

## **Exercise- 5**

### **Perform Linux Code injection on a live process with ptrace**

**Aim:**

To do process code injection on Firefox using ptrace system call.

**Algorithm:**

1. Find out the pid of the running Firefox program.
2. Create the code injection file.
3. Get the pid of the Firefox from the command line arguments.
4. Allocate memory buffers for the shellcode.
5. Attach to the victim process with PTRACE\_ATTACH.
6. Get the register values of the attached process.
7. Use PTRACE\_POKETEXT to insert the shellcode.
8. Detach from the victim process using PTRACE\_DETACH

**Output:**

```
[root@localhost ~]# vi codeinjection.c
[root@localhost ~]# gcc codeinjection.c -o codeinject
[root@localhost ~]#ps -e|grep firefox
1433 ? 00:01:23 firefox
[root@localhost ~]# ./codeinject
1433
----Memory bytecode
injector---- Writing EIP 0x6,
process 1707 [root@localhost
~]#
```

**Result:**

Thus, the process code injection on Firefox has been successfully executed.