WRITEUP PICOCTF

1. **Obedient Cat**
   - **Overview**
     Points: 10
     Category: General Skills
   - **Description**
     This file has a flag in plain sight (aka "in-the-clear"). Download flag.
   - **Hints**
     a) Any hints about entering a command into the Terminal (such as the next one), will start with a '$'... everything after the dollar sign will be typed (or copy and pasted) into your Terminal.
     b) To get the file accessible in your shell, enter the following in the Terminal prompt: $ wget https://mercury.picoctf.net/static/2d24d50b4ebed90c704575627f1f57b2/flag
     c) $ man cat
   - **Approach**
     Pertama-tama, saya mendownload file yang disediakan melalui linux shell dengan command pada hints (b). Lalu, berdasarkan hints (c), saya menggunakan command $ cat <nama file> untuk print output flag.
   - **Flag**
     picoCTF{s4n1ty_v3r1f13d_f28ac910}
2. **Python Wrangling**
   - **Overview**
     Points: 10
     Category: General Skills
   - **Description**
     Python scripts are invoked kind of like programs in the Terminal... Can you run this Python script using this password to get the flag?
   - **Hints**
     a) Get the Python script accessible in your shell by entering the following command in the Terminal prompt: $ wget https://mercury.picoctf.net/static/0bf545252b5120845e3b568b9ad0277e/ende.py
     b) $ man python
   - **Approach**
     Pertama-tama, saya mendownload semua file yang disediakan melalui linux shell dengan command pada hints (a). Lalu, saya membuka setiap file tadi dan mendapatkan hasil berupa file python berisi sebuah program terkunci yang dapat mengenkripsi dan mendeskripsi file lain, file password berisi kumpulan karakter yang digunakan untuk membuka kunci program di file python, dan file flag berupa kumpulan karakter yang terlihat acak dan Panjang. File flag ini seperti hasil enskripsi sehingga saya mencoba mendeskripsikannya dengan menggunakan

command $ python <nama file python> -d <nama file flag>. Dan untuk mendeskripsi file flag tersebut perlu input file password.

- **Flag**
  picoCTF{4p0110_1n_7h3_h0us3_6008014f}

3. **Wave A Flag**
   - **Overview**
     Points: 10
     Category: General Skills
   - **Description**
     Can you invoke help flags for a tool or binary? This program has extraordinarily helpful information...
   - **Hints**
     a) This program will only work in the webshell or another Linux computer.
     b) To get the file accessible in your shell, enter the following in the Terminal prompt: $ wget https://mercury.picoctf.net/static/b28b6021d6040b086c2226ebeb913bc2/warm
     c) Run this program by entering the following in the Terminal prompt: $ ./warm, but you'll first have to make it executable with $ chmod +x warm
     d) -h and --help are the most common arguments to give to programs to get more information from them!
     e) Not every program implements help features like -h and --help.
   - **Approach**
     Pertama-tama, saya mendownload semua file yang disediakan melalui linux shell dengan command pada hints (b). Dari hints (c), file tersebut saya jadikan .exe sehingga dapat dijalankan. Ketika dijalankan muncul "*Hello user! Pass me a -h to learn what I can do!*". Lalu saya jalankan kembali dengan command $ ./warm -h dan menampilkan flagnya
   - **Flag**
     picoCTF{b1scu1ts_4nd_gr4vy_d6969390}
4. **What Is A Net Cat**
   - **Overview**
     Points: 100
     Category: General Skills
   - **Description**
     Using netcat (nc) is going to be pretty important. Can you connect to jupiter.challenges.picoctf.org at port 25103 to get the flag?
   - **Hints**
     a) nc tutorial
   - **Approach**
     Pertama-tama, saya membaca tutorial Net Cat seperti pada hint (a). Karena pada deskripsi hanya perlu connect ke port 25103 dari host jupiter.challenges.picoctf.org tanpa ketentuan

lainnya seperti timer ataupun source port maka bisa menggunakan command $ nc jupiter.challenges.picoctf.org 25103 .Lalu keluar output flagnya

