Setup Instructions for Kali

# Lower difficulty (TicTacToe.c)

This problem requires to be compiled to a binary executable with setuid permission, no stack protection and non-executable stack. ASLR must be disabled on the system.

1. Create a text file on the system.

$ touch /path/to/CoolKidzClub.txt

1. Set the permission of the file to ‘-rw-r--r--’

$ chmod 744 /path/to/CoolKidzClub.txt

1. Change the absolute file path accordingly on ‘TicTacToe.c’ at line 146
2. Compile the file using the following command.

$ gcc -g -fno-stack-protector /path/to/TicTacToe.c -o /path/to/TicTacToe

1. Enable ‘setuid’ on the compiled binary.
2. Ensure every user can use GDB.
3. Create a link to the compiled binary and text file to the home page of every user.

# Higher difficulty (TicTacTwo.c)

This problem is required to be compiled to a 32-bit binary executable with setuid permission, with stack protection and non-executable stack. ASLR must be disabled on the system.

1. Create a text file on the system.

$ touch /path/to/CoolerKidzClub.txt

1. Set the permission of the file to ‘-rw-r--r--’

$ chmod 744 /path/to/CoolerKidzClub.txt

1. Change the absolute file path accordingly on ‘TicTacTwo.c’ at line 147
2. Compile the file using the following command.

$ gcc -g -fstack-protector –m32 /path/to/TicTacTwo.c -o /path/to/TicTacTwo

1. Enable ‘setuid’ on the compiled binary.
2. Ensure ‘pwntools’ python library is installed.
3. Ensure every user can use GDB and Python.
4. Create a link to the compiled binary and text file to the home page of every user.

## Disabling ASLR

1. Open ‘sysctl.conf’ on a text editor.
2. Add the following line at the very end of the file. Save and exit the editor. kernel.randomize\_va\_space=0
3. Use the command to apply the changes immediately.

$ sudo sysctl -p