**Võ Văn Đức 20110635**

**Lab 2. OS security**

Detect OS, services, and vulnerabilities

**Submission:**

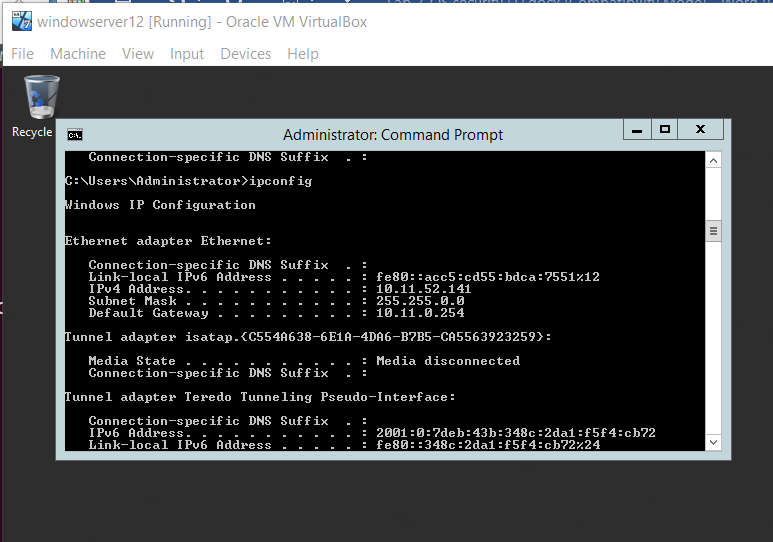
You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations. Simply attaching code without any explanation will not receive credits

**Time duration:** 1 week

Lab guide:

Network Topology:





Window Server 12 có địa chỉ là 10.11.52.141, là máy bị tấn công

Ubuntu là máy tấn công.

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

* Students can use some commands:

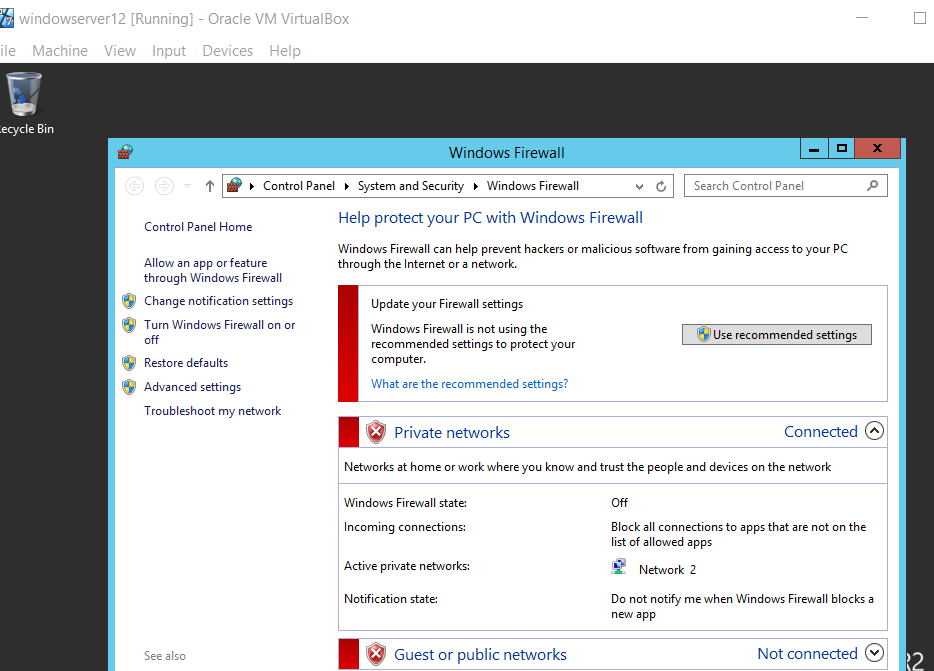
$ sudo nmap –F *<network> //replace <Network> with 192.168.12.0/24*

