|  |  |
| --- | --- |
| **Họ và tên**: Bùi Lê Thủy Tiên  **Mssv**: 22162048  **LAB 01**:  Quét mạng (Scanning networks) | **Nhận xét giáo viên** |

**I. Công đoạn chuần bị thiết bị**

1. **Máy bị tấn công**
   1. **Thông tin máy**

A screenshot of a computer

Description automatically generated

- ***Hệ điều hành***: Microsoft Windows 11 Home Single Language

- ***Network address***: 192.168.0.0 /24

- ***Default gateway***: 192.168.0.1 /24

+ Ấn Window + R 🡪 nhập cmd 🡪 nhập ipconfig

1. **Máy tấn công**
   1. **Thông tin máy**

**A screenshot of a computer

Description automatically generated**

- ***Hệ điều hành:*** Kali Linux

- ***Ip address:*** 192.168.0.113 /24

- ***Default gateway***: 192.168.0.1 /24

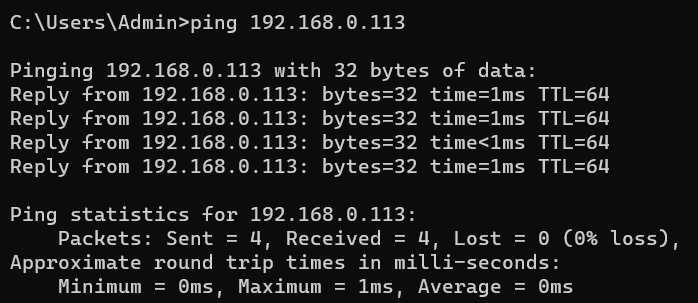
Nếu trưởng hợp máy bạn và máy bị tấn công ***khác*** mạng

+ Đối với VirtualBox, vào Setting máy ảo enable Adapter 2 (unable adapter sẵn có) với lựa chọn Bridge (máy ảo xài chung card mạng với máy thật)

+ Sau đó vào terminal nhấn ifconfig hoặc ip add để có thông tin

1. **Kiểm tra kết nối giữa hai máy**

- Dùng lệnh ping để kiểm tra kết nối giữa 2 máy



**II. Thực hiện**

**1. Yêu cầu 1**

***Using nmap to scan a machine (via IP address or name) to detect an OS & services with TURN ON the firewall on target machine.***

sudo nmap –F *<network>* : thực hiện quét mạng nhanh

**A screen shot of a computer

Description automatically generated**

sudo nmap –O *<IP-target>* : xác định hệ điều hành trên 1 máy chủ, và các lỗ hổng bảo mật

****

sudo nmap –A *<IP-target>* : thực hiện quét toàn diện 1 host

**A computer screen shot of a computer program

Description automatically generated**

sudo nmap –sV *<IP-target>*: quét phiên bản

**A computer screen shot of a computer code

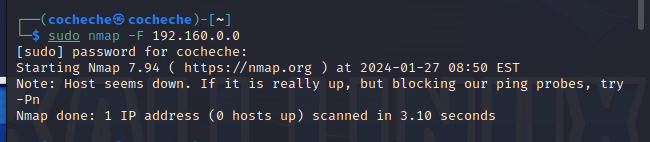
Description automatically generated**

***Using nmap to scan a machine (via IP address or name) to detect an OS & services with TURN OFF the firewall on target machine.***

***Tắt tường lửa***

Đối với win11, vô Settings chọn Privacy and Security sau đó chọn Windows Security và tắt đi

sudo nmap –F *<network>* : thực hiện quét mạng nhanh



sudo nmap –O *<IP-target>* : xác định hệ điều hành trên 1 máy chủ, và các lỗ hổng bảo mật

A computer screen shot of a computer

Description automatically generated

sudo nmap –A *<IP-target>* : thực hiện quét toàn diện 1 host

A screenshot of a computer program

Description automatically generated

sudo nmap –sV *<IP-target>*: quét phiên bản

A computer screen shot of a computer program

Description automatically generated

**🡪** *Khi ta quét lại máy nạn nhân với các lệnh của nmap, ta thấy không thể quét được khi có firewall đang bật. Từ đó rút ra được nhận xét rằng: Firewall giúp ta giảm thiểu các thiệt hại xảy ra khi máy tính bị tấn công, chống kẻ tấn công quét các thông tin trên máy, hệ điều hành của mình, các dịch vụ đang hiện hành trên máy tính***.**

