

1. Obedient Cat:

- cd Downloads
- copy link đề cho
- wget + paste link vào
- ls xem tên file
- dùng cat để đọc file vừa tải => done

2. Python Wrangling:

- cd Downloads
- copy 3 link đề cho
- wget + paste 3 link đó
- ls xem tên 3 file
- cat hoặc less xem từng file một
- ý tưởng là dùng file python để giải mã file flag bằng cách dùng lệnh:
`python <tên_file_python> -d <tên_file_flag>`
- sau đó nhập mật khẩu và chờ sẽ hiện => done

3. Wave a flag:

- cd Downloads
- copy link rồi wget, ls xem tên file

Cách 1:

- Tìm kiếm thử xem trong file có cờ “picoCTF” không
- Tìm bằng 2 cách:
 - + dùng grep: `grep -a “picoCTF” <tên_file>`
 - + dùng strings: `strings <tên_file> | grep “picoCTF”`

Cách 2:

- cat thử thì thấy warm là file nhị phân
- chạy thử warm bằng cú pháp `./warm` thì nó bắt quyền truy cập
- do đó dùng `chmod +x warm` để cấp quyền thực thi cho warm
- sau đó làm theo hướng dẫn, nhập `./warm -h` thì tìm được cờ

4. Nice netcat

- netcat (nc): một tiện ích mạng cho phép thực hiện nhiều tác vụ liên quan đến mạng: kết nối, truyền dữ liệu,...
- copy nguyên lệnh nc của đề bài paste vào terminal
- một danh sách các số hiện ra
- để ý thấy giá trị các số đều ≤ 125 (đối với hệ 10) nên phải nghĩ đến mã ASCII
- chuyển dãy số này từ hệ 10 sang mã ASCII, mã đó là cờ => done

5. Static ain't always noise

- Tải 2 file về

Cách 1:

- cat thử 2 file xem tìm dc cờ không => có cờ ở file static

Cách 2:

- do static là file nhị phân nên muốn đọc được full nội dung phải cần đến file bash script
- chạy thử file bash script bằng cú pháp ./ltdis.sh thì cần quyền truy cập
- cấp quyền truy cập bằng cú pháp chmod +x ltdis.sh
- chạy lại ./ltdis.sh
- có gợi ý là ltdis.sh <program_file>
- chạy ./ltdis.sh static thì hiện thêm 2 file .txt nữa
- cat thử 2 file thì tìm đc cờ

6. Tab, Tab, Attack

- Tải file zip về
- unzip <tên_file>
- cd đến thư mục chứa file cuối cùng (là cái thứ 2 tính từ dưới lên)
- file cuối chứa cờ thì dùng cat để đọc

7. Magikarp Ground Mission

- ssh (secure shell): giao thức mạng dùng để kết nối 2 máy tính từ xa
- mục đích là dùng ssh để kết nối và điều khiển máy chủ, thực hiện các thao tác để lấy cờ.

- ssh ctf-player@venus.picoctf.net -p 58179 có nghĩa là:
kết nối đến máy chủ venus.picoctf.net với tên user là ctf-player và cổng 58179

tùy chọn -p 58179 là chỉ định cổng 58179 thay vì cổng mặc định là 22

- sau khi kết nối xong, hiện ra ctf-player@pico-chall\$, tức là người dùng ctf-player đang tương tác với máy chủ pico-chall, \$ là dấu nhắc lệnh. Chúng ta đang làm việc trên máy chủ pico-chall với quyền của người dùng ctf-player.
- Dùng ls để liệt kê các file và đọc từng file để tìm cờ.

