Họ và tên: Lương Chin Du MSSV:21110870

Môn học: An toàn thông tin Mã môn: INSE330380\_23\_1\_09

Giảng viên hướng dẫn: Huỳnh Nguyên Chính

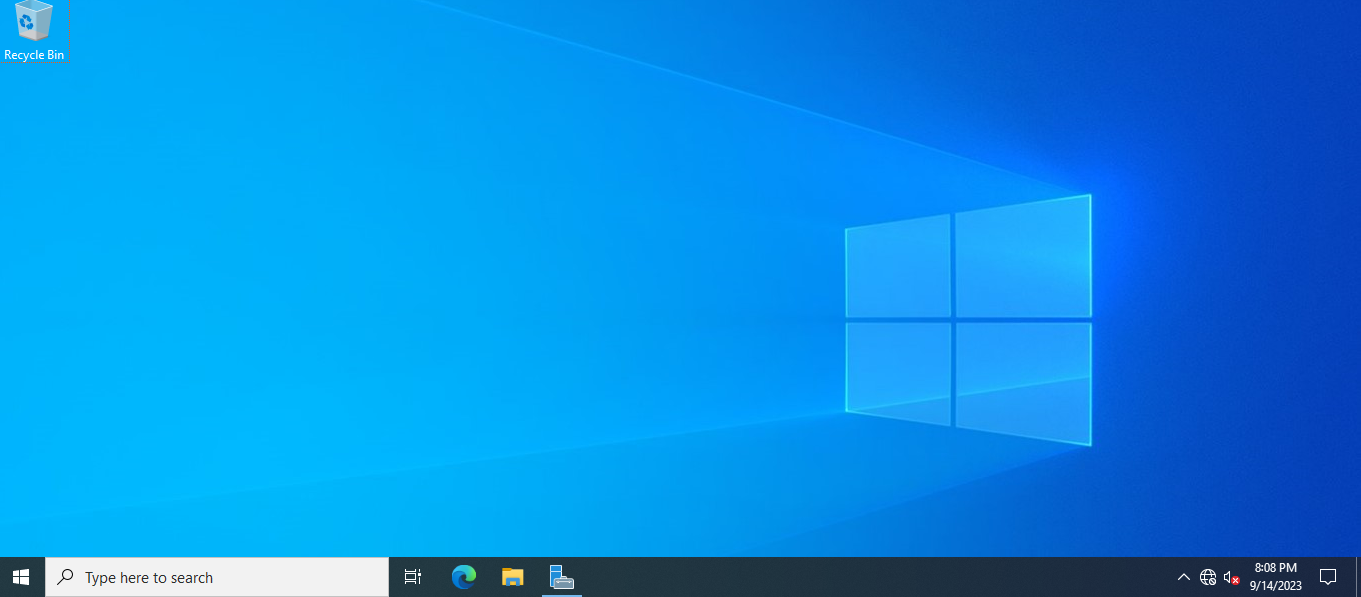
**Lab 1: OS security**

Detect OS, services, and vulnerabilities

**Máy tấn công – Ubuntu 16.04 (32 bit):**

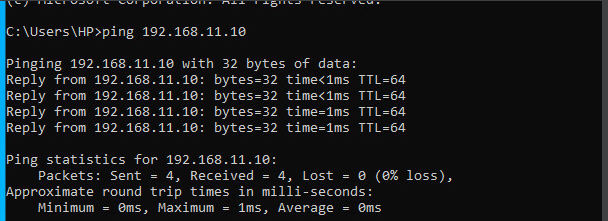
****

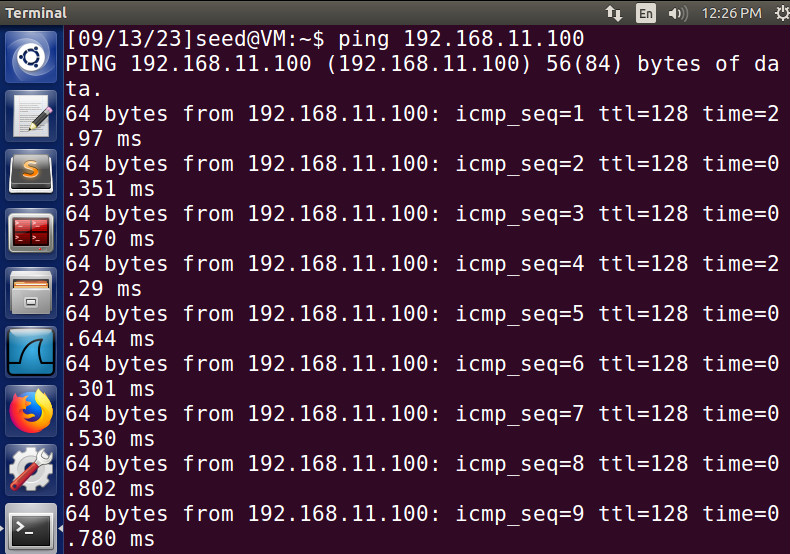
**Máy nạn nhân: Windows 10**



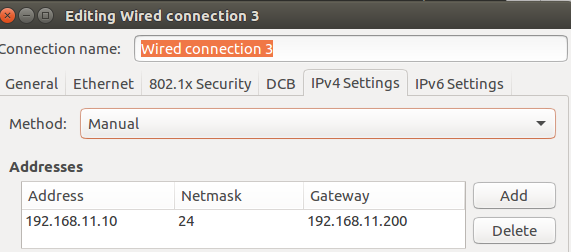
Để bước vào bài lab ta cần:

Chuẩn bị 2 máy ảo phải được kết nối với nhau: Kiểm tra xem 2 máy đã kêt nối với nhau chưa thì ta có thể dùng lệnh ping

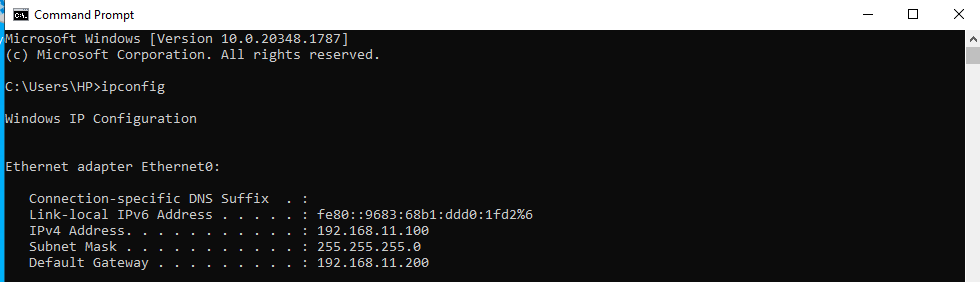




1. Máy tấn công có địa chỉ ip: 192.168.11.10, subnetmask: 255.255.255.0, default gateway: 192.168.11.200



