Week 1 (1/13/23)

General Skills

Obedient Cat: Simply opened the file and copied and pasted the answer which was the only line in the file

Python Wrangling: Opened the picoCTF Webshell, used wget for the Python script and the flag then ran the script with the command: python ende.py -d flag.txt.en then entered the password provided and copied and pasted the flag. Ende.py was the name of the python script, flag.txt.en was the name of the file.

$ man python : gives all the python commands

$ python file\_name : runs a python file or script

Why do you do ende.py -d flag.txt.en instead of ende.py -e flag.txt.en to get the flag? What is the difference between these two commands? Why does it not work with -e but -d instead?

Because when you use help, -h or -help, it tells you to use -d to decrypt the file

1/15/23

Wave a flag:

1. Used wget on the link provided in the picoCTF Webshell
2. Ran the program by entering $ chmod +x warm followed by $ ./warm
3. Enter $ ./warm -h which then gives the flag

What’s a net cat?

1. Entered $ nc url port number to get the flag

Let’s Warm up

1. Use ACII table to convert the hexadecimal to ACII or just use an online converter

Nice netcat…

1. Enter nc url number into shell then convert each number from hexadecimal to ACII to get the flag

1/16/23

Static ain’t always noise

1. Wget the static file and bash script
2. Did $ cat for both static and the script
3. Next did $ strings static to get the flag

1/17/23

### Magikarp Ground Mission

1. Entered ssh ctf-player@venus.picoctf.net -p 56814
2. Entered ls to get directories which gives: 1of3.flag.txt and instructions-to-2of3.txt
3. Entered cat 1of3.flag.txt which gives picoCTF{xxsh\_ (the first part of the flag), cat gives the contents of the file
4. Entered cat instructions-to-2of3.txt which gives Next, go to the root of all things, more succinctly `/`
5. cd .. lets you go back a directory so did that a couple of times which ended up doing nothing
6. Finally, typed cd to go to the home directory then typed ls -a which gave 3of3.flag.txt
7. Entered cat 3of3.flag.txt to get the last part of the flag
8. Entered cd .. then ls -a, twice, to get 2of3.flag.txt
9. Entered cat 2of3.flag.txt to get the middle part of the flag

Key Takeaway:

To move between directories use the cd, to move back one directory do cd .., to go to the home directory use cd. To get a list of all directories use ls -a, this shows all directories so if someone hides something you will see it. Finally, the cat command shows all the contents of a file.

2Warm

1. Used a base 10 to base 2 converter online to convert 42 base 10 to binary base 2

strings it

1. Entered wget with url provided, given strings.1
2. Entered strings strings.1 | grep picoCTF to get flag

Key Takeaway:

Instead of just usings strings you can use grep to filter the otherwise long list of text into specific keywords. Since you know the format of the flag is picoCTF you can filter for picoCTF. To do this do: strings filename | grep keyword

Bases

1. Didn’t know what base was being referred to, looked up solutions, said CTF’s commonly use base of 64
2. Used site to decode base of 64 bDNhcm5fdGgzX3IwcDM1 <https://www.base64decode.org/>

Codebook

1. Download the files in the same directory
2. Run the code.py script with python command to get flag
3. I just ran it but if you open the code with cat you can see the main function prints the flag from the codebook.txt file

convertme.py

1. Download the given file
2. Run the file using python command
3. Convert the given decimal base, 43, to binary base using online converter
4. Input correct answer 101011, to get the flag

fixme1.py

1. Download the given file with wget
2. Use the nano command to edit the code and fix the error (nano fixem1.py), there is an indentation error if you run the file before fixing it with the python command you get and indentation error and the line that is wrong so you could also find the error with that.
3. Run the file with the python command to get the flag once you fix the changes in the code and save it

Key Takeaway:

You can use the nano command to fix errors in code and scripts, to exit nano press control and x simultaneously

