ANALISA KEAMANAN JARINGAN *WLAN* DENGAN METODE *PENETRATION TESTING* DI PT. INDONESIA POWER PLTU JABAR 2 PALABUHANRATU OMU

SKRIPSI

QANSA ALGHIFARI

17184057

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS NUSA PUTRA

SUKABUMI

2021

ABSTRAK

Penggunaan jaringan komputer abad ini sangat berguna dalam segala dari bidang pendidikan hingga industri telah menggunakan jaringan komputer dalam menunjang kegiatannya. PT. Indonesia Power JABAR 2 Palabuhanratu OMU memiliki sistem jaringan *WLAN* yang terpasang hampir di seluruh area pembangkit, hal ini bertujuan untuk menunjang aktifitas operasional perusahaan. Aspek keamanan jaringan *WLAN* harus diperhatikan dan diimplementasikan dengan baik.

Untuk mengetahui kondisi suatu aspek keamanan jaringan WLAN, perlu dilakukan analisa dari aspek keamanan dengan melakukan pengujian, salah satu pengujian yang dapat dilakukan adalah menggunakan metode *penetration testing.* Dalam metode tersebut dapat dilakukan beberapa pengujian seperti *Cracking The Encryption, Spoofing MAC address, Denial of Service,* dan *Packet Sniffing.*

Berdasarkan analisis data dari hasil pengujian yang dilakukan, sistem jaringan *WLAN* milik PT. Indonesia Power JABAR 2 Palabuhanratu OMU, sudah terlindungi dengan baik dari serangkaian pengujian serangan yang telah dilakukan.

Kara kunci : Analisa , Keamanan jaringan, *WLAN*, *Penetration Testing*

ABSTRACT

The use of computer networks in this century is very useful in everything from education to industry has used computer networks to support its activities. PT. Indonesia Power JABAR 2 Palabuhanratu OMU has anetwork system WLAN installed in almost all generating areas, this aims to support the company's operational activities.network security aspects WLAN must be considered and implemented properly.

To find out the condition of a security aspect of a WLAN network, it is necessary to analyze the security aspect by conducting tests, one of the tests that can be done is using themethod penetration testing. In this method, several tests can be carried out such as Cracking The Encryption, Spoofing MAC addresses, Denial of Service, and Packet Sniffing.

Based on data analysis from the results of tests carried out, thenetwork system WLAN belonging to PT. Indonesia Power JABAR 2 Palabuhanratu OMU, has been well protected from a series of attack tests that have been carried out.

Keywords : Analysis, Network security, WLAN, Penetration Testing

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

PT. Indonesia Power merupakan salah satu anak Perusahaan PT. PLN (Persero) yang didirikan pada tanggal 3 Oktober 1995 dengan nama PT. PLN Pembangkitan Jawa Bali I (PT PJB I). Pada tanggal 8 Oktober 2000, PT. PJB I berganti nama menjadi PT. Indonesia Power. Ruang Lingkup Usaha Perusahaan adalah berfokus pada Operasi dan Pemeliharaan Pembangkit Listrik dan Pengembangan Bisnis Solusi Energi. PT. Indonesia Power JABAR 2 Palabuhanratu OMU mengelola PLTU JABAR 2 Palabuhanratu dengan kapasitas 3 X 350MW, yang merupakan Objek Vital Nasional (OBVITNAS), berlokasi di Jl. Raya Pelita Kp. Cipatuguran Desa Jayanti, Kec. Pelabuhanratu, Kab. Sukabumi -Jawa Barat 43364 [1].

Penggunaan jaringan komputer abad ini sangat berguna dalam segala aspek dan sudah menjadi kebutuhan primer bagi sebagian orang. Dari bidang pendidikan hingga industri telah menggunakan jaringan komputer dalam menunjang kegiatannya. Jenis-jenis jaringan komputer berdasarkan area adalah *LAN* (Local Area Network), *WAN* (Wide Area Network), dan *MAN* (Metropolitan Area Network).Jaringan *LAN* adalah jaringan komputer yang hanya mencakup wilayah kecil, seperti jaringan komputer kampus ,gedung, kantor, dan rumah, sekolah atau yang lebih kecil [2]. Penggunaan *LAN* dapat melalui dua media yaitu kabel dan nirkabel atau disebut *WLAN* (Wireless Local Area Network).

