KEAMANAN JARINGAN WLAN TERHADAP SERANGAN *WIRELESS HACKING* PADA DINAS KOMUNIKASI & INFORMATIKA DIY

Mochamad Gilang Hari Wibowo[1], Joko Triyono[2], Edhy Sutanta[3]
[1,2,3] Jurusan Teknik Informatika, FTI, IST AKPRIND Yogyakarta
Email: [1]gilangwibowo19@yahoo.com, [2]zainjack@akprind.ac.id, [3]edhy_sst@yahoo.com

ABSTRAK

Media wireless merupakan salah satu fasilitas penunjang pekerjaan yang penting di Kantor Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta (Dinas Kominfo DIY). Media wireless tersebut memanfaatkan gelombang radio sehingga rentan terhadap ancaman serangan, sehingga perlu diuji keamanannya. Pengujian dilakukan berdasarkan konsep wireless hacking, meliputi ARP spoofing, cracking WPA/WPA keys, bypassing MAC address, dan serangan WPS aktif. Software pendukung yang digunakan adalah Aircrack-ng, Dumper, Jumpstart, T-MAC, Netcut, dan Airodump-ng. Hasil pengujian pada delapan jaringan WLAN *di Dinas Kominfo DIY menunjukkan bahwa sistem keamanan jaringan yang digunakan sudah aman, namun celah keamanan masih terjadi pada beberapa jaringan* WLAN*, pengguna yang sedang menggunakan jaringan* WLAN *masih bisa diserang oleh pengguna lain. Untuk meningkatkan keamanan jaringan* WLAN*, perlu diaktifkan fitur ARP atau binding pada access point atau router agar terhindar dari serangan spoofing seperti nmap, netcut, dan lain-lain.*

Keata kunci*: network security, wireless, wireless hacking.*

1. PENDAHULUAN

Keamanan jaringan WLAN merupakan hal penting yang perlu diketahui oleh pengelola jaringan, agar dapat diketahui tingkat keamanan jaringan yang disediakan. Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta (Dinas Kominfo DIY) merupakan salah satu lembaga dalam lingkungan Pemerintah DIY yang menerapkan jaringan komputer kabel dan WLAN sebagai media pertukaran data/informasi untuk pelayanan umum atau komersial, kepegawaian, dan lainnya. Penggunaan media WLAN tersebut rentan terhadap ancaman serangan karena menggunakan gelombang radio. Penelitian ini dilakukan untuk memperoleh hasil pengujian keamanan jaringan *wireless* pada Dinas Kominfo DIY, sehingga bisa digunakan sebagai masukan bagi pengelola dalam rangka menjaga dan/atau meningkatkan kualitas layanan koneksi jaringan WLAN yang disediakan.

2. KAJIAN LITERATUR

Penelitian [1] telah melakukan analisis keamanan jaringan pada fasilitas koneksi internet (WLAN) terhadap serangan *packet sniffing* dengan objek di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta. Pengujian dilakukan menggunakan aplikasi *netstumbler, insidder* dan *ettercap. Netstumbler* adalah *tools wireless hacking* untuk mendeteksi dan mengidentifikasi sinyal WLAN yang terbuka. *Insidder* adalah *software* alternatif yang fungsinya sama persis dengan *netstumbler*. *Ettercap* adalah *tools packet sniffer* untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. *Ettercap* memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri *password*, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Penelitian ini dilakukan dalam dua tahap, tahap pertama adalah mengidentifikasi keberadaan dan keamanan koneksi WLAN menggunakan *software insider*, dan tahap kedua melakukan serangan *packet sniffing* menggunakan *software ettercap* untuk pengujian keamanan koneksi WLAN. Penelitian tersebut berhasil mendeteksi adanya keamanan WLAN yang terbuka dan terekamnya *username* dan *password*. Kondisi tersebut dapat membahayakan keamanan lalu lintas data para pengguna jaringan WLAN

maupun LAN kabel khususnya para karyawan. Berdasarkan hasil tersebut, telah dilakukan upaya peningkatan keamanan untuk dapat mencegah/menangani serangan *packet sniffing*.