1. Máy nạn nhân có địa chỉ ip là 192.168.11.100, subnetmask: 255.255.255.0, default gateway: 192.168.11.200



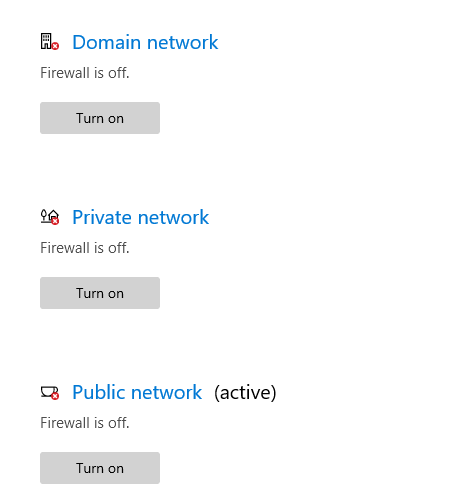
Cài đặt nmap trên ubuntu (nmap là một công cụ quét mạng mạnh mẽ và dùng để phát hiện ra lỗ hổng trong mạng, port, ...). Để cài đặt nmap ta sử dụng lệnh sau:

**$ sudo apt-get install nmap**



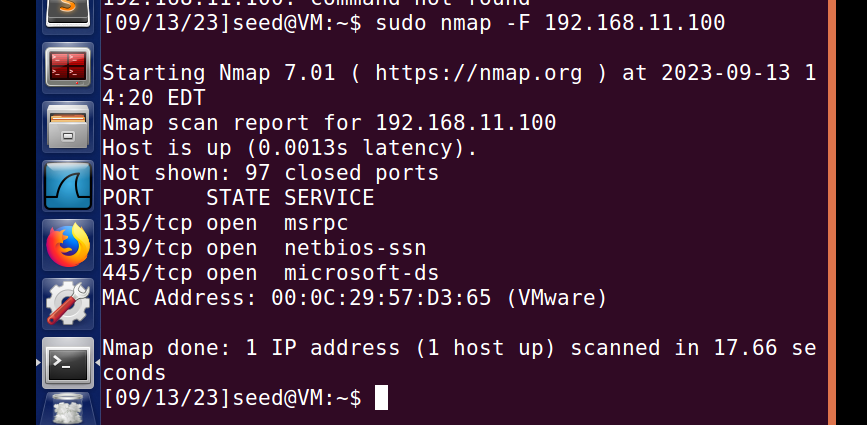
1. Using nmap to scan a machine (via IP address or name) to detect an OS & services (Sử dụng nmap để quét 1 máy nạ nhân (thông qua địa chỉ IP hoặc tên) để phát hiện hệ điều hành và các dịch vụ đang được sử dụng trên máy đó)

* Trường hợp: bên máy nạn nhân (Window 10) tắt tường lửa:

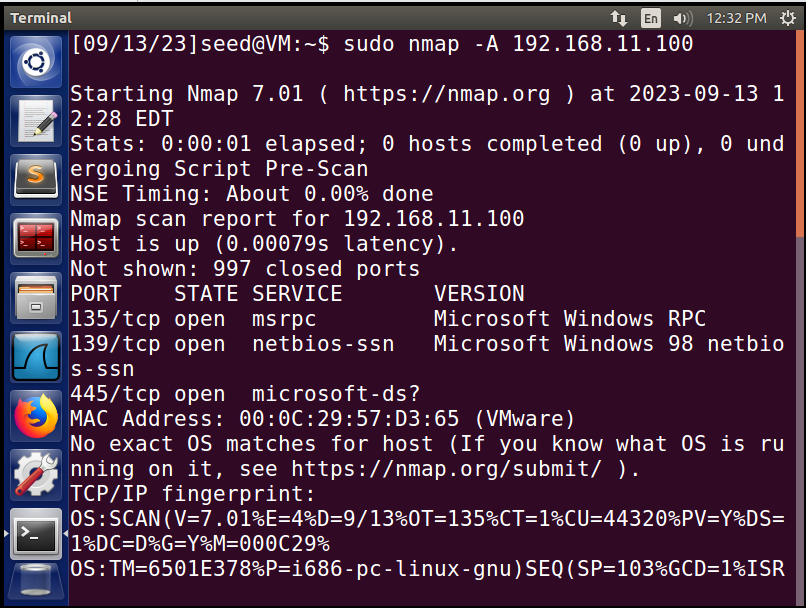


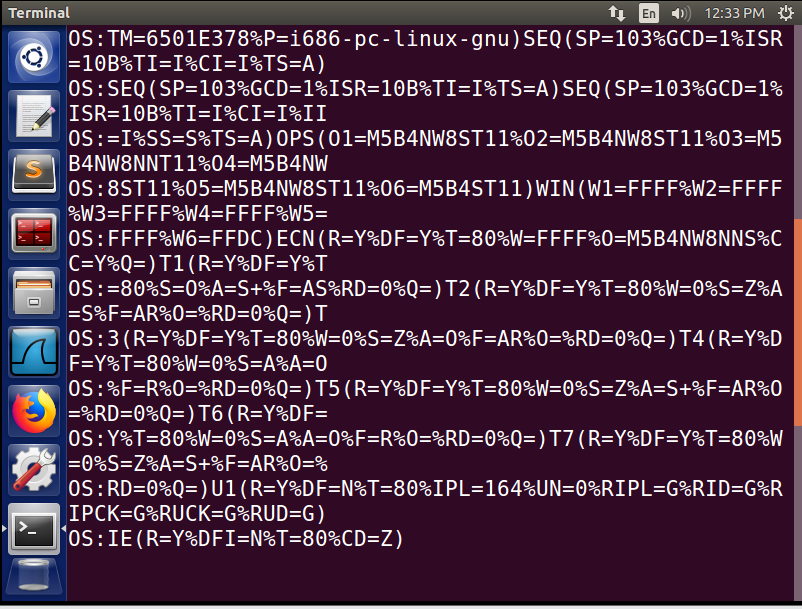
Thực hiện trên máy tấn công (ubuntu 16.04)

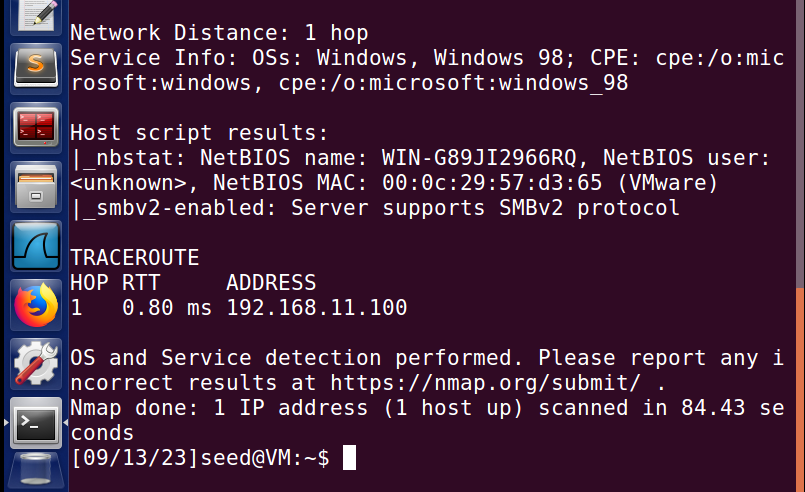
* **Sử dụng lệnh sudo nmap -F 192.168.11.100**



