



Computer Systems Security

CMPN426

Project CTF's Report

Team Member	ID
Amr Ashraf Attia	1200042
Ziad Abd El Wareth	1200471
Marly Mofeed Makram	1200909
Osama Nasser Saber	1200790

Table of Contents

Flags3

Explanation5

 CTF-15

 CTF-2.....5

 CTF-3.....5

 CTF-4.....5

 CTF-5.....6

 CTF-6.....6

 CTF-77

 CTF-8.....7

Flags

CTF-1:

alice was beginning to get very tired of sitting by her sister on the bank and of having nothing to do once or twice she had peeped into the book her sister was reading but it had no pictures or conversations in it and what is the use of a book thought alice without pictures or conversations

so she was considering in her own mind as well as she could for the day made her feel very sleepy and stupid whether the pleasure of making a daisychain would be worth the trouble of getting up and picking the daisies when suddenly a white rabbit with pink eyes ran close by her

there was nothing so very remarkable in that nor did alice think it so very much out of the way to hear the rabbit say to itself oh dear oh dear i shall be too late but when the rabbit actually took a watch out of its waistcoatpocket and looked at it and then hurried on alice started to her feet for it flashed across her mind that she had never before seen a rabbit with either a waistcoatpocket or a watch to take out of it and burning with curiosity she ran across the field after it and was just in time to see it pop down a large rabbithole under the hedge in another moment down went alice after it

the rabbithole went straight on like a tunnel for some way and then dipped suddenly down so suddenly that alice had not a moment to think about stopping herself before she found herself falling down what seemed to be a very deep well

either the well was very deep or she fell very slowly for she had plenty of time as she went down to look about her first she tried to make out what she was coming to but it was too dark to see anything then she looked at the sides of the well and noticed that they were filled with cupboards and bookshelves here and there she saw maps and pictures hung upon pegs she took down a jar from one of the shelves as she passed it was labeled orange marmalade but to her great disappointment it was empty she did not like to drop the jar so managed to put it into one of the cupboards as she fell past it

down down down would the fall never come to an end there was nothing else to do so alice soon began talking to herself dinahll miss me very much tonight i should think dinah was the cat i hope theyll remember her saucer of milk at teatime dinah my dear i wish you were down here with me alice felt that she was dozing off when suddenly thump thump down she came upon a heap of sticks and dry leaves and the fall was over

alice was not a bit hurt and she jumped up in a moment she looked up but it was all dark overhead before her was another long passage and the white rabbit was still in sight hurrying down it there was not a moment to be lost away went alice like the wind and was just in time to

hear it say as it turned a corner oh my ears and whiskers how late its getting she was close behind it when she turned the corner but the rabbit was no longer to be seen

she found herself in a long low hall which was lit up by a row of lamps hanging from the roof there were doors all round the hall but they were all locked and when alice had been all the way down one side and up the other trying every door she walked sadly down the middle wondering how she was ever to get out again

suddenly she came upon a little table all made of solid glass there was nothing on it but a tiny golden key and alices first idea was that this might belong to one of the doors of the hall but alas either the locks were too large or the key was too small but at any rate it would not open any of them however on the second time round she came upon a low curtain she had not noticed before and behind it was a little door about fifteen inches high she tried the little golden key in the lock and to her great delight it fitted

alice opened the door and found that it led into a small passage not much larger than a rathole she knelt down and looked along the passage into the loveliest garden you ever saw how she longed to get out of that dark hall and wander about among those beds of bright flowers and those cool fountains but she could not even get her head through the doorway oh said alice how i wish i could shut up like a telescope i think i could if i only knew how to begin

alice went back to the table half hoping she might find another key on it or at any rate a book of rules for shutting people up like telescopes this time she found a little bottle on it which certainly was not here before said alice and tied round the neck of the bottle was a paper label with the words drink me beautifully printed on it in large letters

no ill look first she said and see whether its marked poison or not for she had never forgotten that if you drink from a bottle marked poison it is almost certain to disagree with you sooner or later however this bottle was not marked poison so alice ventured to taste it and finding it very nice it had a sort of mixed flavor of cherrytart custard pineapple roast turkey toffy and hot buttered toast she very soon finished it off

what a curious feeling said alice i must be shutting up like a telescope

after awhile finding that nothing more happened she decided on going into the garden at once but alas for poor alice when she got to the door she found she had forgotten the little golden key and when she went back to the table for it she found she could not possibly reach it she could see it quite plainly through the glass and she tried her best to climb up one of the legs of the table but it was too slippery and when she had tired herself out with trying the poor little thing sat down and cried

come theres no use in crying like that said alice to herself rather sharply i advise you to leave off this minute she generally gave herself very good advice though she very seldom followed it and sometimes she scolded herself so severely as to bring tears into her eyes

soon her eye fell on a little glass box that was lying under the table she opened it and found in it a very small cake on which the words eat me were beautifully marked in currants well ill eat it said alice and if it makes me grow larger i can reach the key and if it makes me grow smaller i can creep under the door so either way ill get into the garden and i dont care which happens

she ate a little bit and said anxiously to herself which way which way holding her hand on the top of her head to feel which way she was growing and she was quite surprised to find that she remained the same size so she set to work and very soon finished off the cake

CTF-2: picoCTF{p33kab00_1_s33_u_deadbeef}

CTF-3: picoCTF{d72ea4af}

CTF-4: fastctf{a_bit_tricky|

CTF-5: picoCTF{grep_is_good_to_find_things_dba08a45}

CTF-6: The enemies are making a move. We need to act fast.

