1

1.

1. -
2. -
3. -
4. -

, g++?

```
g++ -v test.cpp #          ,   . .
/usr/lib/gcc/x86_64-linux-gnu/11/cc1plus #
as #
/usr/lib/gcc/x86_64-linux-gnu/11/collect2 #
```

cpp- ? ?

```
g++ -E test.cpp # (> test_preprossessed.cpp)
g++ -S test.cpp # (> test.s      )
g++ -c test.s # (> test.o        )
g++ test.o
```

( )? ( )
. , . ##### ?

```
objdump -d a.out -          ,
```

2.

? .

, .

```
readelf -s test.o #       UND
readelf -s a.out #          UND        -

objdump -d test.o #             ,
```

( )? - ELF, #####
, ld C++.

```
ld test.o \
  /usr/lib/gcc/x86_64-linux-gnu/11/crt1.o /usr/lib/gcc/x86_64-linux-gnu/11/crti.o \
  /usr/lib/gcc/x86_64-linux-gnu/11/crtbegin.o \
  -L/usr/lib/x86_64-linux-gnu -L/usr/lib/gcc/x86_64-linux-gnu/11 \
  -lstdc++ -lc -lgcc -lgcc_s \
  /usr/lib/gcc/x86_64-linux-gnu/11/crtend.o /usr/lib/gcc/x86_64-linux-gnu/11/crtn.o \
  -dynamic-linker /lib64/ld-linux-x86-64.so.2

./a.out - No such file or directory.
```

, ?

:

1. startup- (`crt1.o`, `crti.o`, `crtbegin.o`, …)
2. dynamic linker (`-dynamic-linker ...`)
3. entrypoint (`_start` `crt1.o`)

: `g++` , (`g++ -v ...`).

- , . main, main

- segfault, main return, .
  exit(0) return. ## 3. ##### , ?
  - , .. .

```
g++ -static test.cpp
```

.symtab, - ,
.dynsym ,

- , -
?

```
g++ -static test.cpp
```

, . ##### ,
?

```
ldd a.out
```

ldd ? ldd , shared libraries .
“ ” (LD_TRACE_LOADED_OBJECTS=1), dlopen/ ELF dynamic .

:

```
readelf -d a.out
objdump -p a.out
```

C++, ?

```
ldd a.out ( libstdc++.so.6, include iostream)
cd /lib/x86_64-linux-gnu/
sudo mkdir test
sudo mv libstdc++.so.6 test/
cd test/
ls -l # , ( )
cd ..
sudo mv libstdc++.so.6.0.30 test/
LD_LIBRARY_PATH=/lib/x86_64-linux-gnu/test ./a.out
```

?

1. g++ -shared lib.cpp -o libmyfunc.so (shared object)
2. header
   1:

3. sudo mv libmyfunc.so /usr/lib/
4. g++ test.cpp -lmyfunc ( )
 2:
3. g++ test.cpp -lmyfunc -L. (libmyfunc.so,
↪ (-L))
4. LD_LIBRARY_PATH=. ./a.out
 3:
3. g++ test.cpp -lmyfunc -L. -Wl,-rpath,/caos (
↪)

.so: examples/03_shared_lib/ ##### LD_LIBRARY_PATH?
Linux / Unix, , /
. , , ,
. , ##### LD_PRELOAD
LD_LIBRARY_PATH? LD_LIBRARY_PATH ( ).
LD_PRELOAD .so (“ ” libc/).

:

```
LD_PRELOAD=./libhook.so ./a.out
```

LD_PRELOAD interpose: examples/03_ld_preload/ ##### rpath ?
>rpath - , ,

```
-Wl,-rpath,/home/liza/caos  #  -
#-Wl -  ,  ,
```

, ?

```
ltrace -p 27766 #
```

4.

ELF

Elf - Executable Linkable Format (, ,). ELF, ,
. ###### 3 ELF- ? 1. REL (Relocatable file) - 2. DYN (Shared object file) - 3. EXEC (Executable file) - 4. DYN (Position-Independent Executable file) - readelf -a a.out 5. CORE (Core file) ######

```
1.
g++ -c test.cpp
readelf -h test.o # REL
2.
g++ -shared test.cpp -o lib.so
readelf -h lib.so # DYN
3.
g++ -static test.cpp
readelf -h a.out # EXEC
4.
readelf -h a.out # DYN (Position-Independent Executable file)
```

ELF- ?

1. (magic - , . ELF)

2. .text -
3. .data -
4. .rodata - read only data
5. .bss -
6. .symtab - ###### strtab, shstrtab, interp, dynamic?

- `.strtab` — `.symtab` ( ).
- `.shstrtab` — (section header string table).
- `.interp` — (`/lib64/ld-linux-x86-64.so.2`).
- `.dynamic` — dynamic tags (DT_NEEDED, DT_RPATH/DT_RUNPATH, DT_SONAME . .), “ ”.

:

```
readelf -S a.out
readelf -x .interp a.out
readelf -d a.out
```

ELF- ?

1. hexdump -
2. readelf
3. objdump (-t)
4. nm - ##### objcopy? . > **objcopy** , GNU Binutils (, ELF, COFF). , .

```
objcopy --strip-debug input.elf output.elf #
objcopy --dump-section .text=text.bin input.elf #                    .text
objcopy -O binary input.elf output.bin #
```

5.

?

- , ##### ( ) ? .

-

: _ZSt3cin - _Z - , - St - std:: - 3 - - cin - ##### ?

```
c++filt "  "
nm -C a.out #
```

ELF- ?

```
readelf -s a.out
```

strip? `strip` “ ” , `.symtab`/`.strtab` , .

```
strip a.out
strip --strip-debug a.out
```

weak strong ? Bind LOCAL, GLOBAL, WEAK. GLOBAL - , - translation unit' . (strong) LOCAL - static , WEAK - GLOBAL, WEAK, ##### , ? . . - . static, / , translation unit'a. ELF (Visibility): - `DEFAULT` — ( ) - `HIDDEN` — ( ) - `PROTECTED` — , interpose (: “ LD_PRELOAD”)

:

```
g++ -fvisibility=hidden ...
```

: `__attribute__((visibility("hidden")))`. ##### ? > — , , .

, , .

, . .

: , — `main.o` `foo.o`. `main.o` `foo()`, , .

1. `foo.o`, `foo()` , .
2. , `foo()`.
3. , , 0x1000, `foo()` .
4. , , `foo()` .

6.

