

- a. 如果用 gdb 的话，没有影响。

```
Applications ▾ Places ▾ Terminal ▾ Mon 12:41
root@kali-WSU: ~/Desktop/Lab2-BufferOverflows

File Edit View Search Terminal Help
gcc: error: -g: No such file or directory
gcc: error: -fno-stack-protector: No such file or directory
gcc: error: -O: No such file or directory
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ls
badfile BOF BOF.c createBadfile.c test testShellCode.c
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gcc -g -fno-stack-protector BOF.c -o BOF
gcc: error: -g: No such file or directory
gcc: error: -fno-stack-protector: No such file or directory
gcc: error: -O: No such file or directory
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gcc -g -z execstack -fno-stack-protector BOF.c -o BOF
gcc: error: -g: No such file or directory
gcc: error: -z: No such file or directory
gcc: error: execstack: No such file or directory
gcc: error: -fno-stack-protector: No such file or directory
gcc: error: -O: No such file or directory
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gcc -g -fno-stack-protector BOF.c -o BOF
gcc: error: -g: No such file or directory
gcc: error: -fno-stack-protector: No such file or directory
gcc: error: -O: No such file or directory
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gcc
gcc: fatal error: no input files
compilation terminated.
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gcc -g -fno-stack-protector BOF.c -o BOF
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gdb BOF
GNU gdb (Debian 7.7.1-dfsg-5) 7.7.1
Copyright (C) 2014 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 "i586-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 BOF...done.
(gdb) run
Starting program: /root/Desktop/Lab2-BufferOverflows/BOF
Buffer overflow vulnerability starting up...

Program received signal SIGSEGV, Segmentation fault.
0xbffff228 in ?? ()
(gdb)
```

- b. 返回地址没有变化。

```
Applications ▾ Places ▾ Terminal ▾ Mon 12:49
root@kali-WSU: ~/Desktop/Lab2-BufferOverflows

File Edit View Search Terminal Help
ca-certificates foremost.conf inetd.conf machchanger openc1 reaver stunnel x11
ca-certificates.conf fragroute.conf inetsim machine-id opensc subgid xdg
calendar freetds init magic mailcap opt redsocks.conf subgid xdm
chkscrip ftno init.d magic.e1ne mailcap opt reportbug.conf subuid xpdf
chkrootkit.conf ftpchroot inputrc mailcap.order os-release request-key.d subversion xprobe2
cisco-torch fuse.conf inserv mailrc nampath.config rpm sysctl.conf sudoers
console-setup gpi.conf inserv.conf mailrc nampath.config rpm sysctl.conf sudoers
cracklib gpi.conf inserv.conf mailrc nampath.config rpm sysctl.conf sudoers
cron.d gconf iproute2 m4 matplotlibrc passw rsyslog.conf systemd
cron.daily glib iscsi mc
cron.hourly glib iscsi mc
root@kali-WSU:/etc# cd sys
sysctl.d/ systemd/
root@kali-WSU:/etc# cd sys
sysctl.d/ systemd/
root@kali-WSU:/etc# cd sysctl.d/
root@kali-WSU:/etc/sysctl.d# ls
01-disable-aslr.conf 30-postgresql-sys.conf 30-tracker.conf 99-sysctl.conf README.sysctl uhd-usrp2.conf
root@kali-WSU:/etc/sysctl.d# cat 01-disable-aslr.conf
kernel.randomize_va_space=0
root@kali-WSU:/etc/sysctl.d# cd -
root@kali-WSU:~/Desktop/Lab2-BufferOverflows/
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ls
badfile BOF BOF.c createBadfile.c q! test testShellCode.c
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gcc -g -z execstack -fno-stack-protector BOF.c -o BOF
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gdb BOF
GNU gdb (Debian 7.7.1-dfsg-5) 7.7.1
Copyright (C) 2014 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 "i586-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 BOF...done.
(gdb) run
Starting program: /root/Desktop/Lab2-BufferOverflows/BOF
Buffer overflow vulnerability starting up...
process 11990 is executing new program: /bin/dash
#
```

- c. 改变了。

```
Applications ▾ Places ▾ $ -Terminal ▾ Sun 09:09 1 [ ] [ ] [ ]
root@kali-WSU: ~/Desktop/Lab2-BufferOverflows
File Edit View Search Terminal Help
ows/ Lab2-
root@kali-WSU:/home/csc5991-student/Desktop/Lab2-BufferOverflows# ls
BOF.c createBadfile.c testShellCode.c
root@kali-WSU:/home/csc5991-student/Desktop/Lab2-BufferOverflows# cd /
root@kali-WSU:/# ls
0 boot etc initrd.img live-build media opt root sbin sys usr vmlinuz
bin dev home lib lost+found mnt proc run srv tmp var
root@kali-WSU:/# cd root
bash: cd: root: No such file or directory
root@kali-WSU:/# cd root
root@kali-WSU:~# ls
Desktop Pictures randomize_va_spact~ randomize_va_spacx~ Videos
Documents Public randomize_va_spacu~ randomize_va_spacy~
Downloads randomize_va_space~ randomize_va_spacv~ randomize_va_spacz~
Music randomize_va_spacs~ randomize_va_spacw~ Templates
root@kali-WSU:~# cd Desktop/
root@kali-WSU:~/Desktop# ls
Lab2-BufferOverflows
root@kali-WSU:~/Desktop# cd Lab2-BufferOverflows/
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ls
badfile BOF BOF.c createBadfile.c q! test testShellCode.c
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ./BOF
Buffer overflow vulnerability starting up...
Segmentation fault
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# /root/Desktop/Lab2-BufferOverflows/BOF
Buffer overflow vulnerability starting up...
Segmentation fault
root@kali-WSU:~/Desktop/Lab2-BufferOverflows#
```