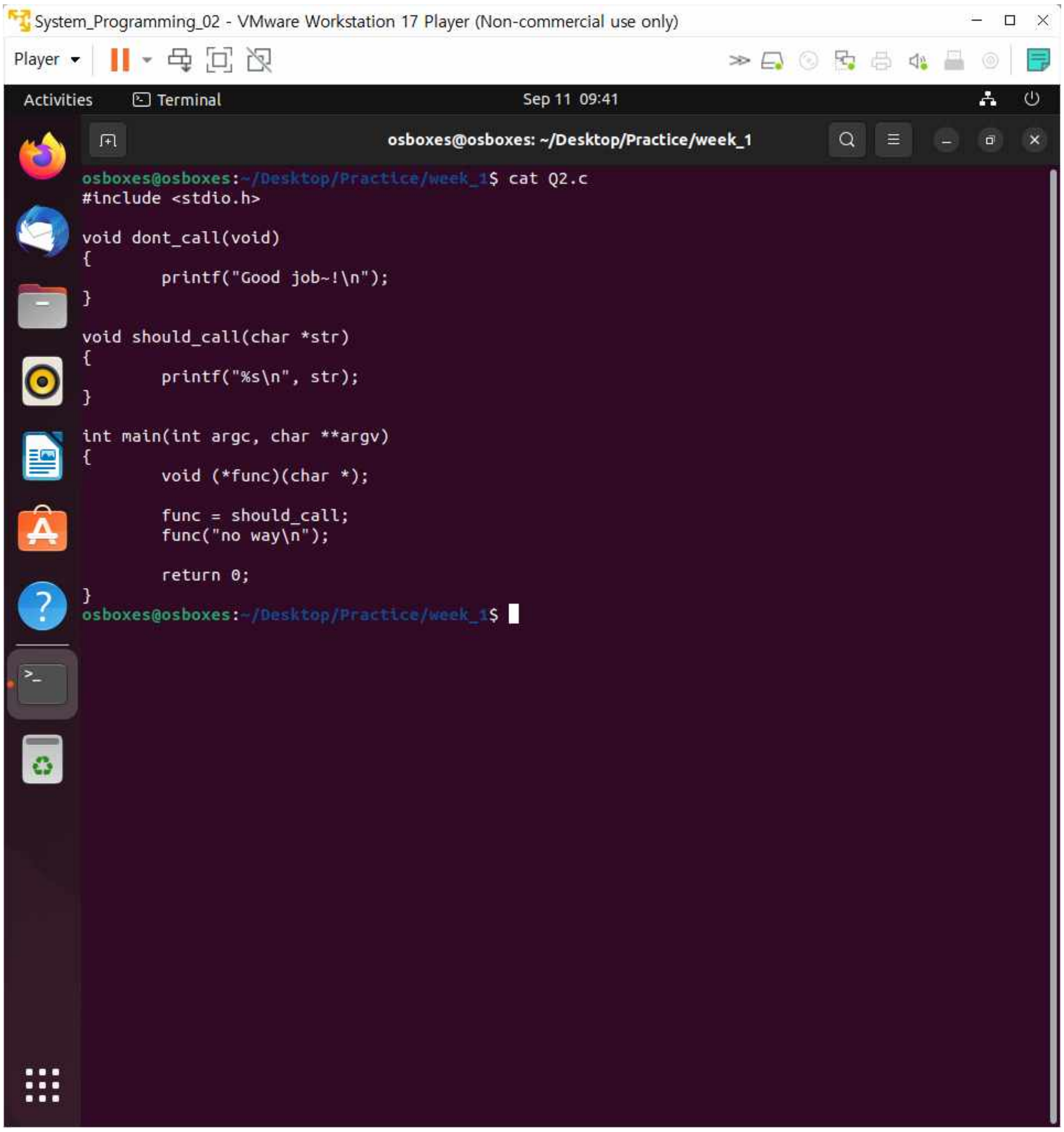
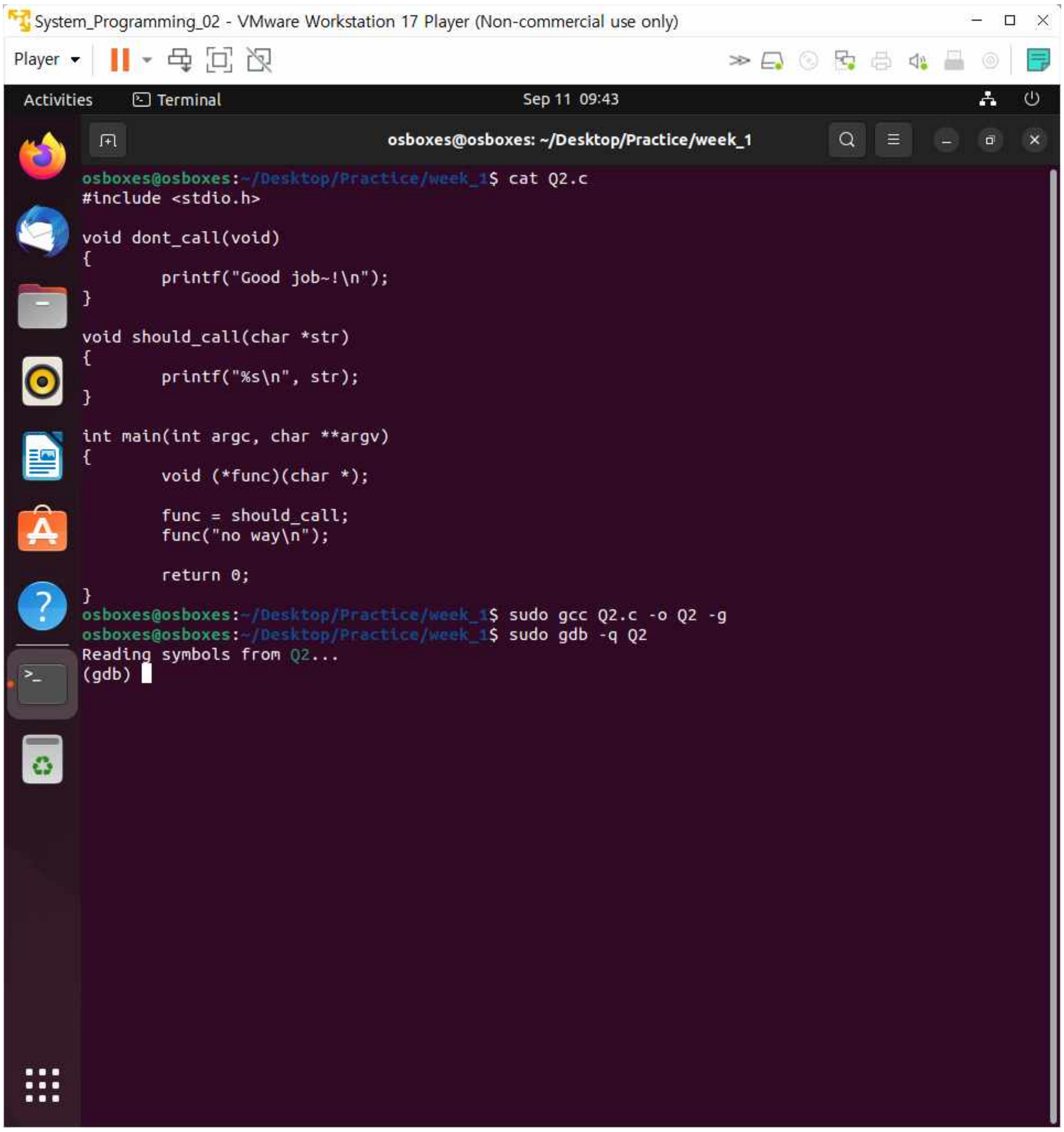
1. Q2.c의 내용