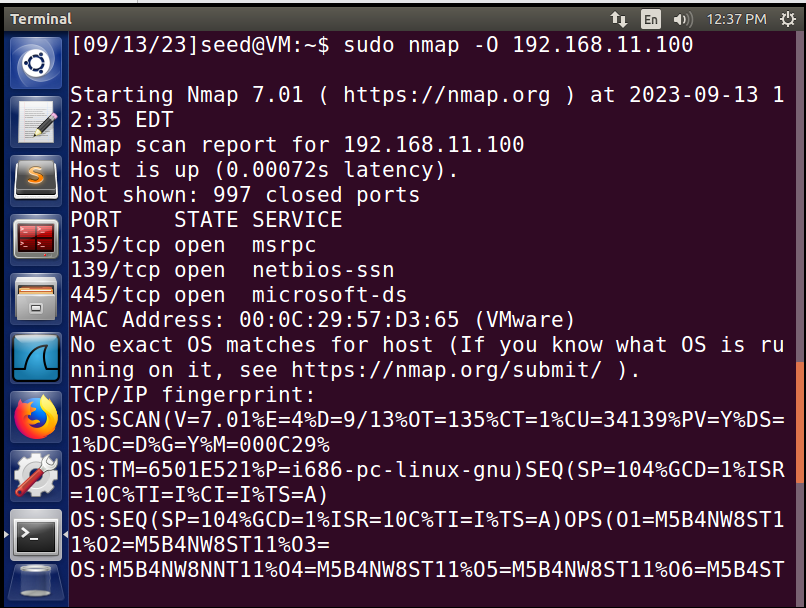
* **Sử dụng lệnh sudo nmap -A 192.168.11.100**

