Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing pada RSUD Alimuddin Umar Di Lampung Barat

[1]Suroso, [2]Sriyanto*
[1]Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya, surosoo858@gmail.com
[2]Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya, sriyanto@darmajaya.ac.id

ABSTRAK

Dalam zaman informasi dan komunikasi saat ini, kebutuhan akan akses informasi yang fleksibel menjadi esensial. Bagi sebagian orang, kemampuan untuk mengakses informasi di mana pun dan kapan pun sangatlah penting. Teknologi nirkabel menjadi solusi yang efektif untuk memenuhi kebutuhan tersebut. Dalam wawancara dengan Bapak Suyatno, yang memimpin Unit Teknologi Informasi di RSUD Alimuddin Umar, disampaikan bahwa rumah sakit tersebut sering mengalami gangguan seperti flooding dan *illegal access*. Oleh karena itu, RSUD Alimuddin Umar menyadari pentingnya menganalisis sistem keamanan jaringan untuk memastikan keamanan, terutama pada jaringan nirkabel. Penggunaan alat bantu standar, seperti metode *Penetration Testing*, diperlukan untuk melakukan analisis keamanan dengan efektif. Hasil pengujian menunjukkan bahwa *access point* 1 memiliki *password* yang mudah ditebak dan rentan terhadap serangan. Oleh karena itu, diperlukan penanganan lebih lanjut dan implementasi *passphrase* yang lebih aman untuk mengatasi celah keamanan tersebut.

Kata Kunci : Keamanan Jaringan, *Brute Force, Penetration Testing*.

ABSTRACT

In the current era of information and communication, the need for flexible access to information has become essential. For some people, the ability to access information anytime, anywhere is crucial. Wireless technology serves as an effective solution to meet these needs. In an interview with Mr. Suyatno, who is in charge of the Information Technology Unit at RSUD Alimuddin Umar, it was revealed that the hospital often experiences disruptions such as flooding and illegal access. Therefore, RSUD Alimuddin Umar recognizes the necessity of analyzing the network security system to ensure the overall security, particularly in the wireless network. Standard tools, such as the Penetration Testing method, are required for an effective security analysis. The test results indicate that access point 1 has a easily guessable password and is vulnerable to attacks. Consequently, further attention and the use of a more secure passphrase are needed to address these security vulnerabilities.
Keywords : Network security, Brute Force, Penetration Testing.

PENDAHULUAN

Keberadaan akses informasi dan komunikasi yang efektif menjadi aspek krusial dalam konteks era informasi saat ini. Bagi banyak individu, ketersediaan informasi yang dapat diakses dengan fleksibilitas di berbagai tempat dan waktu menjadi sebuah keharusan. Dalam menjawab kebutuhan tersebut, teknologi nirkabel muncul sebagai solusi yang dapat memenuhi tuntutan akan konektivitas yang semakin meningkat. Oleh karena itu, upaya pengembangan dan peningkatan teknologi komunikasi menjadi prioritas, baik dalam peningkatan kualitas maupun jumlahnya.

Meskipun keberadaan internet memberikan kenyamanan dalam hal akses, hal tersebut juga membuka peluang terjadinya kejahatan di dalam jaringan. Pencurian data atau peretasan menjadi risiko nyata yang dapat merugikan pengguna jaringan. Serangan dapat berupa upaya mendapatkan sumber daya, mengubah konfigurasi sistem jaringan, atau memanipulasi data dengan mengakses Server untuk merubah konfigurasi tertentu.

Teknologi nirkabel, yang menggunakan gelombang elektromagnetik sebagai media transfer data tanpa kabel, menawarkan kemudahan, kebebasan, mobilitas, dan fleksibilitas tinggi. Kelebihan ini menjadikan teknologi *wireless* menjadi pilihan menarik bagi pengguna komputer yang ingin terhubung dengan jaringan atau internet. Namun, di RSUD Alimuddin Umar, kota Liwa, Kabupaten Lampung Barat, penggunaan jaringan dengan 6 perangkat wireless yang mencakup seluruh area kantor dan dilindungi oleh keamanan WPA2-PSK seringkali menghadapi tantangan dibandingkan dengan jaringan LAN. Jenis serangan tertentu, seperti *Brute Force*, seperti *flooding* dan *illegal access*, yang berusaha meretas *password* dengan mencoba semua kemungkinan kombinasi pada *wordlist*, sering kali menjadi masalah serius. Akibatnya, serangan *flooding* pada perangkat wifi dapat memberikan dampak pada PC, menyebabkan ketidakmampuan PC tersebut untuk mengakses internet.

Dalam menghadapi permasalahan ini, penulis melakukan analisis menggunakan *Penetration Testing*, sebuah alat standar yang dikembangkan oleh organisasi untuk menganalisis keamanan sistem jaringan di instansi atau perusahaan. Dalam konteks ini, peneliti mengusung judul "Evaluasi Keamanan *Wireless Local Area Network* Terhadap Serangan *Brute Force* dengan Memanfaatkan Metode *Penetration Testing*." Dengan dasar masalah yang telah diuraikan, rumusan masalah yang dapat diambil adalah, "Bagaimana langkah-langkah untuk mengevaluasi keamanan *wireless local area network* menggunakan metode *Penetration Testing* pada RSUD Alimuddin Umar di Lampung Barat?"

Pembatasan masalah menjadi suatu kebutuhan untuk menghindari penyimpangan dan menjaga fokus penelitian agar lebih terarah, memudahkan pembahasan, dan mencapai tujuan penelitian. Dalam konteks ini, penelitian ini membatasi analisis pada aspek yang pertama penelitian hanya fokus pada perangkat *nirkabel*, Pengujian terutama difokuskan pada perangkat wifi di unit IT RSUD Alimuddin Umar dan Untuk Metode *Penetration Testing* (Pengumpulan Intelijen, Pemodelan Ancaman, Pelaporan) menjadi landasan utama dalam penelitian.