. **main,** `_start` (entrypoint ELF header). `__libc_start_main`, : 1. (argc/argv/envp, TLS . .) 2. (`.init_array`, /) 3. `main` 4. `exit`, atexit- `.fini_array` ( ) .

? / `.init_array` `main`.

`__cxa_atexit` `exit` (`.fini_array`).

g++ **?** entrypoint:

```
g++ hello.cpp -Wl,-e,main
```

, **,** **?** , main return, . exit(0), , main'a, . ##### main, , _start ? , main, exit(0) main ## 7. ##### . - ? , .

```
g++ -g test.cpp #        DWARF
```

gdb **:** **breakpoint** **,** **(** **),** **?**

```
gdb -g test.cpp
gdb ./a.out
```

```
b [test.cpp:]6 #       breakpoint
b [test.cpp:]f #       breakpoint
run
n # next -
s # step -
p count # print -
```

backtrace ?

```
bt
```

“core dumped” gdb coredump- , ?

core dumped , dump , ,
core

ubuntu /var/lib/apport/coredump, (core - 0) - ulimit -c -
core - ulimit -c unlimited - : 1. core
readelf 2. cpp -g,

```
gdb ./a.out path-to-core-file
# Program received signal SIGSEGV, Segmentation fault.
# 0x0000555555555327 in main () at test.cpp:6
# 6   std::cout << v[100000000];
```

8.

( )?

- ,
, - ?

```
strace -p "proccess-id"
```

?

```
man 2 read
man 2 write
```

read write. **?** **,**
, **,** **?**

```
#include <unistd.h>
#include <cstdlib>
#include <string>

int main() {
  char buffer[100];
  auto taken = read(0, buffer, 100);
  if (taken == -1) {
    auto errno_str = std::to_string(errno);
    write(2, errno_str.data(), errno_str.size());
    exit(1);
  }
```

```
  if (write(1, buffer, taken) == -1) {
    auto errno_str = std::to_string(errno);
    write(2, errno_str.data(), errno_str.size());
    exit(1);
  }
}
```

```
errno -l -
```

: examples/08_read_write/echo.c # 2 ## 9. ##### ? > —
, - . , , .

0. 1. 2. ##### open, close lseek
. ###### open > int open(const char* pathname, int flags [, mode_t mode]) > int creat(const char* pathname, mode_t mode) - openat openat2 - int dirfd -
open

```
int main() {
  int fd = open("./input.txt", O_RDONLY);
  char buff[100];
  read(fd, buf, 10);
  write(1, buf, 10);
}
```

close

int close(int fd) ###### lseek off_t lseek(int fd, off_t offeset, int whence) -
/ ##### , lseek - ?

```
int main() {
  int fd = open("./output.txt", O_WRONLY|O_CREAT);
  int offset = lseek(fd, 50, SEEK_SET);
  const char* buf = "Hello world";
  int res = write(fd, buf, 10);
  std::cout << res;
}
```

```
cat output.txt #Hello worl
#     output.txt 60   .          10
cp output.txt output2.txt
#               ,     output2.txt - 60          60
```

cp , **read** **write.** : `open(src, O_RDONLY)`, `open(dst, O_WRONLY|O_CREAT|O_TRUNC, 0644)`, `read` → `write` 0.

: examples/09_cp/cp.c ## 10. ##### - .
? , ?

```
./a.out > result.txt #
./a.out >> result.txt #
```

(cout cerr) ?

```
./a.out 1>output.txt
./a.out 1>&2
```

- ?

```
./a.out 1> /dev/null
```

tee? tee :

```
./a.out | tee result.txt
```

dup dup2?

int dup(int oldfd) int dup2(int oldfd, int newfd) - , , - - dup2 , newfd. newfd , : , (0), dup 3. 0 , 3

tee. : stdin, stdout, . `read/write`, `iostream`.

: `examples/10_tee/tee.c` ## 11. ##### . ? , > — , , . , - . .

```
df -T -h #
```

: - Windows – **FAT**, NTFS, exFAT - macOS – HFS, APFS, HFS+ - Linux – EXT2, EXT3, EXT4, XFS, JFS ##### 6 Linux? 1. 2. 3. 4. (fifo) 5. 6. (b/c) - ##### ? - , : . ##### inode inode ? inode - . inode .

```
ls -li
```

? , .

(VFS) Linux — , , (, ,). : , . ( ) /proc, /dev/zero, /dev/null, /dev/random ##### swapfile? Linux swapfile , RAM. swapfile, . ## 12. ##### opendir, readdir? `opendir(path)` `DIR*`. `readdir(dir)` `struct dirent*` (`NULL`).
: `readdir` , `free`, `readdir`.

stat, fstat, lstat, fstatat? `stat(path, &st)` — (symlink).
`lstat(path, &st)` — symlink.
`fstat(fd, &st)` — .
`fstatat(dirfd, "name", &st, flags)` — `stat`, `dirfd` ( ).

ls ? : `opendir(".")`, `readdir`, `lstat/fstatat`, (/).

: `examples/12_ls/ls.c`

13.

mv? mv inod' . **link unlink rename** ##### rm? rm ln,

inod' . 0 , . **unlink** ## 14. ##### . ? : - / - - C++ : - “ ”, C++ - ##### , , ?

```
ln -s result.txt a.txt #
ln result.txt a.txt # hard link -
```

- , , - inode ##### ln ? **symlink** - **link** ## 15. ##### . , ?

```
ls -l out.txt #
chmod +x out.txt

1.
2. +x, +w, +r (user, group other)
3. g+x
```

r x - **?** **?** **r -** , **x -** : **r -** . , , **x -** . , ##### , ?

```
chown root out.txt #
chgrp root out.txt #
```

? chown chgrp - chown chmod - chmod ##### suid- , s S ? , . **SUID- (Set User ID)** — Linux/Unix, , , . , . 1. s , SUID- 2. S - SUID- , (. . x). . **:** - /usr/bin/sudo, root - /usr/bin/passwd. `passwd`, `root`, `/etc/shadow`, .

```
chmod +s out.txt
```

sticky bit? Sticky bit / , , root. : `/tmp`.

, , **?** ext* (immutable, append-only . .) `lsattr`, `chattr`.

16.

, **?**

```
cd /proc/"proccess_id"/fd
ls -l
```

, ?

```
cat < /dev/zero
lsof /dev/zero
```

(,)? 1.

