e-ISSN 2338-5197

Analisis Perbandingan Metode Keamanan *Wireless* WEP 128bit Dan WPA Untuk Meningkatkan Keamanan *Wireless*

Muhammad Yanuar Efendi [a,1], Imam Riadi (0510088001) [b,2]

[a] Teknik Informatika Universitas Ahmad Dahlan, Jl. Ringroad Selatan, Bantul, Yogyakarta 55191, Indonesia
[b] Sistem Informasi Universitas Ahmad Dahlan, Jl. Ringroad Selatan, Bantul, Yogyakarta 55191, Indonesia
[1] fendieart@gmail.com; [2] imam.riadi@is.uad.ac.id

ABSTRAK

Teknologi informasi saat ini terus berkembang seiring dengan kebutuhan manusia yang menginginkan kemudahan, kecepatandan keakuratan serta keamanan dalam memperoleh informasi. Jaringan *wireless* sangat dibutuhkan. Masalah utama jaringan wireless adalah keamanan, metode yang sering digunakan adalah otentikasi. Penelitian ini dilakukan percobaan penetrasi protocol enkripsi WEP 128bit dan WPA. Metode pengumpulan data dalam penelitian ini menggunakan metode observasi, studi literatur dan wawancara. Data yang terkumpul digunakan untuk melakukan langkah selanjutnya yaitu melakukan analisa terhadap metode keamanan wireless WEP 128bit dan WPA dengan menggunakan *tools hacking* aircrack-ng. Berdasarkan penelitian yang berjudul Analisis Perbandingan Metode Keamanan *Wireless* WEP 128bit dan WPA Untuk Meningkatkan Keamanan *Wireless* ini menghasilkan sebuah solusi bagi keamanan jaringan wireless yaitu dengan melakukan penerbitan password yang paling aman untuk digunakan. Hasil dari penelitian ini layak dapat digunakan sebagai solusi masalah keamanan jaringan *wireless.*

Kata kunci: Keamanan, *Password, Wireless*, WEP 128bit dan WPA

1. Pendahuluan

Perkembangan teknologi informasi saat ini terus berkembang seiring dengan kebutuhan manusia yang menginginkan kemudahan , kecepatan dan keakuratan serta keamanan dalam memperoleh informasi. Oleh karena itu kemajuan teknologi informasi harus terus diupayakan dan ditingkatkan kualitas dan kuantitasnya. Salah satu kemajuan teknologi informasi dibidang transmisi pada saat ini yang berkembang selain *Fiber Optic* ialah penggunaan perangkat *wireless* LAN *(WLAN : wireless local area network),* dimana perangkat *wireless* LAN memungkinkan adanya hubungan para pengguna untuk mengakses informasi walaupun pada saat kondisi *mobile* (bergerak).

Wi-Fi (Wireless Fidelity) adalah istilah umum untuk peralatan *wireless* LAN, yang juga dikenal dengan WLAN. Biasanya peralatan *Wi-Fi* mengadopsi standar keluarga IEEE 802.11, yang didukung oleh banyak vendor. Istilah jaringan nirkabel atau *wireless* LAN adalah teknologi jaringan yang tidak menggunakan perangkat kabel yang umumnya dijumpai di dalam sebuah jaringan komputer dewasa ini. Teknologi ini sesuai dengan namanya *wireless* yang artinya tanpa kabel, memanfaatkan gelombang radio untuk melakukan interaksi atau komunikasi antar beberapa unit komputer. Insfrastruktur jaringan Nirkabel memiliki satu masalah besar terutama yang membuka akses untuk umum, seperti *hotspot*, adalah masalah keamanannya, dimana banyak terjadi penyerangan oleh satu atau beberapa orang penyerang *(attacker)* baik pada *server* penyedia *hotspot* atau pengguna.

Pengaman sistem jaringan *Wi-Fi* saat ini digunakanlah teknik enkripsi *WEP (WEP 128bit)* dan *WPA.* Enkripsi digunakan untuk mengubah bit setiap paket data untuk melindungi dari para penyusup maupun penyerang, atau pengguna yang tidak berhak. Pengimplementasiannya dalam

