Polkit

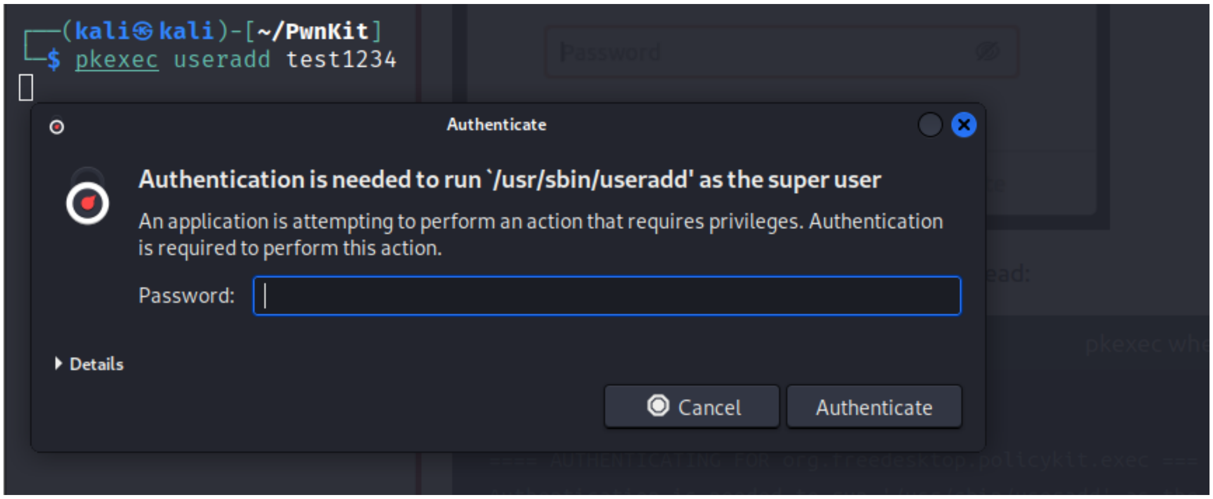
Considering recent events regarding the release of advisory by Qualys regarding the exploitation of Polkit and using it as a privilege escalation vector on major Linux distros, I tried exploiting my own Kali Linux.

Before getting into that, let us see what Polkit is?

Polkit is a part of Linux authorization system which is toolkit used for defining and handling authorization. In simple words, when you want to perform an action which requires higher privileges, it is this toolkit which checks and allows you to perform the action.

When interacting with Polkit we can use the pkexec utility — it is this program that contains the Pwnkit vulnerability.

For example -



```
┌──(kali㉿kali)-[~/PwnKit]
└─$ pkexec useradd test1234
```

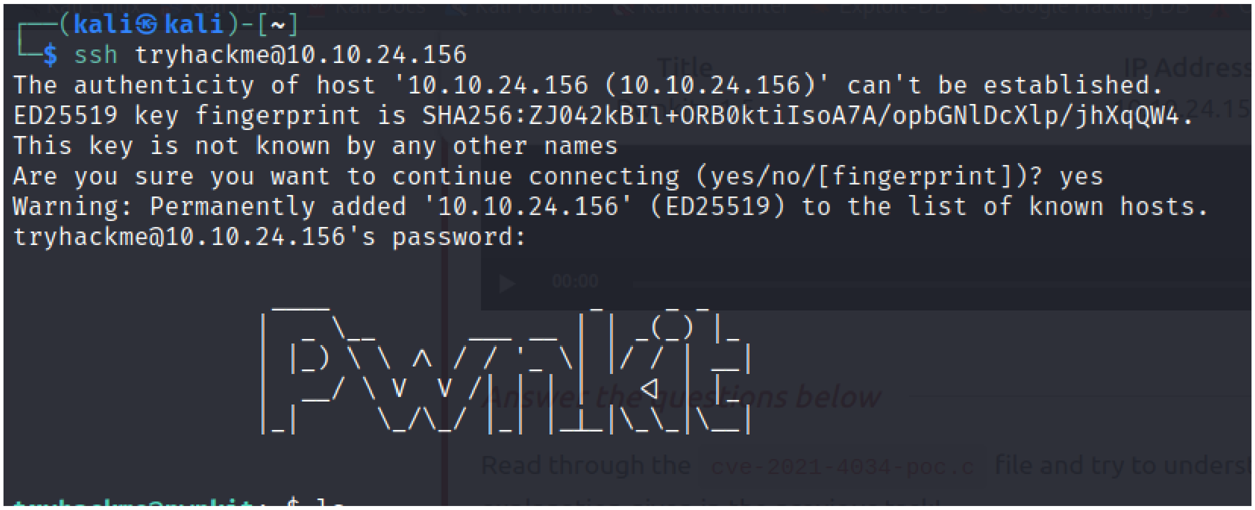
Authenticate

Authentication is needed to run `/usr/sbin/useradd' as the super user

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password:

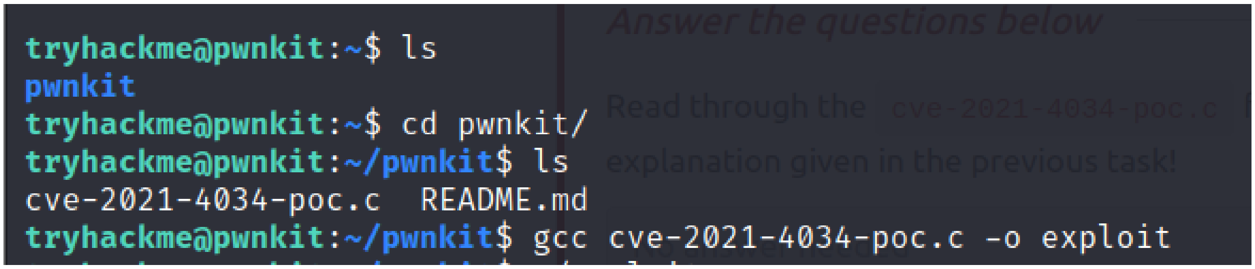
In simpler words, this pkexec command can be used as an alternative to Sudo command.



```
┌──(kali㉿kali)-[~]
└─$ ssh tryhackme@10.10.24.156
The authenticity of host '10.10.24.156 (10.10.24.156)' can't be established.
ED25519 key fingerprint is SHA256:ZJ042kBIl+ORB0ktiIsoA7A/opbGNlDcXlp/jhXqQW4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.24.156' (ED25519) to the list of known hosts.
tryhackme@10.10.24.156's password:

                  ____                 _    _ _
                 |  _ \__      ___ __ | | _(_) |_
                 | |_) \ \ /\ / / '_ \| |/ / | __|
                 |  __/ \ V  V /| | | |   <| | |_
                 |_|     \_/\_/ |_| |_|_|\_\_|\__|


tryhackme@pwnkit:~$ ls
```



```
tryhackme@pwnkit:~$ ls
pwnkit
tryhackme@pwnkit:~$ cd pwnkit/
tryhackme@pwnkit:~/pwnkit$ ls
cve-2021-4034-poc.c  README.md
tryhackme@pwnkit:~/pwnkit$ gcc cve-2021-4034-poc.c -o exploit
```