



**PENGAMANAN JARINGAN *WIRELESS* LAN
DENGAN PROTOKOL EAP-TTLS DAN OTENTIKASI MSCHAPV2
PADA FAKULTAS ILMU KOMPUTER
UPN VETERAN JAKARTA**

SKRIPSI

Kukuh Bagas Permadi

1610511002

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA**

2020



**PENGAMANAN JARINGAN *WIRELESS* LAN
DENGAN PROTOKOL EAP-TTLS DAN OTENTIKASI MSCHAPV2
PADA FAKULTAS ILMU KOMPUTER
UPN VETERAN JAKARTA**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat untuk Kelulusan Mata
Kuliah Tugas Akhir**

Kukuh Bagas Permadi

1610511002

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2020

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Kukuh Bagas Permadi

NIM : 1610511002

Tanggal :

Bilamana di kemudian hari ditemukan ketidak sesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta,.....2020

Yang Menyatakan,



(Kukuh Bagas Permadi)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta,
saya yang bertanda tangan di bawah ini :

Nama : Kukuh Bagas Permadi
NIM : 1610511002
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

Pengamanan Jaringan *Wireless* Dengan Protokol EAP-TTLS Dan Otentikasi MSCHAPv2 Pada Fakultas Ilmu Komputer UPN VETERAN Jakarta

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal :2020

Yang menyatakan,



(Kukuh Bagas Permadi)

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Kukuh Bagas Permadi
NIM	:	1610511002
Program Studi	:	Informatika
Judul Skripsi	:	Pengamanan Jaringan <i>Wireless</i> LAN Dengan Protokol EAP-TTLS Dan Otentikasi MSCHAPv2 Pada Fakultas Ilmu Komputer UPN Veteran Jakarta

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Yuni Widiastiwi, S.Kom, M.Si

Dosen Penguji I



Henki Bayu Seta, S.Kom., M.TI.

Dosen Pembimbing I



Jayanta, S.Kom., M.Si.

Dosen Penguji II



Ria Astriratma, S.Komp., M.Cs.

Dosen Pembimbing II



Anita Muliawati, S.Kom., M.TI.

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 11 Juli 2020



**PENGAMANAN JARINGAN *WIRELESS* LAN DENGAN PROTOKOL
EAP-TTLS DAN OTENTIKASI MSCHAPV2 PADA FAKULTAS ILMU
KOMPUTER UPN VETERAN JAKARTA**

Kukuh Bagas Permadi

ABSTRAK

Penggunaan pada protokol WPA memiliki dua proses, antara lain adalah otentikasi serta enkripsi. Pada tingkat *network* dengan infrastruktur yang besar serta dengan lalu lintas *network* yang tinggi sama halnya dengan universitas, kantor perusahaan atau tempat umum lainnya yang menggunakan *wireless* LAN, proses otentikasi merupakan proses yang pertama kali yang dilakukan agar pengguna jaringan *wireless* LAN dapat mengakses jaringan *internet*. Maka dari itu, tidak hanya aman namun proses otentikasi bisa beroperasi dengan cepat. Solusi dari penelitian ini adalah dengan menerapkan Protokol IEEE 802.1x EAP dengan *Extensible Authentication Protocol – Tunneled Transport Layer Security* (EAP-TTLS) untuk membuat *secure tunnel* (terowongan keamanan) dalam pertukaran kunci pada jaringan *wireless*, serta dengan *inner authentication Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAPv2). Luaran yang dihasilkan pada penelitian ini adalah membangun suatu keamanan pada jaringan *wireless* terpusat pada Fakultas Ilmu Komputer UPN Veteran Jakarta.

Kata Kunci: IEEE 802.1x EAP, EAP-TTLS, MSCHAPv2, RADIUS *Server*, *Wireless* LAN.

**SECURING THE WIRELESS LAN NETWORK WITH EAP-TTLS
PROTOCOL AND MSCHAPV2 AUTHENTICATION IN THE FACULTY
OF COMPUTER SCIENCE UPN VETERAN JAKARTA**

Kukuh Bagas Permadi

ABSTRACT

The use of the WPA protocol has two processes, including authentication and encryption. At the network level with large infrastructure and high network traffic as well as universities, corporate offices or other public places that use wireless LANs, the authentication process is the first process done so that wireless LAN network users can access the internet network. Therefore, it is not only safe but the authentication process can operate quickly. The solution of this research is to implement the IEEE 802.1x EAP Protocol with Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS) to create a secure tunnel (security tunnel) in key exchange on a wireless network, as well as with the inner authentication of the Microsoft Challenge Handshake Authentication Protocol. Version 2 (MSCHAPv2). The output produced in this study is to build a security on a centralized wireless network at the Faculty of Computer Science UPN Veteran Jakarta.

