

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
LEMBAR PENGESAHAN	iii
HALAMAN PERNYATAAN ORSINALITAS	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
DAFTAR ISTILAH	xi
DAFTAR LAMPIRAN	xii
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	3
I.3 Tujuan Penelitian	3
I.4 Batasan Penelitian	3
I.5 Manfaat Penelitian	4
BAB II TINJAUAN PUSTAKA	5
II.1 Penelitian Terdahulu	5
II.2 Keamanan Informasi	9
II.2.1 <i>Web</i>	9
II.2.2 <i>Vulnerability</i>	13
II.2.3 <i>Penetration</i>	13
II.2.4 <i>Vulnerability assessment and Penetration testing (VAPT)</i>	13
II.2.5 <i>VMware</i>	15

II.2.6	<i>Kali Linux</i>	16
II.2.7	NMAP	16
II.2.8	Nessus	16
II.2.9	OWASP ZAP	16
II.2.10	Nikto.....	17
BAB III	METODOLOGI PENELITIAN	18
III.1	Kerangka Berpikir	18
III.2	Sistematika Penyelesaian Masalah.....	19
III.3	Pengumpulan Data	22
III.4	Pengolahan Data.....	22
III.5	Metode Evaluasi	23
III.6	Alasan Pemilihan Metode.....	24
BAB IV	RANCANGAN PENGUJIAN.....	25
IV.1	<i>Scope</i>	25
IV.2	Perancangan Pengujian.....	25
IV.2.1	Perangkat Hardware	25
IV.2.2	Perangkat <i>Software</i>	26
IV.3	<i>Information gathering</i>	26
IV.3.1	Hasil Pengujian menggunakan NMAP	26
IV.4	<i>Vulnerability detection</i>	28
IV.4.1	Pengujian menggunakan Nessus	29
IV.4.2	Pengujian menggunakan OWASP ZAP.....	31
IV.4.3	Pengujian menggunakan Nikto	32
IV.4.4	<i>List Vulnerability</i>	38
IV.4.5	<i>Penetration Testing</i>	41
Bab V	HASIL PENGUJIAN	55

V.1	<i>Remediation</i>	55
V.1.1	Perancangan Mitigasi	55
V.2	Pengujian Ulang Pasca Mitigasi	59
Bab VI	KESIMPULAN DAN SARAN	62
VI.1	Kesimpulan	62
VI.2	Saran	63
DAFTAR PUSTAKA		xii
LAMPIRAN		xiv