

# TCS3451

## CTF

# Assignment Writeup

Group Name: just\_me\_in\_the\_team

Member

ID	Name	Role
1181102970	Azmina Sharaf	Captain

## Category: Cryptography

### Question: Power

Examining the text file, it appears to be in hexadecimal format, so I make use of online CyberChef tool to convert the hex characters to ASCII.

The screenshot shows the CyberChef interface. In the 'Input' section, there is a large block of hex code: 4B525847515453554B5A4B5853544A544F524345344D334D4F355345495154474D523545434D444349354A44533D3D3D. Below this, the 'Output' section shows the converted ASCII string: KRXGQTSUKZKXSTJTORCE4M3M05SEIQTGMR5ECMDCI5JDS==. The 'Operations' sidebar on the left has 'magic' selected, and the 'Magic' recipe is active with 'Depth' set to 3. The 'BAKE!' button is highlighted in green.

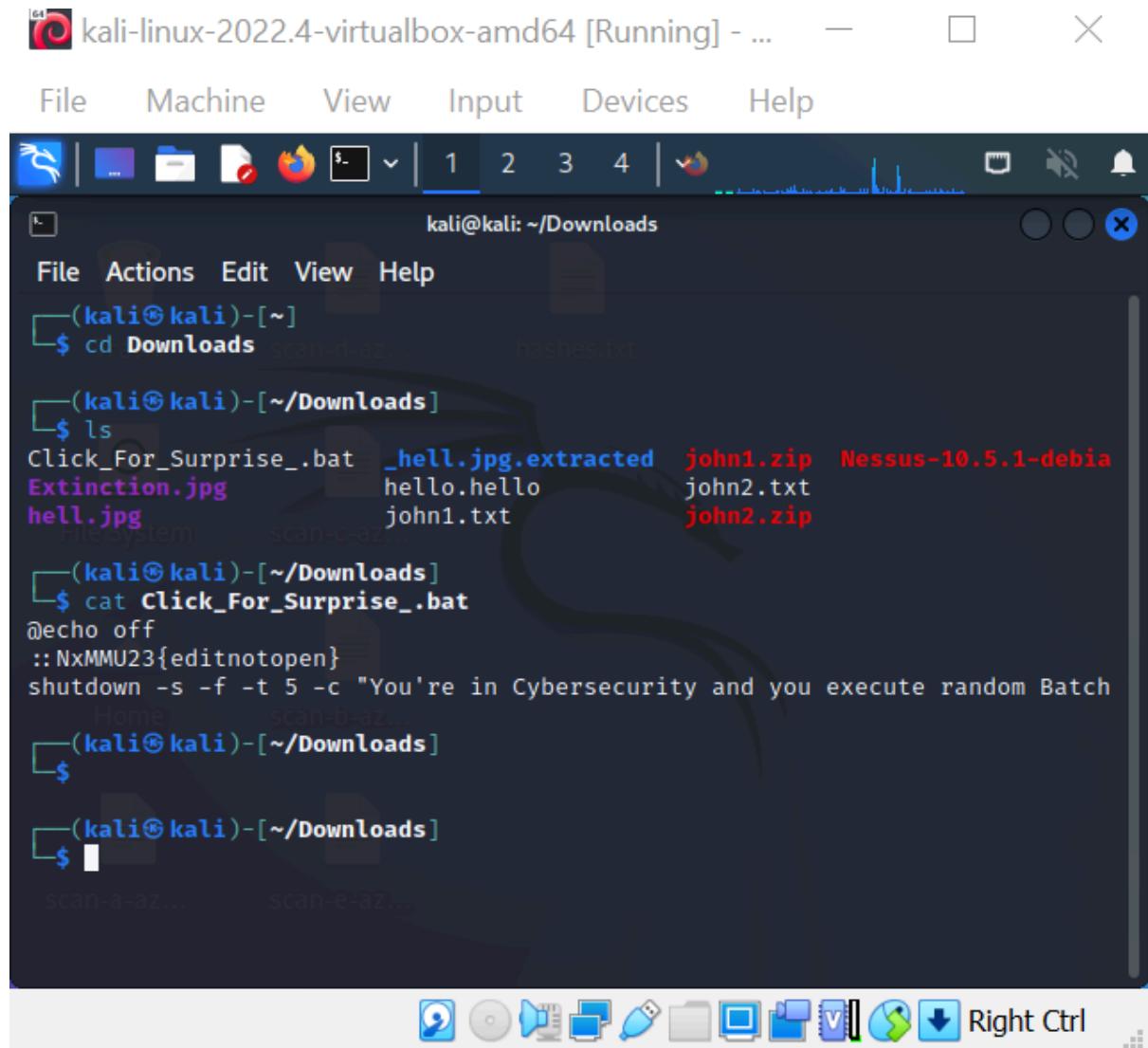
The converted ASCII string appears to be in Base64 encoding.

This screenshot shows the same CyberChef interface after applying the 'magic' operation. The 'Input' section now contains the ASCII string: KRXGQTSUKZKXSTJTORCE4M3M05SEIQTGMR5ECMDCI5JDS==. The 'Output' section shows the converted Base64 string: NxMMU23{C7ypt0\_w04ld}. The 'Operations' sidebar still has 'magic' selected, and the 'Magic' recipe is active with 'Depth' set to 3. The 'BAKE!' button is highlighted in green.

The flag is found!