Penelitian [2] melakukan menganalisis sistem keamanan jaringan WEP *security* menggunakan *distro linux backtrack* di Puri Ayu Homestay. Dalam penelitiannya, peneliti menganalisis sistem keamanan yang digunakan pada jaringan internet agar tidak dicuri atau digunakan oleh orang-orang yang tidak berhak untuk melakukan koneksi. Hasil pengujian menunjukkan bahwa sistem keamanan jaringan mikrotik yang digunakan masih memiliki kelemahan. Berdasarkan hasil tersebut, sistem keamanan jaringan diperbaiki dengan menerapkan sistem keamanan jaringan yang terenkripsi WEP, sehingga data yang dikomunikasikan menjadi lebih aman, tidak mudah dicuri atau digunakan oleh pihak yang tidak bertanggung jawab.

Sebelumnya, [3] juga telah melakukan penelitian tentang analisis kelemahan keamanan pada jaringan WLAN. Dalam penelitian tersebut dilakukan pengujian untuk mengetahui kelemahan jaringan WLAN. Fokus penelitian adalah mengungkap kelemahan pada konfigurasi jaringan dan kelemahan pada jenis enkripsi yang digunakan. Hasil penelitian tersebut menunjukkan bahwa celah kelemahan pada jaringan WLAN dapat terjadi pada empat *layer* yang merupakan proses terjadinya komunikasi data pada media WLAN. Keempat *layer* tersebut adalah *physical*, *network*, *user*, dan *application*. Model penanganan keamanan untuk masing-masing *layer* pada teknologi WLAN dapat dilakukan antara lain dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasi fasilitas MAC *filtering*, dan pemasangan infrastruktur *captive* portal, sehingga koneksi jaringan WLAN menjadi lebih aman.

Jenis-jenis serangan yang dapat digunakan untuk melakukan pengujian keamanan pada jaringan WLAN adaah sebagai berikut [4]:

1. *ARP spoofing/ARP poisoning*.

ARP (Address Resolution Protocol) spoofing adalah satu teknik menyerang pada jaringan komputer lokal baik yang menggunakan media kabel atau WLAN. Teknik ini memungkinkan penyerang bisa mengendus *frames* data pada jaringan lokal dan/atau melakukan modifikasi *traffic* atau bahkan menghentikannya. *ARP spoofing* merupakan konsep dari serangan penyadapan di antara dua mesin yang sedang berkomunikasi atau disebut sebagai *MITM* (*Man in The Middle Attack)*. Prinsip serangan *ARP poisoning* adalah memanfaatkan kelemahan pada teknologi jaringan komputer yang menggunakan *ARP broadcast*. *ARP* berada pada *layer* 2, alamat pada *layer* 2 adalah *MAC address*. Sebagai contoh, *host* (PC) yang terhubung pada sebuah jaringan WLAN ingin menghubungi *host* lain pada jaringan WLAN tersebut, maka dia membutuhkan informasi *MAC address* dari *host* tujuan [5].

2. *Cracking WPA/WPA Keys*

WPA dan WPA2 merupakan protokol keamanan yang diciptakan untuk mengatasi permasalahan pada WEP. Penggunaan WPA dan WPA2 akan menyulitkan *hacker* dalam melakukan injeksi paket, mengirimkan paket yang diambil sebelumnya (*replay attack*), atau serangan lain yang mengancam WEP. *Hacking* terhadap jaringan yang menggunakan WPA atau WPA2 menjadi jauh lebih sulit dilakukan [4]**.** WPA dan WPA2 bisa dijalankan dengan dua modus yaitu personal menggunakan PSK (*pre shared key*) dan *enterprises* menggunakan *server* RADIUS. Kemungkinan *hacking* hanya bisa dilakukan pada WPA dan WPA2 PSK yang paling banyak digunakan oleh pengguna rumahan maupun perusahaan. WPA dan WPA2 PSK menggunakan *passphrase* yang harus diatur di setiap komputer seperti halnya WEP [4]. Berbeda dengan *hacking* WEP, metode yang digunakan untuk melakukan *hacking* terhadap WPA dan WPA2 tidak bisa menggunakan metode statistik. WPA dan WPA2 mempunyai IV (*initial vector*) yang berubah-ubah sehingga tidak ada gunanya mengumpulkan paket data sebanyak-banyaknya seperti pada WEP untuk melakukan mendapatkan *keys* yang digunakan [4]. *Hacking* dengan cara ini membutuhkan waktu yang sangat lama sehingga metode yang paling memungkinkan adalah *brute force* berdasarkan

dictionary file. *Brute force* membutuhkan sebuah file yang berisi *passphrase* yang akan dicoba satu persatu dengan paket *handshake* untuk mencari *keys* yang digunakan [4].

