**Tên: Lê Hải Đăng**

**MSSV: 20110243**

**Lab 2. OS security**

Detect OS, services, and vulnerabilities

Network Topology:

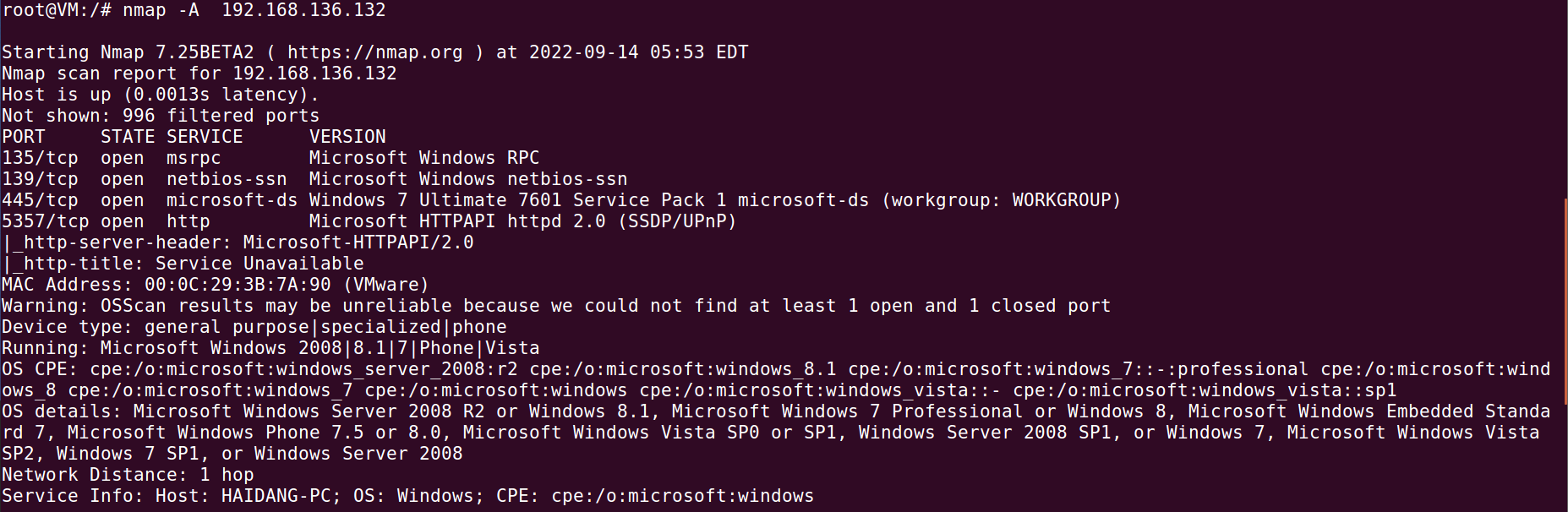


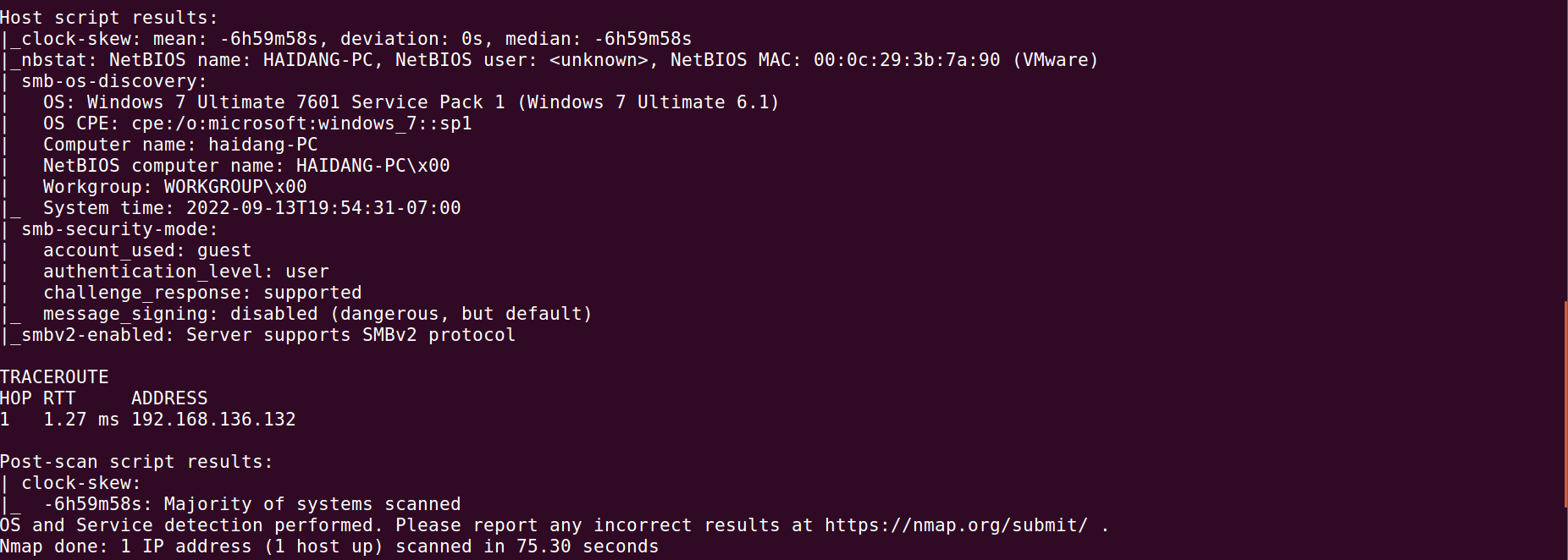
192.168.136.132

Windows 7

1. **Using nmap to scan a machine (via IP address or name) to detect an OS & services**

* Đầu tiên chúng ta phải tắt tường lửa (FireWall) ở máy nạn nhân (Windows 7). Tiếp theo, chúng ta sử dụng