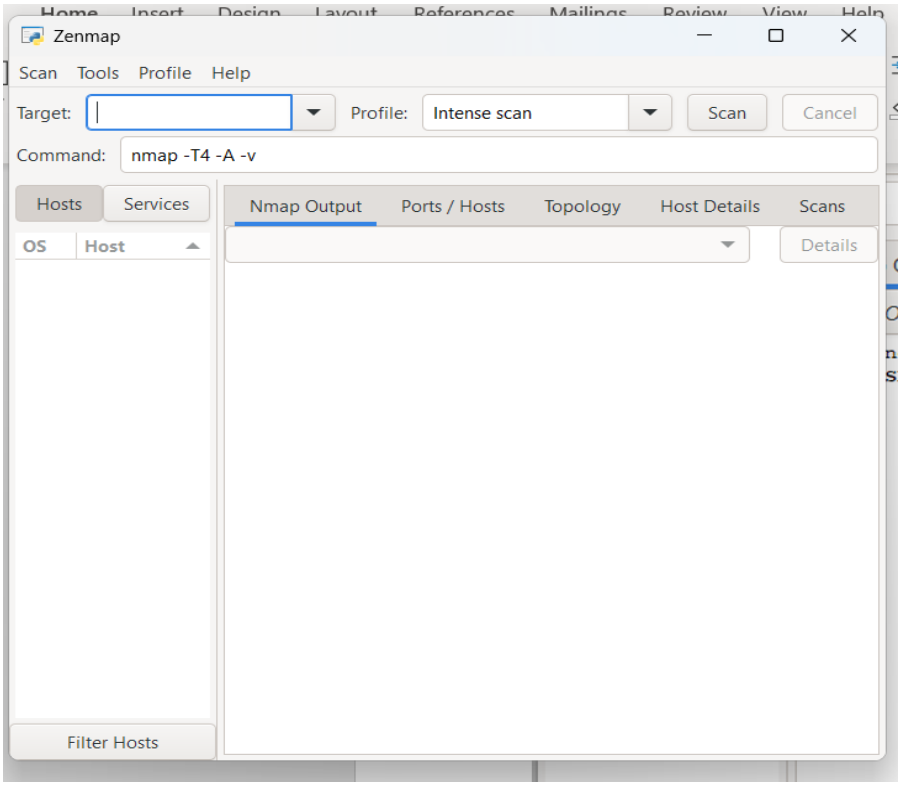
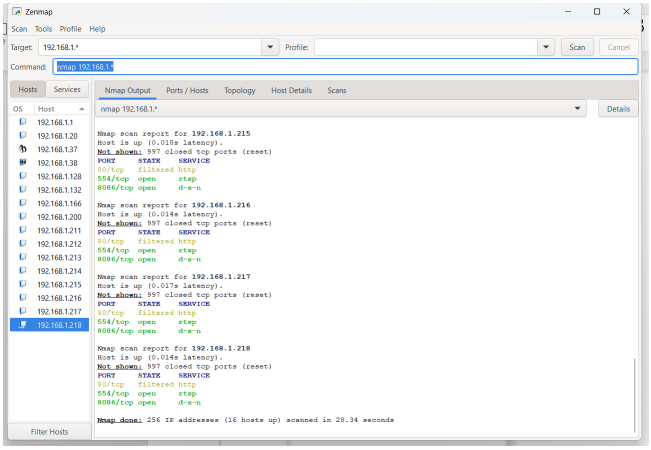
Bài Thực hành 1B

Bài 3: Quét mạng sử dụng Nmap

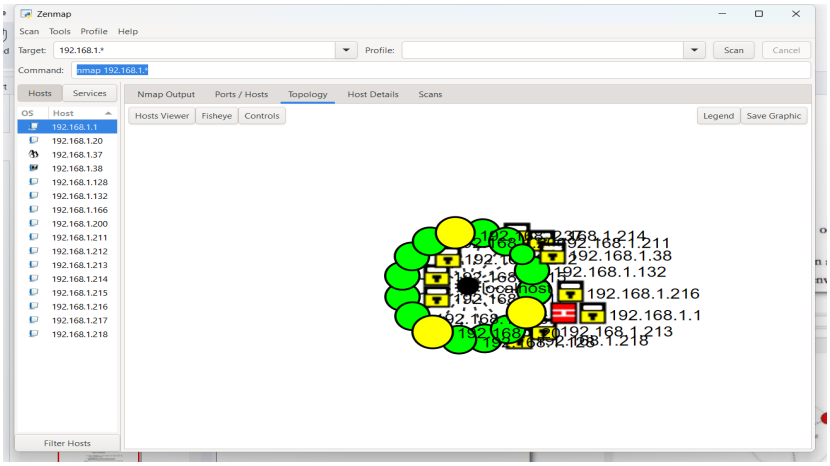
Bước 1: Setup Nmap



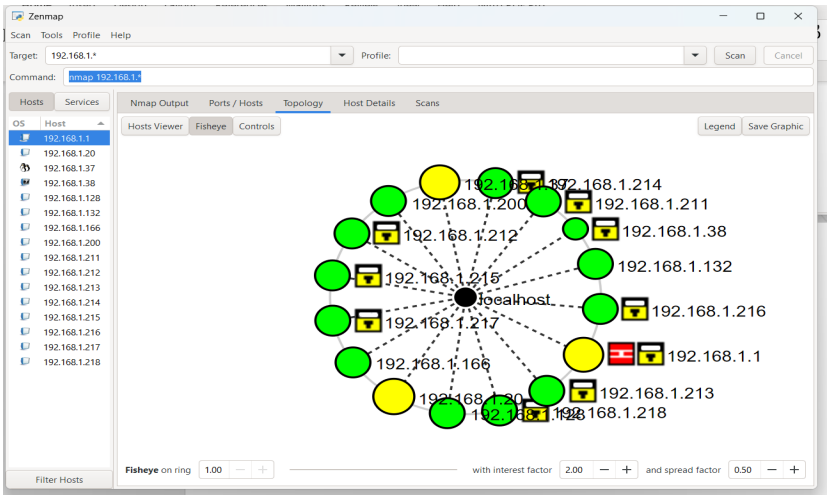
Bước 2: Nhập Nmap 192.168.1.* vào ô command và nhấn scan để quét các máy ảo trong mạng



