

Bài: 4.1 Điều tra - Các khái niệm & kỹ thuật điều tra

Xem bài học trên website để ủng hộ Kteam: [4.1 Điều tra - Các khái niệm & kỹ thuật điều tra](#)

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage [How Kteam](#) nhé!

Tóm tắt chủ đề

Trong những quá trình trước như [FOOTPRINTING](#) & [SCANNING](#), ta đã hiểu được cách thu nhập thông tin từ bất kì tổ chức nào, trang web nào hoặc một mạng lưới nào đó. Chúng ta cũng đã thảo luận về một vài công cụ có thể giúp ích cho ta trong việc thu thập thông tin về mục tiêu cần tìm.

Bây giờ chúng ta sẽ tiến lại gần mục tiêu để quan sát và thu thập các thông tin cụ thể. Những thông tin này rất nhạy cảm, như thông tin mạng lưới, tài nguyên mạng lưới, các đường dẫn, CNMP, DNS và các thông tin liên quan đến giao thức, người dùng hay thông tin của một nhóm nào đó, v.v... Các thông tin nhạy cảm này là cần thiết để truy cập vào hệ thống. Thông tin này được thu thập bằng cách dùng các thông tin khác nhau và các kĩ thuật cũng vô cùng khác nhau một các linh hoạt.

Các khái niệm về Enumeration (Điều Tra)

Enumeration (Điều Tra)

Trong giai đoạn **Enumeration (Điều Tra)**, kẻ xâm nhập khởi tạo các kết nối hoạt động với mục tiêu. Với kết nối hoạt động này, các truy vấn trực tiếp được tạo ra để nhận được nhiều thông tin hơn. Những thông tin này giúp xác định các điểm yếu của hệ thống. Khi kẻ tấn công phát hiện ra các điểm yếu, chúng có thể truy cập trái phép bằng cách sử dụng thông tin được thu thập này để chiếm đoạt tài sản.

Thông tin bị điều tra trong giai đoạn này là:

- Thông tin định tuyến
- Thông tin SNMP
- Thông tin DNS
- Tên máy
- Thông tin người dùng
- Thông tin nhóm
- Ứng dụng và biểu ngữ
- Thông tin chia sẻ qua mạng
- Tài nguyên mạng

Trong các giai đoạn trước, chúng ta không cần quá quan tâm đến bất kỳ vấn đề pháp lý nào. Sử dụng các công cụ cần thiết cho giai đoạn điều tra có thể vượt qua ranh giới pháp lý và có thể bị quy tội thành đồng bọn của kẻ tấn công theo dõi bằng cách sử dụng các kết nối hoạt động với kẻ tấn công. Bạn cần phải được cho phép để thực hiện các hoạt động này.

Kỹ thuật điều tra (Techniques for Enumeration)

Điều tra bằng cách sử dụng Email ID (Enumeration Using Email ID)

Việc trích xuất thông tin bằng ID email có thể cung cấp thông tin hữu ích như tên người dùng, tên miền, v.v. Địa chỉ email chứa tên người dùng và tên miền trong đó.

Điều tra bằng cách sử dụng mật khẩu mặc định (Enumeration using Default Password)

Một cách khác để điều tra là sử dụng mật khẩu mặc định. Mọi thiết bị và phần mềm đều có thông tin đăng nhập và cài đặt mặc định. Cài đặt và cấu hình mặc định này được khuyến nghị thay đổi ngay khi người dùng có sản phẩm. Một số (Thật ra là hầu hết) người dùng tiếp tục sử dụng mật khẩu và cài đặt mặc định. Nó đã dễ dàng cho kẻ tấn công truy cập trái phép bằng thông tin xác thực mặc định. Phát hiện cài đặt mặc định, cấu hình và

mật khẩu của một dòng thiết bị không phải là vấn đề lớn.

