

RADARE2 WORKSHOP

Exploitation

June 3, 2015

BerlinSide

Dairy

Julien (jvoisin) Voisin

- French
- Student
- I suck at exploitation

- "Exploitation with r2" workshop at hack.lu
- Two easy binaires
- We're going to do them together!

DAIRY



- CSAW quals 2013
- ctftime says it's an entry-level CTF
- We'll do it together, step by step.

STRACE WITH R2?

```
--> sn 0xf777cb73 syscall 192 mmap2 (0xffffffffda 0x0 0x23c0f 0x1 No debug register profile defined for 'a4'.
1 No debug register profile defined for 'a5'.
1)
--> sn 0xf777cb1d syscall 6 close (0xffffffffda)
--> sn 0xf777caa1 syscall 33 access (0xffffffffda 0xf777f3d4)
--> sn 0xf777c9a4 syscall 5 open (0xffffffffda 0xf7761838 0x80000)
--> sn 0xf777c9e4 syscall 3 read (0xffffffffda 0x6 0xffff28630)
--> sn 0xf777c92d syscall 197 fstat64 (0xffffffffda 0x6)
--> sn 0xf777cb73 syscall 192 mmap2 (0xffffffffda 0x0 0x1baedc 0x5 No debug register profile defined for 'a4'.
1 No debug register profile defined for 'a5'.
1)
--> sn 0xf777cb73 syscall 192 mmap2 (0xffffffffda 0xf7735000 0x5000 0x3 No debug register profile defined for 'a4'.
1 No debug register profile defined for 'a5'.
1)
--> sn 0xf777cb73 syscall 192 mmap2 (0xffffffffda 0xf773a000 0x1edc 0x3 No debug register profile defined for 'a4'.
1 No debug register profile defined for 'a5'.
1)
--> sn 0xf777cb1d syscall 6 close (0xffffffffda)
--> sn 0xf777cb73 syscall 192 mmap2 (0xffffffffda 0x0 0x1000 0x3 No debug register profile defined for 'a4'.
1 No debug register profile defined for 'a5'.
1)
--> sn 0xf77659f7 syscall 243 set_thread_area (0xffffffffda 0xffff28a30)
--> sn 0xf777cbf4 syscall 125 mprotect (0xffffffffda 0xf7735000 0x3000)
--> sn 0xf777cbf4 syscall 125 mprotect (0xffffffffda 0x804a000 0x1000)
--> sn 0xf777cbf4 syscall 125 mprotect (0xffffffffda 0xf7787000 0x1000)
--> sn 0xf777cbb1 syscall 91 munmap (0xffffffffda)
--> sn 0xf7764c10 syscall 102 socketcall (0xffffffffda 0x1)
--> sn 0xf7764c10 syscall 102 socketcall (0xffffffffda 0xe)
--> sn 0xf7764c10 syscall 102 socketcall (0xffffffffda 0x2)
--> sn 0xf7764c10 syscall 102 socketcall (0xffffffffda 0x4)
--> sn 0xf7764c10 syscall 174 rt_sigaction (0xffffffffda 0x11 0xffff28924)
--> sn 0xf7764c10 syscall 199 unknown (0xffffffffda 0xf7738000 0xffff28924)
--> sn 0xf7764c10 syscall 208 unknown (0xffffffffda 0xffffffff 0x3e8)
--> sn 0xf7764c10 syscall 199 unknown (0xffffffffda 0xf7738000 0x3e8)
--> sn 0xf7764c10 syscall 213 unknown (0xffffffffda 0x3e8 0x3e8)
--> sn 0xf7764c10 syscall 213 unknown (0xffffffffda 0x0 0x3e8)
--> sn 0xf7764c10 syscall 102 socketcall (0xffffffffda 0x5)
```

STRACE

```
jvoisin@kaa 14:31 ~/prez/BerlinSide2015/exploit strace ./fil_chal
execve("./fil_chal", ["/fil_chal"], [/* 90 vars */]) = 0
[ Process PID=5098 runs in 32 bit mode. ]
brk(0) = 0x917f000
access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
mmap2(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xffffffff775d000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=146447, ...}) = 0
mmap2(NULL, 146447, PROT_READ, MAP_PRIVATE, 3, 0) = 0xffffffff7739000
close(3) = 0
access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
open("/lib/i386-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\1\1\1\3\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0\220\210\1\0004\0\0\0"... , 512) = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=1807496, ...}) = 0
mmap2(NULL, 1814236, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0xffffffff757e000
mmap2(0xf7732000, 20480, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1b3000) = 0xffffffff7732000
mmap2(0xf7737000, 7900, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0xffffffff7737000
close(3) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xffffffff757d000
set_thread_area(0xff80b4a0) = 0
mprotect(0xf7732000, 12288, PROT_READ) = 0
mprotect(0x804a000, 4096, PROT_READ) = 0
mprotect(0xf7784000, 4096, PROT_READ) = 0
munmap(0xf7739000, 146447) = 0
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 3
setsockopt(3, SOL_SOCKET, SO_REUSEADDR, [1], 4) = 0
bind(3, {sa_family=AF_INET, sin_port=htons(34266), sin_addr=inet_addr("0.0.0.0")}, 16) = 0
listen(3, 100) = 0
rt_sigaction(SIGCHLD, {0x8048981, [], SA_RESTART}, NULL, 8) = 0
getuid(32) = 1000
setresuid32(4294967295, 1000, 4294967295) = 0
getuid(32) = 1000
setuid32(1000) = 0
setuid32(0) = -1 EPERM (Operation not permitted)
accept(3, 0xffff80b574, [16]) = ? ERESTARTSYS (To be restarted if SA_RESTART is set)
--- SIGWINCH({si_signo=SIGWINCH, si_code=SI_KERNEL}) ---
accept(3,
```



```
jvoisin@kaa 14:38 ~/prez/BerlinSide2015/exploit nc localhost 34266
*****
$ $ $ $ $ AAAAAA *****
* * * * * $ $ $ $ A A * * * * *
* * * * * $ $ $ $ A A A A * * * * *
* * * * * $ $ $ $ A A__A A * * * * *
* * * * * $ $ $ $ A A A A * * * * *
* * * * * $ $ $ $ A AAA A * * * * *
* * * * * $ $ $ $ A A A A * * * * *
* * * * * $ $ $ $ A A A A * * * * *
***** $ $ $ $ $ AAAAAA AAAAAA *****
Dairy

UserName: jvoisin
Password: issuperawesome?
Invalid credentials
jvoisin@kaa 14:39 ~/prez/BerlinSide2015/exploit
```

STRINGS?

```
vaddr=0x080499fd paddr=0x000019fd ordinal=027 sz=11 len=10 section=.rodata type=a string=UserName:
vaddr=0x08049a08 paddr=0x00001a08 ordinal=028 sz=11 len=10 section=.rodata type=a string=Password:
vaddr=0x08049a13 paddr=0x00001a13 ordinal=029 sz=21 len=20 section=.rodata type=a string=Invalid credentials\n
vaddr=0x08049a26 paddr=0x00001a26 ordinal=030 sz=39 len=38 section=.rodata type=a string=Welcome!\nhhttp://youtu.be/KmtzQCSh6xk\n\n
vaddr=0x08049a4f paddr=0x00001a4f ordinal=031 sz=9 len=8 section=.rodata type=a string=csaw2013
vaddr=0x08049a58 paddr=0x00001a58 ordinal=032 sz=10 len=9 section=.rodata type=a string=SimplePWD
[0x080489a8]> |
```

- Check 0x08048e52

- Check 0x08048e52
- Check 0x08048efe

- Check 0x08048e52
- Check 0x08048efe
- Integer overflow!

MITIGATIONS?

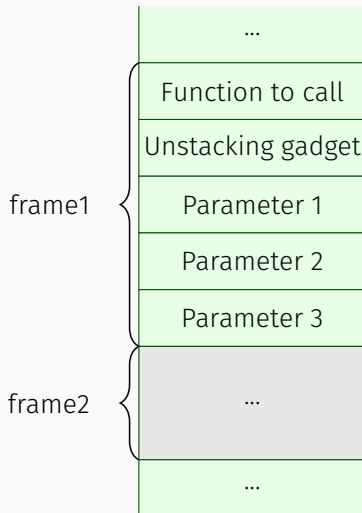
- ✗ NX
- ✗ ASLR
- ✗ Canary
- ✓ System-wide ASLR

- Static analysis
- De Bruijn Pattern

- Static analysis
- De Bruijn Pattern

1056 bytes before overwriting EIP

ROP CHAIN



1. Leak libc address of `read(1)` and return to the vulnerable function

1. Leak libc address of `read(1)` and return to the vulnerable function
2. Compute the offset of `system(2)`

1. Leak libc address of `read(1)` and return to the vulnerable function
2. Compute the offset of `system(2)`
3. Read our command, and write it *somewhere*

1. Leak libc address of `read(1)` and return to the vulnerable function
2. Compute the offset of `system(2)`
3. Read our command, and write it *somewhere*
4. Call `system(3)` on it

1. Leak libc address of `read(1)` and return to the vulnerable function
2. Compute the offset of `system(2)`
3. Read our command, and write it *somewhere*
4. Call `system(3)` on it
5. Send our command

1. Stack is executable

1. Stack is executable
2. No `jmp esp` gadget

1. Stack is executable
2. No `jmp esp` gadget
3. Write `jmp esp` in the `.data segment`

1. Stack is executable
2. No `jmp esp` gadget
3. Write `jmp esp` in the `.data segment`
4. Return to it

1. Stack is executable
2. No `jmp esp` gadget
3. Write `jmp esp` in the `.data segment`
4. Return to it
5. Send our reverse-shell shellcode

1. Stack is executable
2. No `jmp esp` gadget
3. Write `jmp esp` in the `.data segment`
4. Return to it
5. Send our reverse-shell shellcode

1. Stack is executable
2. No `jmp esp` gadget
3. Write `jmp esp` in the `.data segment`
4. Return to it
5. Send our reverse-shell shellcode

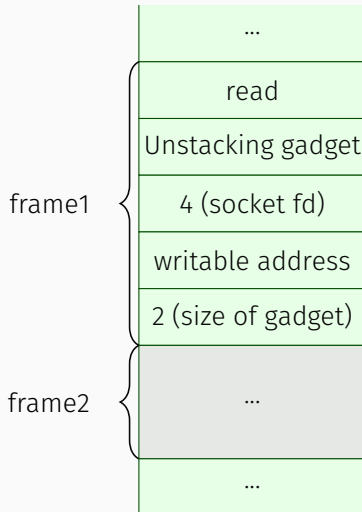
Works regardless of your libc version.

WRITEABLE LOCATION

```
[0x080488c0]> iS~w
idx=17 vaddr=0x0804ae88 paddr=0x00001e88 sz=8 vsz=8 perm=-rw- name=.ctors
idx=18 vaddr=0x0804ae90 paddr=0x00001e90 sz=8 vsz=8 perm=-rw- name=.dtors
idx=19 vaddr=0x0804ae98 paddr=0x00001e98 sz=4 vsz=4 perm=-rw- name=.jcr
idx=20 vaddr=0x0804ae9c paddr=0x00001e9c sz=216 vsz=216 perm=-rw- name=.dynamic
idx=21 vaddr=0x0804af74 paddr=0x00001f74 sz=140 vsz=140 perm=-rw- name=.got
idx=22 vaddr=0x0804b000 paddr=0x00002000 sz=8 vsz=8 perm=-rw- name=.data
idx=23 vaddr=0x0804b008 paddr=0x00002008 sz=24 vsz=24 perm=-rw- name=.bss
idx=27 vaddr=0x0804ae88 paddr=0x00001e88 sz=4096 vsz=4096 perm=-rw- name=phdr1
idx=28 vaddr=0x08048000 paddr=0x00000000 sz=52 vsz=52 perm=-rw- name=ehdr
[0x080488c0]> █
```

Let's use 0x0804b000

ROP CHAIN



Write a working exploit!

- Exploitation is cool
- CTF-oriented
- More to come at REcon

Radare2 is nice.
You should use it.

- Github repo
- Official website
- The r2 blog
- The r2 book
- Twitter