8. Let's warm up, Warmed up, 2Warm (làm tương tự)

Dịch mã đề yêu cầu ra rồi viết theo form “picoCTF{mã_dịch_được}”

9. What's a netcat

- Dùng netcat để kết nối với web bằng cổng đề cho
- nc <tên_web> <số cổng>

10. strings it

- Dùng strings tìm cụm pico hoặc picoCTF trong file tải về

11. Bases:

- Dịch mã đề cho ra mã ASCII, submit picoCTF<mã đã dịch>

12. First grep:

- Dùng grep tìm cụm pico hoặc picoCTF trong file tải về

13. Codebook

Chạy file python bằng lệnh python <tên file python> là tìm được cờ

14. convertme.py

- Tải file python về rồi chạy bằng lệnh python <tên file python>, làm theo yêu cầu để lấy cờ

15. fixme1.py, fixme2.py

- python <tên file> để xem file python lỗi ở đâu
- sau đó dùng nano <tên file> để fix lỗi
- chạy lại python <tên file> thì tìm đc cờ

16. Glitch Cat

- netcat theo đề bài thì thấy cờ nhưng chưa đúng form
- gõ python rồi enter
- cop mã hex rồi enter là ra được phần thông tin cờ phía sau

17. HashingJobApp

- netcat theo đề bài rồi dịch từng từ đề bài cho ra mã hash (dùng web md5 hash)

18. PW Crack 1

- cat để đọc file python tìm pass
- lấy cờ có 2 cách:
 - + python <tên file python> rồi nhập mật khẩu
 - + python <tên file python> -d <tên file text> rồi nhập mật khẩu

19. PW Crack 2

- cat để đọc file python tìm pass
- lấy cờ có 2 cách:
 - + python <tên file python> rồi nhập mật khẩu
 - + python <tên file python> -d <tên file text> rồi nhập mật khẩu

20. PW Crack 3, 4 (làm giống nhau)

Có 3 file:

File python chứa đoạn mã để thực hiện lấy cờ

File cờ đã được mã hóa

File hash bin chứa mật khẩu đúng đã được mã hóa

Nhiệm vụ là tìm mật khẩu đúng trong bộ gồm 7 mật khẩu đã cho bằng đoạn mã python cho sẵn. Nếu gặp đúng mật khẩu thì cờ sẽ hiện.

Sửa lại code:

Làm 1 vòng for duyệt hết các mật khẩu trong danh sách đã cho, nếu gặp đúng mật khẩu thì tìm đc cờ.

The screenshot shows the PyCharm IDE interface for a project named 'PW Cracking 5'. The file explorer on the left shows a directory structure with files like dictionary.txt, level3.flag.txt.enc, level3.hash.bin, level3.py, level5.flag.txt.enc, level5.hash.bin, and level5.py. The main editor window displays the code for level3.py. The code defines a function level_3_pw_check that takes user_pw as input, hashes it, and compares it to a correct hash. It also includes a list of possible passwords and a loop to check each one. The code is as follows:

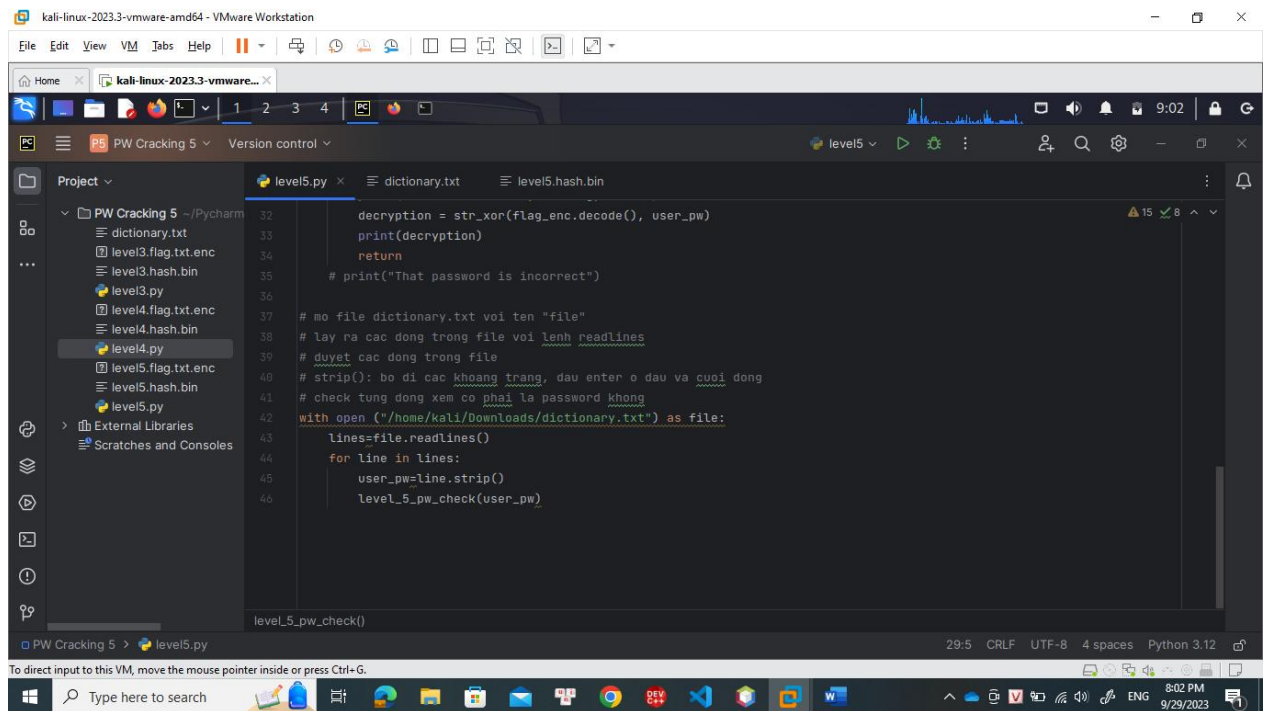
```
1 usage
26 def level_3_pw_check(user_pw):
27     # user_pw = input("Please enter correct password for flag: ")
28     user_pw_hash = hash_pw(user_pw)
29
30
31     if (user_pw_hash == correct_pw_hash):
32         print("Welcome back... your flag, user:")
33         decryption = str_xor(flag_enc.decode(), user_pw)
34         print(decryption)
35         return
36     # print("That password is incorrect")
37
38 pos_pw_list = ["8799", "d3ab", "1ea2", "acaf", "2295", "a9de", "6f3d"]
39
40 for user_pw in pos_pw_list:
41     level_3_pw_check(user_pw)
42
43 # The strings below are 7 possibilities for the correct password.
44 hash_pw()
```

21.PW Crack 5:

Làm tương tự pw crack 3, 4. Nhưng thay vì đọc từ 1 mảng cho trước thì bài này đọc từ file.

The screenshot shows the PyCharm IDE interface for the same project. The file explorer on the left shows the directory structure, including level5.py. The main editor window displays the code for level5.py. The code defines a function level_5_pw_check that takes user_pw as input, hashes it, and compares it to a correct hash. It also includes a list of possible passwords and a loop to check each one. The code is as follows:

```
1 usage
26 def level_5_pw_check(user_pw):
27     # user_pw = input("Please enter correct password for flag: ")
28     user_pw_hash = hash_pw(user_pw)
29
30
31     if (user_pw_hash == correct_pw_hash):
32         print("Welcome back... your flag, user:")
33         decryption = str_xor(flag_enc.decode(), user_pw)
34         print(decryption)
35         return
36     # print("That password is incorrect")
37
38 # mở file dictionary.txt với tên "file"
39 # lấy ra các dòng trong file với lệnh readlines
40 # duyệt các dòng trong file
41 # strip(): bỏ đi các khoảng trắng, dấu enter ở đầu và cuối dòng
42 # check từng dòng xem có phải là password không
43 with open ("/home/kali/Downloads/dictionary.txt") as file:
44     level_5_pw_check()
```



22. runme.py

tải file về rồi pyhon <tên file> lấy cò

23. Serpentine:

Trong code đề cho có hàm `print_flag()` nhưng không được gọi

Do đó có thể gọi nó trong các lựa chọn 'a' 'b' 'c' hoặc gọi ở cuối chương trình bằng cách xóa đi `main()` và ghi `print_flag()`

24. First Find, Big Zip (làm tương tự)

`grep -r "pico"` để tìm cò trong các thư mục và file.

Tùy chọn `-r` để tìm đệ quy toàn bộ cây thư mục, bao gồm thư mục con và tập tin bên trong.