**Category: Miscellaneous**

**Question: Click For Surprise !!!**



The screenshot shows a Kali Linux terminal window titled "kali-linux-2022.4-virtualbox-amd64 [Running]". The terminal is displaying the following command-line session:

```
kali@kali: ~/Downloads
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ cd Downloads scan-d-a...
hashes.txt

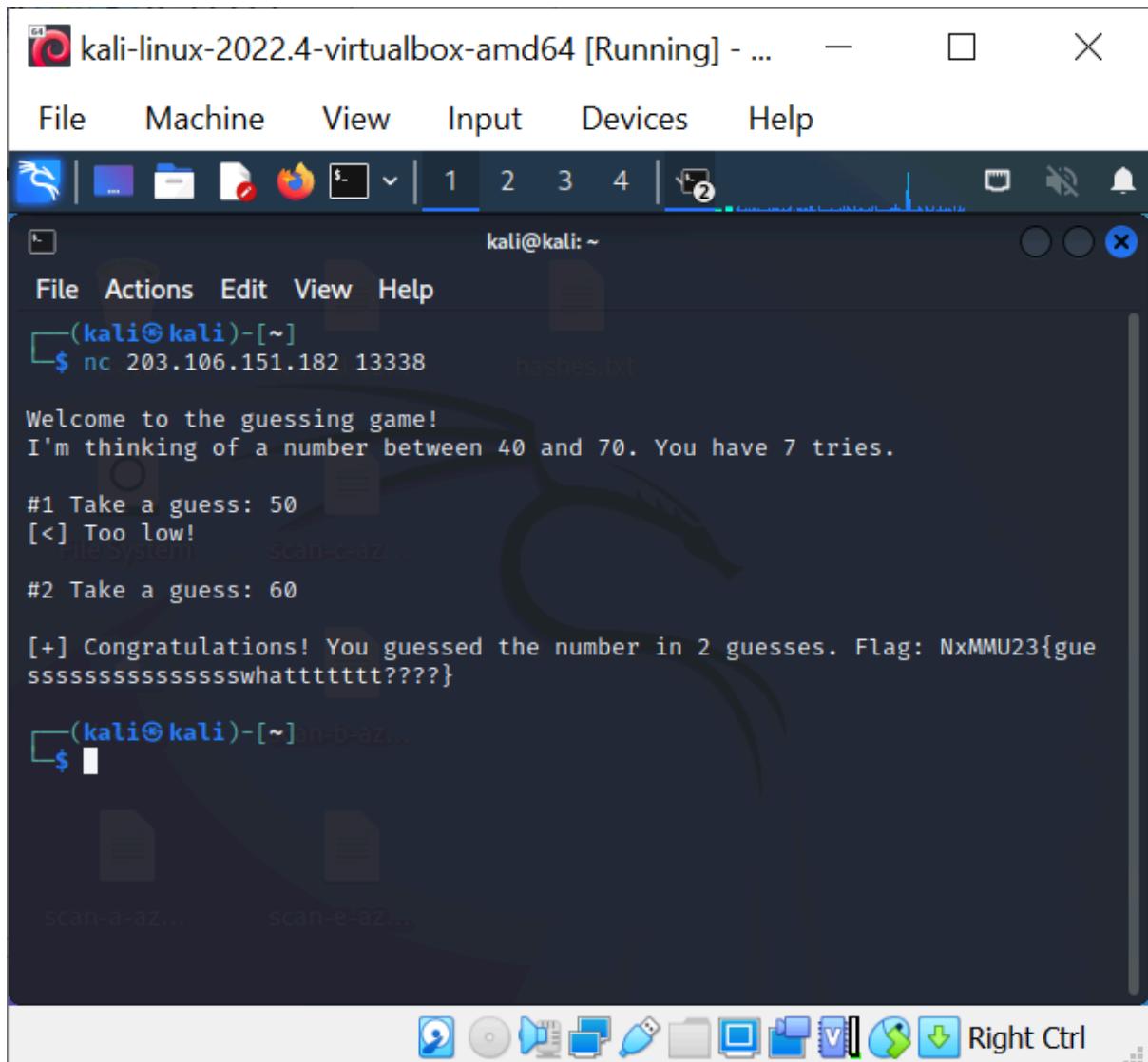
└──(kali㉿kali)-[~/Downloads]
$ ls
Click_For_Surprise_.bat _hell.jpg.extracted john1.zip Nessus-10.5.1-debia
Extinction.jpg hello.hello john2.txt
hell.jpg john1.txt john2.zip

└──(kali㉿kali)-[~/Downloads]
$ cat Click_For_Surprise_.bat
@echo off
:: NxMMU23{editnotopen}
shutdown -s -f -t 5 -c "You're in Cybersecurity and you execute random Batch
Home scan-b-a...
└──(kali㉿kali)-[~/Downloads]
$
```

The terminal window has a dark blue background with light blue text. It includes a standard Linux menu bar at the top and a toolbar with various icons at the bottom.

For this question, I downloaded the .bat file onto my Kali Linux and used the cat command on the linux terminal to reveal the contents of the .bat file.

