Journal of Informatics and Computer Science Vol. 11 No. 2 Oktober 2025
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

ANALISIS RISIKO KEAMANAN *WI-FI.ID MANAGE SERVICE (WMS)* PADA JARINGAN PUBLIK DENGAN TEKNIK *SNIFFING*

SECURITY RISK ANALYSIS OF WI-FI.ID MANAGE SERVICE (WMS) ON PUBLIC NETWORKS USING SNIFFING TECHNIQUE

Tomy Mulia Hasan[1], Rizka Albar[2], Desita Ria Yusian TB[3], M Bayu Wibawa[4]
[1,2,]Jurusan Sistem Informasi, [3-4]Informatika, Fakultas Sains dan Teknologi, Universitas Ubudiyah Indonesia, Banda Aceh
E-mail : [1] tomy.mulia.hasan@gmail.com ,[2]albar@uui.ac.id,[3]desita@uui.ac.id, [4]mbayuw@uui.ac.id

Abstrak - *WiFi.id Manage Service (WMS)* merupakan layanan jaringan publik yang banyak digunakan oleh masyarakat untuk mengakses internet. Namun, penggunaan jaringan publik memiliki risiko keamanan yang tinggi, terutama terkait dengan serangan *sniffing*, autentikasi yang tidak aman, dan eksploitasi port terbuka. Penelitian ini bertujuan untuk menganalisis tingkat keamanan jaringan *WiFi.id Manage Service (WMS)* melalui metode komparatif dengan pendekatan kuantitatif. Pengujian dilakukan dalam kondisi trafik tinggi, yaitu mulai pukul 17.00 WIB, menggunakan berbagai teknik, termasuk pemindaian *IP Address*, *sniffing* paket data dengan *Wireshark*, *port scanning* dengan *Nmap*, dan analisis autentikasi pengguna. Hasil penelitian menunjukkan bahwa sebanyak 65% lalu lintas jaringan masih menggunakan *protokol* HTTP, yang rentan terhadap penyadapan, sedangkan 35% menggunakan HTTPS, yang lebih aman karena terenkripsi. Pengujian *port scanning* mengungkapkan bahwa beberapa perangkat memiliki *port* sensitif terbuka, seperti *port* 22 (SSH) dan 3389 (RDP), yang dapat menjadi target serangan. Selain itu, ditemukan bahwa 50% pengguna masih menggunakan autentikasi berbasis HTTP yang tidak terenkripsi, sementara 30% menggunakan HTTPS dan 20% menggunakan VPN untuk meningkatkan keamanan. Berdasarkan hasil temuan ini, dapat disimpulkan bahwa jaringan *WiFi.id Manage Service (WMS)* masih memiliki beberapa celah keamanan yang dapat dieksploitasi. Untuk meningkatkan keamanan jaringan, disarankan untuk mewajibkan penggunaan HTTPS dan SSL/TLS, menerapkan DNS *over* HTTPS (DoH) atau DNS *over* TLS (DoT), menutup atau mengamankan *port* terbuka yang tidak diperlukan, serta menyarankan pengguna untuk menggunakan VPN saat mengakses jaringan publik. Dengan penerapan rekomendasi tersebut, diharapkan tingkat keamanan *WiFi.id Manage Service (WMS)* dapat meningkat dan risiko eksploitasi jaringan dapat diminimalkan.

Kata Kunci : Keamanan Jaringan, *WiFi.id Manage Service (WMS)*, *Sniffing*, HTTP, HTTPS, *Port Scanning*, VPN.

Abstract - Public Wi-Fi networks, such as WiFi.id Manage Service (WMS), are widely used but often pose significant security risks due to their open nature. This research aims to evaluate the security vulnerabilities of WMS through various network security testing methods, including IP address identification, port scanning, sniffing (HTTP/HTTPS traffic analysis), and authentication security assessments. Testing was conducted during peak usage hours (starting at 17:00 WIB) to observe network activity under high traffic conditions. The results revealed that 65% of network traffic still used HTTP, exposing sensitive user credentials to potential interception, while only 35% of traffic was encrypted using HTTPS. Additionally, port scanning detected multiple open ports (e.g., SSH, RDP, SMB), which could serve as entry points for cyber threats. The authentication analysis showed that 50% of users relied on unencrypted HTTP-based login portals, making them vulnerable to man-in-the-middle (MITM) attacks. Based on these findings, several security enhancements are recommended, including enforcing HTTPS and SSL/TLS encryption, implementing secure DNS over HTTPS (DoH), closing or securing unnecessary open ports, and promoting VPN usage among users. These measures can significantly improve the security posture of WiFi.id Manage Service (WMS) and mitigate risks associated with public network usage.

Keywords: *WiFi.id Manage Service (WMS), Network Security, Sniffing, Port Scanning, Authentication, Public Wi-Fi*

I. PENDAHULUAN

Di era digital yang semakin berkembang, jaringan internet menjadi kebutuhan utama bagi berbagai sektor, termasuk pemerintahan, perusahaan, dan industri jasa. Salah satu bentuk pemanfaatan internet yang paling umum adalah penyediaan akses *Wi-Fi* publik, yang banyak digunakan di tempat-tempat umum seperti pusat perbelanjaan, kampus, perkantoran, dan kafe. Keberadaan *Wi-Fi* publik memungkinkan pengguna untuk tetap terhubung dengan internet guna mendukung aktivitas pekerjaan, pembelajaran, serta hiburan.

Salah satu layanan *Wi-Fi* publik yang banyak digunakan adalah *Wi-Fi.id Manage Service (WMS)*, yang disediakan oleh penyedia layanan internet (ISP) untuk memudahkan pengguna dalam mengakses jaringan internet secara luas. Infrastruktur jaringan ini umumnya menggunakan kabel serat optik sebagai media transmisi utama yang terhubung ke modem atau *access point*. Meskipun memberikan kemudahan akses, jaringan publik seperti *Wi-Fi.id Manage Service (WMS)* memiliki risiko keamanan yang tinggi, terutama dalam aspek perlindungan data pengguna.

