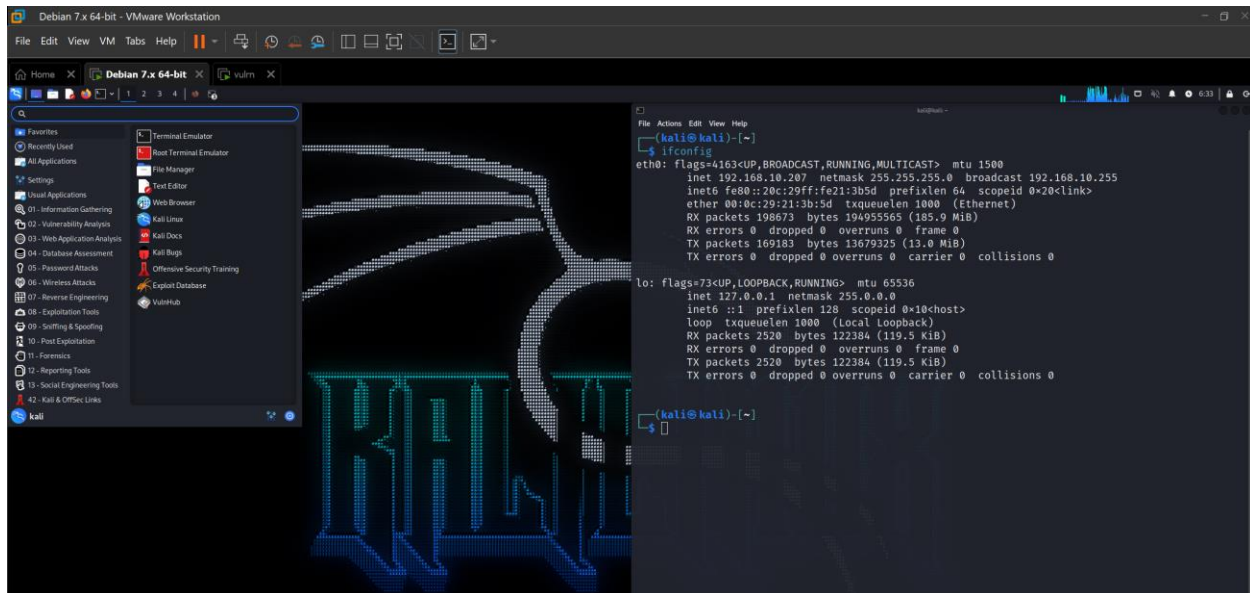
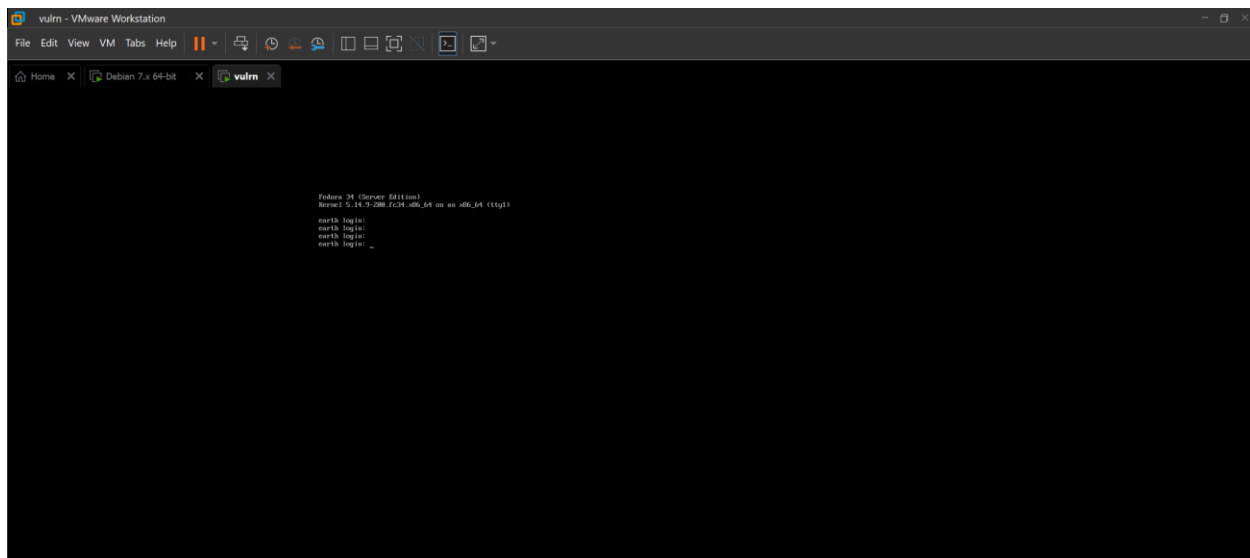


Login both machines:

Kali:



Fedora machine:



Ping and Nmap:

```
File Edit View VM Tabs Help
Debian 7.x 64-bit vuln
root@kali: /home/kali

(root@kali)-[/home/kali]
# nmap -sV 192.168.10.128
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-28 06:35 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.85% done; ETC: 06:36 (0:00:53 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 06:35 (0:00:06 remaining)
Nmap scan report for earth.local (192.168.10.128)
Host is up (0.0018s latency).
Not shown: 985 filtered tcp ports (no-response), 12 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: 00:0C:29:F1:CE:83 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.86 seconds

(root@kali)-[/home/kali]
#
```