**Question: Guessing game**



The screenshot shows a terminal window titled "kali-linux-2022.4-virtualbox-amd64 [Running]". The terminal interface includes a menu bar with File, Machine, View, Input, Devices, and Help, and a toolbar with icons for file operations like copy, paste, and search. The main window has tabs at the top labeled 1, 2, 3, 4, and 2. The current tab shows the command line prompt "kali@kali: ~". The terminal output is as follows:

```
File Actions Edit View Help
[(kali㉿kali)-[~]]$ nc 203.106.151.182 13338
hashes.txt

Welcome to the guessing game!
I'm thinking of a number between 40 and 70. You have 7 tries.

#1 Take a guess: 50
[<] Too low!

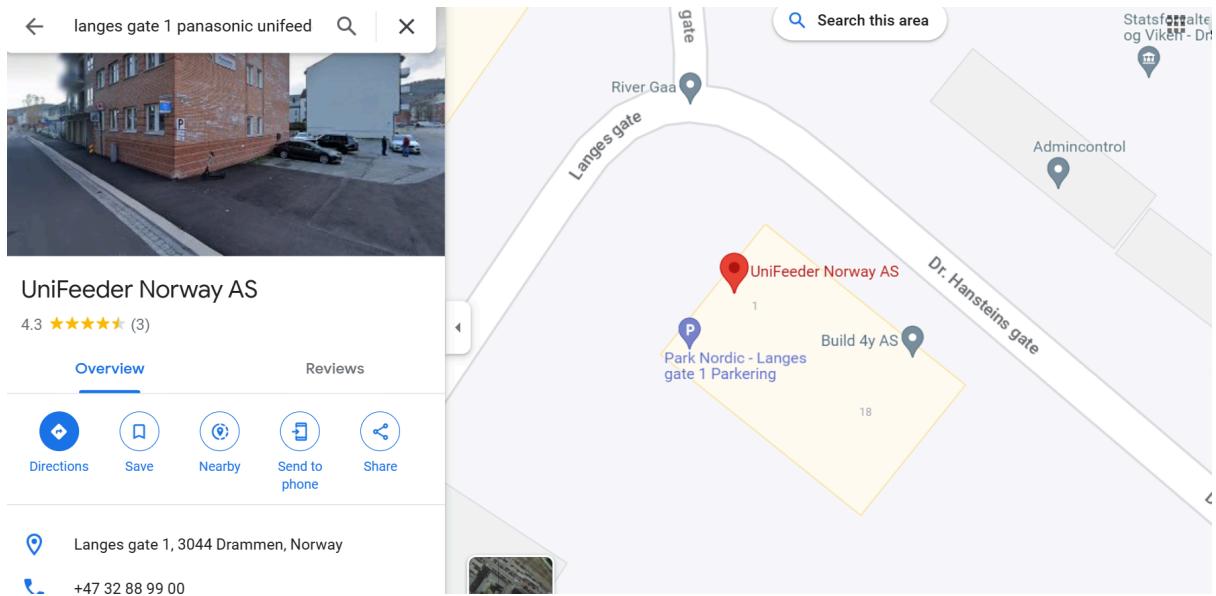
#2 Take a guess: 60

[+] Congratulations! You guessed the number in 2 guesses. Flag: NxMMU23{gue
sssssssssssssssswhatttttt????}
```

The terminal window also displays desktop icons for "scan-a-az...", "scan-e-az...", and other applications.

For this question I ran a netcat scan to find the flag.

## Question: Uncover the Secret Headquarters



To solve this, first I examined the png file to look for clues like building name and what companies its housing, after that a simple google search helped me find the street name which is Dr. Hansteins gate.

## Question: Welcome!

The screenshot shows a Discord interface for the 'mmu-ctf-2023' channel. The channel has several messages:

- OscarLim94 (05/29/2023 12:30 PM): REGISTRATION NOW OPEN: SECURE YOUR SPOT! 🔒
- @everyone (June 9, 2023): Greetings, student! The moment you've been waiting for has arrived. We are thrilled to announce that the registration page is now officially open, presenting you with a golden opportunity to join our competition!
- Siva Mohan (Yesterday at 1:31 PM): @everyone Greetings students! There will be a small briefing on the CTF tomorrow at 9:30 am at 'students-discussion-room' channel and sharp at 10 am we will start our CTF competition. Have a great day and see you all tomorrow!!!
- Siva Mohan (Today at 10:59 AM): @everyone Greetings students! A friendly reminder, if you have any queries or require any help, do reach out to us via this Discord. (edited)

A search bar on the right shows results for 'REGISTRATION NOW OPEN: SECURE YOUR SPOT!'. The results list 13 items, including:

- No sabotaging of other competing players, or in any way hindering their independent progress.
- No brute-forcing of challenge flag/keys against the scoring server.
- No flooding and/or DoS attacks. Teams caught in the act will be penalized by a time penalty or a disqualification.
- No ARP spoofing. Teams caught in the act will be penalized by a time penalty or a disqualification.
- The rules and regulations will or might be updated without prior notice.
- At all times, the decision of the NEXAGATE & MMU CTF Crew is final on any matter in question.
- The flag format: NxMMU23{Multimedia\_University\_Capture\_The\_Flag\_2023}

Below the results, there is a message: Happy hacking! Good luck and have fun. (edited)

To solve this problem I searched the hint in the question in the discord search bar and found the flag.

## Question: Sushi Sleuth

The screenshot shows a TripAdvisor restaurant page for "Shizenya on Hornby". The main headline reads "Fresh, flavourful food with good service." Below it is a five-star rating icon and the text "Review of Shizenya on Hornby". To the left, there's a grid of 141 photos showing various dishes. The restaurant's address is listed as 965 Hornby St, Vancouver, British Columbia V6Z 1V3, Canada (Downtown). It has a phone number (+1 604-568-0013), a website, and an email link. A "Ranked #74 of 2,523 Restaurants in Vancouver" badge is visible. On the right, there's a sidebar with user profiles for AZMINA SHARAF and FARASH ANIMZA, both from MMU. Below the sidebar, a section titled "Viewed restaurants" lists "Shizenya on Hornby" again with its 5-star rating and 309 reviews.

To solve this ctf question, I googled “sushi restaurant vancouver well prepared fresh sushi” "tbg mike” which led me to TripAdvisor where I found the name of the restaurant.

## Question: Dash

The screenshot shows the Dashlane application interface. The left sidebar contains navigation links: Get Started, Logins, Payments (selected), Secure Notes, Personal Info, IDs, Sharing Center, Tools, Password Health, and Dark Web Monitoring. The main area displays a card entry form for "Mayflag Bank". The card details are as follows:

Cardholder name	Jerry Github
Card Number	4528 7458 3528 1568
Security code	•••
Expiration date	04 / 2027
Item name	Mayflag Bank
Card color	Blue
Note	NxMMU23{b54d7f10164 9183dd6737fb0c49f6c

At the bottom right are "Delete" and "Close" buttons.

To acquire the flag first I used kali linux to extract the .zip file and got a .dash file. Then I signed up to Dashlane and created an account. Later I uploaded the .dash file and accessed it using the provided password. The flag was found in the payments section where I used my own account password to view the note.

