

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR ISTILAH	xiii
DAFTAR SINGKATAN	xv
Bab I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	4
I.3 Tujuan Penelitian	5
I.4 Batasan Penelitian	5
I.5 Manfaat Penelitian	5
I.6 Sistematika Penulisan	6
Bab II TINJAUAN PUSTAKA	7
II.1 <i>Wireless Fidelity</i> (Wi-Fi)	7
II.2 <i>Vulnerability Assessment</i>	8
II.3 <i>Penetration Testing</i>	8
II.4 Aspek Keamanan Informasi	9
II.4.1 <i>Confidentiality</i>	9
II.4.2 <i>Integrity</i>	9
II.4.3 <i>Availability</i>	10

II.5	Kali Linux.....	10
II.6	<i>Information System Security Assessment Framework</i>	11
II.6.1	<i>WLAN Security Assessment Methodology</i>	11
II.7	<i>Man In The Middle Attack (MITM)</i>	12
II.7.1	<i>Interception (Penyadapan)</i>	12
II.7.2	<i>Decryption (Dekripsi)</i>	15
II.8	<i>Packet sniffing</i>	16
II.9	Protokol Jaringan.....	16
II.9.1	<i>Hypertext Transfer Protocol</i>	17
II.9.2	<i>Hypertext Transfer Protocol Secure</i>	17
II.9.3	<i>HTTP Strict Transport Security</i>	18
II.9.4	<i>Secure Socket Layer</i>	19
II.9.5	<i>Transport Layer Security (TLS)</i>	19
II.10	Airgeddon	20
II.11	NMAP	21
II.12	Penelitian Sebelumnya.....	21
Bab III	SISTEMATIKA PENYELESAIAN MASALAH.....	23
III.1	Model Konseptual	23
III.2	Sistematika Penelitian	24
III.2.1	<i>Information Gathering</i>	25
III.2.2	<i>Analysis & Research</i>	25
III.2.3	<i>Exploit & Attack</i>	25
III.2.4	<i>Reporting & Presentation</i>	25
III.3	Alasan Pemilihan Metode.....	26
Bab IV	PERANCANGAN PENGUJIAN	27
IV.1	Rancangan Sistem	27

IV.1.1	<i>Hardware</i>	27
IV.1.2	<i>Software</i>	29
IV.2	Alur Perancangan Sistem	34
IV.3	Alur Pengujian.....	35
IV.4	Skenario Pengujian.....	37
IV.4.1	Skenario <i>Information gathering</i> Dengan Metode <i>Scanning</i>	37
IV.4.2	Skenario Penyerangan <i>Deauthentication</i>	38
IV.4.3	Skenario Penyerangan <i>Evil twin attack</i> Dengan <i>Captive portal</i> ...	39
IV.4.4	Skenario Penyerangan <i>Evil twin attack</i> dengan <i>Sniffing</i> dan <i>SSL Stripping</i>	41
IV.4.5	Skenario Penyerangan <i>Unauthorized access</i>	43
IV.4.6	Skenario Penyerangan <i>Telnet Attack</i>	43
Bab V	HASIL DAN ANALISIS	45
V.1	Hasil <i>Information gathering</i>	45
V.1.1	Hasil <i>Scanning</i> NMAP.....	45
V.1.2	Hasil <i>Scanning Greenbone Vulnerability Management (OpenVAS)</i>	48
V.1.3	Audit Hasil <i>Information gathering</i>	48
V.2	Hasil <i>Exploit & Attack</i>	50
V.2.1	Hasil Penyerangan <i>Deauthentication Attack</i>	50
V.2.2	Hasil Penyerangan <i>Evil twin attack</i> Dengan <i>Captive portal</i>	54
V.2.3	Hasil Penyerangan <i>Evil twin attack</i> Dengan <i>Packet Sniffing</i> dan <i>SSL Stripping</i>	58
V.2.4	Hasil Penyerangan <i>Unauthorized access</i>	63
V.2.5	Hasil Penyerangan <i>Telnet Attack</i>	65
V.3	Perbandingan Ketiga Restoran	68
V.4	Pencegahan Serangan	70

Bab VI	KESIMPULAN DAN SARAN	71
VI.1	Kesimpulan.....	71
VI.2	Saran	72
DAFTAR PUSTAKA	73