System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:41
osboxes@osboxes: ~/Desktop/Practice/week_1

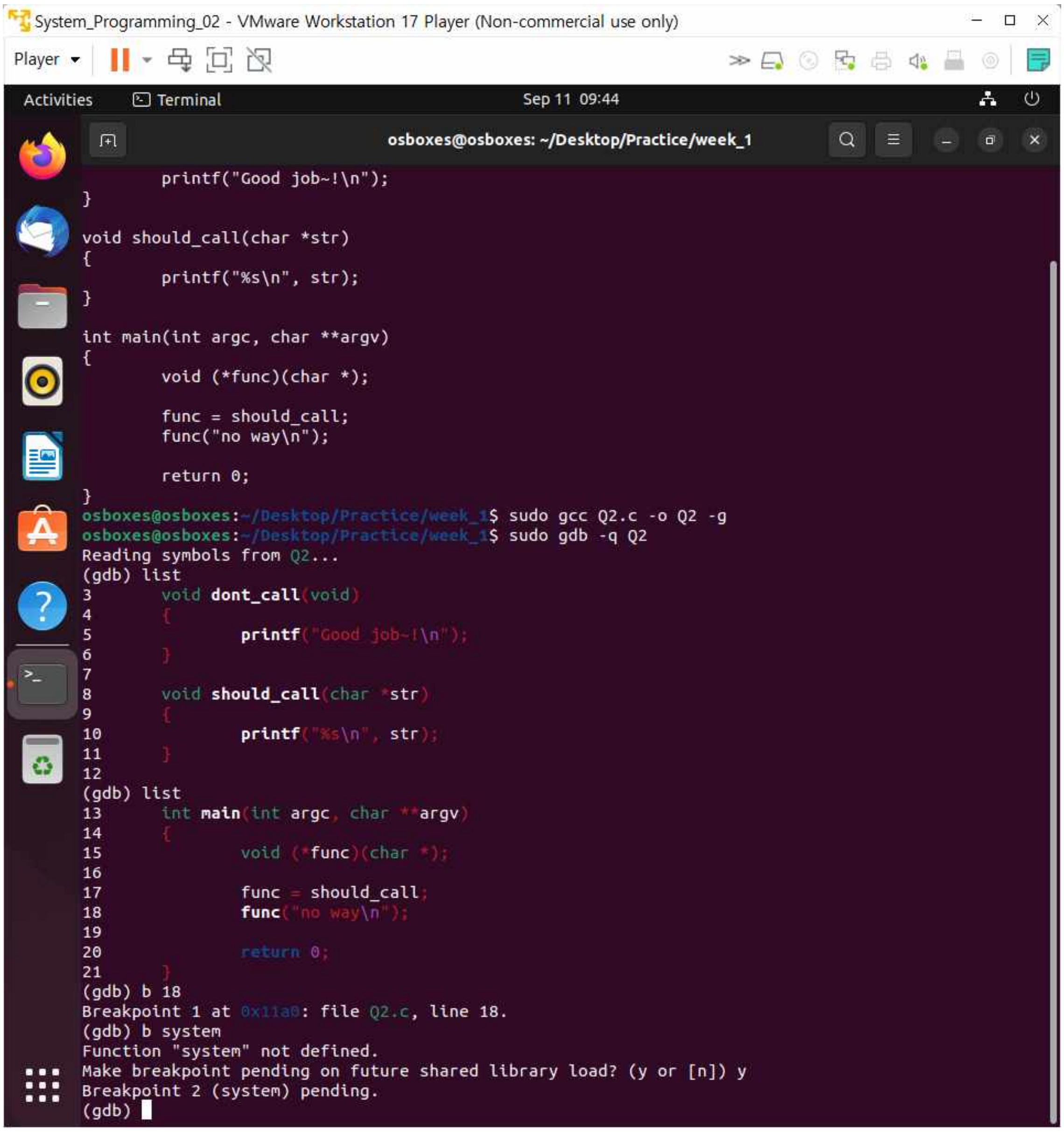
```
osboxes@osboxes:~/Desktop/Practice/week_1$ cat Q2.c
#include <stdio.h>

void dont_call(void)
{
        printf("Good job~!\n");
}

void should_call(char *str)
{
        printf("%s\n", str);
}

int main(int argc, char **argv)
{
        void (*func)(char *);

        func = should_call;
        func("no way\n");

        return 0;
}
osboxes@osboxes:~/Desktop/Practice/week_1$ 
```

2. Q2.c의 디버깅 정보를 포함하여 컴파일 후 gdb실행


System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:43
osboxes@osboxes: ~/Desktop/Practice/week_1

```
osboxes@osboxes:~/Desktop/Practice/week_1$ cat Q2.c
#include <stdio.h>

void dont_call(void)
{
        printf("Good job~!\n");
}

void should_call(char *str)
{
        printf("%s\n", str);
}

int main(int argc, char **argv)
{
        void (*func)(char *);

        func = should_call;
        func("no way\n");

        return 0;
}
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gcc Q2.c -o Q2 -g
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gdb -q Q2
Reading symbols from Q2...
(gdb) 
```