3. *Bypassing MAC Address*

Bypassing MAC address adalah proses mengubah identitas *MAC* untuk mengatasi *MAC address filtering. Attacker* dapat mengubah *MAC address* yang sesungguhnya agar bisa masuk ke dalam jaringan WLAN yang ingin diserang [4]. Serangan *Bypassing MAC address* bisa dilakukan menggunakan media transmisi kabel karena tidak adanya otentikasikeamanan pada jaringan internet yang menggunakan media transmisi kabel. Mengganti *MAC address* memungkinkan dilakukan pada sistem operasi *windows* karena *MAC address* telah dibaca pada NIC (*network interface card*) dan tersimpan pada basis data *windows registry* [6].

4. Menyerang WPS Aktif

WPS (*Wireless Protected Setup)* adalah program sertifikasi opsional yang dikembangkan oleh aliansi WiFi. WPS dirancang untuk memudahkan pengaturan keamanan WiFi di rumah dan kantor kecil. WPS berguna jika suatu saat pemilik jaringan WLAN mengalami lupa *password*, hanya dengan menekan tombol WPS maka pemilik jaringan tersebut dapat mengkoneksikan perangkatnya secara otomatis. Jenis serangan ini hanya bisa menyerang jaringan WLAN bertipe otentikasiWPA_PSK dan WPS_PSK, dan memiliki tipe enkripsi TKIP. Jaringan WLAN pada *smartphone* tidak bisa diserang dengan cara ini karena otentikasinya sudah menggunakan WPA2_PSK [7].

3. METODE PENELITIAN

Penelitian ini dilakukan dalam empat tahapan, yaitu;

a. Studi pendahuluan untuk mengetahui mekanisme pengujian keamanan jaringan WLAN.
b. Survei untuk memperoleh data jaringan WLAN yang tersedia, tipe keamanan yang digunakan, dan *acces point* atau *router* yang digunakan.
c. Pengujian keamanan jaringan WLAN menggunakan metode *penetration testing* dengan langkah sebagai berikut:
   - *Information gathering*, proses ini dilakukan untuk mengetahui informasi tentang jaringan WLAN yang ingin diuji. *Tools* yang digunakan adalah *insidder* dan *airmon-ng*.
   - Analisis awal, proses ini dilakukan untuk menentukan jenis tindakan dan kebutuhan pengujian dengan penetrasi. *Tools* yang digunakan adalah *insidder* dan *airmon-ng*.
   - *Attacking*, proses ini dilakukan untuk melakukan penetrasi jaringan dengan berbagai macam serangan. Tindakan a*ttacking* untuk penetrasi ke jaringan WLAN ditampilkan pada Tabel 1.
d. Analisis keamanan jaringan, hasil pengujian dianalisis untuk mengetahui tingkat keamanan jaringan pada objek penelitian, apabila ditemukan kelemahan maka dapat diberikan alternatif solusi yang relevan.

Tabel 1. *Attacking* jaringan WLAN

Pengujian	Batasan Serangan	Alat Bantu
Serangan pada WPS aktif	Serangan dilakukan pada jaringan WLAN yang aktif WPS-nya. Jaringan WLAN yang akan diserang bertipe WPA2_PSK dan bertipe enkripsi TKIP+AES.	Dumper, Jumpstart
Bypassing MAC address	Serangan dilakukan pada jaringan WLAN.	T-MAC
ARP Spoofing	Serangan attacker berada di tengah-tengah user yang menggunakan jaringan WLAN. Attacker menyerang user yang sedang terkoneksi ke jaringan WLAN.	Netcut
Cracking	Proses scanning dan capture data dilakukan maksimal 30 menit.	Airodump-ng, Aircrack-ng

Untuk pelaksanaan pengujian dalam penelitian ini digunakan perangkat keras dan perangkat lunak pendukung. Spesifikasi alat yang digunakan dalam penelitian adalah Laptop (*Processor core* i3 2,10 Ghz, Memori 2 GB) yang digunakan sebagai sarana melakukan pengujian dan analisa dan *access point* atau *router* yang digunakan untuk mendapatkan informasi tentang jaringan WLAN.

Perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Sistem operasi Kalilinux 2.0 dan Windows.
2. *Aircrack*, digunakan untuk melakukan *cracking* ke jaringan WLAN. *Software* ini bisa didapatkan dengan cara mengunduhnya di terminal linux dengan mengetikkan "*apt-get aircrack*".
3. *Airodump*, digunakan untuk melakukan penyusupan ke jaringan WLAN. *Software* ini bisa didapatkan dengan cara mengunduhnya di terminal *linux* dengan mengetikkan "*apt-get airodump-ng*".
4. *T-MAC* (*Technitium MAC address Changer*), digunakan untuk menyembunyikan *MAC address* asli dan menampilkan yang palsu.
5. *Netcut*, digunakan untuk menyerang pengguna lain dengan cara mematikan koneksi internet pada pengguna lain.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil survei lapangan, diketahui bahwa jaringan WLAN yang tersedia di Dinas Kominfo DIY ada 8 koneksi, yaitu Anila, Anjani, Arjuna, Bagong, Bregodo, Gareng, Kakrasana, dan Sambo. *Acces point* atau *router* yang digunakan memiliki tipe *acces point wireless router* dan *mikrotik*, sedangkan tipe keamanan jaringan yang digunakan adalah *WPA2-Pesonal*. Data koneksi jaringan WLAN yang tersedia di Dinas Kominfo DIY secara lebih terinci ditampilkan pada Tabel 2.

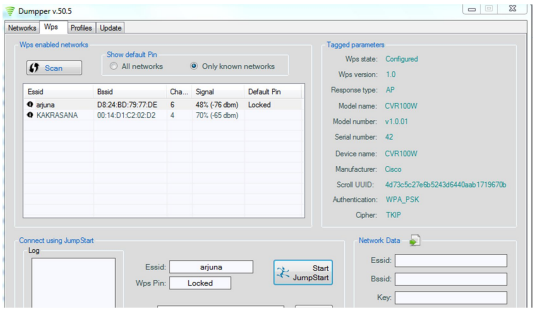
Pengujian serangan ke jaringan WLAN pada penelitian ini dilakukan dua tahap, pengujian pertama dilakukan sebelum dilakukan konfigurasi keamanan jaringan WLAN, sedangkan pengujian kedua dilakukan setelah dilakukan konfigurasi keamanan jaringan WLAN Kedua proses pengujian tersebut dilakukan pada delapan jaringan WLAN yang tersedia, yaitu Anila, Anjani, Arjuna, Bagong, Bregodo, Gareng, Kakrasana, dan Sambo. Pengujian dilakukan menggunakan serangan WPS aktif, *bypassing MAC address*, *ARP spoofing*, dan *cracking*. Pengujian serangan WPS aktif hanya dilakukan pada WLAN Arjuna dan Kakrasana, karena hanya kedua jaringan *wireless* tersebut yang memiliki fitur WPS yang aktif. Pengujian pada WLAN Arjuna dan Kakrasana masing-masing dilakukan 10 kali, dengan waktu rata-rata 47 detik pada Arjuna, dan 50,5 detik pada Kakrasana. Pengujian serangan *bypassing MAC address* dilakukan pada semua jaringan WLAN. Pengujian serangan *ARP spoofing* dilakukan pada empat jaringan *wireless* yaitu Anjani, Arjuna, Bregodo, dan Kakrasana.