C opendir /proc/“proccess_id”/fd. readdir.
stat ###### 2. /proc/“proccess_id”/fd
(readlink) ## 17. ##### .
? . - - . : /dev/nvme0n1 - -
. : /dev/zero - ##### - ,
? , open, close, read, write,
. . ##### Linux
? > Linux — ,
. - /dev/null - . - /dev/zero - .
, - /dev/random /dev/urandom - - -
, stdout / stderr ? tty (/dev/pts/3)
dup2(fd, 1) / dup2(fd, 2).
: ./a.out > /dev/pts/3 2> /dev/pts/3.

CPU, , / SSD? CPU: /proc/cpuinfo,
/sys/devices/system/cpu/
: /proc/meminfo
/ - : /sys/block, /proc/partitions ##### ? >
— (, , , ISO-) ,
.

Linux (UNIX-) /, .
? ?

```
df #                    . /dev/sda1
sudo umount "          " #
sudo mount "          " "          "
```

3 ## 18. ##### . ? > —
. , ,
. ###### 1. :
, .

2. :
(,) , .

3. ##### , , ? >
— , ( ),
— . 4

— , , .
.

RAM (52) . =
B- . 4 . (,)
![[page table.png]] ##### page fault, minor major page fault? page walk
, , page fault - , . ###### 1. **Minor page fault** - :

C , , , ,
. , , .

- :
  – `fork()` .
  .
  – , minor page fault, .
  , (lazy loading), . ,
  , . ###### 2. Major page fault - :
  , , . (,
) .
- :
  , (swap). ##### TLB cache? >
  TLB cache - , . #####
  ( )? Memory management unit
  :

1.
2. ,
3. MMU TLB cahce . ,
4. page walk maps: , TLB cache,
5. . , segfault
6. page walk , page fault: , . , (
   ), . segfault ![[virtual memory.png]] #####
   Segmentation fault ? page fault
   segfault, ( )
   . . ## 19. #####
   ? ![[memory layout.png]] ##### .data, .rodata .bss?

- **data** -
- **rodata** - read only
- **bss** - ##### brk sbrk?

```
cat /proc/$$/maps
 # 5f60b9861000-5f60b9a0d000 rw-p 00000000 00:00 0                  [heap]
 # 5f60b9a0d000 - program break
```

brk , program break. **sbrk** program break'a. -
, - . , ##### ,
?

```
cat /proc/$(pgrep a.out)/maps
```

20.

? , . ,
. ##### segfault ?
, (, 4) , segfault
mremap. `mremap` ( ). ,
“ ”, . ##### mmap ? ?
msync?

```
#include <sys/mman.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <unistd.h>
#include <iostream>

int main() {
  int fd = open("example.txt", O_RDONLY);
  if (fd == -1) {
    exit(1);
  }

  struct stat sb;
  if (fstat(fd, &sb) == -1) {
    exit(1);
  }

  char* data = (char*)mmap(NULL, sb.st_size, PROT_READ | PROT_WRITE, MAP_PRIVATE, fd, 0);
  if (data == MAP_FAILED) {
    exit(1);
  }

  data[0] = 'X';
  std::cout << data << std::endl;

  if (msync(data, sb.st_size, MS_SYNC) == -1) {
    exit(1);
  }

  if (munmap(data, sb.st_size) == -1) {
    exit(1);
  }
}
```

MAP_PRIVATE: , . data O_RDONLY
MAP_SHARED: .

, , . **msync** , .
: examples/20_mmap_file/mmap_edit.c ## 21. ##### ? PROT_READ, PROT_WRITE, PROT_EXEC - , , ##### mprotect ? mprotect - , . . > int mprotect(void* address, size_t len, int prot) ##### , mmap mprotect .

```
#include <sys/stat.h>
#include <unistd.h>
#include <iostream>
#include <fcntl.h>
#include <sys/mman.h>

int main(int argc, char* argv[]) {
  const char* file_name = argv[1];
  double argument = strtod(argv[2], NULL);
```

```
  int fd = open(file_name, O_RDONLY);
  struct stat st = {};
  fstat(fd, &st);

  void* addr = mmap(NULL, st.st_size, PROT_READ|PROT_EXEC, MAP_PRIVATE, fd, 0);
  double (*func)(double) = (double (*)(double)) ((char*)addr + 0x40);

  close(fd);
  double result = func(argument);
  std::cout << argument << std::endl << result;
  munmap(addr, st.st_size);
}


double mysqr(double x) {
  return x * x;
}
```

```
g++ -c func.c
readelf -a func.o #              align        .text
g++ mmap_library.cpp
./a.out func.o 5
```

Illegal intstruction? Illegal intstruction - , : examples/21_mprotect_jit/jit.c, examples/21_mprotect_jit/illegal_instr ## 22. ##### malloc free ? , . malloc , ? ? - malloc sbrk mmap - **MAP_THRESHOLD** , malloc **mmap**. - 128 - 16 - , - sbrk - (MMAP_THRESHOLD) “ ” (program break). , program break (1), . - 16 512 8 (small chunks), , MMAP_THRESHOLD (large chunks) - , 4 . O(1). - . - , , - , , ( ). , , . , , . - , , , , , (8,). ##### fastbins? fastbins – small chunks. , - , . , . - , fastbins. (best suit) , fastbins . ##### malloc ? malloc 2 – brk (sbrk) mmap . # 4 ## 23. ##### ? > - , , , . ##### ? pid, ppid? ? , CPU ?

```
ps aux #
pstree #              ,    F5   htop
```

```
htop #                                    htop
top #
```

VIRT - , **RES** - **SHR** - (shared memory) **CPU** -

PID - id **PPID** - id htop PPID ##### , , ? htop - **NI** (niceness). **Niceness** - “ ” . NI, . -20 20, 0. Priority (PR) niceness .

```
nice -n 10 "command" #                    NI (10)
#            niceness        root'
renice -n 10 "command" #      NI              10
```

uid, euid cwd , ?

uid - id , . (,). **euid** - id , . : sudo. uid , sudo, euid - id root’a **cwd** - , . ###### ? htop ps -eo pid,user,euser,cmd ###### ? - cwd

```
#include <unistd.h>
int main() {
    chdir("/new/directory/path");
    return 0;
}
```

- uid/euid

```
#include <unistd.h>
#include <stdio.h>

int main() {
    if (setuid(1001) != 0) { // seteuid
        perror("Failed to set UID");
        return 1;
    }
    return 0;
}
```

gdb ## 24. ##### , , ? nice/renice **niceness** (NI), “ CPU”. NI, .