- **Flag**
  picoCTF{nEtCat_Mast3ry_d0c64587}

5. **Lets Warm Up**
   - **Overview**
     Points: 50
     Category: General Skills
   - **Description**
     If I told you a word started with 0x70 in hexadecimal, what would it start with in ASCII?
   - **Hints**
     a) Submit your answer in our flag format. For example, if your answer was 'hello', you would submit 'picoCTF{hello}' as the flag.
   - **Approach**
     Pertama-tama, berdasarkan deskripsi, saya harus mengubah hexadecimal dari 0x70 ke sebuah huruf dalam ASCII. Untuk mengubahnya, saya menggunakan website CyberChef (gchq.github.io) sehingga didapatkan huruf ASCII-nya. Lalu, berdasarkan hint (a), huruf tersebut dijadikan sebagai flagnya
   - **Flag**
     picoCTF{p}
6. **Nice Net Cat**
   - **Overview**
     Points: 15
     Category: General Skills
   - **Description**
     There is a nice program that you can talk to by using this command in a shell: $ nc mercury.picoctf.net 22342, but it doesn't speak English...
   - **Hints**
     a) You can practice using netcat with this picoGym problem: what's a netcat?
     b) You can practice reading and writing ASCII with this picoGym problem: Let's Warm Up
   - **Approach**
     Pertama-tama, berdasarkan hint (a), saya langsung menggunakan command : $ nc mercury.picoctf.net 22342. Namun, outputnya berupa kumpulan angka yang terpisah oleh linenya. Berdasarkan hint (b), saya berpikir bahwa output ini berbentuk decimal dan harus diubah menjadi huruf ASCII. Untuk mengubahnya, saya menggunakan website CyberChef (gchq.github.io) dengan menggunakan perintah *From Decimal* dan delimiter berupa line feed sehingga didapatkan huruf ASCII-nya. Kumpulan huruf ini membentuk flag.
   - **Flag**
     picoCTF{g00d_k1tty!_n1c3_k1tty!_5fb5e51d}

7. **Static Ain't Always Noise**
   - **Overview**
     Points: 20
     Category: General Skills
   - **Description**
     Can you look at the data in this binary: static? This BASH script might help!
   - **Hints**
     (None)
   - **Approach**
     Pertama-tama, saya langsung mendownload semua file yang disediakan menggunakan command : $ wget <link>. Setelah itu saya mencoba membuka filenya satu persatu. Pada file *static*, outputnya berupa kumpulan kode yang sulit dibaca. Pada deskripsi diberikan BASH script untuk mempermudah pembacaan file tersebut. BASH script ini bentuk awalnya adalah file biasa. Supaya BASH script dapat dirun, BASH script perlu diubah ke bentuk .exe dengan command $ chmod +x <nama file> dan dirun dengan command $ ./<nama executable>. Ternyata BASH script ini berfungsi untuk disassembly satu file menjadi beberapa file dengan command $ ./<nama executable> <nama file>. Dengan BASH script ini, file static disassembly menjadi tiga file yaitu file awal dan dua file disassembly yangmana satunya berupa kode raw dan satunya lagi berupa string. Flagnya terdapat pada file string ini.
   - **Flag**
     picoCTF{d15a5m_t34s3r_98d35619}

