

**ANALISIS KELEMAHAN PROTOKOL WIRELESS
DENGAN METODE BRUTE FORCE ATTACK
DI KALI LINUX (STUDI KASUS JARINGAN
WIRELESS DI KOTA BATAM)**

SKRIPSI



**Oleh:
Richard Rolando
130210214**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2018**

**ANALISIS KELEMAHAN PROTOKOL WIRELESS
DENGAN METODE BRUTE FORCE ATTACK
DI KALI LINUX (STUDI KASUS JARINGAN
WIRELESS DI KOTA BATAM)**

SKRIPSI

**Untuk memenuhi salah satu syarat
guna memperoleh gelar sarjana**



**Oleh:
Richard Rolando
130210214**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2018**

PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, dan/atau magister), baik di Universitas Putera Batam maupun di perguruan tinggi lain.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 3 Februari 2018
Yang membuat pernyataan,

Richard Rolando
130210214

**ANALISIS KELEMAHAN PROTOKOL WIRELESS
DENGAN METODE BRUTE FORCE ATTACK
DI KALI LINUX (STUDI KASUS JARINGAN
WIRELESS DI KOTA BATAM)**

**Oleh
Richard Rolando
130210214**

**SKRIPSI
Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana**

**Telah disetujui oleh Pembimbing pada tanggal
seperti tertera dibawah ini**

Batam, 3 Februari 2018

**Andi Maslan, S.T., M.SI.
Pembimbing**

ABSTRAK

Perkembangan teknologi sekarang ini semakin pesat, dan hal itu pun berpengaruh dalam kehidupan manusia. Teknologi menjadi suatu kebutuhan yang semakin lama semakin utama. Salah satu teknologi yang saat ini sedang banyak digunakan adalah *wireless local area network* (WLAN). Perangkat-perangkat elektronik yang menggunakan teknologi wireless semakin banyak diproduksi oleh karena kebutuhan akan informasi yang cukup mobile, maka banyak tempat-tempat seperti kantor, café, mall menyediakan layanan wifi (*wireless fidelity*). Akan tetapi layanan tersebut sering kali kurang memperhatikan pengaturan keamanan komunikasi data dalam jaringan tersebut. Kerentanan-kerentanan yang terjadi membuat pengguna wireless meragukan keamanannya. Implementasi WLAN membutuhkan suatu sistem keamanan yang memadai untuk menghindari pengguna yang tidak berhak memasuki jaringan. Penelitian ini bertujuan untuk mengetahui apakah wireless dengan menggunakan media access point memberikan tingkat keamanan yang baik terhadap data user yang sedang mengakses jaringan wireless, untuk mengetahui metode apa sajakah yang digunakan untuk mengamankan data user ketika mengakses jaringan wireless, untuk mengetahui bagaimana system keamanan wireless dengan menggunakan media access point wireless memiliki beberapa metode diantaranya SSID, MAC Filtering, WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*). Secara umum wireless memiliki beberapa tipe serangan diantaranya *passive attacks*, *active attacks*, *man in the middle attacks*, *Brute Force Attacks*

Kata kunci: monitoring, keamanan , WLAN.

ABSTRACT

The innovations of technology is rapidly increasing and influted the human life. Technology become a necessity that is becoming important. One of technology that widely used is wireless local area network (WLAN). Most electronic device that using wireless technology is produced in large scale because the needs of information, so many place such as college, office, café, mall provides a wi-fi service (wireless fidelity). However, these service often pay less attention to secure the network. Vulnerabilities that happens make the user of wireless hesitated the secure of that network. Implementation of WLAN require a security system that sufficient to prevent unauthorized users to entering the network. This study aimed to determine wheter the wireless by using media access point provides a good levelof security for user data that is accessing the network wireless, to know what are the method used to secure user data when access ing the wireless, to know how to use wireless security system media wireless access point has a number of methods including SSID, MAC Filtering, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access). In general has several type of attacks include passive attacks, active attacks, man in the middle attacks, Brute Force Attacks.