CPU affinity , ? CPU affinity — , . : `taskset -p <pid>` ( ), `taskset -pc 0,2 <pid>` ( ). : `sched_setaffinity(pid, ...)`.

process capabilities Linux, ? **capabilities,** ? Capabilities — “ ” root- (`CAP_NET_ADMIN`, `CAP_SYS_PTRACE`).

```
: getcap ./a.out
: setcap cap_net_raw+ep ./a.out
: cat /proc/<pid>/status ( CapEff, CapPrm),  capsh --print.
```

25.

fork **exec.** **exec** **?** **fork** - ,
, . PID . 0, -
PID .

```
//
#include <iostream>
#include <unistd.h>

int main() {
  std::cout << "Hello!" << "\n";
  int pid = fork();
  if (pid == 0) {
    std::cout << "child" << "\n";
  } else {
    std::cout << "parent" << "\n";
  }
}
//    : 2    Hello, child, parent,          cout
```

exec - . , , PID ,
.

exec, .
execve. 1. **execl** - int execl(const char
*path, const char *arg, ..., NULL); execl("/bin/ls", "ls", "-l", NULL); 2. **execv** -
int execv(const char *path, char *const argv[]); c char *args[] = {"ls", "-l",
NULL}; execv("/bin/ls", args);` 3. **execvp** - execve, PATH
int execvp(const char *file, char *const argv[]);

```
    char *args[] = {"ls", "-l", NULL};
    execvp("ls", args);
```

, man 3 exec.

	PATH
execl	
execv	
execle	
execve	
execlp	
execvp	

, - . p - path, l - , v -
, e - .

```
which ls #
#                              execve
```

fork **exec,** **?** , ( )
, ( ) …… ######
fork: - : . - : Copy-on-Write, fork

. ###### exec: - PID: ,
. - : PID, . #####
, fork+exec.

```
#include <iostream>
#include <unistd.h>

int main() {
  int pid = fork();
  if (pid != 0) {
    std::cout << "parent" << std::endl;
    char* argv[] = {"/usr/bin/ls", "/home/liza", NULL};
    char* envp[] = {NULL};
    int code = execve("/usr/bin/ls", argv, envp);
    std::cout << "code: " << code << "\n";
    std::cout << errno << "\n";
  } else {
    std::cout << "child" << "\n";
  }
}
```

: examples/25_fork_exec/fork_exec.c ##### fork- ? **Fork-bomb** — ,
fork(), (,
). .

```
#include <iostream>
#include <unistd.h>

int main() {
  while (true) {
    int pid = fork();
  }
}
```

26.

? man ps - **S** - , , . : - **D** -
, (I/O) - **T** - (SIGSTOP Ctrl+z) - **t** -
- **Z** - - - **R** - ##### ,
? , Ctrl+z, :

```
kill -STOP "proccess-id"
kill -CONT "proccess-id" #           ))))))))))))))))))))))))))))0
#                                ( S+,                    )
#                  ,                    ,
```

fg bg?

```
./a.out & #
jobs #                    ,
```

fg

job, ###### bg .

bg 1 - ##### - , ? - - , , . - , wait() . - - , . ##### , - ?

```
htop # , S
ps u -p "proccess-id" # STAT
```

wait, **?** wait/waitpid “ ” ( ).

```
int status = 0;
waitpid(child_pid, &status, 0);
```

sleep **?** sleep(n) n (-). libc-nanosleep.

27.

rlimit ?

rlimit - . cat /proc/$(pgrep a.out)/limits ##### getrlimit setrlimit?

```
struct rlimit {
    rlim_t rlim_cur;  //
    rlim_t rlim_max;  //
};

int getrlimit(int resource, struct rlimit *rlim);
int setrlimit(int resource, const struct rlimit *rlim);
```

resource - , . man 2 getrlimit. / . ##### / ? setrlimit **RLIMIT_DATA** - , , , **RLIMIT_CPU** - . ##### , ? , , , , .

, , , errno. ## 28. ##### seccomp. > **Seccomp (Secure Computing)** — Linux, , (, SIGSYS), . ##### , . Bad system call (core dumped)?

```
sudo apt-get install libseccomp-dev #
g++ seccomp.cpp -lseccomp #
```

: examples/28_seccomp/seccomp_forbid_getpid.c

```
#include <seccomp.h>
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <iostream>

void seccomp_setup() {
```

```
  scmp_filter_ctx ctx = seccomp_init(SCMP_ACT_ALLOW);
  if (ctx == nullptr) {
    std::cout << "seccomp_init failed" << std::endl;
    exit(1);
  }

  if (seccomp_rule_add(ctx, SCMP_ACT_KILL, SCMP_SYS(clone), 0) != 0) {
    std::cout << "seccomp_rule_add failed" << std::endl;
    seccomp_release(ctx);
    exit(1);
  }

  if (seccomp_load(ctx) != 0) {
    std::cout << "seccomp_load failed" << std::endl;
    seccomp_release(ctx);
    exit(1);
  }
  seccomp_release(ctx);
}

int main() {
  seccomp_setup();
  fork();
  std::cout << errno;
}
```

```
man seccomp_init #
```

29.

?

- IPC (Inter Proccess Communication) ##### ,
?

```
kill -signal "proccess_id"
```

syscall - kill. , #####
, . - SIGHUP - ssh , .
, SIGHUP. . nohup - SIGABRT - abort()
- SIGCHLD - , - SIGCONT - , - SIGILL -
illegal instruction - SIGSYS - bad system call - SIGSEGV - segfault - SIGTSTP - Ctrl+z - SIGSTOP -
, - SIGFPE - floating point exeption - SIGINT - Ctrl+c - SIGQUIT - Ctrl +
- SIGTERM - , kill - SIGKILL - kill -KILL , man 7 signal 2
: **SIGKILL SIGSTOP** ##### ? 5
: - Ign - - Term - - Core - coredump - Stop - - Cont -
segfault?

```
kill -11 <pid>
```

?

```
kill(getpid(), SIGTERM) // syscall
raise(SIGTERM) //
```

?

```
pause() // syscall
```

30.

