ABSTRAK

COMPARISON ANALYSIS OF SNORT, SURICATA AND ZEEK INTRUSION PREVENTION SYSTEM (IPS) PERFORMANCE USING QOS (QUALITY OF SERVICE)

Oleh

Rias Gauri Nurhasanah 19102212

Data security is one part that is stored in a computer network system. To maintain or maintain network and computer security so that unwanted things do not occur from network attacks. Currently, computer network security systems are experiencing developments where firewalls can be equipped with several other computer network security methods such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). There are several open source tools that are commonly used to secure networks, such as Snort, Suricata and Zeek which have superior capabilities in detecting and preventing attacks. In this study, a comparison was made in terms of performance and performance of the three Snort, Suricata and Zeek tools. The attacks used as experiments are SYN Flood and ICMP Flood. To test the performance of the three IPS tools, the authors use quality of service (QOS). Based on the results of the Quality of Service (QoS) test on the ICMP Flood attack, Zeek has the smallest packet loss value of 0.25%, Zeek has the smallest delay value of 45.59 ms compared to Snort and Suricata, Zeek has the smallest jitter value of 1.25 ms compared to Snort and Suricata, Suricata has the highest throughput value of 32400 bit/s compared to Snort and Zeek. In the SYN Flood attack, Zeek has the smallest packet loss value of 0.14%, Zeek has the smallest delay value of 17.9 ms compared to Snort and Suricata, Snort has the smallest value of the smallest jitter is 1.81 ms compared to Zeek and Suricata, Snort has the highest throughput value of 32400 bit/s compared to Suricata and Zeek.

Keywords: ***Intrusion Prevention System*****, Snort, Suricata, Zeek,** ***Quality Of***

ABSTRAK

COMPARISON ANALYSIS OF SNORT, SURICATA AND ZEEK INTRUSION PREVENTION SYSTEM (IPS) PERFORMANCE USING QOS (QUALITY OF SERVICE)

Oleh

Rias Gauri Nurhasanah 19102212

Data security is one part that is stored in a computer network system. To maintain or maintain network and computer security so that unwanted things do not occur from network attacks. Currently, computer network security systems are experiencing developments where firewalls can be equipped with several other computer network security methods such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). There are several open source tools that are commonly used to secure networks, such as Snort, Suricata and Zeek which have superior capabilities in detecting and preventing attacks. In this study, a comparison was made in terms of performance and performance of the three Snort, Suricata and Zeek tools. The attacks used as experiments are SYN Flood and ICMP Flood. To test the performance of the three IPS tools, the authors use quality of service (QOS). Based on the results of the Quality of Service (QoS) test on the ICMP Flood attack, Zeek has the smallest packet loss value of 0.25%, Zeek has the smallest delay value of 45.59 ms compared to Snort and Suricata, Zeek has the smallest jitter value of 1.25 ms compared to Snort and Suricata, Suricata has the highest throughput value of 32400 bit/s compared to Snort and Zeek. In the SYN Flood attack, Zeek has the smallest packet loss value of 0.14%, Zeek has the smallest delay value of 17.9 ms compared to Snort and Suricata, Snort has the smallest value of the smallest jitter is 1.81 ms compared to Zeek and Suricata, Snort has the highest throughput value of 32400 bit/s compared to Suricata and Zeek.

Keywords: Intrusion Prevention System*, Snort, Suricata, Zeek, *Quality Of