DAFTAR ISI

ABSTRAK ..... **i**
ABSTRACT ..... **ii**
KATA PENGANTAR ..... **iii**
DAFTAR ISI ..... **v**
DAFTAR GAMBAR ..... **xi**
DAFTAR TABEL ..... **xiv**
DAFTAR SIMBOL ..... **xvi**
DAFTAR LAMPIRAN ..... **xviii**
BAB 1 PENDAHULUAN **1**
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 2
1.3 Maksud dan Tujuan 3
1.4 Batasan Masalah 3
1.5 Metodologi Penelitian 3
1.5.1 Studi Pustaka 4
1.5.2 Studi Lapangan 4
1.5.3 Metode Evaluasi Sistem Keamanan 4
1.6 Sistematika Penulisan 6
BAB 2 TINJAUAN PUSTAKA **7**
2.1 Profile Tempat Penelitian 9
2.1.1 Sejarah Instansi 9
2.1.2 Visi dan Misi 12
2.1.3 Logo Diskominfo 12
2.1.4 Struktur Organisasi 14
2.1.5 Deskripsi Pekerjaan 15
2.2 Landasan Teori 35
2.2.1 Pengertian Evaluasi 35
2.2.2 Pengertian Sistem 35
2.2.3 Pengertian Jaringan Komputer 36

2.2.3.1 Jenis Jenis Jaringan Komputer 37
2.2.3.2 Media Transmisi Data 38
2.2.3.3 *Ethernet* 41
2.2.3.4 Topologi Jaringan 42
2.2.3.5 Perangkat Jaringan Komputer 45
2.2.3.6 Model Jaringan 46
2.2.3.7 *TCP/IP* 52
2.2.3.8 *UDP* 53
2.2.3.9 *Port* 54
2.2.3.10 *IP Address* Versi 4 55
2.2.4 Keamanan Komputer 57
2.2.4.1 *Security Assessment* 57
2.2.4.2 *Vulnerability Assessment* 58
2.2.4.3 *Penetration Testing* 58
2.2.4.3.1 *White Box* 58
2.2.4.3.2 *Black Box Penetration Testing* 58
2.2.4.3.3 *Grey Box* 59
2.2.4.4 Keterkaitan *Vulnerability Assessment* dan *Penetration Test* 59
2.2.4.5 *CEH (Certified Ethical Hacker)* 59
2.2.5 *Vulnerability* 60
2.2.6 Risiko 61
2.2.7 Aspek dari *Security* 62
2.2.8 Sumber Lubang Keamanan 63
2.2.9 Mengenai *Hacker* dan *Cracker* 64
2.2.10 *Webserver* 65
2.2.11 *Kali Linux Operating System* 65
2.2.11.1 Sejarah *Kali Linux* 66
2.2.11.2 *Download* Distribusi 66
2.2.11.3 *Install Kali Linux* 68
2.2.11.4 *Setting* Alamat IP 68
2.2.11.5 *Update* dan *Upgrade Repository Kali* 70

2.2.11.6 Menambahkan *Source Repository* 71
2.2.11.7 Menambahkan Aplikasi dan *Tools*....71
2.2.11.8 Perintah apt-get dalam Kali Linux....72
2.2.11.9 *Kali Linux Security Tools*....72
2.2.12 *Terminal*....73
2.2.13 *Flowchart*....74
BAB 3 ANALISIS DAN PERANCANGAN 75
3.1 Analisis 75
3.1.1 Analisis Masalah....75
3.1.1.1 Permasalahan Yang Dihadapi....76
3.1.1.2 Pemecahan Masalah Yang Diusulkan....76
3.1.1.3 Analisis Jenis Serangan....77
3.1.2 Analisis *Web Server*....78
3.1.2.1 Analisis Aplikasi *Web Server* 78
3.1.2.2 Analisis Sistem dan Bahasa Pemograman 78
3.1.2.2.1 Sistem 78
3.1.2.2.2 Bahasa Pemograman 79
3.1.2.2.3 Framework....79
3.1.2.3 Analisis DNS 80
3.1.2.3.1 Struktur DNS....81
3.1.2.4 Analisis *Website*....83
3.1.3 Serangan *Cyber* di Indonesia 83
3.1.4 Analisis Metode *Penetration Testing Life Cycle* 84
3.1.4.1 *Reconnaissance*....85
3.1.4.1.1 *Online Research* 86
3.1.4.1.2 *Footprinting*....87
3.1.4.2 *Scanning*....89
3.1.4.2.1 *Network Scanning*....89
3.1.4.2.2 *Vulnerability Scanning* 91
3.1.4.2.3 *Port Scan* 92
3.1.4.3 *Exploitation*....94