8. **Information**
   - **Overview**
     Points: 10
     Category: Forensics
   - **Description**
     Files can always be changed in a secret way. Can you find the flag? cat.jpg
   - **Hints**
     a) Look at the details of the file
     b) Make sure to submit the flag as picoCTF{XXXXX}
   - **Approach**
     Pertama-tama, saya mendownload file yang disediakan menggunakan command : $ wget <link>. Berdasarkan hint (a), saya harus mencari detail dari file tersebut. Karena filenya merupakan file gambar, saya coba pertama kali menggunakan command $ file <nama file> namun output informasinya belum detail. Kemudian saya mencoba menggunakan $ identify -verbose <nama file> dan output informasinya lebih lengkap dari sebelumnya. Namun, dari informasi ini tidak ada string yang mencurigakan. Karena itu saya mencoba membandingkannya dengan menggunakan command $ exiftool <nama file>. Dan benar saja, ketika dibandingkan, saya melihat ada string yang mencurigakan di bagian lisensi. Saya menggunakan website CyberChef (gchq.github.io) untuh mengubah string tersebut. Dengan menggunakan fungsi *Magic* ternyata string ini terenkripsi menggunakan base64. Dan akhirnya string ini dapat diubah menjadi flag

- **Flag**
  picoCTF{the_m3tadata_1s_modified}

9. **Tab, Tab, Attack**
   - **Overview**
     Points: 20
     Category: General Skills

   - **Description**
     Using tabcomplete in the Terminal will add years to your life, esp. when dealing with long rambling directory structures and filenames: Addadshashanammu.zip

   - **Hints**
     a) After `unzip`ing, this problem can be solved with 11 button-presses...(mostly Tab)...

   - **Approach**
     Pertama-tama, saya mendownload file yang disediakan menggunakan command: $ wget <link>. Kemudian, karena ini berbentuk .zip, maka untuk unzipping file ini dengan command: : $ unzip <file>. Ternyata outputnya berupa directory, sehingga berdasarkan hint (a), saya mencoba menggunakan $ cat <file> yang mana untuk mendapat filenya perlu menggunakan tabs berkali-kali.

   - **Flag**
     picoCTF{l3v3l_up!_t4k3_4_r35t!_f3553887}

10. **Magikarp Ground Mission**
    - **Overview**
      Points: 30
      Category: General Skills

    - **Description**
      Do you know how to move between directories and read files in the shell? Start the container, `ssh` to it, and then `ls` once connected to begin. Login via `ssh` as `ctf-player` with the password, `481e7b14`
      Additional details will be available after launching your challenge instance.

    - **Hints**
      a) Finding a cheatsheet for bash would be really helpful!

    - **Approach**
      Pertama-tama, saya klik tombol launch instance agar muncul detail tambahan. Ternyata detail tambahannya berupa connect ke server ssh : "*ssh ctf-player@venus.picoctf.net -p 60771*". Kemudian saya connect ke ssh dengan command tadi dan menginput password yang ada di deskripsi. Kemudian, saya gunakan command $ ls untuk mengetahui isi dari direktorinya dan ternyata muncul file flag part 1 dan file yang berisi instruksi ke file flag part 2. Instruksinya adalah untuk pindah ke direktori root dengan command $ cd /. Di direktori ini, ada beberapa file diantaranya file flag part 2 dan file yang berisi instruksi ke file flag part 3. Instruksinya adalah untuk pindah ke direktori home dengan command $ cd ~. Di direktori ini terdapat file flag part 3. Kemudian, saya menyatikan semua file flag sehingga muncul flagnya.

    - **Flag**

picoCTF{xxsh_0ut_0f_\/\/4t3r_ 1118a9a4}

11. **Warmed Up**
    - **Overview**
      Points: 50
      Category: General Skills
    - **Description**
      What is 0x3D (base 16) in decimal (base 10)?
    - **Hints**
      a) Submit your answer in our flag format. For example, if your answer was '22', you would submit 'picoCTF{22}' as the flag.
    - **Approach**
      Pertama-tama, pada deskripsi, 0x3D merupakan HexaDecimal dan saya menggunakan CyberChef (gchq.github.io) untuk mengubahnya ke decimal. Saya menggunakan perintah from Hex dan to Decimal. Dan berdasarkan hint (a), hasilnya berupa angka dan saya ubah ke format tersebut.
    - **Flag**
      picoCTF{61}