Keywords: IEEE 802.1x EAP, EAP-TTLS, MSCHAPv2, RADIUS Server, Wireless LAN.

DAFTAR ISI

PERNYATAAN ORISINALITAS	I
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	II
LEMBAR PENGESAHAN.....	III
ABSTRAK.....	IV
ABSTRACT	IV
DAFTAR ISI.....	VII
DAFTAR GAMBAR.....	IX
DAFTAR SIMBOL.....	XI
DAFTAR TABEL	XIII
DAFTAR LAMPIRAN	XIII
BAB 1	1
1.1 LATAR BELAKANG	1
1.2 PERUMUSAN MASALAH.....	3
1.3 RUANG LINGKUP.....	3
1.4 TUJUAN PENELITIAN.....	3
1.5 MANFAAT PENELITIAN	4
1.6 LUARAN YANG DIHARAPKAN.....	4
1.7 SISTEMATIKA PENULISAN	4
BAB 2	6
2.1 JARINGAN <i>WIRELESS LOCAL AREA NETWORK</i> (WLAN)	6
2.1.1 <i>Bagian Pada WLAN</i>	7
2.1.1.1 Antena	7
2.1.1.2 <i>Access Point</i> (AP)	7
2.1.1.3 <i>Extension Point</i> (EP)	8
2.1.1.4 <i>Wireless LAN Card</i> (WLANC)	9
2.1.2 <i>Model Pada Wireless LAN</i>	9
2.1.2.1 <i>Model Jaringan Wireless LAN Ad-Hoc</i>	9
2.1.2.2 <i>Model Jaringan Wireless LAN Infrastruktur</i>	10
2.1.3 <i>Komponen Otentikasi Pada 802.1x</i>	11
2.1.3.1 <i>Supplicant</i>	11
2.1.3.2 <i>Authenticator</i>	11
2.1.3.3 <i>Authentication Server</i>	12
2.2 <i>AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING</i> (AAA)	12
2.2.1 <i>Authentication</i>	13
2.2.2 <i>Authorization</i>	13
2.2.3 <i>Accounting</i>	13
2.3 <i>REMOTE DIAL-IN USERS SERVICE</i> (RADIUS).....	13

2.4	FREE RADIUS	14
2.5	TLS/SSL.....	15
2.6	ADVANCED ENCRYPTION STANDARD (AES)	16
2.7	RIVEST, SHAMIR, ADLEMAN (RSA)	16
2.8	SECURE HASH ALGORITHM (SHA-1)	17
2.9	EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)	17
2.9.1	EAP Over RADIUS	17
2.9.2	EAP Over LAN (EAPOL)	18
2.10	EXTENSIBLE AUTHENTICATION PROTOCOL – TUNNELED TRANSPORT LAYER SECURITY (EAP-TTLS)	18
2.11	MICROSOFT CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL VERSION 2 (MSCHAPv2)	19
2.12	PENELITIAN TERKAIT	20
BAB 3	22
3.1	KERANGKA PIKIR	22
3.1.1	Identifikasi Masalah	23
3.1.2	Pengumpulan Data	23
3.1.2.1	Studi Literatur	23
3.1.2.2	Studi Lapangan	24
3.1.3	Tahapan Konfigurasi	24
3.1.3.1	Tahap Pertama	25
3.1.3.2	Tahap Kedua	25
3.1.3.3	Tahap Ketiga	25
3.1.3.4	Tahap Keempat	25
3.1.3.5	Tahap Kelima	25
3.1.3.6	Tahap Keenam	25
3.1.3.7	Tahap Ketujuh	25
3.1.4	Pengujian Sistem	26
3.1.5	Dokumentasi	27
3.2	ALAT BANTU PENELITIAN	27
3.2.1	Peralatan Lunak (Software)	27
3.2.2	Peralatan Keras (Hardware)	27
3.3	JADWAL PENELITIAN	28
BAB 4	29
4.1	ANALISA KEAMANAN SEBELUMNYA	29
4.2	PENGUJIAN SISTEM SEBELUMNYA	29
4.3	ANALISA KEAMANAN YANG DIGUNAKAN	31
4.4	ANALISA CARA KERJA PROTOKOL EAP-TTLS DAN MSCHAPv2	32
4.5	PERBANDINGAN KEDUA KEAMANAN	33
4.6	IMPLEMENTASI	33
4.6.1	Install FreeRADIUS sebagai RADIUS server	34
4.6.2	Konfigurasi File clients.conf	34
4.6.3	Konfigurasi File users.conf	34
4.6.4	Konfigurasi File eap.conf	34

