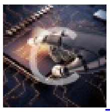
攻防世界 xctf cr4-poor-rsa的 writeup

原创

隐藏起来 于 2020-03-29 17:38:26 发布 1624 收藏 3
分类专栏： CTF # crypto

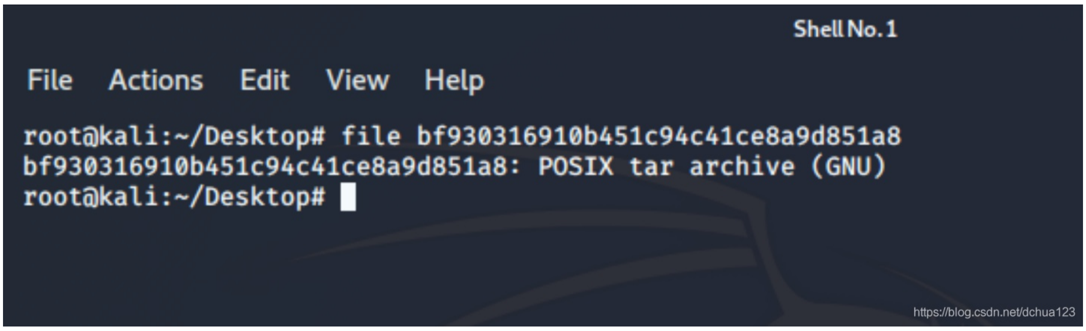
本文链接：https://blog.csdn.net/dchua123/article/details/105182206
版权

CTF 同时被 2 个专栏收录
20 篇文章 3 订阅
订阅专栏



crypto
15 篇文章 0 订阅
订阅专栏

1、下载解压后的是一个文件，用file命令查看是rar文件

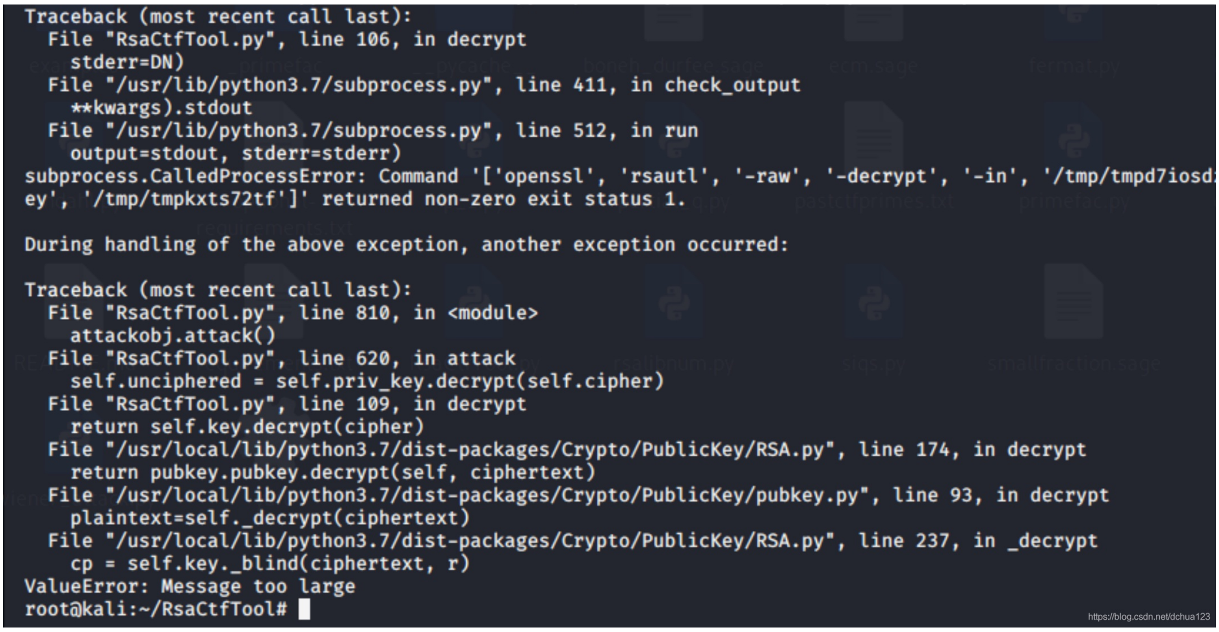


```
root@kali:~/Desktop# file bf930316910b451c94c41ce8a9d851a8
bf930316910b451c94c41ce8a9d851a8: POSIX tar archive (GNU)
root@kali:~/Desktop# 
```

