

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	xi
DAFTAR SIMBOL.....	xii
DAFTAR LAMPIRAN.....	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Identifikasi Masalah	2
1.3 Maksud dan Tujuan.....	2
1.4 Batasan Masalah.....	3
1.5 Metodologi Penelitian	3
1.5.1 Analisis Masalah.....	3
1.5.2 Vulnerability Assessment and Penetration Testing.....	4
1.5.3 Mitigasi Sistem Keamanan.....	5
1.5.4 Pengujian.....	5
1.5.5 Kesimpulan.....	5
1.6 Sistematika Penulisan.....	5
BAB 2 LANDASAN TEORI	7
2.1 Jaringan Komputer	7
2.1.1 LAN (Local Area Network)	7
2.1.2 MAN (Metropolitan Network)	8
2.1.3 WAN (Wide Area Network).....	8
2.1.4 Jaringan WLAN (Wireless Local Area Network)	8
2.1.5 Topologi Jaringan.....	9
2.1.6 Protokol Jaringan.....	11

2.2.	OSI Layer	15
2.1	Keamanan Sistem Informasi	18
2.2	Jenis Jenis Ancaman Keamanan Jaringan.....	20
2.3	VAPT.....	22
2.4	CVSS (Common Vulnerability Scoring System).....	24
2.5	Mikrotik.....	26
2.6	Bettercap.....	26
2.7	LOIC (<i>Low Orbit Ionn Cannon</i>)	27
BAB 3	ANALISIS DAN PERENCANAAN.....	29
3.1	Analisis Masalah	29
3.2	Perencanaan Assessment.....	30
3.2.1	Information Gathering.....	30
3.2.2	Threat Modeling.....	31
3.2.3	Vulnerability Analysis.....	32
3.2.4	Exploitation	32
3.2.5	Post Exploitation.....	36
3.2.6	Reporting.....	36
BAB 4	IMPLEMENTASI DAN HASIL	38
4.1	Information Gathering.....	38
4.2	Threat Modeling.....	39
4.3	Vulnerability Analysis.....	40
4.4	Exploitation.....	40
4.4.1	Pengujian MITM	41
4.4.2	Pengujian DDOS	45
4.5	Post Exploitation	48
4.6	Report.....	50
4.7	Mitigasi Keamanan.....	51
4.7.1	Konfigurasi DNS Over HTTPS	52
4.7.2	Konfigurasi Firewall Rules.....	56
4.8	Pengujian.....	61
4.8.1	Pengujian MITM	62
4.8.2	Pengujian DDOS	65
4.8.3	Performansi Sebelum di dan Sesudah di konfigurasi	71

4.9	Perbandingan Hasil Pengujian Sebelum dan Sesudah Di konfigurasi.....	72
BAB 5	KESIMPULAN.....	74
5.1	Kesimpulan.....	74
5.2	Saran.....	74
DAFTAR PUSTAKA		75