HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 11

MÔN THỰC TẬP CƠ SỞ

Tìm kiếm và khai thác lỗ hổng

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Lớp : D20CQAT02-B

Giảng viên hướng dẫn : Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 5/2023

Table of Contents

1/Lý thuyết:

1.1 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

1.2 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)

1.3 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.Nội dung thực hành:

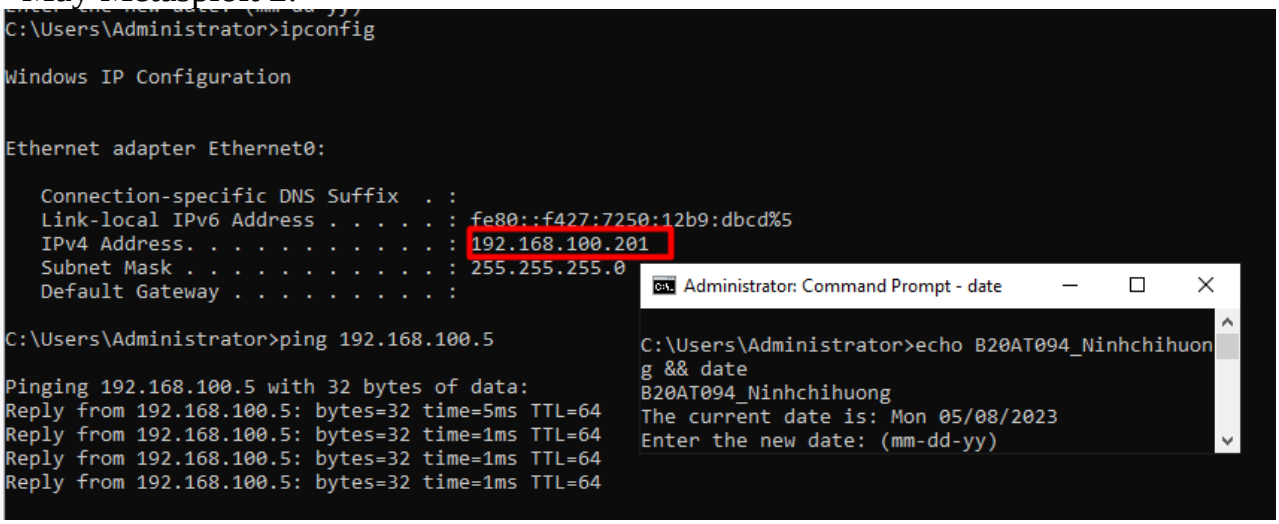
2.1 Chuẩn bị môi trường

-Cài đặt công cụ ảo hóa.

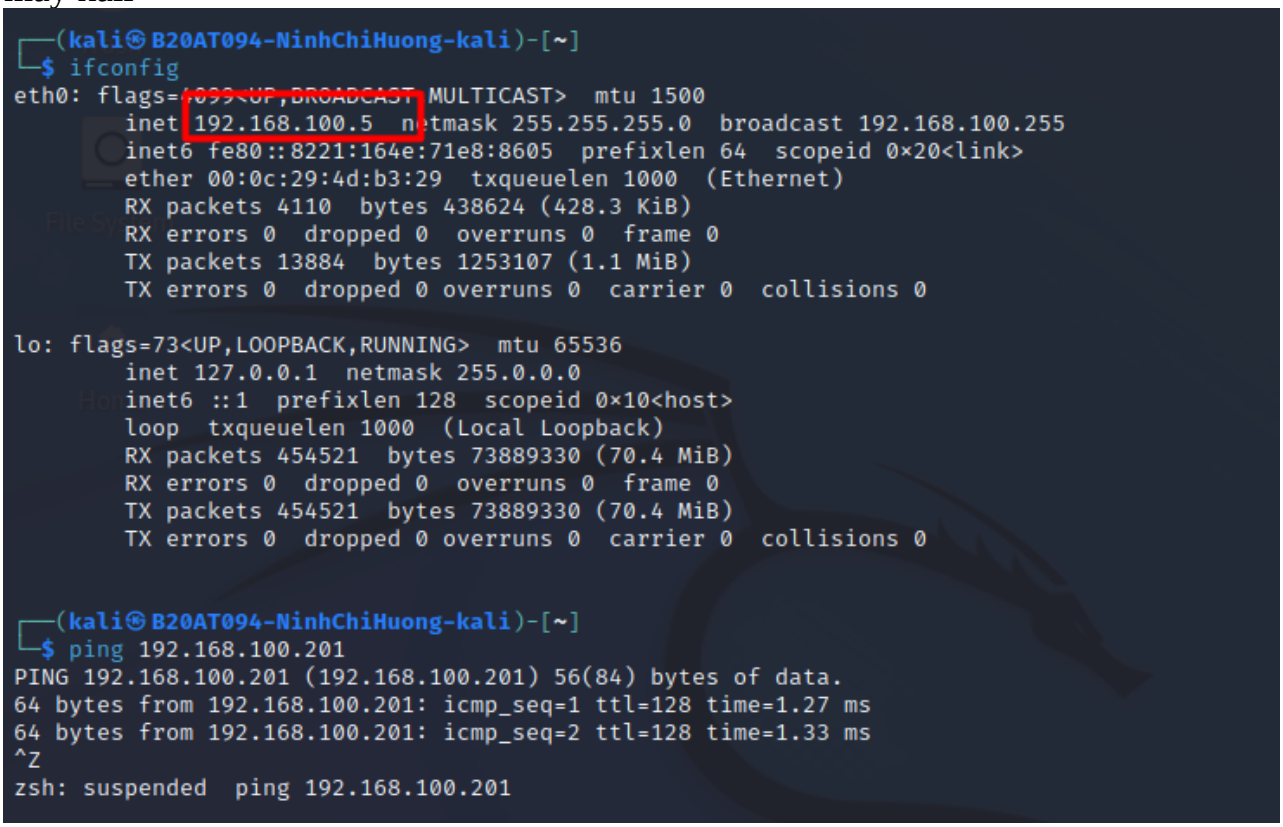
-Cài đặt các công cu: nmap/zenmap, nessus, Metasploit framework