Điều tra bằng cách sử dụng SNMP (Enumeration using SNMP)

Việc **điều tra bằng SNMP** là một quá trình thu thập thông tin thông qua SNMP. Các kẻ tấn công sử dụng các chuỗi cộng đồng mặc định hoặc đoán chuỗi để trích xuất thông tin của một thiết bị. Giao thức SNMP được phát triển để cho phép quản trị viên quản lý thiết bị, chẳng hạn như máy chủ, bộ định tuyến, thiết bị chuyển mạch, máy trạm trên mạng IP. Nó cho phép quản trị viên mạng quản lý hiệu suất mạng của mạng tìm, khắc phục sự cố và giải quyết các vấn đề về mạng, thiết kế và lập kế hoạch phát triển mạng. SNMP là một giao thức giữa các tầng ứng dụng. Nó làm nhiệm vụ liên lạc giữa các nhà quản lý và các đại lý.

Hệ thống SNMP bao gồm ba yếu tố:

- Trình quản lý SNMP (SNMP manager)
- Các tác nhân SNMP (nút được quản lý) (SNMP agents (managed node))
- Cơ sở thông tin quản lý (MIB) (Management Information Base (MIB))

Tấn công Brute Force trên Active Directory (Brute Force Attack on Active Directory)

Active Directory (AD) cung cấp lệnh và kiểm soát tập trung của người dùng miền, máy tính và máy in mạng. Nó hạn chế quyền truy cập vào nguồn mạng chỉ cho người dùng và máy tính được xác định. AD là một mục tiêu lớn, một nguồn thông tin nhạy cảm lớn cho kẻ tấn công. Tấn công Brute Force để khai thác, hoặc tạo truy vấn đến các dịch vụ LDAP được thực hiện để thu thập thông tin như tên người dùng, địa chỉ, thông tin xác thực, thông tin đặc quyền, v.v.

Điều tra thông qua chuyển vùng DNS (Enumeration through DNS Zone Transfer)

Điều tra thông qua quá trình chuyển vùng DNS bao gồm trích xuất thông tin như định vị Máy chủ DNS, bản ghi DNS, các thông tin liên quan đến mạng có giá trị khác như tên máy chủ, địa chỉ IP, tên người dùng, v....v... Chuyển vùng là quá trình cập nhật các máy chủ DNS; Tập vùng mang thông tin có giá trị được truy xuất bởi kẻ tấn công. UDP 53 được sử dụng cho các yêu cầu DNS từ các máy chủ DNS. TCP 53 được sử dụng để chuyển vùng DNS để đảm bảo việc chuyển giao.

Dịch vụ và cổng mạng để Điều tra (Services and Ports to Enumerate)

Dịch vụ	Cổng mạng
Chuyển vùng DNS	TCP 53
Truy vấn DNS	UDP 53
SNMP	UDP 161
SNMP Trap	TCP/UDP 162
Microsoft RPC Endpoint Mapper	TCP/UDP 135
LDAP	TCP/UDP 389
NBNS	UDP 137
Dịch vụ Catalog toàn cầu	TCP/UDP 3268
NetBIOS	TCP 139
SMTP	TCP 25

Lab 4-1: Dịch vụ Điều tra bằng cách sử dụng Nmap (Services Enumeration using Nmap)

Nghiên cứu điển hình (Case Study):

Trong bài Lab này, hãy xem xét mạng **10.10.10.0/24** nơi các thiết bị khác nhau đang chạy. Chúng tôi sẽ Điều tra các dịch vụ, cổng và thông tin hệ điều hành bằng ứng dụng **Nmap** sẵn có trên **Kali Linux**.

Cách thức & Lệnh:

Mở thiết bị đầu cuối của Kali Linux

Nhấn vào lệnh sau:

```
root@kali:~# nmap -sP 10.10.10.0/24
```

Thực hiện **Ping Sweep**(Quét ping) trên mạng con để kiểm tra máy chủ trực tiếp và các thông tin cơ bản khác.