12. **2Warm**
    - **Overview**
      Points: 50
      Category: General Skills
    - **Description**
      Can you convert the number 42 (base 10) to binary (base 2)?
    - **Hints**
      a) Submit your answer in our competition's flag format. For example, if your answer was '11111', you would submit 'picoCTF{11111}' as the flag.
    - **Approach**
      Pertama-tama, pada deskripsi, 42 merupakan Decimal dan saya menggunakan CyberChef (gchq.github.io) untuk mengubahnya ke biner. Saya menggunakan perintah from Decimal dan to Binary. Dan berdasarkan hint (a), hasilnya berupa biner dan saya ubah ke format tersebut
    - **Flag**
      picoCTF{101010}

13. **Strings It**
    - **Overview**
      Points: 100
      Category: General Skills
    - **Description**
      Can you find the flag in file without running it?

- **Hints**
  a) strings

- **Approach**
  Pertama-tama, saya mendownload file yang disediakan menggunakan command: $ wget <link>. Kemudian, karena pada deskripsi filenya tidak perlu dirun, maka agar file menjadi readable, saya menggunakan command: $ strings <file>. Namun, ternyata outputnya masih sulit terbaca, maka sekaligus menggunakan command grep: : $ strings <file> | grep -i "picoCTF" karena grep ini akan mencari kata "picoCTF" dari dalam file. Outputnya berupa flag.

- **Flag**
  picoCTF{5tRIng5_1T_d66c7bb7}

14. Bases

- **Overview**
  Points: 100
  Category: General Skills

- **Description**
  What does this bDNhcm5fdGgzX3IwcDM1 mean? I think it has something to do with bases.

- **Hints**
  a) Submit your answer in our flag format. For example, if your answer was 'hello', you would submit 'picoCTF{hello}' as the flag.

- **Approach**
  Pertama-tama, berdasarkan deskripsi, saya harus mengubah kode diatas yang merupakan base64 menjadi karakter rawnya. Untuk mengubahnya, saya menggunakan website CyberChef (gchq.github.io) sehingga didapatkan karakter rawnya. Lalu, berdasarkan hint (a), huruf tersebut dijadikan sebagai flagnya

- **Flag**
  picoCTF{l3arn_th3_r0p35}

15. First Grep

- **Overview**
  Points: 100
  Category: General Skills

- **Description**
  Can you find the flag in file? This would be really tedious to look through manually, something tells me there is a better way.

- **Hints**
  a) Submit your answer in our flag format. For example, if your answer was 'hello', you would submit 'picoCTF{hello}' as the flag.

- **Approach**
  Pertama-tama, saya mendownload file yang disediakan menggunakan command: $ wget <link>. Kemudian, ketika saya coba read filenya ternyata outputnya sulit dibaca. Berdasarkan

hint (a), dengan menggunakan command $ grep -i “kata kunci” <file>, saya lebih mudah mencari flagnya dengan mengganti kata kunci menjadi “picoCTF”. Tambahan -i agar pencariannya bebas dari huruf sensitive. Outputnya berupa flag.

- **Flag**
  picoCTF{grep_is_good_to_find_things_f77e0797}

16. Code Book

- **Overview**
  Points: 100
  Category: General Skills, Python, Shell

- **Description**
  Run the Python script code.py in the same directory as codebook.txt.

  - Download code.py
  - Download codebook.txt

- **Hints**
  a) On the webshell, use ls to see if both files are in the directory you are in
  b) The str_xor function does not need to be reverse engineered for this challenge.

- **Approach**
  Pertama-tama, saya mendownload file yang disediakan menggunakan command: $ wget <link>. Kemudian, saya coba read file .txt ternyata outputnya hanya berupa kode acak. Kemudian, saya coba read file .py yang ternyata jika dirun dapat print flagnya. Namun, file .py ini memberikan syarat jika ingin print flag maka file .txt harus berada di direktori yang sama. Untuk mengecek hal itu, saya menggunakan command: $ ls. Dan ternyata file .py sudah berada di direktori yang sama dengan file .txt. Karena itu saya bisa run file. .py dengan command $ python <nama file>.

