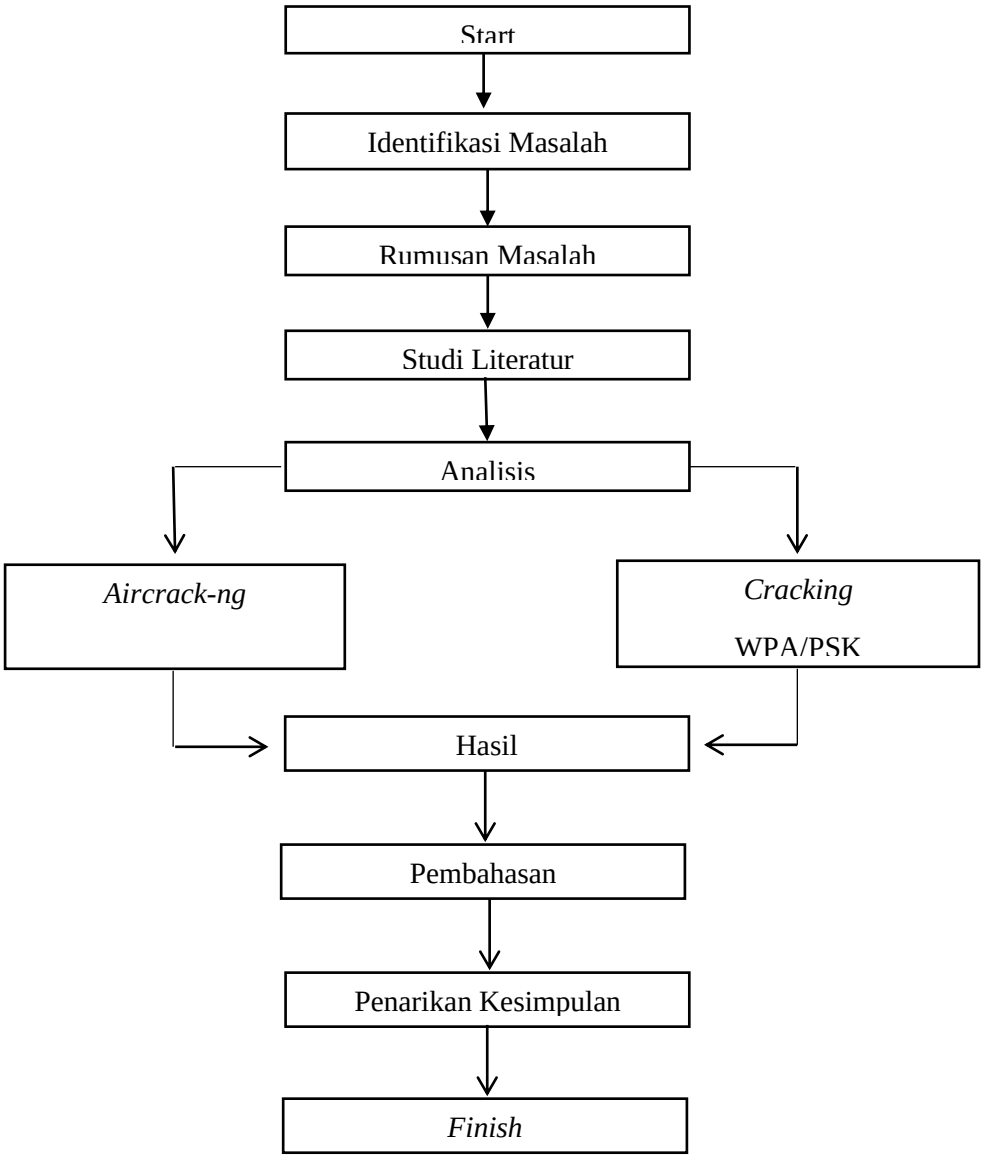
BAB III
METODE PENELITIAN

3.1. Desain Penelitian

Desain penelitian merupakan rencana induk yang berisi metode dan prosedur untuk mengumpulkan dan menganalisis informasi yang dibutuhkan, menetapkan sumber-sumber informasi, teknik yang akan digunakan, metode sampling sampai dengan analisis data untuk dapat menjawab pertanyaan-pertanyaan penelitian (Erlina, 2011:73).

