

## DAFTAR ISI

<b>ABSTRAK.....</b>	<b>i</b>
<b>ABSTRACT .....</b>	<b>ii</b>
<b>KATA PENGANTAR.....</b>	<b>iii</b>
<b>DAFTAR ISI.....</b>	<b>v</b>
<b>DAFTAR GAMBAR .....</b>	<b>viii</b>
<b>DAFTAR TABEL.....</b>	<b>x</b>
<b>DAFTAR SIMBOL .....</b>	<b>xiii</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>xvi</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1    Latar Belakang.....	1
1.2    Rumusan Masalah.....	3
1.3    Maksud dan Tujuan .....	3
1.3.1    Maksud .....	3
1.3.2    Tujuan.....	3
1.4    Batasan Masalah .....	3
1.5    Metodologi Penelitian.....	5
1.5.1    Identifikasi Masalah .....	7
1.5.2    Pengumpulan Data .....	7
1.5.3    Perencanaan dan Persiapan Penetrasi.....	7
1.5.4    Implementasi .....	8
1.5.5    Pemberian Solusi dan Kesimpulan.....	9
1.6    Sistematika Penulisan .....	9
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>11</b>
2.1    Tinjauan Perusahaan .....	11
2.1.1    Profil Perusahaan PT. Dataquest Leverage Indonesia.....	11
2.1.2    Visi dan Misi PT. Dataquest Laverage Indonesia .....	12
2.1.3    Logo Perusahaan .....	13
2.1.4    Struktur Organisasi Perusahaan.....	14
2.1.5    Struktur Organisasi Proyek.....	14
2.1.6    Deskripsi Tugas dan Tanggung Jawab .....	14

2.2	Landasan Teori .....	17
2.2.1	Keamanan Sistem Informasi .....	17
2.2.2	Website .....	19
2.2.3	Web Server .....	19
2.2.4	PHP .....	20
2.2.4.1	Tipe Data .....	21
2.2.4.2	Jenis Tipe Data .....	21
2.2.5	Penetration Testing.....	23
2.2.6	Metode ISSAF .....	25
2.2.7	Terminologi – Terminologi Dasar Dalam Keamanan Sistem ....	27
2.2.7.1	Vulnerability.....	27
2.2.7.2	Threat.....	28
2.2.8	Serangan Siber.....	28
2.2.8.1	Shell Backdoor .....	29
2.2.8.2	Web Deface .....	29
2.2.9	Firewall.....	30
2.2.9.1	Jenis – Jenis Firewall.....	31
2.2.9.2	Mengatur Dan Mengontrol Lalu Lintas Jaringan .....	33
<b>BAB III ANALISIS DAN PERANCANGAN SISTEM.....</b>	<b>36</b>	
3.1	Analisis Masalah.....	36
3.2	Analisis Sistem .....	36
3.2.1	Analisis Studi Kasus.....	36
3.2.2.	Topologi Jaringan.....	37
3.2.3	Metode ISSAF .....	38
3.2.3.1	Planning and Preparation.....	41
3.2.3.2	Assessment .....	41
3.2.3.3	Repoting .....	72
3.2.3.4	Clean Up and Destroying Artefacs.....	79
3.2.4	Analisis Non-fungsional .....	79
3.2.4.1	Analisis Perangkat Keras.....	79
3.2.4.2	Analisis Perangkat Lunak.....	79

<b>BAB IV IMPLEMENTASI .....</b>	<b>80</b>
4.1    Implementasi Sistem.....	80
4.2    Implementasi Perangkat Keras .....	80
4.3    Implementasi Perangkat Lunak .....	80
4.4    Implementasi Penetration Testing .....	81
4.4.1    Planning (Perencanaan).....	81
4.4.2    Assessment (Penilaian) .....	81
4.4.2.1    Information Gathering.....	81
4.4.2.2    Network Mapping .....	88
4.4.2.3    Vulnerability Identification .....	89
4.4.2.4    Penetration Testing.....	90
4.4.2.5    Gaining access and privilege escalation.....	96
4.4.2.6    Enumerating Futher.....	98
4.4.2.7    Compromise remote user/sites .....	99
4.4.2.8    Maintaining Access .....	101
4.4.2.9    Covering Tracks .....	102
4.4.3    Repoting .....	103
4.4.3.1    Ruang Lingkup.....	103
4.4.3.2    Tools yang digunakan .....	103
4.4.3.3    Exploit yang digunakan.....	103
4.4.3.4    Waktu dan tempat dilakukan pentest .....	104
4.4.3.5    Hasil implementasi.....	104
4.4.3.6    Daftar kerentanan yang ditemukan .....	110
4.4.4    Clean up and destroying artefact.....	111
4.4.5    Pemberian rekomendasi .....	112
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>117</b>
5.1    Kesimpulan dan Saran .....	117
<b>DAFTAR PUSTAKA .....</b>	<b>118</b>
<b>LAMPIRAN.....</b>	<b>120</b>