ret2syscall

系统调用

系统调用是操作系统提供的一组功能接口，用于为应用程序实现一系列高权限的功能服务，例如IO接口的打开关闭读写，进程的创建终止等功能。简单的来说就是一些由系统内核提供的函数。但是调用这些函数的方法比较特殊，以Linux系统为例，在汇编环境下64位程序通过`syscall`指令进行系统调用，由`rax`寄存器传递系统调用号，传参顺序依次为`rdi`，`rsi`，`rdx`，`r10`，`r8`，`r9`，返回值存在`rax`中；而32为程序通过`int 80`操作进行系统调用，由`eax`寄存器传递系统调用号，传参顺序依次为`ebx`，`ecx`，`edx`，`esi`，`edi`，`ebp`，返回值存在`eax`中。32位和64位Linux系统调用表可以在这个文档最后面找到。

在Linux的glibc中，大部分系统调用已经被封装成普通的函数，如`read`，`write`，`open`，`execve`等，同时也将`syscall`指令进行了封装，以64位Linux的glibc位例，调用`read(0, buf, 0x10)`函数也可以是`syscall(0, 0, buf, 0x10)`（实际read函数的封装还会有一些其他的处理，但是功能基本等价）。

ret2syscall

如果一个程序中使用了syscall，那么我们构造ROP链就可以使用syscall来getshell。而构造ROP链主要就是为了实现调用`execve("/bin/sh", NULL, NULL)`（execve为系统调用）。

一点点小技巧

`read`和`write`函数返回值为输入或者输出的字符串的长度，而返回值存在`ax`寄存器中。可以利用这两个函数来控制系统调用需要的`rax`的值。

Linux系统调用表

32位Linux系统调用表

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
restart_syscall	0x00	-	-	-	-	-	-
exit	0x01	int error_code	-	-	-	-	-
fork	0x02	-	-	-	-	-	-
read	0x03	unsigned int fd	char *buf	size_t count	-	-	-
write	0x04	unsigned int fd	const char *buf	size_t count	-	-	-
open	0x05	const char *filename	int flags	umode_t mode	-	-	-
close	0x06	unsigned int fd	-	-	-	-	-
waitpid	0x07	pid_t pid	int *stat_addr	int options	-	-	-
creat	0x08	const char *pathname	umode_t mode	-	-	-	-
link	0x09	const char *oldname	const char *newname	-	-	-	-
unlink	0x0a	const char *pathname	-	-	-	-	-
execve	0x0b	const char *filename	const char *const *argv	const char *const *envp	-	-	-
chdir	0x0c	const char *filename	-	-	-	-	-
time	0x0d	time_t *tloc	-	-	-	-	-
mknod	0x0e	const char *filename	umode_t mode	unsigned dev	-	-	-
chmod	0x0f	const char *filename	umode_t mode	-	-	-	-
lchown	0x10	const char *filename	uid_t user	gid_t group	-	-	-
break	0x11	?	?	?	?	?	?
oldstat	0x12	?	?	?	?	?	?
lseek	0x13	unsigned int fd	off_t offset	unsigned int whence	-	-	-
getpid	0x14	-	-	-	-	-	-
mount	0x15	char *dev_name	char *dir_name	char *type	unsigned long flags	void *data	-
umount	0x16	char *name	int flags	-	-	-	-
setuid	0x17	uid_t uid	-	-	-	-	-
getuid	0x18	-	-	-	-	-	-
stime	0x19	time_t *tptr	-	-	-	-	-
ptrace	0x1a	long request	long pid	unsigned long addr	unsigned long data	-	-
alarm	0x1b	unsigned int seconds	-	-	-	-	-
oldfstat	0x1c	?	?	?	?	?	?
pause	0x1d	-	-	-	-	-	-
utime	0x1e	char *filename	struct utimbuf *times	-	-	-	-
stty	0x1f	?	?	?	?	?	?
gtty	0x20	?	?	?	?	?	?
access	0x21	const char *filename	int mode	-	-	-	-
nice	0x22	int increment	-	-	-	-	-
ftime	0x23	?	?	?	?	?	?
sync	0x24	-	-	-	-	-	-
kill	0x25	pid_t pid	int sig	-	-	-	-
rename	0x26	const char *oldname	const char *newname	-	-	-	-
mkdir	0x27	const char *pathname	umode_t mode	-	-	-	-
rmdir	0x28	const char *pathname	-	-	-	-	-
dup	0x29	unsigned int fildes	-	-	-	-	-
pipe	0x2a	int *fildes	-	-	-	-	-
times	0x2b	struct tms *tbuf	-	-	-	-	-
prof	0x2c	?	?	?	?	?	?
brk	0x2d	unsigned long brk	-	-	-	-	-
setgid	0x2e	gid_t gid	-	-	-	-	-

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
getgid	0x2f	-	-	-	-	-	-
signal	0x30	int sig	__sighandler_t handler	-	-	-	-
geteuid	0x31	-	-	-	-	-	-
getegid	0x32	-	-	-	-	-	-
acct	0x33	const char *name	-	-	-	-	-
umount2	0x34	?	?	?	?	?	?
lock	0x35	?	?	?	?	?	?
ioctl	0x36	unsigned int fd	unsigned int cmd	unsigned long arg	-	-	-
fcntl	0x37	unsigned int fd	unsigned int cmd	unsigned long arg	-	-	-
mpx	0x38	?	?	?	?	?	?
setpgid	0x39	pid_t pid	pid_t pgid	-	-	-	-
ulimit	0x3a	?	?	?	?	?	?
oldolduname	0x3b	?	?	?	?	?	?
umask	0x3c	int mask	-	-	-	-	-
chroot	0x3d	const char *filename	-	-	-	-	-
ustat	0x3e	unsigned dev	struct ustat *ubuf	-	-	-	-
dup2	0x3f	unsigned int oldfd	unsigned int newfd	-	-	-	-
getppid	0x40	-	-	-	-	-	-
getpgrp	0x41	-	-	-	-	-	-
setsid	0x42	-	-	-	-	-	-
sigaction	0x43	int	const struct old_sigaction *	struct old_sigaction *	-	-	-
sgetmask	0x44	-	-	-	-	-	-
ssetmask	0x45	int newmask	-	-	-	-	-
setreuid	0x46	uid_t ruid	uid_t euid	-	-	-	-
setregid	0x47	gid_t rgid	gid_t egid	-	-	-	-
sigsuspend	0x48	int unused1	int unused2	old_sigset_t mask	-	-	-
sigpending	0x49	old_sigset_t *uset	-	-	-	-	-
sethostname	0x4a	char *name	int len	-	-	-	-
setrlimit	0x4b	unsigned int resource	struct rlimit *rlim	-	-	-	-
getrlimit	0x4c	unsigned int resource	struct rlimit *rlim	-	-	-	-
getrusage	0x4d	int who	struct rusage *ru	-	-	-	-
gettimeofday	0x4e	struct timeval *tv	struct timezone *tz	-	-	-	-
settimeofday	0x4f	struct timeval *tv	struct timezone *tz	-	-	-	-
getgroups	0x50	int gidsetsize	gid_t *grouplist	-	-	-	-
setgroups	0x51	int gidsetsize	gid_t *grouplist	-	-	-	-
select	0x52	int n	fd_set *inp	fd_set *outp	fd_set *exp	struct timeval *tvp	-
symlink	0x53	const char *old	const char *new	-	-	-	-
oldlstat	0x54	?	?	?	?	?	?
readlink	0x55	const char *path	char *buf	int bufsiz	-	-	-
uselib	0x56	const char *library	-	-	-	-	-
swapon	0x57	const char *specialfile	int swap_flags	-	-	-	-
reboot	0x58	int magic1	int magic2	unsigned int cmd	void *arg	-	-
readdir	0x59	?	?	?	?	?	?
mmap	0x5a	?	?	?	?	?	?
munmap	0x5b	unsigned long addr	size_t len	-	-	-	-
truncate	0x5c	const char *path	long length	-	-	-	-
ftruncate	0x5d	unsigned int fd	unsigned long length	-	-	-	-
fchmod	0x5e	unsigned int fd	umode_t mode	-	-	-	-
fchown	0x5f	unsigned int fd	uid_t user	gid_t group	-	-	-
getpriority	0x60	int which	int who	-	-	-	-
setpriority	0x61	int which	int who	int niceval	-	-	-

