

## DAFTAR ISI

ABSTRAK	iii
ABSTRACT	iv
LEMBAR PENGESAHAN	v
LEMBAR PERNYATAAN ORISINALITAS	vi
KATA PENGANTAR	i
DAFTAR ISI	iii
DAFTAR GAMBAR	vi
DAFTAR TABEL	ix
Daftar Lampiran	x
BAB I PENDAHULUAN	11
I.1 Latar Belakang	11
I.2 Rumusan Masalah	14
I.3 Tujuan dan Manfaat	14
I.4 Batasan Masalah	15
I.5 Metodologi Penelitian	16
BAB II TINJAUAN PUSTAKA	17
II.1 Penelitian Terdahulu	17
II.2 Dasar Teori	23
II.2.1 Sistem Informasi	23
II.2.2 Keamanan Sistem Informasi	24
II.2.4 ISSAF (Information System Security Assessment Framework)	25
II.2.5 Black Box Testing	26
II.2.6 Kali Linux	26
II.2.7 Shodan	26
II.2.8 Censys	27
II.2.9 NMAP	27

II.2.10 SQL MAP	27
II.2.11 Nikto	27
II.2.12 Zap	28
II.2.13 Legion	29
II.2.14 Hydra	29
II.2.15 Wireshark	29
II.2.16 Cookie manager	29
II.2.17 Vulnerability assessment	30
II.2.18 Cross-Site Request Forgery (CSRF)	30
II.2.19 Session Hijacking	30
II.2.20 Cross-Site Scripting (XSS)	31
II.2.21 SQL Injection (SQLI)	31
II.2.22 Insecure Direct Object Reference (IDOR)	31
II.2.23 Bruteforce attack	32
II.2.25 SSL/TLS	32
II.2.26 Domain Name Server	32
II.2.27 Cookies	33
BAB III METODOLOGI	34
III.1 Metode Penelitian	34
III.2 Alat dan Bahan Penelitian	34
III.3 Prosedur Penelitian	36
III.3.1 Menentukan Topik	37
III.3.2 Studi Literatur	37
III.3.3 Planing and preparation	37
III.3.4 Assesment	37
III.3.5 Reporting, Clean – up and Destroy Artefacts	
39	
III.4 Deskripsi Objek	41

BAB IV HASIL DAN PEMBAHASAN	42
IV.1 Planing and preparation	42
IV.1 Wawancara dan Observasi	42
IV.1.2 Pembelian Server dummy	42
IV.1.3 Instalasi e-raport pada server dummy	42
IV.2 Assesment	42
IV.2.1 Information Gathering	42
IV.2.2 Network mapping	44
IV.2.3 Vulnerability Identification	53
IV.2.4 Penetration Testing	64
IV.2.5 Gaining Access and Privilege Escalation	65
IV.2.6 Enumerating Further	68
IV.2.7 Compromise Remote User/Sites	69
IV.2.8 Maintaning Access	69
IV.2.9 Corvering Tracks	70
IV.3 Hasil Temuan dan Rekomendasi	70
IV.3.1 Hasil dan rekomendasi pada server dummy	70
IV.3.2 Hasil dan rekomendasi pada server production	78
IV.4 Reporting dan Clean-up and Destroy Artefacts	83
BAB V KESIMPULAN DAN SARAN	86
V.1 Kesimpulan	86
V.1.1 Kondisi keamanan sistem informasi	86
V.1.2 Hasil Pengujian	87
V.1.3 Rekomendasi Pengujian	89
V.2 Saran	90
BAB VI DAFTAR PUSTAKA	92
LAMPIRAN	96

Lampiran I. Surat balasan pihak sekolah	96
Lampiran II. Dokumen hasil wawancara	97
Lampiran III. Dokumentasi wawancara	102
Lampiran IV Spesifikasi minimum untuk eraport	103
Lampiran V Tahap instalasi e-raport	103
Lampiran VI Registrasi e-raport	105
Lampiran VII Pembelian server dummy	105
Lampiran VIII. Dokumen hasil reporting	106
Lampiran XI. Dokumentasi hasil reporting	107