e-ISSN 2338-5197

berbagai macam teknik enkripsi yang digunakan untuk mengamankan jaringan *wireless* diantaranya adalah WEP dan WPA. *WEP (Wired Equivalent Privacy)* pada standar 802.11 merupakan enkripsi opsional dan standar otentikasi yang diterapkan pada beberapa *wireless network interface card* (NIC) dan didukung oleh beberapa vendor access point. WEP bersifat opsional WEP bersifat opsional karena standar enkripsi yang telah disetujui dikonfigurasi sebelum koneksi pengguna *wireless* ke *acces point.* Sesudah pengguna dikonfigurasi pada access point dan pengguna, semua komunikasi yang dikirim melalui udara, dienkripsikan sehingga menyediakan koneksi yang aman dan sulit disusupi. *WPA (Wi-fi Protected Access)* menawarkan kunci enkripsi yang dinamis dan otentikasi secara mutual. Beberapa vendor telah mendukung WPA, sehingga mempermudah implementasinya. WPA menyediakan pengaturan dan implementasi yang cukup mudah tanpa melakukan perubahan yang berarti pada desain hardware WLAN 802.11. Fitur-fitur keamanan yang lebih kuat sangat berhubungan dengan kekuatan pada metode enkripsinya. Hotspot di SMA Muhammadiyah 1 KLaten saat ini sering digunakan guru serta siswa untuk mengakses internet. Hotspot di SMA Muhammadiyah 1 Klaten masih menggunakan metode keamanan wireless WEP dan masih menggunakan password yang lemah sehingga berpeluang untuk disusupi oleh pengguna ilegal. Hal-hal tersebut terjadi tentunya telah melewati beberapa aspek pengamanan yang telah ada. Layanan hotspot SMA Muhammadiyah 1 Klaten menggunakan teknik enkripsi WEP 128bit dan WEP, sehingga jaringannya mudah untuk ditembus.

Berdasarkan latar belakang tersebut maka akan dilakukan studi kasus di SMA Muhammdiyah 1 Klaten yang akan dibahas ”Analisis Perbandingan Metode Keamanan Jaringan Wireless WEP 128bit dan WPA Untuk Meningkatkan Keamanan Wireless”, dengan tujuan untuk membangun dan meningkatkan suatu jaringan *Wireless* LAN yang lebih aman serta membantu dalam proses memanajemen dan pengamanan suatu jaringan *Wireless* LAN, terutama yang digunakan dijaringan publik *Hotspot.*

2. Kajian Pustaka

Penelitian yang dilakukan mengacu pada penelitian terdahulu yang dilakukan oleh: Desmon Sharon, Sapri dan Reno Supardi (2014) Membangun jaringan WLAN *(Wireless Local Area Network)* untuk mengatasi masalah-masalah jaringan LAN sederhana yang ada pada CV.BIQ., Randy Mentang, Alicia A. E. Sinsuw, Xaverius B. N. Najoan (2015) Perancangan dan analisis keamanan jaringan nirkabel menggunakan wireless Intrusion Detection System, Gilang Kumala Dewi, Budi Murtiyasa, Dedi Gunawan (2016) Analisa keamanan jaringan *wireless* di sekolah menengah Al Firdaus, Santi Dwi Ratnasari, Dwi Safiroh Utsalina (2017) Implementasi penanganan serangan *MAC-Clone* pada *hotspot* mikrotik di STMIK Pradnya Paramita Malang.

Berdasarkan beberapa penelitian yang telah dilakukan di atas, belum ditemukan penelitian yang membahas *password* terbaik yang harus diterapkan sebagai solusi keamanan *wireless.* Maka dilakukan penelitian lebih lanjut, sehingga dapat memberikan solusi keamanan jaringan *wireless.*

a. Wireless Network

Menurut Lfikri (2010) Local Area Network (LAN) merupakan jarinan yang terbentuk dari gabungan beberapa komputer yang tersambung melalui saluran fisik (kabel). Wireless LAN (WLAN) itu sendiri berarti jaringan LAN tanpa kabel. Teknologi ini muncul seiring dengan perkembangan serta kebutuhan untuk akses jaringan yang bergerak (mobile) dan tidak membutuhkan kabel sebagai media transmisinya.

b. WEP

Menurut Bayu (2011) Wep merupakan standar keamanan dan enkripsi pertama yang digunakan pada wireless. WEP *(Wired Equivalent Privacy)* adalah suatu metode pengamanan jaringan nirkabel, disebut juga dengan *Shared Key Authentication. Shared Key Authentication* adalah metode otentikasi yang dibutuhkan untuk penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan oleh administrator ke klien maupun *access point* dan WEP mempunyai standar 802.11b.

e-ISSN 2338-5197

c. WPA

Menurut Bayu (2011) merupakan rahasia umum jika WEP *(Wired Equivalent Privacy)* tidak lagi mampu diandalkan untuk menyediakan koneksi nirkabel *(wireless)* yang aman. Menyikapi kelemahan yang dimiliki oleh WEP, telah dikembangkan sebuah teknik pengamanan baru yang disebut sebagai WPA *(WiFi Protected Access).* Teknik WPA adalah model kompatibel dengan spesifikasi standar draf IEEE 802.11i. Teknik ini mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, interoperasi, mampu digunakan untuk menggantikan WEP, dapat diimplementasikan pada pengguna rumahan atau *corporate* dan tersedia untuk publik.

