**Makefiles and Kernel Modules**

Make file is special file that contains objects and its target dependencies. Make is Unix utility that used for execution of makefile.It keeps track of the files that are changed (or updated).

If we do not use makefiles we will need to recompile entire project for changes made to even a single file. This is extremely inefficient as it involves recompiling hundreds of files.

In contrast, a makefile based approach only relies on the information from make. Only the changed file is recompiled and integrated into the project, which saves a great deal of time.

Kernel module is program that can be loaded or unloaded dynamically from kernel. Module can be loaded on the fly without recompiling it.

Without kernel module, adding new features to the kernel requires recompilation.

Further, it also takes a long time to compile as kernel size is large. Since kernel modules can be dynamically loaded and unloaded based on the requirement, memory can be used efficiently by the kernel.

We are using kernel module to load the secret into kernel space memory, which we then attack from user space programs.

Trapping Exceptions in C

In our Program we need to trap memory access violation error. C does not have any inbuilt exception handling mechanism. Hence, we write our own error handling utility.

Error handling utility is based on Signal concept. Interrupt is raised by the kernel on receipt of error signal from the CPU. We make use of the signal library to manipulate our error buffer.

We initialize a checkpoint buffer to initial state, i.e., no errors generated. We also define error handler function, where we reset the checkpoint buffer to initial state.

SIGSEGV is the error thrown by the CPU on encountering invalid memory access. The handler function is registered with SIGSEGV.

We check for exception by sampling the check point buffer. If there is no error, we proceed with the attack. Once the attack has occurred, the error is detected, and our error handler is called, which resets the checkpoint state, to prevent fatal error.