

DAFTAR ISI

INTISARI	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	x
DAFTAR ISTILAH	xi
BAB I PENDAHULUAN	
1.1 Tujuan	1
1.2 Latar Belakang	1
1.3 Spesifikasi	4
1.4 Sistematika Penulisan	5
BAB II DASAR TEORI	
2.1 Jaringan Nirkabel	6
2.2 Protokol Keamanan AAA	9
2.3 <i>Extensible Authentication Protocol (EAP)</i>	14
2.4 Kriptografi Asimetris	20
2.5 <i>Secure Socket Layer (SSL)</i>	21
BAB III PEDOMAN – PEDOMAN	
3.1 Alur Pembelajaran	28
3.2 Rangkuman Setiap Pedoman	29
3.2.1 Pedoman Praktikum Topik 1 – Pengenalan Jaringan Nirkabel	29
3.2.2 Pedoman Praktikum Topik 2 – Pengenalan dan <i>Instalasi</i> <i>Remote Access Dial In User Service (RADIUS)</i>	32

3.2.3	Pedoman Praktikum Topik 3 – Pembuatan Sistem Keamanan Jaringan Nirkabel dengan Metode <i>Protected Extensible Authentication Protocol</i> (PEAP)	33
3.2.4	Pedoman Praktikum Topik 4 – Pengujian Jaringan Nirkabel Dengan Metode <i>Dictionary Attack</i> Menggunakan <i>Aircrack-ng</i>	35
BAB IV	PENGUJIAN DAN ANALISIS	
4.1	Pengujian Metode <i>Protected Extensible Authentication Protocol</i> (PEAP)	36
4.1.1	Perancangan Jaringan	36
4.1.2	Konfigurasi Jaringan	37
4.1.3	Komponen-Komponen yang Digunakan	39
4.1.4	Hasil dan Analisis.....	40
4.2	Pengujian Serangan Terhadap Metode PEAP menggunakan <i>Dictionary Attack</i>	58
4.3	Pengujian Pedoman Praktikum	61
BAB V	KESIMPULAN DAN SARAN	
5.1	Kesimpulan	62
5.2	Saran Pengembangan Skripsi	63
DAFTAR PUSTAKA	64
LAMPIRAN	65

DAFTAR GAMBAR

Gambar 2.1.	Skema Standar 802.1X [6]	9
Gambar 2.2.	Format Paket RADIUS [7]	10
Gambar 2.3.	Cara Kerja RADIUS	13
Gambar 2.4.	Aliran Pesan EAP	15
Gambar 2.5.	PEAP Tahap 1 dan 2	19
Gambar 2.6.	Algoritma RSA	21
Gambar 2.7.	Protokol SSL <i>Handshake</i>	22
Gambar 2.8.	Sertifikat X.509	24
Gambar 2.9.	Sertifikat Digital pada Sistem Operasi <i>Windows</i> dengan format <i>.der</i>	25
Gambar 2.10	Sertifikat Digital pada Sistem Operasi <i>Linux</i> dengan Format <i>.pem</i>	26
Gambar 2.11.	Sertifikat Digital yang di <i>Capture</i> Menggunakan Perangkat Lunak <i>Wireshark</i>	27
Gambar 4.1.	Perancangan Jaringan Metode PEAP	36
Gambar 4.2.	PEAP Tahap 1 dan 2	40
Gambar 4.3.	Hasil <i>Capture</i> proses autentikasi PEAP.....	41
Gambar 4.4.	Paket EAP <i>Request Identity</i>	42
Gambar 4.5.	Paket EAP <i>Response Identity</i>	43
Gambar 4.6.	Paket EAP <i>Request Protected EAP</i> (PEAP).....	44
Gambar 4.7.	Protokol SSL <i>Handshake</i>	45
Gambar 4.8.	Paket EAP <i>Response Clie Hello</i>	46
Gambar 4.9.	Paket EAP <i>Request server Hello</i> , sertifikat server, <i>server key exchange</i> , <i>server hello done</i>	47
Gambar 4.10.	Isi Paket <i>Server Hello</i>	48
Gambar 4.11.	Isi Paket Sertifikat Digital.....	49
Gambar 4.12.	Isi Paket <i>Server Key Exchange</i>	50
Gambar 4.13.	Isi Paket <i>Server Hello Done</i>	50
Gambar 4.14.	Paket <i>Client key exchange</i> , <i>change chiper spec</i> , <i>encrypted handshake message</i>	51

Gambar 4.15. Isi dari paket <i>Client key exchange, change chiper spec, encrypted handshake message</i>	51
Gambar 4.16. Paket <i>Change chiper spec, encrypted handshake message</i>	52
Gambar 4.17. Paket <i>EAP Response – PEAP</i>	53
Gambar 4.18. Paket <i>EAP - Request Identity Dalam Tunnel TLS</i>	54
Gambar 4.19. Paket <i>EAP - Response Identity Dalam Tunnel TLS</i>	55
Gambar 4.20. <i>EAP – Success</i>	56
Gambar 4.21. Proses Monitoring Dengan <i>Aircrack</i>	59
Gambar 4.22. Pengiriman Paket Deautentikasi	59
Gambar 4.23. Proses <i>Cracking Password</i>	60



DAFTAR ISTILAH

AAA	<i>Authentication, Authorization, Accounting</i>
AP	<i>Access Point</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
DNS	<i>Domain Name System</i>
EAP	<i>Extensible Authentication Protocol</i>
CHAP	<i>Challenge Handshake Authentication Protocol</i>
EAP-TLS	<i>EAP-Transport Layer Security</i>
EAP-TTLS	<i>EAP-Tunneled Transport Layer Security</i>
EAPOL	<i>Extensible Authentication Protocol Over LAN</i>
IPv4	<i>Internet Protocol version 4</i>
IP	<i>Internet Protocol</i>
IETF	<i>Internet Engineering Task Force</i>
LAN	<i>Local Area Network</i>
OS	<i>Operating System</i>
PC	<i>Personal Computer</i>
PEAP	<i>Protected Extensible Authentication Protocol</i>
RADIUS	<i>Remote Authentication Dial In User Service</i>
IP	<i>Routing Information Protocol</i>
SSL	<i>Secure Socket Layer</i>
TCP	<i>Transmission Control Protocol</i>
TKIP	<i>Temporal Key Integrity Protocol</i>

UDP	<i>User Datagram Protocol</i>
WAN	<i>Wide Area Network</i>
WEP	<i>Wired Equivalent Privacy</i>
WPA	<i>Wi-fi Protected Access</i>

