CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. x, No. x, Mei 2018, hlm. x-x

TINGKAT KEAMANAN JARINGAN HOME WI-FI DI KOTA YOGYAKARTA TERHADAP PASSWORD ATTACK

Panggih Gumelaring Praja[1], Muhammad Taufiq Nuruzzaman[2], Bambang Sugiantoro[3], Mandahadi Kusuma[4]

[1,2,3,4]Informatika, Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia
Email: [1]panggihgp05@gmail.com, [2]m.taufiq@uin-suka.ac.id, [3]bambang.sugiantoro@uin-suka.ac.id, [4]mandahadi.kusuma@uin-suka.ac.id

(Naskah masuk: dd mmm yyyy, diterima untuk diterbitkan: dd mmm yyyy)

Abstrak

Penggunaan teknologi Wi-Fi yang meningkat seiring berjalanannya waktu menimbulkan keresahan dikarenakan masalah keamanan jaringan yang masih mendapat sedikit perhatian. Kota Yogyakarta sebagai penyandang kota dengan indeks literasi digital tertinggi dan perencanaan program *smart city*-nya belum ada jaminan keamanan terkait permasalahan ini. Penelitian ini ditunjukan untuk mengkaji tingkat keamanan jaringan *home* Wi Fi terhadap *password attack* untuk keperluan data statistik dan bahan edukasi. Metode pengambilan sampel yang digunakan yaitu teknik *quota sampling* dan *penetration testing* sebagai metode pengumpulan datanya. Hasil penelitian menunjukan serangan WPA *cracking* dan WPS *cracking* berhasil mendapatkan sebagian kecil akses *login* berupa *password* serta mengukur persentase keamanan tingkat kota maupun di setiap kecamatannya. Selain data serangan, terdapat beberapa rekomendasi untuk melindungi *access point* supaya terhindar dari serangan tersebut.

Kata kunci: *Wi-Fi, password attack, WPA cracking, WPS cracking*

THE SECURITY LEVEL OF HOME WI-FI NETWORKS AGAINST PASSWORD ATTACKS

Abstract

The escalating use of Wi-Fi technology has raised concerns due to network security issues that often receive inadequate attention. Despite Yogyakarta's status as a city with the highest digital literacy index and its smart city program initiatives, there is no guaranteed security regarding these problems. This research aims to assess the security level of home Wi-Fi networks against password attacks for statistical data and educational purposes. The sampling method employed was quota sampling, with penetration testing used as the data collection method. The research results indicate that WPA cracking and WPS cracking attacks successfully obtained a small portion of login credentials in the form of passwords, and measured the percentage of security levels at the city level and in each sub-district. In addition to the attack data, several recommendations are provided to protect access points from these attacks.

***Keywords**: Wi-Fi, password attack, WPA cracking, WPS cracking*

1. PENDAHULUAN

Penggunaan teknologi *Wireless Fidelity* (Wi-Fi) terus meningkat seiring berjalannya waktu. Hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2022 menunjukkan angka 20,61% masyarakat Indonesia menggunakan *home* Wi-Fi untuk mendapatkan koneksi internet (APJII, 2022). Pada tahun 2023, Sekretaris Jenderal APJII Zulfadly Syam mengatakan ada kenaikan pengguna internet rumah (*home* Wi-Fi) sebanyak 0,15% dari tahun sebelumnya serta penurunan pengguna *mobile* data sebanyak 0,33% (CNN Indonesia, 2023). Peningkatan ini mulai masif ketika pandemi COVID-19 tahun 2020 yang salah satu penyebabnya adalah pemberlakuan *Work From Home* (WFH) (Rahmi, 2023). Hal tersebut yang membuat masyarakat mulai beramai-ramai menggunakan *home* Wi-Fi untuk keperluan akses internet yang dianggap lebih murah dan efisien untuk keperluan sehari-hari. Dikarenakan penggunaannya yang mudah, mulai dari pemasangan sampai perawatan, baik pengguna maupun penyedia layanan cenderung menyepelekan masalah keamanannya dan hanya fokus pada fungsionalnya saja.

Secara umum, kelemahan teknologi *wireless* terbagi menjadi dua yaitu kelemahan konfigurasi dan jenis enkripsi yang digunakan (Supriyanto, 2006). Pengguna yang awam akan teknologi biasanya hanya memanfaatkan konfigurasi *default*

yang telah disediakan oleh penyedia layanan. Penyedia layanan lebih mengutamakan kemudahan akses seperti cara mengganti kata sandi, mengganti nama SSID, atau pihak yang harus dihubungi apabila terjadi masalah daripada perihal keamanan jaringan. Jenis standar keamanan pada Wi-Fi seperti WEP, WPA, dan WPA2 sudah bukan menjadi fondasi utama dalam mengamankan kata sandi. WPA-PSK yang sekarang banyak digunakan dan salah satu standar keamanan baru juga sudah dapat dipecahkan menggunakan metode *dictionary attack* secara *offline* (Sinambela, 2007). Metode keamanan yang tersedia perlu dikombinasikan dengan kesadaran pengguna akan masalah keamanan seperti penggunaan kata sandi yang kuat, penggunaan *firewall*, dan keamanan fisiknya.

