*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v22i1.14767*

# *Development of a Penetration Testing Framework for Identifying Security Vulnerability Solutions in WiFi Networks*

Pengembangan Framewok Penetration Testing untuk Proses Pencarian Solusi Kerentanan Keamanan pada Jaringan Wifi

**Ali Imran[1], Shelvie Nidya Neyman[2], Hendra Rahmawan[3]**

[1,2,3] Ilmu Komputer, Institut Pertanian Bogor, Indonesia

[1*]alialiali@apps.ipb.ac.id, [2]shelvie@apps.ipb.ac.id, [3]hrahmawan@apps.ipb.ac.id
**: Penulis korenspondensi* (*corresponding author*)

***Informasi Artikel***
*Received: December 2024*
*Revised: January 2025*
*Accepted: January 2025*
*Published: February 2025*

***Abstract***

*The rapid increase in internet users has driven the development of WiFi networks, which play a crucial role in providing secure internet access, especially within Industry 4.0 and Industry 5.0 environments that rely on efficient data exchange. Penetration testing (pentest) is a vital approach for auditing and evaluating the security level of WiFi networks. Several frameworks such as PTES, PETA, and ISSAF are often used as references, although only a few are explicitly designed for WiFi networks. This study proposes a modification of the PTES framework to better align with the security characteristics of WiFi networks by providing relevant solution recommendations. The integration of the Boyer-Moore algorithm is employed as an efficient method to identify solutions for detected vulnerabilities. The implementation of this framework is demonstrated through testing the suggestion process, which produces solution recommendations based on vulnerabilities found during the pentest. The Boyer-Moore algorithm exhibits high efficiency in generating recommendations with a response time of 0.0000087 seconds.*

*Keywords: penetration testing; WiFi security; Boyer-Moore algorithm*
Kata kunci: Pengujian Penetrasi; Keamanan Jaringan WiFi; algoritma Boyer Moore.

**Abstrak**

Peningkatan pesat jumlah pengguna internet mendorong perkembangan jaringan WiFi yang sangat penting untuk menyediakan akses internet yang aman, terutama dalam lingkungan Industri 4.0 dan Industri 5.0 yang mengandalkan pertukaran data yang efisien. Pengujian penetrasi (pentest) adalah pendekatan penting dalam melakukan audit serta mengevaluasi tingkat keamanan jaringan WiFi. Beberapa framework seperti PTES, PETA, dan ISSAF kerap dijadikan acuan, meskipun hanya sebagian kecil yang secara eksplisit

*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v22i1.14767*

dirancang untuk jaringan WiFi. Penelitian ini mengusulkan modifikasi terhadap framework PTES agar lebih selaras dengan karakteristik keamanan jaringan WiFi, dengan memberikan rekomendasi solusi yang relevan. Integrasi algoritma Boyer-Moore digunakan sebagai metode yang efisien dalam mengidentifikasi solusi atas kerentanan yang ditemukan. Implementasi framework ini berhasil dibuktikan melalui pengujian dari proses suggestions, yang menghasilkan rekomendasi solusi berdasarkan kerentanan yang ditemukan selama proses pentest. Algoritma Boyer-Moore menunjukkan efisiensi tinggi dalam menghasilkan rekomendasi dengan waktu respons mencapai 0,0000087 detik.

## 1. Pendahuluan

Penggunaan teknologi digital saat ini menjadikan internet sebagai sarana utama untuk mengakses beragam layanan online. Pada tahun 2022, tercatat sebanyak 210 juta penduduk Indonesia menggunakan internet, berdasarkan data dari Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII), dari total populasi sekitar 272 juta jiwa [1]. Berbagai layanan teknologi dapat terhubung melalui internet, yang merupakan bentuk penerapan dari sistem jaringan komputer. Komputer yang saling terhubung melalui media transmisi membentuk sebuah jaringan yang memungkinkan pertukaran informasi dan pengiriman data [2]. Saat ini, penggunaan jaringan komputer atau internet sangat penting dalam mendukung operasional seperti administrasi pemerintahan, pendidikan, dan perdagangan. Implementasi sistem Industri 4.0 dan pengembangan menuju Industri 5.0 semakin memperkuat peran internet sebagai infrastruktur utama untuk memenuhi kebutuhan data yang semakin besar dan cepat [3]. Salah satu media akses internet yang umum digunakan masyarakat adalah Wireless Fidelity (WiFi). Berdasarkan data dari APJII, pada tahun 2022 terdapat sekitar 46,5 juta orang di Indonesia atau setara dengan 22,18% populasi telah menggunakan jaringan WiFi [1].

