HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

Bài 10: Tìm kiếm và khai thác lỗ hổng

Họ và tên giảng viên:	TS.Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

I. Mục đích

- Hiểu được các mối đe dọa và lỗ hổng.
- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ lổng như: nmap/zenmap, nessus, Metasploit framework.
- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/zenmap, nessus, Metasploit framework.

II. Nội dung thực hành

2.1 Tìm hiểu lý thuyết

Tài liệu tham khảo:

Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.

Tài liệu CEH, https://www.eccouncil.org/programs/certified-ethical-hackerceh/

Lab 14 của CSSIA CompTIA Security+® Supported Labs

Tìm hiểu lý thuyết:

Nmap

Nmap là một công cụ quét mạng mạnh mẽ và linh hoạt, được sử dụng để khám phá các máy chủ và dịch vụ trên mạng. Nmap có thể cung cấp nhiều thông tin về các máy chủ, như địa chỉ IP, hệ điều hành, cổng mở, phiên bản phần mềm và nhiều hơn nữa. Nmap cũng có thể thực hiện các kỹ thuật quét nâng cao, như quét SYN, quét ACK, quét Xmas và quét FIN. Nmap có thể chạy trên nhiều hệ điều hành khác nhau, bao gồm Windows, Linux, MacOS và BSD. Nmap có giao diện dòng lệnh và giao diện đồ họa (Zenmap). Nmap là một công cụ miễn phí và mã nguồn mở, được phát triển bởi Gordon Lyon (còn được biết đến với tên Fyodor) và cộng đồng Nmap.

Nessus

Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable. Nessus cho phép người dùng phát hiện và khắc phục các lỗ hổng bảo mật trên các hệ thống mạng, ứng dụng và thiết bị. Nessus có thể quét các loại lỗ hổng như:

- Lỗ hổng cho phép một hacker từ xa kiểm soát hoặc truy cập dữ liệu nhạy cảm trên hệ thống.

- Cấu hình sai (ví dụ như chuyển tiếp thư mở, các bản vá lỗi bị thiếu,...).

- Mật khẩu mặc định, một vài mật khẩu thường được sử dụng, và mật khẩu trống trên các tài khoản hệ thống.

- Tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại

- Vi phạm các tiêu chuẩn bảo mật (ví dụ như PCI DSS).

Nessus có giao diện web trực quan và dễ sử dụng, cho phép người dùng thiết lập các chính sách quét, lựa chọn các mục tiêu quét, xem và xuất kết quả quét. Nessus cũng có thể tích hợp với các công cụ quản lý an ninh khác để cung cấp giải pháp an ninh toàn diện.

Nessus sử dụng các trình cắm (plugin) để thực hiện các bài kiểm tra lỗ hổng. Các trình cắm được viết bằng ngôn ngữ NASL (Nessus Attack Scripting Language), một ngôn ngữ kịch bản tối ưu cho tương tác mạng. Công ty Tenable cập nhật hàng tuần các trình cắm mới để đáp ứng các lỗ hổng mới được phát hiện.

Metasploit Framework

Metasploit Framework là một nền tảng mã nguồn mở dựa trên Ruby được sử dụng bởi các chuyên gia an ninh thông tin và các tin tặc để tìm kiếm, khai thác và xác nhận các lỗ hổng của hệ thống. Nền tảng này bao gồm nhiều công cụ khai thác và công cụ kiểm thử xâm nhập.

Metasploit Framework cho phép người dùng tạo ra các module khai thác, payload, encoder và nmap để thực hiện các cuộc tấn công trên các mục tiêu khác

nhau. Nó cũng hỗ trợ việc sử dụng các công cụ bên ngoài như Nessus, Nmap, John the Ripper và Wireshark.

Metasploit Framework có thể chạy trên nhiều hệ điều hành khác nhau như Windows, Linux, MacOS và Unix. Nó có giao diện dòng lệnh (console) và giao diện đồ họa (GUI) để người dùng lựa chọn. Nó cũng có phiên bản thương mại là Metasploit Pro, cung cấp nhiều tính năng nâng cao hơn.