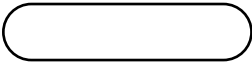


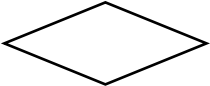
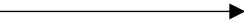
4.6.5 Konfigurasi <i>Wireless Access Point</i>	34
4.6.6 Menjalankan <i>FreeRADIUS</i>	36
4.7 PROSES PENGUJIAN PENGGUNA KE JARINGAN <i>WIRELESS</i>	36
4.8 <i>MONITORING</i> PENGGUNA JARINGAN	40
4.9 PENGUJIAN SISTEM YANG DIGUNAKAN	40
4.10 ANALISA HASIL KINERJA KEDUA KEAMANAN	41
BAB 5	43
5.1 KESIMPULAN	43
5.2 SARAN	43
DAFTAR PUSTAKA	45
RIWAYAT HIDUP	47
LAMPIRAN	48

DAFTAR GAMBAR

Gambar 1. Ilustrasi Antena <i>Wireless LAN</i>	7
Gambar 2. Infrastruktur Jaringan Dengan <i>Access Point</i>	8
Gambar 3. Infrastruktur Jaringan Dengan Menggunakan <i>Extension Point</i>	9
Gambar 4. Model <i>Ad-Hoc</i>	10
Gambar 5. Model Jaringan Infrastruktur	11
Gambar 6. Komponen Otentikasi 802.1x	12
Gambar 7. Cara Kerja Koneksi Protokol RADIUS	14
Gambar 8. Infrastruktur Keamanan SSL/TLS	16
Gambar 9. Model Arsitektur Jaringan Untuk EAP-TTLS	19
Gambar 10. <i>Flowchart</i> Tahapan Penelitian	22
Gambar 11. <i>Flowchart</i> Tahapan Konfigurasi	24
Gambar 12. <i>Flowchart</i> Pengujian Sistem	26
Gambar 13. <i>Airodump-ng</i> mendapatkan <i>handshake</i>	30
Gambar 14. <i>Aircrack-ng</i> mendapatkan kata sandi	31
Gambar 15. Hasil pada <i>wireshark</i> dalam membuat jalur TLS	32
Gambar 16. Hasil pada <i>wireshark</i> paket EAP telah berhasil	33
Gambar 17. Konfigurasi <i>Wireless Router</i> Pada <i>SSID Setting</i>	35
Gambar 18. Konfigurasi <i>Wireless Router</i> Pada <i>Security</i>	36
Gambar 19. <i>FreeRadius</i> Siap Dijalankan	36
Gambar 20. Tampilan Menambah Perangkat <i>Wireless</i> Secara Manual	37
Gambar 21. Tampilan <i>Security</i> Pada Pengaturan Manual	38

Gambar 22. Tampilan 802.1x <i>Settings</i> Pada “ <i>Advanced Settings</i> ”	39
Gambar 23. <i>User</i> Berhasil Terhubung Dengan Jaringan “SelasarFIK”	40
Gambar 24. <i>Monitoring</i> Sistem Pada RADIUS <i>Server</i>	40
Gambar 25. <i>Airodump-ng</i> tidak mendapatkan <i>handshake</i> jaringan SelasarFIK ..	41
Gambar 26. Tampilan Konfigurasi <i>File clients.conf</i>	48
Gambar 27. Tampilan Konfigurasi <i>File users.conf</i>	52
Gambar 28. Tampilan Konfigurasi <i>File eap.conf</i>	61

DAFTAR SIMBOL

<i>Model</i>	<i>Symbol</i>	Ketereangan
<i>Terminal</i>		Mengartikan permulaan maupun akhir dari operasi.
Proses		Mengartikan sebuah aktivitas pada kondisi saat itu berlangsung atau sebuah <i>output</i> dari suatu aktivitas.
<i>Predefine</i>		Simbol ini sebagai pelaksanaan suatu bagian prosedur.
<i>Decision</i>		Mengartikan suatu kondisi untuk memilih dari sejumlah pilihan dari proses tertentu.
<i>Sequence</i>		Urutan atau arah terjadinya proses-proses berjalan.

DAFTAR TABEL

Tabel 1. Tabel Penelitian Terkait	20
Tabel 2. Tabel Jadwal Pekerjaan Penelitian	28
Tabel 3. Perbandingan Kedua Keamanan	33

DAFTAR LAMPIRAN

LAMPIRAN 1. KONFIGURASI PENUH <i>FILE CLIENTS.CONF</i>	47
LAMPIRAN 2. KONFIGURASI PENUH <i>FILE USERS.CONF</i> ERROR! BOOKMARK NOT DEFINED.1	
LAMPIRAN 3. KONFIGURASI PENUH <i>FILE EAP.CONF</i>	59