HarveyHunt / **ctfs**

Branch: **master** ▾ **ctfs** / 2016 / sharif / reverse / getit / **getit.md** **Find file** **Copy path**

HarveyHunt Add sharif 2016 getit writeup 5ae57bc on Dec 19, 2016

1 contributor

311 lines (295 sloc) 13.4 KB

getit

> Open and read the flag file!

The provided file is an x86-64 binary that provides no output, `file` tells us the following:

```
getit: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.24,
BuildID[sha1]=e389cd7a4b9272ba80f85d7eb604176f6106c61e, not stripped
```

My next step was to `strace` the binary and see if it provides any clues. The following is the output:

```
execve("./getit", ["./getit"], [/* 32 vars */]) = 0
brk(NULL)                               = 0x167a000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=163641, ...}) = 0
mmap(NULL, 163641, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f0995db2000
close(3)                                = 0
open("/usr/lib/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260\3\2\0\0\0\0\0"...,
832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=1951744, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7f0995db0000
mmap(NULL, 3791152, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) =
0x7f099581a000
mprotect(0x7f09959af000, 2093056, PROT_NONE) = 0
mmap(0x7f0995bae000, 24576, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x194000) = 0x7f0995bae000
mmap(0x7f0995bb4000, 14640, PROT_READ|PROT_WRITE,
MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f0995bb4000
close(3)                                = 0
arch_prctl(ARCH_SET_FS, 0x7f0995db1440) = 0
mprotect(0x7f0995bae000, 16384, PROT_READ) = 0
mprotect(0x600000, 4096, PROT_READ)     = 0
mprotect(0x7f0995dda000, 4096, PROT_READ) = 0
munmap(0x7f0995db2000, 163641)          = 0
brk(NULL)                               = 0x167a000
brk(0x169b000)                          = 0x169b000
open("/tmp/flag.txt", O_WRONLY|O_CREAT|O_TRUNC, 0666) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
write(3, "********************************"..., 44) = 44
lseek(3, 30, SEEK_SET)                  = 30
write(3, "5", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 24, SEEK_SET)                  = 24
write(3, "a", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 25, SEEK_SET)                  = 25
write(3, "e", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 32, SEEK_SET)                  = 32
```

```
write(3, "1", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 40, SEEK_SET)                  = 40
write(3, "8", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 36, SEEK_SET)                  = 36
write(3, "3", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 28, SEEK_SET)                  = 28
write(3, "2", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 17, SEEK_SET)                  = 17
write(3, "7", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 34, SEEK_SET)                  = 34
write(3, "2", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 39, SEEK_SET)                  = 39
write(3, "5", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 16, SEEK_SET)                  = 16
write(3, "2", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 33, SEEK_SET)                  = 33
write(3, "1", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 19, SEEK_SET)                  = 19
write(3, "f", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 26, SEEK_SET)                  = 26
write(3, "b", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 5, SEEK_SET)                   = 5
write(3, "f", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 3, SEEK_SET)                   = 3
write(3, "r", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 29, SEEK_SET)                  = 29
write(3, "d", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 27, SEEK_SET)                  = 27
write(3, "f", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 31, SEEK_SET)                  = 31
write(3, "9", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 4, SEEK_SET)                   = 4
write(3, "i", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 8, SEEK_SET)                   = 8
write(3, "F", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 15, SEEK_SET)                  = 15
write(3, "9", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
```

```
write(3, "********************************"..., 44) = 44
lseek(3, 37, SEEK_SET)                  = 37
write(3, "c", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 42, SEEK_SET)                  = 42
write(3, "}", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 14, SEEK_SET)                  = 14
write(3, "5", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 41, SEEK_SET)                  = 41
write(3, "9", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 2, SEEK_SET)                   = 2
write(3, "a", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 23, SEEK_SET)                  = 23
write(3, "8", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 21, SEEK_SET)                  = 21
write(3, "f", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 0, SEEK_SET)                   = 0
write(3, "S", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 10, SEEK_SET)                  = 10
write(3, "b", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 20, SEEK_SET)                  = 20
write(3, "c", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 7, SEEK_SET)                   = 7
write(3, "T", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 11, SEEK_SET)                  = 11
write(3, "7", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 1, SEEK_SET)                   = 1
write(3, "h", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 13, SEEK_SET)                  = 13
write(3, "c", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 6, SEEK_SET)                   = 6
write(3, "C", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 38, SEEK_SET)                  = 38
write(3, "6", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 18, SEEK_SET)                  = 18
write(3, "5", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 35, SEEK_SET)                  = 35
write(3, "2", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 12, SEEK_SET)                  = 12
```

```
write(3, "0", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 22, SEEK_SET)                  = 22
write(3, "a", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
lseek(3, 9, SEEK_SET)                   = 9
write(3, "{", 1)                        = 1
lseek(3, 0, SEEK_SET)                   = 0
write(3, "********************************"..., 44) = 44
close(3)                                = 0
unlink("/tmp/flag.txt")                 = 0
exit_group(0)                           = ?
+++ exited with 0 +++
```

Combing through the output, I noticed that the file mentioned in the description is located at `/tmp/flag.txt`

```
open("/tmp/flag.txt", O_WRONLY|O_CREAT|O_TRUNC, 0666) = 3
```

The binary then writes stars to the file, seeks to a location in the file and writes a character - which we can safely assume is the flag contents. After each `lseek` and `write` pair, the binary overwrites the flag with stars.

```
write(3, "********************************"..., 44) = 44
lseek(3, 30, SEEK_SET)                  = 30
write(3, "5", 1)                        = 1
```

We could read through the entire trace, keeping track of the file pointer and working out where each character will be placed. I preferred to use some bash to speed up the process.

I started the binary in `gdb` and set a breakpoint on the `write` libc call. I then ran the binary until the first breakpoint and then executed the following in my shell, in order to append the contents of flag.txt to my own text file after each file modification:

```
while inotifywait /tmp/flag.txt; do cat /tmp/flag.txt >> flag.txt; done
```

After continuing the binary's execution after each breakpoint, a text file containing all of the characters in the flag was produced. Upon stripping the lines with only stars, I was left with the flag contents:

```
*************************e*****************
******************************5************
************************a******************
*************************e*****************
********************************1**********
****************************************8**
************************************3******
****************************2**************
*****************7*************************
**********************************2********
***************************************5***
****************2**************************
*********************************1*********
*******************f***********************
**************************b****************
*****f*************************************
***r***************************************
*****************************d*************
***************************f***************
*******************************9***********
****i**************************************
********F**********************************
***************9***************************
*************************************c*****
******************************************}
**************5****************************
*****************************************9*
**a****************************************
```

```
***********************8*******************
*********************f*********************
S******************************************
**********b********************************
********************c**********************
*******T***********************************
***********7*******************************
*h*****************************************
*************c*****************************
******C************************************
**************************************6****
******************5************************
***********************************2*******
************0******************************
**********************a********************
*********{*********************************
```

After putting the characters together in the correct order, I submitted the flag for a juicy 50 points. :-)