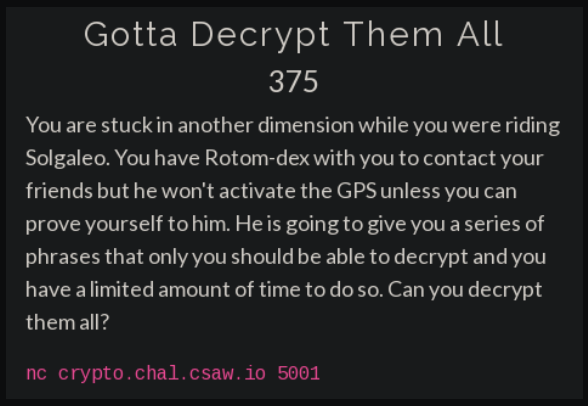
Gotta Decrypt Them All

CSAW 2021 CTF

GoProSlowYo



2021-09-10

Contents

Gotta Decrypt Them All

Writeup by: GoProSlowYo solved by Perryman

Team: OnlyFeet

Writeup URL: GitHub

```
You are stuck in another dimension while you were riding Solgaleo. You
   have Rotom-dex with you to contact your friends but he won't
   activate the GPS unless you can prove yourself to him. He is going
   to give you a series of phrases that only you should be able to
   decrypt and you have a limited amount of time to do so. Can you
   decrypt them all?

nc crypto.chal.csaw.io 5001
```

Solve Script

```python
from pwn import *
import base64
import subprocess
import re
import codecs


def decodemorse(morse):
    p = morse
    p = p.replace('.---- ', '1')
    p = p.replace('..--- ', '2')
    p = p.replace('...-- ', '3')
    p = p.replace('....- ', '4')
    p = p.replace('..... ', '5')
    p = p.replace('-.... ', '6')
    p = p.replace('--... ', '7')
    p = p.replace('---.. ', '8')
    p = p.replace('----. ', '9')
    p = p.replace('----- ', '0')
    p = p.split('/')
    p = ''.join([chr(int(i)) for i in p])
    print(p)
    p = base64.b64decode(p).decode("utf-8")
    p = p.split('\n')
    p = [i.split(' = ') for i in p]
    N = int(p[0][1])
```

```
    e = int(p[1][1])
    c = int(p[2][1])
    print(p)
    print(N)
    print(e)
    print(c)
    command = "python3 ./RsaCtfTool/RsaCtfTool.py -n " + \
        str(N) + " -e " + str(e) + " --uncipher " + \
        str(c) + " --attack cube_root"

    process = subprocess.Popen(command.split(), stdout=subprocess.PIPE)
    output, error = process.communicate()
    result = re.findall(b"(?<=STR : b').*(?=')", output)
    result = result[0].decode("utf-8")
    result = codecs.encode(result, 'rot_13')
    print(f'{result=}')
    return result


def sendit(r, x, variable_name="", verbose=True):
    r.sendline(str(x))
    if verbose:
        print(f"\tsend {variable_name}: {x}")


def recvit(r, variable_name="", verbose=True):
    s = r.recv().strip()
    s = s.decode("utf-8")
    if verbose:
        print(f"\treceived {variable_name}: {s}")
    return s


def tryit():
    curcase = 1
    with remote("crypto.chal.csaw.io", 5001) as r:
        r.recvuntil('What does this mean?')
        v = recvit(r, verbose=False)

        v = r.recvuntil('\r\n>>')
        v = v.decode("utf-8")
        v = v.strip('\r\n>>')

        a = decodemorse(v)
        print(f'{a=}')
        sendit(r, a, verbose=True)  # decode and send answer back

        q = r.recvuntil('What does this mean?')
        print(f'{q=}')
        v = recvit(r, verbose=False)
        v = r.recvuntil('\r\n>>')
```

```
        v = v.decode("utf-8")
        v = v.strip('\r\n>>')
        a = decodemorse(v)
        print(f'{a=}')
        sendit(r, a, verbose=True)  # decode and send answer back

        q = r.recvuntil('What does this mean?')
        print(f'{q=}')
        v = recvit(r, verbose=False)
        v = r.recvuntil('\r\n>>')
        v = v.decode("utf-8")
        v = v.strip('\r\n>>')
        a = decodemorse(v)
        print(f'{a=}')
        sendit(r, a, verbose=True)  # decode and send answer back

        q = r.recvuntil('What does this mean?')
        print(f'{q=}')
        v = recvit(r, verbose=False)
        v = r.recvuntil('\r\n>>')
        v = v.decode("utf-8")
        v = v.strip('\r\n>>')
        a = decodemorse(v)
        print(f'{a=}')
        sendit(r, a, verbose=True)  # decode and send answer back

        q = r.recvuntil('What does this mean?')
        print(f'{q=}')
        v = recvit(r, verbose=False)
        v = r.recvuntil('\r\n>>')
        v = v.decode("utf-8")
        v = v.strip('\r\n>>')
        a = decodemorse(v)
        print(f'{a=}')
        sendit(r, a, verbose=True)  # decode and send answer back

        q = r.recvuntil('What does this mean?')
        print(f'{q=}')
        v = recvit(r, verbose=False)
        v = r.recvuntil('\r\n>>')
        v = v.decode("utf-8")
        v = v.strip('\r\n>>')
        a = decodemorse(v)
        print(f'{a=}')
        sendit(r, a, verbose=True)  # decode and send answer back

        print('***********')
        v = recvit(r, verbose=True)
        v = recvit(r, verbose=True)
        v = recvit(r, verbose=True)

```

```
129
130 tryit()
```

Victory

Submit the flag and claim the points:

flag{some FLAG}