Desain penelitian yang baik harus memuat hal-hal berupa rencana tentang sumber dan tipe informasi yang relevan sesuai dengan kebutuhan peneliti, strategi atau gambaran pendekatan yang digunakan dalam pengumpulan dan analisis data, serta jadwal dan anngaran penelitian yang diperlukan harus diuraikan secara jelas.

Menurut (Suryabrata, 2010: 94) penelitian *action research* atau penelitian tindakan bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara pendekatan baru dan untuk memecahkan masalah dengan penerapan langsung di dunia kerja atau dunia actual yang lain. Sedangkan menurut (Darmadi, 2011: 6) penelitian *action research* bertujuan untuk memecahkan masalah-masalah setempat dengan menggunakan metode ilmiah. Penelitian ini hanya memperhatikan masalah setempat, tidak peduli apakah hasil-hasil yang diperoleh juga dapat diberlakukan ditempat-tempat lain atau tidak.



Gambar 3.1 Desain Penelitian

Berikut adalah penjelasan dari desain penelitian yang ada pada gambar diatas:

a. Identifikasi masalah

Penelitian diawali dengan melakukan studi pendahuluan untuk mengidentifikasi permasalahan yang berkaitan dengan topik penelitian agar

peneliti mendapatkan apa yang sesungguhnya menjadi masalah untuk dipecahkan.

b. Perumusan masalah

Pada tahap ini, peneliti merumuskan masalah yang telah didapatkan secara lebih spesifik agar masalah tersebut dapat dijawab dengan baik melalui penelitian.

c. Studi Literatur

Mempelajari buku-buku dan jurnal-jurnal refrensi yang berhubungan dengan penelitian yang dijalankan, yaitu: Buku *Metode Penelitian Bisnis* (Sugiyono, 2012). Buku *Metode Penelitian Pendidikan* (Darmadi, 2011). Buku *Belajar Cepat Teori, Praktek dan Simulasi Jaringan Komputer & Internet* (Maslan, 2012). Buku *Wireless Networking: Panduan Lengkap Membangun Jaringan Wireless Tampa Teknisi* (Utomo, 2012). Buku *Mastering Wireless Penetration Testing for Highly Secured Environments* (John, 2015). Buku *Kali Linux 200% Attack* (Sto, 2014). Jurnal *Wireless Network Security Protocols A Comparative Study* (Sukhija & Gupta, 2012). Jurnal *Keamanan pada jaringan wireless* (Herdiana, 2014). Jurnal *Analisis Keamanan Jaringan Wireless Yang Menggunakan Captive Portal* (setyawan, Bangkit Kurnia Ari Syafrizal, 2012).

d. Analisis

Analisis data merupakan kegiatan setelah data dari seluruh responden atau sumber data lain terkumpul. Kegiatan dalam analisis adalah

menggelompokkan data berdasarkan variable yang diteliti, melakukan perhitungan untuk menjawab rumus (Sudaryono, 2015)

e. *Aircrack-ng*

Aircrack-ng adalah *tools auditor security* yang ditunjukan melakukan *penetrasi* pada keamanan jaringan *wireless*. *Aircrack-ng* memiliki kemampuan untuk melakukan *cracking* pada protokol 802.11 (*wireless*) dengan *endkripsi* WEP WPA/WPA2-PSK dengan berbagai metode seperti *brute force attack.*

f. *Cracking*

Kegiatan membobol suatu sistem komputer dengan tujuan mengambil atau membobol *password*. *Cracker* biasanya mencoba masuk kedalam suatu sistem komputer tampa izin, tergantung individu ini biasanya berniat jahat/buruk.

g. Hasil

Hasil diambil dari penulis setelah melakukan percobaan dengan memaparkan sebagaimana yang direncanakan atau menghadapi kendala tertentu menjelaskan kendala yang dihadapi. Penyajian hasil penelitian dapat diawali dari hasil implementasi.

h. Pembahasan

Mengungkapkan berbagai penyelesaian dari masalah-masalah yang ditetapkan sebelumnya dan memberi jawaban terhadap masalah yang akhirnya akan mengarahkan kepada kesimpulan yang akan diambil.

i. Penarikan Kesimpulan

Kesimpulan merupakan bagian penutup dari masalah yang ditunjukan kepada objek yang berhubungan dengan tujuan penulisan.

