p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

ANALISIS KEAMANAN WIRELESS LAN PADA JARINGAN DENGAN AUTENTIKASI CAPTIVE PORTAL

Fitra Nugraha, M.Kom[1)]

[1)] *Teknik Informatika Universitas Kuningan*
Jl Cut Nyak Dien No 36 A Cijoho Kabupaten Kuningan
Email : fitra@uniku.ac.id[1)]

Abstrak

Penelitian ini membahas tentang analisis keamanan Wireless LAN (Wireless Local Area Network) terhadap serangan luar pada protokol Wireless Protected Access (WPA), Web Proxy, dan Virtual Private Network (VPN), yang digunakan untuk menyerang LAN.
Penelitian akan dilakukan di Jaringan UNIKUNET (Jaringan Wireless Universitas Kuningan Kampus 1) yang menggunakan captive portal sebagai media autentikasi jaringan public hotspotnya. Tiga jenis perangkat lunak yang digunakan sebagai penyerang yaitu, penyerang Visual Network Stumbler, Aircrack dan Wireshark. Perangkat lunak tersebut digunakan di laptop pada jarak 5m sampai 25m dari titik akses LAN Nirkabel. Dari hasil experimen terlihat waktu tercepat direspon oleh Protokol WPA diberikan oleh penyerang Visual Network Stumbler, diikuti oleh Aircrack dan Wireshark, dan kemungkinan celah keamanan yang didapat.
Kata kunci: *Wireless Protected Access, Captive Portal, WLAN, Web Proxy* dan *Virtual Private Network*

Abstract

This study discusses the analysis of Wireless LAN (Wireless Local Area Network) security against external attacks on the Wireless Protected Access (WPA), Web Proxy, and Virtual Private Network (VPN) protocols, which are used to attack LANs.
The research will be conducted at the UNIKUNET Network (Kuningan University Campus Wireless Network 1) that uses captive portal as a media authentication for its public hotspot network. Three types of software are used as attackers, namely, attackers Visual Network Stumbler, Aircrack and Wireshark. The software is used on laptops at a distance of 5m to 25m from the Wireless LAN access point. From the experimental results, it was seen that the fastest time was responded to by the WPA Protocol provided by Visual Network Stumbler attackers, followed by Aircrack and Wireshark, and possible security gaps were obtained.
Keywords: Wireless Protected Access, Captive Portal, WLAN, Web Proxy and Virtual Private Network

1. PENDAHULUAN

Perkembangan teknologi komunikasi ini juga didukung dengan semakin mening-katnya kemajuan infrastruktur dan teknologi. Salah satu perkembangan teknologi komunikasi dan informasi ini adalah komu-nikasi menggunakan wireless. Ini ditandai keuntungan dari shared data dan shared resources. Dengan *Wireless Local Area Network* (Wireless LAN) pengguna dapat mengakses informasi tanpa mencari tempat untuk *plug in* dan dapat men*set-up* jaringan tanpa menarik kabel. *Wireless* LAN dapat mengatasi masalah kekurangan wired network, karena mempunyai kelebihan dibandingkan antara lain sebagai berikut: *Mobility*, *Scalability*, *Installation Speed and Simplicity*, *Installation Fleksibility*, *Reduced cost of ownership*. Teknologi informasi bukan Teknologi *wireless* yang menghasilkan berbagai kemudahan juga membawa dampak bagi para pengguna jasa internet baik industri, pendidikan dan user mandiri. Perkembangan ini juga dapat dirasakan secara langsung oleh kita dengan banyaknya *wireless hotspot* yang tersedia

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

dimana - mana. Selain dapat membantu serta melahirkan berbagai inovasi yang positif tetapi juga melahirkan sisi negative, dan ini selalu terjadi tidak terkecuali pada perkembangan *wireless*.