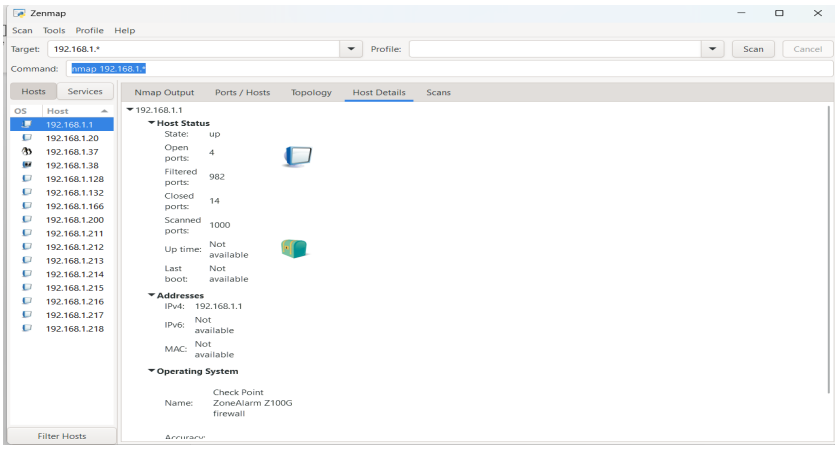
Bước 3: Sơ đồ mạng



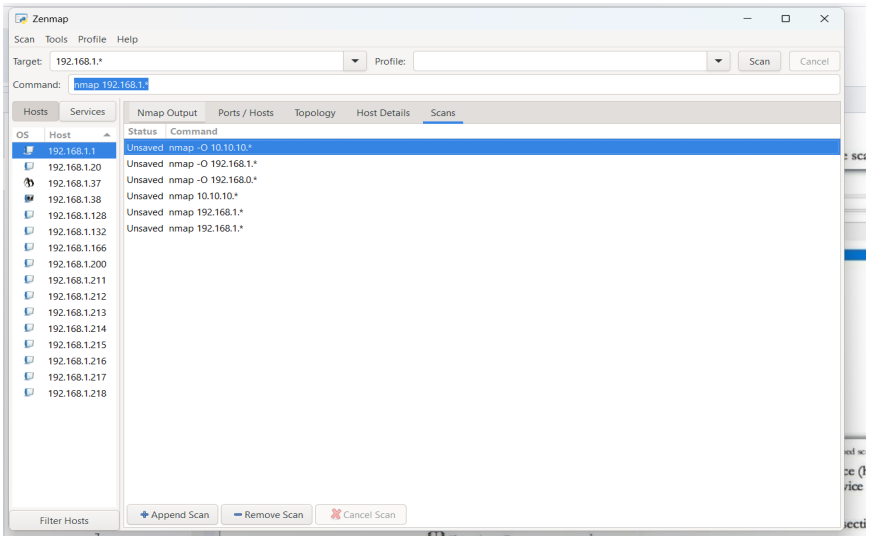
Bước 4: Chế độ fiheye



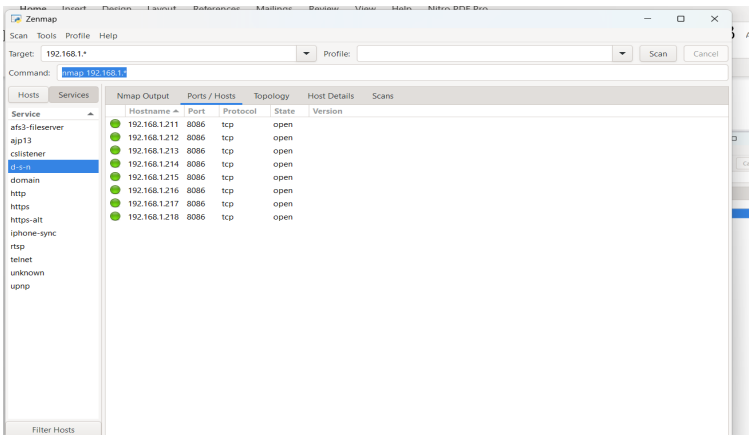
Bước 5: Host detail



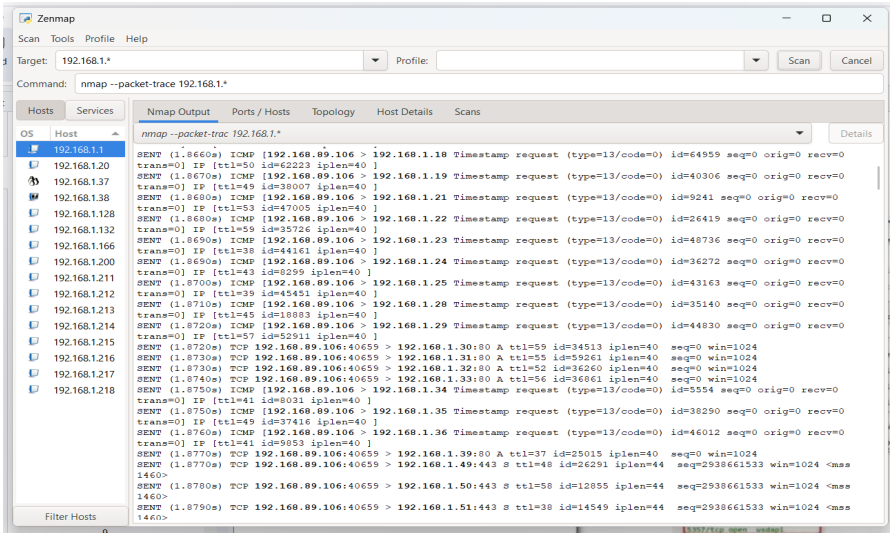
Bước 6: Trạng thái quét



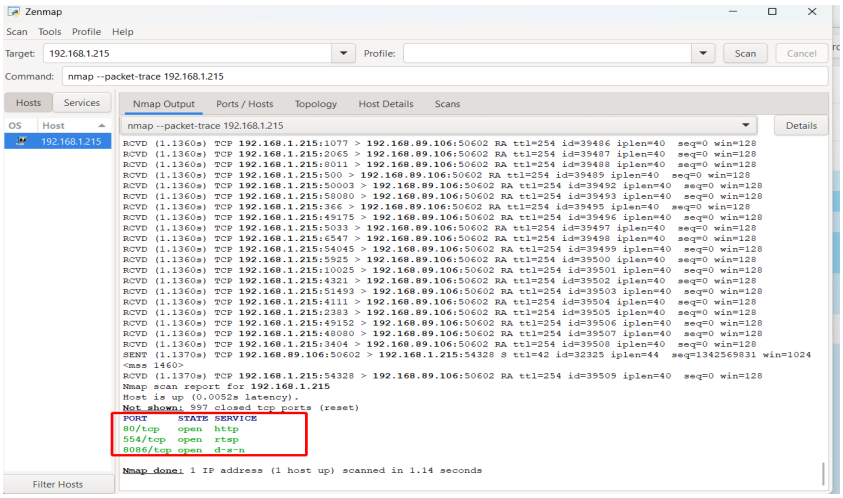
Bước 7: Chi tiết dịch vụ theo cổng



