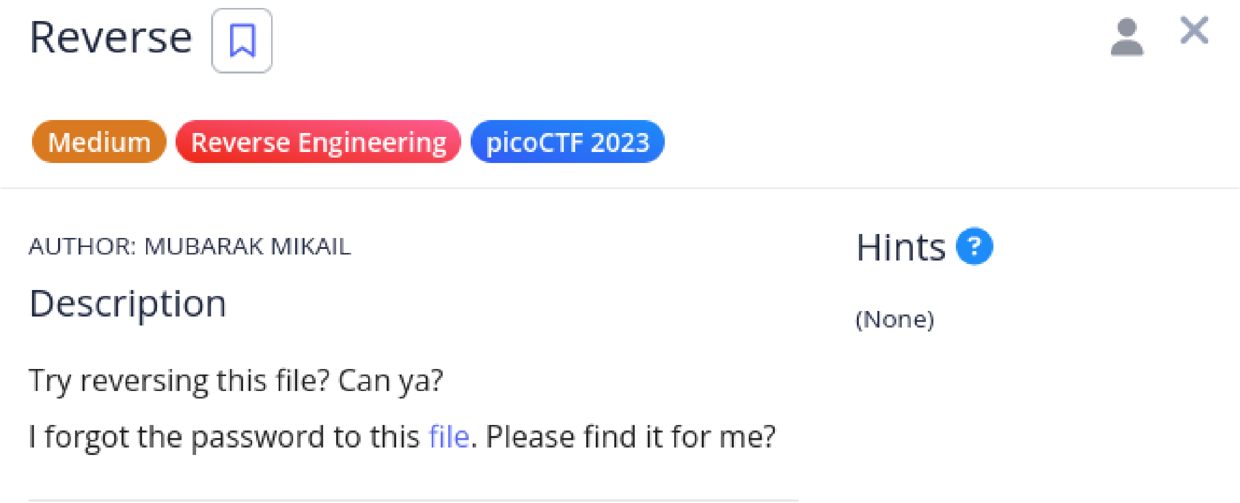
LinkedIn: Kelvin Kimotho



Reverse

Medium Reverse Engineering picoCTF 2023

AUTHOR: MUBARAK MIKAIL

Description

Try reversing this file? Can ya?

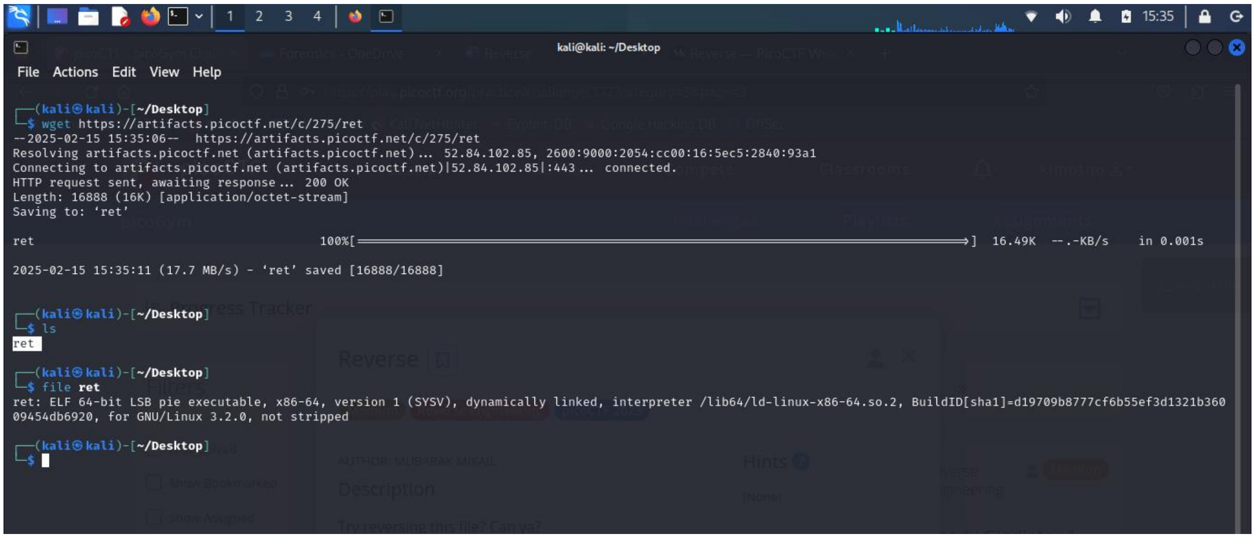
I forgot the password to this file. Please find it for me?