3.2. Operasional Variable

Menurut (Erlina, 2011: 48) operasional *variable* atau disebut dengan Menurut (Erlina, 2011: 48) operasional variable atau disebut dengan mendefinisikan konsep secara operasional adalah menjelaskan karakteristik dari objek ke dalam elemen-elemen yang dapat diobesrvasi yang menyebabkan konsep dapat diukur dan dioperasionalkan ke dalam penelitian. Setiap konsep variablel yang digunakan dalam penelitian harus memiliki definisi yang jelas. Dengan operasional variable, peneliti dapat mengumpulkasn, mengukur, atau menghitung informasi melalui logika empiris. Istilah-istilah dalam operasional variable harus dapat diuji dan mempunyai rujukan empiris.

3.2.1. Variabel Penelitian

Variabel penelitian adalah sesuatu yang dapat membedakan atau mengubah nilai. Nilai dapat berbeda pada waktu yang berbeda untuk objek atau orang yang sama, atau nilai dapat berubah dalam waktu yang sama untuk orang atau obyek yang berbeda (Erlina, 2011: 36)

3.2.1.1. Protokol Keamanan Jaringan *Brute Force Attack*

Pada penelitian ini *Brute Force Attack* bukanlah sebagai variable tapi berfungsi sebagai alat atau metode mengumpulkan data mengenai kelemahan *protocol* keamanan jaringan *wireless* di Kota Batam. *Brute Force Attack* melakukan serangan *Password guessing* secara terus menerus pada suatu jaringan *wireless* , Hingga *Password* tersebut didapatkan.

Tabel 3.1 *Brute Force Attack*

Variabel	**Indikator**	***Value***
Brute Force Attack	*Dictonary Attack*	*Ordinal*
	Hybrid Brute Force Attack	*Ordinal*

3.3. Objek Monitoring

Objek monitoring dalam penelitian ini adalah segala sesuatu yang dijadikan subjek atau objek penelitian yang dikehendaki peneliti. Maka yang akan dijadikan objek dalam melakukan penelitian ini sebagai berikut.

Penelitian ini dilakukan dengan menggunakan perangkat berupa *laptop Dell* dengan *system operasi Kali Linux 2.2, Processor Core i7 2.00Ghz dan RAM 6 GB.* Perangkat jaringan *wireless* yang digunakan yaitu *modem router TP-Link TD-W8151N, modem router TP-Link TD-W8101G, modem router TP-Link TD-W8951ND.* Peneliti menggunakan *Tools Airodump-ng* untuk *wireless* melakukan *capture packet data* pada jaringan *wireless* yang menggunakan protokol keamanan WPA2. Selanjutnya hasil *capture packet data* tersebut akan diuji

dengan *sotware Aircrack-ng 1.2 RC 3* untuk melakukan *capture Handshake* dan *serangan Brute Force Attack.*

3.4. Teknik Pengumpulan Data

Ada beberapa metode pengumpulan data diantaranya dari arsip/dokumentasi (data *sekunder*), wawancara (data *primer*), dan observasi (data *primer*), kuesioner (data *primer*). Secara umum, terdapat dua sumber data untuk menentukan proses pengumpulan data yang akan dilakukan yaitu data *primer* dan *sekunder*. Data *primer* merupakan data yang dikumpulkan berdasarkan interaksi langsung antara pengumpul data dan sumber data. Ada beberapa teknik pengumpulan data *primer*, yaitu *survey*, *observasi* dan *eksperimen*. Sedangkan data *sekunder* dikumpulkan dari sumber-sumber tercetak, dimana data itu telah dikumpulkan oleh pihak lain sebelumnya. Sumber data *sekunder* misalnya buku, laporan perusahaan, jurnal, internet dan sebagainya (Erlina, 2011: 31) Teknik pengumpulan data yang digunakan peneliti adalah *observasi* (data *primer*) dan kajian dokumen (data *sekunder*).

