1. Try running a VHost fuzzing scan on 'academy.htb', and see what other VHosts you get. What other VHosts did you get?

Thêm tên miền academy.htb vào /etc/hosts



Quét các tên miền phụ

```bash

ffuf -w /root/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u http://academy.htb:49864 -H "Host: FUZZ.academy.htb"

```

Kết quả trả vềA screenshot of a computer

Description automatically generated

Ta nhận được rất nhiều đầu ra không cần thiết, talọc đầu ra bằng cách sử dụng tùy chọn -fs để lọc kích thước của các phản hồi được trả về: -fs 985 trong trường hợp này, chạy theo lệnh sẽ giúp chỉ nhận được những phản hồi nằm ngoài kích thước 985 này, nghĩa là hiện tại chúng tôi có vhost cho miền Academy.htb:

```bash

ffuf -w /root/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u http://academy.htb:49864 -H "Host: FUZZ.academy.htb" -fs 986

```

A screenshot of a computer

Description automatically generated

Ta tìm được 2 miền phụ admin.academy.htb và test.academy.htb

P/s:test.academy.htb

Thêm 2 tên miền phụ vào /etc/hosts

