ABSTRAK

ANALISIS SISTEM KEAMANAN PADA *SOFTWARE-DEFINED NETWORK* DENGAN *HYBRID HONEYPOT* MENGGUNAKAN *QUALITY OF SERVICE*

Oleh

Revanza Hafiz Erianto

20102142

Indonesia memiliki jumlah pengguna internet mencapai 185,3 juta (66,5% populasi) pada awal 2024, Indonesia menghadapi lonjakan ancaman siber yang signifikan. Pada 2023 tercatat 603.276.807 serangan siber, termasuk serangan *Distributed Denial of Service (DDoS)* yang menyebabkan gangguan pada *domain* Pemilu 2024, serta 11.081.392 upaya *SSH Brute Force* terhadap situs pemerintahan. Untuk menjawab tantangan ini, penelitian ini merancang sistem keamanan berbasis *Software-Defined Network (SDN)* menggunakan *Hybrid Honeypot* yang dilengkapi *Intrusion Detection System (IDS)* untuk mendeteksi dan membelokkan serangan. Hasil penelitian menunjukkan bahwa serangan *DDoS ICMP Flood, SYN Flood, HTTP Flood,* dan *SSH Brute Force* berhasil dialihkan ke *Honeypot* menggunakan *Flow Rules* pada *Floodlight Controller*, sehingga *server* tetap aman. Pengukuran *Quality of Service* menunjukkan bahwa serangan *SYN Flood* menaikkan *throughput* dari 172,5 *bit/s* pada menit ke-5 menjadi 182,6 *bit/s* pada menit ke-20, dengan *delay* menurun dari 13.219 *ms* menjadi 10.244 *ms*. Serangan *HTTP Flood* menyebabkan *throughput* menurun dari 545,5 *bit/s* pada menit ke-5 menjadi 490,3 *bit/s* pada menit ke-20, sementara *delay* meningkat dari 153.945 *ms* menjadi 296,158 *ms*. *ICMP Flood* menunjukkan *throughput* yang stabil di sekitar 8.000 *bit/s*, namun *packet loss* meningkat hingga 3,05% pada menit ke-20, dengan *delay* berubah dari 60,06 *ms* pada menit ke-5 menjadi 62,11 *ms* pada menit ke-20. Sementara itu, serangan *SSH Brute Force* meningkatkan *throughput* dari 3,24 *bit/s* pada menit ke-5 menjadi 3,81 *bit/s* pada menit ke-20, sementara *delay* menurun dari 367 *ms* menjadi 272 *ms*.

Kata Kunci : ***Distributed Denial of Service, Hybrid Honeypot, Intrusion Detection Systems, Quality of Service, Software-Defined Network, SSH Brute Force***