Pengujian Serangan WPS Aktif

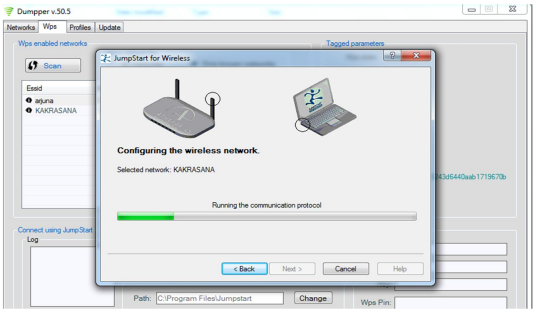
Pada pengujian ini dilakukan *scanning* WPS untuk mengetahui jaringan *wireless* WPS yang aktif. Proses tersebut ditampilkan pada Gambar 1. Jaringan *wireless* yang terdeteksi WPS aktif dapat dilakukan proses *jumpstart* untuk menyerang jaringan *wireless*. Proses tersebut ditampilkan pada Gambar 2.

Tabel 2. Koneksi jaringan WLAN di Dinas Kominfo DIY

Jaringan WLAN	Tipe keamanan	Jumlah Chanel	Max Rate	Vendor	Tipe Network	Pengelola
Anila	WPA2-Pesonal	1	54	Tidak diketahui	Infrastructure	Tidak diketahui
Anjani	WPA2-Pesonal	1	100	Tidak diketahui	Infrastructure	Tidak diketahui
Arjuna	WPA2-Pesonal	6	144	Cisco System	Infrastructure	Diskominfo DIY
Bagong	WPA2-Pesonal	1	54	Tidak diketahui	Infrastructure	Tidak diketahui
Bregodo	WPA2-Pesonal	1	144	Tidak diketahui	Infrastructure	Diskominfo DIY
Gareng	WPA2-Pesonal	5	450	Tidak diketahui	Infrastructure	Tidak diketahui
Kakrasana	WPA2-Pesonal	4	300	TRENDnet	Infrastructure	Diskominfo DIY
Sambo	WPA2-Pesonal	3	255	Tidak diketahui	Infrastructure	Tidak diketahui

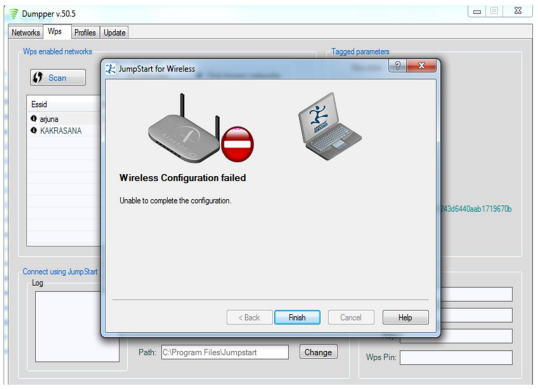


Gambar 1. Jaringan WLAN WPS yang aktif



Gambar 2. Proses *jumpstart* pada WLAN

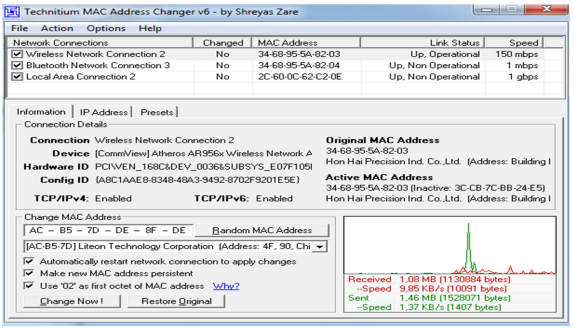
Keberhasilan akses ilegal ke jaringan *wireless* tersebut antara lain dipengaruhi oleh tingkat enkripsi pada *access point* dan stabilitas jaringan pada saat dilakukan penyerangan. Jaringan *wireless* akan bisa diserang menggunakan *dumper* dan *jumpstart* jika hanya memiliki tipe auntentifikasi WPA_PSK dan WPS_PSK dan tipe enkripsi TKIP. Tipe-tipe tersebut dijumpai pada *access point* atau *router* model lama, Sedangkan model baru memiliki tipe auntentifikasi minimal WPA2_PSK dan tipe enkripsi AES, sehingga sangat sulit diserang menggunakan *dumper* dan *jumpstart*. Kegagalan proses penyerangan tersebut dapat dilihat pada Gambar 3.