Pada dasarnya, jaringan yang terhubung ke internet rentan terhadap berbagai ancaman siber, salah satunya adalah serangan *sniffing*. *Sniffing* merupakan teknik penyadapan yang memungkinkan pihak tidak bertanggung jawab untuk menangkap, membaca, atau bahkan memodifikasi data yang dikirimkan melalui jaringan. Ancaman ini dapat terjadi ketika pengguna

melakukan autentikasi pada situs web atau aplikasi, di mana informasi yang dikirim melalui jaringan dapat dicegat oleh peretas untuk mencuri kredensial, mengakses informasi sensitif, atau menyebarkan malware. Serangan *sniffing* dapat terjadi baik pada jaringan Local Area Network (LAN) maupun jaringan Wireless Fidelity (*Wi-Fi*) yang menggunakan *access point* publik.

Meskipun keamanan jaringan menjadi faktor yang sangat penting, hingga saat ini masih banyak layanan *Wi-Fi* publik yang belum memiliki sistem perlindungan yang optimal terhadap ancaman *sniffing*. Selain itu, belum banyak penelitian yang secara khusus menguji tingkat keamanan jaringan *Wi-Fi.id Manage Service (WMS)* dalam menghadapi ancaman ini. Oleh karena itu, diperlukan pengujian dan analisis terhadap risiko keamanan yang mungkin terjadi dalam jaringan tersebut agar dapat memberikan pemahaman lebih mendalam tentang tingkat kerentanannya serta langkah-langkah mitigasi yang diperlukan.

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan judul "Analisis Risiko Keamanan *Wi-Fi.id Manage Service (WMS)* pada Jaringan Publik dengan Teknik *Sniffing*". Penelitian ini bertujuan untuk mengidentifikasi risiko keamanan jaringan *Wi-Fi.id Manage Service (WMS)* yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab melalui metode *sniffing*. Dengan menggunakan perangkat lunak Wireshark, penelitian ini akan menguji kemungkinan penyadapan data dalam jaringan publik serta menganalisis potensi ancaman yang dapat terjadi. Diharapkan hasil penelitian ini dapat memberikan rekomendasi terhadap peningkatan sistem keamanan jaringan guna meminimalkan risiko serangan *sniffing* dan melindungi pengguna *Wi-Fi* publik dari ancaman kejahatan siber.

II. STUDI PUSTAKA

A. *Internet Service Provider* (ISP)

Internet Service Provider (ISP) berasal dari kata internet yang dapat diartikan sebagai hubungan antara komputer satu dengan komputer lainnya yang membentuk sistem jaringan hingga seluruh dunia. Sedangkan kata *service* dalam bahasa Indonesia berarti layanan atau jasa. Maka dari itu pengertian ISP adalah penyedia layanan internet. Yakni suatu perusahaan yang bergerak dalam bidang jasa pelayanan internet untuk menghubungkan antara komputer pengguna dengan jaringan internet. ISP ini, memiliki infrastruktur telekomunikasi yang terkoneksi ke internet. Yang mana nantinya ISP tersebut akan membagi kapasitas koneksi internet miliknya kepada para pelanggan yang juga membutuhkan jasa koneksi internet (Savala Rizki Ramadhan, 2022).

B. Jenis Layanan *Internet Service Provider* (ISP)

Menurut Savala Rizki Ramadhan, 2022. Masyarakat belum mengenal apa ISP itu sesungguhnya. Masyarakat menganggap ISP adalah pelayanan internet secara umum saja, namun pada kenyataannya banyak jenis layanan ISPyang belum diketahui masyarakat secara terperinci. Adapun jenis layanan ISP antara lain seperti:

a. *Dial-Up Connection*
   Dial-up connection merupakan jenis layanan internet yang menggunakan modem dan kabel telepon untuk terhubung ke internet. Pada umumnya akses dial-up ini digunakan di warnet. Jenis ini sudah jarang diminati masyarakat di zaman sekarang, sebab gaya hidup masyarakat semakin tinggi dan warnet sudah mulai jarang peminatnya lagi.
b. *Dedicated Connection*
   Ialah jenis koneksi yang menetap 24 jam. Adapun jenis layanan internet ini banyak digunakan oleh perusahaan atau sebuah tempat yang banyak menggunakan koneksi internet dan digunakan oleh komputer dengan jumlah yang banyak pula. Berbeda dengan yang lain, sebab biasanya jenis *Internet Service Provider* ini umum digunakan pada perusahaan yang mempunyai jumlah karyawan yang besar dan memiliki komputer yang banyak.
c. Internet *Wireless*
   Wireless ialah salah satu jenis layanan internet yang dalam menggunakannya sudah tanpa bantuan sebuah kabel. Layanan akses internet ini tidak dipungut biaya telepon, namun hanya dikenakan tarif pemakaian internetnya saja. Sebagian besar masyarakat pengguna sekarang ini lebih suka memakai jenis ini karena dirasa lebih praktis dan efesien.
d. Internet *Mobile Acces*
   Ialah layanan ISP yang diperuntukkan bagi para pengguna perangkat telepon genggam dimana pengguna bisa terhubung ke internet melalui perangkat yang mereka masing-masing miliki. Jenis ISP ini paling banyak dipakai untuk akses internet pada telepon genggam yang mendukung GSM maupun CDMA.

C. Kelebihan dan Kelemahan *Internet Service Provider* (ISP

Menurut M Isma'atul Mazidah, 2022. *Internet Service Provider* yang digunakan adalah jenis *wireless*. Adapun kelebihan *Internet Service Provider Wireless* antara lain:

a. Kecepatan internet lebih cepat dan stabil. Apabila menghubungkan
   perangkat dengan internet memakai paket data, maka akan memiliki keterbatasan akses dengan batasan *gigabyte* yang dimiliki oleh seseorang. Penggunaan ISP *wireless* ini koneksi yang dihasilkan lebih cepat dan stabil dibandingkan internet dengan paket data.
b. Tidak bergantung pada kabel. ISP *wireless* dalam hal
   menghubungkan user dengan router sudah tidak menggunakan kabel, tidak seperti sistem

pemasangan internet dengan cara lama yang mana harus memiliki perangkat yang tersambung pada kabel yang menghubungkannya dengan jaringan internet.

c. Dapat digunakan pada perangkat manapun.
ISP dengan jenis *wireless* ini tidak hanya dikhususkan pada *smartphone* saja ataupun perangkat komputer saja. Menggunakan ISP jenis *wireless* ini jaringan internet dapat terkoneksi dengan berbagai jenis perangkat, mulai dari komputer, tablet, hingga smartphone, bahkan tidak akan bergantung pada spesifikasinya.

