

```

1: # include <stdio.h>
2: # include <stdlib.h>
3: # include <stdio.h>
4: # include <string.h>
5: # include <windows.h>
6:
7: int main(void)
8: {
9:     char *shellcode = "\x33\xc9\x64\x8b\x49\x30\x8b\x49\x0c\x8b"
10:    "\x49\x1c\x8b\x59\x08\x8b\x41\x20\x8b\x09"
11:    "\x80\x78\x0c\x33\x75\xf2\x8b\xeb\x03\x6d"
12:    "\x3c\x8b\x6d\x78\x03\xeb\x8b\x45\x20\x03"
13:    "\xc3\x33\xd2\x8b\x34\x90\x03\xf3\x42\x81"
14:    "\x3e\x47\x65\x74\x50\x75\xf2\x81\x7e\x04"
15:    "\x72\x6f\x63\x41\x75\xe9\x8b\x75\x24\x03"
16:    "\xf3\x66\x8b\x14\x56\x8b\x75\x1c\x03\xf3"
17:    "\x8b\x74\x96\xfc\x03\xf3\x33\xff\x57\x68"
18:    "\x61\x72\x79\x41\x68\x4c\x69\x62\x72\x68"
19:    "\x4c\x6f\x61\x64\x54\x53\xff\xd6\x33\xc9"
20:    "\x57\x66\xb9\x33\x32\x51\x68\x75\x73\x65"
21:    "\x72\x54\xff\xd0\x57\x68\x6f\x78\x41\x01"
22:    "\xfe\x4c\x24\x03\x68\x61\x67\x65\x42\x68"
23:    "\x4d\x65\x73\x73\x54\x50\xff\xd6\x57\x68"
24:    "\x72\x6c\x64\x21\x68\x6f\x20\x57\x6f\x68"
25:    "\x48\x65\x6c\x6c\x8b\xcc\x57\x57\x51\x57"
26:    "\xff\xd0\x57\x68\x65\x73\x73\x01\xfe\x4c"
27:    "\x24\x03\x68\x50\x72\x6f\x63\x68\x45\x78"
28:    "\x69\x74\x54\x53\xff\xd6\x57\xff\xd0";
29:
30:     DWORD variable;
31:     BOOL ret = VirtualProtect (shellcode, strlen(shellcode),
32:     PAGE_EXECUTE_READWRITE, &variable);
33:
34:     if (!ret) {
35:         printf ("VirtualProtect\n");
36:         return EXIT_FAILURE;
37:     }
38:
39:     printf("strlen(shellcode)=%d\n", strlen(shellcode));//print out length of shellcode
40:
41:     ((void (*)(void))shellcode)();//Execute Shellcode
42:
43:     return EXIT_SUCCESS;
44: }

```