? **signal** **sigaction** **signal** - **sigaction** - . sigaction . SA_NODEFER .

```
#include <stdio.h>
#include <signal.h>
#include <stdlib.h>
#include <iostream>

void handler(int signum) {
  std::cout << "signal occurred\n";
  sleep(5);
}

int main() {
  struct sigaction sa;
  sa.sa_handler = &handler;
  sigemptyset(&sa.sa_mask);
  sa.sa_flags = SA_NODEFER;

  if (sigaction(SIGINT, &sa, NULL) == -1) {
    std::cout << "sigaction";
    exit(1);
  }

  sleep(5);

  int* ptr = NULL;
  *ptr = 10;
  std::cout << "after segfault";
}
```

: sleep , , , .
, segfault - .

```
#include <stdio.h>
#include <iostream>
#include <signal.h>

void handler(int signum) {
  std::cout << "caught " << signum << std::endl;
}

int main() {
  signal(SIGSEGV, &handler);
  int* p = nullptr;
  std::cout << *p;
```

```
}
```

caught 11, , , ,

```
#include <stdio.h>
#include <iostream>
#include <signal.h>

int* p = NULL;
int a = 0;

void handler(int signum) {
  std::cout << "caught " << signum << std::endl;
  p = &a;
}

int main() {
  signal(SIGSEGV, &handler);
  std::cout << *p;
}
//
```

, ?

```
#include <stdio.h>
#include <signal.h>

void handler(int signum) {
  printf("Signal number %d received\n",#include <stdio.h>
#include <signal.h>

void handler(int signum) {
  printf("Signal number %d received\n", signum);
  sleep(5);
  printf("Signal number %d done\n", signum);
}

int main() {
  signal(SIGINT, &handler);
  signal(SIGTSTP, &handler);
  getchar();
} signum);
  sleep(5);
  printf("Signal number %d done\n", signum);
}

int main() {
  signal(SIGINT, &handler);
  signal(SIGTSTP, &handler);
  getchar();
}
```

- SIGINT, SIGTSTP, SIGTSTP
- , , , . . . Ctrl+c, , Ctrl+c - . handler, SIGINT (, 10 SIGINT)
- , ##### - ? sigaction.

```
sigfillset(&sa.sa_mask); //
sigaddset(&sa.sa_mask, SIGUSR1); //
sigaction(SIGINT, &sa, NULL)
```

, - ?

1. , errno EINTR (Interrupted System Call).
2. (automatically restarted) , SA_RESTART sigaction.
3. : , O_NONBLOCK (-). ##### signal-safety ? **async-signal-safe** (write, _exit, signal/sigaction). printf, malloc, new, std::cout . . handler' UB (/). — , (/). ## 31. ##### pipes? >Pipes - IPC.

```
int pipe(int pipefd[2], int flags);
```

- - , , -
- , ##### pipe pipe.

```
#include <unistd.h>
#include <stdio.h>
#include <string.h>
#include <sys/wait.h>
#include <stdlib.h>

int main(int argc, char* argv[]) {
  char buf[1000];
  int pipefd[2];
  pipe(pipefd);

  int cpid = fork();
  if (cpid == 0) {
    close(pipefd[1]);

    while (read(pipefd[0], &buf, 1) > 0) {
      write(STDOUT_FILENO, &buf, 1);
    }

    write(STDOUT_FILENO, "\n", 1);
    close(pipefd[0]);
    _exit(0);
  } else {
```

```
    close(pipefd[0]);
    sleep(1);
    write(pipefd[1], argv[1], strlen(argv[1]));
    close(pipefd[1]);
    wait(NULL);
    exit(0);
  }
}
```

: pipe, while , pipe . read, , - , . pipefd[1] , - , , 0 ##### Broken pipe? Broken pipe

```
#include <unistd.h>
#include <string.h>
#include <sys/wait.h>
#include <stdlib.h>
#include <signal.h>
#include <iostream>

void handle(int signum) {
  std::cout << "caught " << signum << std::endl;
}

int main(int argc, char* argv[]) {
  int pipefd[2];
  pipe(pipefd);
  signal(SIGPIPE, &handle);
  int cpid = fork();
  if (cpid == 0) {
    close(pipefd[1]);
    close(pipefd[0]);
    _exit(0);
  } else {
    close(pipefd[0]);
    sleep(1);
    write(pipefd[1], argv[1], strlen(argv[1]));
    close(pipefd[1]);
    wait(NULL);
    exit(0);
  }
}
```

| **bash ?** | ( ) Bash C `pipe()`, `fork()`, `dup2()`, `execvp()`. | , (pipe) . ## 32. ##### fifo- ? > FIFO - IPC.

- , p (pipe)
- `PIPE_BUF` . , , fifo , , . ##### , ?

```
mkfifo myfifo #
int mkfifo(const char* pathname, mode_t mode) #
```

, **fifo?** , **fifo?**

- FIFO, .
  , PIPE_BUF (4096 Linux).
- PIPE_BUF, .
- : A “Hello”. B “World”. HelloWorld WorldHello,
  “Hello” “World” , PIPE_BUF. ######
  – FIFO, , FIFO .
  FIFO .
- :
  – A B FIFO: A . B .
  . ## 33. ##### ? > Shared memory -
  IPC.

- 1 2. - System five, ,
UNIX- . - , POSIX. #####
? ###### 1.

```
int shmget(key_t key, size_t size, int shmflg) //
void* shmat(int shmid, const void* shmaddr, int shmflg) // attach,
int shmdt(const void* shmaddr) //
int shmctl(int shmid, int cmd, struct shmid_ds *buf); //          ,
key_t ftok(const char *pathname, int proj_id)
```

2.

```
int shm_open(const char *name, int oflag, mode_t mode); //
int shm_unlink(const char *name); //
```

ftok - , . proj_id - .

, . 1.

```
// writer
#include <stdio.h>
#include <stdlib.h>
#include <sys/ipc.h>
#include <sys/shm.h>

#define SHM_SIZE 1024  //

int main() {
  key_t key = 1234;  //       ,      writer.c

  //                      , IPC_CREAT     ,
  int shmid = shmget(key, SHM_SIZE, IPC_CREAT | 0666);
  if (shmid < 0) {
    perror("shmget");
    exit(1);
  }
```

```
  //
  char *data = (char *)shmat(shmid, NULL, 0);
  if (data == (char *)(-1)) {
    perror("shmat");
    exit(1);
  }

  //
  fgets(data, SHM_SIZE, stdin);
  getchar();

  shmdt(data);

  return 0;
}
```

```
// writer
#include <stdio.h>
#include <stdlib.h>
#include <sys/ipc.h>
#include <sys/shm.h>

#define SHM_SIZE 1024  //

int main() {
  key_t key = 1234;  //        ,       writer.c

  //
  int shmid = shmget(key, SHM_SIZE, 0666);
  if (shmid < 0) {
    perror("shmget");
    exit(1);
  }

  //
  char *data = (char *)shmat(shmid, NULL, 0);
  if (data == (char *)(-1)) {
    perror("shmat");
    exit(1);
  }

  //
  printf("           : %s", data);

  //
  shmdt(data);

  //
  shmctl(shmid, IPC_RMID, NULL);

  return 0;
```

```
}
```

: - - int, . , - IPC_CREAT - - writer, . reader . ! ###### 2.

```
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
#include <sys/mman.h>
#include <unistd.h>
#include <string.h>

#define SHM_NAME "/shared_memory_example"  //
#define SHM_SIZE 1024                      //

int main() {
  //
  int shm_fd = shm_open(SHM_NAME, O_CREAT | O_RDWR, 0666);
  if (shm_fd == -1) {
    perror("shm_open");
    exit(1);
  }

  //
  if (ftruncate(shm_fd, SHM_SIZE) == -1) {
    perror("ftruncate");
    exit(1);
  }

  //
  char* shared_memory = (char*)mmap(NULL, SHM_SIZE, PROT_READ | PROT_WRITE, MAP_SHARED,
   ↪  shm_fd, 0);
  if (shared_memory == MAP_FAILED) {
    perror("mmap");
    exit(1);
  }

  //
  fgets(shared_memory, SHM_SIZE, stdin);

  //
  munmap(shared_memory, SHM_SIZE);
  close(shm_fd);

  getchar();
  return 0;
}
```

```
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
```

```c
#include <sys/mman.h>
#include <unistd.h>

#define SHM_NAME "/shared_memory_example"  //
#define SHM_SIZE 1024                      //

int main() {
    //
    int shm_fd = shm_open(SHM_NAME, O_RDWR, 0666);
    if (shm_fd == -1) {
        perror("shm_open");
        exit(1);
    }

    //
    char *shared_memory = mmap(NULL, SHM_SIZE, PROT_READ | PROT_WRITE, MAP_SHARED,
     ↪  shm_fd, 0);
    if (shared_memory == MAP_FAILED) {
        perror("mmap");
        exit(1);
    }

    //
    printf("           : %s", shared_memory);

    //
    munmap(shared_memory, SHM_SIZE);
    close(shm_fd);

    //
    shm_unlink(SHM_NAME);

    return 0;
}
```

: - , /dev/shm ##### ,
?

```
ipcs -m
strace ipcs #              ,     ipcs
cat /proc/sysvipc/shm
```

, ?

```
cd /proc/<proccess_id>/maps/
#                    .              p (private)
#    s (shared)
```

34.

(, threads,)?

Threads - , ( ), ( )
thread ++.

```
#include <thread>
#include <iostream>

void job(char c) {
  for (int i = 0; i < 100000; ++i) {
    std::cout << c;
  }
}

int main() {
  std::thread t(job, 'a'); //                    thread
  job('b'); //
  t.join();
}
```

-

```
void job() {
  std::vector<int> v;
  for (int i = 0; i < 100000; ++i) {
    v.push_back(i);
  }
}

int main() {
  std::thread t(job);
  job();
  t.join();
}
```

- , ##### join detach? , main
, ? `join()` . , main

`detatch()` . `std::thread`
`std::thread`. `std::thread` C++ , , ,
.

( ) main. , thread
SIGABRT ## 35. ##### race condition? > **Race condition ( ) — ,**
, ,
.

, (, ,
-) .

: . , ,
, .

. ##### , UB -
.

```
std::vector<int> v;
```

```
void job() {
  for (int i = 0; i < 100000; ++i) {
    v.push_back(i);
  }
}

int main() {
  std::thread t(job);
  job();
  t.join();
}
```

. , ##### ? race condition .
> mutex - , - . .

```
std::vector<int> v;
std::mutex m;

void job() {
  m.lock();
  // Critical section
  for (int i = 0; i < 100000; ++i) {
    v.push_back(i);
  }
  m.unlock();
}

int main() {
  std::thread t(job);
  job();;
  t.join();
}
```

mutex : . mutex , lock() (, lock() mutex' ,) ##### deadlock ? , >
Deadlock — , ( ) , ,
. , .

, > Deadlock - , - unlock (,).
- RAII mutex. (std::lock_guard) ## 36. ##### std::thread, ?

```
#include <iostream>
#include <sys/mman.h>
#include <sched.h>
#include <sys/wait.h>

class Thread {
  using Callable = void(*)();
public:
  Thread(Callable func): func(func) {
    stack = mmap(
        NULL, STACK_SIZE, PROT_READ|PROT_WRITE,
```

```
        MAP_PRIVATE|MAP_ANONYMOUS|MAP_STACK, -1, 0);
    pid = clone(
        threadRoutine, stack, CLONE_VM|CLONE_FS|CLONE_FILES|CLONE_SIGHAND|CLONE_THREAD|
                        CLONE_SYSVSEM|CLONE_SETTLS|CLONE_PARENT_SETTID|
                        CLONE_CHILD_CLEARTID, (void*)func);
  }

  void join() {
    int status;
    waitpid(pid, &status, 0);
    pid = -1;
  }

  ~Thread() {
    if (pid > 0) {
      std::terminate();
    }
    munmap(stack, STACK_SIZE);
  }
private:

  static int threadRoutine(void* arg) {
    Callable routine = reinterpret_cast<Callable>(arg);
    routine();
    return 0;
  }

  static const int STACK_SIZE = 8392704;
  Callable func;
  void* stack;
  int pid = -1;
};

void f() {
  for (int i = 0; i < 100; ++i) {
    std::cout << i << " ";
  }
  std::cout << std::endl;
}

int main() {
  Thread t(f);
  f();
  t.join();
}
```

type erasure . . ##### clone ? c int clone(int (*fn)(void *), void *stack, int flags, void *arg, ... /* pid_t *parent_tid, void *tls, pid_t *child_tid */); - **fn** - - **stack** - . - **flags** - . , . CLONE_… - **arg** - , ##### ,

clone, std::thread

```
//                                -
stack = mmap(NULL, STACK_SIZE, PROT_READ|PROT_WRITE,
            MAP_PRIVATE|MAP_ANONYMOUS|MAP_STACK, -1, 0);
clone(func, stack, CLONE_VM|CLONE_FS|CLONE_FILES|CLONE_SIGHAND|
            CLONE_THREAD|CLONE_SYSVSEM|CLONE_SETTLS|CLONE_PARENT_SETTID|
             LONE_CHILD_CLEARTID, /*arg*/);
//
```

? Linux **LWP (Lightweight Processes)**, , . — , . ##### - ? > **-** — , Linux. , , - . **-**

- execve, , ,
- fork, wait ##### tid, tgid, , pid? >**tgid** - , PID . >**tid** - . >**pid** - . .

htop, . htop pid tid. H. TID, , !

```
ps -eLf # LWP         TID, TGID         PID
```

?

```
int tkill(int tid, int sig);
```

joinable “ ” clone+futex: `examples/36_clone_thread/clone_thread.c` # 5 ## 37. ##### Linux, ? — . “ ” (, N).