3. Metode Penelitian

a. Subyek Penelitian

Dalam penelitian ini yang menjadi subyek penelitian adalah : Analisis perbandingan metode keamanan wireless WEP 128bit dan WPA yang diharapkan menghasilkan solusi mitigasi yang dapat meningkatkan keamanan wireless.

b. Metode Pengumpulan Data

Metode pengumpulan data merupakan suatu metode atau cara untuk mendapatkan data-data yang dibutuhkan dalam menyelesaikan penelitian ini. Adapun metode yang digunakan adalah:

a. Metode Literatur

Metode pengumpulan data yang digunakan adalah metode studi literatur yang sebagian besar berasal dari artikel-artikel di internet, jurnal-jurnal ilmiah, *e-book*, dan buku-buku teks. Semua literatur tersebut berhubungan dengan tema-tema seputar jaringan *wireless.*

b. Metode Observasi

Observasi dilakukan dengan pengamatan secara langsung ke lokasi dengan mencatat data yang dibutuhkan, sehingga diperoleh data yang sistematis untuk dijadikan informasi.

c. Metode Wawancara

Metode wawancara merupakan salah satu metode pengumpulan data yang umum digunakan untuk mendapatkan data berupa keterangan lisan dari administrator dan staff IT sebagai narasumber.

4. Hasil Dan Pembahasan

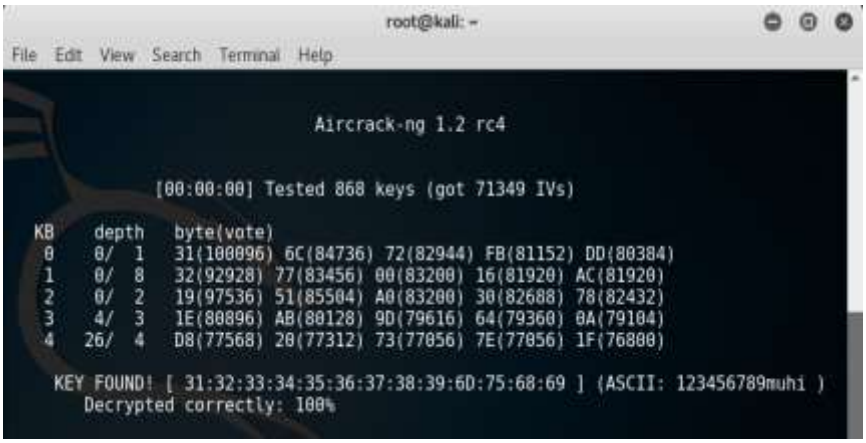
a. Implementasi

Pada tahap implementasi meliputi hacking WEP dan WPA, mempersiapkan komputer dan alat pendukung yang digunakan untuk melakukan penelitian.

Hacking WEP

Implementasi *hacking wireless* WEP *(Wired Equivalent Privacy)* ini dibagi menjadi tiga tahapan, tahapan pertama adalah melakukan analisa *wireless*, tahapan kedua adalah melakukan *capture* paket data dan tahapan terakhir adalah mendeskripsi *key* dari paket data yang direkam. Implementasi *hacking* WEP ini menggunakan *tools aircrack-ng. Aircrack-ng* sendiri adalah sebuah *tools* pengembalian *key* atau dekripsi *key* dari sebuah paket data yang telah terekan dan sudah tersimpan pada *wordlist.* Hasil deskripsi *key* menggunakan *aircrack-ng* dapat dilihat pada gambar 1.

