

Nama : Zumardi Irfan

Nim : 09040581721014

Prodi : TKJ5

Mata Kuliah : TPKI

Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless

BAB I

- Teknologi Keamanan Firewall masih memiliki beberapa kelemahan
- IDS sulit membedakan antara aktivitas legal dengan trafik malicious
- Serangan yang paling sering digunakan adalah Port Scanning dan DOS

BAB III

- Gambaran Umum Sistem
- Rancangan Honeypot
- Rancangan Iptables
- Skenario Serangan

BAB IV

- Scanning Host dan Port
- Serangan Tcp Flood
- Serangan Http Flood
- Serangan Udp Flood
- Serangan Ddos ke Server

Perkembangan teknologi jaringan terutama sistem keamanan jaringan yang semakin berkembang menuntut agar sistem keamanan untuk berkembang. Honeyd merupakan honeypot dengan jenis low interaction yang memiliki resiko jauh lebih kecil dibandingkan dengan jenis high interaction karena interaksi terhadap honeypot tidak langsung melibatkan sistem yang sesungguhnya. Pada penelitian ini, honeyd yang dipadu dengan iptables diimplementasikan pada jaringan lokal dengan mencoba beberapa serangan seperti scanning host, DoS dan Ddos.

Dari hasil log honeyd data informasi yang didapat diolah dengan honeyd-viz dan diharapkan dapat menjadi masukan dan solusi untuk menentukan kebijakan keamanan pada jaringan dan membuat sistem lebih aman. Dalam percobaan yang dilakukan honeyd dapat mendeteksi serangan yang dilakukan oleh Netscan android dalam scanning host pada jaringan. Pada percobaan serangan Ddos dengan Loic didapatkan nilai rata-rata sebelum serangan beban cpu sebesar 15,25% dan setelah serangan beban cpu sebesar 45,98% dan setelah pembelokkan serangan beban cpu sebesar 30,83%.