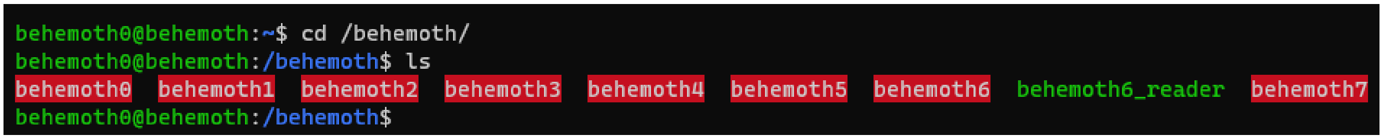
Behemoth Level 0

ssh behemoth0@behemoth.labs.overthewire.org -p 2221
Password is behemoth0



```
behemoth0@behemoth:~$ cd /behemoth/
behemoth0@behemoth:/behemoth$ ls
behemoth0  behemoth1  behemoth2  behemoth3  behemoth4  behemoth5  behemoth6  behemoth6_reader  behemoth7
behemoth0@behemoth:/behemoth$
```

There are multiple binaries in this folder, but for level 0 the primary focus will be behemoth0.

Basic Static Analysis

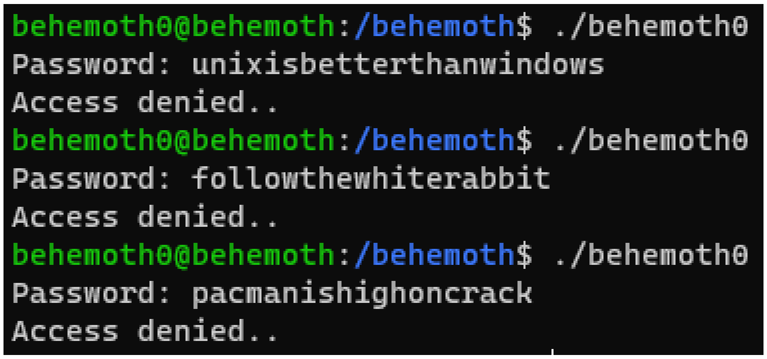
behemoth0@behemoth:/behemoth$ file behemoth0
behemoth0: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=42ba07767dc03cbeb365c18ac0bbeb191842dff7, not stripped

Behemoth0 is a dynamically linked executable and it is not stripped

When using the command “strings behemoth0” the output was
puts
setreuid
printf
strlen
system
geteuid
strcmp
unixisbetterthanwindows
followthewhiterabbit
pacmanishighoncrack
Password:
%64s
Access granted..
/bin/sh
Access denied..
;*2$"
GCC: (Debian 6.3.0-18+deb9u1) 6.3.0 20170516
Crtstuff.c
Main

Some interesting strings….

Dynamic Analysis

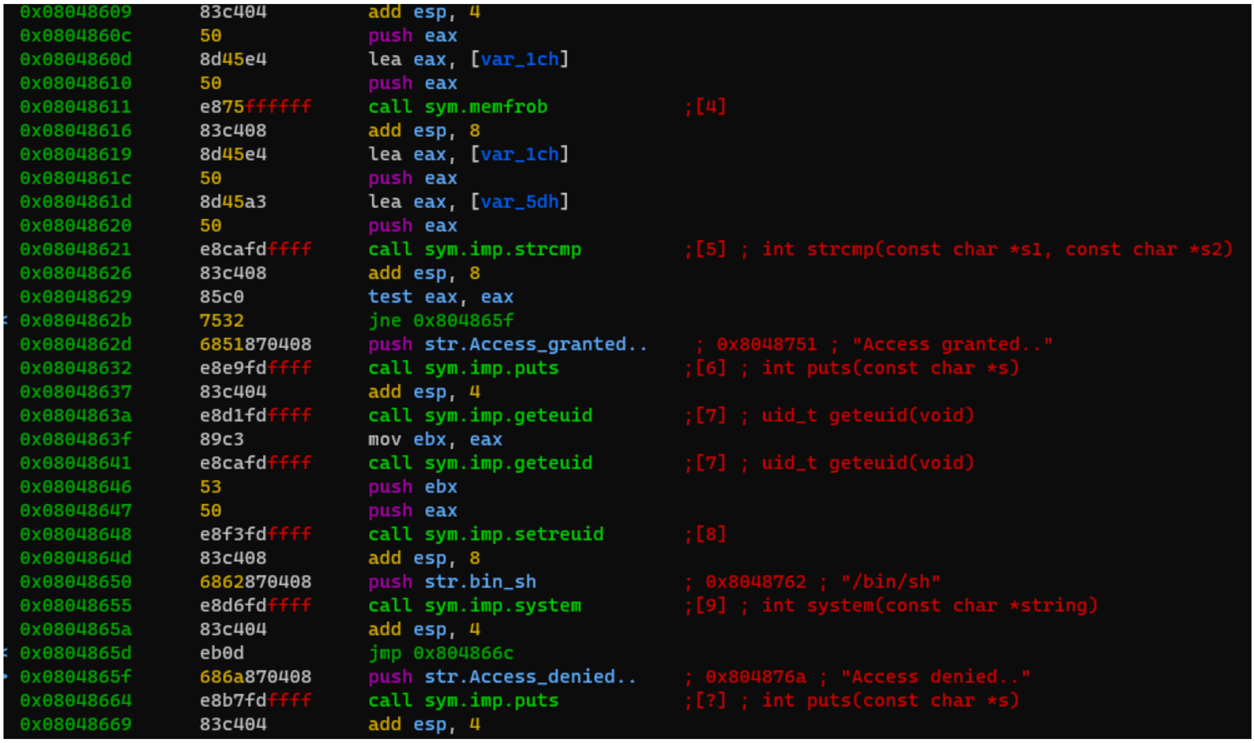


```
behemoth0@behemoth:/behemoth$ ./behemoth0
Password: unixisbetterthanwindows
Access denied..
behemoth0@behemoth:/behemoth$ ./behemoth0
Password: followthewhiterabbit
Access denied..
behemoth0@behemoth:/behemoth$ ./behemoth0
Password: pacmanishighoncrack
Access denied..
```

