Lab 2: Kiểm tra thông tin trên mạng bằng công cụ SuperScan

A. Lý Thuyết

Tấn công do thám là gì ?

1. Tấn công do thám

Là hình thức tấn công nhằm thu thập các thông tin về hệ thống mục tiêu, từ đó phát hiện ra các điểm yếu. Tấn công do thám thường để làm bàn đạp cho cuộc tấn công truy cập hoặc tấn công từ chối dịch vụ về sau.

Cách thức mà kẻ tấn công tiến hành như sau: đầu tiên dùng kỹ thuật ping sweep để kiểm tra xem hệ thống nạn nhân đang có những địa chỉ IP nào đang hoạt động. Sau đó kẻ tấn công sẽ kiểm tra những dịch vụ đang chạy, những cổng đang mở trên những địa chỉ IP tìm thấy ở trên. Công cụ mà kẻ tấn công thường sử dụng ở bước này là Nmap.

Sau khi xác định được những cổng đang mở, kẻ tấn công sẽ gửi các truy vấn tới các cổng này để biết được thông tin về các phần mềm, hệ điều hành đang chạy. Sau khi có trong tay các thông tin này, kẻ tấn công sẽ tìm cách khai thác các lỗ hổng đang tồn tại trên hệ thống đó. Kẻ tấn công có kinh nghiệm sẽ lựa chọn thời điểm phù hợp để thực hiện việc khai thác lỗ hổng để tránh bị phát hiện.

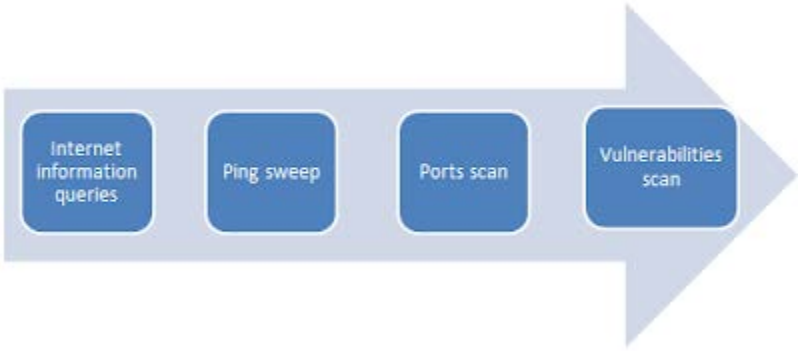
Để tấn công thăm dò, hacker thường dùng các công cụ:

- Truy vấn thông tin Internet
- **Supersan 4.1**
- Ping sweep
- Port Scan
- Packet sniffer

Truy vấn thông tin Internet

Khi hacker muốn tấn công mạng một tổ chức, một công ty, đầu tiên hắn ta sẽ tìm hiểu xem tổ chức hay công ty đó có sở hữu website có tên miền là gì. Sau đó hacker sẽ sử dụng các công cụ tìm

kiếm để truy vấn các thông tin về chủ sở hữu tên miền, địa chỉ (địa lý) gắn với tên miền đó. Thêm nữa, có thể truy ra ai đang sở hữu địa chỉ IP và tên miền đang gắn với địa chỉ IP này.



Ping sweep and port scan

- Là 2 công cụ dùng để phát hiện lỗ hổng trên các thiết bị và hệ thống. Các công cụ này sẽ kiểm tra thông tin về địa chỉ IP, cổng, hệ điều hành, phiên bản hệ điều hành, dữ liệu trên cổng TCP và UDP. Kẻ tấn công sử dụng các thông tin này cho mục đích tấn công.

Ping sweep là kỹ thuật quét một dải địa chỉ IP để phát hiện xem có thiết bị nào đang sở hữu địa chỉ IP trong dải đó. Công cụ ping sweep sẽ gửi gói tin ICMP echo request tới tất cả các địa chỉ IP trong dải và chờ đợi gói tin ICMP echo reply phản hồi từ các thiết bị.

