

## DAFTAR ISI

<b>Halaman Judul</b>	<b>ii</b>
<b>Halaman Pengesahan</b>	<b>iii</b>
<b>Halaman Pernyataan</b>	<b>iv</b>
<b>Halaman Persembahan</b>	<b>v</b>
<b>PRAKATA</b>	<b>vi</b>
<b>INTISARI</b>	<b>xv</b>
<b>ABSTRACT</b>	<b>xvii</b>
<b>I PENDAHULUAN</b>	<b>1</b>
1.1 Latar Belakang . . . . .	1
1.2 Perumusan Masalah . . . . .	4
1.3 Batasan Masalah . . . . .	4
1.4 Tujuan Penelitian . . . . .	5
1.5 Manfaat Penelitian . . . . .	6
1.6 Kontribusi Penelitian . . . . .	6
<b>II TINJAUAN PUSTAKA</b>	<b>8</b>
2.1 Tinjauan umum pendekatan kriptografis untuk penanganan ARP <i>poisoning/spoofing</i> . . . . .	8
2.2 Tinjauan umum pendekatan <i>hardware</i> untuk penanganan ARP <i>poisoning/spoofing</i> . . . . .	19
2.3 Tinjauan umum pendekatan <i>software</i> untuk penanganan ARP <i>poisoning/spoofing</i> . . . . .	27
2.4 Tinjauan umum pendekatan <i>voting</i> untuk penanganan ARP <i>poisoning/spoofing</i> . . . . .	39
2.5 Tinjauan umum pendekatan <i>kernel-based patch</i> untuk penanganan ARP <i>poisoning/spoofing</i> . . . . .	45
2.6 Tinjauan umum pendekatan entri statis ( <i>static entry</i> ) untuk penanganan ARP <i>poisoning/spoofing</i> . . . . .	48

2.7	Tinjauan umum pendekatan lainnya untuk penanganan ARP <i>poisoning/spoofing</i> . . . . .	50
2.8	Perbandingan dengan metode yang diusulkan . . . . .	57
2.8.1	ARPWATCH . . . . .	57
2.8.2	Keunggulan metode yang diusulkan . . . . .	58
<b>III LANDASAN TEORI</b>		<b>61</b>
3.1	MitM-ARP <i>spoofing</i> . . . . .	61
3.2	DHCP untuk pengamanan ARP <i>cache</i> . . . . .	64
3.3	<i>Layer 3</i> dan <i>layer 2 filtering</i> . . . . .	69
<b>IV METODE PENELITIAN</b>		<b>73</b>
4.1	Solusi <i>router</i> . . . . .	74
4.2	Solusi <i>network host</i> . . . . .	77
4.3	Skenario pengujian . . . . .	82
4.4	Skenario yang diasumsikan . . . . .	83
4.5	<i>Threat model</i> . . . . .	83
<b>V IMPLEMENTASI</b>		<b>86</b>
5.1	<i>Hardware</i> dan <i>software</i> . . . . .	86
5.2	Topologi jaringan . . . . .	87
5.3	Konfigurasi awal eksperimen . . . . .	87
5.4	Implementasi solusi <i>router</i> . . . . .	88
5.5	Implementasi solusi <i>network host</i> . . . . .	90
5.6	Implementasi di dunia nyata . . . . .	98
<b>VI HASIL PENELITIAN DAN PEMBAHASAN</b>		<b>100</b>
6.1	Hasil pengujian skenario 1 . . . . .	101
6.2	Hasil pengujian skenario 2 . . . . .	102
6.3	Hasil pengujian skenario 3 . . . . .	104
6.4	Hasil pengujian skenario 4 . . . . .	105
6.5	Evaluasi kinerja . . . . .	106
6.6	<i>Snapshot</i> dan anomali <i>ping</i> RTT . . . . .	112
6.7	Hasil perbandingan <i>requirement</i> dengan ARPWATCH . . . . .	114
6.8	Serangan canggih ( <i>sophisticated</i> ) . . . . .	114

<b>VII KESIMPULAN DAN SARAN</b>	<b>116</b>
7.1 Kesimpulan . . . . .	116
7.2 Saran . . . . .	116
<b>DAFTAR PUSTAKA</b>	<b>118</b>