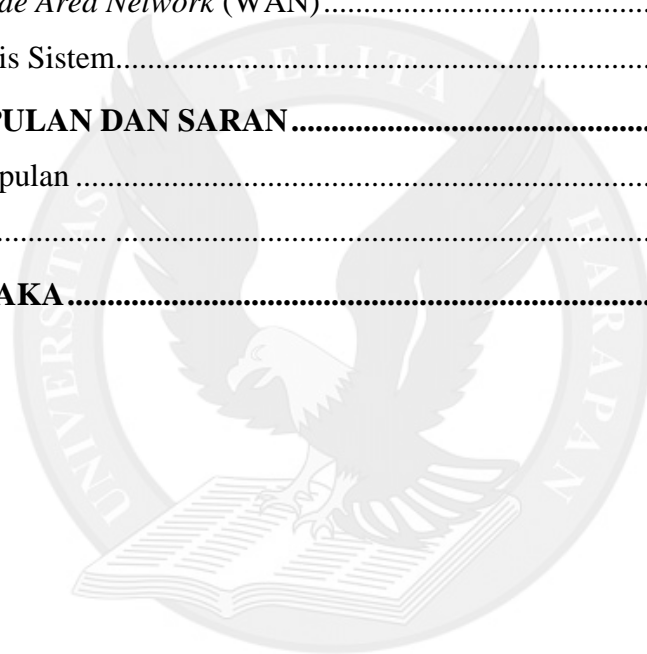


DAFTAR ISI

halaman

PERNYATAAN KEASLIAN KARYA TUGAS AKHIR.....	ii
PERSETUJUAN DOSEN PEMBIMBING TUGAS AKHIR	iii
PERSETUJUAN TIM PENGUJI TUGAS AKHIR.....	iv
ABSTRACT.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Permasalahan.....	1
1.2 Pokok Permasalahan	2
1.3 Pembatasan Masalah.....	2
1.4 Tujuan Penelitian	4
1.5 Sistematika Penulisan	4
BAB II LANDASAN TEORI	6
2.1 Keamanan Pada Jaringan Komputer.....	6
2.1.1 <i>Privacy</i>	7
2.1.2 <i>Integrity</i>	7
2.1.3 <i>Authentication</i>	8
2.1.4 <i>Availability</i>	8
2.2 Konsep-Konsep Keamanan yang Digunakan	8
2.2.1 <i>Secure Socket Layer</i>	8
2.2.2 <i>Transport Layer Security</i>	10
2.2.3 <i>Internet Protocol Security</i>	13
2.2.4 <i>Virtual Private Network</i>	16
2.2.4.1 <i>Virtual Private Network PPTP (VPN PPTP)</i>	20
2.2.4.1 <i>Virtual Private Network L2TP (VPN L2TP)</i>	22
2.3 <i>Man-In-The-Middle Attack</i>	24

BAB III PERANCANGAN SISTEM SIMULASI DAN IMPLEMENTASI....	26
3.1 Pembuatan Sistem Simulasi Komunikasi <i>Web Server</i> dengan <i>Web Client</i>	28
3.1.1 Sistem simulasi komunikasi <i>web server</i> dengan <i>web client</i> sederhana..	29
3.1.2 Pengaplikasian SSLv3 atau TLSv1 pada <i>web server</i>	36
3.1.3 Pengaplikasian VPN PPTP pada <i>web server</i> dan <i>web client</i>	41
3.1.4 Pengaplikasian VPN L2TP/IPSec pada <i>web server</i> dan <i>web client</i>	47
BAB IV PENGUJIAN DAN ANALISIS SISTEM.....	50
4.1 Pengujian Terhadap Proses yang Dilalui Sistem	50
4.1.1 Pengujian terhadap pengaplikasian SSLv3 atau TLSv1 pada jaringan <i>Local Area Network (LAN)</i>	51
4.1.2 Pengujian terhadap pengaplikasian SSLv3 atau TLSv1 pada jaringan <i>Wide Area Network (WAN)</i>	62
4.2 Analisis Sistem.....	66
BAB V KESIMPULAN DAN SARAN.....	71
5.1 Kesimpulan	71
5.2 Saran.....	72
DAFTAR PUSTAKA.....	73