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
profil	0x62	?	?	?	?	?	?
statfs	0x63	const char * path	struct statfs *buf	-	-	-	-
fstatfs	0x64	unsigned int fd	struct statfs *buf	-	-	-	-
ioperm	0x65	unsigned long from	unsigned long num	int on	-	-	-
socketcall	0x66	int call	unsigned long *args	-	-	-	-
syslog	0x67	int type	char *buf	int len	-	-	-
setitimer	0x68	int which	struct itimerval *value	struct itimerval *ovalue	-	-	-
getitimer	0x69	int which	struct itimerval *value	-	-	-	-
stat	0x6a	const char *filename	struct __old_kernel_stat *statbuf	-	-	-	-
lstat	0x6b	const char *filename	struct __old_kernel_stat *statbuf	-	-	-	-
fstat	0x6c	unsigned int fd	struct __old_kernel_stat *statbuf	-	-	-	-
olduname	0x6d	struct oldold_utsname *	-	-	-	-	-
iopl	0x6e	?	?	?	?	?	?
vhangup	0x6f	-	-	-	-	-	-
idle	0x70	?	?	?	?	?	?
vm86old	0x71	?	?	?	?	?	?
wait4	0x72	pid_t pid	int *stat_addr	int options	struct rusage *ru	-	-
swapoff	0x73	const char *specialfile	-	-	-	-	-
sysinfo	0x74	struct sysinfo *info	-	-	-	-	-
ipc	0x75	unsigned int call	int first	unsigned long second	unsigned long third	void *ptr	long fifth
fsync	0x76	unsigned int fd	-	-	-	-	-
sigreturn	0x77	?	?	?	?	?	?
clone	0x78	unsigned long	unsigned long	int *	int *	unsigned long	-
setdomainname	0x79	char *name	int len	-	-	-	-
uname	0x7a	struct old_utsname *	-	-	-	-	-
modify_ldt	0x7b	?	?	?	?	?	?
adjtimex	0x7c	struct __kernel_timex *txc_p	-	-	-	-	-
mprotect	0x7d	unsigned long start	size_t len	unsigned long prot	-	-	-
sigprocmask	0x7e	int how	old_sigset_t *set	old_sigset_t *oset	-	-	-
create_module	0x7f	?	?	?	?	?	?
init_module	0x80	void *umod	unsigned long len	const char *uargs	-	-	-
delete_module	0x81	const char *name_user	unsigned int flags	-	-	-	-
get_kernel_syms	0x82	?	?	?	?	?	?
quotactl	0x83	unsigned int cmd	const char *special	qid_t id	void *addr	-	-
getpgid	0x84	pid_t pid	-	-	-	-	-
fchdir	0x85	unsigned int fd	-	-	-	-	-
bdflush	0x86	int func	long data	-	-	-	-
sysfs	0x87	int option	unsigned long arg1	unsigned long arg2	-	-	-
personality	0x88	unsigned int personality	-	-	-	-	-
afs_syscall	0x89	?	?	?	?	?	?
setfsuid	0x8a	uid_t uid	-	-	-	-	-
setfsgid	0x8b	gid_t gid	-	-	-	-	-
_llseek	0x8c	?	?	?	?	?	?
getdents	0x8d	unsigned int fd	struct linux_dirent *dirent	unsigned int count	-	-	-

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
_newselect	0x8e	?	?	?	?	?	?
flock	0x8f	unsigned int fd	unsigned int cmd	-	-	-	-
msync	0x90	unsigned long start	size_t len	int flags	-	-	-
readv	0x91	unsigned long fd	const struct iovec *vec	unsigned long vlen	-	-	-
writev	0x92	unsigned long fd	const struct iovec *vec	unsigned long vlen	-	-	-
getsid	0x93	pid_t pid	-	-	-	-	-
fdatasync	0x94	unsigned int fd	-	-	-	-	-
_sysctl	0x95	?	?	?	?	?	?
mlock	0x96	unsigned long start	size_t len	-	-	-	-
munlock	0x97	unsigned long start	size_t len	-	-	-	-
mlockall	0x98	int flags	-	-	-	-	-
munlockall	0x99	-	-	-	-	-	-
sched_setparam	0x9a	pid_t pid	struct sched_param *param	-	-	-	-
sched_getparam	0x9b	pid_t pid	struct sched_param *param	-	-	-	-
sched_setscheduler	0x9c	pid_t pid	int policy	struct sched_param *param	-	-	-
sched_getscheduler	0x9d	pid_t pid	-	-	-	-	-
sched_yield	0x9e	-	-	-	-	-	-
sched_get_priority_max	0x9f	int policy	-	-	-	-	-
sched_get_priority_min	0xa0	int policy	-	-	-	-	-
sched_rr_get_interval	0xa1	pid_t pid	struct __kernel_timespec *interval	-	-	-	-
nanosleep	0xa2	struct __kernel_timespec *rqtp	struct __kernel_timespec *rmtp	-	-	-	-
mremap	0xa3	unsigned long addr	unsigned long old_len	unsigned long new_len	unsigned long flags	unsigned long new_addr	-
setresuid	0xa4	uid_t ruid	uid_t euid	uid_t suid	-	-	-
getresuid	0xa5	uid_t *ruid	uid_t *euid	uid_t *suid	-	-	-
vm86	0xa6	?	?	?	?	?	?
query_module	0xa7	?	?	?	?	?	?
poll	0xa8	struct pollfd *ufds	unsigned int nfds	int timeout	-	-	-
nfsservctl	0xa9	?	?	?	?	?	?
setresgid	0xaa	gid_t rgid	gid_t egid	gid_t sgid	-	-	-
getresgid	0xab	gid_t *rgid	gid_t *egid	gid_t *sgid	-	-	-
prctl	0xac	int option	unsigned long arg2	unsigned long arg3	unsigned long arg4	unsigned long arg5	-
rt_sigreturn	0xad	?	?	?	?	?	?
rt_sigaction	0xae	int	const struct sigaction *	struct sigaction *	size_t	-	-
rt_sigprocmask	0xaf	int how	sigset_t *set	sigset_t *oset	size_t sigsetsize	-	-
rt_sigpending	0xb0	sigset_t *set	size_t sigsetsize	-	-	-	-
rt_sigtimedwait	0xb1	const sigset_t *uthese	siginfo_t *uinfo	const struct __kernel_timespec *uts	size_t sigsetsize	-	-
rt_sigqueueinfo	0xb2	pid_t pid	int sig	siginfo_t *uinfo	-	-	-
rt_sigsuspend	0xb3	sigset_t *unewset	size_t sigsetsize	-	-	-	-
pread64	0xb4	unsigned int fd	char *buf	size_t count	loff_t pos	-	-
pwrite64	0xb5	unsigned int fd	const char *buf	size_t count	loff_t pos	-	-
chown	0xb6	const char *filename	uid_t user	gid_t group	-	-	-
getcwd	0xb7	char *buf	unsigned long size	-	-	-	-
capget	0xb8	cap_user_header_t header	cap_user_data_t dataptr	-	-	-	-
capset	0xb9	cap_user_header_t header	const cap_user_data_t data	-	-	-	-

