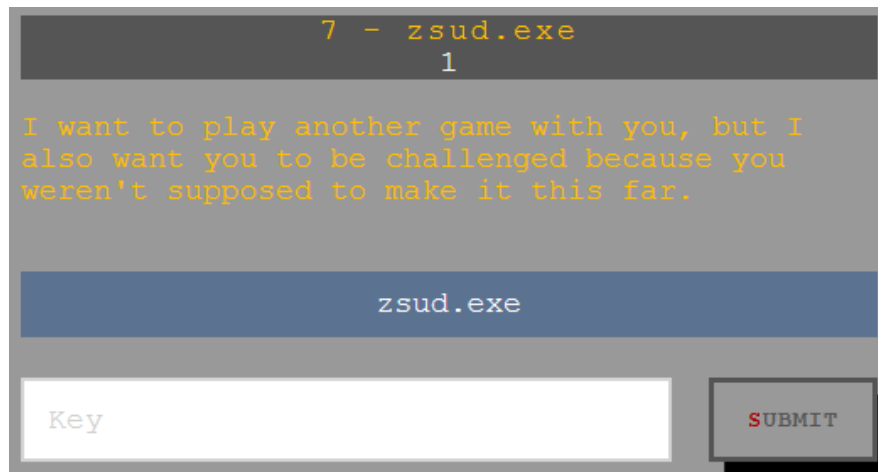


Write-up cho Chal7 của Flare-on4.

1. Thu thập thông tin

- Target nhận được là một file exe: `zsud.exe`



- Kiểm tra thông tin sơ bộ:
 - o Định dạng file là: **PE32**
 - o Được code bằng Visual C: **Microsoft Visual C/C++(2013)[-]**
 - o Tìm kiếm thông tin về string, thấy có một số string thú vị sau:

Mozilla/5.0 (iPhone; CPU iPhone OS 8_0 like Mac OS X) AppleWebKit/600.1.3 (KHTML, like Gecko) Versio..

M:\whiskey_tango_flareon.dll

soooooo_sorry_zis_is_not_ze_flag

<http://127.0.0.1:9999/some/thing.asp>

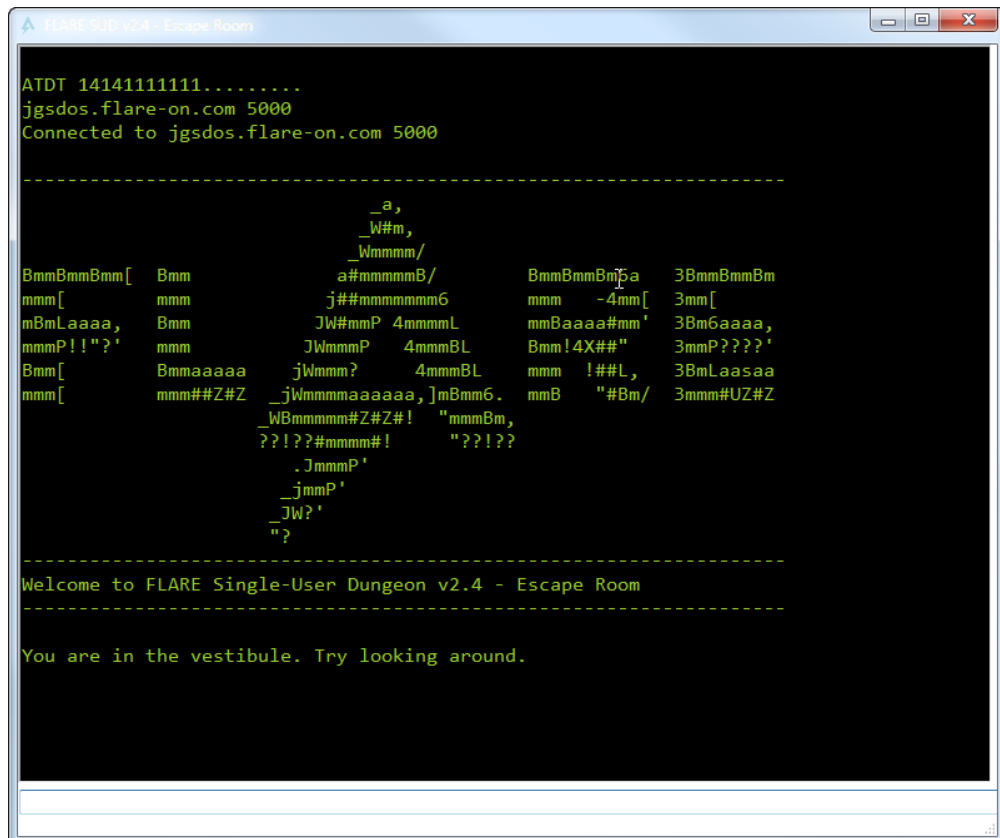
- o Tìm kiếm thông tin liên quan tới Crypto: thấy có các thông tin liên quan tới Base64; Rijndael
- o Mở file bằng một trình Hex Editor bất kỳ, tìm kiếm và thấy có dấu hiệu của một PE file khác. Khả năng `zsud.exe` khi chạy sẽ drop ra PE file này. Thông tin về PE file được tìm thấy nằm tại offset như trong hình dưới:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
5:70B0h:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ýý..
5:70C0h:	B8)	00	00	00	00	00	00	40	00	00	00	00	00	00	00	(,).@.....
5:70D0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
5:70E0h:	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00€...
5:70F0h:	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..'Í!..LÍ!Th
5:7100h:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
5:7110h:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
5:7120h:	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
5:7130h:	50	45	00	00	4C	01	03	00	20	E1	A8	59	00	00	00	00	PE..L... á`Y....
5:7140h:	00	00	00	00	E0	00	02	21	0B	01	0B	00	00	0A	00	00à..!.....
5:7150h:	00	06	00	00	00	00	00	00	7E	29	00	00	00	20	00	00~)....
5:7160h:	00	40	00	00	00	00	00	10	00	20	00	00	00	02	00	00	.@.....
5:7170h:	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00
5:7180h:	00	80	00	00	00	02	00	00	00	00	00	00	03	00	40	85	.€.....@...
5:7190h:	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00
5:71A0h:	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00
5:71B0h:	30	29	00	00	4B	00	00	00	00	40	00	00	A0	02	00	00	0)..K....@..
5:71C0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
5:71D0h:	00	60	00	00	0C	00	00	00	00	00	00	00	00	00	00	00	..`.....
5:71E0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
5:71F0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
5:7200h:	00	00	00	00	00	00	00	00	00	20	00	00	08	00	00	00
5:7210h:	00	00	00	00	00	00	00	00	08	20	00	00	48	00	00	00H...
5:7220h:	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00text...
5:7230h:	84	09	00	00	00	20	00	00	00	0A	00	00	00	02	00	00
5:7240h:	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60`
5:7250h:	2E	72	73	72	63	00	00	00	A0	02	00	00	00	40	00	00	.rsrc... ..@..