Gambar 3. *Jumpstart* gagal pada WLAN

Bypassing MAC Address

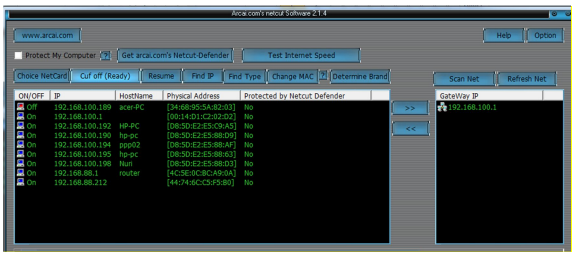
Pada pengujian ini dilakukan perubahan nilai *network address* pada *wireless adapter* menggunakan *MAC address* tujuan yang akan digunakan untuk mengakses jaringan WLAN. Pada pengujian ini penggunaan *MAC address* gagal terkoneksi ke jaringan WLAN, tidak bisa mengakses jaringan WLAN karena tidak mendapat *IP address* jaringan WLAN yang dituju, sehingga tidak terjadi komunikasi data. Proses tersebut ditampilkan pada Gambar 4.



Gambar 4. B*ypassing MAC address*

ARP Spoofing

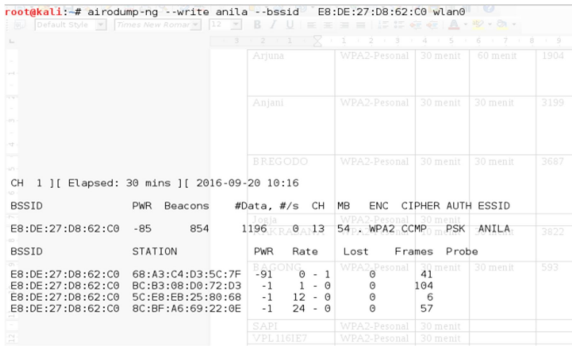
Pengujian ini dilakukan untuk mengetahui apakah pengguna yang sedang terhubung pada jaringan WLAN aman atau tidak. Aplikasi *netcut* digunakan untuk melihat pengguna yang terhubung pada jaringan WLAN, selanjutnya dilakukan proses *scanning*, dan serangan ke salah satu pengguna dengan cara mematikannya (*OFF*). Proses ini tampak seperti Gambar 5.



Gambar 5. *Cut off user* yang terhubung WLAN

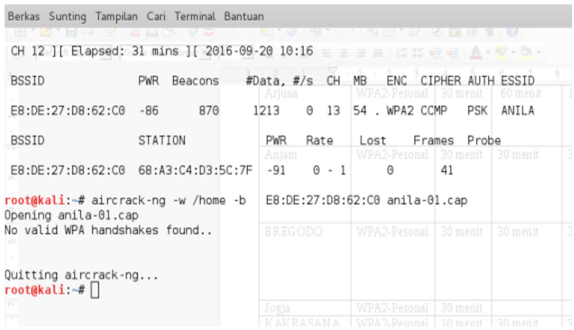
Cracking

Proses *capturing* jaringan WLAN Anila yang menerapkan *WPA2-Personal*, dilakukan proses *scanning* selama 30 menit dan proses rekam selama 30 menit, jumlah proses yang terjadi sebanyak 870 dan diperoleh hasil proses rekam sebanyak 1.213 data, seperti ditampilkan pada Gambar 6.



Gambar 6. Proses *capturing* pada WLAN Anila

Proses *cracking* ke WLAN Anila gagal karena *WPA handshakes* yang ditemukan tidak valid untuk mendapatkan *password*. Hal ini nampak pada Gambar 7.