Sử dụng nmap/zenmap để quét các cổng dịch vụ

- Máy Metasploit 2:



máy kali

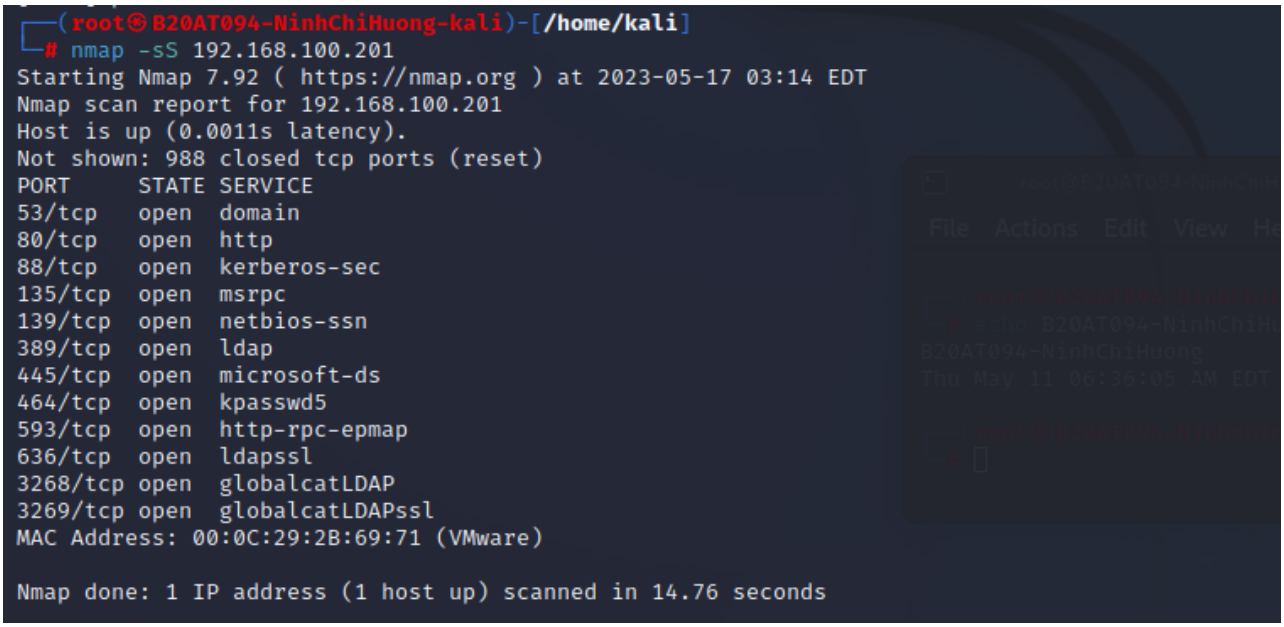


• Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework.

