Vol. IX, No. 2, September 2016

## RANCANG BANGUN APLIKASI *WIRELESS* PENETRATION TEST PADA SISTEM OPERASI LINUX

Aditya Dwipayana<sup>1</sup>, I Made Oka Widyantara<sup>2</sup>, Ni Made Ary Esta Wirastuti<sup>3</sup> Jurusan Teknik Elektro dan Komputer Fakultas Teknik Universitas Udayana Jln. Jalan Kampus Bukit Jimbaran 80361 INDONESIA Email: aditya.dwipayana@gmail.com<sup>1</sup>, oka\_widyantara@yahoo.com<sup>2</sup>, arydev\_02@yahoo.com<sup>3</sup>

#### ABSTRAK

Algoritma enkripsi adalah pertahanan pertama terhadap serangan jaringan. *Wired Equivalent Privacy* (WEP) dan *Wi-Fi Protected Access* (WPA) digunakan untuk mengamankan jaringan pada standar 802.11, akan tetapi enkripsi ini memiliki banyak kelemahan. Aplikasi-aplikasi penetrasi berbasis linux seperti *aircrack, airodump, aireplay* mampu memanfaatkan kelemahan tersebut untuk dapat terkoneksi ke dalam jaringan dan bahkan mencuri data. Sayangnya aplikasi penetrasi berbasis *text* mengakibatkan kesulitan tersendiri bagi pengguna umum karena harus mengingat format perintah pada setiap aplikasi. Penelitian ini berhasil menyederhanakan penggunaan aplikasi penetrasi berbasis *text* dengan cara membangun sebuah antarmuka menggunakan *QTdesigner* serta memberikan *review* proses penetrasi terhadap keamanan WEP dan WPA menggunakan antar muka yang diusulkan.

Kata Kunci: Encryption, 802.11, WEP, WPA, Aircrack, QTdesigner, Python.

#### ABSTRACT

Encryption algorithm is the first defense against network attacks. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) is used to secure 802.11-based networks, but these encryption has many weakness. Linux's tools such as aircrack, airodump, aireplay are able to exploit that weakness to gain access to the network and even steal the data. Unfortunately, text based application causing its own complexcity for common user because they must remember the format command on each application. This study managed to simplify the use of text based penetration application by build an interface using QTdesigner as well as provide a review of WEP and WPA penetration process using proposed interface system.

Keywords: Encryption, 802.11, WEP, WPA, Aircrack, QTdesigner, Python.

#### 1 PENDAHULUAN

Wireless Local Area Network (WLAN) adalah suatu jaringan area local tanpa kabel dimana media transmisinya dapat berupa frekuensi radio (RF) dan infrared (IR) (Widyantara et al, 2010). Tingkat ancaman pada teknologi *wireless* semakin berkembang sejalan dengan perkembangan teknologi *wireless*. Sifat jaringan *wireless* yang *mobile* memicu meningkatnya potensi ancaman keamanan yang lebih besar dibandingkan jaringan kabel. Sehingga untuk mencegah akses

yang tidak sah, IEEE memperkenalkan standar keamanan nirkabel pertama pada tahun 1999 yang disebut Wired Equivalent Privacy (WEP). Algoritma enkripsi WEP ini menggunakan algoritma Rivest Chiper 4 (RC4) dari RSA Data Security.Namun, algoritma enkripsi ini tidak bertahan lama.Pada tahun 2001 ditemukannya celah keamanan pada algoritma key scheduling RC4 (Fluhrer et al, 2001). Sejak saat itu standar WEP dikenal dengan enkripsi protocol yang lemah. Sehingga pada tahun 2003, Standar ini kemudian digantikan oleh Wi-Fi Protected Access (WPA) dan berlanjut digantikan oleh standar 802.11i atau yang lebih dikenal dengan nama WPA2 pada tahun 2004.Algoritma WPA ternyata juga memiliki kelemahan pada Authentifikasi Pre-shared dan kev Temporal Key Integrity Protocol.

Aircrack. airodump, aireplay adalah beberapa aplikasi yang berfungsi untuk melakukan penetrasi pada jaringan wireless. Aplikasi ini mencoba mengekploitasi kelemahan-kelemahan yang hadir pada alogitma enkripsi WEP dan WPA. Namun sayangnya, aplikasi tersebut dijalankan melalui commandline sehingga pengguna harus mengetahui baris perintah yang harus dijalankan. Penelitian ini mengusulkan sebuah *interface* untuk mempermudah pengguna dalam melakukan penetrasi terhadap suatu jaringan wireless. Interface pada penelitian ini dibangun dengan memanfaatkan aplikasi *Qt-designer*  yang menghubungkan *interface* dengan aplikasi berbasis *text*.