lệnh ‘nmap -A *192.168.136.132’* quét máy nạn nhân xem các thông tin như: hệ điều hành là gì, các port được mở, các service…

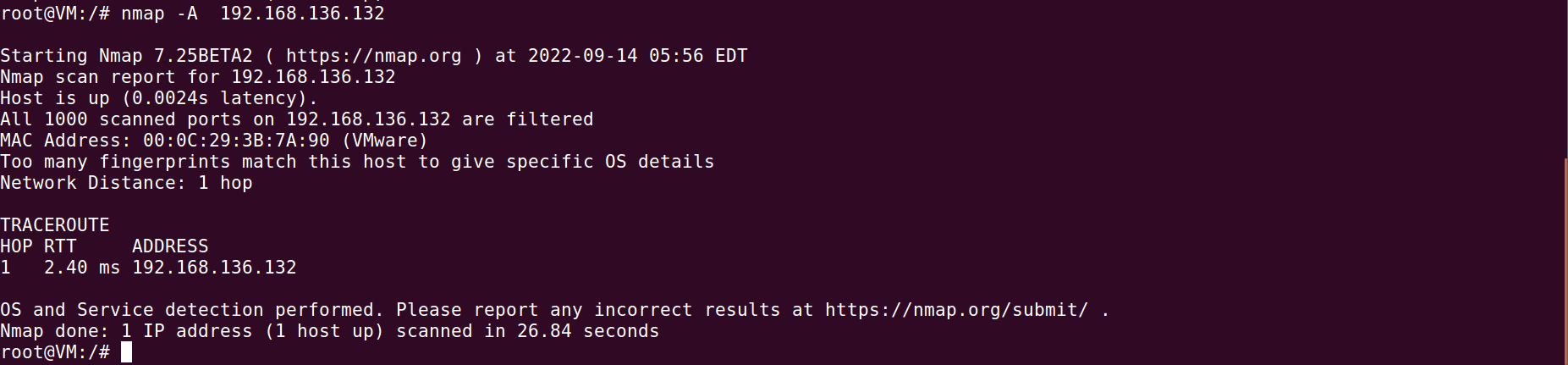
**

Sau khi quét xong chúng ta thấy được một số thông tin quan trọng như:

+ Máy nạn nhân sử dụng Windows 7 Ultimate phiên bản 6.1

+ Các port đang được mở: 135, 139, 445…

+ Các service: msrpc,netbios-ssn, microsoft-ds, http…   
Và quá trình quét mất 75.30 giây.

