

## DAFTAR ISI

ABSTRAK.....	i
ABSTRACT.....	ii
KATA PENGANTAR .....	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR .....	viii
DAFTAR TABEL.....	x
DAFTAR LAMPIRAN.....	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang masalah .....	1
1.2 Identifikasi Masalah .....	3
1.3 Maksud dan Tujuan .....	3
1.4 Batasan Masalah.....	4
1.5 Metodologi Penelitian .....	4
1.6 Metode Pengumpulan Data .....	4
1.7 Alur Penelitian.....	5
1.8 Sistematika Penulisan.....	6
BAB II LANDASAN TEORI.....	9
2.1. Profil Dan Tempat Penelitian .....	9
2.1.1 Profil Dinas Komunikasi Dan Informatika Bandung .....	9
2.1.2 Visi dan Misi .....	10
2.1.3 Struktur Organisasi.....	11
2.2 Landasan Teori .....	11
2.2.1 Penetrating Testing Execution Standard (PTES) .....	11
2.2.1.1 <i>Pre-Engagement Interaction</i> .....	12
2.2.2 <i>Information Systems Security Assessment Framework (ISSAF)</i> .....	15
2.2.3 <i>Open Web Application Security Project (OWASP)</i> .....	18
2.2.4 <i>Accunetix</i> .....	20
2.2.5 <i>Risk Rating Methodology</i> .....	21

BAB III ANALISA DAN PERANCANGAN SISTEM.....	27
3.1. Analisis Sistem.....	27
3.2 Analisis <i>Framework</i> .....	27
3.2.1 <i>The Penetration Execution Standard (PTES)</i> .....	27
3.2.1.1 <i>Pre-Engagement Interaction</i> .....	28
3.2.1.2 <i>Intelligence Gathering</i> .....	28
3.2.1.3 <i>Vulnerability Analysis</i> .....	32
3.2.1.4 <i>Exploitation</i> .....	34
3.3.2 <i>Information System Security Assesment Framework (ISSAF)</i> .....	36
3.3.2.1 <i>Information Gathering</i> .....	37
3.3.2.2 <i>Network Mapping</i> .....	38
3.3.2.3 <i>Vulnerability Identification</i> .....	41
3.3.2.4 <i>Penetration</i> .....	43
3.3.2.5 <i>Gaining Acces &amp; Privilege Escalation</i> .....	45
3.3.2.6 <i>Enumerate Further</i> .....	45
3.3.2.7 <i>Compromise Remote User/Sites</i> .....	46
3.3.2.8 <i>Maintaining Access</i> .....	46
3.3.2.9 <i>Covering The Track</i> .....	46
3.3.2.10 <i>Reporting</i> .....	46
3.3.2.11 <i>Clean And Destroy Artifacts</i> .....	46
3.3.3 <i>Open Web Application Security Project (OWASP)</i> .....	46
3.3.3.1 Reconaissancc .....	47
3.3.3.2 <i>Scanning</i> .....	51
3.3.3.3 <i>Exploitation</i> .....	54
3.3.3.4 <i>Maintaining Access</i> .....	56
3.3.3.5 <i>Reporting</i> .....	56
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM .....	59
4.1 <i>The Penetration Execution Standard (PTES)</i> .....	59
4.1.1 <i>Pre-Engagement Interaction</i> .....	59
4.1.2 <i>Intelligence Gathering</i> .....	59
4.1.3 <i>Vulnerability Analysis</i> .....	61
4.1.4 <i>Explotation</i> .....	63

4.1.5	<i>Reporting</i> .....	64
4.1.5.1	<i>Executive Level Reporting</i> .....	64
4.1.5.2	<i>Technical Reporting</i> .....	66
4.2	<i>Information System Security Assesment Framework (ISSAF)</i> .....	67
4.2.1	<i>Information Gathering</i> .....	67
4.2.2	<i>Network Mapping</i> .....	68
4.2.3	<i>Vulnerability Identification</i> .....	69
4.2.4	<i>Penetration</i> .....	71
4.2.5	<i>Reporting</i> .....	72
4.2.5.1	<i>Management Summary</i> .....	72
4.2.5.2	<i>Scope Of The Project</i> .....	73
4.2.5.3	<i>Vulnerability Scan Report</i> .....	73
4.2.5.4	<i>Exploit Report</i> .....	73
4.3	<i>Open Web Application Security Project (OWASP)</i> .....	74
4.3.1	<i>Reconnaissance</i> .....	74
4.3.2	<i>Scanning</i> .....	77
4.3.3	<i>Exploitation</i> .....	78
4.3.4	<i>Reporting</i> .....	79
4.3.4.1	<i>Likelihood</i> .....	80
4.3.4.2	<i>Impact</i> .....	84
4.3.4.3	<i>Klasifikasi Kerentanan</i> .....	87
4.5	<i>Analisis Perbedaan Framework</i> .....	88
BAB V KESIMPULAN DAN SARAN .....		91
5.1.	<i>Kesimpulan</i> .....	91
DAFTAR PUSTAKA .....		93