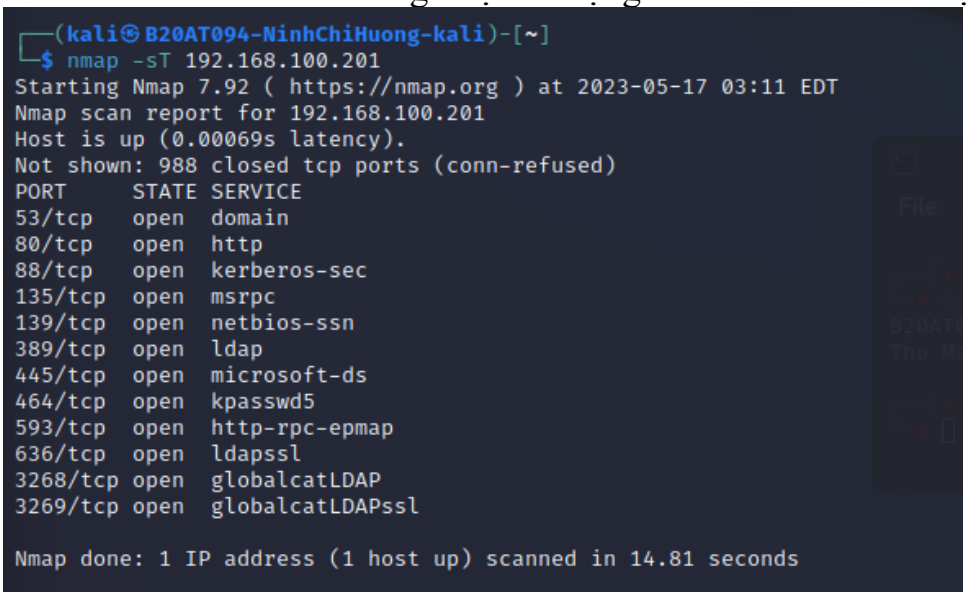
Sử dụng nmap/zenmap để quét các cổng dịch vụ giao thức trên Windows

Server 2019

o Dịch vụ TCP SYN scan: nmap gửi một gói tin tới port mục tiêu của Windowws Server. Nếu nhận được ACK_SYN thì port đó đang ở trạng thái open, nmap sẽ gửi gói tin RST để đóng kết nối thay vì gửi ACK để hoàn tất quá trình bắt tay 3 bước (vì thế kĩ thuật này được gọi là half open scan). Nếu nhận được RST thì port đó ở trạng thái close. Nếu sau 1 lần gửi mà không nhận được trả lời hoặc nhận được ICMP type 3 thì port ở trạng thái đã bị firewall chặn



Dịch vụ TCP connect scan: Kỹ thuật này cho kết quả tương đương như TCP SYN scan, nếu nhận được ACK_SYN nmap sẽ gửi gói tin ACK để hoàn tất quá trình bắt tay 3 bước. TCP connect scan được dùng khi user không có quyền truy cập raw packet để thực hiện SYN scan. TCP connect scan sử dụng TCP stack của hệ điều hành để tạo ra 1 kết nối bình thường với mục tiêu, do thực hiện 1 kết nối đầy đủ nên kỹ thuật này dễ bị phát hiện bởi hệ thống log của mục tiêu do đó SYN scan thường được sử dụng nhiều hơn để tránh bị phát hiện



o Dịch vụ UDP scan: nmap sử dụng gói tin UDP tới 1 port của mục tiêu nếu nhận được gói tin ICMP port unreachable error (type 3, code 3) thì port đó ở trạng thái close. Nếu nhận được ICMP unreachable error (type 3, codes 1, 2, 9, 10,

hoặc 13) thì port đó ở trạng thái filtered. Nếu không nhận được gì thì port ở trạng thái open hoặc filtered. Nếu nhận được gói tin UDP thì poet đó ở trạng thái open.