Port scan là công cụ quét cổng. Mỗi dịch vụ chạy trên máy đều gắn với một cổng (well-known port). Công cụ quét cổng sẽ quét một dải các cổng để phát hiện xem cổng nào đang lắng nghe yêu cầu. Nguyên lý là gửi bản tin đến cổng và chờ đợi phản hồi. Nếu có phản hồi từ cổng nào đó tức là cổng đó đang được sử dụng.

Kẻ tấn công sẽ sử dụng kết hợp các công cụ trên theo nguyên lý: đầu tiên truy vấn thông tin trên Internet để lấy thông tin về địa chỉ IP của tên miền mà hắn muốn tấn công. Tiếp đó dùng công cụ ping sweep để quét tìm các máy đang hoạt động. Tiếp theo sử dụng công cụ port scan để lấy được thông tin về các cổng và dịch vụ đang hoạt động trên các máy. Sau đó kẻ tấn công tiếp tục rà soát các dịch vụ này để tìm ra những điểm yếu có thể khai thác.

Packet Sniffer

Video Packet Tracer 6.2 có dùng thiết bị sniffer

Là một công cụ cho phép cấu hình card mạng ở chế độ hỗn độn (promiscuous mode), là chế độ có thể chặn bắt các gói tin bất kỳ chạy trên mạng LAN. Với công cụ này, kẻ tấn công có thể bắt các gói tin đang được gửi qua lại trên mạng LAN và phân tích. Nếu gói tin không được mã hóa thì kẻ tấn công sẽ dễ dàng đọc được nội dung.

Tình huống ở đây có thể là một nhân viên IT bất mãn với sếp, anh ta muốn dò la các thông tin từ máy tính của sếp. Bằng cách sử dụng công cụ packet sniffer, anh ta có thể chặn bắt các gói tin được gửi trong mạng LAN và lọc ra gói tin có địa chỉ nguồn từ máy của sếp, sau đó đọc nội dung.

Một điều lưu ý ở đây là để có thể chặn bắt gói tin, máy của kẻ tấn công phải nằm cùng subnet với hệ thống nạn nhân hoặc chiếm được quyền quản lý thiết bị switch.

Một công cụ Sniffer thường được sử dụng là wireshark (https://forum.whitehat.vn/threads/8165-Su-dung-Wireshark-de-phan-tich-goi-du-lieu-trong-he-thong-mang.html)

2. Cách phòng chống tấn công do thám

Trong thực tế cuộc sống, nếu người bảo vệ phát hiện một kẻ thường xuyên qua lại rình mò trước căn biệt thự của một đại gia chủ thì sẽ nghi vấn và cảnh giác. Tương tự như vậy với hệ thống mạng. Bạn cần có hệ thống phát hiện và ngăn chặn xâm nhập. Hệ thống này nếu thấy số lượng các gói tin ICMP echo request/s nhiều bất thường (do ping sweep) thì sẽ cảnh báo đến người quản trị (admin). Khi admin nhận được thông tin cảnh báo, sẽ rà soát lại hệ thống:

- Xác minh và quyết định việc ngăn chặn kết nối từ các IP do thám.

- Tắt những dịch vụ không cần thiết.

- Update các bản vá lỗi cho hệ điều hành và ứng dụng.

- Thay đổi mật khẩu quản trị nếu thấy cần thiết.

Còn nếu việc do thám xuất phát từ một máy tính nội bộ (https://forum.whitehat.vn/archive/index.php/t-4739.html) thì ngay từ khi xây dựng hệ thống mạng, admin cần nghĩ đến các giải pháp như:

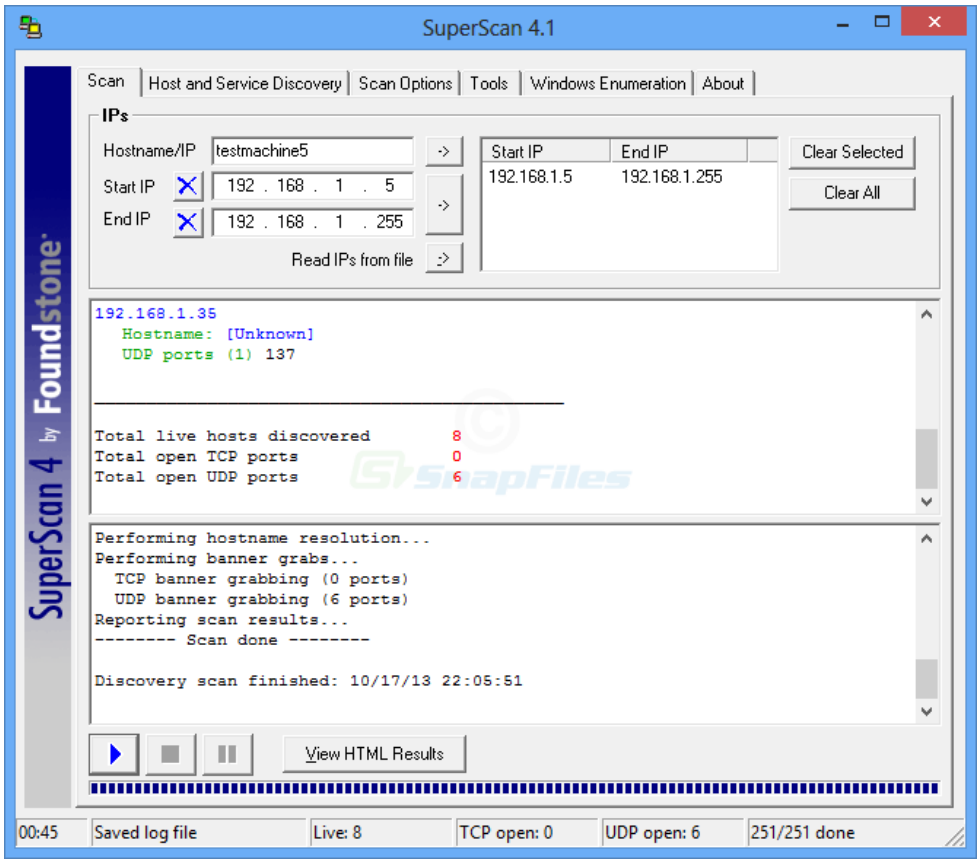
- VLAN: nhóm các máy tính của các phòng ban vào các VLAN khác nhau

- Củng cố an ninh trên các thiết bị mạng (sẽ đề cập ở các bài viết sau) để tránh bị chiếm quyền điều khiển.

- Mã hóa thông tin nhạy cảm trước khi gửi đi.

3. Phần mềm Supersan 4.1

SuperScan là phần mềm quét cổng dựa trên kết nối miễn phí được thiết kế để phát hiện các cổng TCP và UDP đang mở trên máy tính đích, xác định dịch vụ nào đang chạy trên các cổng đó và chạy các truy vấn như whois, ping, ICMP traceroute và Hostname.



Superscan 4.0, là bản cập nhật được viết lại mới hoàn toàn so với các phiên bản Superscan khác (phiên bản 3, phát hành năm 2000), có tính năng liệt kê cửa sổ, có thể liệt kê nhiều thông tin quan trọng liên quan đến Microsoft Windows như:

- Thông tin NetBIOS

- Tài khoản Người dùng và Nhóm
- Mạng chia sẻ
- Miền đáng tin cậy
- Dịch vụ - đang chạy hoặc đã dừng

Superscan là một công cụ được sử dụng bởi các quản trị viên hệ thống, cracker và những người trong lĩnh vực an ninh mạng dùng để đánh giá tính bảo mật của hệ thống mạng máy tính. Quản trị viên hệ thống có thể sử dụng nó để kiểm tra các cổng mở trái phép có thể có trên mạng máy tính của họ, trong khi những kẻ tấn công thì sử dụng Superscan để quét các cổng không an toàn nhằm truy cập bất hợp pháp vào hệ thống.

