được phát hiện hơn so với lệnh quét ban đầu, do --packet-trace cung cấp chi tiết sâu hơn



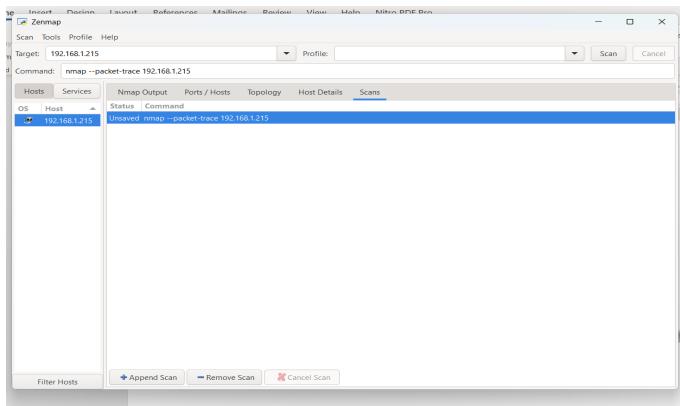
Bước 11: Sơ đồ topology



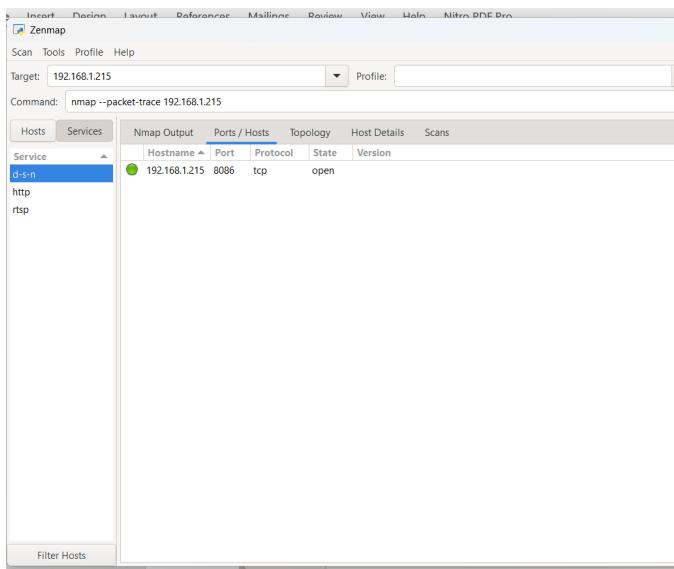
Bước 12: Host detail



Bước 13: Tab scans



Bước 14: Tab service



Bước 15: Thực hiện Slow Comprehensive Scan

```

Target: 192.168.1.215
Profile: Slow comprehensive scan
Command: nmap -sS -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 192.168.1.215

```

NSM: Script Pre-scanning.

Initiating NSE at 20:54

NSM: [shodan] Network scan failed immediately

NSM: [shodan] Error: Please specify your shodan API key with the shodan-api.apikey argument

NSM: [mtraces] A source IP must be provided through fromip argument.

No profinet devices in the submit

Completed NSE at 20:54, 10.48s elapsed

Initiating NSE at 20:54

Completed NSE at 20:54, 0.00s elapsed

Initiating NSE at 20:54

Completed NSE at 20:54, 0.00s elapsed

Pre-scanning 1 host

[multicast-profinet-discovery: 0]

[hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See <https://www.robtex.com/api/>]

[targets-aam: 0]

[targets-aam: aam is a mandatory parameter]

[http-robtex-sharedns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See <https://www.robtex.com/api/>]

Initiating Ping Scan at 20:54

Scanning 192.168.1.215 (7 ports)

Completed Ping Scan at 20:54, 0.12s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host at 20:54

Completed Parallel DNS resolution of 1 host at 20:54, 0.03s elapsed

Initiating SYN Stealth Scan at 20:54

Scanning 192.168.1.215 (1000 ports)

Discovered open port 8086/tcp on 192.168.1.215

Discovered open port 554/tcp on 192.168.1.215

Discovered open port 8086/tcp on 192.168.1.215

Completed SYN Stealth Scan at 20:54, 0.68s elapsed (1000 total ports)

Initiating UDP Scan at 20:54

Scanning 192.168.1.215 (1000 ports)