Untuk membatasi permasalahan yang meluas, maka permalahan yang akan dibahas dalam penelitian ini dibatasi pada infrastruktur protokol keamanan Wireless LAN yang berbasis Captive Portal. Analisis dilakukan melalui beberapa kajian white paper dan wacana yang ada serta melakukan eksperimen dengan melakukan serangan (attack) terhadap infrastruktur Wireless LAN. Protokol keamanan Wireless LAN yang digunakan dalam penelitian yaitu Wireless Protected Access (WPA), Web Proxy, dan Virtual Private Network (VPN). Dengan menggunakan 3 tools attacker yaitu Network Stumbler, Aircrack, dan Wireshark.

Serangan *Wireless LAN*

Jaringan *wireless* sangatlah rentan terhadap serangan, hal ini dikarenakan jaringan *wireless* tidak dapat dibatasi oleh sebuah gedung seperti yang diterapkan pada jaringan berbasis kabel. Sinyal radio yang dipancarkan oleh perangkat *wireless* dalam melakukan proses transmisi data didalam sebuah jaringan dapat dengan mudah diterima/ditangkap oleh pengguna komputer lain selain pengguna dalam satu jaringan hanya dengan menggunakan perangkat yang kompatibel dengan jaringan *wireless* seperti kartu jaringan *wireless*.

Wireless Protected Access (WPA) ditawarkan sebagai solusi keamanan yang lebih baik daripada WEP. WPA merupakan bagian dari standar yang dikembangkan oleh *Robust Security Network* (RSN). WPA dirancang untuk dapat berjalan dengan beberapa sistem perangkat keras yang ada saat ini, namun dibutuhkan dukungan peningkatan kemampuan perangkat lunak (*software upgrade*).

Pada perkembangan selanjutnya, dimana algoritma RC4 digantikan oleh algoritma enkripsi baru yaitu *Advance Encryption System* (AES) dengan panjang kunci sepanjang 256 bit. Dukungan peningkatan keamanan *Wireless LAN* yang disediakan WPA adalah meliputi Otentikasi dan Kendali Akses, Enkripsi dan Integritas Data. Standar tersebut ternyata masih mem-punyai banyak titik kelemahan dalam keamanan, karena itulah dikembangkan pembagian lapisan keamanan yang sudah ada menjadi tiga yaitu:

1. Lapisan *Wireless LAN, a*dalah lapisan yang berhubungan dengan proses transmisi data termasuk juga untuk melakukan enkripsi dan deskripsi.
2. Lapisan Otentikasi, adalah lapisan dimana terjadi proses pengambilan keputusan mengenai pemberian otentikasi kepada pengguna berdasarkan informasi identitas yang diberikan. Dengan kata lain adalah untuk membuktikan apakah identitas yang diberikan sudah benar.
3. Lapisan Kendali Akses, adalah lapisan tengah yang mengatur pemberian akses kepada pengguna berdasarkan informasi dari lapisan otentikasi.

Otentikasi dan Kendali Akses dalam WPA

Otentikasi yang didukung oleh WPA adalah otentikasi dengan menggunakan *preshared key* dan otentikasi dengan meng-gunakan *server based key*. Otentikasi dengan *preshared key* adalah model otentikasi dengan menggunakan WEP [2]. Sedangkan otentifikasi dengan *server based key* adalah model otentifikasi dengan menggunakan akses kontrol.

WPA mendefinisikan dua macam kunci rahasia, yaitu *pairwise key* dan *group key*. *Pairwiseway* adalah kunci yang digunakan antara *wireless user* dengan *access point*, Kunci ini hanya dapat digunakan dalam transmisi data di antara kedua belah pihak tersebut (*unicast*). *Pairwise key* maupun *group key* mempunyai manajemen kunci tersendiri yang disebut dengan *pairwise key hierarchy* dan *group key hierarchy*

Enkripsi dalam WPA

WPA menggunakan protokol enkripsi yang disebut dengan *Temporary Key Integrity Protocol* (TKIP). TKIP mendukung pengubahan kunci (*rekeying*) untuk *pairwise key* dan *group key*. Fitur-fitur keamanan yang disediakan oleh TKIP adalah:

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

1. Penambahan besar ukuran *initialization vector* untuk mencegah terjadinya pengulangan nilai *initialization vector*.
2. Pengubahan cara pemilihan *initialization vector* untuk mencegah terjadinya *weak key*, juga mencegah terjadinya kemungkinan *replay attack*.Pengubahan kunci enkripsi untuk setiap paket yang dikirimkan (*per packet key mixing*).
3. Penggunaan *message integrity protocol* yang lebih baik untuk mencegah terjadinya modifikasi pesan.
4. Penggunaan mekanisme untuk melakukan distribusi maupun perubahan terhadap kunci rahasia yang digunakan.