Semakin meningkatnya pemanfaatan WiFi menjadikan aspek keandalan dan keamanan jaringan sebagai hal yang sangat krusial [4]. Tingkat keamanan jaringan WiFi dapat dievaluasi menggunakan audit keamanan berbasis metode penetration testing. Pengujian penetrasi (pentest) adalah metode legal yang mensimulasikan serangan terhadap suatu sistem, termasuk tindakan akses tanpa izin dan aktivitas yang berpotensi merugikan, guna menemukan kelemahan keamanan serta menyusun strategi mitigasi yang tepat [5]. Pengujian penetrasi bertujuan untuk mengidentifikasi kelemahan dalam sistem serta menyarankan langkah-langkah perbaikan guna mengurangi potensi serangan [6].

Teknik untuk melakukan pentest ada beragam berdasarkan framework yang sudah tersedia, diantaranya ialah PTES, PETA, NIST SP 800-115, OWASP, OSSTMM, ISSAF. Framework Penetration Testing Execution Standard (PTES) telah digunakan dalam penelitian sebelumnya untuk melakukan penilaian terhadap keamanan jaringan WiFi. Penelitian ini menghasilkan informasi audit atau laporan terkait kerentanan yang diperoleh, dan juga solusi yang diberikan oleh pentester setelah menerapkan framework PTES dalam melakukan pentest jaringan [4] [7]. Selain PTES juga ada Information System Security Assessment Framework (ISSAF), penelitian

ini dilakukan pada satu institusi yang menghasilkan nilai tingkat kerentanan dari percobaan pentest yang dilakukan [2]. Contoh penelitian lain menggunakan framework ini ialah melakukan pentest terhadap jaringan wirelass LAN pada restaurant yang menyediakan akses jaringan WiFi. Penelitian ini menghasilkan informasi mengenai celah keamanan setelah dilakukan pengujian penetrasi, yang kemudian dievaluasi dengan memberikan rekomendasi solusi atas kerentanan yang ditemukan [6].

Penggunaan *framework pentest* menggunakan PTES dan ISSAF dalam melakukan audit dan menilai keamanan jaringan WiFi, sudah sangat membantu untuk memberikan pedoman kepada admin jaringan WiFi agar dapat membangun jaringan WiFi yang memiliki tingkat keamanan yang baik. Namun dari penerapan *framework pentest* membutuhkan ahli pentester yang mengerti cara memberikan solusi dari celah keamanan jaringan WiFi yang diperoleh, belum ada sistem yang menyediakan kumpulan *suggestions* sebagai solusi kerentanan yang ditemukan setelah melakukan pentest untuk dapat mempermudah dalam menanganinya. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan *framework pentest* PTES yang telah ada guna mempermudah tugas para pentester serta administrator jaringan WiFi. Dengan cara menyediakan kumpulan *suggestions* sebagai solusi dari kerentanan yang muncul pada penerapan jaringan WiFi yang digunakan. Tujuannya agar dapat mempermudah dalam membangun jaringan WiFi yang handal pada aspek keamanannya. Pada prosesnya fitur saran akan dibantu oleh algoritma pencocokan string, yang berfungsi sebagai metode pendukung dalam mencari solusi untuk kerentanan yang ditemukan. Metode string matching memungkinkan pencarian posisi atau informasi yang relevan dengan akurat [8] [9] .

Sebagai bagian dari pendukung penelitian, kajian literatur dari berbagai sumber dijalankan guna mendalami topik penelitian ini.

### 1.1. WiFi

Teknologi Wireless Fidelity atau WiFi berfungsi sebagai media jaringan yang menyediakan akses internet tanpa kabel dengan fleksibilitas yang baik [6]. WiFi *controller* berfungsi sebagai alat yang memusatkan perangkat titik WiFi atau AP agar mudah untuk di konfigurasi dan dikelola [10].

### 1.2. Penetration Testing

*Penetration testing* atau pentest merupakan metode pengujian yang melibatkan eksploitasi sistem menggunakan skenario penyerangan, seperti akses ilegal [5]. Penetrasi dilakukan ke target sistem untuk mendapatkan kontrol akses [11]. Tujuan utamanya adalah mengidentifikasi celah kerentanan yang ada dalam sistem sekaligus melakukan evaluasi terhadap keamanan jaringan guna mengurangi risiko serangan dari pelaku kejahatan [6].

### 1.3. PTES

*Penetration Testing Execution Standard*, atau yang sering disingkat PTES, adalah sebuah kerangka kerja yang dikembangkan sejak tahun 2010 untuk memberikan panduan pengujian yang sistematis dan rinci. PTES memiliki 7 tahapan inti.

#### 1.3.1. *Pre-engagement Interactions*

Proses ini melibatkan penyediaan teknik serta perangkat yang diperlukan dalam persiapan pengujian penetrasi. Informasi diperoleh dari berbagai sumber, termasuk pengalaman penguji berpengalaman. Langkah ini penting sebelum memulai pentest.

#### 1.3.2. *Intellegence Gathering*

*Intellegence Gathering* merupakan proses pengumpulan data yang membantu dalam merancang langkah tindakan berdasarkan kesepakatan dengan target.