$ sudo nmap –O *<IP-target> //replace <IP-target> with 192.168.12.254*

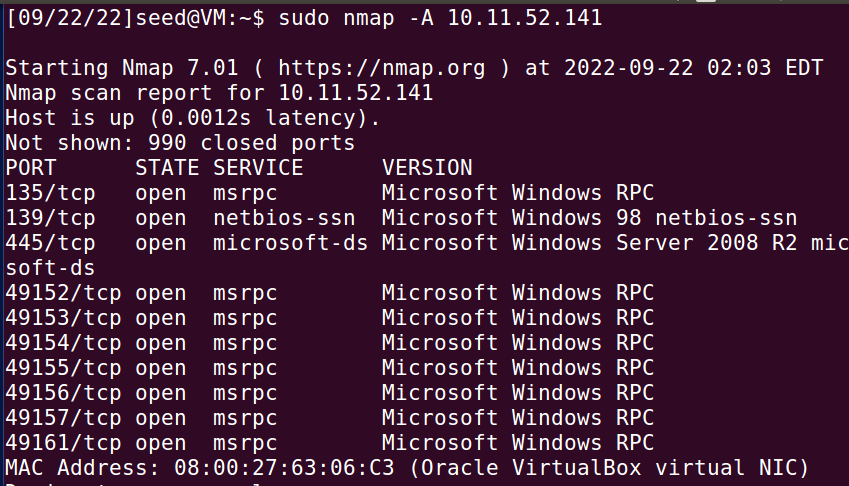
$ sudo nmap –A *<IP-target>*

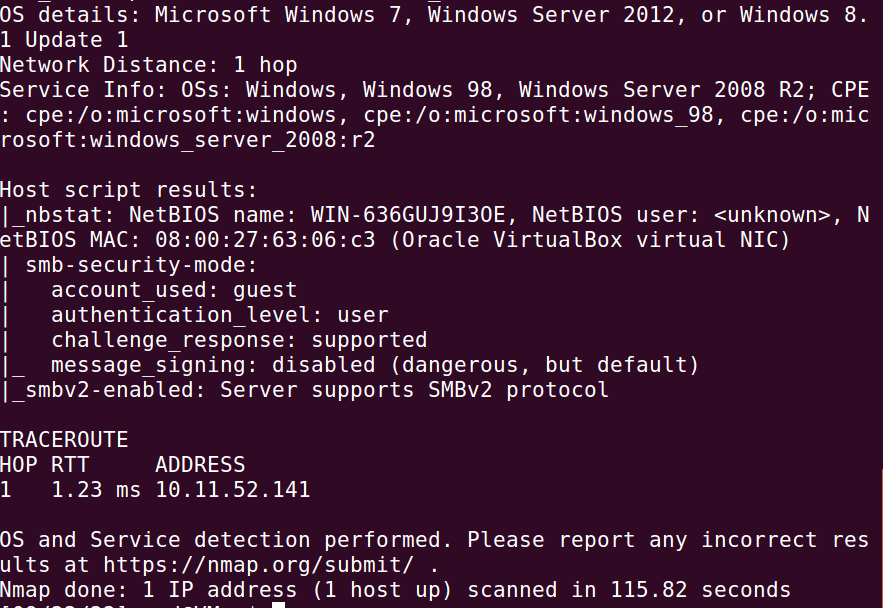
$ sudo nmap –sV *<IP-target>*

* Find the differences when using these commands with:
* Turn off the firewall on the target machine (192.168.12.254)