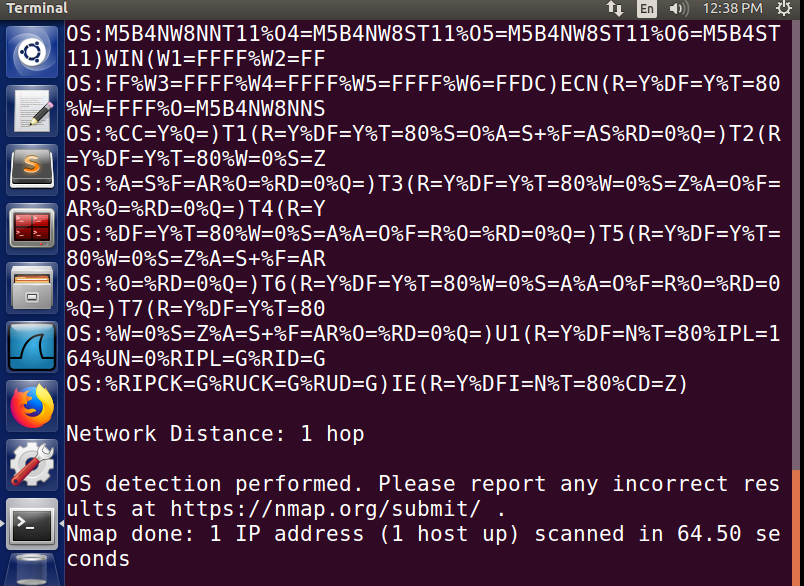




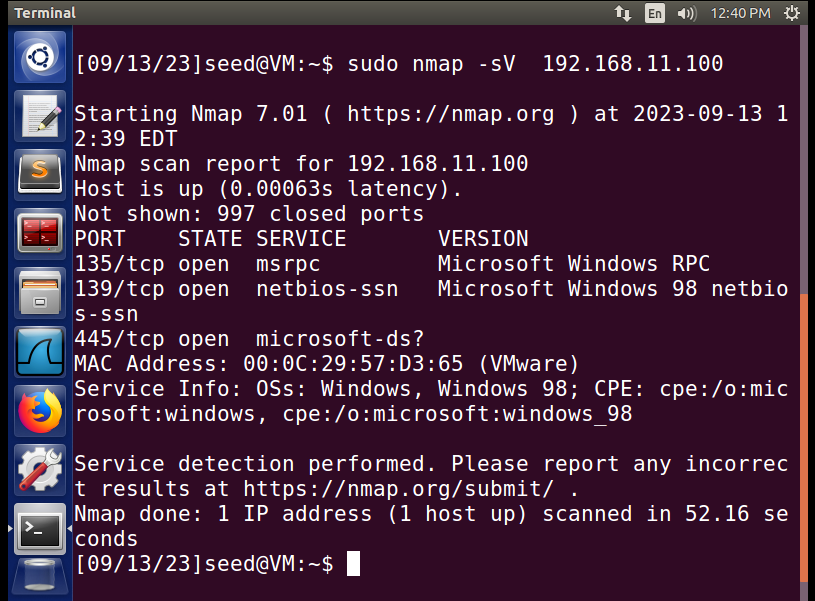


* **Sử dụng lệnh sudo nmap -O 192.168.11.100**



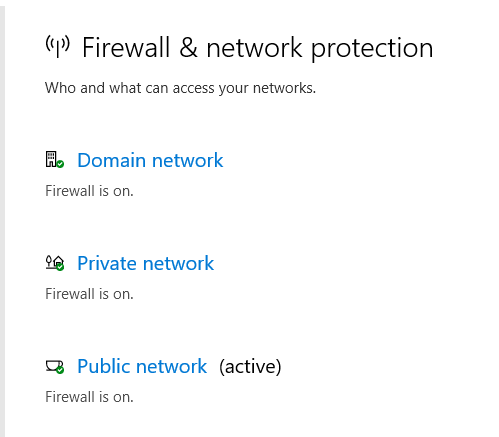


* **Sử dụng lệnh sudo nmap -sV 192.168.11.100**

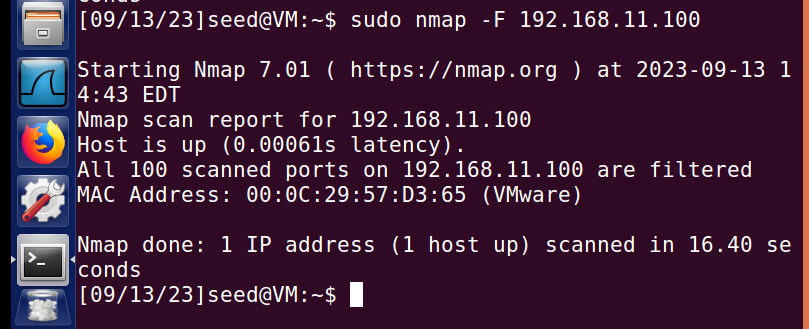


🡪Sau khi sử dụng các lệnh trên ta thu được các kết quả sau: danh sách các port đang mở, cùng với các service đang được dùng, các thông tin về hệ điều hành và máy victim…

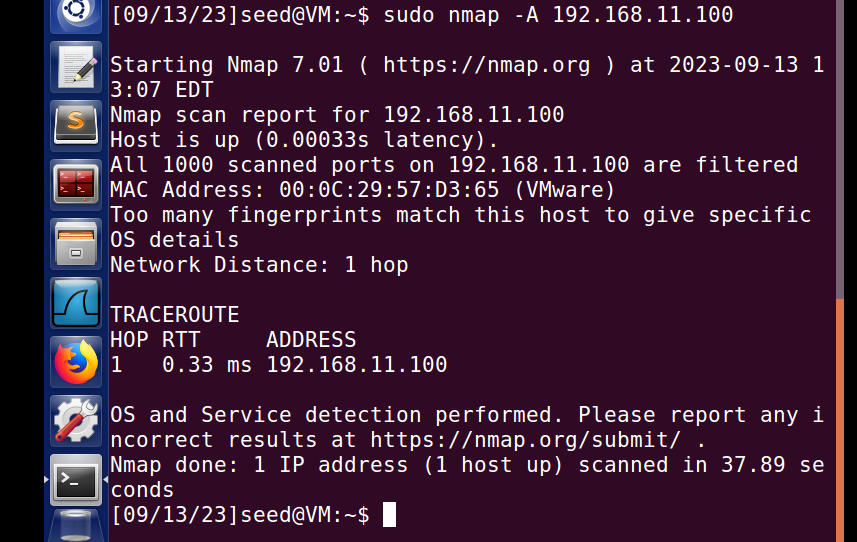
* Trường hợp: bên máy nạn nhân (Window 10) bật tường lửa:



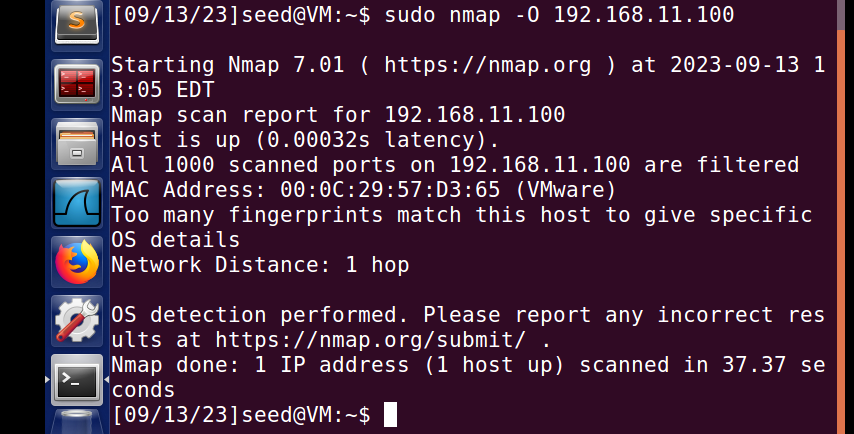
* **Sử dụng lệnh sudo nmap -F 192.168.11.100**

