DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI v
DAFTAR GAMBAR vii
DAFTAR TABEL viii
DAFTAR SIMBOL ix
DAFTAR LAMPIRAN xi
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Identifikasi Masalah 2
1.3 Maksud dan Tujuan 3
1.4 Batasan Masalah 3
1.5 Alur Penelitian 4
1.6 Sistematika Penulisan 5
BAB 2 LANDASAN TEORI 7
2.1 Profil Tempat Penelitian 7
2.1.1 Profil Dinas Komunikasi dan Informatika Jawa Barat 7
2.1.2 Visi dan Misi 8
2.1.3 Struktur Organisasi 9
2.2 Landasan Teori 9
2.2.1 Keamanan Informasi 9
2.2.2 Jaringan Internet 11
2.2.3 Konsep Dasar Jaringan Komputer 11
2.2.4 Open Systems Interconnection 13
2.2.5 Nomor *Port* 15
2.2.6 Web 16
2.2.7 Vulnerability Assessment 16
2.2.8 Black box Testing 17
2.2.9 Information Gathering 17
2.2.10 Footprinting 17
2.2.11 Open Web Application Security Project (OWASP) 18
2.2.12 Apache 40

2.2.13 Whatweb 40
2.2.14 Nmap 40
2.2.15 Whois 41
2.2.16 Acunetix 41
2.2.17 Common Vulnerabilities and Exposures (CVE) 42
BAB 3 ANALISIS MASALAH 43
3.1 Analisis Masalah 43
3.1.1 Permasalahan Yang Dihadapi 44
3.1.2 Pemecahan Masalah Yang Diusulkan 44
3.2 Black Box Penetration Testing 44
3.2.1 Tahap I – *Pre Engagement Interaction* 45
3.2.2 Tahap II – *Information Gathering* 47
3.2.3 Tahap III – *Analysis Vulnerability* 64
3.2.4 Tahap IV – *Manual Validation* 95
3.2.5 Tahap V – *Reporting* 99
BAB 4 IMPLEMENTASI DAN EVALUASI HASIL 101
4.1 Implementasi 101
4.1.1 *Manual Validation* 101
4.1.2 *Reporting* 116
BAB 5 KESIMPULAN DAN SARAN 141
5.1 Kesimpulan 141
5.2 Saran 141
DAFTAR PUSTAKA 143