* Ở đây, chúng ta sẽ thử bật tường lửa để xem sự khác nhau giữa có tương lửa và không có tương lửa khi quét. Chúng ta chạy lại lệnh nmap -A 192.168.136.132

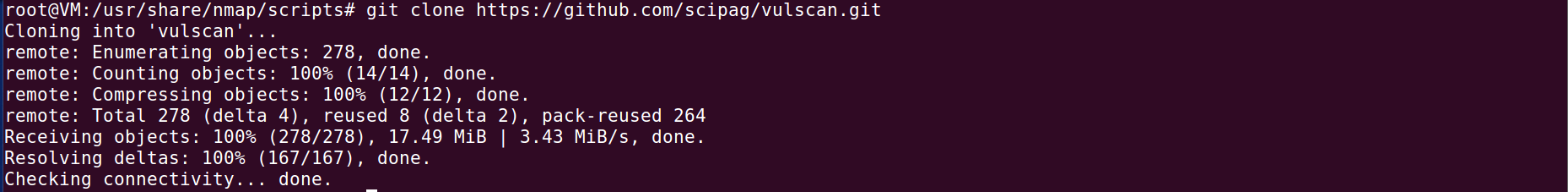
Kết qua ta thấy, những thông tin quan trọng đã không được quét ra, ta chỉ xem được địa chỉ MAC: 00:0C:29:3B:7A:90.

* Vậy ta đã thấy được tường lửa (FireWall) giúp chúng ta bảo vệ hệ thống khỏi các mối đe dạo bảo mật thông qua địa chỉ IP / giao thức khi đồng thời truy cập vào thế giới bên ngoài thông qua mạng diện rộng và Internet.

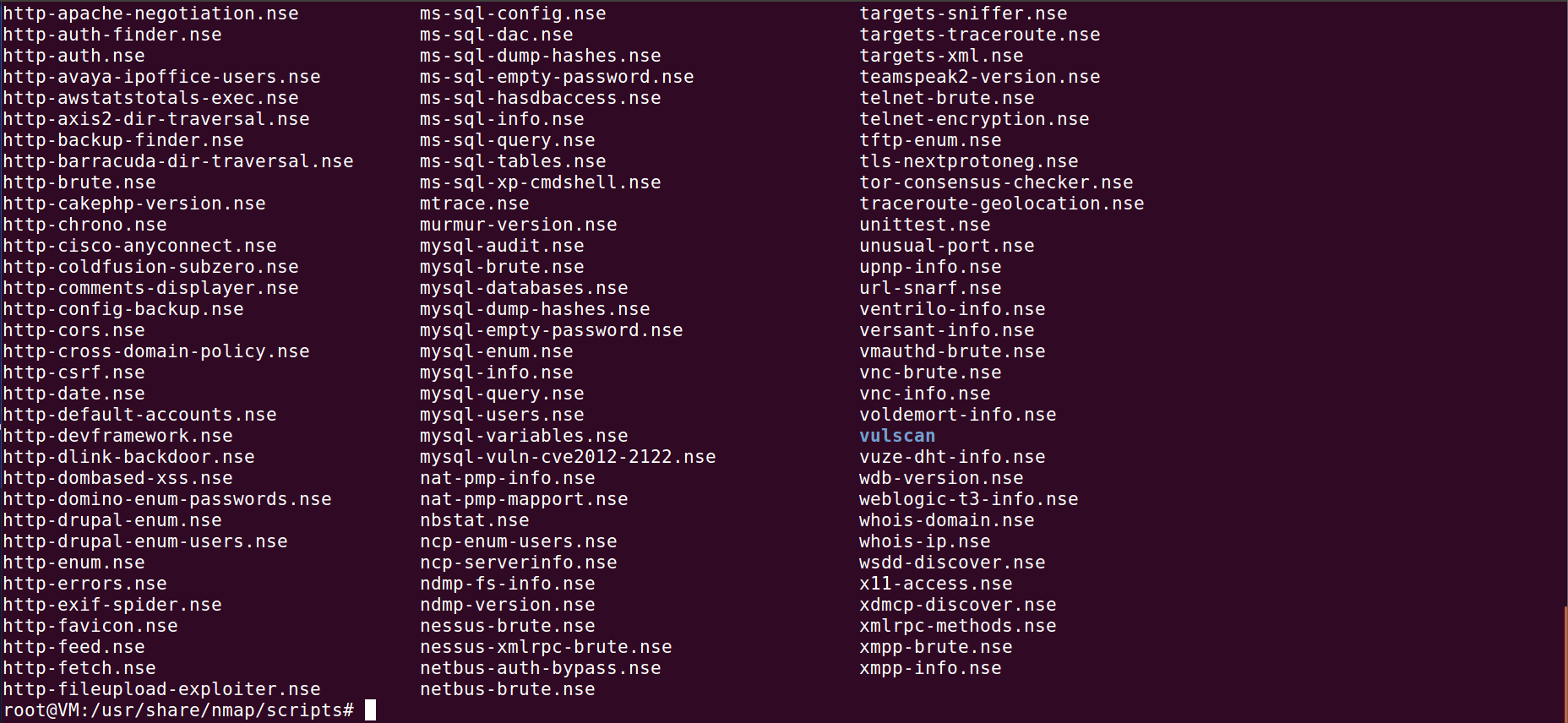
1. **Using nmap with vul-scrip to detect vulnerabilities on an OS**