****

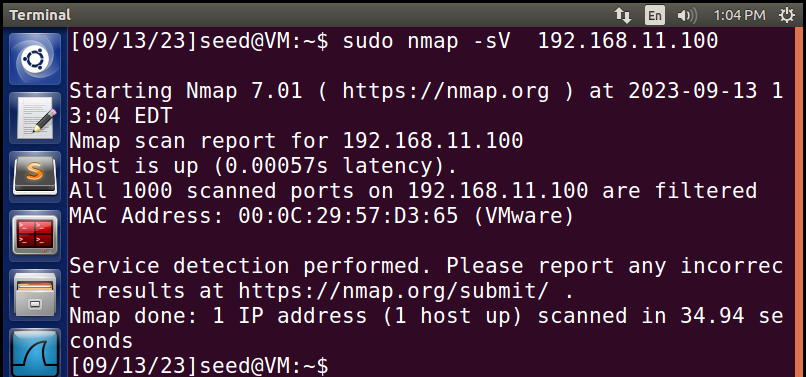
* **Sử dụng lệnh sudo nmap -A 192.168.11.100**



* **Sử dụng lệnh sudo nmap -O 192.168.11.100**



* **Sử dụng lệnh sudo nmap -sV 192.168.11.100**



* Khi ta quét lại máy nạn nhân với các lệnh (sudo nmap -A 192.168.11.100, sudo nmap -O 192.168.11.100, sudo nmap -sV 192.168.11.100, sudo nmap -F 192.168.11.100) ta thấy không thể quét được các cổng, hệ điều hành và các dịch vụ đang sử dụng là gì, do 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.

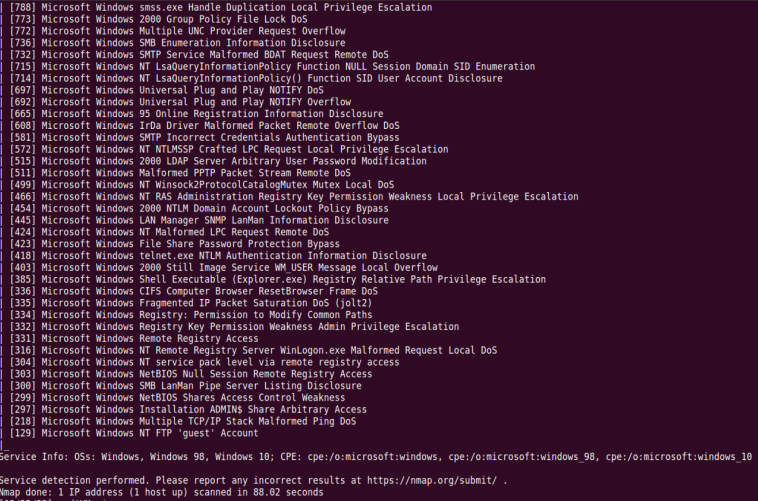
Bài 2: **Using nmap with vul-scrip to detect vulnerabilities on an OS**

Cài đặt vul-scrip để phát hiện các lỗ hổng bằng lệnh:

**$git clone https://github.com/scipag/vulscan scipag\_vulscan**

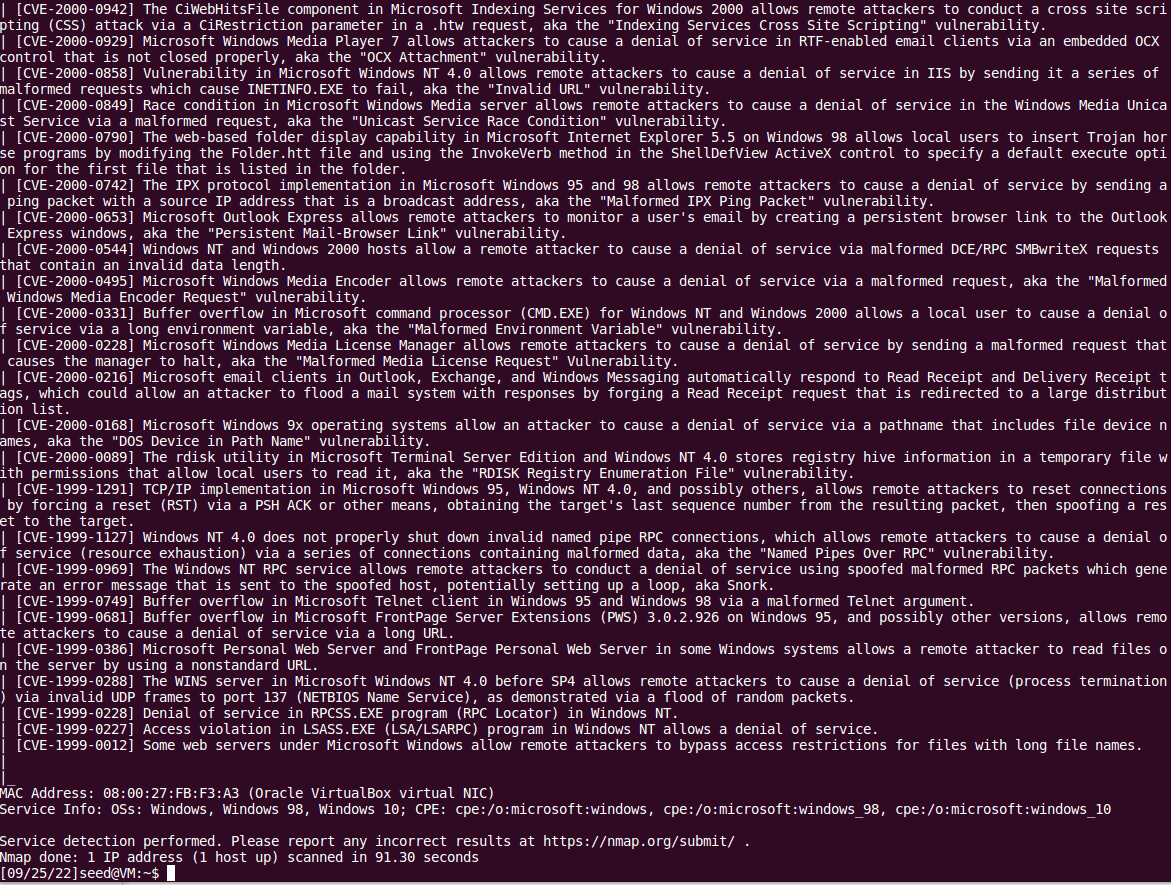
**Chạy lệnh:** $sudo nmap -sV --script=vulscan/vulscan.nse 192.168.11.100

(lệnh này sẽ chạy nmap với các tùy chọn để quét thiết bị có IP 192.168.11.100, xác định các cổng mạng đang mở và các dịch vụ đang chạy trên các cổng đó, sau đó kiểm tra các lỗ hổng bảo mật đã biết trên các dịch vụ này bằng cách sử dụng tập lệnh script vulscan.nse)



* **Sinh ra nhiều lỗ hổng và muốn tìm lỗ hổng có mã CVE ta dùng lệnh:**

**$ sudo nmap --script vulscan --script-args vulscandb=cve.csv -sV 192.168.11.100**



**Thông tin về năm lỗ hổng CVE (Common Vulnerability Exposures)**

**1.CVE-1999-1291:** Việc triển khai TCP / IP trong Microsoft Windows 95, Windows NT 4.0 và có thể cả những người khác, cho phép kẻ tấn công từ xa đặt lại kết nối bằng cách buộc đặt lại (RST) thông qua PSH ACK hoặc các phương tiện khác, lấy số thứ tự cuối cùng của mục tiêu từ gói kết quả, sau đó giả mạo đặt lại mục tiêu. <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-1999-1291>

<https://www.opencve.io/cve/CVE-1999-1291>

|  |  |
| --- | --- |
| Access Vector (network) | lỗ hổng có thể được tấn công từ xa thông qua mạng, mà không yêu cầu tấn công đối tượng phải có quyền truy cập cục bộ vào hệ thống. |
| Access Complexity (low) | để khai thác lỗ hổng, kẻ tấn công không cần phải thực hiện các thao tác phức tạp hoặc có kiến thức cao về hệ thống. |
| Authentication (none) | không cần xác thực để khai thác lỗ hổng |
| Confidentiality Impact (none) | không có nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Integrity Impact (none) | nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Availability Impact (parital) | lỗ hổng gây ra một mức độ tác động đáng kể đến khả năng sẵn sàng của hệ thống hoặc dịch vụ, nhưng không gây ra sự sụp đổ hoàn toàn. |
| ID CWE | không xác định |

**2.CVE-2000-0216**: Ứng dụng email khách của Microsoft trong Outlook, Exchange và Windows Messaging tự động phản hồi các thẻ Biên nhận đã đọc và Biên nhận gửi, điều này có thể cho phép kẻ tấn công tràn ngập hệ thống thư bằng các phản hồi bằng cách giả mạo yêu cầu Biên nhận đã đọc được chuyển hướng đến một danh sách phân phối lớn. <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2000-0216>

<https://www.opencve.io/cve/CVE-2000-0216>

|  |  |
| --- | --- |
| Access Vector (network) | lỗ hổng có thể được tấn công từ xa thông qua mạng, mà không yêu cầu tấn công đối tượng phải có quyền truy cập cục bộ vào hệ thống. |
| Access Complexity (low) | để khai thác lỗ hổng, kẻ tấn công không cần phải thực hiện các thao tác phức tạp hoặc có kiến thức cao về hệ thống. |
| Authentication (none) | không cần xác thực để khai thác lỗ hổng |
| Confidentiality Impact (none) | không có nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Integrity Impact (none) | nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Availability Impact (parital) | lỗ hổng gây ra một mức độ tác động đáng kể đến khả năng sẵn sàng của hệ thống hoặc dịch vụ, nhưng không gây ra sự sụp đổ hoàn toàn. |
| ID CWE | không xác định |

**3.CVE-1999-0681:** Tràn bộ đệm trong Microsoft FrontPage Server Extensions (PWS) 3.0.2.926 trên Windows 95 và có thể cả các phiên bản khác, cho phép kẻ tấn công từ xa gây ra tình trạng từ chối dịch vụ thông qua một URL dài.

