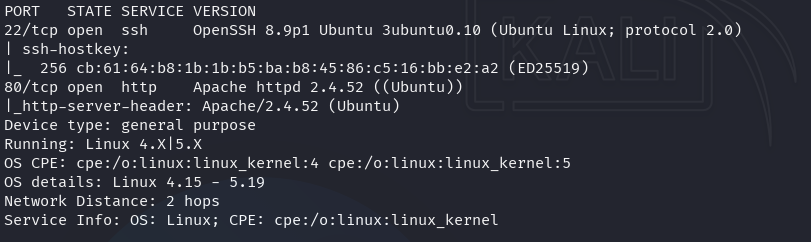
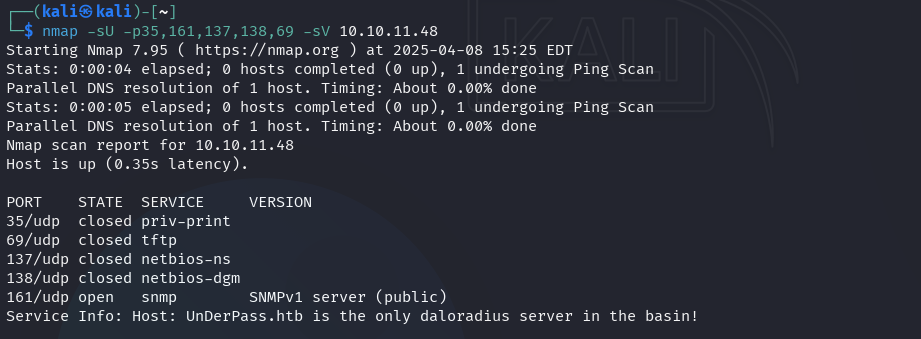
B1: Scanning network



Ta thấy có cổng 22 và 80 đang chạy với dịch vụ ssh và

Nhg khi kiểm tra thì cổng 80 vẫn để apache mặc định và khi dir fuzzing thì k ra kết quả nào cả

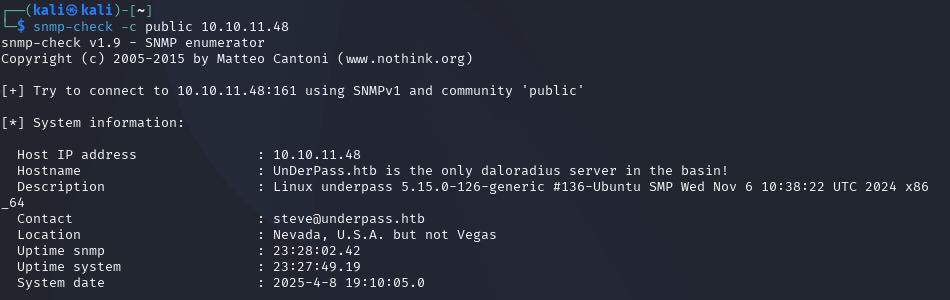
B2: Chuyển qua scan UDP



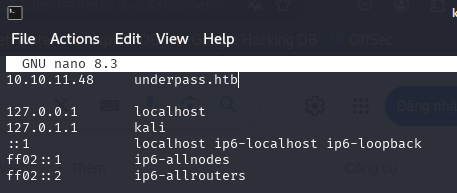
Cổng đáng chú ý ở đây là cổng 161 chạy snmp, có thể kiểm tra thông qua 1 vài tool snmp