Daerah Istimewa Yogyakarta (DIY) menjadi Provinsi dengan indeks literasi digital tertinggi dalam skala nasional pada tahun 2021-2022 (Kemenkominfo, 2022). Dalam survei tersebut, skala penentuan sampel di DIY sebesar 74% untuk wilayah perkotaan dari 110 responden. Kota Yogyakarta tentu menyumbang sebagian besar data tersebut dan bisa dikatakan menjadi salah satu kota dengan indeks literasi digital tertinggi. Salah satu bentuk dukungan pemerintah untuk meningkatkan literasi digital masyarakat adalah dengan pengadaan Wi-Fi gratis yang bersifat publik dalam program *Jogja Smart Service* (JSS) dan telah menyediakan setidaknya 524 titik dan akan terus bertambah (Adminwarta, 2021) JSS juga menjadi bagian penting dalam pengembangan Kota Yogyakarta sebagai *smart city* untuk mewujudkan *smart culture* (*smart education* dan *smart tourism*) (Faidat and Khozin, 2018). Selain literasi digital, Dinas Pendidikan Pemuda dan Olahraga (Disdikpora) yang bekerja sama dengan Dinas Perpustakaan dan Kearsipan (DPK) berhasil membuat 31 kampung baca hingga akhir 2022 sebagai sentra edukasi masyarakat (Setyono, 2023).

Indeks literasi yang tinggi serta program *smart city* menjadi alasan utama peneliti untuk mencari tahu tingkat keamanan *home* Wi-Fi di Kota Yogyakarta terhadap *password attack*. Hal ini dilakukan untuk mengukur seberapa *aware* masyarakat terhadap keamanan *access point* (AP) yang dimiliki sehingga dapat mencegah jenis serangan yang lebih berbahaya.

2. TINJAUAN PUSTAKAN

2.1. Konsep Keamanan Jaringan

Konsep keamanan jaringan yang dipaparkan oleh (Rushadi, 2018) berkaitan dengan pentingnya menjaga validitas dan integritas data serta terjaminnya ketersediaan layanan bagi penggunanya.

Keamanan ini berfungsi untuk melindungi sistem dari berbagai macam serangan yang dilakukan oleh pihak luar. Masalah keamanan jaringan biasanya bertolak belakang dengan aksesnya, semakin mudah akses yang tersedia makan keamanan semakin rentan. Jaringan dengan keamanan yang baik maka aksesnya semakin sulit dan terbatas.

Adapun metode keamanan protokol WLAN menurut (Fauzi and Maulana, 2018) adalah sebagai berikut:

a. *Wired Equivalent Privacy* (WEP)

Standar keamanan WEP merupakan protokol keamanan pertama yang diterapkan pada jaringan wireless. Standar ini menggunakan algoritma RC4 untuk enkripsi datanya (Kaur, 2017). Penerapan protokol ini sangat tidak disarankan karena dinilai sangat rentan dan mudah dipecahkan.

b. Wi-Fi *Protected Access-Pre-Shared Key* (WPA-PSK)

Pada standar keamanan ini terdapat dua jenis enkripsi yang ditawarkan yaitu *Temporal Key Integrity Protocol* (TKIP) dan *Advanced Encryption Standard* (AES). Penerapan TKIP pada WPA dinilai masih kurang aman. Sedangkan, penerapan AES yang merupakan enkripsi modern kurang cocok dengan standar WPA dikarenakan AES biasa ditemui pada standar keamanan WPA2 yang tidak didukung oleh perangkat lama.

c. WPA2-PSK

Standar ini menawarkan jenis enkripsi yang sama seperti WPA yaitu TKIP dan AES. Penggunaan TKIP yang merupakan jenis enkripsi lama sangat tidak disarankan kecuali jika memiliki perangkat yang tidak mendukung WPA2-PSK (AES). Sedangkan, standar keamanan WPA2-PSK (AES) justru menjadi pilihan yang aman dan ideal untuk diterapkan pada jaringan WLAN saat ini.

d. WPA/WPA2-PSK

Standar ini menawarkan kombinasi dari WPA dan WPA2 sekaligus dengan jenis enkripsinya yaitu TKIP dan AES. Tujuan dari adanya standar keamanan ini adalah supaya perangkat lama dan perangkat baru tetap bisa mendapat akses ke jaringan dengan standar yang didukung oleh perangkat tersebut. Akan tetapi, kombinasi ini justru memiliki kerentanan karena terdapat protokol lama yaitu WPA dan TKIP.

e. WPA3

WPA3 merupakan standar keamanan terbaru dengan tingkat keamanan yang lebih tinggi dibanding dengan WPA2. Standar keamanan yang dirilis tahun 2018 ini menggunakan *Simultaneous Authentication of Equals* (SAE) untuk autentikasinya menggantikan PSK (van Oorschot, 2021). Metode enkripsi ini memungkinkan jaringan tidak dapat diserang menggunakan dictionary attack secara offline (Kwon and Choi, 2021). Sayangnya, protokol keamanan ini belum banyak digunakan dan banyak perangkat yang belum terdapat fitur keamanan ini.

f. W-Fi *Protected Setup* (WPS)

WPS merupakan program sertifikasi opsional yang dirancang untuk memudahkan pengaturan

jaringan Wi-Fi dalam lingkup rumah dan kantor kecil (Wi-Fi Alliance, 2007) . WPS mempunyai dua metode dalam konfigurasinya yaitu *Press Button Configuration* (PBC) dan memasukkan PIN (Rianto, 2013). Kedua metode ini digunakan untuk proses koneksi ke jaringan tanpa harus memasukkan *password*.

2.2. *Wireless Local Area Network Hacking*

Aktivitas wireless hacking dinilai lebih rentan dikarenakan bisa dilakukan tanpa mengharuskan penyerang berada pada tempat tertentu dan dapat dilakukan kapan pun selama masih berada di jangkauan jaringan (Zam, 2016). WLAN *hacking* umumnya dilakukan untuk mendapat akses internet. Jaringan WLAN juga biasanya dijadikan target sebagai bahan uji coba serangan *wireless* oleh orang yang baru belajar *hacking*.

a. Wifite

Wifite merupakan sebuah *tool* untuk audit keamanan jaringan *wireless*. Pada Wifite terdapat beberapa fitur yang dapat digunakan untuk berbagai jenis serangan wireless dan bekerja secara otomatis (*automate tool*) untuk jenis serangan WPA dan WPS.

b. Wi-Fi *Protected Setup Cracking*

Istilah lain dari WPS *cracking* adalah PIN *brute-force attack* dikarenakan yang menjadi target dalam serangan ini adalah PIN dari *router* untuk akses jaringan. Adapun cara kerja dari metode ini adalah *router* memberikan PIN sebanyak 8 digit yang akan digunakan *client* sebagai akses masuk ke jaringan tanpa harus memasukkan *password* (Ajay, Amritha and Sethumadhavan, 2021).

