Jurnal Informatika dan Teknologi (JICode) Vol.1 No.1 Halaman : 9-12, Ebruari 2024
ISSN:

ANALISIS KUALITAS LAYANAN JARINGAN INTERNET WIFI PUSDISKOM DENGAN METODE PENERATION TESTING

Anshori[1], Hasym Azwar [2], Alfina Yuliana[3]
Fakultas Sains Dan Teknologi, Universitas Nurul Huda
Email: anshori@unuha.ac.id, hasymmuhammad2@gmail.com, alfinayuliana5021@gmail.com

ABSTRAK

Penelitian ini membahas analisis kualitas layanan jaringan internet WiFi di Pusat Pendidikan Komunikasi (Pusdikom) menggunakan metode penetration *testing*. Penelitian bertujuan untuk mengevaluasi keamanan dan kinerja jaringan WiFi tersebut. Metode penetration *testing* digunakan untuk mengidentifikasi potensi kerentanan, mengukur tingkat keamanan, dan menilai respons jaringan terhadap serangan. Hasil penelitian diharapkan dapat memberikan pemahaman mendalam tentang kualitas layanan jaringan WiFi di Pusdikom, serta rekomendasi perbaikan untuk meningkatkan keamanan dan kinerja jaringan. Penelitian ini bertujuan untuk menganalisis keamanan layanan jaringan WiFi melalui penerapan metode *penetration testing*. Metode ini digunakan untuk mengidentifikasi potensi kerentanan dan risiko keamanan pada infrastruktur jaringan WiFi. Melalui serangkaian uji penetrasi, penelitian ini mengevaluasi tingkat keamanan, mengidentifikasi potensi celah keamanan, dan memberikan rekomendasi perbaikan untuk meningkatkan keamanan layanan jaringan WiFi. Hasil penelitian diharapkan dapat memberikan wawasan yang mendalam bagi administrator jaringan untuk meningkatkan keamanan infrastruktur WiFi mereka. Penelitian ini membahas analisis layanan jaringan WiFi melalui penerapan metode *penetration testing*. Tujuan utama adalah mengevaluasi keamanan jaringan dan mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak tidak berwenang. Penelitian ini menggunakan pendekatan sistematis untuk menguji integritas, kerahasiaan, dan ketersediaan layanan WiFi. Hasilnya memberikan wawasan mendalam tentang keamanan jaringan, memberikan landasan untuk perbaikan keamanan yang lebih baik dalam infrastruktur WiFi.

Kata kunci: Jaringan, Kualitas, Layanana, Metode, WiFi

1. PENDAHULUAN

Kemajuan teknologi informasi di era saat ini seperti saat ini semakin memudahkan masyarakat dalam mengakses informasi. Dengan demikian,semua jenis informasi mudah diakses melalui internet. Salah satu teknologi yang digunakan oleh data adalah teknologi transfer nirkabel. Perkembangan teknologi internet sangat pesat, dan media yang digunakan termasuk media kabel dan nirkabel juga terus berkembang pesat. *Wireless* mempunyai beberapa keunggulan dibandingkan media kabel dalam hal kemudahan akses informasi dan internet, yakni. bisa lebih mudah dan fleksibel, selain perkembangan teknologi, tingkat kejahatan dunia maya juga semakin meningkat, oleh karena itu keamanan jaringan menjadi hal yang penting. Serangan ini dilakukan untuk mengatasi masalah yang disebutkan di atas dan mencari cara untuk mencegahnya, sehingga kelayakan perlindungan jaringan area lokal nirkabel (WLAN). Kemajuan teknologi informasi dan sistem pertahanan siber saat ini berkembang dengan sangat cepat untuk mencegah pencurian data. Banyaknya pengguna internet di Indonesia tentunya memerlukan pemantauan dan keamanan sistem untuk mencegah serangan kejahatan siber. Berdasarkan laporan Pusat Operasi Keamanan Siber Negara (Pusopskamsina), pengelola Ruang Badan Siber dan Sandi Negara (BSSN)

melaporkan adanya 88.414.926 4.444 serangan siber berlangsung dari 1..20.20 Januari hingga 12 April. pola seranganyang paling umum adalahaktivitas trojan 56% dan pengumpulan data (pengumpulan data) hingga 43%[3][2][1].

