ANALISIS KEAMANAN JARINGAN PADA LAYANAN INTERNET PUBLIK MENGGUNAKAN METODE *PENETRATION TESTING EXECUTION STANDARD* (PTES) DPRD PROVINSI SUMATRA SELATAN

Angga Pratama[1], Dedy Syamsuar[2]
Fakultas Ilmu Komputer,Universitas Bina Darma
Email: Ap186702@gmail.com[1], dedy_syamsuar@binadarma.ac.id[2]

ABSTRACT

The development of internet technology is very fast, and the media used is also growing rapidly,including wired and wireless media. The DPRD for the province of South Sumatra is one of the centers ofgovernment, which provides various services to the community, so that every employee and staff accessesone Wireless Local Area Network (WLAN) which uses only one SSID where all important data sharing activities are in one network. This security test is done by looking for security holes in the WLAN network. Therefore, the authors conducted an experiment with the Penetration Testing Execution Standard (PTES) method using four parameters, namely ARP Spoofing attack, Bypassing MAC Authentication, Cracking The Encryption and Man In The Middle Attack to test the security level of the existing WLAN network. The results of the four parameters of the attack carried out, namely three successfully run in one try, it can be concluded that the security system of the Secretariat of the South Sumatra Provincial Dprd Secretariat is safe but can still be attacked by attacks bypassing MAC Address, ARP Spoofing and Man In The Middle Attack. so that security is more guaranteed to activate the MAC Filtering feature and for passwords use a combination of numbers, symbols, capital and small letters at least 8 characters.

Keywords: *WLAN, Penetration Testing Execution Standard (PTES), ARP Spoofing, Bypassing MAC Authentication, Cracking The Encryption, Man In The Middle Attack, network security.*

ABSTRAK

Perkembangan teknologi internet sangat pesat, dan media yang digunakan juga terus berkembang dengan cepat, diantaranya adalah media kabel dan nirkabel *(wireless*). DPRD provinsi Sumatra selatan adalah salah satu pusat pemerintahan, yang memberikan berbagai macam layanan kepada masyarakat untuk itu setiap karyawan dan staff mengakses satu jaringan *Wireless Local Area Network* (WLAN) yang hanya menggunakan satu SSID dimana semua aktivitas sharing data-data penting dalam satu jaringan. Pengujiankeamanan ini dilakuan dengan mencari celah keamanan yang terdapat pada jaringan WLAN. Maka dari itu penulis melakukan percobaan dengan Metode Penetration Testing Execution Standard (PTES) menggunakan empat parameter yaitu serangan ARP *Spoofing, Bypassing MAC Authentication, Cracking The Encryption* dan *Man In The Middle Attack* untuk menguji tingkat keamanan jaringan WLAN yang ada. Hasil dari empat parameter serangan yang dilakukan yaitu tiga berhasil dijalankan dalam satu kali percobaan, maka dapat disimpulkan bahwa sistem keamanan jaringan wireless Sekretariat Dprd Provinsi Sumatra Selatan sudah aman akan tetapi masih bisa diserang oleh serangan *bypassing* MAC *Address*, ARP *Spoofingdan Man In The Middle Attack*, agar kemanan lebih terjamin diaktifkan fitur MAC Filteringdan untuk password mengunakan kombinasi angka, simbol, huruf kapital dan kecil minimal 8 karakter.

Kata Kunci: WLAN, *Penetration Testing Execution Standard* (PTES), ARP Spoofing, *Bypassing MACAuthentication, Cracking The Encryption, Man In The Middle Attack*, keamanan jaringan.

1. PENDAHULUAN

Perkembangan teknologi internet sangat pesat, begitupun dengan media yang digunakan juga terus berkembang dengan cepat, diantaranya adalah media kabel dan nirkabel (*wireless*). *Wireless* memiliki beberapa keunggulan dibandingkan dengan media kabel dalam hal kemudahan mengakses data dan mengakses internet, yaitu bisa lebih mudah dan fleksibel, selain perkembangan teknologi tingkat kejahatan dunia maya juga ikut meningkat sehingga perlu akan pentingnya keamanan jaringan.