Adapun tujuan dari penelitian ini adalah untuk menganalisis sistem keamanan jaringan RSUD Alimuddin Umar dengan menggunakan metode *penetration testing*. Dengan demikian, penulis dapat menilai efektivitas sistem keamanan jaringan *wireless* di RSUD Alimuddin Umar. Tujuan penelitian ini melibatkan dua aspek utama yaitu Menilai sistem keamanan wireless yang telah

diterapkan di RSUD Alimuddin Umar dan Mengimplementasikan *Penetration Testing* sebagai metode analisis keamanan jaringan *wireless*.

Beberapa penelitian terdahulu yang telah dilaksanakan oleh peneliti-peneliti sebelumnya memberikan pandangan yang relevan terhadap penelitian ini. [1]dalam penelitiannya tentang analisis keamanan jaringan WLAN dengan metode *penetration testing*, memusatkan perhatian pada tahap Intelligence *Gathering, Threat Modeling,* dan *Reporting,* sementara penelitian sebelumnya hanya berfokus pada tahap perencanaan. [2]dalam penelitiannya mengenai analisis sistem keamanan jaringan wireless dengan tipe keamanan WEP, WPAPSK/WPA2PSK, dan Mac Address menggunakan metode penetration testing. Meskipun keduanya melibatkan analisis Penetration Testing, penelitian ini membedakan diri dengan penggunaan aplikasi VPN Book oleh penulis. [3] melakukan penelitian terkait analisis keamanan jaringan wireless di PT. Mora Telematika Indonesia Regional Palembang dengan metode pengembangan Penetration Testing. Hasilnya menunjukkan kerentanan dalam jaringan wireless local area network PT. Mora Telematika Indonesia. Penelitian ini berbeda dengan penelitian sebelumnya yang tidak melibatkan tahapan Penetration Testing, hanya mengandalkan tools dari Kali Linux. [4]dalam penelitiannya mengenai monitoring sistem keamanan jaringan komputer dengan menggunakan software Nmap. Penelitian ini lebih berfokus pada analisis daripada pengembangan jaringan. Abraham Yano [5] mengevaluasi keamanan jaringan wireless di STMIK Mataram Meskipun menggunakan metode analisis, monitoring, dan observasi, penelitian ini memiliki perbedaan dalam metode yang digunakan dan hasil yang diperoleh. [3] dalam penelitiannya terkait metode penetration testing pada keamanan jaringan wireless menggunakan metode pengembangan Penetration Testing. Hasilnya menunjukkan kerentanan seperti WPA2 Cracking, DoS, Password Router Wireless Cracking, dan AP Isolation Testing pada jaringan internal dan publik. Perbedaannya dengan penelitian sebelumnya adalah penulis memanfaatkan tahapan reporting sebagai langkah akhir penelitian.

a. Evaluasi

Evaluasi merupakan suatu langkah terencana dan sistematik yang dilaksanakan untuk mengevaluasi dan menilai berbagai aspek dari suatu objek, program, kegiatan, atau sistem[6]. Proses ini mencakup pengukuran kinerja, efektivitas, efisiensi, dan dampaknya terhadap tujuan yang diinginkan. Evaluasi tidak hanya terbatas pada satu bidang, melainkan dapat merujuk pada beragam konteks seperti pendidikan, manajemen, ilmu sosial, lingkungan, dan bidang lainnya. Tujuan utama dari evaluasi adalah menyediakan informasi yang akurat dan obyektif guna mendukung pengambilan keputusan yang cerdas, mengidentifikasi area perbaikan, dan merancang langkah-langkah pengembangan selanjutnya. Dengan demikian, evaluasi menjadi alat yang penting dalam meningkatkan kualitas dan hasil dari berbagai inisiatif atau program.

b. *Wireless Local Area Network* (WLAN)

WLAN, atau *Wireless Local Area Network*, adalah suatu jaringan komunikasi nirkabel yang memungkinkan perangkat-perangkat elektronik seperti komputer, laptop, smartphone, atau perangkat lainnya dapat terhubung ke jaringan komputer tanpa menggunakan kabel fisik[7].

Jaringan ini menggunakan gelombang elektromagnetik, seperti radiofrekuensi, untuk mentransfer data antar perangkat yang terhubung. WLAN memungkinkan fleksibilitas dan mobilitas dalam akses jaringan, membebaskan pengguna dari keterbatasan kabel fisik dan memungkinkan koneksi yang lebih mudah di berbagai lokasi. Keamanan dalam WLAN umumnya diterapkan melalui protokol keamanan seperti WPA (Wi-Fi Protected Access) untuk melindungi data yang dikirimkan melalui jaringan nirkabel ini.

c. Keamanan Jaringan

Keamanan jaringan merujuk pada serangkaian langkah dan strategi yang diimplementasikan untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya yang terdapat dalam suatu jaringan komputer[8]. Tujuan utama dari keamanan jaringan adalah untuk mencegah akses yang tidak sah, melindungi data dari perubahan atau pencurian, serta memastikan bahwa layanan dan sumber daya jaringan tetap beroperasi secara optimal.

Langkah-langkah keamanan jaringan mencakup sejumlah aspek, seperti penggunaan otentikasi yang kuat untuk memastikan identitas pengguna, penggunaan enkripsi data agar tidak dapat dibaca oleh pihak yang tidak sah, penerapan firewall untuk memonitor dan mengontrol lalu lintas jaringan, dan pemantauan secara terus-menerus terhadap aktivitas jaringan untuk mendeteksi potensi ancaman keamanan.

Keamanan jaringan juga melibatkan manajemen kebijakan keamanan yang jelas, pembaruan perangkat lunak secara teratur untuk mengatasi kerentanan keamanan yang baru muncul, serta pelatihan pengguna agar dapat mengidentifikasi dan menghindari tindakan yang dapat membahayakan keamanan jaringan.

Dengan menerapkan langkah-langkah ini, suatu organisasi atau entitas dapat menciptakan lingkungan jaringan yang aman, yang dapat menjaga keberlanjutan operasionalnya dan melindungi informasi serta sumber daya yang ada di dalamnya.