**2.** **Using nmap with vul-scrip to detect vulnerabilities on an OS**

A screenshot of a computer program

Description automatically generatedA screenshot of a computer program

Description automatically generated

*\* Ở bước này chúng ta vẫn phải tắt tường lửa, đây là một số lỗi hỏng của máy khi bị scan.*

***5 lỗ hổng của máy:***

**CVE-2010-3222**

**Xác định lỗ hổng**

Stack-based buffer overflow trong Remote Procedure Call Subsystem (RPCSS) trong Microsoft Windows XP SP2 và SP3 và Server 2003 SP2 cho phép người dùng cục bộ có được các đặc quyền thông qua thông báo LPC được tạo thủ công yêu cầu kết nối LRPC từ máy chủ LPC đến máy khách, hay còn gọi là "LPC Message Buffer Overrun Vulnerability."

*Affected Products*: Microsoft Windows XP SP2 and SP3, Microsoft Windows Server 2003 SP2

*Vulnerability Type*: Stack-based buffer overflow

*Impact:* Privilege escalation (local user to SYSTEM), Arbitrary code execution, Denial-of-service

Severity:



**CVE-2010-2742**

**Xác định lỗ hỏng**

Dịch vụ Netlogon RPC trong Microsoft Windows Server 2003 SP2 và Server 2008 Gold, SP2 và R2, khi vai trò bộ điều khiển miền được bật, cho phép kẻ tấn công từ xa thực hiện từ chối dịch vụ (hủy tham chiếu con trỏ NULL và khởi động lại) thông qua gói RPC được tạo thủ công, hay còn gọi là "Netlogon RPC Null dereference DOS Vulnerability."

*Affected Products*: Microsoft Windows Server 2003 SP2 (when the domain controller role is enabled), Microsoft Windows Server 2008 Gold, SP2, and R2 (when the domain controller role is enabled)

*Vulnerability Type*: Remote denial-of-service (DoS)

*Impact*: Remote attackers can crash the Netlogon RPC service, potentially rebooting the system. This could lead to disruption of services, data loss, and other security risks.

*Severity:*

A close up of a logo

Description automatically generated**CVE-2010-2729**

**Xác định lỗ hỏng**

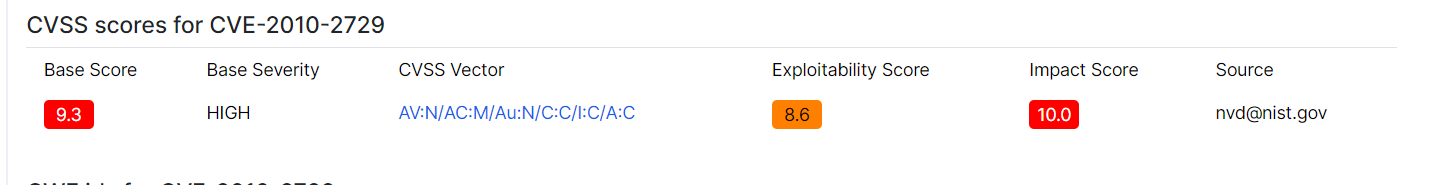
CVE-2010-2729, còn được gọi là "Print Spooler Service Impersonation Vulnerability", là một lỗ hổng nghiêm trọng ảnh hưởng đến dịch vụ Print Splooler trong một số phiên bản Microsoft Windows. Nó cho phép những kẻ tấn công từ xa, không được xác thực thực thi mã tùy ý với các đặc quyền hệ thống, giúp chúng có toàn quyền kiểm soát hệ thống bị ảnh hưởng.

