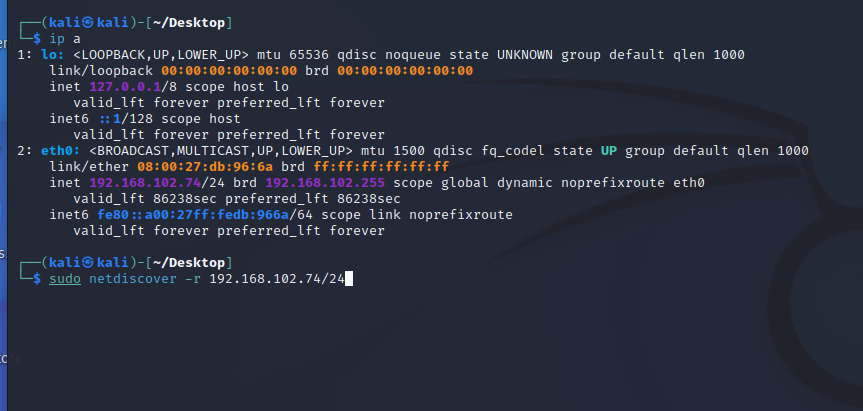
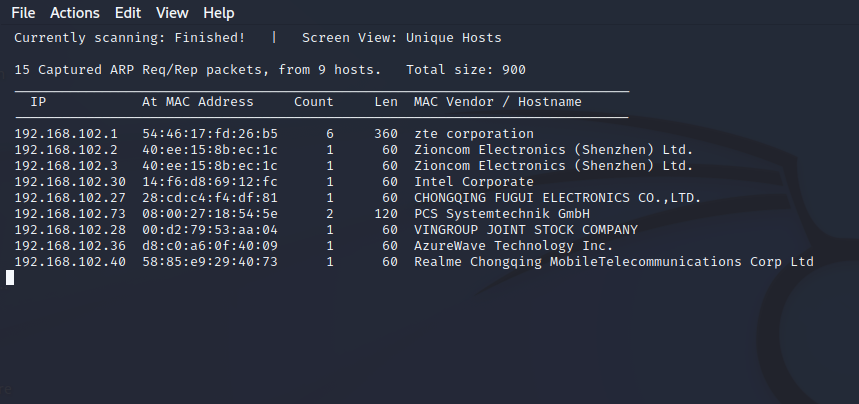
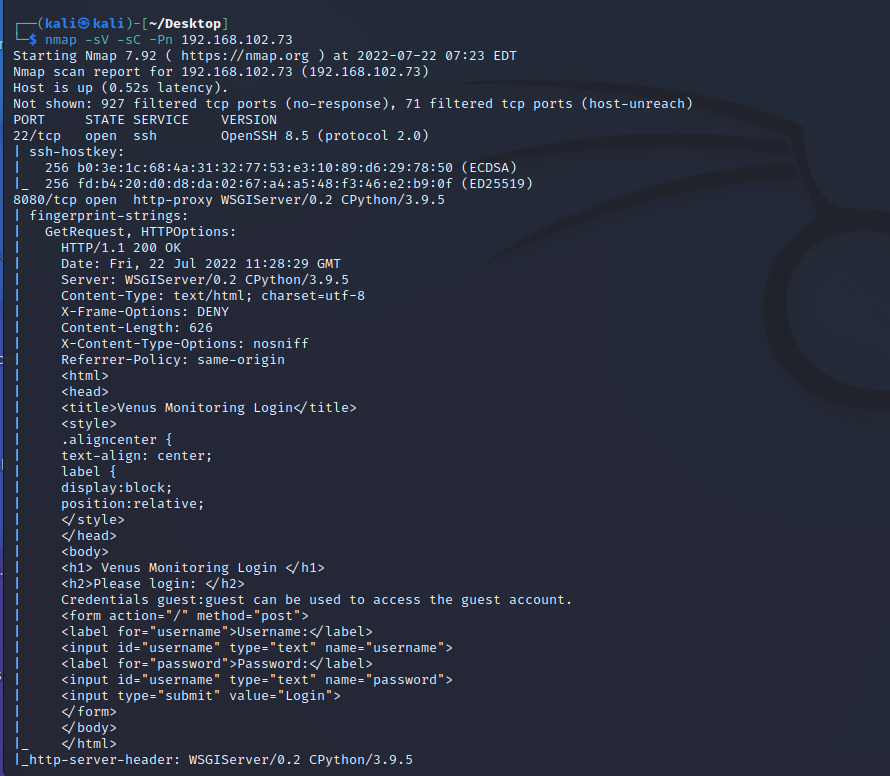
- Dùng netdiscover để tìm kiếm ip của Venus



