ABSTRACT

Programs are a very important part of technological advances in this era. Many programs are created by reliable programmers who of course have to meet the needs of technological advancement itself. In making a program, of course there are several important factors that must be fulfilled, one of which is the security factor of the program itself. Usually, hackers attack more applications through programs, one of the programs that is vulnerable to attack is a program in C language. This type of programming language is known to be vulnerable to cyber attacks, especially buffer overflow attacks. Because the C language doesn't have automatic bounds checking to check the boundaries of a buffer. This attack can be triggered by an input that is added in excess of the amount or size of data that will fill the memory of the program being run and this attack will provide access control to the program. There are several methods that can be done to detect buffer overflow attacks, one method that can be used is the taint analysis method. This method is used to check for potential functions as a buffer overflow threat by prioritizing an accuracy percentage of 90% and an execution time of 0.026 seconds on the test results.

Keywords: ***C Language Program, Buffer Overflow Attacks, Taint analysis***