INTISARI

Internet of Things (IoT) merupakan teknologi yang memungkinkan terjadinya komunikasi antara perangkat elektronik dan sensor melalui internet. Perkembangannya begitu masif dan akan terus bertambah dengan hadirnya internet 5G. Sayangnya, meningkatnya penggunaan perangkat IoT terutama perangkat IoT rumahan juga dibarengi dengan berkembangnya kerentanan keamanan pada jaringan rumah. Jaringan rumah sendiri merupakan lingkungan yang tidak aman karena cenderung mudah dilakukan penyerangan akibat minimnya pengawasan pengguna terhadap perangkat-perangkat IoT yang dimilikinya. Hal ini memaksa pengguna untuk mengisolasi perangkat IoT dari jaringan utama rumahnya. Untuk mengisolasi perangkat IoT dari jaringan utama rumah, dapat digunakan Raspberry Pi. Raspberry Pi dapat difungsikan sebagai *Wireless Access Point* (WAP) dan *firewall* bagi perangkat IoT. Iptables merupakan *firewall* bawaan Linux yang menawarkan kemudahan dalam pengaplikasiannya sehingga sesuai untuk digunakan pada Raspberry Pi 3. Beberapa aturan yang dibuat di antaranya penolakan akses ke jaringan dan akses *remote* dari perangkat tidak sah, serta pembatasan paket TCP SYN akibat *SYN flood* yang mampu berimplikasi pada terjadinya *Distributed Denial of Service* (DDoS). Penelitian ini juga mengidentifikasi perbedaan penggunaan beberapa *chain* iptables terhadap penggunaan CPU Raspberry Pi ketika terjadi *SYN flood*. Selain itu, demi mendukung terpantaunya serangan-serangan yang terjadi, dapat digunakan *ELK Stack.* Dengan ini, serangan seperti percobaan akses ke jaringan, pengendalian perangkat, hingga *SYN flood* dapat dipantau dan diminimalkan dampaknya.

Kata kunci: *Internet of Things* (IoT), Raspberry Pi, iptables, *SYN Flood, ELK Stack*

ABSTRACT

Internet of Things (IoT) is a technology that supports communication between electronic devices and censors through internet. IoT is massively growing and will continue to grow as 5G internet will gradually comes into life. However, the growth of IoT especially smart homes doesn't come with nothing but more vulnerabilities on home networks. Home networks is an ideal environment to be attacked due to lack of control of IoT devices by the owner. This compels the owner to isolate their IoT devices from main home network. To make this happens, Raspberry Pi comes for rescue. Raspberry Pi can function as Wireless Access Point (WAP) and firewall at once for IoT devices. Iptables is a default firewall on Linux which offers simplicity to users which can be applied in Raspberry Pi. Some rules that can be implemented is denying unauthorized devices to access IoT network and remoting IoT devices, and limiting TCP SYN packet as results of SYN flood which can affect to Distributed Denial of Service (DDoS). This research will also compare some iptables chains against Raspberry Pi CPU in handling SYN flooding. Lastly, this research also provides monitoring solution for any unwanted packets that hit the firewall by utilizing ELK Stack. ELK Stack offers logs visualization that makes it easier for the owner to detect access attempt to network, remote control, and SYN flooding.

Keywords: Internet of Things (IoT), Raspberry Pi, Iptables, SYN Flood, ELK Stack