

## ABSTRAK

Program merupakan bagian yang sangat penting dari kemajuan teknologi pada zaman seperti sekarang. Program banyak di ciptakan oleh *programmer-programmer* handal yang tentunya harus memenuhi kebutuhan dari kemajuan teknologi itu sendiri, dalam membuat suatu program pastinya ada beberapa faktor penting yang harus di penuhi salah satunya adalah faktor keamanan dari program itu sendiri. Biasanya peretas lebih banyak menyerang aplikasi melalui program, salah satu program yang rentan terhadap serangan yaitu program dengan bahasa C. Bahasa pemrograman jenis ini di kenal rentan terhadap serangan *cyber* khususnya serangan *buffer overflow*. Karena bahasa C tidak memiliki *automatic bounds checking* untuk mengecek batasan suatu *buffer*. Serangan ini dapat dipicu oleh suatu masukan yang ditambahkan secara berlebihan melebihi jumlah atau ukuran data yang akan memenuhi *memory* pada program yang di jalankan dan serangan ini akan memberikan *access control* pada program tersebut. Terdapat beberapa metode yang bisa di lakukan untuk mendeteksi serangan *buffer overflow*, salah satu metode yang dapat di gunakan adalah dengan metode *taint analysis*. Metode ini berfungsi untuk mengecek fungsi – fungsi yang berpotensi sebagai ancaman *buffer overflow* dengan mengedepankan presentase akurasi sebesar 90% dan waktu eksekusi 0.026 detik pada hasil uji cobanya.

**Kata Kunci:** Program Bahasa C, Serangan *Buffer Overflow*, *Static taint analysis*