Nhập lệnh:

```
root @ kali: ~ # nmap -sU -p 10.10.10.12
```

Quét cổng UDP cho cổng 161 (Cổng SNMP) cho máy chủ đích 10.10.10.12. Kết quả cho thấy cổng SNMP 161 được mở và đã được phân loại. Bây giờ hãy nhập lệnh dưới để thực hiện quét bí mật trên máy chủ đích 10.10.10.12

```
root @ kali: ~ # nmap -sS 10.10.10.12
```

Kết quả cho thấy một danh sách các cổng mở và các dịch vụ đang chạy trên máy chủ đích. Nhập lệnh dưới để quét hệ điều hành & phiên bản trên máy chủ đích 10.10.10.12.

```
root @ kali: ~ # nmap -sSV -O 10.10.10.12
```

NetBIOS Enumeration

NetBIOS là **Network Basic Input / Output System** (đầu vào / đầu ra mạng cơ bản của hệ thống) là một chương trình cho phép giao tiếp giữa các ứng dụng khác nhau chạy trên các hệ thống khác nhau trong mạng lưới khu vực địa phương.

Dịch vụ **NetBIOS** sử dụng một chuỗi ký tự 16-ASCII duy nhất để xác định các thiết bị mạng qua TCP / IP. 15 ký tự ban đầu là để xác định thiết bị, ký tự thứ 16 là xác định dịch vụ.

Dịch vụ NetBIOS sử dụng cổng TCP 139. NetBIOS qua TCP (NetBT) sử dụng các cổng TCP và UDP sau đây:

- UDP port 137 (tên dịch vụ)
- UDP port 138 (dịch vụ datagram)
- TCP port 139 (dịch vụ phiên)

Sử dụng **NetBIOS Enumeration**, kẻ tấn công có thể khám phá:

- Danh sách các máy trong miền (List of Machines within a domain)
- Chia sẻ file
- Tên người sử dụng
- Thông tin nhóm
- Mật khẩu

- Các chính sách

Tên **NetBIOS** được phân thành các loại sau:

- Duy nhất
- Nhóm
- Tên miền
- Nhóm Internet
- Multihomed (Đa lượng)

Tên	Mã Hex	Loại	Thông tin
<computername>	0	U	Dịch vụ máy trạm
<computername>	1	U	Dịch vụ thư tín
<\\-__MSBROWSE__>	1	G	Master Browse
<computername>	2	U	Dịch vụ thư tín
<computername>	6	U	Dịch vụ máy chủ RAS
<computername>	1F	U	Dịch vụ NetDDE
<computername>	20	U	Dịch vụ máy chủ thư mục
<computername>	21	U	Dịch vụ máy khách RAS
<computername>	22	U	Microsoft Exchange Interchange(MSMail Connector)
<computername>	23	U	Cửa hàng trao đổi Microsoft
<computername>	24	U	U Danh mục trao đổi Microsoft
<computername>	30	U	Dịch vụ chia sẻ máy chủ Modem
<computername>	31	U	Dịch vụ chia sẻ Modem máy khách
<computername>	43	U	SMS Điều khiển máy khách từ xa

<computername>	44	U	
<computername>	45	U	
<computername>	46	U	
<computername>	4C	U	
<computername>	42	U	
<computername>	52	U	
<computername>	87	U	
<computername>	6A	U	
<computername>	BE	U	
<computername>	BF	U	
<username>	3	U	
<domain>	0	G	
<domain>	1B	U	
<domain>	1C	G	
<domain>	1D	U	
<domain>	1E	G	
<INet~Services>	1C	G	
<IS~computer name	0	U	
<computername>	[2B]	U	
IRISMULTICAST	[2F]	G	
IRISNAMESEVER	[33]	G	
Forte_\$ND800ZA	[20]	U	

Công cụ Điều tra NetBIOS (NetBIOS Enumeration Tool)

Lệnh **nbstat** là một công cụ hữu ích để hiển thị thông tin về **NetBIOS** qua số liệu thống kê **TCP / IP**. Nó cũng được sử dụng để hiển thị thông tin như bảng tên NetBIOS, bộ nhớ đệm tên và các thông tin khác. Lệnh sử dụng tiện ích nbstat được hiển thị dưới đây:

:

```
nbstat.exe -a "NetBIOS name of the remote system."
```

```
nbstat -A 192.168.1.10
```

