Vortex 3 -> Vortex 4

Chamaeleon

For this challenge, we use a buffer overflow to inject shellcode into the vortex3 executable that will give effectively give us a shell with level 4 privileges. We decided to use open-source shellcode from https://www.exploit-db.com/shellcode/. The code we wish to inject is only 31 bytes. Our goal is to rewrite one of the redirects in the destructor code so that our shellcode is triggered. We can do this using the lpp variable. If we find the address of the end of the destructor commands list, this should be a piece of cake. Fortunately, we can test the code in our own personal environment and use a debugger to find out exactly the address we need to write. Using a brute force method, we found the location as \x12\x83\x04\x08. Now, we give the vortex3 executable our shellcode to write in our buffer. Then, we use a no-operation byte (0x90) to shift our buffer. The lpp variable is 128 bytes in front of the start of our buffer, so we must write the NOP 128 times minus the length of the shell code plus four to get us in the right position. Finally, we write in the address of the destructor commands so that lpp now stores that address. This will cause our shellcode (which we wrote at the beginning of the buffer) to be executed as part of the destructor commands when exit() is called. This should finally give us the shell we were looking for with level 4 privileges. To implement this method, we make a python script (code in vor3_bytes.py) to write the bytes that we need. Then, we use those bytes as the arguments for the vortex3 executable. Keep in mind that this is an argument, not stdin. This should bring up a shell for us. We then type in “cat /etc/vortex_pass/vortex4” to give us the password.

The password is 2YmgK1=jw