



Crypto : Weak RSA



Once extracted we got those two files



Some google research and we found a tools for decode them

<https://github.com/Ganapati/RsaCtfTool>

Download it and follow those step for install all dependencies.

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 <http://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

Move or copy&past key.pub and flag.enc into the RsaCtfTool directory, where RsaCtfTool.py is located.

```
cp key.pub /git/RsaCtfTool/  
cp flag.enc /git/RsaCtfTool/
```

Execute RsaCtfTool and get the flag.

```
root@kali:/opt/RsaCtfTool# python2 RsaCtfTool.py --publickey ./key.pub --uncipherfile ./flag.enc --verbose --private
[*] Performing hastads attack.
[*] Performing factordb attack.
-----BEGIN RSA PRIVATE KEY-----
MIIC0QIBAAKBgQMw03kPsUnaNabUlaubn7ip4pNEXjvU0xjvLwUhtybr6Ng4undL
tSQPCPf7ygoUKh1KYeqXMPtmhKjRos3xioTy23CZu0l3WiSLiRKSVYyqBc9d8rxj
NMXuUI0iN038ealcR4p44zfHI66INPuKmTG3RQP/6p5hv1PYcWmErEeDewKBgGEX
xgRIsTlFGrW2C2JXoSvakMCWD60eAH0W2PpDqlqq0FD8JA5UFK0roQk0jhLWSVu8
c6DLpWJQQLXHPqP702qIg/gx2o0bm4EzrCEJ4gYo6Ax+U7q6T0WhQpiBHnC0ojE8
kUoqMhfALpUaruTJ6zmj8IA1e1M6bMqVF8srlb/NAiBhwngxi+Cbie3YBogNzGJV
h10vAgw+i7cQqiiwEiPFNQJBAYZr5r2KkHVjGcZNLRAoXrzJjVhb7knZE5oEYo
nEI+h2gQSt1bavv3YVxhcisTVuNrlgQo58eGb4c9dtY2bLMCQQIX2W9IbtJ26KzZ
C/5HPsVqgxWtuP5hN80Lf3ohhojr1NigJwc6o68dtKScaE05A33vmNpuWqKucecT
0HEVxuE5AiBhwngxi+Cbie3YBogNzGJVh10vAgw+i7cQqiiwEiPFNQIgYcJ4MYvg
m4nt2AaIDcxiVYddLwIMPou3EKoosBIjxTUCQQCnqbJMPEQHpg5LI6MQi8ixFRqo
+KwoBrwYfZlGEwZxdK2Ms0jgeta5jFFS11Fwk5+GyimnRzVcEbADJno/8BKe
-----END RSA PRIVATE KEY-----
[+] Clear text : !c000o@0g0X00{Dn(0D0000x000"0000.,0-)!06W0000000Q+0L00-J90000{00_0SD0YC#004L00U0
0p00/AHTB{s1mpl3_Wi3n3rs_4tt4ck}
```

Flag = HTB{s1mpl3_Wi3n3rs_4tt4ck}