DAFTAR GAMBAR

	halaman
Gambar 2.1. <i>Flowchart</i> proses SSL yang terjadi pada <i>server</i> dan <i>client</i>	10
Gambar 2.2. <i>Network-to-network</i> dan <i>host-to-network</i>	14
Gambar 2.3. Arsitektur pada IPSec.....	15
Gambar 2.4. <i>Tunneling</i> pada VPN	19
Gambar 2.5. <i>Compulsory</i> L2TP	23
Gambar 2.6. <i>Voluntary</i> L2TP.....	23
Gambar 3.1. Sistem simulasi komunikasi <i>web server</i> dengan <i>web client</i> pada jaringan LAN	26
Gambar 3.2. Sistem simulasi komunikasi <i>web server</i> dengan <i>web client</i> pada jaringan WAN	27
Gambar 3.3. Halaman 404 Not Found	28
Gambar 3.4. Status koneksi aktif sebelum <i>web server</i> di- <i>install</i> menggunakan perintah <i>netstat -a</i>	30
Gambar 3.5. Tampilan awal <i>Apache Web Server</i> saat di- <i>install</i>	31
Gambar 3.6. Tampilan beberapa data yang perlu diisi pada <i>Apache Web Server</i>	32
Gambar 3.7. <i>Port</i> 80 (HTTP) yang aktif.....	33
Gambar 3.8. <i>Web browser</i> pada komputer <i>client</i> saat meminta <i>http://192/168.0/101</i> . 34	
Gambar 3.9. <i>Web browser</i> pada komputer <i>client</i> saat meminta <i>dynamic DNS</i> komputer <i>server</i> pada <i>port</i> 2100	36
Gambar 3.10. Menciptakan <i>certificate</i> yang baru.....	38
Gambar 3.11. Tampilan <i>https://192.168.0.101/</i> pada <i>Windows Internet Explorer</i>	39
Gambar 3.12. Tampilan <i>port</i> 443 (HTTPS) yang aktif.....	40
Gambar 3.13. <i>Web browser</i> pada komputer <i>client</i> saat meminta <i>dynamic DNS</i> komputer <i>server</i> pada <i>port</i> 2200	41
Gambar 3.14. Tampilan <i>Server Manager</i> pada <i>Windows Server 2008</i>	42
Gambar 3.15. Tampilan <i>Routing and Remote Access</i> pada <i>Windows Server 2008</i>	43
Gambar 3.16. Tampilan <i>ports</i> VPN pada kondisi status <i>inactive</i> pada <i>Windows Server 2008</i>	44
Gambar 3.17. Tampilan tipe pilihan PPTP VPN pada komputer <i>client</i>	45
Gambar 3.18. Tampilan status <i>active</i> VPN PPTP pada komputer <i>server</i>	46

Gambar 3.19. IP <i>address private</i> pada <i>web client</i>	46
Gambar 3.20. Tampilan tipe pilihan VPN L2TP/IPSec pada komputer <i>client</i>	47
Gambar 3.21. Tampilan <i>pre-shared key</i> pada komputer <i>server</i>	48
Gambar 3.22. Tampilan <i>pre-shared key</i> pada komputer <i>client</i>	48
Gambar 3.23. Tampilan status <i>active</i> VPN L2TP/IPSec pada komputer <i>server</i>	49
Gambar 4.1. Sistem simulasi komunikasi antara <i>web server</i> dengan <i>web client</i> yang mengalami serangan pada jaringan LAN	50
Gambar 4.2. Tampilan https://192.168.0.101/ pada <i>web browser</i> komputer <i>hacker</i> ...	52
Gambar 4.3. Tampilan awal <i>software Cain&Abel</i>	53
Gambar 4.4. Tabel informasi IP <i>addresses</i> target serangan.....	54
Gambar 4.5. Tabel informasi ARP <i>Poison Routing</i> (APR) jaringan LAN	55
Gambar 4.6. Serangan APR diaktifkan.....	56
Gambar 4.7. Tampilan https://192.168.0.101/ pada <i>web browser</i> komputer <i>client</i>	57
Gambar 4.8. Tampilan https://192.168.0.101/test2.html pada <i>web browser</i> komputer <i>hacker</i>	57
Gambar 4.9. Proses pembuatan <i>fake certificate</i>	58
Gambar 4.10. Tampilan hasil proses ARP berupa <i>username</i> dan <i>password</i>	59
Gambar 4.11. Tampilan tabel informasi ARP <i>Poison Routing</i> (APR) jaringan <i>internet</i> pada jaringan LAN	60
Gambar 4.12. Tampilan https://login.yahoo.com/config/mail?.src=ym&.intl=us	61
Gambar 4.13. Pembuatan <i>fake certificate</i> oleh <i>software Cain&Abel</i>	61
Gambar 4.14. Hasil proses APR pada situs https://login.yahoo.com/config/mail?.src=ym&.intl=us	62
Gambar 4.15. Sistem simulasi komunikasi antara <i>web server</i> dengan <i>web client</i> yang mengalami serangan pada jaringan WAN.....	64
Gambar 4.16. Tampilan tabel informasi ARP <i>Poison Routing</i> (APR) jaringan <i>internet</i> pada jaringan WAN	64
Gambar 4.17. Proses ARP <i>poisoning</i> pada jaringan WAN	64
Gambar 4.18. Tampilan <i>error</i> https://ronnyns.dyndns.org:2200/test2.html	65

DAFTAR TABEL

	halaman
Tabel 4.1. Tabel Perbandingan SSL/TLS, VPN PPTP, VPN L2TP/IPSec pada jaringan LAN	24
Tabel 4.2. Tabel Perbandingan SSL/TLS, VPN PPTP, VPN L2TP/IPSec pada jaringan WAN	24