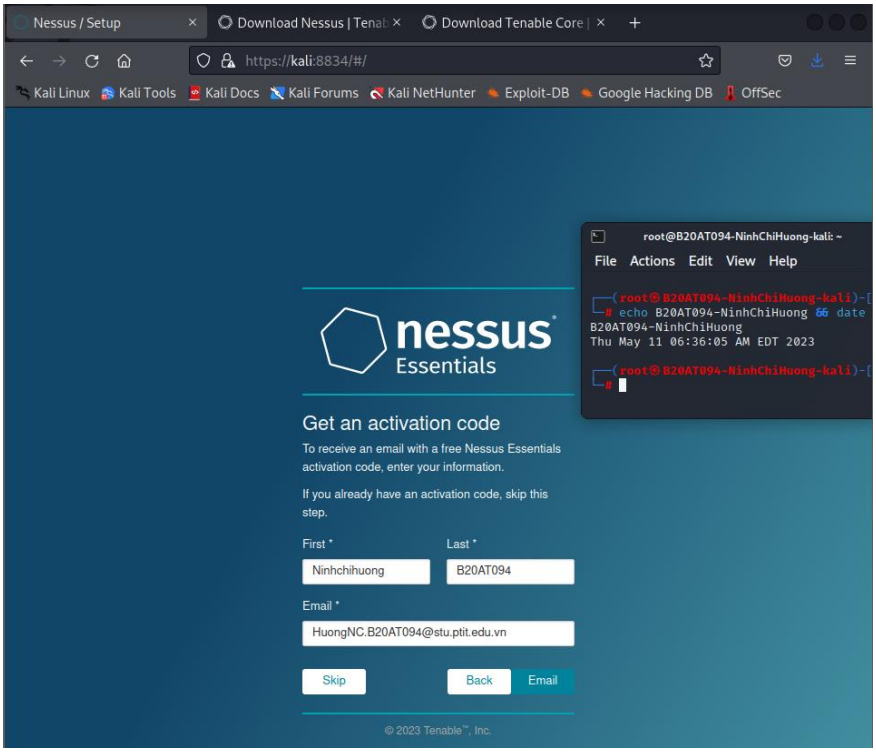
```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[/home/kali]
└─# nmap -PU 192.168.100.201
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-17 03:15 EDT
Nmap scan report for 192.168.100.201
Host is up (0.0010s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:0C:29:2B:69:71 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.94 seconds
```

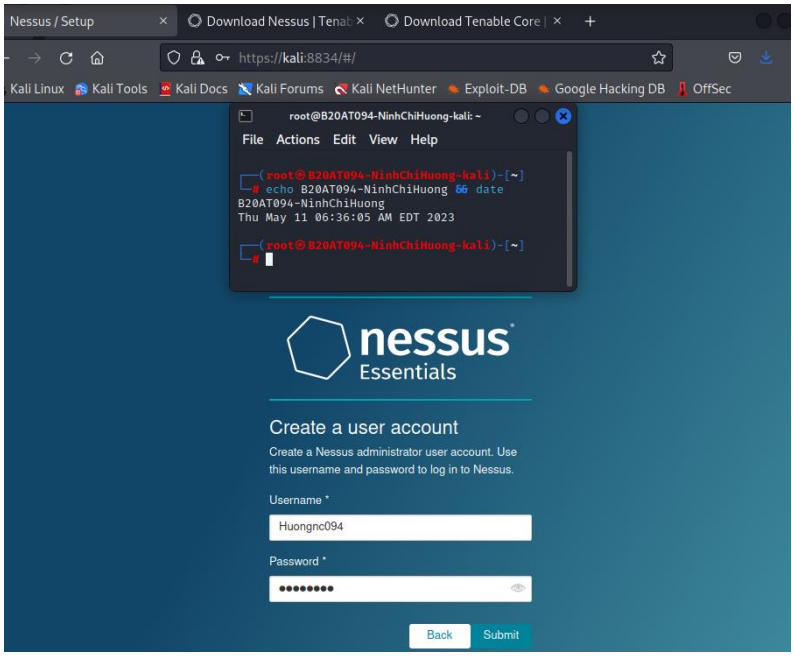
Sử dụng nessus để quét các lỗ hổng trên máy windows XP

o Cài đặt nessus trên Kali Linux.