- **Flag**
  picoCTF{c0d3b00k_455157_197a982c }

17. Convertme.py

- **Overview**
  Points: 100
  Category: General Skills, Python, Base

- **Description**
  Run the Python script and convert the given number from decimal to binary to get the flag.
  Download Python script

- **Hints**
  a) Look up a decimal to binary number conversion app on the web or use your computer's calculator!
  b) The str_xor function does not need to be reverse engineered for this challenge.
  c) If you have Python on your computer, you can download the script normally and run it. Otherwise, use the wget command in the webshell.

d) To use wget in the webshell, first right click on the download link and select 'Copy Link' or 'Copy Link Address'
e) Type everything after the dollar sign in the webshell: $ wget , then paste the link after the space after wget and press enter. This will download the script for you in the webshell so you can run it!
f) Finally, to run the script, type everything after the dollar sign and then press enter: $ python3 convertme.py

- **Approach**
  Pertama-tama, saya mendownload file yang disediakan menggunakan command: $ wget <link>. Kemudian, berdasarkan hint (f), saya run file .py dan outputnya adalah "*If 43 is in decimal base, what is it in binary base?"*. Dan dibawahnya berupa inputan user untuk jawabannya. Saya pun input "*101011*". Kemudian muncul flagnya.

- **Flag**
  picoCTF{4ll_y0ur_b4535_9c3b7d4d}

18. Fixme1.py

- **Overview**
  Points: 100
  Category: General Skills, Python,

- **Description**
  Fix the syntax error in this Python script to print the flag. Download Python script

- **Hints**
  a) Indentation is very meaningful in Python
  b) To view the file in the webshell, do: $ nano fixme1.py
  c) To exit nano, press Ctrl and x and follow the on-screen prompts.
  d) To use wget in the webshell, first right click on the download link and select 'Copy Link' or 'Copy Link Address'
  e) The str_xor function does not need to be reverse engineered for this challenge.
- **Approach**
  Pertama-tama, saya mendownload file yang disediakan menggunakan command: $ wget <link>. Kemudian, saya coba run filenya dan ternyata filenya ada error berupa "*IndentationError: unexpected indent*" yang artinya ada kesalahan indentasi di line tertentu, seperti pada hint (a). Kemudian, berdasarkan hint (b), saya mengedit file .py dengan command: $ nano <nama_file>. Pada line yang terdapat error tersebut, seharusnya tidak boleh ada indentasi karena bukan bagian dari fungsi. Setelah disave, saya run lagi dan outputnya adalah flag.

- **Flag**
  picoCTF{1nd3nt1ty_cr1515_182342f7}

19. Fixme2.py

- **Overview**
  Points: 100
  Category: General Skills, Python,

- **Description**

Fix the syntax error in this Python script to print the flag. Download Python script

- **Hints**
  f) Are equality and assignment the same symbol?
  g) To view the file in the webshell, do: $ nano fixme1.py
  h) To exit nano, press Ctrl and x and follow the on-screen prompts.
  i) The str_xor function does not need to be reverse engineered for this challenge.
- **Approach**
  Pertama-tama, saya mendownload file yang disediakan menggunakan command: $ wget <link>. Kemudian, saya coba run filenya dan ternyata filenya ada error berupa "*SyntaxError: invalid syntax. Maybe you meant '==' or ':=' instead of '= ' ?*". Kemudian, berdasarkan hint (b), saya mengedit file .py dengan command: $ nano <nama_file>. Pada line yang salah tadi seharusnya menggunakan *equality operand*, bukan *assignment operand* karena if harus membandikan case, seperti pada hint (a). Setelah disave, saya run lagi dan outputnya adalah flag.

- **Flag**
  picoCTF{3qu4l1ty_n0t_4551gnm3nt_e8814d03}

20.