- Quan sát thông tin sơ bộ PE file trên, nhận thấy đây là một file dạng dll, có tên là: **flareon.dll**. File dll này có thể được code bằng .NET và code của nó có gọi gì đó liên quan tới PowerShell:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
5:7770h:	00	00	00	00	00	00	00	00	00	3C	4D	6F	64	75	6C	65<Module
5:7780h:	3E	00	66	6C	61	72	65	6F	6E	2E	64	6C	6C	00	66	6F	>.flareon.dll.fo
5:7790h:	75	72	00	66	6C	61	72	65	6F	6E	00	6D	73	63	6F	72	ur.flareon.mscor
5:77A0h:	6C	69	62	00	53	79	73	74	65	6D	00	4F	62	6A	65	63	lib.System.Objec
5:77B0h:	74	00	44	65	63	72	79	70	74	32	00	53	6D	74	68	00	t.Decrypt2.Smth.
5:77C0h:	2E	63	74	6F	72	00	63	69	70	68	65	72	54	65	78	74	.ctor.cipherText
5:77D0h:	00	6B	65	79	00	61	72	67	00	53	79	73	74	65	6D	2E	.key.arg.System.
5:77E0h:	52	75	6E	74	69	6D	65	2E	43	6F	6D	70	69	6C	65	72	Runtime.Compiler
5:77F0h:	53	65	72	76	69	63	65	73	00	43	6F	6D	70	69	6C	61	Services.Compila
5:7800h:	74	69	6F	6E	52	65	6C	61	78	61	74	69	6F	6E	73	41	tionRelaxationsA
5:7810h:	74	74	72	69	62	75	74	65	00	52	75	6E	74	69	6D	65	ttribute.Runtime
5:7820h:	43	6F	6D	70	61	74	69	62	69	6C	69	74	79	41	74	74	CompatibilityAtt
5:7830h:	72	69	62	75	74	65	00	53	79	73	74	65	6D	2E	54	65	tribute.System.Te
5:7840h:	78	74	00	45	6E	63	6F	64	69	6E	67	00	67	65	74	5F	xt.Encoding.get_
5:7850h:	55	54	46	38	00	47	65	74	42	79	74	65	73	00	42	79	UTF8.GetBytes.By
5:7860h:	74	65	00	53	79	73	74	65	6D	2E	53	65	63	75	72	69	te.System.Security.
5:7870h:	74	79	2E	43	72	79	70	74	6F	67	72	61	70	68	79	00	ty.Cryptography.
5:7880h:	52	69	6A	6E	64	61	65	6C	4D	61	6E	61	67	65	64	00	RijndaelManaged.
5:7890h:	53	79	6D	6D	65	74	72	69	63	41	6C	67	6F	72	69	74	SymmetricAlgorit
5:78A0h:	68	6D	00	73	65	74	5F	4B	65	79	00	73	65	74	5F	49	hm.set_Key.set_I
5:78B0h:	56	00	67	65	74	5F	4B	65	79	00	67	65	74	5F	49	56	V.get_Key.get_IV
5:78C0h:	00	49	43	72	79	70	74	6F	54	72	61	6E	73	66	6F	72	.ICryptoTransfor
5:78D0h:	6D	00	43	72	65	61	74	65	44	65	63	72	79	70	74	6F	m.CreateDecrypto
5:78E0h:	72	00	53	79	73	74	65	6D	2E	49	4F	00	4D	65	6D	6F	r.System.IO.Memo
5:78F0h:	72	79	53	74	72	65	61	6D	00	43	72	79	70	74	6F	53	ryStream.CryptoS
5:7900h:	74	72	65	61	6D	00	53	74	72	65	61	6D	00	43	72	79	tream.Stream.Cry
5:7910h:	70	74	6F	53	74	72	65	61	6D	4D	6F	64	65	00	53	74	ptoStreamMode.St
5:7920h:	72	65	61	6D	52	65	61	64	65	72	00	54	65	78	74	52	reamReader.TextR
5:7930h:	65	61	64	65	72	00	52	65	61	64	54	6F	45	6E	64	00	eadler.ReadToEnd.
5:7940h:	49	44	69	73	70	6F	73	61	62	6C	65	00	44	69	73	70	IDisposable.Disp
5:7950h:	6F	73	65	00	53	79	73	74	65	6D	2E	4D	61	6E	61	67	ose.System.Manag
5:7960h:	65	6D	65	6E	74	2E	41	75	74	6F	6D	61	74	69	6F	6E	ement.Automation
5:7970h:	00	50	6F	77	65	72	53	68	65	6C	6C	00	43	72	65	61	.PowerShell.Crea
5:7980h:	74	65	00	43	6F	6E	76	65	72	74	00	46	72	6F	6D	42	te.Convert.FromB
5:7990h:	61	73	65	36	34	53	74	72	69	6E	67	00	41	64	64	53	ase64String.AddS
5:79A0h:	63	72	69	70	74	00	53	79	73	74	65	6D	2E	43	6F	6C	cript.System.Col
5:79B0h:	6C	65	63	74	69	6F	6E	73	2E	4F	62	6A	65	63	74	4D	lections.ObjectM
5:79C0h:	6F	64	65	6C	00	43	6F	6C	6C	65	63	74	69	6F	6E	60	odel.Collection`

- Chạy thử file zsud.exe, nhận được giao diện của Escape Room:



- Tìm hiểu thông qua help thì biết được đây là một mini game, người chơi phải đi theo ý đồ của tác giả, sau đó tiến hành các hành động như nhặt đồ, mặc đồ, bỏ đồ đã nhặt, nói chuyện với ai đó ...

2. Extract embedded flareon.dll

Sử dụng công cụ của bên thứ ba để kiểm tra lại, có được thông tin về file PE file được nhúng là một DLL và kích thước của file này:

```
Win32 executable found at offset 0x0 size 385536 bytes
Win32 DLL found at offset 0x570b0 size 4608 bytes
2 PE file(s) found from the whole file.
```

Thực hiện trích xuất toàn bộ file DLL từ file zsud.exe và lưu lại với tên là **flareon.dll**:

```
[+] Size of PE file: (0x1200) 4608 bytes = 4.50 kb
PE file successfully carved!
```

Kiểm tra file flareon.dll, biết được file này được code bằng .NET (đúng như thông tin đã phán đoán ở trên): **.NET(v4.0.30319)[-]**. Sử dụng công cụ dnSpy để decompile, có được toàn bộ class four cùng với 2 method là **Smth** và **Decrypt2** như sau:

```

1 // flareon.four
2 // Token: 0x06000002 RID: 2 RVA: 0x00002164 File Offset: 0x00000364
3 public static int Smth(string arg)
4 {
5     using (PowerShell powerShell = PowerShell.Create())
6     {
7         try
8         {
9             byte[] cipherText = Convert.FromBase64String(arg);
10            string script = four.Decrypt2(cipherText, "soooooo_sorry_zis_is_not_ze_flag");
11            powerShell.AddScript(script);
12            Collection<PSObject> collection = powerShell.Invoke();
13            foreach (PSObject value in collection)
14            {
15                Console.WriteLine(value);
16            }
17        }
18        catch (Exception ex)
19        {
20            Console.WriteLine("Exception received");
21        }
22    }
23    return 0;
24 }

