EVALUASI APLIKASI EXPLOID WIFI DI TINGKAT AVAILABILITY DAN VULNERABILITY

Timur Dali Purwanto
Fakultas Vokasi, Program Studi Teknik Komputer
Universitas Bina Darma
Email: timoerok@gmail.com

Alek Wijaya
Fakultas Ilmu Komputer, Program Studi Teknik Informatika
Universitas Bina Darma
Email: allec_wj@yahoo.com

ABSTRAK

Pada sistem jaringan *wireless* sering terjadi masalah yaitu salah satunya keamanan *wifi* yang menggunakan keamanan *WPA, WPA2,* dan *WEP* yang ditinjau dari *vulneravility*. Karena teknologi *wireless* memanfaatkan frekwensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Sekarang ini sudah banyak tool aplikasi *exploit wifi* yang di gunakan oleh *hacker* atau *attacker* salah satunya *tool Reaver* dan *tool Aircrack* dalam system operasi kali linux, dari kedua *tool* tersebut peneliti ingin mencari perbandingan dari tingkat *availability*. Karena kedua *too*l tersebut menurut peneliti adalah *tool* yang terbaik saat ini. Dalam penelitian ini parameter yang akan di ukur adalah seberapa capat waktu ackes ke jaringan wifi, seberapa cepat menembus keamanan wifi, dan berapa besaran biter yang di dapat. Dari hasil penelitian dan uji coba maka di simpulkan bahwa untuk segi kecepatan *aircrack* yang lebih cepat untuk memecah password karena *bruteforce* dengan *wordlist*, *reaver* langsung *scanning password wifi* namun memakan waktu sangat lama hampir 13 jam untuk waktu terlama

Kata kunci: *tool reaver* dan *aircrack, avability* dan *vurnability bruteforce, wordlist.*

ABSTRACT

In wireless network systems often occur a problem that is one of the wifi security that uses the security of WPA, WPA2, and WEP in terms of vulneravility. Because wireless technology utilizes high frequencies to deliver a communication, the vulnerability to security is also higher than with other communications technologies. Now there are many wifi exploit application tools that are used by hackers or attackers one of the tools reaver and Aircrack tool in linux operating system, from both tools the researchers want to find a comparison of the availability level. Because the two tools are according to researchers is the best tool today. In this study the parameters to be measured is how much time to wifi ackes wifi network, how fast penetrate wifi security, and how the amount of biter in the can. From the results of research and experiments it is concluded that for the speed facets of aircrack faster to break the password because bruteforce with wordlist, reaver directly scanning the wifi password but take very long time almost 13 hours for the longest time.

Keywords: *reaver and aircrack tool, avability and vurnability bruteforce, wordlist.*

1. PENDAHULUAN

Pada saat berasosiasi menggunakan *wireless* yang terkoneksi dengan media *access point* menggunakan *security WPA* apakah aman dari serangan *hacker*? Ternyata *WPA, WEP* dan *WPA2* masih ada yang mengklaim masih di bobol. [1] menyatakan *WPA, WEP* dan *WPA2* pernah di bobol oleh *attacker*, dalam artian belum aman. Bagaiman cara mengamankan serangan tersebut? Sebelum melakukan pengamanan terlebih dahulu mengetahui bagaimana cara *attacker* melakukan penyerangan kejaringan *wifi* menggunakan *tools* yang sering digunakan para *attacker* atau *cracker* khususnya dalam jaringan wifi tool tersebut adalah *Reaver, aircrack, macchanger, Crunch, Wash, Fern Wifi Cracker, oclHashcat, Wireshark,Wifite, dan* terahir *Pixiewps.* Dari beberapa tool tersebut ada dua *tool* yang akan di pakai dan di perbandingkan.

[2] *Aircrack* adalah salah satu alat yang paling populer untuk WEP / WPA / WPA2 retak. *The Aircrack-ng suite* berisi alat untuk menangkap paket dan jabat tangan, *de-authenticate* terhubung klien dan menghasilkan lalu lintas dan alat-alat untuk melakukan kekerasan dan serangan kamus. [3] *Reaver*

merupakan tool yang terbaru untuk *cracking wifi* dengan *WPA protected* dan ini adalah salah satu *tool* yang digunakan kedua tool tersebut yang akan di gunakan untuk melakukan exploitasi *wifi*. Dari kedua *tool* tersebut mana yang terbaik? Berdasarkan dari pertanyaan dan latar belakang yang diuraikan diatas, maka peneliti tertarik untuk melakukan perbandingan suatu perangkat aplikasi exploit pada jaringan *wifi* yang menggunakan keamanan *WPA*, *WPA2* dan *WEP*.