Sekretariat DPRD provinsi Sumatra selatan merupakan salah satu tempat karyaran pegawai honor kerja menggunakan, Layanan internet yang digunakan adalah jaringan *Wireless Local Area Network* (WLAN) yang menggunakan satu wireless access poin untuk mengakses jaringan lokal dan internet, wifi pada skretarit memiliki keamanan WPA2-PSK yang memiliki kelemahan yaitu password wifi dapat di *crack* serta wifi sekretariat DPRD tersebut belum mengaktifkan MAC *address filtering* sehingga siapa saja bisa masuk karena tidak ada pembatasan MAC address, ini berbahaya karena wifi dapat terkena serangan dari orang yang tidak bertanggung jawab. Berdasarkan permasalahan diatas penulis melakukan penetrasi serangan dengan menggunakan empat parameter yaitu ARP *Spoofing, Bypassing* MAC *Authentication, Cracking The Encryption* dan *Man In The Middle Attack*

Serangan ini dilakukan bertujuan untuk mengatasi permasalahan diatas dan menemukan cara pencegahan nya, maka perlu dilakukan pengujian untuk mengetahui kelakayan keamanan internet publik *Wireless Local Area Network* (WLAN). Salah satu metode yang digunakan untuk pengujian sistem keamanan tersebut adalah dengan metode *penetration testing*. Penetration testing adalah salah satu metode yang digunakan untuk melakukan analisis terhadap suatu objek yang akan dipenetrasi. Dari uraian diatas, maka penulis tertarik untuk mengangkat judul "Analisis Keamanan Jaringan Pada Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (PTES)".

2. METODOLOGI PENELITAN

2.1 Kerangka Berfikir

Dalam menjelaskan sebuah permasalahan kerangka berfikir atau alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut.

2.2 Tmeline Penelitian

Dalam penelitian yang dilakuakan, diperlukan timeline atau batasan waktu agar apa yang akan dilakukan dapat terencana dengan baik, berikut adalah timeline yang dibuat oleh penulis dalam penelitian ini.

2.3 Analisis Permasalahan

Jaringan *Wireless Local Area Network (*WLAN) sebagai sarana untuk pekerja dan pengunjung untuk mengakses jaringan internet melalui *Smart phone* dan *Personal Computer* (PC). *wifi* pada seketariat memiliki keamanan WPA2-PSK yang memiliki kelemahan yaitu *password wifi* dapat di *crack* serta wifi padaseketriat tersebut belum mengaktifkan MAC *address filtering.*

2.4 Threat Modeling

Pada proses ini penulis berfokus pada pengidentifikasian sebuah ancaman (*threat*) terhadap target yang bertujuan untuk mepermudah menentukan serangan, target yang akan diidentifikasi adalah jaringan *Wireless Local Area Network* (WLAN) yang terdapat pada Sekretariat DPRD Provinsi SumatraSelatan karena memiliki celah keamanan.

2.5 Skema Penyerangan atau Implementasi Penyerangan

Pada tahap ini adalah proses lanjutan dari metode *penetration testing execution standart* (PTES) yang membahas tentang pencarian celah keamanan berdasarkan informasi yang diperoleh, melakukan serangan, analisis sistem yang ada dan dampak dari serangan yang dilakukan dan memberikan hasil laporan yang dapat digunakan untuk memperbaiki celah keamanan yang ada

2.6 Konsep dan Arsitektur Jaringan komputer

Menurut Iwan Sofana [3] "Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer, dalam bahasa populer dapat di jelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer, dan perangkat lain seperti router, switch dan sebagainya". Alat yang bisa terhubung dengan satu lainya untuk memudahkan memahami jaringan komputer para ahli sudah membagi beberapa klasifikasi, di antaranya berdasarkan area atau skala, berdasarkan media transmisi data atau penghantar, dan berdasarkan fungsi, "Jaringan komputer merupakan gabungan antara teknologi komputer dan teknologi komunikasi". Sopandi [4]. Perkembangan teknologi jaringan komputer semakin memudahkan masyarakat dalam memenuhi kebutuhan informasi. Salah satu teknologi yang dikembangkan adalah teknologi media transmisi nirkabel atau *wireless*.

2.7 Topologi Jaringan Komputer

Menurut Iwan Sofana [3] "Topologi dapat diartikan sebagai layout atau arsitektur atau diagram jaringan komputer. Topologi merupakan suatu aturan atau *rules* bagaimana menghubungkan komputer (*node*) secara fisik. Topologi berkaitan dengan cara komponen-komponen jaringan (seperti: *server, workstation, router, switch*) saling berkomunikasi melalui media transmisi data. Ada dua kategori topologi yaitu *Physical topology* (Topologi Fisik) berkaitan dengan layout atau bentuk jaringan. Sedangkan topologi logika berkaitan dengan bagaimana data mengalir di dalam topologi fisik. Jika topologi fisik diibaratkan seperti tubuh, maka topologi logika dapat diibaratkan seperti aliran darah yangmengalir dalam tubuh.