Selanjutnya Menurut M Isma'atul Mazidah, 2022. Mengenai kekurangan *Internet Service Provider*. *Wireless* di antaranya adalah:

a. Rawan terkena *hack*. Kekurangan pada ISP *wireless* ialah mudahnya perangkat untuk terkena *hack* oleh beberapa orang di sekitar yang juga memerlukan internet. Dimana untuk beberapa orang yang paham akan internet akan mudah untuk mengakses sebuah jaringan *Wi-Fi* milik beberapa orang di sekitarnya tanpa izin terlebih dahulu.
b. Jika sinyal drop akses internet akan terganggu. Sinyal yang drop ini bisa disebabkan oleh beberapa hal, salah satunya adalah cuaca yang buruk sehingga jaringan internet menjadi lebih lambat untuk terhubung ke perangkat. Kemudian cuaca buruk seperti petir atau angin kencang, di beberapa kejadian menyebabkan kabel LAN putus atau listrik padam menjadikan jaringan internet *wireless* ini ikut padam.
c. Keterbatasan jarak. Walaupun jenis layanan internet ini sudah tanpa kabel, ternyata internet dengan sistem *wireless* ini, yakni sebuah perangkat tidak akan memiliki akses ke internet apabila berada di lokasi ruangan yang berjauhan dengan *router* yang terpasang.
d. Penggunaan *user* dalam jumlah banyak dalam satu *router* akan menghambat kecepatan koneksi internet. Hal ini dikarenakan apabila dalam satu *router* tersambung banyak perangkat, maka koneksi yang didapatkan juga berebutan satu sama lain.

D. *Wi-Fi.id Manage Service* (WMS)

Wi-Fi.id Manage Service (WMS) adalah layanan yang disediakan oleh *Wi-Fi.id* untuk mengelola konektivitas dan akses pengguna ke jaringan *Wi-Fi* secara lebih efisien dan aman. Layanan ini dirancang untuk memudahkan pengelolaan jaringan *Wi-Fi* di berbagai lingkungan, baik itu di perusahaan, institusi pendidikan, tempat umum, maupun kawasan komersial. Berikut adalah komponen utama dan manfaat dari *Wi-Fi.id Manage Service* (WMS)

E. Komponen Utama WMS

a. Portal Pengelolaan:
- **Dashboard Sentral**: Memberikan tampilan keseluruhan dari jaringan *Wi-Fi*, termasuk status koneksi, perangkat yang terhubung, dan penggunaan bandwidth.
- **Konfigurasi Jaringan**: Memungkinkan administrator untuk mengatur parameter jaringan seperti SSID, kebijakan keamanan, dan prioritas bandwidth.

b. Autentikasi dan Keamanan:
- ***Single Sign-On (SSO)***: Memungkinkan pengguna untuk mengakses berbagai layanan *Wi-Fi* tanpa perlu login berulang kali.
- ***Two-Factor Authentication (2FA)***: Menambahkan lapisan keamanan dengan memerlukan verifikasi kedua selain kata sandi.
- ***Enkripsi Data***: Mengamankan data yang dikirim melalui jaringan *Wi-Fi* dengan protokol enkripsi terbaru.

c. Kontrol Akses Pengguna:
- ***Role-Based Access Control***: Menyediakan hak akses yang berbeda berdasarkan peran pengguna, seperti administrator, pengguna biasa, atau tamu.
- **Manajemen Akses Tamu**: Menyediakan akses sementara dan aman bagi tamu melalui portal pendaftaran mandiri.

d. Manajemen Perangkat:
- **Profiling Perangkat**: Mengidentifikasi perangkat berdasarkan karakteristik unik untuk manajemen yang lebih baik.
- **Dukungan *BYOD***: Memungkinkan pengguna untuk menghubungkan perangkat pribadi mereka dengan aman ke jaringan.

e. Monitoring dan Analitik:
- ***Monitoring Real-Time***: Memantau aktivitas jaringan secara real-time untuk mendeteksi dan mengatasi masalah dengan cepat.
  - **Laporan Penggunaan**: Memberikan laporan terperinci tentang penggunaan jaringan, perangkat yang terhubung, dan pola konsumsi bandwidth.

F. Manfaat WMS

a. **Pengelolaan yang Terpusat**: Memudahkan administrator jaringan dalam mengelola dan memantau seluruh aspek jaringan *Wi-Fi* dari satu titik pusat.
b. **Keamanan yang Lebih Baik**: Dengan fitur autentikasi dan enkripsi, jaringan *Wi-Fi* menjadi lebih aman dari ancaman luar.
c. **Kemudahan Akses untuk Pengguna**: Pengguna dapat dengan mudah mengakses

jaringan *Wi-Fi* dengan proses login yang sederhana dan aman.

d. **Kontrol yang Lebih Baik atas Akses Pengguna**: Memungkinkan pengaturan hak akses yang lebih fleksibel dan sesuai dengan kebutuhan masing-masing pengguna atau kelompok pengguna.

e. **Peningkatan Pengalaman Pengguna**: Menyediakan koneksi yang stabil dan cepat, serta mengurangi gangguan dan downtime jaringan.