Penelitian ini dilakukan di warnet Pusdiskom BK 10 tepatnya di dekat Tugu Hansip. Peneletian ini menggunakan metode *penetration testing* adalah proses menguji keamanan suatu sistem jaringan komputer dengan cara melakukan simulasi nyata. Tujuan dari *pentest* adalah mencari tahu kelemahan-kelemahan dalam sistem tadi dan mencegah adanya kemungkinan *hacking*. Jenis ini fokus pada pengujian keamanan jaringan dan infrastruktur yang digunakan oleh perusahaan. Tujuannya adalah untuk mengidentifikasi apakah ada celah keamanan pada jaringan yang dapat dimanfaatkan oleh penyerang. Keamanan *system wireless* bisa dibagi menjadi empat bagian yaitu a) Keamanan aplikasi. Yang berarti keamanan aplikasi *user* dan aplikasi standar seperti email. b) Keamanan perangkat. Bagaimana memproteksi perangkat fisik dari kasus kerusakan, hilang ataupun dicuri. c) Keamanan dari komunikasi *wireless*. Bagaimana memproteksi pesan saat dikirimkan. d) Keamanan *server* yang terkoneksi menggunakan internet atau jaringan kabel[1]. Resiko serangan yang mungkin akan terjadi pada standard 802.11b dapat dikatagorikan kedalam tujuh jenis serangan, yaitu *Insertion Attack*, *Interception* dan *Monitoring Traffic Wireless*, *Jamming* (dikenal dengan *denial of service*), *Client-to-Client Attack*, *Brute Force Attack Againts Access point Password*, *Attack againts encription*, dan *Misconfiguratio*[3].

2. METODOLOGI PENELITIAN

Pada penelitian ini kami mrnggunakan metode *Penetration Testing* adalah metode untuk mengevaluasi sistem keamanan perangkat atau komputer dengan cara mensimulasikan serangan siber secara nyata. Metode ini dilakukan oleh seseorang ahli di bidangnya yang disebut *pentester*. *Pentester* tersebut akan mencoba menemukan celah atau kerentanan dalam sistem keamanan. Pengujian penetrasi merupakan bagian dari jenis *peretasanetis* yaitu metode dan prosedur pengujian keamanan. Pengujian penetrasi adalah Tindakan mengevaluasi suatu sistem dengan melakukan serangan untuk menemukan celah keamanan pada sistem. Pada jaringan nirkabel, pengujian penetrasi digunakan untuk menambahkan *firewall kerouter* yang dapat mengurangi risiko kerentanan pada sistem atau data yang dikandungnya. Metode ini di bagi menjadi 3 bagian yaitu, a) Metode *Blackbox Testing* adalah sebuah metode yang dipakai untuk menguji sebuah *software* tanpa harus memperhatikan detail *software* [3] Pengujian ini hanya memeriksa nilai keluaran berdasarkan nilai masukan masing-masing. Tidak ada Upaya untuk mengetahui kode program apa yang *output* pakai. b) *White box testing* adalah salah satu tekni pengujian *software* yang berfokus pada komponen di dalam *software* seperti desain, struktur coding-an, dan cara kerja *software* dari awal hingga akhir. Sedangkan *black box testing* hanya melakukan penilaian fungsionalitas *software*. c) *Grey Box Testing* adalah sebuah metodologi kombinasi dari *Black Box* dan *White Box Testing*, menguji *software* berdasarkan spesifikasi tetapi menggunakan cara kerja dari dalam. *Grey Box* dapat di gunakan dengan baik dalam pengujian tim.

