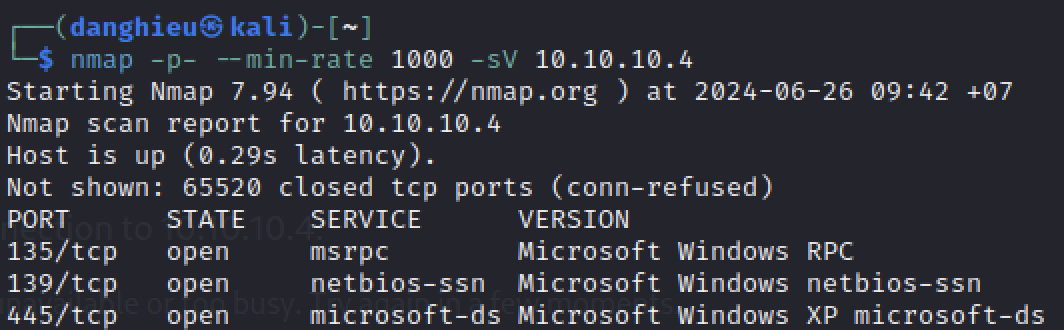
**Legacy**



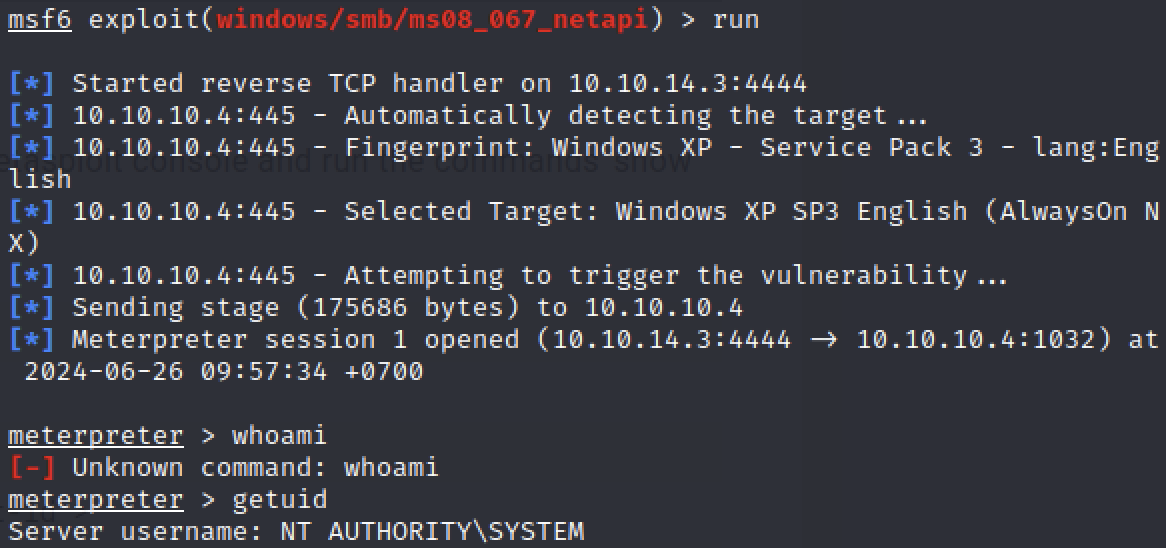
Máy chủ đang dùng 1 hệ điều hành rất cũ nên có nhiều khai thác có sẵn.

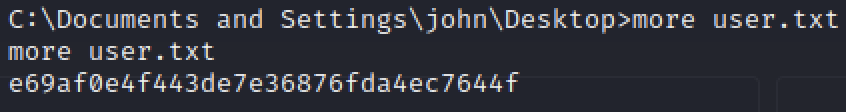
Mình tìm thấy 1 CVE có thể thực thi mã từ xa: MS08-067