### 2 KELEMAHAN PADA STANDAR 802.11

De-authentication adalah contoh sebuah serangan yang dapat bekerja pada protocol WEP bahkan WPA (Tews et al, 2009). Serangan De-authentication ini bekerja dengan cara mengirim banyak paket De-authentication ke jaringan wireless sehingga mengacaukan wireless service client. Serangan ini dapat mengakibatkan terputusnya koneksi seluruh pengguna wireless yang lain :

## 2.1 Kelemahan Algoritma Enkripsi WEP

WEP adalah algoritma enkripsi yang dikembangkan oleh IEEE. Algoritma enkripsi WEP menggunakan algoritma RC4 dan menggunakan 2 buah ukuran kunci yakni 40 bit dan 104 bit. Pengguna *wireless* yang dapat terkoneksi dengan *accesspoint* adalah hanya pengguna yang mempunyai kunci rahasia yang sama. Metode enkripsi pada algoritma WEP disebut simetrik, karena WEP menggunakan kunci yang sama dalam mengenkripsi dan mendekripsi data.

Algoritma enkripsi WEP memiliki berbagai kelemahan antara lain :

- Algoritma RC4 yang digunakan dalam WEP dapat dipecahkan.
- WEP masih menggunakan kunci yang bersifat statis.

- Kelemahan pada *initializationvector* (IV).
- Kelemahan pada integritas pesan *Cyclic Redundancy Check* (CRC-32).

Serangan-serangan terhadap kelemahan WEP antara lain :

• FMSAttack

Serangan ini disebut FMS attack karena diambil dari singkatan nama ketiga penemu celah keamanan ini yakni Fluhrer, Mantin, dan Shamir. FMS attack dilakukan dengan cara mengumpulkan initialization vector lemah dalam jumlah banyak. Semakin banyak IV lemah yang didapat maka semakin cepat cracking dapat dilakukan.

• Choping Attack

Pertama kali ditemukan oleh seseorang dengan identitas di internet bernama h1kari. Tidak seperti FMS *attack*, teknik ini hanya membutuhkan IV unik yang kemudian dgunakan pada proses *cracking* kunci WEP. IV unik mampu mengurangi kebutuhan IV lemah dalam melakukan *cracking* WEP.

Kedua serangan diatas membutuhkan waktu dan paket data yang cukup, sehingga untuk mempercepat proses *cracking*, para *cracker* biasanya melakukan

## 2.2 Kelemahan Algoritma Enkripsi WPA

Wi-Fi Protected Access (WPA) adalah sebuah algoritma enkripsi yang dikembangkan oleh *Wi-Fi Alliance* sebagai upaya penyempumaan kelemahan-kelemahan yang ditemukan pada algoritma enkripsi *Wired Equivalent Privacy* (WEP). Perubahan yang paling signifikan adalah penambahan *Pre-Shared Key* (PSK) dan *Temporal Key Integrity Protocol* (TKIP). Penambahan TKIP tersebut ternyata tidak menjamin algoritma enkripsi WPA dari kelemahan-kelemahan.

Kelemahan-kelemahan pada algoritma enkripsi WPA antara lain :

- Authentifikasi Pre-shared key (PSK) yang digunakan pada algoritma enkripsi WPA sangat rentan terhadap serangan offline dictionary attacks.
- *Temporal Key IntegrityProtocol* (TKIP) yang digunakan pada algoritma enkripsi WPA juga rentan terhadap serangan *ChopChop attack* karena sama-sama menggunakan RC4 seperti WEP.

#### **3** SKEMA SISTEM

Perancangan aplikasi wireless penetration test dibangun pada sistem operasi linux. Sistem operasi yang digunakan adalah Linux Ubuntu 8.04. Perancangan sistem ini dilakukan melalui 4 tahap yakni pembuatan *flowchart* sistem, pembuatan Diagram context, pembuatan DFD level 0 dan pembuatan DFD level 1. Keempat proses tersebut mampu mewakili langkah-langkah penetrasi algoritma enkripsi WEP dan WPA.