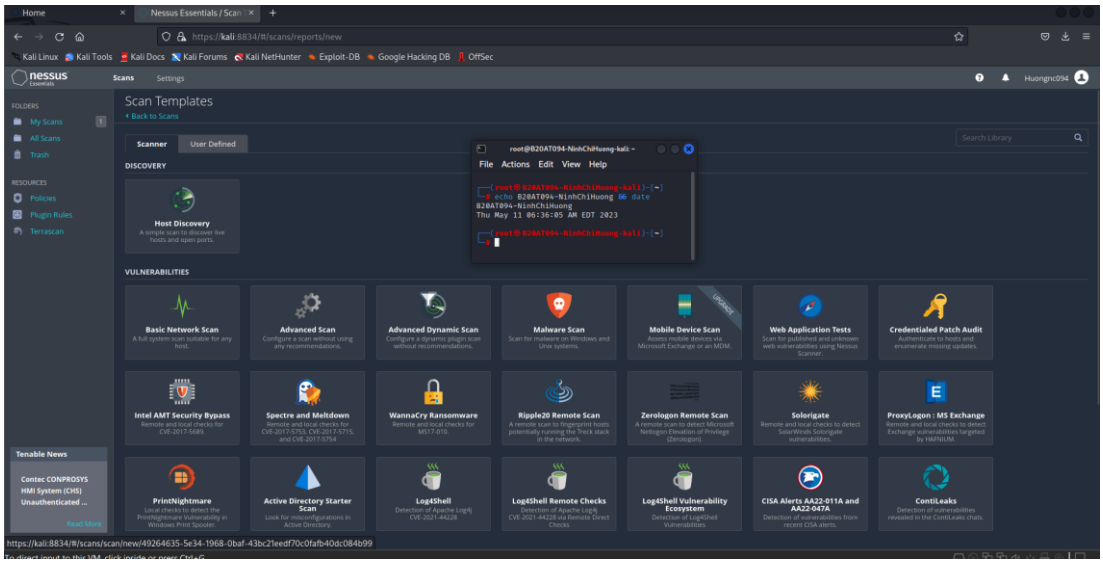
```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[/home/kali/Downloads]
└─# dpkg -i Nessus-10.5.2-ubuntu1404_amd64(1).deb
(Reading database ... 348991 files and directories currently installed.)
Preparing to unpack Nessus-10.5.2-ubuntu1404_amd64(1).deb ...
Unpacking nessus (10.5.2) over (8.15.9) ...
Setting up nessus (10.5.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
```

```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[/home/kali/Downloads]
└─# systemctl start nessusd

┌──(root㉿B20AT094-NinhChiHuong-kali)-[/home/kali/Downloads]
└─# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
     Active: active (running) since Wed 2023-05-17 03:46:36 EDT; 16s ago
   Main PID: 229736 (nessus-service)
      Tasks: 4 (limit: 2264)
     Memory: 27.1M
        CPU: 616ms
     CGroup: /system.slice/nessusd.service
             ├─229736 /opt/nessus/sbin/nessus-service -q
             └─229738 nessusd -q

May 17 03:46:36 B20AT094-NinhChiHuong-kali systemd[1]: Started The Nessus Vulnerability Scanner.
```