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
sigaltstack	0xba	const struct sigaltstack *uss	struct sigaltstack *uoss	-	-	-	-
sendfile	0xbb	int out_fd	int in_fd	off_t *offset	size_t count	-	-
getpmsg	0xbc	?	?	?	?	?	?
putpmsg	0xbd	?	?	?	?	?	?
vfork	0xbe	-	-	-	-	-	-
ugetrlimit	0xbf	?	?	?	?	?	?
mmap2	0xc0	?	?	?	?	?	?
truncate64	0xc1	const char *path	loff_t length	-	-	-	-
ftruncate64	0xc2	unsigned int fd	loff_t length	-	-	-	-
stat64	0xc3	const char *filename	struct stat64 *statbuf	-	-	-	-
lstat64	0xc4	const char *filename	struct stat64 *statbuf	-	-	-	-
fstat64	0xc5	unsigned long fd	struct stat64 *statbuf	-	-	-	-
lchown32	0xc6	?	?	?	?	?	?
getuid32	0xc7	?	?	?	?	?	?
getgid32	0xc8	?	?	?	?	?	?
geteuid32	0xc9	?	?	?	?	?	?
getegid32	0xca	?	?	?	?	?	?
setreuid32	0xcb	?	?	?	?	?	?
setregid32	0xcc	?	?	?	?	?	?
getgroups32	0xcd	?	?	?	?	?	?
setgroups32	0xce	?	?	?	?	?	?
fchown32	0xcf	?	?	?	?	?	?
setresuid32	0xd0	?	?	?	?	?	?
getresuid32	0xd1	?	?	?	?	?	?
setresgid32	0xd2	?	?	?	?	?	?
getresgid32	0xd3	?	?	?	?	?	?
chown32	0xd4	?	?	?	?	?	?
setuid32	0xd5	?	?	?	?	?	?
setgid32	0xd6	?	?	?	?	?	?
setfsuid32	0xd7	?	?	?	?	?	?
setfsgid32	0xd8	?	?	?	?	?	?
pivot_root	0xd9	const char *new_root	const char *put_old	-	-	-	-
mincore	0xda	unsigned long start	size_t len	unsigned char * vec	-	-	-
madvise	0xdb	unsigned long start	size_t len	int behavior	-	-	-
getdents64	0xdc	unsigned int fd	struct linux_dirent64 *dirent	unsigned int count	-	-	-
fcntl64	0xdd	unsigned int fd	unsigned int cmd	unsigned long arg	-	-	-
not implemented	0xde						
not implemented	0xdf						
gettid	0xe0	-	-	-	-	-	-
readahead	0xe1	int fd	loff_t offset	size_t count	-	-	-
setxattr	0xe2	const char *path	const char *name	const void *value	size_t size	int flags	-
lsetxattr	0xe3	const char *path	const char *name	const void *value	size_t size	int flags	-
fsetxattr	0xe4	int fd	const char *name	const void *value	size_t size	int flags	-
getxattr	0xe5	const char *path	const char *name	void *value	size_t size	-	-
lgetxattr	0xe6	const char *path	const char *name	void *value	size_t size	-	-
fgetxattr	0xe7	int fd	const char *name	void *value	size_t size	-	-
listxattr	0xe8	const char *path	char *list	size_t size	-	-	-
llistxattr	0xe9	const char *path	char *list	size_t size	-	-	-
flistxattr	0xea	int fd	char *list	size_t size	-	-	-
removexattr	0xeb	const char *path	const char *name	-	-	-	-
lremovexattr	0xec	const char *path	const char *name	-	-	-	-

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
fremovexattr	0xed	int fd	const char *name	-	-	-	-
tkill	0xee	pid_t pid	int sig	-	-	-	-
sendfile64	0xef	int out_fd	int in_fd	loff_t *offset	size_t count	-	-
futex	0xf0	u32 *uaddr	int op	u32 val	struct __kernel_timespec *utime	u32 *uaddr2	u32 val3
sched_setaffinity	0xf1	pid_t pid	unsigned int len	unsigned long *user_mask_ptr	-	-	-
sched_getaffinity	0xf2	pid_t pid	unsigned int len	unsigned long *user_mask_ptr	-	-	-
set_thread_area	0xf3	?	?	?	?	?	?
get_thread_area	0xf4	?	?	?	?	?	?
io_setup	0xf5	unsigned nr_reqs	aio_context_t *ctx	-	-	-	-
io_destroy	0xf6	aio_context_t ctx	-	-	-	-	-
io_getevents	0xf7	aio_context_t ctx_id	long min_nr	long nr	struct io_event *events	struct __kernel_timespec *timeout	-
io_submit	0xf8	aio_context_t	long	struct iocb * *	-	-	-
io_cancel	0xf9	aio_context_t ctx_id	struct iocb *iocb	struct io_event *result	-	-	-
fadvise64	0xfa	int fd	loff_t offset	size_t len	int advice	-	-
not implemented	0xfb						
exit_group	0xfc	int error_code	-	-	-	-	-
lookup_dcookie	0xfd	u64 cookie64	char *buf	size_t len	-	-	-
epoll_create	0xfe	int size	-	-	-	-	-
epoll_ctl	0xff	int epfd	int op	int fd	struct epoll_event *event	-	-
epoll_wait	0x100	int epfd	struct epoll_event *events	int maxevents	int timeout	-	-
remap_file_pages	0x101	unsigned long start	unsigned long size	unsigned long prot	unsigned long pgoff	unsigned long flags	-
set_tid_address	0x102	int *tidptr	-	-	-	-	-
timer_create	0x103	clockid_t which_clock	struct sigevent *timer_event_spec	timer_t * created_timer_id	-	-	-
timer_settime	0x104	timer_t timer_id	int flags	const struct __kernel_itimerspec *new_setting	struct __kernel_itimerspec *old_setting	-	-
timer_gettime	0x105	timer_t timer_id	struct __kernel_itimerspec *setting	-	-	-	-
timer_getoverrun	0x106	timer_t timer_id	-	-	-	-	-
timer_delete	0x107	timer_t timer_id	-	-	-	-	-
clock_settime	0x108	clockid_t which_clock	const struct __kernel_timespec *tp	-	-	-	-
clock_gettime	0x109	clockid_t which_clock	struct __kernel_timespec *tp	-	-	-	-
clock_getres	0x10a	clockid_t which_clock	struct __kernel_timespec *tp	-	-	-	-
clock_nanosleep	0x10b	clockid_t which_clock	int flags	const struct __kernel_timespec *rqtp	struct __kernel_timespec *rmtp	-	-
statfs64	0x10c	const char *path	size_t sz	struct statfs64 *buf	-	-	-
fstatfs64	0x10d	unsigned int fd	size_t sz	struct statfs64 *buf	-	-	-
tgkill	0x10e	pid_t tgid	pid_t pid	int sig	-	-	-
utimes	0x10f	char *filename	struct timeval *utimes	-	-	-	-
fadvise64_64	0x110	int fd	loff_t offset	loff_t len	int advice	-	-
vserver	0x111	?	?	?	?	?	?
mbind	0x112	unsigned long start	unsigned long len	unsigned long mode	const unsigned long *nmask	unsigned long maxnode	unsigned flags
get_mempolicy	0x113	int *policy	unsigned long *nmask	unsigned long maxnode	unsigned long addr	unsigned long flags	-
set_mempolicy	0x114	int mode	const unsigned long *nmask	unsigned long maxnode	-	-	-