1) *Privacy* (Kerahasiaan):

Kerahasiaan dalam konteks keamanan jaringan merujuk pada perlindungan informasi dari akses yang tidak sah atau tidak sah. Langkah-langkah keamanan harus dirancang untuk mencegah orang yang tidak berwenang mendapatkan akses ke data atau informasi yang bersifat pribadi atau rahasia.

2) *Message Integrity* (Integritas Pesan):

Integritas pesan menunjukkan bahwa informasi atau pesan tidak mengalami perubahan yang tidak sah selama transmisi atau penyimpanan. Langkah-langkah keamanan, seperti penggunaan tanda tangan digital atau fungsi hash, dapat memastikan bahwa pesan tetap utuh dan tidak dimanipulasi oleh pihak yang tidak berwenang.

3) *End Point Authentication* (Otentikasi Titik Akhir):

Otentikasi titik akhir adalah proses memastikan identitas dan keabsahan pihak yang terlibat dalam komunikasi, seperti perangkat atau pengguna di ujung jaringan. Ini membantu mencegah akses yang tidak sah dengan memverifikasi bahwa pihak yang berkomunikasi adalah yang seharusnya.

4) *Non-repudiation* (Tidak Dapat Dibantah):

Tidak dapat dibantah menunjukkan bahwa suatu entitas tidak dapat menyangkal keterlibatannya dalam suatu transaksi atau

komunikasi. Non-repudiation melibatkan penggunaan tanda tangan digital atau catatan audit untuk memastikan bahwa pihak yang terlibat tidak dapat membantah tindakan atau pernyataannya.

d. Jaringan Komputer

Jaringan komputer adalah suatu sistem yang terdiri dari dua atau lebih perangkat komputer yang saling terhubung melalui berbagai media komunikasi, seperti kabel atau nirkabel, dengan tujuan untuk berbagi sumber daya dan informasi[9]. Dalam jaringan komputer, perangkat-perangkat ini dapat berkomunikasi dan berinteraksi satu sama lain, memungkinkan pertukaran data, file, atau layanan di antara mereka.

Jaringan komputer dapat memiliki berbagai skala, mulai dari jaringan lokal *(Local Area Network/LAN*) yang mencakup area terbatas seperti sebuah gedung atau kantor, hingga jaringan yang lebih luas seperti jaringan wilayah metropolitan (*Metropolitan Area Network/MAN*) atau jaringan global yang dikenal sebagai Internet[10]. Komunikasi dalam jaringan komputer dapat dilakukan melalui berbagai protokol dan teknologi, termasuk *Transmission Control Protocol/Internet Protocol (TCP/IP), Ethernet, Wi-Fi*, dan lainnya.

Keuntungan dari jaringan komputer mencakup kemampuan untuk berbagi sumber daya seperti printer atau file, meningkatkan efisiensi dalam pertukaran informasi, dan memungkinkan kolaborasi antara pengguna yang berbeda lokasi. Namun, keamanan dan privasi menjadi perhatian utama dalam pengelolaan jaringan komputer, sehingga diperlukan langkah-langkah keamanan untuk melindungi data dan informasi yang beredar di dalamnya.

e. *Brute Force*

Brute force adalah suatu metode serangan dalam dunia keamanan komputer yang mencoba semua kemungkinan kombinasi yang ada untuk mendapatkan akses ke suatu sistem atau mendekripsi informasi terenkripsi[11]. Dalam konteks ini, serangan *brute force* umumnya digunakan untuk meretas kata sandi atau kunci enkripsi dengan mencoba secara berulang-ulang hingga menemukan kombinasi yang benar. Metode *brute force* ini bekerja dengan mencoba semua kemungkinan kombinasi secara sistematis, tanpa memerlukan pengetahuan terkait kelemahan atau keunikan sistem yang diserang. Serangan ini dapat menjadi efektif jika kata sandi atau kunci enkripsi yang digunakan relatif lemah atau memiliki kompleksitas yang rendah.

Untuk mengatasi serangan brute force, banyak sistem keamanan komputer menggunakan langkah-langkah seperti pembatasan jumlah percobaan login, penerapan kata sandi yang kuat, dan penggunaan metode otentikasi dua faktor[11]. Dengan langkah-langkah keamanan yang memadai, serangan brute force dapat diminimalkan atau dicegah, sehingga menjaga keamanan sistem dan data dari upaya yang bersifat membabi buta ini.

f. *Penetration Testing*

Penetration Testing, atau yang sering disebut sebagai uji penetrasi[12], adalah suatu proses evaluasi keamanan yang dilakukan pada suatu sistem komputer, jaringan, atau aplikasi untuk mengidentifikasi dan mengevaluasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak sah. Tujuan utama dari Penetration Testing adalah untuk menguji kehandalan sistem keamanan suatu entitas dan menemukan kelemahan-kelemahan yang mungkin dapat dimanfaatkan oleh penyerang.Proses Penetration Testing melibatkan simulasi serangan yang

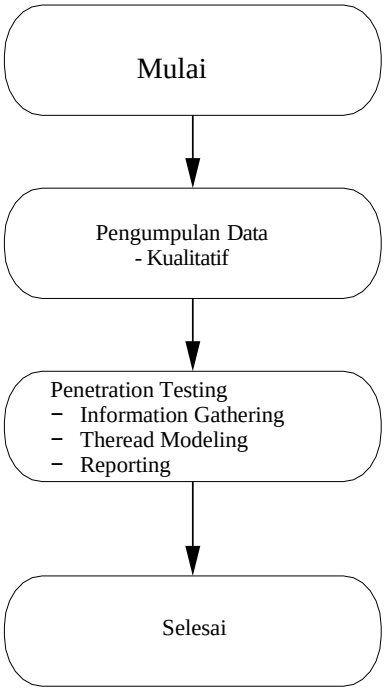
dilakukan secara kontrol terhadap sistem atau aplikasi target. Langkah-langkahnya mencakup identifikasi potensi titik lemah, penetrasi atau penetrasi ke dalam sistem, pengumpulan data yang relevan, serta pelaporan hasil temuan dan rekomendasi perbaikan. Tim uji penetrasi, yang biasanya terdiri dari para ahli keamanan yang terampil, mencoba untuk menguji batasan dan keefektifan sistem keamanan dengan cara yang dapat mencerminkan serangan dunia nyata.Penetration Testing juga memberikan pemilik sistem atau aplikasi pemahaman mendalam tentang tingkat risiko keamanan yang mereka hadapi dan membantu dalam mengambil langkah-langkah proaktif untuk memperkuat keamanan. Dengan melakukan uji penetrasi secara berkala, entitas dapat meningkatkan ketahanan keamanan mereka dan menjaga integritas serta kerahasiaan data mereka.