Saat ini PT. Indonesia Power JABAR 2 Palabuhanratu OMU memiliki sistem jaringan *WLAN* yang terpasang hampir di seluruh area pembangkit, hal ini bertujuan untuk menunjang aktifitas pertukaran data operasional perusahaan seperti data kepegawaian, laporan kinerja pembangkit, biaya operasional dan data penting lainnya dalam mengelola pembangkit. PT. Indonesia Power JABAR 2 Palabuhanratu OMU merupakan Objek Vital Nasional dengan pengelolaan pembangkit yang melibatkan banyak pekerja dan mitra,maka aspek

kemanan jaringan yang ada, perlu diperhatikan dan diimplementasikan dengan baik, agar jaringan yang digunakan aman dari eksploitasi oleh pihak yang tidak bertanggung jawab dan terhindar dari terganggunya kelancaran pengelolaan pembangkit hingga dapat tercurinya data penting melalui jaringan.

Berbagai macam serangan yang mungkin terjadi pada jaringan *WLAN* diantaranya adalah *Packet Sniffing*, DOS (*Denial of Service*), *Spoofing MAC address*, dan *Eavesdropping*. Beberapa metode yang dapat dilakukan untuk pengujian aspek keamanan jaringan *WLAN* diantaranya adalah *War Driving* dan *Penetration Testing*. *War driving* adalah kegiatan yang bergerak mengelilingi area tertentu dan memetaka populasi *access point wireless* untuk tujuan statistik. *Wardriving* bergerak mengelilingi area yang sudah dipetakan rutenya untuk menentukan *access point wireless* pada area tersebut [3]. *Penetration Testing* atau *PenTest* merupakan cara melakukan pengujian terhadap sistem jaringan komputer dengan mensimulasikan bentuk-bentuk serangan terhadap jaringan [4]. Metode *penetration testing* digunakan dalam penelitian ini karena sesuai dengan kebutuhan penelitian dan memiliki beberapa jenis pengujian serangan yang dapat dilakukan untuk menguji aspek keamanan jaringan.

Rizky Wahyu Ismail, Rully Pramudita, dari Universitas Bina Insani pada tahun 2020 telah melakukan penelitian dengan judul "Metode *Penetration Testing* pada Keamanan Jaringan *Wireless Wardriving* PT.Puma Makmur Aneka Engineering Bekasi" [3].Kemudian Harry Dwi Sabdho, Maria Ulfa dari Universitas Bina Darma Palembang pada tahun 2018 dengan penelitian berjudul Analisis Keamanan Jaringan *Wireless* Menggunakan Metode *Penetration Testing* Pada Kantor PT. Mora Telematika Indonesia Regional Palembang [5]. Dalam penelitian ini diharapkan dapat membantu dalam mencari celah aspek keamaanan *WLAN* dengan metode *penetration testing* dan memberikan rekomendasi untuk meningkatkan aspek keamanan jaringan *WLAN* yang ada di PT. Indonesia Power JABAR 2 Palabuhanratu OMU.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah yang sudah dijelaskan, terdapat rumusan masalah sebagai berikut;

1. Bagaimana kondisi aspek kemanan jaringan *WLAN* di PT. Indonesia Power JABAR 2 Palabuhanratu OMU.
2. Bagaimana cara melakukan pengujian aspek keamanan jaringan *WLAN* menggunakan metode *penetration testing* di PT. Indonesia Power JABAR 2 Palabuhanratu OMU.

1.3 Batasan Masalah

Batasan masalah dalam penelitian yang akan penulis lakukan adalah :

1. Pengujian hanya menggunakan metode *penetration testing* dan dilakukan di PT. Indonesia Power JABAR 2 Palabuhanratu OMU.
2. Pengujian serangan yang akan penulis lakukan berupa *Cracking The Encryption, Spoofing MAC address, Denial of Service,* dan *PacketSniffing.*
3. Penulis hanya melakukan analisis terhadap pengujian aspek keamanan jaringan *WLAN* yang dilakukan dan memberi usulan atau masukan yang dapat dilakukan untuk meningkatkan aspek keamanan jaringan *WLAN*.

