PENGAMANAN *WIRELESS LOCAL AREA NETWORK* DARI SERANGAN *ADDRESS RESOLUTION PROTOCOL SPOOFING* MENGGUNAKAN PENDEKATAN DETEKSI PASIF DAN *DEAUTHENTICATION ATTACK* BERBASIS RASPBERRY PI

Ilham Ramadhan

ABSTRAK

ARP (*Address Resolution Protocol*) merupakan protokol yang menerjemahkan IP *address* menjadi MAC *address.* ARP tidak memfasilitasi fitur otentikasi dalam melakukan tugasnya. Oleh karena itu, protokol ARP sangat rentan terhadap serangan pemalsuan identitas atau disebut dengan MiTM (*Man in The Middle Attack*). Serangan dari eksploitasi protokol ARP disebut ARP *spoofing attack*. Solusi yang ditawarkan dalam penelitian ini adalah membuat sistem pengamanan yang dapat mendeteksi dan mencegah terjadinya serangan ARP *spoofing*. Sistem ini dapat mendeteksi serangan ARP *spoofing* dengan membandingkan MAC *address* dari *router* asli, yang disimpan secara statis, dengan MAC *address* dari *router* yang ada pada ARP *cache table*. Ketika sistem berhasil mendeteksi adanya serangan, sistem akan merespon dengan melakukan *deauthentication attack* pada MAC *address* penyerang yang didapat dari MAC *address router* pada ARP *cache table*. Dengan dikeluarkannya penyerang dari jaringan WLAN, maka penyerang tidak bisa melakukan serangan ARP *spoofing* pada jaringan tersebut. Sistem ini berjalan pada Raspberry Pi Model B. Didapatkan waktu rata-rata yang dibutuhkan untuk mendeteksi serangan ARP *Spoofing* adalah 0.922 detik dan waktu rata-rata yang dibutuhkan untuk merespon adalah 3.02 detik.

Kata kunci: ARP, MAC *address*, IP *address*, ARP *spoofing*, MiTM, otentikasi, *deauthentication attack*, ARP *cache table*, Raspberry Pi

SECURING WIRELESS LOCAL AREA NETWORK FROM ADDRESS RESOLUTION PROTOCOL SPOOFING ATTACK USING PASSIVE DETECTION APPROACH AND DEAUTHENTICATION ATTACK BASED ON RASPBERRY PI

Ilham Ramadhan

ABSTRACT

ARP (Address Resolution Protocol) is a protocol that translates IP addresses into MAC addresses. ARP does not facilitate the authentication feature in doing its job. Therefore, the ARP protocol is very vulnerable to fake identity attacks or what is called MiTM (Man in The Middle Attack). Attacks from exploiting the ARP protocol are called ARP spoofing attacks. The solution offered in this research is to create a security system that can detect and prevent ARP spoofing attacks. This system can detect ARP spoofing attacks by comparing the MAC address of the original router, which is stored statically, with the MAC address of the router in the ARP cache table. When the system successfully detects an attack, the system will respond by performing a deauthentication attack on the attacker's MAC address obtained from the router MAC address in the ARP cache table. By removing the attacker from the WLAN network, the attacker cannot perform an ARP spoofing attack on that network. This system runs on the Raspberry Pi Model B. The average time it takes to detect ARP Spoofing attacks is 0.922 seconds and the average time needed to respond is 3.02 seconds.

Keywords : ARP, MAC *address*, IP *address*, ARP *spoofing*, MiTM, authentication,

deauthentication attack, ARP *cache table*, Raspberry Pi