CTF HACKON 2021
OSINT - PROJECT MAYHEM 2

HackOn 2021

https://www.hackon.es/
@HackOnURJC

ENUNCIADO

Comunicaciones interceptadas hablan de la elaboración de una bom-ba. Tenemos que saber cuál va a ser el objetivo para poder evitar una catástrofe.Tal y como indica el mensaje anterior, el método de comunicación ha cambiado.

Nota: formato de flag habitual.

FLAG

HackOn{M0nk3Y1sL4nd}

SOLUCIÓN

Al ser el último reto, nos queda muy poca información con la que trabajar. La primera pista, es el siguiente tuit: “I like to put reviews on the sites I visit.” Esta pista se refiere claramente al tercer yúltimo reto, y habla de “reviews”. La otra pista es un keybase. En el keybase sólo hay guardado una clave PGP. Al importar esta clave, nos da un correo (que se podrá averiguar también), caradeangel1999@gmail.com.

```
~/Desktop
 curl https://keybase.io/caradeangel1999/pgp_keys.asc | gpg --import
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4706  100  4706    0     0   8433      0 --:--:-- --:--:-- --:--:--  8433
gpg: key E08AD82435D9F4C7: public key "Jared Leton <caradeangel1999@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Ahora tenemos que comprobar las reseñas publicadas por este correo. ¿Pero cómo hacemos esto? Necesitamos el GoogleID.

Se pueden usar herramientas automatizadas para esta función, como GHunt o esta página web:

```
1       https://tools.epieos.com/google-account.php
2
```

También se puede obtener de manera manual, añadiendo a contactos el correo en cuestión y buscando manualmente el ID, siguiendo writeups online, como este:

https://www.uk-osint.net/gmailids.html

Una vez tenemos el GoogleID, lo insertamos al final de la siguiente url:

```
https://www.google.com/maps/contrib/ID

```