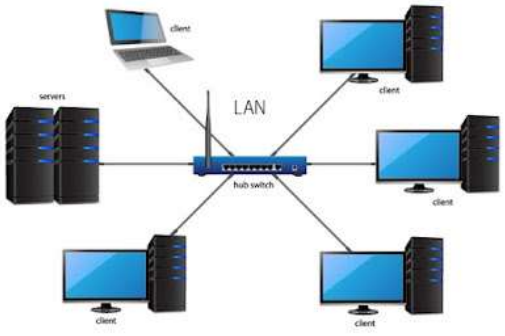
Dengan *Wi-Fi.id Manage Service*, organisasi dapat memastikan bahwa jaringan *Wi-Fi* mereka dikelola dengan cara yang aman, efisien, dan user-friendly, memberikan pengalaman terbaik bagi pengguna sekaligus menjaga integritas dan keamanan jaringan. https://*Wi-Fi*.id/bisnis Diakses, pukul 21.38 WIB pada tanggal 2 Juni 2024.

G. Jaringan Komputer

Jaringan komputer (*computer network)* dapat diartikan sebagai dua atau lebih komputer yang dihubungkan dengan sebuah sistem komunikasi. Jaringan komputer menggunakan teknik komunikasi data namun lebih mementingkan arti dari tiap bit dalam proses pengiriman hingga diterima oleh tujuannya.

Pada awalnya komputer didefinisikan sebagai sistem yang terdiri dari perangkat keras dan perangkat lunak dan manusia sebagai brainwarenya. Namun demikian saat ini sebuah sistem komputer didefinisikan sebagai perangkat keras, perangkat lunak dan jaringan, serta manusia yang tetap berdiri sebagai pengelola yang membangun sistem, memberikan perintah, dan menjaganya, (Fatma Suhaila, 2019).

Dua unit komputer dikatakan terhubung atau terkoneksi apabila keduanya bisa saling bertukar informasi dan berbagi data, berbagi *resource* yang dimiliki, seperti file, printer, media penyimpanan *(Hardisk, floppy disk, cd-room, flash disk, dll).* Data yg berupa teks, audio, maupun video bergerak melalui media kabel atau tanpa kabel sehingga memungkinkan pengguna perangkat komputer dapat saling bertukar data/*file*, mencetak data dengan printer yang sama dan menggunakan *hardware* dan *software* yang terkoneksi dalam jaringan yang sama.



Gambar 1. Jaringan komputer

H. Komponen Jaringan Komputer

Adapun komponen jaringan computer yang digunakan antara lain :

a. Modem

Modem berasal dari singkatan *Modulator Demodulator*. *Modulator* merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa *(carrier)* dan siap untuk dikirimkan, sedangkan *Demodulator* adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik . Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah (Rian Okta Putra, 2021).

Gambar 2. Modem

I. *IP Address*

IP *address* adalah alamat logika yang diberikan ke peralatan jaringan yang menggunakan protokol TCP/IP. IP *address* terdiri dari 32 bit angka *binary*, yang ditulis dalam empat kelompok terdari dari 8 bit (oktat) yang dipisah oleh tanda titik (Rian Okta Putra, 2021).

Contohnya:

11000000.00010000.00001010.00000001

Atau dapat ditulis dalam bentuk empat kelompok format desimal (0-
255) misalnya :

192.16.10.1

Baik bilangan *binary* dan desimal merepresentasikan nilai yang sama. Namun IP *address* lebih mudah dimengerti dalam notasi bilangan desimal. Salah satu masalah dengan penggunaan bilangan *binary* adalah pengulangan bilangan 0 dan 1 yang panjang akan membuat kesempatan terjadi kesalahan semakin besar (Rian Okta Putra, 2021).

IP *address* yang terdiri atas 32 bit angka dikenal sebagai IP versi 4 (IPv4). IP *address* terdiri atas dua bagian yaitu *network ID* dan *host* ID, dimana *network* ID menentukan alamat jaringan sedangkan *host* ID menentukan alamat *host* atau komputer. Oleh sebab itu, IP *address* memberikan alamat lengkap suatu komputer berupa gabungan alamat jaringan dan alamat *host.*

Berapa jumlah kelompok angka yang termasuk *network* ID dan berapa yang termasuk *host* ID adalah bergantung pada kelas IP *address* yang dipakai (Rian Okta Putra, 2021).

a. Pembagian *Class* IP *Addressing*

IP *address* dapat dibedakan menjadi lima kelas, yaitu A, B, C, dan D, (Mansfield,2002,p134). Dalam hal ini kelas A, B, dan C digunakan untuk *address* biasa. Sedangkan kelas D untuk *multicasting* (224.0.0.0-239.255.255.255) (Rian Okta Putra, 2021).

1. Class* A *address

Class A didesain untuk men*support network* yang besar, dengan jumlah lebih dari 16 juta *host address* yang tersedia. IP *address Class* A hanya menggunakan oktet yang pertama untuk menunjukkan *network address*, dan tiga oktet sisanya tersedia untuk *host address*.

Bit pertama dari *Class* A *address* adalah 0. Dengan bit pertama adalah 0 maka angka terendah yang dapat direpresentasikan adalah 00000000 dalam bilangan biner sedangkan dalam bilangan desimal adalah 0. Dan angka tertinggi yang dapat direpresentasikan adalah 01111111 dalam bilangan biner dan dalam bilangan desimal adalah 127. Angka 0 dan 127 tidak dapat digunakan, serta IP *address* 127.0.0.0 tidak dapat digunakan karena dipakai untuk *loopback testing*, maka alamat IP *address* yang oktet pertamanya yang dimulai dengan angka antara 1 sampai 126 di dalam oktet pertama adalah alamat *Class* A (Rian Okta Putra, 2021).

2. Class B address

Class B *address* didesain untuk men*support* kebutuhan jaringan dengan ukuran menengah sampai dengan ukutan besar. Sebuah IP *address Class* B menggunakan dua oktet pertama dari empat oktet untuk menunjukkan *network address*, dan sisanya menunjukkan *host address*.

