PENGAMANAN DENGAN STANDAR IEEE802.1x PADA JARINGAN WIRELESS

ARIS SULISTIONO
41508110123

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2015

PENGAMANAN DENGAN STANDAR IEEE802.1x PADA JARINGAN WIRELESS

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

ARIS SULISTIONO
41508110123

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2015

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NIM	:	41508110123
NAMA	:	ARIS SULISTIONO
Judul Skripsi	:	PENGAMANAN DENGAN STANDAR IEEE802.1x PADA JARINGAN WIRELESS

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam skripsi saya terdapat unsur plagiarisme, maka saya siap untuk mendapatkan sanksi akademis yang terkait dengan hal tersebut.

Jakarta, Juli 2015

Aris Sulistiono

LEMBAR PENGESAHAN

Nama	:	Aris Sulistiono
NIM	:	41508110123
Jurusan	:	Teknik Informatika
Fakultas	:	Ilmu Komputer
Judul	:	Pengamanan Dengan Standar IEEE802.1x Pada Jaringan Wireless

Jakarta, Juli 2015

Disetujui dan diterima oleh,

Tri Daryanto, S.Kom, MT.

Dosen Pembimbing

Sabar Rudiarto, M.Kom.

Kaprodi Teknik Informatika

Umniy Salamah, ST, MMSI.

Koordinator Tugas Akhir

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas karunia yang telah diberikan kepada penulis sehingga penulis dapat menyelesaikan Laporan Tugas Akhir tepat pada waktunya, dimana Laporan Tugas Akhir tersebut merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa Laporan Tugas Akhir ini masih belum dapat dikatakan sempurna. Karena itu, kritik dan saran akan diterima dengan senang hati. Penulis juga menyadari bahwa Laporan Tugas Akhir ini takkan dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Maka dari itu, dengan segala kerendahan hati, Penulis ingin menyampaikan ucapan terima kasih kepada :

1. Tri Daryanto, S.Kom, MT, selaku Pembimbing Tugas Akhir yang telah membimbing penulis dengan semua nasihat, semangat dan ilmunya dalam menyusun laporan tugas akhir ini.
2. Sabar Rudiarto, M.Kom. selaku Kaprodi Teknik Informatika Universitas Mercu Buana.
3. Umniy Salamah, ST, MMSI, selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercu Buana
4. Kedua orang tua yang selama ini telah membesarkan penulis dan juga semua saudara tercinta yang telah memberi dukungan.
5. Beserta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat penulis sebutkan satu per satu.

Semoga Tuhan Yang Maha Esa membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin

Jakarta, Juli 2015

ABSTRACT

Information technology is growing/ developing and enable users to work. One of the technologies that is used to facilitate users is wireless networks or is named wireless. However, with that such ease, without realizing the network is vulnerable to cyber crime. By using security system on the network, which standard IEEE802.1x using digital certificate, the network can be secured from unwanted/unauthorized user to access by authenticating user use RADIUS and digital certificate.

Keywords : Wireless security, IEEE802.1x, RADIUS, Digital Certificate.

xi+52 pages; 30 figures; 15 scripts; 3 tables

ABSTRAK

Teknologi Informasi semakin berkembang dan memudahkan para pengguna untuk melakukan aktivitas. Salah satu teknologi yang digunakan untuk memudahkan para pengguna adalah jaringan nirkabel atau biasa disebut dengan *wireless*. Namun dengan adanya kemudahan tersebut, tanpa disadari jaringan sangat rentan terhadap kejahatan *cyber*. Dengan menggunakan sistem keamanan pada jaringan, yaitu standar IEEE802.1x dengan menggunakan sertifikat digital, maka jaringan dapat diamankan dari pengguna yang tidak dikehendaki untuk melakukan akses dengan cara otentikasi user menggunakan RADIUS dan sertifikat digital.

Kata kunci : Keamanan Wireless, IEEE802.1x , RADIUS, Sertifikat digital.

xi+52 halaman; 30 gambar; 15 skrip; 3 tabel

DAFTAR ISI

LEMBAR PERNYATAAN i
LEMBAR PENGESAHAN ii
KATA PENGANTAR iii
ABSTRACT iv
ABSTRAK v
DAFTAR ISI vi
DAFTAR GAMBAR viii
DAFTAR SKRIP x
DAFTAR TABEL xi
BAB I PENDAHULUAN
1.1. Latar Belakang 1
1.2. Perumusan Masalah 2
1.3. Batasan Masalah 2
1.4. Metodologi Penelitian 2
1.5. Tujuan dan Manfaat Penelitian 3
1.6. Sistematika Penulisan 4
BAB II LANDASAN TEORI
2.1. IEEE 5
2.2. Jaringan Wireless 5
2.2.1. Sejarah Wireless 5
2.2.2. Open System 7
2.2.3. Shared Key Authentication 8
2.2.4. Wired Equivalen Privacy 10
2.2.5. WPA Pre-Shared Key (WPA Personal) 10
2.2.6. WPA2 Pre-Shared Key (WPA2 Personal) 10
2.3. 802.1x 11
2.3.1. Sejarah 802.1x 12
2.3.2. Proses Otentikasi pada 802.1x 12
2.3.3. EAP (Extensible Authentication Protocol) 14
2.3.4. EAP-TLS 15