3.1.4.3.1 *Engine Website Exploitation* 94
3.1.4.3.2 *Plugins Website Exploitation* 94
3.1.4.3.3 *Themes Website Exploitation* 95
3.1.4.3.4 *Username dan Password Exploitation* 95
3.1.4.4 *Maintaining Access* 97
3.1.4.4.1 *Malware (malicious software)* 97
3.1.4.4.2 *Backdoor* 98
3.1.4.5 *Reporting* 100
3.1.4.5.1 *Documentation* 100
3.1.4.5.2 *Presentation* 100
3.1.5 *Black Box Penetration Testing* 101
3.1.5.1 Tahap I – *Pre Engagement Interaction* 103
3.1.5.2 Tahap II – *Information Gathering* 103
3.1.5.3 Tahap III – *Vulerability Scanning* 103
3.1.5.4 Tahap IV – *Manual Validation* 103
3.1.5.5 Tahap V - Laporan 103
3.1.6 Analisis Keamanan 104
3.1.6.1 Pengamanan tahap *Reconnaisannce* 104
3.1.6.1.1 Pengaturan *Robots.txt (Crawler)* 104
3.1.6.1.2 Proteksi halaman dengan *password* 106
3.1.6.2 Pengamanan tahap *Scanning* 106
3.1.6.2.1 Pengamanan pada DNS *Info* 107
3.1.6.2.2 Pengamanan pada *website* 107
3.1.6.2.2.1 Pengamanan pada engine website (CMS) 107
3.1.6.2.2.1.1 Pengamanan Versi CMS 107
3.1.6.2.2.1.2 Pengaturan *file permission* 108
3.1.6.2.2.1.3 *Backup* data *website* 109
3.1.6.2.2.1.4 *Update* ke versi terbaru 109
3.1.6.2.2.1.5 Hapus *file readme.html* 109
3.1.6.2.2.2 Pengamanan pada *plugins* dan *themes website* 109
3.1.6.2.2.2.1 Pengamanan pada *plugins* dan *themes* berbahaya 109

3.1.6.2.2.2.2 *Download plugins* dan *themes* dari sumbernya 110
3.1.6.2.2.2.3 *Update plugins* dan *themes* ke versi terbaru 110
3.1.6.2.2.3 Pengamanan pada username dan password 110
3.1.6.2.2.3.1 Pengamanan pada data privasi 110
3.1.6.2.2.3.2 Pengamanan pada *username* 110
3.1.6.2.2.3.3 Pengamanan pada *password* 111
3.1.6.2.3 Pengamanan pada *open port* 111
3.1.6.2.3.1 Menutup servis yang tidak digunakan 111
3.1.6.2.3.2 Pemantau adanya serangan 111
3.1.7 Analisis Kebutuhan Komputer *Pentester* 112
3.1.7.1 Kebutuhan Perangkat Keras (*Hardware*) 112
3.1.7.2 Kebutuhan Perangkat Lunak (*Software*) 112
3.1.7.2.1 *Kali Linux Operating System* 112
3.1.7.2.2 *Kali Linux Security Tools* 113
3.2 Perancangan Sistem 113
3.2.1 Simulasi Jaringan 113
3.2.2 Perancangan *Website* Diskominfo 114
BAB 4 IMPLEMENTASI **117**
4.1 Implementasi 117
4.1.1 *Vulnerability* pada *Website* 117
4.1.1.1 *Reconnaissance* 117
4.1.1.1.1 *Online Research* 118
4.1.1.1.1.1 Google Dork 118
4.1.1.1.1.2 Exploit Database 119
4.1.1.1.2 *Footprinting* 121
4.1.1.1.2.1 Whois 121
4.1.1.1.2.2 NSLookup 123
4.1.1.1.2.3 DNSEnum 124
4.1.1.2 *Scanning* 130
4.1.1.2.1 *Network Scanning* 130
4.1.1.2.2 *Vulnerability Scanning* 131

4.1.1.2.2.1 Pengecekan Aplikasi Web 131
4.1.1.2.2.2 Whatweb 131
4.1.1.2.2.3 WPScan 134
4.1.1.2.2.3.1 WPScan *vulnerability* pada *engine website* 135
4.1.1.2.2.3.2 WPScan *vulnerability* pada *themes website* 137
4.1.1.2.2.3.3 WPScan *vulnerability* pada *plugins website* 138
4.1.1.2.2.3.4 WPScan *vulnerability* pada *username website* 142
4.1.1.2.3 *Port Scanning* 143
4.1.2 Rangkuman *Scanning Vulnerability* 144
4.1.2.1 Proses *Scanning* Whois 144
4.1.2.2 Proses *Scanning* NSLookup 144
4.1.2.3 Proses *Scanning* DNSEnum 144
4.1.2.4 Proses *Network Scanning* 145
4.1.2.5 Proses *Scanning* Whatweb 145
4.1.2.6 Proses WPScan *Vulnerability Engine Website* 145
4.1.2.7 Proses WPScan *Vulnerability Themes Website* 146
4.1.2.8 Proses WPScan *Vulnerability Plugins Website* 146
4.1.2.9 Proses WPScan *Vulnerability Username Website* 147
4.1.2.10 Proses *Port Scanning* 147
4.2 Pengujian 148
4.2.1 Pengujian pada *Script Core Engine Website* 148
4.2.2 Pengujian pada *Plugins Website* 150
4.2.3 Pengujian pada *Themes* 153
BAB 5 KESIMPULAN DAN SARAN 155
5.1 Kesimpulan 155
5.2 Saran 155
DAFTAR PUSTAKA 157