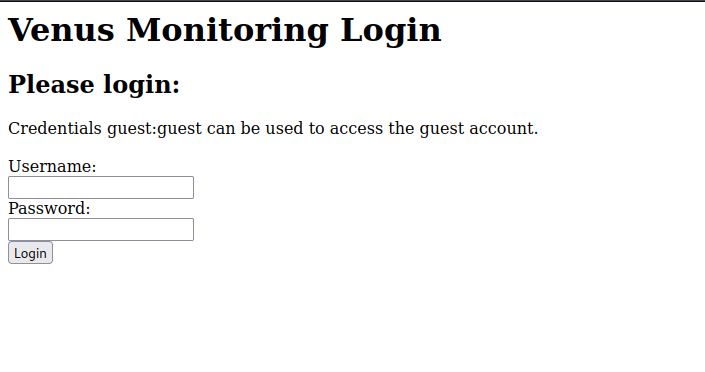


- ip là 192.168.102.73 (Hostname PCS Systemtechnik GmbH là thứ ta cần để ý để biết được ip)

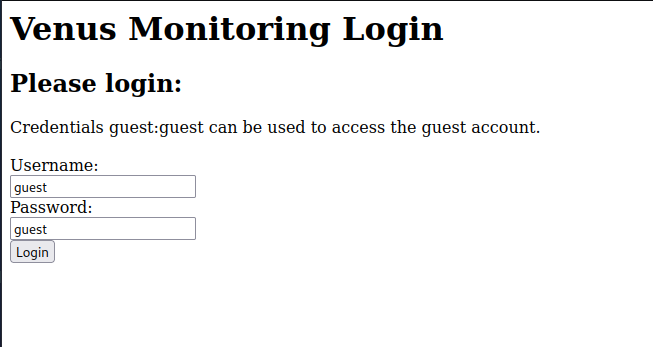
- Dùng nmap để kiểm tra các port

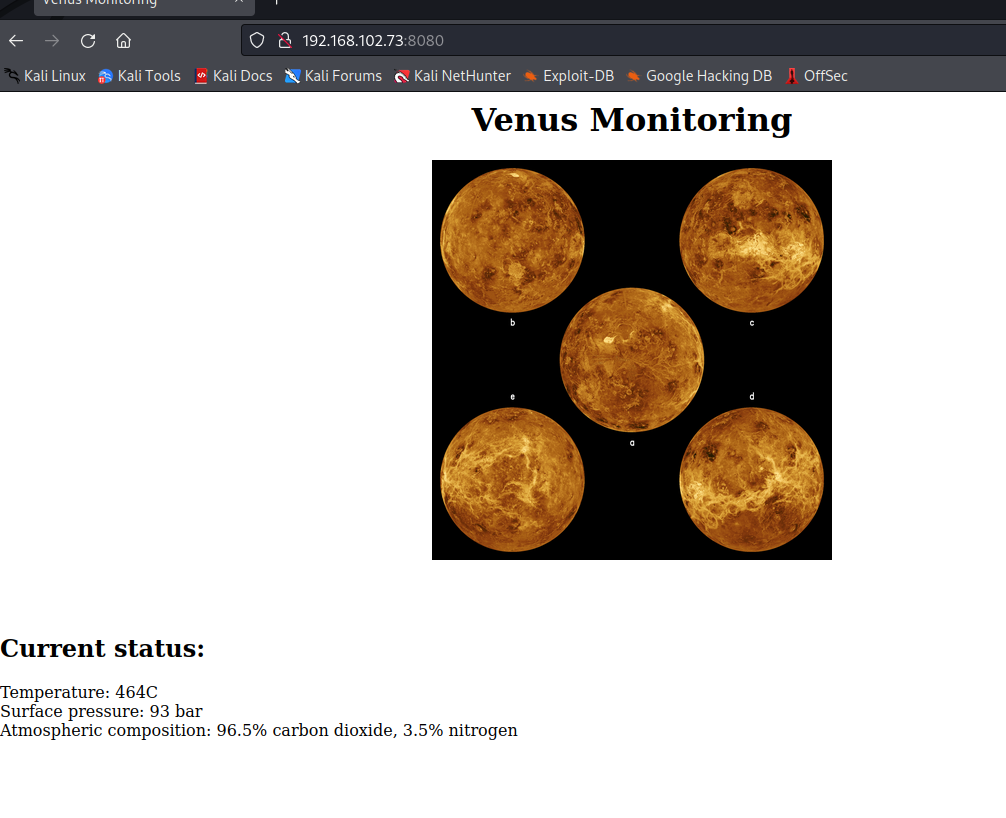


- Mở trình duyệt, vào thử trang

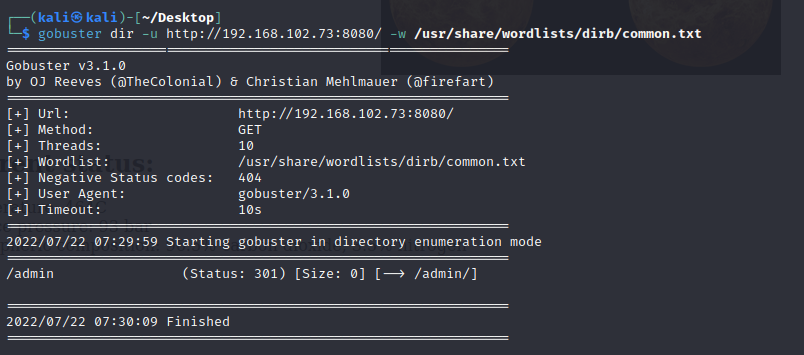