#### 1.3.3. *Threat Modelling*

*Threat Modelling* merupakan proses identifikasi metode pemodelan ancaman yang berfokus pada proses bisnis dan aset organisasi guna menentukan risiko serta menetapkan prioritas target.

#### 1.3.4. *Vulnerability Analysis*

Mengidentifikasi kerentanan yang dapat dieksploitasi berdasarkan pemodelan ancaman.

#### 1.3.5. *Exploitation*

Fokus pada perencanaan dan pengambilan keputusan untuk mengakses titik masuk bernilai tinggi dalam sistem.

#### 1.3.6. *Post Exploitation*

Menilai nilai sistem yang dikompromikan dan memberikan rekomendasi pertahanan, termasuk identifikasi data sensitif dan konfigurasi jaringan.

#### 1.3.7. *Reporting*

Tujuan dari tahapan ini adalah menentukan nilai kerentanan dan mendokumentasikan hasil untuk pengelolaan dan mitigasi

### 1.4. Algoritma string matching

Algoritma *String Matching* merupakan metode pencarian *string* atau teks yang berguna untuk menemukan suatu posisi atau informasi yang sesuai [8] [9]. Proses kerja algoritma tersebut meliputi pencarian pola pada setiap teks yang dibandingkan dengan teks lain hingga ditemukan kecocokan sesuai dengan pola atau kata kunci yang sudah dikenali [12].

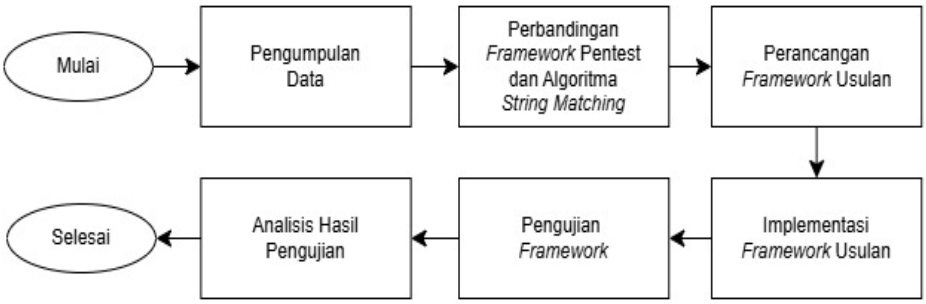
### 1.5. Boyer-moore

Algoritma *boyer-moore* merupakan algoritma *string matching* yang dikembangkan oleh Robert S.Boyer dan J.Strother Moore pada tahun 1977. Algoritma ini digunakan untuk menemukan kecocokan kata atau pola dengan pendekatan pencarian dari kanan ke kiri [13]. Algoritma *boyer-moore* menjadi sangat cepat jika string yang dicari tersebut panjang. Cara kerja algoritma ini ialah dengan melakukan pergeseran dari kanan ke kiri menggunakan aturan *good suffix* dan *bad character* pada aturan tabel *last occurrence* [14].

## 2. Metode/Perancangan

Tahapan dalam penelitian ini meliputi enam langkah pokok: pengumpulan data, membandingkan *framework* dan algoritma, merancang *framework* usulan, mengimplementasikan *framework*, melakukan pengujian, dan akhirnya menganalisis hasil pengujian. Gambar 1 merupakan diagram alur tahapan penelitian yang akan dilaksanakan.

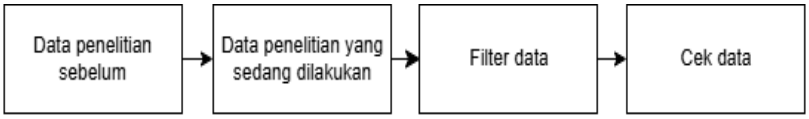
*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v22i1.14767*




**Gambar 1.** Tahapan penelitian

## 2.1. Pengumpulan data

Data penelitian ini merupakan data kumpulan solusi pada penelitian yang sudah dilakukan oleh [2] [4] [6] [7] [11] [15], serta penambahan dengan penelitian yang saat ini dilakukan. Gambar 2 menunjukkan tahapan dalam pengumpulan data penelitian. Data solusi tersebut dikumpulkan dalam bentuk *spreadsheet* dengan tujuan untuk kemudahan aksesibilitas dan mudah dimengerti oleh berbagai macam pengguna.




Gambar 2. Sub-tahapan pengumpulan data

## 2.2. Perbandingan *framework* dan algoritma

Perbandingan *framework* pentest dan algoritma *string matching* bertujuan untuk mendapatkan informasi penerapan *framework* pentest yang sudah ada, sehingga memudahkan untuk membuat perancangan usulan pengembangan *framework* pentest. Tabel 1 dan 2 merupakan hasil perbandingan *framework* pentest dan algoritma *string matching* dari hasil studi literatur.