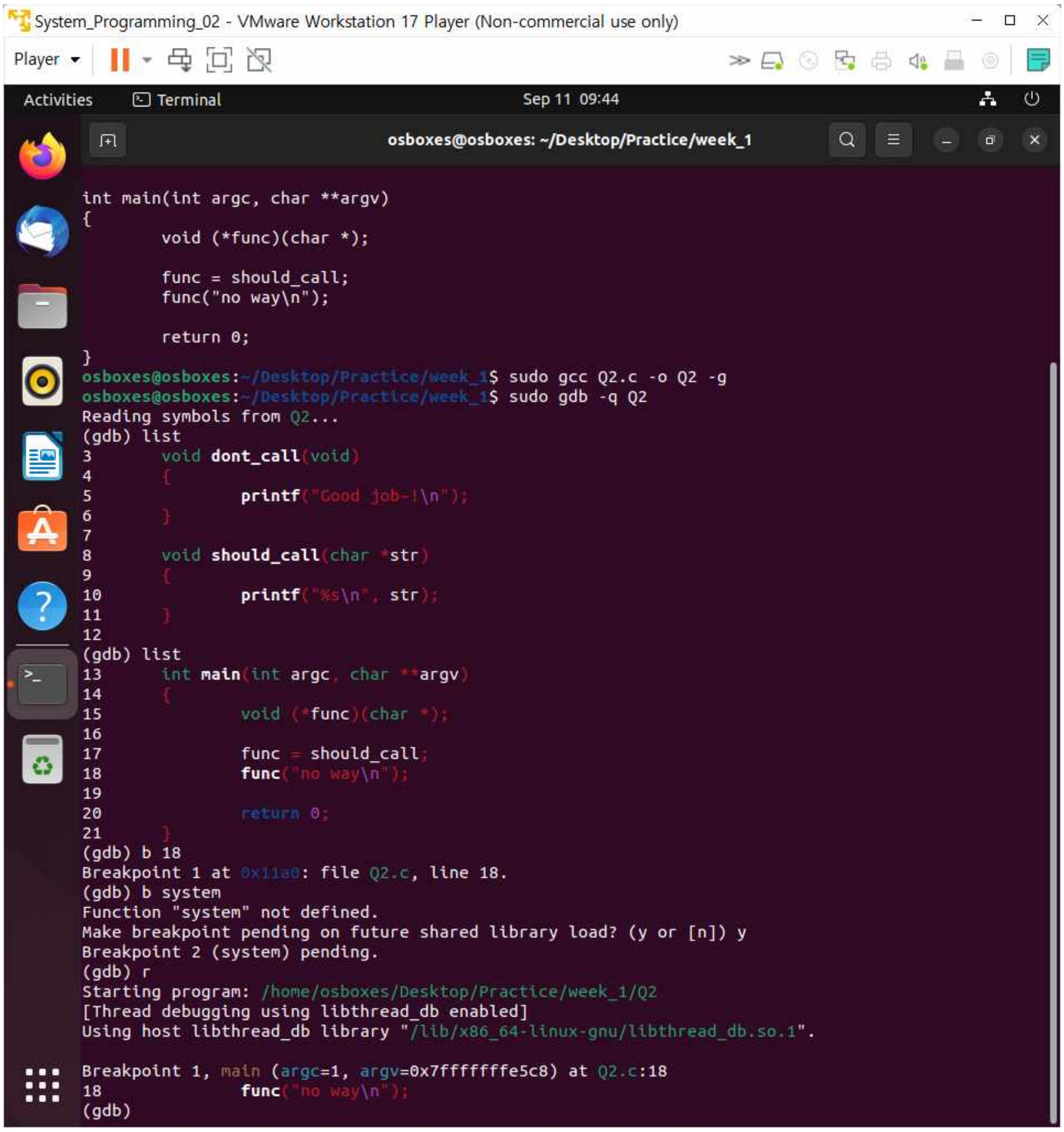
3. 18번 라인의 func실행 라인과 system함수에 breakpoint를 설정한다



System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:44
osboxes@osboxes: ~/Desktop/Practice/week_1

