Recon 00: đọc file robots.txt

Recon 01: trang lỗi 404 có thể rò rỉ thông tin về công nghệ web được dùng bởi công ty hoặc ứng dụng. Nó cũng cho phép bạn xác định các tập tin tồn tại khi bạn bắt đầu bruteforce thư mục.

Recon 02: tập tin security.txt ở /.well-known/security.txt

Recon 03: Đọc source HTML để xem các thư mục lưu trữ tập tin

Một số thư mục bị lỗi index do cấu hình sai

Recon 04: Trước khi dùng tool để bruteforce thư mục bị ẩn, kiểm tra trước các thư mục phổ biến như /admin

Recon 05: ffuf -w directory-list-1.0.txt -u https://hackycorp.com/FUZZ -c

Recon 06,07: virtual host

Recon 08: Khi truy cập máy chủ TLS, nó thường kiểm tra nội dung của chứng chỉ. Chứng chỉ này dùng cho nhiều tên miền. Bạn có thể khám phá thêm được subdomain

https://crt.sh

Recon 09: Điều tra header để tìm thêm thông tin về phiên bản và công nghệ sử dụng

Recon 11: Brute force virtual host

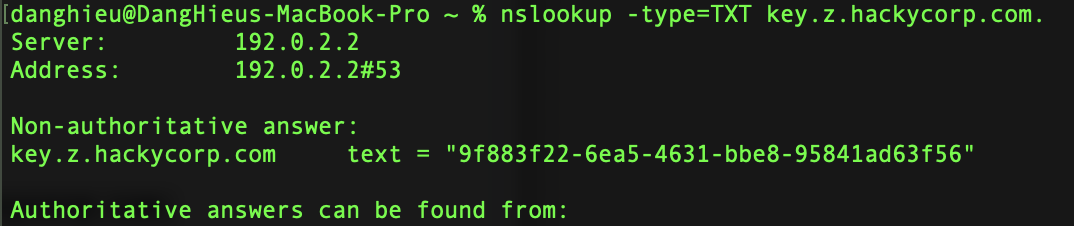
ffuf -u https://hackycorp.com -c -w ./Wordlists/subdomains-top1million-5000.txt -H 'Host:FUZZ.hackycorp.com' -fs 107

Recon 12: Load Balancer

Yêu cầu được gửi đi 1 ứng dụng có thể thực hiện bởi nhiều hệ thống backend. Bạn có thể gửi cùng 1 yêu cầu nhiều lần để kiểm tra xem có nhiều hệ thống backend không

