NeverLAN CTF

Crypto : BabyRSA

Value : 250 pts

Difficulty : Unknown

Description : We’ve intercepted this RSA encrypted message **2193 1745 2164 970 1466 2495 1438 1412 1745 1745 2302 1163 2181 1613 1438 884 2495 2302 2164 2181 884 2302 1703 1924 2302 1801 1412 2495 53 1337 2217** we know it was encrypted with the following public key **e : 569 n: 2533**

Attachment : None

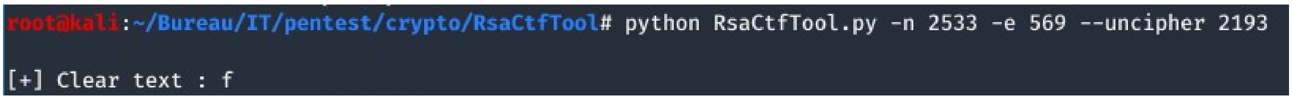
Solution :

First we need to download RsaCtfTool from github. Follow the list bellow for install the tool.

Source : https://github.com/Ganapati/RsaCtfTool

1. git clone https://github.com/Ganapati/RsaCtfTool.git
2. cd RsaCtfTool
3. apt-get install libmpc-dev
4. pip2 install gmpy2
5. pip2 install -r optional-requirements.txt
6. git clone https://github.com/hellman/libnum.git
7. cd libnum
8. python setup.py build
9. python setup.py install
10. apt-get install python3-crypto
11. apt-get install python3-gmpy2

Once the tool installed, we can start to uncipher the message.



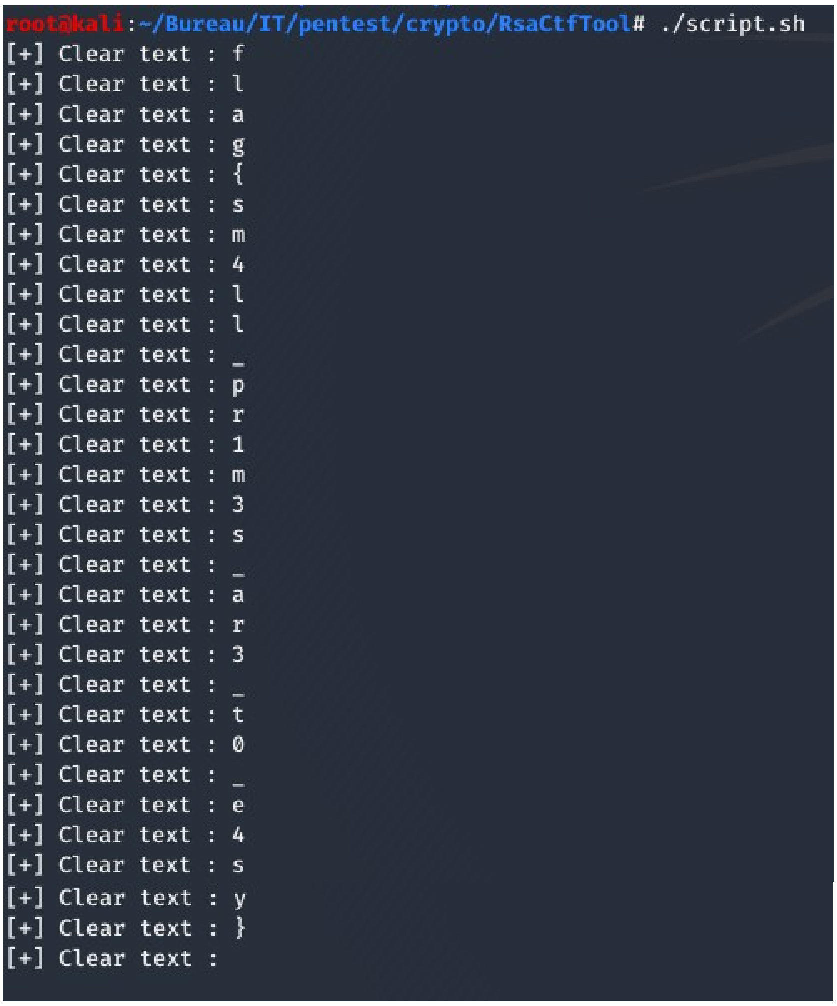
```
root@kali:~/Bureau/IT/pentest/crypto/RsaCtfTool# python RsaCtfTool.py -n 2533 -e 569 --uncipher 2193

[+] Clear text : f
```

It seem to work, the first cipher is the letter «f» for flag.

My team mate @SteelWolf, make a little bash script for automate the process.

```
#!/bin/bash


rsa="RsaCtfTool.py"

cypher=(2193 1745 2164 970 1466 2495 1438 1412 1745 1745 2302 1163 2181 1613 1438 884 2495 2302 2164 2181 884 2302 1703 1924 2302 1801 1412 2495 53 1337 2217)

n="2533"
e="569"

for i in "${cypher[@]}"
do
   python $rsa -n $n -e $e --uncipher $i
done
```

Give it execution right with «chmod +x script.sh» and execute it.



```
root@kali:~/Bureau/IT/pentest/crypto/RsaCtfTool# ./script.sh
[+] Clear text : f
[+] Clear text : l
[+] Clear text : a
[+] Clear text : g
[+] Clear text : {
[+] Clear text : s
[+] Clear text : m
[+] Clear text : 4
[+] Clear text : l
[+] Clear text : l
[+] Clear text : _
[+] Clear text : p
[+] Clear text : r
[+] Clear text : 1
[+] Clear text : m
[+] Clear text : 3
[+] Clear text : s
[+] Clear text : _
[+] Clear text : a
[+] Clear text : r
[+] Clear text : 3
[+] Clear text : _
[+] Clear text : t
[+] Clear text : 0
[+] Clear text : _
[+] Clear text : e
[+] Clear text : 4
[+] Clear text : s
[+] Clear text : y
[+] Clear text : }
[+] Clear text :
```

Flag : flag{sm4ll_pr1m3s_ar3_t0_e4sy}