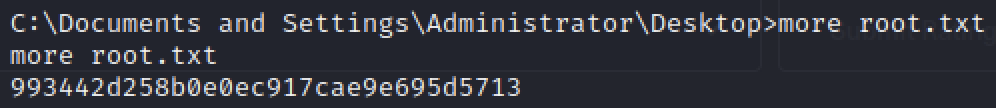
msf > use exploit/windows/smb/ms08\_067\_netapi

msf exploit(ms08\_067\_netapi) > show options

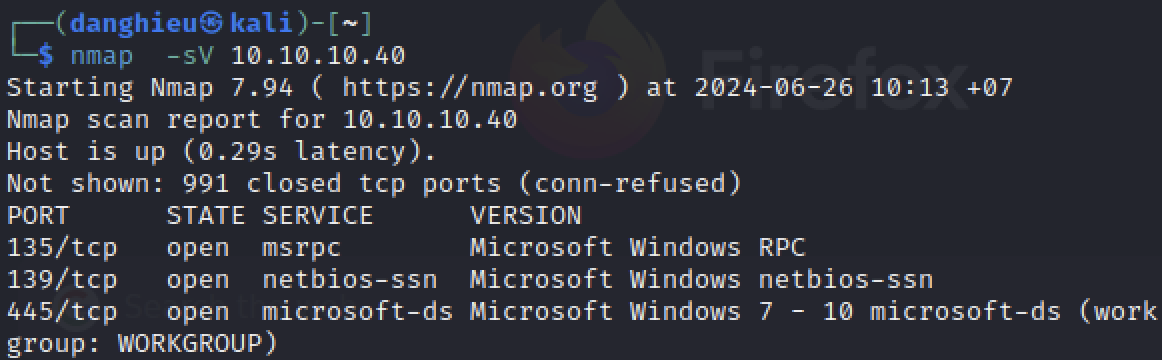
msf exploit(ms08\_067\_netapi) > exploit

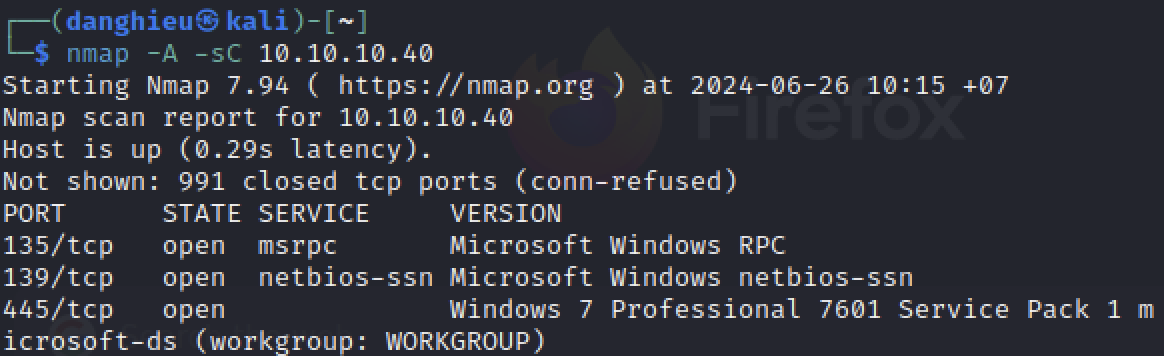






**Blue**



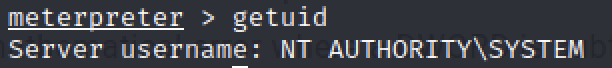


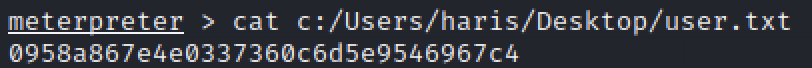
🡺 Bạn thấy là nmap -A quét kĩ hơn -sV

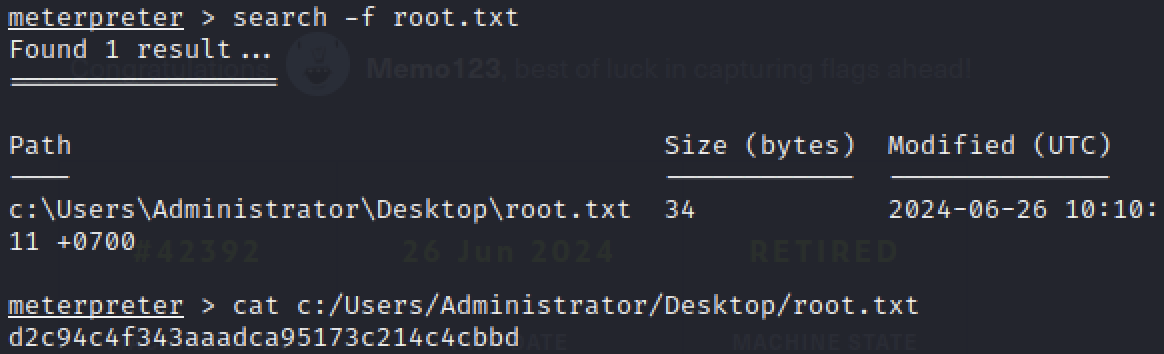
Máy chủ đang dùng 1 hệ điều hành khá cũ nên có nhiều khai thác có sẵn.