B. Thực Hành

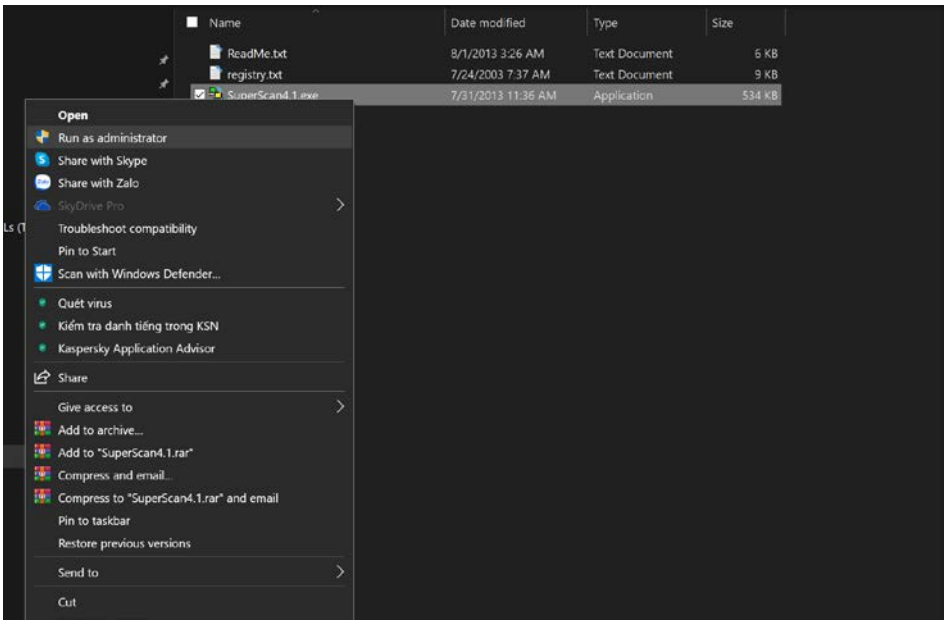
1. Mục Đích

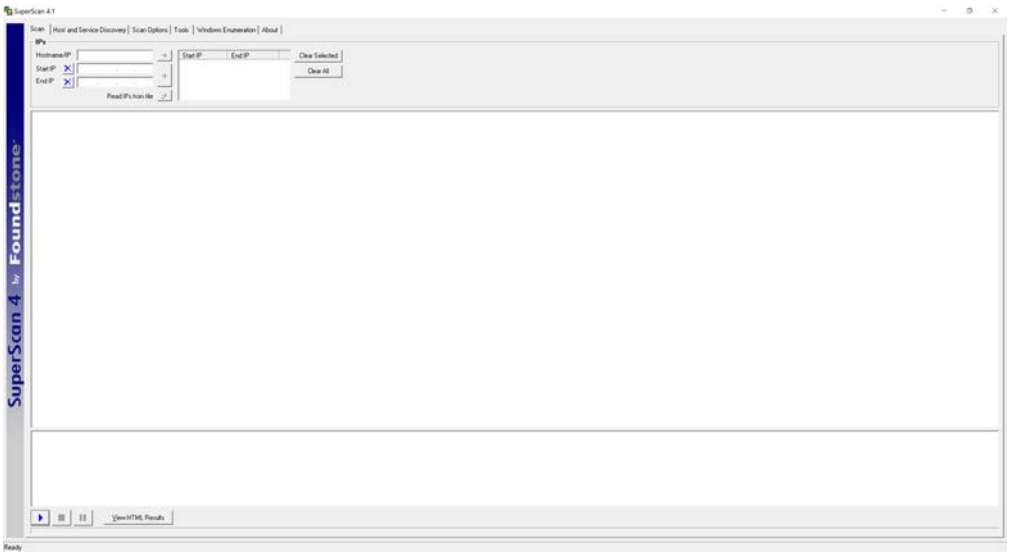
Trong bài lab này chúng ta sẽ tiến hành kiểm tra thông tin trên mạng bằng công cụ SuperScan. Cụ thể hơn, chúng ta sẽ dùng Super Scan để quét 1 IP và xác định cá lỗ hổng có thể xâm nhập vào hệ thống thông qua các port mà phần mềm xác định mở.