- Theo như nội dung trên màn hình thì ta có thể đăng nhập bằng username và mật khẩu là guest



- Chu

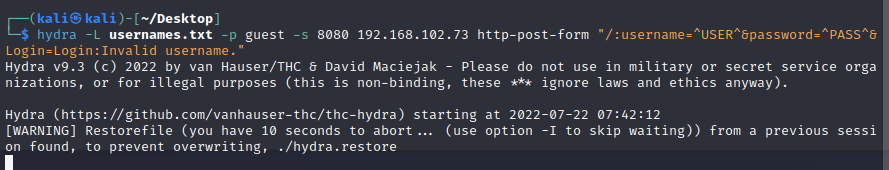
- Chưa có gì mới lạ, ta thử dùng gobuster để tìm thêm đường dẫn



- Phát hiện có /admin và ta thử vào xem

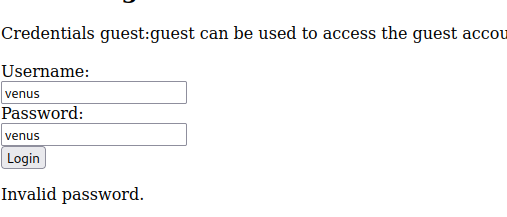


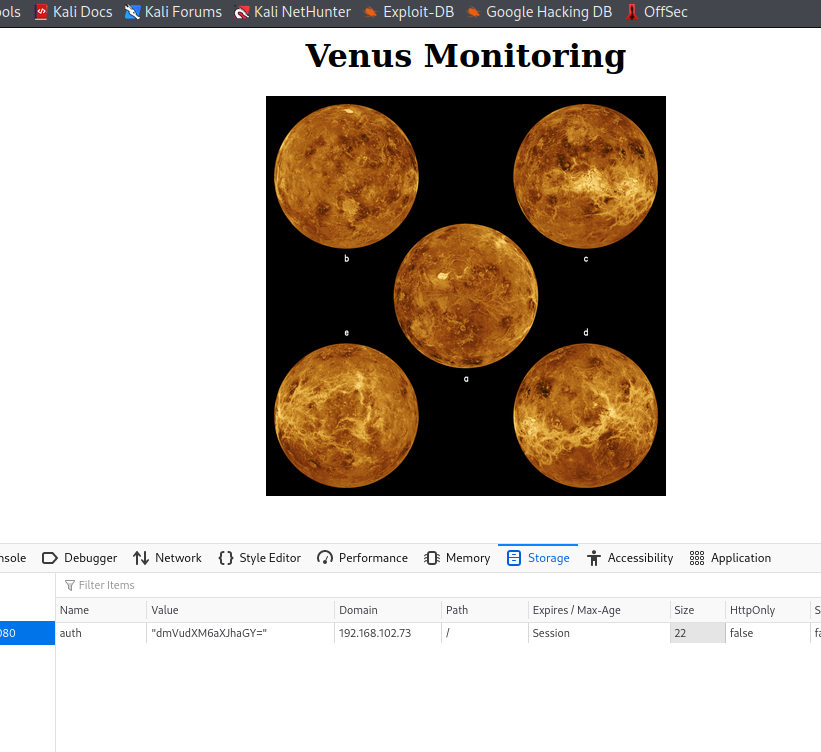
- Thử dùng hydra để bruteforce ra các username sử dụng mật khẩu guest