2、改后缀解压得flag.b64和key.pub。尝试用RsaCtfTool解密，于是先对flag进行base64解码，保持为flag.b64.bin

```
python3 RsaCtfTool.py --publickey ~/Desktop/key.pub --uncipherfile ~/Desktop/flag.b64.bin
```

结果报错了，如下：



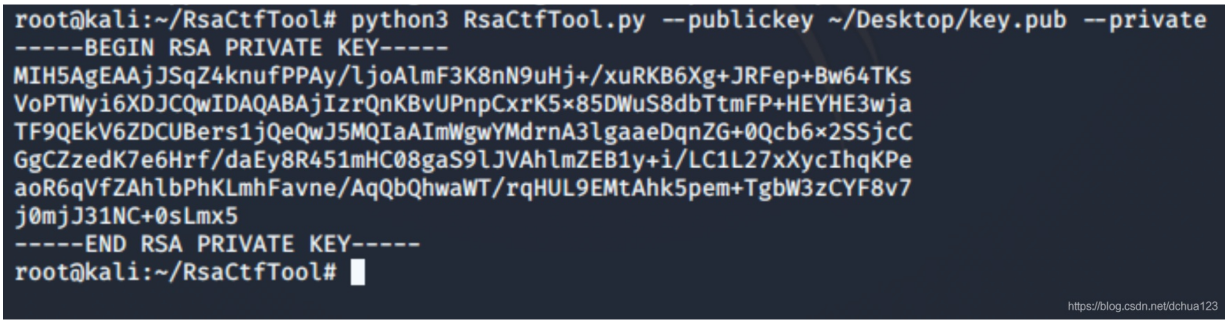
```
Traceback (most recent call last):
  File "RsaCtfTool.py", line 106, in decrypt
    stderr=DN)
  File "/usr/lib/python3.7/subprocess.py", line 411, in check_output
    **kwargs).stdout
  File "/usr/lib/python3.7/subprocess.py", line 512, in run
    output=stdout, stderr=stderr)
subprocess.CalledProcessError: Command '['openssl', 'rsautl', '-raw', '-decrypt', '-in', '/tmp/tmpd7iosd
ey', '/tmp/tmpkxts72tf']' returned non-zero exit status 1.

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "RsaCtfTool.py", line 810, in <module>
    attackobj.attack()
  File "RsaCtfTool.py", line 620, in attack
    self.unciphered = self.priv_key.decrypt(self.cipher)
  File "RsaCtfTool.py", line 109, in decrypt
    return self.key.decrypt(cipher)
  File "/usr/local/lib/python3.7/dist-packages/Crypto/PublicKey/RSA.py", line 174, in decrypt
    return pubkey.pubkey.decrypt(self, ciphertext)
  File "/usr/local/lib/python3.7/dist-packages/Crypto/PublicKey/pubkey.py", line 93, in decrypt
    plaintext=self._decrypt(ciphertext)
  File "/usr/local/lib/python3.7/dist-packages/Crypto/PublicKey/RSA.py", line 237, in _decrypt
    cp = self.key._blind(ciphertext, r)
ValueError: Message too large
root@kali:~/RsaCtfTool# █
```