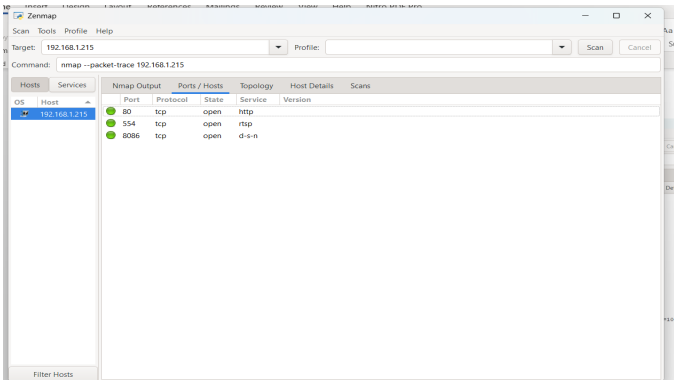
Bước 8: Dùng nmap --packet-trace 192.168.1.* để theo dõi mọi gói tin được gửi và nhận bởi Nmap



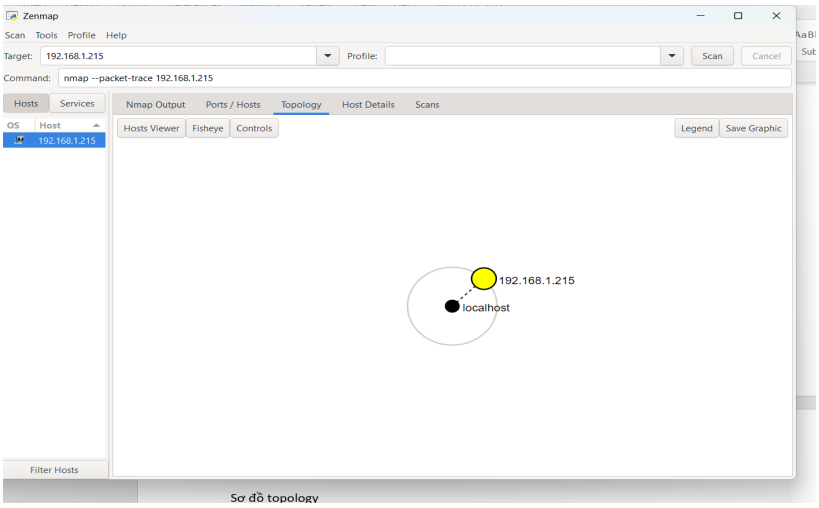
Bước 9: Các cổng đã quét



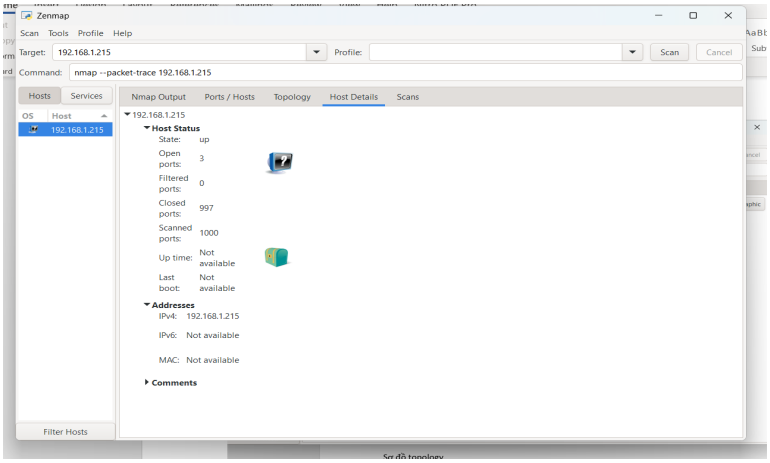
Bước 10: Có thể thấy nhiều cổng được phát hiện hơn so với lệnh quét ban đầu, do --packet-trace cung cấp chi tiết sâu hơn