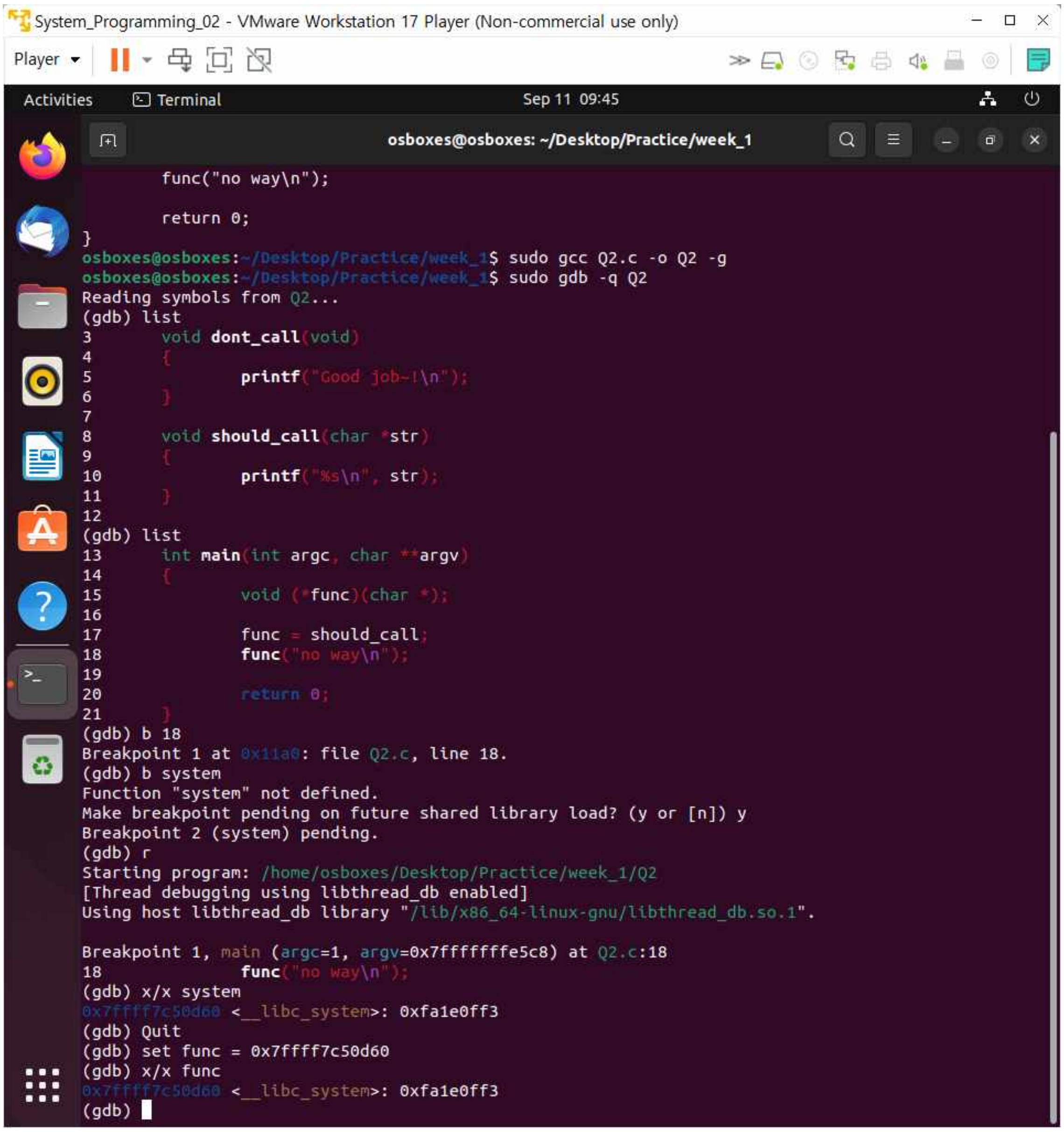
```
        printf("Good job~!\n");
}

void should_call(char *str)
{
        printf("%s\n", str);
}

int main(int argc, char **argv)
{
        void (*func)(char *);

        func = should_call;
        func("no way\n");

        return 0;
}
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gcc Q2.c -o Q2 -g
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gdb -q Q2
Reading symbols from Q2...
(gdb) list
3       void dont_call(void)
4       {
5               printf("Good job~!\n");
6       }
7
8       void should_call(char *str)
9       {
10              printf("%s\n", str);
11      }
12
(gdb) list
13      int main(int argc, char **argv)
14      {
15              void (*func)(char *);
16
17              func = should_call;
18              func("no way\n");
19
20              return 0;
21      }
(gdb) b 18
Breakpoint 1 at 0x11a0: file Q2.c, line 18.
(gdb) b system
Function "system" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 2 (system) pending.
(gdb) 
```

4. r로 시작


System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:44
osboxes@osboxes: ~/Desktop/Practice/week_1

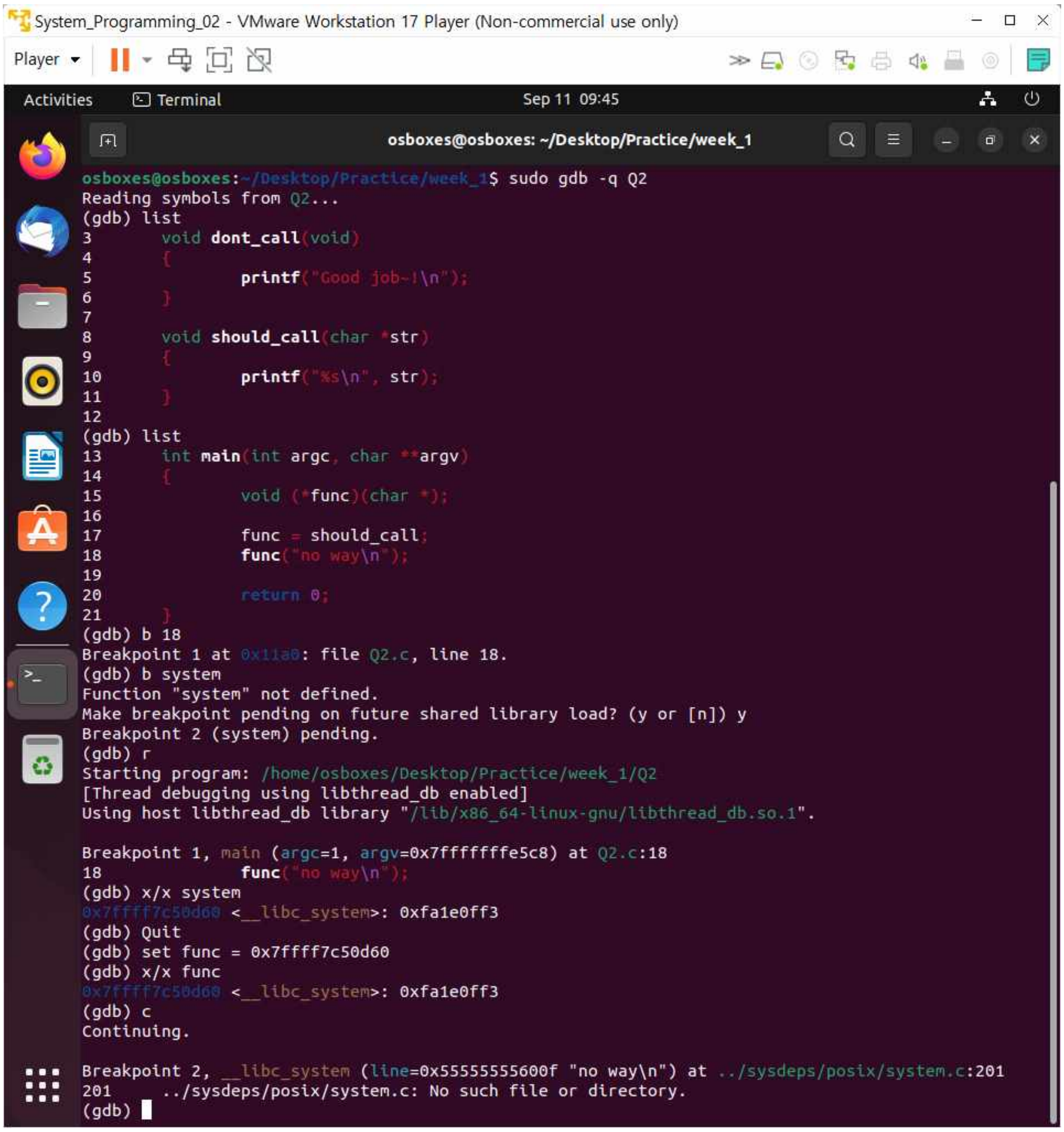
```
int main(int argc, char **argv)
{
        void (*func)(char *);

        func = should_call;
        func("no way\n");

        return 0;
}
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gcc Q2.c -o Q2 -g
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gdb -q Q2
Reading symbols from Q2...
(gdb) list
3       void dont_call(void)
4       {
5               printf("Good job~!\n");
6       }
7
8       void should_call(char *str)
9       {
10              printf("%s\n", str);
11      }
12
(gdb) list
13      int main(int argc, char **argv)
14      {
15              void (*func)(char *);
16
17              func = should_call;
18              func("no way\n");
19
20              return 0;
21      }
(gdb) b 18
Breakpoint 1 at 0x11a0: file Q2.c, line 18.
(gdb) b system
Function "system" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 2 (system) pending.
(gdb) r
Starting program: /home/osboxes/Desktop/Practice/week_1/Q2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main (argc=1, argv=0x7fffffffe5c8) at Q2.c:18
18              func("no way\n");
(gdb)
```