Celah inilah yang dimanfaatkan penyerang untuk mendapatkan akses dengan cara melakukan *brute force* PIN dan mencocokan dengan PIN yang dimiliki *router*. Metode ini biasanya dalam kondisi *enable* di beberapa *router access point* sehingga tidak disadari pengguna dan *password* yang kuat akan tetap bisa ditebak jika serangan ini berhasil (Weidman, 2014).

c. Wi-Fi *Protected Access Cracking*

Kelemahan WPA/WPA2-PSK adalah pada proses autentikasinya. Proses autentikasi berupa *four-way handshake* dapat ditangkap melalui udara (Ajay, Amritha and Sethumadhavan, 2021). Penangkapan ini terjadi ketika client melakukan de-autentikasi dengan *access point* karena ulah penyerang yang mencoba memutus koneksi sementara. Hasil dari penangkapan ini disimpan dalam format *file* *.cap yang akan digunakan untuk *dictionary attack* secara *offline*.

WPA/WPA2 *cracking* memanfaatkan *file* hasil *capturing four-way handshake* dan *dictionary wordlist*. Secara umum, proses *cracking* ini dimulai dengan mengidentifikasi target, melakukan de-autentikasi, mendapatkan informasi handshake, melakukan *brute force*, dan verifikasi akses. Jaringan dengan *password* yang lemah akan lebih mudah terkena serangan ini sehingga mengakibatkan adanya akses ilegal dari pihak luar.

3. METODOLOGI

2.1. Waktu dan Tempat Penelitian

Waktu yang diperlukan dalam penelitian ini adalah 24 hari dari 21 Februari-15 Maret 2024 dengan rata-rata 5-6 jam kerja setiap harinya. Penelitian ini dilakukan di 45 Kelurahan yang tersebar di seluruh Kota Yogyakarta. Sampel diambil di masjid-masjid, pos-pos ronda, dan jalanan warga sebagai titik pengambilan sampel.

2.2. Alat dan Bahan

Alat digunakan sebagai penunjang fisik untuk proses pengambilan data, sedangkan bahan berperan pada *resource* untuk efektifitas alat yang dipakai, sebagaimana ditampilkan pada Tabel 1.

Tabel 1 Alat dan Bahan Penelitian

Alat	Bahan
Laptop: OS Windows 11 RAM 8,00 GB SSD 256 GB	Virtualbox versi 6.1 2021 OS Kali Linux 2021.3 amd64 Tool Wifite2 2.5.8 *Password dictionary* wordlist-*probable.txt* (*modification*)
Network Adapter: TP-Link TL-WN722N versi 1.10	*Access point* target

2.3. Metode Penelitian

a. Populasi dan Sampel

Pada penelitian ini, populasi yang akan digunakan adalah Jaringan *home* Wi-Fi yang tersebar di seluruh Kota Yogyakarta (14 Kecamatan, 45 Desa/Kelurahan). Dikarenakan tidak ada sumber data valid terkait jumlah objeknya, maka peneliti menetapkan populasi dengan status tidak diketahui atau tak terhingga.

Teknik pengambilan sampel yang digunakan dalam penelitian ini adalah *quota sampling*. *Quota sampling* merupakan teknik untuk menentukan sampel dari populasi dengan kriteria tertentu sampai jumlah (kuota) yang diinginkan (Sugiyono, 2013).

Berdasarkan populasi yang jumlahnya tidak diketahui atau tak terhingga, maka teknik penentuan jumlah sampel dilakukan menggunakan rumus Lemeshow untuk menentukan jumlah sampel minimal dalam penelitian ini. Penentuan estimasi reliabilitas (*reliability of estimates*) dari penelitian ini diukur berdasarkan ukuran standar *error*-nya (Levy and Lemeshow, 2008). Perhitungan penentuan

jumlah sampel menggunakan rumus Lemeshow sebagai berikut:

n = Jumlah sampel minimal

$Z^2\left(1-\frac{\alpha}{2}\right)$ = Derajat kepercayaan (95%, Z = 1,96)

P = Proporsi populasi/maksimal estimasi (50% = 0.5)

d = Besar toleransi kesalahan (7% = 0.07)

$$n = \frac{Z^2\left(1-\frac{\alpha}{2}\right)P(1-P)}{d^2}$$

$$n = \frac{(1{,}96)^2\ 0.5(1-0.5)}{0{,}07^2} = \frac{3{,}8416\ x\ 0{,}25}{0{,}0049} = 196$$

Jumlah sampel minimal yang didapat dari rumus Lemeshow adalah 196 sampel dan akan dibulatkan menjadi 225 sampel dengan pertimbangan pemerataan pengambilan sampel di wilayah yang telah ditentukan dengan rincian 5 sampel per kelurahan.

Adapun karakteristik/kriteria dari sampel yang akan diambil adalah sebagai berikut:

1. Jaringan Wi-Fi yang digunakan untuk internet rumah (*home* Wi-Fi)
2. Jaringan Wi-Fi menggunakan frekuensi 2.4 GHz
3. Terdapat client yang terkoneksi seminimalnya 1 (satu) (WPA *cracking*)

b. Metode Pengumpulan Data

Metode yang digunakan untuk mengumpulkan data pada penelitian ini adalah *Penetration Testing* (*pentest*). *Pentest* merupakan metode pengujian yang melibatkan simulasi serangan nyata untuk menilai keamanan sistem. Metode ini tidak hanya menutup celah kerentanan tetapi juga mencoba mengeksploitasinya. Hal ini dilakukan untuk menilai risiko kerugian suatu sistem apabila berhasil dieksploitasi (Weidman, 2014). Jenis strategi *pentest* yang akan dipakai adalah *Black Box Strategy*. Pada strategi *black box*, *pentester* tidak dimodali informasi tentang sistem yang akan diujinya (Phong and Yan, 2014). Data-data yang dibutuhkan harus dicari sendiri tanpa ada pihak yang memberikan informasi.