behemoth0@behemoth:/behemoth$ r2 -d behemoth0

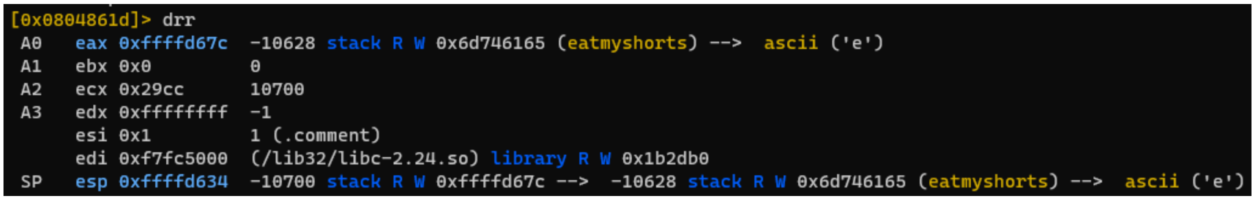
[0xf7fd9a20]> aaaaaa
The command “aaaaaa ” basically tells Radare2 to analyse the file.

[0xf7fd9a20]> s main
Go to function main (seek main)



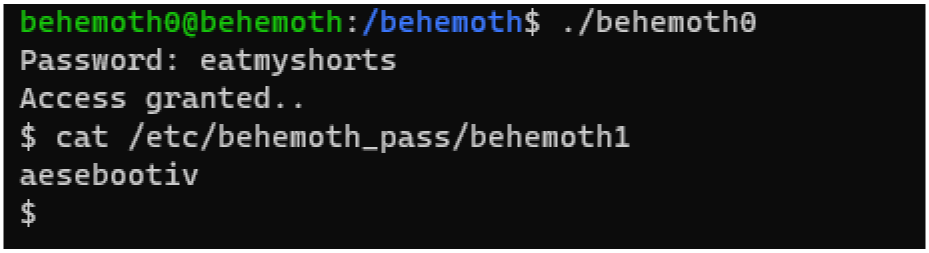
```
  0x08048609      83c404          add esp, 4
  0x0804860c      50              push eax
  0x0804860d      8d45e4          lea eax, [var_1ch]
  0x08048610      50              push eax
  0x08048611      e875ffffff      call sym.memfrob           ;[4]
  0x08048616      83c408          add esp, 8
  0x08048619      8d45e4          lea eax, [var_1ch]
  0x0804861c      50              push eax
  0x0804861d      8d45a3          lea eax, [var_5dh]
  0x08048620      50              push eax
  0x08048621      e8cafdffff      call sym.imp.strcmp        ;[5] ; int strcmp(const char *s1, const char *s2)
  0x08048626      83c408          add esp, 8
  0x08048629      85c0            test eax, eax
< 0x0804862b      7532            jne 0x804865f
  0x0804862d      6851870408      push str.Access_granted..   ; 0x8048751 ; "Access granted.."
  0x08048632      e8e9fdffff      call sym.imp.puts          ;[6] ; int puts(const char *s)
  0x08048637      83c404          add esp, 4
  0x0804863a      e8d1fdffff      call sym.imp.geteuid       ;[7] ; uid_t geteuid(void)
  0x0804863f      89c3            mov ebx, eax
  0x08048641      e8cafdffff      call sym.imp.geteuid       ;[7] ; uid_t geteuid(void)
  0x08048646      53              push ebx
  0x08048647      50              push eax
  0x08048648      e8f3fdffff      call sym.imp.setreuid      ;[8]
  0x0804864d      83c408          add esp, 8
  0x08048650      6862870408      push str.bin_sh            ; 0x8048762 ; "/bin/sh"
  0x08048655      e8d6fdffff      call sym.imp.system        ;[9] ; int system(const char *string)
  0x0804865a      83c404          add esp, 4
< 0x0804865d      eb0d            jmp 0x804866c
> 0x0804865f      686a870408      push str.Access_denied..   ; 0x804876a ; "Access denied.."
  0x08048664      e8b7fdffff      call sym.imp.puts          ;[?] ; int puts(const char *s)
  0x08048669      83c404          add esp, 4
```

At 0x08048621 the function strcmp is being called and the variable [var_5dh] is being passed into it.
[0x080485db] db 0x804861d



```
[0x0804861d]> drr
 A0    eax 0xffffd67c  -10628 stack R W 0x6d746165 (eatmyshorts) -->  ascii ('e')
 A1    ebx 0x0         0
 A2    ecx 0x29cc      10700
 A3    edx 0xffffffff  -1
       esi 0x1         1 (.comment)
       edi 0xf7fc5000  (/lib32/libc-2.24.so) library R W 0x1b2db0
 SP    esp 0xffffd634  -10700 stack R W 0xffffd67c -->  -10628 stack R W 0x6d746165 (eatmyshorts) -->  ascii ('e')
```

The string “eatmyshorts” passed into the function strcmp



```
behemoth0@behemoth:/behemoth$ ./behemoth0
Password: eatmyshorts
Access granted..
$ cat /etc/behemoth_pass/behemoth1
aesebootiv
$
```

The password for the behemoth1@behemoth.labs.overthewire.org is aesebootiv