Metasploit Framework là một công cụ mạnh mẽ và linh hoạt cho việc kiểm tra xâm nhập và khai thác lỗ hổng. Tuy nhiên, nó cũng có thể bị lợi dụng bởi các tin tặc để gây ra thiệt hại cho các hệ thống và mạng. Do đó, người dùng cần tuân thủ đạo đức và pháp luật khi sử dụng nền tảng này.

2.2. Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Các công cụ nmap/zenmap, nessus, Metasploit framework

2.3. Các bước thực hiện

2.3.1. Chuẩn bị môi trường

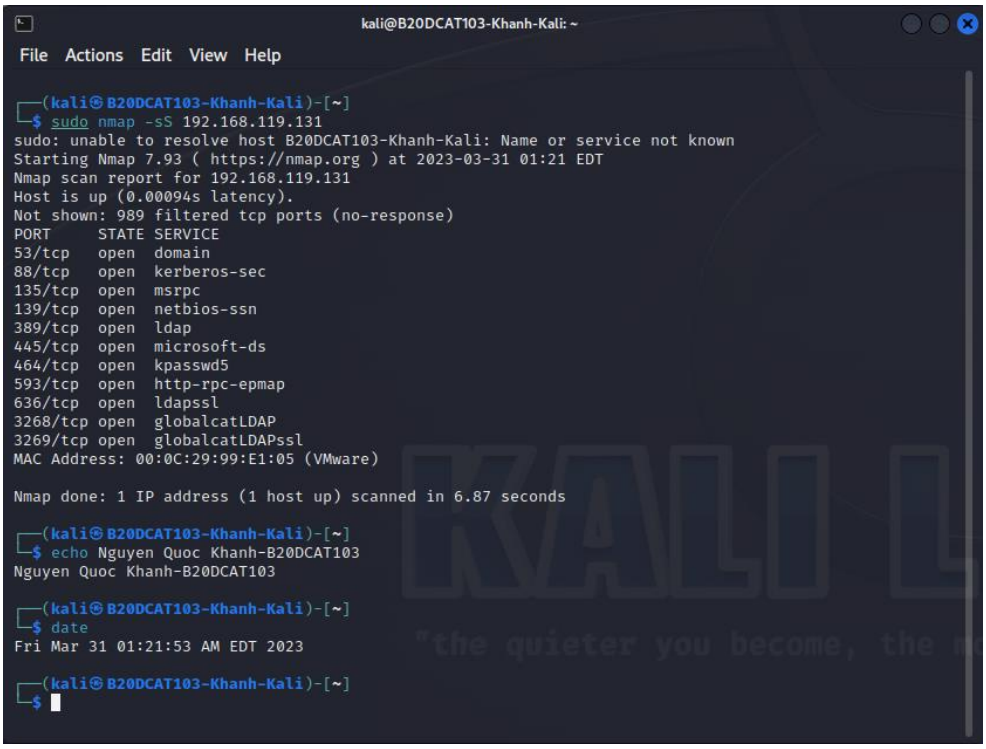
- Cài đặt công cụ ảo hóa.
- Cài đặt các công cụ: nmap/zenmap, nessus, Metasploit framework.

2.3.2. Nội dung thử nghiệm

Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework.

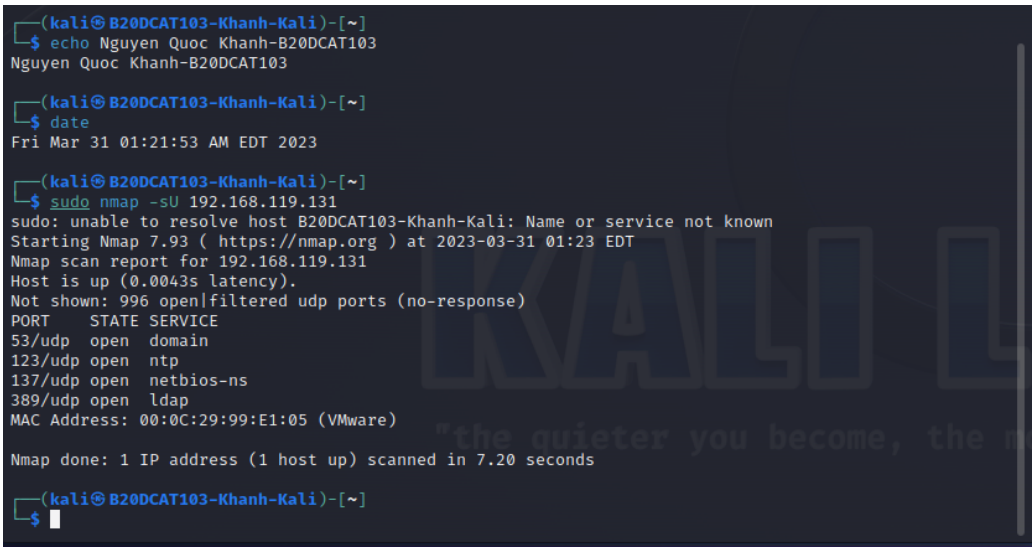
Sử dụng nmap/zenmap để quét các cổng dịch vụ (ít nhất 2 cổng).

