ABSTRACT

This research focuses on identifying and profiling IBM QRadar in demonstrating its detection capabilities against various types of cyber attacks. The identification and profiling process utilizes an experimental platform consisting of three virtualization servers: Kali Linux for penetration testing and network security, IBM QRadar as a SIEM system to detect and analyze security threats within the network, and CentOS as the Target Client. The categories of attack techniques used include port scanning, brute force, and DDoS attacks. The testing results indicate that IBM QRadar can detect malicious activities through the analysis of rule indicators for these categories of attacks. For port scanning, detection encompasses the number of requests to various ports. For brute force, detection includes unusual request patterns. Meanwhile, for DDoS attacks, detection includes the frequency of connection requests. The analysis, based on control functions from the test results, categorized into aspects of Identification, Authentication, Authorization, and Accounting, shows that the log results of the attacks are analyzed and documented by IBM QRadar. From the logs documented by IBM QRadar, comparisons were made using the Response Time metric and the Granularity metric. The Response Time metric shows that the Hping 3 attack has the fastest response time of 11 seconds, while the Medusa attack has the longest response time of 1850 seconds. Additionally, the granularity metric shows that the Hydra, Brutespray, and Medusa attacks have the highest total scores of 39, while the LOIC and Slowloris attacks rank last with a total score of 27. This demonstrates IBM QRadar's ability to record and analyze the details of each attack very well. These conclusions show that IBM QRadar can detect and respond to various types of cyber attacks based on Threat Intelligence and Threat Behavior monitoring.

Keywords — ***Security Control Function,*** **IBM QRadar, SIEM,** ***Threat Intelligence, Threat Behavior***