5. func함수를 system함수로 변경


System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:45
osboxes@osboxes: ~/Desktop/Practice/week_1

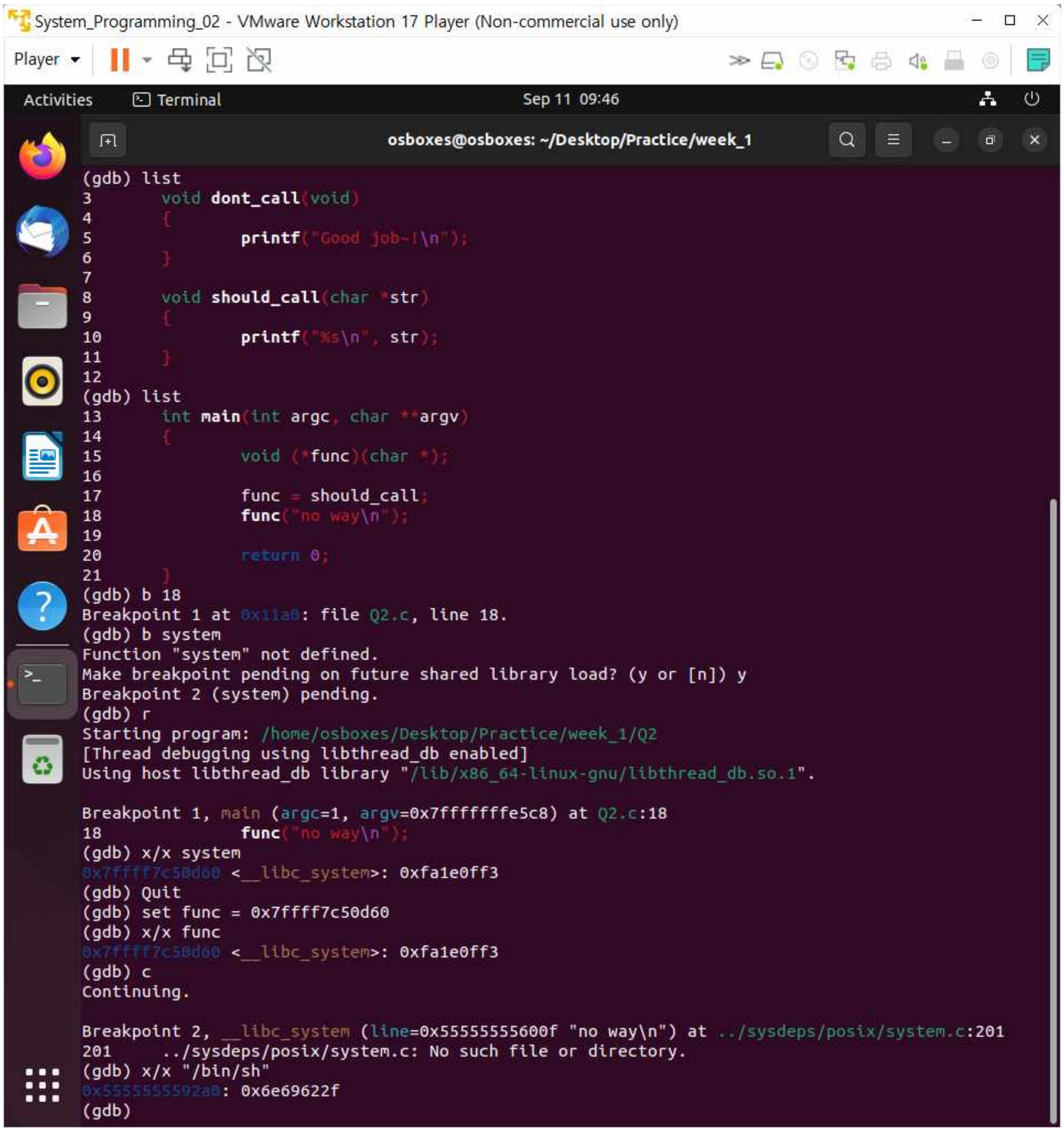
```
        func("no way\n");

        return 0;
}
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gcc Q2.c -o Q2 -g
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gdb -q Q2
Reading symbols from Q2...
(gdb) list
3       void dont_call(void)
4       {
5               printf("Good job~!\n");
6       }
7
8       void should_call(char *str)
9       {
10              printf("%s\n", str);
11      }
12
(gdb) list
13      int main(int argc, char **argv)
14      {
15              void (*func)(char *);
16
17              func = should_call;
18              func("no way\n");
19
20              return 0;
21      }
(gdb) b 18
Breakpoint 1 at 0x11a0: file Q2.c, line 18.
(gdb) b system
Function "system" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 2 (system) pending.
(gdb) r
Starting program: /home/osboxes/Desktop/Practice/week_1/Q2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main (argc=1, argv=0x7fffffffe5c8) at Q2.c:18
18              func("no way\n");
(gdb) x/x system
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) Quit
(gdb) set func = 0x7ffff7c50d60
(gdb) x/x func
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) 
```

