Errata for *Hacking, 2nd edition* (updated to 22nd printing)

Page 3: In the last paragraph, "DCMA" should now read "DMCA."

Page 19: The code in *firstprog.c* that reads:

```
printf("Hello, world!\n");
```

should now read:

```
puts("Hello, world!\n");
```

Page 22: In the first paragraph, the second to last sentence should now read: "The 32-bit processors have 2^32 (or 4,294,967,296) possible addresses, while current 64-bit processors have a 48-bit address space, allowing for 2^48 addresses."

Page 25: The last sentence of the first full paragraph should note that EIP points to a memory address at 0x804837a, not 0x804838a.

Page 38: The line in the last paragraph that reads:
"The character array was defined, so 20 bytes are allocated for it, but only 12 of these bytes are actually used."
should now read:
"The character array was defined, so 20 bytes are allocated for it, but only 15 of these bytes are actually used."

Page 55: In the code listing for the *pointer_types3.c* program, the first `for` loop's comment should read: "`Iterate through the char array with the int_pointer`." The second `for` loop's comment should read: "`Iterate through the int array with the char_pointer`."

Page 56: In the code listing for the *pointer_types4.c* program, the first comment should read: "`Iterate through the char array with the void_pointer`." The second comment should read: "`Iterate through the int array with an unsigned integer`."

Page 57: In the code listing for the *pointer_types5.c* program, the first comment should read: "`Iterate through the char array with an unsigned integer.`" The second comment should read: "`Iterate through the int array with an unsigned integer.`"

Page 71: In the *stack_example.c* code, the text should read "The local variables for the function include a 4-byte integer called `flag` and a 10-character buffer called `buffer`."

Page 72: In the block of code at the top of the page, the second line which reads:
`(gdb) disass test_function()`
should now read:
`(gdb) disass test_function`

Page 74: The (2) should be placed at `0xbffff7dc` in the `gdb` listing. This is the last hexword on the second line of the stack listing, directly above where the (4) is. The hexvalue for that position in the text is `0x080483b9`.

Page 87: In section 0x282, in the first section after output, the sentence that reads:
"For the other two simplenote files, the owner is reader and the group is users."
should now read:
"For the other two `simplenote*` files, the owner is reader and the group is users and reader."

Page 88: In section 0x282, the first sentence of the page after the code should read: "The first command (`chmod 731`) gives read, write, and execute permissions to the user . . ."

Page 114: The statistic "increase your chances of finding the ace from 33 percent to 50 percent" should now read "33 percent to 66 percent"

Page 128: In the diagram, "`return_value` variable" should be "`auth_flag` variable"

Page 148: The third paragraph of this page makes an incorrect reference to *notesearch_exploit.c*. It should read *exploit_notesearch.c.*

Page 153: The last sentence of the fourth paragraph should read: “The same password with a different salt produces a different hash.”

Page 197: In the third line, “next later” should be “next layer.”

Page 298: The line in the last paragraph:
“The extra backslash doesn’t matter and is effectively ignored.”
should instead read:
“The extra slash doesn’t matter and is effectively ignored.”