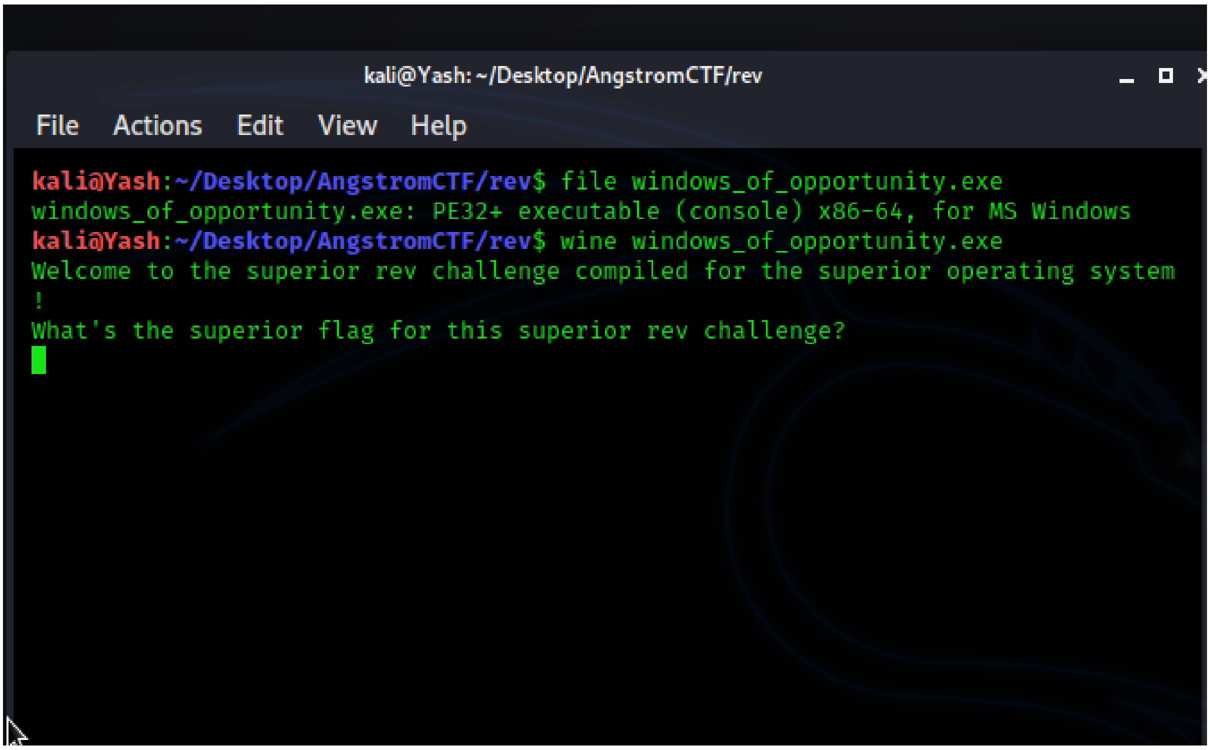
Description:

Windows Of Opportunity:

Clam's a windows elitist and he just can't stand seeing all of these Linux challenges! So, he decided to step in and create his own rev challenge with the "superior" operating system.

Hint- You can probably solve it just by looking at the disassembly.