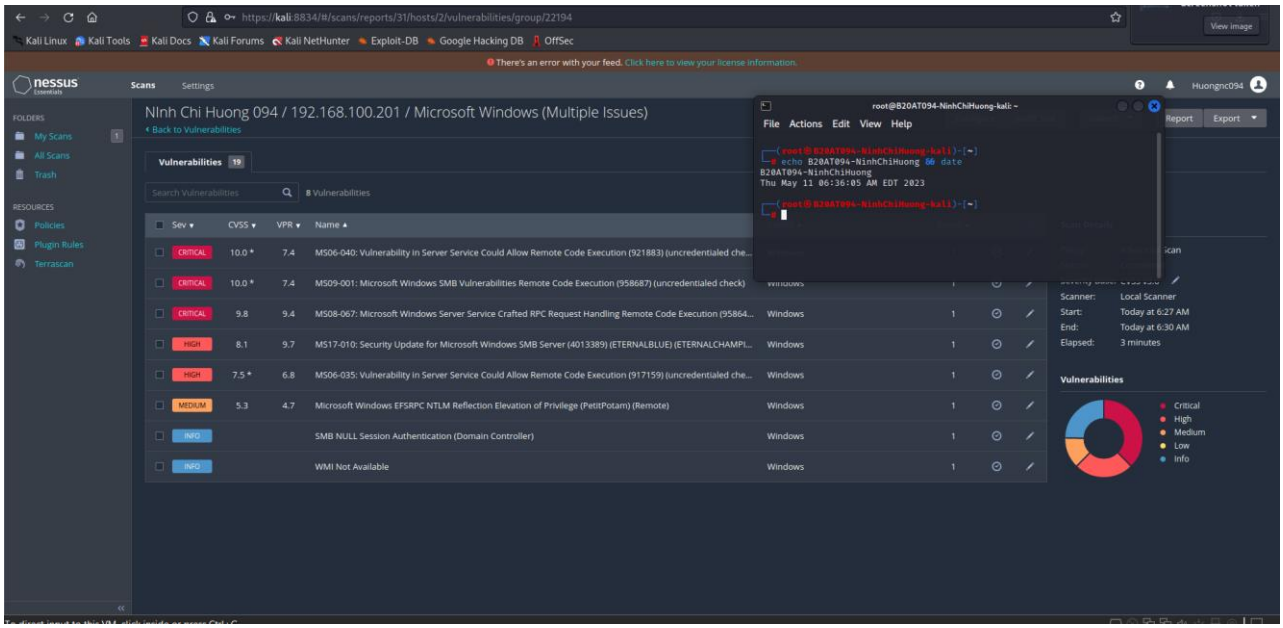


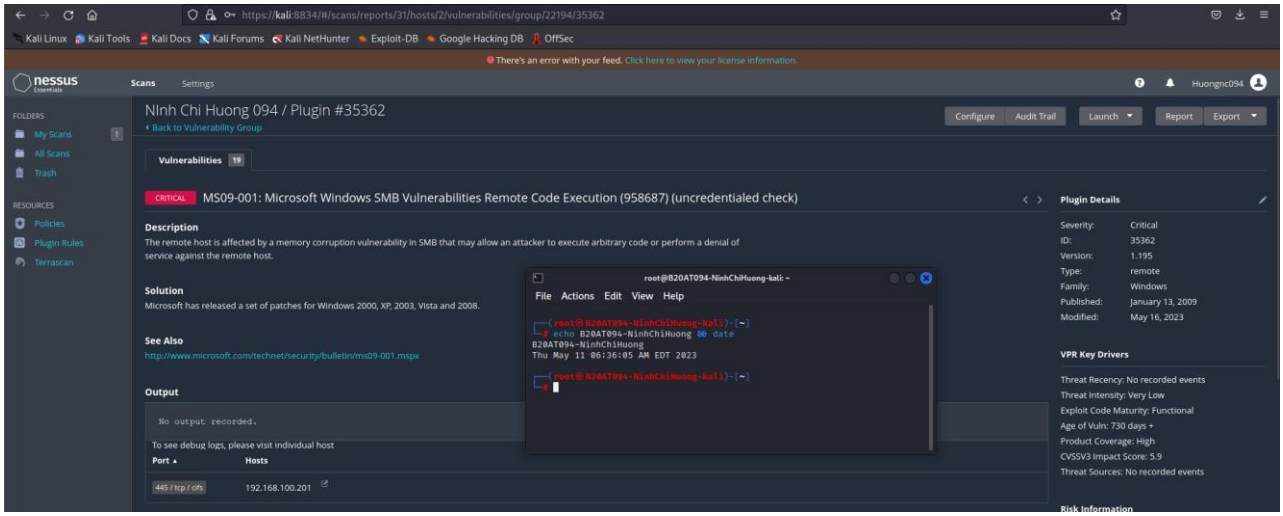


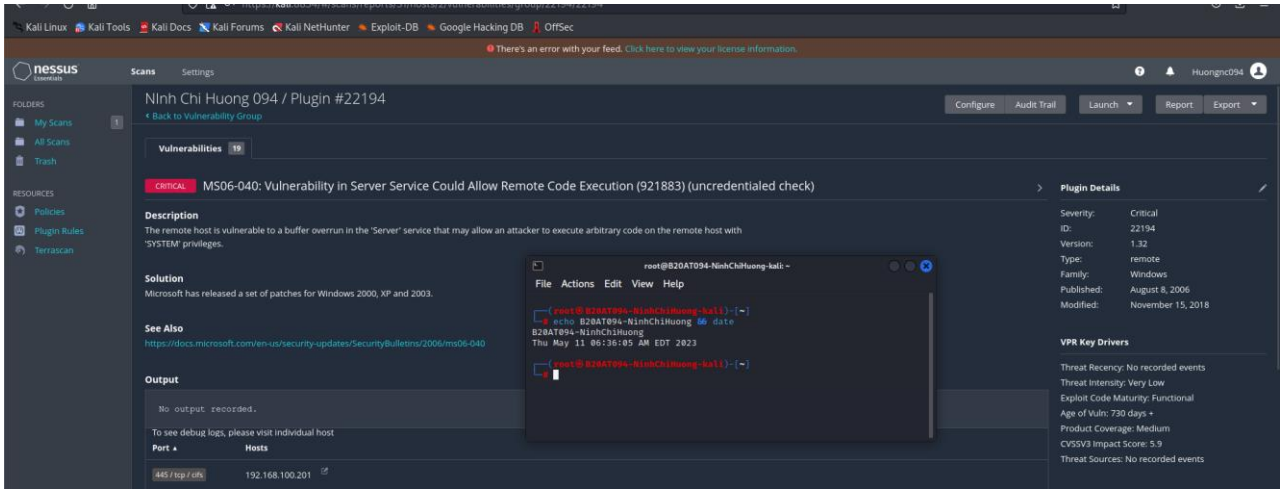
Tiến hành quét máy windows XP

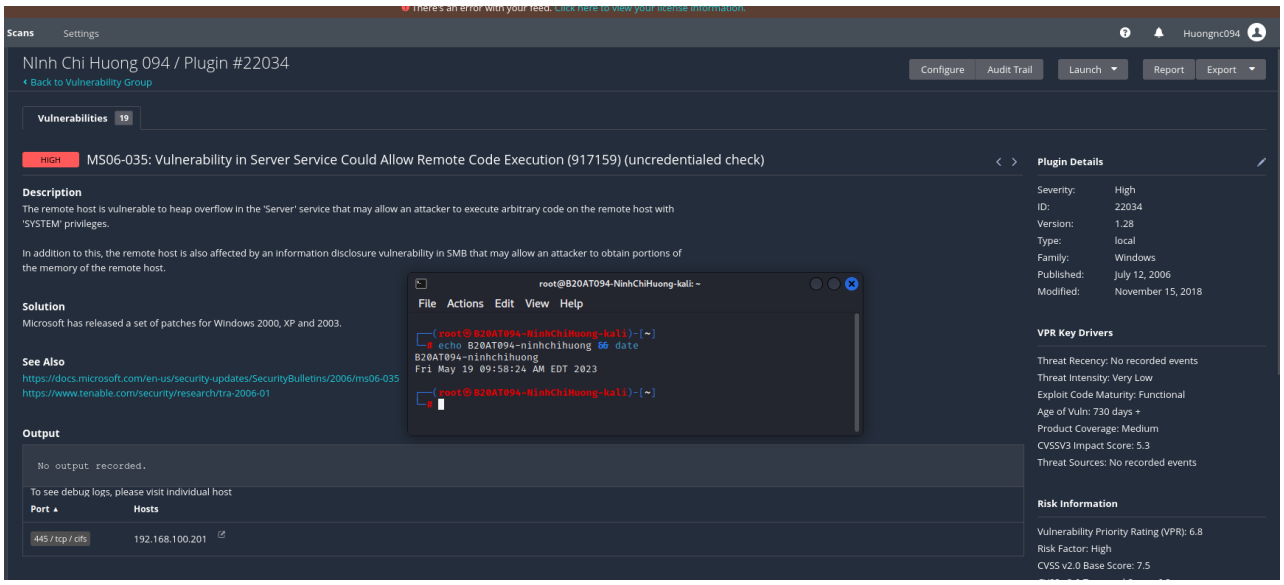