**Tabel 1**. Perbandingan framework [16]

| No | Nama | Pembaruan | Mudah Digunakan |
|---|---|---|---|
| 1 | *PTES* | 2022 | Iya |
| 2 | *PETA* | 2016 | Iya |
| 3 | *ISSAF* | 2006 | Tidak |

**Tabel 2**. Perbandingan algoritma [8] [9]

| No | Nama | Kecepatan | Mudah Digunakan |
|---|---|---|---|
| 1 | *Brute Force* | Cukup Cepat | Iya |
| 2 | *KMP* | Cukup Cepat | Iya |
| 3 | *Boyer-Moore* | Cepat | Iya |

## 2.3. Perancangan dan Pengembangan

Pada tahapan ini melakukan pengkajian ulang pada *framework* pentest. Merumuskan ulang bagian-bagian yang dapat ditingkatkan khusus untuk penerapan jaringan WiFi agar lebih handal dalam memberikan solusi kerentanan.

### 2.4. Implementasi

Implementasi *framework* pentest dilakukan pada jaringan asli yang ada di kampus STIEMBI. Kampus tersebut menerapkan jaringan WiFi untuk mendukung sarana dan prasarana. Implementasi dilakukan dari proses 1-8 pada hasil perancangan *framework* usulan yang sudah dilakukan pada tahapan sebelumnya.

### 2.5. Pengujian

Pada tahap ini dilakukan pengujian terhadap framework pengembangan yang diusulkan untuk melakukan pentest pada jaringan WiFi. Pengujian difokuskan pada dua aspek utama, yakni pengujian fungsionalitas dan performa dari framework tersebut dalam menguji jaringan WiFi.

### 2.6. Analisis hasil pengujian

Pada tahap ini, seluruh hasil dari pengujian fungsional dan performa *framework* pentest dianalisis secara mendalam. Data berupa rekomendasi solusi akan didokumentasikan dengan keterangan asal usul solusi tersebut. Kemungkinan munculnya solusi baru juga dapat terjadi berdasarkan temuan kerentanan selama pentest. Selain itu, waktu yang dibutuhkan algoritma *string matching* Boyer-Moore dalam menemukan solusi akan dicatat sebagai bagian dari analisis hasil pengujian[17].

## 3. Hasil dan Pembahasan

Rancangan *framework* pentest untuk memudahkan pemberian rekomendasi solusi pada jaringan WiFi dengan mengembangkan *framework* yang sudah dibandingkan sebelumnya yaitu PTES. Data penelitian merupakan kumpulan data rekomendasi solusi yang berisikan teknik serangan dan solusi. Berdasarkan pengumpulan dataset, jumlah data yang dikumpulkan berjumlah 100 data solusi. Data tersebut perlu diolah dengan melakukan pra proses data agar solusi lebih mudah dilakukan pencarian menggunakan algoritma string matching boyer-moore. Pra proses ini melakukan penambahan labeling kolom pada data solusi. Proses pelabelan bertujuan untuk memperjelas data terkait teknik serangan serta solusi yang disediakan, yang mencakup kolom masalah, indikator serangan, pola, dan tingkat prioritas. Kolom masalah adalah definisi dari teknik serangan yang digunakan, kolom tanda serangan adalah ciri-ciri dari teknik serangan, kolom pattern adalah pola yang akan digunakan untuk mencocokan dengan pencarian solusi, kolom priority adalah nilai tingkat prioritas yang paling disarankan dalam solusi yang diberikan pada proses suggestions. Tabel 3 merupakan sample dari data yang sudah dikumpulkan, sedangkan Tabel 4 merupakan hasil dari pra proses data.

**Tabel 3**. Data penelitian

| No | Teknik Serangan | Solusi |
|---|---|---|
| 1 | *Evil Twin* | Memeriksa SSID dan alamat IP sebelum terhubung. |
| 2 | *WPA2 Attack* | Menggunakan WPA3 yang merupakan protokol keamanan Wi-Fi terbaru. |
| 3 | *DoS Attack* | Mengatur firewall untuk memblokir lalu lintas yang tidak sah. |