25. Chrono:

- Tự động hóa các tác vụ trong thời gian cụ thể trên linux: dùng crontab (nằm trong `etc` – thư mục chứa các tệp tin cấu hình cho hệ thống và ứng dụng).
- ssh đến trang web đề cho với user picoplayer:

`ssh <tên user>@<tên web> -p <port>`

- đọc crontab từ thư mục `etc`:

`cat /etc/crontab`

26. money-ware:

- Tra google tên phần mềm độc hại bằng địa chỉ mà đề cung cấp, kết quả là Petya.
- Petya là một phần mềm nhắm vào hệ điều hành windows, tấn công vào hệ thống khởi động. Khi hệ thống nhiễm Petya, nó sẽ hiện thông báo đòi tiền chuộc bằng Bitcoin để nhận được key giải mã.

27. Permissions

ssh đến server và công đã cho, thử liệt kê xem trong root có file nào không thì bị chặn

```

(kali@kali)-[/dev]
└─$ cd ~

(kali@kali)-[~]
└─$ em admin has pr
exit(em: command not found)

(kali@kali)-[~]
└─$ ssh -p 56186 picoplayer@saturn.picoctf.net
The authenticity of host '[saturn.picoctf.net]:56186 ([13.59.203.175]:56186)' can't be established.
ED25519 key fingerprint is SHA256:HKm/BwIC+mhj23v08tXULrgLFYvzP6gQH2IwGU1QTok.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:7: [hashed name]
  ~/.ssh/known_hosts:9: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[saturn.picoctf.net]:56186' (ED25519) to the list of known hosts.
picoplayer@saturn.picoctf.net's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.19.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

picoplayer@challenge:~$ ls /root
ls: cannot open directory '/root': Permission denied
picoplayer@challenge:~$

```

Thử thêm sudo vào trước ls vẫn không đc

```

Warning: Permanently added '[saturn.picoctf.net]:56186' (ED25519) to the list of known hosts.
picoplayer@saturn.picoctf.net's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.19.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

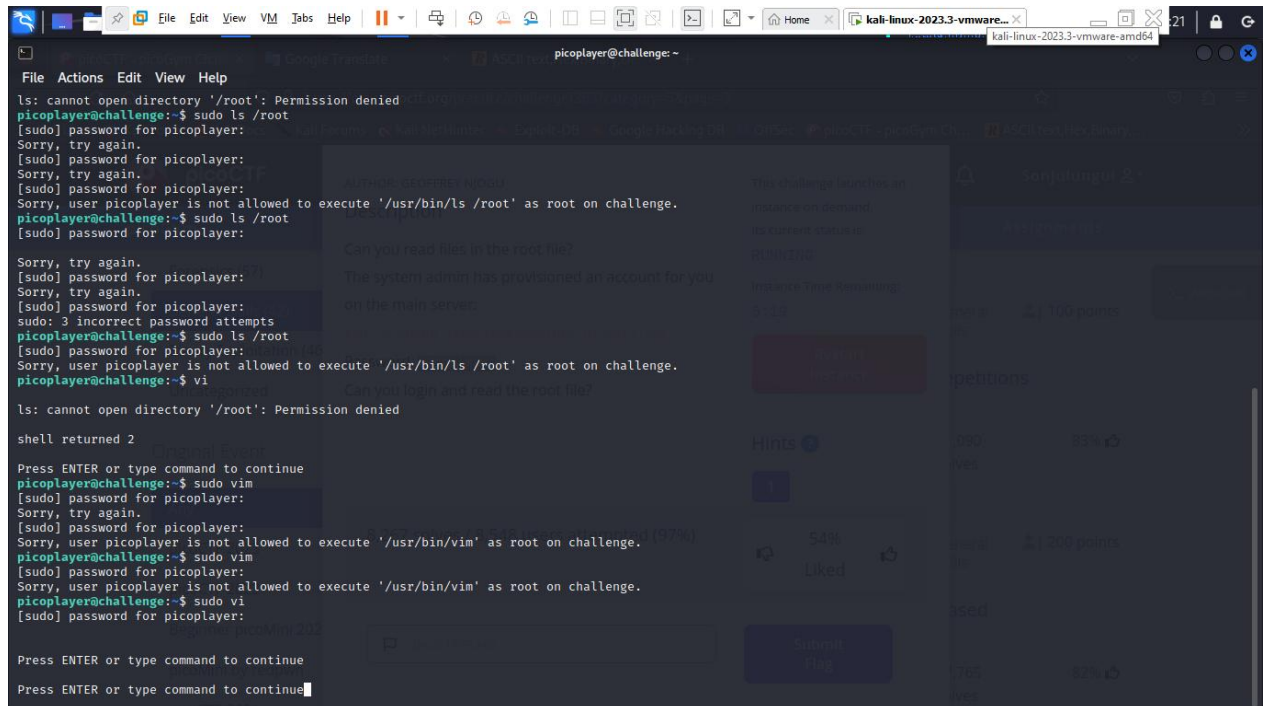
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

picoplayer@challenge:~$ ls /root
ls: cannot open directory '/root': Permission denied
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/ls /root' as root on challenge.
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
sudo: 3 incorrect password attempts
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/ls /root' as root on challenge.
picoplayer@challenge:~$