1.4 Tujuan Penelitian

Tujuan dalam penelitian yang akan penulis lakukan adalah :

1. Mengidentifikasi aspek keamanan jaringan *WLAN* di PT. Indonesia Power PLTU JABAR 2 Palabuhanratu OMU.
2. Menemukan celah keamanan jaringan *WLAN* di PT. Indonesia Power PLTU JABAR 2 Palabuhanratu OMU dengan metode *penetration testing*.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah :

1. Dapat menemukan celah pada aspek keamanan jaringan *WLAN.*
2. Dapat mengetahui cara melakukan pengujian keamanan jaringan *WLAN* menggunaan metode *penetration testing*.
3. Dapat menjadi dokumen rekomendasi dalam meningkatkan aspek keamanan jaringan *WLAN*.

1.6 Sistematika Penulisan

Sistematika penulisan dari penelitian yang akan dilakukan adalah :

1. Bab 1 Pendahuluan

   Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian,

2. Bab II Tinjauan Pustaka

   Bab ini memuat rujukan atau landasan untuk penelitian yang dilakukan. Dapat berupa penelitian terkait, landasan teori, dan kerangka pemikiran dalam melakukan penelitian.

3. Bab III Metode Penelitian

   Bab ini berisikan prosedur, alat-alat, & bahan yg dipakai pada penelitian yang bersifat spesial & spesifik untuk penelitian yang dirancang. Sehingga jika metode ini dilakukan sekali lagi oleh peneliti yangg berbeda, maka akan diperoleh hasil yang sama dengan peneliti sebelumnya. Ini siesuai dengan prinsip objektivitas pada pandangan positivisme.

4. Bab IV Hasil dan Pembahasan

   Bab ini berisikan hasil dan pembahasan dari penelitian yang dilakukan oleh penulis.

5. Bab V Penutup

Bab ini berisikan kesimpulan dan saran dari penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] I. Power, “Indonesia Power,” 2017. https://www.indonesiapower.co.id/id/profil/Pages/Sekilas-Indonesia-Power.aspx.

[2] Ewa Haris Sembiring and Novendra, “Perancangan Jaringan LAN Menggunakan Software Cisco Paket Tracer Di SMKN1 Minas,” *Univ. Lancang kuning*, pp. 1–15, 2019.

[3] R. W. Ismail and R. Pramudita, “Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi,” *J. Mhs. Bina Insa.*, vol. 5, no. 1, pp. 53–62, 2020.

[4] I. K. Bayu, M. Yamin, and L. F. Aksara, “Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO,” *SemanTIK*, vol. 3, no. 2, pp. 69–78, 2017.

[5] H. D. Sabdho and M. Ulfa, “Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang,” *Semhavok*, vol. 1, no. 1, pp. 15–24, 2018.

[6] D. M. Sari, M. Yamin, and L. B. Aksara, “Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing,” *SemanTIK*, vol. 3, no. 2, pp. 203–208, 2017, doi: 10.1016/j.neuropharm.2007.08.010.

[7] L. D. Samsumar, K. Gunawan, D. Program, S. Manajemen, D. Program, and S. Komputerisasi, “Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi,” *Ilm. Teknol. Inf. Terap.*, vol. IV, no. 1, pp. 73–82, 2017.

[8] S. Kharisma Riyanti, “Analisis Kelemahan Keamanan Jaringan Wireless Pada RS. Surya Asih Menggunakan QoS,” vol. Vol 6, No, 2018, [Online]. Available: http://www.ojs.stmikpringsewu.ac.id/index.php/kmsi/article/view/651/583#.

[9] S. S. S. Naibaho, “ANALYSIS OF WIFI NETWORK SECURITY AGAINST PACKET.”,2017.

[10] H. Haeruddin and A. Kurniadi, “Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6),” *Comb. Manag. Business, Innov. Educ. Soc. Sci.*, vol. 1, no. 1, pp. 508–515, 2021.

[11] T. Adi Kurniawan, “ANALISA KEAMANAN JARINGAN WIFI TERHADAP SERANGAN PACKET SNIFFING,” vol. 2507, no. February, pp. 1–9, 2020.