

Cutter Training

r2con 2019

Training Materials: bit.ly/2m0dsbY

Introduction

Exercise 1: Tiny Vault

Download [TinyVault.zip](#)

This is a small crackme.

Find the correct input that will print “Welcome to the vault!”

Exercise 2: M1ghty Ransomware

Download [M1ghtyRansomware.zip](#) (password: “cutter”)

You are given with two files, a binary file and an encrypted image.

Your goal is to analyze the binary with Cutter, detect the encryption algorithms and the keys used to encrypt the flag.

Write a script to Decrypt the image and get the FLAG!

*try using the **Emulation** feature*



flag.png



M1ghtyRansomware.exe

Exercise 2: M1ghty Ransomware - Hints

fcn.140001440 -> **Main Function**

fcn.1400012c0 -> **RC4**

fcn.140001090 -> **KSA** (part of RC4 Algorithm)

fcn.140001190 -> **PRGA** (part of RC4 Algorithm)

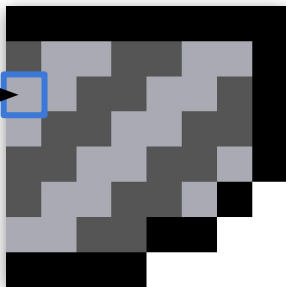
Exercise 3: Gameboy



<http://www.huderlem.com/demos/gameboy2bpp.html>

Diagram illustrating the layout of a 128-bit vector (represented as a sequence of 16 hex digits) grouped into 8 rows (row 0 to row 7). The vector is divided into two 64-bit halves, each containing four 16-bit segments. The segments are labeled as follows:

Row	Segment 1 (16 bits)	Segment 2 (16 bits)	Segment 3 (16 bits)	Segment 4 (16 bits)
row 0	ff	ff	66	99
row 1	cc	33	99	66
row 2	33	cc	66	99
row 3	cc	33	ff	ff
row 4	ff	ff	66	99
row 5	cc	33	99	66
row 6	33	cc	66	99
row 7	cc	33	ff	ff

$$01 = 1$$


```
import base64
a = base64.b64decode(b)
b = base64.b64encode(a)
```

w6d <base64>