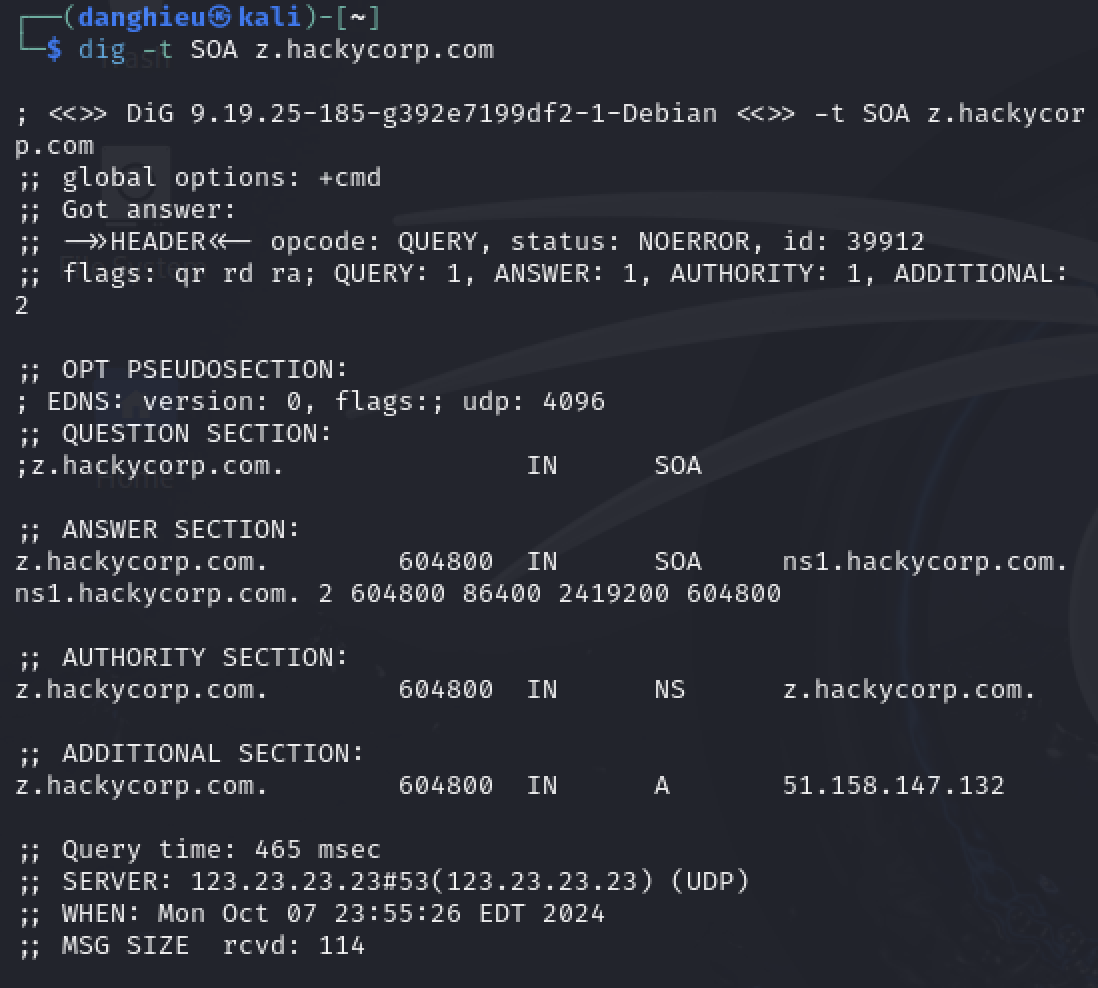
Recon 13:

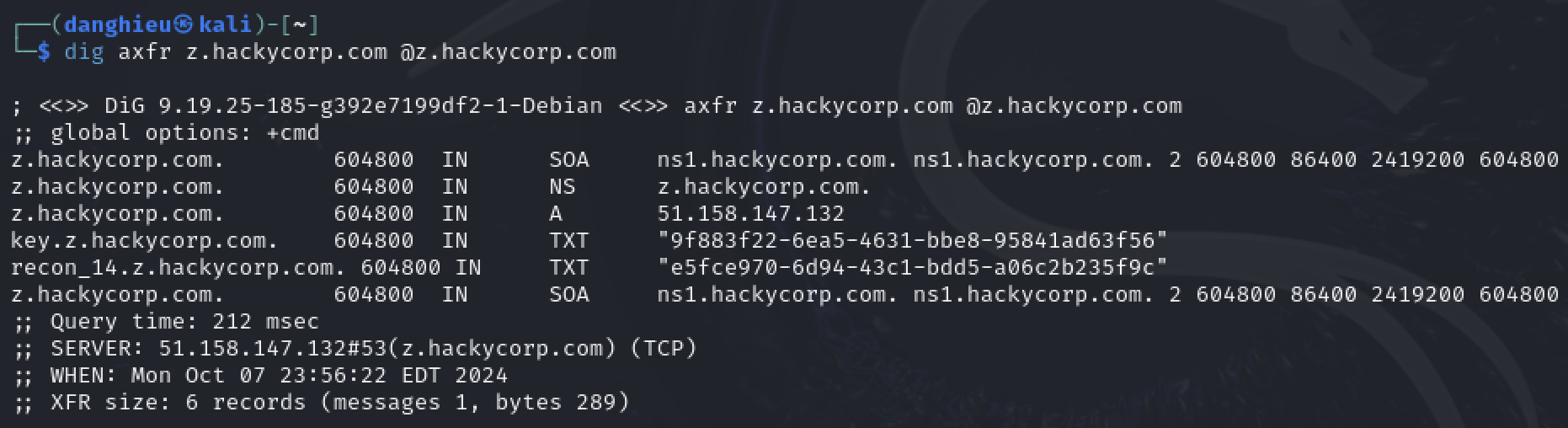
Bản ghi TXT thường hiển thị người sở hữu tên miền hoặc để lưu trữ thông tin cấu hình dịch vụ