Metode *observasi* merupakan prosedur yang sistematis dan standar dalam pengumpulan data. Pemakaian cara ini didasarkan pada konsep, devinisi dan pengukuran variabelnya. Dengan observasi, peneliti dapat memperoleh ukuran variable yang bukti empirisnya dapat diambil melalui pernyataan yang di ajukan. Disini peneliti tidak hanya berkomunikasi dengan orang, tetapi juga objek penelitian yang lain (Suryabrata, 2010: 92) Observasi dalam penelitian ini melakukan pengamatan pengujian indikator protocol keamanan jaringan yaitu,

WPA2 (*Wi-Fi Protected Access 2*) terhadap serangan *Brute Force Attack* pada jaringan *wireless.*

Dalam melakukan observasi pada jaringan *wireless*, peneliti menggunakan *tools Aircrack-ng 1.2 RC 3*. Dalam penelitiaan ini menggunakan, peneliti menggunakan *tools* tersebut pada *system operasi Kali Linux 2.2*

3.5. Metode Analisis Data

Analisis data adalah proses mencari dan menyusun secara sistematis data yang diperoleh dari hasil wawancara, catatan lapangan, dan dokumentasi, dengan cara mengorganisasikan data ke dalam kategori, menjabarkan ke dalam unit-unit, melakukan sintesa, menyusun kedalam pola, memilih mana yang penting dan yang akan dipelajari, dalam membuat kesimpulan sehingga mudah dipahami oleh diri sendiri maupun orang lain (Sugiyono, 2012: 428)

3.5.1. Metode *Brute Force Attcak*

Brute Force Attack adalah metode yang digunakan untuk meretas *password* atau *kriptografi* dengan *algoritma Brute Force*. Kecepatan peretasan ini bergantung pada panjang pendeknya *password* atau *kriptografi* yang ingin dipecahkan.

Feasibilityn dari sebuah *brute force attack* tergantung dari panjangnya *chiper* yang ingin dipecahkan, dan jumlah komputasi yang tersedia untuk penyerang. Salah satu contohnya bernama *Aircrack-ng* mencoba semua kombinasi yang mungkin dari karakter yang telah didefinisikan sebelum atau set

karakter yang kustom melawan sebuah *password* yang telah terenkripsi di *brute force dialog.*

Kuncinya adalah mencoba semua kemungkinan *password* dengan *formula* seperti berikut.

$$KS = L^{(m)} + L^{(m+1)} + L^{(m+2)} + ... + L^{(M)}$$

Rumus 3.1 Rumus mencari total *password*

L = jumlah karakter yang kita ingin definsikan

m = panjang minimum dari kunci

M = panjang maksimal dari kunci

Contohnya saat kita ingin meretas sebuah *wireless pasword* dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter, dengan panjang *password* 7 maka *brute force cracker* harus mencoba KS = 26^1 + 26^2 + 26^3 + ... + 26^7 = 8353082582 kunci yang berbeda. Jika ingin meretas *password* yang sama dengan set karakter set.