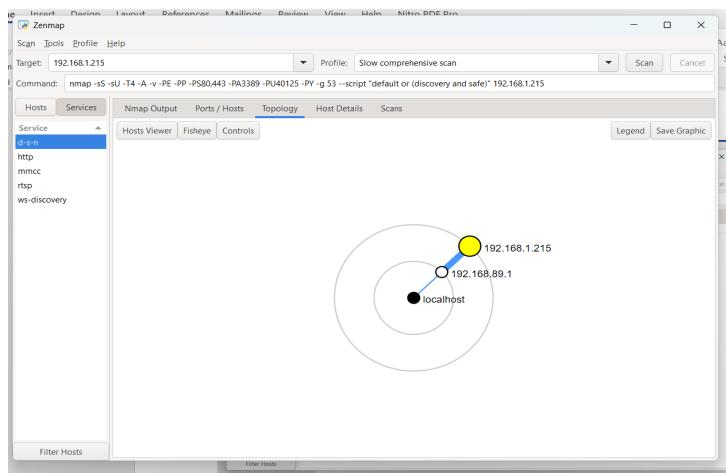
Completed UDP Scan at 20:54, 2.27s elapsed (1000 total ports)

Initiating Service scan at 20:54

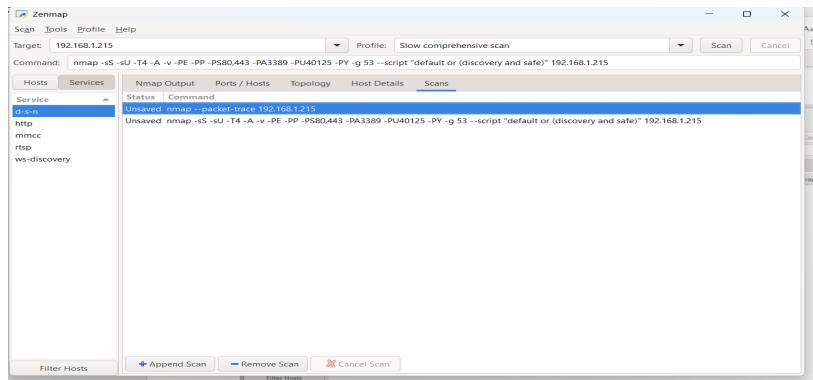
Bước 16: Port và host

Hostname	Port	Protocol	State	Version
