Find Eve 1

Lore

Welcome to MI5!

Sorry, but you won’t have time to settle in because your first mission has already arrived.
To provide some context, Eve is an agent who joined our agency five years ago and had been working on the search for the Hoxne treasure. We have finally found a map that seems to lead to the treasure. However, the traitor Eve has fled with the map.
Your mission is simple: find Eve.

Agent, Eve left subtle traces in her choice of words and references. A strange post-it found on her desk, stuck to a book titled *Neuromancer* by William Gibson, bore the inscription:
"Within the maze of the matrix, intelligence always plays a double game. Look where it all begins, and you’ll uncover the one pulling the strings."

We believe she was referring to a classic piece of cyberpunk literature, where manipulation and betrayal are central themes. If you are astute enough to decipher this riddle, you will uncover the key hidden within this futuristic digital universe.

Hint

First, decrypt with a key and a salt, you'll cry while searching for the only word.
Then, decode the first layer of encoding, which uses a format specific to IPv6 (compact representation).

Solution

Part 1

File analyse

The data file given have 208 bytes with practically-random entropy.
208 is a multiple of 16, which is like a block cipher of some kind (AES).
No extension so it isn't crypted on internet → It use a commande.
Most common AES command is `openssl`.
The hint say that a key and a salt is need.
No `Salted__<the_salt>` at the start of the encrypted data so the salt is specified manually as hex.

The command :
`openssl enc -d -aes-256-cbc -salt -pbkdf2 -S <salt> -in MessageSecret -out MessageDecrypt -k <key>`

Key

Research *Neuromancer* by William Gibson, the lore says to find "the one pulling the strings" that is *Wintermute* the mastermind of this book.
⇒ The key is *Wintermute*.

Salt

It's already complicate, so for the salt, there is no need to search more information.

Hash 256 (same 256 as the one use in AES) of `Wintermute` :
`dfd05592762aa2ac733a8b185956f6cb55a58949a29e77d087ce93b186db33bb`

A salt need 16 caracters, so we take the first 16 caracters of this hash.
⇒ `dfd05592762aa2ac`

Decryptage :

```
$ openssl enc -d -aes-256-cbc -salt -pbkdf2 -S dfd05592762aa2ac -in MessageSecret -out MessageDecrypt -k Wintermute
$ cat MessageDecrypt
E-o$#PitX$EFeiIY-}K6Wgv8DWpZU8VRRrhAaE{iE($I#E(%#?b1Wc9AaZ4GWo=?*ax5TuZ*?GOVRmI8bZ;PVb#x$MAV@(&OGH6gdvY^GAZkEEYcn@}E-o$#E-o$#Ng!xpc4Z)RZy;=C
VRmI8d2e+rAa`XaY-}KHWo2|AX>K59a&K;QAa7<MbZBKDV{C6@Yc2{dE-n
```

Part 2

The hint say that the first layer use IPv6.

The message retrieved :

`E-o$#PitX$EFeiIY-}K6Wgv8DWpZU8VRRrhAaE{iE($I#E(%#?b1Wc9AaZ4GWo=?*ax5TuZ*?GOVRmI8bZ;PVb#x$MAV@(&OGH6gdvY^GAZkEEYcn@}E-o$#E-o$#Ng!xpc4Z)RZy;=CVRmI`

Use any online tools to decrypt a IPv6 (ASCII85 with alphabet defined in RFC 1924) message.

End

The final Message is :

...
Okay, I'll be there at 5 p.m.
...
Yes, I remember, you have to put a HACKDAY{r3D j@Ck37}...
...
I have to leave you, we'll meet in front of the clock.
...

And the flag is : 'HACKDAY{r3D j@Ck37}' (Red Jacket)