Berikut metode sederhana *Brute Force Attack* Dengan karakter set “ABCDEFGHIJKLMNOPQRSTUVWXYZ” dengan jumlah 26 karakter dengan panjang *password* 2 maka *brute force* dapat melakukan kemungkinan 676 kunci yang berbeda. Dengan mencari *Password* “BC”

Tabel 3.2 Metode *Brute Force Attack* mencari “BC”

No	Password
1	AA
2	AB
3	AC
4	AD

No	Password
12	AL
13	AM
14	AO
15	AP

No	Password
24	AX
25	AY
26	AZ
27	BA

5	AE		16	AQ		28	BB
6	AF		17	AR		29	BC
7	AG		18	AS			
8	AH		19	AT			
9	AI		20	AU			
10	AJ		21	AV			
11	AK		23	AW			

Berikut metode sederhana *Brute Force Attack* Dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter dengan panjang *password* 2 maka *brute force* dapat melakukan kemungkinan 676 kunci yang berbeda. Dengan mencari *Password* "CL"

Tabel 3.3 Metode *Brute Force Attack* mencari "CL"

No	Password	No	Password	No	Password	No	Password
1	AA	17	AQ	33	BG	49	BW
2	AB	18	AR	34	BH	50	BX
3	AC	19	AS	35	BI	51	BY
4	AD	20	AT	36	BJ	52	BZ
5	AE	21	AU	37	BK	53	CA
6	AF	22	AV	38	BL	54	CB
7	AG	23	AW	39	BM	55	CC

8	AH	24	AX	40	BN	56	CD
9	AI	25	AY	41	BO	57	CE
10	AJ	26	AZ	42	BP	58	CF
11	AK	27	BA	43	BQ	59	CG
12	AL	28	BB	44	BR	60	CH
13	AM	29	BC	45	BS	61	CI
14	AN	30	BD	46	BT	62	CJ
15	AO	31	BE	47	BU	63	CK
16	AP	32	BF	48	BV	64	CL

Berikut metode sederhana *Brute Force Attack* Dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter dengan panjang *password* 2 maka *brute force* dapat melakukan kemungkinan 676 kunci yang berbeda. Dengan mencari *Password* "DI"

Tabel 3.4 Metode *Brute Force Attack* Mencari "DI"

No	Password	No	Password	No	Password	No	Password
1	AA	24	AX	47	BU	70	CR
2	AB	25	AY	48	BV	71	CS
3	AC	26	BZ	49	BW	72	CT
4	AD	27	BA	50	BX	73	CU
5	AE	28	BB	51	BY	74	CV

6	AF		39	BC		52	BZ		75	CW
7	AG		30	BD		53	CA		76	CX
8	AH		31	BE		54	CB		77	CY
9	AI		32	BF		55	CC		78	DZ
10	AJ		33	BG		56	CD		79	DA
11	AK		34	BH		57	CE		80	DB
12	AL		35	BI		58	CF		81	DC
13	AM		36	BJ		59	CG		82	DD
14	AN		37	BK		60	CH		83	DE
15	AO		38	BL		61	CI		84	DF
16	AP		39	BM		62	CJ		85	DG
17	AQ		40	BN		63	CK		86	DH
18	AR		41	BO		64	CL		87	DI
19	AS		42	BP		65	CM			
20	AT		43	BQ		66	CN			
21	AU		44	BR		67	CO			
22	AV		45	BS		68	CP			
23	AW		46	BT		69	CQ			

3.5.2. Pengujian *Dictionary Attack*

Dictionary Attack serangan berturut-turut dengan menggunakan daftar kata-kata, lalu mengenkripsinya, dan membandingkan dengan *one way hash* dari sistem. Jika *hash* sama, maka *password* sukses di-*crack*, dan kata itu adalah *password*.

Serangan *Brute Force* pada suatu jaringan dengan cara *Dictionary Attack* memerlukan daftar *password* dengan jumlah yang banyak. Semakin banyak jumlah *password* yang dimiliki maka kemungkinan *password* yang akan ditemukan semakin tinggi. Penulis menggunakan daftar *password* yang di buat melalu**i** *Crunch* di *Kali Linux.*

Berikut ini adalah tabel *Password List* untuk *wireless dictionary attack* di RRI Batam dengan jumlah 20 *password* dari total 282,475,249 *password* yang penulis gunakan.