g. Ancaman-Ancaman Jaringan Komputer

Ancaman terhadap jaringan komputer adalah beragam situasi atau tindakan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan data dalam suatu jaringan[13]. Berikut adalah beberapa jenis ancama yang dapat mengintai jaringan komputer:

1) *Malwar*e:Merupakan perangkat lunak berbahaya yang dirancang untuk merusak atau merusak sistem komputer[14]. Malware melibatkan *virus, worm, trojan, spyware,* dan ransomware yang dapat merusak data atau mengakses informasi tanpa izin.
2) Serangan DoS (*Denial of Service*): Bertujuan untuk membuat sumber daya jaringan tidak dapat diakses oleh pengguna yang sah dengan cara mengalirkan lalu lintas yang sangat tinggi ke suatu situs atau server[15]. Hal ini menyebabkan kelambatan atau bahkan kegagalan fungsi sistem.
3) Serangan DDoS (*Distributed Denial of Service*): Mirip dengan serangan DoS, namun melibatkan lebih dari satu sumber serangan yang terdistribusi secara geografis. Ini membuat serangan lebih sulit dideteksi dan ditangani.
4) Serangan *Man-in-the-Middle* (MitM): Seorang penyerang mencoba memasuki komunikasi antara dua pihak dan dapat mencuri atau memanipulasi data yang dikirimkan antar keduanya tanpa sepengetahuan mereka.
5) Serangan *Phishing*: Pengecoh mencoba untuk mendapatkan informasi rahasia, seperti kata sandi atau informasi keuangan, dengan menyamar sebagai entitas tepercaya melalui email, pesan instan, atau situs web palsu.
6) Serangan *Ransomwar*e: Melibatkan enkripsi data pada sistem target dan meminta pembayaran tebusan untuk mengembalikan akses atau mengembalikan data yang terenkripsi.
7) Serangan *Zero-Day*: Mengeksploitasi kerentanan yang belum diketahui atau diperbaiki dalam perangkat lunak atau sistem operasi tertentu sebelum vendor mengeluarkan pembaruan atau perbaikan.
8) Serangan *Brute Force*: Melibatkan upaya untuk menebak kata sandi atau kunci enkripsi dengan mencoba semua kombinasi yang mungkin.
9) *Sniffing dan Spoofing: Sniffing* melibatkan perekaman dan pemantauan lalu lintas jaringan, sedangkan spoofing melibatkan

penyamaran identitas untuk mendapatkan



akses yang tidak sah[16].

10) Serangan Fisik: Ancaman nyata terhadap perangkat keras jaringan, seperti pencurian perangkat atau kerusakan fisik yang dapat mengakibatkan kegagalan sistem.
11) Serangan *Trojan Horse*: Merupakan perangkat lunak yang tampaknya berguna atau sah, tetapi menyembunyikan komponen berbahaya yang dapat merusak atau mengendalikan sistem setelah diunduh atau dijalankan.
12) Serangan *SQL Injection*: Melibatkan penyisipan kode SQL berbahaya ke dalam input pengguna pada aplikasi web, yang dapat menyebabkan akses tidak sah atau manipulasi database. Serangan ini memanfaatkan celah keamanan dalam implementasi query SQL pada aplikasi.

METODOLOGI PENELITIAN

Menurut Penelitian ini mengadopsi metode penelitian sebagai suatu pendekatan atau langkah-langkah tertentu yang memiliki tahapan yang terstruktur dan sistematis[17]. Metode ini diaplikasikan dengan tujuan untuk mengatasi permasalahan yang menjadi fokus penelitian. Pendekatan yang digunakan dalam penelitian ini adalah analisis penelitian kualitatif yang bersifat deskriptif. Pilihan ini didasarkan pada sifat permasalahan yang bersifat deskriptif, yang memerlukan gambaran atau deskripsi yang detail terkait dengan keadaan subjek atau objek yang menjadi fokus penelitian[18]. Selain itu, tahapan analisis sistem jaringan juga merupakan bagian integral dari penelitian ini, dengan langkah-langkah yang telah ditetapkan untuk mencapai hasil yang terstruktur dan informatif. Tahapan penelitian dapat dilihat pada gambar berikut:

Gambar 1. Tahapan Penelitian

a. Pengumpulan Data

Berikut adalah bebarapa metode pengumpulan data yang peneliti gunakan dalam melakukan penelitian

1. Observasi

Dalam pelaksanaan metode ini, peneliti melakukan survei lokasi untuk menghimpun informasi terkait RSUD Alimuddin Umar. Kegiatan survei ini bertujuan untuk mengidentifikasi data mengenai perangkat dan pengguna wireless, serta aspek keamanannya.

2. Wawancara

Dalam fase ini, peneliti melakukan wawancara dengan karyawan di Laboratorium Komputer RSUD Alimuddin Umar. Tujuannya adalah untuk memperoleh informasi mengenai perkembangan dan fungsi dari jaringan komputer yang ada.

3. Studi Pustaka

Pada langkah ini, mencari data atau informasi terkait judul skripsi yang terkait dengan permasalahan yang sedang dihadapi. Sumber data dan informasi berasal dari jurnal, buku, dan skripsi sebelumnya untuk mendukung penelitian lebih lanjut.

b. Berikut ini adalah langkah-langkah dari bagian metode *Penetration Testing* (Pentes) yang digunakan oleh penulis dalam melakukan analisis dalam penelitian ini.

