Planet Earth - CTF Report

Author: Karandeep Singh Sehgal

Date: June 03, 2025

Target: Planet Earth (VulnHub)

Difficulty: Easy-Medium

Flags Captured: User, Root

# 1. Objective

The objective was to perform reconnaissance, exploitation, and privilege escalation on the target virtual machine to capture two flags: a user-level and a root-level flag.

# 2. Reconnaissance

## 2.1 Network Discovery

Used netdiscover to identify the target's IP:

netdiscover –i <interface>

Target IP: 192.168.56.104

## 2.2 Nmap Scan

nmap -sC -sV -p- –T4 192.168.56.101

Open Ports:  
- 22/tcp - SSH  
- 80/tcp - HTTP  
- 443/tcp - HTTPS

## 2.3 SSL Certificate Analysis

Domains discovered:  
- earth.local  
- terratest.earth.local

Updated /etc/hosts accordingly.

# 3. Web Enumeration

Browsed https://earth.local and https://terratest.earth.local.

Used gobuster to find hidden directories:

gobuster dir -u https://earth.local -w /usr/share/wordlists/dirb/common.txt -k

Found:  
- /admin  
- /robots.txt → testingnotes.txt and testdata.txt

# 4. Exploitation

Used CyberChef to decrypt XOR-based credentials using testdata.txt.

Credentials:  
- Username: terra  
- Password: earthclimatechangebad4humans

Logged into /admin panel and used command execution to get reverse shell.

User flag captured from terra's home directory.

# 5. Privilege Escalation

Found SUID binary /usr/bin/reset\_root.

Used ltrace to analyze and bypass its checks.

Created required file to trigger password reset.  
Switched to root user using password: Earth

Root flag captured from /root/root.txt.

# 6. Flags

User Flag: [user\_flag\_3353b67d6437f07ba7d34afd7d2fc27d]

Root Flag: [root\_flag\_b0da9554d29db2117b02aa8b66ec492e]

# 7. Conclusion

This CTF box provided a great blend of web enumeration, basic XOR cryptanalysis, and creative privilege escalation using a custom SUID binary. While labeled “easy,” the box required thoughtful enumeration and analysis.