

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR ORISINALITAS	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR.....	vi
UCAPAN TERIMA KASIH	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	6
1.3 Tujuan dan Manfaat.....	6
1.4 Batasan Masalah	7
1.5 Metode Penelitian	7
BAB II TINJAUAN PUSTAKA	9
2.1 Kajian Pustaka	9
2.2 Landasan Teori	19
2.2.1 Analisis	19
2.2.2 <i>Website</i>	19
2.2.3 Keamanan Jaringan.....	19
2.2.4 <i>Web Server</i>	21

2.2.5	<i>Penetration Testing</i>	21
2.2.6	<i>Penetration Testing Excecution Standard (PTES)</i>	22
2.2.7	<i>Kali Linux</i>	24
2.2.8	<i>VirtualBox</i>	25
2.2.9	<i>OWASP ZAP</i>	26
2.2.10	<i>NMAP</i>	27
2.2.11	<i>Xray</i>	28
2.2.12	<i>SQL Injection</i>	29
2.2.13	<i>XSS (Cross Site Scripting)</i>	29
2.2.14	<i>DdoS</i>	30
BAB III	METODE PENELITIAN	31
3.1	Subjek dan Objek Penelitian.....	31
3.2	Alat dan Bahan	31
3.2.1	Alat	31
3.2.2	Objek Penelitian	33
3.3	Diagram Alir Penelitian.....	34
3.3.1	Pengumpulan Data.....	35
3.3.2	Studi Literatur.....	35
3.3.3	Identifikasi dan Perumusan Masalah.....	35
3.3.4	Impelementasi <i>Penetration Testing Execution Standard (PTES)</i>	35
3.3.3.1	<i>Pre-engagement Interaction</i>	36
3.3.3.2	<i>Intelligence Gathering</i>	36
3.3.3.3	<i>Threat Modeling</i>	36
3.3.3.4	<i>Vulnerability Analysis</i>	37
3.3.3.5	<i>Exploitation</i>	37

3.3.3.6	<i>Post Exploitation</i>	37
3.3.3.7	<i>Reporting</i>	37
BAB IV HASIL DAN PEMBAHASAN		39
4.1	<i>Pre-engagement Interaction</i>	39
4.2	<i>Intelligence Gathering</i>	39
4.3	<i>Threat Modeling</i>	43
4.4	<i>Vulnerability Analysis</i>	44
4.4.1	Analisis dengan tools OWASP ZAP	44
4.4.2	Analisis Menggunakan Xray	50
4.5	Exploitation	52
4.5.1	<i>SQL Injection</i>	52
4.5.2	<i>XSS (Cross-Site Scripting)</i>	54
4.5.3	<i>Clickjacking</i>	56
4.5.4	<i>Distributed Denial of Service (DDoS)</i>	57
4.6	Post Exploitation	59
4.7	Reporting	61
BAB V KESIMPULAN DAN SARAN		65
5.1	Kesimpulan	65
5.2	Saran	66
DAFTAR PUSTAKA		67
LAMPIRAN		72