Dua bit pertama dari oktet pertama *Class* B selalu 10. Sisa dari enam bit berikutnya diisi baik oleh 0 dan 1, oleh karena itu angka terendah yang dapat direpresentasikan dalam bilangan biner adalah 10000000 dan dalam bilangan desimal adalah 128, sedangkan angka tertinggi yang dapat direpresentasikan dalam bilangan biner adalah 10111111 dan dalam bilangan desimal adalah 191. *Address* IP yang oktet pertamanya dimulai dengan angka 128-191 adalah alamat *Class* B (Rian Okta Putra, 2021).

3. Class C address

Class C *address* adalah kebanyakan yang dipakai untuk alamat *address* yang sebenarnya. Alamat ini dimaksudkan untuk men*support* jaringan kecil dengan jumlah maksimum 254 *host*. (Nanang Khaerul Anwar, 2010)

Class C *address* dimulai dengan bilangan binary 110. Oleh karena itu, angka terendah yang dapat direpresentasikan adalah 11000000 dalam bilangan *binary* dan dalam bilangan desimal adalah 192 sedangkan angka tertinggi yang dapat direpresentasikan adalah 11011111 dalam bilangan *binary* dan dalam bilangan desimal adalah 223. *Address* IP yang oktet pertamanya dimulai dengan angka 192 – 223 adalah alamat *Class* C (Rian Okta Putra, 2021).

4. Class D address

Class D *address* diciptakan untuk memungkinkan *multicasting* di dalam suatu IP *address*. *Multicast address* adalah *network address* unik yang menunjukkan paket dengan *address* tujuan ke *group predefined* dari sebuah IP *address*, oleh karena itu *single unit* dapat *mentransmit* aliran tunggal dari data secara *simultan* ke penerima lebih dari satu. (R.Fitria, 2020)

Class D *address* dimulai dengan bilangan *binary* 1110. Oleh karena itu, angka terendah yang dapat direpresentasikan adalah 11100000 dalam bilangan *binary* dan dalam bilangan desimal adalah 224 sedangkan angkat tertinggi yang dapat direpresentasikan adalah 11101111 dalam bilangan *binary* dan dalam bilangan desimal adalah 239. *Address* IP yang oktet pertamanya dimulai dengan angka 224 – 239 adalah alamat *Class* D (Rian Okta Putra, 2021).

J. Ancaman Keamanan Jaringan Komputer

Keamanan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer: penyalah gunaan informasi *Internet of Things*, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer. (Z. Munawar dan N.I.Putri, 2020)

Pertama Kesalahan Informasi *Internet of Things*, Biasanya, dalam proses menggunakan komputer, banyak pengguna lebih tenang saat mengklik situs web dan mengunduh gambar, *file*, dan sebagainya, dan tidak akan digunakan setelah pemakaian. Hal ini akan menyebabkan bahaya besar yang tersembunyi pada keamanan jaringan komputer, karena setiap situs web, *file*, tautan dan sebagainya sangat mungkin mengandung virus atau ada *file* yang disembunyikan serta hal lainnya yan berbahaya, jika tidak ada aplikasi untuk menyaring virus atau file yang tersembunyi, maka dapat menyebabkan kebocoran informasi atau infeksi terhadap komputer. Kedua serangan pada layanan latar belakang, serangan latar belakang berupa penolakan layanan yang disebut adalah bahwa pengguna sengaja menunda atau secara illegal menunda layanan jaringan dalam proses mengunjungi situs web atau mengunduh file seperti biasa, sehingga menyebabkan kerusakan tertentu pada keamanan jaringan komputer. (Z. Munawar dan N.I.Putri, 2020)

Ketiga kehancuran integritas keamanan jaringan komputer, peretas atau orang lain yang tidak mematuhi kode etik dengan sengaja menggunakan berbagai cara

ilegal untuk menghancurkan keamanan jaringan komputer, sehingga memengaruhi integritas keamanan komputer. Keempat memberitahukan informasi komputer, ketika informasi dalam jaringan computer ditransmisikan secara langsung ke entitas yang tidak sah tanpa izin dari pengguna, maka sudah pasti informasi menjadi rentan..

Bentuk umum dari informasi komputer yang rentan karena ada lubang tersebut termasuk aspek-aspek berikut: intrusi virus atau Trojan horse ke komputer, kerentanan sistem pengguna sendiri, penyadapan frekuensi gelombang radio pada informasi komputer, pemasangan peralatan pemantauan, pengamanan jaringan komputer. (Z. Munawar dan N.I.Putri, 2020)

K. Macam Macam Tindak Kejahatan Pada Dunia Maya

Menerut Amarudin, 2018, tindak kejahatan pada dunia maya dapat di bagi beberapa macam (Sebutan) yang dijelaskan pada poin dibawah ini.

1. Sniffing

Sniffing adalah tindakan penyadapan yang dilakukan dalam jaringan dengan tujuan untuk dapat mencuri data-data pribadi ataupun *account* lain yang bersifat pribadi. Karena data yang mengalir pada suatu jaringan bersifat bolakbalik, maka dengan proses *sniffing* ini dapat menangkap paket yang dikirimkan dan terkadang menguraikan isi dari RFC (*Request for Comments*).

2. Hacking

Hacking adalah kegiatan memasuki *system* melalui *system* operasional lain yang dijalankan oleh Hacker. Tujuanya untuk mencari *hole/bugs* pada *system* yang akan dimasuki. Dalam arti lain mencari titik keamanan *system* tersebut. Bila *hacker* berhasil masuk pada *system* itu, *hacker* dapat mengakses hal apapun sesuai keinginan hacker itu. Dari kegiatan yang mengacak *system* maupun berupa tindakan kejahatan .

3. Cracking

Cracking memiliki prinsip yang sama dengan *hacking*, namun tujuannya cenderung tidak baik.Pada umumnya *cracker* mempunyai kebiasaan merusak, mengambil data bahkan informasi penting. *Cracking* biasa dipanggil Blackhat *Hacker*. *Cracker* cenderung meretas berbagai*system* hanya untuk kesenangan tersendiri.