Mình tìm thấy 1 CVE: MS17-010 EternalBlue

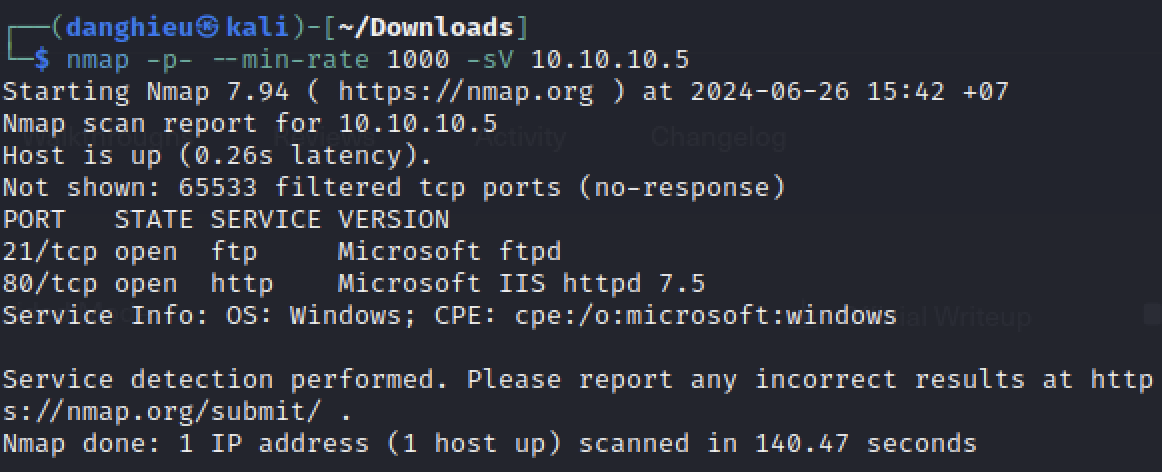


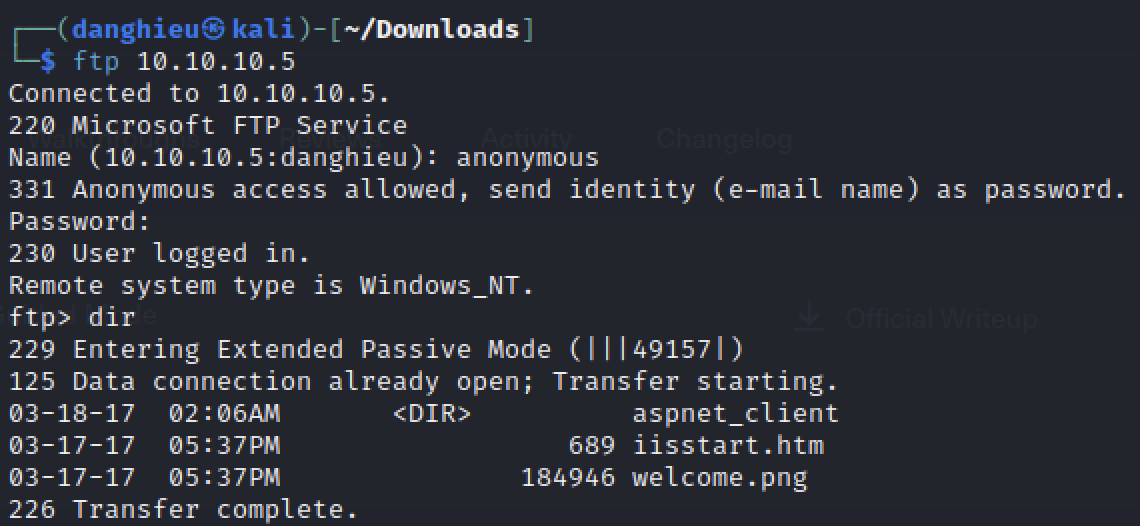






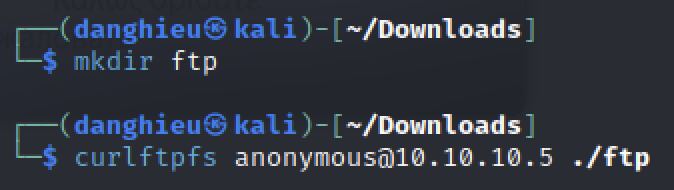
