

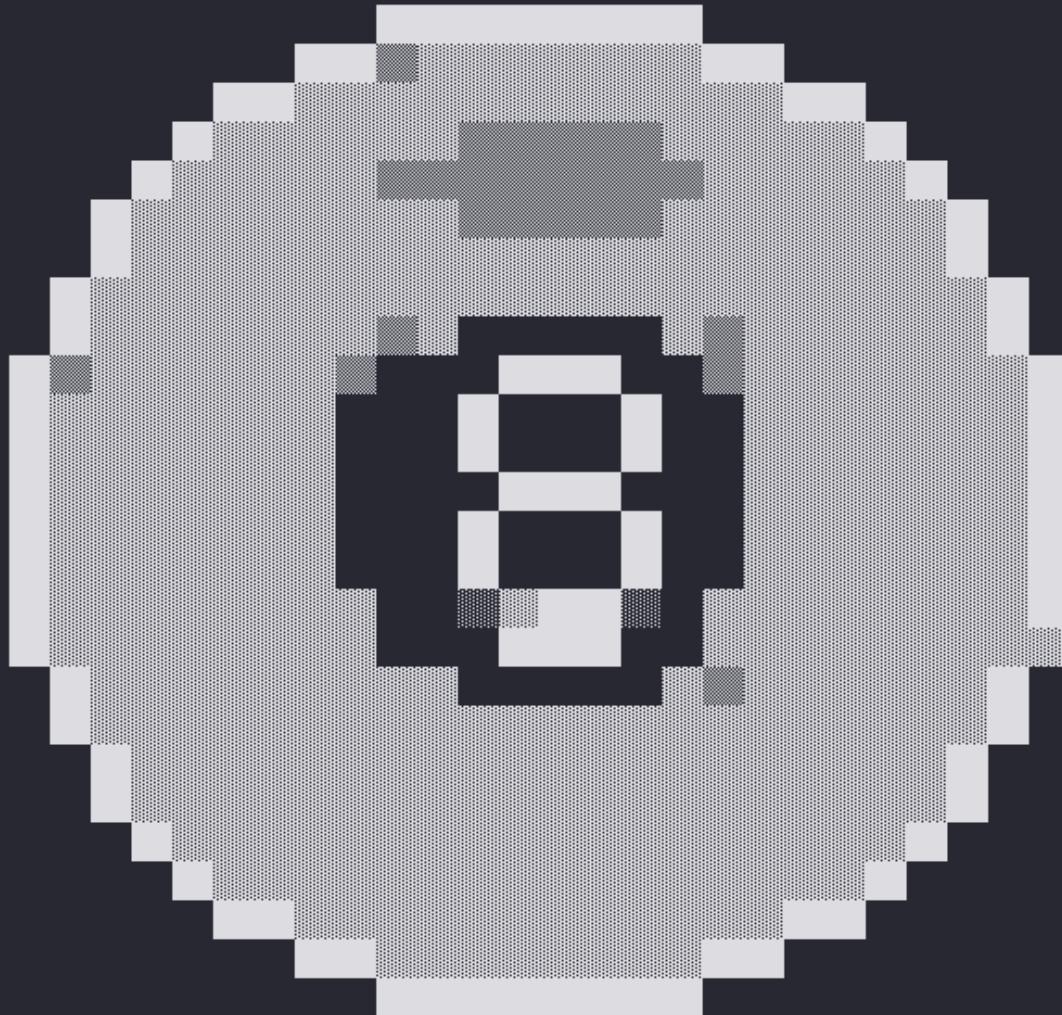


Название:	Шар предсказаний
Категория:	Реверс-инжиниринг
Уровень:	Лёгкая
Очки:	350
Описание:	Шар предскажет всё! Но кроме флага, конечно)
Теги:	Побайтовое шифрование, стековая самописня VM
Автор:	ROP

Прохождение:

Изучаем данный нам файл.

```
> ./ball.elf
```



Я отвечу на любой вопрос!

Задать вопрос: Ты знаешь флаг?

Ты что, нет!