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
mq_open	0x115	const char *name	int oflag	umode_t mode	struct mq_attr *attr	-	-
mq_unlink	0x116	const char *name	-	-	-	-	-
mq_timedsend	0x117	mqd_t mqdes	const char *msg_ptr	size_t msg_len	unsigned int msg_prio	const struct __kernel_timespec *abs_timeout	-
mq_timedreceive	0x118	mqd_t mqdes	char *msg_ptr	size_t msg_len	unsigned int *msg_prio	const struct __kernel_timespec *abs_timeout	-
mq_notify	0x119	mqd_t mqdes	const struct sigevent *notification	-	-	-	-
mq_getsetattr	0x11a	mqd_t mqdes	const struct mq_attr *mqstat	struct mq_attr *omqstat	-	-	-
kexec_load	0x11b	unsigned long entry	unsigned long nr_segments	struct kexec_segment *segments	unsigned long flags	-	-
waitid	0x11c	int which	pid_t pid	struct siginfo *infop	int options	struct rusage *ru	-
not implemented	0x11d						
add_key	0x11e	const char *_type	const char *_description	const void *_payload	size_t plen	key_serial_t destringid	-
request_key	0x11f	const char *_type	const char *_description	const char *_callout_info	key_serial_t destringid	-	-
keyctl	0x120	int cmd	unsigned long arg2	unsigned long arg3	unsigned long arg4	unsigned long arg5	-
ioprio_set	0x121	int which	int who	int ioprio	-	-	-
ioprio_get	0x122	int which	int who	-	-	-	-
inotify_init	0x123	-	-	-	-	-	-
inotify_add_watch	0x124	int fd	const char *path	u32 mask	-	-	-
inotify_rm_watch	0x125	int fd	__s32 wd	-	-	-	-
migrate_pages	0x126	pid_t pid	unsigned long maxnode	const unsigned long *from	const unsigned long *to	-	-
openat	0x127	int dfd	const char *filename	int flags	umode_t mode	-	-
mkdirat	0x128	int dfd	const char * pathname	umode_t mode	-	-	-
mknodat	0x129	int dfd	const char * filename	umode_t mode	unsigned dev	-	-
fchownat	0x12a	int dfd	const char *filename	uid_t user	gid_t group	int flag	-
futimesat	0x12b	int dfd	const char *filename	struct timeval *utimes	-	-	-
fstatat64	0x12c	int dfd	const char *filename	struct stat64 *statbuf	int flag	-	-
unlinkat	0x12d	int dfd	const char * pathname	int flag	-	-	-
renameat	0x12e	int olddfd	const char * oldname	int newdfd	const char * newname	-	-
linkat	0x12f	int olddfd	const char *oldname	int newdfd	const char *newname	int flags	-
symlinkat	0x130	const char * oldname	int newdfd	const char * newname	-	-	-
readlinkat	0x131	int dfd	const char *path	char *buf	int bufsiz	-	-
fchmodat	0x132	int dfd	const char * filename	umode_t mode	-	-	-
faccessat	0x133	int dfd	const char *filename	int mode	-	-	-
pselect6	0x134	int	fd_set *	fd_set *	fd_set *	struct __kernel_timespec *	void *
ppoll	0x135	struct pollfd *	unsigned int	struct __kernel_timespec *	const sigset_t *	size_t	-
unshare	0x136	unsigned long unshare_flags	-	-	-	-	-
set_robust_list	0x137	struct robust_list_head *head	size_t len	-	-	-	-
get_robust_list	0x138	int pid	struct robust_list_head * *head_ptr	size_t *len_ptr	-	-	-
splice	0x139	int fd_in	loff_t *off_in	int fd_out	loff_t *off_out	size_t len	unsigned int flags

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
sync_file_range	0x13a	int fd	loff_t offset	loff_t nbytes	unsigned int flags	-	-
tee	0x13b	int fdin	int fdout	size_t len	unsigned int flags	-	-
vmsplice	0x13c	int fd	const struct iovec *iov	unsigned long nr_segs	unsigned int flags	-	-
move_pages	0x13d	pid_t pid	unsigned long nr_pages	const void * *pages	const int *nodes	int *status	int flags
getcpu	0x13e	unsigned *cpu	unsigned *node	struct getcpu_cache *cache	-	-	-
epoll_pwait	0x13f	int epfd	struct epoll_event *events	int maxevents	int timeout	const sigset_t *sigmask	size_t sigsetsize
utimensat	0x140	int dfd	const char *filename	struct __kernel_timespec *utimes	int flags	-	-
signalfd	0x141	int ufd	sigset_t *user_mask	size_t sizemask	-	-	-
timerfd_create	0x142	int clockid	int flags	-	-	-	-
eventfd	0x143	unsigned int count	-	-	-	-	-
fallocate	0x144	int fd	int mode	loff_t offset	loff_t len	-	-
timerfd_settime	0x145	int ufd	int flags	const struct __kernel_itimerspec *utmr	struct __kernel_itimerspec *otmr	-	-
timerfd_gettime	0x146	int ufd	struct __kernel_itimerspec *otmr	-	-	-	-
signalfd4	0x147	int ufd	sigset_t *user_mask	size_t sizemask	int flags	-	-
eventfd2	0x148	unsigned int count	int flags	-	-	-	-
epoll_create1	0x149	int flags	-	-	-	-	-
dup3	0x14a	unsigned int oldfd	unsigned int newfd	int flags	-	-	-
pipe2	0x14b	int *fildes	int flags	-	-	-	-
inotify_init1	0x14c	int flags	-	-	-	-	-
preadv	0x14d	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	-
pwritev	0x14e	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	-
rt_tgsigqueueinfo	0x14f	pid_t tgid	pid_t pid	int sig	siginfo_t *uinfo	-	-
perf_event_open	0x150	struct perf_event_attr *attr_uptr	pid_t pid	int cpu	int group_fd	unsigned long flags	-
recvmmsg	0x151	int fd	struct mmsghdr *msg	unsigned int vlen	unsigned flags	struct __kernel_timespec *timeout	-
fanotify_init	0x152	unsigned int flags	unsigned int event_f_flags	-	-	-	-
fanotify_mark	0x153	int fanotify_fd	unsigned int flags	u64 mask	int fd	const char *pathname	-
prlimit64	0x154	pid_t pid	unsigned int resource	const struct rlimit64 *new_rlim	struct rlimit64 *old_rlim	-	-
name_to_handle_at	0x155	int dfd	const char *name	struct file_handle *handle	int *mnt_id	int flag	-
open_by_handle_at	0x156	int mountdirfd	struct file_handle *handle	int flags	-	-	-
clock_adjtime	0x157	clockid_t which_clock	struct __kernel_timex *tx	-	-	-	-
syncfs	0x158	int fd	-	-	-	-	-
sendmmsg	0x159	int fd	struct mmsghdr *msg	unsigned int vlen	unsigned flags	-	-
setns	0x15a	int fd	int nstype	-	-	-	-
process_vm_readv	0x15b	pid_t pid	const struct iovec *lvec	unsigned long liovcnt	const struct iovec *rvec	unsigned long riovcnt	unsigned long flags
process_vm_writev	0x15c	pid_t pid	const struct iovec *lvec	unsigned long liovcnt	const struct iovec *rvec	unsigned long riovcnt	unsigned long flags
kcmp	0x15d	pid_t pid1	pid_t pid2	int type	unsigned long idx1	unsigned long idx2	-
finit_module	0x15e	int fd	const char *uargs	int flags	-	-	-
sched_setattr	0x15f	pid_t pid	struct sched_attr *attr	unsigned int flags	-	-	-
sched_getattr	0x160	pid_t pid	struct sched_attr *attr	unsigned int size	unsigned int flags	-	-

