

## 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]

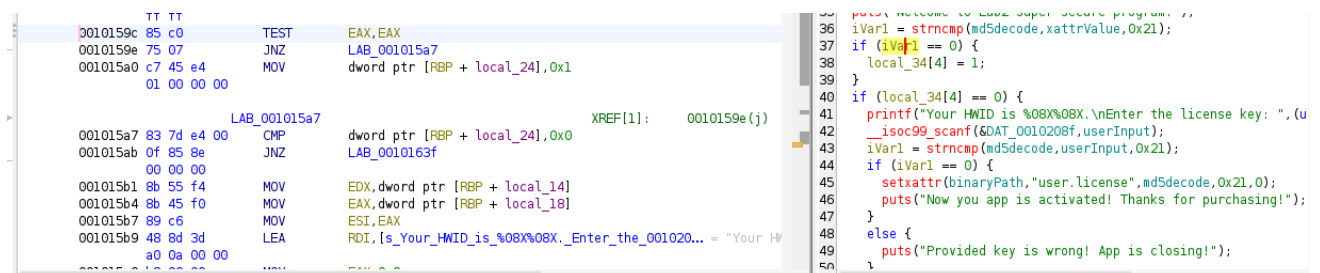
    return ''.join(f"{b:02x}" for b in digest_reversed)

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:

```
ff ff
0010159c 85 c0 TEST EAX,EAX
0010159e eb 00 JMP LAB_001015a0

LAB_001015a0
001015a0 c7 45 e4 MOV dword ptr [RBP + array[16]],0x1 XREF[1]: 0010159e(j)
01 00 00 00
001015a7 83 7d e4 CMP dword ptr [RBP + array[16]],0x0
001015ab 0f 85 8e JNZ LAB_0010163f
00 00 00
001015b1 8b 55 f4 MOV EDX,dword ptr [RBP + array[32]]
001015b4 8b 45 f0 MOV EAX,dword ptr [RBP + array[28]]
001015b7 89 c6 MOV ESI,EAX
001015b9 48 8d 3d LEA RDI,[s_Your_HWID_is_%08X%08X_Enter_the_001020... = "Your HWID is %08X%08X
a0 0a 00 00
001015c0 b8 00 00 MOV EAX,0x0
00 00
001015c5 e8 56 fb CALL <EXTERNAL>::printf int printf(char * __form
ff ff
001015ca 48 8d 35 LEA RSI,[userInput] = ??
af 4a 00 00
001015d1 48 e4 3d LEA RNT,[0x00000000] = 0x00000000

27 array[8] = array[3] << 0x18 | array[3] >> 0x18 | (array[3] & 0xff00)
28 ;
29 snprintf(HWID,0x11,"%08X%08X",(ulong)array[7],(ulong)array[8]);
30 calc_md5(HWID,0x10);
31 for (array[5] = 0; (int)array[5] < 0x10; array[5] = array[5] + 1) {
32     sprintf(md5decode + (int)(array[5] * 2),"%02x",(ulong)(byte)md5dige
33 }
34
35 readlink("/proc/self/exe",binaryPath,0x1000);
36 getxattr(binaryPath,"user.license",xattrValue,0x1000);
37 puts("Welcome to Lab2 super secure program!");
38 strncpy(md5decode,xattrValue,0x21);
39 array[4] = 1;
40 puts("Your app is licensed to this PC!");
41 system("read -p '\Press Enter to continue...\'' var");
42 if (local_10 == *(long *)(&in_FS_OFFSET + 0x28)) {
43     return 0;
44 }
45 /* WARNING: Subroutine does not return */
46 __stack_chk_fail();
47
```

#### 4. Тесты:

##### 1. Само приложение

```
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. Бин патч:

До:

```
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ls
bin-patcher hack_app hack_app_patched_2 hack_app_unpatched keygen.py lab2_patcher libssl1.1_1.1.1f-1ubuntu2.24_amd64.deb test.txt
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ vindiff <(xxd hack_app_unpatched) <(xxd hack_app_patched_2)
2 files to edit
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$