Terdapat 4 langkah utama dalam *pentest* sebagaimana yang digambarkan di Gambar 1 dengan rincian sebagai berikut:

1. Information Gathering

Pada tahap ini, penulis melakukan pengumpulan informasi yang akan dijadikan bahan dalam proses uji keamanan jaringan. Dikarenakan uji keamanan ini dilakukan dengan *black box testing*, pengumpulan informasi dilakukan secara mandiri berdasarkan analisis kemungkinan-kemungkinan yang dibutuhkan. Adapun bentuk analisisnya berupa, titik-titik tempat dilakukan *scanning* jaringan, nama SSID jaringan, jenis keamanan yang digunakan, dan kemungkinan *password* yang diterapkan.

2. Threat Modeling

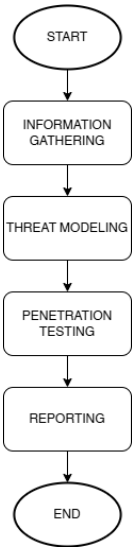
Setelah informasi terkumpul, langkah selanjutnya adalah menganalisis dan memodelkan potensi ancaman pada jaringan Wi-Fi. Informasi yang 27 didapatkan, seperti jenis standar keamanan yang dipakai, digunakan penulis untuk menganalisis serangan yang akan dipakai pada uji keamanan nantinya. Pada penelitian ini, uji keamanan yang akan digunakan adalah WPA *cracking* dan/atau WPS *cracking*.

3. Penetration Testing

Tahap ini merupakan inti dari metode *penetration testing*. Setelah data terkumpul dan dilakukan pemodelan, maka uji penetrasi bisa dilakukan. Uji penetrasi melibatkan serangan yang sebelumnya sudah ditentukan pada tahap pemodelan. Tujuan dari tahap ini adalah mengetahui hasil dari uji keamanan, berhasil atau tidaknya serangan, sehingga dapat dianalisis dan didokumentasikan pada tahap selanjutnya.

4. Reporting

Tahap terakhir adalah dokumentasi dari uji keamanan yang telah dilakukan pada tahap sebelumnya. Dokumentasi ditulis dalam bentuk laporan dan hasil analisis mengenai temuan celah keamanan, identifikasi risiko, dan pemberian rekomendasi solusi dari celah keamanan yang ditemukan.



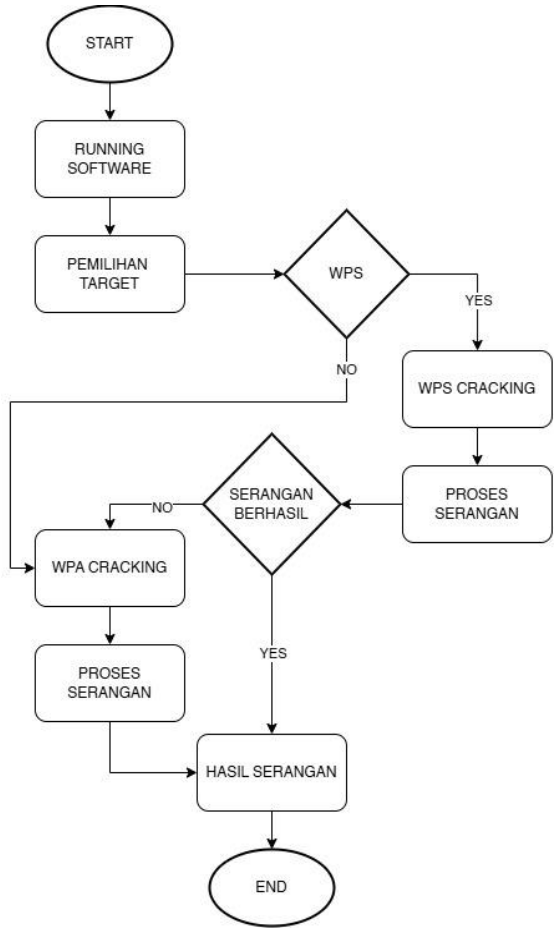
Gambar 1 Alur Pentration Testing

4. PEMBAHASAN

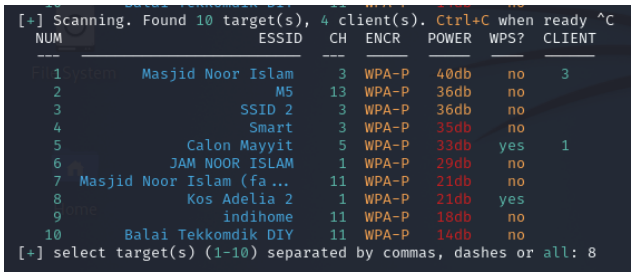
3.1 Penetration Testing

Pada penelitian ini, jenis metode serangan yang digunakan adalah WPS *cracking* dan WPA *cracking* dengan *tool* Wifite. Dua metode ini bertujuan untuk mengetahui *password* dari *access point* (AP) dengan celah yang berbeda. WPS *cracking* memanfaatkan celah konfigurasi WPS PIN untuk mendapatkan akses ke jaringan dengan melakukan *brute force* PIN, sedangkan WPA *cracking* memanfaatkan *file handshake* yang didapat untuk mendapatkan *hash password* kemudian dicocokkan melalui serangan *dictionary attack* secara *offline*.

