

## DAFTAR ISI

HALAMAN PENGESAHAN .....	ii
HALAMAN PERSEMBAHAN .....	iv
KATA PENGANTAR .....	v
DAFTAR ISI .....	vi
DAFTAR TABEL .....	ix
DAFTAR GAMBAR .....	x
DAFTAR SINGKATAN .....	xiv
INTISARI .....	xvii
ABSTRACT .....	xviii
BAB I. PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	4
1.3 Batasan Tugas akhir .....	5
1.4 Tujuan Tugas akhir .....	5
1.5 Manfaat Tugas akhir .....	5
1.6 Sistematika Tugas Akhir .....	5
BAB II. TINJAUAN PUSTAKA DAN DASAR TEORI .....	7
2.1 Tinjauan Pustaka .....	7
2.2 Dasar Teori .....	10
2.2.1. Fundamental Keamanan Informasi .....	10
2.2.2. Hacker .....	15
2.2.3. Tim Keamanan Informasi .....	17
2.2.4. Kali Linux .....	22
2.2.5. Metasploit Framework .....	23
2.2.6. Bahasa Pemrograman Python .....	31
2.2.7. Process-Memory Organization .....	32

2.2.8.	Memory Segment.....	37
2.2.9.	Buffer Overflow.....	38
2.2.10.	Bahasa Pemrograman C.....	45
2.2.11.	<i>Debugger</i> .....	46
2.2.12.	Assembly.....	49
2.2.13.	Kode berbahaya ( <i>ShellCode</i> ).....	53
2.2.14.	SandBox.....	55
2.2.15.	Virtual Machine VirtualBox.....	55
2.2.16.	Sistem Operasi Windows XP.....	57
2.2.17.	Sistem Operasi Ubuntu.....	58
2.2.18.	FTP Server.....	58
2.2.19.	CVE-2013-4730.....	59
<b>BAB III.</b>	<b>METODE TUGAS AKHIR.....</b>	<b>61</b>
3.1	Alat dan Bahan.....	61
3.1.1.	Perangkat Keras.....	61
3.1.2.	Perangkat Lunak.....	61
3.2	Metode Penelitian Tugas Akhir.....	62
3.3	Diagram Alir Penelitian.....	64
3.2.1.	Studi Literatur.....	65
3.2.2.	Analisis Kebutuhan dan Persiapan Alat dan Bahan.....	66
3.2.3.	Penetration Test.....	70
3.2.4.	Analisis Data dan Penulisan Laporan.....	79
<b>BAB IV.</b>	<b>HASIL DAN PEMBAHASAN.....</b>	<b>80</b>
4.1	Pra-simulasi.....	80
4.2	Simulasi Pada Target Pertama.....	85
4.1.1.	Pembuatan FTP Client.....	85
4.1.2.	Vulnerability Analysis.....	87

4.1.3.	Exploitation.....	92
4.1.4.	Post Exploitation.....	96
4.3	Simulasi pada Target Kedua.....	101
4.2.1.	Pembuatan Program Rentan.....	101
4.2.2.	Vulnerability Analysis .....	104
4.2.3.	Exploitation.....	106
4.2.4.	Eksploitasi Tanpa Keamanan.....	108
4.2.5.	Eksploitasi Dengan ASLR. ....	109
4.2.6.	Eksploitasi Dengan DEP.....	111
4.2.7.	Eksploitasi Dengan <i>Stack Protector</i> .....	113
4.2.8.	Eksploitasi Dengan kode yang Sudah Diperbaiki.....	115
4.4	Kelebihan dan Kekurangan Tugas Akhir .....	117
4.5.1.	Kelebihan Tugas Akhir .....	117
4.5.2.	Kekurangan Tugas Akhir .....	117
BAB V.	KESIMPULAN DAN SARAN.....	119
5.1	Kesimpulan .....	119
5.2	Saran .....	119
DAFTAR PUSTAKA.....		120