We are provided with the file

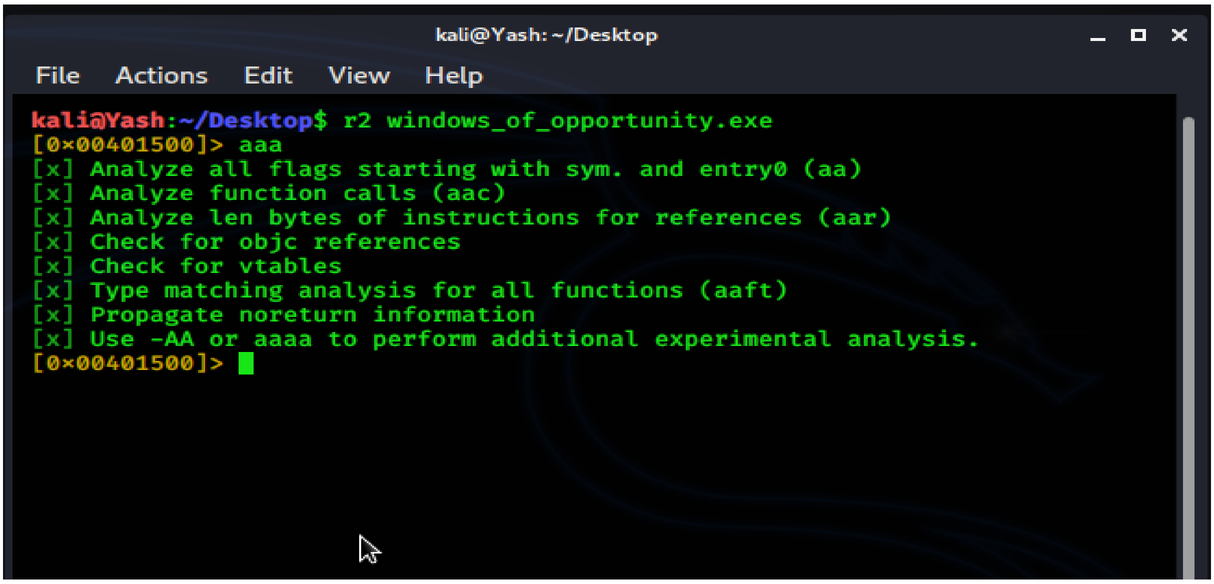

kali@Yash: ~/Desktop/AngstromCTF/rev
File Actions Edit View Help

```
kali@Yash:~/Desktop/AngstromCTF/rev$ file windows_of_opportunity.exe
windows_of_opportunity.exe: PE32+ executable (console) x86-64, for MS Windows
kali@Yash:~/Desktop/AngstromCTF/rev$ wine windows_of_opportunity.exe
Welcome to the superior rev challenge compiled for the superior operating system
!
What's the superior flag for this superior rev challenge?
```

From the hint section, we got to know that to look at any disassembler.

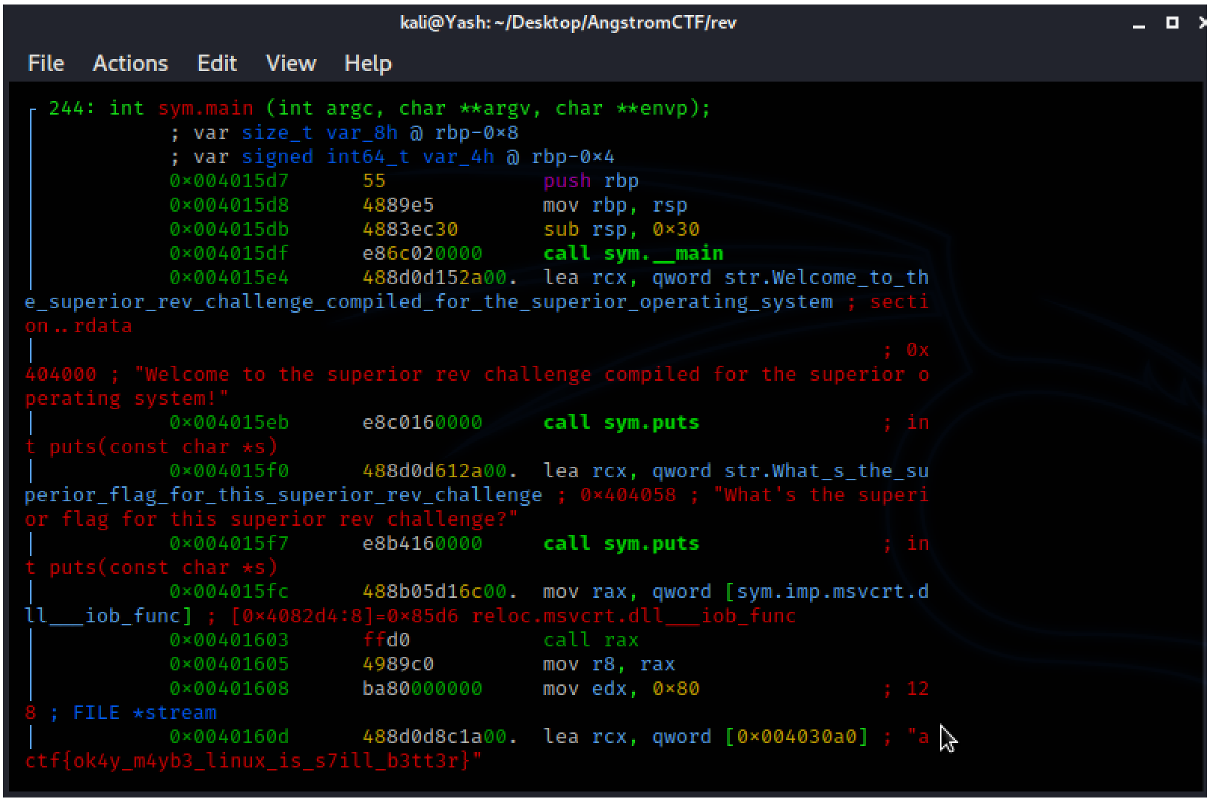
Let’s open windows_of_opportunity.exe file in radare2