6. c로 계속


System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:45
osboxes@osboxes: ~/Desktop/Practice/week_1

```
osboxes@osboxes:~/Desktop/Practice/week_1$ sudo gdb -q Q2
Reading symbols from Q2...
(gdb) list
3       void dont_call(void)
4       {
5               printf("Good job~!\n");
6       }
7
8       void should_call(char *str)
9       {
10              printf("%s\n", str);
11      }
12
(gdb) list
13      int main(int argc, char **argv)
14      {
15              void (*func)(char *);
16
17              func = should_call;
18              func("no way\n");
19
20              return 0;
21      }
(gdb) b 18
Breakpoint 1 at 0x11a0: file Q2.c, line 18.
(gdb) b system
Function "system" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 2 (system) pending.
(gdb) r
Starting program: /home/osboxes/Desktop/Practice/week_1/Q2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main (argc=1, argv=0x7fffffffe5c8) at Q2.c:18
18              func("no way\n");
(gdb) x/x system
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) Quit
(gdb) set func = 0x7ffff7c50d60
(gdb) x/x func
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) c
Continuing.

Breakpoint 2, __libc_system (line=0x55555555600f "no way\n") at ../sysdeps/posix/system.c:201
201     ../sysdeps/posix/system.c: No such file or directory.
(gdb) 
```

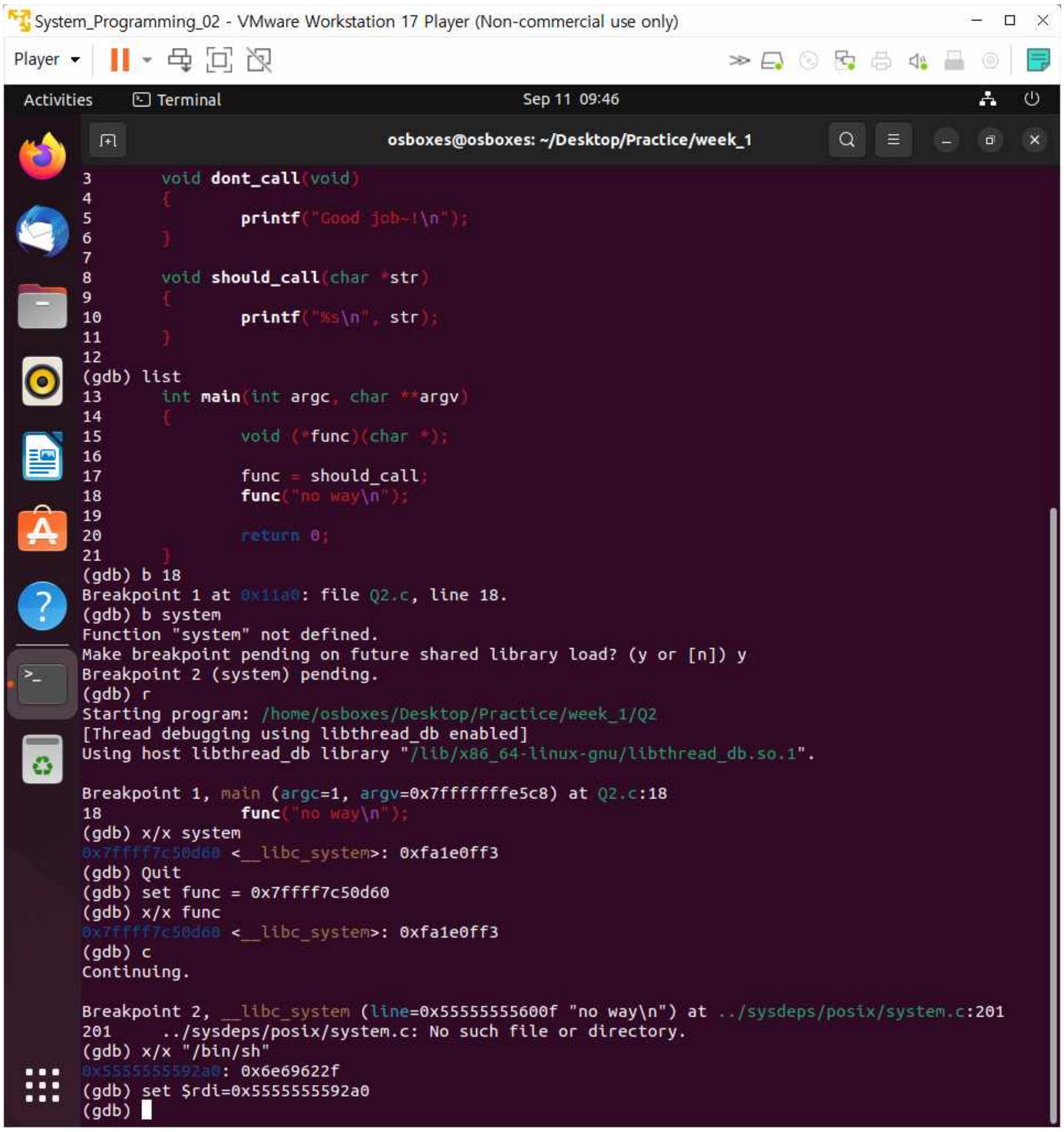
7. "/bin/sh"문자열의 16진 주소값을 복사한다



System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:46
osboxes@osboxes: ~/Desktop/Practice/week_1

