



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**IMPLEMENTASI ARP *SPOOFING PREVENTION*
SYSTEM PADA JARINGAN BERBASIS
OPENFLOW SWITCH**

Skripsi

Diajukan sebagai salah satu syarat untuk
memperoleh gelar Sarjana Komputer



Roderick Markus Irawan

11110210012

PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG

2015

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI ARP SPOOFING PREVENTION SYSTEM PADA JARINGAN BERBASIS OPENFLOW SWITCH

Oleh

Nama: Roderick Markus Irawan

NIM: 11110210012

Fakultas: Teknologi Informasi dan Komunikasi

Program Studi: Sistem Komputer

Tangerang, 29 Juni 2015

Ketua Sidang

Dosen Penguji

(Dr. Hugeng)

Dosen Pembimbing

(Kanisius Karyono, S.T., M.T.)

Ketua Program Studi

(Hargyo Tri Nugroho, S.Kom, M.Sc.)

(Kanisius Karyono, S.T., M.T.)

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya :

Nama : Roderick Markus Irawan

NIM : 11110210012

Fakultas : Teknologi Informasi dan Komunikasi

Program Studi : Sistem Komputer

menyatakan bahwa skripsi yang berjudul *IMPLEMENTASI ARP SPOOFING PREVENTION SYSTEM PADA JARINGAN BERBASIS OPENFLOW SWITCH* adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Tangerang, 29 Juni 2015

(Roderick Markus Irawan)

UMMN

ABSTRAK

Salah satu serangan yang sering terjadi pada jaringan komputer adalah *Address Resolution Protocol (ARP) spoofing*, dimana penyerang mengirimkan paket ARP palsu dalam *Local Area Network (LAN)* yang bertujuan untuk mematikan suatu *service* atau mendapatkan data – data yang dimiliki oleh korban. Penanganan *ARP spoofing* yang ada pada umumnya masih memiliki beberapa batasan seperti hanya terbatas pada jaringan *static*, memerlukan pergantian pada seluruh *host* di jaringan, atau memerlukan perangkat yang terlalu mahal sehingga tidak mudah untuk diimplementasikan. Penelitian ini mengusulkan sebuah bentuk pencegahan serangan *ARP spoofing* menggunakan teknik *stateful protocol analysis* dan memanfaatkan fitur – fitur yang dimiliki *OpenFlow switch* sebagai mekanisme pencegahan serangan baru dalam keamanan jaringan. Pengujian dilakukan pada jaringan virtual menggunakan aplikasi *Mininet* dengan menggunakan *POX* sebagai *controller* untuk *OpenFlow switch*. Pada pengujian yang dilakukan dengan berbagai skenario dan arsitektur, *controller* yang dihasilkan sebagai *network-based intrusion prevention system* dapat dengan baik mendeteksi serta mencegah penyerang dengan bentuk pengisolasian penyerang dari jaringan lokal sehingga meningkatkan tingkat keamanan jaringan lokal.

Kata kunci: *ARP spoofing, OpenFlow, intrusion prevention*

UMMN

ABSTRACT

One of the most frequent attack in a computer network is Address Resolution Protocol (ARP) spoofing where the attacker sends a false ARP packet within Local Area Network (LAN) that designed to denied a service or get datas from the victims. Most defenses of this attack still have some limitations such as limited to a static network, need to change all hosts' network stack or need to use expensive equipment so it is not easy to be implemented. This research proposes and tested a form of prevention with stateful protocol analysis technique and using some features of OpenFlow switch as a new intrusion prevention mechanism in a network security. The trials were done in a virtual network generated by Mininet and POX as the controller for the OpenFlow switch. By testing with various skenarios of attack and network architecture, the produced controller as a network-based prevention system successfully detects and prevents the attackers with isolating them from the local network so that increased local network security.

Keywords: ARP spoofing, OpenFlow, intrusion prevention

UMMN

KATA PENGANTAR

Puji dan syukur dipanjatkan kepada Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya laporan skripsi ini dapat diselesaikan dengan judul “Implementasi ARP *Spoofing Prevention* Pada Jaringan Berbasis OpenFlow *Switch*” yang diajukan kepada Program Studi Sistem Komputer, Fakultas Teknologi Informasi dan Komunikasi, Universitas Multimedia Nusantara.

