./level0

In the home directories of the **users** in the **Rainfall** project, each user possesses an **executable file** formatted as **ELF 32-bit**. To transfer these files to our local system, we consistently utilized the **scp** command with the following syntax:

```
scp -P 4242 user@192.168.xxx.xxx:filename localfilename
```

We decompiled each file with ***Ghidra***. Given that the direct translation from **assembly** can be nebulous at times, we took the liberty of renaming variables and making slight code adjustments for better readability.

In the different levels of the project, every time we establish an **SSH** connection to a **levelx** user, the terminal presents us with a comprehensive list of security protections:

GCC Stack Protector: If there is a canary on the stack and it changes, the program exits, preventing exploits to defend against stack buffer overflows.

Strict User Copy Checks: Bolsters kernel security by adding checks during data transfers between user and kernel space, averting unsafe transfers.

Restrict /dev/mem | /dev/kmem: Limits direct memory access from user-space, reducing certain attack vectors.

grsecurity / PaX: A comprehensive Linux kernel security patch, incorporating exploit mitigations like address space protection.

Kernel Heap Hardening (KERNHEAP): Enhances kernel heap security, making heap exploit attempts harder.

System-wide ASLR: Shuffles memory addresses of system processes, increasing unpredictability and thwarting attacks that rely on specific memory locations.

RELRO: Ensures certain memory sections, including the Global Offset Table, are read-only post program initialization, making overwrites tough.

STACK CANARY: any small random value placed on the stack to detect buffer overflows. If a buffer overflow occurs, the canary value will likely be overwritten

NX (No-eXecute): A CPU feature that designates memory areas as non-executable, hindering exploits relying on executing code from these regions.

PIE: Allows executables to operate at various memory addresses, enhancing memory unpredictability when paired with ASLR.

RPATH/RUNPATH: ELF binary attributes dictating dynamic library search paths. Misconfigurations can lead to library hijacking.

./level0²

```c
int main(int argc, char **argv)
{
    int input_val = atoi(argv[1]);

    if (input_val == 423)
    {
        char *cmd = strdup("/bin/sh");

        __gid_t egid = getegid();
        __uid_t euid = geteuid();

        setresgid(egid, egid, egid);
        setresuid(euid, euid, euid);

        execv("/bin/sh", &cmd);
    }
    else
        fwrite("No !\n", 1, 5, stderr);

    return 0;
}
```

To successfully enter the conditional **if** statement in the code, the program must receive 423 as its first argument.

If this condition is met, the program spawns a **shell** that allows us to operate with the permissions of **level1**.

```
level0@RainFall:~$ ./level0 423

$ whoami
level1

$ cat /home/user/level1/.pass
1fe8a524fa4bec01ca4ea2a869af2a02260d4a7d5fe7e7c24d8617e6dca12d3a

$ su level1
Password: 1fe8a524fa4bec01ca4ea2a869af2a02260d4a7d5fe7e7c24d8617e6dca12d3a

level1@RainFall:~$
```