B3: Kiểm tra thông tin snmp

Sử dụng tool snmp-check



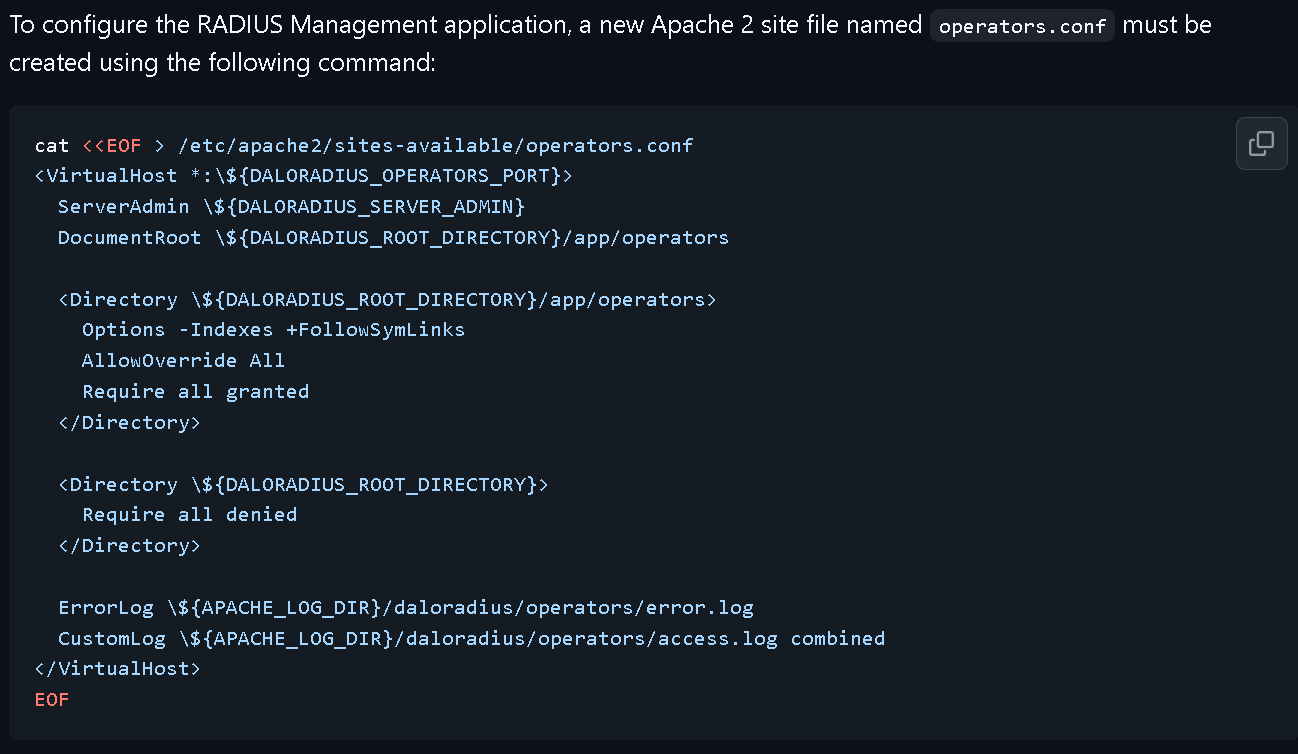
Ở đây có hiển thị chạy dalordius server và thông tin 1 tk email steve



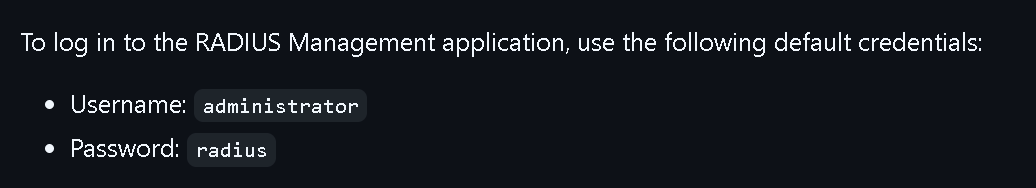
Ta thêm tên miền underpass vào /etc/hosts

Ta có thể xem thông tin về daloRadius [ở đây.](https://github.com/lirantal/daloradius/tree/master)