*Affected Products*: Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, Windows 7 (when printer sharing is enabled)

*Vulnerability Type*: Service impersonation vulnerability

*Impact*: Remote code execution with SYSTEM privileges

*Severity:*



**CVE-2010-3139**

**Xác định lỗ hỏng**

CVE-2010-3139 là một lỗ hổng nghiêm trọng ảnh hưởng đến Microsoft Windows Progman Group Converter (grpconv.exe) trong Windows XP, Server 2003 và 2000. Nó cho phép người dùng cục bộ và những kẻ tấn công từ xa có thể thực thi mã tùy ý và tiến hành các cuộc tấn công chiếm quyền điều khiển DLL.

*Affected Products:* Microsoft Windows XP Service Pack 3 and prior, Windows Server 2003 Service Pack 2 and prior, Windows 2000 Service Pack 4 and prior

*Vulnerability type:* Untrusted search path vulnerability

*Impact:* Arbitrary code execution, DLL hijacking

*Severity:* Critical

*CVSS score:* theo <https://www.cvedetails.com/>

A screenshot of a computer

Description automatically generated

**CVE-2010-2567**

**Xác định lỗ hỏng**

CVE-2010-2567 là một lỗ hổng nghiêm trọng ảnh hưởng đến việc triển khai máy khách RPC trong Microsoft Windows XP SP2 và SP3 cũng như Server 2003 SP2. Nó cho phép kẻ tấn công từ xa thực thi mã tùy ý trên các hệ thống dễ bị tấn công bằng cách gửi phản hồi không đúng định dạng tới yêu cầu RPC. Lỗ hổng này còn được gọi là "RPC Memory Corruption Vulnerability."

*Affected Products*: Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2

*Vulnerability type*: Memory corruption

*Impact*: Arbitrary code execution

*Severity:* Critical

*CVE score:* theo <https://www.cvedetails.com/>

A close up of a computer screen

Description automatically generated

**3. Sử dụng metaploit để truy cập vào các máy với các lỗ hổng remote**

***Cài đặt và cấu hình***

Trước tiên, bạn cần cài đặt Metasploit Framework trên máy tính của bạn. Bạn có thể tìm hướng dẫn cài đặt cụ thể dựa trên hệ điều hành mà bạn đang sử dụng. Sau khi cài đặt xong, mở terminal và gõ ***msfconsole*** để khởi động Metasploit Console.

- Máy tấn công:

**A screenshot of a computer

Description automatically generated**

- Máy target: metasploitable2

A screenshot of a computer

Description automatically generated

- Bước 1: Tiến hành kiểm tra kết nối mạng giữa 2 máy bằng lệnh ping

A screenshot of a computer screen

Description automatically generated

Bước 2: Tiến hành scan các port đang mở của máy target

A screenshot of a computer program

Description automatically generated

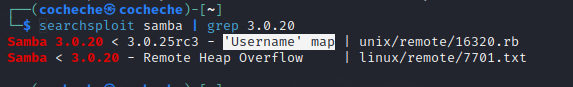
Bước 3: scan version xem những module nào có thể xài cho máy target

A screenshot of a computer screen

Description automatically generated

Bước 4: dùng searchsploit tìm

- searchsploit samba | grep 3.0.20



Bước 5: chọn module tấn công

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generatedA computer screen shot of a program

Description automatically generatedA screenshot of a computer

Description automatically generated

**4. Hướng khắc phục**

\* Hướng khắc phục để chống lại quá trình quét mạng của attacker:

- *Sử dụng tường lửa (Firewall)*

Cấu hình tường lửa để chặn các cổng không sử dụng.

Sử dụng các quy tắc lọc IP để hạn chế truy cập từ các địa chỉ IP đáng ngờ.

Kích hoạt chức năng giám sát và cảnh báo của tường lửa.

- *Cập nhật phần mềm và hệ điều hành*

Luôn cập nhật các bản vá bảo mật mới nhất cho hệ điều hành và phần mềm.

Sử dụng các phần mềm diệt virus và chống phần mềm độc hại uy tín.

- *Mã hóa dữ liệu*

Sử dụng các phương pháp mã hóa để bảo vệ dữ liệu nhạy cảm.

Sử dụng VPN để mã hóa lưu lượng truy cập internet.