```

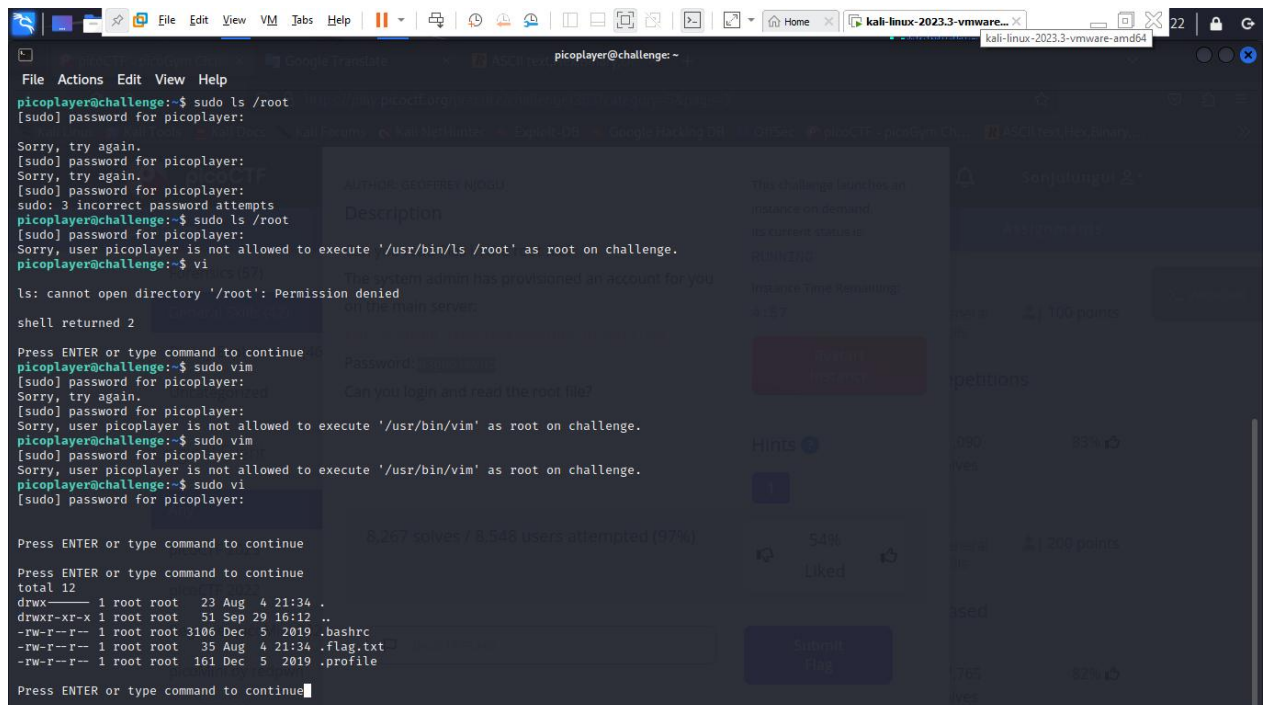

Dùng “sudo vi” đọc file: gõ “sudo vi” rồi enter

Nhập “:! ls /root” để đọc các file trong root, kết quả là không thấy gì cả
=> có file ẩn.