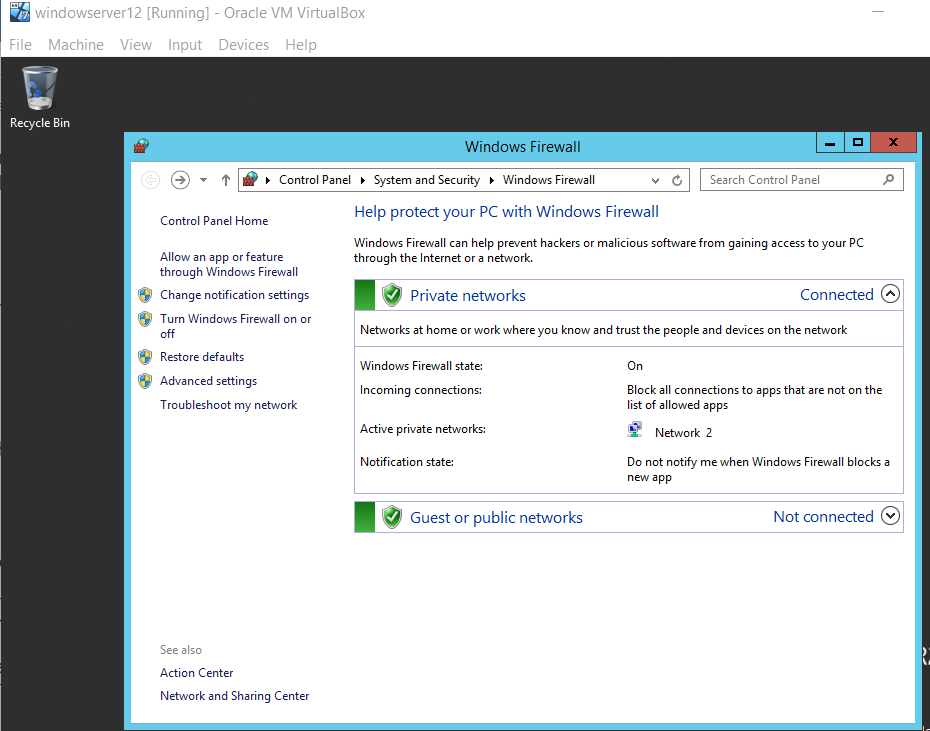
Tiến hành quét dịch vụ và những thông tin khác mà window server đang sử dụng từ ubuntu

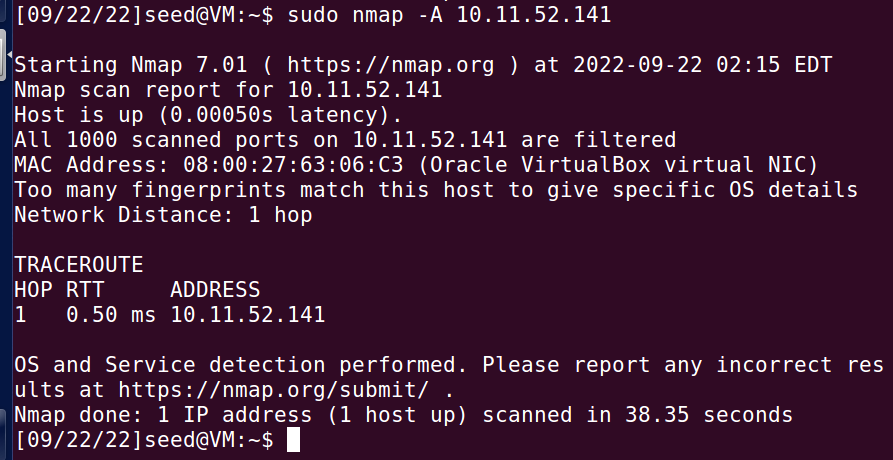
* 



Thông tin về hệ điều hành của window server, thời gian quét của Ubuntu

* Turn on the firewall on the target machine





Sau khi bật tưởng lửa của máy bị tấn công, thì máy tấn công không thể quét được thông tin gì từ máy bị tấn công. => Tường lửa giống chống tấn công từ bên ngoài.

* Students use some other options of the nmap to detect the target.

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

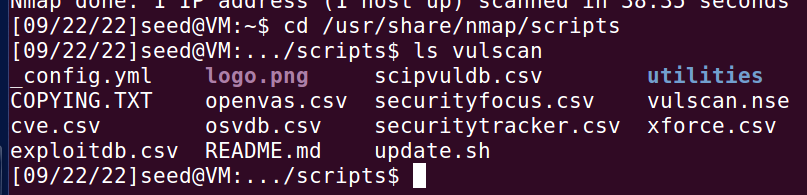
**Step 1.** Install vul-scrip (to detect detailed vulnerabilities)