- Thì sau khi bruteforce xong chúng ta sẽ có hai user đó là venus và Magellan

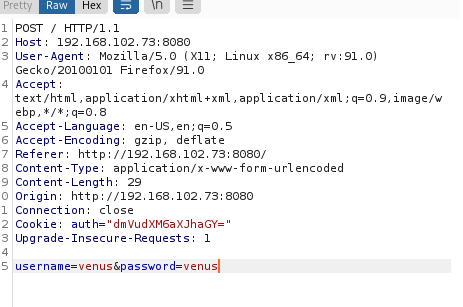
- Ta thử đăng nhập bằng username và mật khẩu là venus



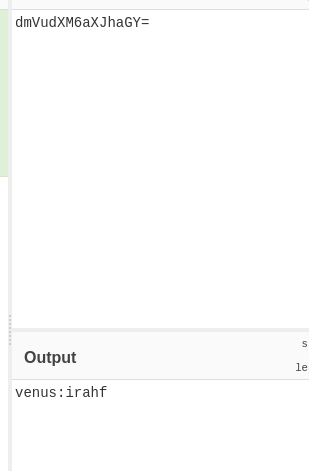


- venus vào được nhưng magellan thì lại không

- Giờ ta sẽ dùng burpsuite để can thiệp vào và thay đổi username của venus thành magellan, xem cookie có thay đổi gì không

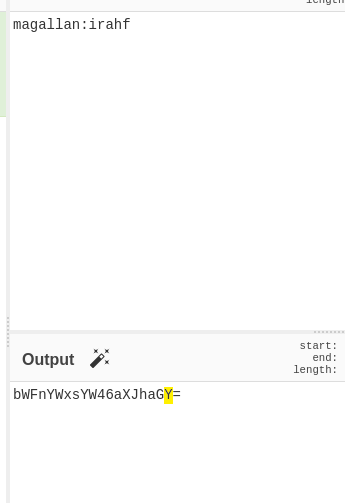


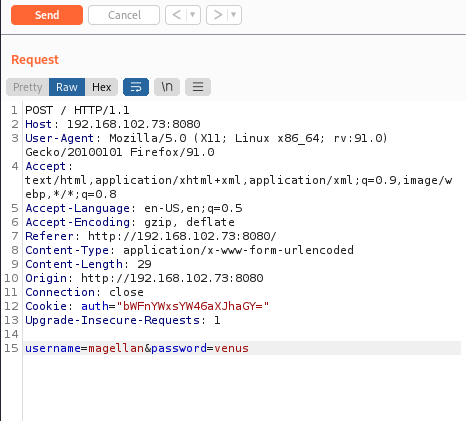
- Đầu tiên ta sẽ sửa phần username thành magellan, tiếp đến là ở phần cookie ban đầu (dmVudXM6aXJhaGY=) đó chính là mật khẩu của venus đã được mã hoá dạng base64 và rot13 (irahf chính là mật khẩu) (Dùng cyberchef để giải mã)