 e-ISSN 2338-5197

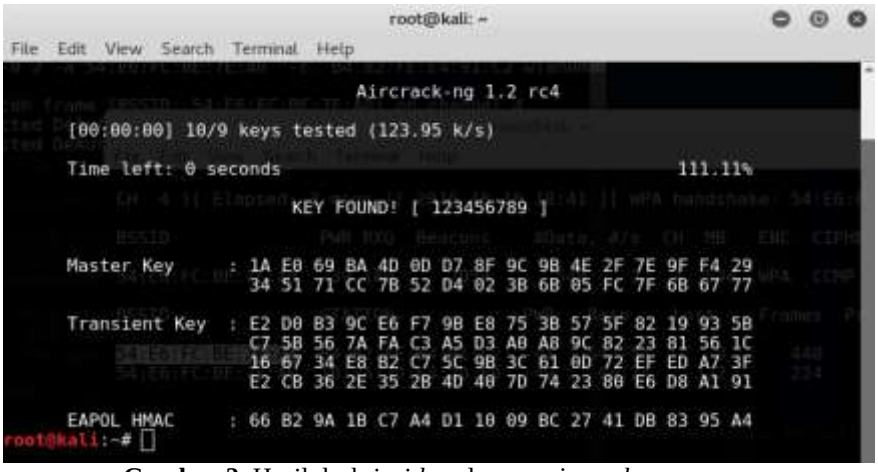


Gambar 1. Hasil deskripsi *key* dengan *aircrack-ng*

Pada gambar 1 terlihat ditemukan sebuah *key* yaitu : 31:32:33:34:35:36:37:38:39:6D:75:68:69, yang dalam ASCII *password* dari ESSID MUHI adalah 123456789muhi. Waktu yang dibutuhkan untuk melakukan *cracking* WEP adalah sekitar 20 menit.

Hacking WPA

Implementasi *hacking* WPA mempunyai tahapan yang hampir sama seperti *hacking* WEP, perbedaannya WPA men-*capture* WPA *Handshake* bukan IVs seperti ketika mengaudit WEP. WPA *Handshake* adalah sekumpulan *file* hasil dari tangkapan pada lalu lintas jaringan pada *access point* (AP) tertentu yang dijadikan sebagai target. *Hacking* WPA dibagi menjadi tiga tahapan, tahap pertama melakukan analisa *wireless*, tahap kedua adalah melakukan *capture* data dan tahapan terakhir adalah melakukan deskripsi *key*. Deskripsi *key PSK* dengan menggunakan *aircrack-ng* dapat dilihat pada gambar 2.



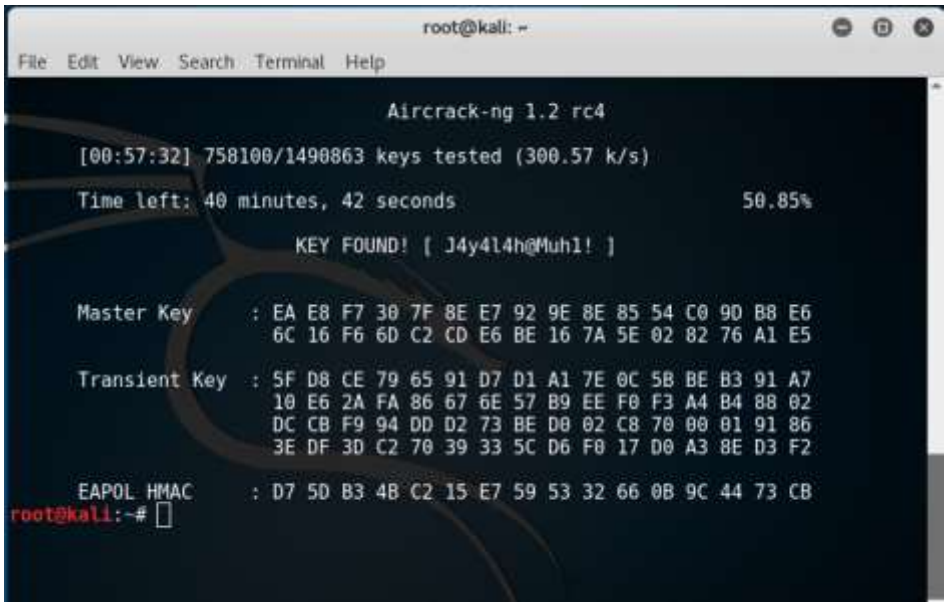
Gambar 2. Hasil deskripsi *key* dengan *aircrack-ng*

Pada gambar 2 di atas terlihat ditemukan sebuah *key* yaitu 123456789, yang merupakan *password* dari ESSID MUHI. Waktu yang dibutuhkan untuk melakukan cracking WPA adalah sekitar 1 jam atau bisa lebih karena cracking WPA ini sangat bergantung pada ketepatan *dictionary* dan *wordlist*.