```

```

1 // flareon.four
2 // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
3 private static string Decrypt2(byte[] cipherText, string key)
4 {
5     byte[] bytes = Encoding.UTF8.GetBytes(key);
6     byte[] array = new byte[16];
7     byte[] iv = array;
8     string result = null;
9     using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
10    {
11        rijndaelManaged.Key = bytes;
12        rijndaelManaged.IV = iv;
13        ICryptoTransform transform = rijndaelManaged.CreateDecryptor(rijndaelManaged.Key, rijndaelManaged.IV);
14        using (MemoryStream memoryStream = new MemoryStream(cipherText))
15        {
16            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, transform, CryptoStreamMode.Read))
17            {
18                using (StreamReader streamReader = new StreamReader(cryptoStream))
19                {
20                    result = streamReader.ReadToEnd();
21                }
22            }
23        }
24    }
25    return result;
26 }

```

Nghiên cứu toàn bộ code trên:

- **Smth(string arg)**: method này nhận tham số truyền vào là một chuỗi có dạng Base64String, chuỗi này được chuyển đổi và lưu vào một mảng byte[] là cipherText. Sau đó sẽ gọi method Decrypt2 để tiến hành giải mã cipherText thu được.
- **Decrypt2(byte[] cipherText, string key)**: thực hiện giải mã toàn bộ cipherText với key giải mã là "soooooo_sorry_zis_is_not_ze_flag".
- Kết quả sau khi giải mã sẽ là một PowerShell script được lưu vào biến script. Sau đó, thực hiện script này thông qua **powerShell.Invoke()**.

Như vậy, để có được PowerShell script, phải tìm được chuỗi Base64 đầu vào để giải mã là gì.

3. Tìm chuỗi Base64 và lấy PowerShell script

Kết hợp với quá trình phân tích tĩnh bằng IDA và debug thông qua OllyDbg, tìm được nơi khởi tạo ra chuỗi Base64 có độ dài 0x0000E12D (57645) tại **sub_4023D0()**.

Address	Value	Comment
0018ECA0	0059ADF8	
0018ECA4	0018ED04	UNICODE "M:\whiskey_tango_flareon.dll"
0018ECA8	005C6C48	UNICODE "flareon.four"
0018ECAC	005BA5D0	UNICODE "Smth"
0018ECB0	005758B0	UNICODE "Sbogppc38m/yviiq2JXr-GM4WBTByadKkg6ssIToRSDY5x5Uwgnllk0pSf8m78tttUoMIT7uZtNYT+OsuipIqz1lQjHAe50o0XXs8"
0018ECB4	0018E9F8	
0018ECB8	00000000	
0018ECBC	00000058	
0018ECC0	00000000	
0018ECC4	00000002	
0018ECC8	00591F28	ASCII "CorBindToRuntimeEx"
0018ECCC	00000002	
0018ECD0	00560050	UNICODE "v4.0.30319"
0018ECD4	00000002	
0018ECD8	005C6C48	UNICODE "flareon.four"
0018EDEC	00000002	
0018EE00	00591B18	ASCII "mscoree.dll"
0018EE04	00000002	

Address	Hex dump	ASCII
005758B0	53 00 62 00 6F 00 67 00 70 00 70 00 63 00 33 00	S . b . o . g . p . p . c . 3 .
005758C0	38 00 6D 00 2F 00 79 00 76 00 69 00 69 00 71 00	8 . m . / . y . v . i . i . q .
005758D0	32 00 4A 00 58 00 72 00 47 00 4D 00 34 00 57 00	2 . J . X . r . G . M . 4 . W .
005758E0	42 00 54 00 42 00 79 00 61 00 64 00 4B 00 6B 00	B . T . B . y . a . d . K . k .
005758F0	67 00 36 00 73 00 73 00 49 00 54 00 6F 00 52 00	g . 6 . s . s . I . T . o . R .
00575900	53 00 44 00 59 00 35 00 78 00 35 00 55 00 77 00	S . D . Y . 5 . x . 5 . U . w .
00575910	67 00 6E 00 31 00 6C 00 6B 00 30 00 70 00 53 00	g . n . l . l . k . 0 . p . S .
00575920	66 00 38 00 6D 00 37 00 38 00 74 00 74 00 74 00	f . 8 . m . 7 . 8 . t . t . t .
00575930	55 00 6F 00 4D 00 49 00 54 00 37 00 75 00 5A 00	U . o . M . I . T . 7 . u . Z .
00575940	74 00 4E 00 59 00 54 00 74 00 4F 00 73 00 75 00	t . N . Y . T . t . O . s . u .
00575950	69 00 70 00 49 00 71 00 7A 00 6C 00 31 00 51 00	i . p . I . q . z . l . l . Q .
00575960	6A 00 48 00 41 00 65 00 35 00 4F 00 6F 00 30 00	j . H . A . e . 5 . 0 . o . 0 .
00575970	58 00 58 00 73 00 38 00 2B 00 47 00 52 00 77 00	X . X . s . 8 . + . G . R . w .
00575980	77 00 76 00 79 00 75 00 52 00 36 00 6F 00 75 00	w . v . y . u . R . 6 . o . u .
00575990	51 00 61 00 45 00 57 00 6F 00 6C 00 34 00 70 00	Q . a . E . W . o . l . 4 . p .
005759A0	62 00 69 00 32 00 50 00 68 00 52 00 54 00 69 00	b . i . 2 . P . h . R . T . i .
005759B0	2B 00 67 00 65 00 6F 00 53 00 78 00 56 00 76 00	+ . g . e . o . S . x . V . v .
005759C0	42 00 42 00 76 00 79 00 52 00 78 00 44 00 76 00	B . B . v . y . R . x . D . v .
005759D0	76 00 73 00 6A 00 57 00 70 00 65 00 69 00 45 00	v . s . j . W . p . e . i . E .
005759E0	49 00 46 00 78 00 6C 00 6C 00 48 00 49 00 5A 00	I . F . x . l . l . H . I . Z .
005759F0	53 00 76 00 33 00 68 00 52 00 36 00 31 00 50 00	S . v . 3 . h . R . 6 . 1 . P .
00575A00	33 00 4D 00 76 00 4C 00 58 00 62 00 65 00 4B 00	3 . M . v . L . X . b . e . K .
00575A10	53 00 77 00 6F 00 48 00 6C 00 37 00 65 00 6D 00	S . w . o . H . l . 7 . e . m .
00575A20	56 00 61 00 2F 00 31 00 73 00 2B 00 51 00 32 00	V . a . / . l . s . + . Q . 2 .
00575A30	31 00 4F 00 48 00 6B 00 63 00 69 00 45 00 49 00	1 . O . H . k . c . i . E . I .
00575A40	74 00 4D 00 73 00 4C 00 73 00 59 00 69 00 63 00	t . M . s . L . s . Y . i . c .
00575A50	55 00 67 00 66 00 4A 00 53 00 6E 00 74 00 46 00	U . g . f . J . S . n . t . F .
00575A60	39 00 4D 00 6A 00 6E 00 70 00 78 00 68 00 67 00	9 . M . j . n . p . x . h . g .
00575A70	46 00 65 00 71 00 52 00 77 00 32 00 55 00 4D 00	F . e . q . R . w . 2 . U . M .
00575A80	59 00 6D 00 64 00 6A 00 6C 00 53 00 41 00 6D 00	Y . m . d . j . l . S . A . m .
00575A90	4E 00 4F 00 6A 00 61 00 79 00 6A 00 54 00 37 00	N . O . j . a . y . j . T . 7 .
00575AA0	5A 00 64 00 45 00 47 00 72 00 64 00 38 00 76 00	Z . d . E . G . r . d . 8 . v .
00575AB0	48 00 65 00 36 00 45 00 69 00 41 00 66 00 4C 00	H . e . 6 . E . i . A . f . L .