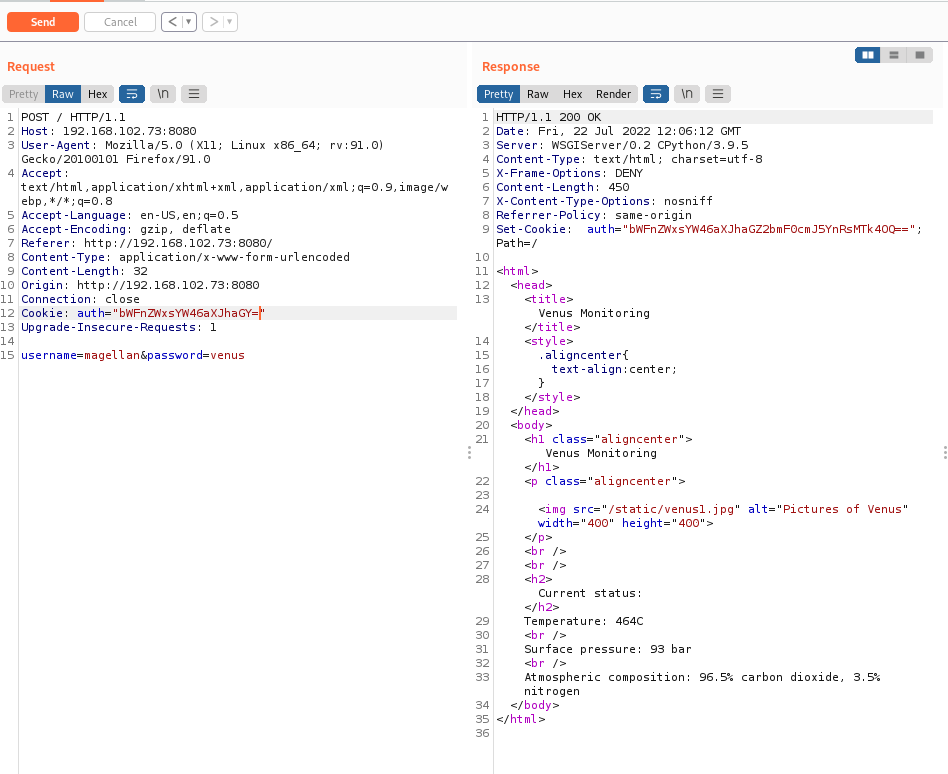
- Vì ta sẽ đổi username thành magellan nên phần cookie ta cũng phải thay đổi lại

- Chuyển nó về lại dạng base64 và thay vào phần cookie trong burpsuite



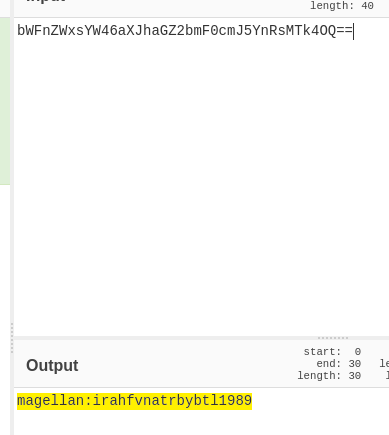


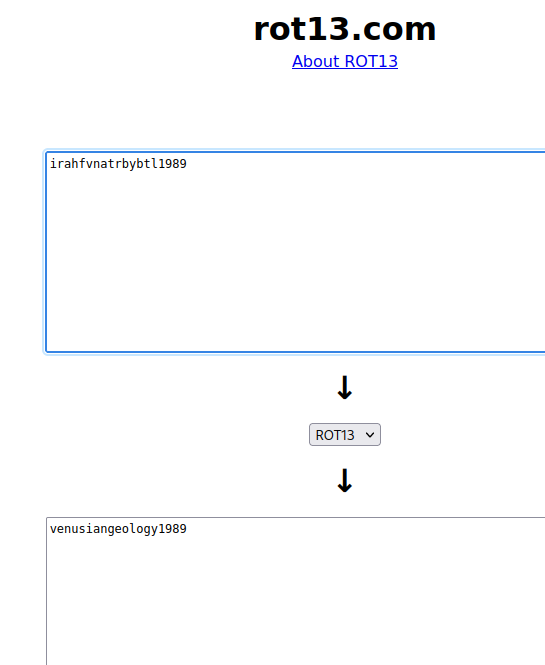
- Sau đó bấm send và ta sẽ được một cookie mới



