ANALISA PERBANDINGAN SISTEM KEAMANAN WPA2-PSK DENGAN CAPTIVE PORTAL PADA JARINGAN WIRELESS MENGGUNAKAN METODE WIRELESS PENETRATION TESTING

Studi Kasus: PT. Yoshugi Putra Mandiri

SKRIPSI

disusun oleh

Erfan Wahyudi

12.11.6123

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015

ANALISA PERBANDINGAN SISTEM KEAMANAN WPA2-PSK DENGAN CAPTIVE PORTAL PADA JARINGAN WIRELESS MENGGUNAKAN METODE WIRELESS PENETRATION TESTING

Studi Kasus: PT. Yoshugi Putra Mandiri

SKRIPSI

untuk meemenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Erfan Wahyudi

12.11.6123

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015

PERSETUJUAN

SKRIPSI

ANALISA PERBANDINGAN SISTEM KEAMANAN WPA2-PSK DENGAN CAPTIVE PORTAL PADA JARINGAN *WIRELESS* MENGGUNAKAN METODE *WIRELESS PENETRATION TESTING*

Studi Kasus: PT. Yoshugi Putra Mandiri

yang dipersiapkan dan disusun oleh

Erfan Wahyudi

12.11.6123

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 Februari 2015

Dosen Pembimbing,

Emha Taufiq Luthfi, ST, M.Kom
NIK. 190302125

PENGESAHAN

SKRIPSI

ANALISA PERBANDINGAN SISTEM KEAMANAN WPA2-PSK DENGAN CAPTIVE PORTAL PADA JARINGAN *WIRELESS* MENGGUNAKAN METODE *WIRELESS PENETRATION TESTING*

Studi Kasus: PT. Yoshugi Putra Mandiri

yang disusun oleh

Erfan Wahyudi
12.11.6123

telah dipertahankan di depan Dewan Penguji
pada tanggal 13 Mei 2015

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Emha Taufiq Luthfi, ST, M.Kom **NIK. 190302125**	
Kusnawi, S.Kom, M.Eng **NIK. 190302112**	
Agus Purwanto, M.Kom **NIK. 190302229**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 Juni 2015

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

HALAMAN PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa Skripsi ini merupakan karya saya sendiri (ASLI) dan isi dalam skripsi ini tidak terdapat pada karya yang pernah diajukan oleh orrang lain untuk memperoleh gelar akademis disuatu Institusi Pendidikan dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 1 Juni 2015

Erfan Wahyudi
NIM. 12.11.6123

MOTTO

- *"Hai orang-orang mukmin, jika kamu menolong agama ALLAH, niscaya DIA akan menolongmu dan meneguhkan kedudukanmu" (QS. 47:7)*

- *"Karena sesungguhnya sesudah kesulitan itu ada kemudahan" (QS. Al Insyirah : 5)*

- Tinggalkanlah rasa malas dan marah, karena keduanya adalah kunci segala keburukan. Barang siapa yang malas. Ia tidak akan dapat melaksanakan hak orang lain, dan barang siapa yang suka marah maka ia tidak akan sabar mengemban kebenaran.

- Jangan malas menuntut ilmu..!!! Para ulama berkorban harta hanya untuk mendapatkan ilmu, lantas dengan fasilitasmu yang lengkap seperti saat ini engkau masih malas dan enggan untuk belajar..??

    1. Imam Malik bin Anas menjual atap rumahnya untuk membiayai kehidupannya demi mendapatkan ilmu
    2. Imam Yahya bin Ma'in menginfakkan semua harta warisannya untuk mencari hadist hingga tidak memiliki sandal yang dia pakainya
    3. Semangat Ibnul Jauzi menuntut ilmu tidak pernah kendor wlaau dalam keadaan lapar
    4. Muhammad bin Hasan Asy Syaibani tidak pernah tidur malam hanya untuk belajar dan beribadah
    5. Ubaid bin Ya'isy Al Kufi selama tiga puluh tahun disuapi saudarinya jika hendak makan karena sibuk menulis hadist

- Ketika seseorang memiliki tekat tinggi yang melangit, maka semua rintangan dan halangan menjadi sesuatu yang sangat dicintainya

- Ketika seseorang mengunggulimu dalam hal dunia, maka unggulilah dia dalam hal akhirat

PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

Bapak & Ibu tercinta

Bapak Musa, S.Pd & Ibu Siria Hastuti Handayani

Mereka adalah oraangtua yang hebat yang telah membesarkan dan mendidikku dengan penuh kasih sayang

Terimakasih atas pengorbanan, nasehat, dan do'a yang tiada hentinya Bapak & Ibu berikan kepadaku selama ini.