## Question: Rock Paper Gunting

The screenshot is pretty self-explanatory

## Category: Osint

### Question: Look For MrDonde flag

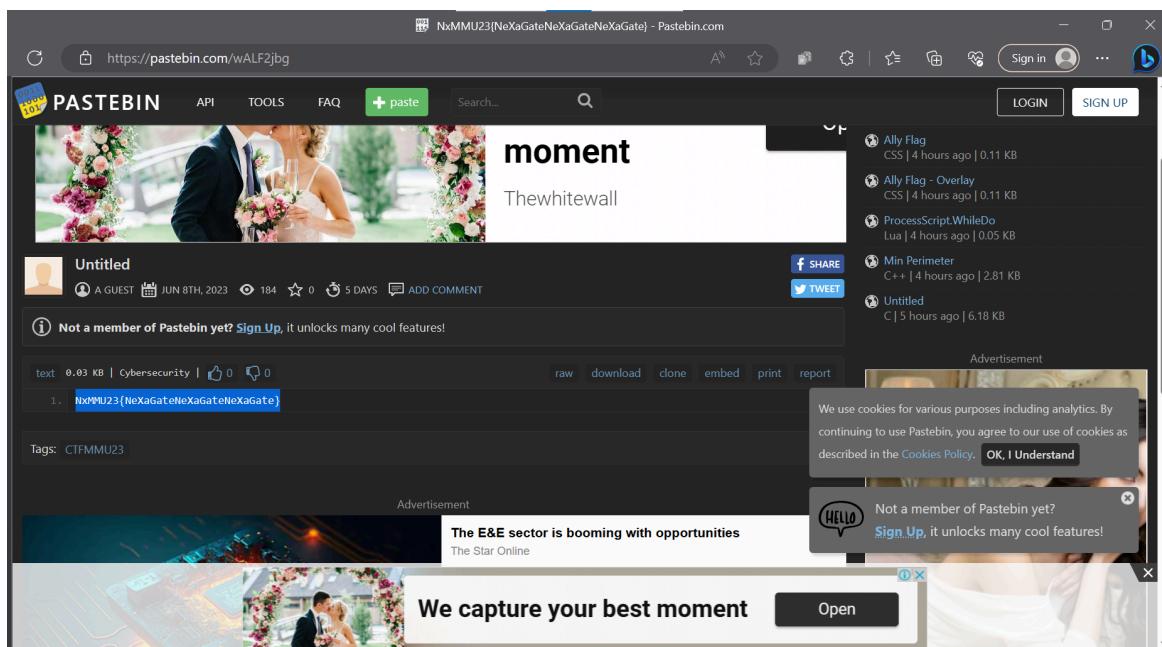
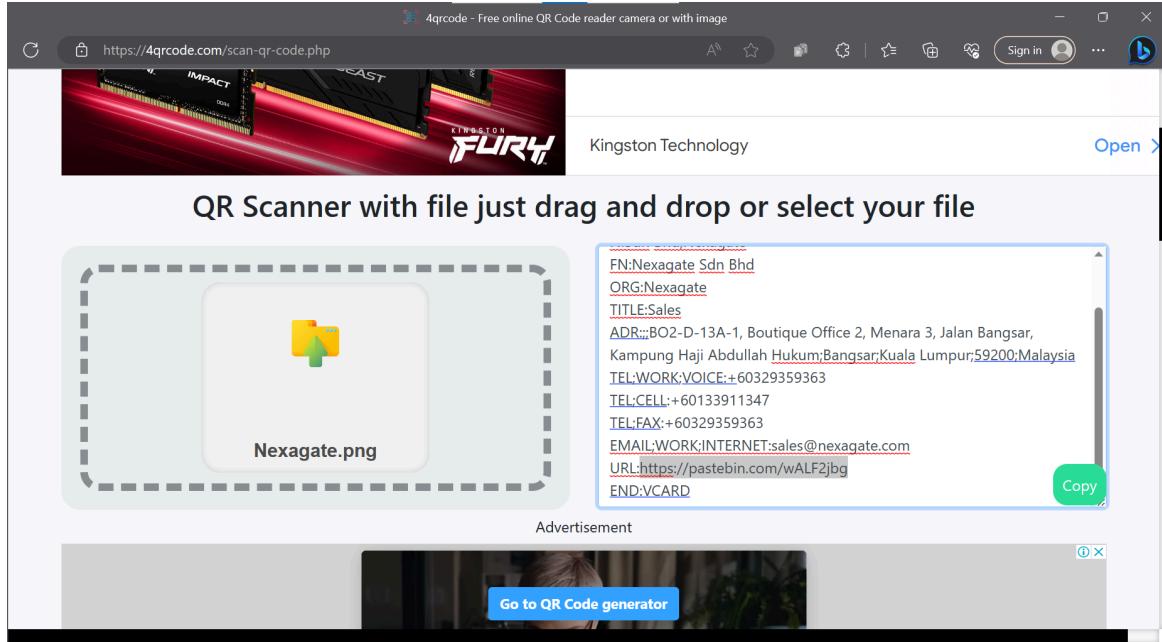
The screenshot shows the Twitter profile page for user @MrDonde898562. The profile picture is a placeholder. The bio reads: "Joined June 2023", "0 Following", "0 Followers", and "Not followed by anyone you're following". Below the bio, there are tabs for "Tweets", "Replies", "Media", and "Likes". A single tweet from MrDonde is visible, containing the text: "MrDonde @MrDonde898562 · 16h ++++++[>+>+++++>++++++>+++++++].". To the right of the profile, there's a sidebar titled "You might like" with three recommended accounts: "Demon Slayer: Kim..." (@DemonSlayerUSA), "One Piece" (@OnePieceAnime), and "AnimeTV チェーン" (@animetv\_jp). Below that is a section titled "Trends for you" with trending topics: "#SPM2022" and "#SingaporeOpen2023".

The screenshot shows the Brainfuck Language - Online Decoder, Translator, Interpreter tool at <https://www.dcode.fr/brainfuck-language>. The main interface has sections for "BRAINFUCK INTERPRETER" and "BRAINFUCK ENCODER". In the interpreter section, the input is set to "++++++[>+>+++++>++++++>+++++++].". The output window shows the decoded text: "Nxmnu23{Osint\_is\_great}". Below the input, memory values are listed: "[1] = (10)", "[2] = 3 (51)", "[3] = a (97)", and "[4] = } (125)". The encoder section has a "PLAINTEXT TO CODE IN BRAINF\*\*K" input field containing "dcode BrainFuck". There are also "EXECUTE" and "ENCRYPT" buttons. The right side of the page contains a "Summary" section with links to various Brainfuck-related topics and a "Similar pages" section with links to other tools like ReverseFuck, JSFuck, LOLCODE, and Binaryfuck.

