



SH4DOWEEN 2024



CHALLENGE

8 SOLVES

Find IP

200

En la profundas conversaciones de los admins, se ha filtrado un nombre de usuario, ¿seras capaz de encontrarlo y extraer la informacion necesario?
Formato de la flag: ShByte{IP:Puerto}

FindIP.zip

Submit

Reto OSINT FindIP – Easy

Se observa que el reto incluye un archivo en formato TXT que, al parecer, contiene el historial de un chat de Discord. Dentro del archivo, encontramos información sobre un usuario en una red social, lo cual podría ser una pista clave.

```
chat_discord.txt
> cat chat_discord.txt --plain -l java
[YukaFake]: Bueno, cabrones, el plan ya está en marcha. ¿Quién cree que va a tener los pantalones para mandarle mensaje al pinche John? A ver si alguien cae en la trampa.
[briancgx]: jaja ¡A huevo! Conociendo a la banda, ya sabes que mínimo uno le manda el mensaje a @smith_john56008 en los primeros minutos, así de ansiosos están. Solo espero que no se caguen en el intento.

[Maroko]: jaja Ojalá, pero imagínate la cara que van a poner cuando vean que el mensaje es tan directo. Solo tienen que escribir "IGiveMeIp"... si tan solo supieran que no es tan fácil como creen.
[Lychi3]: Ya veo venir los memes y los mensajes frustrados. Van a pensar que John responde de volada, pero nada más no va a pasar ni madres, jaja. Los vamos a dejar colgados un rato.

[YukaFake]: Así es la vida, que aprendan a ser pacientes. Además, con lo trolls que son, a ver si no empiezan a mandarle mensajes como locos al pobre de John. jaja Al rato nos bloquea a todos.

[briancgx]: Solo espero que no se pongan intensos, ya ves cómo son. Unos van a hacerle spam al John y otros, ya sabes, van a reclamar de por qué no les responde. La neta, entre más desesperados, mejor.

[Maroko]: Se van a querer arrancar los pelos cuando vean que John ni los pela. O si responde, seguro les manda una IP que no tiene nada que ver. Pero ese es el chiste, que se quiebren un rato, jaja.
[Lychi3]: Lo bueno es que nosotros nomás estamos aquí mirando el show. A ver quién es el primero que viene a quejarse de que no le respondieron nada, o de que John les dijo puras pendejadas.

[YukaFake]: O peor, ¿te imaginas si al final les da una pista falsa? ¡Van a empezar a sospechar hasta de su propia sombra! Pero, bueno, para eso estamos aquí, para ver cómo se les complica.

[briancgx]: Entonces así queda: ya les dimos el nombre @smith_john56008 y el mensaje "IGiveMeIp". Si se atreven, es su bronca. Nosotros nomás nos sentamos a ver el desastre.
[Maroko]: Exacto, ¡a ver qué pasa! Con suerte, alguien se lanza de lleno. Esto va a estar divertido.

[Lychi3]: jaja Ya veo venir las capturas de pantalla de las respuestas de John o peor, de que no les dijo nada y andan buscando pistas en Twitter como locos. Ojalá lo disfruten, porque nosotros sí lo haremos.

[YukaFake]: Así que, equipo, atentos al show. En cuanto alguien caiga en la trampa y empiece a decir que John no responde, ya sabemos que funcionó. ¡Va a estar de lujo verlos desesperados!
```

Chat de proporcionado

Elabora: Joshua Aviles by @YukaFake



SH4DOWEEN 2024

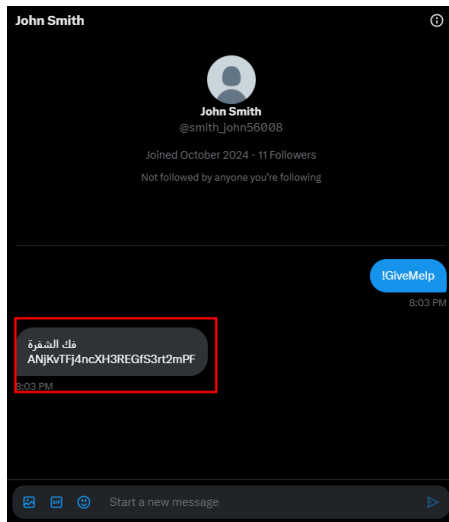


Procedemos a buscar al usuario en varias plataformas sociales, y finalmente lo encontramos en **Twitter**. Esto confirma que hemos identificado el perfil correcto para continuar con el reto.