2. METODE PENELITIAN

Penelitian difokuskan kepada bagaimana menformulasikan permasalahan yang ada dan diidentifikasi dan dirumuskan berdasarkan aspek keamanan protokol *Wireless* LAN. Kemudian menyusun suatu hipotesa sebagai jawaban atau kesimpulan awal dan strategi untuk menguji apakah hipotesa tersebut merupakan jawaban atas permasalahan yang ada.

Tahapan

Dalam penelitian ini penulis menggunakan beberapa tahapan yang diawali dengan :

1. Membuat suatu perancangan dengan menggunakan topologi infrastruktural dengan 5 (lima) wireless user yang dihubungkan dengan 1 (satu) *server* melalui 1 (satu) *access point* dan 1 (satu) penyerang.
2. Melakukan percobaan serangan terhadap infrastruktur *Wireless LAN* dengan menggunakan protokol keamanan WPA, *Web Proxy* dan *Virtual Private Network* dengan perbedaan jarak antara penyerang dan *access point* dengan kekuatan signal yang berbeda yaitu dengan posisi jarak 5 meter, 10 meter, 15 meter, 20 meter, 25 meter.

Analisis Data

Data dianalisis dengan menggunakan beberapa tahapan pengujian sebagai berikut: 1. Mengidentifikasikan atau memonitor konfigurasi keberadaan *hotspot* dengan menggunakan *software Network Stumbler 0.4.0.*

1. Kemudian berhubungan dengan membuka *wireless network connection.*
2. Berusaha memecahkan *password* pada *access point* yang digunakan meng-gunakan *software Aircrack-ng-0.9.3-win* .
3. Serangan tersebut diukur data yang dikirim, data yang diterima dan data yang hilang menggunakan *software Network Stumbler 0.4.0* .

Uji coba serangan pemanipulasian *IP address* dilakukan dengan 2 metoda pengujian :

***Metode 1* :**

1. Melakukan koneksi berdasarkan informasi *MAC Address* dan Mendapatkan *IP Address* lalu membuka *session* koneksi *Wireless* dengan melakukan *login ke Web Proxy* dan terhubung dengan *server.*

- Melakukan penyadapan paket untuk mendapatkan *MAC Address* yang sah dengan menggunakan *software Network Stumbler* serta memalsukan *MAC Address* miliknya dan melakukan koneksi dengan *access point* berdasarkan *MAC address* yang dipalsukan.

***Metode 2* :**

1. Melakukan koneksi dengan *access point* berdasarkan *MAC Address* yang dipalsukan dan mendapatkan *IP Address* dan koneksi *Wireless LAN* dibuka dengan melakukan *login* ke *Web Proxy.*
2. Melakukan koneksi dengan *access point* berdasarkan *MAC address* yang dipalsukan dan mendapatkan *IP Address* dan tidak dapat membuka *session* koneksi *Wireless LAN* saat *login* ke *Web Proxy.*

Hasil yang diharapkan pada sisi penyerang

Serangan berhasil jika *IP Address* dari *wireless user* dan penyerang berbeda (yang didapat dari *server*) dan Serangan gagal jika *IP Address* dari *wireless user* dan penyerang sama (yang didapat dari *server*). Jika serangan gagal maka dilakukan konfigurasi *IP Address* secara

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

manual pada salah satu *device* supaya mendapatkan *IP Address* berbeda.