**Devel**



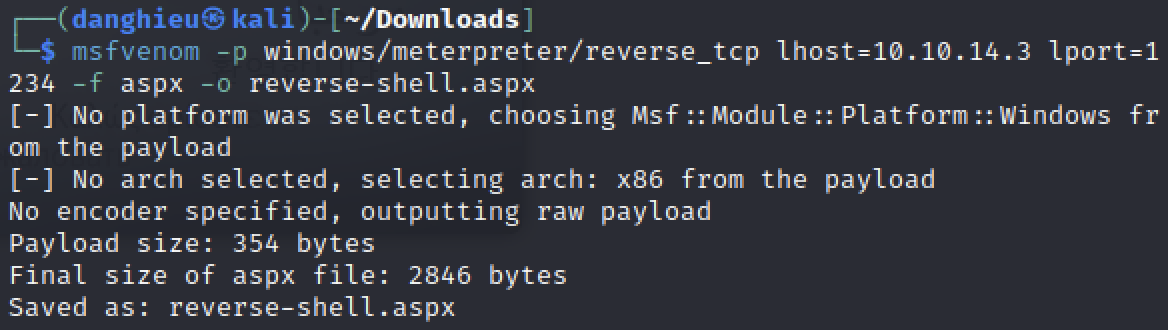


Thư mục lưu trữ tập tin trong ftp giống với web root.

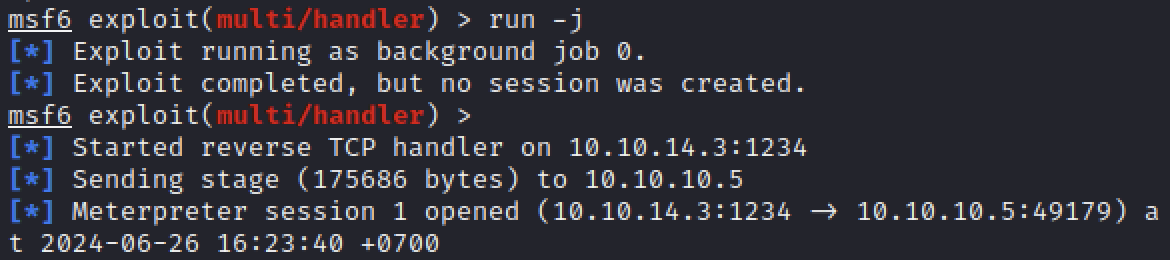
Mình sẽ mount share bằng curlftpfs và upload reverse-shell.

