ABSTRAK

Penelitian ini berfokus pada identifikasi dan *profiling* IBM QRadar dalam menunjukkan kemampuan deteksi terhadap berbagai jenis serangan siber. Proses identifikasi dan *profiling* ini menggunakan platform eksperimen yang terdiri dari tiga *server* virtualisasi, yaitu Kali Linux sebagai pengujian penetrasi dan keamanan jaringan, IBM QRadar sebagai SIEM untuk mendeteksi dan menganalisis ancaman keamanan dalam jaringan, serta CentOS sebagai *Target Client*. Kategori teknik serangan yang digunakan adalah *port scanning*, *brute force*, dan DDoS. Hasil pengujian menunjukkan bahwa IBM QRadar mampu mendeteksi aktivitas berbahaya melalui analisis indikator *rules* pada kategori serangan tersebut. Untuk *port scanning*, deteksi mencakup banyaknya permintaan ke berbagai *port*. Pada *brute force*, deteksi mencakup pola permintaan yang tidak biasa. Sementara itu, pada DDoS, deteksi mencakup frekuensi permintaan koneksi. Analisis dilakukan berdasarkan fungsi kontrol pada hasil pengujian dikategorikan berdarsarkan aspek *Identification*, *Authentication*, *Authorization*, dan *Accounting* menunjukkan hasil *log* dari serangan dilakukan analisis dan pencatatan oleh IBM QRadar. Dari hasil *log* yang di dokumentasikan oleh IBM QRadar dilakukan perbandingan metrik *Response Time* dan metrik Granularitas. Metrik *Response Time* menunjukkan bahwa serangan Hping 3 memiliki waktu respons tercepat yaitu 11 detik, sementara serangan Medusa memiliki waktu respons terlama yaitu 1850 detik. Selain itu, metrik granularitas menunjukkan bahwa serangan Hydra, Brutespray, dan Medusa memiliki skor total tertinggi yaitu 39, sementara serangan LOIC dan Slowloris menempati posisi terakhir dengan skor total 27. Hal ini menunjukkan kemampuan IBM QRadar untuk mencatat dan menganalisis detail setiap serangan dengan sangat baik. Kesimpulan tersebut menunjukkan bahwa IBM QRadar mampu mendeteksi dan merespons berbagai jenis serangan siber berdasarkan *Threat Intelligence* dan monitoring *Threat Behavior*.

Kata kunci — **Fungsi Kontrol Keamanan, IBM QRadar, SIEM, *Threat Behavior*, *Threat Intelligence***