2. METODOLOGI PENELITIAN

Dalam penelitian ini menggunakan metode penelitian *Action Research* atau metode tindakan. Penelitian tindakan merupakan penelitian yang bertujuan mengembangkan metode kerja yang paling efisien, sehingga biaya produksi dapat ditekan dan produktifitas lembaga dapat meningkat [4].

Action Research menurut Davison, dkk. (2004) [5] yaitu penelitian tindakan yang mendeskripsikan, menginterprestasikan dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau interversi dengan tujuan perbaikan atau partisipasi. Adapun tahapan penelitian yang merupakan bagian dari *Action Research* ini yaitu:

a) Melakukan Diagnosa (*Diagnosing*)
   Peneliti melakukan diagnosa terhadap sistem jaringan *wireless*.
b) Membuat Rencana Tindakan (*Action Planing*)
   Peneliti melakukan rencana tindakan yang akan dilakukan pada jaringan *wifi* dengan membuat pengujian sistem keamanan jaringan yang menggunakan metode exploitasi.
c) Melakukan Tindakan (*Action Taking*)
   Peneliti mengimplementasikan rencana dengan tindakan yang telah dibuat dengan menjalankan tahapan-tahapan mengikuti testing terhadap jaringan wifi untuk mendpatkan celah.
d) Dari sistem jaringan *wifi* dan juga mendapatkan analisis dari hasil pencegahan dari *Reaver* dan *Aircrack*.
e) Melakukan Evaluasi (*Evaluating*)
   Peneliti melaksanakan evaluasi hasil dari penetrasi dan pencegahan yang telah dilakukan pada jaringan *wifi*.
f) Menentukan Pembelajaran (*Specifying Learning*)
   Melakukan review tahapan-tahapan yang telah berakhir dan mempelajari kriteria celah keamanan dan cara menanganinya.

2.1 Metode Pengumpulan Data

Dalam penelitian ini akan menggunakan beberapa metode pengumpulan data, berikut adalah metode pengumpulan akan digunakan :

