快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术 <=
- 安全技术
- 业界动态

本类热门
- 初探数据包分析程序设计
- 杀毒软件的简单实现
- readasm的使用范例
- 半开扫描程序
- 注册表操作（RingZ_RgeEdit）
- proftpd 1.2.7/1.2.9rc2 remote root exploit

intel x86 类NOP 指令列表(修订版)

提交文章： bkbll
提交日期： 2003-09-10
文章属性： 原创
文档类别： 编程技术
浏览次数： 今2次/总3056次

intel x86 类NOP 指令列表(修订版)
bkbll(bkbll@cnhonker.net)
2003/09/10

这篇文章是无聊的时候写的, 因为看到phrack 61上面的fake-nop的东东, 觉得有意思.
后来又受到eyas(cooleyas@21cn.com)的启发,从intel指令手册上找了找,下面是我试验通过可以替换NOP的指令.
注1: 这里不考虑双字节或以上的指令的fake-nop编码.
注2: eyas加了xchg指令.

16进制机器码	x86汇编指令	指令意义	可能影响的寄存器或标志位
06	PUSHL %es	es进栈	esp
0E	PUSHL %cs	cs进栈	esp
16	PUSHL %ss	ss进栈	esp
1E	PUSHL %ds	ds进栈	esp
27	DAA	加法小数位调整	AF CF PF SF ZF AL
2F	DAS	减法小数位调整	AF CF PF SF ZF AL
37	AAA	加法的ASCII调整	AF CF AL
3F	AAS	减法小数位调整	AF CF AL
40	INC %eax	%eax加1	AF OF PF SF ZF eax
41	INC %ecx	%ecx加1	AF OF PF SF ZF ecx
42	INC %edx	%edx加1	AF OF PF SF ZF edx
43	INC %ebx	%ebx加1	AF OF PF SF ZF ebx
44	INC %esp	%esp加1	AF OF PF SF ZF esp
45	INC %ebp	%ebp加1	AF OF PF SF ZF ebp
46	INC %esi	%esi加1	AF OF PF SF ZF esi
47	INC %edi	%edi加1	AF OF PF SF ZF

edi			
48	DEC %eax	%eax减1	AF OF PF SF ZF
eax			
49	DEC %ecx	%ecx减1	AF OF PF SF ZF
ecx			
4A	DEC %edx	%edx减1	AF OF PF SF ZF
edx			
4B	DEC %ebx	%ebx减1	AF OF PF SF ZF
ebx			
4C	DEC %esp	%esp减1	AF OF PF SF ZF
esp			
4D	DEC %ebp	%ebp减1	AF OF PF SF ZF
ebp			
4E	DEC %esi	%esi减1	AF OF PF SF ZF
esi			
4F	DEC %edi	%edi减1	AF OF PF SF ZF
edi			
50	PUSHL %eax	eax进栈	esp
51	PUSHL %ecx	ecx进栈	esp
52	PUSHL %edx	edx进栈	esp
53	PUSHL %ebx	ebx进栈	esp
54	PUSHL %esp	esp进栈	esp
55	PUSHL %ebp	ebp进栈	esp
56	PUSHL %esi	esi进栈	esp
57	PUSHL %edi	edi进栈	esp
90	NOP	(NULL)	(NULL)
91	XCHG %ecx,%eax	交换寄存器内容	eax,ecx
92	XCHG %edx,%eax	交换寄存器内容	edx,eax
93	XCHG %ebx,%eax	交换寄存器内容	ebx,eax
95	XCHG %ebp,%eax	交换寄存器内容	ebp,eax
96	XCHG %esi,%eax	交换寄存器内容	esi,eax
97	XCHG %edi,%eax	交换寄存器内容	edi,eax
98	CBW	将byte的AL转换成word的EAX	EAX
9B	WAIT	等待CPU处理完数据	(NULL)
D6	无效指令	(NULL)	(NULL)
F5	CMC	转换CF标志位(开关)	CF
F8	CLC	清CF位(CF=0)	CF
F9	STC	设置CF位(CF=1)	CF
FC	CLD	设置DF位(DF=1)	DF
FD	STD	清理DF位(DF=0)	DF

1. 上面利用XCHG/PUSHL/INC/DEC的方法程序应该不会出错, 可以正常到目的, 但寄存器内容被改变了.inc eax就改变了eax的值,
只能算无奈的办法.
2. 利用改变标志寄存器位是个不错的想法, 基本上不会影响流程, 但看到还是改变了CPU的东西还是不满意.
3. \x90(NOP),\x9b(wait),\xd6(bad) 这三个指令不错, 都不会改变程序的流程, 又不会改变寄存器的东东.
这里尤其指明的是\xd6指令, 在intel手册上没查到对应什么指令, 但在linux下和windows下发现系统对于这个是继续
执行下一条指令,和NOP相似.
在我看来,上面这些指令利用顺序优先级最好是:

\x90(NOP) > \xd6 > \x9b > 改变标志寄存器的操作指令 > INC/DEC/PUSHL/XCHG

//thx to eyas

参考资料:
1. <<Intel Assemble Instruction Set>> (不记得从哪里下载)
2. <<8086/8088指令与机器码转换对照表>> By 怜香(于2002-10-18发表) (不记得从哪里下载的)

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net