Vortex Level 2 to Level 3

The executable file 'vortex2' essentially executes the command 'tar cf /tmp/ownership.$$.tar' while taking 3 additional arguments. This command creates a tar file called ownership.$$.tar and throws the 3 file paths that you give it into the tar.

The important part of this command is that it executes as vortex3 with the associated privileges, so it can take any file that vortex3 can access and add the file to the tar. The file that we are hunting for is in /etc/vortex_pass/vortex3. We pass this file as an argument for the vortex2 executable to bundle in the tar. The executable needs 3 files, so we can just give it the same file to bundle in two more times. The command should look like:

a)   /vortex/vortex2 /etc/vortex_pass/vortex3 /etc/vortex_pass/vortex3 /etc/vortex_pass/vortex3

There. Now the password is in a tar file called ownership.$$.tar. Note that bash interprets $$ as the pid of the shell. We need to wrap the file name in single quotes to protect it.

Since the tar is in /tmp, we can access it. Using vim, you can simply type in **vim '/tmp/ownership.$$.tar'** and view the contents of the tar. However, printing to standard output is a little cleaner, so let's just use tar extraction to get the file.

b)   tar xf '/tmp/ownership.$$.tar' --to-stdout

The xf argument tells tar that we are extracting the tar file '/tmp/ownership.$$.tar'. The --to-stdout flag tells tar that we want the contents printed out. Executing command **a** followed by command **b** should give you the password.

Spoiler Alert:

The password is 64ncXTvx#