syscall name	eax	arg0 (ebx)	arg1 (ecx)	arg2 (edx)	arg3 (esi)	arg4 (edi)	arg5 (ebp)
renameat2	0x161	int olddfd	const char *oldname	int newdfd	const char *newname	unsigned int flags	-
seccomp	0x162	unsigned int op	unsigned int flags	void *uargs	-	-	-
getrandom	0x163	char *buf	size_t count	unsigned int flags	-	-	-
memfd_create	0x164	const char *uname_ptr	unsigned int flags	-	-	-	-
bpf	0x165	int cmd	union bpf_attr *attr	unsigned int size	-	-	-
execveat	0x166	int dfd	const char *filename	const char *const *argv	const char *const *envp	int flags	-
socket	0x167	int	int	int	-	-	-
socketpair	0x168	int	int	int	int *	-	-
bind	0x169	int	struct sockaddr *	int	-	-	-
connect	0x16a	int	struct sockaddr *	int	-	-	-
listen	0x16b	int	int	-	-	-	-
accept4	0x16c	int	struct sockaddr *	int *	int	-	-
getsockopt	0x16d	int fd	int level	int optname	char *optval	int *optlen	-
setsockopt	0x16e	int fd	int level	int optname	char *optval	int optlen	-
getsockname	0x16f	int	struct sockaddr *	int *	-	-	-
getpeername	0x170	int	struct sockaddr *	int *	-	-	-
sendto	0x171	int	void *	size_t	unsigned	struct sockaddr *	int
sendmsg	0x172	int fd	struct user_msghdr *msg	unsigned flags	-	-	-
recvfrom	0x173	int	void *	size_t	unsigned	struct sockaddr *	int *
recvmsg	0x174	int fd	struct user_msghdr *msg	unsigned flags	-	-	-
shutdown	0x175	int	int	-	-	-	-
userfaultfd	0x176	int flags	-	-	-	-	-
membarrier	0x177	int cmd	int flags	-	-	-	-
mlock2	0x178	unsigned long start	size_t len	int flags	-	-	-
copy_file_range	0x179	int fd_in	loff_t *off_in	int fd_out	loff_t *off_out	size_t len	unsigned int flags
preadv2	0x17a	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	rwf_t flags
pwritev2	0x17b	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	rwf_t flags
pkey_mprotect	0x17c	unsigned long start	size_t len	unsigned long prot	int pkey	-	-
pkey_alloc	0x17d	unsigned long flags	unsigned long init_val	-	-	-	-
pkey_free	0x17e	int pkey	-	-	-	-	-
statx	0x17f	int dfd	const char *path	unsigned flags	unsigned mask	struct statx *buffer	-
arch_prctl	0x180	?	?	?	?	?	?

64位Linux系统调用

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
read	0x00	unsigned int fd	char *buf	size_t count	-	-	-
write	0x01	unsigned int fd	const char *buf	size_t count	-	-	-
open	0x02	const char *filename	int flags	umode_t mode	-	-	-
close	0x03	unsigned int fd	-	-	-	-	-
stat	0x04	const char *filename	struct __old_kernel_stat *statbuf	-	-	-	-
fstat	0x05	unsigned int fd	struct __old_kernel_stat *statbuf	-	-	-	-
lstat	0x06	const char *filename	struct __old_kernel_stat *statbuf	-	-	-	-
poll	0x07	struct pollfd *ufds	unsigned int nfds	int timeout	-	-	-
lseek	0x08	unsigned int fd	off_t offset	unsigned int whence	-	-	-
mmap	0x09	?	?	?	?	?	?
mprotect	0x0a	unsigned long start	size_t len	unsigned long prot	-	-	-
munmap	0x0b	unsigned long addr	size_t len	-	-	-	-
brk	0x0c	unsigned long brk	-	-	-	-	-
rt_sigaction	0x0d	int	const struct sigaction *	struct sigaction *	size_t	-	-
rt_sigprocmask	0x0e	int how	sigset_t *set	sigset_t *oset	size_t sigsetsize	-	-
rt_sigreturn	0x0f	?	?	?	?	?	?
ioctl	0x10	unsigned int fd	unsigned int cmd	unsigned long arg	-	-	-
pread64	0x11	unsigned int fd	char *buf	size_t count	loff_t pos	-	-
pwrite64	0x12	unsigned int fd	const char *buf	size_t count	loff_t pos	-	-
readv	0x13	unsigned long fd	const struct iovec *vec	unsigned long vlen	-	-	-
writev	0x14	unsigned long fd	const struct iovec *vec	unsigned long vlen	-	-	-
access	0x15	const char *filename	int mode	-	-	-	-
pipe	0x16	int *fildes	-	-	-	-	-
select	0x17	int n	fd_set *inp	fd_set *outp	fd_set *exp	struct timeval *tvp	-
sched_yield	0x18	-	-	-	-	-	-
mremap	0x19	unsigned long addr	unsigned long old_len	unsigned long new_len	unsigned long flags	unsigned long new_addr	-
msync	0x1a	unsigned long start	size_t len	int flags	-	-	-
mincore	0x1b	unsigned long start	size_t len	unsigned char * vec	-	-	-
madvise	0x1c	unsigned long start	size_t len	int behavior	-	-	-
shmget	0x1d	key_t key	size_t size	int flag	-	-	-
shmat	0x1e	int shmid	char *shmaddr	int shmflg	-	-	-
shmctl	0x1f	int shmid	int cmd	struct shmid_ds *buf	-	-	-
dup	0x20	unsigned int fildes	-	-	-	-	-
dup2	0x21	unsigned int oldfd	unsigned int newfd	-	-	-	-
pause	0x22	-	-	-	-	-	-
nanosleep	0x23	struct __kernel_timespec *rqtp	struct __kernel_timespec *rmtp	-	-	-	-
getitimer	0x24	int which	struct itimerval *value	-	-	-	-
alarm	0x25	unsigned int seconds	-	-	-	-	-
setitimer	0x26	int which	struct itimerval *value	struct itimerval *ovalue	-	-	-
getpid	0x27	-	-	-	-	-	-
sendfile	0x28	int out_fd	int in_fd	off_t *offset	size_t count	-	-
socket	0x29	int	int	int	-	-	-
connect	0x2a	int	struct sockaddr *	int	-	-	-

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
accept	0x2b	int	struct sockaddr *	int *	-	-	-
sendto	0x2c	int	void *	size_t	unsigned	struct sockaddr *	int
recvfrom	0x2d	int	void *	size_t	unsigned	struct sockaddr *	int *
sendmsg	0x2e	int fd	struct user_msghdr *msg	unsigned flags	-	-	-
recvmsg	0x2f	int fd	struct user_msghdr *msg	unsigned flags	-	-	-
shutdown	0x30	int	int	-	-	-	-
bind	0x31	int	struct sockaddr *	int	-	-	-
listen	0x32	int	int	-	-	-	-
getsockname	0x33	int	struct sockaddr *	int *	-	-	-
getpeername	0x34	int	struct sockaddr *	int *	-	-	-
socketpair	0x35	int	int	int	int *	-	-
setsockopt	0x36	int fd	int level	int optname	char *optval	int optlen	-
getsockopt	0x37	int fd	int level	int optname	char *optval	int *optlen	-
clone	0x38	unsigned long	unsigned long	int *	int *	unsigned long	-
fork	0x39	-	-	-	-	-	-
vfork	0x3a	-	-	-	-	-	-
execve	0x3b	const char *filename	const char *const *argv	const char *const *envp	-	-	-
exit	0x3c	int error_code	-	-	-	-	-
wait4	0x3d	pid_t pid	int *stat_addr	int options	struct rusage *ru	-	-
kill	0x3e	pid_t pid	int sig	-	-	-	-
uname	0x3f	struct old_utsname *	-	-	-	-	-
semget	0x40	key_t key	int nsems	int semflg	-	-	-
semop	0x41	int semid	struct sembuf *sops	unsigned nsops	-	-	-
semctl	0x42	int semid	int semnum	int cmd	unsigned long arg	-	-
shmdt	0x43	char *shmaddr	-	-	-	-	-
msgget	0x44	key_t key	int msgflg	-	-	-	-
msgsnd	0x45	int msqid	struct msgbuf *msgp	size_t msgsz	int msgflg	-	-
msgrcv	0x46	int msqid	struct msgbuf *msgp	size_t msgsz	long msgtyp	int msgflg	-
msgctl	0x47	int msqid	int cmd	struct msqid_ds *buf	-	-	-
fcntl	0x48	unsigned int fd	unsigned int cmd	unsigned long arg	-	-	-
flock	0x49	unsigned int fd	unsigned int cmd	-	-	-	-
fsync	0x4a	unsigned int fd	-	-	-	-	-
fdatasync	0x4b	unsigned int fd	-	-	-	-	-
truncate	0x4c	const char *path	long length	-	-	-	-
ftruncate	0x4d	unsigned int fd	unsigned long length	-	-	-	-
getdents	0x4e	unsigned int fd	struct linux_dirent *dirent	unsigned int count	-	-	-
getcwd	0x4f	char *buf	unsigned long size	-	-	-	-
chdir	0x50	const char *filename	-	-	-	-	-
fchdir	0x51	unsigned int fd	-	-	-	-	-
rename	0x52	const char *oldname	const char *newname	-	-	-	-
mkdir	0x53	const char *pathname	umode_t mode	-	-	-	-
rmdir	0x54	const char *pathname	-	-	-	-	-
creat	0x55	const char *pathname	umode_t mode	-	-	-	-
link	0x56	const char *oldname	const char *newname	-	-	-	-
unlink	0x57	const char *pathname	-	-	-	-	-
symlink	0x58	const char *old	const char *new	-	-	-	-
readlink	0x59	const char *path	char *buf	int bufsiz	-	-	-