Recon 14: Zone Transfer

Zone Transger thường dùng để đồng bộ hóa nhiều máy chủ DNS. Chỉ có danh sách các máy chủ được xác định trước mới có thể thực hiện thao tác này. Đôi khi truy suất thông tin này cho bạn quyền truy cập vào máy chủ mới



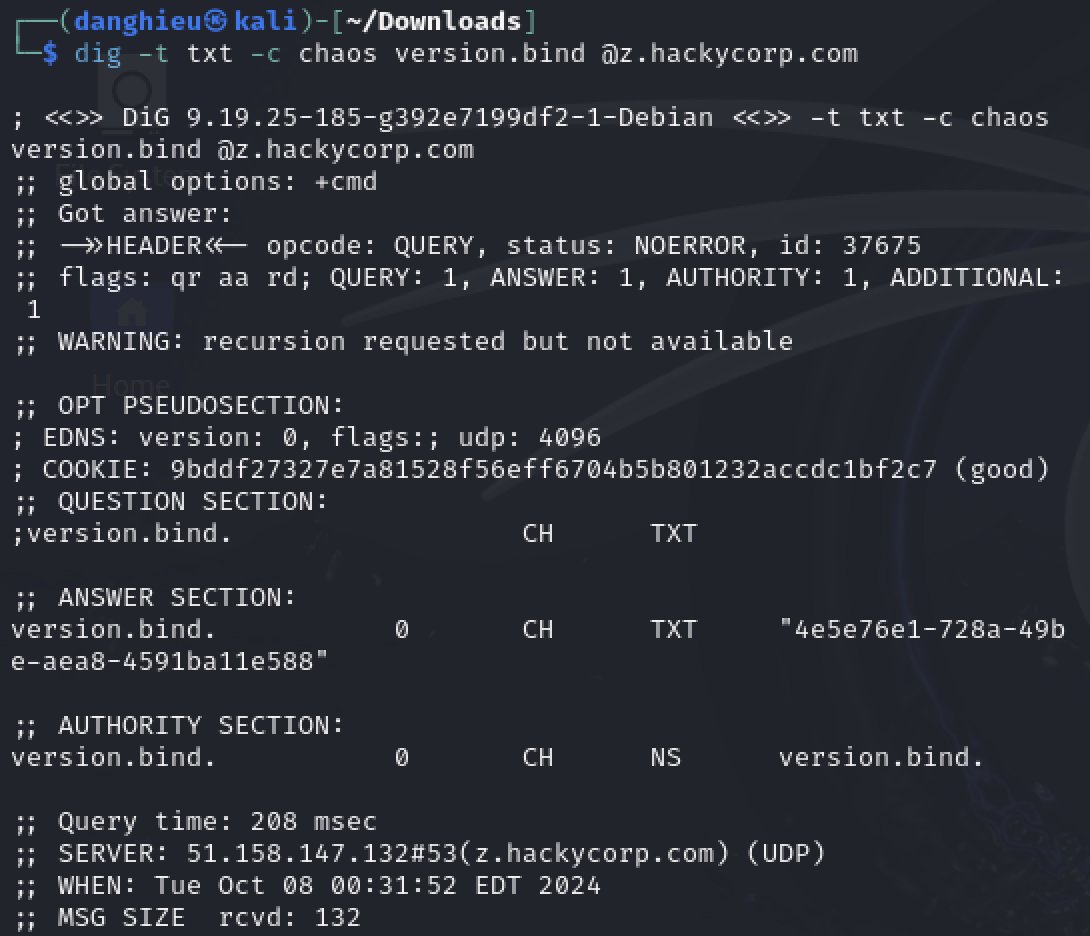


Recon 15

Recon 16:

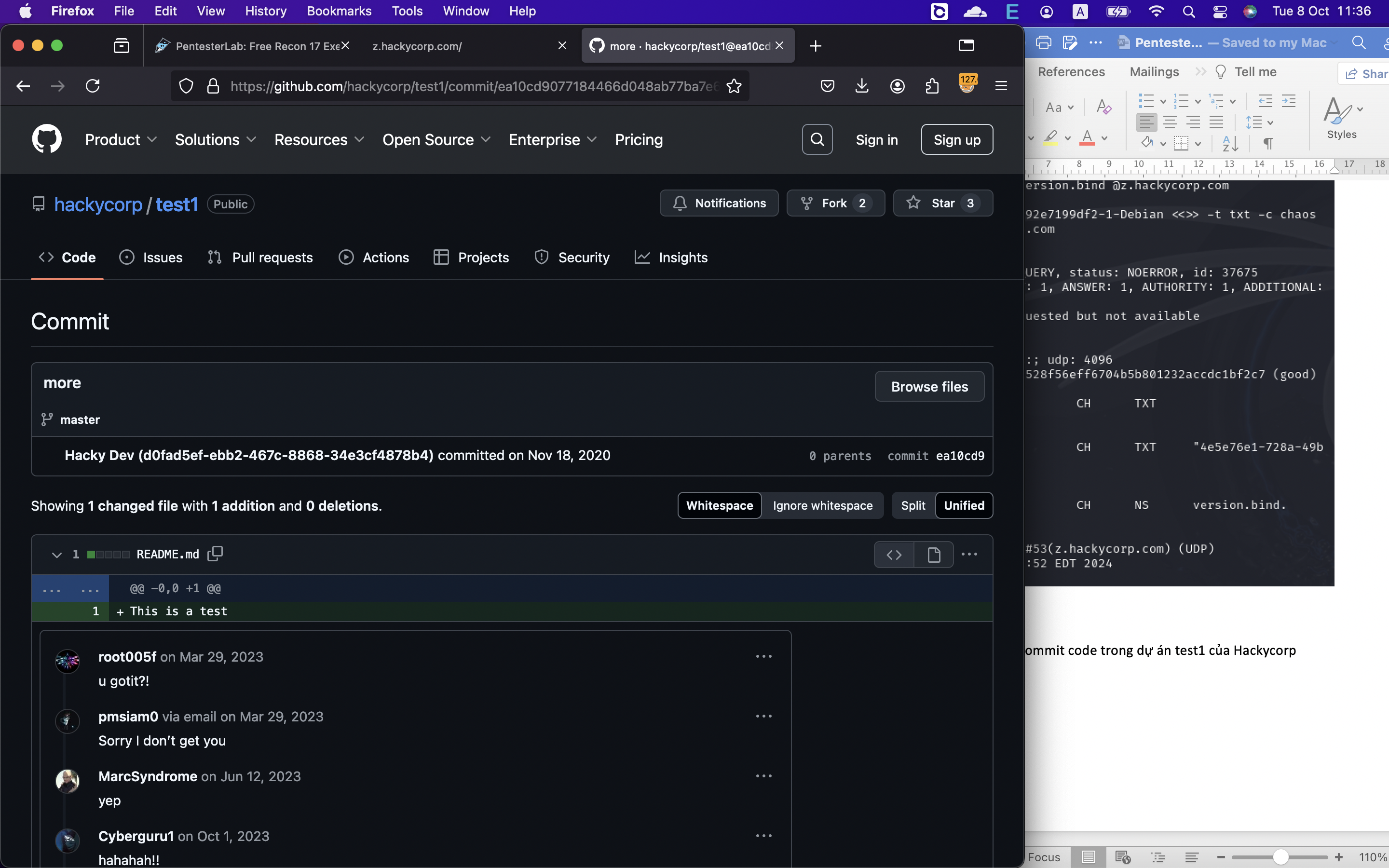
Bind là 1 trong những máy chủ DNS được sử dụng phổ biến nhất.

Lấy được phiên bản của bind do z.hackycorp.com sử dụng



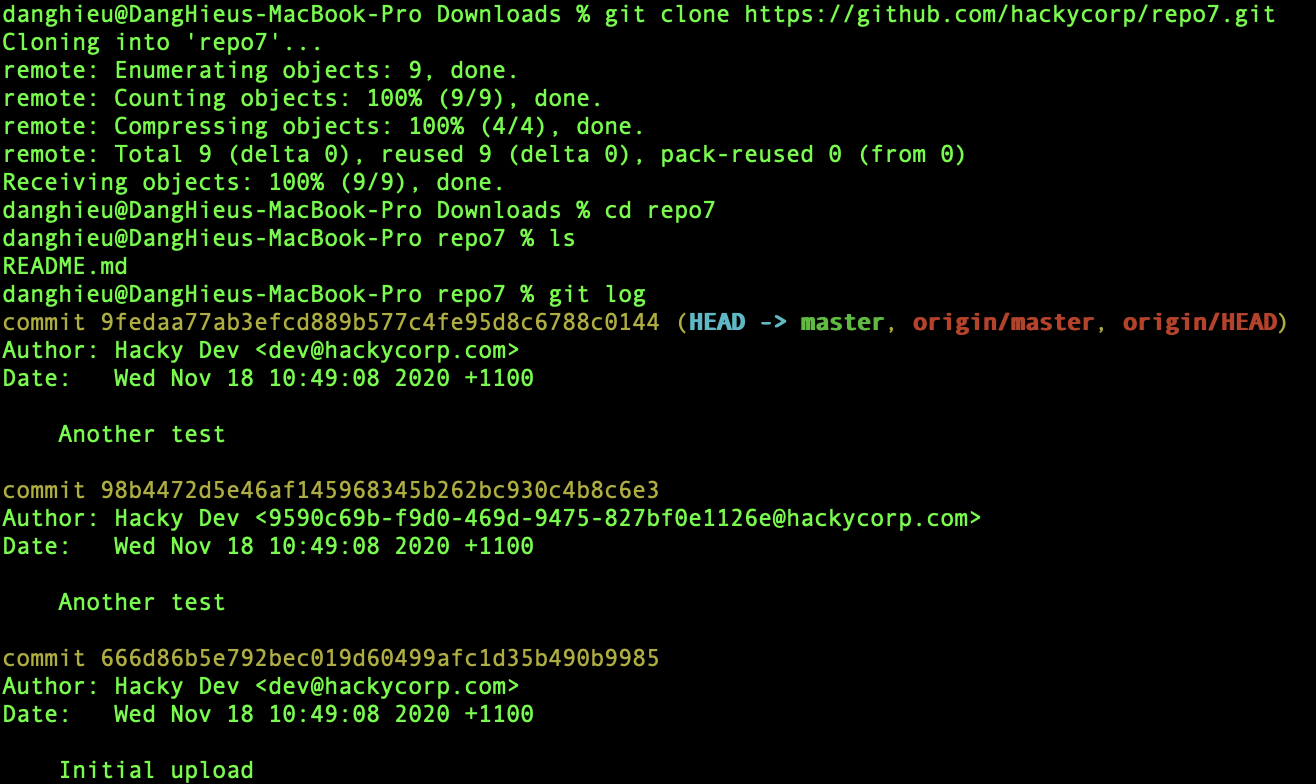
Recon 17:

Xem tên của lập trình viên đã commit code trong dự án test1 của Hackycorp



Recon 19:

Xem địa chỉ email của các commit trong kho chứa repo 7



Recon 20:

Xem branches trong repo 3:

