

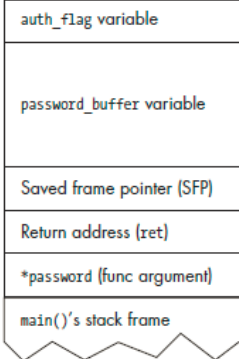
# Hacking, 2nd edition

## The Art of Exploitation

by Jon Erickson

errata updated to print 23

Page	Error	Correction	Print corrected
3	The Digital Millennium Copyright Act ( <b>DCMA</b> ) of 1998 makes it illegal to discuss or provide technology that might be used to bypass industry consumer controls.	The Digital Millennium Copyright Act ( <b>DMCA</b> ) of 1998 makes it illegal to discuss or provide technology that might be used to bypass industry consumer controls.	Print 3
19	<pre>printf("Hello, world!\n");</pre>	<pre>puts("Hello, world!\n");</pre>	Print 19
22	The 32-bit processors have $2^{32}$ (or 4,294,967,296) possible addresses, while the 64-bit <b>ones have <math>2^{64}</math> (<math>1.84467441 \times 10^{19}</math>) possible</b> addresses.	The 32-bit processors have $2^{32}$ (or 4,294,967,296) possible addresses, while current 64-bit <b>processors have a 48-bit address space, allowing for <math>2^{48}</math></b> addresses.	Print 5
25	Currently, it points to a memory address at <b>0x804838a</b> .	Currently, it points to a memory address at <b>0x804837a</b> .	Print 5
38	The character array was defined, so 20 bytes are allocated for it, but only <b>12</b> of these bytes are actually used.	The character array was defined, so 20 bytes are allocated for it, but only <b>15</b> of these bytes are actually used.	Print 8
55–57	<pre>for(i=0; i &lt; 5; i++) { // Iterate through the int array with the int_pointer. --snip-- for(i=0; i &lt; 5; i++) { // Iterate through the char array with the char_pointer.</pre>	<pre>for(i=0; i &lt; 5; i++) { // Iterate through the char array with the int_pointer. --snip-- for(i=0; i &lt; 5; i++) { // Iterate through the int array with the char_pointer.</pre>	Print 3
71	The local variables for the function include a <b>single character</b> called flag and a 10-character buffer called buffer	The local variables for the function include a <b>4-byte integer</b> called flag and a 10-character buffer called buffer	Print 3
72	<pre>(gdb) disass test_function()</pre>	<pre>(gdb) disass test_function</pre>	Print 9
87	For the other two <b>simplenote</b> files, the owner is reader and the group is users.	For the other two <b>simplenote*</b> files, the owner is reader and the group is users <b>and reader</b> .	Print 3
88	The first command ( <code>chmod 721</code> ) gives read, write, and execute permissions to the user	The first command ( <code>chmod 731</code> ) gives read, write, and execute permissions to the user	Print 4
114	... increase your chances of finding the ace from 33 percent to <b>50</b> percent	... increase your chances of finding the ace from 33 percent to <b>66</b> percent	Print 3

Page	Error	Correction	Print corrected
128	Figure replacement	 <p>The diagram shows a vertical stack of memory frames. From top to bottom, the frames are: 'auth_flag variable', 'password_buffer variable', 'Saved frame pointer (SFP)', 'Return address (ret)', '*password (func argument)', and 'main()'s stack frame'. The bottom frame has a jagged, sawtooth-like bottom edge.</p>	Print 4
148	The <code>system()</code> function is used in the <code>notesearch_exploit.c</code> program to execute a command.	The <code>system()</code> function is used in the <code>exploit_notesearch.c</code> program to execute a command.	Print 5
153	The same password with a different salt produces a different <b>salt</b> .	The same password with a different salt produces a different <b>hash</b> .	Print 4
197	The next <b>later</b> is the data link layer.	The next <b>layer</b> is the data link layer.	Print 19
298	The extra <b>backslash</b> doesn't matter and is effectively ignored	The extra <b>slash</b> doesn't matter and is effectively ignored	Print 8