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian kami di warnet tersebut adalah kami dapat menganalisis jaringan wifi pusdiskom dengan mengguakan Metode *penetration testing* dan kami mengajukan pertanyaan yang sangat efektif dan membuahkan hasil yang maksimal,dari pertanyaan tersebutdan kami mendapatkan sebuah jawaban yang elegan cukup simple dari pemilik warnet tersebut[4], yaitu:

a) Mempunyai bandwith sebesar : 20mbps
b) Hasil cek speedtest : 20mbps
c) Pasword WiFi tersebut : (BISMILAH123)
d) Rating Kecepatan : 7-10
e) Pengguna WiFi : Pegawai dan Pelanggan

Dalam proses yang dilakukan tentu ada beberapa aspek yang dapat kami pertimbangkan dalam hasil analisis jaringan WiFi Pusdiskom[5], yaitu:

1) Keamanan Jaringan:
   Evaluasi jaringan dilakukan dengan melakukan evaluasi penggunaan protokol keamanan seperti WPA3, WPA2, atau WEP. Selain melakukan evalasi jaringan selanjutnya dilakukan periksa konfigurasi sandi yang kuat dan kebijakan otentikasi yang tepat.
2) Frekuensi dan Kanal.
   Pada aspek frekuensi dan kanal dilakukan optimalisasi penggunaan frekuensi dan kanal untuk menghindari interferensi. Pada optimalisasi dilakukan juga identifikasi perangkat yang menggunakan frekuensi yang sama.
3) Kecepatan dan Kinerja.
   Pada aspek ini dilakukan pengukuran kecepatan transfer data di berbagai lokasi dalam jaringan. Serta Identifikasi faktor yang mempengaruhi kinerja, seperti hambatan fisik atau interferensi elektromagnetik.
4) Monitoring Trafik.
   Pada aspek monitoring trafik dilakukan peninjauan lalu lintas jaringan untuk mendeteksi anomali atau aktivitas mencurigakan.

Dari pembahasan yang telah dilakukan dengan tahapan-tahapan proses dan peninjauan aspek-aspek penilaian maka didapatkan hasil dari penelitian analisis jaringan WiFi Pusdiskom, yaitu :

1) Keamanan Jaringan
   Pada hasil keamanan jaringan terdapat penggunaan kata sandi yang kuat dan enkripsi WPA3 pada sebagian besar perangkat. Maka direkomendasikan pada user untuk rutin memperbarui kata sandi dan memastikan seluruh perangkat menggunakan enkripsi yang aman.
2) Kualitas Signal.
   Hasil pada kualitas signal beberapa area memiliki kualitas sinyal yang rendah, mungkin disebabkan oleh interferensi. Rekomendasi pemetaan ulang perangkat dan penyesuaian saluran untuk mengoptimalkan kualitas sinyal.
3) Jumlah Perangkat Terhubung.
   Hasil pada jumlah perangkay yang terhubung dalam batas normal, tetapi perangkat yang tidak dikenal ditemukan. Rekomendasi: Periksa dan identifikasi perangkat yang tidak dikenal, dan perbarui kebijakan keamanan.

4. KESIMPULAN

Kesimpulan yang kami dapat dari menganalisis jaringan wifi pusdiskom dengan mengguakan Metode Peneration Testing adalah Terdapat penggunaan kata sandi yang kuat dan enkripsi WPA3 pada sebagian besar perangkat. Rekomendasi: Rutin memperbarui kata sandi dan memastikan seluruh perangkat menggunakan enkripsi yang aman. Pembaruan sandi dapat meminimalisirkan masuknya jaringan yang tidak dikenali dam menghindari serangan yang tidak di kenali.

DAFTAR PUSTAKA

[1] A. Pratama, D. Syamsuar, F. I. Komputer, dan U. B. Darma, “Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (Ptes) Dprd Provinsi Sumatra Selatan,” hal. 441–446.

[2] G. Aryo *et al.*, “Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing di SMK Xyz Tana Toraja,” *Anal. Keamanan Jar. Wirel. Menggunakan Metod. Penetration Test. di SMK Xyz Tana Toraja*, vol. 2, no. 2, hal. 1–7, 2022, [Daring]. Tersedia pada: https://doi.org/10.47178/infinity.v2i2

[3] R. W. Ismail dan R. Pramudita, “Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi,” *J. Mhs. Bina Insa.*,

vol. 5, no. 1, hal. 53–62, 2020.

[4] R. Rachman, "Analisis Keamanan Jaringan Wireless Lan(Wlan) Dengan Metode Penetration TestingPada Pt.Pln (Persero) Sektor PengendalianPembangkitan Pekanbaru," *Skripsi*, 2021.

[5] Harry Dwi Sabdho dan Ulfa Maria, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang," *Semhavok*, vol. 1, no. 1, hal. 15–24, 2018.