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
chmod	0x5a	const char *filename	umode_t mode	-	-	-	-
fchmod	0x5b	unsigned int fd	umode_t mode	-	-	-	-
chown	0x5c	const char *filename	uid_t user	gid_t group	-	-	-
fchown	0x5d	unsigned int fd	uid_t user	gid_t group	-	-	-
lchown	0x5e	const char *filename	uid_t user	gid_t group	-	-	-
umask	0x5f	int mask	-	-	-	-	-
gettimeofday	0x60	struct timeval *tv	struct timezone *tz	-	-	-	-
getrlimit	0x61	unsigned int resource	struct rlimit *rlim	-	-	-	-
getrusage	0x62	int who	struct rusage *ru	-	-	-	-
sysinfo	0x63	struct sysinfo *info	-	-	-	-	-
times	0x64	struct tms *tbuf	-	-	-	-	-
ptrace	0x65	long request	long pid	unsigned long addr	unsigned long data	-	-
getuid	0x66	-	-	-	-	-	-
syslog	0x67	int type	char *buf	int len	-	-	-
getgid	0x68	-	-	-	-	-	-
setuid	0x69	uid_t uid	-	-	-	-	-
setgid	0x6a	gid_t gid	-	-	-	-	-
geteuid	0x6b	-	-	-	-	-	-
getegid	0x6c	-	-	-	-	-	-
setpgid	0x6d	pid_t pid	pid_t pgid	-	-	-	-
getppid	0x6e	-	-	-	-	-	-
getpgrp	0x6f	-	-	-	-	-	-
setsid	0x70	-	-	-	-	-	-
setreuid	0x71	uid_t ruid	uid_t euid	-	-	-	-
setregid	0x72	gid_t rgid	gid_t egid	-	-	-	-
getgroups	0x73	int gidsetsize	gid_t *grouplist	-	-	-	-
setgroups	0x74	int gidsetsize	gid_t *grouplist	-	-	-	-
setresuid	0x75	uid_t ruid	uid_t euid	uid_t suid	-	-	-
getresuid	0x76	uid_t *ruid	uid_t *euid	uid_t *suid	-	-	-
setresgid	0x77	gid_t rgid	gid_t egid	gid_t sgid	-	-	-
getresgid	0x78	gid_t *rgid	gid_t *egid	gid_t *sgid	-	-	-
getpgid	0x79	pid_t pid	-	-	-	-	-
setfsuid	0x7a	uid_t uid	-	-	-	-	-
setfsgid	0x7b	gid_t gid	-	-	-	-	-
getsid	0x7c	pid_t pid	-	-	-	-	-
capget	0x7d	cap_user_header_t header	cap_user_data_t dataptr	-	-	-	-
capset	0x7e	cap_user_header_t header	const cap_user_data_t data	-	-	-	-
rt_sigpending	0x7f	sigset_t *set	size_t sigsetsize	-	-	-	-
rt_sigtimedwait	0x80	const sigset_t *uthese	siginfo_t *uinfo	const struct __kernel_timespec *uts	size_t sigsetsize	-	-
rt_sigqueueinfo	0x81	pid_t pid	int sig	siginfo_t *uinfo	-	-	-
rt_sigsuspend	0x82	sigset_t *unewset	size_t sigsetsize	-	-	-	-
sigaltstack	0x83	const struct sigaltstack *uss	struct sigaltstack *uoss	-	-	-	-
utime	0x84	char *filename	struct utimbuf *times	-	-	-	-
mknod	0x85	const char *filename	umode_t mode	unsigned dev	-	-	-
uselib	0x86	const char *library	-	-	-	-	-
personality	0x87	unsigned int personality	-	-	-	-	-
ustat	0x88	unsigned dev	struct ustat *ubuf	-	-	-	-
statfs	0x89	const char * path	struct statfs *buf	-	-	-	-

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
fstatfs	0x8a	unsigned int fd	struct statfs *buf	-	-	-	-
sysfs	0x8b	int option	unsigned long arg1	unsigned long arg2	-	-	-
getpriority	0x8c	int which	int who	-	-	-	-
setpriority	0x8d	int which	int who	int niceval	-	-	-
sched_setparam	0x8e	pid_t pid	struct sched_param *param	-	-	-	-
sched_getparam	0x8f	pid_t pid	struct sched_param *param	-	-	-	-
sched_setscheduler	0x90	pid_t pid	int policy	struct sched_param *param	-	-	-
sched_getscheduler	0x91	pid_t pid	-	-	-	-	-
sched_get_priority_max	0x92	int policy	-	-	-	-	-
sched_get_priority_min	0x93	int policy	-	-	-	-	-
sched_rr_get_interval	0x94	pid_t pid	struct __kernel_timespec *interval	-	-	-	-
mlock	0x95	unsigned long start	size_t len	-	-	-	-
munlock	0x96	unsigned long start	size_t len	-	-	-	-
mlockall	0x97	int flags	-	-	-	-	-
munlockall	0x98	-	-	-	-	-	-
vhangup	0x99	-	-	-	-	-	-
modify_ldt	0x9a	?	?	?	?	?	?
pivot_root	0x9b	const char *new_root	const char *put_old	-	-	-	-
_sysctl	0x9c	?	?	?	?	?	?
prctl	0x9d	int option	unsigned long arg2	unsigned long arg3	unsigned long arg4	unsigned long arg5	-
arch_prctl	0x9e	?	?	?	?	?	?
adjtimex	0x9f	struct __kernel_timex *txc_p	-	-	-	-	-
setrlimit	0xa0	unsigned int resource	struct rlimit *rlim	-	-	-	-
chroot	0xa1	const char *filename	-	-	-	-	-
sync	0xa2	-	-	-	-	-	-
acct	0xa3	const char *name	-	-	-	-	-
settimeofday	0xa4	struct timeval *tv	struct timezone *tz	-	-	-	-
mount	0xa5	char *dev_name	char *dir_name	char *type	unsigned long flags	void *data	-
umount2	0xa6	?	?	?	?	?	?
swapon	0xa7	const char *specialfile	int swap_flags	-	-	-	-
swapoff	0xa8	const char *specialfile	-	-	-	-	-
reboot	0xa9	int magic1	int magic2	unsigned int cmd	void *arg	-	-
sethostname	0xaa	char *name	int len	-	-	-	-
setdomainname	0xab	char *name	int len	-	-	-	-
iopl	0xac	?	?	?	?	?	?
ioperm	0xad	unsigned long from	unsigned long num	int on	-	-	-
create_module	0xae	?	?	?	?	?	?
init_module	0xaf	void *umod	unsigned long len	const char *uargs	-	-	-
delete_module	0xb0	const char *name_user	unsigned int flags	-	-	-	-
get_kernel_syms	0xb1	?	?	?	?	?	?
query_module	0xb2	?	?	?	?	?	?
quotactl	0xb3	unsigned int cmd	const char *special	qid_t id	void *addr	-	-
nfsservctl	0xb4	?	?	?	?	?	?
getpmsg	0xb5	?	?	?	?	?	?
putpmsg	0xb6	?	?	?	?	?	?
afs_syscall	0xb7	?	?	?	?	?	?
tuxcall	0xb8	?	?	?	?	?	?