Found MrDonde on twitter, and then translated his tweets via brainfuck decoder to get the flag.

## Category: Steganography

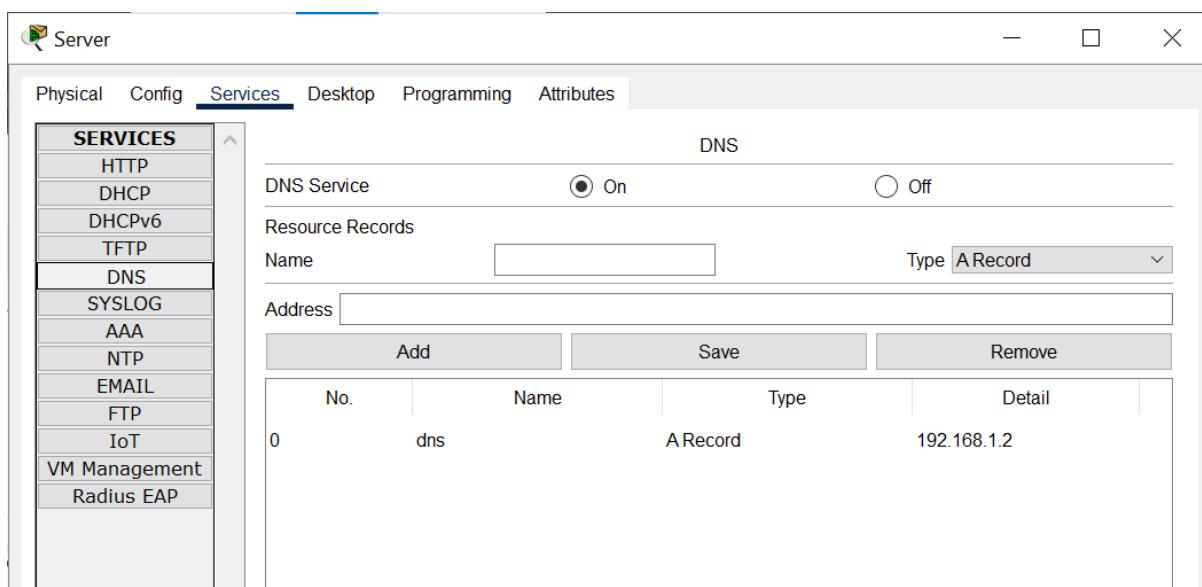
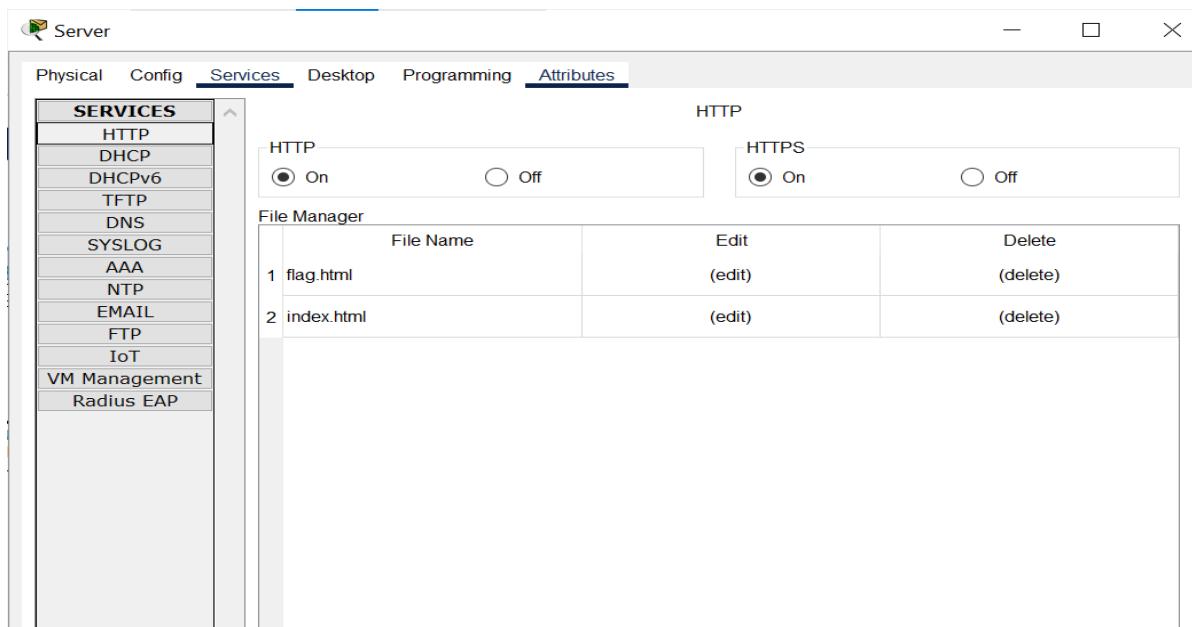
### Question: Quick Response



For this question I scanned the qr code with an online scanner first, and then I visited the URL from the results and found the flag.

## Category: Forensics

### Question: Packet



The image shows two windows from a network configuration tool. The top window is titled 'Server' and has tabs for Physical, Config, Services, Desktop, Programming, and Attributes. The 'Desktop' tab is selected, showing an 'IP Configuration' dialog. The configuration is set to 'Static' with the following values:

IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	192.168.1.2

The bottom window is titled 'PC' and also has tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is selected, showing a 'Web Browser' dialog. The URL field contains 'https://192.168.1.2/flag.html'. The page content area displays the text: 'Flag is NxMMU23{7cd5a3880f446e7bc13b0f8b3cc5f2b0}'.

To solve this question at first I gave IP addresses to the server and the PC. I made the web server the DNS server too. I configured the PC's IP as well. Then I found the flag by typing the dns address in the web browser of the PC.

