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

SKRIPSI

Ilham Ramadhan

1610511041

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2020

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

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Kelulusan Mata Kuliah Skripsi

Ilham Ramadhan

1610511041

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2020

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Ilham Ramadhan
NIM : 1610511041
Tanggal : 26 Mei 2020

Bilamana di kemudian hari ditemukan ketidak sesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 26 Mei 2020
Yang Menyatakan,

(Ilham Ramadhan)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta,

saya yang bertanda tangan di bawah ini :

Nama	: Ilham Ramadhan
NIM	: 1610511041
Fakultas	: Ilmu Komputer
Program Studi	: Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right)* atas karya ilmiah saya yang berjudul:

Pengamanan *Wireless Local Area Network* dari Serangan *Address Resolution Protocol Spoofing* Menggunakan Pendekatan Deteksi Pasif dan *Deauthentication Attack* Berbasis Raspberry Pi

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data *(database)*, merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 26 Mei 2020

Yang menyatakan,

(Ilham Ramadhan)

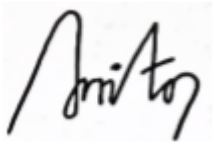
PERSETUJUAN SKRIPSI

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama	: Ilham Ramadhan
NIM	: 1610511041
Program Studi	: Informatika
Judul Tugas Akhir	: Pengamanan Wireless Local Area Network dari Serangan Address Resolution Protocol Spoofing Menggunakan Pendekatan Deteksi Pasif dan Deauthentication Attack Berbasis Raspberry Pi

Sebagai bagian persyaratan yang diperlukan untuk mengikuti ujian sidang Skripsi/Tugas Akhir pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Menyetujui,



Anita Muliawati, S.Kom., MTI.
Ketua Program Studi

Menyetujui,

Henki Bayu Seta, S.Kom., M.TI.
Pembimbing I

Menyetujui,

Ria Astriratma, S.Komp., M.Cs
Pembimbing II

Ditetapkan di : Jakarta

Tanggal Ujian : 27 Mei 2020

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

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala karunia-Nya sehingga skripsi ini berhasil diselesaikan. Judul yang dipilih dalam penelitian ini yang dilaksanakan sejak 2019 ini adalah "Pengamanan Wireless Local Area Network dari Serangan Address Resolution Protocol Spoofing Menggunakan Pendekatan Deteksi Pasif dan Deauthentication Attack Berbasis Raspberry Pi". Penulis ingin mengucapkan terima kasih kepada:

1. Kedua orang tua penulis, Iskandar Prilian Ariesandi dan Ilya Harjanti.
2. Bapak Henki Bayu Seta, S.Kom., M.TI. dan Ibu Ria, Ria Astriratma, S. Kom., M.Cs., selaku dosen pembimbing yang telah memberikan saran yang bermanfaat.
3. Ibu Anita Muliawati, S.Kom, MTI., selaku Ketua Jurusan Informatika Universitas Pembangunan Nasional "Veteran" Jakarta.
4. Ibu Dr. Ermatita, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jakarta.

Jakarta, 27 Mei 2020

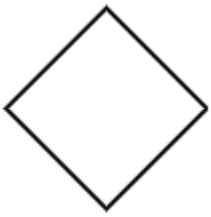
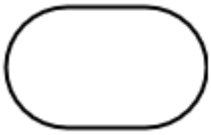
Penulis,

(Ilham Ramadhan)

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR SIMBOL

Simbol	Nama Simbol	Keterangan
	Simbol Proses	Menggambarkan Proses
	Simbol Keputusan	Menggambarkan keputusan berdasarkan kondisi yang diberikan
	Simbol Terminator	Simbol untuk permulaan atau akhir sebuah kegiatan
	Simbol Fungsi	Simbol yang menandakan implementasi fungsi
	Simbol Arus Program	Sebagai petunjuk arus proses pada program

DAFTAR TABEL