00001550: c20a 0000 e857 fcff ffb9 0010 0000 488d ...W.....H.
00001560: 15db 2a00 0048 8d35 b90a 0000 488d 3d0d ...H.S...H.=
00001570: 3b00 00e8 58fc ffff 488d 3db9 0a00 00e8 ...X...H.=...
00001580: bcfb ffff ba21 0000 0048 8d35 b02a 0000 .....H.S.*..
00001590: 488d 3da9 3a00 00e8 b4fb ffff 85c0 7507 H.=.....V.
000015a0: c745 e401 0000 0083 7de4 000f 850e 0000 ..E.....).....
000015b0: 008b 55f4 8b45 f089 c648 8d3d a00a 0000 ..U..E...H.=...
000015c0: b800 0000 00e8 56fb ffff 488d 35af 4a00 .....V...H.S.J.
000015d0: 0048 8d3d b70a 0000 b800 0000 00e8 0efc ..H.=.....
000015e0: ffff ba21 0000 0048 8d35 924a 0000 488d ....H.S.J..H.
000015f0: 3d4b 3a00 00e8 56fb ffff 85c0 7533 41b8 =K:...V.....u3A.

00001550: c20a 0000 e857 fcff ffb9 0010 0000 488d ...W.....H.
00001560: 15db 2a00 0048 8d35 b90a 0000 488d 3d0d ...H.S...H.=
00001570: 3b00 00e8 58fc ffff 488d 3db9 0a00 00e8 ...X...H.=...
00001580: bcfb ffff ba21 0000 0048 8d35 b02a 0000 .....H.S.*..
00001590: 488d 3da9 3a00 00e8 b4fb ffff 85c0 eb00 H.=.....V.
000015a0: c745 e401 0000 0083 7de4 000f 850e 0000 ..E.....).....
000015b0: 008b 55f4 8b45 f089 c648 8d3d a00a 0000 ..U..E...H.=...
000015c0: b800 0000 00e8 56fb ffff 488d 35af 4a00 .....V...H.S.J.
000015d0: 0048 8d3d b70a 0000 b800 0000 00e8 0efc ..H.=.....
000015e0: ffff ba21 0000 0048 8d35 924a 0000 488d ....H.S.J..H.
000015f0: 3d4b 3a00 00e8 56fb ffff 85c0 7533 41b8 =K:...V.....u3A.
```

После:

```
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ vimdiff <(xxd hack_app_unpatched) <(xxd hack_app_patched_2)
2 files to edit
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$
```

## Два теста:

```
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ vimdiff <(xxd hack_app_unpatched) <(xxd hack_app_patched_2)
2 files to edit
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ chmod +x hack_app_unpatched
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./hack_app_unpatched
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$ cp hack_app hack_app_unpatched1
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./lab2_patcher hack_app_unpatched1
[✓] Патч применён: 0x159E=0xEB, 0x159F=0x00
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ chmod +x hack_app_unpatched1
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./hack_app_unpatched1
Welcome to Lab2 super secure program!
Your app is licensed to this PC!
Press Enter to continue...
```

## 4. Программный код:

```
use std::fs::{OpenOptions, File};
use std::io::{Seek, SeekFrom, Write};

fn main() -> std::io::Result<()> {
    let path = std::env::args().nth(1).expect("Укажи путь к бинарнику");
    let mut file = OpenOptions::new()
        .read(true)
        .write(true)
        .open(&path)?;

    // Патч 1
    file.seek(SeekFrom::Start(0x0000159E))?;
    file.write_all(&[0xEB]);

    // Патч 2
    file.seek(SeekFrom::Start(0x0000159F))?;
    file.write_all(&[0x00]);

    println!("[✓] Патч применён: 0x159E=0xEB, 0x159F=0x00");
    Ok(())
}
```