**Category: Web**

**Question: Infobase**

The screenshot shows a web browser window titled "Info Base" with the URL <https://nexaxmmu-infobase.chals.io/>. The page contains a terminal-like interface on the left and a company status summary on the right.

**Terminal Output:**

```
Nx9MMU23[306a7cab6963e425876e21e0c785bbba]
> /ping google.com | cat ./flag.txt
[+] Starting scan on google.com | cat ./flag.txt
Enter '/help' for all commands
```

**Company Status Summary:**

// COMPANY_STATUS	
nexaQATE	
Since 2010	
Founders: Khalid, ElWendy	
Certified: ISO 27001/2013, CREST-accredited	
Completed Project: 500+	
Current Aim: Improve everyone's security posture by identifying and protect data from leakages and threats.	

Used the /help command to see the list of commands available and then played around with the ping command to find the flag

**Question: Persistance**

Pretty Self-explanatory. I used the curl command on my kali linux terminal and kept trying til I found the flag. (Unfortunately I closed the terminal and realized I didnt take a screenshot after.)

## Category: Steganography

### Question: Surrender

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/WhiteFlag
$ ls
Click_For_Surprise..bat hello.hello          Nessus-10.5.1-debian10_amd64.deb
click_for_surprise_  john1.txt                pun_labyrinth.zip
Extinction.jpg       john2.zip               shell.zip
forensic_clone.zip   john2.txt              Vault-2023-04-11.dash
forensic_clone.zip   john1.zip              WhiteFlag.txt
hell.jpg             misc_Dash.zip
hell.jpg.extracted   misc_FindMeIfYouCan.zip
hell1.jpg            misc_FindMeIfYouCan.zip
hell1.jpg.extracted misc_Dash.zip
$ cat WhiteFlag.txt
$ ls
Click_For_Surprise..bat hello.hello          Nessus-10.5.1-debian10_amd64.deb
code.png             john1.txt                pun_labyrinth.zip
click_for_surprise_  john2.zip               shell.zip
Extinction.jpg       john2.txt              Vault-2023-04-11.dash
forensic_clone.zip   john1.zip              WhiteFlag.txt
hell.jpg             misc_Dash.zip
hell.jpg.extracted   misc_FindMeIfYouCan.zip
hell1.jpg            misc_FindMeIfYouCan.zip
hell1.jpg.extracted misc_Dash.zip
$ binwalk WhiteFlag.zip
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----      -----
0           0x0          Zip archive data, at least v2.0 to extract, compressed size: 375, uncompressed size: 375, name: WhiteFlag/Flag.zip
401         0x191        End of Zip archive, footer length: 22
423         0x1A7        Zip archive data, at least v2.0 to extract, compressed size: 6070548, uncompressed size: 6080253, name: WhiteFlag/passwd.png
6571251     0x9C43D3    End Of Zip archive, footer length: 22
$ ls
$ ls
Archive: WhiteFlag.zip
Extracting: WhiteFlag/flag.zip
Inflating: WhiteFlag/passwd.png
$ ls
$ ls
Click_For_Surprise..bat Extinction.jpg forensic_clone.zip hell.jpg.extracted john1.txt john2.txt misc_Dash.zip Nessus-10.5.1-debian10_amd64.deb shell.zip WhiteFlag WhiteFlag.zip
code.png             forensic_clone hell.jpg             john1.zip john2.zip misc_FindMeIfYouCan.zip pun_labyrinth.zip Vault-2023-04-11.dash WhiteFlag.txt
$ cat WhiteFlag
cat: WhiteFlag: Is a directory
$ cd WhiteFlag
$
```

Steganography Online

https://stylesuxx.github.io/steganography/

Encode Decode

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

Choose File passwd.png

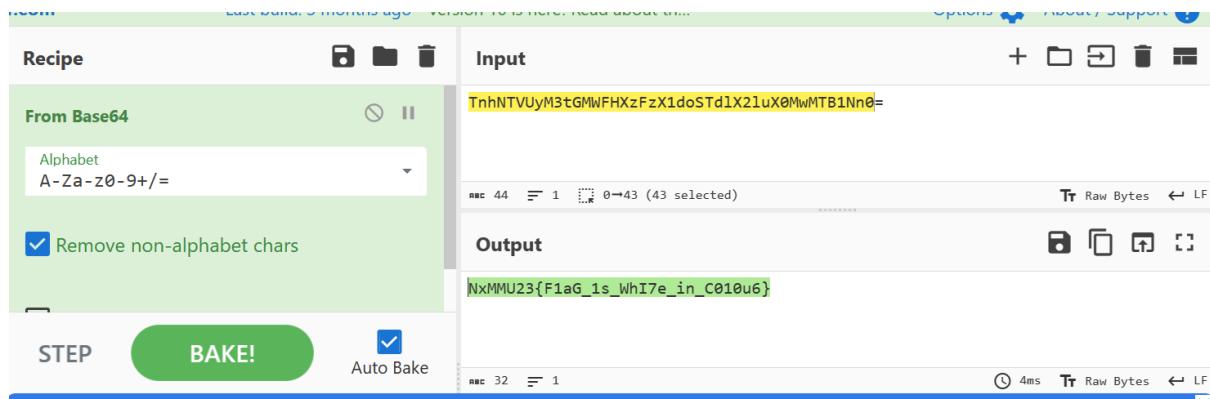
Decode

Hidden message