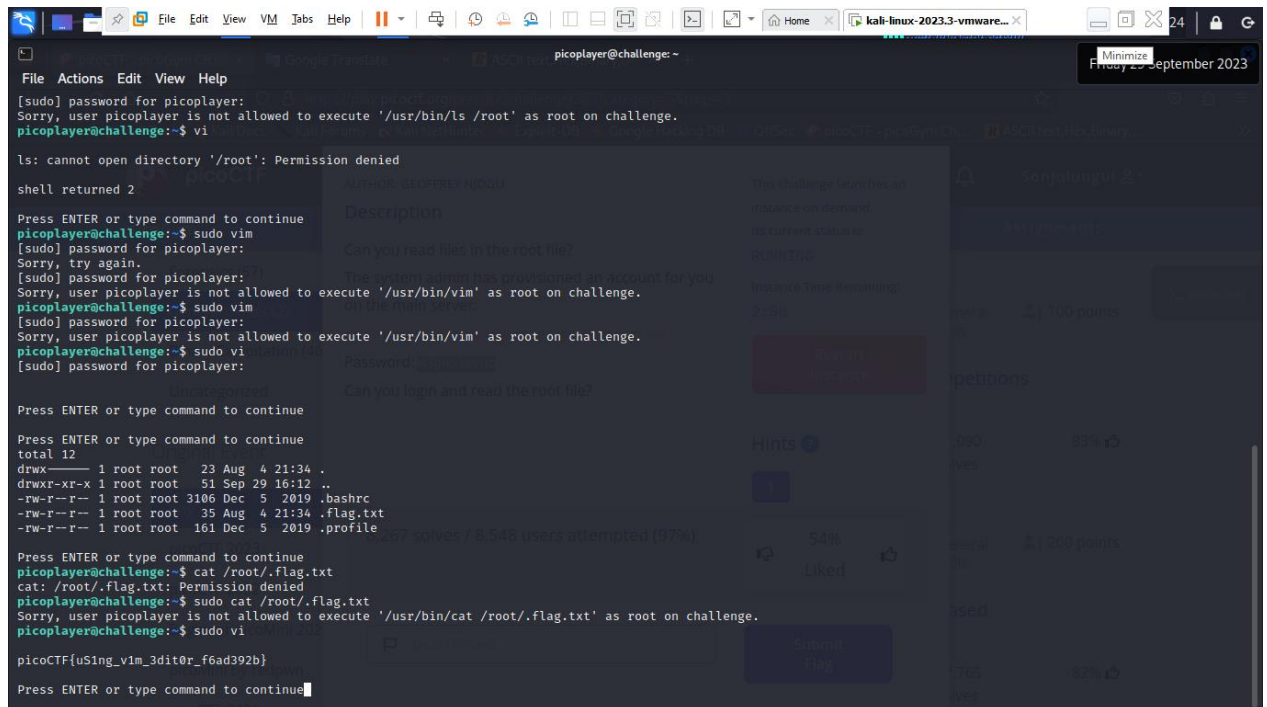
```
File Actions Edit View Help
picoplayer@challenge: ~
ls: cannot open directory '/root': Permission denied
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/ls /root' as root on challenge.
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
sudo: 3 incorrect password attempts
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/ls /root' as root on challenge.
picoplayer@challenge:~$ vi
ls: cannot open directory '/root': Permission denied
shell returned 2
Press ENTER or type command to continue
picoplayer@challenge:~$ sudo vim
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:~$ sudo vim
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:~$ sudo vi
[sudo] password for picoplayer:
Press ENTER or type command to continue
Press ENTER or type command to continue
```