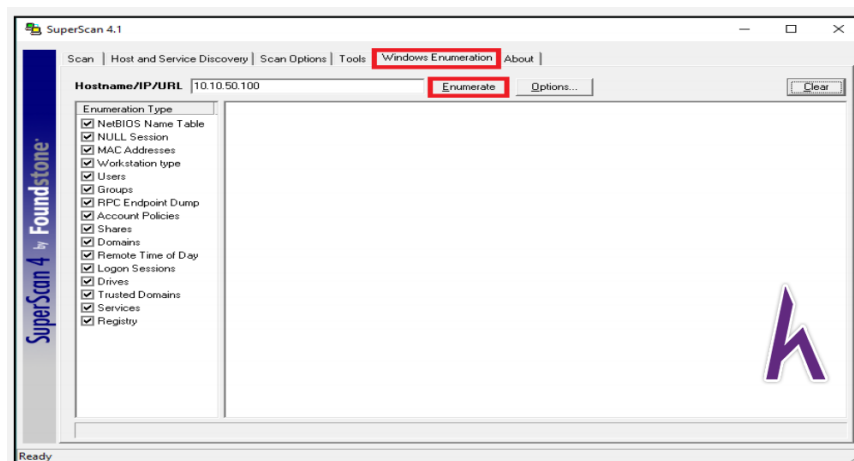
Lệnh **nbstat** có thể được sử dụng cùng với một số tùy chọn, Điều tra các tùy chọn có sẵn cho lệnh **nbstat** như sau:

Tùy chọn	Mô tả
-a	Với tên máy chủ, hiển thị bảng tên NetBIOS, địa chỉ MAC thông tin.
-A	Với địa chỉ IP, hiển thị bảng tên NetBIOS, địa chỉ MAC thông tin.
-c	Thông tin bộ nhớ cache tên NetBIOS.
-n	Hiển thị tên được đăng ký cục bộ bởi các ứng dụng NetBIOS như máy chủ và trình chuyển hướng.
-r	Hiển thị số lượng tất cả các tên được giải quyết bằng cách phát hoặc máy chủ WINS.
-s	Điều tra bảng phiên NetBIOS và chuyển đổi địa chỉ IP đích vào tên NetBIOS của máy tính.
-S	Điều tra các phiên NetBIOS hiện hành, trạng thái, cùng với địa chỉ IP.

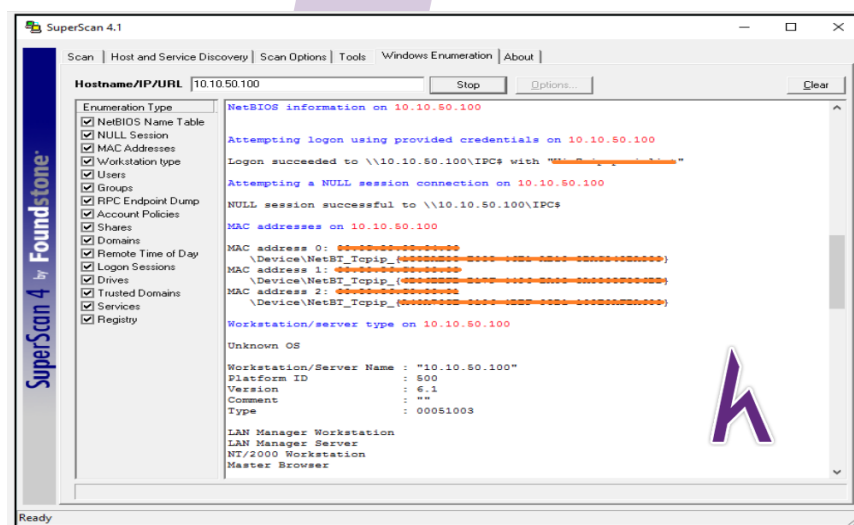
Lab 4-2: Điều tra sử dụng công cụ SuperScan

Thủ tục

Mở phần mềm **SuperScan**, Chuyển đến tab **Windows Enumeration**. Nhập tên máy chủ hoặc địa chỉ IP của máy tính Windows muốn đến. Chuyển đến nút **Options** để tùy chỉnh việc điều tra. Chọn kiểu điều tra từ phần bên trái. Sau khi định dạng, để bắt đầu quá trình liệt kê thì bấm nút **Enumerate** để khởi tạo quá trình.