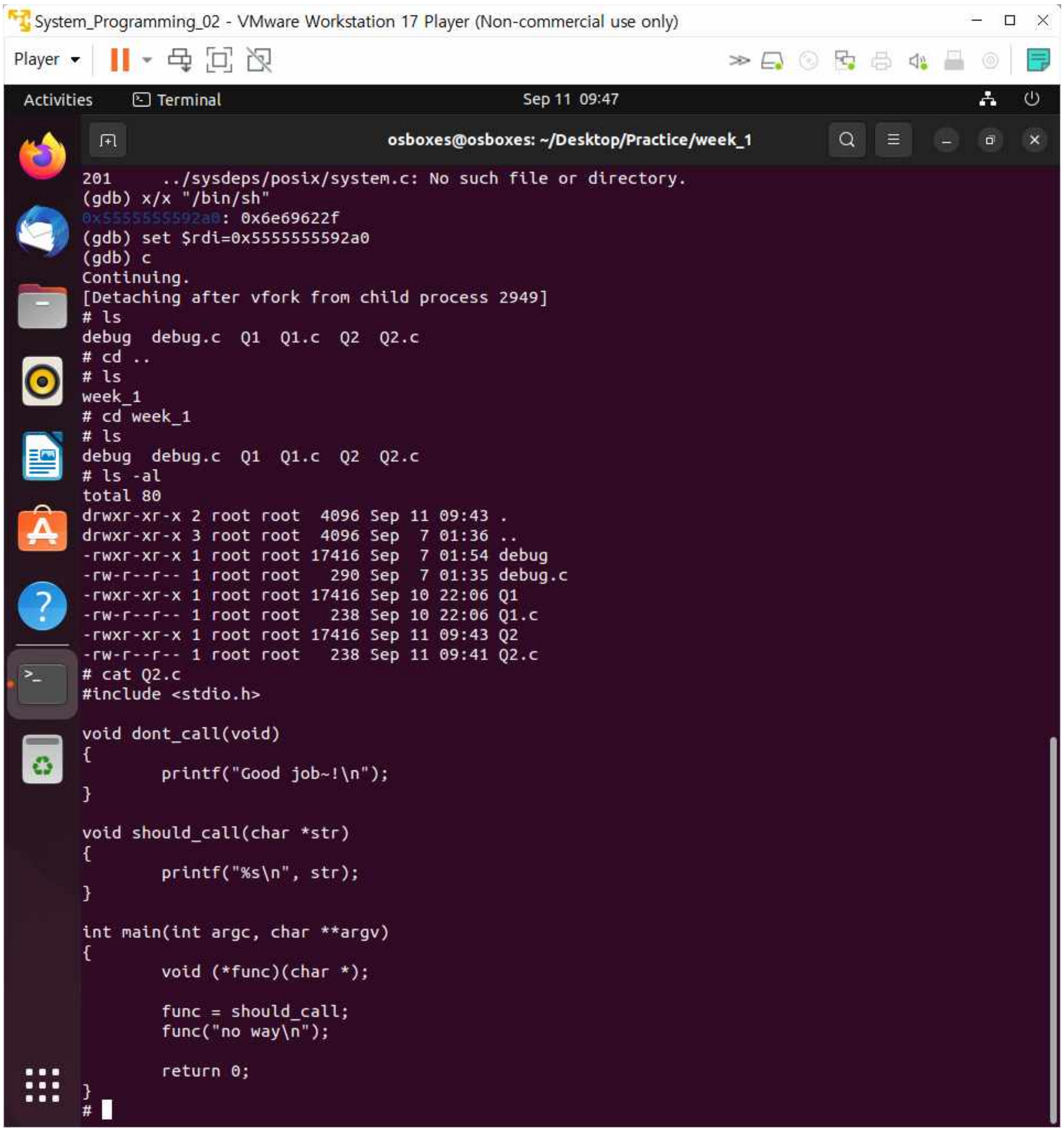
```
(gdb) list
3       void dont_call(void)
4       {
5               printf("Good job~!\n");
6       }
7
8       void should_call(char *str)
9       {
10              printf("%s\n", str);
11      }
12
(gdb) list
13      int main(int argc, char **argv)
14      {
15              void (*func)(char *);
16
17              func = should_call;
18              func("no way\n");
19
20              return 0;
21      }
(gdb) b 18
Breakpoint 1 at 0x11a0: file Q2.c, line 18.
(gdb) b system
Function "system" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 2 (system) pending.
(gdb) r
Starting program: /home/osboxes/Desktop/Practice/week_1/Q2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main (argc=1, argv=0x7fffffffe5c8) at Q2.c:18
18              func("no way\n");
(gdb) x/x system
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) Quit
(gdb) set func = 0x7ffff7c50d60
(gdb) x/x func
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) c
Continuing.

Breakpoint 2, __libc_system (line=0x55555555600f "no way\n") at ../sysdeps/posix/system.c:201
201     ../sysdeps/posix/system.c: No such file or directory.
(gdb) x/x "/bin/sh"
0x5555555592a0: 0x6e69622f
(gdb)
```

8. rdi레지스터의 값을 "/bin/sh"문자열의 주소값으로 변경한다


System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:46
osboxes@osboxes: ~/Desktop/Practice/week_1

