DAFTAR ISI

ABSTRAK i

ABSTRACT ii

KATA PENGANTAR iii

DAFTAR ISI v

DAFTAR GAMBAR ix

DAFTAR TABEL xi

DAFTAR SIMBOL xiii

DAFTAR LAMPIRAN xv

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

1.6 Metode Pengumpulan Data 3

1.7 Metode Penetrasi Jaringan 4

1.6 Sistematika Penulisan 6

BAB II TINJAUAN PUSTAKA 9

2.1 Profil Perusahaan 9

2.2 Sejarah Perusahaan 9

2.3 Logo 10
2.3.1 Logo Dinas Kesehatan Jawa Barat 11
2.3.2 Makna Logo Dinas Kesehatan Jawa Barat 12
2.4 Struktur Organisasi 12
2.4.1 Struktur Organisasi Dinas Kesehatan Jawa Barat 13
2.5 Landasan Teori 15
2.6 Jaringan Komputer 15
2.6.1 Manfaat Jaringan Komputer 15
2.6.2 Tipe-tipe jaringan komputer 16
2.6.2.1 Jaringan LAN 16
2.6.2.2 Jaringan WLAN 18
2.6.3 Keamanan Jaringan 20
2.6.3.1 Macam-macam keamanan jaringan 22
2.6.3.2 Ancaman keamanan 22
2.6.3.3 Penyebab serangan 23
2.6.4 Jenis jenis serangan 24
2.6.4.1 *Denial of service* (DOS) 24
2.6.4.2 *Port Scanning* 28
2.6.4.3 *Ping Flooding* 29
2.6.4.4 *Sniffing* 29
2.7 Intrusion Detection System (IDS) 31
2.8 Perangkat Lunak Pendukung 46
2.8.1 PHP 46

2.8.2 MySQL 47
BAB III 49
3.1 *Pre-Engagement* 49
3.1.1 *Questionnaires* 49
3.1.1.1 Pertanyaan *Network Penetration Test* 49
3.1.1.2 Pertanyaan *Wireless Network Penetration test* 50
3.1.1.3 Pertanyaan *Physical Penetration Test* 51
3.1.1.4 Pertanyaan *Administrator Sistem* 51
3.1.2 Landasan Hukum Pengujian *Denial of Service* pada Dinas Kesehatan Provinsi Jawa Barat 52
3.2 *Intelligence Gathering* 52
3.2.1 Analisis Jaringan Komputer 54
3.2.3 Rentan IP 58
3.2.4 *Covert Gathering* 59
3.2.4.1 Pemindaian *Wireless* 60
3.2.4.2 Identifikasi Perangkat *Wifi* 60
3.2.5 *Footprinting* 61
3.2.5.1 *Footprinting Internal* 62
3.3 *Threat Modeling* 62
3.3.1 Analisa Tujuan Bisnis 63
3.3.1.1 Penempatan Perangat *wifi* 63
3.3.1.2 Sumber Daya Manusia Dinas Kesehatan Provinsi Jawa Barat 64

3.3.1.3 Permodelan Pengujian Keamanan Jaringan Dinas Kesehatan Provinsi Jawa Barat 66
3.4 *Vulnerability Analisis* 67
3.4.1 Pengujian Aktif 68
3.4.1.1 Pengujian otomatis 68
3.4.1.2 *Audit* Kerentanan Sistem Oprasi Penyerang 68
3.4.2 Pengujian Pasif 70
3.4.2.1 Analisis Metadata 70
BAB IV IMPLEMENTASI DAN PEMBAHASAN 71
4.1 Exploitation 71
4.1.1 Alur Exploitation 71
4.1.2 Evasion 72
4.1.3 Identifikasi Dan Manipulasi Lalulintas Target 76
4.1.4 Brute Force 80
4.2 Post Exploitation 86
4.2.1 Pillaging 86
4.3 Reporting 87
BAB V KESIMPULAN DAN SARAN 99
5.1 Kesimpulan 99
5.2 Saran 100
DAFTAR PUSTAKA 101