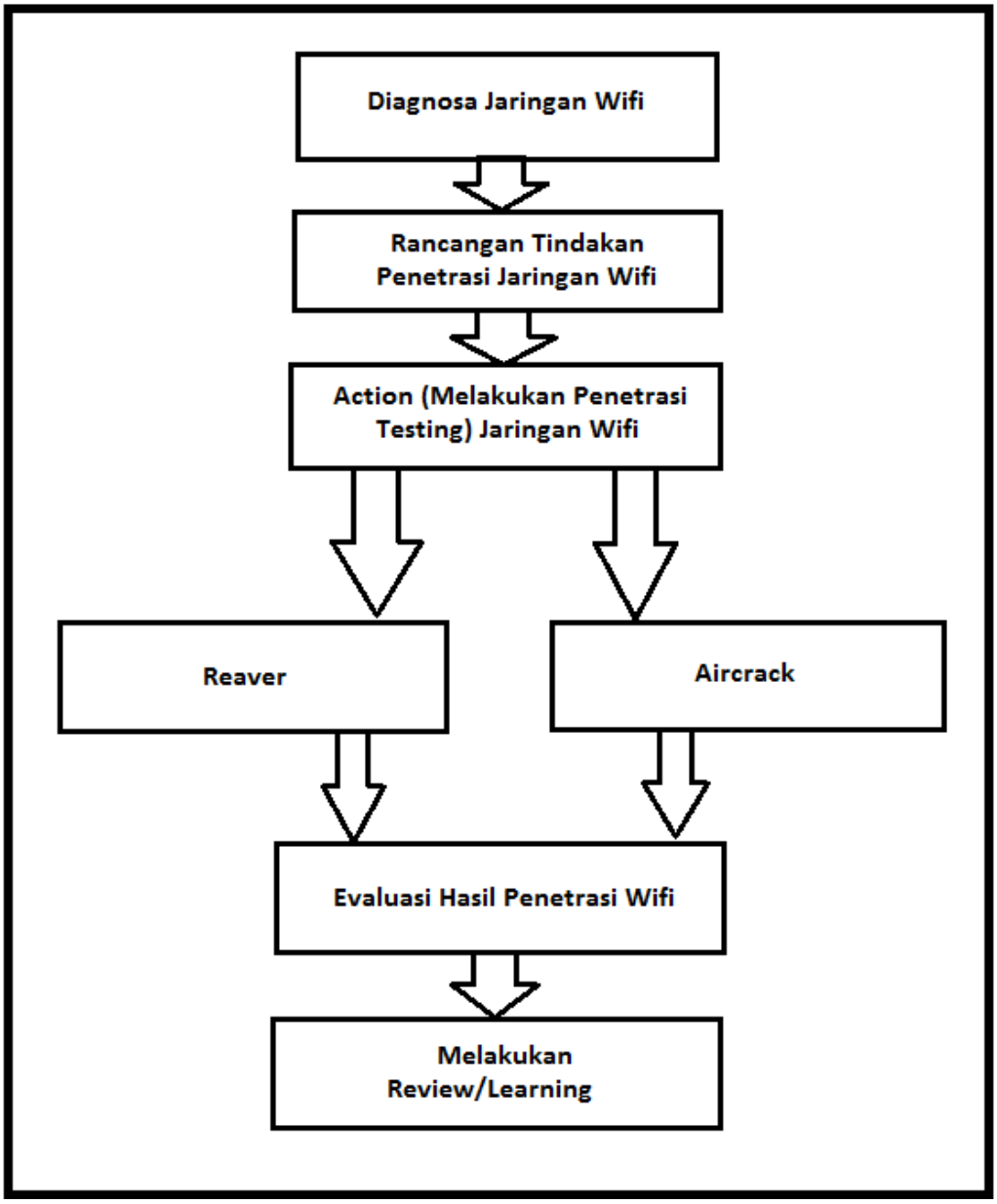
a) Pengamatan *(Observasi)*. Data dikumpulkan untuk mendapatkan hasil yang jelas tentang penelitian ini dalam melakukan pengamatan tentang exploitasi *wifi*.
b) Pengujian (*Testing*). Data diperoleh dari pengujian exploitasi *wifi* yang dilakukan.

2.2 Kerangka Kerja

Tahapan yang terpenting dalam satu penelitian adalah menyusun kerangka kerja. Kerangka kerja yang terkonseptualisasi dengan baik dapat mengetahui pada gejala-gejala pengamatan, yang pernah dijelaskan oleh W Gulo [6] Konseptualisasi adalah proses pembentukan konsep dengan bertitik tolak pada gejala-gejala pengamatan. Kerangka Kerja yang tergambar dibawah dapat dijelaskan sebagai berikut:

a) Sebuah jaringan *wifi* yang akan menjadi objek utama untuk melakukan
b) penetrasi pada penelitian ini.
c) Melakukan diagnosa pada jaringan untuk mengetahui bagian-bagian dari jaringan yang mempunyai celah keamanan, sehingga peneliti dapat menentukan tempat yang tepat untuk dilakukan penetrasi.
d) Didalam penelitian ini akan dilakukan pengujian internal. Pada pengujian internal ini dilakukan penetrasi sesudah proses autentikasi *wireless* dengan tujuan mencari celah keamanan yang bisa dieksplorasi oleh pengguna, untuk pengujian secara internal ini peneliti melakukan serangan yang bersifat pasif dimana serangan tidak mempengaruhi kinerja sistem.

e) Pada tahap Action Taking, tindakan yang akan dilakukan adalah pengujian penetrasi menggunakan *tools reaver* dan *aircrack* Pengujian akan dilakukan kedua tools tersebut untuk mendapatkan hasil dari keamanan jaringan wifi dan mendapat perbandingan dari kedua tool.
f) Evaluasi pada tahapan ini peneliti akan melakukan sebuah kesimpulan mengenai bagaimana cara mengetahui celah dari suatu sistem wifi yang ada dan membuat suatu laporan dari hasil pengujian jaringan.
g) Dokumentasi dan pelaporan meliputi statistik persentase keberhasilan dalam teknik pengujian dan tabel hasil pengujian.