: - POSIX semaphores: `sem_init` ( ), `sem_open` ( ) - System V: `semget/semop/semctl`

futex? `futex` (fast userspace mutex) — “ ” : userspace , .

std::mutex **futex** : `std::atomic<int> state` (0 , 1). `lock()` CAS 0→1. — `futex(FUTEX_WAIT, 1)`. `unlock()` 0 `futex(FUTEX_WAKE, 1)`.

: `examples/37_futex_mutex/futex_mutex.cpp`

38.

? **?**

-

: 1. **: - x86/x86-64**: Intel AMD. — NASM, MASM, GAS. - **ARM**: , . ARM . - 1. **: - Intel-** (NASM, MASM): , , x86 `mov eax, ebx`. - **AT&T-** (GAS): GNU Assembler, `%` `$` (`movl %eax, %ebx`). ##### ?

x86 > - 1. rax - ,
2. rbx - base, . 3. rcx - counter, . 4. rdx - data,
, . : 8 64. .
ax - 16- . eax - 32- , rax - 64- . 16
32 , ax (16) eax ##### : mov,
, . **mov**:

```
mov    to, from
mov    [to], from //        to          from
```

+:

```
int x = 4;
int y = 2;
x += y:

mov     eax, DWORD PTR [rbp-8]
add     DWORD PTR [rbp-4], eax
```

```
long long x = 4;
int y = 2;

mov     eax, DWORD PTR [rbp-12]
cdqe
add     QWORD PTR [rbp-8], rax
//            x   eax -
// cdqe - "        eax   rax".       -        2
```

- eax
- sub ( ) *:

```
int x = 4;
int y = 2;
x *= y:

mov     eax, DWORD PTR [rbp-4]
imul    eax, DWORD PTR [rbp-8]
mov     DWORD PTR [rbp-4], eax
```

- , ,

/:

```
int x = 4;
int y = 2;
x /= y;

mov     eax, DWORD PTR [rbp-4]
cdq
idiv    DWORD PTR [rbp-8] //       ,            a
mov     DWORD PTR [rbp-4], eax
```

- ,
- eax, - edx ###### / mul div - .
sub, add

```
x *= 5

mov     edx, DWORD PTR [rbp-4]
mov     eax, edx
sal     eax, 2 //                2,  . .         4
add     eax, edx
mov     DWORD PTR [rbp-4], eax
```

```
//
x /= 3;

mov     eax, DWORD PTR [rbp-4]
movsx   rdx, eax //
imul    rdx, rdx, 1431655766
mov     rcx, rdx
shr     rcx, 32 //
cdq
mov     eax, ecx
sub     eax, edx
mov     DWORD PTR [rbp-4], eax


and    operand1, operand2
or     operand1, operand2
xor    operand1, operand2
not    operand
```

39. ##### . .

```
jmp     .L2 //
```

```
if (x > 4) {
  goto mylabel;
}

cmp     DWORD PTR [rbp-4], 4
jle     .L4    // jump less equal,        if
jle     .L2    //    if'a
```

- , 64 , -
- (CF, OF, PF, SZ, ZF),

(cmp test)

1. **(unsigned)**

(, cmp).

---

je/jz	(equal)	ZF = 1	,
jne/jnz	(not equal)	ZF = 0	,
jb/jnae	(below)	CF = 1	,
jnb/jae	(above/equal)	CF = 0	,
ja/jnbe	(above)	CF = 0 ZF = 0	,
jbe/na	(below/equal)	CF = 1 ZF = 1	,

2. **(signed)** (, cmp).

jl/jnge	(less)	SF OF	,
jge/jnl	(greater/equal)	SF = OF	,
jg/jnle	(greater)	ZF = 0 SF = OF	,
jle/jng	(less/equal)	ZF = 1 SF OF	,

3.

.

jc	CF = 1 CF
jnc	CF = 0 CF
jo	OF = 1 OF
jno	OF = 0 OF
js	SF = 1 SF
jns	SF = 0 SF
jp/jpe	PF = 1 PF
jnp/jpo	PF = 0 PF

if, while for ? if

- , . if'

```
if (x < y) { x = y; }
int z = 0;
```

```
mov     eax, DWORD PTR [rbp-4]
cmp     eax, DWORD PTR [rbp-8]
jge     .L2
mov     eax, DWORD PTR [rbp-8]
mov     DWORD PTR [rbp-4], eax

.L2:
mov     DWORD PTR [rbp-12], 0
```

for

```
for (int i = 0; i < 100; ++i) { ++x; }
```

```
mov     DWORD PTR [rbp-8], 0 //          i
jmp     .L2

.L3:  //    for
add     DWORD PTR [rbp-4], 1
add     DWORD PTR [rbp-8], 1

.L2: //
cmp     DWORD PTR [rbp-8], 99
jle     .L3
```

while

for,

```
while (x < 100) { ++x; }

jmp     .L2

.L3:
add     DWORD PTR [rbp-4], 1

.L2:
cmp     DWORD PTR [rbp-4], 99
jle     .L3
```

40.