Các lỗ hổng bảo mật nghiêm trọng trên máy windows XP









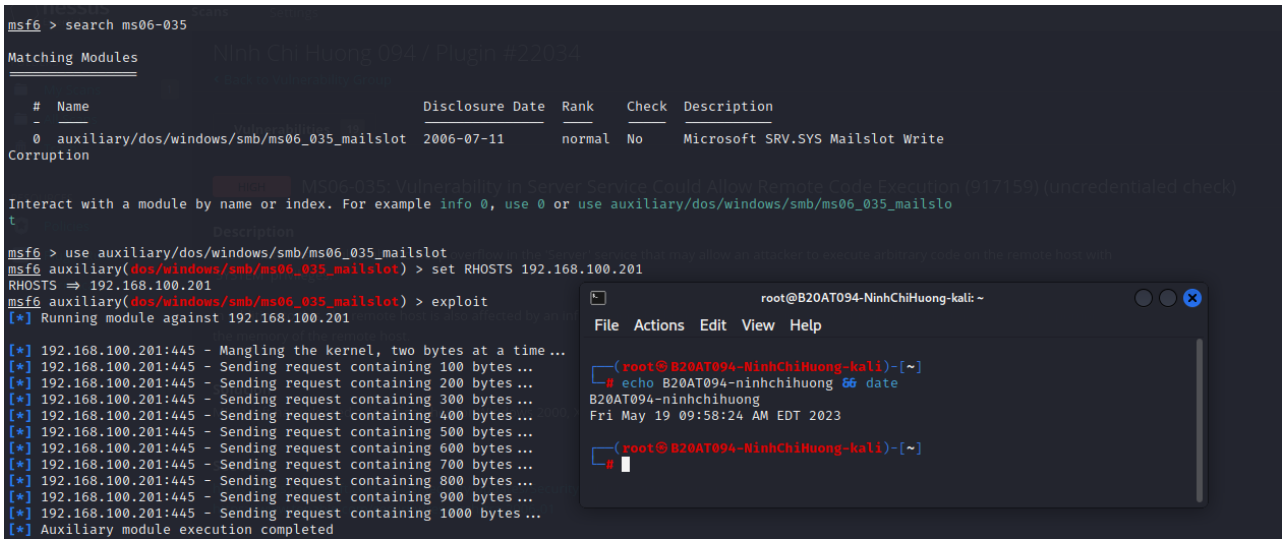
Sử dụng Metaploit framework khai thác lỗ hổng trên Windows XP

