

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
PRAKATA	iv
ARTI LAMBANG DAN SINGKATAN	vi
ABSTRACT	ix
INTISARI	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	6
1.3 Kontribusi Penelitian	6
1.4 Tujuan Penelitian	10
1.5 Manfaat penelitian	10
1.6 Batasan masalah	10
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	11
2.1 Tinjauan Pustaka	11
2.1.1 Asesmen keamanan	11
2.1.2 Keamanan Sistem dan Uji Penetrasi	12
2.1.3 <i>Information Systems Security Assessment Framework (ISSAF)</i>	12
2.1.4 Perkembangan <i>OWASP TOP 10</i>	18
2.2 Landasan Teori	18
2.2.1 Keamanan Informasi	18
2.2.2 <i>Information Systems Security Assessment Framework (ISSAF)</i>	21
2.2.3 Uji Penetrasi	21
2.2.4 Perbedaan antara <i>penetration tester</i> dan <i>attacker</i>	22
2.2.5 Tujuan Uji Penetrasi	22
2.2.6 Klasifikasi Uji Penetrasi	23
2.2.6.1 Uji Berdasarkan Informasi	23
2.2.6.2 Uji Berdasarkan Keagresifan	24
2.2.6.3 Uji Berdasarkan Ruang Lingkup	24
2.2.6.4 Uji Berdasarkan Pendekatan	25
2.2.6.5 Uji Berdasarkan Teknik Yang Digunakan	25
2.2.6.6 Uji berdasarkan Titik Awal Serangan	26
2.2.7 Jenis Metode Uji Penetrasi	26
2.2.8 <i>Open Web Application Security Project Top Ten 2017</i>	27
2.2.9 <i>OWASP Risk Rating Methodology</i>	30
2.2.9.1 Identifikasi Resiko	30
2.2.9.2 Faktor Memperkirakan Kemungkinan	30
2.2.9.2.1 Faktor <i>Threat Agent</i>	31
2.2.9.2.2 Faktor <i>Vulnerability</i>	31
2.2.9.3 Faktor Memperkirakan Dampak	32
2.2.9.3.1 Faktor <i>Technical impact</i>	33

2.2.9.3.2	Faktor <i>Business Impact</i>	33
2.2.9.4	Menentukan Tingkat Keparahan Resiko	35
2.3	Pertanyaan Penelitian	35
BAB III	METODOLOGI	36
3.1	Bahan Penelitian	36
3.2	Alat Penelitian	36
3.3	Diagram Alur Penelitian	39
3.3.1	Telaah dan Kondisi Sistem Keamanan Objek Penelitian	40
3.3.2	Pemilihan Metode Pengujian	45
3.3.3	Tahap Uji Penetrasi	48
3.3.3.1	<i>Planning and Preparation</i>	48
3.3.3.2	<i>Assessment</i>	48
3.3.3.2.1	<i>Information Gathering</i>	49
3.3.3.2.2	<i>Network Mapping</i>	50
3.3.3.2.3	<i>Vulnerability Identifiaction</i>	50
3.3.3.2.4	<i>Exploitation</i>	50
3.3.3.2.5	<i>Gaining Access & Privilege Escalation</i>	51
3.3.3.2.6	<i>Maintaining Access & Covering Tracks</i>	51
3.3.3.3	<i>Reporting and Cleaning</i>	52
3.3.3.3.1	Solusi Dan penyajian data.....	52
3.3.3.3.2	Menentukan Tingkat Keparahan Dampak	52
3.3.3.3.2.1	Menilai Faktor <i>Agent</i>	53
3.3.3.3.2.2	Menilai Faktor <i>Vulnerability</i>	54
3.3.3.3.2.3	Menilai Faktor <i>Technical Impact</i>	54
3.3.3.3.2.4	Menilai Faktor <i>Business Impact</i>	55
3.3.3.3.2.5	Menilai Dampak Resiko.....	56
BAB IV	HASIL DAN PEMBAHASAN	59
4.1	<i>Planning and Preparation</i>	59
4.2	<i>Assessment</i>	60
4.2.1	<i>Information Gathering</i>	60
4.2.2	<i>Network Mapping</i>	66
4.2.3	<i>Vulnerability Identification</i>	71
4.2.3.1	<i>Vulnerability Identification citee.te.ugm.ac.id</i>	72
4.2.3.2	<i>Vulnerability Identification cna.te.ugm.ac.id</i>	74
4.2.3.3	<i>Vulnerability Identification hci.te.ugm.ac.id</i>	75
4.2.3.4	<i>Vulnerability Identificationme.te.ugm.ac.id</i>	76
4.2.3.5	<i>Vulnerability Identification pasca.jteti.ugm.ac.id</i>	77
4.2.3.6	<i>Vulnerability Identification pervasive.te.ugm.ac.id</i>	78
4.2.3.7	<i>Vulnerability Identificationplc.jteti.ugm.ac.id</i>	79
4.2.3.8	<i>Vulnerability Identification te.ugm.ac.id</i>	80
4.2.4	<i>Exploitation</i>	81
4.2.4.1	<i>Exploitation cna.te.ugm.ac.id</i>	81
4.2.4.2	<i>Exploitation me.te.ugm.ac.id</i>	82
4.2.4.3	<i>Exploitation pasca.jteti.ugm.ac.id</i>	84
4.2.5	<i>Gaining Access & Privilege Escalation</i>	85
4.2.6	<i>Maintaining Access & Covering Tracks</i>	88

4.3	<i>Reporting and Cleaning</i>	89
4.3.1	<i>Executive Summary</i>	89
4.3.2	<i>Summary Finding</i>	90
4.3.3	<i>Attack Summary</i>	91
4.3.4	Ringkasan Akhir	94
4.3.5	Rekomendasi	94
4.3.6	Solusi dan penyajian data.....	95
4.3.7	Menentukan Dampak.....	98
4.3.7.1	Menilai Faktor <i>Threat Agent</i>	98
4.3.7.2	Menilai Faktor <i>Vulnerability</i>	99
4.3.7.3	Menilai Faktor <i>Technical Impact</i>	100
4.3.7.4	Menilai Faktor <i>Business Impact</i>	101
4.3.7.5	Menilai Dampak Resiko	103
4.4	Pembahasan.....	106
4.4.1	Kelebihan Dan Kelemahan ISSAF	109
BAB V	Kesimpulan dan Saran	111
5.1	Kesimpulan	111
5.2	Saran	112
DAFTAR PUSTAKA	113
LAMPIRAN	116