?

```
section .text
global is_prime

is_prime:

  cmp  eax, 2
  jb   .not_prime  //          jb,                jl
  je   .is_prime

  test eax, 1
  jz   .not_prime

  mov  ecx, 3  // ecx -
  mov  ebx, eax

.check_loop:
  mov  eax, ecx
  mul  eax    //      mul         ,              eax
  cmp  eax, ebx
  jg   .is_prime

  mov  edx, 0
  mov  eax, ebx
```

```
  div  ecx
  cmp  edx, 0
  je   .not_prime

  add  ecx, 2
  jmp  .check_loop

.is_prime :
  mov  eax, 1
  ret

.not_prime:
  xor  eax, eax
  ret
```

```
#include <iostream>
//               extern "C",
extern "C" int is_prime(int n);

int main() {
  int number;

  std::cout << "Enter a number: ";
  std::cin >> number;

  int result = is_prime(number);
  if (result) {
    std::cout << number << " is a prime number" << std::endl;
  } else {
    std::cout << " is not a prime number" << std::endl;
  }
}
```

```
nasm -f elf64 is_prime.asm
g++ is_prime.cpp is_prime.o
```

: examples/40_asm_is_prime/ ##### gdb ?
, ?

```
g++ -g is_prime.cpp is_prime.o
gdb ./a.out
b is_prime
disassemble #                ,
b *0x0000555555555313 #
stepi #    si,
info registers #
```

41.

call ret

call - jump' , -
(rip) **ret** - , call. ,

. ##### ? , - ,
. “ ” - rbp #### stack pointer base pointer, ebp
esp? **rsp** - , stack pointer, ( ) **rbp** - , base
pointer, #####
? : 1. call, 2. **rbp**
3. rbp rsp : 4. rbp rbp 5.
ret ##### ? ? 1. rdi - 1- 2. rsi
- 2- 3. rdx - 3- 4. rcx - 4- 5. r8 - **5**- 6. r9 - **6**- ,
. , , . == **:**
is_prime rax 1- ?.. == 32- ,
eax…. ##### -fno-omit-frame-pointer, ?

`(rbp)` `backtrace`

backtrace , , base pointer `-fomit-frame-pointer`.
`-fno-omit-frame-pointer` `rbp` frame pointer.

42.

? stack protector, ,
-fno-stack-protector?

char*, (scanf, cin) , .
, , - ,
ret

: - fstack-protector - , , .
. : rbp , . . -
NX- : , (,). ,
, fno-stack-protector . ##### “Stack
smashing detected”?

```
#include <cstdio>

void f() {
  char buf[10];
  scanf("%s", buf);
}

int main() {
  f();
}
```

`./a.out` -

stack-protector - : `examples/42_stack_smash/smash.c` ##### ASLR
? ASLR (Address Space Layout Randomization) — / / /
.

```
cat /proc/sys/kernel/randomize_va_space
sudo sysctl -w kernel.randomize_va_space=0
sudo sysctl -w kernel.randomize_va_space=2
```

43.

. , ?

(CPU cache) — , ,
, . (RAM),
. ,
.

: - L1 - . . , - . -
2 64 ( ) - L2 - L1. , .
, ( ). 256 512 - L3 - .
. . 1 8 #####
?

`lscpu`

- **L1d cache:** 1
- **L1i cache:** 1
- **L2 cache:** 2.
- **L3 cache:** 3. ,

```
cat /sys/devices/system/cpu/cpu0/cache/index0/size # L1d      0
cat /sys/devices/system/cpu/cpu0/cache/index1/size # L1i      0
cat /sys/devices/system/cpu/cpu0/cache/index2/size # L2      0
cat /sys/devices/system/cpu/cpu0/cache/index3/size # L3
```

- ? **,** **?**

- (cache line) — ,
(RAM). 32 128 (64).

- , - , , ,
- . - - , .
, - 16 ##### : cache line :
`stride` . `stride=64` ( ) “ ” , `stride=4` —
.

: `examples/43_cache/cacheline_stride.cpp`

: : (L1/L2/L3/DRAM) .

: `examples/43_cache/cache_levels.cpp`

44.

branch prediction, **?** , if , .
, , , ,
(,)

, .
, . ##### (C++20,),
if ? ?

```
//       c++20
if (...) [[likely]] {}

if (...) [[unlikely]] {}
```

```
//   c++20, 1      ,
if (__builtin_expect(x > 0, 1)) {}
```

, : 1. , . 2. . ##### : branch prediction :
(,). mispredict → .

: examples/44_branch_prediction/branch_prediction.cpp

45.

instruction-level parallelism (ILP) **?** ILP —
(, execution units).

out-of-order execution **?** Out-of-order —
, , execution units. , / (
Spectre-).

? “ ” (/) .
— , — , (/) .

: ILP (vs) : , ,
— ILP.

: examples/45_ilp_oOO/ilp.cpp

46.

? Intel intrinsics, ? SIMD, AVX? SIMD — “ —
”. AVX/AVX2/AVX-512 x86 .
Intrinsics — / , SIMD- (_mm256_add_ps).

? SSE: XMM (128-bit), AVX/AVX2: YMM (256-bit), AVX-512:
ZMM (512-bit).

: float AVX2.

: examples/46_simd_avx/avx_add.cpp

47.

? **asm()** .
volatile , .

asm(): - - , % - , ,
$ - - , - , #####
, ? **rdtsc**
. ,
: , ##### :
asm : examples/47_inline_asm/swap.c

timing attacks? : **constant time** (/), (volatile/), rdtsc/ .

rdtsc: examples/47_inline_asm/rdtsc.c

48.

? **syscall?** — call address space.
— (ring 0) entrypoint' (MSR) .

, **syscall** libc : objdump -d a.out | grep syscall.

execve (x86-64 Linux): examples/48_syscall_execve/execve_syscal

49.

? . Ring 0 — kernel, Ring 3 — user.
(hlt, lidt, mov cr*) kernel mode.

, **?** **IDT?** — , CPU (IRQ, page fault, int n).
IDT (Interrupt Descriptor Table) — , CPU / .

? — kernel mode entrypoint.
— (syscall), / .

asm **?** int3 (SIGTRAP), ud2 (SIGILL).

: examples/49_interrupts/int3.c, examples/49_interrupts/ud2.c ##### ?
(Ring Protection Levels) — ,
.
, , , . - **Ring 0 (0)** — **(kernel mode):**

- (kernel), , .

- **Ring 1 (1)** — **:**
  - , , ,
    0.
- **Ring 2 (2)** — **:**
  - , , 1.
  - , ,
    .
- **Ring 3 (3)** — **(user mode):**
  - .
  - , .
  - 3 . #####
    ? ? :

- , :
  1. HLT -
  2. INVLPG - TLB
  3. LIDT - . ,
  4. MOV CR - - , . CR0 - , . CR2 - page fault. -

- .
  ##### ? syscall? Syscall - , . - . syscall, . .
  .

  , , .
  .

  ,

```
g++ -static syscall.asm
objump -d a.out > output.txt
```