Just do **r2 windows_of_opportunity.exe** in your terminal window and analysis this file.



```
kali@Yash:~/Desktop$ r2 windows_of_opportunity.exe
[0x00401500]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for objc references
[x] Check for vtables
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
[0x00401500]>
```

Then go through main function

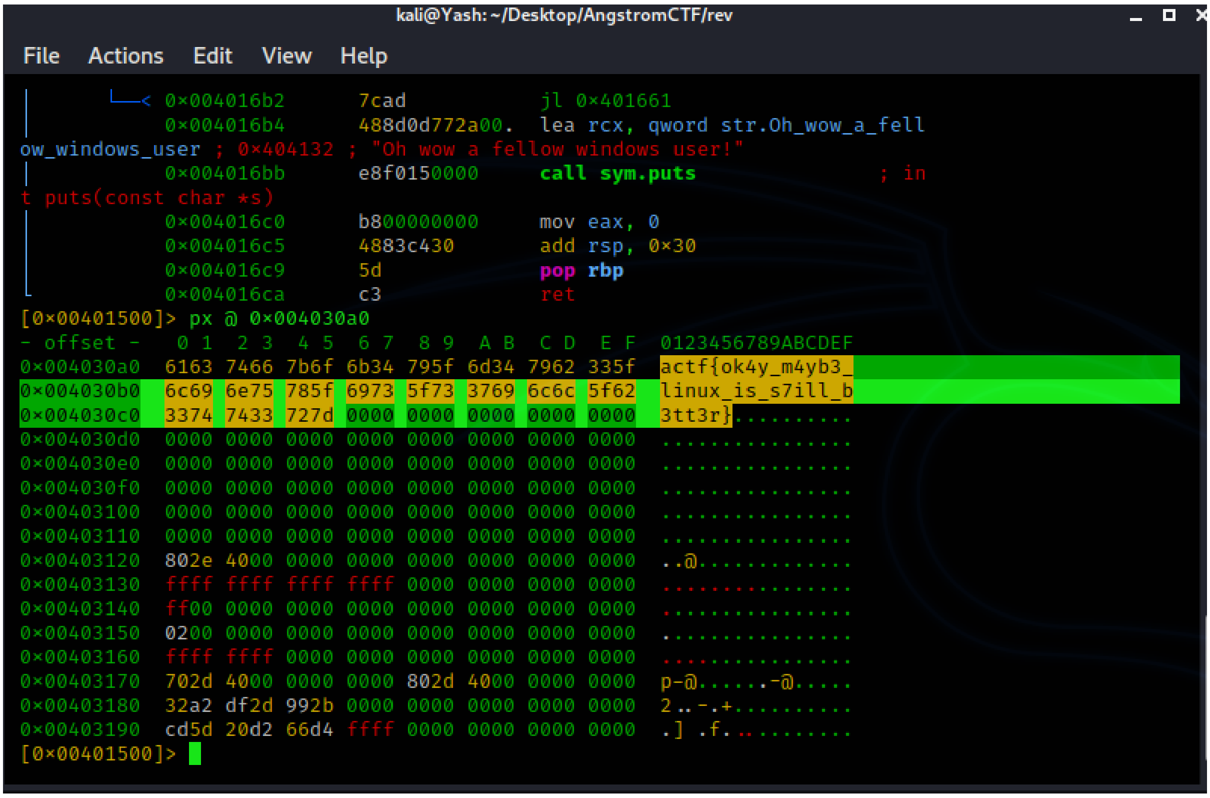


kali@Yash: ~/Desktop/AngstromCTF/rev
File Actions Edit View Help

```
┌ 244: int sym.main (int argc, char **argv, char **envp);
│           ; var size_t var_8h @ rbp-0×8
│           ; var signed int64_t var_4h @ rbp-0×4
│           0×004015d7      55             push rbp
│           0×004015d8      4889e5         mov rbp, rsp
│           0×004015db      4883ec30       sub rsp, 0×30
│           0×004015df      e86c020000     call sym.__main
│           0×004015e4      488d0d152a00.  lea rcx, qword str.Welcome_to_th
e_superior_rev_challenge_compiled_for_the_superior_operating_system ; secti
on..rdata
│                                                                     ; 0x
404000 ; "Welcome to the superior rev challenge compiled for the superior o
perating system!"
│           0×004015eb      e8c0160000     call sym.puts              ; in
t puts(const char *s)
│           0×004015f0      488d0d612a00.  lea rcx, qword str.What_s_the_su
perior_flag_for_this_superior_rev_challenge ; 0×404058 ; "What's the superi
or flag for this superior rev challenge?"
│           0×004015f7      e8b4160000     call sym.puts              ; in
t puts(const char *s)
│           0×004015fc      488b05d16c00.  mov rax, qword [sym.imp.msvcrt.d
ll___iob_func] ; [0×4082d4:8]=0×85d6 reloc.msvcrt.dll___iob_func
│           0×00401603      ffd0           call rax
│           0×00401605      4989c0         mov r8, rax
│           0×00401608      ba80000000     mov edx, 0×80              ; 12
8 ; FILE *stream
│           0×0040160d      488d0d8c1a00.  lea rcx, qword [0×004030a0] ; "a