1/18/23

Fixme2.py

1. Entered wget to download the python script
2. Entered python to run script to find the error, on line 22
3. Entered nano to fix the error in the script by changing = to ==, saved changes, exit nano
4. Entered python again to run the corrected script and get the flag

Glitch Cat

1. Connect to server using netcat by entering nc url numbers
2. Press control c on keyboard to close connection and return to command prompt
3. Enter python
4. Print the flag string to get the flag in the correct format

Takeaway: Control and d exits out of python, control and c closes connection to server, you can use python to convert ascii to text

HashingJobApp

1. Connect to the server using netcat by entering nc url numbers
2. Use a website to hash the text and input the answer
3. Repeat until you get the flag

<https://www.md5hashgenerator.com/>

PW Crack 1

1. Download the password checker and the encrypted flag
2. Enter cat to view the code of the password checker to get the password
3. Enter python and run the password checker, input the correct password retrieved from previous step to get the flag

PW Crack 2

1. Download the password checker and the encrypted flag with wget
2. Enter cat to view the code of the password checker to get the password
3. The password is in ascii so enter python then print the ascii to convert to text
4. Exit out of python with control and d
5. Enter python to run the level2.py, enter the obtained password to get the flag

PW Crack 3

1. Download the password check, flag, and hash
2. Enter nano to modify code, use a for loop to loop over the list of potential passwords and recursively call the password checker function to get the flag

PW Crack 4

Basically the same as PW Crack 3

PW Crack 5

1. Download the password checker, flag, hash, dictionary
2. Enter nano to change the password checker, comment out the user input and the print line that prints when the password is incorrect (there is going to be too many outputs)
3. Put a with statement to open the dictionary and test each line in the dictionary by recursively calling the function that hashes the password. Also use the strip function for each line to get rid of spaces.
4. An alternative method to the with statement is to open the dictionary with the possible passwords with open function, then create a list of the possible passwords using the readlines method and store in a variable, then create a for loop going over each line in that variable, in the for loop set a variable equal to each line without whitespace using the strip method, finally recursively call the function that checks if the password is correct pass in the line as parameter.

Key Takeaways:

Review PW Crack 5 more closely, never seen the with statement before wondering if there is another way to write it. After looking closely, I found a method that is more in line with what I have learned in class which I detail in step 4.

1/19/23

runme.py

1. Download the python script and run to get the flag

Serpentine

1. Download the python script
2. Enter python to run script, it doesn't print flag
3. Enter nano to fix the script to print flag, in the main call when you press choice b, to print flag, it prints and error message instead of running the print flag method so make the change and save and then exit nano
4. Run the script entering python once again after fixing the script, choose choice b to print the flag

First Find

1. Download the zip file using wget
2. Enter the unzip command to unzip the zip file
3. Locate the file named ‘uber-secret.txt’, enter cat followed by the whole directory for uber-secret.txt to get the flag

Big Zip

1. Download the zip file with wget
2. Unzip the file with the unzip command
3. Search for the flag using grep, to look at every file in a directory and its subdirectories do grep -r search\_term directorypath. In this case it was grep -r picoCTF big-zip-files to get the flag

Based

1. Connect to the server using netcat or the nc command
2. Complete the challenge by decoding the data encodings into words and inputting answers to get a flag. The first was binary, so I used a binary to text converter online, the second was octal and the third was hexadecimal. I also used an online converter for these two.

Plumbing

1. Connect to the server by entering nc, the output is a bunch of useless lines so you have to filter for picoCTF
2. Enter nc url number | grep picoCTF to get the flag

Key Takeaway:

Redirection is where you can make the output of one program the input of another program. You can use pipes, |, to chain commands together in linux so that you can perform more than one command at a time.

1/21/23

Mus1c

1. Download the song
2. Enter cat to view the song
3. Recognize the pattern in the song looks like a coding language use words that come up frequently in the song to search for the name of the language
4. Copy and past the lyrics in an online converter for the language called rockstar
5. The converted output looks like ascii so decode it to find the flag