BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan internet saat ini merupakan kebutuhan mutlak dan menjadi kebutuhan pokok pada perkembangan jaman di masyarakat khususnya pada Informasi dan Komunikasi pada saat ini, bahkan untuk sebagian orang, mereka memerlukan informasi kapan pun dan dimanapun mereka berada. Dan teknologi yang mampu memenuhi kebutuhan tersebut adalah teknologi *wireless*.

Teknologi jaringan *Wireless* saat ini merupakan salah satu bentuk perkembangan di sektor telkomunikasi. Dalam penerapan teknologi jringan *Wireless* bukan berarti tidak mempunyai masalah yang harus dihadapi, salah satu masalah yang dihadapi adalah sistem keamanan pada teknologi jaringan *Wireless*.

Masalah yang akan dihadapi apabila menerapkan jaringan *Wireless* adalah isu tentang keamanaanya. Banyak pihak yang menyakini bahwa sistem keamanan *Wireless*, dan banyak pula pihak yang menyakini bahwa sistem keamanan *Wireless* yang mengunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan yang lain.

Berdasrakan hasil studi pustaka yang dilakaukan, sistem keamanan yang benar-benar mampu memberikan keamanan lebih *Source* adalah dengan mengunakan sistem keamanan *Remot Authentication Dial In User Service* (RADIUS) *Server* mengunakan *Authentication* captive portal. Namun pada saat ini, banyak pihak yang masih mengunakan kemananan WPA2-PSK Sebagai sistem

keamanan *Wireless* mereka untuk menghindari kemungkinan pengunaan akses internet secara ilegal oleh pihak yang tidak memiliki hak akses. Permasalahan yang dihadapi adalah membandingkan sistem keamanan jaringan *Wireless* WPA2-PSK dengan *Remote Authentication Dial In User Service* (RADIUS) *Server* Mikrotik Mengunakan Metode Penetration Testing

Dari Penelitian yang dilakukan adalah melakukan analisis sistem keamanan WPA2-PSK dan RADIUS *Server* dengan *Captive Portal* mengunakan metode wireless penetration testing. Unutk menghasilkan sistem keamanan mana yang lebih aman digunakan pada jaringan *Wireless* saat ini.

1.2 Rumusan Masalah

Dari penjelasan latar belakang diatas , maka dapat dirumuskan masalah sebagi berikut:

1. Bagaimana metode *Penetration Testing* dapat digunakan untuk mencari celah dan kerentanan dalam keamanan jaringan *nirkabel*.?
2. Bagaimana hasil dari perbandingan dua sistem keamanan WPA2-PSK dan RADIUS Server yang ada di jaringan *Wireless*.?

1.3 Batasan Masalah

Agar penelitian ini tidak menyimpang dari perumusan masalah maka penulis membatasi pembahasan dan penelitian skripsi ini. Adapun batasan yaitu:

1. Metode yang digunakan pada pengujian ini adalah *penetration testing*.
2. Aplikasi yang digunakan untuk mencari kelemahan, dan kerentanan keamanan *wireles* yang diuji adalah Whireshark,Nessus, dan

Aircrack-ng, nantinya akan dipilih dan dibandingkan mana yang lebih efektif.

3. Pengujian yang dilakukan hanya melakukan penelitian pada jaringan *Wireless*.
4. Pengujian yang dilakukan hanya menguji kekuatan dan kelemahan dari WPA2-PSK dan RADIUS Server.
5. Menggunakan Indihome sebagai layanan internet.
6. Sistem operasi yang digunakan pada komputer adalah Windows 10 dan Ubuntu 16.04 TLS.
7. Penelitian yang dilakukan mengunakan *Router* mikrotik RB951Ui-2HnD.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Maksud dari penelitian ini adalah menemukan celah dan kerentanan pada sistem keamanan WPA2-PSK dan Radius Server mengunakan metode *Wireless Penetration Testing*.

1.4.2 Tujuan

Tujuan dari penyusuna skripsi ini, adalah:

1. Memberikan informasi tentang kerentannan keamanan WPA2-PSK dan Radius Server dalam sebuah jaringan *Wireless*.
2. Menentukan sistem keamanan mana diantara WPA2-PSK dan RADIUS serer yang lebih *Source*.