2.8 Keamanan Jaringan

Menurut Santoso [2] Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebih besar dari pada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun network security biasanya bertentangan dengan network access, dimana bila network access semakin mudah, maka network security semakin rawan, begitu pula sebaliknya. Menurut Bayu, Yamin, & Aksara [1] Sebuah sistem yang aman (*secure system*) diasumsikan sebagai sebuah sistem dimana seorang *intruder* harus mengorbankan banyak waktu, tenaga, dan biaya besar yang tidak dikehendakinya dalam rangka penyerangan tersebut, atau resiko yang harus dikeluarkan sangat tidak sebanding dengan keuntungan yang akan diperoleh.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Data

Pada tahapan ini penulis melakukan implementasi sesuai dengan tahapan-tahapan dari metode Penetration Testing Execution Standard (PTES) yang sudah dijelaskan pada sub bab sebelumnya. Dimana penulis melakukan simulasi serangan untuk mengetahui keamanan jaringan WLAN di sekretariat dprd, dengan melakukan serangan ARP Spoofing, Bypassing MAC Authentication, Cracking The Encryption dan Man In The Middle Attack. Penetrasi yang dilakukan yaitu tipe Overt penetration testing dimana penulis melakukan pengujian keamanan jaringan dengan sepengetahuan sekretariat tersebut.

3.2 Implemtasi Penyerangan

Cracking The Encryption dengan menggunakan tools aircrack-ng Serangan Cracking The Encryption terhadap jaringan yang menggunakan WPA2- PSK dengan tools aircrack-ng dan metode bruto force berdasarkan dictionary file. Bruto force membutuhkan sebuah file yang berisi passphrase yang akan dicoba satu persatu dengan paket handshake untuk mencari keys yang digunakan. Adapun serangan dilakukan sebanyak dua kali Adapun serangan dilakukan sebanyak dua kali yang pertama gagal dan serangan ke dua berhasil, penulis mendapatkan password dari wifi yang berada di ruangan sekretariat dengan cara social engginering artinya melakukan pendekatan dengan mengamati sekretariat tersebut dan mengumpulkan kata-kata yang dimungkinkan untuk dijadikan password. Selanjutnya kumpulan kata-kata tersebut dimasukan kedalam wordlist, dengan menggunakan metode bruto force membantu kita untuk mencari password sebenarnya. Artinya password wifi dengan keamanan WPA2-PSK bisa ditebak dengan memasukan kata-kata kedalam wordlist yang sudah dibuat oleh penulis. Berikut adalah tampilan dari proses Cracking The Encryption yang dilakukan oleh penulis dengan menggunakan tools Aircrack-ng.

3.3 Report dari metode Penetration Testing Execution Standard (PTES)

Dari seluruh tahap pengujian yang telah dilakukan, maka penulis dapat menyampaikan hasil dari Penetration Testing Execution Standard pada jaringan *Wireless Local Area Network* (WLAN) yang dilakukan pada Sekretariat Dprd. Berikut adalah laporan dari hasil pengujian keamanan.

Table 1. Hasil dari pengujian Penetration Testing Execution Standard (PTES)

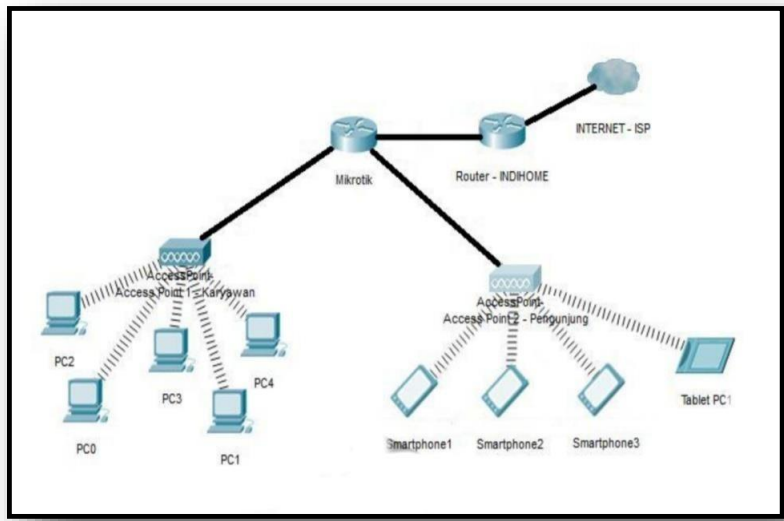
Pengujian	Batasan Serangan	Alat Bantu	Status Serangan
Cracking theencryption	*Dictionary Word, Handshake* user lain, Channel yang digunakandan BSSID dari *access* poin.	Aircrack-ng	Gagal Berhasil
ARP *Spoofing*	IP user MAC *address*, satu jaringan WLAN	TuxCut	Berhasil
Bypassing MAC Address	List MAC User lain yangterhubung di jaringan	Macchanger	Berhasil
Man In The Middle Attack	*Ip address, file extention .bat dan* terhubung dijaringan	Keylogger	Berhasil

