

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 two panes. The left pane displays assembly code with labels like LAB_001015a0 and XREF[1]. The right pane shows corresponding C-like pseudocode. The pseudocode includes file operations (readlink, getxattr), string manipulations (snprintf, calc_md5, sprintf, strcmp), and system calls (read, write). It also contains a welcome message and a license check logic involving MD5 decoding and comparison.

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

LAB_001015a0
    MOV    dword ptr [RBP + array[16]],0x1
    CMP    dword ptr [RBP + array[16]],0x0
    JNZ    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"]
    a0 04 00 00
    a0 04 00 00
    MOV    EAX,0x0
    a0 00 00
    CALL   <EXTERNAL>::printf
    ff ff
    LEA    RSI,[userInput]
    af 48 8d 35
    af 49 00 00
    LEA    RDI,[fmt %08X%08X]
    af 49 00 24
    I EA

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("Your app is licensed to this PC!");
system("read -p \nPress Enter to continue...\` var");
if (local_10 == *(long *) (in_FS_OFFSET + 0x28)) {
    return 0;
}
_stack_chk_fail();
/* WARNING: Subroutine does not return */

```

4. Код для бин-патча:

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

fn main() -> std::io::Result<()> {
    let path = std::env::args().nth(1).expect("Укажите путь к бинарному файлу");
    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(())
}
```

3. Тесты:

1. Само приложение

```
ildar-islamov@ildar-islamov-VMware-Virtual-Platform:~/labs/lab2$ ./hack_app
Welcome to Lab2 super secure program!
Your HWID is 410FA400FFFFB8B07.
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$ vimdiff <(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 488dW.....H. 00001560: 15db 2a00 0048 b90a 0000 488d 3d0d ...*.H.5....H.=. 00001570: 3b00 00e8 58fc ffff 488d 3db9 0000 00e8 ;...X..H.=.... 00001580: bcfb ffff ba21 0000 0048 8d35 b02a 0000!..H.5.*.. 00001590: 488d 3da9 3a00 00e8 b4fb ffff 85c0 7507 H.=:.....U. 000015a0: c745 e401 0000 0083 7de4 000f 858e 0000 ..E.....). 000015b0: 0088 55f4 8b45 f089 c648 8d3d a00a 0000 ..U..E..H.=.... 000015c0: b800 0000 00e8 56fb ffff 488d 35af 4a00V..H.5.J. 000015d0: 0048 8d3d b70a 0000 b800 0000 00e8 0efc ..H.=..... 000015e0: ffffff ba21 0000 0048 8d35 924a 0000 488d ..!.H.5.J..H. 000015f0: 3d4b 3a00 00e8 56fb ffff 85c0 7533 41b8 =K:..V.....uA. + +- 750 lines: 00001500: 0000 0000 b921 0000 0048 8d15 303a 0000!..H.0:.....	00001550: c20a 0000 e857 fcff ffb9 0010 0000 488dW.....H. 00001560: 15db 2a00 0048 b90a 0000 488d 3d0d ...*.H.5....H.=. 00001570: 3b00 00e8 58fc ffff 488d 3db9 0000 00e8 ;...X..H.=.... 00001580: bcfb ba21 0000 0048 8d35 b02a 0000!..H.5.*.. 00001590: 488d 3da9 3a00 00e8 b4fb ffff 85c0 eb00 H.=:.....U. 000015a0: c745 e401 0000 0083 7de4 000f 858e 0000 ..E.....). 000015b0: 0088 55f4 8b45 f089 c648 8d3d a00a 0000 ..U..E..H.=.... 000015c0: b800 0000 00e8 56fb ffff 488d 35af 4a00V..H.5.J. 000015d0: 0048 8d3d b70a 0000 b800 0000 00e8 0efc ..H.=..... 000015e0: ffffff ba21 0000 0048 8d35 924a 0000 488d ..!.H.5.J..H. 000015f0: 3d4b 3a00 00e8 56fb ffff 85c0 7533 41b8 =K:..V.....uA. + +- 750 lines: 00001500: 0000 0000 b921 0000 0048 8d15 303a 0000!..H.0:.....
--	---

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$
```

00001570: 3b00 00e8 58fc ffff 488d 3db9 0a00 00e8 ;...X..H.=.... 00001580: bcfb ffff ba21 0000 0048 8d35 b02a 0000!..H.5.*.. 00001590: 488d 3da9 3a00 00e8 b4fb ffff 85c0 eb00 H.=:..... 000015a0: c745 e401 0000 0083 7de4 000f 858e 0000 ..E.....). 000015b0: 0088 55f4 8b45 f089 c648 8d3d a00a 0000 ..U..E..H.=.... 000015c0: b800 0000 00e8 56fb ffff 488d 35af 4a00V..H.5.J. 000015d0: 0048 8d3d b70a 0000 b800 0000 00e8 0efc ..H.=..... 000015e0: ffffff ba21 0000 0048 8d35 924a 0000 488d ..!.H.5.J..H. 000015f0: 3d4b 3a00 00e8 56fb ffff 85c0 7533 41b8 =K:..V.....uA. 00001600: 0000 0000 b921 0000 0048 8d15 303a 0000!..H.0:....	00001570: 3b00 00e8 58fc ffff 488d 3db9 0a00 00e8 ;...X..H.=.... 00001580: bcfb ffff ba21 0000 0048 8d35 b02a 0000!..H.5.*.. 00001590: 488d 3da9 3a00 00e8 b4fb ffff 85c0 eb00 H.=:..... 000015a0: c745 e401 0000 0083 7de4 000f 858e 0000 ..E.....). 000015b0: 0088 55f4 8b45 f089 c648 8d3d a00a 0000 ..U..E..H.=.... 000015c0: b800 0000 00e8 56fb ffff 488d 35af 4a00V..H.5.J. 000015d0: 0048 8d3d b70a 0000 b800 0000 00e8 0efc ..H.=..... 000015e0: ffffff ba21 0000 0048 8d35 924a 0000 488d ..!.H.5.J..H. 000015f0: 3d4b 3a00 00e8 56fb ffff 85c0 7533 41b8 =K:..V.....uA. 00001600: 0000 0000 b921 0000 0048 8d15 303a 0000!..H.0:....
--	--

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...
```