WRITEUP: Ke paaaaaRSA
Categoría: Crypto

Enunciado

Nos han proporcionado este ZIP con un mensaje oculto que necesitamos obtener. Este mensaje ha sido cifrado mediante RSA (el cual es un tipo de cifrado asimétrico). Por motivos de seguridad, también han añadido una contraseña al ZIP, pero al parecer no debe ser muy robusta. ¿Serás capaz de descifrar el mensaje?

Resolución

El nombre del ZIP, junto al nombre del reto, ya nos proporcionan pistas sobre por dónde irán los tiros. Se trata de un reto orientado principalmente al sistema criptográfico de clave pública conocido como RSA. El primer paso será generar un hash del ZIP protegido con contraseña:

```
zip2john your_file.zip > zip.hash
```

Veamos si John The Ripper es capaz de mapearlo con alguna de sus contraseñas conocidas:

```
john zip.hash
```

```
└─$ john zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
hallowell        (Weak_RSA.zip)
1g 0:00:00:00 DONE 2/3 (2024-01-29 19:44) 11.11g/s 891377p/s 891377c/s 891377C/s 123456..ferrises
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Figura 1: Usando las wordlists por defecto de John The Ripper

Vemos que así es! La *passphrase* parece ser **hallowell**, y se encuentra en el diccionario *password.lst* de la mencionada herramienta. Ahora trataremos de descomprimir el ZIP, introduciendo dicha contraseña:

```
unzip Weak_RSA.zip
```

Vemos que el contenido del ZIP es el siguiente:

- **flag.enc**: la flag cifrada
- **key.pub**: una llave pública (probablemente débil en cuanto a longitud según el nombre del ZIP...

En este caso particular de trata de una clave pública de 256 bits (débil e insegura, efectivamente). Existe una herramienta (probablemente haya alguna más) la cual se aprovecha de esta debilidad para forzar a lograr una clave privada que 'matchee' con esta clave pública, permitiendo así descifrar cualquier mensaje que haya sido cifrado con dicha clave pública. Es el caso de RsaCtfTool (ver `https://github.com/RsaCtfTool/RsaCtfTool?tab=readme-ov-file`). Tras su descarga, podremos ejecutar el siguiente comando para obtener una clave privada:

```
./RsaCtfTool/RsaCtfTool.py --publickey key.pub --private
```

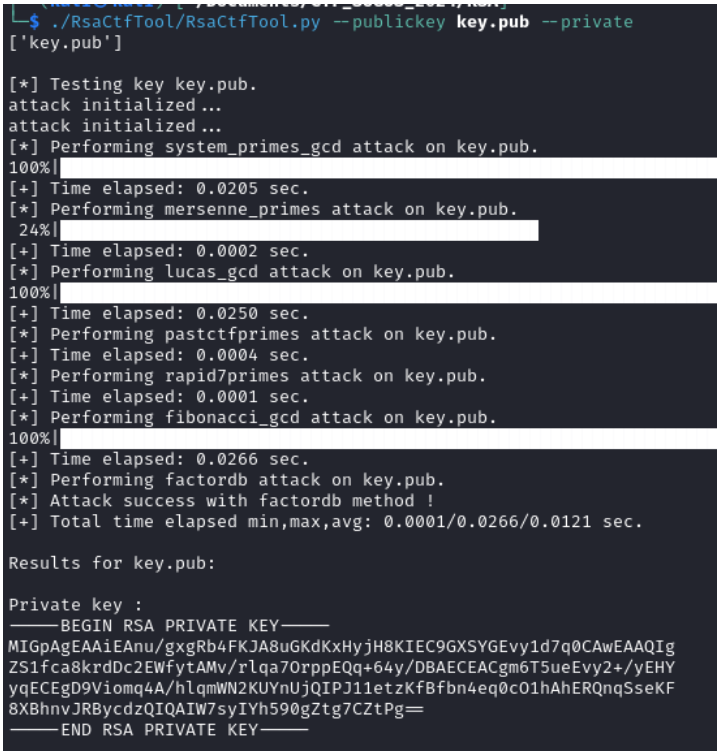


Figura 2: Forzando la clave privada

Esta clave privada obtenida como resultado por el terminal, tendremos que copiar y pegarla en un nuevo fichero, el cual llamaremos *priv.key*. Finalmente podremos emplear alguna herramienta como OpenSSL para, a partir de un mensaje cifrado y una clave privada válida (como es el caso de la forzada), descifrar dicho mensaje para lograr el contenido original (el mensaje en texto plano). Emplearemos el siguiente comando:

```
openssl pkeyutl -decrypt -inkey priv.key -in flag.enc -out dec_flag.txt
```

La flag resultante es:

```
SUGUS{R54_pro!}
```