Gambar 1. Kerangka Berpikir

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Hasil ini berdasarkan hasil uji coba *reserch* di laboratorium dengan menggunakan perangkat atau alat sesuai dengan kerangka berpikir, dengan jarak 8 m dari AP target dan frekuensi sebesar 2,4 MHz dengan aliran *bandwith* sebesar 2 Mbps menggunakan aplikasi *aircrack-ng* dan aplikasi *reaver* yang menghasilkan parameter yang telah di uji dari hasil uji tersebut diambil nilai rata-rata tercepat (*accessb Time* dan *Crack Time*) atau tebesar (*bandwitdth*).

Peneliti melakukan evaluasi dari hasil penetrasi dan akan melihat hasil dari perbandingan dari kedua aplikasi yang di uji yaitu aplikasi *aircrack* dan *reaver* dapat dilihat dari ketiga tabel di bawah ini.

Tabel 1. Hasil uji coba menggunakan *aircrack*-ng

No	*Bandwith (bps)*	*Bandwith Nyata (bps)*	*Crack Time (s)*	*Access Time (s)*	*Keterangan*
1	2000	1622	10	120	WPA
2	2000	1532	15	6	WPE
3	2000	217	25	600	WPA2
4	2000	7	10	18	WPE
5	2000	11	10	24	WPA2
6	2000	29	10	480	WPA
7	2000	2580	10	780	WPA2
8	2000	2304	10	6	WPA2
9	2000	2651	10	120	WPA
10	2000	2311	851	1080	WPE
	Rata-rata	***1326,4***	***96,1***	***323,4***	

Tabel 2. Hasil uji coba menggunakan tools reaver

No	*Bandwith (bps)*	*Bandwith Nyata (bps)*	*Crack Time (s)*	*Access Time (s)*	*Keterangan*
1	2000	176	1932	38	WPA
2	2000	1931	45631	18	WPE
3	2000	217	31231	1500	WPA2
4	2000	253	16831	8	WPE
5	2000	11	13231	38	WPA2
6	2000	29	2232	12	WPA
7	2000	645	6031	2700	WPA2
8	2000	1821	5232	120	WPA2
9	2000	764	9631	24	WPA
10	2000	2301	3271	38	WPE
	Rata-rata	***814,8***	***13525,3***	***449,6***	

Tabel 3. Perbandingan dua *tools*

INDUKSI	*TOOLS*	*WPA*	*WEP*	*WPA2*
Kecepatan Akses (Access Time)	*Aircrack*	240	240	325,5
	Reaver	24,667	24,667	1089,5
Bandwith	*Aircrack*	1434	1434	1278
	Reaver	323	323	673,5
INDUKSI	***TOOLS***	***WPA***	***WEP***	***WPA2***
Waktu pembobolan	*Aircrack*	10	10	13,74
(*Crack Time*)	Reaver	4598,3	4598,3	13931,25

3.2 Pembahasan

Berdasarkan hasil dari penelitian dimana terdapat 3 (tiga) Perbandingan dua aplikasi dalam bentuk tabel berdasarkan parameter statement untuk rekomendasi berdasarkan hasil fakta saat melakukan uji penestrasi.

Tabel 1 di merupakan hasil uji coba menggunakan *aircrack*-ng yang dilakukan sebanyak 10 kali percobaan. Dimana rata-rata *bandwith* nyata digunakan sebesar 1.326,4 bps yang kurang dari 2 Mbps. *Crack Time* merupakan kemampuan (*availbility*) tools dalam melakukan bobol password yang dengan kecepatan rata-rata sebesar 96,1 s dan pada *access time* digunakan untuk kemampuan meretas sistem jaringan *wireless* dengan kecepatan sebesar 323,4 s. Berdasarkan keterangan hasil uji dapat disimpulkan bahwa jaringan wariless sangat rentan *(vulnerability*) atau mudah di hack oleh hacker dengan kecepat *Crack Time* 10 s dan *access time* nya dengan kecepatan 6 s yang dibandingan hasil ujian lainnya