Identificación de usuario

Siguiendo las instrucciones mencionadas en el chat proporcionado en el archivo, enviamos un mensaje al usuario con el comando !GiveMelp, esperando obtener una respuesta relevante para avanzar en el desafío.



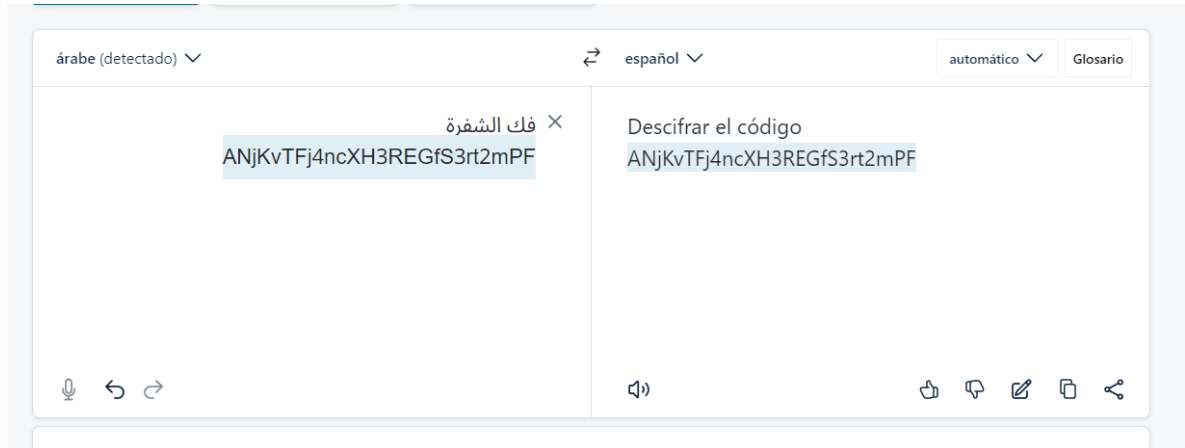
Mensaje que nos envia el usuario



SH4DOWEEN 2024

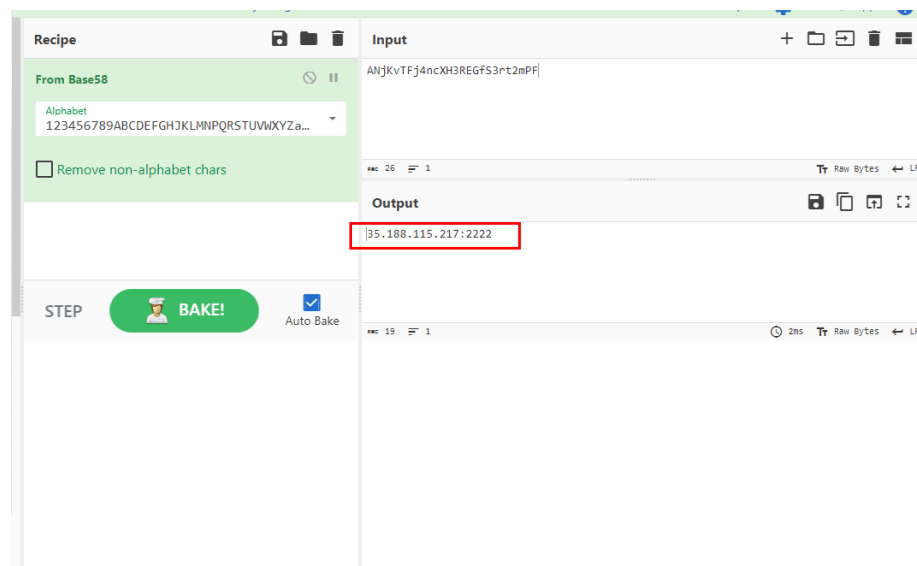


El usuario responde con un mensaje en lo que parece ser un idioma desconocido, acompañado de caracteres extraños. Para interpretar el contenido, copiamos el mensaje y lo pegamos en **DeepL** para identificar el idioma y traducirlo. Esto nos permite entender mejor la respuesta y verificar si contiene alguna pista o información relevante para continuar con el reto.



Traducción de DeepL

Tras obtener la traducción, el mensaje nos indica que debemos descifrar un texto. Siguiendo esta pista, copiamos el contenido y lo ingresamos en **CyberChef**, donde obtenemos el resultado esperado. Con esto en mano, solo queda darle el formato especificado en el reto para completar la solución.



Decodeado en base58