Adding host to config file:

```
(root@kali)-[/home/kali]
```

```
# echo "192.168.10.128 terratest.earth.local" >> /etc/hosts
```

```
Home Debian 7.x 64-bit vuln
root@kali: /home/kali

(root@kali)-[/home/kali]
# echo "192.168.10.128 earth.local" >> /etc/hosts

(root@kali)-[/home/kali]
#
```

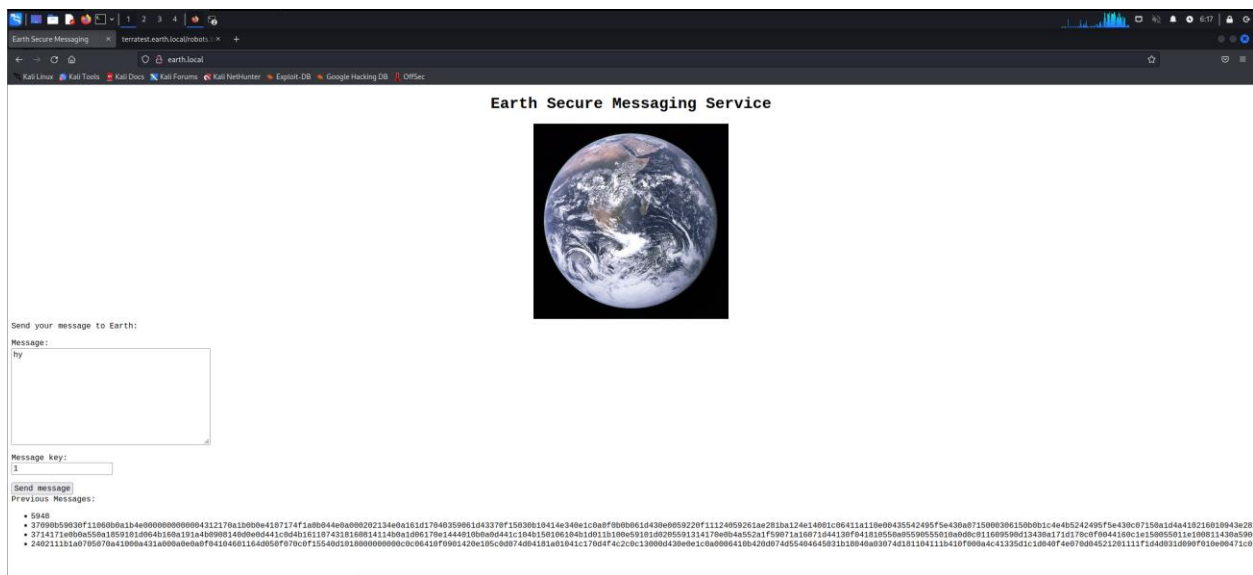
```
root@kali: /home/kali
# echo "192.168.10.128 earth.local" >> /etc/hosts

root@kali: /home/kali
# echo "192.168.10.128 terratest.earth.local" >> /etc/hosts

root@kali: /home/kali
#
```

Send your message to Earth:
Message:
ty

Open browser:
<http://earth.local/>

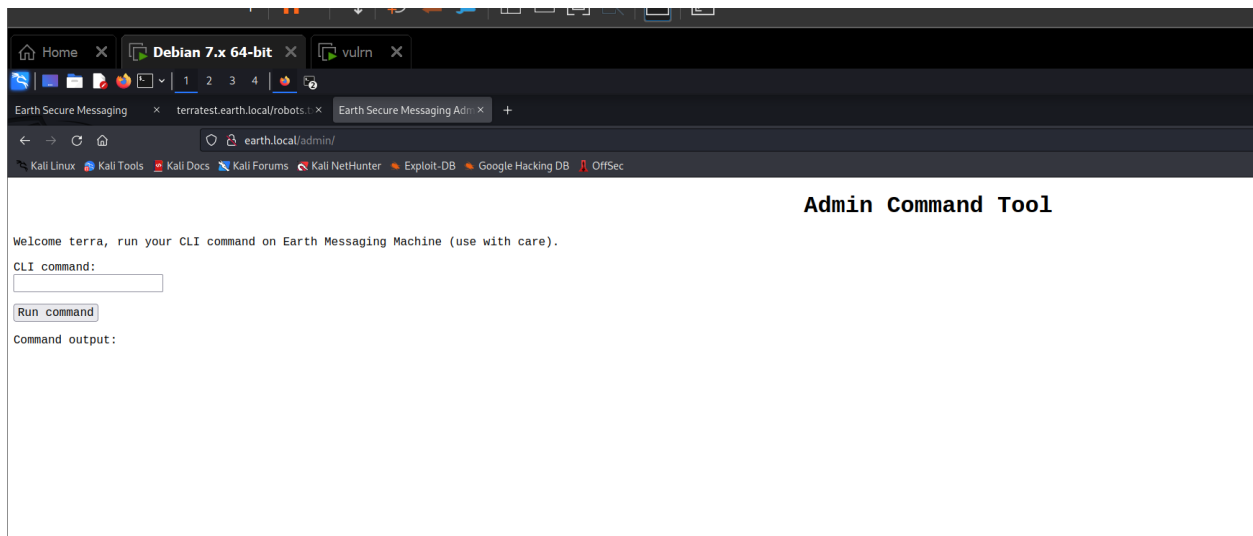


Go to earth.local/admin and log in.