**Step 1.** Install vul-scrip (to detect detailed vulnerabilities)

+ Di chuyển vào thư mục */usr/share/nmap/scripts* và tiến hành cài đặt vulscan bằng lệnh: ‘*git clone https://github.com/scipag/vulscan.git*’



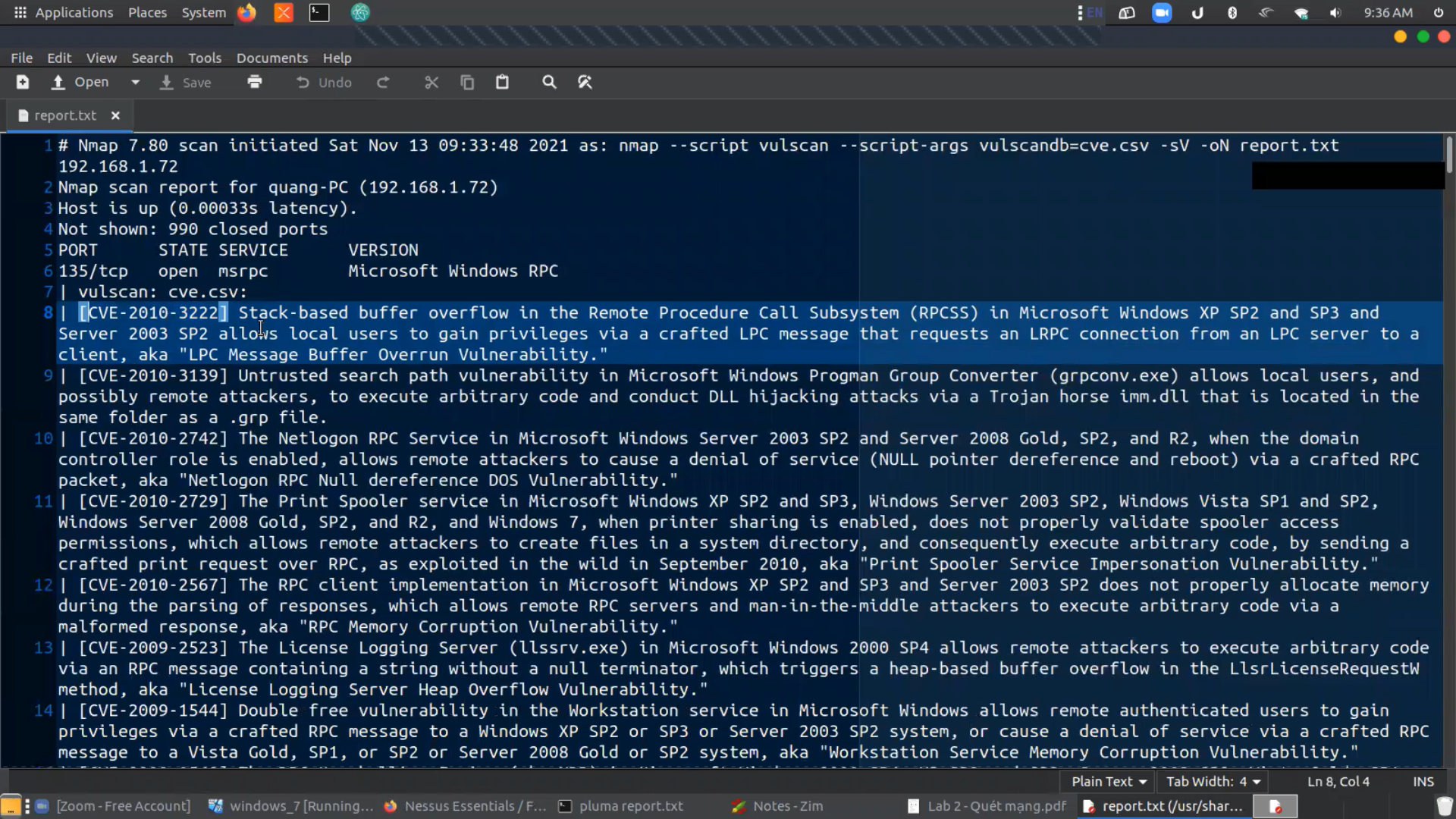
+ Sau khi cài xong chúng ta tiến hành kiểm tra lại xem đã có vulscan chưa bằng cách gõ lệnh: ‘ls’. Sau khi chạy ta đã thấy vulscan.