百思不得其解，以为是pycrypto的问题，安装重新卸载，或者安装crypto都不行，那就只能换思路了。

3、考虑到可以用私钥进行解密，于是先生成私钥：

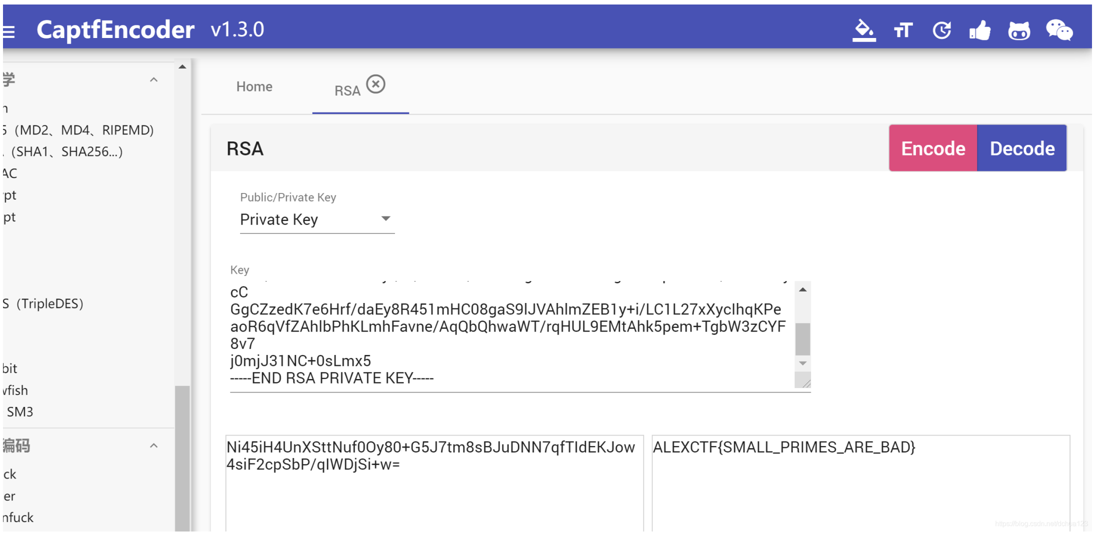
```
python3 RsaCtfTool.py --publickey ~/Desktop/key.pub --privatekey
```

生成私钥如下：



```
root@kali:~/RsaCtfTool# python3 RsaCtfTool.py --publickey ~/Desktop/key.pub --private
-----BEGIN RSA PRIVATE KEY-----
MIH5AgEAAjJSqZ4knufPPAy/ljoAlmF3K8nN9uHj+/xuRKB6Xg+JRFep+Bw64TKs
VoPTWyi6XDJCQwIDAQABAjIzrQnKBvUPnpCxrK5×85DWuS8dbTtmFP+HEYHE3wja
TF9QEkV6ZDCUBers1jQeQwJ5MQIaAImWgwYMdrnA3lgaaeDqnZG+0Qcb6×2SSjcC
GgCZzedK7e6Hrf/daEy8R451mHC08gaS9lJVAhlmZEB1y+i/LC1L27xXycIhqKPe
aoR6qVfZAhlbPhKLmhFavne/AqQbQhwaWT/rqHUL9EMtAhk5pem+TgbW3zCYF8v7
j0mjJ31NC+0sLmx5
-----END RSA PRIVATE KEY-----
root@kali:~/RsaCtfTool# █
```

4、丢到工具里去解密，注意这里的文本为未解密的base64编码：



Public/Private Key
Private Key

Key

```
cC
GgCZzedK7e6Hrf/daEy8R451mHC08gaS9lJVAhlmZEB1y+i/LC1L27xXycIhqKPe
aoR6qVfZAhlbPhKLmhFavne/AqQbQhwaWT/rqHUL9EMtAhk5pem+TgbW3zCYF
8v7
j0mjJ31NC+0sLmx5
-----END RSA PRIVATE KEY-----
```

```
Ni45iH4UnXSttNuf0Oy80+G5J7tm8sBJuDNN7qfTIdEKJow
4siF2cpSbP/qIWDjSi+w=
```

```
ALEXCTF{SMALL_PRIMES_ARE_BAD}
```

得flag：

```
ALEXCTF{SMALL_PRIMES_ARE_BAD}
```