3. HASIL DAN PEMBAHASAN

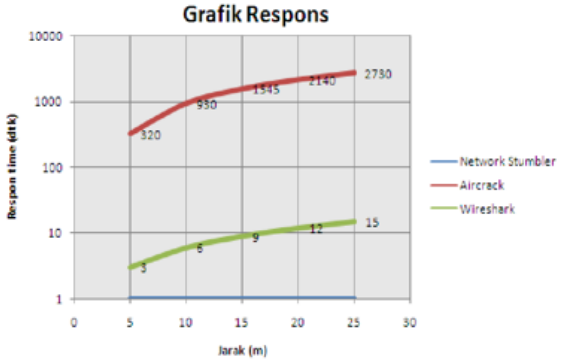
Dalam merancang model keamanan, aset jaringan yang beresiko perlu diperhatikan seperti titik kelemahan dalam sistem keamanannya, atau gangguan yang datang dari sipenyerang, serta motivasi serangan tersebut untuk masing-masing potensi kelemahan yang ada. Mengenai hal tersebut sangat diperlukan untuk mengambil suatu tindakan perlindungan keamanan yang dibutuhkan.

Hasil Analisis dengan Protokol WPA

Dengan Protokol WPA dapat mengatasi kelemahan pada integritas data dan ketersediaan pada sistem. Dan penulis mencoba melakukan percobaan untuk membuktikan kelemahan protokol WPA jika diterapkan pada *Wireless LAN*, yaitu dengan melakukan serangan terhadap *encryption* (*Network Key* atau *password*) yang digunakan oleh *access point*

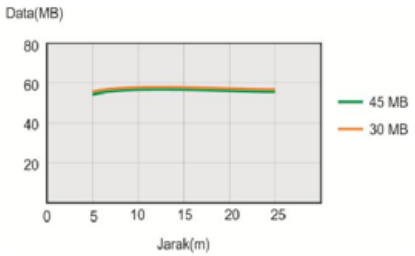
Tabel 1. Hasil Percobaan Serangan terhadap Protokol WPA

Jarak (m)	Network Stumbler	Aircrack	Wireshark
	Respon time rata2 (detik)	Respon time rata2 (detik)	Respon time rata2 (detik)
5	0	320	3
10	0	930	6
15	0	1545	9
20	0	2140	12
25	0	2730	15

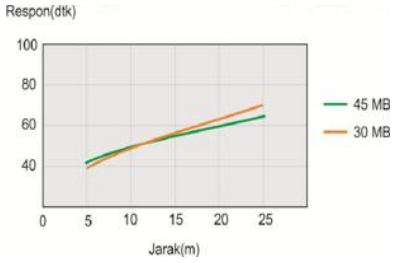


Gambar 1. Grafik Respons Time terhadap Protokol WPA.

Dari grafik Respons Time terlihat bahwa Network Stumbler yang paling cepat mendeteksi sistem keamanannya sedangkan Aircrack yang paling lambat. Kemudian juga melakukan serangan terhadap peng-ambilan data yang dikirimkan oleh *wireless user* dengan meng-gunakan proto-kol WPA ke *server*. Dan hasilnya bisa dengan mudah terkoneksi dengan *access point*. Dan juga dapat melakukan pengambilan data sehingga data yang diterima mengalami masalah seperti dijelaskan pada gambar 2 dan gambar 3.

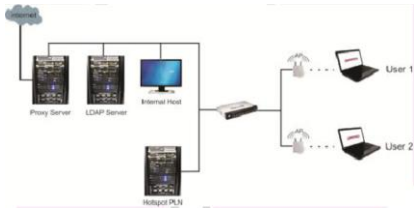


Gambar 2. Jumlah Paket Data yang Diterima.



Gambar 3. Respon Time Data yang diterima di Server.

Hasil Analisis Dengan Keamanan *Web Proxy*



Gambar 4. Arsitektur Wireless LAN

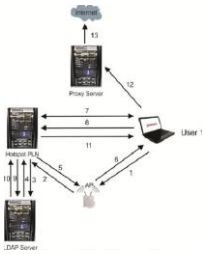
Dari gambar tersebut arsitektur *Wireless LAN* dan jaringan kabel merupakan bagian dari jaringan terintegrasi. Akses kontrol terhadap *device* yang ingin melakukan koneksi dilakukan dengan menggunakan *MAC Address* dari pengguna yang disimpan dalam *server* LDAP (*Lightweight Direction Access Protocol*). Proses