Chúng ta có thể down tool Super Scan tại www.foundstone.com

2. Demo Tiến Hành Các Bước Tham Dò với website www.chotot.com

Bước 1: Sau khi down Super Scan về máy, bạn chạy chương trình với **Run as Administrator** như hình dưới:





Bước 2: Dò tìm thông số một IP

Hostname/IP: Điền vào IP muốn quét (hoặc địa chỉ một trang web : www.vnexpress.net)

Hoặc bạn cũng có thể Scan cả 1 range IP:

- Start IP : IP bắt đầu

- End IP : IP kết thúc

Để bắt đầu quét ta click vào nút start ở góc trái bên dưới

Ngoài ra Super Scan còn có các options khác như:

- Host and Services Discovery: Dùng để thay đổi số port bạn muốn quét của IP đó hoặc dựa trên danh sách Port list có sẵn.

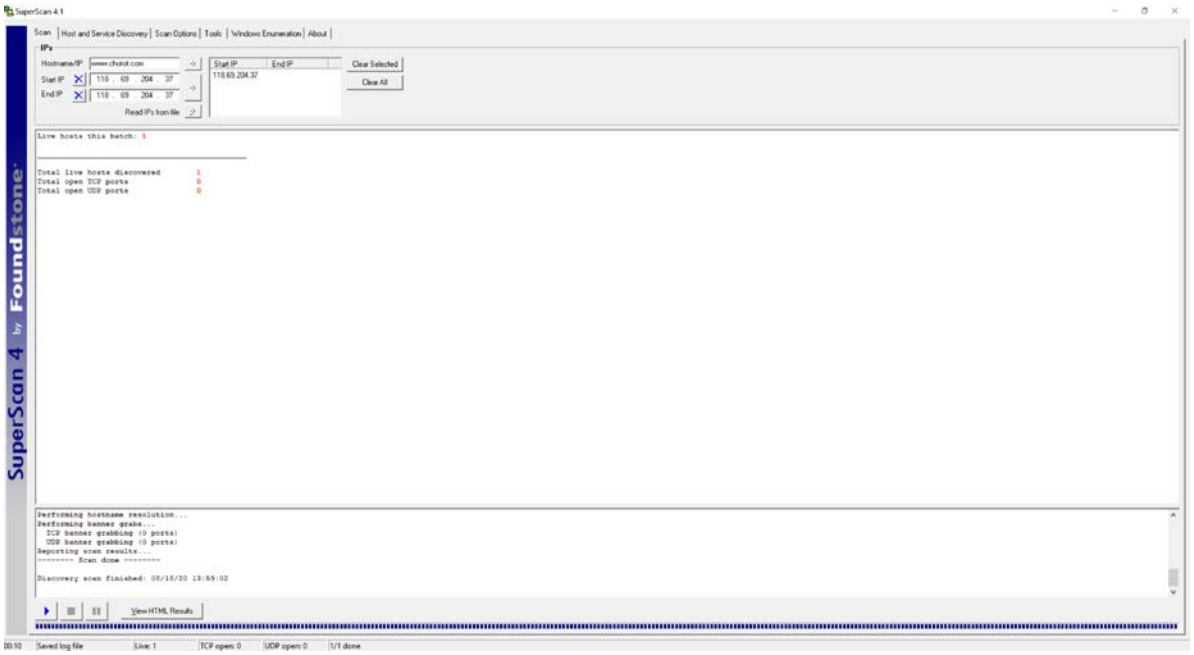
- Scan Options: Thay đổi các tham số host và services.

- Tools: Các chức năng để kiểm tra, tìm kiếm thông tin của 1 IP hoặc domain. (Ping, whois, HTTP Header request,…)