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
security	0xb9	?	?	?	?	?	?
gettid	0xba	-	-	-	-	-	-
readahead	0xbb	int fd	loff_t offset	size_t count	-	-	-
setxattr	0xbc	const char *path	const char *name	const void *value	size_t size	int flags	-
lsetxattr	0xbd	const char *path	const char *name	const void *value	size_t size	int flags	-
fsetxattr	0xbe	int fd	const char *name	const void *value	size_t size	int flags	-
getxattr	0xbf	const char *path	const char *name	void *value	size_t size	-	-
lgetxattr	0xc0	const char *path	const char *name	void *value	size_t size	-	-
fgetxattr	0xc1	int fd	const char *name	void *value	size_t size	-	-
listxattr	0xc2	const char *path	char *list	size_t size	-	-	-
llistxattr	0xc3	const char *path	char *list	size_t size	-	-	-
flistxattr	0xc4	int fd	char *list	size_t size	-	-	-
removexattr	0xc5	const char *path	const char *name	-	-	-	-
lremovexattr	0xc6	const char *path	const char *name	-	-	-	-
fremovexattr	0xc7	int fd	const char *name	-	-	-	-
tkill	0xc8	pid_t pid	int sig	-	-	-	-
time	0xc9	time_t *tloc	-	-	-	-	-
futex	0xca	u32 *uaddr	int op	u32 val	struct __kernel_timespec *utime	u32 *uaddr2	u32 val3
sched_setaffinity	0xcb	pid_t pid	unsigned int len	unsigned long *user_mask_ptr	-	-	-
sched_getaffinity	0xcc	pid_t pid	unsigned int len	unsigned long *user_mask_ptr	-	-	-
set_thread_area	0xcd	?	?	?	?	?	?
io_setup	0xce	unsigned nr_reqs	aio_context_t *ctx	-	-	-	-
io_destroy	0xcf	aio_context_t ctx	-	-	-	-	-
io_getevents	0xd0	aio_context_t ctx_id	long min_nr	long nr	struct io_event *events	struct __kernel_timespec *timeout	-
io_submit	0xd1	aio_context_t	long	struct iocb * *	-	-	-
io_cancel	0xd2	aio_context_t ctx_id	struct iocb *iocb	struct io_event *result	-	-	-
get_thread_area	0xd3	?	?	?	?	?	?
lookup_dcookie	0xd4	u64 cookie64	char *buf	size_t len	-	-	-
epoll_create	0xd5	int size	-	-	-	-	-
epoll_ctl_old	0xd6	?	?	?	?	?	?
epoll_wait_old	0xd7	?	?	?	?	?	?
remap_file_pages	0xd8	unsigned long start	unsigned long size	unsigned long prot	unsigned long pgoff	unsigned long flags	-
getdents64	0xd9	unsigned int fd	struct linux_dirent64 *dirent	unsigned int count	-	-	-
set_tid_address	0xda	int *tidptr	-	-	-	-	-
restart_syscall	0xdb	-	-	-	-	-	-
semtimedop	0xdc	int semid	struct sembuf *sops	unsigned nsops	const struct __kernel_timespec *timeout	-	-
fadvise64	0xdd	int fd	loff_t offset	size_t len	int advice	-	-
timer_create	0xde	clockid_t which_clock	struct sigevent *timer_event_spec	timer_t * created_timer_id	-	-	-
timer_settime	0xdf	timer_t timer_id	int flags	const struct __kernel_itimerspec *new_setting	struct __kernel_itimerspec *old_setting	-	-
timer_gettime	0xe0	timer_t timer_id	struct __kernel_itimerspec *setting	-	-	-	-
timer_getoverrun	0xe1	timer_t timer_id	-	-	-	-	-
timer_delete	0xe2	timer_t timer_id	-	-	-	-	-
clock_settime	0xe3	clockid_t which_clock	const struct __kernel_timespec *tp	-	-	-	-
clock_gettime	0xe4	clockid_t which_clock	struct __kernel_timespec *tp	-	-	-	-

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
clock_getres	0xe5	clockid_t which_clock	struct __kernel_timespec *tp	-	-	-	-
clock_nanosleep	0xe6	clockid_t which_clock	int flags	const struct __kernel_timespec *rqtp	struct __kernel_timespec *rmtp	-	-
exit_group	0xe7	int error_code	-	-	-	-	-
epoll_wait	0xe8	int epfd	struct epoll_event *events	int maxevents	int timeout	-	-
epoll_ctl	0xe9	int epfd	int op	int fd	struct epoll_event *event	-	-
tgkill	0xea	pid_t tgid	pid_t pid	int sig	-	-	-
utimes	0xeb	char *filename	struct timeval *utimes	-	-	-	-
vserver	0xec	?	?	?	?	?	?
mbind	0xed	unsigned long start	unsigned long len	unsigned long mode	const unsigned long *nmask	unsigned long maxnode	unsigned flags
set_mempolicy	0xee	int mode	const unsigned long *nmask	unsigned long maxnode	-	-	-
get_mempolicy	0xef	int *policy	unsigned long *nmask	unsigned long maxnode	unsigned long addr	unsigned long flags	-
mq_open	0xf0	const char *name	int oflag	umode_t mode	struct mq_attr *attr	-	-
mq_unlink	0xf1	const char *name	-	-	-	-	-
mq_timedsend	0xf2	mqd_t mqdes	const char *msg_ptr	size_t msg_len	unsigned int msg_prio	const struct __kernel_timespec *abs_timeout	-
mq_timedreceive	0xf3	mqd_t mqdes	char *msg_ptr	size_t msg_len	unsigned int *msg_prio	const struct __kernel_timespec *abs_timeout	-
mq_notify	0xf4	mqd_t mqdes	const struct sigevent *notification	-	-	-	-
mq_getsetattr	0xf5	mqd_t mqdes	const struct mq_attr *mqstat	struct mq_attr *omqstat	-	-	-
kexec_load	0xf6	unsigned long entry	unsigned long nr_segments	struct kexec_segment *segments	unsigned long flags	-	-
waitid	0xf7	int which	pid_t pid	struct siginfo *infop	int options	struct rusage *ru	-
add_key	0xf8	const char *_type	const char *_description	const void *_payload	size_t plen	key_serial_t destringid	-
request_key	0xf9	const char *_type	const char *_description	const char *_callout_info	key_serial_t destringid	-	-
keyctl	0xfa	int cmd	unsigned long arg2	unsigned long arg3	unsigned long arg4	unsigned long arg5	-
ioprio_set	0xfb	int which	int who	int ioprio	-	-	-
ioprio_get	0xfc	int which	int who	-	-	-	-
inotify_init	0xfd	-	-	-	-	-	-
inotify_add_watch	0xfe	int fd	const char *path	u32 mask	-	-	-
inotify_rm_watch	0xff	int fd	__s32 wd	-	-	-	-
migrate_pages	0x100	pid_t pid	unsigned long maxnode	const unsigned long *from	const unsigned long *to	-	-
openat	0x101	int dfd	const char *filename	int flags	umode_t mode	-	-
mkdirat	0x102	int dfd	const char * pathname	umode_t mode	-	-	-
mknodat	0x103	int dfd	const char * filename	umode_t mode	unsigned dev	-	-
fchownat	0x104	int dfd	const char *filename	uid_t user	gid_t group	int flag	-
futimesat	0x105	int dfd	const char *filename	struct timeval *utimes	-	-	-
newfstatat	0x106	int dfd	const char *filename	struct stat *statbuf	int flag	-	-
unlinkat	0x107	int dfd	const char * pathname	int flag	-	-	-
renameat	0x108	int olddfd	const char * oldname	int newdfd	const char * newname	-	-
linkat	0x109	int olddfd	const char *oldname	int newdfd	const char *newname	int flags	-
symlinkat	0x10a	const char * oldname	int newdfd	const char * newname	-	-	-