**Tabel 4**. Hasil pra proses data

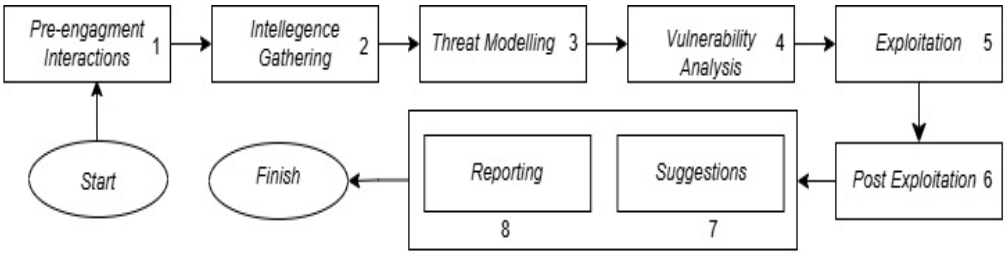
| No | Teknik Serangan | Solusi | *Labeling* | | | |
|---|---|---|---|---|---|---|
| | | | **Masalah** | **Tanda serangan** | ***Pattern*** | ***Priority*** |
| 1 | *Evil Twin* | Memeriksa SSID dan alamat IP sebelum terhubung. | Mengelabui pengguna dengan menggunakan jaringan wifi palsu. | Muncul peringatan keamanan dan koneksi tidak stabil. | evil twin | 1 |
| 2 | *WPA2 Attack* | Menggunakan WPA3 yang merupakan protokol keamanan Wi-Fi terbaru. | Mencoba memecahkan kata sandi pada jaringan WiFi dengan protokol WPA/WPA2. | Koneksi Wi-Fi tidak stabil dan aktivitas system tidak biasa. | wpa | 1 |
| 3 | *DoS Attack* | Mengatur firewall untuk memblokir lalu lintas yang tidak sah. | Menghabiskan *resource* perangkat wifi hingga mengalami kendala atau mati. | Koneksi Wi-Fi lambat atau terputus-putus. | DoS | 1 |

### 3.1. Perbandingan *framework* dan algoritma

Hasil dari perbandingan *framework* pentest dan algoritma *string matching* yang sudah dijelaskan pada bagian metode, maka *framework* PTES dipilih untuk dikembangkan karena memiliki kemudahan dan keterbaruan dibandingkan dengan *framework* lainnya. Algoritma *boyer-moore* dipilih untuk digunakan pada peningkatan *framework* pentest karena memiliki kecepatan yang baik dalam proses pencocokan *string matching*.

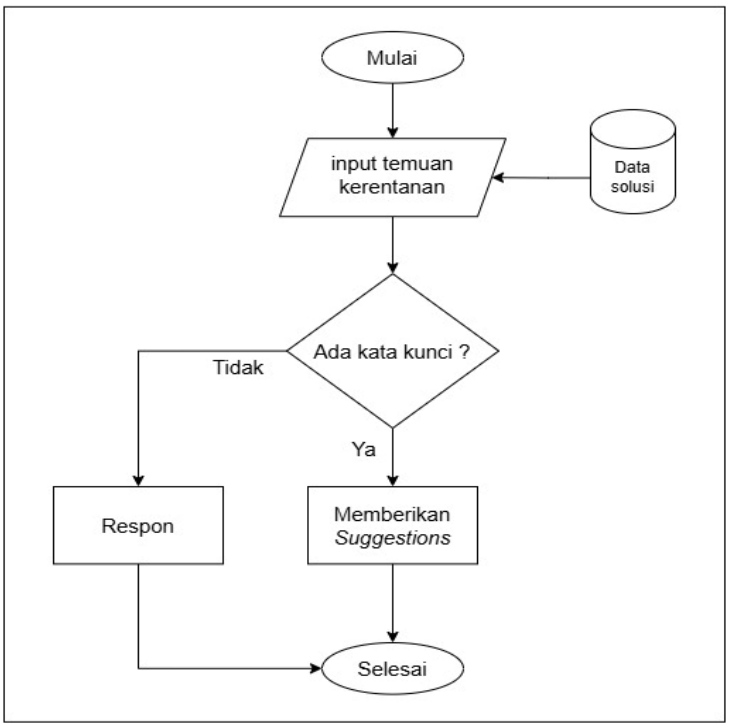
### 3.2. Perancangan dan pengembangan

Rancangan *framework* pentest untuk memudahkan pemberian rekomendasi solusi pada jaringan WiFi dengan mengembangkan *framework* yang sudah dibandingkan sebelumnya yaitu PTES. *Framework* PTES sudah sangat baik dalam penerapannya, namun tahapan untuk mempermudah dalam pemberian rekomendasi solusi belum tersedia. Sebagai solusi, dalam perancangan dan pengembangan framework pentest ini ditambahkan proses ke-7 berupa suggestions dari PTES, yang melengkapi tahapan 1 sampai 6 yang sudah diterapkan. Gambar 3 merupakan usulan perancangan dan pengembangan *framework* pentest. Gambar 4 merupakan proses dari *suggestions*.