3.4 Evaluasi

Dari hasi metode Penetration Testing Execution Standard yang dilakukan pada sekretariat dprd. Maka diketahui bahwa keamanan jaringan Wireless Local Area Network (WLAN) yang digunakanadalah jenis WPA2-PSK (Wi-Fi Protected Access - Pre-Shared Key) Personal.

3.5 Usulan Infrastruktur

Setelah dilakukan pengujian celah keamanan jaringan dengan metode *Penetration Testing Execution Standard* pada jaringan *Wireless Local Area Network* (WLAN) di sekretariat DPRD, makapenulis memberikan usulan untuk infrastruktur keamanan jaringan yang lebih baik. Berikut adalah bagan dari keamanan WLAN infrastruktur yang diusulkan oleh penulis kepada sekretariat



Gambar 1. Infrastrukture yang diusulkan

Penulis mengusulkan menggunakan tambahan mikrotik dalam perancangan infrastruktur yang baru, agar dapat membuat halaman login (captive portal) agar setiap user harus login dengan username dan password yang diberikan. Hal ini bertujuan agar tidak sembarangan orang bisa mengakses jaringan tersebut, karena hanya orang yang mempunyai username dan password yang bisa masuk kedalam jaringan.

Menggunakan 2 access point ke dalam 1 mikrotik. Access point pertama khusus untuk karyawan sekretariat dan access point kedua khusus untuk pengunjung yang datang. Hal ini dibuat agar komunikasi data tidak saling tergangu dan lebih aman karena adanya perbedaan jalur data dan komunikasi dalam jaringan wireless dan jika terdapat kerusakan pada salah satu access point akan ada access point yang lainnya yang bisa digunakan sementara.

4. KESIMPULAN

Pengujian keamanan jaringan Wireless Local Area Network (WLAN) dengan menggunakan metode Penetration Testing Execution Standard (PTES) di DPRD Sekretariat Prompinsi Sumatra Selatan melalui pengujian serangan cracking the encryption, Bypassing MAC Address, ARP Spoofing, dan Man in the middle Attack..

Dari hasil pengujian tersebut menunjukkan bahwa keamanan jaringan Wireless Local Area Network (WLAN) pada DPRD Sekretariat Prompinsi Sumatra Selatan sudah aman, karena access point atau router jaringan Wireless Local Area Network (WLAN) yang tersedia sudah menerapkan sistem keamanan setingkat WPA/WPA2-PSK tapi masih bisa tembus jika passwordnya terdapat di dalam data base word list yang sudah dibuat dan di jalankan dengan teknik bruto force.

Celah keamanan pada jaringan wireless yang terdapat pada DPRD Sekretariat Prompinsi Sumatra Selatan adalah pengaturan dan infrastruktur yang masih perlu untuk perbaikan karena infrastruktur yang sekarang juga memperngaruhi tingkat keamanan pada suatu jaringan, dan pengguna yang sedang menggunakan jaringan Wireless Local Area Network (WLAN) masih bisa diserang karena kurangnya edukasi tentang kejahatan di dunia maya sekarang ini sehingga

memanfaatkan human error untuk melakukan serangan Man In The Middle Attack (MITM), dan melakukan serangan lain pun ternyata berhasil dengan menggukanan teknik bypassing MAC Address dan ARP Spoofing serangan ini mengarah pada wireless yang terdapat celah keamananya

DAFTAR PUSTAKA

[1] Bayu, I. K., Yamin, M., & Aksara, L. F. J. s. (2017). *Analisa Keamanan Jaringan WLAN Dengan Metode Penetration Testing* (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO). *3*(2).
[2] Santoso, J. D. (2019). *Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System*. *1*(3), 44-50.
[3] Sofana, Iwan (2015). *Membangun Jaringan Komputer: Mudah membuat Jaringan Komputer (Wire & Wireless) untuk Pengguna Windows dan Linux*: Bandung: Informatika Bandung.
[4] Sopandi, D. (2006). *Instalasi dan konfigurasi jaringan komputer*.