Di balik keberhasilan dari tuntasnya laporan ini penulis ingin mengucapkan terima kasih kepada:

1. Kedua orang tua penulis yang selalu mendoakan dan mendukung dalam setiap perjalanan penulis,
2. Bapak Hargyo Tri Nugroho, S.Kom., M.Sc., selaku pembimbing akademik sekaligus dosen pembimbing yang telah mengarahkan dan mendidik penulis dalam pengerjaan skripsi ini,
3. Bapak Kanisius Karyono, S.T., M.T., selaku Dekan Fakultas Teknologi Informasi dan Komunikasi, selaku Ketua Program Studi Sistem Komputer Universitas Multimedia Nusantara,
4. Rekan – rekan seperjuangan Sistem Komputer 2011 (Alexander Samuel, Rio Raymundus, Troy Afiat, Henry Gunawan, Amelia Wonosardono, Marcella Astrid, dan Candhika Anhari) yang telah memberikan dukungan dan semangat yang luar biasa,
5. Saudara – saudara penulis yang telah menyemangati dan mendoakan penulis,
6. Dosen – dosen yang telah berbagi ilmu dan pengalaman selama penulis menempuh pendidikan di Universitas Multimedia Nusantara,
7. Semua pihak terkait yang tidak bisa disebutkan satu per satu.

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PENGESAHAN SKRIPSI	ii
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	iii
ABSTRAK	iv
ABSTRACT.....	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	x
PENDAHULUAN	1
1.1. LATAR BELAKANG MASALAH	1
1.2. RUMUSAN MASALAH	3
1.3. BATASAN MASALAH	3
1.4. TUJUAN PENELITIAN	3
1.5. MANFAAT PENELITIAN	3
1.5.1. Manfaat Akademis	4
1.5.2. Manfaat Praktis	4
KERANGKA TEORITIS	5
2.1. LANDASAN TEORI	5
2.1.1. Local Area Network	5
2.1.2. Address Resolution Protocol.....	7
2.1.3. Intrusion Detection and Prevention System.....	9
2.2. PENELITIAN TERKAIT	11
2.2.1. An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks	11
2.2.2. Genuine ARP	12
2.2.3. Antidote.....	13
METODOLOGI PENELITIAN.....	14
3.1. JENIS PENELITIAN.....	14
3.2. INSTRUMEN PENELITIAN.....	14
3.3. LOKASI DAN WAKTU PENELITIAN	15

3.4.	PERANCANGAN SISTEM	15
3.4.1.	Jenis dan Metode Pendeteksian.....	16
3.5.	PEMBANGUNAN APLIKASI <i>CONTROLLER</i>	18
3.6.	PENGOLAHAN DAN ANALISIS DATA PENELITIAN.....	18
UJI COBA DAN PEMBAHASAN.....		19
4.1.	IMPLEMENTASI DAN UJI COBA	19
4.2.	METODE PENGUJIAN	20
4.2.1.	Pengujian dengan arsitektur 1 skenario A.....	22
4.2.2.	Pengujian dengan arsitektur 1 skenario B.....	24
4.2.3.	Pengujian dengan arsitektur 1 skenario C.....	26
4.2.4.	Pengujian dengan arsitektur 2 skenario A.....	28
4.2.5.	Pengujian dengan arsitektur 2 skenario B.....	28
4.2.6.	Pengujian dengan arsitektur 2 skenario C.....	29
4.2.7.	Pengujian dengan arsitektur 3 skenario A.....	30
4.2.8.	Pengujian dengan arsitektur 3 skenario B.....	31
4.2.9.	Pengujian dengan arsitektur 3 skenario C.....	34
4.3.	PEMBAHASAN.....	38
4.3.1.	Pendeteksian ARP <i>Spoofing</i>	39
4.3.2.	Pencegahan ARP <i>Spoofing</i>	39
KESIMPULAN DAN SARAN.....		41
5.1.	KESIMPULAN	41
5.2.	SARAN.....	42
DAFTAR PUSTAKA		43
LAMPIRAN.....		45

