3.43

A.

|  |  |
| --- | --- |
| 08 04 86 43 | 返回地址 |
| bf ff fc 94 | %ebp |
| 00 00 00 03 | %edi |
| 00 00 00 02 | %esi |
| 00 00 00 01 | %ebx |
| 37 36 35 34 | 缓冲区 |
| 33 32 31 30 | 缓冲区 |

B.

|  |  |
| --- | --- |
| 08 04 86 00 | 破坏返回地址（最后一个字节为输入的’\0’） |
| 33 32 31 30 | 破坏%ebp |
| 39 38 37 36 | 破坏%edi |
| 35 34 33 32 | 破坏%esi |
| 31 30 39 38 | 破坏%ebx |
| 37 36 35 34 | 缓冲区 |
| 33 32 31 30 | 缓冲区 |

C.

试图返回先前的08048643地址，然而输入时末尾有空字符’\0’，破坏了返回地址的低字节。

D.

%edx, %esi, %edi, %ebp的值被破坏。

E.

应当把strlen(buf)+k（k为大于等于1的正整数）作为malloc的参数，并且对返回地址进行检查，是否为空.

3.44

A.

地址范围大约为(d-b)\*16^3=2^13

B.

若尝试一个有128字节的nop sled的缓冲区溢出，则枚举2^13/2^7=2^6=64个起始地址即可穷尽。

3.45

A.

在不带保护者的版本中，buf保存在-20(%dbp)中，v保存在-8(%ebp)中；

在带保护者的版本中，buf保存在-20(%ebp)中，v保存在-24(%ebp)中，金丝雀保存在-8(%ebp)中；

B.

带保护者的版本中，由于v的地址比buf更低，若buf溢出，则会直接影响到金丝雀的值，而不会干扰到v。假若v在金丝雀和buf之间，即使金丝雀检测到溢出，v已经被破坏。

3.47

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| src\_t | dest\_t | 指令 | S | D |
| long | long | movq | %rdi | %rax |
| int | long | movslq | %edi | %rax |
| char | long | movsbq | %dil | %rax |
| unsigned int | unsigned long | movl | %edi | %eax |
| unsigned char | unsigned long | movzbq | %dil | %rax |
| long | int | movl | %edi | %eax |
| unsigned long | unsigned | movl | %edi | %eax |

3.48

long arithprob(int a, long b, char c, int d);