Keyword: monitoring, security, WLAN.

KATA PENGANTAR

Dengan mengucap puji syukur kehadiran Allah SWT yang telah melimpahkan segala rahmat dan karunia-NYA, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam
3. Anggiat Marubah Siringo, S.Kom., M.Kom. selaku Dosen Pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Kedua orang tua saya yang senantiasa memberikan doa dan dukungan.
6. Keluarga yang turut memberikan doa dan dukungan.
7. Rekan-rekan mahasiswa/i Universitas Putera Batam yang saling mendukung dan memotivasi.

8. Jasmine Rafilidya azzahra yang memberikan masukan dukungan moral doa dan motivasi.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

Batam, 3 Februari 2018

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	ii
HALAMAN PERNYATAAN.....	iii
HALAMAN PENGESAHAN.....	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xii
DAFTAR RUMUS	xiii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Penelitian	1
1.2. Identifikasi Masalah.....	5
1.3. Batasan Masalah	6
1.5. Tujuan Penelitian	6
1.6. Manfaat Penelitian.....	7
 BAB II KAJIAN PUSTAKA.....	 8
2.1. Teori Dasar.....	8
2.1.1. Internet Protokol	8
2.1.2. Jaringan <i>Wireless</i>	9
2.1.2.1. Komponen Utama Jaringan <i>Wireless</i>	12
2.1.2.2. Standarisasi <i>Wireless</i>	14
2.1.2.3. Topologi Jaringan <i>Wireless</i>	17
2.1.2.4. Keuntungan dan Kelemahan Jaringan <i>Wireless</i>	18
2.1.3. Keamanan Jaringan.....	23
2.1.3.1. Indikator Protokol Keamanan Jaringan <i>Wireless</i>	24
2.1.3.2. Indikator <i>Brute Force Attack</i>	29
2.1.4. Kali Linux	31
2.2. Tools.....	32
2.2.1. <i>Aircrack-ng</i>	32
2.2.2. <i>Macchanger</i>	34
2.2.3. <i>Crunch</i>	35
2.3. Penelitian Terdahulu	35
2.4. Kerangka Pemikiran.....	43
 BAB III METODE PENELITIAN	 45
3.1. Desain Penelitian	45
3.2. Operasional Variable	49
3.2.1. Variabel Penelitian.....	49

3.2.1.1.	Protokol Keamanan Jaringan Brute Force Attack	50
3.3.	Objek Monitoring.....	50
3.4.	Teknik Pengumpulan Data.....	51
3.5.	Metode Analisis Data.....	52
3.5.1.	Metode <i>Brute Force Attcak</i>	52
3.5.2.	Pengujian <i>Dictionary Attack</i>	56
3.5.3.	Pengujian <i>Hybrid Brute Force Attack</i>	60
3.5.4.	Pengujian Protokol Keamanan WPA2.....	62
3.6.	Lokasi dan jadwal Penelitian	63
3.6.1.	Lokasi.....	63
3.6.2.	Jadwal Penelitian	64
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....		65
4.1.	Hasil Penelitian	65
4.1.2.1	Cracking WPA2	66
4.1.2.2	Pengujian <i>Hybrid Brute Force Attack</i>	70
4.1.2.3	Pengujian <i>Dictionary Attack</i>	74
4.1.3.1	Analisis Protokol Keamanan WPA2.....	80
4.4.	Pembahasan.....	84
BAB V SIMPULAN DAN SARAN.....		87
5.1.	Simpulan	87
5.2.	Saran	88
DAFTAR PUSTAKA.....		89

