BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari percobaan dan pembahasan sebelumnya, dapat disimpulkan bahwa penelitian implementasi ARP *spoofing prevention* pada jaringan berbasis OpenFlow *switch* berhasil dilakukan. Penelitian ini menghasilkan sebuah *controller* sebagai *network-based intrusion prevention system* yang menjamin keamanan pada jaringan lokal dari serangan ARP *spoofing* dengan mekanisme yang diimplementasikan pada *controller* yang bekerja dengan OpenFlow *switch*. Dengan menggunakan teknik *stateful protocol analysis* dan memanfaatkan fitur – fitur yang dimiliki oleh OpenFlow *switch*, *controller* dapat mendeteksi, menentukan IP dan MAC asli, serta mencegah terjadinya ARP *spoofing* pada jaringan. Pada tabel 5.1 dapat dilihat bahwa penelitian ini berhasil mengatasi kekurangan pada beberapa penelitian terkait dalam pendeteksian ARP *spoofing*. Sebagai langkah tambahan dalam pencegahan terjadinya serangan ARP *spoofing*, *controller* akan menginstruksikan OpenFlow *switch* untuk mengisolasi penyerang yang terdeteksi dan telah melewati nilai *threshold* sehingga mengurangi kemungkinan terjadinya serangan berikutnya. Hal ini membuat tingkat keamanan pada jaringan lokal menjadi bertambah dari serangan ARP *spoofing*.

Tabel 5. 1. Perbandingan dengan penelitian terkait

Penelitian	Cara Kerja	Batasan yang dimiliki	Hal yang diatasi
Genuine ARP	Mendeteksi ARP *spoofing* dengan *broadcast-reply mechanism*, *Certifier*, dan *pending table*.	Harus diterapkan pada seluruh *host* di dalam jaringan, tidak dinamis.	Tidak perlu penerapan pada tiap *host* di jaringan. Pendeteksian dan pencegahan dilakukan oleh *controller*.
Antidote	Mendeteksi ARP *spoofing* dengan membandingkan ARP *cache* dan menolak IP dari MAC yang berbeda jika IP dan MAC pada ARP *cache* masih aktif.	Spoofer dapat tidak terdeteksi jika paket palsu mencapai ARP *cache* terlebih dahulu.	Pasangan IP dan MAC *address* asli dapat diketahui meskipun paket palsu mencapai ARP *cache* terlebih dahulu.

5.2. Saran

Beberapa saran yang berguna untuk pengembangan penelitian ini adalah:

1. Mengembangkan pendeteksian jenis serangan jaringan lain yang dapat dideteksi oleh *controller* untuk menambah tingkat keamanan jaringan.
2. Melakukan uji coba dengan jaringan asli untuk mengetahui respon dari berbagai host dengan spesifikasi yang berbeda - beda.