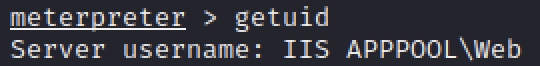


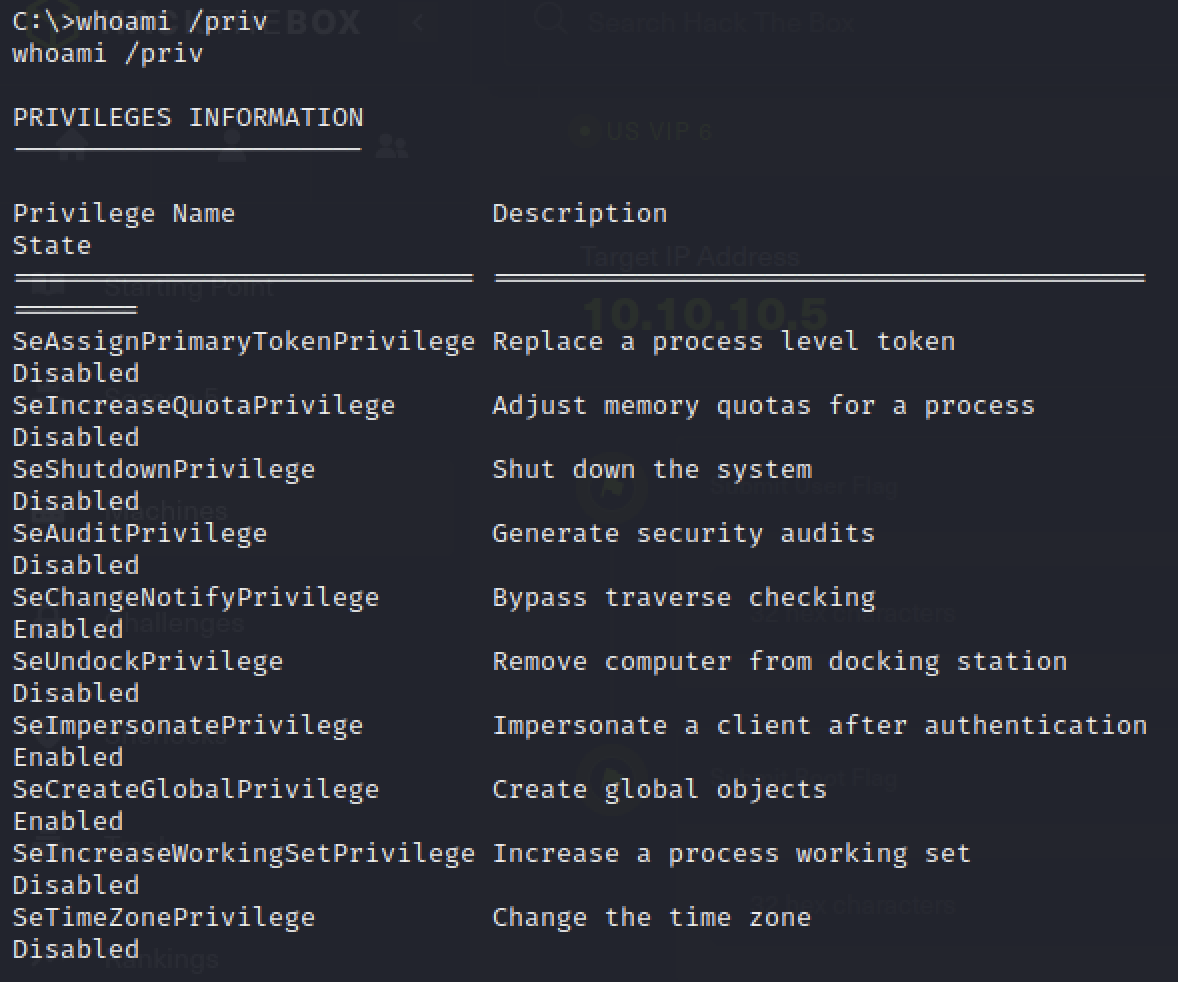
Trang web chạy bằng ngôn ngữ aspx nên mình tạo reverse-shell.aspx

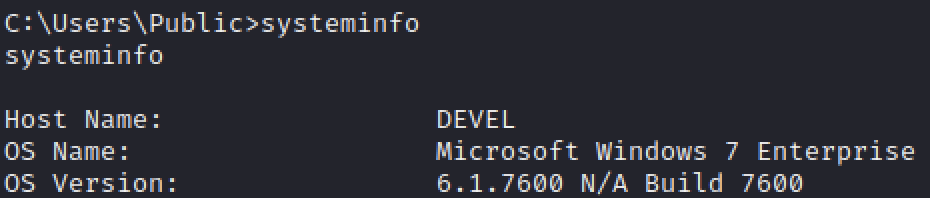


Di chuyển reverse-shell.aspx vào thư mục ftp, chạy tệp thực thi:









Mình thấy máy chủ là Windows 7 x86, có đặc quyền SeImpersonate rất thích hợp để tấn công JuicyPotato. Nhưng khai thác như vậy rất mất thời gian, mình nên quét xem máy chủ còn dính lỗ hổng gì không.

Tiện đang có meterpreter shell, mình chạy Local\_Exploit\_Suggester, cho chúng ta các module leo thang đặc quyền:

* exploit/windows/local/bypassuac\_eventvwr
* exploit/windows/local/ms10\_015\_kitrap0d

Nếu ta leo thang đặc quyền bằng module bypassuac\_eventvwr sẽ thất bại vì bạn không nằm trong nhóm Administrator. Khai thác ms10\_015 sẽ làm nên điều khác biệt:

