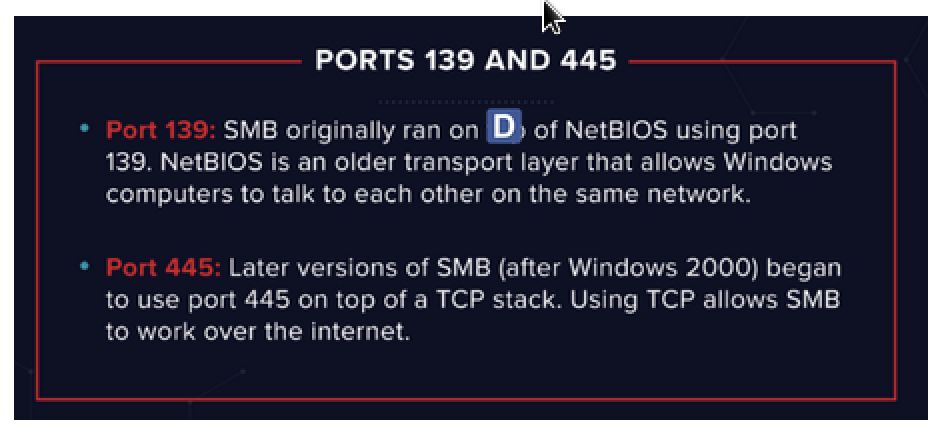
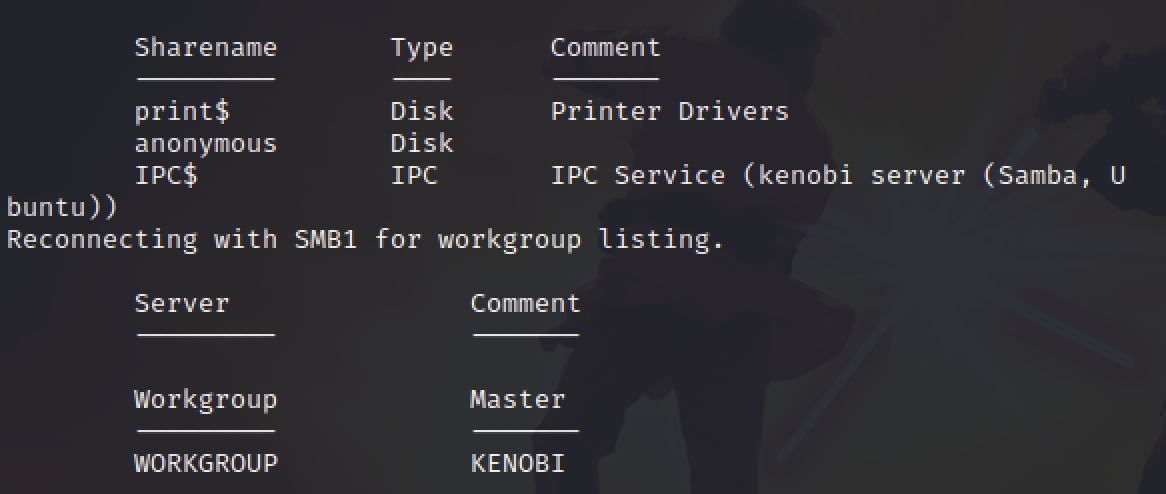
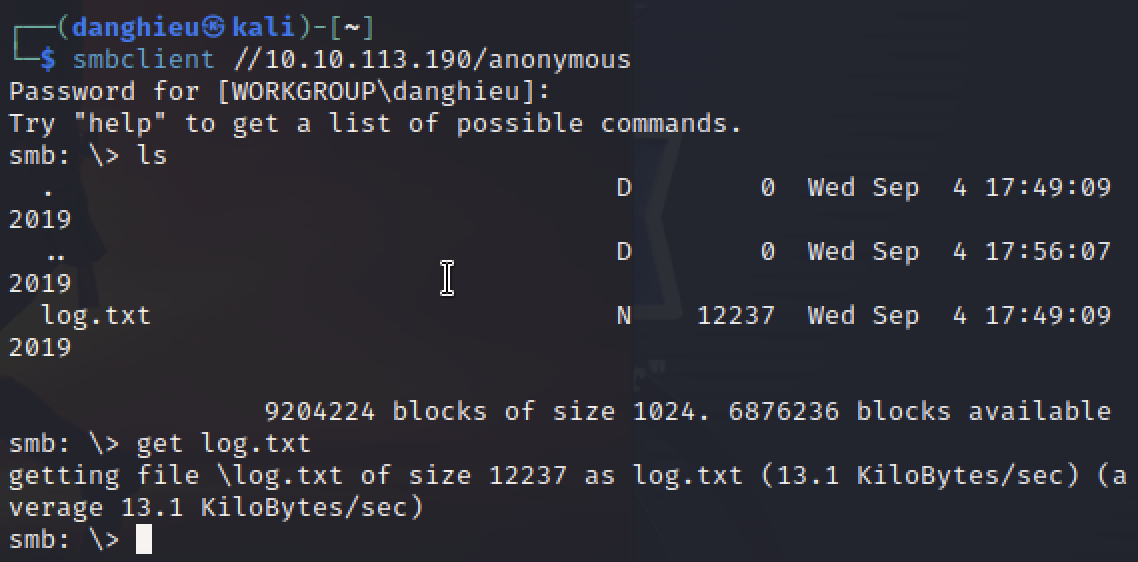


SMB có hai cổng: 445 và 139



enum4linux -a 10.10.113.190





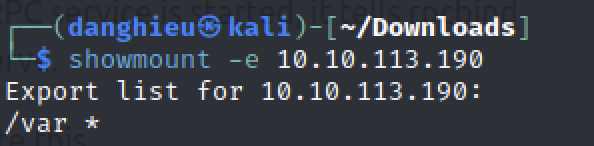
Mở file logs.txt, bạn tìm được:

* Thông tin về SSH key
* Thông tin về máy chủ ProFTPD

Nmap scan có hiện cổng 111 chạy dịch vụ rpcbind. Đó chỉ là máy chủ chuyển đổi số các cuộc gọi từ xa (RPC) sang 1 địa chỉ chung. Khi dịch vụ RPC được bắt đầu, nó sẽ báo cho rpcbind địa chỉ mà nó đang nghe và số các cuộc gọi từ xa mà nó đã chuẩn bị để vận chuyển.

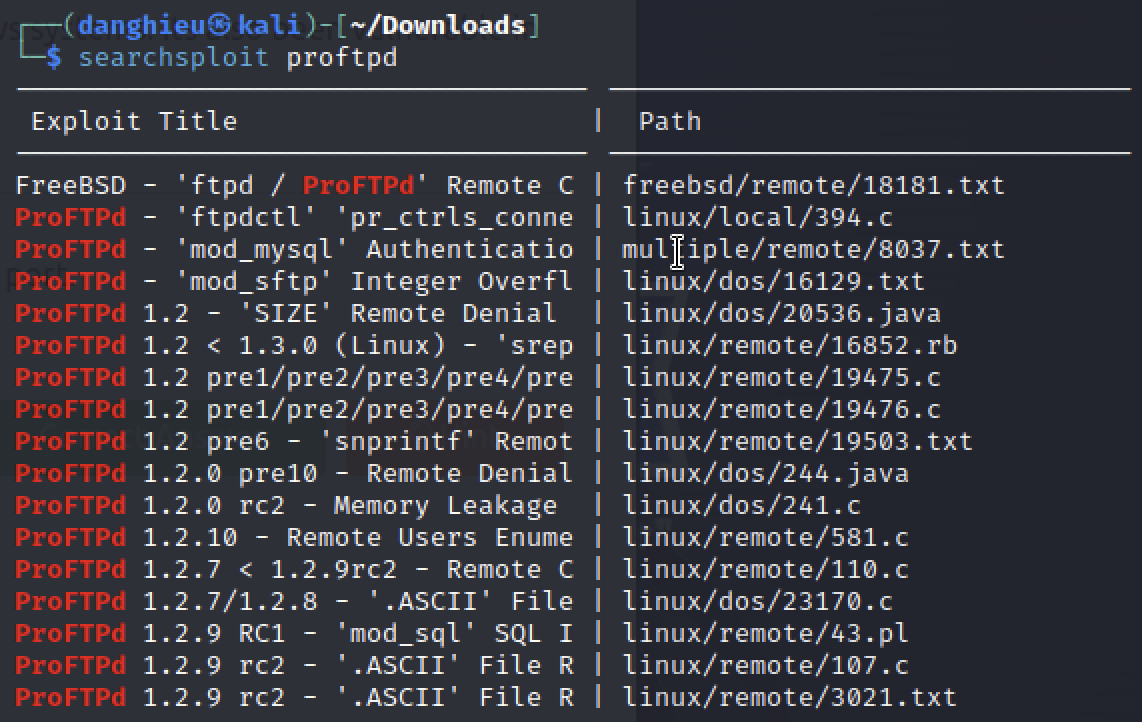
Trong trường hợp này, port 111 là truy cập đến hệ thống file trên mạng (NFS)

Liệt kê hệ thống file trên nfs:



Mount: /var

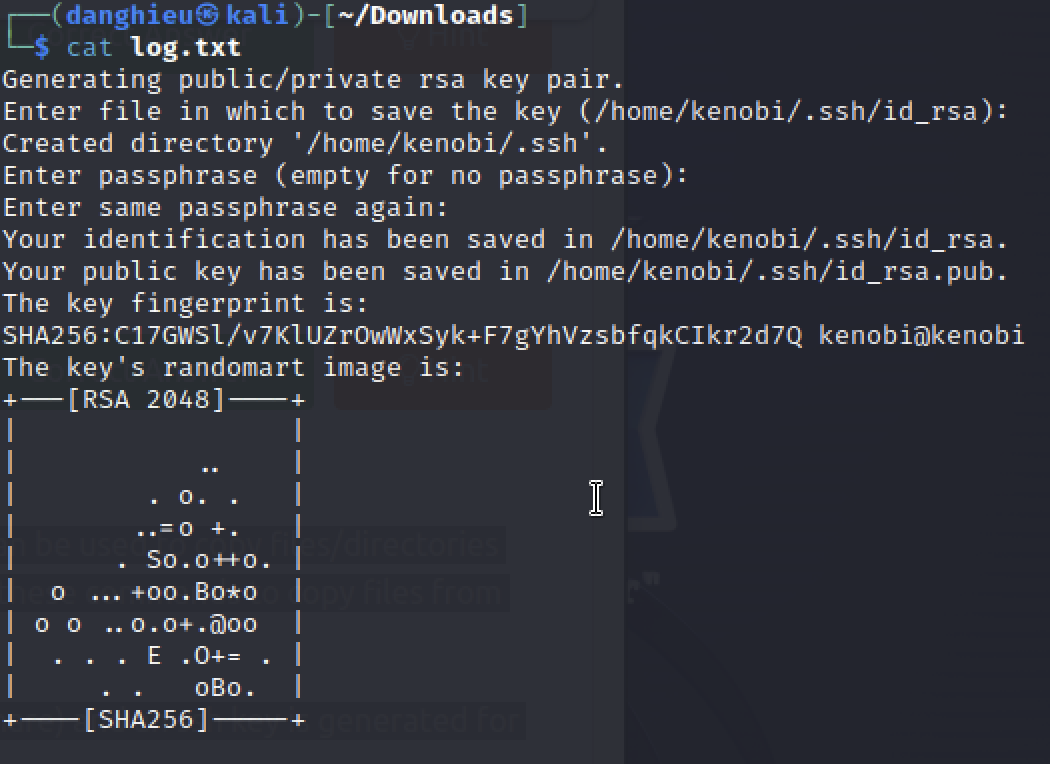
ProFtpd là 1 máy chủ FTP mã nguồn mở và miễn phí, tương thích với hệ điều hành Unix và Windows. Nó cũng bị dính lỗ hổng ở các phiên bản trước.

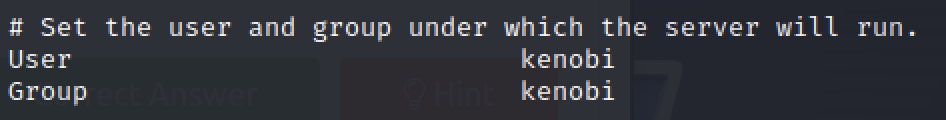


Bạn nên chọn 1 khai thác từ module mod\_copy của ProFtpd.

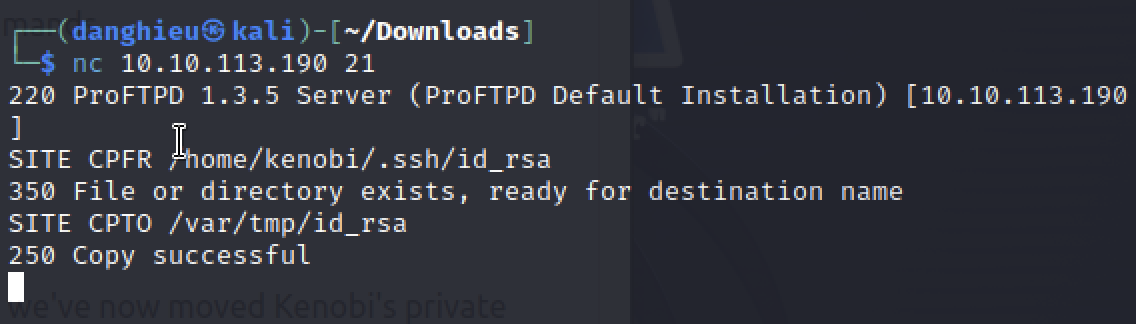
Module mod\_copy thực thi lệnh SITE CPFR và SITE CPTO, có thể được dùng để sao chép tập tin/thư mục từ vị trí A đến vị trí B trong máy chủ.

Chúng ta biết user đang chạy dịch vụ FTP là Kenobi và có 1 ssh key.



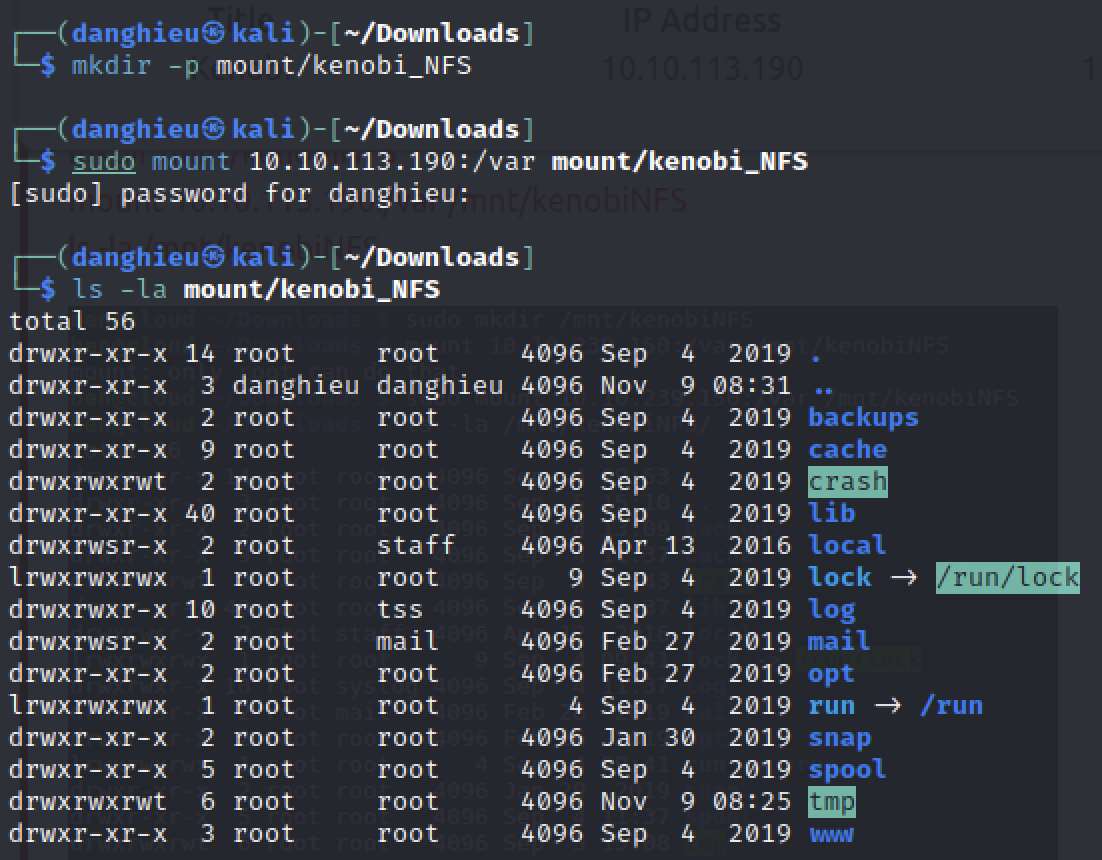


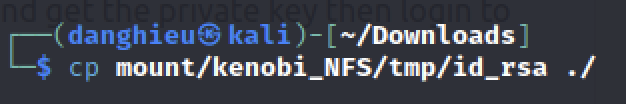
Ta sẽ sao chép private key của Kenobi bằng lệnh SITE CPFR và SITE CPTO

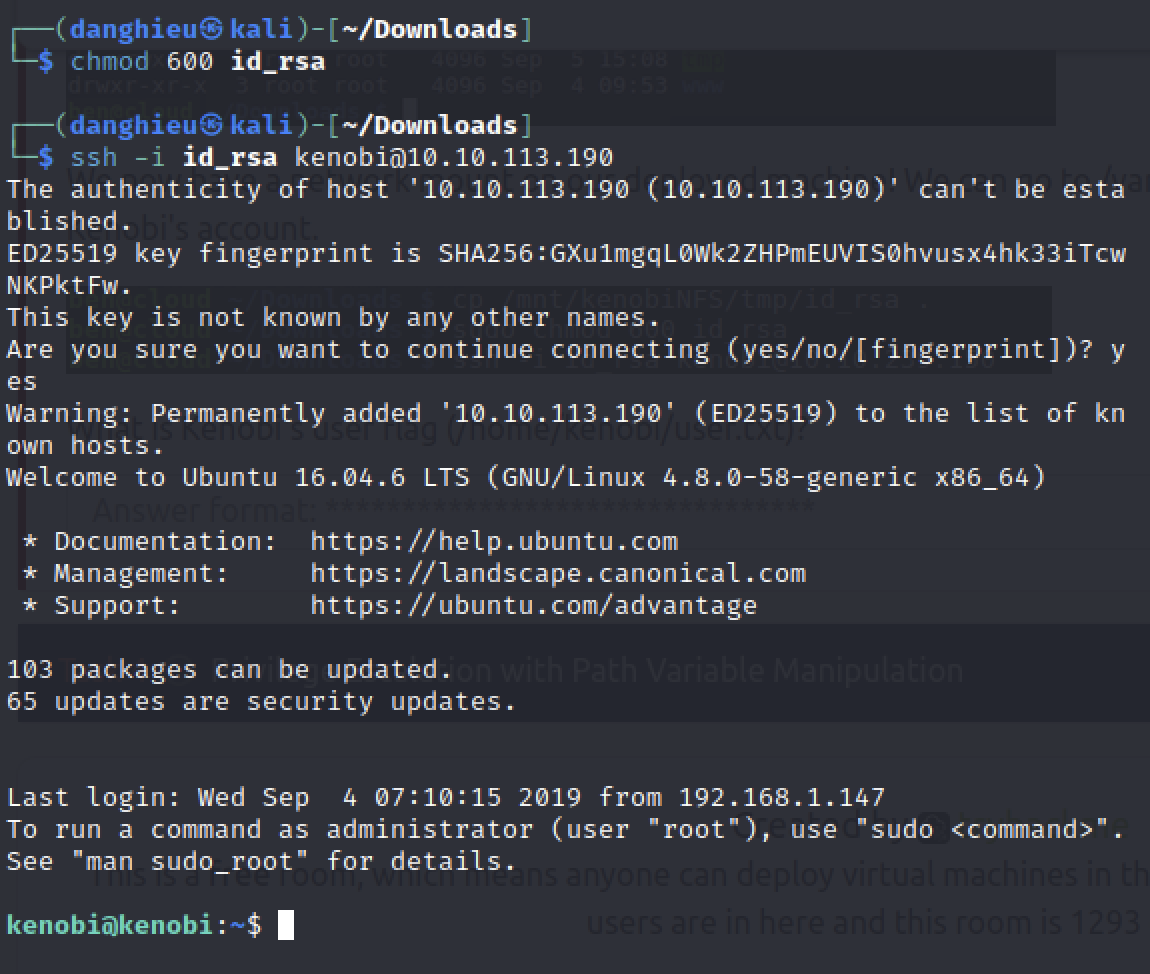


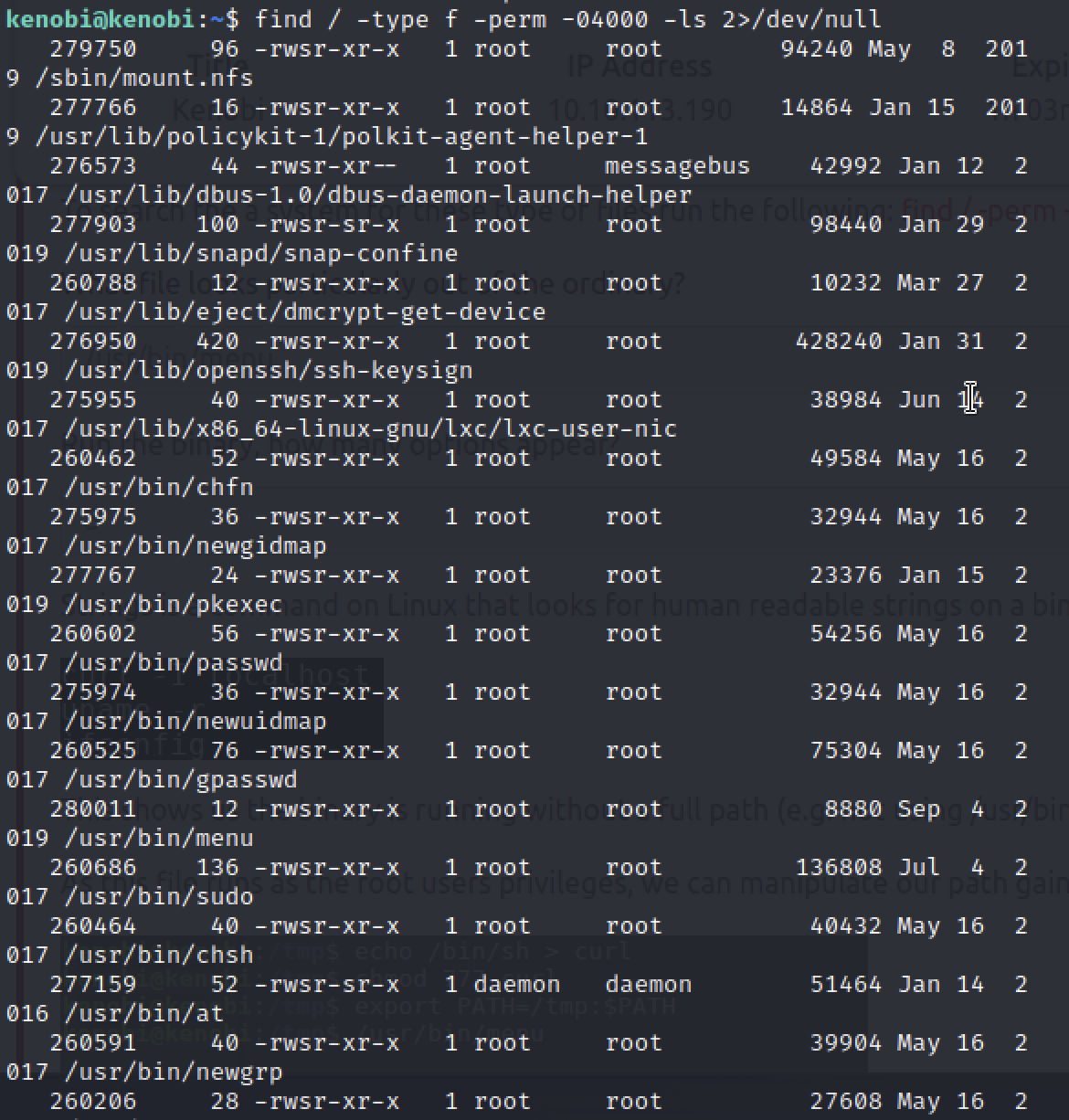
Ta biết thư mục /var là 1 mount có thể thấy nên ta chuyển private key đến thư mục /var/tmp.