Hints

(None)

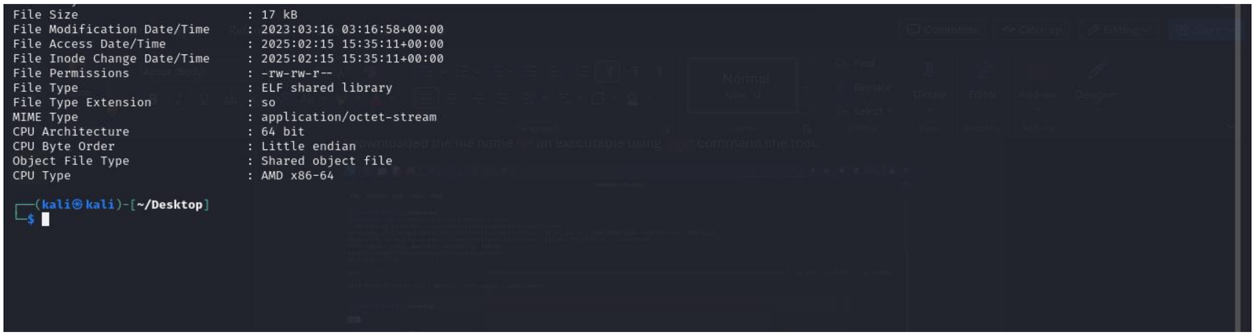
Solution

I downloaded the file name ret an executable using wget command line tool.



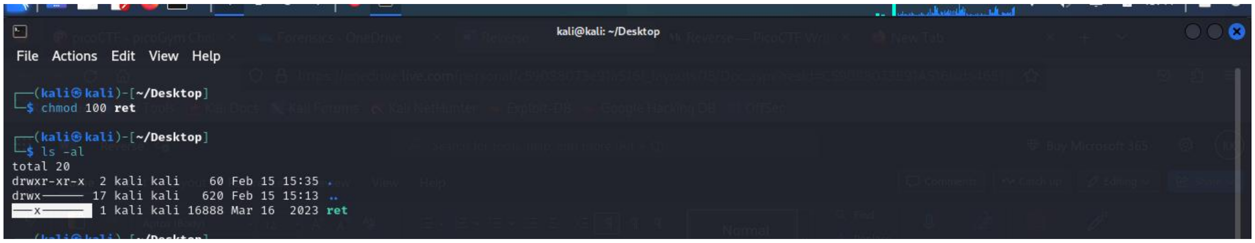
```
┌──(kali㉿kali)-[~/Desktop]
└─$ wget https://artifacts.picoctf.net/c/275/ret
--2025-02-15 15:35:06--  https://artifacts.picoctf.net/c/275/ret
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 52.84.102.85, 2600:9000:2054:cc00:16:5ec5:2840:93a1
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|52.84.102.85|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16888 (16K) [application/octet-stream]
Saving to: ‘ret’

ret                          100%[==================================================>]  16.49K  --.-KB/s    in 0.001s

2025-02-15 15:35:11 (17.7 MB/s) - ‘ret’ saved [16888/16888]


┌──(kali㉿kali)-[~/Desktop]
└─$ ls
ret

┌──(kali㉿kali)-[~/Desktop]
└─$ file ret
ret: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=d19709b8777cf6b55ef3d1321b360
09454db6920, for GNU/Linux 3.2.0, not stripped

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

I first tried learning about the file, its metadata using the exiftool but found no flag.



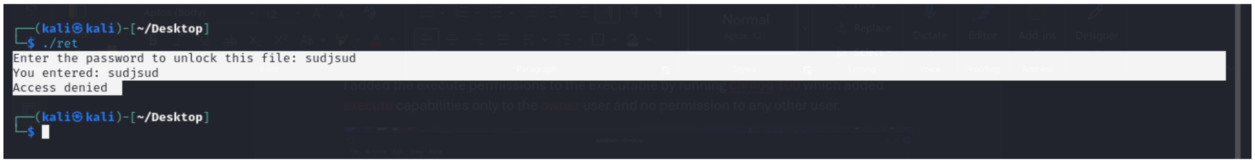
```
File Size                       : 17 kB
File Modification Date/Time     : 2023:03:16 03:16:58+00:00
File Access Date/Time           : 2025:02:15 15:35:11+00:00
File Inode Change Date/Time     : 2025:02:15 15:35:11+00:00
File Permissions                : -rw-rw-r--
File Type                       : ELF shared library
File Type Extension             : so
MIME Type                       : application/octet-stream
CPU Architecture                : 64 bit
CPU Byte Order                  : Little endian
Object File Type                : Shared object file
CPU Type                        : AMD x86-64

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

I added the execute permissions to the executable by running chmod 100 which added execute capabilities only to the owner user and no permission to any other user.



