1-9. Buffer overflow question

Based on the buffer overflow lab, function `test`() calls `getbuf`() which calls `Gets`(`char`*). The following is the debugger output when the program is paused at code address `0x08048e4a` inside function `Gets`() before executing the "`leave`" instruction, i.e. the `Gets`() function's stack frame is still intact.

Notes: (a) the size of the buffer and stack location might be different from your lab. (b) Answer all address/pointer values in hex.

```
(gdb) x /24xw $ebp

0x55402020 <...>: 0x55402060  0x08048ca0  0x55402040  0x55402044

0x55402030 <...>: 0xf7fb8000  0xf7fb8000  0x55402060  0xf7e3708d

0x55402040 <...>: 0x74736554  0x00000031  0x00000000  0xf7e3721d

0x55402050 <...>: 0xffffd000  0x080490bc  0xf7fb8d60  0x0804a4bf

0x55402060 <...>: 0x55402080  0x08048c27  0xf7f2b136  0xf7f2b1cd

0x55402070 <...>: 0x2cf5bf57  0x08048fae  0x0804a4bf  0x000000f4


(gdb) disassemble

Dump of assembler code for function Gets:

   0x08048de1 <+0>:     push   %ebp

   0x08048de2 <+1>:     mov    %esp,%ebp

   0x08048de4 <+3>:     sub    $0x18,%esp

   ...

   0x08048e47 <+102>:   mov    0x8(%ebp),%eax

=> 0x08048e4a <+105>:   leave

   0x08048e4b <+106>:   ret

End of assembler dump.
```

- What is the base pointer (address) for each of these functions' stack frame?

`Gets`(): (1) _____

`getbuf`(): (2) _____

`test`(): (3) _____

- Where in memory (address) is the return address back to function `test`() stored? (4)

_____

- Where in memory (address) is the buffer that function `getbuf`() passed to function `Gets`()? The actual location of the buffer, NOT the location of the parameter. (5) _____

- What will be the value of %`esp` right after line `0x08048e4b`, the "`ret`" instruction in function `Gets`(), finish executing? The address at top of the stack after function `Gets`() completes. (6) _____

- What is the byte value, in hex, stored at memory location `0x55402042`? (7) _____
- What is the input string that was typed from console and received by function `Gets`()? Give the actual string in ASCII characters. (8)

  _____
- In order to exploit the buffer overflow bug in this code and make function `getbuf`() jump to function `smoke`() instead of return to function `test`(), how many bytes of padding do I need in the input string before entering the address of `smoke`()? Give number in decimal. (9) _____