

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL	xi
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN	xv
DAFTAR ISTILAH	xvi
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Tujuan Penelitian	3
1.4. Batasan Penelitian	3
1.5. Manfaat Penelitian	4
1.6. Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1. Literatur Terkait Teori.....	5
2.2. Dasar Teori.....	13
2.2.1. Sistem Informasi	13
2.2.2. Keamanan Sistem Informasi	13
2.2.3. <i>Black Box Testing</i>	15
2.2.4. Uji Penetrasi	16
2.2.5. <i>Information System Security Assessment (ISSAF)</i>	17

2.2.6.	<i>Common Vulnerability Scoring System (CVSS)</i>	20
2.2.7.	VMWare.....	26
2.2.8.	Alat-Alat Dalam Uji Penetrasi	27
2.2.9.	Teknik Serangan Uji Penetrasi.....	31
BAB III METODOLOGI PENELITIAN		33
3.1.	Sistematika Penyelesaian Masalah.....	33
3.2.	Prosedur Penelitian.....	34
3.2.1.	<i>Planning and Preparation</i>	34
3.2.2.	<i>Assessment</i>	35
3.2.3.	<i>Reporting, Clean Up and Destroy Artefacts</i>	37
3.3.	Metode Penelitian.....	39
3.4.	Alat dan Bahan Penelitian.....	40
3.4.1.	<i>Hardware</i>	40
3.4.2.	<i>Software</i>	40
BAB IV PENGUMPULAN DAN PENGOLAHAN DATA.....		42
4.1.	<i>Planning and Preparation</i>	42
4.1.1.	Studi Literatur	42
4.1.2.	Wawancara.....	42
4.1.3.	<i>Information Gathering</i>	43
4.1.3.1.	Pencarian Internet.....	44
4.1.3.2.	Wappalyzer	44
4.1.3.3.	Nslookup	45
4.1.3.4.	Whois	46
4.1.3.5.	Hasil <i>information gathering</i>	48
4.1.4.	<i>Network Mapping</i>	49
4.1.4.1.	Nmap.....	49

4.1.4.2.	Sslabs	50
4.1.4.3.	Hasil <i>network mapping</i>	51
BAB V ANALISIS DAN PEMBAHASAN.....		53
5.1.	<i>Assessment</i>	53
5.1.1.	<i>Vulnerability Assessment</i>	53
5.1.1.1.	OWASP ZAP	53
5.1.1.2.	Nikto.....	58
5.1.1.3.	Manual Test.....	59
5.1.1.4.	Hasil <i>vulnerability identification</i>	62
5.1.2.	<i>Penetration Testing</i>	63
5.1.2.1.	XSS	63
5.1.2.2.	SQL Injection	65
5.1.2.3.	<i>Local File Inclusion (LFI)</i>	68
5.1.2.4.	Hasil <i>penetration testing</i>	69
5.1.3.	<i>Gaining Access and Privilege Escalation</i>	70
5.1.3.1.	Hasil <i>gaining access and privilege escalation</i>	72
5.1.4.	<i>Enumerating Further</i>	72
5.1.4.1.	Hasil <i>enumerating further</i>	75
5.1.5.	<i>Compromise Remote User/Sites</i>	76
5.1.5.1.	Netcat	77
5.1.5.2.	Hasil <i>compromise remote user</i>	77
5.1.6.	<i>Maintaining Access</i>	78
5.1.7.	<i>Covering Tracks</i>	79
5.2.	<i>Reporting, Clean Up and Destroy</i>	79
5.2.1.	Analisis dan Pembahasan Data Hasil Uji.....	79
5.2.2.	Skala Prioritas Perbaikan	93

5.2.3.	Validasi <i>Expert</i>	103
5.2.4.	<i>Clean Up, and Destroy Artefacts</i>	104
5.2.5.	Konfirmasi Hasil Temuan dan Pemberian Rekomendasi	105
BAB VI KESIMPULAN DAN SARAN.....		107
6.1.	Kesimpulan	107
6.2.	Saran.....	108
DAFTAR PUSTAKA		109
LAMPIRAN.....		115
	Lampiran Surat Pengantar dan Pengambilan Data	115
	Lampiran Temuan Pengujian	116
	Lampiran Wawancara.....	122
	Lampiran Perjanjian Kerahasiaan Pengujian Bertanda Tangan	126
	Lampiran Profil Validator	127
	Lampiran Sertifikat Validator.....	129
	Lampiran Surat Pernyataan Kerahasiaan Validator	130
	Lampiran Lembar Validasi.....	131
	Lampiran Dokumen <i>Report ISSAF</i>	132