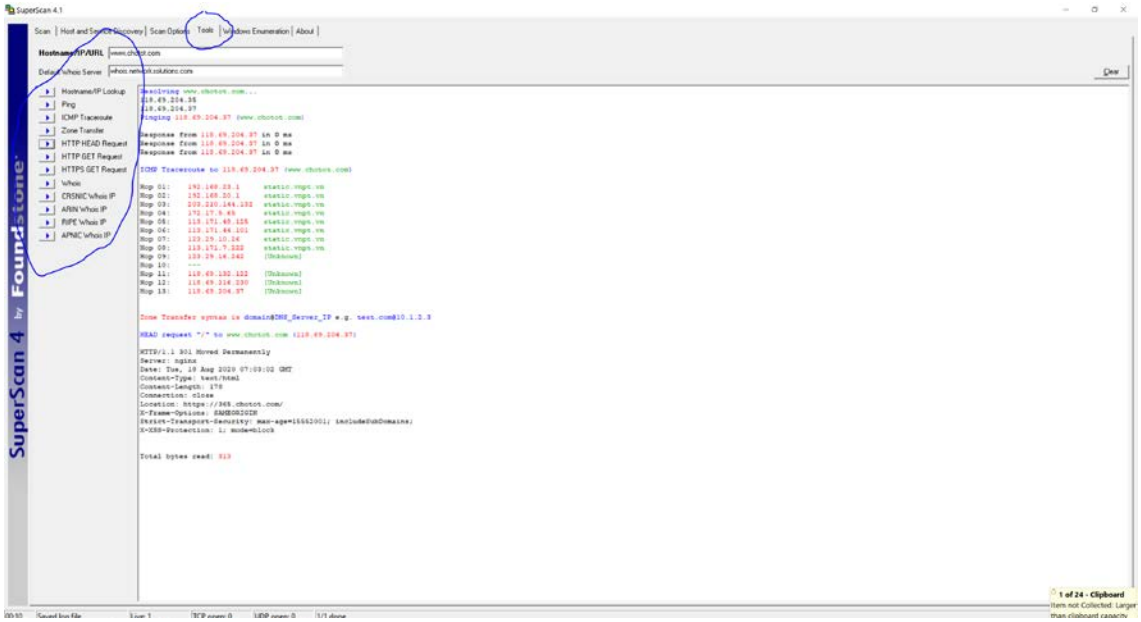
- Windows Enumeration: Thông tin mở rộng về IP hoặc Domain (NetBIOS,Mac address, Workstation,…)

Demo ví dụ với website: www.chotot.com

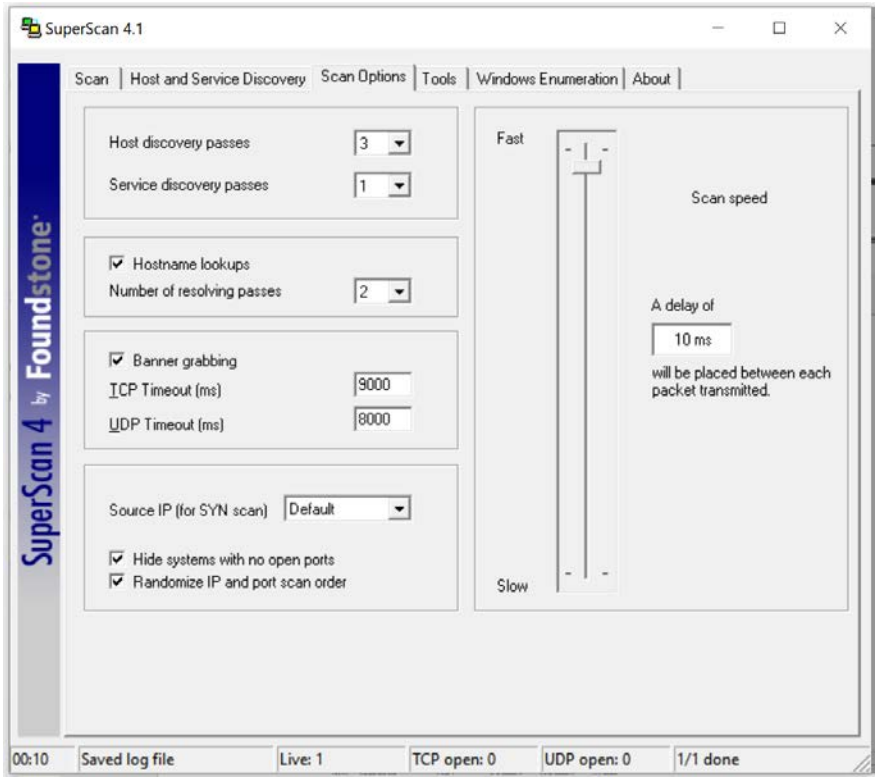
a. Ta gõ hostname www.chotot.com vào lập tức ta có được phân giả IP là: 118.69.204.37



