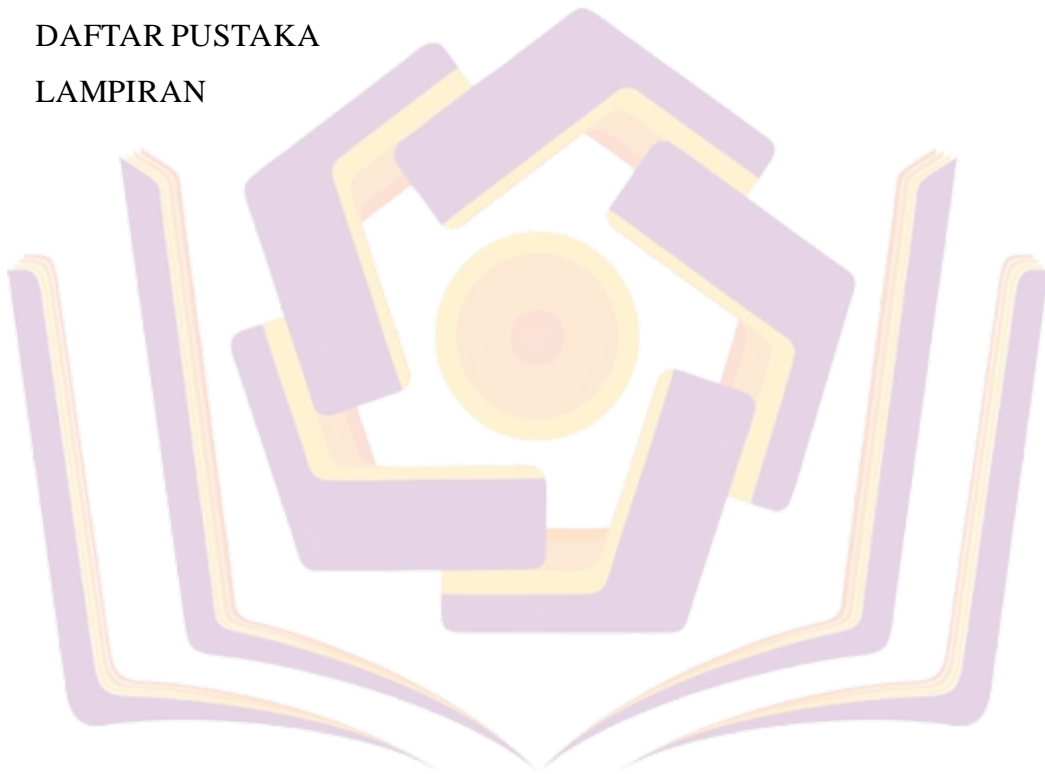


DAFTAR ISI

HALAMAN SAMBUTAN.....	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN.....	vi
HALAMAN MOTTO	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN.....	xvi
INTISARI.....	xvii
<i>ABSTRACT</i>	xviii
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah.....	1
B. Rumusan Masalah	5
C. Batasan Masalah	6
D. Tujuan Penelitian	6
E. Manfaat Penelitian	7
BAB II TINJAUAN PUSTAKA.....	8
A. Landasan Teori.....	8
B. Penelitian Sebelumnya	12
BAB III METODE PENELITIAN.....	17
A. Tempat dan Waktu Penelitian	17
B. Metode Pengumpulan Data.....	17
C. Alat dan Bahan Penelitian.....	18
D. Konsep Penelitian	19

BAB IV HASIL DAN PEMBAHASAN	27
A. Identifikasi Masalah	27
B. Pembuatan <i>Ransomware</i>	28
C. Simulasi Serangan	40
D. Analisis Mekanisme Kerja <i>Ransomware</i>	46
BAB V PENUTUP	51
A. Kesimpulan	51
B. Saran	52
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2.1. Perbandingan Dengan Penelitian Terdahulu	16
---	----



DAFTAR GAMBAR

Gambar 3.4. 1. Konsep Penelitian.....	20
Gambar 3.4. 2. Metode Linear Sequential Process	22
Gambar 3.4. 3. Alur Simulasi Serangan.....	25
Gambar 4.2. 1. Instalasi Python	29
Gambar 4.2. 2. Instalasi Pycryptodome	30
Gambar 4.2. 3. Instalasi Pyinstaller	30
Gambar 4.2. 4. Pembuatan Tebusan.....	31
Gambar 4.2. 5. Kode Program Mengambil Direktori Profil Pengguna.....	32
Gambar 4.2. 6. Program Menetapkan Direktori Target	32
Gambar 4.2. 7. Program excecludeExtention.....	33
Gambar 4.2. 8. Kode Program key_file	33
Gambar 4.2. 9. Kode Program scanRecurse.....	34
Gambar 4.2. 10. Kode Program fungsi scanRecurse().....	35
Gambar 4.2. 11. Kode Program encrypt_file().....	36
Gambar 4.2. 12. Kode Program Fungsi create_ransom_note().....	37
Gambar 4.2. 13. Kode Program implementasi main()	39
Gambar 4.2. 14. Hasil Pengubahan Ekstensi	39
Gambar 4.2. 15. Testing Menggunakan Python.....	40
Gambar 4.2. 16. File Testing Sebelum dan Sesudah Terenkripsi	40
Gambar 4.3. 1. Email Phising dari Penyerang	42
Gambar 4.3. 2. Email Phising Target	43
Gambar 4.3. 3. Hasil Download dari Klik Link	43
Gambar 4.3. 4. Sebelum Terenkripsi.....	44
Gambar 4.3. 5. File Terenkripsi	45
Gambar 4.3. 6. Pesan Tebusan	45
Gambar 4.4. 1. Hasil Analisis menggunakan VirusTotal.....	47
Gambar 4.4. 2. Analisi Manual File Terenkripsi.....	48
Gambar 4.4. 3. Hasil Analisis Manual Pesan Tebusan	49

Gambar 4.4. 4. Isi File Terenkripsi49

Gambar 4.4. 5. Perbandingan Salinan File Asli dan File Terenkripsi.....50



DAFTAR LAMPIRAN

- Lampiran 1. Kode Enkripsi
- Lampiran 2. Kartu Pembimbing 1
- Lampiran 3. Kartu Pembimbing 2