1) Information Gathering

Pada tahap ini, penulis mengumpulkan data yang sering disebut sebagai passive penetration testing. Ini dikategorikan sebagai passive karena proses pengumpulan data dilakukan secara manual melalui dokumentasi dari pihak terkait dan informasi terbuka yang terkait dengan sistem yang akan diuji. Jenis analisis ini mencakup evaluasi jaringan dan topologi yang sedang berjalan, kebutuhan pengguna, serta perangkat lunak dan perangkat keras yang digunakan.

2) Threat Modeling

Tahap ini merupakan upaya penulis untuk mensimulasikan serangan dengan tujuan memperoleh username dan password dari jaringan wireless. Teknik penyerangan yang digunakan mencakup metode Brute Force dan vpn book.

3) Reporting

Pada tahap ini, penulis melakukan analisis terhadap hasil-hasil dari tahap sebelumnya, mengidentifikasi kerentanan yang terdeteksi selama pengujian, menentukan risiko yang terkait, dan memberikan rekomendasi terkait langkah-langkah untuk mengurangi kerentanan yang telah diidentifikasi.

c. Lokasi Penelitian

Tempat melakukan penelitian di Rumah Sakit Umum Daerah Alimuddin Umar yang berada di Kabupaten Lampung Barat Provinsi Lampung.

HASIL DAN PEMBAHASAN

Bagian ini menjelaskan hasil dari analisa yang sudah dilakukan oleh penulis yang terbagi dalam beberapa tahapan berikut ini:

A. Hasil Pengumpulan Data

Penerapan metode Penetration Testing dari tahap Information Gathering hingga Reporting mencakup hasil pengumpulan data, analisis uji coba serangan, dan identifikasi kerentanan jaringan. Dalam penelitian ini, hasil-hasil tersebut dibahas secara terinci, mencakup data yang terkumpul, analisis uji coba serangan, serta memberikan langkah-langkah dan solusi untuk mengurangi kerentanan yang terdeteksi dalam jaringan wireless RSUD Alimuddin Umar.

1. Observasi

Hasil pengamatan yang dilakukan oleh peneliti di RSUD Alimuddin Umar telah disetujui untuk dijadikan subjek penelitian. Judul penelitian ini adalah analisis keamanan jaringan lokal nirkabel (WLAN) terhadap serangan brute force dengan menggunakan metode penetration testing. RSUD Alimuddin Umar bersedia memberikan data dan informasi yang diperlukan untuk penelitian ini. Informasi yang diberikan mencakup skema jaringan yang sedang digunakan saat ini dan hasil pengamatan. Dari hasil observasi tersebut, peneliti menemukan bahwa RS H.L. Manambai Abdul Kadir menerapkan keamanan yang baik dengan menggunakan pengaturan default dari access point untuk melindungi jaringan nirkabel itu sendiri.

2. Wawancara

Pada tahap wawancara, proses interaksi langsung dilaksanakan. Metode wawancara ini melibatkan pemberian pertanyaan secara langsung kepada tim IT di RSUD Alimuddin Umar. Dalam proses wawancara ini, pihak tersebut menyatakan dukungannya terhadap penelitian mengenai

analisis keamanan jaringan di RSUD Alimuddin Umar.

3. Studi pustaka

Penguatan penelitian ini diperoleh melalui telaah literatur yang saya lakukan. Referensi mengenai konsep dan teknik ditemukan dari buku, jurnal, dan tugas akhir yang tercakup dalam tinjauan literatur dan dasar teori.

B. Information Gathering

Dari proses pengumpulan informasi yang telah dilakukan, dapat diuraikan beberapa poin hasil analisis mengenai kebutuhan perangkat, kebutuhan pengguna, dan kebutuhan layanan yang diperlukan.

1. Analisis Kebutuhan Perangkat Keras (*Hardware*)

Laptop dengan spesifikasi sebagai berikut:

a.*Prosesor : Intel® Core (TM) i5-4200U CPU @1.60GHz(4CPU), 2.30GHz*

b.Memory : 8 GB DDR4

c.Hardisk : 1 TB dan SSD 512Gb

d.VGA : 2 Gb

2. Analisis Kebutuhan Perangkat Lunak (*Software)*

Software yang digunakan dengan spesifikasi sebagai berikut:

a.Kali linux : 7(32 Bit)

b.Google Chrome : 92.0

c.Pvn book : 3.4.7

3. Identitas Perangakat Yang Di Uji Acces poin TL-WR840N

Wireless router ini memiliki dua antena 5dBi yang dapat meningkatkan transmisi sinyal nirkabel dan penerimaan. Dilengkapi dengan 4 port Ethernet cepat, TL-WR840N menyediakan koneksi Wi-Fi yang andal dan juga opsi koneksi kabel untuk rumah berukuran sedang. Dengan demikian, keluarga dapat menikmati koneksi Wi-Fi cepat bersama-sama melalui smartphone, tablet, dan laptop.

TL-WR840N sesuai dengan standar IEEE 802.11n, mampu membentuk jaringan nirkabel dengan kecepatan hingga 15 kali lipat dan jangkauan 5 kali lipat dari produk 11g konvensional. Kecepatan transmisi yang mencapai 300Mbps juga menjadi salah satu fitur unggulan dari perangkat ini.

Tabel 1 identitas tp-ling TL-WR840N

Spesifikasi	**Kecepatn**	**Frekuensi band**	**Availability**
802.11b	11 mb/s	2.4 GHz	b
802.11g	54 mb/s	2.4 GHz	b, g
802.11n	300 mb/s	2.4 GHz	b, g, n

C. Threat Modeling

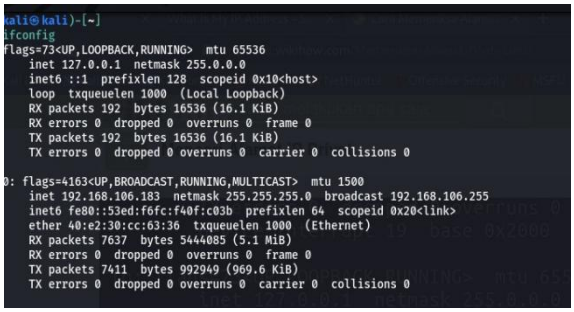
Berdasarkan informasi arsitektur dan topologi yang telah saya peroleh, pada langkah ini saya akan melakukan simulasi serangan untuk mendapatkan password dari jaringan nirkabel. Dalam konteks ini, saya akan mensimulasikan diri sebagai seorang peretas yang beroperasi di dalam jaringan RSUD Alimuddin Umar. Serangan ini akan dilakukan pada jaringan nirkabel yang telah diamankan menggunakan metode WPA/WPA2 PSK.