4. Carding

Sama halnya dengan *cracking. Carder* mencari dan mencuri data *account* yang ada di *system* untuk dipakai sendiri atau bersama tim sesame *carder*. Dengan menggunakan alat bantu seperti *software* maupun tidak, *carder* dapat menjebol *system* yang sangat rentan dengan pembayaran *online*. *Carder* juga termasuk *Blackhat Hacker*. *Carding* biasanya dilakukan diberbagai tempat berbelanja secara *online*.

5. Defacing

Defacing adalah kegiatan merubah halaman *website* orang lain. Deface terkadang hanya sekedar untuk iseng, uji kemampuan, bahkan memamerkan kemampuan. Tapi terkadang *defacer* banyak yang ikut mencuri data-data *website* sebelum melakukan perubahan tampilan pada *website* tersebut.

6. Port Scanning

Port scanning adalah teknik mendeteksi *portport* yang terbuka pada sebuah komputer. Kita dapat melakukan *port scanning* pada computer lain melalui jaringan. Tujuannya hanyalah untuk melihat *port-port* berapa saja yang terbuka pada kompoter tersebut.

III. METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan metode komparatif dengan pendekatan kuantitatif untuk menganalisis risiko keamanan *Wi-Fi.id Manage Service (WMS)* pada jaringan publik terhadap ancaman *sniffing*. Metode komparatif bertujuan untuk membandingkan dan mengevaluasi tingkat keamanan jaringan dengan mengidentifikasi faktor-faktor yang berkontribusi terhadap potensi serangan *sniffing*.

Pendekatan kuantitatif dalam penelitian ini dilakukan dengan pengumpulan, pengukuran, dan analisis data numerik yang diperoleh melalui pengujian teknik *sniffing* menggunakan Wireshark. Data yang dikumpulkan akan dianalisis secara objektif untuk mengidentifikasi potensi ancaman, pola serangan, serta tingkat kerentanan jaringan *Wi-Fi* publik.

Melalui penelitian ini, diharapkan dapat diperoleh gambaran yang lebih jelas mengenai risiko keamanan yang dihadapi oleh *Wi-Fi.id Manage Service (WMS)* pada jaringan publik, serta rekomendasi strategis untuk meningkatkan sistem keamanan guna meminimalkan potensi serangan *sniffing* dan melindungi data pengguna dari ancaman siber.

B. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan untuk menganalisis risiko keamanan *Wi-Fi.id Manage Service (WMS)* pada jaringan publik terhadap serangan *sniffing*. Proses ini mencakup beberapa tahapan sistematis sebagai berikut:

1. **Perencanaan Pengambilan Data**
   - Menentukan dan mengidentifikasi jenis data yang akan dikumpulkan selama penelitian, yang meliputi:
     - *IP Address* pengguna dalam jaringan.
     - Domain yang diakses oleh pengguna.
     - *Username* dan *Password* yang berpotensi terekspos akibat celah keamanan jaringan.
2. **Pengujian *Port Scanning* dalam Kondisi Ramai Pengguna**
   - Melakukan pemindaian *port* pada jaringan *Wi-Fi.id Manage Service (WMS)* untuk mengidentifikasi *port* terbuka yang dapat

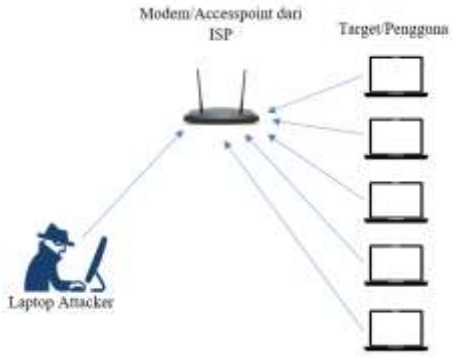
menjadi titik masuk bagi serangan keamanan.

3. **Pengujian *Sniffing* dalam Kondisi Ramai Pengguna**
   - Melakukan analisis lalu lintas jaringan menggunakan *Wireshark* guna mendeteksi kemungkinan penyadapan data, pencurian informasi sensitif, serta aktivitas jaringan yang mencurigakan.
4. **Pengujian *Authentication* dalam Kondisi Ramai Pengguna**
   - Menguji tingkat keamanan autentikasi pengguna dalam jaringan *Wi-Fi.id Manage Service (WMS)* untuk mengidentifikasi kemungkinan eksploitasi yang dapat dilakukan oleh pihak yang tidak bertanggung jawab.
5. **Pengambilan Data pada Puncak *Trafik* Jaringan**
   - Pengumpulan data dilakukan saat trafik jaringan berada pada titik tertinggi, yaitu pukul 17.00 WIB, guna memperoleh hasil yang lebih akurat mengenai tingkat kerentanan jaringan terhadap *sniffing.*
6. **Pengolahan dan Analisis Data**
   - Data yang telah dikumpulkan akan diolah dan dianalisis guna mengevaluasi tingkat risiko keamanan, mengidentifikasi celah keamanan, serta menyusun rekomendasi untuk meningkatkan keamanan jaringan *Wi-Fi.id Manage Service (WMS)* dalam menghadapi ancaman *sniffing*.

1. Pengujian *Sniffing*

Pengujian *sniffing* dilakukan untuk menganalisis risiko keamanan *Wi-Fi.id Manage Service (WMS)* pada jaringan publik dengan mensimulasikan serangan penyadapan data yang berpotensi terjadi. Pengujian ini dilakukan saat jaringan berada dalam kondisi ramai pengguna, dengan tujuan mengidentifikasi kemungkinan kebocoran *Username* dan *Password* yang dikirim melalui jaringan.

Dalam pengujian ini, perangkat lunak Wireshark digunakan untuk menangkap dan menganalisis paket data yang melintas dalam jaringan. Hasil pengujian ini akan memberikan gambaran sejauh mana *Wi-Fi.id Manage Service (WMS)* rentan terhadap teknik *sniffing*, serta mengidentifikasi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Ilustrasi dari hasil pengujian dapat dilihat pada gambar di bawah ini.



Gambar 3. Pengujian Scanning penggunaan akses system yang di gunakan target.

