CTF’s General Skills first 10 assignments writeups:

1. Lets Warm Up:
    a. Searched for an ASCII table online.
    b. 0x70 resulted in the letter p.
2. Warmed Up:
    a. To convert 0x3D to decimal
        i. 3(16) = 48
        ii. D = 13
    b. Result: 48 + 13 = 61.
3. 2Warm:
    a. I used an online calculator to get 42 (base 10) to binary.
    b. Result: 101010
4. Obedient Cat:
    a. Downloaded the file flag.txt.
    b. Used “cat flag.txt” to show the output on the terminal and get the flag.
    c. picoCTF{s41n1ty_v3r1f13d_f28ac910}
5. Wave a flag:
    a. Downloaded the file warm.
    b. Tried to execute it using “./warm”, however, it didn’t have executable permissions.
    c. Used “chmod +x warm” to add the permission.
    d. Tried to execute again with the command “./warm -h” and got the flag.
    e. picoCTF{b1scu1ts_4nd_gr4vy_d6969390}
6. Nice netcat…:
    a. Wrote the command “nc mercury.picoctf.net 22342” on the terminal as stated on the problem.
    b. It printed a list of numbers on the console, to decipher the flag I used an online ASCII code converter.
    c. picoCTF{g00d_k1tty!_n1c3_k1tty!_5fb5e51d}
7. Tab, Tab, Attack:
    a. Downloaded the file Addadshashanammu.zip.
    b. Used the command “unzip Addadshashanammu.zip” to extract the files.

c. After extracting the files, I used the command “cd” and the tab key to autocomplete the directories names and navigate through them until I found a file named “fang-of-haynekhtnamet”.
d. I used the command “./fang-of-haynekhtnamet” and got the flag.
e. picoCTF{l3v3l_up!_t4k3_4_r35t!_f3553887}

8. Python Wrangling:
   a. Downloaded the 3 files: ende.py, flag.txt.en and pw.txt
   b. Used “cat pw.txt” to get the password.
   c. Used “python3 ende.py -h” to see if I could get some useful information about the script.
   d. After reading the help section I used “python3 endy.py -d flag.txt.en”, enter the password from pw.txt and got the flag.
   e. picoCTF{4p0110_1n_7h3_h0us3_6008014f}
9. Magikarp Ground Mission:
   a. Launched the instance and typed in the command “ssh ctf-player@venus.picoctf.net -p 54013” and used the password given in the problem to connect.
   b. Then I used the command “ls” to see what folders where available and found 2: 1of3.flag.txt that contained a piece of the flag by using “cat 1of3.flag.txt “and instructions-to-2of3.txt that by using “cat instructions-to-2of3.txt” it mentioned to go the root /.
   c. To continue the command used was “cd /” and then I used “ls” again to see what was available. Two files were important: 2of3.flag.txt and instructions-to-3of3.txt. With “cat 2of3.flag.txt” the second part of the flag was available and with “cat instructions-to-3of3.txt” I was informed to go to the home folder.
   d. Finally, I used “cd” to go back, used “ls” and found 3of3.flag.txt that had the final part of the flag that I got by using “cat 3of3.flag.txt”
   e. picoCTF{xxsh_0ut_0f_\/\/4t3r_1118a9a4}
10. Static ain’t always noise:
   a. Downloaded 2 files: itdis.sh and static.
   b. Tried executing itdis.sh, but didn’t have the permissions so I used “chmod +x itdish.sh”
   c. Tried “./itdish.sh”, however nothing happened so I used “cat itdish.sh” to print out the code and tried to understand how it worked.
   d. After reading I used “./itdish.sh static” and it created a new file named “static.ltdis.strings.txt” with only the strings from static.

e. Finally, I used “grep “pico” static.ltdis.strings.txt” to search for the flag and got it.
f. picoCTF{d15a5m_t34s3r_98d35619}