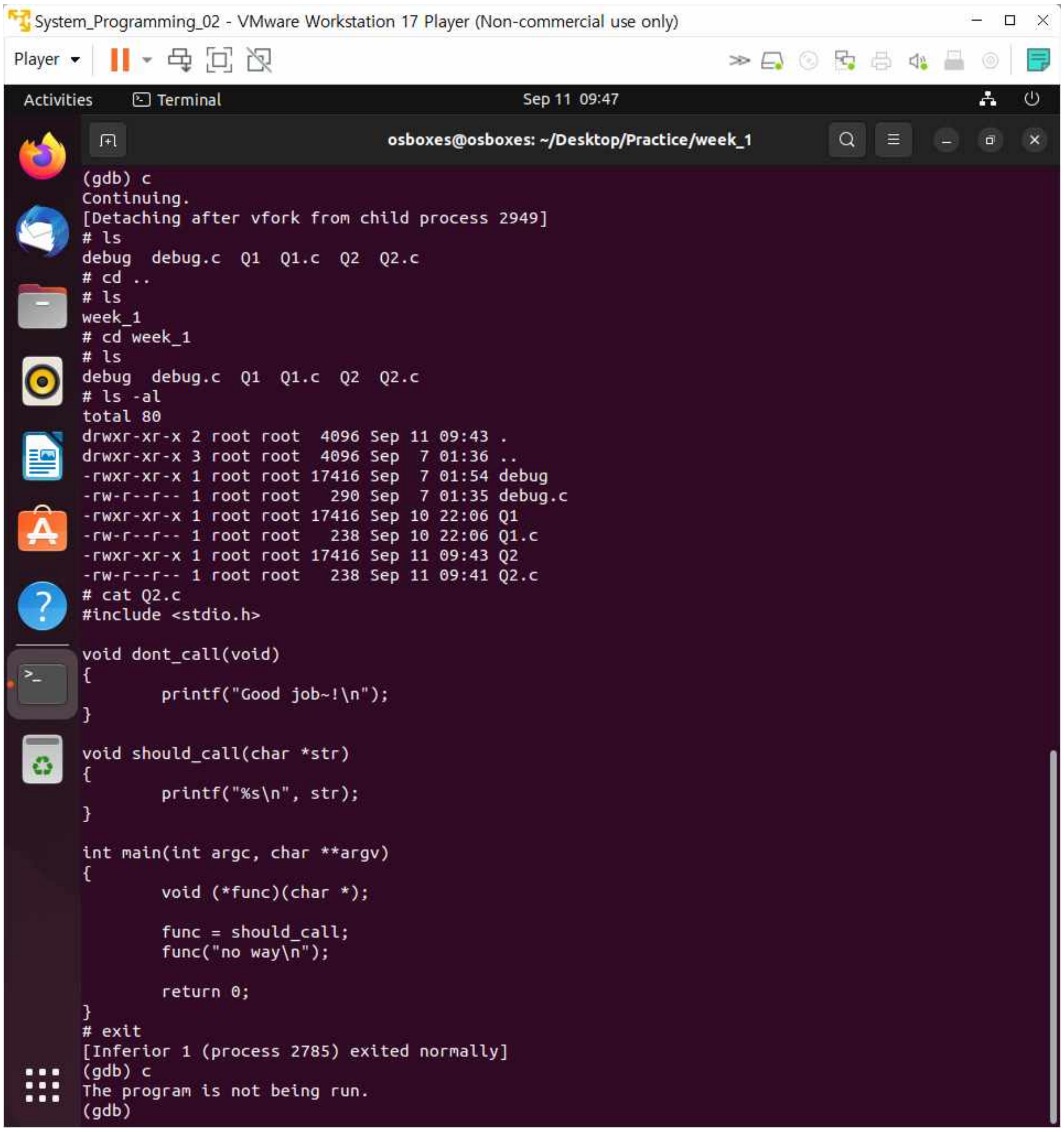
```
3       void dont_call(void)
4       {
5               printf("Good job~!\n");
6       }
7
8       void should_call(char *str)
9       {
10              printf("%s\n", str);
11      }
12
(gdb) list
13      int main(int argc, char **argv)
14      {
15              void (*func)(char *);
16
17              func = should_call;
18              func("no way\n");
19
20              return 0;
21      }
(gdb) b 18
Breakpoint 1 at 0x11a0: file Q2.c, line 18.
(gdb) b system
Function "system" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 2 (system) pending.
(gdb) r
Starting program: /home/osboxes/Desktop/Practice/week_1/Q2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main (argc=1, argv=0x7fffffffe5c8) at Q2.c:18
18              func("no way\n");
(gdb) x/x system
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) Quit
(gdb) set func = 0x7ffff7c50d60
(gdb) x/x func
0x7ffff7c50d60 <__libc_system>: 0xfa1e0ff3
(gdb) c
Continuing.

Breakpoint 2, __libc_system (line=0x55555555600f "no way\n") at ../sysdeps/posix/system.c:201
201     ../sysdeps/posix/system.c: No such file or directory.
(gdb) x/x "/bin/sh"
0x5555555592a0: 0x6e69622f
(gdb) set $rdi=0x5555555592a0
(gdb) 
```

9. c를 눌러 계속하면 셸이 실행된다


System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:47
osboxes@osboxes: ~/Desktop/Practice/week_1

```
201     ../sysdeps/posix/system.c: No such file or directory.
(gdb) x/x "/bin/sh"
0x5555555592a0: 0x6e69622f
(gdb) set $rdi=0x5555555592a0
(gdb) c
Continuing.
[Detaching after vfork from child process 2949]
# ls
debug  debug.c  Q1  Q1.c  Q2  Q2.c
# cd ..
# ls
week_1
# cd week_1
# ls
debug  debug.c  Q1  Q1.c  Q2  Q2.c
# ls -al
total 80
drwxr-xr-x 2 root root  4096 Sep 11 09:43 .
drwxr-xr-x 3 root root  4096 Sep  7 01:36 ..
-rwxr-xr-x 1 root root 17416 Sep  7 01:54 debug
-rw-r--r-- 1 root root   290 Sep  7 01:35 debug.c
-rwxr-xr-x 1 root root 17416 Sep 10 22:06 Q1
-rw-r--r-- 1 root root   238 Sep 10 22:06 Q1.c
-rwxr-xr-x 1 root root 17416 Sep 11 09:43 Q2
-rw-r--r-- 1 root root   238 Sep 11 09:41 Q2.c
# cat Q2.c
#include <stdio.h>

void dont_call(void)
{
        printf("Good job~!\n");
}

void should_call(char *str)
{
        printf("%s\n", str);
}

int main(int argc, char **argv)
{
        void (*func)(char *);

        func = should_call;
        func("no way\n");

        return 0;
}
# 
```

10. exit을 입력하여 나간다


System_Programming_02 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Sep 11 09:47
osboxes@osboxes: ~/Desktop/Practice/week_1

```
(gdb) c
Continuing.
[Detaching after vfork from child process 2949]
# ls
debug  debug.c  Q1  Q1.c  Q2  Q2.c
# cd ..
# ls
week_1
# cd week_1
# ls
debug  debug.c  Q1  Q1.c  Q2  Q2.c
# ls -al
total 80
drwxr-xr-x 2 root root  4096 Sep 11 09:43 .
drwxr-xr-x 3 root root  4096 Sep  7 01:36 ..
-rwxr-xr-x 1 root root 17416 Sep  7 01:54 debug
-rw-r--r-- 1 root root   290 Sep  7 01:35 debug.c
-rwxr-xr-x 1 root root 17416 Sep 10 22:06 Q1
-rw-r--r-- 1 root root   238 Sep 10 22:06 Q1.c
-rwxr-xr-x 1 root root 17416 Sep 11 09:43 Q2
-rw-r--r-- 1 root root   238 Sep 11 09:41 Q2.c
# cat Q2.c
#include <stdio.h>

void dont_call(void)
{
        printf("Good job~!\n");
}

void should_call(char *str)
{
        printf("%s\n", str);
}

int main(int argc, char **argv)
{
        void (*func)(char *);

        func = should_call;
        func("no way\n");

        return 0;
}
# exit
[Inferior 1 (process 2785) exited normally]
(gdb) c
The program is not being run.
(gdb)
```