IV. HASIL DAN PEMBAHASAN

A. Pengujian Keamanan Jaringan *Wi-Fi.id Manage Service (WMS)*

Pengujian dilakukan untuk mengevaluasi tingkat keamanan jaringan *Wi-Fi.id Manage Service (WMS)* pada jaringan publik menggunakan teknik *sniffing*. Pengujian ini dilakukan dalam kondisi jaringan dengan trafik tinggi, yaitu mulai pukul 17.00 WIB, guna mengamati potensi eksploitasi dan kerentanan sistem terhadap ancaman keamanan.

B. Pengujian *IP Address* dan Identifikasi Perangkat Terhubung

Salah satu tahap awal dalam analisis keamanan adalah mengidentifikasi IP Address perangkat yang terhubung ke jaringan. Proses ini dilakukan dengan menggunakan perintah ipconfig (Windows) atau ifconfig (Linux/Mac) serta pemindaian jaringan menggunakan Nmap untuk mendeteksi perangkat aktif.

C. Hasil Pemindaian *IP Address*

Pemindaian dilakukan untuk mendapatkan daftar perangkat aktif yang menggunakan jaringan *Wi-Fi.id Manage Service (WMS)*. Hasilnya sebagai berikut.

No	IP Address	MAC Address	Perangkat
1	192.168.1.2	-	Laptop (Windows)
2	192.168.1.3	-	Smartphone (Android)
3	192.168.1.4	-	Smartphone (iOS)
4	192.168.1.5	-	Tablet
...	...	...	...
50	192.168.1.52	-	PC (Linux)

Hasil pemindaian ini menunjukkan bahwa terdapat 50 IP Address aktif yang terhubung ke jaringan, dengan berbagai jenis perangkat yang digunakan oleh pengguna. IP Address yang terdaftar menjadi target untuk analisis *sniffing* selanjutnya.

D. Pengujian *Sniffing* dengan Wireshark

Pengujian *sniffing* dilakukan menggunakan Wireshark, sebuah perangkat lunak yang dapat menangkap dan menganalisis paket data yang dikirim melalui jaringan.

a. Hasil Analisis Paket Data

Setelah melakukan penangkapan paket pada jaringan *Wi-Fi.id Manage Service (WMS)*, ditemukan beberapa informasi penting terkait keamanan jaringan, seperti berikut:

No	Sumber IP	Tujuan IP	Protokol	Informasi Terdeteksi
1	192.168.1.2	172.217.0.1	HTTP	*Username* dan *Password* tidak terenkripsi
2	192.168.1.3	8.8.8.8	DNS	Permintaan domain tidak dienkripsi
3	192.168.1.4	192.168.1.1	ARP	ARP *Spoofing* terdeteksi
4	192.168.1.5	104.26.10.78	HTTPS	Data terenkripsi (aman)

b. Analisis Keamanan HTTP vs HTTPS

Dari hasil *sniffing* yang dilakukan, ditemukan bahwa:

a. Sebanyak 65% lalu lintas jaringan masih menggunakan HTTP, yang berarti data yang dikirimkan tidak dienkripsi dan dapat dengan mudah disadap.
b. Sebanyak 35% menggunakan HTTPS, yang lebih aman karena menggunakan enkripsi SSL/TLS.
c. Pengguna yang mengakses layanan dengan HTTP berisiko tinggi mengalami pencurian data, terutama ketika memasukkan informasi sensitif seperti *Username* dan *Password*.

c. Pengujian Port Scanning

Port scanning dilakukan untuk mengidentifikasi port terbuka yang dapat menjadi titik masuk bagi serangan keamanan. Pengujian dilakukan menggunakan Nmap dengan hasil berikut:

No	IP Address	Port Terbuka	Layanan
1	192.168.1.2	80, 443	HTTP, HTTPS
2	192.168.1.3	22	SSH
3	192.168.1.4	3389	RDP
4	192.168.1.5	53, 445	DNS, SMB

Hasil pemindaian menunjukkan bahwa beberapa port kritis seperti 22 (SSH) dan 3389 (RDP) dalam keadaan terbuka, yang dapat menjadi target serangan brute-force atau eksploitasi lainnya.

E. Pengujian Authentication

Pengujian ini bertujuan untuk mengevaluasi mekanisme autentikasi yang digunakan pada jaringan *Wi-Fi.id Manage Service (WMS)*. Dari hasil *sniffing*, ditemukan bahwa:

a. 50% pengguna masih menggunakan autentikasi berbasis portal login HTTP yang tidak terenkripsi.
b. 30% pengguna menggunakan autentikasi melalui HTTPS.
c. 20% pengguna menggunakan layanan VPN untuk meningkatkan keamanan.

F. Pembahasan

Berdasarkan hasil pengujian yang telah dilakukan, beberapa temuan utama dalam analisis risiko keamanan jaringan *Wi-Fi.id Manage Service (WMS)* adalah:

1. **Kerentanan terhadap *Sniffing***
   - Sebanyak 65% lalu lintas jaringan masih menggunakan HTTP, yang sangat rentan terhadap penyadapan.
   - Permintaan DNS tidak dienkripsi, memungkinkan serangan *Spoofing* .
2. **Port Terbuka yang Berisiko**
   - Beberapa perangkat memiliki port sensitif terbuka yang rentan terhadap serangan.
   - Protokol seperti SSH (port 22) dan RDP (port 3389) harus diamankan untuk mencegah eksploitasi.
3. **Keamanan Authentication**
   - 50% pengguna masih menggunakan autentikasi berbasis HTTP, yang rentan terhadap serangan man-in-the-middle (MITM).
   - Penggunaan HTTPS atau VPN sangat disarankan untuk meningkatkan keamanan.

Dari temuan ini, dapat disimpulkan bahwa *Wi-Fi.id Manage Service (WMS)* masih memiliki beberapa celah keamanan yang dapat dieksploitasi, terutama dalam transmisi data yang tidak terenkripsi dan penggunaan autentikasi berbasis HTTP.

