PC技术辅导:断点设置表 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/284/2021_2022_PC_E6_8A_80_E6_9C_AF_E8_BE_c97_284872.htm 一般处理： bpx hmemcpy （万能断点） bpx MessageBox bpx MessageBoxExA bpx MessageBeep bpx SendMessage bpx GetDlgItemText bpx GetDlgItemInt bpx GetWindowText bpx GetWindowWord bpx GetWindowInt bpx DialogBoxParamA bpx createWindow bpx createWindowEx bpx ShowWindow bpx 0updateWindow bmsg xxxx wm_move bmsg xxxx wm_gettext bmsg xxxx wm_command bmsg xxxx wm_activate bmsg xxxx wm_create bmsg xxxx wm_destroy 时间相关: bpint 21 if ah==2A (DOS) bpx GetLocalTime bpx GetFileTime bpx GetSystemtime CD-ROM 或磁盘相关: bpint 13 if ah==2 (DOS) bpint 13 if ah==3 (DOS) bpint 13 if ah==4 (DOS) bpx GetFileAttributesA bpx GetFileSize bpx GetDriveType bpx GetLastError bpx ReadFile bpio -h (Your CD-ROM Port Address) R 软件狗相关: bpio -h 278 R bpio -h 378 R 文件访问相关: bpint 21 if ah==3dh (DOS) bpint 31 if ah==3fh (DOS) bpint 21 if ah==3dh (DOS) bpx ReadFile bpx WriteFile bpx createFile bpx SetFilePointer bpx GetSystemDirectory INI 初始化文件相关: bpx GetPrivateProfileString bpx GetPrivateProfileInt bpx WritePrivateProfileString bpx WritePrivateProfileInt 注册表相关: bpx RegcreateKey bpx Reg0deleteKey bpx RegCloseKey bpx RegOpenKey bpx RegQueryValue 注册标志相关: bpx cs:eip if EAX==0 内存标准相关: bpmb cs:eip rw if 0x30:0x45AA==0 显示相关: bpx 0x30:0x45AA do "d 0x30:0x44BB" bpx CS:0x66CC do "?

EAX" 利用S命令设断： S [-cu][address L length data-list] address :搜索的起始地址 length :搜索的长度(字节长) data-list :可以是一系列字节,也可以是字符串, 字符串可以用单引号或双引号括住 例如：S 30:0 L ffffffff ’********’ 100Test 下载频道开通, 各类考试题目直接下载。详细请访问 www.100test.com