О /tmp/Шар > █

Если посмотреть строки через IDA, то можно заметить:

```

?? LOAD:0000... 0000001C C /lib64/ld-linux-x86-64.so.2
?? LOAD:0000... 00000006 C fgets
?? LOAD:0000... 00000006 C stdin
?? LOAD:0000... 00000011 C __stack_chk_fail
?? LOAD:0000... 00000012 C __libc_start_main
?? LOAD:0000... 00000006 C srand
?? LOAD:0000... 0000000F C __cxa_finalize
?? LOAD:0000... 00000007 C printf
?? LOAD:0000... 00000008 C strncmp
?? LOAD:0000... 0000000A C libc.so.6
?? LOAD:0000... 0000000A C GLIBC_2.4
?? LOAD:0000... 0000000C C GLIBC_2.2.5
?? LOAD:0000... 0000000B C GLIBC_2.34
?? LOAD:0000... 0000001C C __ITM_deregisterTMCloneTable
?? LOAD:0000... 0000000F C __gmon_start__
?? LOAD:0000... 0000001A C __ITM_registerTMCloneTable
?? .rodata:000... 00000019 C Скорее всего.
?? .rodata:000... 00000013 C Это точно.
?? .rodata:000... 00000024 C Вообще ни капельки.
?? .rodata:000... 00000007 C 1000%.
?? .rodata:000... 0000001E C Подумай об этом.
?? .rodata:000... 00000015 C Ты что, нет!
?? .rodata:000... 00000012 C : p@s5_f0R_arClve
?? .eh_frame:0... 00000006 C 9*3$\"
?? .data:0000... 0000003A C ;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 90\n
?? .data:0000... 0000000E C dEKXK?dXQXqjdw
?? .data:0000... 00000006 C (\\"rb`!
?? .data:0000... 00000005 C !a:P/
?? .data:0000... 00000005 C @Al@P
?? .data:0000... 00000005 C 7.UK4
?? .data:0000... 00000006 C /uf('.
?? .data:0000... 00000005 C h\ace]
?? .data:0000... 00000005 C d\*\*Fw
?? .data:0000... 00000005 C z2h*^
?? .data:0000... 00000006 C Mb_]j\\
?? .data:0000... 00000005 C \v*h\n
?? .data:0000... 00000007 C ]Llh63.

Line 23 of 111
.....
```

Попробуем его на архиве, что дан вместе с файлом. Успешно подходит. Мы получили битый ELF-файл. Это можно понять, сравнив его с [ball.elf](#) в Нех-редакторе.

010 Editor - C:\Users\fff\Desktop\ball.e

	0	1	2	3	4	5	6	
0000h:	7F	45	4C	46	02	01	01	00
0010h:	03	00	3E	00	01	00	00	00
0020h:	40	00	00	00	00	00	00	00
0030h:	00	00	00	00	40	00	38	00
0040h:	06	00	00	00	04	00	00	00
0050h:	40	00	00	00	00	00	00	00

010 Editor - C:\Users\fff\Desktop\give_flag

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	00	45	4C	46	00	99	01	00	99	00	00	00	00	00	00	00	.ELF.™..™.....
0010h:	03	00	3E	00	01	00	00	00	80	10	00	00	00	00	00	00	..>.....€.....
0020h:	40	00	00	00	00	00	00	00	D0	36	00	00	00	00	00	00	@.....Đ6.....
0030h:	00	00	00	00	40	00	38	00	0D	00	40	00	1F	00	1E	00@.8...@.....
0040h:	06	00	00	00	04	00	00	00	40	00	00	00	00	00	00	00@.....
0050h:	40	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	@.....@.....
0060h:	D8	02	00	00	00	00	00	00	D8	02	00	00	00	00	00	00	Ø.....Ø.....

Меняем 0 на 0x7F. Также есть другие изменения в заголовках:

010 Editor - C:\Users\fff\Desktop\give_flag

File Edit Search View Format Scripts Templates Debug Tools Window Help

Startup ball.elf give_flag x

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	7F	45	4C	46	02	01	01	00	00	p0	00	00	00	00	00	.ELF.....	
0010h:	03	00	3E	00	01	00	00	00	80	10	00	00	00	00	00	...>.....€.....	
0020h:	40	00	00	00	00	00	00	00	D0	36	00	00	00	00	00	@.....Đ6.....	
0030h:	00	00	00	00	40	00	38	00	0D	00	40	00	1F	00	1E	00@.8...@.....
0040h:	06	00	00	00	04	00	00	00	40	00	00	00	00	00	00@.....	
0050h:	40	00	00	00	00	00	00	00	40	00	00	00	00	00	00	@.....@.....	
0060h:	D8	02	00	00	00	00	00	00	D8	02	00	00	00	00	00	Ø.....Ø.....	
0070h:	08	00	00	00	00	00	00	00	03	00	00	00	04	00	00	00	
0080h:	18	03	00	00	00	00	00	00	18	03	00	00	00	00	00	
0090h:	18	03	00	00	00	00	00	00	1C	00	00	00	00	00	00	
00A0h:	1C	00	00	00	00	00	00	01	00	00	00	00	00	00	00	...	
00B0h:	01	00	00	00	04	00	00	00	00	00	00	00	00	00	00	...	
00C0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

На скрине показан запатченный вариант. Теперь его можно открыть в IDA. Далее посмотрев код и изменения флага до `puts`, можно получить флаг.