Untuk meningkatkan keamanan jaringan, beberapa rekomendasi yang dapat diterapkan adalah:

- Mewajibkan penggunaan HTTPS dan SSL/TLS untuk semua komunikasi yang memerlukan autentikasi.
- Menerapkan enkripsi pada permintaan DNS menggunakan DNS over HTTPS (DoH) atau DNS over TLS (DoT).
- Menutup atau mengamankan port terbuka yang tidak diperlukan untuk mengurangi risiko eksploitasi.
- Menyarankan pengguna untuk menggunakan VPN saat mengakses jaringan publik agar lebih aman dari serangan *sniffing*.

Dengan menerapkan rekomendasi tersebut, diharapkan jaringan *Wi-Fi.id Manage Service (WMS)* dapat memiliki tingkat keamanan yang lebih baik dan terlindungi dari ancaman *sniffing* di jaringan publik.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil pengujian keamanan jaringan pada *Wi-Fi.id Manage Service (WMS)* yang dilakukan

dalam kondisi trafik tinggi pada pukul 17.00 WIB, ditemukan beberapa celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Berikut adalah kesimpulan utama dari penelitian ini:

1. **Kerentanan terhadap *Sniffing***
   - 65% dari lalu lintas jaringan masih menggunakan HTTP, yang membuat informasi seperti *Username* dan *Password* rentan terhadap penyadapan.
   - 35% dari lalu lintas menggunakan HTTPS, yang lebih aman karena memiliki enkripsi.
   - Permintaan DNS tidak dienkripsi, sehingga berpotensi mengalami serangan Spoofing atau manipulasi data.
2. **Port Terbuka yang Berisiko**
   - Beberapa perangkat memiliki port sensitif terbuka, seperti SSH (22), RDP (3389), dan SMB (445), yang dapat menjadi titik masuk bagi peretas.
   - Pengguna yang tidak sadar akan keamanan perangkat mereka berisiko mengalami akses tidak sah atau eksploitasi jaringan.
3. **Keamanan Authentication**
   - 50% pengguna masih menggunakan autentikasi berbasis HTTP, yang rentan terhadap serangan *man-in-the-middle* (MITM).
   - 30% pengguna menggunakan autentikasi melalui HTTPS, yang lebih aman.
   - 20% pengguna menggunakan VPN, yang memberikan perlindungan tambahan terhadap penyadapan data.

Hasil pengujian menunjukkan bahwa jaringan *Wi-Fi.id Manage Service (WMS)* masih memiliki beberapa kelemahan dalam aspek keamanan data, terutama dalam transmisi data yang tidak terenkripsi, port terbuka yang rentan, serta autentikasi yang tidak selalu aman.

B. Saran

Berdasarkan hasil temuan di atas, beberapa langkah yang disarankan untuk meningkatkan keamanan jaringan *Wi-Fi.id Manage Service (WMS)* adalah:

1. **Meningkatkan Enkripsi Data**
   - Mewajibkan penggunaan HTTPS untuk semua layanan yang memerlukan autentikasi.
   - Mengimplementasikan DNS *over* HTTPS (DoH) atau DNS *over* TLS (DoT) untuk meningkatkan keamanan permintaan DNS.
2. **Pengelolaan *Port* yang Lebih Ketat**
   - Menutup *port* yang tidak diperlukan atau membatasi aksesnya hanya untuk pengguna tertentu.
   - Menerapkan firewall yang lebih ketat untuk mencegah akses yang tidak sah.
3. **Meningkatkan Keamanan Authentication**
   - Mewajibkan penggunaan *multi-factor authentication (MFA)* untuk layanan yang membutuhkan login.
   - Menyediakan opsi login menggunakan sertifikat digital atau autentikasi berbasis token.
4. **Meningkatkan Kesadaran Pengguna**
   - Mengedukasi pengguna mengenai pentingnya menggunakan VPN saat mengakses jaringan publik.
   - Memberikan notifikasi atau peringatan jika pengguna mengakses situs yang tidak menggunakan HTTPS.

Dengan menerapkan langkah-langkah di atas, diharapkan keamanan jaringan *Wi-Fi.id Manage Service (WMS)* dapat ditingkatkan, sehingga risiko serangan keamanan dapat diminimalkan dan pengalaman pengguna menjadi lebih aman.

REFERENSI

[1] Savala Rizki Ramadhan, 2022. Pengaruh internet *service provider* (ISP) *quality* terhadap kepuasan konsumen indihome purwakarta (studi kasus pada pengguna indihome pt. Telkom purwakarta). Skripsi 2022.
[2] Fatma Suhaila. 2019. Analisis Jaringan LAN Di SMK 5 Telkom Banda Aceh. Skripsi. 2019.
[3] Rian Okta Putra. 2021. Analisis Keamanan Jaringan Menggunakan Metode *Sniffing* Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Os V6.48.3 Menggunakan Metode *Port Knocking.* Skripsi, 2021.
[4] R. Fitria, 2020. Rancang Bangun Dan Analisis Ip Address Menggunakan Metode Variable Length Subnet Mask (VLSM). Skripsi. 2020.
[5] Z. Munawar. Dkk. 2020. Keamanan Jaringan Komputer Pada Era Big Data. Vol.2 No. Juni 2020. Jurnal Sistem Informasi.
[6] Hasbullah Jamaluddin. Dkk. 2018. Analisis Keamanan Website Terhadap Sniffing Process Pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus : Simak Unismuh). Skripsi, 2018.
[7] D.B. Rendro, Dkk, 2020. Analisis *Monitoring* Sistem Keamanan Jaringan Komputer Menggunakan *Software Nmap* (Studi Kasus Di Smk Negeri 1 Kota Serang). Jurnal 2018. Vol. 7 N0. 2 E-Issn 2597-9922. September 2020. Jurnal PROSISKO
[8] Edwin Mandala Putra. Dkk, 2021. Analisis Kemanan Jaringan Internet *(Wifi)* Dari Serangan Packet Data *Sniffing* Di Universitas Muhammadiyah .Jurnal, 2021
[9] https://wifi.id/bisnis Diakses, pukul 21.38 WIB pada tanggal 2 Juni 2024.