Gambar 2 menjelaskan tentang proses serangan pada target yang dimulai dengan menjalankan Wifite kemudian akan ditampilkan list AP yang tertangkap oleh *network adapter*. Gambar 3 menampilkan informasi AP yang didapat dari hasil proses scanning seperti nama AP, *channel*, jenis enkripsi, besar *desible* (db), penggunaan WPS, dan jumlah *client*.



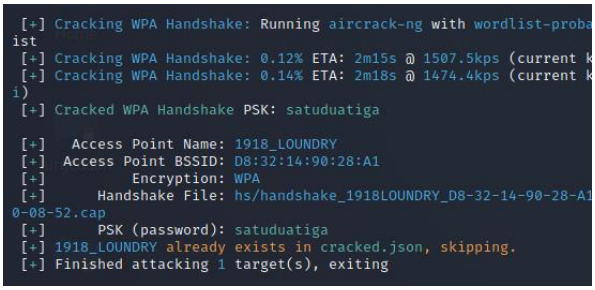
Gambar 2 Proses *Penetration Testing Target*



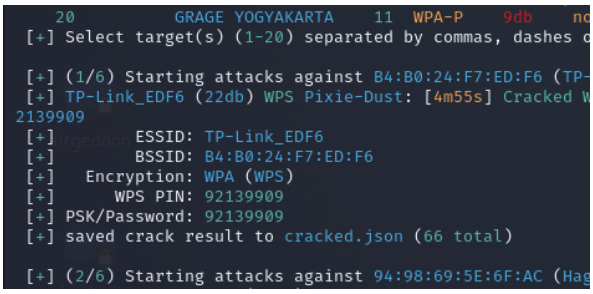
Gambar 3 Hasil *Scanning Target*

Apabila AP target terdapat fitur WPS, maka serangan pertama yang diluncurkan adalah WPS *cracking* (WPS *Pixie-dust*) dengan estimasi serangan maksimal 5 menit. Jika serangan ini gagal akan dilanjutkan menggunakan metode *brute force* atau WPA *cracking* dengan estimasi waktu 5-10 menit tergantung dari proses mendapatkan *file* autentikasinya yang kemudian dilakukan pencocokan dengan *password dictionary* yang sudah terkoneksi.

Proses serangan berhasil diukur dari berhasil atau tidaknya mendapatkan *password* AP target. Pada Gambar 4 menunjukan output dari contoh serangan WPA yang berhasil dengan adanya informasi *password* yang diaplikasikan pada AP tersebut. Sedangkan, Gambar 5 merupakan hasil dari serangan WPS yang sukses dengan informasi yang sama dengan serangan WPA, perbedaannya hanya terletak pada informasi PIN yang dimiliki AP dengan fitur WPS aktif.



Gambar 4 Hasil Serangan WPA



Gambar 5 Hasil Seerangan WPS

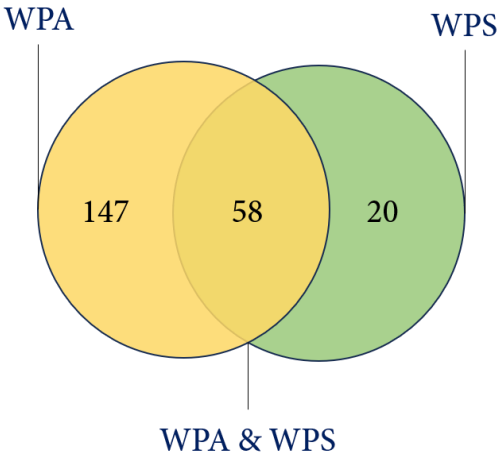
3.2 Hasil Pengujian Keamanan Home Wi-Fi

Hasil dari *penetration testing* menggunakan metode *password attack* WPA *cracking* dan WPS *cracking* menunjukkan 15,56% dari 225 *home* Wi-Fi berhasil didapatkan *password*-nya dan 84,44% gagal. Setiap AP mendapat serangan yang berbeda sesuai dengan kondisi konfigurasi yang digunakan. AP yang menggunakan konfigurasi WPS akan mendapat serangan WPS *cracking* (WPS *Pixie-Dust*) dan apabila serangan gagal maka akan dilanjut dengan serangan WPA *cracking* (WPA *Handshake Captured*).

Adapun data yang didapatkan dalam proses tersebut adalah nama SSID, BSSID, standar keamanan/enkripsi, dan konfigurasi yang digunakan. Data-data ini berperan penting dalam menentukan serangan dan analisis kemungkinan serangan berhasil.

Gambar 6 menunjukkan jumlah serangan WPS sebanyak 78 dan serangan WPA 205. Dua ratus dua puluh lima (225) AP tersebut 20 di antaranya hanya mendapat serangan WPS, 147 hanya serangan WPA, dan 58 mendapatkan serangan WPS dan WPA. Sedangkan, Tabel 2 menampilkan data serangan

berhasil dan serangan gagal dari jenis serangan yang digunakan. Serangan WPS mendapat persentase keberhasilan 19,23% dari 78 serangan. Sedangkan serangan WPA hanya mendapat persentase keberhasilan 9,75% dari total 205 serangan.