#### 3.1 Flowchart Sistem

*Flowchart* berfungsi untuk menggambarkan alur data secara keseluruhan pada suatu sistem. *Flowchart* dari sistem *wireless penetration test* ditunjukan pada Gambar 1.



Gambar 1. Flowchart Sistem.

#### 3.2 Diagram Context

*Diagram context* untuk sistem wireless penetration test ditunjukkan pada Gambar 2.



Gambar 2. Diagram Context

Diagram context adalah Diagram level tertinggi dari Data Flow Diagram (DFD). Diagram context menggambarkan hubungan sistem dengan entitas-entitas eksternal serta menunjukan masukan/*input* dan keluaran/*output* sistem secara keseluruhan.

#### 3.3 DFD Level 0

DFD *level* 0 berfungsi untuk menggambarkan *internal* sistem secara keseluruhan. Proses *monitoring* data adalah proses untuk memonitoring/mengcapture paket data yang dikirim oleh accesspoint. Sedangkan proses *cracking* adalah proses pencarian *password* terhadap data yang telah dikumpulkan.



Gambar 3. DFDLevel 0

#### 3.4 DFD Level 1

Pada DFD *level* 1, proses *cracking* dijabarkan menjadi 2 proses yang lebih kecil, yakni proses WEP *cracking* dan WPA *cracking*.



Gambar 4. DFD Level 1.

Pada proses WEP cracking (2.1), masukan/input dari proses ini adalah capfile dari hasil proses monitoring data. Sedangkan Keluaran/output dari proses ini adalah password hasil cracking. Untuk proses WPA cracking (2.2) terdapat 2 masukan/input untuk proses ini yakni, wordlist dan capfile. Keluaran/output dari proses ini adalah password hasil cracking.

#### 4 IMPLEMENTASI SISTEM

Secara garis besar implementasi sistem wireless penetration test ini terbagi kedalam 2 proses inti yaitu proses monitoring paket data dan proses cracking. Seluruh proses tersebut ditampilkan dalam bentuk antarmuka grafis. Langkah-langkah melakukan penetrasi untuk wireless cracking dibangun berurutan serta dipisahkan ke dalam lima menu berbeda yang terdiri dari Setup, Scan, WEP cracking, WPA Cracking dan Cracking Password sehingga memudahkan pengguna dalam menggunakan aplikasi.

Langkah pertama dalam melakukan proses penetrasi terhadap suatu jaringan wireless adalah melakukan konfigurasi sistem pada *menu setup* seperti ditunjukan pada Gambar 5. Pada *menu* ini, pengguna dapat mengkonfigurasi :

#### • Lokasi file

Lokasi *file* adalah lokasi tempat menyimpan *file log* sistem, *file backup mac address, file captured packet*, dll. Tombol *delete old* data berfungsi untuk menghapus seluruh *log* terakhir dengan cara menjalankan perintah *rm* -f \*.cap \*.csv \*.xor \*.netxml.

#### Konfigurasi wireless adapter

Pengguna dapat memilih *wireless adapter* yang akan digunakan serta mengaktifkan/ mematikan *mode monitor* pada *wireless adapter* tersebut dengan bantuan aplikasi *airmon* dengan menjalan perintah *airmon-ng start wlan0*.

#### Mengganti Mac address

Pengguna dapat mengganti *mac address* dari *wireless* card yang digunakan untuk menjaga privasi (menyembunyikan jati diri) pengguna tersebut. Perintah yang dijalankan oleh sistem adalah *macchanger –mac mon0*.

#### • Restore Mac address

Seperti namanya, tombol ini berfungsi untuk mengembalikan *mac address* dari *wireless* card ke keadaan semula.

