Behind the Scenes - Writeup

HackTheBox - Reversing – Very Easy

Written by Ron Jost

```
hacker5preme:~/HTB/Challenges/Reversing/VeryEasy/rev_behindthescenes$ file behindthescenes
behindthescenes: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld
-linux-x86-64.so.2, BuildID[sha1]=e60ae4c886619b869178148afd12d0a5428bfe18, for GNU/Linux 3.2.0, not stripped
```

After finding out, that it is a Linux executable, lets find out what it does.

```
hacker5preme:~/HTB/Challenges/Reversing/VeryEasy/rev_behindthescenes$ ./behindthescenes
./challenge <password>
```

It shows, that we don‘t have to crack something but instead find the password. Therefore we run the string command to check for a password.

```
hacker5preme:~/HTB/Challenges/Reversing/VeryEasy/rev_behindthescenes$ strings behindthescenes
/lib64/ld-linux-x86-64.so.2
libc.so.6
strncmp
puts
__stack_chk_fail
printf
strlen
sigemptyset
memset
sigaction
__cxa_finalize
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
./challenge <password>
> HTB{%s}
```

Strings shows us that between *./challenge <password>* and *HTB{%s}* is the section we have to be looking at. Therefore we fire up radare2, search for strings and hexdump it.

```
hacker5preme:~/HTB/Challenges/Reversing/VeryEasy/rev_behindthescenes$ r2 behindthescenes
Warning: run r2 with -e bin.cache=true to fix relocations in disassembly
 -- phrack, better than java in the browser -- jvoisin
[0x00001140]> iz
[Strings]
nth paddr      vaddr      len size section type  string
―――――――――――――――――――――――――――――――――――――――――――――――――――――――――
0   0x00002004 0x00002004 22  23   .rodata ascii ./challenge <password>
1   0x0000202b 0x0000202b 10  11   .rodata ascii > HTB{%s}\n

[0x00001140]> px @0x00002004
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x00002004  2e2f 6368 616c 6c65 6e67 6520 3c70 6173  ./challenge <pas
0x00002014  7377 6f72 643e 0049 747a 005f 306e 004c  sword>.Itz._0n.L
0x00002024  795f 0055 4432 003e 2048 5442 7b25 737d  y_.UD2.> HTB{%s}
0x00002034  0a00 0000 011b 033b 4c00 0000 0800 0000  .......;L.......
0x00002044  e8ef ffff 8000 0000 78f0 ffff a800 0000  ........x.......
0x00002054  88f0 ffff c000 0000 08f1 ffff 6800 0000  ............h...
0x00002064  f1f1 ffff d800 0000 29f2 ffff f800 0000  ........).......
0x00002074  18f4 ffff 1801 0000 88f4 ffff 6001 0000  ............`...
0x00002084  0000 0000 1400 0000 0000 0000 017a 5200  .............zR.
0x00002094  0178 1001 1b0c 0708 9001 0000 1400 0000  .x..............
0x000020a4  1c00 0000 98f0 ffff 2f00 0000 0044 0710  ......../....D..
0x000020b4  0000 0000 2400 0000 3400 0000 60ef ffff  ....$...4...`...
0x000020c4  9000 0000 000e 1046 0e18 4a0f 0b77 0880  .......F..J..w..
0x000020d4  003f 1a3a 2a33 2422 0000 0000 1400 0000  .?.:*3$"........
0x000020e4  5c00 0000 c8ef ffff 1000 0000 0000 0000  \...............
0x000020f4  0000 0000 1400 0000 7400 0000 c0ef ffff  ........t.......
[0x00001140]>
```