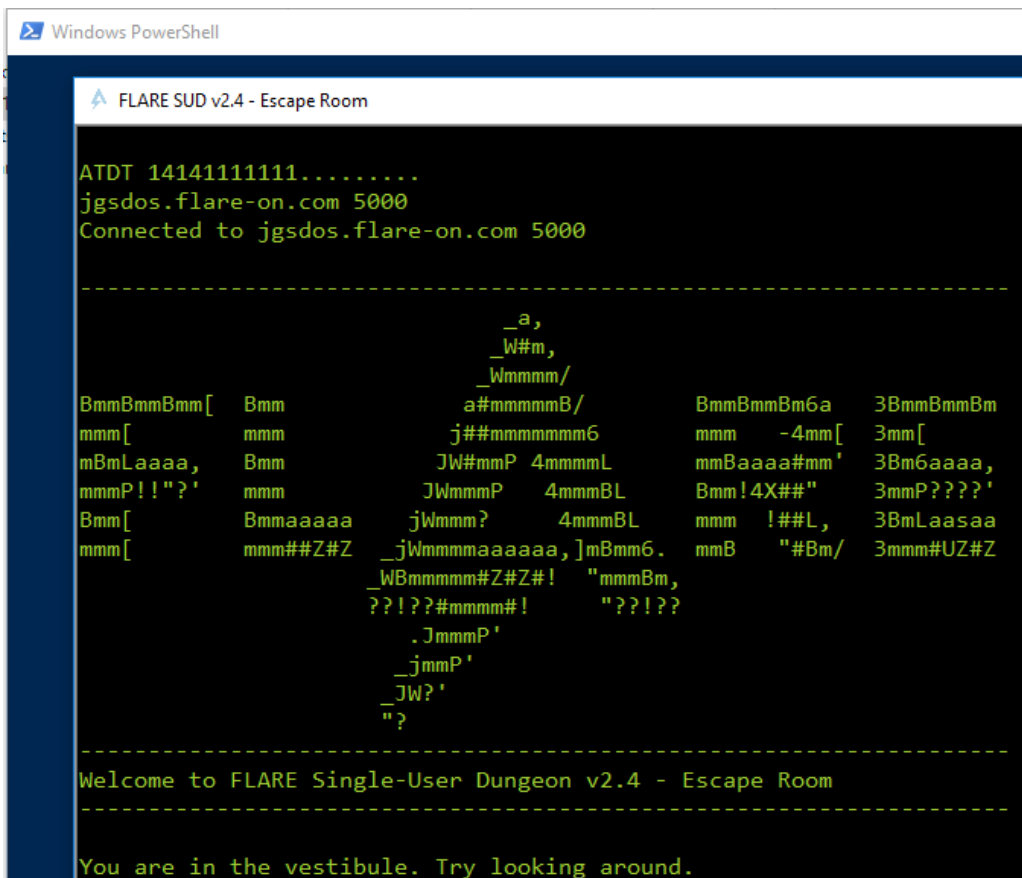
Lấy toàn bộ nội dung của chuỗi Base64 này, sau đó viết lại một chương trình nhỏ thực hiện thao tác như code của file flareon.dll để giải mã toàn bộ chuỗi Base64. Kết quả thu được chính là PowerShell script cần tìm. PowerShell này chứa toàn bộ mã nguồn của mini game Escape Room:

```

1 #####
2 # Welcome to the 2017 FLARE-ON Challenge mega-script. Have fun!
3 #####
4 Set-StrictMode -Version 2.0
5 $logo = @"
6 -----
7
8         _a,
9         _W#m,
10        _Wmmm/
11
12 BmmBmmBmm[  Bmm          a#mmmmmmB/      BmmBmmBm6a  3BmmBmmBm
13 mmm[          mmm          j#mmmmmmmm6      mmm  -4mm[  3mm[
14 mBmLaaaa,    Bmm          JW#mmP  4mmmmL      mmBaaaa#mm'  3Bm6aaaa,
15 mmmP!"?'     mmm          JWmmP  4mmmmBL     Bmm!4X##"    3mmP?????'
16 Bmm[          Bmmaaaaa    jWmm?  4mmmmBL     mmm  !##L,    3BmLaasaa
17 mmm[          mmm##Z#Z    _jWmmmmaaaaaa,]mBmm6.  mmB  "#Bm/  3mmm#UZ#Z
18
19         _WBmmmm#Z#Z#!  "mmmBm,
20         ???##mmmm#!    "??!??
21         .JmmP'
22         _jmmP'
23         _JW?'
24         "?
25 -----
26
27 Welcome to FLARE Single-User Dungeon v2.4 - Escape Room
28 -----
29 "@
30
31 #####
32 # Graeber + Dbo = Graebo? Dber?
33 #####
34 iex ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(
35 "U0VULWl0RW0gIHZhUklyYkxFOlM1MiAgKCBbdHlwRV0oICdSdU5UaScgICsgICdtZS5JTLRFUm9"+
36 "wc2VSJyAgKydWSUMnKydFUy5DYWxsJyAgKyAgJ0l0R0MnKydVblZFTlRpTycrICAnbicgICkgIC"+
37 "kgICA7ICAgICAgJHFwZGphWiAgID0gIFtUeVBFXSggICdyJyArJ1VuVlNRS5JJysgJ050ZScrI"+
38

```

Chạy thử ps script, giao diện của game xuất hiện tương tự như lúc thực thi file `zsud.exe`:



```

Windows PowerShell
FLARE SUD v2.4 - Escape Room

ATDT 1414111111.....
jgsdos.flare-on.com 5000
Connected to jgsdos.flare-on.com 5000

-----

         _a,
         _W#m,
         _Wmmm/

BmmBmmBmm[  Bmm          a#mmmmmmB/      BmmBmmBm6a  3BmmBmmBm
mmm[          mmm          j#mmmmmmmm6      mmm  -4mm[  3mm[
mBmLaaaa,    Bmm          JW#mmP  4mmmmL      mmBaaaa#mm'  3Bm6aaaa,
mmmP!"?'     mmm          JWmmP  4mmmmBL     Bmm!4X##"    3mmP?????'
Bmm[          Bmmaaaaa    jWmm?  4mmmmBL     mmm  !##L,    3BmLaasaa
mmm[          mmm##Z#Z    _jWmmmmaaaaaa,]mBmm6.  mmB  "#Bm/  3mmm#UZ#Z

         _WBmmmm#Z#Z#!  "mmmBm,
         ???##mmmm#!    "??!??
         .JmmP'
         _jmmP'
         _JW?'
         "?

-----

Welcome to FLARE Single-User Dungeon v2.4 - Escape Room

You are in the vestibule. Try looking around.

```


4. Tìm hiểu code của PowerShell

Sau một vài ngày đọc code và debug PowerShell script, tìm được một số thông tin rất quan trọng như sau:

- File này có sử dụng tới các hàm `srand()` và `rand()` nằm trong lib `msvcr.dll`:

```
.(-f 'Set-Item') Variable:q21s ([Type](-f 'aPpdaMain'));
&(-f 'set-Item') (Variable:xIRwF) ([Type](-f 'rEFLectiOn.emIT.ASseMBlYBuildErAcCesS'));
function GET-MsvCRT { $DynASSEMBLY = &(-f 'New-Object') (-f 'System.Reflection.AssemblyName')((-f 'Win32Lib'));
$aSSEMBLYBuILdeR = $q21s::"CurRenTdomain"."deFLinedYNamIcAssEmbLy"($DynASSEMBLY), $xIRwF:"RUN";
$ModuleBuILdeR = $aSSEMBLYBuILdeR.(-f 'DefineDynamicModule').Invoke((-f 'Win32Lib'), $fALSe);
$typeBuILdeR = $ModuleBuILdeR.(-f 'DefineType').Invoke((-f 'msvcrt'), (-f 'PublicClass'));
$Meth_SrAnd = $TypeBuILdeR.(-f 'DefineMethod').Invoke((-f 'srand'), [Reflection.MethodAttributes] (-f 'PublicStatic'), [Void], [Type[]] @([Int32]));
$Meth_rAnd = $TypeBuILdeR.(-f 'DefineMethod').Invoke((-f 'rand'), [Reflection.MethodAttributes] (-f 'PublicStatic'), [Int32], [Type[]] @());
$ATTR_SrAnd = &(-f 'Get-CustomAttr') (-f 'msvcr.dll') (-f 'srand') $fALSe;
$ATTR_rAnd = &(-f 'Get-CustomAttr') (-f 'msvcrt.dll') (-f 'rand') $fALSe;
$mETH_srAnd.(-f 'SetCustomAttribute').Invoke($ATTR_SrAnd);
$mETH_rAnd.(-f 'SetCustomAttribute').Invoke($ATTR_rAnd);
return $TypeBuILdeR.(-f 'CreateType').Invoke();
}
```

- Khi vào chơi game, sẽ đứng tại vị trí `$map.StartingRoom = $vestibule`. Thông tin tại vị trí này là **"You are in the vestibule. Try looking around."**.
- Từ vị trí `$vestibule`, nếu đi 's' thì chắc chắn sẽ bị **'locked out'**. Vì đây chính là đường một chiều:

```
$outside = New-Room "Outside" "You're locked out. It doesn't look like there's a way back in."
Add-RoomLink $outside 'n' $outside
Add-RoomLink $outside 'e' $outside

$vestibule = New-Room "the vestibule" "This is surely the entrance to a great company."
Add-RoomLink $vestibule 's' $outside -OneWay
```

- Từ vị trí `$vestibule` chỉ có một bước đi duy nhất ('n') là tới được `$lobby`:

```
$lobby = New-Room "the lobby" "There is a reception desk with ferns on either side, and a sign that says MANDIANT."
Add-RoomLink $vestibule 'n' $lobby
```

- Tại `$lobby` sẽ thấy có "reception desk". Quan sát bàn của lễ tân sẽ thấy có **"a sign-in sheet and laptop on top and a few drawers on the sides"**. Đọc code của script thì thấy tại drawers sẽ có một cái "key".

```
> | drawers
The drawers are mostly empty, except the bottom-right drawer which contains some junk. It has a key.
```

- "key" được định nghĩa là một chuỗi như sau:

```
$key = New-Thing "a key" "You BANKBEPuXzP2E1KfSjM041qGjY8RjK0p++RcL2RUFv59RbJzbbj38SezGc9EzKtVjJb0061dnehbxyJGa60UJXSkQnr9BU3WsyMNsVd/XtN9/bkesgmsASHvroc2N6Y9IgcVvLaYg4U8TtyI9CKj598yFTMc1/koEDpZuh
tBydz2h0UfIBiYRxfAR1W5t3dAEH8B9r93n4dPm9h1qg23rdSRP4TH8666k3J0X1RQXV7pZC6h0uX8V8qEdmF5KpNBjJAK0Jf16eCr45p9j61Lh1T061FEZ1VTEK0ID+T9D1VUR0B9a37whIAKEvuyyp5+Tspyh0GLH1YcWfZL8DyXmmrhvzta2nJ+FT160Kq
AAKJduCy6YrGmWfR0ChpeuLZL7Cq1Jwh27y8h0V198G1K0p02COQJNjlp1e450LtbR0pH80YceYXbyRL3k892uX8BSBxnd90eL80AdJkN95V8T83+rj53k3YLwR2961LsCfdKvK411d/Xa//
e+8q1xMeUCidnNSw4H10tdpl.rpfYnCvK8cad1RC6hG1tbtCknTCUinXCCDEINW5V13v5VxKPGaww/1RU7F281c+o3T1dWpXkcfks62V051FjVzrT28+QuB28+YrAcKPhFZALYKLU03R5V3w645148tykT168evyRF/
Fnp4VTN1MQHKPj+Y6YChZnrBnd1RDPfmlwX0Q1bdeaeZ5a3Agg12w0pP8nF69vVaq4qjxyr11PL9hd7cBfqnghjyby/
t78TZOthX++w62kMl0Ez612Ch0p3vzq1/91Q1g9WAgLdq1AhkKbFSM7K6PFSReyphx27uzxHAL1P7LX1V709v4ccrHE7dJpu15Swhx3rL35BA15ndMabuJ1Er0pMlWCYfhpSj6GLOH0U/
Pq6oktZ9BL5V11PcxaVvH6GfClmMe61MSFD8hYJXg7xbwKDVIS6B5-jB8fxNUfNW/2ZLjtv28mpPsvJHdQnxj+hpFLg1B7D5eozj1gU0Y01RLmA0X0M5D1LAmoZu3hx2Fte1x03hJpxYU70d1611MLA1XaeUzjQhYBdfadbeA8BdM5Kx2XFjfrjY1/f/
1d0cXSL=9R0RNDJWjyE1jW2Pv0Utpb8KqJURK1X/Xp5y59vCncacotUC06rWu8y54P8M/
L17AR0WY2jg1Hnazz02Kk1fABR6F0XSYdy101Wk.rpCKM2BTE1G2MEF90c.rV99SLER7U1u027G16ZuMfGYbHSPeAfhg93BR0n15y13457SNT5W06nf06c7CzTsksVal/
rd1Cpks8HAQRdTKC+41S0FHyYz153Pup1maL.FEtLn7Cp63+H0e2x4JW9XFf41xVhSB0B+l1SR127TG3aYeHEJ38NsYedVhZpCh3R88R0KZCq1TAhpgzaB0VYAc6VhLPS8KPsM1kBF0GN1gCk1jgg6MTIBacFL1gMhJd8uMHyBvKdMf/ea8+70rV1U/
Wx8UzjVx1+9ScKed7qqv1KjKupfBeTe7rj3KGY9P9GrDPX70P2zy1D5xJN1kKSE458T1xughjKPPKReR8H1anoL1fJwFK+kgj0Wk4Lr5M1rX35GbyY8Se/m52M1uSpaedAS/TWjY1d7d/raHkRQ4DDYq60m4wFBFRcGkKehwZQjC0Suc1VKW021ESTFw/
Sj745NAQBSr1egYxWwV30e6yeg+X35G00jVKTyRASHvMJKZKAzpcP7Yk2oPwz3T1njY1davQj0FjcbL9JdIchv95Yf+aucQw70rW7CnQd51vc2AT208E8Ej38UW82cGfYE031X0gu5ghE7L1q90Fu+OdLvtZ1.3bXNyhBUdMj/
1XhJZH8PZ04Bl9n0Ubt1q2TSwL1H1VqHq3DybcVd/4Vv9j9gR04Yd1awVafY0wQ3Mh0bzuc5860Kux1TtH06B8X/5n11Rw09484Blvul1qBv0+8ChZ5inFer1G3JqU5p91L7vzCp170M4pvc2BTKLUdwnajLp0REN0q/rrX0yzttb/
```