3. Memberikan informasi mana sistem keamanan yang lebih *source* jika digunakan dalam jaringan *Wireless.*
4. Untuk memenuhi persyaratan gelar sarjana di Universitas Amikom Yogyakarta.

a. Manfaat Penelitian

Hasil dari penulisan skripsi ini, antara lain:

1. Pembaca dapat mengetahui tentang adanya analisis dalam jaringan *Wireless.*
2. Pembaca dapat memahami masalah keamanan yang terdapat dalam jaringan *wireless.*
3. Diketahuinya informasi untuk mengamankan sebuah jaringan *Wireless* agar terhindar dari serangan, dan meningkatkan kinerja jaringan *Wireless.*
4. Memberikan masukan terhadap para administrator jaringan dalam membangun jaringan *Wireless,* sehingga dapat menjaga sistem yang ada didalamnya.

b. Metode Penelitian

Metode yang digunakan dalam penelitian skripsi ini mengunakan metode *Wireless Penetration Testing.*

1.6.1 Metode *penetration testing*

Tahapan dalam metode *Wireless Penetration Testing,* meliputi:

1.6.1.1 *Intelligence Gathering*

Tahap ini merupakan tahap pengumpulan informai pada jaringan, layanan aplikasi, pencarian informasi tentang obyek atau foot printing pada ruang lingkup yang telah ditetapkan. Selama tahap ini penguji mencoba mengidentifikasikan mekanisme perlindungan yang ada pada sistem.

1.6.1.2 *Vulnerability Analysis*

Pada tahap ini penguji mencari dan menetapkan tingkat kemanan. Analisa terhadap kemungkinan kerentanan yang ditentukan akan memunculakan laporan teknis seperti port yang terbuka, dan lain lain.

1.6.1.3 *Threat Modeling*

Berdasarkan informasi yang didapatkan dari tahap-tahap sebelumnya, pada tahap ini penguji akan menentukan serangan yang efektif.

1.6.1.4 *Password Cracking*

Pada tahap ini penguji akan langsung melakukan *Cracking Password* berdasarkan informasi yang sudah didapatkan dengan mengunakan metode yang ditentukan pada tahap *threat modeling*.

1.6.1.5 *Reporting*

Reporting merupakan hasil akhir dari pengujian sistem. Penguji menyampaikan apa saja yang telah dilakukan dan apa saja temuan selama menguji sitem. Kemudian penguji menyampaikan bagaimana pemilik sistem memperbaiki dan menutup kerentanan.

1.7 Sistematika Penulisan

Sistematika penulisan bertujuan untuk mempermudah pemahaman dan penelaahan penelitian. Dalam laporan penelitian ini, sistematika penilisaan terdiri dari lima bab, masing-masing uraian yang scara garis besar dapat dijelaskan sebagai berikut:

BAB I PENDAHULUAN

Dalam bab ini pendahuluan yang materinya sbagain besar menyempurnakan usulan penelitian yang brisikan tentang latar blakang masalah, rumusan masalah, batasan masalah, maksut dan tujuan pnlitian dan sistmatika pnulisan.

BAB II LANDASAN TEORI

Dalam bab ini mnguraikan tori –tori yang mendasari scara terinci yang memuat tentang pngertian jaringan *Wireless*, sitem keamanan WPA2-PSK dan *Remot Authentication Dial In User Service* (RADIUS) *Server*.

BAB III INDENTIFIKASI DAN ANALISIS

Dalm bab ini menguraikan tentang gambaran objek penelitian, analisis semua permasalahan, perancangan sistem baik secara umum maupun spesifik.

BAB IV PENGUJIAN DAN HASIL

Dalam hal ini menjelaskan tentang hasil yang sudah dilakukan oleh peneliti bagaimana cara melakkukan analisis keamanan jaringan WPA2-PSK dan Radius Server, dan melakukan pembahasan dari penelitian yang sudah dilakukan oleh peneliti.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini menjelaskan kesimpulan yang diperoleh dari hasil penelitian dan saran sebagai pemecahan masalah yang berguna untuk pencapaian yang lebih baik.