CTF-7: CMPN{Spring2024}

CTF-8: THANKYOUFORSAVINGMETHEFLAGISMOSCOW

Explanation

CTF-1

1. First, we calculated the frequency of each character in the English language.
2. We used some popular mapping from the internet already calculated using some kind of language analysis, but it does not work.
3. We used some trying and error for mapping the letters to find a text related to the English language.
4. Finally, we substituted the letters using a Python Code written by us, included in the CTF-1 file.

CTF-2

1. We used wireshark tool to be able to trace the packets.
2. We found that most of the data is encrypted, so any hope will come from an http request.
3. We searched and tried to export any file within the response.
4. We found an encrypted file called %2f containing the flag.
5. Finally, we decrypted it using ROT13 decryption algorithm.

CTF-3

1. We used StegSolve Tool to add the RGB values of the two images.
2. A Flag appeared 😊

CTF-4

1. We transferred the text into binary string.
2. We used circular left shift with many offsets.
3. Finally, the flag appeared with offset 1, the code is included.

CTF-5

1. We wrote a command on the terminal: `cat logs | grep '{' -n`.
2. The flag suddenly appeared.

CTF-6

1. We started by debugging and understanding the given algorithm.
2. We used reverse process technique, and since a hint was given that the key is one letter only, so we looped on all letters, but to reduce the complexity of the decrypt algorithm we looped only on the first 15 letters in the alphabet.
3. Then the key was letter f 😊, code is included.

```
CTF-6 (New Encryption) > decrypt.py > ...
1  import string
2
3  START = ord("a")
4  CHARSET = string.ascii_lowercase[:16]
5
6  Codiumate: Options | Test this function
7  def decode_b16(middle):
8      decoded = ""
9      for i in range(0, len(middle), 2):
10         index1 = CHARSET.index(middle[i])
11         b1 = "{0:04b}".format(index1)
12         if i + 1 < len(middle):
13             index2 = CHARSET.index(middle[i + 1])
14             b2 = "{0:04b}".format(index2)
15             decoded += chr(int(b1 + b2, 2))
16         else:
17             decoded += chr(int(b1, 2))
18     return decoded
19
20  Codiumate: Options | Test this function
21  def caesar_shift(c, k, i):
22      index = CHARSET.index(c)
23      value = (index - ord(k) + 2 * START) % len(CHARSET) + 97
24      return chr(int(value))
25
26  cipher = "jikmkjgekjkckjkbknkjlhgekflgkjgekbkfkpnkcklgekfgkdbklkjcgcgejlkjgekckjkjkigelikdgekfkhligeckkflhligc"
27  for j in range(15):
28      key = chr(j + 97)
29      middle = ""
30      for i, c in enumerate(cipher):
31          middle += caesar_shift(c, key[i % len(key)], i)
32      plain = decode_b16(middle)
33      print("The plain text for key: " + key + " is: ")
34      print(plain)
35      print()
```

CTF-7

1. First, we tried to search for the strings hidden within the image, but nothing was found 😞 .
2. Then we tried to brute force the password of the image using StegExtract and a wordlist called “rockyou.txt” with 14 million passwords 💀 , but it didn’t work.
3. Finally, we discovered the hint given that the password to extract the flag is HIDING 😏 .
4. We used StegExtract tool with password HIDING to extract the flag.

CTF-8

1. First, we used a morse code decoder to extract the code.
Online morse code decoder:

<https://morsecode.world/international/decoder/audio-decoder-adaptive.html>

2. Then, we used strings command on the audio file.

```
~{[]-
~{[]-
~{[]-
https://en.wikipedia.org/wiki/Nihilist_cipher?keyword=polybius
96 57 47 66 62 38 55 67 55 35 68 44 48 95 66 65 57 65 53 75 78 77 55 36 47 55 45
66 87 34 46 48 33 77
(anr@kali)-[~/Desktop/security project/CTF/CTF-8 (Can You Help Me)]
```

3. We searched for this algorithm and found an online tool to decrypt the cipher text using the given keyword and the extracted key “RUSSIAN”.

Decoder link: <https://www.dcode.fr/nihilist-cipher>

