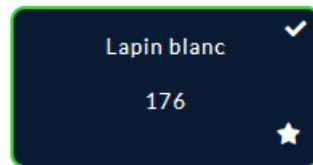


Side Channel and Fault Attacks




Challenge 170 résolutions

Lapin blanc

177

side-channel and fault attacks



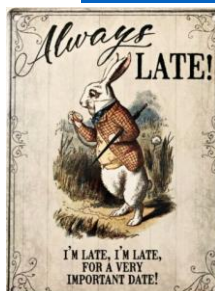
Saurez-vous retrouver la phrase de passe pour accéder au pays des merveilles d'Alice ?
La porte n'est pas très patiente, **vous n'avez que 10 minutes** pour l'ouvrir. Bonne chance !

nc challenges.france-cybersecurity-challenge.fr 2350

Flag

Submit

Le but manifeste est de deviner un terme (ou phrase ou locution) qui fasse ouvrir la porte en sésame. Il est fait appel à de l'analyse proche du « Time attack » évaluant la *lenteur d'affichage* des caractères. Ensuite, en parvenant à décoder le début de chaîne avec un algorithme, il est aisé d'avoir des termes. En effet, la recherche de parole émise par le lapin blanc de Alice au Pays des Merveilles fait converger. Ce site de Disney à l'exemple évoque la citation <https://news.disney.com/alice-in-wonderland-quotes>



```
(kali㉿kali)-[~/volatility]
$ nc challenges.france-cybersecurity-challenge.fr 2350
[0000014065] Initializing Wonderland...
[0001326216] Searching for a tiny golden key ...
[0001678413] Looking for a door...
[0001990596] Trying to unlock the door...


||
|| THE DOOR ||
||          ||
|)          | What's the magic phrase? |
||          /_____ \
||      ^   ^
||     _ 
|)
||
||
|| _____

Answer: I'm late, I'm late, I'm late!" "I'm late, I'm late! For a very important date!"
[0022526907] The door is thinking...
[0022584051] Your magic phrase is invalid, the door refuses to open.
Answer: I'm late, I'm late, I'm late!" "I'm late, I'm late! For a very important date!"
[0068155902] The door is thinking...
[0068212982] Your magic phrase is invalid, the door refuses to open.
Answer: I'm late, I'm late, I'm late! I'm late, I'm late! For a very important date!
[0137670663] The door is thinking...
[0137727740] Your magic phrase is invalid, the door refuses to open.
Answer: I'm late, I'm late! For a very important date!
[0160526319] The door is thinking...
[0160714477] FCSC{t1m1Ng_1s_K3y_8u7_74K1nG_u00r_t1mE_is_NEce554rY}

(kali㉿kali)-[~/volatility]
$
```

Et, après un ou deux essais pour accélérer la recherche : I'm late, I'm late! For a very important date!

Le flag qui s'affiche est donc : FCSC{t1m1Ng_1s_K3y_8u7_74K1nG_u00r_t1mE_is_NEce554rY}