Analisis deteksi serangan address resolution protocol spoofing pada jaringan berbasis openflow switch = Analysis of address resolution protocol spoofing attack detection on openflow switch based network

Rania Ramadhani, author

Abstrak

Penelitian ini memberikan bentuk pencegahan lain untuk ARP spoofing dengan menggunakan teknik stateful protocol analysis dan memperbaiki kekurangan dua penelitian yang pernah ada yaitu Genuine ARP dan Antidote serta memanfaatkan fitur-fitur yang dimiliki oleh OpenFlow switch. Pengujian dilakukan pada jaringan virtual menggunakan aplikasi Mininet dan POX sebagai controller untuk OpenFlow switch dengan masing-masing tiga skenario dan arsitektur, yang menguji keamanan jaringan dengan protokol OpenFlow switch serta pencegahan dari controller.
Pengujian tersebut 100% berhasil membuktikan bahwa controller yang dihasilkan berfungsi sebagai network-based intrusion prevention system yang dapat mendeteksi pasangan IP-MAC address yang asli serta mencegah penyerang dengan melakukan drop flow pada OpenFlow switch sehingga meningkatkan tingkat keamanan jaringan lokal.
<hr>This research provided another form of prevention for ARP spoofing using stateful protocol analysis technique and improved the lack of two previous researches which were Genuine ARP and Antidote and took advantages of features of the OpenFlow switch. Tests were performed on a virtual network using Mininet and POX application as controller for OpenFlow switches with three scenarios and architectures on each, which test the network security using protocol OpenFlow switches as well as test the prevention of the controller.
The testing proved that the controller resulted 100% served as network-based intrusion prevention system which could detect a pair of original IP-MAC address and prevent an attacker by doing drop flow on OpenFlow switch, thereby it increased the level of local network security.