**Step 2.** Run with the command:

Ở bước này ta sẽ chạy lệnh như bên dưới để quét các lỗ hổng trên máy nạn nhân (192.168.136.132). Phần ‘-oN report.txt’ là để giúp chúng ta dễ xem các lỗ hổng hơn.

nmap –script vulscan –script-args vulscandb=cve.csv -sV 192.168.136.132 -oN report.txt



Giải thích các lỗ hổng có mã CVE:

1. CVE-2010-3222: Tràn bộ đệm dựa trên ngăn xếp trong Hệ thống con Cuộc gọi Thủ tục Từ xa (RPCSS) trong Microsoft Windows XP SP2 và SP3 và Server 2003 SP2 cho phép người dùng cục bộ có được đặc quyền thông qua thông báo LPC được tạo thủ công yêu cầu kết nối LRPC từ máy chủ LPC tới máy khách, hay còn gọi là "Lỗ hổng tràn bộ đệm thư LPC."

|  |  |
| --- | --- |
| CVSS Score | 7.2 |
| Confidentiality Impact | Complete (Có toàn bộ thông tin tiết lộ, dẫn đến tất cả các tệp hệ thống bị tiết lộ.) |
| Integrity Impact | Complete (Có một sự xâm phạm hoàn toàn về tính toàn vẹn của hệ thống. Mất hoàn toàn khả năng bảo vệ hệ thống, dẫn đến toàn bộ hệ thống bị xâm phạm.) |
| Availability Impact | Complete (Tài nguyên bị ảnh hưởng đã tắt hoàn toàn. Kẻ tấn công có thể làm cho tài nguyên hoàn toàn không khả dụng.) |
| Access Complexity | Low (Điều kiện tiếp cận chuyên biệt hoặc các tình tiết giảm nhẹ không tồn tại. Cần rất ít kiến ​​thức hoặc kỹ năng để khai thác.) |
| Authentication | Not required (Không cần xác thực để khai thác lỗ hổng.) |
| Gained Access | None |
| Vulnerability Type(s) | OverflowGain privileges |
| CWE ID | 119 |

1. CVE-2010-3139: Lỗ hổng đường dẫn tìm kiếm không đáng tin cậy trong Microsoft Windows Progman Group Converter (grpconv.exe) cho phép người dùng cục bộ và có thể cả những kẻ tấn công từ xa, thực thi mã tùy ý và tiến hành các cuộc tấn công chiếm quyền điều khiển DLL thông qua một con ngựa Trojan, Imm.dll nằm trong cùng thư mục với a. tệp grp.

|  |  |
| --- | --- |
| CVSS Score | 9.3 |
| Confidentiality Impact | Complete (Có toàn bộ thông tin tiết lộ, dẫn đến tất cả các tệp hệ thống bị tiết lộ.) |
| Integrity Impact | Complete (Có một sự xâm phạm hoàn toàn về tính toàn vẹn của hệ thống. Mất hoàn toàn khả năng bảo vệ hệ thống, dẫn đến toàn bộ hệ thống bị xâm phạm.) |
| Availability Impact | Complete (Tài nguyên bị ảnh hưởng đã tắt hoàn toàn. Kẻ tấn công có thể làm cho tài nguyên hoàn toàn không khả dụng.) |
| Access Complexity | Medium (Các điều kiện truy cập hơi chuyên biệt. Một số điều kiện tiên quyết phải được thỏa mãn để khai thác). |
| Authentication | Not required (Không cần xác thực để khai thác lỗ hổng.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code |
| CWE ID | Id CWE không được xác định cho lỗ hổng này |

