In this CTF challenge, we were given 2 points of interests.

1. 10 images of chess board filled with pieces already set in place.
2. A note with a unreadable string: “=T.(./vj+AX`k,`%[@-mM[p0\M\*\_Oy”

Our first goal in this challenge is to decipher the chess boards. One of the in-text clues given is that ‘John is a competitive chess player and loves playing white side.’ Therefore, after analyzing the 10 images, we noticed that each board is one move away from checkmate from the white side.

By using a chess simulator, we can get all 10 Portable Game Notation (PGN) moves from the images.

With respective to the image numbering given (1.png to 10.png), these are the 10 moves in each image that leads to a checkmate.

1. Nh6# (f5 to h6 knight)
2. Rg8# (g2 to g8 rook)
3. Bg5# (e3 to g5 bishop)
4. Nf7# (e5 to f7 knight)
5. f4# (f2 to f4 pawn)
6. Qb8# (g3 to b8 queen)
7. Bg6# (d3 to g6 bishop)
8. Qe4# (e8 to e4 queen)
9. Rc7# (c1 to c7 rook)
10. Na4# (c3 to a4 knight)

Our second goal is understand the note with the unreadable string. At first, we tried decoding the using ROT, testing the values received from the images, but to no avail. However, when we tried encoding the string instead, it produced something legible. Not only that, after trying ROT-6 (from Nh6#, the first number found above), the results came back with a clue.

Graphical user interface, text, application, chat or text message

Description automatically generated

We chose ‘94 PRINTABLE ASCII CHARACTERS’ as that is the format the current unreadable string is written in.

Graphical user interface, text, application, chat or text message

Description automatically generated

In the results, we notice that the first 3 values ‘CZ4’ seems to be corrected to how a flag is formatted in this competition.

Yet, there is no way for the first 6 strings in the unreadable string, “=T.(./” , to become “CZ4067”.

However, “=T.” was encoded into “CZ4” using ROT-6, the number found in the “1.png”

Therefore, the solution would be to split the 30-character string into sets of 3, and encode it using number found in the PGN.

\*Sets of 3 because chess notation is in sets of 3

|  |  |  |
| --- | --- | --- |
| String (In sets of 3) | ROT-value | Results |
| =T. | 6 | CZ4 |
| (./ | 8 | 067 |
| vj+ | 5 | {o0 |
| AX` | 7 | H\_g |
| k,` | 4 | o0d |
| %[@ | 8 | -cH |
| -mM | 6 | 3sS |
| [p0 | 4 | \_t4 |
| \M\* | 7 | cT1 |
| \_Oy | 4 | cS} |

Adding those together,

Flag : CZ4067{o0H\_go0d-cH3sS\_t4cT1cS}