Université Gustave Eiffel

ESIEE PARIS

TP - Buffer Overflow

Hadrien Barral

revision 1.3

Exercise

Code

```c
#include <stdio.h>
#include <stdlib.h>

#pragma GCC diagnostic ignored "-Wimplicit-function-declaration"

[[gnu::noinline]]
void secret_function(void)
{
    printf("You are now in the secret function.\n");
    printf("Congratulations, you have solved this question!\n");
    exit(0);
}

[[gnu::noinline]]
int horribly_vulnerable(void) {
    char array[400];
    printf("Enter some wonderful text:\n");
    gets(array);
    printf("FYI, your input was: '%s'\n", array);
    return 0;
}

int main(void) {
    horribly_vulnerable();
    return 0;
}
```

Questions

1. Identify the security issue
2. Disable ASLR: `echo 0 | sudo tee /proc/sys/kernel/randomize_va_space`
3. Compile the code: `gcc -O2 -fno-stack-protector -z execstack -o vuln -g vuln.c`
4. Craft an input which makes the program crash
5. Find out why the program crashes
6. Craft an input which makes the program jump to the `secret_function` function
7. Craft an input which turn the program into a shell
8. Remove `-fno-stack-protector`, then find out why your previous solution does not work anymore.
9. (Bonus, only if you have finished the previous questions) Remove `-z execstack`, and start again.