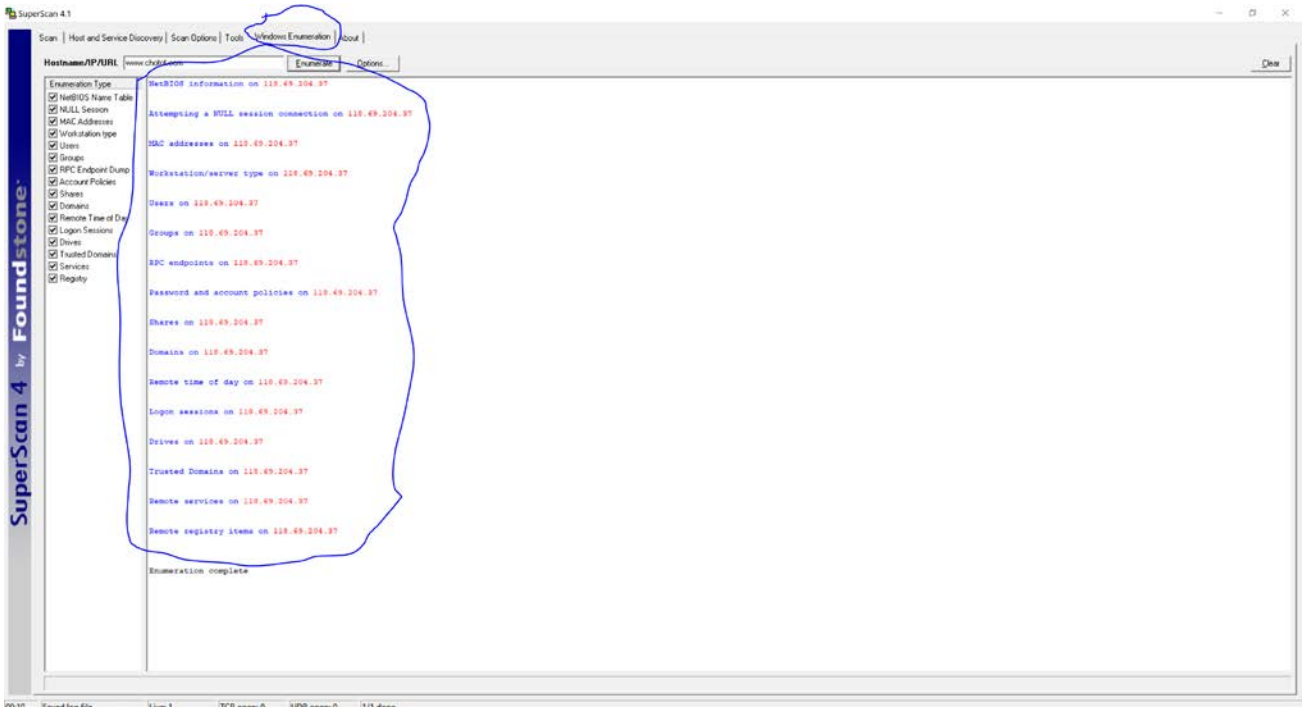
b. Tiếp theo các bạn vào Tool của Superscan để tiếp tục khai thác các thông tin của www.chotot.com



c. Thay đổi các thông số scan trong mục Scan Option



d. Khai thác các thông tin của Domain với NetBios, Mac Addresses….



3. Yêu Cầu Lab

Dùng phần mềm Super Scan 4.1 để khảo sát các thông tin của 1 website hay 1 IP bất kỳ trên mạng mà các bạn muốn.

a. Trình bày theo từng bước giống Demon.

b. Trình bày rõ ý nghĩa của từng phần trong bài Lab.

ví dụ : ICMP Traceroute to 118.69.204.37 (www.chotot.com) là dùng để tìm đường đi của gói tin từ PC của mình đến IP 118.69.204.37 la qua 13 hop