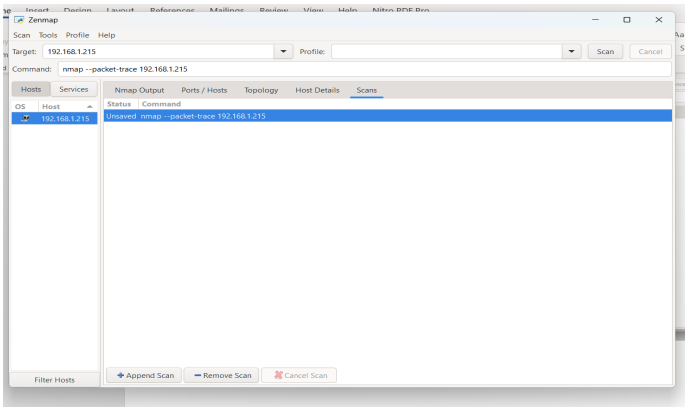
Bước 11: Sơ đồ topology



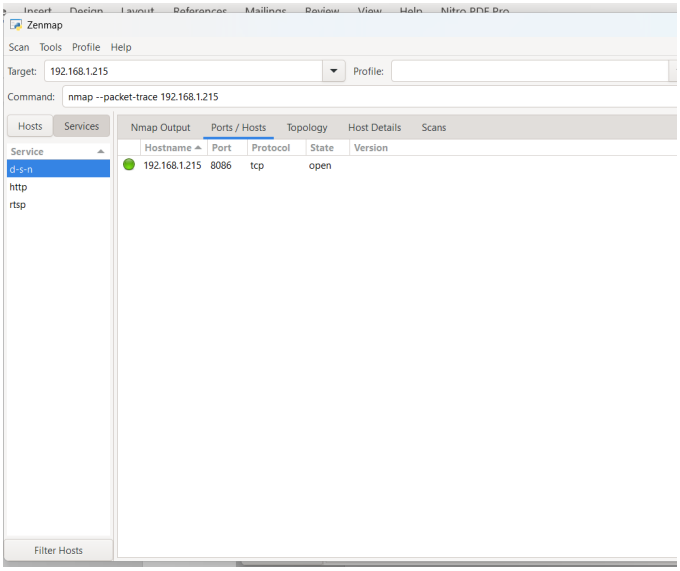
Bước 12: Host detail



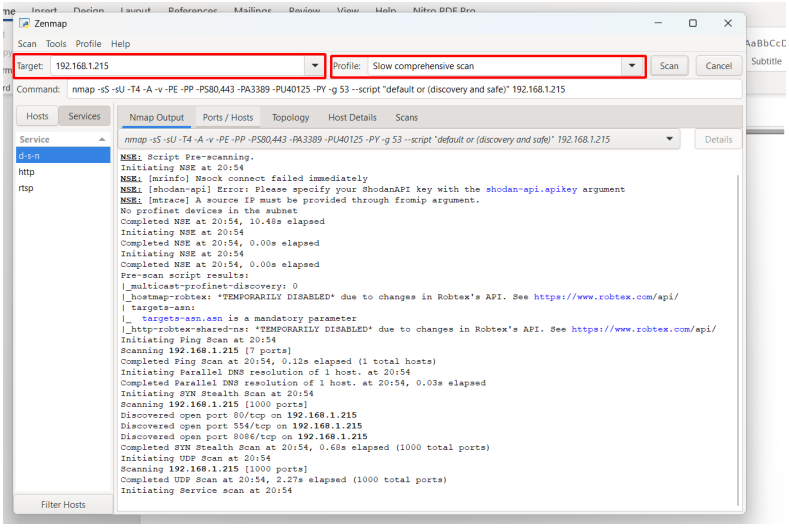
Bước 13: Tab scans



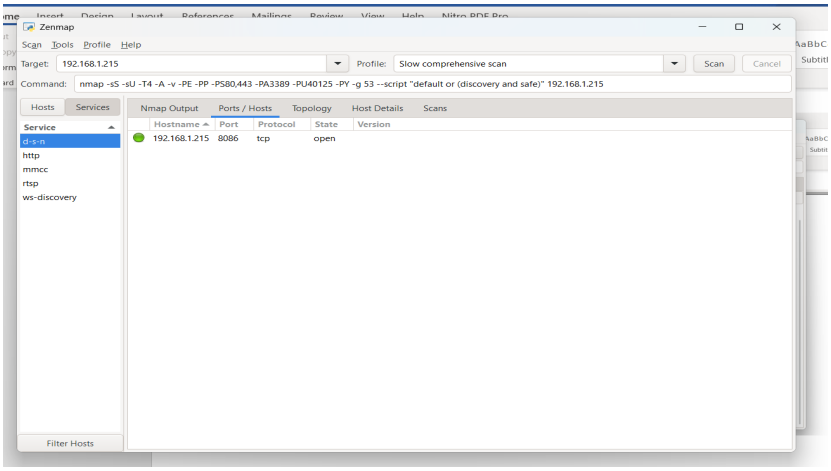
Bước 14: Tab service



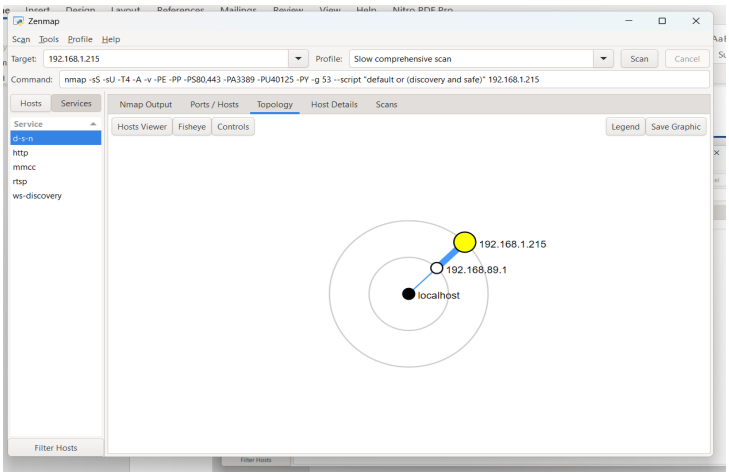
Bước 15: Thực hiên Slow Comprehensive Scan