1. Instalasi vpn book

Berikut adalah panduan instalasi VPN Book yang dapat dilihat melalui ilustrasi di bawah ini. Pentester dapat mengubah alamat IP mereka menggunakan alat VPN Book. Alamat IP yang digunakan oleh pentester adalah 192.168.106.183. Informasi antarmuka pentester dapat ditemukan dalam ilustrasi berikut.

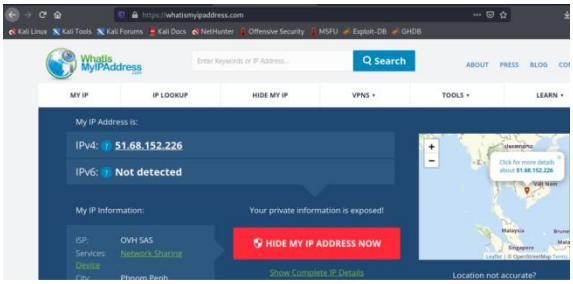
Gambar 2 Pengecekan IP Adress

Memasang VPN Book untuk mengubah alamat IP dapat dilakukan dengan langkah-langkah berikut. Ketik perintah "openvpn vpnbook-pl226-tcp80.ovpn" pada terminal Linux. Tampilan proses pemasangan VPN Book dapat ditemukan dalam ilustrasi di bawah ini.



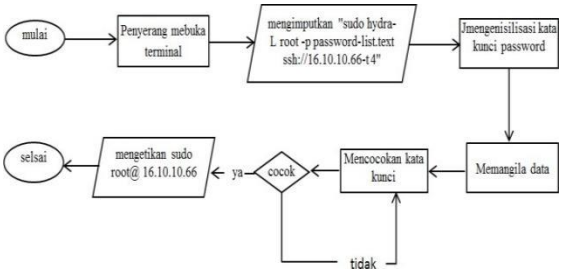
Gambar 3 Proses Install vpn book

Pengecekan pengubahan alamat IP telah dilakukan. Untuk membuktikan bahwa alamat IP telah berhasil diubah, verifikasi dilakukan dengan memeriksa IP dan wilayah melalui situs https://whatismyipaddress.com/. Berikut adalah tampilan dari perubahan IP yang dapat dilihat dalam gambar.



Gambar 4 Pembuktian IP Adress yang dirubah

2. Flowchat brute force



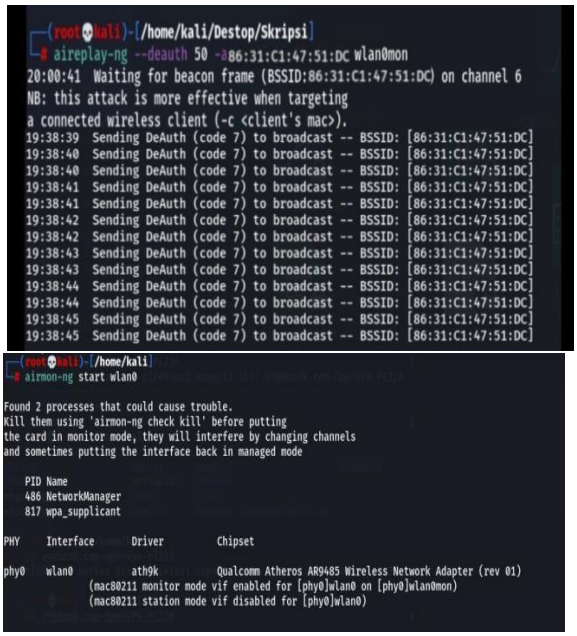
Gambar 5 *Flowchart Brute Force*

Pada serangan SSH brute force ini, penyerang berusaha untuk mendapatkan username dan password yang dimiliki oleh server menggunakan aplikasi Hydra, yang beroperasi melalui command prompt. Penyerang mencoba menebak password dengan menginputkan perintah sesuai dengan gambar

1. Setelah perintah diinputkan, aplikasi Hydra akan memulai proses inisialisasi kata kunci password, yang kemudian diambil dari data yang tersedia. Hydra akan mencocokkan kata kunci password dengan daftar password yang ada; jika terdapat kecocokan dalam password-list.txt, penyerang akan melancarkan serangan SSH brute force terhadap server menggunakan mode root. Namun, jika kata kunci password tidak cocok, proses pencocokan akan diulang kembali.

3. Mengaktifkan mode monitoring *interface WLAN*

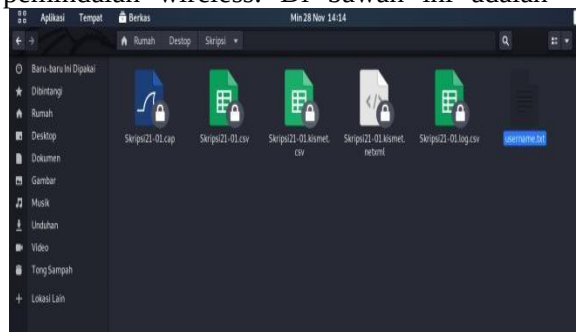
Gunanya tools aircrack-ng perlu diaktifkan dengan mengonfigurasi mode monitoring pada antarmuka wlan0 melalui perintah "airmon-ng start wlan0". Berikut ini adalah ilustrasi dari tampilan mode monitoring yang dapat ditemukan dalam gambar berikut.