toot Delete ald files elect Wireless Interface Enable/Uisable Monitor Mode Rescan wireless interfaces Interface MAC Chipset Driver Nucle wilen0 00:27:19:bb:/7a Railink 2573 US rt73usb - [phy] Managed Iorige Mac Terface name : wilan0 Chunge MAC address ake MAC : 00:27:19:bc://aio/ Restore original MAC address			Where sav	e all logs & cap ?			
elect Wirelass Interface Enable/Disable Monitor Mode Interface MAC Object Driven Nude awlano 00:27:19:bb:7a Ralink 2573 U: rt73usb - [phy] Managed Iurige Ma: rterface name : Wism0 Chunge MAC ddlrcss Restore original MAC address	root	۲				Delete old	files
Enable//Disable Monitor Mode         Rescan wireless interfaces           Interface         MAC         Chipkel         Driven         Nuide           I wilsno         00:27:19:bc:7a Rallink 2573 US rt73usb - [phy] Managed         Image Mailer           Isinger Mailer         Chunge MAC         Chunge MAC address           Restore original MAC         00:27:19:bc:7a;07         Restore original MAC address	elec	t Wireless	s Interface —				
Interface         M4C         Original         Driver         Mule           1         wlano         00:27:19:bc:7a         Rallink 2573 US rt73usb - [phy] Managed           1         orige Mail		Enable/	Disable Monitor	Mode	Rescan	wireless interfac	:es
1         Wlano         00:27:19:bc:7a Rallink 2573 Ut rt73usb - [phy] Nanaged           1ain go Mai	_		Y			1	
Terrige Mai nterface name : WI300 Chungo MAC addross ake MAC : 00:2719.5c:7a:07 Restore original MAC address		Interface wine0	MAC	Chipsel	Driven Litet73.uch fa	Mude but Managed	
ake MAC : 00:27:19.bc:/a:07 Restore original MAC address	1	Intertace wian0	00:27:19:b	Chipsel c:7a Ralink 2573	Driven Uš rt73usb - [j	Mude Shyl Managed	
ake MAC { 00:27:19.bc:7a:07 Restore original MAC address	<b>1</b> Dor	intertace wian0 ge Mac	MAC 00:27:19:b	Chipsel c:7a Ralink 2573	Driven US rt73usb - (p	Mude Shyi Managed	
	1 Char	Interface wian0 ge Mac — face name	MAC D0:27:19:b	Chiped c:7a Ralink 2573	Driven US rt73usb - (p Chi	Mide hyl Managed ange MAC addre	35

Gambar 5. Tampilan menusetup

Gambar 6 menampilkan *men uscan*. *Menu scan* berfungsi untuk melakukan *scaning* terhadap jaringan *wireless* yang tersedia. Pada *menu scan*, pengguna dapat memilih *channel wireless* serta *delay time* yang akan digunakan. Proses *scaning* dilakukan melalui tombol *rescan network* yang kemudian menjalankan perintah *airodump-ng –output-format csv –write* '/tmp/wepwpacracker'.

hannel: all c	hannels (* Sec	.onds. 10 👘	10	estan networks
Essid	Bssid	Channel	Signal	Enc
Internet u	natis episoraer	1:08	1	75 WPA TRIP PSK
<b>15:24 - reso</b>	ar networks [50	(cess)		
45:24 - read 49:31 into	ar networks (54	ccess) iter mode [Failure]		



Gambar 7 menunjukan tampilan menu WEP cracking. Menu ini berfungsi untuk melakukan cracking terhadap jaringan wireless yang menggunakan tipe algoritma enkripsi WEP. Menu ini dibagi menjadi 2 bagian penting yaitu monitoring packet dan injeksi packet

Pada bagian *monitorin gpacket* terdapat tombol *start monitoring* yang berfungsi untuk meng*capture* data yang dikirim oleh accesss *point* dengan cara menjalankan perintah *airodump-ng* –*c Channel* –*w File* –*bssid MacAP Wireless Adapter*. Perintah tersebut akan memunculkan *pop-up shell* seperti ditunjukan pada Gambar 8.

Pada bagian *inject packet* terdapat 2 tombol, yakni *Fake auth to AP* dan *ARP request replay*. Tombol *fake auth to AP* berfungsi untuk melakukan authentifikasi palsu ke *access point* dengan cara menjalankan perintah *aireplay* -1 0 – *eSSIDAP –a MacAP –h MacWirelessAdapterWirelessAdapter*.

Sedangkan tombol *ARP request replay* berfungsi untuk melakukan serangan *arp request* terhadap accesss *point* dengan tujuan mempercepat proses pengumpulan *Initialization Vector* (IV). Tombol ini akan menjalankan perintah *aireplay* -3 -b *MacAP* -h

Wire less A dapter Mac Wire less A dapter.

Perintah tersebut memunculkan pop-up shell seperti yang ditunjukan pada Gambar



Gambar 7. Tampilan form WEP Cracking



Gambar 8. Tampilan Start Monitoring.