Enter the credentials:

Username: terra

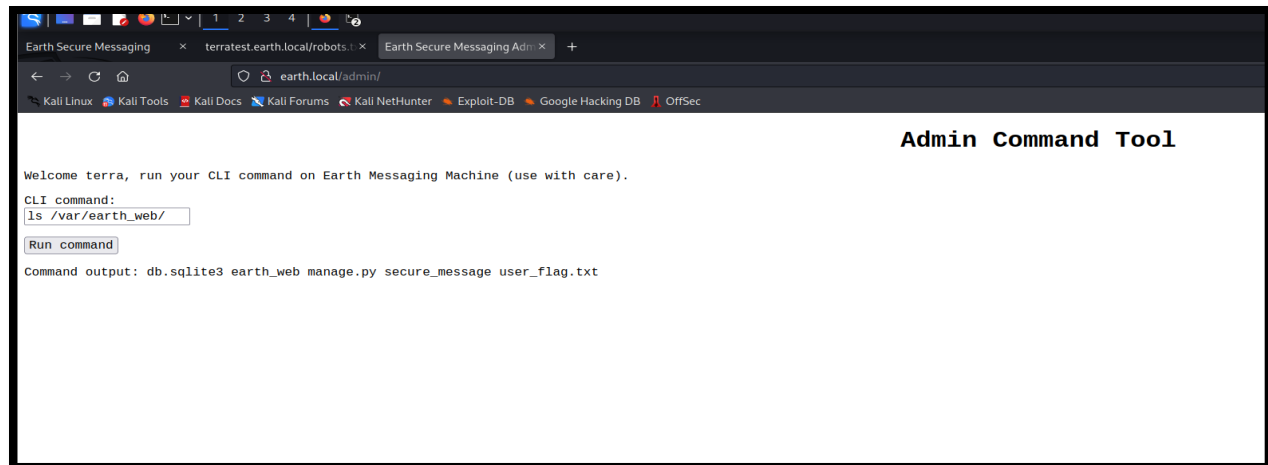
Password: earthclimatechangebad4humans



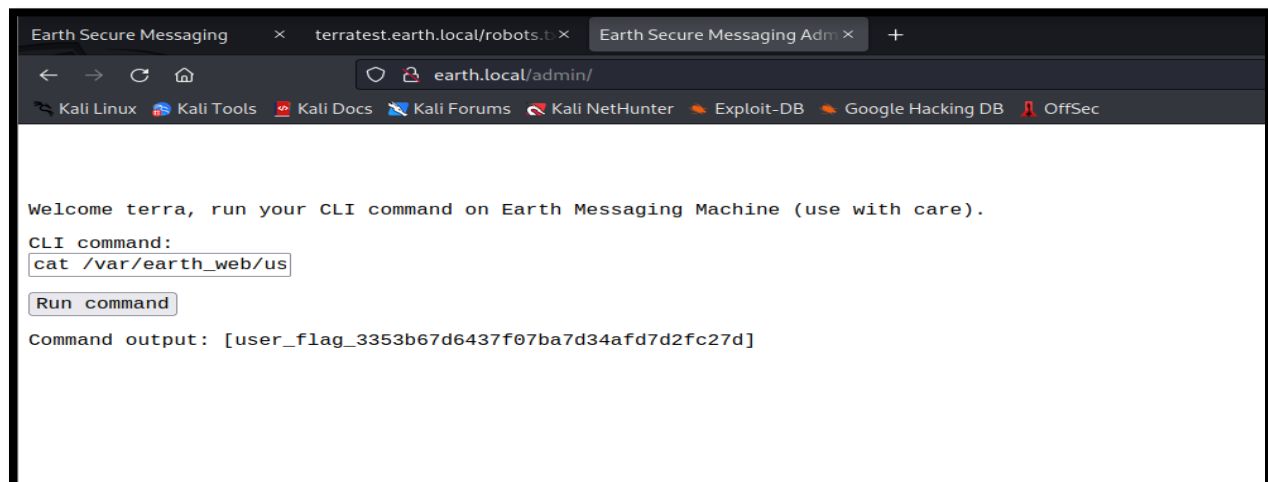
Run the command :`cd /home; ls -al;pwd`



run the command `ls /var/earth_web/`



Flag:



Conclusion:

After obtaining preliminary get right of entry to, similarly exploration revealed susceptible offerings at the Fedora machine, leading to privilege escalation. Utilizing discovered vulnerabilities, additional data exfiltration and lateral movement maneuvers had been accomplished, highlighting capability security gaps for remediation.