Sau khi khởi động Enumeration, nó sẽ thu thập thông tin về máy mục tiêu, chẳng hạn như thông tin địa chỉ **MAC**, thông tin hệ điều hành và các thông tin khác tùy thuộc vào loại điều tra được chọn trước khi bắt đầu quá trình.



Hiển thị thông tin người dùng của máy mục tiêu cùng với tên đầy đủ, nhận xét hệ thống, thông tin đăng nhập lần cuối, thông tin hết hạn mật khẩu, thông tin thay đổi mật khẩu, số lượng thông tin đăng nhập và số lần đếm mật khẩu không hợp lệ, v.v.

Kết quả hiển thị thông tin về chính sách tài khoản và mật khẩu, chia sẻ thông tin, thông tin đăng nhập từ xa, v.v...

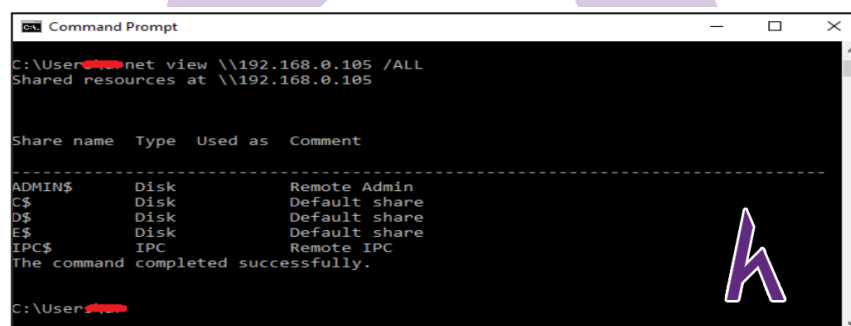
Một số công cụ hữu ích khác là:

Công cụ Điều tra NetBIOS	Mô tả
Hyena	Hyena dựa trên GUI, công cụ Điều tra NetBIOS hiển thị chia sẻ, thông tin đăng nhập của người dùng và các thông tin liên quan khác
Winfingerprint	Winfingerprint là công cụ Điều tra NetBIOS có khả năng cung cấp thông tin như hệ điều hành, thông người sử dụng & nhóm, cổ phiếu, phiên và dịch vụ, SID và nhiều thông tin khác.
NetBIOS Enumerator	NetBIOS Enumerator là công cụ Điều tra NetBIOS dựa trên GUI có khả năng cung cấp chức năng quét cổng, quản lý bộ nhớ động, xác định hệ điều hành, theo dõi, thông tin DNS, thông tin máy chủ và nhiều tính năng tùy thuộc vào phiên bản phần mềm.
Nsauditor Network Security Auditor	Theo dõi mạng Nsauditor cung cấp một số thông tin chi tiết về các dịch vụ chạy cục bộ, với các tùy chọn để tìm hiểu từng kết nối và phân tích hệ thống từ xa, chấm dứt kết nối và xem dữ liệu.

Dùng Net View để điều tra tài nguyên được chia sẻ (Enumerating Shared Resources Using Net View)

Net View là tiện ích được sử dụng để hiển thị thông tin về tất cả các nguồn được chia sẻ của máy chủ hoặc nhóm làm việc từ xa. Cú pháp lệnh cho tiện ích Net View là :

```
C:\Users\>net view [\\computername [/CACHE] | [/ALL] | /DOMAIN[:domainname]]
```



```

Command Prompt
C:\User>net view \\192.168.0.105 /ALL
Shared resources at \\192.168.0.105

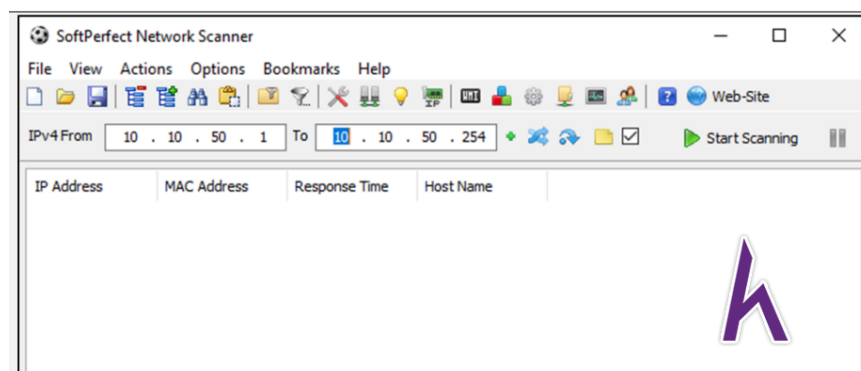
Share name  Type  Used as  Comment
-----
ADMIN$      Disk      Remote Admin
C$          Disk      Default share
D$          Disk      Default share
E$          Disk      Default share
IPC$        IPC       Remote IPC
The command completed successfully.
C:\User>