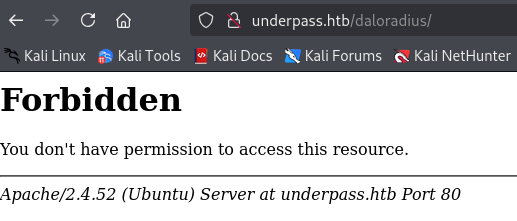
Có thể nhận ra rằng



Truy cập được tới daloradius = <https://<hostname>/daloraidus>

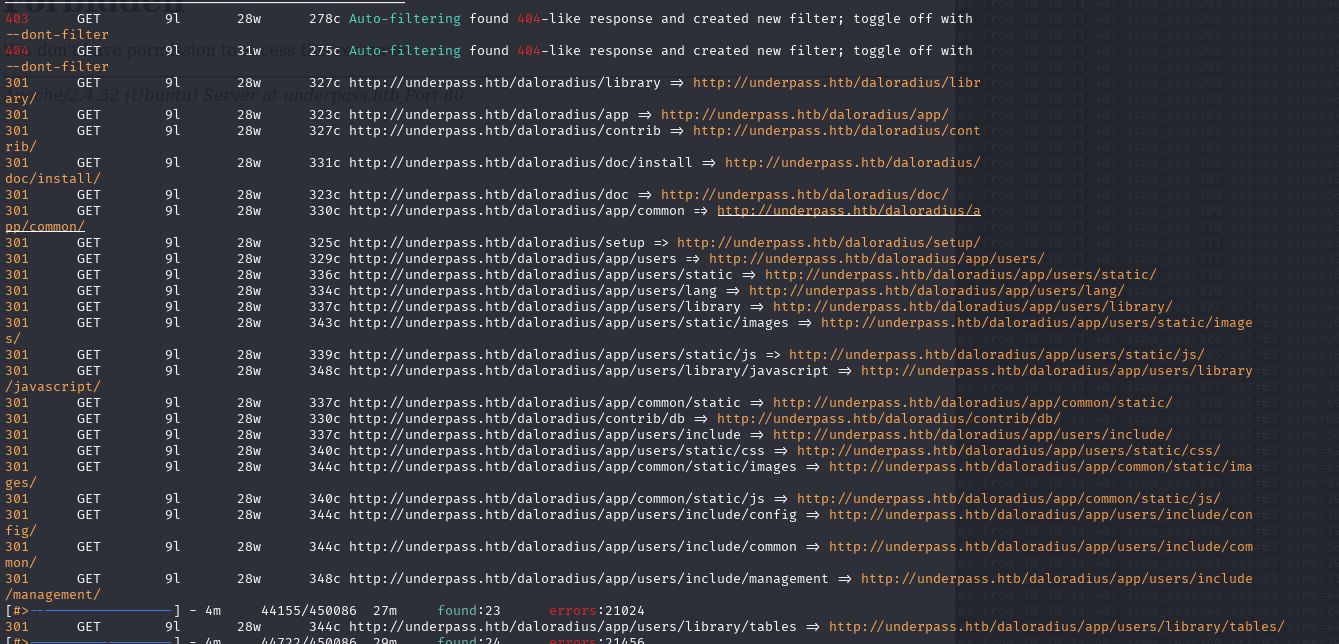


Các thông tin mặc định



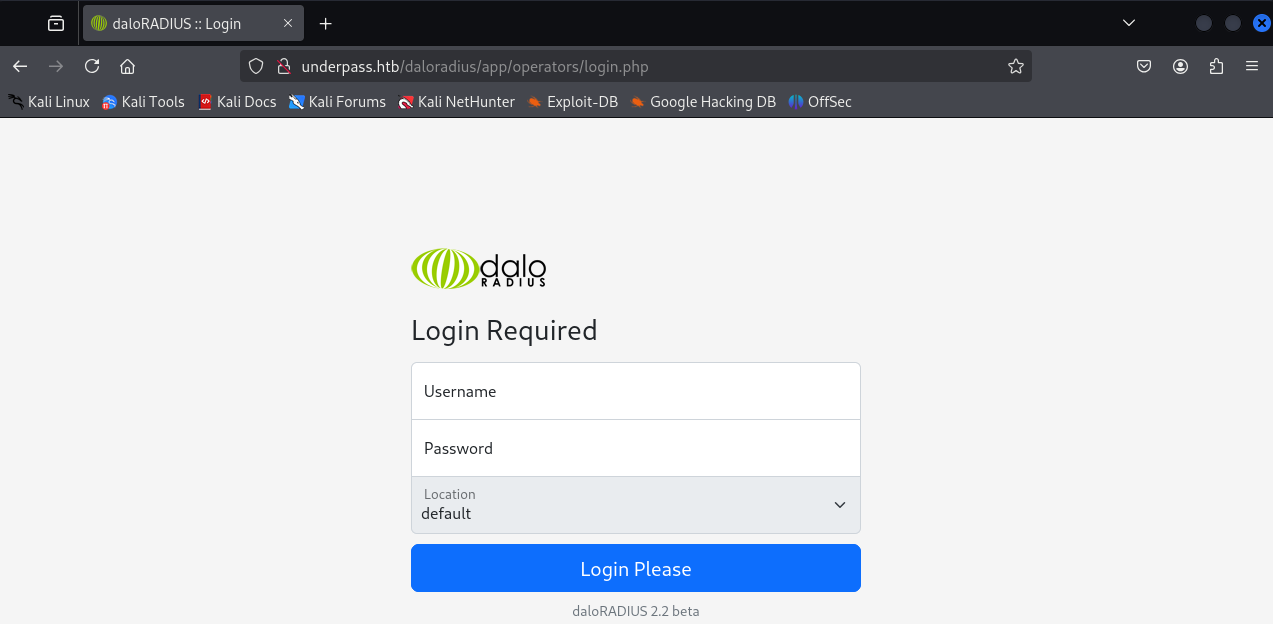
Tiếc là k thể đăng nhập vào dc