```
TnhNTVUyM3tGMWFHXzFzX1doSTdIX2luX0MwMTB1Nn0=
```

Input

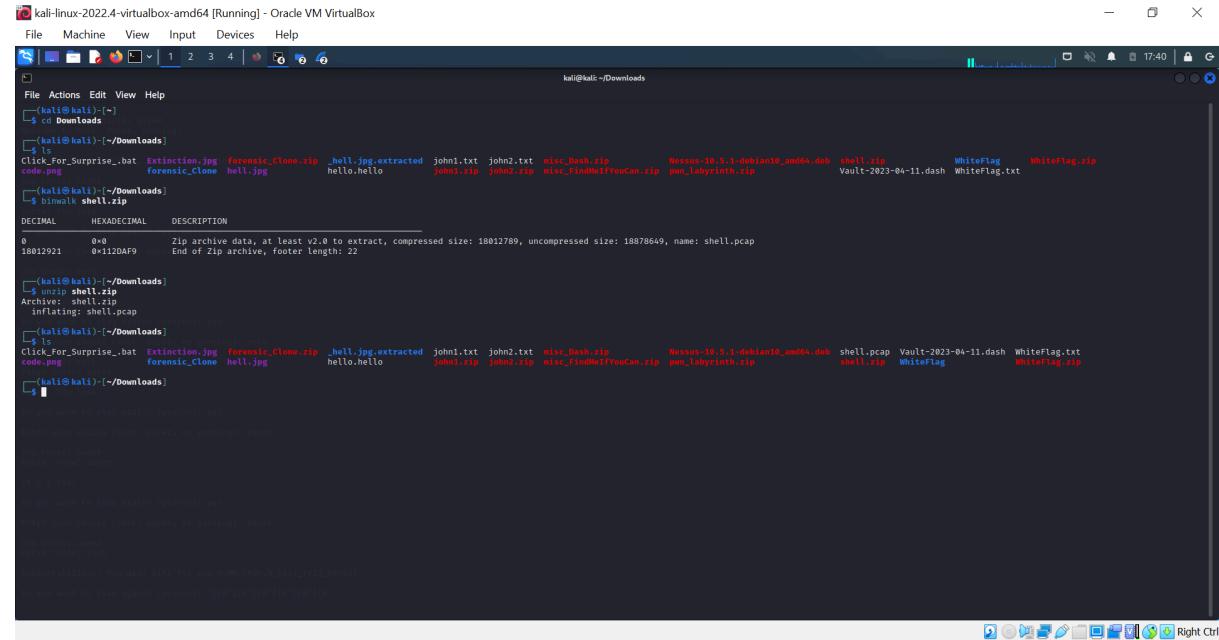




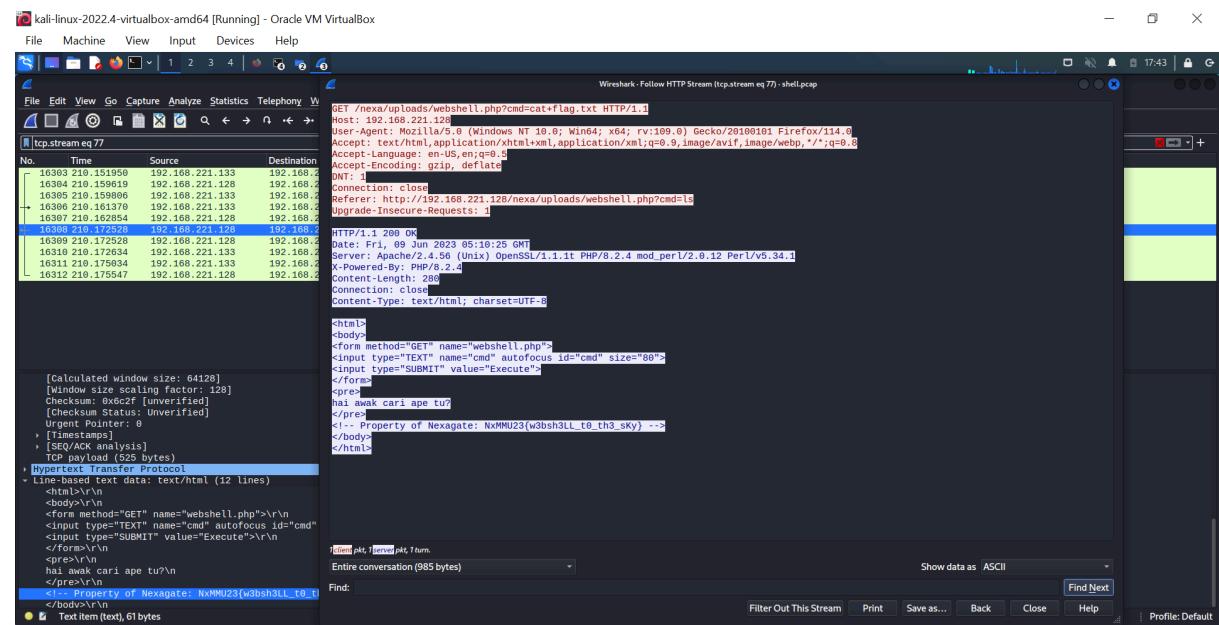
For this question, at first I scanned the WhiteFlag.zip using binwalk and then unzipped it. I was met with flag.zip and passwd.png file. I used an online steganography file to decode the png file. The code was in hexadecimal so I made use of cyberchef to convert it into string and found the flag.

## Category: Forensics

### Question: SHell



A screenshot of a terminal window titled "kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the user navigating to their Downloads directory and extracting a file named "shell.zip". The output of the extraction command is displayed, showing various files and their descriptions. The terminal window has a dark background with light-colored text.



A screenshot of the Wireshark application, which is a network traffic analyzer. The interface shows a list of captured network packets. A specific session is being analyzed, with the details pane showing an HTTP GET request to "/nexa/uploads/webshell.php?cmd=cat+flag.txt" from host 192.168.221.128 to host 192.168.221.129. The content pane displays the response, which includes the flag "WhiteFlag". The bottom pane shows the raw hex and ASCII data of the packet.

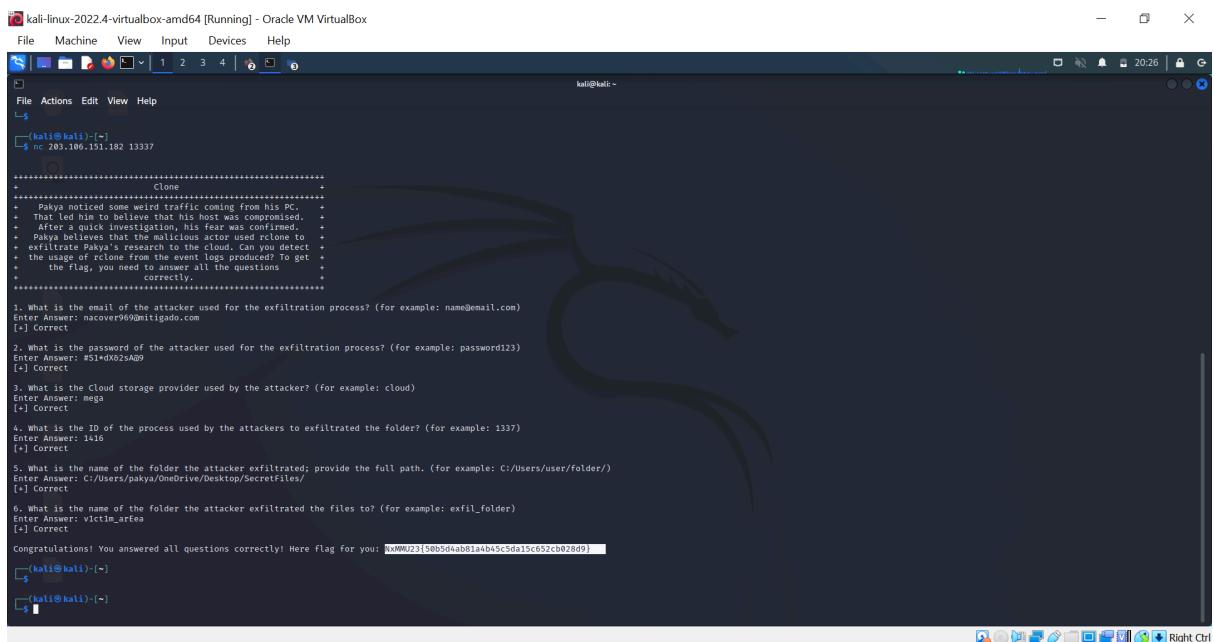
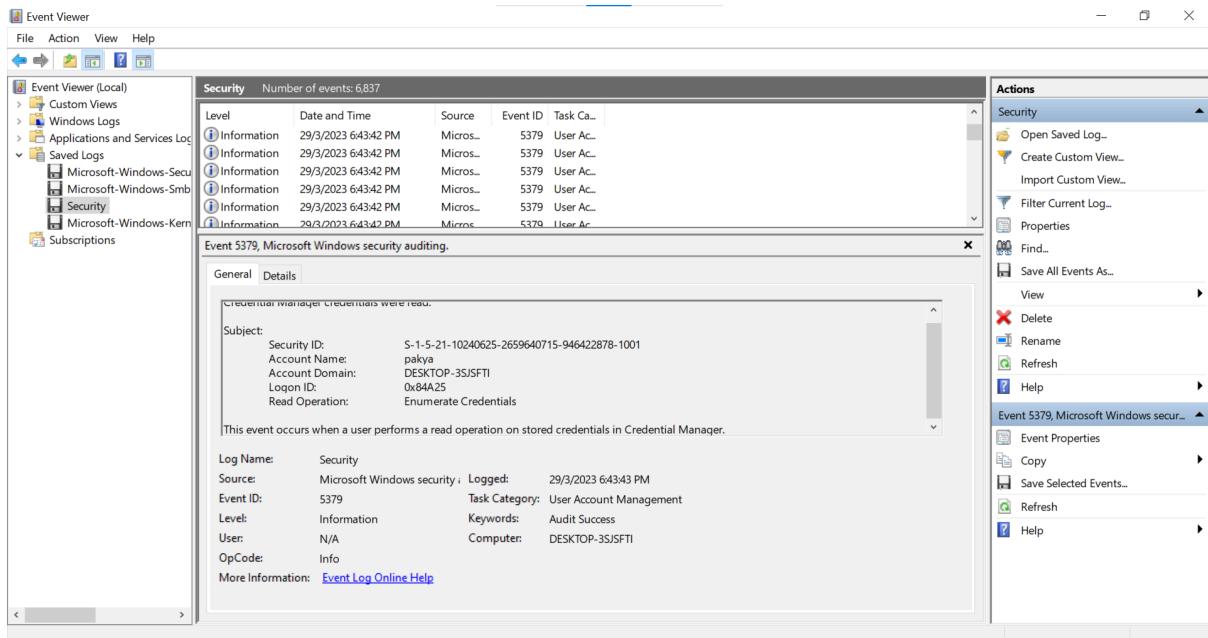