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

otentikasi ke dalam jaringan dilakukan dengan melalui *Web Proxy* yang menggunakan protokol *Secure Socket Layer* (SSL). SSL adalah protokol keamanan yang bekerja di atas lapisan ke 4 (empat) OSI (*transport layer*), dimana semua data-data yang melalui protokol ini akan dienkripsi. Setelah pengguna terotentikasi, maka pengguna akan mendapatkan hak akses kedalam jaringan kabel internal dan ke internal (dengan menggunakan *proxy server*). Pengguna *Wireless LAN* menggunakan *Web Proxy* dengan protokol SSL dalam proses otentifikasi, memberikan perlindungan keamanan terhadap pencurian informasi *wireless username* dan *password* karena data-data tersebut ditransmisikan dalam bentuk terenkripsi. Proses koneksi *wireless user* dapat dilihat pada Gambar 5.

Proses koneksi Wireless yang terjadi adalah sebagai berikut :

1. Wireless user melakukan proses koneksi dengan access point dengan menggunakan open system authentication (tanpa menggunakan WEP).
2. Access point melakukan akses kontrol terhadap permintaaan koneksi dari wireless user dengan melakukan query ke hotspot berdasarkan informasi MAC Address yang dimiliki oleh wireless user.
3. Query yang diterima oleh hotspot diteruskan ke server untuk mendapatkan informasi apakah MAC Address dari wireless user merupakan device yang sudah terdaftar.
4. Server memberikan konfirmasi apakah MAC Address terdapat didalam database atau tidak.
5. *Hotspot* tersebut menerima informasi dari *server* dan kemudian memberikan konfirmasi proses asosiasi diterima atau tidak berdasarkan informasi tersebut, yaitu apabila *MAC Address* sudah terdaftar maka proses asosiasi diterima dan demikian sebaliknya.
6. Access point memberikan konfirmasi ke wireless user bahwa proses asosiasi telah berhasil dilakukan atau tidak.
7. Apabila proses asosiasi berhasil, akan dilakukan proses-proses berikutnya (pro-ses ke tujuh dan seterusnya).
8. Setelah wireless user mendapatkan sebuah IP address, diperlukan suatu pro-ses otentifikasi untuk memastikan bahwa wireless user merupakan pengguna yang memang mempunyai hak akses. Untuk itu, wireless user harus memasukan informasi berupa wireless username dan password melalui Web Proxy yang menggunakan protokol SSL. Dimana data-data yang ditrasnsmisikan akan dienkripsi sehingga mencegah kemung-kinan penyerang dapat mengetahui identitas rahasia dari wireless user.
9. Server memberikan respon apakah proses otentifikasi diterima atau tidak dengan memeriksakan apakah kombinasi wireless username dan pasword terdapat dalam direktori database.

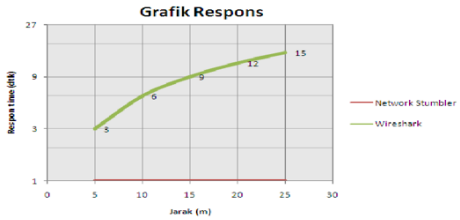


Gambar 5. Proses Koneksi Wireless LAN

Protokol - protokol tersebut menyediakan otentifikasi, enkripsi dan integritas daya yang tangguh. Protokol yang lain terdapat dilapisan atas (*application layer*) seperti HTTP, FTP dan *telnet* bukan merupakan protokol yang aman karena semua data yang ditransmisikan merupakan *text* biasa. Implementasi jaringan *Wireless LAN* dilingkungan Universitas Kuningan tidak menggunakan keamanan lapisan *data link layer* (seperti WEP dan WPA), karena itu transmisi data dari protokol yang "tidak aman" tersebut tetap ditransmisikan dalam bentuk *text* biasa (*clear text*). Hal ini berarti titik kelemahan dalam keamanan yang dapat dimanfaatkan penyerang untuk menyadap transmisi data tersebut dan men-coba untuk melakukan serangan terhadap

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

otentifikasi dan akses kontrol dari sistem *WebProxy* di jaringan Universitas Kuningan. Serangan dilakukan adalah *session hijacking*, yaitu serangan yang dilakukan untuk mencuri *session* dari seorang *wireless user* yang sudah ter-otentifikasi dengan *access point*.