Ta dùng feroxbuster để tìm xem còn thư mục hay file hay ho nào k

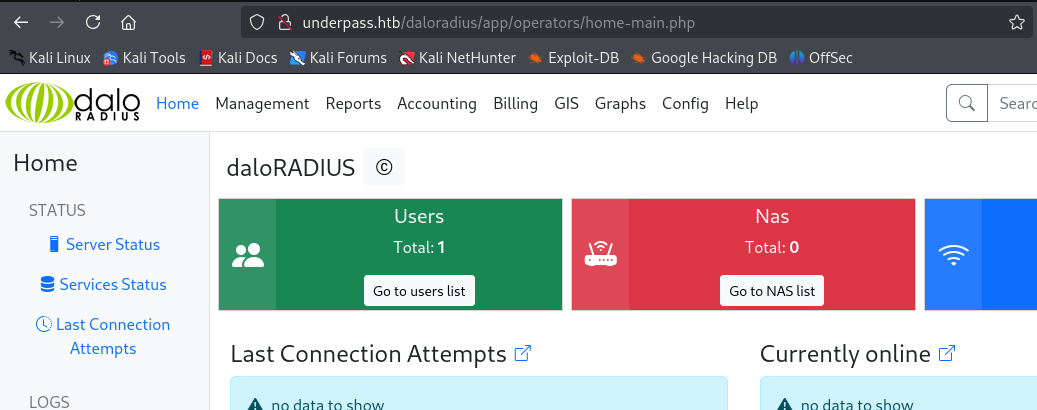


Ta thấy tất cả các thư mục hay ho đều nằm trong /app, tiếp tục đào sâu vào nó và thấy có 1 trang operators mặc định để config như đã đề cập trong git.