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

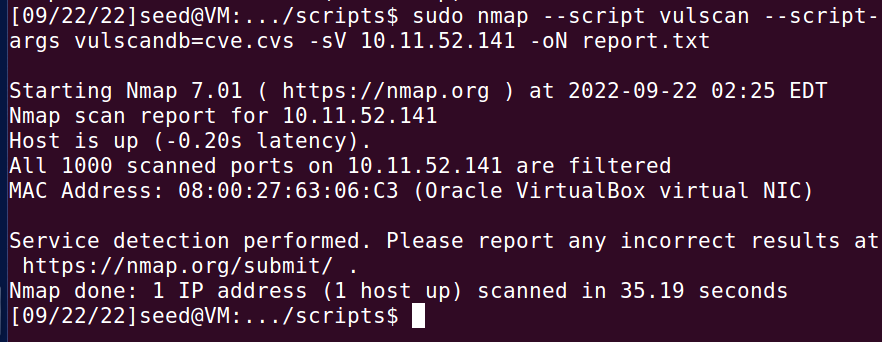
$sudo ln -s `pwd`/scipag\_vulscan /usr/share/nmap/scripts/vulscan

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

nmap -sV --script=vulscan/vulscan.nse *<IP-target>*



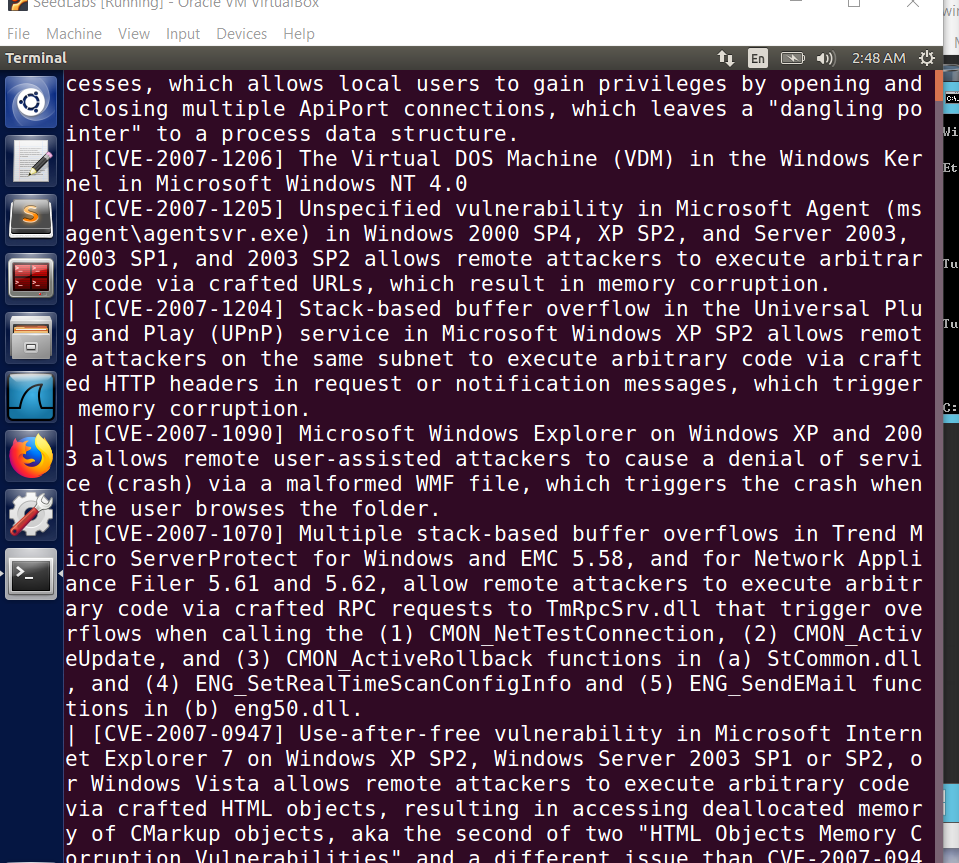
Tìm được vị trí file cve.csv ở trong vulscan