**Gambar 3**. *Framework* usulan pengembangan

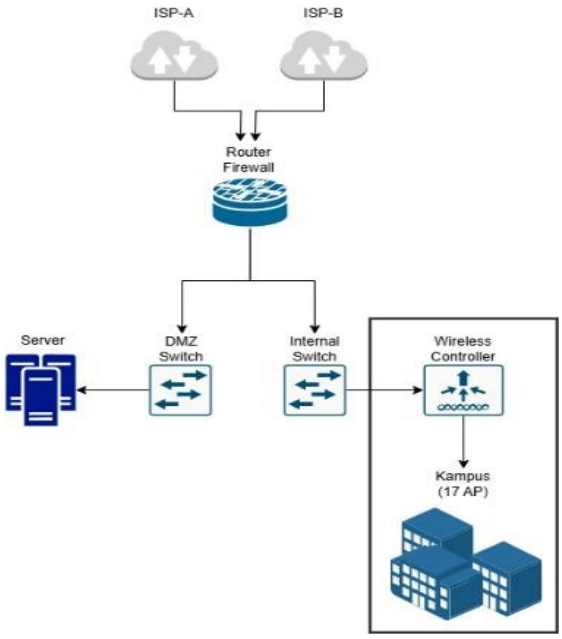
*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v22i1.14767*




**Gambar 4** .Proses *suggestions*

### 3.3. Implementasi

*Framework* usulan diterapkan di jaringan kampus. Tahapan ini mencakup semua proses termasuk *suggestions.* Hasil dari tahapan ini adalah mendapatkan rekomendasi solusi dari kerentanan keamanan jaringan WiFi yang ditemukan. Gambar 5 merupakan topologi jaringan yang digunakan.

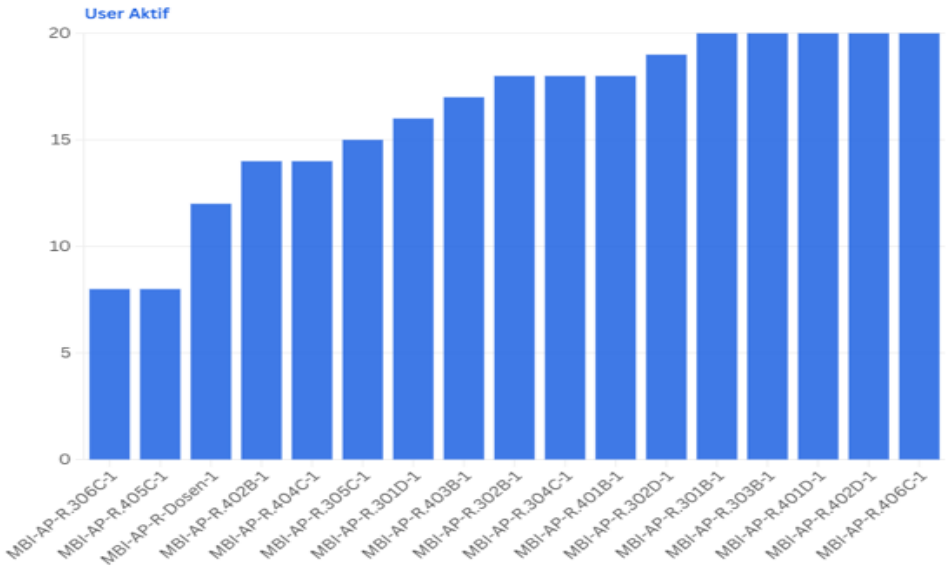



**Gambar 5**. Topologi jaringan

*ISSN: 1829-667X / E-ISSN: 2460-9021*
*DOI:10.31515/telematika.v22i1.14767*

Topologi dihasil berdasarkan hasil observasi langsung. Informasi yang didapatkan diantaranya adalah perangkat AP berjumlah 17 titik, jaringan menggunakan perangkat MikroTik dengan fitur CAPsMAN, posisi pentester berada pada area kotak hitam pada gambar sebagai titik fokus implementasi pentest.

Identifikasi tujuan dibuat diantaranya adalah melakukan evaluasi kontrol akses pada implementasi CAPsMAN, menguji ketahanan WiFi dengan serangan WPA, MITM, Deauthentication, Evil Twin, DoS, dan Bruteforce. Gambar 6 menunjukkan bahwa terdapat 200 pengguna aktif yang terhubung ke jaringan WiFi.




**Gambar 6**. Pengguna aktif

**Tabel 4** Penilaian kerentanan

| **Target** | **Jumlah** | ***Threat Level*** | | | | | |
|---|---|---|---|---|---|---|---|
| | | ***Extreme*** | ***High*** | ***Elevated*** | ***Moderated*** | ***Low*** | ***Total*** |
| *CAP-AP* | 17 | 1 | 1 | 2 | 3 | 1 | 8 |
| *CAP-Manager* | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| *Others* | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

Tabel 5 merupakan hasil dari penilaian kerentanan yang diperoleh. Hasil dari penilaian kerentanan yang diperoleh dengan *threat level* yang berbeda menunjukan bahwa implementasi jaringan WiFi pada jaringan kampus masih memungkinkan untuk diretas. Pada tabel tersebut merupakan hasil identifikasi kerentanan yang berpotensi dapat dieksloitasi hingga berdampak pada hal-hal negatif pada jaringan WiFi. Setelah nilai kerentanan diperoleh, tahap berikutnya adalah melakukan eksploitasi guna menguji efektivitas dari kerentanan yang ditemukan. Seluruh eksploitasi berhasil dilakukan, kecuali pada teknik serangan DoS yang tidak menunjukkan hasil. Langkah selanjutnya adalah mencari solusi dari kerentanan yang berhasil dieksploitasi, yaitu wpa2, MITM, *evil twin*, *deauthentication*, dan *bruteforce*.