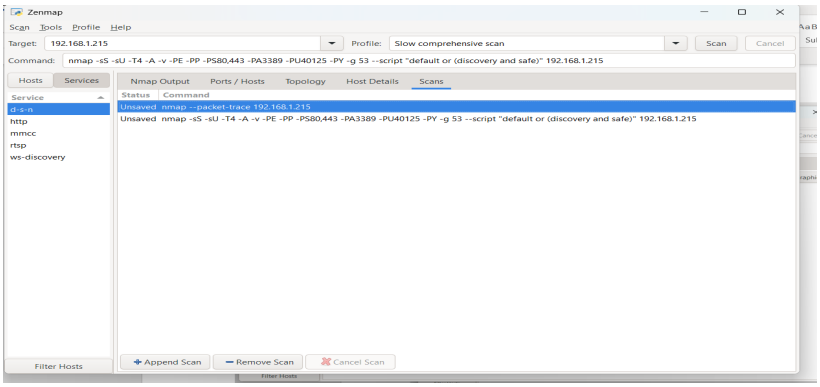
Bước 16: Port và host



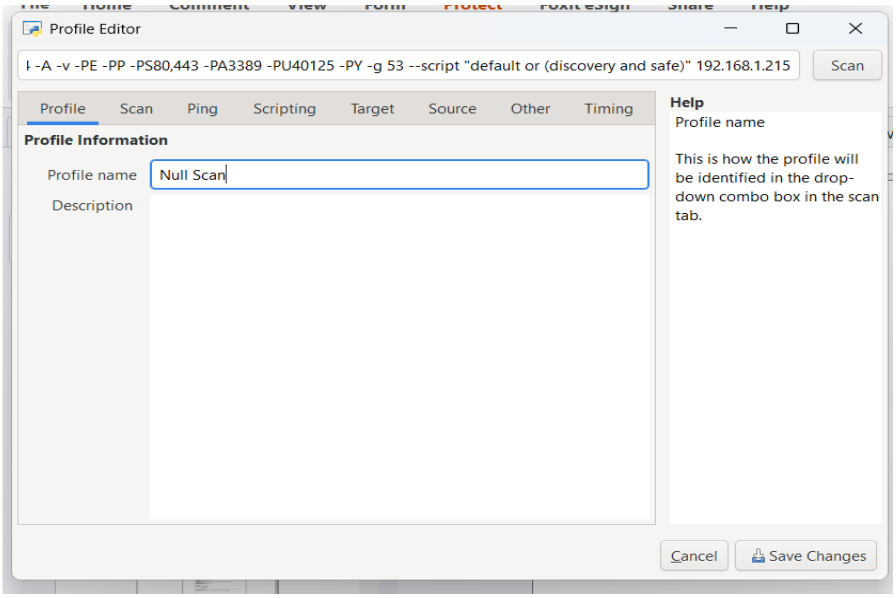
Bước 17: Topology



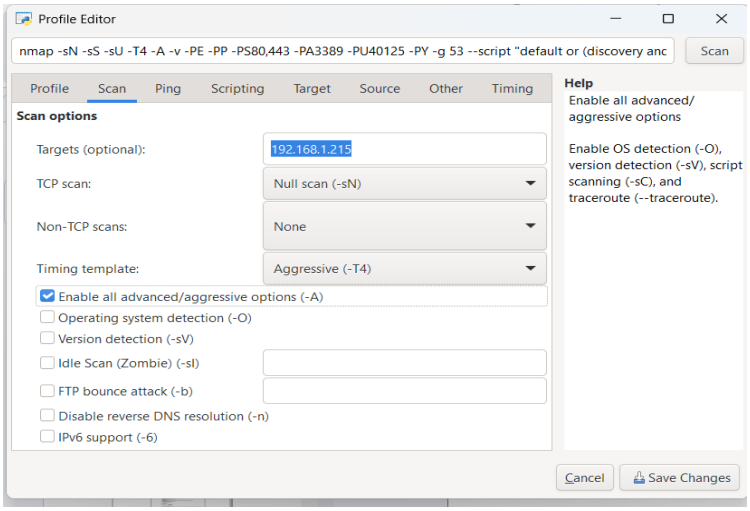
Bước 18: Scans



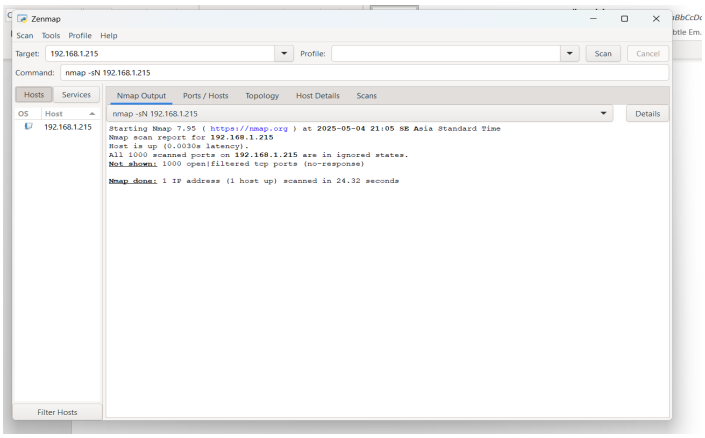
Bước 19: Tạo mới profile null scan



Bước 20:

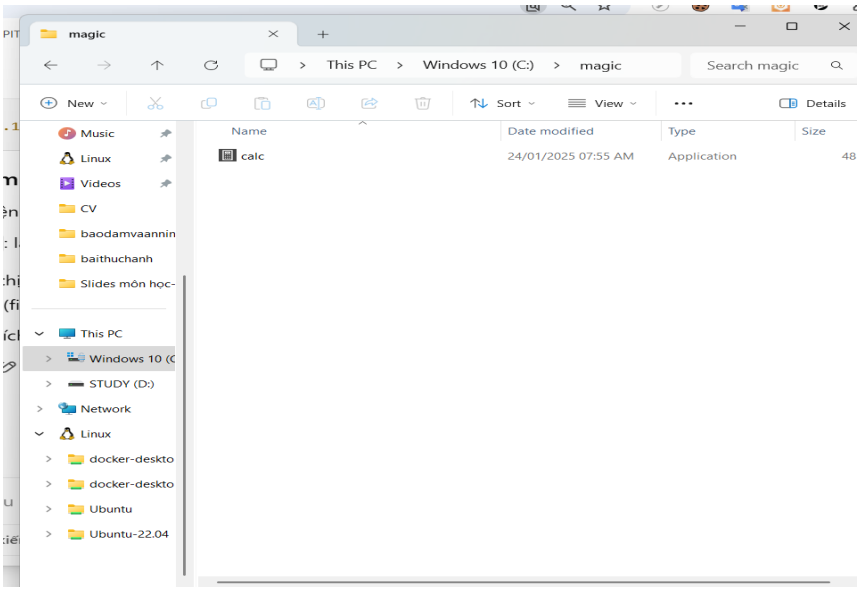


Bước 21: Quét mạng với null scan

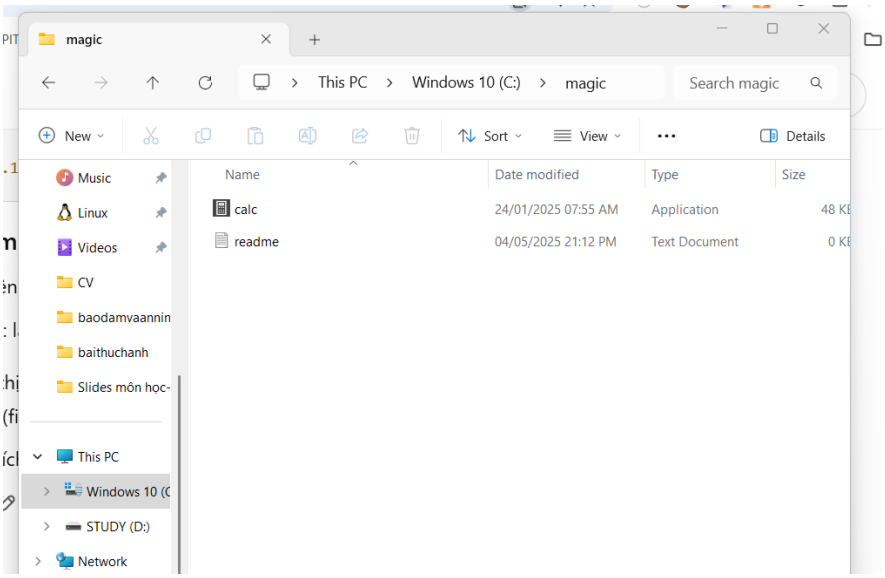


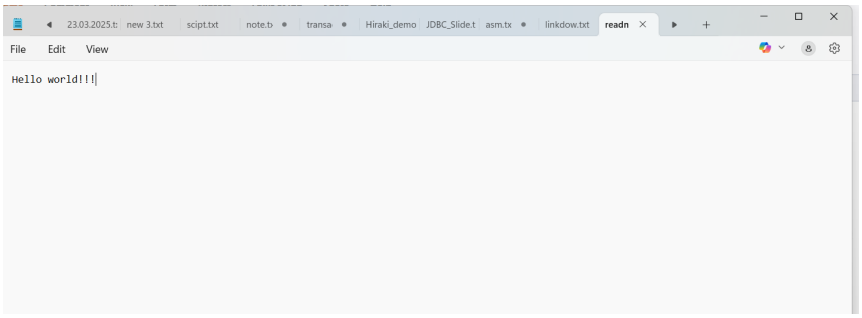
Bài 4: Ẩn file sử dụng NTFS Streams

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



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

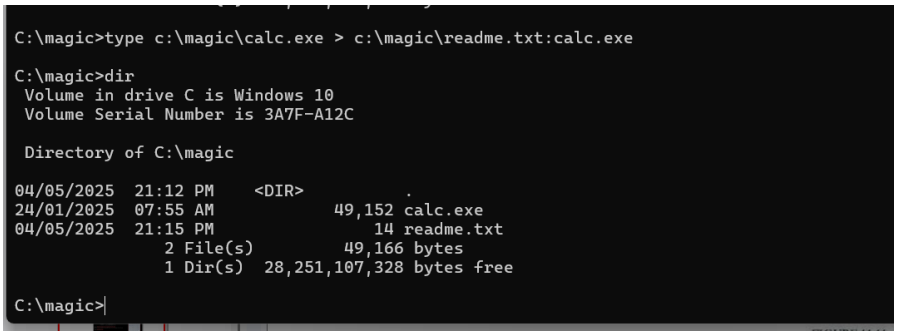




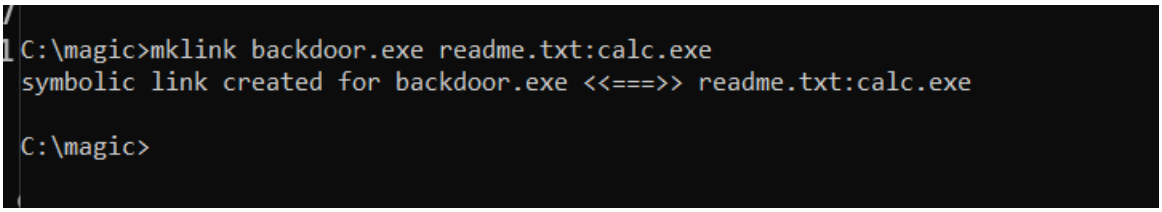
Bước 3: Dùng lệnh dir để liệt kê các file và thư mục con

```
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: Ẩn file calc.exe bên trong readme.txt