Nhập “:! ls -la /root” liệt kê các file ẩn => thấy có file .flag.txt



```
File Actions Edit View Help
picoplayer@challenge: ~
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
sudo: 3 incorrect password attempts
picoplayer@challenge:~$ sudo ls /root
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/ls /root' as root on challenge.
picoplayer@challenge:~$ vi
ls: cannot open directory '/root': Permission denied
shell returned 2
Press ENTER or type command to continue
picoplayer@challenge:~$ sudo vim
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:~$ sudo vim
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:~$ sudo vi
[sudo] password for picoplayer:
Press ENTER or type command to continue
Press ENTER or type command to continue
total 12
drwxr-xr-x 1 root root 23 Aug 4 21:34 .
drwxr-xr-x 1 root root 51 Sep 29 16:12 ..
-rw-r--r-- 1 root root 3106 Dec 5 2019 .bashrc
-rw-r--r-- 1 root root 35 Aug 4 21:34 .flag.txt
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
```

Vẫn trong sudo vi, nhập “:! cat /root/.flag.txt” để đọc nội dung file cờ.



```
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/ls /root' as root on challenge.
picoplayer@challenge:~$ vi

ls: cannot open directory '/root': Permission denied
shell returned 2

Press ENTER or type command to continue
picoplayer@challenge:~$ sudo vim
[sudo] password for picoplayer:
Sorry, try again.
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:~$ sudo vim
[sudo] password for picoplayer:
Sorry, user picoplayer is not allowed to execute '/usr/bin/vim' as root on challenge.
picoplayer@challenge:~$ sudo vi
[sudo] password for picoplayer:
Press ENTER or type command to continue

Press ENTER or type command to continue
total 12
drwx----- 1 root root 23 Aug 4 21:34 .
drwxr-xr-x 1 root root 51 Sep 29 16:12 ..
-rw-r--r-- 1 root root 3106 Dec 5 2019 .bashrc
-rw-r--r-- 1 root root 35 Aug 4 21:34 .flag.txt
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile

Press ENTER or type command to continue
picoplayer@challenge:~$ cat /root/.flag.txt
cat: /root/.flag.txt: Permission denied
picoplayer@challenge:~$ sudo cat /root/.flag.txt
Sorry, user picoplayer is not allowed to execute '/usr/bin/cat /root/.flag.txt' as root on challenge.
picoplayer@challenge:~$ sudo vi
picoCTF{uSing_vim_3dit0r_f6ad392b}

Press ENTER or type command to continue
```

28. repetitions

- Tải về cat file thì thấy nội dung kết thúc bằng dấu “==” => khả năng là base64
- Giải mã file đó bằng lệnh giải mã của base64
base64 -d <tên file>
- Giải mã 1 lần vẫn chưa ra => giải mã tiếp đến khi nào ra thì thôi :v
- base64 -d <tên file> | base64 -d
vẫn chưa ra => giải mã tiếp
- base64 -d <tên file> | base64 -d | base64 -d
- tiếp tục đến khi tìm được cờ

29. useless

- ssh đến server theo đề bài yêu cầu
- ls
- thấy file useless => cat xem nội dung
- gõ man useless thì thấy cờ

30. ascii number

chuyển mã hex sang ascii

31. Based:

- Chuyển đổi các cơ số sang mã ASCII
- Do có 1 số cơ số lạ v1 (không biết là hệ 10 hay hệ 8, etc..) nên dùng CyberChef.
- Cop số vào input của cyberchef và di chuột vào cây đĩa thần ở cạnh output, chữ sẽ hiện lên :v

- Ghi chữ thấy được vào terminal và làm cho đến khi lấy được cờ.

32. plumbing

- netcat đến địa chỉ đề cho thì thấy hiện ra thông báo đây không phải cách tìm cờ.
- do đó dùng pipe |
- nc <địa chỉ> <số cổng> | grep "pico"

⇒ tìm đc cờ.

33. music

- Bài hát đề cho được viết theo 1 ngôn ngữ tên "rockstar"
- Lên google gõ rockstar language rồi vào phần try it
- Cop bài hát vào rồi "Rock"
- Output là 1 dãy các số => chuyển các số đó sang ASCII rồi nộp cờ.