```

Lab 4-3: Điều tra bằng SoftPerfect Network Scanner Tool (Enumeration using SoftPerfect Network Scanner Tool)

Cách thức

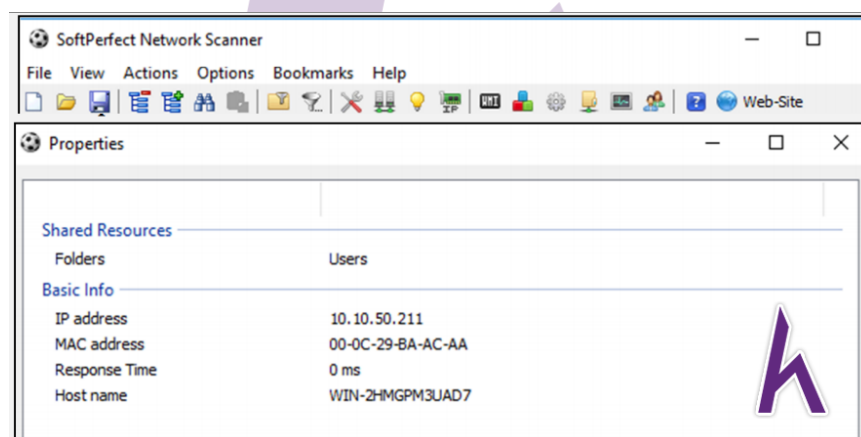
Tải xuống và cài đặt công cụ **SoftPerfect Network Scanner**. Trong bài Lab này, chúng tôi sử dụng **Windows Server 2016** để thực hiện quét bằng **SoftPerfect Network Scanner** quét nguồn được chia sẻ trong mạng. Sau khi cài đặt, hãy chạy ứng dụng và nhập phạm vi địa chỉ IP để quét.



Bây giờ, nhấn vào nút **Start Scanning**

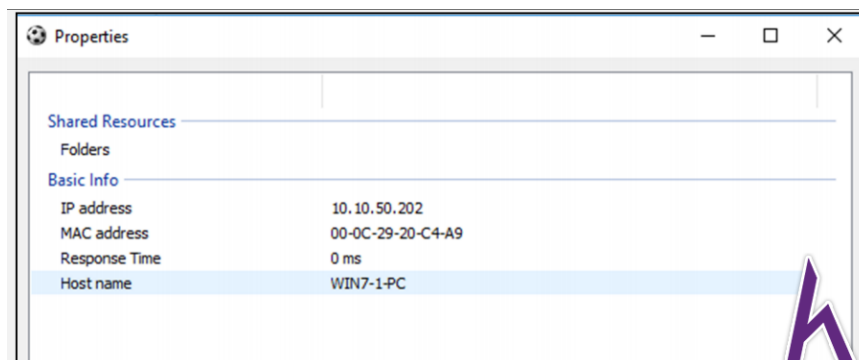
SoftPerfect Network Scanning đang quét tìm mục tiêu trong một phạm vi nhất định

Sau khi quét, chọn host mà bạn muốn và nhấn chuột phải vào nó > Chọn **Properties**



Màn hình đang hiển thị những nguồn đã được chia sẻ về host này. Host này đã chia sẻ các tập tin với nhiều người dùng khác nhau

Bây giờ, chọn một host khác, tiếp tục nhấn **Properties**



Như màn hình hiển thị, tức là host này không chia sẻ bất kỳ tài nguyên nào