Sử dụng nmap để quét cổng dịch vụ giao thức TCP trên Windows Server 2019(IP:192.168.119.131):



Dịch vụ FTP ở cổng 21 là cổng dịch vụ của giao thức Đây là một giao thức mạng được sử dụng để truyền tải tập tin giữa máy tính và một máy chủ trên Internet hoặc giữa các máy tính trong mạng. Giao thức FTP (File Transfer Protocol) có một số lỗ hổng bảo mật nghiêm trọng có thể dẫn đến việc tấn công máy chủ.

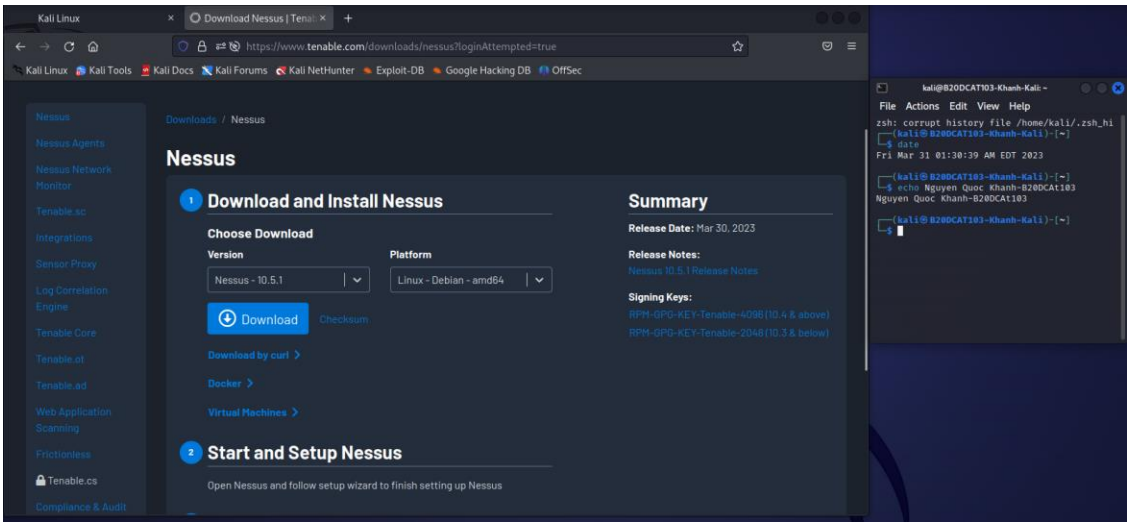
Sử dụng nmap để quét cổng dịch vụ giao thức UDP trên Windows Server 2019:

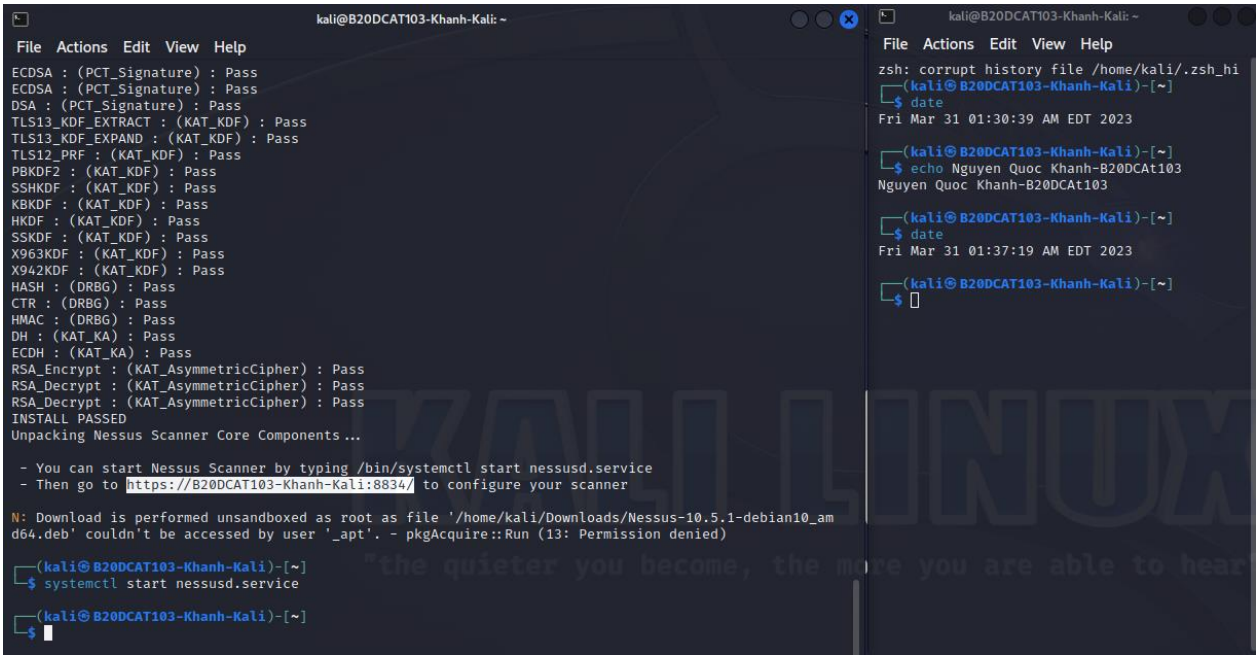


Các cổng dịch vụ trên có netbios-ns, là cổng dịch vụ của giao thức NetBIOS, công nghệ nối mạng của Windows. Nó được thiết kế trong môi trường mạng LAN để chia sẻ tài nguyên. Do đặc tính được thiết kế cho mạng LAN để chia sẻ tài nguyên nên tính bảo mật của giao thức NetBIOS rất thấp. Lỗ hổng này cho phép bất cứ kẻ xâm nhập trái phép nào cũng có thể dễ dàng truy cập đến các tài nguyên dùng chung nhạy cảm một cách dễ dàng. Quét UDP là một kỹ thuật quét cổng mạng dựa trên giao thức UDP, một giao thức không đáng tin cậy không có kiểm soát lưu lượng. Quét UDP có thể giúp phát hiện các dịch vụ mạng nhạy cảm hoặc tiềm ẩn nguy cơ bảo mật trên các cổng UDP.

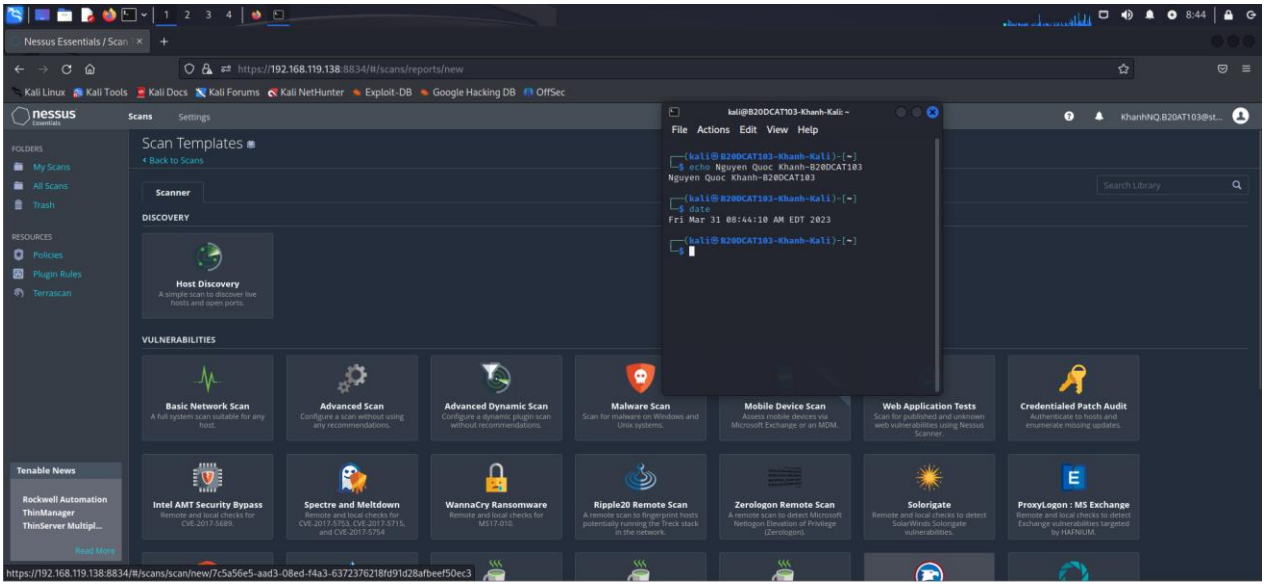
Sử dụng nessus để quét các lỗ hổng (ít nhất 2 lỗ hổng).