Adik-Adikku tersayang

Luthvia Zahara Fatin & Hanif Az Zahid Abdillah

Kalian bagai malaikat kecil yang memberiku semangat untuk terus belajar, tiada momen yang paling mengharukan saat kumpul dengan kalian bersama Bapak dan Ibu tercinta

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat ALLAH SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan skripsi dengan judul **"Analisa Perbandingan Sistem Keamanan WPA2-PSK Dengan Captive Portal Pada Jaringan Wireless Menggunakan Metode Wireless Penetration Testing (Studi Kasus: PT. Yoshugi Putra Mandiri)".**

Terselesaikannya skripsi ini dengan baik berkat dukungan, motivasi, petunjuk dan bimbingan dari berbagai pihak. Oleh karena itu penulis mengucapkan terimakasih yang sebesar-besarnya kepada:

1. Ayah dan Ibu yang dengan tulus memberikan do'a dan dukungan moral serta materil.
2. Prof. Dr. M. Suyanto, MM, selaku ketua STMIK AMIKOM Yogyakarta
3. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta
4. Bapak Emha Taufiq Luthfi, ST, M.Kom selaku pembimbing utama.
5. Bapak Yoyok Rubiantono, ST selaku Direktur Utama PT. Yoshugi Putra Mandiri yang telah memberikan izin serta dukungan sehingga penelitian ini dapat selesai sesuai yang direncanakan.
6. Berbagai pihak yang telah memberikan bantuan dan dorongan serta berbagai pengalaman pada proses penyusunan skripsi ini.

Terakhir semoga segala bantuan yang telah diberikan, sebagai amal soleh dan senantiasa mendapat Ridho Allah SWT. Sehingga pada akhirnya skripsi ini dapat bermanfaat bagi kemajuan pendidikan khususnya dalam bidang teknologi informasi.

Dalam penulisan skripsi ini tentunya tidak lepas dari kekurangan, baik aspek kualitas maupun kuantitas dari materi penelitian yang disajikan. Semua ini didasarkaan dari keterbatasan yang dimiliki penulis. Penulis menyadari bahwa skripsi ini jauh dari sempurna sehingga penulis membutuhkan kritik dan saran yang bersifat membangun untuk kemajuan pendidikan di masa yang akan datang.

Yogyakarta, April 2015

Erfan Wahyudi

DAFTAR ISI

Halaman Judul i

Halaman Persetujuan Dosen Pembimbing ii

Halaman Pengesahan iii

Motto iv

Persembahan v

Kata Pengantar vi

Daftar Isi viii

Daftar Tabel xii

Daftar Gambar xiii

Daftar Lampiran xvi

Intisari xvii

Abstract xviii

BAB I PENDAHULUAN 1

1.1 Latar Belakang Masalah 1

1.2 Rumusan Masalah 2

1.3 Batasan Masalah 2

1.4 Tujuan Penelitian 4

1.5 Manfaat Penelitian 4

1.6 Metodologi Penelitian 4

1.7 Sistematika Penulisan 6

BAB II LANDASAN TEORI 8

2.1 Tinjauan Pustaka 8

2.2 Wireless dan Sejarahnya 9

2.2.1 Topologi Jaringan Wireless 10

2.2.1.1 Mode Ad-Hoc 10
2.2.1.2 Mode Infrastruktur 10
2.2.2 Jenis Serangann Pada Wireless 11
2.2.2.1 Passive Attack 11
2.2.2.2 Active Attack 13
2.2.3 Mekanisme Keamanan Wireless 16
2.2.3.1 Service Set Identifier (SSID) 16
2.2.3.2 MAC Address Filtering 17
2.2.3.3 WEP 17
2.2.3.4 Wifi Protected Access (WPA/WPA2) 18
2.2.4 RADIUS Server 20
2.2.4.1 Prinsip Kerja RADIUS Server 20
2.2.4.2 Authentication, Authorization, Accounting(AAA) 21
2.2.5 Captive Portal (Hotspot) 23
2.2.5.1 Pengertian Captive Portal 23
2.2.5.2 Fungsi Captive Portal 24
2.2.5.3 Cara Kerja Captive Portal 24
2.3 Penetration Testing 25
2.3.1 Definisi Penetration Testing 25
2.3.2 Legalitas Penetration Testing 26
2.3.3 Mekanisme Penetration Testing 27
2.3.4 Tools Penetration Testing 28
2.3.4.1 BackBox 28
2.3.4.2 Aircrack-ng 28
2.3.4.3 Wireshark 29

