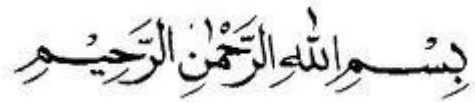


KATA PENGANTAR



Puji dan syukur penulis persembahkan kehadiran Allah SWT atas rahmat, karunia, hidayah serta kasih sayang yang diberikan selama pengerjaan Tugas Akhir yang berjudul **“ANALISIS KEAMANAN JARINGAN VIDEO CONFERENCE PADA PROTOKOL H.323 MENGGUNAKAN METODE AUTHENTICATION DAN KEY SWITCH”** sehingga dapat terselesaikan. Tidak lupa shalawat serta salam penulis haturkan atas junjungan kita Rasulullah Muhammad SAW yang telah membawa kecerahan di dunia ini.

Tugas Akhir ini disusun untuk memenuhi salah satu syarat dalam menyelesaikan pendidikan pada Program Sarjana Teknik Telekomunikasi Fakultas Elektro dan Komunikasi IT Telkom. Penulis menyadari bahwa Tugas Akhir ini masih jauh dari kesempurnaan yang disebabkan karena keterbatasan penulis. Untuk itu saran dan kritik yang bersifat membangun dari pembaca sangat penulis harapkan demi perbaikan dimasa mendatang.

Dengan segala kerendahan hati, penulis berharap semoga Tugas Akhir ini dapat bermanfaat bagi para pembaca dan penulis khususnya, juga bagi dunia teknologi telekomunikasi dan dunia pendidikan pada umumnya.

Bandung, 3 Oktober 2014

Penulis

DAFTAR ISI

HALAMAN JUDUL	
LEMBAR PENGESAHAN	
LEMBAR PERNYATAAN ORISINALITAS	
ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
UCAPAN TERIMA KASIH	iv
DAFTAR ISI	vii
DAFTAR SINGKATAN	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan	2
1.3 Rumusan Masalah	2
1.4 Batasan Masalah	2
1.5 Metode Penulisan	3
1.6 Sistematika Penulisan	4
BAB II DASAR TEORI	5
2.1 Definisi Video Conference	5
2.2 Protokol H.323	5

2.2.1	Arsitektur Protokol H.323	6
2.2.2	Keunggulan Protokol H.323	10
2.2.3	Layanan Pada Protokol H.323	12
2.3	Protokol H.235	13
2.4	Mengamankan Protokol H.323	14
2.4.1	Metode Authentication	14
2.4.2	Metode Key Switch	15
2.5	Gangguan Keamanan Jaringan Video Conference Pada Skype	17
2.5.1	Insertion Attack (Level 1)	17
2.5.2	Interception Dan Monitoring Traffic Wireless (Level 2).....	17
2.5.3	Client-to-Client Attack (Level 3)	18
2.6	Teori Performansi Pada Jaringan Video Conference	19
2.6.1	Throughput	19
2.6.2	Delay	19
2.6.3	Jitter	19
2.6.4	Packet Loss	20
BAB III	PERANCANGAN DAN REALISASI	20
3.1	Pendahuluan	20
3.2	Peralatan Yang Digunakan	21
3.2.1	Perangkat Keras (Hardware)	21
3.2.2	Perangkat Lunak (Software)	22
3.3	Pemodelan Jaringan	23
3.4	Pengamanan Menggunakan Metode Authentication dan Key Switch	26
3.4.1	Metode Authentication Pada Skype	26

3.4.2 Metode Key Switch Pada ViCon	27
3.5 Skenario Pengujian Dengan Gangguan	28
3.6.1 Skenario #1 (Insertion Attack)	28
3.6.2 Skenario #2 (Interception And Monitoring)	28
3.6.3 Skenario #3 (Client-to-Client Attack)	28

BAB IV ANALISIS

4.1 Proses Pengambilan Data Pada Metode Authentication Dengan Wireshark	29
4.1.1 Capture Data Pada Skenario #1	29
4.1.2 Capture Data Pada Skenario #2	35
4.2 Proses Pengambilan Data Pada Metode Key Switch Dengan Wireshark.....	38
4.2.1 Capture Data Pada Skenario #1	38
4.2.2 Capture Data Pada Skenario #2	42
4.3 Proses pengambilan Data Pada Metode Authentication Dengan OPNET	44
4.3.1 Capture Data Pada Skenario #1	44
4.3.2 Capture Data Pada Skenario #2	45
4.4 Proses Pengambilan Data Pada metode Key Switch Dengan OPNET	47
4.4.1 Capture Data Pada Skenario #1	47
4.4.2 Capture Data Pada Skenario #2	48

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan	50
5.2 Saran	51

DAFTAR PUSTAKA 52

LAMPIRAN A

LAMPIRAN B