Gambar 7. Proses *cracking* pada WLAN Anila

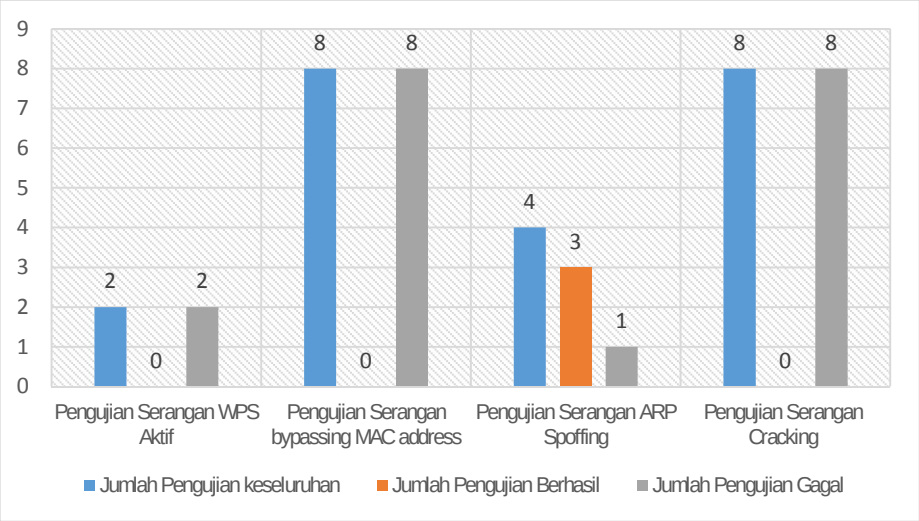
Pada pengujian pertama hanya jaringan *wireless* Arjuna yang gagal diserang. Hasil pengujian serangan pertama ditampilkan pada Tabel 3. Pengujian kedua dilakukan pada seluruh koneksi WLAN yang sama dengan pengujian pertama. Hasil pengujian kedua menunjukkan bahwa seluruh serangan gagal menyerang jaringan WLAN. Secara terinci hasil pengujian tersebut tampak pada Tabel 4, sedangkan secara teringkas ditunjukkan pada Tabel 5. Selanjutnya, Gambar 8 menampilkan rangkuman hasil pengujian serangan yang gagal dan berhasil sebelum konfigurasi keamanan jaringan WLAN, sedangkan Gambar 9 menampilkan rangkuman hasil pengujian serangan setelah dilakukan konfigurasi keamanan jaringan WLAN.

Tabel 3. Hasil pengujian serangan sebelum konfigurasi keamanan jaringan WLAN

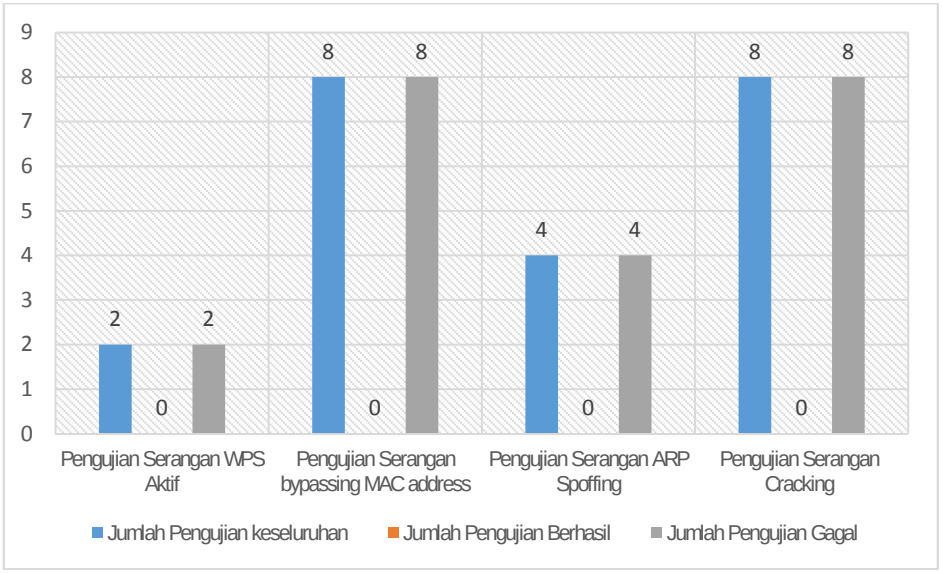
Jaringan WLAN (SSID)	Tipe keamanan	WPS Aktif	Bypassing MAC Address	ARP Spoofing	Cracking
Anila	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal
Anjani	WPA2-Pesonal	Tidak diuji	Gagal	Berhasil	Gagal
Arjuna	WPA2-Pesonal	Gagal	Gagal	Gagal	Gagal
Bagong	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal
Bregodo	WPA2-Pesonal	Tidak diuji	Gagal	Berhasil	Gagal
Gareng	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal
Kakrasana	WPA2-Pesonal	Gagal	Gagal	Berhasil	Gagal
Sambo	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal

Tabel 4. Hasil pengujian serangan setelah konfigurasi keamanan jaringan WLAN

Jaringan WLAN (SSID)	Tipe keamanan	WPS Aktif	Bypassing MAC Address	ARP Spoofing	Cracking
Anila	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal
Anjani	WPA2-Pesonal	Tidak diuji	Gagal	Gagal	Gagal
Arjuna	WPA2-Pesonal	Gagal	Gagal	Gagal	Gagal
Bagong	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal
Bregodo	WPA2-Pesonal	Tidak diuji	Gagal	Gagal	Gagal
Gareng	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal
Kakrasana	WPA2-Pesonal	Gagal	Gagal	Gagal	Gagal
Sambo	WPA2-Pesonal	Tidak diuji	Gagal	Tidak diuji	Gagal



Gambar 8. Grafik data hasil pengujian sebelum konfigurasi



Gambar 9. Grafik data hasil pengujian setelah konfigurasi

Berdasarkan perbandingan hasil pengujian pertama dan kedua dapat diketahui bahwa sebelum dilakukan konfigurasi keamanan jaringan WLAN pengujian *ARP spoofing* berhasil mengganggu aktifitas jaringan WLAN. Hal ini dibuktikan dengan adanya 3 jaringan WLAN yang mengalami masalah setelah dilakukan pengujian tersebut, sedangkan pada 3 pengujian lainnya jaringan WLAN tidak mengalami masalah karena penggunaan enkripsi pada *access point* atau *router* mampu menangkal serangan-serangan tersebut. Setelah dilakukan konfigurasi keamanan jaringan WLAN seluruh jaringan tidak berhasil diserang, sehingga aman digunakan oleh pengguna dan para pengguna tidak akan terganggu lagi oleh pengguna illegal.

5. KESIMPULAN

Hasil pengujian pada penelitian ini menunjukkan bahwa keamanan jaringan WLAN di Dinas Kominfo DIY sudah aman, karena *access point* atau *router* jaringan WLAN yang tersedia sudah menerapkan sistem keamanan setingkat WPA/WPA2-PSK. Celah keamanan pada

beberapa jaringan WLAN adalah pengguna yang sedang menggunakan jaringan WLAN masih bisa diserang oleh pengguna lain pada jaringan *wireless* yang sama. Untuk meningkatkan keamanan jaringan WLAN di Dinas Kominfo DIY perlu diaktifkan fitur *ARP* atau *binding* pada *access point* atau *router* agar terhindar dari serangan *spoofing* seperti *nmap*, *netcut*, dan lain-lain, sehingga pengguna menjadi aman dalam menggunakan jaringan WLAN tanpa diganggu oleh pengguna lainnya.

6. DAFTAR PUSTAKA

[1]. Nugroho, B.A. 2012. *Analisis Keamanan Jaringan Pada Fasilitas Internet (WiFi) Terhadap Serangan Packet Sniffing*. Universitas Muhamdiyah Surakarta. Surakarta.

[2]. Ervianto, D. 2012. *Analisis Sistem Keamanan Jaringan Wep Security Menggunakan Distro Linux Backtrack Pada Puri Ayu Homestay*. STMIK AMIKOM Yogyakarta. Yogyakarta.

[3]. Supriyanto, A. 2006. Analisis Kelemahan Keamanan pada Jaringan Wireless. *Jurnal Teknologi Informasi Dinamik*. XI(1): 38-46.

[4]. S'to. (2007). *Wireless Kungfu Networking & Hacking.* Jakarta: Jasakom.

[5]. Mundzir, M. (2015). *Trik Bobol Jaringan Wireless*. Yogyakarta: Notebook.

[6]. Ciampa, M. (2012). *Security + Guide to Network Security Fundamental*. Boston: Course Technology.

[7]. Hurley, C. (2007). *Wardriving & Wireless Penetration Testing*. Rockland: Syngress.