Setelah menjalankan *script* untuk me*monitoring packet*, selanjutkan

pengguna dapat melakukan serangan dengan mengklik tombol Fake Auth to AP yang diikuti dengan mengklik tombol ARP Request Replay. Maka akan muncul sebuah pop-up shell seperti gambar di bawah ini.

12			MEL & M	ta un	acker.						100		
Setup	Scan	WEP Cracking	WPA Crac	king	Cracking	Pass	word	6					
		L. 23.		10 00 b	ash -c "a	irepla	<b>19-11</b>	g - 3 - b (	20:21	1:22:38	14817	B -h 00:27	200
-Moni	tor Paci	101		and 16	it markets	Loost 1	1 685	requests	and I	6.72 BCE2	3 dent	sure and	10. 197
10000				had 150	III packets	Loot	HD1	requisits	and it	(715 eCl)	L. sent	tilli packs	(42
121			Cherry March	lead 167	63 packets	(got.)	182	requests	and a	1787 ACKS	), sent	1916 packe	ta(5)
			start Mon	lead 112	III packets	(got )	. HE	requests	and 4	RED.3 HORS	2, sent	1965 packs	ta (4
				lead 163	99 packets	(got.)	182	requests	and it	ABED ACTS	J, seni	5015 pieck.	a., (9
				lead 165	i26 packets	(got :	1.669	requests	and 4	1910 RCR)	i), sent	: 5065 packs	ts(5
				load 100	04 packets	(sot )	1. ARP	requests	and 4	4557 ACKs	i), sent	: 5116 packs	ta(9
				lead 162	tall partoets	fgot :	i HRP	requests	and 1	5006 ACK)	), sent	5165 pecks	1
- Injac	t Parke			lead 170	N6 packets	(got :	1.665	requests	and 5	9052 ROO	3, seri	1 5217 pecke	ts.,,(9
- 9 - 9	12 22 22	NO		load 171	164 packets	(sot :	1.485	10445353	and 5	5656 AON	it. send	: 5265 packs	ta(4
			Jake mil	lead 172	00 parkets	(got )	1467	requests	and 5	5145 AOK	3,. 2011	t 5316 pecke	5
			1222222222	bad 174	//E packets	(sot :	. HO	re-quect.s	and 3	SUH HOD	12, aent	t p.SH4 pecke	ta(4)
				inad 1/f	197 packets	(got )	182	110patolis	and	242 8(8)	13, 2011	: 5415 pecke	z.,
		3	vita technica	land 17)	127 packets	(got :	1.180	requests	and 5	CONTRACTOR	12, sent	t 5467 packs	1(9)
				200 1/1	727 pacheta	1901	115	LE-dripogra	400 3	1556 HURS	if' serie	1 2015 packs	5
				mad 1H1	to packet a	cust.	180	requests	and	INC REAL	2, 3881	tons packs	See. 64
				995 180	tha backets	Cgot .	- HR2*	requests	and t	1451 HUKS	2, 2477	Dalo packs	140
				2003 104	top peotets	1901	- NC	requisits	and	PACE HURS	Er ben	COLO POCKE	···· (2
				hei in	on pacters	egos .	HE	requests	are :	Then He as	CA, SHEET	DATE BALKS	8

Gambar 9. Tampilan ARP request replay.

Menu WPA cracking seperti ditunjukan pada Gambar 10 digunakan melakukan untuk cracking terhadap menggunakan jaringan wireless yang algoritma enkripsi WPA. Menu ini dibagi menjadi 2 bagian penting, yakni bagian monitoring packet dan wpa handshake attack. Pada bagian monitoring packet terdapat tombol start sniffing and logging yang berfungsi untuk mengcapture data yang dikirimkan oleh access point dengan cara menjalankan perintah *airodump-ng* -cChannel -wFile -bssid MacAP WirelessAdapter.

Pada bagian WPA *handshake attack* terdapat 2 tombol yakni tombol *autoload victim clients* yang berfungsi untuk memutus koneksi *wireless* penguna lain dengan perintah *aireplay -0 AttackNumber –a MacAP –c MacClient WirelessAdapter.* Serangan ini dimaksudkan agar *client* yang terputus berusaha terkoneksi kembali ke *access*  *point* sehingga sistem dapat meng*capture* paket *handshake* yang terjadi.

Gambar 11 menunjukan tampilan *pop-upshell* ketika pengguna mengklik tombol start sniffing and logging.



Gambar 10. Tampilan *menu* WPA *Cracking*.



