BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Informasi dan komunikasi pada saat ini mutlak menjadi suatu kebutuhan pokok yang harus dipenuhi. Bahkan untuk sebagian orang, mereka memerlukan informasi kapan pun dan dimana pun mereka berada. Dan teknologi yang mampu memenuhi kebutuhan tersebut adalah teknologi *wireless*.

Wireless menawarkan beragam kemudahan, kebebasan, mobilitas, dan fleksibilitas yang tinggi. Teknologi wireless memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Kemudahan-kemudahan yang ditawarkan wireless LAN menjadi data tarik tersendiri bagi para pengguna komputer dalam menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet.

Masalah yang akan dihadapi apabila menerapkan jaringan wireless adalah isu tentang keamanannya. Banyak pihak yang masih mempertanyakan tentang keamanan wireless, dan banyak pula pihak yang meyakini bahwa sistem keamanan wireless yang menggunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan wireless yang lain.

Berdasarkan hasil studi pustaka yang dilakukan, sistem keamanan wirelessyang benar-benar mampu memberikan keamanan yang lebih *secure* adalah dengan menggunakan sistem keamanan *Remote Authentication Dial In User Servie* (RADIUS) *server* menggunakan autentikasi Captive Portal. Namun pada saat ini, banyak pihak yang masih menggunakan WPA2-PSK sebagai sistem keamanan *wireless* mereka untuk menghindari kemungkinan penggunaan akses internet secara

ilegal oleh orang yang tidak memiliki hak akses.

Berdasarkan permasalahan tersebut, penulis tertarik untuk mengajukan penelitian dengan judul "Analisa Perbandingan Sistem Keamanan WPA2-PSK Dengan Captive Portal Pada Wireless Menggunakan Metode *Wireless Penetration Testing* di Divisi Networking & IT Solution PT. Yoshugi Putra Mandiri.

1.2 Rumusan Masalah

Untuk memperjelas dan mengarahkan penelitian ini agar hasil yang didapat sesuai dengan yang diharapkan, maka masalah yang ada dapat dirumuskan sebagai berikut :

1. Bagaimana caranya menguji sistem keamanan WPA2-PSK dengan Captive Portal pada jaringan *wireless* serta mengetahui perbandingan keamanan dari keduanya?

1.3 Batasan Masalah

Mengingat luasnya cakupan bahasan tentang perbandingan keamanan WPA2-PSK dengan Captive Portal, agar hasil penelitian lebih terarah sesuai dengan yang diharapkan maka perlu disusun batasan masalah seperti berikut :

1. Pengujian sistem keamanan wireless WPA2-PSK dilakukan di lingkungan kantor divisi *Networking & IT Solution* PT. Yoshugi Putra Mandiri.
2. Pengujian sistem keamanan *wireless* Captive Portal dilakukan pada *Radius Server* Captive Portal yang dibangun oleh peneliti menggunakan *wireless router* berbasis OpenWRT..
3. Melakukan analisa *vulnerability* pada *Radius Server* menggunakan *tools* Nessus 4, Wireshark, dan *tools* Aircrack-ng untuk menganalisa *vulnerability*

pada WPA2-PSK.