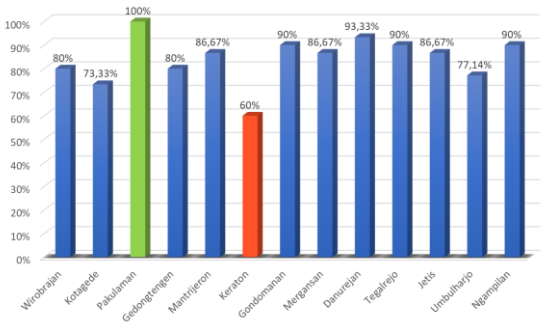


Gambar 6 Data Serangan

Tabel 2 Detail Persentase Serangan

SERANGAN	TOTAL	GAGAL	BERHASIL	KEBERHASILAN (%)
WPS	78	63	15	19,23%
WPA	205	185	20	9,75%

Kecamatan dengan tingkat persentase keamanan tertinggi yaitu di Kecamatan Pakualaman dengan persentase 100% dari 10 AP. Sedangkan Kecamatan Kraton menjadi yang paling rentan dengan persentase 60% dari 15 AP. Kecamatan lain berada pada tingkat keamanan yang baik antara 73%-96% seperti data pada Gambar 4.



Gambar 7 Persentase Keamanan Per kecamatan

Setiap kecamatan memiliki karakteristik AP yang berbeda-beda. Sebagai contoh di Kelurahan Kadipaten, Kecamatan Kraton, di satu titik uji pengambilan sampel terdapat 2 AP yang berhasil terkena serangan WPS. Hal ini diasumsikan bahwa beberapa AP berasal dari *provider* yang sama sehingga *setting* fitur WPS-nya aktif secara *default* yang meneyababkan celah untuk serangan WPS. Begitu juga di Kelurahan Gedongkiwo, Kecamatan Mantrijeron, di satu titik uji pengambilan sampel dari 3 serangan WPS tidak ada yang berhasil.

Di sisi lain, kecamatan yang rentan terhadap serangan WPA seperti Umbulharjo dan Kotagede cenderung menggunakan *password* dengan kombinasi angka saja, baik urutan angka atau berupa tanggal tertentu. Oleh karena itu, AP di sekitaran daerah ini penggunaan *password*-nya cenderung lemah tanpa adanya kombinasi yang kuat.

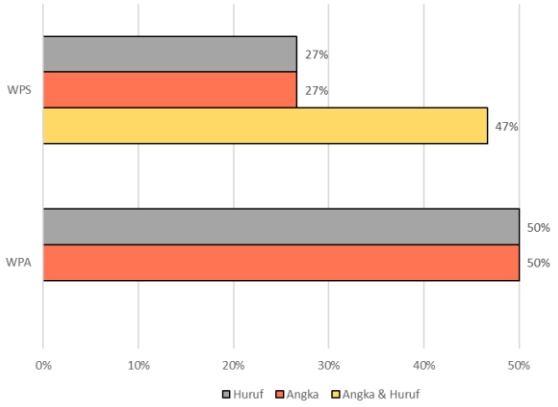
3.3 Wi-Fi Protected Access (WPA) Cracking

WPA *cracking* merupakan serangan paling banyak yang digunakan pada penelitian ini. Serangan ini memanfaatkan *file handshake* yang di-*capture* setelah melakukan *deauthing* dan *listening* antara *client* dan AP. Proses serangan ini juga terbilang cukup lama dikarenakan harus menunggu Wifite mendapat *file handshake* (*default timeout* 5 menit) dan proses *brute force* pencocokan *password* (3 menit).

Permasalahan yang dihadapi dalam proses serangan ini adalah tidak semua AP terhubung dengan *client*. Hal tersebut menyebabkan serangan WPA tidak bisa dilakukan karena tidak ada autentikasi yang didapat. Selain itu, beberapa AP juga memiliki sistem pertahanan dari *Denial of Service* (DoS) dan *brute force* sehingga proses serangan tidak berjalan maksimal.

Keberhasilan serangan WPA dipengaruhi oleh kombinasi *password* yang digunakan. Dari 205 AP, 20 di antaranya berhasil didapatkan PSK/*password login*-nya. Hal ini dikarenakan kombinasi *password* yang kurang kuat dan cenderung mudah ditebak. Selain itu juga, tidak atau kurangnya metode pertahanan terhadap serangan ini sehingga membuat proses penyerangan lebih mudah dilakukan dengan tingkat keberhasilan yang tinggi.

Adapun kombinasi *password* yang digunakan oleh AP yang berhasil diserang adalah 50% menggunakan angka dan 50% menggunakan huruf. Gambar 5 menunjukkan tidak ada yang menggunakan kombinasi angka dan huruf maupun spesial karakter sehingga *password* lebih rentan. Penggunaan angka dan hurufnya juga sangat lemah dan terlalu umum digunakan, sehingga penyerang bisa memperkirakan *password*-nya. Merek AP yang berhasil didapatkan di antaranya ZTE, TP-Link, Huawei, dan Tenda.



Gambar 8 Data Kombinasi Password

3.4 Wi-Fi *Protected Setup (WPS) Cracking*

WPS *cracking* memanfaatkan celah konfigurasi WPS PIN pada AP. Serangan ini lebih mudah dilakukan daripada serangan WPA dikarenakan hanya butuh waktu 1-2 menit untuk mengidentifikasi keberhasilan/kegagalan serangan. Kekurangan dari serangan ini adalah tidak semua AP menggunakan konfigurasi WPS dan apabila menggunakan WPS pun tidak semua menggunakan WPS PIN (WPS *Press Button Configuration* (PBC)).

Dalam proses serangan WPS, tidak ada permasalahan serius yang dihadapi. Hanya beberapa AP mempunyai mekanisme pertahanan yang cukup terhadap jenis serangan ini. Mekanisme ini bergantung pada konfigurasi yang diterapkan seperti respons WPS *lock*, *switch* konfigurasi PBC, dan *non-active* WPS. Respons ini juga tidak langsung dilakukan AP saat terjadi serangan, beberapa di antaranya butuh 2-3 kali serangan untuk merespons bahwa ada akses berbahaya yang mencoba mendapatkan data akses.