Gambar 11. Tampilan *pop-upshell start* sniffing *and logging*.

Gambar 12 menunjukan tampilan ketika pengguna mengklik tombol client deauthentication yang menyebabkan client tersebut terputus dan melakukan authentifikasi ulang ke accesss point. Ketika sistem mendeteksi adanya paket handshake maka akan terlihat pada pojok kanan atas pada bagian WPA handshake.

I SI WEP & WPA Cra	Croolsnill_dumpbssid 00:80:48:7F:9B:94 mon0; read
Schup Scan WEP Cracking WPA Cracking	$\label{eq:constraint} \begin{array}{llllllllllllllllllllllllllllllllllll$
Start Sriffing and Le	
-WPA bandshake attack And victim client BAC:	THOMENTERS TO AN AND AN AND AN AND AN AND AN AND AN
76:D0:F2:\$3:6F:14	Bash-e-laireplay-ng -0 4 -a 00:80;48:77:98:94 -c 70:1     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0) - c (0)     Control (S)   m -205 -c (0)
Autoload victim clie	22(275)2 -studiet 3- converses Jan. M. S. W. [79(145-2)96566(14)] [ 0 as 22(275)3 -studiet 3- converses Jan. M. S. W. [79(145-2)96566(14)] [ 0 ad
Add the deauth number:	22:21:03 [ending D- converted Deficiting 97 #05.175:04512:95:001411.0.03 22:2-03 [ending D- converse Deficiting 01:40.179:04512:95:001411.0.03
10	
Now you need to capture the HandShake, start the	
Client deauthenticat	

# Gambar 12. Tampilan *start* sniffing and logging.

Menu terakhir adalah menu cracking password. Tampilan menu ini ditunjukan pada Gambar 13.Menu ini berfungsi untuk melakukan cracking terhadap password data yang telah dikumpulkan sebelumnya. Pada menu ini terdapat 2 tombol untuk melakukan crackingpassword sesuai dengan tipe algoritma enkripsinya.

		Aircrack-ng - Crac	k WEP password	
PA Cracking — dd you diction:	irv:			
home/gech4/sk	ripsiy			
	A	rcrack-ng - Crack	WPA password	



Cracking terhadap WEP dapat dilakukan setelah packet data yang terkumpul menunjukan lebih dari 5000.Dengan menekan tombol Aircrack-ng – Crack WEP password. Tombol ini akan menjalankan perintah aircrack –z –b MacAP \*.cap.

<b>H</b>			WEP & V	VPA Cra	cker		
Sahin	Gran	WEP Cracking	10 E	N	root*.cap; read	t *	
Same	- acan	wer cracking	1.000		Aircrack-mg 1	.0 r1645	
Try	P Cracki to Craci	ng k if you have (>5	0001		[00:00:00] Tested 24 keys [go	t 13332 (Va)	
WP	A Cracki	Airci	ack-1 0	depth 1/ 3 3/ 4 0/ 1 0/ 2 0/ 1	byte(uste) R0(10696) 31(19176) 20(17920) 32(17408) FB(17152) 84(16640) 33(21504) 40(19660) 34(19432) 34(19200) 85(19344) 54(17320) 74(19200) 18(19125) 54(13136)	2F(17320) 3B(17320) 96(16640) 3B(15640) EA(18432) 64(10176) 55(17664) 9F(17664) 96(17320) 6F(17664)	
Ade	d you die at	tionary:	_	leorypt	KEY FOUNDI [ 31:32:38:34: ed correctly: 100Z	35 ] (46011; 12345 )	
100	UL.	Airc	ack-r				
_							

Gambar 14. Tampilan WEP cracking.

Gambar 14 adalah tampilaan sistem ketika berhasil melakukan *cracking* terhadap WEP ditandai dengan tulisan *KEY FOUND*. Berbeda dengan *cracking* WEP. *Cracking* WPA dilakukan dengan cara menyediakan *wordlist* yang akan digunakan dalam melakukan WPA *cracking* dan kemudian menekan tombol *Aircrack-ng* – *Crack* WPA *password* seperti ditunjukan pada Gambar 15.