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
readlinkat	0x10b	int dfd	const char *path	char *buf	int bufsiz	-	-
fchmodat	0x10c	int dfd	const char * filename	umode_t mode	-	-	-
faccessat	0x10d	int dfd	const char *filename	int mode	-	-	-
pselect6	0x10e	int	fd_set *	fd_set *	fd_set *	struct __kernel_timespec *	void *
ppoll	0x10f	struct pollfd *	unsigned int	struct __kernel_timespec *	const sigset_t *	size_t	-
unshare	0x110	unsigned long unshare_flags	-	-	-	-	-
set_robust_list	0x111	struct robust_list_head *head	size_t len	-	-	-	-
get_robust_list	0x112	int pid	struct robust_list_head * *head_ptr	size_t *len_ptr	-	-	-
splice	0x113	int fd_in	loff_t *off_in	int fd_out	loff_t *off_out	size_t len	unsigned int flags
tee	0x114	int fdin	int fdout	size_t len	unsigned int flags	-	-
sync_file_range	0x115	int fd	loff_t offset	loff_t nbytes	unsigned int flags	-	-
vmsplice	0x116	int fd	const struct iovec *iov	unsigned long nr_segs	unsigned int flags	-	-
move_pages	0x117	pid_t pid	unsigned long nr_pages	const void * *pages	const int *nodes	int *status	int flags
utimensat	0x118	int dfd	const char *filename	struct __kernel_timespec *utimes	int flags	-	-
epoll_pwait	0x119	int epfd	struct epoll_event *events	int maxevents	int timeout	const sigset_t *sigmask	size_t sigsetsize
signalfd	0x11a	int ufd	sigset_t *user_mask	size_t sizemask	-	-	-
timerfd_create	0x11b	int clockid	int flags	-	-	-	-
eventfd	0x11c	unsigned int count	-	-	-	-	-
fallocate	0x11d	int fd	int mode	loff_t offset	loff_t len	-	-
timerfd_settime	0x11e	int ufd	int flags	const struct __kernel_itimerspec *utmr	struct __kernel_itimerspec *otmr	-	-
timerfd_gettime	0x11f	int ufd	struct __kernel_itimerspec *otmr	-	-	-	-
accept4	0x120	int	struct sockaddr *	int *	int	-	-
signalfd4	0x121	int ufd	sigset_t *user_mask	size_t sizemask	int flags	-	-
eventfd2	0x122	unsigned int count	int flags	-	-	-	-
epoll_create1	0x123	int flags	-	-	-	-	-
dup3	0x124	unsigned int oldfd	unsigned int newfd	int flags	-	-	-
pipe2	0x125	int *fildes	int flags	-	-	-	-
inotify_init1	0x126	int flags	-	-	-	-	-
preadv	0x127	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	-
pwritev	0x128	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	-
rt_tgsigqueueinfo	0x129	pid_t tgid	pid_t pid	int sig	siginfo_t *uinfo	-	-
perf_event_open	0x12a	struct perf_event_attr *attr_uptr	pid_t pid	int cpu	int group_fd	unsigned long flags	-
recvmmsg	0x12b	int fd	struct mmsghdr *msg	unsigned int vlen	unsigned flags	struct __kernel_timespec *timeout	-
fanotify_init	0x12c	unsigned int flags	unsigned int event_f_flags	-	-	-	-
fanotify_mark	0x12d	int fanotify_fd	unsigned int flags	u64 mask	int fd	const char *pathname	-
prlimit64	0x12e	pid_t pid	unsigned int resource	const struct rlimit64 *new_rlim	struct rlimit64 *old_rlim	-	-
name_to_handle_at	0x12f	int dfd	const char *name	struct file_handle *handle	int *mnt_id	int flag	-
open_by_handle_at	0x130	int mountdirfd	struct file_handle *handle	int flags	-	-	-

syscall name	rax	arg0 (rdi)	arg1 (rsi)	arg2 (rdx)	arg3 (r10)	arg4 (r8)	arg5 (r9)
clock_adjtime	0x131	clockid_t which_clock	struct __kernel_timex *tx	-	-	-	-
syncfs	0x132	int fd	-	-	-	-	-
sendmmsg	0x133	int fd	struct mmsghdr *msg	unsigned int vlen	unsigned flags	-	-
setns	0x134	int fd	int nstype	-	-	-	-
getcpu	0x135	unsigned *cpu	unsigned *node	struct getcpu_cache *cache	-	-	-
process_vm_readv	0x136	pid_t pid	const struct iovec *lvec	unsigned long liovcnt	const struct iovec *rvec	unsigned long riovcnt	unsigned long flags
process_vm_writev	0x137	pid_t pid	const struct iovec *lvec	unsigned long liovcnt	const struct iovec *rvec	unsigned long riovcnt	unsigned long flags
kcmp	0x138	pid_t pid1	pid_t pid2	int type	unsigned long idx1	unsigned long idx2	-
finit_module	0x139	int fd	const char *uargs	int flags	-	-	-
sched_setattr	0x13a	pid_t pid	struct sched_attr *attr	unsigned int flags	-	-	-
sched_getattr	0x13b	pid_t pid	struct sched_attr *attr	unsigned int size	unsigned int flags	-	-
renameat2	0x13c	int olddfd	const char *oldname	int newdfd	const char *newname	unsigned int flags	-
seccomp	0x13d	unsigned int op	unsigned int flags	void *uargs	-	-	-
getrandom	0x13e	char *buf	size_t count	unsigned int flags	-	-	-
memfd_create	0x13f	const char *uname_ptr	unsigned int flags	-	-	-	-
kexec_file_load	0x140	int kernel_fd	int initrd_fd	unsigned long cmdline_len	const char *cmdline_ptr	unsigned long flags	-
bpf	0x141	int cmd	union bpf_attr *attr	unsigned int size	-	-	-
execveat	0x142	int dfd	const char *filename	const char *const *argv	const char *const *envp	int flags	-
userfaultfd	0x143	int flags	-	-	-	-	-
membarrier	0x144	int cmd	int flags	-	-	-	-
mlock2	0x145	unsigned long start	size_t len	int flags	-	-	-
copy_file_range	0x146	int fd_in	loff_t *off_in	int fd_out	loff_t *off_out	size_t len	unsigned int flags
preadv2	0x147	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	rwf_t flags
pwritev2	0x148	unsigned long fd	const struct iovec *vec	unsigned long vlen	unsigned long pos_l	unsigned long pos_h	rwf_t flags
pkey_mprotect	0x149	unsigned long start	size_t len	unsigned long prot	int pkey	-	-
pkey_alloc	0x14a	unsigned long flags	unsigned long init_val	-	-	-	-
pkey_free	0x14b	int pkey	-	-	-	-	-
statx	0x14c	int dfd	const char *path	unsigned flags	unsigned mask	struct statx *buffer	-