1. CVE-2010-2742: 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 kích hoạt, cho phép kẻ tấn công từ xa gây ra từ chối dịch vụ (tham khảo con trỏ NULL và khởi động lại) thông qua gói RPC được chế tạo, hay còn gọi là "Lỗ hổng bảo mật DOS Null dereference của Netlogon."

|  |  |
| --- | --- |
| CVSS Score | 5.4 |
| Confidentiality Impact | None (Không có ảnh hưởng đến tính bảo mật của hệ thống.) |
| Integrity Impact | None (Không có tác động đến tính toàn vẹn của hệ thống) |
| Availability Impact | Complete (Tài nguyên bị ảnh hưởng đã bị tắt hoàn toàn. Kẻ tấn công có thể khiến tài nguyên hoàn toàn không khả dụng.) |
| Access Complexity | High (Có các điều kiện truy cập chuyên biệt. Khó khai thác và phải thỏa mãn một số điều kiện đặc biệt để khai thác) |
| Authentication | Not required (Không cần xác thực để khai thác lỗ hổng.) |
| Gained Access | None |
| Vulnerability Type(s) | Denial Of Service |
| CWE ID | Id CWE không được xác định cho lỗ hổng này |

1. CVE-2010-2729: Dịch vụ Bộ đệm in trong Microsoft Windows XP SP2 và SP3, Windows Server 2003 SP2, Windows Vista SP1 và SP2, Windows Server 2008 Gold, SP2 và R2 và Windows 7, khi chia sẻ máy in được bật, không xác thực đúng quyền truy cập bộ đệm , cho phép những kẻ tấn công từ xa tạo tệp trong thư mục hệ thống và do đó thực thi mã tùy ý, bằng cách gửi yêu cầu in thủ công qua RPC, như được khai thác trong tự nhiên vào tháng 9 năm 2010, còn gọi là "Lỗ hổng mạo danh dịch vụ bộ đệm in".

|  |  |
| --- | --- |
| CVSS Score | 9.3 |
| Confidentiality Impact | Complete (Có toàn bộ thông tin tiết lộ, dẫn đến tất cả các tệp hệ thống bị tiết lộ.) |
| Integrity Impact | Complete (Có một sự xâm phạm hoàn toàn về tính toàn vẹn của hệ thống. Mất hoàn toàn khả năng bảo vệ hệ thống, dẫn đến toàn bộ hệ thống bị xâm phạm.) |
| Availability Impact | Complete (Tài nguyên bị ảnh hưởng đã bị tắt hoàn toàn. Kẻ tấn công có thể khiến tài nguyên hoàn toàn không khả dụng.) |
| Access Complexity | Medium (Các điều kiện truy cập hơi chuyên biệt. Một số điều kiện tiên quyết phải được thỏa mãn để khai thác). |
| Authentication | Not required (Không cần xác thực để khai thác lỗ hổng.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code |
| CWE ID | 20 |

1. CVE-2010-2567: Việc triển khai máy khách RPC trong Microsoft Windows XP SP2 và SP3 và Server 2003 SP2 không phân bổ bộ nhớ đúng cách trong quá trình phân tích cú pháp các phản hồi, điều này cho phép các máy chủ RPC từ xa và những kẻ tấn công trung gian thực thi mã tùy ý thông qua một phản hồi không đúng định dạng, hay còn gọi là "Lỗ hổng bảo mật do hỏng bộ nhớ RPC."

|  |  |
| --- | --- |
| CVSS Score | 9.3 |
| Confidentiality Impact | Complete (Có toàn bộ thông tin tiết lộ, dẫn đến tất cả các tệp hệ thống bị tiết lộ.) |
| Integrity Impact | Complete (Có một sự xâm phạm hoàn toàn về tính toàn vẹn của hệ thống. Mất hoàn toàn khả năng bảo vệ hệ thống, dẫn đến toàn bộ hệ thống bị xâm phạm.) |
| Availability Impact | Complete (Tài nguyên bị ảnh hưởng đã bị tắt hoàn toàn. Kẻ tấn công có thể khiến tài nguyên hoàn toàn không khả dụng.) |
| Access Complexity | Medium (Các điều kiện truy cập hơi chuyên biệt. Một số điều kiện tiên quyết phải được thỏa mãn để khai thác). |
| Authentication | Not required (Không cần xác thực để khai thác lỗ hổng.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code Memory corruption |
| CWE ID | 94 |