34. flag_shop

- ý tưởng là chọn number_flag sao cho total_cost tràn kiểu int và trở thành số âm.
- do total_cost=number_flag*900 mà kiểu int là 2,147,483,647 nên đem 2,147,483,647 chia cho 900 thì được phạm số cần thiết để tràn là > 2386092
- thử 2386093 và 2386094 không được, 2386095 trở lên thì được

35. Special

- ssh đến server và số cổng đề cho
- viết 1 số lệnh bình thường như ls, clear... thì thấy bị đánh lỗi chính tả
- thử gõ 2 lệnh liên: Cat & clear
- Thử gõ Cat & find. thì thấy hiện file flag
- Gõ tiếp Cat & cat blargh/flag.txt

36.1_wanna_b3_a_r0ck5tar

- Chạy sudo cài đặt trình chuyển đổi rockstar thành python:
sudo pip install rockstar-py
- Chạy lệnh rockstar-py -i lyrics.txt thì trong Downloads hiện thêm file output.py
- python output.py thì thấy hiện các chữ số đáng ngờ: Tommy = 66 Music = 79 Jamming = 78 Tommy = 74 Rock = 86 Tommy = 73
- sắp xếp lại thì được: 66 79 78 74 86 73
- dịch ra mã ascii thì được cụm BONJVI, nộp lên là picoCTF{BONJVI} thì sai
- để ý trong code thấy có 1 dòng là "They are dazzled audiences" rồi mới in đến Rock = 86
- vậy thì dòng đầy khả năng là music 79 => thêm chữ O thành cụm BONJOVI => done

37. Specialer

- ssh đến web với địa chỉ cổng đề cho
- thử dùng các lệnh xem có được không => không dùng được cat, ls... và dùng được echo
- tra mạng xem có cách nào in ra nội dung file bằng echo không thì có và cú pháp là:
echo "\$(<tên đường dẫn/file)"
- dùng echo liệt kê các file/thư mục
echo *
- dùng thử cách trên đọc nhưng không được
- khả năng những thứ vừa liệt kê là thư mục => dùng tiếp
echo */*
- đọc file bằng cách trên

```

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.3-vmware... x
kali@kali: ~
File Actions Edit View Help
Specialer$ cat
-bash: cat: command not found
Specialer$ echo "$(cat abra)"
-bash: cat: command not found

Specialer$ echo "$(<abra>)"
> ^C
Specialer$ echo "$(<abra>)"
(<abra>)
Specialer$ echo "$(<abra>)"
(<abra>)
Specialer$ echo "$(<abra>)"
(<abra>)
Specialer$ echo "$(<abra>)"
-bash: command substitution: line 12: syntax error near unexpected token `)'
-bash: command substitution: line 12: `<abra>)"'
Specialer$ echo "$(<abra>)"
(<abra>)

Specialer$ echo "$(<abra/cadabra.txt>)"ng (70)
(<abra/cadabra.txt>)
Specialer$ echo "$(<abra>)"
(<abra>)

Specialer$ echo "$(<abra/cadabra.txt>)"
Nothing up my sleeve!
Specialer$ echo "$(<abra/cadaniel.txt>)"
Yes, I did it! I really did it! I'm a true wizard!
Specialer$ echo "$(<cala/kazam.txt>)"
return 0 picoCTF{y0u_d0n7_4ppr3c1473_wh47_w3r3_d01ng_h3r3_38f5cc78}
Specialer$ Connection to saturn.picoctf.net closed by remote host.
Connection to saturn.picoctf.net closed.

kali@kali: ~

```

⇒ dùng echo để liệt kê các đường dẫn

echo */** (cứ */* đến khi nào tới giới hạn thì thôi)

Ví dụ: nếu các thư mục chỉ chứa đến 1 file

Có 3 thư mục a, b, c và các file sâu nhất cũng chỉ là a/file1, b/file2, c/file3, c/file4... thì rõ ràng chỉ echo */* là liệt kê được hết

Nếu viết là echo */** hoặc */**/* ... thì kết quả in ra màn hình terminal là */** hoặc */**/* (vì */* đã là sâu nhất rồi)