2.4.	RADIUS (Remote Authentication Dial-In User Service)	16
2.4.1.	Sejarah RADIUS	16
2.4.2.	NAS (Network Acces Server)	16
2.4.3.	AAA (Authentication, Authorization, Accounting)	17
2.5.	PKI (Public Key Infrastructure)	18
2.5.1.	Sertifikat Digital	18
2.5.2.	CA (Certificate Authorities)	19
2.5.3.	Kriptografi Asimetris	20
2.6.	Linux	21
2.7.	Tujuan Keamanan	21
2.8.	Kelemahan Keamanan Pada Wireless	22
2.9.	Ancaman Keamanan Pada Wireless	23
BAB III	ANALISA DAN PERANCANGAN	
3.1.	Pengujian Keamanan Wireless	25
3.1.1.	Skenario Pengujian Keamanan	26
3.1.2.	WPA/WPA2 Cracking	27
3.1.3.	Mac Address Spoofing	30
3.2.	Perancangan Jaringan Wireless dengan Standar IEEE802.1x	31
3.2.1.	Access Point	33
3.2.2.	Server RADIUS	34
3.2.3.	Sertifikat Digital	36
3.2.4.	Analisa Proses	37
3.3.	Analisa Pada WPA, WPA2, 802.1x	39
BAB IV	PENGUJIAN	
4.1.	Lingkungan Pengujian	41
4.2.	Pengujian Otentikasi	41
4.3.	Pengujian Keamanan Jaringan Wireless IEEE802.1x	45
4.4.	Analisa Hasil Pengujian	47
BAB V	PENUTUP	
5.1.	Kesimpulan	49
5.2.	Saran	50
DAFTAR PUSTAKA		51

DAFTAR GAMBAR

Gambar 2.1	Otentikasi open system (Robert J. Bartz, 2009)	7
Gambar 2.2	Shared Key otentikasi (Robert J. Bartz, 2009)	9
Gambar 2.3	Skema dasar standar 802.1x (Strand, 2004)	11
Gambar 2.4	Proses otentikasi pada 802.1x (wikipedia.org, 2015)	13
Gambar 2.5	Autentikasi EAP (wikipedia.org, 2015)	15
Gambar 2.6	Setiap sertifikat digital memiliki struktur yang semua isinya berguna untuk proses identifikasi (Harris, 2012).	19
Gambar 2.7	Analogi pertukaran sertifikat digital (Harris, 2012)	20
Gambar 2.8	Tujuan Keamanan (Harris, 2012)	22
Gambar 3.1	Desain jaringan sebelum menggunakan standar IEEE802.1x	26
Gambar 3.2	Diagram skenario pengujian keamanan	27
Gambar 3.3	Skenario pengujian WPA/WPA2 Cracking	28
Gambar 3.4	Konfigurasi Card Wireless sebagai monitoring	28
Gambar 3.5	Scan Access Point	29
Gambar 3.6	Capture data dengan airodump-ng	29
Gambar 3.7	Dekrip data capture	30
Gambar 3.8	Skenario pengujian Mac Address Spoofing	31
Gambar 3.9	Memalsukan mac address	31
Gambar 3.10	Desain jaringan dengan standar IEEE802.1x	32
Gambar 3.11	Konfigurasi Acces Point	33
Gambar 3.12	Konfigurasi ip address	34
Gambar 3.13	Diagram Proses otentikasi 802.1x	38
Gambar 4.1	Pengaturan client otentikasi	42
Gambar 4.2	Otentikasi berhasil	42
Gambar 4.3	Penggunaan private key password tidak sah...	43
Gambar 4.4	Penggantian sertifikat tidak sah	44
Gambar 4.5	Private key password otentikasi	44
Gambar 4.6	Start airmon-ng	45
Gambar 4.7	Scan target	45
Gambar 4.8	Start airodump-ng	46

Gambar 4.9 Cracking password..... 46

DAFTAR SKRIP

Skrip 3.1	Instalasi FreeRadius	34
Skrip 3.2	Konfigurasi koneksi untuk Access Point	34
Skrip 3.3	Konfigurasi autentikasi EAP	35
Skrip 3.4	Konfigurasi TLS	35
Skrip 3.5	Konfigurasi user password	35
Skrip 3.6	Generate ca.key	36
Skrip 3.7	Generate ca.csr	36
Skrip 3.8	Generate ca.crt	36
Skrip 3.9	Skrip Generate server.key	36
Skrip 3.10	Generate server.csr	36
Skrip 3.11	Generate server.crt	36
Skrip 3.12	Generate client.key	37
Skrip 3.13	Generate client.csr	37
Skrip 3.14	Generate client.crt	37
Skrip 3.15	Generate client.p12	37

DAFTAR TABEL

Tabel 3.1 39
Tabel 4.1 47
Tabel 4.2 47