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Perbandingan Model OSI dan TCP/IP	8
Gambar 2.2 Pembagian jaringan <i>wireless</i> berdasarkan jangkauanya	9
Gambar 2.3 Model Kerja AP	12
Gambar 2.4 AP yang lebih dari satu	13
Gambar 2.5 Model AP dan <i>Extension Point</i>	13
Gambar 2.6 <i>MAC address spoofing</i>	34
Gambar 2.7 Kerangka Pemikiran	44
Gambar 3.1 Desain Penelitian	46
Gambar 4.1 <i>macchanger</i>	66
Gambar 4.2 <i>Mode monitor</i>	67
Gambar 4.3 <i>listing access point</i>	68
Gambar 4.4 <i>Airodump-ng</i>	68
Gambar 4.5 <i>aireplay-ng</i>	69
Gambar 4.6 <i>Aircrack-ng</i>	69
Gambar 4.7 <i>Capture Packets</i> dengan <i>Airodump-ng</i> RRI Batam	71
Gambar 4.8 Hasil <i>key found</i> dengan <i>Aircrack-ng</i> 1.2 RC 3	71
Gambar 4.9 <i>Capture Packets</i> dengan <i>Airodump-ng</i> Indosat Batam	72
Gambar 4.10 Hasil <i>key found</i> Indosat Batam	72
Gambar 4.11 Hasil <i>key found</i> Indomaret Baloi	74
Gambar 4.12 <i>Capture Packets</i> dengan <i>Airodump-ng</i> RRI Batam	75
Gambar 4.13 Hasil <i>key found</i> RRI Batam	76
Gambar 4.14 <i>Capture Packets</i> dengan <i>Airodump-ng</i> Indosat Batam	77
Gambar 4.15 Hasil <i>key found</i> Indosat Batam	77
Gambar 4.16 <i>Capture Packets</i> dengan <i>Airodump-ng</i> Indomaret Baloi	78
Gambar 4.17 Hasil <i>key found</i> Indomaret Baloi	79

DAFTAR TABEL

	Halaman
Tabel 2.1 Pembagain jaringan <i>wireless</i> berdasarkan jangkauanya.	11
Tabel 2.2 Standarisasi <i>wireless</i>	15
Tabel 2.3 Data versi <i>Kali Linux</i> hingga Januari 2014	31
Tabel 2.4 List <i>Tools Aircrack-ng</i>	33
Tabel 2.5 Kerangka Pemikiran	44
Tabel 3.1 <i>Brute Force Attack</i>	44
Tabel 3.2 Metode <i>Brute Force Attack</i> mencari “BC”	53
Tabel 3.3 Metode <i>Brute Force Attack</i> mencari “CL”	54
Tabel 3.4 Metode <i>Brute Force Attack</i> Mencari “DI”	55
Tabel 3.5 <i>Password List Dictionary Attack</i> RRI Batam.....	57
Tabel 3.6 <i>Password List Dictionary Attack</i> Indosat Batam	58
Tabel 3.7 <i>Password List Dictionary Attack</i> Indomaret Baloi	59
Tabel 3.8 <i>Password List Hybrid Brute Force Attack</i>	61
Tabel 3.9 Data Protokol Keamanan WPA2.....	62
Tabel 3.10 Jadwal Penelitian.....	64
Tabel 4.1 Hasil pengujian <i>Dictionary Attack</i>	73
Tabel 4.2 Hasil pengujian <i>Dictionary Attack</i>	73
Tabel 4.3 Hasil pengujian <i>Dictionary Attack</i>	74
Tabel 4.4 Hasil pengujian <i>Dictionary Attack</i>	76
Tabel 4.5 Hasil pengujian <i>Dictionary Attack</i>	78
Tabel 4.6 Hasil pengujian <i>Dictionary Attack</i>	79
Tabel 4.7 Data Pengujian <i>Hybrid Brute Force Attack</i> pada protokol WPA2	81
Tabel 4.8 Data Pengujian <i>Dictionary Attack</i> pada protokol WPA2.....	81

DAFTAR RUMUS

	Halaman
Rumus 3.1 Rumus mencari total <i>password</i>	53
Rumus 4.1 perhitungan <i>password</i> RRI Batam.....	82
Rumus 4.2 perhitungan <i>password</i> Indosat Batam.....	83
Rumus 4.3 perhitungan <i>password</i> Indomaret Baloi.....	83