

1. Написал key-gen и бинпатч:

```
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ls  
hack_app  hack_app_patched_2  keygen.py  libssl1.1_1.1.1f-1ubuntu2.24_amd64.deb  test.txt  
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$
```

2. Код keygen:

```
import hashlib

def calc_md5_16bytes(hwid_16: str) -> str:
    data = hwid_16.encode("ascii")
    digest = hashlib.md5(data).digest()
    digest_reversed = digest[::-1]

    return ''.join(f"{b:02x}" for b in digest_reversed)

if __name__ == "__main__":
    hwid = input("Введите HWID (ровно 16 символов ASCII): ").strip()

    if len(hwid) != 16:
        print("HWID должен быть ровно 16 ASCII символов")
    else:
        result = calc_md5_16bytes(hwid)
        print("MD5 (как в приложении):", result)
```

3. Чтобы сделать бинпатч, заменил инструкцию JNZ (0010159e) на просто JMP на блок, где работает 'защищенная' часть приложения (вывод в консоль, что приложение лицензировано на вашем пк):

Было:



Стало:

The screenshot shows a debugger interface with assembly code on the left and corresponding C-like pseudocode on the right. The assembly code is in Intel syntax, and the pseudocode is a decompiled representation of the program's logic.

```
0010159c ff ff          TEST    EAX,EAX
0010159e eb 00          JMP     LAB_001015a0

LAB_001015a0:
    MOV     dword ptr [RBP + array[16]],0x1
    CMP     dword ptr [RBP + array[16]],0x0
    JNZ     LAB_0010163f

LAB_0010163f:
    MOV     EDX,dword ptr [RBP + array[32]]
    MOV     EAX,dword ptr [RBP + array[28]]
    MOV     ESI,EAX
    LEA     RDI,[s_Your_HWID_is_%08X%08X_.Enter_the_001020... = "Your HWID is %08X%08"]
    MOV     a0 00 00 00
    MOV     EAX,0x0
    MOV     a0 00 00
    CALL   <EXTERNAL>::printf
    int printf(char * __form
               = ??)
    LEA     RSI,[userInput]
    MOV     af 40 00 00
    INT    INT_0000000f

array[0] = array[3] <> 0x18 | array[3] >> 0x18 | (array[3] & 0xffff)
;
snprintf(HWID,0x11,"%08X%08X", (ulong)array[7],(ulong)array[8]);
calc_md5(HWID,0x10);
for (array[5] = 0; (int)array[5] < 0x10; array[5] = array[5] + 1) {
    sprintf(md5Decode + (int)(array[5] * 2), "%02x", (ulong)(byte)md5Digest[5]);
}
array[4] = 1;
puts("Welcome to Lab2 super secure program!");
strncpy(md5Decode,xattrValue,0x21);
if (local_10 == *(long *) (in_FS_OFFSET + 0x28)) {
    return 0;
}
__stack_chk_fail();
/* WARNING: Subroutine does not return */

```

4. Тесты:

1. Само приложение

```
hack_app  hack_app_patched_2  keygen.py  libssl1.1_1.1.1f-1ubuntu2.24_amd64.deb  test.txt
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./hack_app
Welcome to Lab2 super secure program!
Your HWID is 410FA400FFFB8B07.
Enter the license key: asdasd
Provided key is wrong! App is closing!
Press Enter to continue...
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$
```

2. keygen:

```
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ python3 keygen.py
Введите HWID (ровно 16 символов ASCII): 410FA400FFFB8B07
MD5 (как в приложении): ad3d64c16baedfd58828bfed13a22c0a
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./hack_app
Welcome to Lab2 super secure program!
Your HWID is 410FA400FFFB8B07.
Enter the license key: ad3d64c16baedfd58828bfed13a22c0a
Now you app is activated! Thanks for purchasing!
Press Enter to continue...
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./hack_app
Welcome to Lab2 super secure program!
Your app is licensed to this PC!
Press Enter to continue...
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ getfattr -x user.license hack_app
getfattr: invalid option -- 'x'
Usage: getfattr [-hRLP] [-n name|-d] [-e en] [-m pattern] path...
Try 'getfattr --help' for more information.
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ getfattr hack_app -h
# file: hack_app
user.license
```

3. Бинпатч:

```
hack_app  hack_app_patched_2  keygen.py  libssl1.1_1.1.1f-1ubuntu2.24_amd64.deb  test.txt
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./hack_app_patched_2
Welcome to Lab2 super secure program!
Your app is licensed to this PC!
Press Enter to continue...
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$
```