- Khi nhặt "key" tại drawer, sẽ gọi tới hàm `Invoke-TransferThing([PSObject][ref]$container_old, [PSObject][ref]$container_new, $thing)`. Đoạn code này sẽ kiểm tra nếu như đã nhặt được key thì sẽ gọi hàm `srand(42)` dùng để khởi tạo một số ngẫu nhiên theo số seed là 42. Hàm `srand()` thường sẽ được gọi trước khi gọi hàm `rand()`.


```

function Invoke-TransferThing([PSObject][ref]$container_old, [PSObject][ref]$container_new, $thing) {
    $ret = $false

    if ($thing.Fixed -eq $false) {
        $al = [System.Collections.ArrayList]($container_old.Contents)
        $al.Remove($thing)
        $container_old.Contents = @($al)

        $container_new.Contents += $thing
        $ret = $true

        if (($thing.Keywords -Contains "key") -and ($container_new -eq $script:char)){
            ${Msv`c`RT>::("{1}{0}"-f 'rand', 's').Invoke(42)}
        }
    }

    return $ret
}

```

- Sau khi lấy được **key** thì mỗi bước đi tiếp theo trong mê cung đều gọi tới hàm **Invoke-MoveDirection(\$char, \$room, \$direction, \$trailing)**. Tại hàm này sẽ gọi hàm **rand() % 6** để sinh số ngẫu nhiên nằm trong khoảng từ 0 – 5. Hàm này như sau:

```

function Invoke-MoveDirection($char, $room, $direction, $trailing) {
    $nextroom = $null
    $movetext = "You can't go $direction."
    $statechange_tristate = $null

    $nextroom = Get-RoomAdjoining $room $direction
    if ($nextroom -ne $null) {
        $key = Get-ThingByKeyword $char 'key'
        if (($key -ne $null) -and ($script:okaystopnow -eq $false)) {
            $dir_short = ([String]$direction[0]).ToLower()

            ${N} = ${sC`Ri`Pt:MS`VcRt}::("{1}{0}" -f'nd','ra').Invoke()%6

            if ($directions_enum[$dir_short] -eq ($n)) {
                $script:key_directions += $dir_short
                $newdesc = Invoke-XformKey $script:key_directions $key.Desc
                $key.Desc = $newdesc
                if ($newdesc.Contains("@")) {
                    $nextroom = $script:map.StartingRoom
                    $script:okaystopnow = $true
                }
                $statechange_tristate = $true
            } else {
                $statechange_tristate = $false
            }
        }
    }

    $script:room = $nextroom
    $movetext = "You go $($directions_short[$direction.ToLower()])"

    if ($statechange_tristate -eq $true) {
        $movetext += "`nThe key emanates some warmth..."
    } elseif ($statechange_tristate -eq $false) {
        $movetext += "`nHmm..."
    }

    if ($script:autolook -eq $true) {
        $movetext += "`n$(Get-LookText $char $script:room $trailing)"
    }
} else {
    $movetext = "You can't go that way."
}

return "$movetext"
}

```

- Biến `$dir_short` lúc này sẽ chứa thông tin về hướng di chuyển của người chơi, ``${N}` lúc này sẽ chứa số ngẫu nhiên được tạo bởi hàm `rand()%6`. Lệnh `$directions_enum[$dir_short] -eq ($n)` sẽ kiểm tra xem *giá trị của bước dịch chuyển mà người dùng nhập vào có trùng khớp với số ngẫu nhiên được tạo ra bởi hàm `rand()` không?* Nếu trùng thì sẽ thực hiện gọi tới hàm `Invoke-`

`XformKey([String]$keytext, [String]$desc)` để biến đổi nội dung của "key" đã nhậ được ban đầu.

- Code thực hiện biến đổi **key** tại hàm **Invoke-XformKey([String]\$keytext, [String]\$desc)** như sau:

```
function Invoke-XformKey([String]$keytext, [String]$desc) {
    $newdesc = $desc

    Try {
        $split = $desc.Split()
        $text = $split[0..($split.Length-2)]
        $encoded = $split[-1]
        $encoded_ursafe = $encoded.Replace('+', '-').Replace('/', '_').Replace('=', '%3D')
        $uri = "${script:baseurl}?k=${keytext}&e=${encoded_ursafe}"

        $r = Invoke-WebRequest -UseBasicParsing "$uri"

        $decoded = $r.Content

        if ($decoded.ToLower() -NotContains "whale") {
            $newdesc = "$text $decoded"
        }
    } Catch {
        Add-ConsoleText "..."
    }

    return $newdesc
}
```

- Kiểm tra thông tin về `$directions_enum`, thu được một thông tin rất giá trị như sau:

```
↑ $directions_enum: [Hashtable: 6]
  ▶ [0]: [s, 1]
  ▶ [1]: [n, 0]
  ▶ [2]: [u, 4]
  ▶ [3]: [e, 2]
  ▶ [4]: [w, 3]
  ▶ [5]: [d, 5]
```

- Dựa vào thông tin trên, có thể thấy ứng với một bước di chuyển trong mê cung, thì sẽ sử dụng `$directions_enum` để mapping kí tự nhập vào tương ứng với số mấy. Ví dụ: nếu nhập vào là "w" thì sẽ tương ứng với số "3", nhập "e" tương ứng với số "2" ...
- Như vậy, từ đây nhận thấy có một điều hơi vô lý, nếu như sử dụng hàm `rand() % 6` để sinh số ngẫu nhiên trong khoảng từ 0 – 5 thì việc nhập kí tự để di chuyển trong mê cung sẽ rất khó cho kết quả so sánh bằng như đã đề cập ở lệnh `if` bên trên. May mắn lắm thì mới trùng thoi ☺, và tôi cũng có được vài lần vô tình nhập trùng với số do `rand` tạo ra, lolz.
- Do khi run file `zsud.exe` thì mới bung PowerShell để chạy game, và khi PowerShell gọi tới `srand(42)` và `rand() % 6` thì khả năng các hàm này có thể đã bị can thiệp bởi file binary rồi.

