

Crash Reference Card (32-bit)

Reg	Usage	Saved
EAX	Argument #1 / Return Lo	no
EBX	Local variable	yes
ECX	Argument #3	no
EDX	Argument #2 / Return Hi	no
ESI	Local variables	yes
EDI		yes
EBP	(Stack base pointer)	yes
ESP	Stack pointer	yes

Virtual Memory Layout

00000000 - BFFFFFFF	user space
C0000000 - F7xxxxxx	directmap (incl. kernel)
F7xxxxxx - FF7FE000	vmalloc (incl. modules)
FF800000 - FFC00000	kmap
FFDxxxxx - FFFFF000	fixmaps (incl. VDSO)

Poison Values

0x00100100	deleted list_head next
0x00200200	deleted list_head prev
0xbd	destroyed secure key
0x6c	freed flexible array

AT&T Assembler Syntax

Prefixes

% register
\$ immediate
0x hex number

`movl $0x1,0x28(%ecx,%eax,4)`
 $0x28 + \%ecx + \%eax * 4$

Suffixes

b 8-bit (byte)
w 16-bit (word)
l 32-bit (long)
q 64-bit (quad)

Running crash

sh\$ **crash vmlinux.debug boot/vmlinux.gz vmcore**

Calling Conventions

	Function	Syscall
1	EAX	EBX
2	EDX	ECX
3	ECX	EDX
4	—	ESI
5	—	EDI
6	—	EBP
Return	EAX	EAX
RetHi	EDX	—
Syscall number:		EAX

Crash Reference Card (64-bit)

Reg	Usage	Saved	Reg	Usage	Saved
RAX	Return value	no	R8	Argument #5	no
RBX	Local variable	yes	R9	Argument #6	no
RCX	Argument #4	no	R10	Scratch registers	no
RDX	Argument #3	no	R11		no
RSI	Argument #2	no	R12	Local variables	yes
RDI	Argument #1	no	R13		yes
RBP	(Stack base pointer)	yes	R14		yes
RSP	Stack pointer	yes	R15		yes

Virtual Memory Layout

0000000000000000 - 00007FFFFFFFFFFFFF	user space
DEAD0000xxxxxxxx	pointer poisons
FFFF800000000000 - FFFF87FFFFFFFFFFFF	hypervisor area
FFFF880000000000 - FFFFC7FFFFFFFFFFFF	direct mapping
FFFC900000000000 - FFFE87FFFFFFFFFFFF	vmalloc/ioremap
FFFEA00000000000 - FFFEAFFFFFFFFFFFFF	vmemmap
FFFFFFFF80000000 - FFFFFFFFF9FFFFFFFF	kernel text+data
FFFFFFFFFA00000000 - FFFFFFFFFFxxxxxx	kernel modules
FFFFFFFFFFFFxxxxxx - FFFFFFFFFF5FFFFF	permanent fixmaps
FFFFFFFFFFFF600000 - FFFFFFFFFFDFFFFFFF	vsyscalls (deprecated)

Calling Conventions	Function	Syscall
1	RDI	RDI
2	RSI	RSI
3	RDX	RDX
4	RCX	R10
5	R8	R8
6	R9	R9
Return	RAX	RAX
RetHi	RDX	-
Syscall number:		RAX