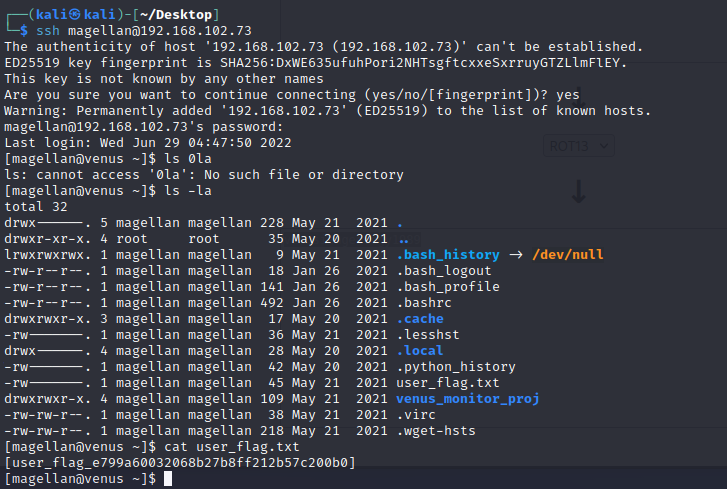
- Ở phần Set-Cookie: bWFnZWxsYW46aXJhaGZ2bmF0cmJ5YnRsMTk4OQ==, đó chính là mật khẩu cho user magellan

- Dùng cyberchef và rot13 để giải mã và ta được mật khẩu là venusiangeology1989

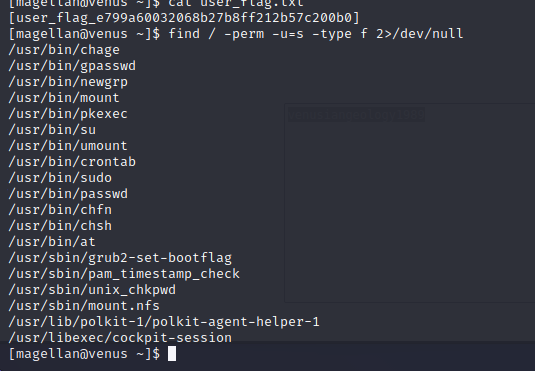




- ssh vào magellan, nhập mật khẩu và tìm user flag



- Giờ chúng ta cần tìm xem có tệp tin nào có quyền cao để từ đó mà leo thang quyền



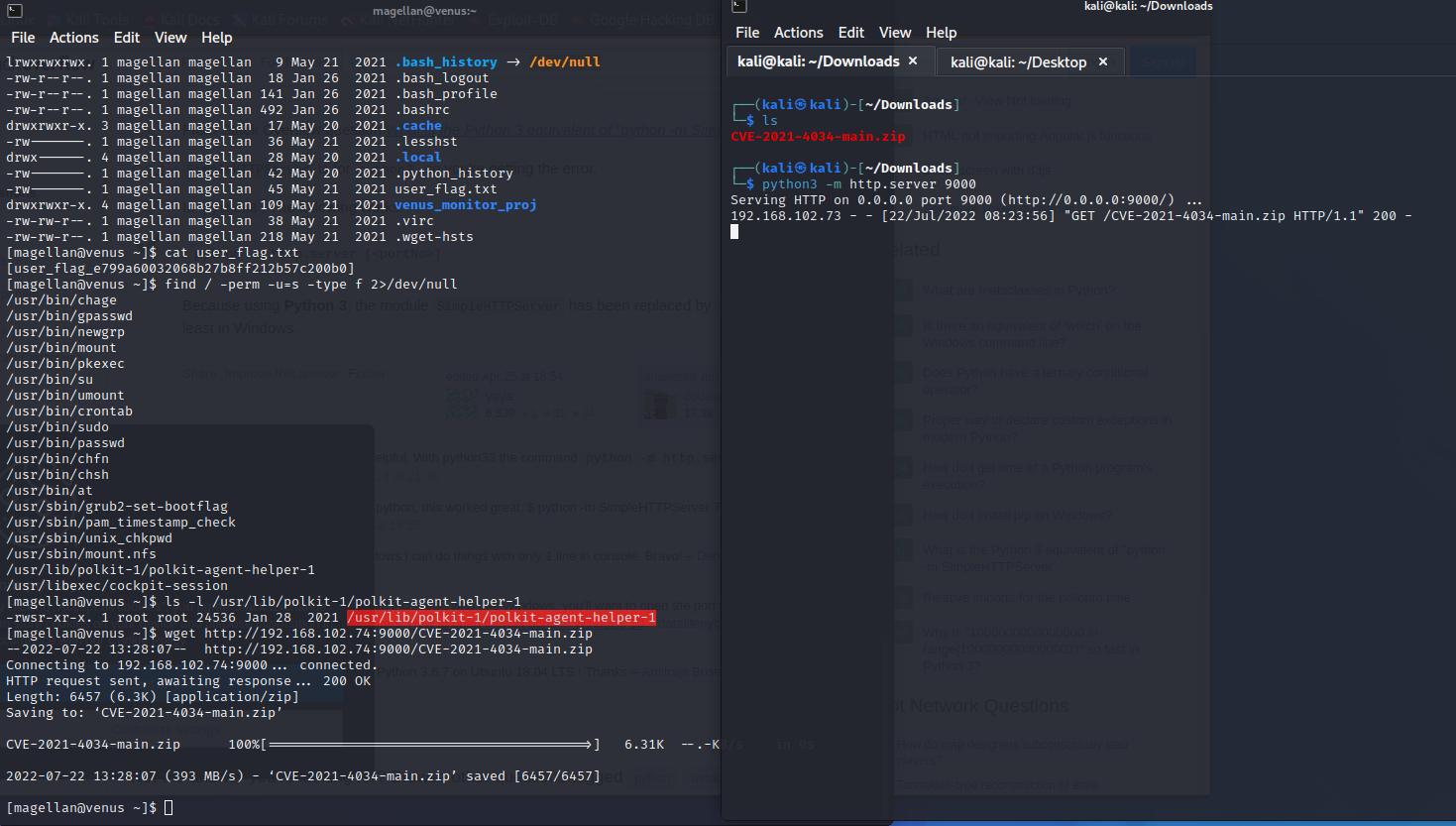
- Ta thấy có polkit-agent-helper-1 là khả thi