Tabel 3.5 *Password List Dictionary Attack* RRI Batam

Password List Dictionary Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	aaaaaadeui	Alphabet	10
2	aaaayadeui	Alphabet	10
3	aaaayadeui	Alphabet	10
4	ddddddeui	Alphabet	10
5	ddddyadeui	Alphabet	10
6	deuayadeui	Alphabet	10
7	eeeeeeeeui	Alphabet	10
8	deeeeedeui	Alphabet	10
9	eeeeeyadeui	Alphabet	10
10	iiiiiiiiui	Alphabet	10
11	iiiiiideui	Alphabet	10
12	uuuuuuueui	Alphabet	10
13	uuuayadeui	Alphabet	10

14	ueuayadeui	Alphabet	10
15	ttuayadeui	Alphabet	10
16	tttayadeui	Alphabet	10
17	teuayadeui	Alphabet	10
18	yyyyyydeui	Alphabet	10
19	yyyayadeui	Alphabet	10
20	yeuayadeui	Alphabet	10

Berikut ini adalah tabel *Password List* untuk *wireless dictionary attack* di Indosat Batam dengan jumlah 20 *password* dari total 10,077,696 *password* yang penulis gunakan.

Tabel 3.6 *Password List Dictionary Attack* Indosat Batam

Password List Dictionary Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	3ddeemoor	Alphabet	9
2	33demoorr	Alphabet	9
3	333demmor	Alphabet	9
4	ddemmor33	Alphabet	9
5	ddddemor3	Alphabet	9
6	eeemmor33	Alphabet	9
7	eemmmmor3	Alphabet	9
8	eemmoorr3	Alphabet	9
9	meeeoorr3	Alphabet	9
10	mmeeoorr3	Alphabet	9

11	mmeeor333	Alphabet	9
12	mmeeoor33	Alphabet	9
13	mmeeorr33	Alphabet	9
14	orreomm33	Alphabet	9
15	oreoomm33	Alphabet	9
16	oredoom3	Alphabet	9
17	oredoom33	Alphabet	9
18	reedoom33	Alphabet	9
19	reddoom33	Alphabet	9
20	reddom333	Alphabet	9

Berikut ini adalah tabel *Password List* untuk *wireless dictionary attack* di Indomaret Baloi dengan jumlah 20 *password* dari total 134,217,728 *password* yang penulis gunakan.

Tabel 3.7 *Password List Dictionary Attack* Indomaret Baloi

Password List Dictionary Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	001admnrt	Alphabet	9
2	011admnrt	Alphabet	9
3	01aadmnrt	Alphabet	9
4	01addmnrt	Alphabet	9
5	1aadmnrt0	Alphabet	9
6	11admnrt0	Alphabet	9
7	1addmnr0t	Alphabet	9

8	a0dm1nnrt	Alphabet	9
9	addm0n1rt	Alphabet	9
10	admnn0r1t	Alphabet	9
11	damnrat01	Alphabet	9
12	d1ndmrat0	Alphabet	9
13	d1nd0mart	Alphabet	9
14	m1d0nar1t	Alphabet	9
15	mdnan0r1t	Alphabet	9
16	martmldor	Alphabet	9
17	martd1nd0	Alphabet	9
18	nartd1nd0	Alphabet	9
19	rtmartd10	Alphabet	9
20	tdmnn0ra1	Alphabet	9

Pengujian *Dictionary Attack* dilakukan dengan *software Aircrack-ng* 1.2 RC 3. Hasil pengujian dari *Dictionary Attack* dirumuskan dalam bentuk tabel.

3.5.3. Pengujian *Hybrid Brute Force Attack*

Hybrid Brute Force Attack merupakan serangan berturut-turut dengan menggunakan daftar kata-kata dalam kamus yang telah dimodifikasi. *Password* dimodifikasi dengan menambahkan pada *password* list kemungkinan *password* yang digunakan oleh pemilik jaringan *wireless* yang di *attack*.

