ABSTRAK

Universitas Pembangunan Nasional (UPN) "Veteran" Yogyakarta terdapat unit yang bertugas untuk mengawasi dan mengelola jalur informasi atau data-data dari setiap prodi dan jurusan ialah UPT Teknologi Informasi dan Komunikasi (TIK).

UPT TIK tercatat pernah menjadi sasaran serangan DDoS berupa serangan *scanning* dan *flooding attack* berupa ribuan request paket yang membanjiri server selama beberapa jam yang membuat server down untuk beberapa saat. Saat ini di UPN ketika mengalami hambatan server *down*, dosen, staff dan *user* akan melaporkan permasalahan tersebut *via telephone.* Hal ini akan menyulitkan staff yang bertugas sebagai *administror* jaringan jika menangani banyaknya laporan akibat server *dow*n. Selain kuranganya staff yang bertugas, mengamati serangan masih dilakukan secara manual dalam mengawasi ribuan paket data yang masuk dengan mengandalkan pengalaman dan *knowladge* penanganan serangan sehingga dibutuhkan aplikasi monitoring yang mampu mendeteksi serangan dengan cepat.

Hasil dari penelitian ini adalah berupa aplikasi monitoring flooding attack menggunakan algoritma *k-means* dengan teknik *clustering*. Dari pengujian penelitian menghasilkan informasi serangan yang selanjutnya diproses untuk dikategorikan tingkatan serangannya menjadi high, medium atau low. Tingkat keberhasilan rata-rata berdasakan skenario serangan menggunakan *tools* pada penelitian ini 73,18% untuk *success rate* paket yang ditangkap oleh *snort*. Tujuan dari pembuatan penelitian ini adalah membuat aplikasi monitoring dengan memanfaatkan snort untuk menggatikan pelaporan serangan yang masih manual melalui *telephone.*

Kata Kunci: DDoS, Scanning, *flooding attack,* Server, algoritma *k-means, clustering*