[**https://www.opencve.io/cve/CVE-1999-0681**](https://www.opencve.io/cve/CVE-1999-0681)

|  |  |
| --- | --- |
| Access Vector (network) | lỗ hổng có thể được tấn công từ xa thông qua mạng, mà không yêu cầu tấn công đối tượng phải có quyền truy cập cục bộ vào hệ thống. |
| Access Complexity (low) | để khai thác lỗ hổng, kẻ tấn công không cần phải thực hiện các thao tác phức tạp hoặc có kiến thức cao về hệ thống. |
| Authentication (none) | không cần xác thực để khai thác lỗ hổng |
| Confidentiality Impact (none) | Không có nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Integrity Impact (none) | nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Availability Impact (parital) | lỗ hổng gây ra một mức độ tác động đáng kể đến khả năng sẵn sàng của hệ thống hoặc dịch vụ, nhưng không gây ra sự sụp đổ hoàn toàn. |
| ID CWE | không xác định |

**4.CVE-2000-0929:** Microsoft Windows Media Player 7 cho phép kẻ tấn công gây ra tình trạng từ chối dịch vụ trong ứng dụng email khách hỗ trợ RTF thông qua điều khiển OCX nhúng không được đóng đúng cách, hay còn gọi là lỗ hổng "OCX Attachment".

[**https://www.opencve.io/cve/CVE-2000-0929**](https://www.opencve.io/cve/CVE-2000-0929)

|  |  |
| --- | --- |
| Access Vector (network) | lỗ hổng có thể được tấn công từ xa thông qua mạng, mà không yêu cầu tấn công đối tượng phải có quyền truy cập cục bộ vào hệ thống. |
| Access Complexity (low) | để khai thác lỗ hổng, kẻ tấn công không cần phải thực hiện các thao tác phức tạp hoặc có kiến thức cao về hệ thống. |
| Authentication (none) | không cần xác thực để khai thác lỗ hổng |
| Confidentiality Impact (none) | Không có nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Integrity Impact (none) | nguy cơ thông tin bí mật bị tiết lộ hoặc truy cập không ủy quyền đến các tài nguyên bảo mật. |
| Availability Impact (parital) | lỗ hổng gây ra một mức độ tác động đáng kể đến khả năng sẵn sàng của hệ thống hoặc dịch vụ, nhưng không gây ra sự sụp đổ hoàn toàn. |
| ID CWE | không xác định |

**5.CVE-2000-0790:** Khả năng hiển thị thư mục dựa trên web trong Microsoft Internet Explorer 5.5 trên Windows 98 cho phép người dùng cục bộ chèn các chương trình Trojan horse bằng cách sửa đổi tệp Folder.htt và sử dụng phương pháp InvokeVerb trong điều khiển ShellDefView ActiveX để chỉ định tùy chọn thực thi mặc định cho tệp đầu tiên được liệt kê trong thư mục.

[**https://www.opencve.io/cve/CVE-2000-0790**](https://www.opencve.io/cve/CVE-2000-0790)

|  |  |
| --- | --- |
| Access Vector (local) | lỗ hổng có thể được khai thác bởi một kẻ tấn công cần phải có quyền truy cập cục bộ vào hệ thống |
| Access Complexity (low) | để khai thác lỗ hổng, kẻ tấn công không cần phải thực hiện các thao tác phức tạp hoặc có kiến thức cao về hệ thống. |
| Authentication (none) | không cần xác thực để khai thác lỗ hổng |
| Confidentiality Impact (partial) | lỗ hổng có tác động đến tính bảo mật của thông tin trong hệ thống, nhưng tác động không hoàn toàn làm tiết lộ thông tin. Có thể có một số sự tiết lộ thông tin nhưng không nghiêm trọng. |
| Integrity Impact (partial) | tác động không hoàn toàn làm hỏng dữ liệu hoặc tài nguyên. |
| Availability Impact (parital) | lỗ hổng gây ra một mức độ tác động đáng kể đến khả năng sẵn sàng của hệ thống hoặc dịch vụ, nhưng không gây ra sự sụp đổ hoàn toàn. |
| ID CWE | không xác định |