# *Pwnkit : CVE-2021-4034*

CVE-2021-4034 (colloquially dubbed "Pwnkit") is a terrifying **L**ocal **P**rivilege **E**scalation (LPE) vulnerability, located in the "Polkit" package installed by default on almost every major distribution of the Linux operating system (as well as many other *nix operating systems). In other words, it affects virtually every mainstream Linux system on the planet.

# *Pwnkit : Background*

This vulnerability exist in “Policy Toolkit” or Polkit in linux systems , allowing an attacker to attain root access over linux machine also called LPE- local privilege escalation .

what is polkit ?

it is a part of linux authorization system , whenever we try to run high privileges tasks , polkit determines whether we have correct set of permissions or not .

it is integrated with systemd and is much more configurable then sudo .

okay , so while interacting with polkit , we have a pkexec utility .

so what vulnerable is , is pkexec utility here .

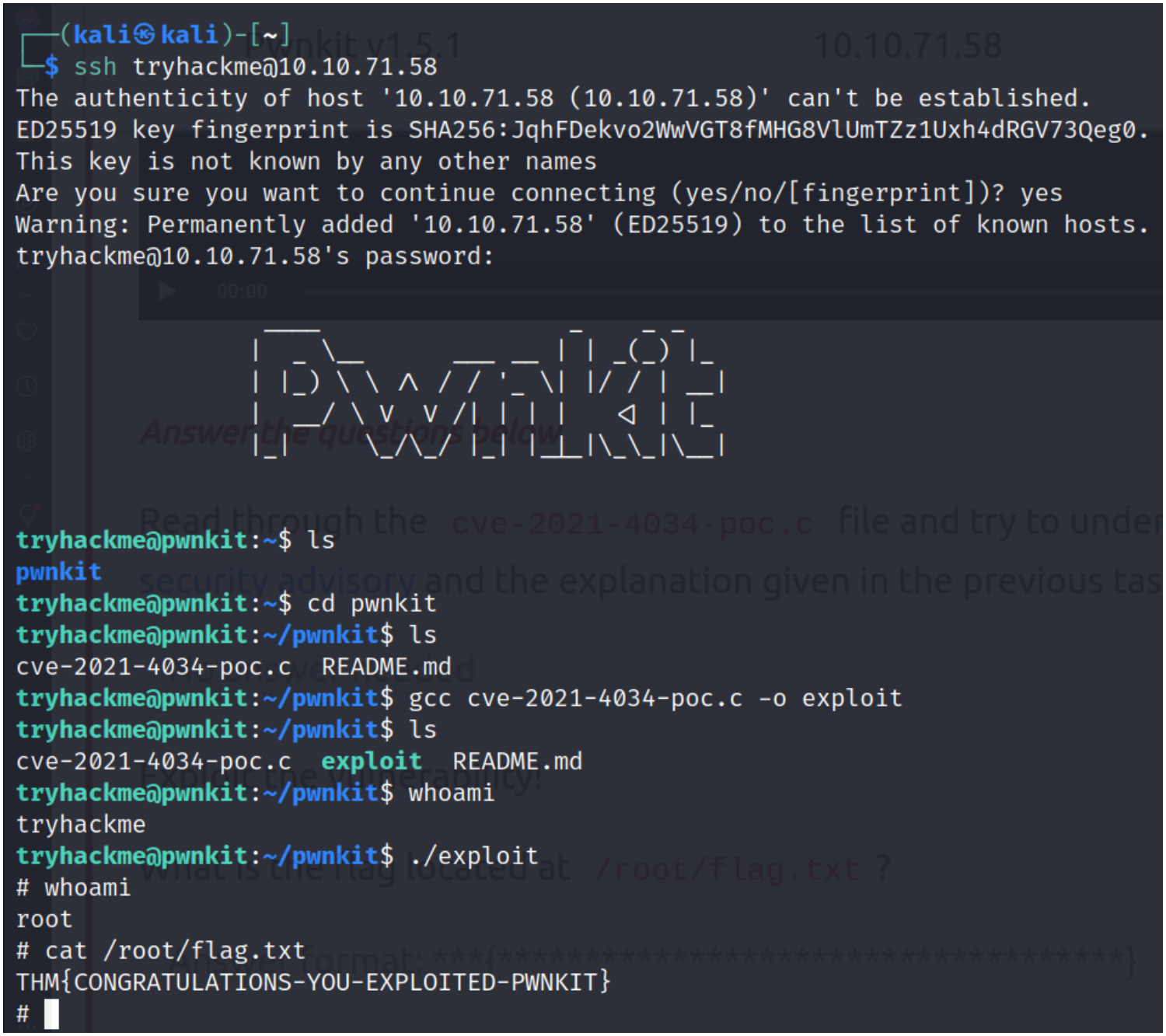
so to simply make it understandable ,  the pkexec utility does not handle command-line arguments safely .

which leads to a out-of-bounds write or memory corruption , which leads to manipulation of environment .

more specifically , when we give a command line argument , it passes through a for-loop starting at an index of 1 and if we pass no arguments , the offset n remains 1 and we bypass the loop and overwriting the next environment variable and giving us root access .

# *Pwnkit : Exploitation*

here is just a simple proof of concept , we will use a pre-written exploit and run it to show that we got root access.




so , first we compiled the binary as “exploit” , then showed that we had user access and as soon as we run the exploit we have root access and flag .

# *Pwnkit : Patch*

In distributions which have not yet released

patched versions of the package, the recommended hotfix is to simply remove the SUID bit from the pkexec binary. This can be done with a command such as the following:

```
tryhackme@pwnkit:~/pwnkit$ ./exploit
# sudo chmod 0755 `which pkexec`
# exit
tryhackme@pwnkit:~/pwnkit$ ./exploit
GLib: Cannot convert message: Could not open converter from “UTF-8” to “PWNKIT”
pkexec must be setuid root
tryhackme@pwnkit:~/pwnkit$
```

now it has been patched successfully .