Ta truy cập vào trang đăng nhập operators

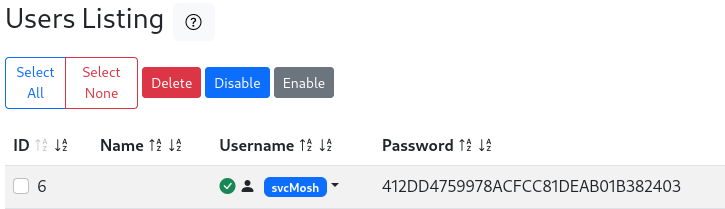


Thử sử dụng thông tin mặc định ghi ở trong git

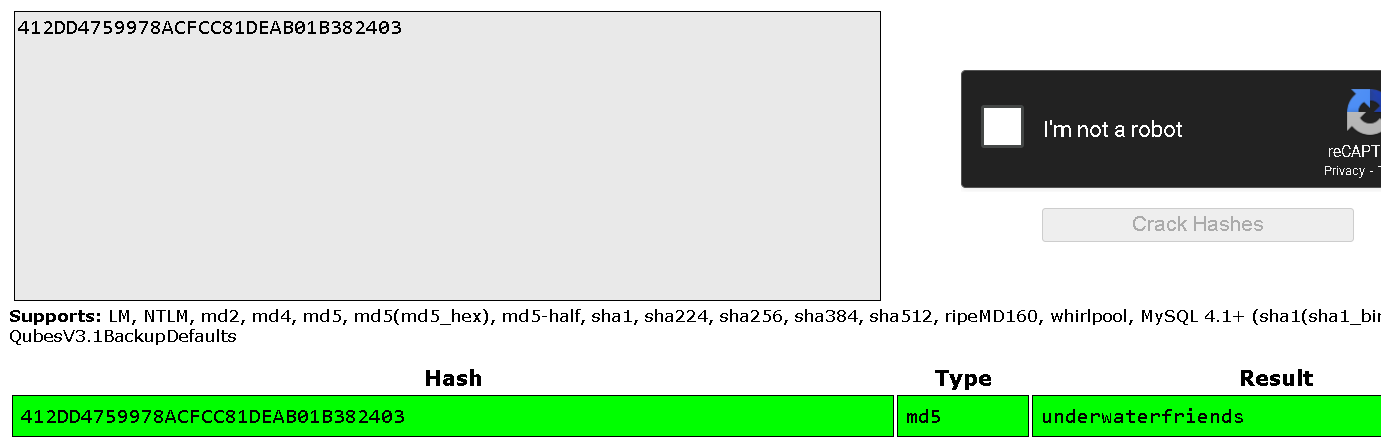


Đăng nhập thành công

Tiếp tục kiểm tra thông tin user

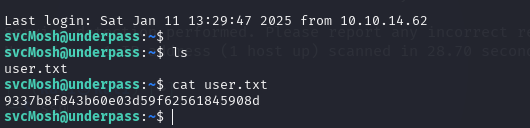


Ta có được 1 tài khoản với tên svcMosh và hash mật khẩu là 412DD4759978ACFCC81DEAB01B382403. Sau khi sử dụng crackstation ta có dc mk là:

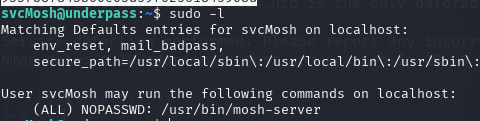


underwaterfriends

Ta SSH vào với thông tin lấy được ở trên và thành công lấy dc user flag

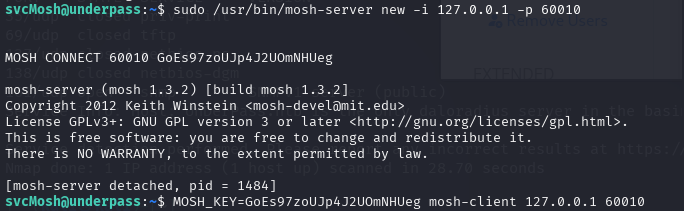


B6: leo thang đặc quyền

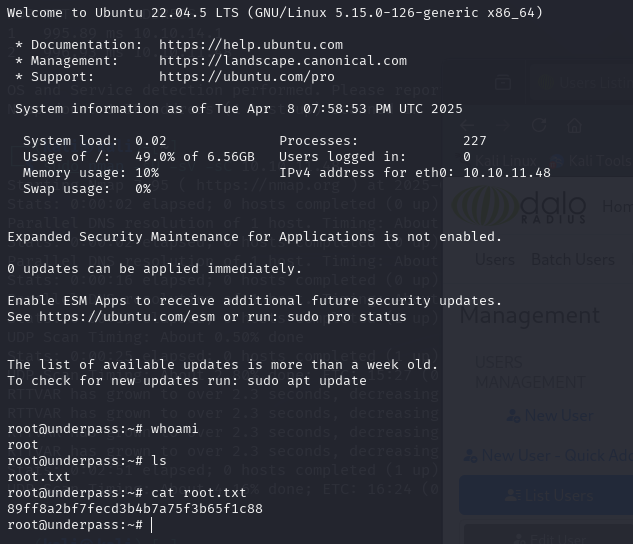


Kiểm tra thì với tài khoản này ta có thể thực thi mosh-server (mobile shell)

Ta có thể tận dụng để leo thang đặc quyền thông qua phương thức này [medium.com](https://medium.com/@momo334678/mosh-server-sudo-privilege-escalation-82ef833bb246)



Ta lấy được rootflag



Hoàn thành