Gambar 6 Tahap Monitoring

4. Scaning wireless

Perintah "airodump-ng wlan0mon" pada konsol digunakan untuk melakukan pemindaian wireless. Di bawah ini adalah

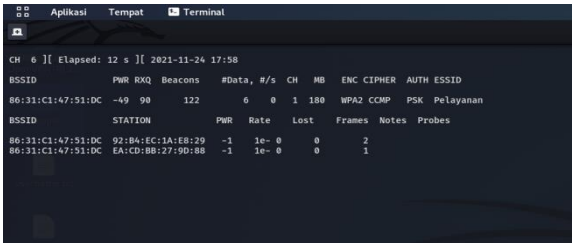


tampilan hasil keluaran setelah mengetikkan perintah "airodump-ng wlan0mon" yang dapat dilihat dalam gambar berikut.

Gambar 7 *Scanning Wireless*

5. Proses *handshake*

Perintah "airodump-ng -w skripsi21 -C 1 -bssid 86:31:C1:47:51:DC wlan0mon" digunakan untuk melakukan koneksi atau handshake antarmuka pentester dengan perangkat nirkabel target. Berikut ini adalah tampilan hasil handshake perangkat, yang dapat dilihat dalam gambar berikut.



Gambar 8 Proses *Handshake*

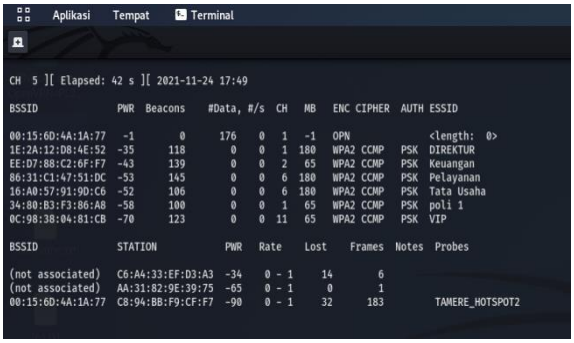
6. Injeksi paket

Perintah "aireplay-ng --deauth 50 --a 86:31:C1:47:51:DC wlan0mon" digunakan untuk mengirimkan sinyal deauth (deauthenticating) sebanyak 50 kali ke perangkat wireless dengan alamat MAC 86:31:C1:47:51:DC. Ini bertujuan untuk memaksa perangkat tersebut keluar dari jaringan nirkabel. Jika sudah dianggap cukup, pengguna dapat menghentikan proses dengan menekan ctrl+c.

Gambar 9 Proses *Injeksi Paket*

7. hasil dari *handshake*

Langkah selanjutnya adalah mengecek apakah terdapat file yang telah disimpan sebelumnya dalam folder. Ilustrasinya dapat dilihat pada



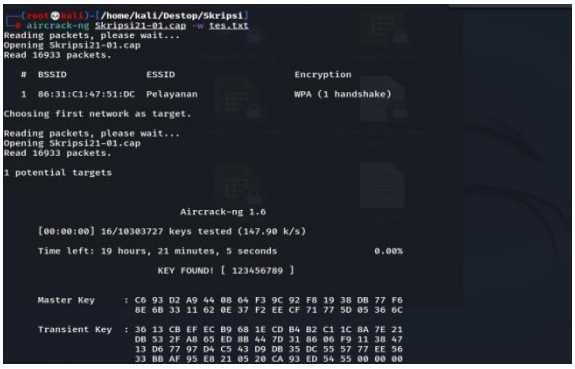
Gambar 6 di bawah ini.

Gambar 10 Hasil dari *Handshake*

8. Proses cracking 1

Perintah "aircrack-ng skripsi21-01.cap -w tes.txt"

digunakan untuk memuat file daftar kata yang telah dibuat oleh pentester dan menjalankan alat aircrack-ng untuk melakukan serangan brute force pada perangkat nirkabel target. Berikut ini adalah tampilan dari aircrack yang dapat ditemukan dalam gambar berikut.



Gambar 11 Proses *Checking 1*

9. Proses *cracking 2*

Perintah "aircrack-ng skripsi21-01.cap -w tes.txt" digunakan untuk memuat daftar kata yang telah disiapkan oleh pentester dan menjalankan alat aircrack-ng untuk melakukan serangan brute force pada perangkat nirkabel target. Berikut adalah tampilan dari aircrack yang dapat ditemukan dalam gambar berikut.

Gambar 12 Proses Checking 2

D. Reporting

Dari hasil penelitian yang telah dilakukan, pada tahap pelaporan, saya menyimpulkan beberapa temuan, termasuk hasil penyerangan access point dan solusi untuk mengamankan serangan brute force.

1. Tabel peneyerangan

Tabel 2 Hasil Penyerangan

Jenis Serangan	Informasi yang dibutuhkan	Status
Brute force attack	Mendapatkan informasi kemungkinan password	Sukses
Brute force attack	Mendapatkan informasi kemungkin	Gagal

Dalam tabel ini dijelaskan hasil penyerangan yang dilakukan oleh pentester pada Access Point 1 dan Access Point 2. Dari dua serangan yang dilakukan dengan metode brute force attack yang sama, serangan pada Access Point 1 berhasil mendapatkan password untuk mengakses jaringan nirkabel, sedangkan serangan pada Access Point 2 tidak berhasil mendapatkan password tersebut.

Dapat disimpulkan bahwa Access Point 1 memiliki password yang sangat mudah ditebak dan rentan terhadap serangan, sehingga memerlukan penanganan yang lebih baik dan penerapan passphrase yang lebih kuat sebagai perlindungan bagi jaringan nirkabel. Penggunaan passphrase yang kuat menjadi kunci utama dalam menjaga keamanan sebuah jaringan nirkabel.

2. Data log Penyerangan

Jika kita mempertimbangkan bahwa access point umumnya beroperasi selama beberapa hari, penyerang yang tekun mungkin masih dapat berhasil menyerang access point yang mendukung WPS. Serangan ini memiliki biaya rendah dan tingkat keberhasilan yang lebih tinggi dibandingkan dengan mencoba meretas WPA/WPA2-PSK.