Dikarenakan serangan ini tidak bergantung pada *dictionary password* seperti serangan WPA, kombinasi *password* yang kuat tidak terlalu penting sebagai mekanisme pertahanan. Data serangan berhasil yang ditampilkan pada Gambar 8 di atas menunjukkan 7 dari 20 AP menggunakan kombinasi huruf dan angka yang cukup kuat untuk mencegah serangan WPA, 4 menggunakan kombinasi huruf, dan 4 sisanya menggunakan kombinasi angka.

Adapun informasi yang didapat dari serangan ini seperti PIN yang digunakan untuk autentikasi, nama SSID, dan PSK. Merek AP yang berhasil diketahui di antaranya Nokia, Huawei, Android, dan TP-Link.

3.5 Solusi Pengamanan

Jenis serangan WPA *cracking* maupun WPS *cracking* tidak dapat dihindari hanya dengan penggunaan *password* yang kuat atau standar keamanan yang kuat. Perlu kombinasi konfigurasi pertahanan serta pengetahuan yang cukup supaya *home* Wi-Fi yang digunakan aman. Berikut ini merupakan rekomendasi pengamanan *home* Wi-Fi dari 2 jenis serangan tersebut berdasarkan analisis hasil penelitian yang dilakukan:

a. Melakukan update firmware terbaru

Update firmware dilakukan untuk memperbaharui sistem dari AP. Biasanya terdapat fitur baru yang diberikan termasuk sistem keamanan. Sayangnya hal ini jarang sekali dilakukan oleh pengguna *home* Wi-Fi dikarenakan tidak semua pengguna tahu caranya. Cara melakukan *update*-nya adalah dengan memasukkan *file update*, yang di-*donwload* dari *website* resmi, melalui halaman admin.

b. Menerapkan konfigurasi keamanan

Penerapan konfigurasi keamanan tidak hanya mengaplikasikan standar keamanan/enkripsi saja. Tidak sedikit AP dalam lingkup *home* Wi-Fi tidak menerapkan fitur keamanan yang disediakan seperti *firewall* dan kontrol akses.

c. Menggunakan standar keamanan terbaru

Standar keamanan menentukan jenis enkripsi yang digunakan seperti WPA TKIP, WPA2-AES, dan WPA3-SEA. Dari 225 AP hanya 1 yang menggunakan keamanan terbaru WPA3 dan sisanya menggunakan WPA2 CCMP/AES. Standar keamanan yang direkomendasikan adalah WPA3 SEA yang salah satu fitur utamanya adalah mencegah serangan *brute force*.

d. Menonaktifkan fitur WPS

Fitur WPS sangat membantu apabila terdapat banyak *client* yang ingin terkoneksi ke jaringan secara serentak. Akan tetapi fitur ini bisa menjadi celah keamanan apabila dibiarkan *enable* saat tidak dipakai dan cara melakukan *disable* WPS ada pada halaman admin. Konfigurasi PIN berbahaya terhadap serangan WPS *cracking*, sedangkan konfigurasi PBC berbahaya terhadap serangan fisik apabila posisi fisik AP mudah dijangkau. Oleh karena itu, fitur WPS ini harus dinonaktifkan apabila tidak digunakan.

e. Menggunakan kombinasi *password* yang kuat

Penggunaan *password* yang kuat tidak harus menyulitkan dan susah diingat. *Password* kuat di sini berarti tidak menggunakan *password default* atau yang sering digunakan dan mudah ditebak. Hal ini sangat penting untuk menghindari risiko keberhasilan yang tinggi dari serangan *brute force* atau *dictionary attack*.

f. Mengamanan fisik AP

Beberapa AP yang ditemukan saat penelitian, terutama di masjid-masjid, berada dalam posisi yang mudah dijangkau. Hal ini berbahaya untuk jenis serangan WPS PBC dan rentan terhadap pencurian.

Pengaplikasian pengamanan ini akan mencegah penyerang untuk tidak dapat melakukan kontrol pada jaringan yang dapat membahayakan para *client* yang terkoneksi dengan jaringan tersebut. Potensi serangan seperti penyebaran *malware*, *man in the middle* (MITM), Dos, dan berbagai jenis serangan lain yang dapat memanipulasi jaringan tidak akan terjadi selama celah-celah serangan tertutup.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil uji penetration testing menggunakan metode *password attack* dengan jenis serangan WPA *cracking* dan WPS *cracking* didapatkan kesimpulan sebagai berikut:

a. Persentase keamanan home Wi-Fi di Kota Yogyakarta terhadap *password attack* sebesar 84,44% dari 225 AP yang tersebar di 45 kelurahan. Nilai tersebut terbilang cukup aman dengan latar belakang Kota Yogyakarta sebagai bagian dari Kota dengan indeks literasi tertinggi.
b. Persentase keamanan tertinggi terletak di Kecamatan Pakualaman dengan persentase 100% dan keamanan terendah Kecamatan Kraton dengan persentase 60%.

Angka-angka tersebut masih tergolong rawan mengingat latar belakang Kota Yogyakarta yang memiliki banyak keunggulan. Oleh karena itu, diperlukan banyak penelitian serupa di tempat lain yang dapat menjadi pembanding untuk penentuan kebijakan yang lebih efektif.

5.2. Saran

Saran yang diberikan oleh peneliti terkait keamanan jaringan di Kota Yogyakarta terhadap *password attack* adalah sebagai berikut:

a. Perlu adanya pemahaman yang cukup untuk mengelola jaringan *home* Wi-Fi terutama masalah keamanannya. Hal ini penting sebagai pengguna untuk mendapatkan fasilitas keamanan yang cukup dari pihak penyedia layanan.
b. Diharapkan untuk penelitian selanjutnya tidak hanya mengambil data AP saja tetapi juga data pengguna AP dalam bentuk survei/wawancara. Perlu dipertimbangkan juga mekanisme pengambilan sampel seperti tempat dan waktu pengambilan supaya lebih terstruktur dan banyak data yang bisa didapatkan.
c. Diharapkan untuk penelitian selanjutnya untuk mengadakan kerja sama dengan penyedia layanan tertentu guna mengalisis kebijakan penggunaan *home* Wi-Fi serta perilaku pengguna selama masa sewa.

DAFTAR PUSTAKA

Adminwarta (2021) *Penggunaan Teknologi di Kota Yogya Dukung Terciptanya Aktivitas Produktif*. Available at: https://warta.jogjakota.go.id/detail/index/17442 (Accessed: 13 February 2024).

Ajay, A., Amritha, P. P. and Sethumadhavan, M. (2021) 'Automated WPA2 Cracking Using Improved Dictionary and WPS Pin Attack', *Advances in Electrical and Computer Technologies, Lecture Notes in Electrical Engineering 711*, pp. 323–334.

APJII (2022) *Survei Perilaku Penggunaan Internet*, *Asosiasi Penyedia Jasa Internet Indonesia*. Jakarta. Available at: https://apjii.or.id/download_survei/2feb5ef7-3f51-487d-86dc-6b7abec2b171.

CNN Indonesia (2023) *Wi-Fi dan Paket Data, Mana yang Lebih Banyak Dipakai Warga Indonesia?* Available at: https://www.cnnindonesia.com/teknologi/20230517111117-192-950700/wifi-atau-paket-data-mana-yang-lebih-banyak-dipakai-warga-indonesia (Accessed: 13 February 2024).

Faidat, N. and Khozin, M. (2018) 'Analisa Strategi Pengembangan Kota Pintar (Smart City): Studi Kasus Kota Yogyakarta', *JIP (Jurnal Ilmu Pemerintahan) : Kajian Ilmu Pemerintahan dan Politik Daerah*, 3(2), pp. 171–180. doi: 10.24905/jip.3.2.2018.171-180.

Fauzi, A. and Maulana, A. (2018) *Jaringan Komputer*, *repository.nusamandiri.ac.id*. Jakarta: Universitas Nusamandiri. Available at: https://repository.nusamandiri.ac.id/index.php/repo/viewitem/15976.

Kaur, J. (2017) 'WiFi Security: WEP, WPA, and WPA2', *International Journal of Control Theory and Application*, 10(May).

Kemenkominfo (2022) 'Status Literasi Digital di Indonesia 2022', *Kominfo*, (November), pp. 205–207. Available at: https://www.c2es.org/content/renewable-energy/.

Kwon, S. and Choi, H. K. (2021) 'Evolution of Wi-

Fi Protected Access: Security Challenges', *IEEE Consumer Electronics Magazine*, 10(1), pp. 74–81. doi: 10.1109/MCE.2020.3010778.

Levy, P. S. and Lemeshow, S. (2008) *Sampling of Populations*. Fourth Edi, *Sampling of Populations*. Fourth Edi. Edited by R. M. Groves et al. New Jersey: John Wiley & Sons, Inc. doi: 10.1002/9780470374597.

van Oorschot, P. C. (2021) 'Wireless LAN Security: 802.11 and Wi-Fi', in van Oorschot, P. C. (ed.) *Computer Security and the Internet*. Cham: Springer International Publishing, pp. 339–373. doi: 10.1007/978-3-030-83411-1_12.

Phong, C. T. and Yan, W. Q. (2014) 'An Overview of Penetration Testing', *International Journal of Digital Crime and Forensics*, 6(4), pp. 50–74. doi: 10.4018/ijdcf.2014100104.

Rahmi, Y. (2023) *Survei APJII: Pengguna Internet di Indonesia Tembus 215 Juta Orang*, *Bisnis Tekno*. Available at: https://teknologi.bisnis.com/read/20230308/101/1635219/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang (Accessed: 13 February 2024).

Rianto, I. D. (2013) 'Anticipating WPS PIN Vulnerability to Secure Wireless Network', *ComTech: Computer, Mathematics and Engineering Applications*, 4(2), pp. 1116–1121. doi: 10.21512/comtech.v4i2.2554.

Rushadi, S. (2018) 'Konsep Keamanan Jaringan Komputer dengan Infrastruktur Demilitarized Zone', *Sharing Knowledge and Experience Konsep*, (October), pp. 1–5. Available at: https://www.researchgate.net/publication/328130248_Konsep_Keamanan_Jaringan_Komputer_dengan_Infrastruktur_Demilitarized_Zone.

Setyono (2023) *31 Kampung Baca di Kota Yogyakarta Berkembang Jadi Sentra Edukasi*, *Eduwara*. Available at: https://eduwara.com/31-kampung-baca-di-kota-yogyakarta-berkembang-jadi-sentra-edukasi (Accessed: 16 March 2024).

Sinambela, J. M. (2007) 'Keamanan Wireless LAN (Wifi)', in *Seminar Wireless dan Keamanan Wireless*. Sleman: http://josh.staff.ugm.ac.id, p. 5. Available at: https://josh.rootbrain.com/seminar/Makalah Seminar Keamanan Wifi UNY-Josua M Sinambela .pdf.

Sugiyono (2013) *Metode Penelitian Kuantitatif Kualitatif dan R&D*. 19th edn, *Penerbit Alfabeta*. 19th edn. Bandung: Alfabeta.

Supriyanto, A. (2006) 'Analisis Kelemahan Keamanan pada Jaringan Wireless', *Jurnal Teknologi Informasi Dinamik*, 11(1), pp. 38–46.

Weidman, G. (2014) *PENETRATION TESTING : A Hands-On Introduction to Hacking*. Edited by A. Law. San Francisco: William Pollock.

Wi-Fi Alliance (2007) *Discover Wi-Fi : Wi-Fi Protected Setup*. Available at: https://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup (Accessed: 27 November 2023).

Zam, E. (2016) *Buku Sakti Wireless Hacking*. Jakarta: Elex Media Komputindo.