## ABSTRAK

*Vulnerability Scanning* merupakan salah satu tahap awal yang digunakan dalam praktek *penetration testing* atau *pentesting*, *vulnerability scanning* dapat dikatakan sebagai salah satu proses vital karena bisa menentukan bagaimana kegiatan penetration testing dilakukan nantinya. Metode konvensional mengharuskan *scanning* dilakukan secara keseluruhan di mana hal tersebut memakan waktu yang cukup lama serta menggunakan *resource* yang cukup besar. Pada *paper* ini, penulis mengusulkan sebuah model yang dibangun berdasarkan salah satu jenis Algoritma *Boosting*, yaitu *Gradient Boosting* untuk ditetapkan sebagai dasar melakukan *vulnerability scan* berdasarkan *port response* dari *host* sasaran. *Port* yang digunakan sebagai parameter pun hanya terdiri dari lima jenis *port* yang ditentukan dari beberapa referensi buku, di mana dari data yang didapat menyatakan bahwa tiga dari lima *port* ini memiliki persentase sebesar 65% paling sering dan *vulnerable* terhadap aktivitas eksploitasi, *port* tersebut mencakup *TCP* 22, *TCP* 80, *TCP* 443, *UDP* 53, dan *UDP* 80. Dari hasil pengujian yang dilakukan sebanyak 15 (lima belas) kali dengan metode CV atau *Cross Validation*, model yang dibangun dengan menerapkan Algoritma *Gradient Boosting* mendapatkan hasil akurasi, presisi, dan *recall* berturut-turut sebesar 98.810%, 98.903%, dan 98.812% serta *error rate* sebesar 0.00260.



**Kata Kunci**: *Vulnerability Scanning, Port Response,* Pembelajaran Mesin, *Boosting, Gradient Boosting.*