Selon Se	at: ] 194	EP Cuscking	WPA Cresking	CH 1 Elevel:	9 x	1 20	12-11	-22	2:5	e 1	. 89	i he	shi	ale.	. 11	018004
article ac		D Clarking	tirn clarking	PISED	PUR RO	3	www		Det		14	CH.	HE	EN	10	CIP-6
-WEP Cra	icking-			60:80:48:77:83:94	-63 10	,	5741		1763	7	30	1	54	, MP	2	TREE
Try to t	rark if	you have (>h	000) packets	BISSED	STHE10	1		P	æ	Rø	te:	Lo	62	Pack	at a	a Ph
12		Aircs	ack-ng - Decrypt (	M 00:00:48:7*:93:94 00:90:48:7*:93:94	01:40: 70:54:0	12:95	:DF:B		13	24	-24		15		19	26 85
WIN CR	rking			8 2		ro	ate.c	ap	re	ad:						
Add you	diction	ary:					41	e-sed	. mg	, i.,	0 14	645				
adit.txt					Laboration	e Lee						1.74				
		Airca	acking Crock WF	12	1001002	~ ~	1.2545	000	100	120	Vaca	NS				
-				-		11/	0,01	1	123-	1564	01					
				Parter Koy	t in. Rit	80 EB 12 12	32.0	113	33 15	25 10	54 Z	9 3E 0 III	ii ii	97 9 4	51 5	92 E0 95 D
				fransient Ke	: 24 7' F8 F8	10 00 10 00 10 10 10 00 10 10 10 10 10 10 10 10 10 10 10 10 1	NET TO	4 AF A (4 7 13 0 63	111111	EL IA	11000	5 A7	22.5	54 S S S S S S S S S S S S S S S S S S S	1979	A 15 80 39 40 71
				54400, HINC	: 14	20 M	30 6	: 6F	Ŧ	59	AB 7	F E:	:3	77 6	60 1	AD F1

Gambar 15. Tampilan WPA cracking.

#### 5 SIMPULAN

telah memaparkan Paper ini tahapan-tahapan perancangan interface aplikasi wirelesspenetration test dengan cara memanfaatkan tab widget yang teratur untuk memisahkan langkah-langkah penggunaan aplikasi. Sedangkan integrasi antara aplikasi berbasis text dengan interface dilakukan dengan cara

membangun sebuah "slot" pada setiap tombol. Setiap tombol yang ditekan akan memerintahkan sistem operasi untuk menjalankan perintah/commandtextbased. Interface yang dihasilkan mampu mempermudah proses penetrasi pada jaringan wireless dengan tetap mengacu pada langkah-langkah yang sama pada aplikasi berbasis *text* tanpa harus menghafal baris perintah seperti pada mode text.

#### 6 DAFTAR PUSTAKA

- A. Bittau, M. Handley, J. Lackey, "The final nail in WEP's coffin," in IEEESymposium on Security and Privacy, 2006.
- Fluhrer, S., Mantin, I., & Shamir, A., "Weaknesses in the key scheduling algorithm of RC4," in International Workshop on Selected Areas in Cryptography. 2001. pages 1-24.
- G. Mouhcine, L. Aboubakr and B. Amine Benamrane, "Wireless Networks Security: Proof of ChopChop Attack," in World of Wireless, Mobile and Multimedia Networks, 2008.
- J. Bellardo and S. Savage, "802.11 Denialof-Service Attacks: Real Vulnerabilities and Practical Solutions," in USENIX Security Symposium,2003, pages 15-28.
- P. S. Ambavkar, P. U. Patil, B. B. Meshram, and P. K. Swamy, " WPA exploitation in the world of wireless network," *Int J Adv Res Comput Eng Technol.* 2012.

- Tews, E., & Beck, M., "Practical attacks against WEP and WPA", in Proceedings of the second ACM conference on Wireless network security. 2009. pages 79-86.
- Widyantara, I. M. O., Cahyono, B. D., Setiawan W., "Analisa Horizontal Handover Terhadap QoS Layanan Streaming Multimedia E-Learning Pada Jaringan WLAN 802.11," Jurnal Teknologi Elektro, Vol.14. 2015.
- Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11, 1997.
- Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amandment 6 Medium Access Control (MAC) Security Enhancements, IEEE Std. 802.11i, 2004.
- S'to, *Wireless* Kung fu : Networking & Hacking, Jasakom, 2007.
- (2009) Aircrack website. [Online]. Available: https://www.aircrackng.org/doku.php?id=korek\_chopch op.
- (2012) Qt Designer Manual. [Online]. Available: http://doc.qt.io/qt-4.8/designer-manual.html.