2.3.4.4 Nessus 30
2.3.4.5 Mac Changer 30
2.3.4.1 Ettercap 31
BAB III ANALISIS DAN PERANCANGAN SISTEM 32
3.1 Tinjauan Umum 32
3.1.1 Sejarah Perusahaan 32
3.1.2 Visi dan Misi Perusahaan 33
3.1.2.1 Visi 33
3.1.2.2 Misi 33
3.1.3 Struktur Organisasi 33
3.1.3.1 Bagan Struktur Organisasi Perusahaan 33
3.2 Analisis Sistem 34
3.2.1 Intelligence Gathering 34
3.2.1.1 Kondisi WLAN 34
3.2.1.2 Jenis Keamanan Wireless Yang Digunakan 35
3.2.1.3 Observasi Lapangan 36
3.2.2 Vulnerability Analysis 38
3.2.2.1 Vulnerability Analysis Pada Captive Portal 38
3.2.2.2 Vulnerability Analysis Pada WPA2-PSK 44
3.2.3 Identifikasi Masalah 46
3.2.4 Threat Modelling 49
BAB IV HASIL DAN PEMBAHASAN 52
4.1 Proses Pengujian dan Cracking Password 52
4.1.1 Pengujian Pada WPA2-PSK 52
4.1.1.1 Brute Force Dengan Dictionary File 52

4.1.1.2 MAC Address Spoofing 58
4.1.1.3 Sniffing to Eavesdrop 61
4.1.1.4 Man in the Middle Attack 65
4.1.1.5 Ping of Death 72
4.1.1.6 Deauthentication Attack 74
4.1.2 Pengujian Pada Captive Portal 76
4.1.2.1 Brute Force Dengan Dictionary File 76
4.1.2.2 MAC Address Spoofing 80
4.1.2.3 Sniffing to Eavesdrop 84
4.1.2.4 Man in the Middle Attack 85
4.1.2.5 Ping of Death 88
4.1.2.6 Deauthentication Attack 90
4.2 Laporan Perbandingan 91
BAB V PENUTUP 94
5.1 Kesimpulan 94
5.1 Saran 95
DAFTAR PUSTAKA 96
LAMPIRAN 97