Gambar 6. Grafik Respons Time terhadap Protokol *Web Proxy*.

Dari grafik Respons Time terlihat bahwa Network Stumbler yang paling cepat mendeteksi sistem keamanannya sedangkan Wireshark yang paling lambat.

Serangan pada *Virtual Private Network*

Melakukan percobaan serangan terhadap *hotspot* yang menggunakan keamanan ***Virtual Private Network*** dengan berusaha memecahkan *wireless username dan password* dengan jarak yang berbeda dan percobaan untuk mencari *session* koneksi. Dari percobaan yang dilakukan meng-gunakan *software aircrack* penulis hanya dapat mengidentifikasikan atau memonitor kon-figurasi keberadaan *hotspot* tanpa bias memecahkan *wireless username* dan *password* yang dimiliki *wireless user* asli (Gambar 4.8). Penulis juga hanya bisa mengetahui *IP Address wireless user* asli tanpa bisa merubah *IP Address wireless user* asli.

4. KESIMPULAN

Dari hasil penelitian dan percobaan pada Wireless LAN dapat disimpulkan sebagai berikut :

1. Penggunaan keamanan dengan protokol WPA, Web Proxy dan Virtual Private Network (VPN) kurang memberikan perlindungan keamanan dari Network Stumbler.
2. Penggunaan protokol dengan WPA maka respon time rata-rata untuk Network Stumbler lebih cepat dari Wireshark sedangkan Aircrack respon time rata-rata 45 menit untuk jarak 25 m.
3. Penggunaan protokol dengan Web Proxy maka respon time rata-rata untuk Network Stumbler lebih cepat dari Wireshark sedangkan Aircrack tidak berhasil.
4. Penggunaan protokol dengan VPN maka respon time rata-rata untuk Network Stumbler lebih cepat sedangkan respon time rata-rata Wireshark dan Aircrack tidak berhasil.

5. SARAN

Sesuai dengan permasalahan yang ada, maka diberikan beberapa saran yang dapat digunakan dalam penanganan masalah di masa mendatang.

Saran dari kegiatan penelitian ini adalah sebagai berikut:

1. Sistem keamanan dengan menggunakan Protokol VPN lebih baik dibandingkan dengan menggunakan Protokol Web Proxy atau WPA.
2. Untuk kegiatan penelitian selanjutnya, penulis menyarankan untuk melakukan penelitian protokol lain terhadap Network Stumbler.

Daftar Pustaka

[Arbough, 2001] Arbough, William A, Narendar Shankar and Y.C Justine Wan, 2001. Your 802.11 Wireless Network Has No Clothes. Departemen of Computer Science University of Maryland. 22 September 2004

[Glendinning, 2003] Glendinning, Ducan. 2003. 802.11 Security. Intel Corporation. 5 Oktober 2004 http://www.intel.com/idf/us/fall2003/presentations/ FO3USMOB169_OS.Pdf

[Stallings, 2003] Stallings, William. 2003. Cryptography and Network Security. New Jersey: Prentice Hall.

p-ISSN : 2527-4856, e-ISSN : 2614-5413
https://journal.uniku.ac.id/index.php/buffer

Lasa, H. S., 2009. Kamus Kepustakawanan Indonesia. Yogyakarta: Pustaka Book Publisher.

LIPI, 2005. Jurnal Online. [Online] Available at: http://www.jurnal.lipi.go.id/ [Accessed 30/03/2014].

Biodata Penulis

Fitra Nugraha, M.Kom, memperoleh gelar sarjana di Universitas Kuningan (S.Kom) Jurusan Sistem Informasi pada tahun 2011. Dan memperoleh gelar Magister Komputer (M.Kom) dari Universitas Budi Luhur Jakarta pada tahun 2015. Saat ini menjadi Dosen di Universitas Kuningan Jawa Barat. Jurusan Teknik Informatika Fakultas Ilmu Komputer di Universitas Kuningan.