192.168.1.215	8086	tcp	open	

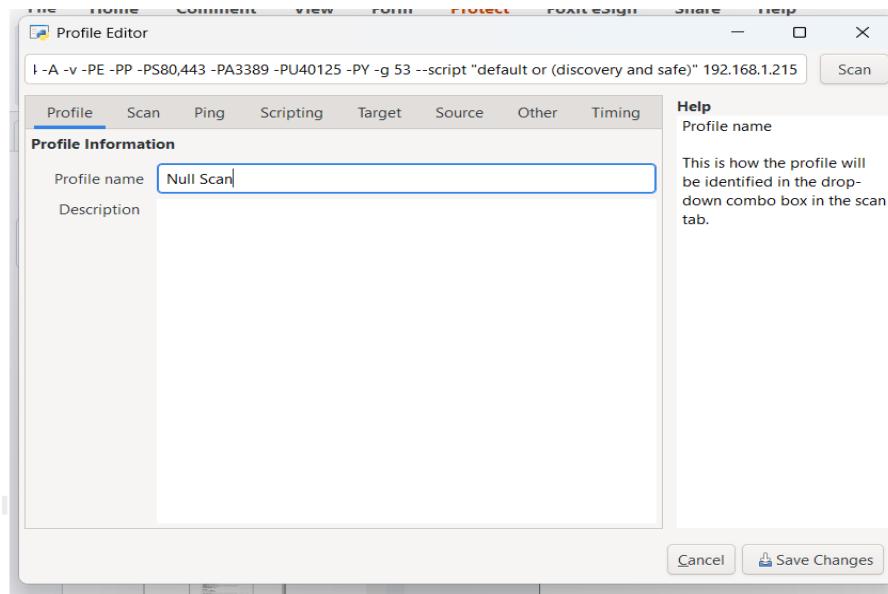
Bước 17: Topology



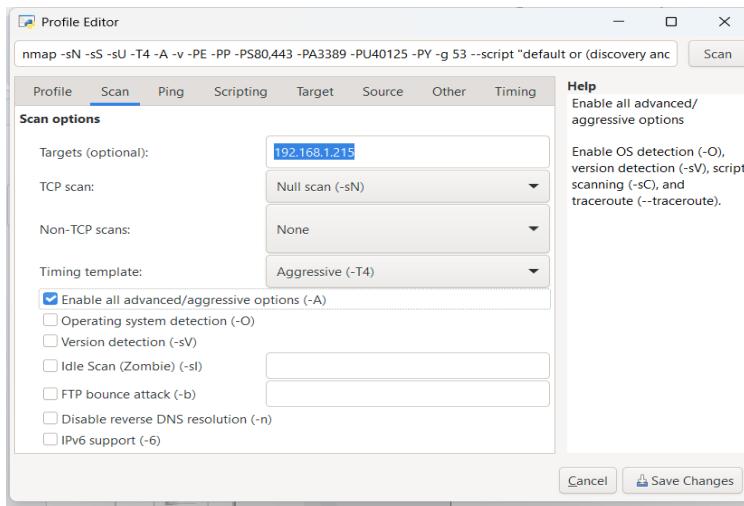
Bước 18: Scans



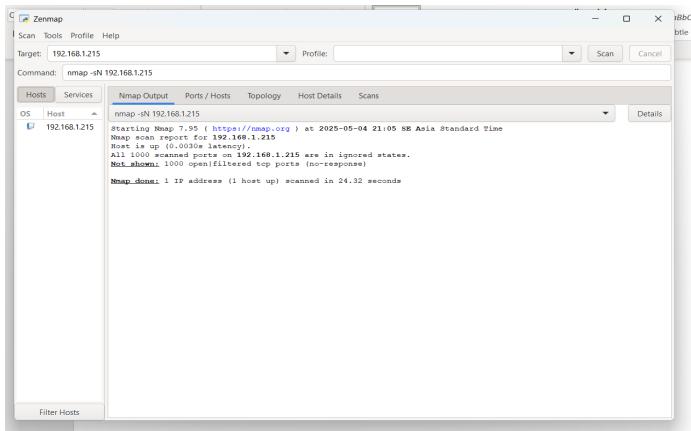
Bước 19: Tạo mới profile null scan



Bước 20:

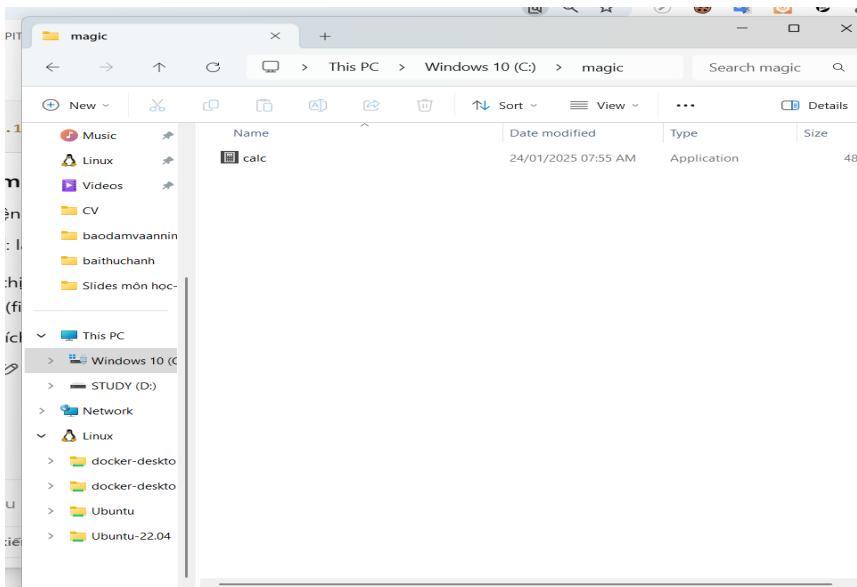


Bước 21: Quét mạng với null scan

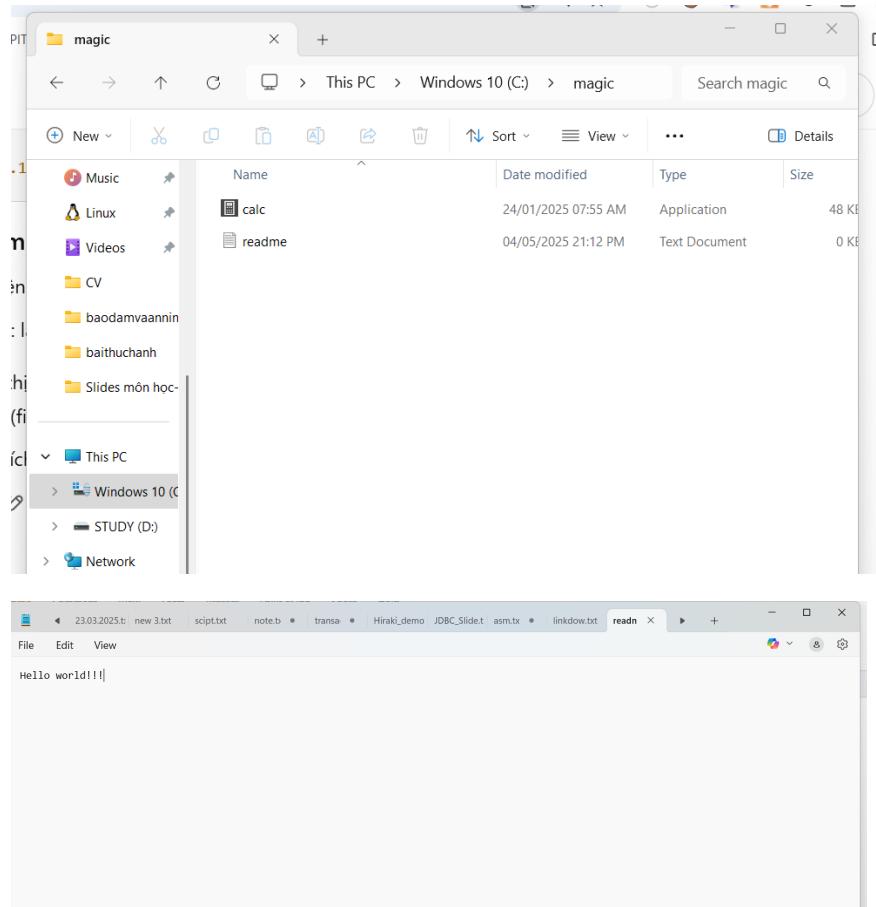


Bài 4: Ân file sử dụng NTFS Streams

Bước 1: Copy calc.exe từ C:\Windows\System32 sang C:\magic



Bước 2: Tạo file readme và gõ nội dung hello world



Bước 3: Dùng lệnh dir để liệt kê các file và thư mục con

```
C:\magic>dir
Volume in drive C is Windows 10
Volume Serial Number is 3A7F-A12C

Directory of C:\magic

04/05/2025  21:12 PM    <DIR>      .
24/01/2025  07:55 AM      49,152 calc.exe
04/05/2025  21:12 PM           14 readme.txt
                  2 File(s)      49,166 bytes
                  1 Dir(s)  28,260,614,144 bytes free

C:\magic>
```

Bước 4: Ân file calc.exe bên trong readme.txt

```
C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe
C:\magic>dir
Volume in drive C is Windows 10
Volume Serial Number is 3A7F-A12C

Directory of C:\magic

04/05/2025  21:12 PM    <DIR>
24/01/2025  07:55 AM           49,152 calc.exe
04/05/2025  21:15 PM           14 readme.txt
               2 File(s)      49,166 bytes
               1 Dir(s)  28,251,107,328 bytes free

C:\magic>
```

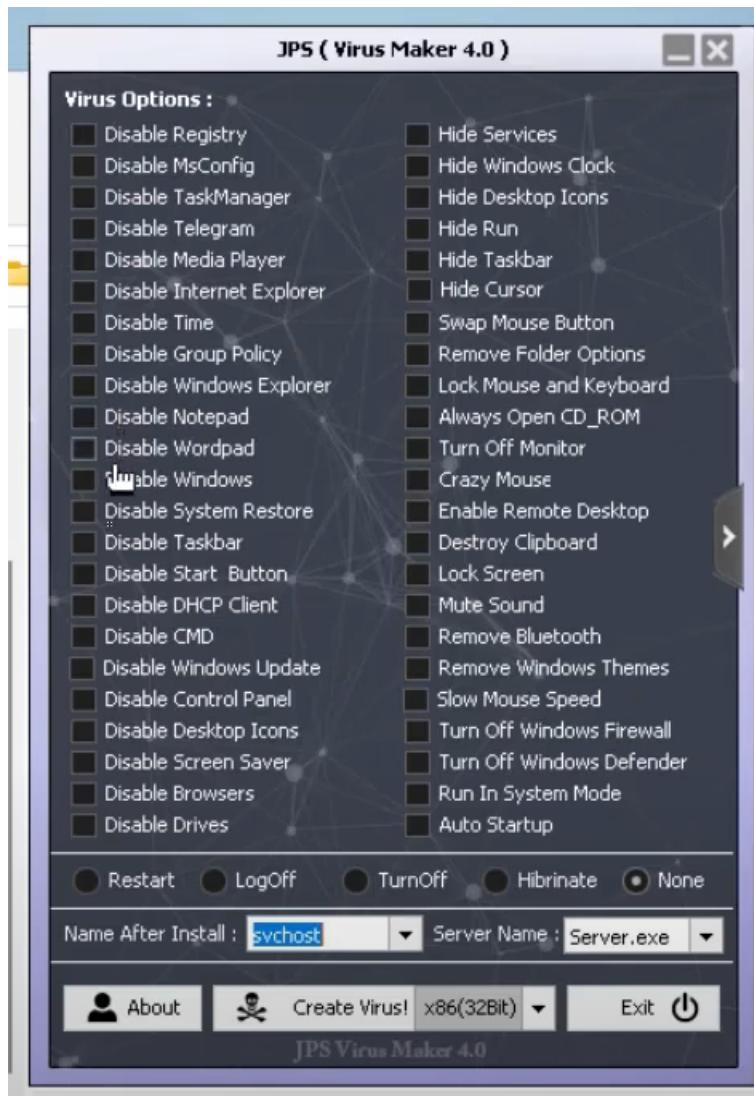
Bước 5: Tạo shorcut vfa gõ backdor thì calc.ext sẽ được bật

```
C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<==>> readme.txt:calc.exe

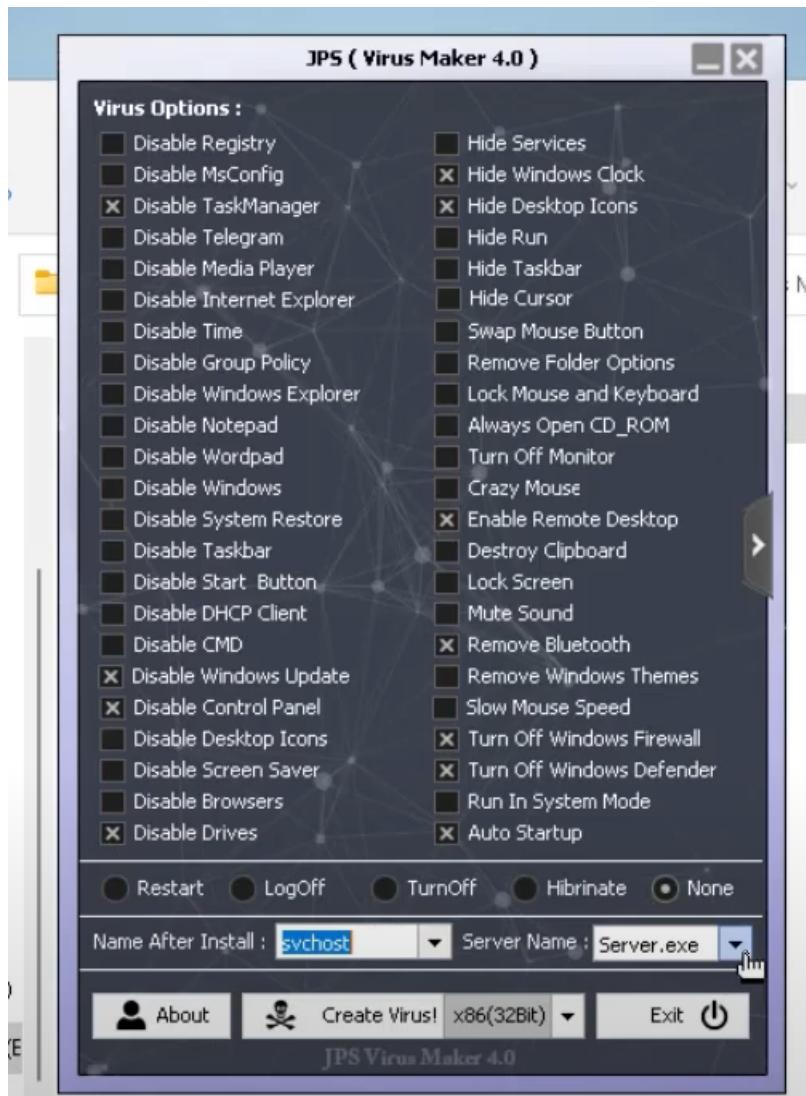
C:\magic>
```

Bài 5: Tạo Virus với công cụ JPS Virus Marker Tool

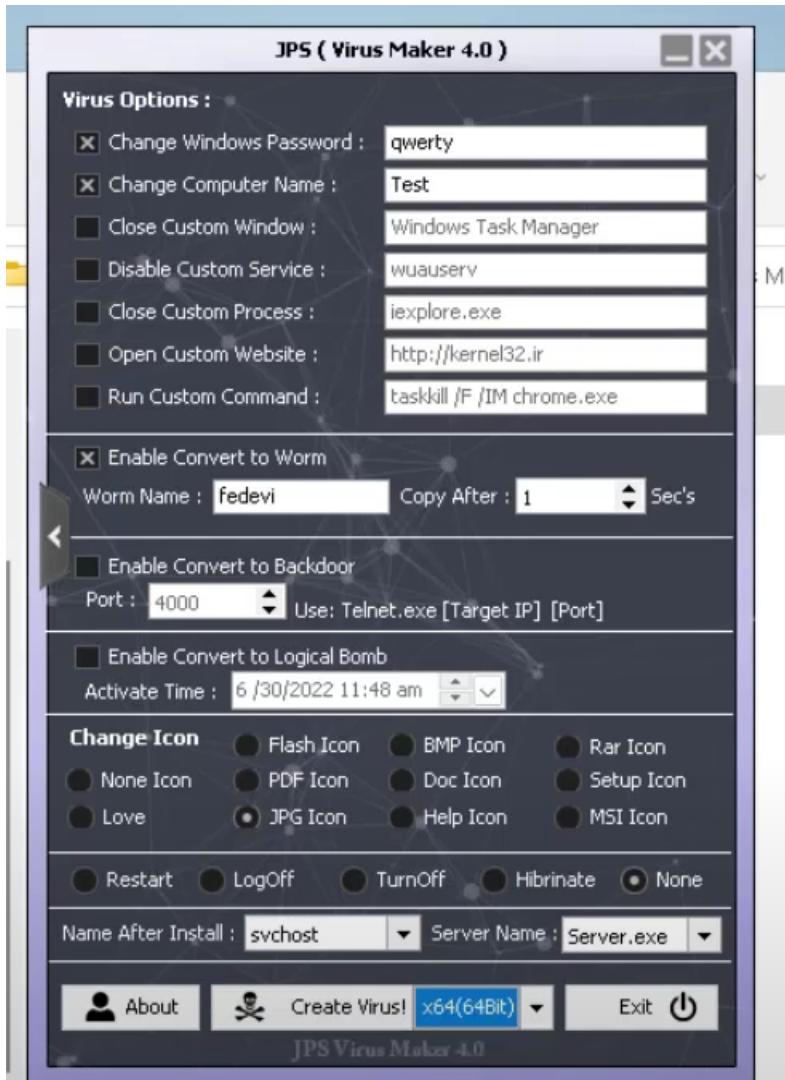
Bước 1: Cài đặt JPS



Bước 2: Chọn các thao tác mã độc



Bước 3: Setup các tham số



Bước 4: Hoàn thành

