ANALISA DAN PERANCANGAN SISTEM KEAMANAN JARINGAN *WEBSERVER* DARI SERANGAN *DENIAL OF SERVICE* (*DOS*) DENGAN MENGGUNAKAN METODE *PENETRATION TEST*

NPM: 1131048
HARINTO JULINSYAH

ABSTRAK

Webserver seringkali menjadi *target* dari berbagai jenis serangan. Keamanan *webserver* biasanya merupakan masalah dari seorang administrator. Seorang administrator bertugas untuk mengawasi dan melakukan tindakan preventif ketika terjadi aksi penyusupan dan serangan. Masalah timbul ketika sang adminstrator sedang tidak berada pada posisi siap sedia. Misalnya sakit, berada diluar jam kerja, atau adanya kepentingan mendadak. Sedangkan, serangan terhadap *server* bisa terjadi kapan saja. Tujuan dari penelitian ini adalah melakukan analisa keamanan *webserver* dengan simulasi serangan *Denial of Service* (*DoS*) terhadap dampak *request*, *resource CPU usage*, *RAM usage*, dan *Network* sebelum dan setelah menerapkan *Iptables.*

Pengujian keamanan *webserver* dilakukan dengan metode *penetration testing*. *Penetration testing* mencakup empat (4) tahap, yaitu *planning*, *security assessment*, *attack*, dan *report.*

Berdasarkan hasil pengujian serangan *DoS* terhadap *webserver* sebelum menerapkan *Iptables, request* yang dihasilkan sebanyak 179709 dalam durasi 1 menit dan 11 detik, sementara *server* merespon 175820 *request* dengan tingkat *request* 2531.11/detik. Sedangkan, setelah diterapkan *Iptables, webserver* merespon 19 *request* dari total 23520 *request* dalam durasi 1 menit 11 detik dengan tingkat *request* 331,27/detik. Kemudian, pada sisi *performance* sistem kinerja *server* terjadi peningkatan nilai *CPU history* 62,4% ketika terjadi serangan, akan tetapi setelah diterapkan *Iptables*, *CPU history* menurun menjadi 12,9%. Oleh karena itu, dengan menerapkan *Iptables* dapat memblokir adanya serangan *DoS* atau penyusupan serta dapat diantisipasi dengan cepat.

Kata kunci: *Webserver, Penetration Testing, Denial of Service* (*DoS*), *Iptables.*