### 3.4. Pengujian

Hasil dari pengujian fungsionalitas adalah berhasil mendapatkan rekomendasi solusi dari pencarian sebanyak 10x dengan beragam pertanyaan. Hasil dari pengujian performansi adalah mendapatkan waktu kecepatan selama proses pencarian solusi berlangsung, nilai rata-rata yang diperoleh oleh algoritma *boyer-moore* dalam melakukan pencarian solusi adalah 0.0000087s.

### 3.5. Analisis hasil pengujian

Pada tahap terakhir, dilakukan analisis hasil pengujian dari dua tahap pengujian yang dilakukan sebelumnya pada pengujian fungsionalitas dan pengujian performansi. Percobaan untuk menguji fungsionalitas dalam menemukan rekomendasi solusi kerentanan menunjukkan hasil yang berhasil. Teks yang digunakan harus memuat pola sesuai dengan yang ditetapkan oleh algoritma Boyer-Moore, karena tanpa pola tersebut pencarian tidak membuahkan hasil. Dari 10 variasi pertanyaan yang dicoba, semuanya memberikan data solusi yang hampir identik.

Rekomendasi solusi perbaikan yang tidak berasal dari penelitian yang sudah ada merupakan rekomendasi baru yang dihasilkan dari ujicoba praktik yang sudah dilakukan oleh peniliti selama melakukan ujicoba pentest dengan berbagai temuan celah dan teknik kerentanan pada jaringan WiFi. Solusi yang direkomendasikan tidak dapat diimplementasikan karena lingkungan jaringan WiFi saat ini sudah berbeda dari kondisi awal saat penelitian dilakukan.

Pada pengujian performansi percobaan untuk melihat performa kecepatan dalam melakukan proses pencarian data solusi. Hasil rata-rata nilai yang diperoleh menggunakan algoritma *boyer-moore* adalah 0.0000087s dari pengujian pencarian data solusi dengan 10 kali pertanyaan beragam pada *sample* pencarian kerentanan teknik serangan wpa.

## 4. Kesimpulan dan Saran

### 4.1. Kesimpulan

Sistem *suggestions* menjalankan pencocokan pola berdasarkan permintaan solusi yang diajukan oleh pentester. Tujuan utama dari pengembangan *framework pentest wifi* adalah memudahkan pentester untuk mencari rekomendasi solusi perbaikan kerentanan WiFi. Penelitian ini menerapkan algoritma string matching Boyer-Moore sebagai pendekatan dalam metode pencarian solusi yang direkomendasikan. Algoritma *boyer-moore* merupakan *exact string matching* yang di dalam prosesnya harus menyertakan pola kata kunci agar pencarian dapat berhasil ditemukan, sehingga dalam pencocokan pola sangat mungkin gagal jika tidak cocok dalam pola yang sudah ditentukan.

Pengembangan framework untuk kebutuhan pengujian penetrasi pada jaringan WiFi telah berhasil diselesaikan. Keberhasilan ini ditunjukkan oleh hasil uji fungsionalitas pada fitur saran, yang dapat mempermudah proses pemberian rekomendasi solusi terhadap kerentanan yang teridentifikasi selama pentest. Hasil performa evaluasi waktu kecepatan perolehan pada algoritma *boyer-moore* ialah 0.0000087s, dalam hal ini penggunaan algoritma *boyer-moore* dapat dihandalkan untuk mencari kecepatan dalam *exact string matching*.

### 4.2. Saran

Penggunaan algoritma exact string matching dalam hal ini *boyer-moore* dapat ditingkatkan atau digantikan dengan metode yang lebih baik dalam memudahkan pencarian data solusi agar dapat meminimalisir kegagalan dalam jumlah data yang besar dan beragam. Kecerdasan buatan dapat

menjadi pilihan strategis untuk menurunkan risiko kesalahan atau ketidaksesuaian dalam proses pencarian solusi, seperti dengan penerapan teknik fuzzy partial matching dan lainnya.

Keberagaman strategi serangan membuat proses pemberian solusi perbaikan menjadi lebih kompleks. Data solusi pentest perlu ditambahkan mengikuti perkembangan teknik serangan yang beragam tersebut, dan jika semakin besar data solusi tersebut dapat dikategorikan menjadi lebih spesifik agar memudahkan dalam pengelolaan data dalam jumlah yang lebih banyak. Penggunaan sistem manajemen basis data, baik berbasis SQL maupun Non-SQL, dapat dijadikan opsi ketika solusi memerlukan pengelolaan data yang besar dan kompleks.