DAFTAR TABEL

Tabel 2.1 Tabel Perbandingan Penelitian..... 9

Tabel 3.1 Tabel Identifikasi Masalah Secara Fisik dan Potensi Kerugian..... 36

Tabel 3.2 Tabel Hasil Scanning Menggunakan Nessus..... 43

Tabel 3.3 Tabel Variabel Kerentanan 46

Tabel 3.4 Tabel Perancangan Pembuktian..... 49

Tabel 4.1 Tabel IP dan MAC Target..... 66

Tabel 4.2 Tabel Laporan Perbandingan Hasil Pengujian..... 92

DAFTAR GAMBAR

Gambar 2.1 Model AAA 21

Gambar 2.2 Tampilan Awal Wireshark 29

Gambar 3.1 Struktur Organisasi Perusahaan 34

Gambar 3.2 Membuat Policy Scan 39

Gambar 3.3 Konfigurasi Untuk Melakukan Scanning 40

Gambar 3.4 Tampilan Reports Pada Hasil Scanning 41

Gambar 3.5 List Vulnerability yang Ditemukan 41

Gambar 3.6 Informasi Detail Dari Suatu Vulnerability 42

Gambar 3.7 Aircrack-ng 44

Gambar 3.8 Mencari Informasi Jaringan Wireless 45

Gambar 4.1 Mencari Informasi Menggunakan Airodump-ng 53

Gambar 4.2 Mendapatkan Paket Handshake 54

Gambar 4.3 Proses Mendapatkan Paket Handshake 55

Gambar 4.4 Deauthentication Attack untuk mendapatkan handshake 56

Gambar 4.5 Cracking WPA2 Key 56

Gambar 4.6 Proses Mencocokkan Password 57

Gambar 4.7 Password Ditemukan 58

Gambar 4.8 Informasi MAC Saat Ini 58

Gambar 4.9 Informasi MAC Client yang Terkoneksi ke Jaringan 59

Gambar 4.10 Non-aktifkan Interface wlan0 60

Gambar 4.11 Mengganti MAC address 60

Gambar 4.12 Aktifkan Kembali Interface wlan0 61

Gambar 4.13 MAC Address wlan0 Berhasil Dirubah 61

Gambar 4.14 Ping ke www.google.com berhasil 62

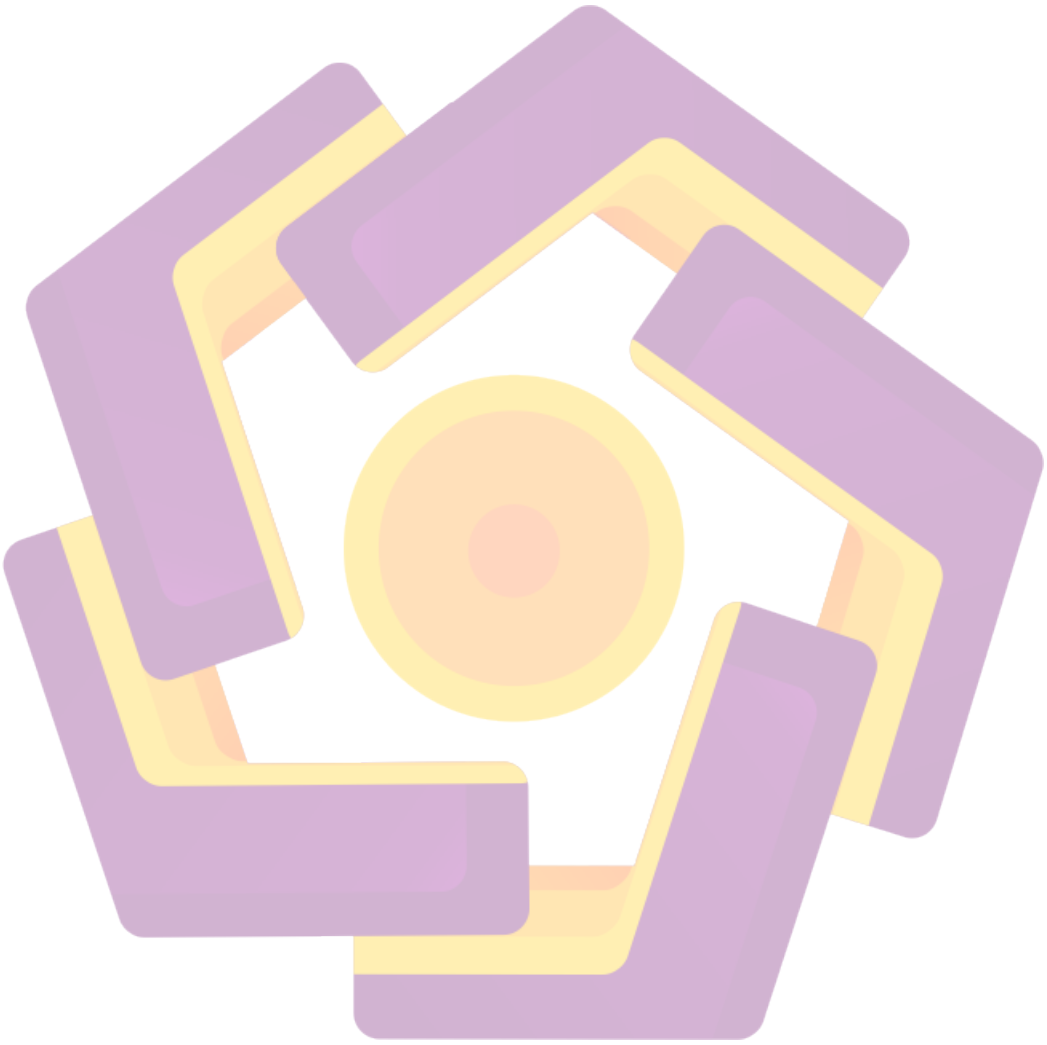
Gambar 4.15 Menjalankan Wireshark 63
Gambar 4.16 Filter HTTP WPA2-PSK..... 64
Gambar 4.17 Eavesdroping Berhasil di WPA2-PSK..... 64
Gambar 4.18 Pilih Interface Pada Ettercap 66
Gambar 4.19 Host List WPA2-PSK 67
Gambar 4.20 Menentukan Target MITM..... 68
Gambar 4.21 Kotak Dialog MITM ARP Poisoning 68
Gambar 4.22 ARP Poisoning Dijalankan 69
Gambar 4.23 Menjalankan Wireshark Untuk MITM 69
Gambar 4.24 Filter HTTP MITM 70
Gambar 4.25 ARP Spoofing Berhasil di WPA2-PSK 71
Gambar 4.26 Informasi wlan0 POD WPA2-PSK..... 72
Gambar 4.27 Ping of Death WPA2..... 73
Gambar 4.28 Mengirimkan Paket Ping WPA2 73
Gambar 4.29 Informasi Yang Dibutuhkan Deauth WPA2 74
Gambar 4.30 Melancarkan Serangan Deauthentication WPA2..... 75
Gambar 4.31 Deauthentication WPA2 Berhasil 75
Gambar 4.32 Mencari Informasi Captive Portal 77
Gambar 4.33 Mendapatkan Paket Handshake Captive Portal 77
Gambar 4.34 Proses Mendapatkan Handshake Captive Portal..... 78
Gambar 4.35 Deauthentication Untuk Mendapatkan Handshake..... 79
Gambar 4.36 Cracking Captive Portal Key Gagal 79
Gambar 4.37 Informasi MAC Saat Ini..... 80
Gambar 4.38 Informasi MAC Client Yang Terkoneksi Ke Jaringan 81
Gambar 4.39 Non-aktifkan Interface wlan0..... 81

