NC STATE UNIVERSITY
Message Board

Course: CSC501 - 001
Forum: PA1 Discussion

Go to: **Different Course** | **Forum List** | **Topic List**

Author	Topic: How to use the register dump given by trap?

adhanas   Sat Feb 1 19:53   [who]

Xinu trap!
exception 13 (general protection violation) currpid 48 (<])
eflags 10213 eip 14 error code 00000000 (0)
register dump:
eax 00ff00ff (16711935)
ecx 00000212 (530)
edx 00000864 (2148)
ebx 0000645f (25695)
esp 00011294 (70292)
ebp 00011294 (70292)
esi 00ffdf82 (16768898)
edi 000112a0 (70304)

What to make out of this info? How to decode the instruction 0x14? A quick look at the x86 instruction set manual has multiple instructions mapped to 0x14 based on the modes. Not much in eflags, either.

All I could get is: I, somewhere messed up the memory where the proc's name is stored. Now, how could one backtrack to the code which might have caused this by using the above presented info?

Thanks!

[Post New Topic]   [Post a Reply]

WolfWare - Message Board - last update 30-Aug-2001