Pony7 Wiki

Decrypt It - Writeup by Maxima

Challenge

```
$ ./cryptooo SECCON{*************************}
Encrypted(44): waUqjjDGnYxVyvUOLN8HquEO0J5Dqkh/zr/3KXJCEnw=
```

what's the key?

cryptooo.zip
[https://github.com/SECCON/SECCON2015_online_CTF/blob/master/Crypto/300_Decrypt%20it/cry

Solution

The binary takes an argument and shows us the encrypted argument, encoded in base64.

```
$ ./cryptooo aaaaaaaaaaaaaaaaaaa
Encrypted(28): 8yc36kAk+W405+OOjZ5l+sd+hg==
```

We can quickly notice that changing one character doesn't change the beginning of the encrypted argument:

```
$ ./cryptooo aaaaaaaaaaaaaaaaaab
Encrypted(28): 8yc36kAk+W405+OOjZ5l+sd+hQ==
```

Thus we can easily brute force character by character, using a Python script:

```
#!/usr/bin/env python3
import subprocess
import re
import base64


def encrypt(flag):
    if not flag:
        return b''

    print('Encrypting %s' % flag)
    p = subprocess.Popen(['./cryptooo', flag], stdout=subprocess.PIPE)
    p.wait()
    buf = p.stdout.read().decode('ascii')

    groups = re.search(r'Encrypted\(\d+\): (.*)\n', buf)
    data = groups.group(1)
    return base64.b64decode(data)

charset = ''.join(chr(c) for c in range(32, 127))
encrypted = base64.b64decode('waUqjjDGnYxVyvUOLN8HquEO0J5Dqkh/zr/3KXJCEnw=')

flag = ''
while encrypt(flag) != encrypted:
    found = False

    for c in charset:
        if encrypted.startswith(encrypt(flag + c)):
            flag += c
            found = True
            break

    assert found

print('Found flag: %s' % flag)
```

The flag is SECCON{Cry_Pto_Oo_Oo1Oo_oo_Oo_O}

Author

Maxime Arthaud [mailto:maxime@arthaud.me] 2015/12/07 09:56