I scanned the shell.zip using binwalt and then unzipped it and found shell.pcap which i opened using wireshark. I filtered the whole thing by http and found the flag in one of them.

## Category: Miscellaneous

## Question: FindMeIfYouCan

I scanned the zip file using binwalk and then unzipped it. Then I ran a command where basically it will try to find a txt file that doesn't match a specific pattern, and that's how I got my flag 😊

## Question: Clone



For this question, I found the details regarding the impersonator using Event Viewer. The event ID is 1416.

Multimedia University Capture The Flag 2023 powered by Nexigate Sdn Bhd

https://nexaxmmu.ctfd.io/challenges

Sign in

- Cryptography
  - | — Power (50)
- Forensics
  - | — Packet (75)
  - | — Shell (75)
  - | — Clone (100)
- Miscellaneous
  - | — Sushi Sleuth (20)
  - | — Click For Surprise !!! (25)
  - | — Guessing Game (25)
  - | — Rock Paper Gunting (25)
  - | — The Enigmatic Letter (25)
    - | — Uncover the Secret Headquarters (25)
    - | — Welcome! (25)
    - | — Dash (50)
    - | — FindMeIfYouCan (50)
    - | — PakyaFormation (50)
- Osint
  - | — Look for MrDonde Flag (20)
- Pwn
  - | — Labyrinth (75)
- Steganography
  - | — Quick Response (50)
  - | — Surrender (50)
- Web
  - | — Clueless: Wargame [Unrecorded] (0)
  - | — Infrabase (75)
  - | — MagicWord (75)
  - | — Persistence (75)