Câu hỏi đặt ra, làm thế nào để biết vị trí mà binary can thiệp tới các hàm `srand()` và `rand()`?

5. Sử dụng FLOSS để deobfuscate strings

Trong quá trình nghiên cứu binary, tôi không tìm thấy thông tin về thư viện `msvcrt.dll` cũng như các hàm như `srand()` và `rand()`. Khả năng thông tin về chúng đã bị encrypted/obfuscated trong binary.

Lúc này, chợt nhớ FLARE team có một công cụ là **FLOSS (FireEye Labs Obfuscated String Solver)** chuyên dùng để deobfuscate strings. Chạy thử công cụ này với file `zsud.exe`, có được kết quả như sau:

```
FLOSS decoded 17 strings
1023442870282056
httpapi.dll
HttpInitialize
HttpCreateHttpHandle
HttpAddUrl
HttpRemoveUrl
HttpTerminate
HttpReceiveHttpRequest
HttpSendHttpResponse
Failed, HRESULT 0x0x. Try on a Win7 system with this installed - tinyurl.com/winmgfwk4
A2 h
A2 h
System.Management.Automation.dll probably could not be found or was not compatible. Maybe you need this? tinyurl.com/winmgfwk4
mscorlib.dll
CorBindToRuntimeEx
msvcrt.dll
srand

FLOSS extracted 2 stackstrings
isca
AA((
```

Theo kết quả có được thì FLOSS đã decoded được các string liên quan tới `msvcrt.dll` và `srand`. Sử dụng tùy chọn `-i` của FLOSS tạo ra một IDAPython script để chú thích string đã được giải mã vào file IDB của IDA.

```
$ floss -i zsud_decoded_strings.py zsud.exe
```

Kết quả sau khi chạy script trong IDA:

```
Annotating 19 strings from FLOSS for zsud.exe
FLOSS: string "1023442870282056" decoded at VA 0x426E1E
FLOSS: string "httpapi.dll" decoded at VA 0x408103
FLOSS: string "HttpInitialize" decoded at VA 0x4081EB
FLOSS: string "HttpCreateHttpHandle" decoded at VA 0x408241
FLOSS: string "HttpAddUrl" decoded at VA 0x408291
FLOSS: string "HttpRemoveUrl" decoded at VA 0x4082E1
FLOSS: string "HttpTerminate" decoded at VA 0x408314
FLOSS: string "HttpReceiveHttpRequest" decoded at VA 0x408343
FLOSS: string "HttpSendHttpResponse" decoded at VA 0x408372
FLOSS: string "Failed, HRESULT 0x0x. Try on a Win7 system with this installed - tinyurl.com/winmgfwk4" decoded at VA 0x402878
FLOSS: string "A2 h" decoded at VA 0x402836
FLOSS: string "A2 h" decoded at VA 0x402836
FLOSS: string "System.Management.Automation.dll probably could not be found or was not compatible. Maybe you need this? tinyurl.com/winmgfwk4" decoded at VA 0x402836
FLOSS: string "mscorlib.dll" decoded at VA 0x402547
FLOSS: string "CorBindToRuntimeEx" decoded at VA 0x402562
FLOSS: string "msvcrt.dll" decoded at VA 0x4066EB
FLOSS: string "srand" decoded at VA 0x406703
Imported decoded strings from FLOSS
```

6. Xác định bảng index các bước đi trong mê cung

Theo thông tin mà FLOSS cung cấp, sẽ tới được đoạn code giải mã các chuỗi `msvcrt.dll` và `srand`:

```
int __cdecl sub_406530()
{
    int result; // eax@1
    int result_cpy; // ebx@1
    HANDLE hThread; // eax@2
    HMODULE h_msvcrt; // edi@2
    int (*v4)(void); // eax@3
    int v5; // [sp+8h] [bp-10h]@1
    LPCSTR lpFileName; // [sp+Ch] [bp-Ch]@1
```

```

int v7; // [sp+10h] [bp-8h]@1
LPCSTR lpProcName; // [sp+14h] [bp-4h]@1

v5 = 1;
lpFileName = "bitsigd.dll";
v7 = 1;
lpProcName = "InitializeEx";
result = sub_40114A();
result_cpy = result;
if ( !result )
{
    return result;
}
sub_42A020();
hThread = GetCurrentThread();
sub_42A500(hThread);
sub_4298C0((int)UnmapViewOfFile_0, a2);
sub_4298C0((int)CloseHandle_0, sub_401145);
sub_4298C0((int)GetFileInformationByHandle_0, sub_401082);
sub_4298C0((int)FreeLibrary_0, sub_401078);
sub_4298C0((int)OpenFile_0, sub_401032);
sub_4298C0((int)MapViewOfFile_0, sub_40114F);
sub_4298C0((int)MapViewOfFileEx_0, sub_4010E6);
sub_4298C0((int)GetFileSize_0, sub_40104B);
sub_4298C0((int)GetFileSizeEx_0, sub_401023);
sub_4298C0((int)ReadFile_0, sub_401014);
sub_4298C0((int)ReadFileEx_0, sub_401005);
sub_4298C0((int)ReadFileScatter_0, sub_401091);
sub_4298C0((int>CreateFileA_0, sub_40109B);
sub_4298C0((int>CreateFileW_0, sub_40111D);
sub_4298C0((int>CreateFileMappingA_0, sub_401055);
sub_4298C0((int>CreateFileMappingW_0, sub_401122);
sub_4298C0((int)GetFileAttributesA_0, sub_40102D);
sub_4298C0((int)GetFileAttributesW_0, sub_4010D2);
sub_4298C0((int)GetFileAttributesExA_0, sub_40112C);
sub_4298C0((int)GetFileAttributesExW_0, sub_4010F0);
sub_4298C0((int)LoadLibraryA_0, sub_40100A);
sub_4298C0((int)LoadLibraryW_0, sub_4010FF);
sub_4298C0((int)&LoadLibraryExA_0, sub_401037);
sub_4298C0((int)LoadLibraryExW_0, sub_401087);
decode_string(&v5, (const char *)&unk_43F6E8);// FLOSS: msvcrt.dll
decode_string(&v7, (const char *)&unk_43F6F8);// FLOSS: srand
h_msvcrt = LoadLibraryA(lpFileName);
if ( h_msvcrt )
{

```

```

    rand_func = (int (*)(void))GetProcAddress(h_msvcrtdll, lpProcName + 1); // address
of the rand function
    v4 = (int (*)(void))GetProcAddress(h_msvcrtdll, lpProcName); // address of the
srand function
    srand_func = v4;
}
else
{
    v4 = srand_func;
    result_cpy = 0;
}
if ( !rand_func || !v4 )
{
    result_cpy = 0;
}
sub_4298C0((int)&rand_func, sub_401019); // rand is hooked
sub_4298C0((int)&srand_func, sub_4010B9); // srand is hooked
if ( _ms_p5_mp_test_fdiv() )
{
    result_cpy = 0;
}
result = result_cpy;
return result;
}

```

Tổng kết lại, sub_406530() thực hiện nhiệm vụ sau:

- Gọi hàm decode_string để giải mã ra các chuỗi msvcrtdll và srand.
- Lấy handle của msvcrtdll thông qua API LoadLibraryA.
- Lấy địa chỉ của các hàm rand và srand trong thư viện msvcrtdll thông qua API GetProcAddress.
- Thực hiện hook hai hàm rand và srand.