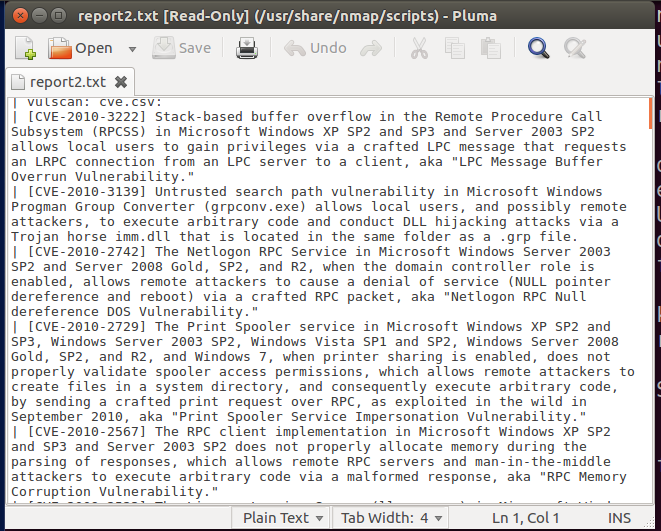


Quét các lỗ hổng CVE và ghi vào file report.txt



* Mở file report.txt và lấy 5 lổ hổng CVE để tìm hiểu và giải thích





Chọn: CVE-2010-3222; CVE-2010-3139; CVE-2010-2742; CVE-2010-2729; CVE-2010-2567

CVE-2010-3222:

Tràn bộ đệm dựa trên stack trong the Remote Procedure Call Subsystem (RPCSS) trong Microsoft Windows XP SP2 và SP3 và Server 2003 SP2 cho phép người dùng cục bộ có được đặc quyền thông qua LPC message được tạo thủ công mà yêu cầu kết nối LRPC từ máy chủ LPC tới máy khách, hay còn gọi là “LPL Message Buffer Overrun Vulnerability."

CVSS Score 7.2

Confidentiality Impact: Complete ( 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 (the affected resource đã tắt hoàn toàn. Kẻ tấn công có thể làm cho tài nguyên hoàn toàn không khả dụng.)

Access Complexity: Low (Không có các điều kiện tiếp cận chuyên biệt. 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

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 a Trojan horse Imm.dll nằm trong cùng thư mục với a.grp.

CVSS Score 9.3

Confidentiality Impact: Complete ( 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 (the affected resource đã tắt hoàn toàn. Kẻ tấn công có thể làm cho tài nguyên hoàn toàn không khả dụng.)

Access Complexity: Medium (Điều kiện truy cập hơi đặc biệt, một số điều kiện tiên quyết khi truy cập phải được thoã mãn.)

Authentication: Not required (Không cần xác thực để khai thác lỗ hổng.)

Gained Access: None

CVE-2010-2742:

Dịch vụ Netlogon RPC trong Microsoft Windows Server 2003 SP2 và Server 2008 Gold, SP2 và R2, khi vai trò domain controller được kích hoạt, cho phép kẻ tấn công từ xa gây ra từ chối dịch vụ thông qua gói RP, 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 (the affected resource đã tắt hoàn toàn. Kẻ tấn công có thể làm cho tài nguyên hoàn toàn không khả dụng.)

Access Complexity: High (Điều kiện truy cập chuyên biệt đối với từng trường hợp tồn tại. 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

CVE-2010-2729:

Dịch vụ Print Spooler 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 printer sharing 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 "Print Spooler Service Impersonation Vulberability".

CVSS Score 9.3

Confidentiality Impact: Complete ( Không có ảnh hưởng đến tính bảo mật của hệ thống.)

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 (the affected resource đã ngừng hoạt động hoàn toàn. Kẻ tấn công có thể làm cho tài nguyên hoàn toàn không khả dụng.)

Access Complexity: Medium (Điều kiện truy cập hơi đặc biệt, một số điều kiện tiên quyết khi truy cập phải được thoã mãn.)

Authentication: Not required (Không cần xác thực để khai thác lỗ hổng.)

Gained Access: None

CVE-2010-2567:

Việc thực thi the RPC client in Microsoft Windows XP SP2 và SP3 và Server 2003 SP2 sẽ không phân bổ bộ nhớ một cách phù hợp 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 ( Không có ảnh hưởng đến tính bảo mật của hệ thống.)

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 (the affected resource đã ngừng hoạt động hoàn toàn. Kẻ tấn công có thể làm cho tài nguyên hoàn toàn không khả dụng.)

Access Complexity: Medium (Điều kiện truy cập hơi đặc biệt, một số điều kiện tiên quyết khi truy cập phải được thoã mãn.)

Authentication: Not required (Không cần xác thực để khai thác lỗ hổng.)

Gained Access: None

**Note:** see the website for more details: <https://securitytrails.com/blog/nmap-vulnerability-scan>

Sv chọn khoảng 5 lỗ hổng có mã CVE, tìm hiểu và giải thích lỗ hổng đó, ghi trong báo cáo.