Mount thư mục /var/tmp đến máy cục bộ:

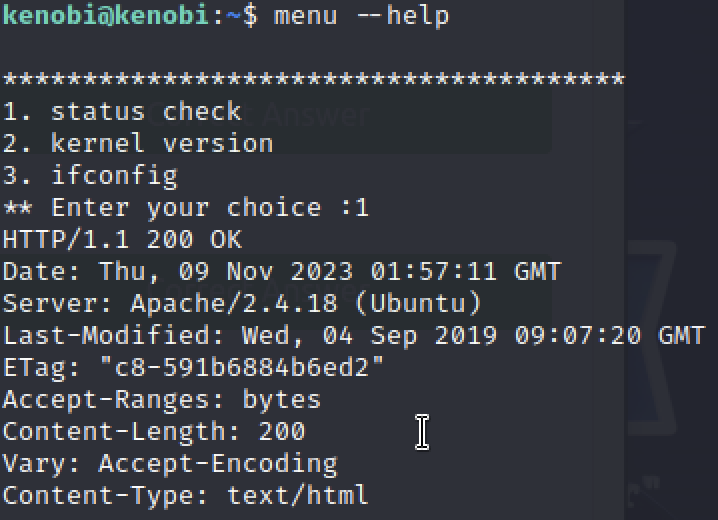


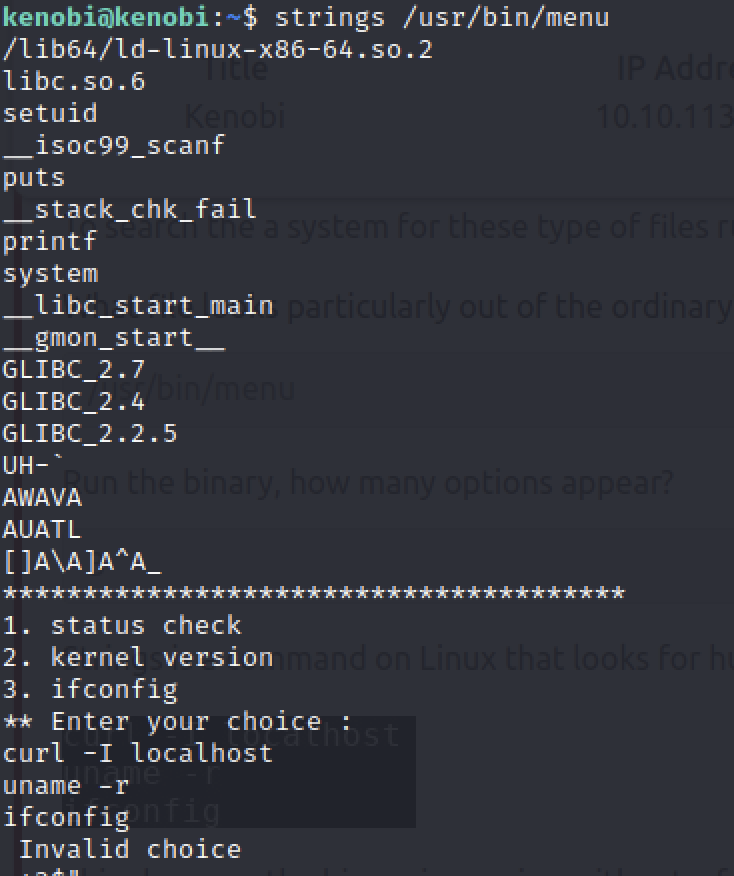




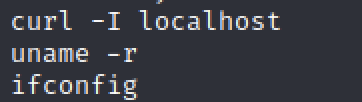


Ta thấy có 1 lệnh rất kì lạ : /usr/bin/menu





Đó là file nhị phân do kenobi tự viết, không có full đường dẫn (/usr/bin/curl , /usr/bin/uname).



Vì file menu chạy dưới đặc quyền của root nên mình có thể tận dụng nó để leo thang đặc quyền.