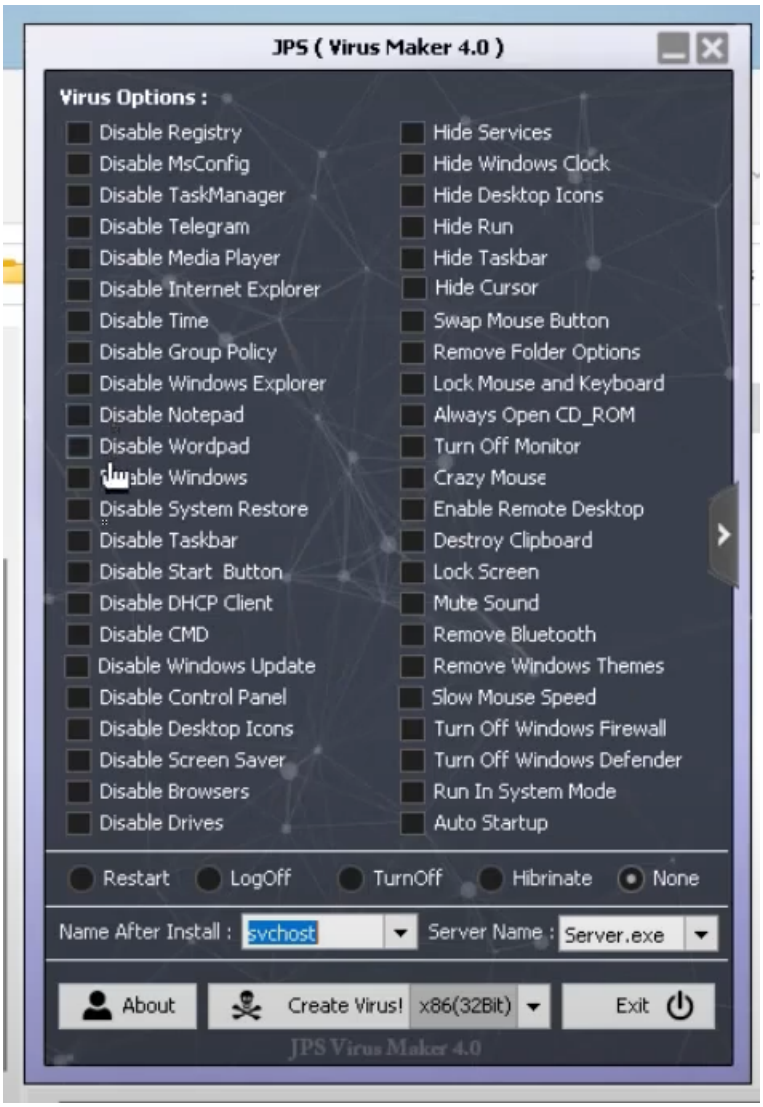


Bước 5: Tạo shorcut vfa gõ backdor thì calc.ext sẽ được bật

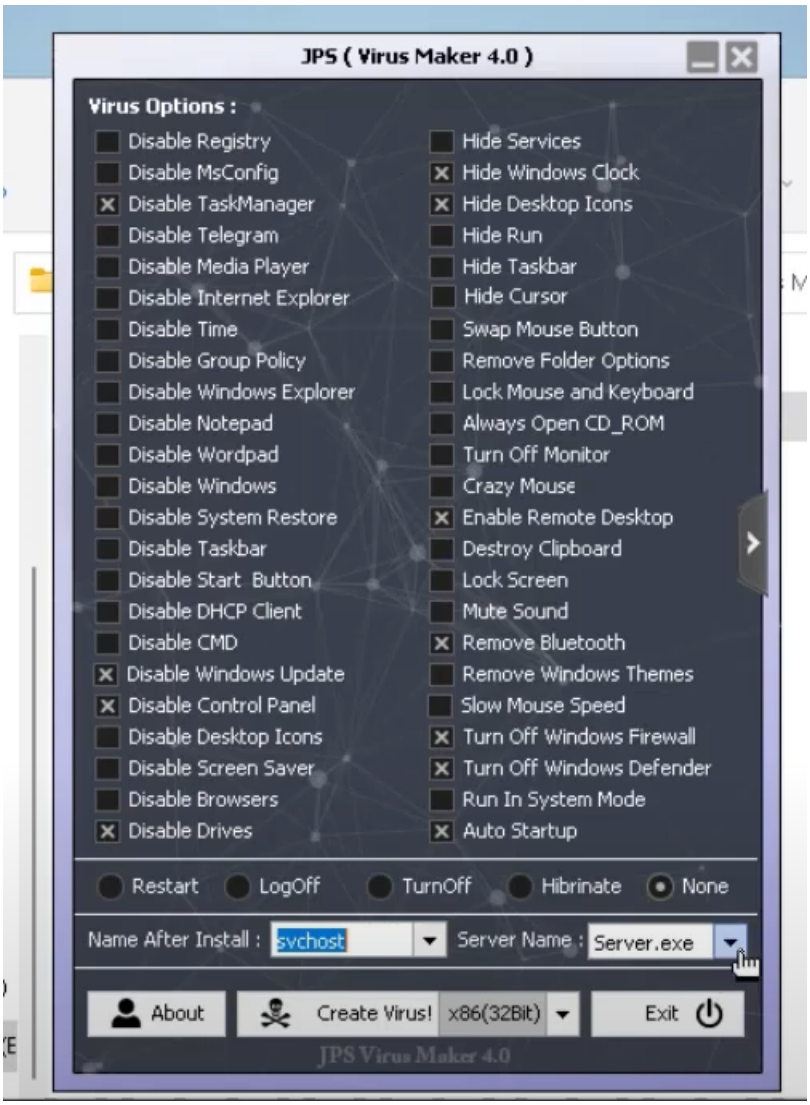


Bài 5: Tạo Virus với công cụ JPS Virus Marker Tool

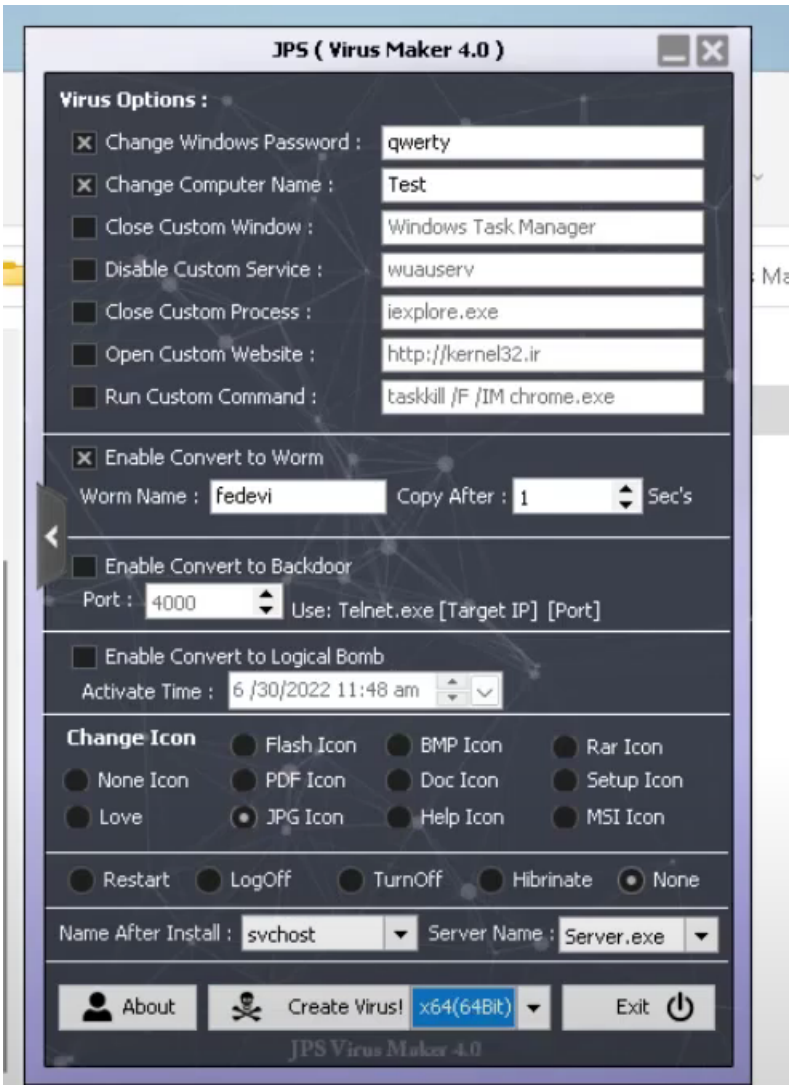
Bước 1: Cài đặt JPS



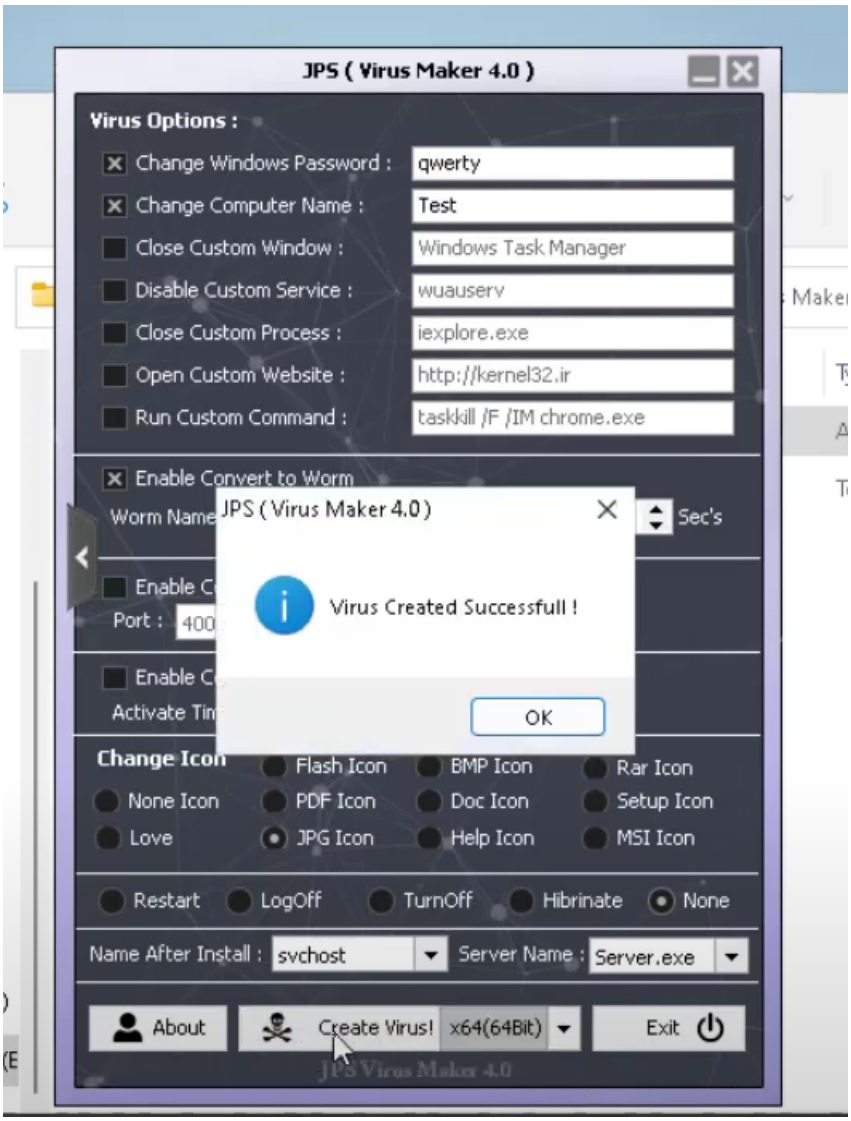
Bước 2: Chọn các thao tác mã độc



Bước 3: Setup các tham số



Bước 4: Hoàn thành


JPS (Virus Maker 4.0)
Virus Options :
Change Windows Password :
qwerty
Change Computer Name :
Test
Close Custom Window :
Windows Task Manager
Disable Custom Service :
wuauserv
Close Custom Process :
iexplore.exe
Open Custom Website :
http://kernel32.ir
Run Custom Command :
taskkill /F /IM chrome.exe
Enable Convert to Worm
Worm Name
Sec's
Enable C
Port :
400
Enable C
Activate Tin
JPS (Virus Maker 4.0)
Virus Created Successfull !
OK
Change Icon
Flash Icon
BMP Icon
Rar Icon
None Icon
PDF Icon
Doc Icon
Setup Icon
Love
JPG Icon
Help Icon
MSI Icon
Restart
LogOff
TurnOff
Hibrinate
None
Name After Install :
svchost
Server Name :
Server.exe
About
Create Virus!
x64(64Bit)
Exit
JPS Virus Maker 4.0