Gambar 4.40 Mengganti MAC Address 82
Gambar 4.41 Aktifkan Kembali Interface wlan0 82
Gambar 4.42 MAC Address wlan0 Berhasil Diganti..... 83
Gambar 4.43 Ping Ke www.google.com Berhasil 83
Gambar 4.44 List Paket HTTP Yang Ditangkap Pada Captive Portal..... 84
Gambar 4.45 Analisa Paket HTTP Gagal 85
Gambar 4.46 Pilih Interface Ettercap 86
Gambar 4.47 Host List Ettercap Captive Portal 87
Gambar 4.48 ARP Spoofing Captive Portal Gagal 87
Gambar 4.49 Informasi wlan0..... 88
Gambar 4.50 Melakukan Serangan Ping..... 89
Gambar 4.51 Proses Mengirimkan Paket Ping 89
Gambar 4.52 Informasi Yang Dibutuhkan Deauth Captive Portal 90
Gambar 4.53 Melancarkan Serangan Deauthentication Captive Portal..... 91
Gambar 4.54 Deauthentication Captive Portal Berhasil 91

DAFTAR LAMPIRAN

Lampiran 1 Hasil Scanning Captive Portal Menggunakan Nessus..... 99

Lampiran 2 Dokumen Perjanjian Kerjasama 104



INTISARI

Salah satu perubahan besar di sektor telekomunikasi adalah penggunaan teknologi nirkabel atau wireless. Namun banyak masalah yang harus dihadapi ketika mengimplementasikan jaringan wireless ini, salah satunya adalah masalah keamanan. Banyak pihak yang masih mempertanyakan tentang keamanan wireless, dan banyak pula pihak yang meyakini bahwa sistem keamanan wireless yang menggunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan wireless yang lain.

Namun berdasarkan hasil studi pustaka yang dilakukan, sistem keamanan wireless yang benar-benar mampu memberikan keamanan yang lebih *secure* adalah dengan menggunakan sistem keamanan *Remote Authentication Dial In User Servie* (RADIUS) *server*. Namun pada saat ini, banyak pihak yang masih menggunakan WPA2-PSK sebagai sistem keamanan wireless mereka untuk menghindari kemungkinan penggunaan akses internet secara ilegal oleh orang yang tidak memiliki hak akses.

Penelitian yang dilakukan di PT. Yoshugi Putra Mandiri ini bertujuan untuk menganalisa perbandingan kedua sistem keamanan jaringan wireless diatas dan menyimpulkan hasil pengujiannya untuk mengetahui sistem yang mana yang benar-benar aman untuk jaringan wireless. Pengujian dilakukan dengan menggunakan metode wireless penetration testing.

Kata Kunci : WPA2-PSK, RADIUS, Captive Portal, Penetration Testing

ABSTRACT

One of the major changes in the telecommunications sector is the use of wireless technology or wireless. But many problems that must be faced when implementing a wireless network, one of which is security. Many people are still questions about wireless security, and there are many who believe that the wireless security system that uses WPA2-PSK is more secure than other wireless security system.

However, based on the results of the literature study conducted, wireless security systems are actually able to provide a more secure security is to use a security system Remote Authentication Dial In User Servie (RADIUS) server. However, at this time, many people are still using WPA2-PSK wireless security system as they are to avoid the possibility of illegal use of the internet access by people who do not have access rights.

Research conducted at PT. Yoshugi Putra Mandiri aims to analyze the comparison of the two systems over the wireless network security and conclude the test results to determine which systems are completely safe for wireless networks. Tests carried out using the method of wireless penetration testing.

***Keywords**: WPA2-PSK, RADIUS, Captive Portal, Penetration Testing*