Ta sẽ khai thác lỗ hổng MS06-035 như hình trên

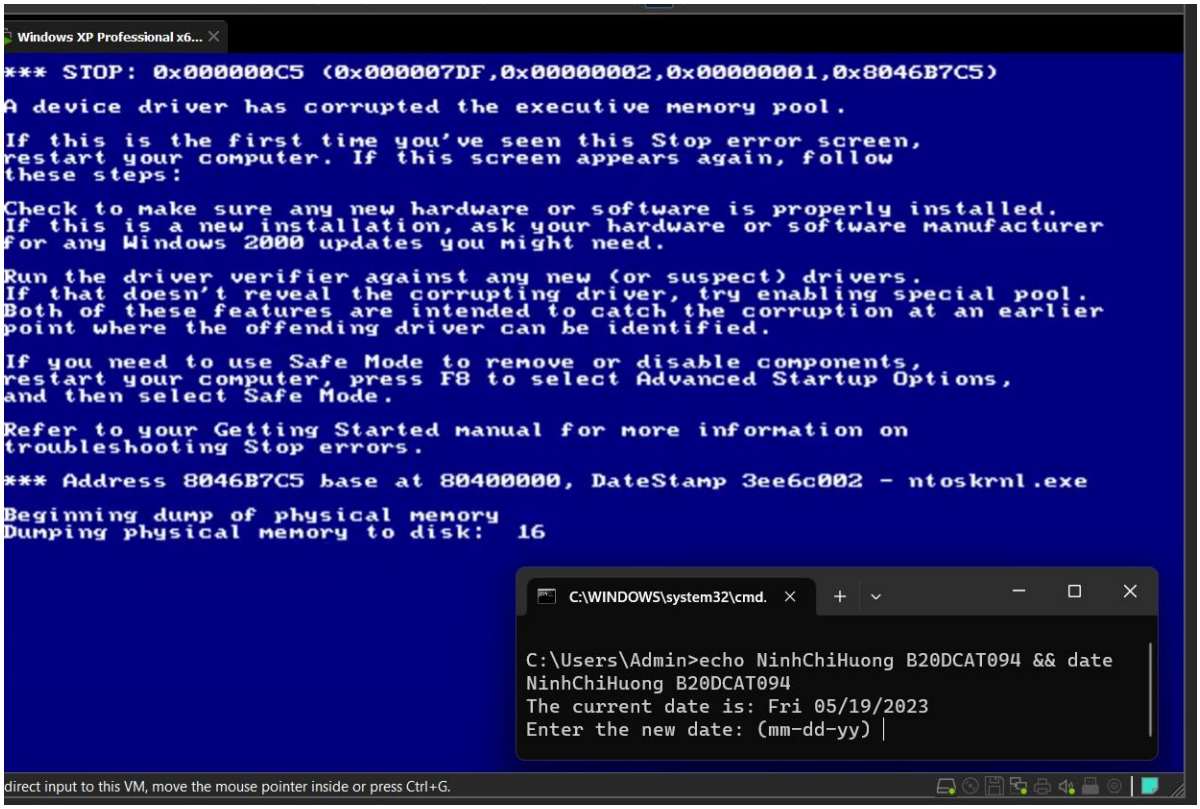
Lỗ hổng MS06-035 là một lỗ hổng bảo mật trong hệ điều hành Windows của Microsoft, được phát hiện vào tháng 6 năm 2006. Lỗ hổng này cho phép tin tặc thực hiện tấn công từ xa và thực hiện mã độc trên hệ thống mà không cần sự cho phép của người dùng.

Lỗ hổng này có liên quan đến giao thức Server Message Block (SMB) trong Windows, được sử dụng để chia sẻ tài liệu và dữ liệu trên mạng. Khi tin tặc khai thác lỗ hổng này, họ có thể gửi một gói tin SMB đặc biệt tới hệ thống và thực hiện mã độc trên hệ thống.

Khai báo module tấn công, sau đó set RHOST để chỉ IP victim



Ngay lập tức máy windows XP bị crash



3. 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-hacker-ceh/

• Lab 14 của CSSIA CompTIA Security+® Supported Labs