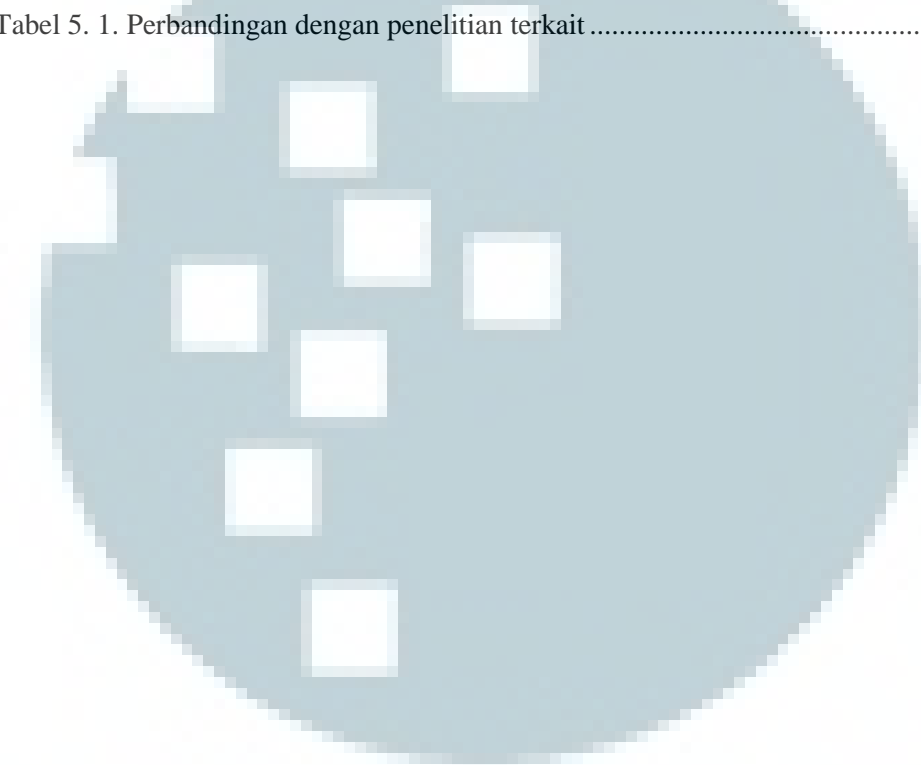
UMMN

DAFTAR GAMBAR

Gambar 2. 1. Bagian – bagian OpenFlow <i>switch</i> [3]	7
Gambar 3. 1 Rancangan Sistem [3]	15
Gambar 3. 2 Flow Chart pendeteksian ARP <i>spoofing</i>	17
Gambar 4. 1 Skenario arsitektur dengan menggunakan satu OpenFlow <i>switch</i>	20
Gambar 4. 2 Skenario arsitektur dengan menggunakan dua OpenFlow <i>switch</i>	21
Gambar 4. 3 Skenario arsitektur dengan menggunakan satu OpenFlow <i>switch</i> dan satu generic <i>switch</i>	21
Gambar 4. 4 Pemblokiran <i>spoofers</i> yang terdeteksi	23
Gambar 4. 5 <i>Spoofing</i> pada ARP <i>cache</i> di <i>controller</i>	25
Gambar 4. 6 <i>Controller</i> memperbarui ARP <i>cache</i> dengan ARP asli.....	25
Gambar 4. 7 <i>Challenge</i> ARP <i>request</i> yang diterima <i>spoofers</i>	26
Gambar 4. 8 Kedua <i>hosts</i> membalas <i>challenge</i> ARP <i>request</i>	27
Gambar 4. 9 <i>Second host</i> diabaikan oleh <i>controller</i>	27
Gambar 4. 10 <i>Controller</i> berisi ARP palsu dan mengira <i>host</i> asli sebagai <i>spoofers</i>	32
Gambar 4. 11 <i>Controller</i> menemukan pasangan IP dan MAC <i>address</i> yang asli	32
Gambar 4. 12 ARP <i>table</i> pada <i>host</i> 5 berisi ARP palsu.....	33
Gambar 4. 13 ARP <i>table</i> pada <i>host</i> 6 berisi ARP palsu.....	33
Gambar 4. 14 ARP <i>cache controller</i> saat serangan berlangsung.....	34
Gambar 4. 15 <i>Controller</i> menerima jawaban <i>challenge</i> dari kedua <i>hosts</i> dan mencatat ARP dari <i>host</i> yg pertama melakukan ping	35
Gambar 4. 16 Ping <i>host</i> pertama berhenti dijawab saat <i>host</i> kedua melakukan ping pada <i>icmp_req</i> = 10 dan berlanjut saat <i>icmp_req</i> = 56.....	36
Gambar 4. 17 Ping <i>host</i> kedua berhenti pada <i>icmp_req</i> = 46 karena <i>race condition</i>	36

DAFTAR TABEL

Tabel 2. 1. Mekanisme yang digunakan dalam pengamanan ARP.....	12
Tabel 2. 2. Penurunan performa untuk pengamanan ARP.....	12
Tabel 4. 1. Hasil percobaan tiap skenario dan arsitektur	37
Tabel 4. 2. Perbandingan hasil uji coba dengan hasil yang diharapkan.....	37
Tabel 5. 1. Perbandingan dengan penelitian terkait	42



UMN