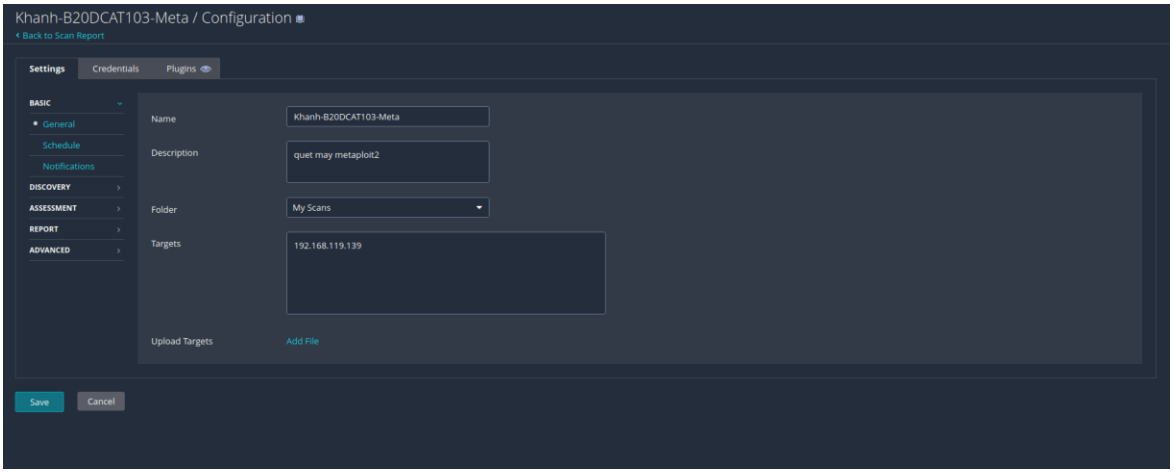
Cài đặt thành công, tạo tài khoản và truy cập được Nessus trên trình duyệt Web:



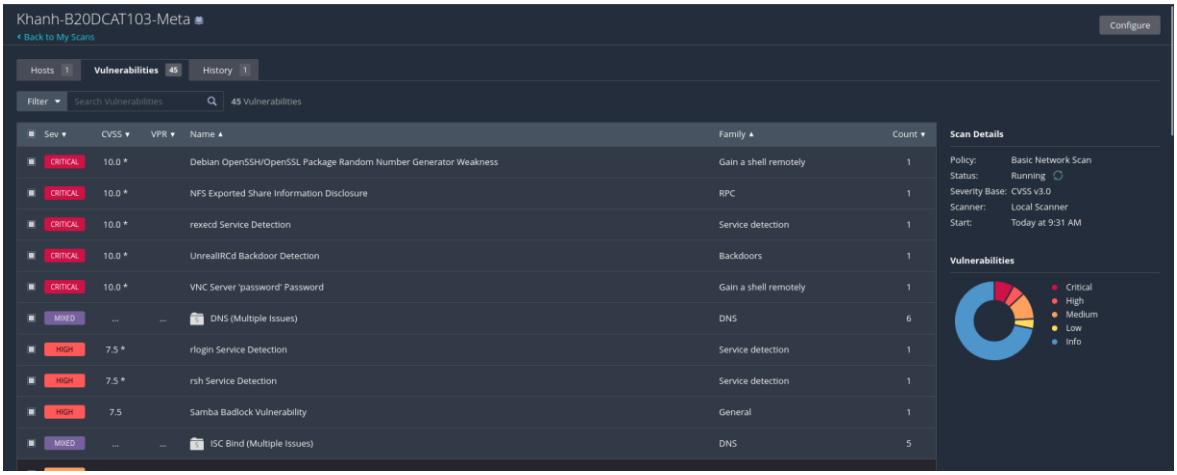


Sử dụng Nessus để quét các lỗ hổng trên metasploit có địa chỉ IP: 192.168.119.139

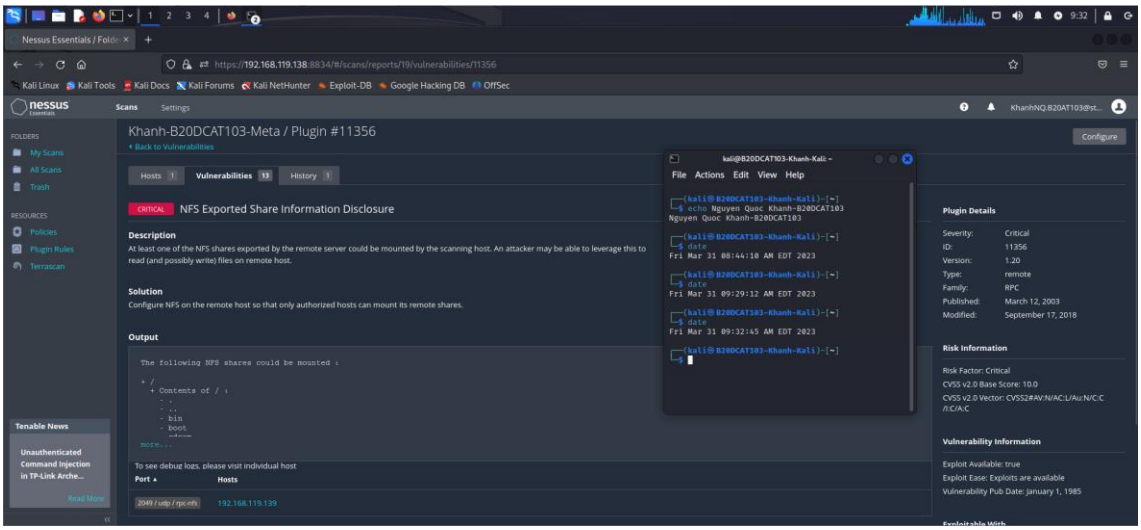




Nessus quét được các lỗ hổng trên Metasploit2:

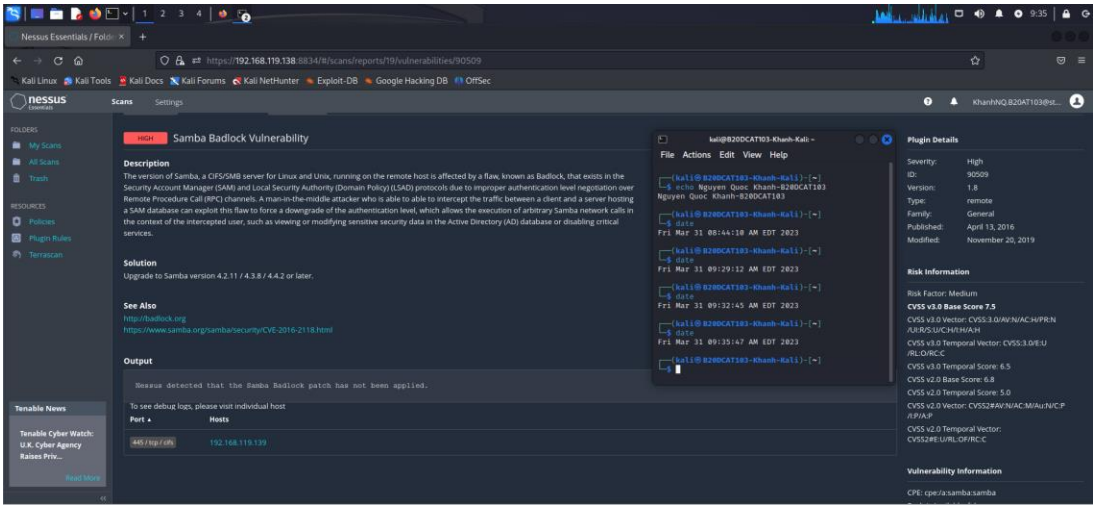


Lỗ hổng NFS Exported Share Information Disclosure



Lỗ hổng NFS Exported Share Information Disclosure là một lỗ hổng bảo mật cho phép kẻ tấn công có thể truy cập vào các tệp và thư mục được chia sẻ trên máy chủ NFS (Network File System) mà không cần xác thực. Lỗ hổng này xuất hiện do máy chủ NFS không kiểm tra địa chỉ IP của kẻ tấn công khi cung cấp quyền truy cập vào các tài nguyên được chia sẻ. Điều này có thể cho phép kẻ tấn công có thể đọc, ghi hoặc xóa các tệp và thư mục trên máy chủ NFS, gây ra việc rò rỉ thông tin nhạy cảm, thay đổi hoặc hủy hoại dữ liệu.

Lỗ hổng Samba Badlock Vulnerability



Lỗ hổng Samba Badlock Vulnerability là một lỗ hổng bảo mật nghiêm trọng ảnh hưởng đến hầu hết các phiên bản Windows và Samba, một phần mềm mã nguồn mở cho phép chia sẻ dữ liệu qua mạng giữa các hệ điều hành khác nhau. Lỗ hổng này cho phép kẻ tấn công có thể thực hiện các cuộc tấn công Man-in-the-Middle (MITM) để đánh cắp hoặc thay đổi thông tin nhạy cảm trên mạng.

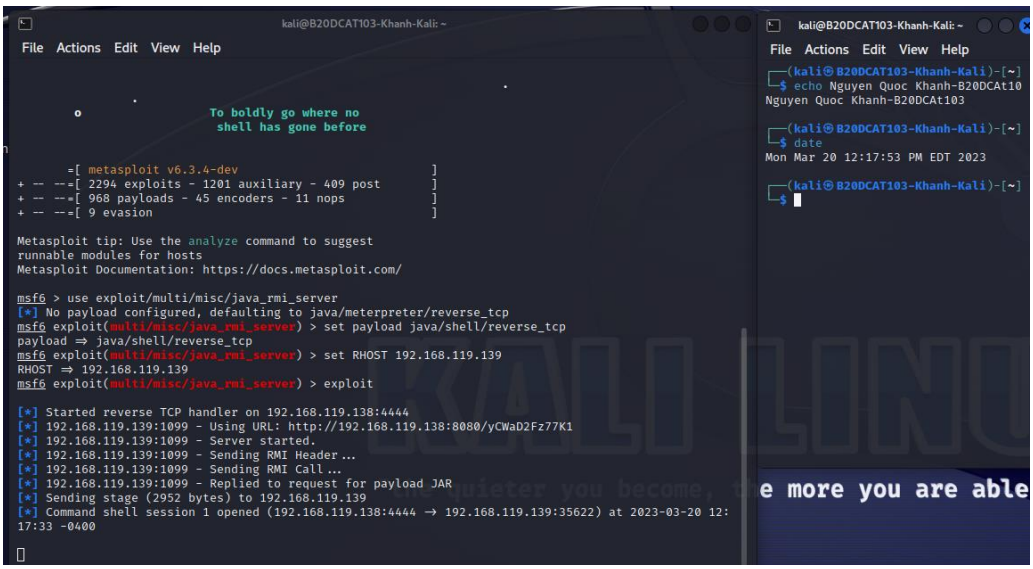
Sử dụng Metasploit framework khai thác lỗ hổng (ít nhất khai thác thành công 1 lỗ hổng trên máy nạn nhân).

Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công

- Chọn payload cho thực thi
- Đặt địa chỉ máy victim
- Thực thi tấn công:

  ➔ Nếu thực hiện thành công hệ thống sẽ báo “Command shell session 1 opened”



- Chạy các lệnh trong phiên khai thác đang mở:
  - whoami
  - uname -a
  - hostname