ctf{ok4y_m4yb3_linux_is_s7ill_b3tt3r}"
```

Here you can clearly see that the flag is at address 0x004030a0

So you can hexdump at this address and you will get the flag.



kali@Yash: ~/Desktop/AngstromCTF/rev
File Actions Edit View Help

```
│       └─< 0×004016b2      7cad           jl 0×401661
│           0×004016b4      488d0d772a00.  lea rcx, qword str.Oh_wow_a_fell
ow_windows_user ; 0×404132 ; "Oh wow a fellow windows user!"
│           0×004016bb      e8f0150000     call sym.puts              ; in
t puts(const char *s)
│           0×004016c0      b800000000     mov eax, 0
│           0×004016c5      4883c430       add rsp, 0×30
│           0×004016c9      5d             pop rbp
└           0×004016ca      c3             ret
[0×00401500]> px @ 0×004030a0
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0×004030a0  6163 7466 7b6f 6b34 795f 6d34 7962 335f  actf{ok4y_m4yb3_
0×004030b0  6c69 6e75 785f 6973 5f73 3769 6c6c 5f62  linux_is_s7ill_b
0×004030c0  3374 7433 727d 0000 0000 0000 0000 0000  3tt3r}..........
0×004030d0  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×004030e0  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×004030f0  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×00403100  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×00403110  0000 0000 0000 0000 0000 0000 0000 0000  ................
0×00403120  802e 4000 0000 0000 0000 0000 0000 0000  ..@.............
0×00403130  ffff ffff ffff ffff 0000 0000 0000 0000  ................
0×00403140  ff00 0000 0000 0000 0000 0000 0000 0000  ................
0×00403150  0200 0000 0000 0000 0000 0000 0000 0000  ................
0×00403160  ffff ffff 0000 0000 0000 0000 0000 0000  ................
0×00403170  702d 4000 0000 0000 802d 4000 0000 0000  p-@......-@.....
0×00403180  32a2 df2d 992b 0000 0000 0000 0000 0000  2..-.+..........
0×00403190  cd5d 20d2 66d4 ffff 0000 0000 0000 0000  .] .f...........
[0×00401500]> 
```

The flag is : actf{ok4y_m4yb3_linux_is_s7ill_b3tt3r}