**REPORT**

**Yêu cầu:** Sử dụng tool nmap để quét thiết bị biết thông tin về hệ điều hành, ports và các dịch vụ của thiết bị, ngoài ra hãy xem sự khác biệt giữa máy bị target bật firewall và ko bật.

Sử dụng tool nmap vulscan để quét lỗ hổng bảo mật CVE và tìm hiểu giải thích lỗ hổng đó ( ~5)

**Kịch bản:** Sử dụng 2 máy ảo để giả lập tấn công, máy thứ nhất dùng kali linux và máy thứ hai dùng win11, máy ảo kali linux sẽ tấn công đến máy ảo win11

**Công cụ / mô hình:** Sử dụng Vmware Workstation Pro version 17.8 để thực hiện, và tool nmap có sẵn đồng thời tải các scripts của vulscan để quét lỗ hổng bảo mật, với mô hình Bridge

**Setup:**

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

**Steps:** Dùng lệnh ip a show để check ip máy kali linux có địa chỉ ip là 192.168.1.7/24.

A screenshot of a computer screen

AI-generated content may be incorrect.

Trong win11 vô setting chỉnh địa chỉ IPv4 thành 192.168.1.72/24 với DNS là 8.8.8.8

A screenshot of a computer

AI-generated content may be incorrect.

**Bài 1: Nhớ tắt tường lửa**

Sử dụng lệnh **sudo nmap -F 192.168.1.72** để quét nhanh các ports đang mở

A computer screen shot of a computer

AI-generated content may be incorrect.

Sử dụng lệnh **sudo nmap -O 192.168.1.72** để quét hệ điều hành máy là gì ( **OS** )

A screenshot of a computer

AI-generated content may be incorrect.

Sử dụng lệnh **sudo nmap -A 192.168.1.72** để quét thông tin các ports và services, OS và ping,…

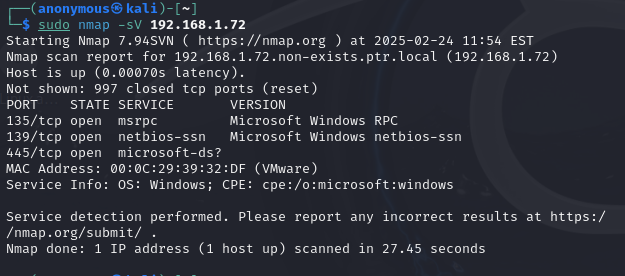
A computer screen shot of a computer program

AI-generated content may be incorrect.

A computer screen with white text

AI-generated content may be incorrect.

Sử dụng lệnh **sudo nmap -sV 192.168.1.72** để quét các dịch vụ các ports



**Bài 2:** Tắt tường lửa từ máy bị target

Git clone về các scripts về từ github bằng lệnh git clone https://github.com/scipag/vulscan scipag\_vulscan.

Sau đó install vulscan vào nmap bằng lệnh **sudo ln -s `pwd`/scipag\_vulscan /usr/share/nmap/scripts/vulscan**

A blue text on a black background

AI-generated content may be incorrect.

Nhập lệnh **cd /usr/share/nmap/scripts** và nhập lệnh ls để check đã có tệp vulscan chưa

Sau đó nhập lệnh **ls vulsca**n để check có các scripts trong tệp vulscan chưa

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer program

AI-generated content may be incorrect.

Nếu có thì dùng lệnh **sudo nmap –script=/usr/share/nmap/scripts/vulscan.nse –script-args vulscandb=cve.csv -sV -oN report.txt 192.168.1.7**2 để quét các lỗ hổng CVE và tạo ra file txt lưu các lỗi đó

**Results:**

**Bài 1:**

* **Bật Firewall**

A computer screen shot of a computer screen

AI-generated content may be incorrect.

* **Tắt Firewall**

A computer screen shot of a computer program

AI-generated content may be incorrect. A computer screen with white text

AI-generated content may be incorrect.

**Bài 2:**

****

**Đánh giá:**

**CVE-2010-3222:** Lỗ hổng bảo mật trong Windows Kernel của Microsoft Windows được công bố năm 2010. Xử lý các giá trị con trỏ, nếu kẻ tấn công khai thác thành công họ có thể thực thi mã tùy ý với quyền cao hơn có thể lên tới đặc quyền. Sử dung ứng dụng độc hại để kích hoạt lỗi này và thực thi mã quyền System giành quyền kiểm soát toàn bộ máy tính.

**CVE-2010-3139:** Lỗ hổng bảo mật trong Microsoft Windows Shell được phát hiện năm 2010. Lỗi này xử lý các shortcut (.LNK) ko an toàn. Một shortcut độc hại có thể được thiết kế thưc thi mã tùy ý khi người dùng mở hoặc xem nó. Điều này dẫn đến việc chiếm quyền kiểm soát hệ thống.

**CVE-2010-2742:** Lỗ hổng bảo mật trong Windows Local Security Authority Subsystem Service của Microsoft Windows được phát hiện năm 2010. Nếu khai thác thành công có thể gây ra lỗ từ chối dịch vụ (DoS) bằng cách là hệ thống treo hoặc khởi động lại.

**CVE-2010-2729:** Lỗ hổng bảo mật nghiêm trọng trong Print Spooler Service của Microsoft Windows được phát hiện vào năm 2010, Kẻ tấn công gửi file in ấn độc hại qua mạng. Khi Windows Print Spooler xử lý tập tin này nó có thể thực thi mã độc với quyền System dẫn đến quyền điều khiển hoàn toàn hệ thống.

**CVE-2009-1544:** Lỗ hổng thực thi mã từ xa trong Adobe Reader & Acrobat vào năm 2009. Lỗ hổng này bị khai thác để thực thi mã từ xa (RCE) cho phép kẻ tấn công chiếm quyền kiểm soát hệ thống của nạn nhân.