ABSTRAK

Pertumbuhan terhadap serangan DDoS dan serangan *ransomware* pada industri ritel meningkat di beberapa tahun terakhir. Berdasarkan laporan Verizon pada tahun 2023, *Denial-of-Service* dan *Ransomware* menjadi insiden yang paling sering terjadi. Salah satu cara untuk memitigasi serangan tersebut adalah dengan meningkatkan keamanan jaringan. Kontrol keamanan pada jaringan dapat berupa penerapan *firewall*, *honeypot*, IDS, dan *proxy*. Penelitian ini mencoba untuk menganalisis dan menguji performa keamanan jaringan pada PT XYZ terhadap serangan DDoS dan serangan *ransomware*, serta merancang mitigasi serangan DDoS dan serangan *ransomware* pada PT XYZ dengan kontrol keamanan yang baru. Penelitian dilakukan pada *security testing environment* yang menyerupai lingkungan pada PT XYZ agar tidak mengganggu operasional bisnis perusahaan. Penerapan *firewall* dan *reverse proxy* untuk memitigasi serangan DDoS berhasil dilakukan dan hasilnya kontrol keamanan tersebut mampu mengurangi *impact* dari serangan dengan *flag* SYN, TCP, dan HTTP dengan perubahan rata-rata kenaikan pada *throughput* sebesar 6,67 Mbps, rata-rata nilai pada *jitter* sebesar 2,23 ms, rata-rata persentase penurunan *latency* sebesar 86,67%, rata-rata persentase penurunan *packet loss* sebesar 87%, dan rata-rata persentase penurunan penggunaan CPU pada *firewall* sebesar 49,67%. Selain itu, penerapan Suricata sebagai IDS juga mampu mendeteksi adanya serangan DDoS dan serangan *ransomware* dengan *rule* dari ET Open.

Kata kunci: keamanan jaringan, *ransomware*, DDoS, *firewall*, *honeypot*, Suricata, ritel

ABSTRACT

The retail industry has seen a significant rise in DDoS and ransomware attacks over recent years. According to Verizon's 2023 report, Denial-of-Service and ransomware rank among the most frequent incidents. Strengthening network security is one of the key strategies to mitigate these threats. Security measures such as firewalls, honeypots, IDS, and proxies are essential components. This study aims to analyze and evaluate the performance of network security at PT XYZ in responding to DDoS and ransomware attacks while designing new mitigation strategies. The research was conducted in a security testing environment that simulates PT XYZ's operational setup, ensuring no disruption to business operations. The implementation of firewalls and reverse proxies successfully mitigated DDoS attacks, demonstrating their ability to reduce the impact of such threats involving SYN, TCP, and HTTP flags resulted in an average throughput increase of 6.67 Mbps, an average jitter value of 2.23 ms, a significant 86.67% decrease in latency, an 87% reduction in packet loss, and a 49.67% drop in CPU usage on the firewal.. Additionally, Suricata was employed as an IDS and effectively detected both DDoS and ransomware attacks using ET Open rules.

Keywords: *network security*, *ransomware*, DDoS, *firewall*, *honeypot*, Suricata, *retail*