**Звіт  
до лабораторної роботи № 4**

**з курсу: «Комп’ютерні системи»**

**з теми: «Основи роботи з Аssembler»**

**студента 3 курсу КІ групи СА**

**ФРЕКС**

**Бузанова Дмитра**

**Хід роботи**

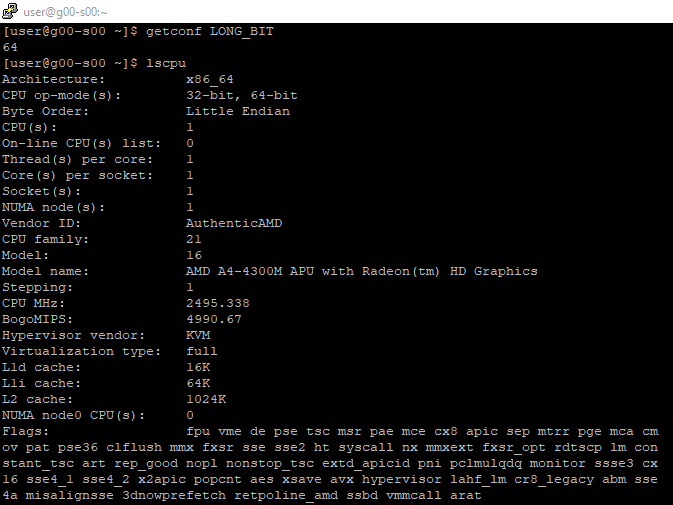
*Варіант індивідуального завдання* ***№5***

**Посилання на репозиторій:**

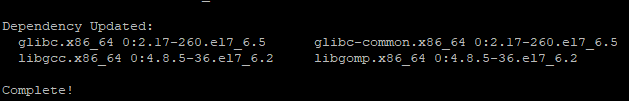
<https://github.com/DmytroBuzanov/CS_labs/tree/master/lab4>

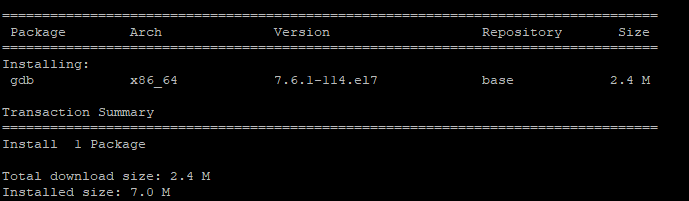
1. **Підготовка середовища розробки**

- для роботи підготовлено комп’ютер з необхідною архітектурою:



* встановлюємо необхідні пакети GCC, GDB, GNU Make та GNU Binutils:





* Завантажте в нього файл із символами та програму-заготовку:
* [defs.h](http://tilde.slu.kiev.ua/cs/asm/defs.h)
* [exit.s](http://tilde.slu.kiev.ua/cs/asm/exit.s)

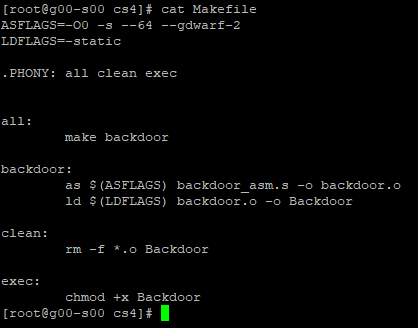


* Виконайте асемблювання програми-заготовки та зв'язування:
* as -o exit.o -c exit.s
* ld -static -o exit exit.o

Пересвідчіться у тому, що виконуваний файл працездатний. Програма повинна нічого не робити і не виводити жодних помилок



**Makefile:**



**Індивідуальне завдання**

## **Чорний хід**

Створіть програму, яка відкриє TCP-сокет на заданому порті, та при підключенні до цього порта запустить програму /bin/bash із усіма стандартними дескрипторами перевизначеними на з'єднаний сокет.

### **Псевдокод**

/\* declare in .bss section \*/

struct sockaddr\_in sin = { 0, 0, 0 };

/\* declare in .data section \*/

int sock;

int fd;

/\* declare in .text section \*/

const char \*bash = "/bin/bash";

main() {

   sock = socket(AF\_INET, SOCK\_STREAM, IPPROTO\_TCP);

   sin.sin\_family = AF\_INET;

   sin.sin\_port = 0x7527; /\* = htons(10101) \*/

   bind(sock, &sin, sizeof(sin));

   listen(sock, 1);

   fd = accept(sock, NULL, NULL);

   dup2(fd, stdin);

   dup2(fd, stdout);

   dup2(fd, stderr);    execve(bash, NULL, NULL); }

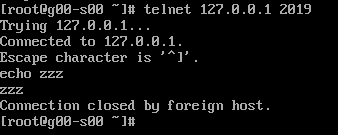
### **Перевірка**

telnet localhost 10101

і ввести пару команд типу echo ZZZ

**Демонстрація результату роботи:**





**Висновки**: під час виконання цієї лабораторної роботи було:

* розглянуто МПНР Assembler, опановано її основні принципи;
* створено Makefile; освоєно навички відлагоджування;
* виконано індивідуальне завдання згідно з прикріпленим варіантом (Чорний хід), тобто проведено час, відведений на виконання завдань, непомітно, з великим захопленням і задоволенням