4.2 Perbandingan Waktu Deskripsi *Password*

Pengujian *password* ini dilakukan dengan membandingkan beberapa *password* dengan menggunakan *tool* penetrasi *hacking Bactrack OS* atau *Kali Linux* dengan metode *brute force* sebagai solusi keamanan *wireless*. Perbandingan *password* ini berdasarkan waktu yang dibutuhkan untuk membobol *password* tersebut. Deskripsi *password* seperti terlihat pada gambar 3.

e-ISSN 2338-5197



Gambar 3. Hasil deskripsi *key* dengan *aircrack-ng*

Pada gambar 3 di atas terlihat ditemukan *password* J4y4l4h@Muh1!, dengan waktu yang dibutuhkan untuk deskripsi *key* adalah 1 jam. Deskripsi *key* ini dilakukan dengan membandingkan waktu yang dibutuhkan. Hasil dari perbandingan *password* terlihat pada tabel 1.

Tabel 1. Perbandingan waktu deskripsi *key*

No.	*Password*	Waktu
1	1234566789	5 menit
2	123456789muhi	10 menit
3	J4y4l4hMuh1	30menit
4	J4y4l4h@Muh1!	1 jam
5	*J4y4l4h@Muh1!*	5 jam

Pada tabel 1 di atas terlihat bahwa deskripsi *key* dengan *password* yang semakin rumit dibutuhkan waktu yang lebih lama. *Password* yang aman adalah *password* yang menggunakan kombinasi huruf besar, huruf kecil, angka dan simbol atau karakter.

5. Kesimpulan

Berdasarkan penelitian yang dilakukan dengan melakukan penetrasi hacking pada kedua metode tersebut metode kemanan WPA memiliki tingkat kemananan yang lebih baik daripada metode WEP. Berdasarkan data yang diperoleh dari perbandingan waktu deskripsi password yang dilakukan dapat memberikan solusi (mitigasi) bagi administrator untuk mengatasi masalah kemanan jaringan *wireless.*

Daftar Pustaka

Deris Stiawan Dian Palupi Rini. 2009. *Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS pada Jaringan Wireless Publik Hotspot*. Fakultas Ilmu Komputer Uneversitas Sriwijaya, Palembang.

Desmon, Sharon dkk. 2014. *Membangun Jaringan Wireless Locl Area Network (WLAN) Pada CV.BIQ Bengkulu.* Teknik Komputer Universitas Dehasen, Bengkulu.

Gilang dkk. 2016**.** *Analisa Keamanan Jaringan Wireless Di Sekolah Menengah Al Firdaus***.** Teknik Informatika Universitas Muhammadiyah Surakarta.

e-ISSN 2338-5197

Herdiana, Yudi. 2014. *Keamanan Pada Jaringan Wireless.* Teknik Informatika Universitas Bale, Bandung.

Imam Cartealy. 2013. *Linux Networking.* Jakarta: Jasakom.

Lfikri. 2010. Sejarah dan Perkembangan Wireless LAN. http://lfikri.wordpress.com/2010/04/09/sejarah-dan-perkembangan-teknologi-wireless/ (diakses pada 24 November 2013, pukul 00.38).

Mentang, Randy dkk. 2015. *Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System.* Teknik Elektro UNSRAT, Manado.

Micro, Andi. 2011. *Dasar-Dasar Jaringan Komputer.* Yogyakarta: ClearOS Indonesia.

Rico. 2014. *Analisis Celah Lapisan Keamanan Pada Jaringan Nirkabel.* Teknik Informatika STIKOM Dinamika Bangsa.

Santi Dwi Ratnasari dan Dwi Safiroh Utsalina. 2017. *Implementasi Penanganan Serangan Mac-Clone Pada Hotspot Mikrotik Di STIMIK Pradnya Paramita Malang.* Teknik Informatika STMIK Pradnya Paramita, Malang.

Sembiring, Irwan dkk. 2009. *Analisa dan Implementasi Sistem Keamanan Jaringan Komputer dengan Iptables sebagai Firewall Menggunakan Metode Port Knocking*. Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Salatiga.

Sebtian, Bayu. 2011. Keamanan Wireless LAN dengan WEP, WPA, dan WPA2. http://bayuneuer.blogspot.com/2011/01/cara-mengkonfigurasi-access-point.html (diakses pada 26 November 2013, 12.37).

Supriyanto, Aji. 2006. *Analisis Kelemahan Keamanan pada Jaringan Wireless.* Teknologi Informasi FTI Universitas Stikubank, Semarang.

Surahmat, dkk. 2014. *Analisis Keamanan Sistem WPA Radius.* Teknik Informatika Universitas Bina Darma, Palembang.

Wagito. 2007. *Jaringan Komputer: Teori dan implementasi Berbasis Linux.* Yogyakarta. Gava Media