Berikut adalah *password* yang penulis modifikasi untuk *Hybrid Brute Force Attack* dengan jumlah 20 *password* dari total 92,600 *password* yang digunakan:

Tabel 3.8 *Password List Hybrid Brute Force Attack*

Password List Hybrid Brute Force Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	Chocoverona	Alphabet	11
2	poldakepri123	Alphanumeric	13
3	Lewishamilton	Alphabet	13
4	Teuayadeui	Alphabet	10
5	Barcelona	Alphabet	9
6	Zakizari678	Alphanumeric	11
7	Rachmimustar6	Alphanumeric	13
8	Rriindonesia	Alphabet	12
9	Kapoldabatam	Alphabet	12
10	Indomaret9966	Numeric	13
11	Speedy123	Alphanumeric	9
12	Admin123	Alphanumeric	8
13	Love123456	Alphanumeric	10
14	Administrator	Alphabet	13
15	Samsung123	Alphanumeric	10
16	Internet	Alphabet	8
17	Sweetlove	Alphabet	9
18	Cafe9876	Alphanumeric	8
19	Afterall79	Alphanumeric	10
20	Aircraft3340	Alphanumeric	12

Pengujian *Hybrid Brute Force Attack* dilakukan dengan *software Aircrack-ng 1.2 RC 3*. Hasil pengujian dari *Hybrid Brute Force Attack* dirumuskan dalam bentuk tabel.

3.5.4. Pengujian Protokol Keamanan WPA2

Wi-FI *Protected Access* (WPA2) menerapkan standar IEEE 802.11i dan merupakan pengembangan lebih dari WPA. WPA2 diperkenalkan pada bulan September 2004 oleh Wi-Fi *Alliance*. Pengujian ini dilakukan pada beberapa lokasi di Kota Batam yaitu kantor RRI Batam, Indomaret Baloi, Indosat Batam Center.

Pengujian dilakukan dengan *tools Aircrack-ng* 1.2 RC 3. Untuk melakukan serangan *dictionary Attack dan Hybrid Brute Force Attack.* Hasil dari pengujian protokol keamanan WPA2 dirumuskan dalam bentuk tabel.

Tabel 3.9 Data Protokol Keamanan WPA2

Lokasi	Lokasi pengujian *Dictionary Attack* dan *Hybrid Brute Force Attack*
Password	*Password* yang digunakan pada jaringan *wireless*
Jenis *Password*	Jenis *password* yang digunakan terdiri dari *alphabet, numeric* dan *alphanumeric*
Panjang *Password*	Panjang karakter *password* yang digunakan
Posisi *Password*	Posisi *password* yang ditemukan pada *password list*
k/s (key/second)	Kecepatan *Dictionary Attack* dan *Hybrid Brute Force Attack* melakukan *brute force password* pada jaringan *wireless* per detik

Password Ditemukan	Berhasil atau tidak serangan *Dictionary Attack* dan *Hybrid Brute Force Attack* yang dilakukan pada jaringan *wireless*

3.6. Lokasi dan jadwal Penelitian

Lokasi dan jadwal penelitian ini berdasarkan lokasi dan jadwal yang sudah dijalani oleh peneliti dimulai dari penginputan judul penelitian sampai dengan sebelum batas akhir pengumpulan hasil penelitian.

3.6.1. Lokasi

Penelitian dilakukan pada jaringan wireless yang menggunakan protokol keamanan jaringan WPA2 *(Wi-Fi Protected Access 2)*, yang berada di kota batam diantaranya kantor RRI Batam Center, Indomaret Baloi, Kantor Indosat Batam Center

3.6.2. Jadwal Penelitian

Penelitian ini dilakukan pada tanggal Maret 2017 sampai Agustus 2017. Pengumpulan data tidak akan menggangu aktivitas yang sedang dilakukan oleh responden dan disesuaikan dengan jadwal penelitian yang terjadwal.

Tabel 3.10 Jadwal Penelitian

No	Kegiatan	Tahun 2016 – 2017																							
		Maret 2017				April 2017				Mei 2017				Juni 2017				Juli 2017				Agustus 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Penyusunan Pendahuluan																								
2	Penyusunan Tinjauan Pustaka																								
3	Penyusunan Metode Penelitian																								
4	Hasil Penelitan dan Pembahasan																								
5	Simpulan dan Saran																								