Sau khi thực hiện toàn bộ code trên, hàm rand() gốc bị thay đổi, nhảy tới **jmp**

zsud.00401019 <-- rand_mod()

Address	Hex dump	Disassembly	Comment	Label
75ECC070	\$. E9 A44F538A	jmp zsud.00401019		rand
75ECC075	. 8B48 14	mov ecx, dword ptr [eax+0x14]		
75ECC078	. 69C9 FD430300	imul ecx, ecx, 0x343FD		
75ECC07E	. 81C1 C39E2600	add ecx, 0x269EC3		
75ECC084	. 8948 14	mov dword ptr [eax+0x14], ecx		
75ECC087	. 8BC1	mov eax, ecx		
75ECC089	. C1E8 10	shr eax, 0x10		
75ECC08C	. 25 FF7F0000	and eax, 0x7FFF		
75ECC091	. C3	ret		

Lệnh cũ của hàm rand() được lưu lại tại địa chỉ:

Address	Hex dump	Disassembly	Comment
359B0798	E8 319E5140	call msvcrtdll.75ECA5CE	
359B079D	- E9 D3B85140	jmp msvcrtdll.75ECC075	jump back to rand()
359B07A2	CC	int3	

Hàm srand() gốc cũng bị thay đổi, nhảy tới `jmp zsud.004010B9 <-- srand_mod()`

Address	Hex dump	Disassembly	Comment	Label
75ECF757	- E9 5D19538A	jmp zsud.004010B9		srand
75ECF75C	. E8 6DAEFFFF	call 75ECA5CE		
75ECF761	. 8B4D 08	mov ecx, dword ptr [ebp+0x8]		
75ECF764	. 8948 14	mov dword ptr [eax+0x14], ecx		
75ECF767	. 5D	pop ebp		
75ECF768	. C3	retn		

Lệnh cũ của hàm srand() được lưu lại tại địa chỉ:

Address	Hex dump	Disassembly	Comment
359B07E0	8BFF	mov edi, edi	
359B07E2	55	push ebp	
359B07E3	8BEC	mov ebp, esp	
359B07E5	- E9 72EF5140	jmp msvcrt.75ECF75C	jump back to srand()
359B07EA	CC	int3	

Nhớ lại phần phân tích code của PowerShell, sau khi game thực thi hoàn toàn, người chơi nhấn được **key** thì sẽ gọi srand(42). Lúc này, hàm srand đã bị hooked để nhảy tới địa chỉ 0x004010B9. Từ 0x004010B9 sẽ tới sub_407140:

```
int __cdecl sub_407140(int seed_number)
{
    signed int flag; // ecx@1

    flag = dword_45BD28;
    if ( seed_number == 42 ) // seed = 42?
    {
        flag = 1;
    }
    dword_45BD28 = flag;
    return srand_func(); // jump to location that stored original instruction of
srand()
}
```

Code tại sub_407140 sẽ thực hiện việc gán `dword_45BD28` giá trị bằng **1**. Như đã mô tả, khi nhận được key, thì bất kỳ bước đi tiếp theo trong mê cung đều sẽ gọi tới hàm `rand() % 6` để tạo số ngẫu nhiên trong khoảng **0 – 5** và so sánh với giá trị số được mapping tương ứng với bước dịch chuyển. Nếu bằng nhau thì sẽ gọi hàm `Invoke-XformKey` để biến đổi key. Hàm rand lúc này đã bị hooked để nhảy tới địa chỉ 0x00401019. Từ địa chỉ 0x00401019 sẽ tới sub_4070F0:

```
int __cdecl sub_4070F0()
{
    int result; // eax@3
    const WCHAR *retaddr; // [sp+0h] [bp+0h]@2

    if ( dword_45BD28 && j_au_re_GetModuleHandleExW(retaddr) )
    {
        result = index_table[i]; // index table is located at 0x459CB8
        i = (i + 1) % val_53; // i in range 0 .. 52
    }
}
```



```

else
{
    result = rand_func();           // jump to location that stored original
instruction of rand()
}
return result;
}

```

Code tại sub_4070F0 sẽ thực hiện việc lấy giá trị tại index_table tại địa chỉ 0x459CB8. Bảng này chứa các index như sau:

Address	Hex dump	ASCII
00459CB8	03 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00	L.....7..
00459CC8	02 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00	7.....
00459CD8	00 00 00 00 02 00 00 00 03 00 00 00 00 00 00 00L..
00459CE8	02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00L..
00459CF8	03 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00]..
00459D08	05 00 00 00 04 00 00 00 00 00 00 00 05 00 00 00
00459D18	04 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00]..
00459D28	00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00]..
00459D38	01 00 00 00 02 00 00 00 03 00 00 00 05 00 00 00L..
00459D48	04 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00].....7..
00459D58	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00	L.....7..
00459D68	01 00 00 00 02 00 00 00 03 00 00 00 01 00 00 007..
00459D78	02 00 00 00 03 00 00 00 05 00 00 00 04 00 00 00	7..... ..
00459D88	00 00 00 00 35 00 00 00 00 00 00 00 00 00 00 005.....

Dựa vào bảng trên, có thể thấy sau khi nhặt được **key** thì các bước di chuyển tiếp theo trong mê cung phải tuân theo bảng này. Kết hợp bảng này và bảng mapping có được ở trên, sẽ suy ra được các bước đi tương ứng.

Sau khi đi tới được phòng của Kevin thực hiện các thao tác sau để lấy key:

```

You see:
Kevin Mandia
Kevin Mandia's Desk
A football helmet

Exits: South

> get helmet
You get A football helmet.

> wear helmet
You put the helmet on your head. It looks objectively awesome.

> drop key
You drop a key

> say Kevin hello

Kevin says, with a nod and a wink: '6D 75 64 64 31 6E 67 5F 62 79 5F 79 30 75 72 35
33 6C 70 68 40 66 6C 61 72 65 2D 6F 6E 2E 63 6F 6D'.

Bet you didn't know he could speak hexadecimal! :-)
```

Với chuỗi hexa mà Kevin cung cấp, ta có được flag để submit là:
mudd1ng_by_y0ur531ph@flare-on.com

"You are in the maze. The maze you are in...

In the maze, you saw the maze ...

See some thing, you get some thing

Go around, North, South, East, West, Up, Down..

Long long long ... Nightmare..so long

Shell shell shell ... the Ghost in the shell

Wear some thing, You drop some thing...

Say to Kevin, Kevin: "Hello mate!! Long time no see .. you look tired, lolz!!"

Here is something, you become the king!!!....."



Hết.

m4n0w4r