Metode pencarian rekomendasi solusi atau *suggestions* diharapkan bisa lebih praktis dalam memberikan solusi perbaikan atau secara otomatis dapat membaca kerentanan pada jaringan WiFi seperti halnya penerapan intrusion *detection system* atau dikenal sebagai IDS dan juga penerapan *intrusion prevention system* atau dikenal sebagai IPS.

## Daftar Pustaka

[1] APJII, "Profil Internet Indonesia 2022," APJII, Jakarta, 2022.

[2] M. Rusdan, D. T. H. Manurung and F. K. Genta, "Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia)," *TEST: Enginering & Management*, vol. 83, no. May - June 2020, p. 15714 – 15719 , 2020.

[3] B. Meindl and J. Mendonça, "Mapping Industry 4.0 Technologies: From Cyber-Physical Systems to Artificial Intelligence," vol. 1, pp. 1-32, November 2021.

[4] F. Z. Lidanta, A. Almaarif and A. Budiyono, "Vulnerability Analysis of Wireless LAN Networks Using Penetration Testing Execution Standard: A Case Study of Cafes in Palembang," in *2021 International Conference on ICT for Smart Society (ICISS)*, Bandung, Indonesia, 2021.

[5] T. S. Gunawan, M. K. Lim, M. Kartiwi, N. A. Malik and N. Ismail, "Penetration Testing using Kali Linux: SQL Injection, XSS, Wordpres, and WPA2 Attacks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 729-737, November 2018.

[6] J. A. Pratama, A. Almaarif and A. Budiono, "Vulnerability Analysis of Wireless LAN Networks using ISSAF WLAN Security Assessment Methodology: A Case Study of Restaurant in East Jakarta," in *2021 4th International Conference of Computer and Informatics Engineering (IC2IE)*, Depok, Indonesia, 2021.

[7] D. N. Astrida, A. R. Saputra and A. I. Assaufi, "Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES)," *Sinkron: Jurnal dan Penelitian Teknik Informatika*, vol. 6, no. 1, pp. 147-154, Januari 2021.

[8] A. G. M. Sanjung and N. , "Analysis of Chatbot Response Constancy Using Boyer Moore Algorithm," *SISTEMASI: Jurnal Sistem Informasi*, vol. 11, no. 1, pp. 207-222; https://doi.org/10.32520/stmsi.v11i1.1728, 2022.

[9] S. R. Cakrawijaya and B. Kriswantara, "Perbandingan KInerja Algoritma String Matching Boyer-Moore & Knuth_Morris-Pratt pada Seo Web Server," *Komputasi: Jurnal Ilmiah Ilmu Komputer dan Matematika*, vol. 18, no. 2, pp. 97-102, 2021.

[10] I. Koulouras, I. Bobotsaris, S. V. Margariti, E. Stergiou and a. Stylios, "Assessment of SDN Controllers in Wireless Environment Using a Multi-Criteria Technique," vol. 14, no. 9, pp. 1-16, 28 Agustus 2023.

[11] H.-J. Lu and Y. Yu, "Research on WiFi Penetration Testing with Kali Linux," no. 1, pp. 1-8, 27 Februari 2021.

[12] C. F. Irawan and M. R. Pratama, "Perbandingan Algoritma Boyer-Moore dan Brute Force pada Pencarian Kamus Besar Bahasa Indonesia Berbasis Android," *BIOS: Jurnal teknologi Informasi dan Rekayasa Komputer*, vol. 1, no. 2, p. doi: https://doi.org/10.37148/bios.v1i2.13, September 2020.

[13] R. Rahim, A. S. Ahmar, A. P. Ardyanti and D. Nofriansyah, "Visual Approach of Searching Process using Boyer-Moore Algorithm," in *International Conference on Information and Communication Technology (IconICT)* , 2017.

[14] F. Fitriyah, W. R. P. Gayo, A. N. Handayani, A. P. Wibawa and F. Kurniawan, "The Implementation of Boyer-Moore Algorithm in WEB Based Computer and Informatic Terms Dictionary," in *2020 4th International Conference on Vocational Education and Training (ICOVET)*, Malang, Indonesia, 2020.

[15] S.-L. Wang, J. Wang, C. Feng and Z.-P. Pan, "Wireless Network Penetration Testing and Security Auditing," in *3rd Annual International Conference on Information Technology and Applications (ITA 2016)*, 2016.

[16] T. Klíma, "PETA: Methodology of Information Systems Security Penetration Testing," *Acta Informatica Pragensia*, vol. 5, no. 2, pp. 98-117, 2016.

[17] A. Halbouni, L.-Y. Ong and L. M. Chew, "Wireless Security Protocols WPA3: A Systematic Literature Review," pp. 1-13, doi: 10.1109/ACCESS.2023.3322931, Januari 2023.