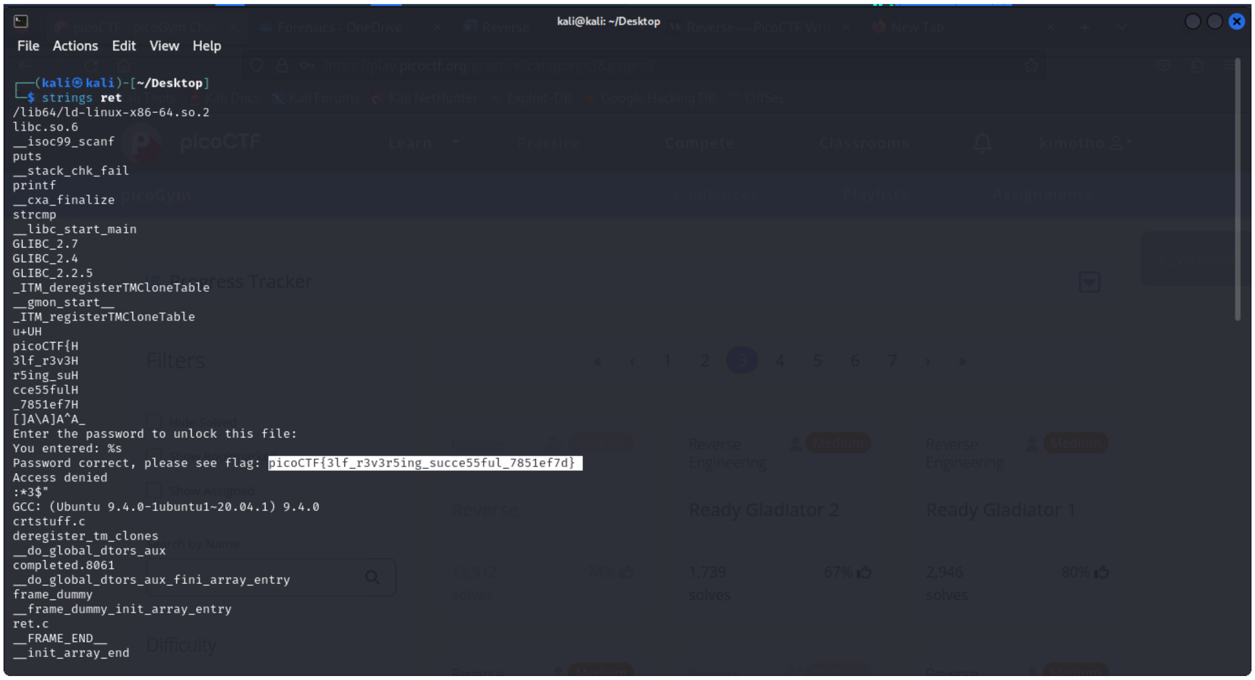
```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 100 ret

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -al
total 20
drwxr-xr-x  2 kali kali    60 Feb 15 15:35 .
drwx------ 17 kali kali   620 Feb 15 15:13 ..
---x------  1 kali kali 16888 Mar 16  2023 ret
┌──(kali㉿kali)-[~/Desktop]
```

Then i ran it which prompted me for a password. I had no password.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./ret
Enter the password to unlock this file: sudjsud
You entered: sudjsud
Access denied

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

I tried inspecting the file’s contents using the strings command line tool which revealed the flag embedded within the output strings as picoCTF{3lf_r3v3r5ing_succe55ful_7851ef7d}.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ strings ret
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
puts
__stack_chk_fail
printf
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
picoCTF{H
3lf_r3v3H
r5ing_suH
cce55fulH
_7851ef7H
[]A\A]A^A_
Enter the password to unlock this file:
You entered: %s
Password correct, please see flag: picoCTF{3lf_r3v3r5ing_succe55ful_7851ef7d}
Access denied
:*3$"
GCC: (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8061
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
ret.c
__FRAME_END__
__init_array_end
```