Tabel 2 adalah hasil uji coba menggunakan aplikasi *reaver* yang dilakukan sebanyak 10 kali percobaan. Dimana rata-rata bandwith nyata digunakan sebesar 814,8 bps yang kurang dari 2 Mbps. *Crack Time* merupakan kemampuan *(availbility) tools* dalam melakukan bobol *password* yang dengan kecepatan rata-rata sebesar 13525,3 s dan pada *access time* digunakan untuk kemampuan meretas sistem jaringan *wireless* dengan kecepatan sebesar 449,6 s. Berdasarkan keterangan hasil uji dapat disimpulkan bahwa jaringan *wariless* sangat rentan atau mudah di hack oleh hacker dengan kecepat *Crack Time* 1932 s dan *access time* nya dengan kecepatan 8 s yang dibandingan hasil ujian lainnya, tetapi bila *dibandingkan tools rever dan tools aircrack-ng, tools rever* lebih lamban.

Dari hasil tabel 3 berdasarkan nilai rata-rata kedua tools yang di uji menghasilan, induksinya adalah *bandwith, access time*, dan *Crack Time*. Yang di nilai dari *availability* atau (kemampuan) *reaver* lebih simpel dalam pengerjaan. Karena tidak melakukan *bruteforce*, namun memakan waktu lama untuk memecahkan password wifinya ± 5 jam kalu di jam kan. dan *vulnerability* (kerentanan) *password* udah di scanning. Sedangkan *aircrack* dalam pengerjaanya sedikit lebih rumit karena harus melakukan *bruteforce* namun saat memecah *password* lebih cepat karena sudah melakukan *bruteforce* dengan *wordlist* ± 3 jam di wpa dilihat dari *Crack Time*. Dari kedua *tools bandwith* yang di dapat hampir sama, namun dilihat dari waktu pembobolan lebih cepat *aircrack* dari pada reaver.

Cara mengatasi biar sulit untuk di bobol pakailah wpa2 enterprice dan pakai *password* dengan kombinasi yang susah untuk di tebak karna kalau memakai kombinasi yang mudah di tebak atau biasa, mudah sekali di pecah dengan cara *bruteforc*e dengan *wordlist*

4. KESIMPULAN

Adapun hasil dari analisis penelitian ditarik beberapa kesimpulan sebagai berikut :

a) Dari kedua aplikasi yang telah diuji untuk melihat tingkat *availability* dan *vulnerability*, maka disimpulkan bahwa aplikasi *aircrack* lebih cepat untuk menembus *password wifi*, namun *aircrack* lebih rumit dibandingkan dengan *reaver* karena harus melakukan *bruteforce* dengan wordlist. Sedangkan *reaver* langsung melakukan *scanning password* tapi membutuhkan waktu yang sangat lama.
b) Dari segi kerentanan *wifi* yang menggunakan wpa2 lebih sulit untuk ditembus dibandingkan dengan *wifi* yang menggunkana keamanan wep dan wpa. Namun untuk lebih bagus lagi *wifi* yang menggunakan wpa2 lebih baik menggunakan *password* dengan kombinasi yang rumit agar sulit di pecahkan
c) Dengan penjelasan ini, pengguna internet yang menggunakan *wifi* mulai sadar dan mulai merubah *password* dengan teknologi terbaru dan juga mulai menggunakan *mikrotik*. Semakin banyak pengguna *wifi*, semakin lambat juga koneksi internet.

DAFTAR PUSTAKA

[1] Davison, R. M., Martinsons, M. G., Kock N., (2004), *Journal :* Information Systems *Journal : Principles of Canonical Action Research* 14, 65–86.

[2] Hurley Crish, R,F,D,B. (2007). ”WarDriving and *Wireless* Penetration Testing”, Syngress Publishing, Inc. Rockland.

[3] Marco Alamanni (2015). “Kali Linux *Wireless* Penetration Testing Essentials”, Packt Publishing Ltd. Birmingham B3 2PB, UK.

[4] Madya, S, (2006) *Teori dan Praktik Penelitian Tindakan (Action Research),* Alfabeta: Bandung.

[5] Kennedy, David., O’Gorman, Jim., Kearn, Devon., Aharoni, Mati` (2011) .*Metasploit The Penetration Tester’s Guide*. HD MOORE. San Francisco.

[6] Gulo, W. (2010). ” Metodologi Penelitian”. PT. Grasindo. Jakarta.