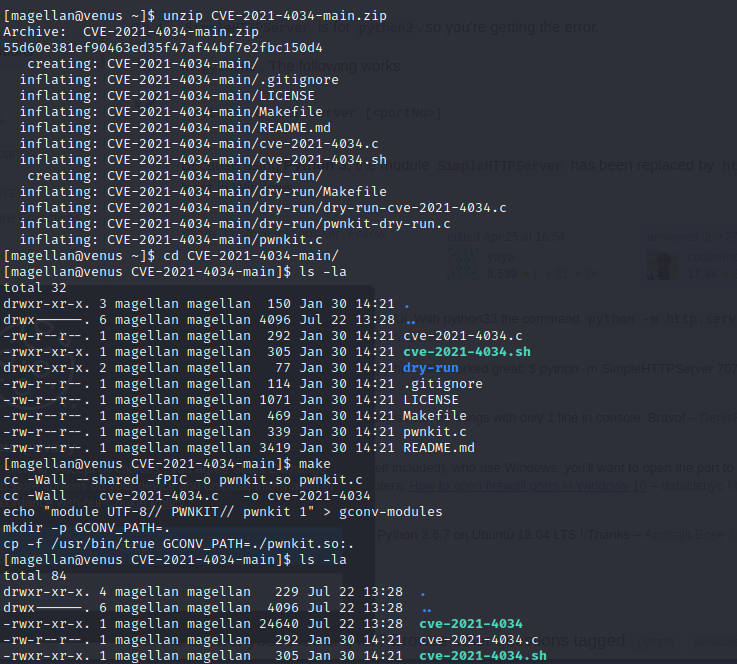


- Trước khi tìm kiếm lỗ hổng, phải kiểm tra phiên bản của tập file mà mình muốn exploit

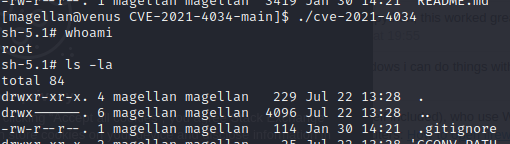
- Khi ta lên mạng tìm kiếm exploit cho polkit-agent-helper-1 thì phát hiện có lỗ hổng CVE-2021-4034 mà ta có thể dùng để leo quyền

- Lên github để lấy code về, chuyển file zip qua máy ta đang tấn công, unzip và chạy nó





- Chạy cve-2021-4034



- Đã lên được root thành công, giờ chỉ còn việc đi kiếm root flag