Tabel 3 Data Log

Upaya sebelum mengunci	Waktu penguncian	Upaya per menit	Waktu serangan maksimum	Waktu serangan maksimum	komentar
11000	0detik	46.15	3.97menit	0.17hari	tidak terkunci
?		4.20	43,65menit	1,82jam	NetgearWGR614v10
3	1detik	2.82	65.08menit	2.71jam	Persyaratan untuk WSC 2.0
15	60detik	0.25	737.31menit	30.72jam	Mengunci konfigurasi membuat brute force kurang praktis
10	60detik	0.17	1103.97	46.00jam	
5	60detik	0.08	2203.97	91.83jam	

Dikarenakan hampir semua vendor router atau access point utama telah dilengkapi dengan perangkat bersertifikasi WPS dan WPS-PIN yang merupakan persyaratan wajib untuk sertifikasi, diperkirakan banyak perangkat yang rentan terhadap serangan semacam ini. Meskipun memiliki periode penguncian yang cukup lama mungkin bukan persyaratan untuk sertifikasi, hal

ini kemungkinan menjadi persyaratan dalam Spesifikasi WSC (baru) Versi 28. Saya sudah menghubungi Wi-Fi Alliance mengenai hal ini, tetapi mereka belum memberikan tanggapan.

Kolaborasi dengan vendor akan menjadi langkah penting untuk mengidentifikasi semua perangkat yang rentan. Kemudian, tugas vendor adalah menerapkan mitigasi dan merilis firmware baru. Pengguna akhir yang terdampak harus diberitahu mengenai kerentanan ini dan disarankan untuk menonaktifkan WPS atau melakukan pembaruan firmware ke versi yang lebih aman jika tersedia.

SIMPULAN

Dari analisis dan penjelasan sebelumnya, dapat disimpulkan bahwa hasil dari analisis keamanan jaringan nirkabel dengan menggunakan metode penetration testing di RSUD Alimuddin Umar menunjukkan adanya beberapa celah keamanan yang perlu mendapatkan perhatian lebih dari pihak unit IT RSUD Alimuddin Umar. Terdapat banyak peluang bagi pihak yang tidak berkepentingan untuk mengeksploitasi kelemahan dalam sistem keamanan jaringan, khususnya pada aspek keamanan jaringan nirkabel.

DAFTAR PUSTAKA

[1] A. Keamanan Jaringan, W. Dengan, K. Bayu, M. Yamin, L. F. Aksara, dan J. T. Informatika, "Metode Penetration Testing (Studi Kasus : Laboratorium Sistem Informasi Dan Programming Teknik Informatika UHO)," vol. 3, no. 2, hlm. 69–78.

[2] D. Maya, Yamin, dan Aksara Bahtiar, 2017 "Analisis Sistem Keamanan Jaringan Wireless menggunakan metode penetration testing," *Semantik*, vol. 3, no. 2, hlm. 203–208.

[3] U. Bina, D. Palembang, H. D. Sabdho, dan M. Ulfa, "Seminar Hasil Penelitian Vokasi (Semhavok) Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor Pt. Mora Telematika Indonesia Regional Palembang".

[4] D. Bayu Rendro dan W. Nugroho Aji, 2020, "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang)," vol. 7, no. 2.

[5] L. Delsi Samsumar dan K. Gunawan, 2017, "Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi Kasus Di Kampus Stmik Mataram,".

[6] L. Delsi Samsumar *dkk.*, 2018, "Pengembangan Jaringan Komputer Nirkabel (Wifi) Menggunakan Mikrotik Router (Studi Kasus Pada Sma Pgri Aikmel)," *Jurnal METHODIKA*, vol. 4, no. 1.

[7] M. Y. Simargolang dan A. Widarma, 2022, "Quality Of Service (QoS) Untuk Analisis Performance Jaringan Wireless Area Network (WLAN) Quality Of Service (QoS) For Network Performance Analysis Wireless Area Network (WLAN)," *Journal of Computing Engineering, System and Science)*, vol. 7, no. 1, hlm. 162–171, [Daring]. Tersedia pada: www.jurnal.unimed.ac.id

[8] E. Agus Darmadi Politeknik Tri Mitra Karya Mandiri, B. Semper Jomin Baru, dan C. - Karawang, "Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless Untuk Meningkatkan Keamanan Jaringan Komputer."

[9] M. Fluorida Fibrianda dan A. Bhawiyuga, 2018, "Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM)," [Daring]. Tersedia pada: http://j-ptiik.ub.ac.id

[10] D. Bayu Rendro dan W. Nugroho Aji, 2020, "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang)," vol. 7, no. 2.

[11] S. Bahri, 2023, "Perancangan Keamanan

Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," *INDOTECH Indonesian Journal of Education And Computer Science*, vol. 1, no. 3, hlm.

[12] M. Hasibuan dan A. M. Elhanafi, 2022, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box," *sudo Jurnal Teknik Informatika*, vol. 1, no. 4, hlm. 171–177, Des 2022, doi: 10.56211/sudo.v1i4.160.

[13] S. Rumalutur, 2014, "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong,".

[14] M. Routerboard, P. Silitonga, I. Sri Morina, F. S. Ilmu Komputer Unika St Thomas, dan R. Haji Adam Malik Medan, 2014, "Analisis QoS (Quality of Service) Jaringan Kampus dengan Menggunakan,".

[15] A. T. Laksono dan M. A. H. Nasution, 2020, "Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 1, no. 2, hlm. 83, Jan 2020, doi: 10.30865/json.v1i2.1920.

[16] F. Prasetyo Eka Putra, A. Zulfikri, M. Abroril Huda, dan M. Surur, 2023, "Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Firewall Filtering Dengan Port Blocking," *Digital Transformation Technology (Digitech) | e*, vol. 3, no. 2, 2023, doi: 10.47709/digitech.v3i2.3379.

[17] G. A. Nurahma dan W. Hendriani, 2021, "Tinjauan sistematis studi kasus dalam penelitian kualitatif," *Mediapsi*, vol. 7, no. 2, hlm. 119–129, Des 2021, doi: 10.21776/ub.mps.2021.007.02.4.

[18] H. Yanto,n 2020, "Intruder Detection Monitoring System in Computer Networks Using Snort Based Sms Alert (Sistem Monitoring Deteksi Penyusup Dalam Jaringan Komputer Menggunakan Snort Berbasis Sms Alert)," *Jurnal KomtekInfo*, vol. 7, no. 2, doi: 10.35134/komtekinfo.v7i2.