HTB x Uni CTF 2020 - Quals

Challenge: Weak RSA (crypto)

by santatecla[UOC]

“A rogue employe managed to steal a file from his work computer, he encrypted the file with RSA before he got apprehended. We only managed to recover the public key, can you help us decrypt this ciphertext?”

OS: “Ubuntu:20.04”
Tools: strings, grep

En este reto se entrega un .zip que contiene un archivo llamado “flag.enc”(flag cifrada) y otro “pubkey.pem”(clave pública RSA). El reto es similar al reto de HackTheBox con el mismo nombre, con esta herramienta “https://github.com/Ganapati/RsaCtfTool” se puede descifrar la flag facilmente:

```
$ python3 ./RsaCtfTool.py --publickey pubkey.pem --uncipherfile flag.enc
...
HTB{b16_e_5m4ll_d_3qu4l5_w31n3r_4774ck}'
```