4. Metode pengujian yang digunakan adalah metode *Wireless Penetration Testing*.
5. Pengujian sistem keamanan (*hacking*) menggunakan Backbox 4, Macchanger, dan aircrack-ng, ettercap, dan wireshark.
6. Pengujian ini tidak melakukan serangan terhadap konfigurasi dan algoritma sistem keamanan yang diuji.
7. Jenis serangan yang dilakukan dalam pengujian ini adalah *Brute Force, MAC Address Spoofing, Sniffing to Eavesdrop, Man in the Middle Attack* serta *Denial of Service* yang meliputi serangan *Deauthentication Attack* dan *Ping of Death*.
8. Penelitian ini tidak membahas algoritma dari enkripsi sistem keamanan *wireless* yang digunakan.
9. Pengujian serangan *Brute Force* pada WPA2-PSK maupun Captve Portal menggunakan *Dictionary file*.
10. Pengujian serangan MAC *address spoofing* pada WPA2-PSK maupun Captive Portal menggunakan airodump-ng dan macchanger.
11. Pengujian serangan *Ping of Death* pada WPA2-PSK maupun Captive Portal hanya menggunakan *tool ping* pada Backbox linux.
12. Pengujian serangan *Sniffing to Eavesdrop* pada WPA2-PSK maupun Captive Portal hanya menggunakan *tool* wireshark untuk mendapatkan dan menganalisa paket pada protokol http.
13. Pengujian serangan *Man in the Middle Attack* pada WPA2-PSK maupun

Captive Portal dilakukan menggunakan tools ettercap dan wireshark.

14. Pengujian serangan *Deauthentication Attack* pada WPA2-PSK maupun Captive Portal hanya menggunakan aireplay-ng melalui *command line*.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Sebagai syarat untuk menyelesaikann pendidikan program Strata 1 (S1) di jurusan Teknik Informatika pada Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta
2. Menganalisa kelemahan keamanan jaringan wireless yang menggunakan WPA2-PSK dan Captive Portal.
3. Memberi saran berupa rekomendasi dari kelemahan sistem pada divisi *Networking & IT Solution* PT. Yoshugi Putra Mandiri.

1.5 Manfaat Penelitian

Manfaat dari dilakukannya penelitian ini adalah mengetahui jenis keamanan wireless mana yang lebih aman antara jaringan wireless yang menggunakan sistem keamanan WPA2-PSK dengan yang menggunakan Captive Portal.

1.6 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penulisan tugas akhir ini meliputi :

1. Metode *Wireless Network Penetration Testing Methodology*
   a. *Intelligence gathering*; pengumpulan informasi tentang target
   b. *Vulnerability analysis*; melakukan analisa kerentanan
   c. *Threat modelling*; menyusun rencana pembuktian

d. *Password Cracking*; tahap pengujian cracking password

e. *Reporting*; menyampaikan laporan analisis dan pembuktian

2. Metode Wawancara

Pengumpulan data dan informasi dengan cara melakukan wawancara secara langsung dengan admin jaringan wireless yang ada di divisi *Networking & IT Solution* PT. Yoshugi Putra Mandiri.

3. Studi Pustaka

Studi literatur merupakan cara pengumpulan data dengan cara mengumpulkan, mengkaji, dan mendalami teori-teori yang berhubungan dengan fokus penelitian. Peneliti menggunakan studi lieratur untuk mengumpulkan data yang diperlukan dalam penelitian yang berupa teori-teori dari para ahli dan berbagai literatur untuk mendukung penelitian. Hal ini dimaksudkan untuk memperoleh data teoritis yang sekiranya dapat mendukung kebenaran data yang diperoleh melalui penelitian dan dapat menunjang hasil dari penelitian tersebut.

4. Observasi

Observasi yaitu pengamatan yang meliputi kegiatan pemusatan perhatian terhadap suatu objek dengan menggunakan seluruh alat indera. Arikunto (2010) mengemukakan bahwa "mengobservasi dapat dilakukan melalui penglihatan, penciuman, pendengaran, perabaan, dan pengecapan". Melalui observasi ini peneliti akan mengumpulkan data yang diperlukan untuk penelitian dengan cara melakukan wawancara terhadap

administrator jaringan untuk mengetahui topologi jaringan wireless, manajemen jaringan, dan sistem keamanan wireless yang digunakan.

1.7 Sistematika Penulisan

Penelitian yang dilakukan akan disusun dalam laporan kedalam beberapa bab pembahasan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, metode pengumpulan data, dan sistematika penulisan laporan penelitian.

BAB II LANDASAN TEORI

Pada bab ini diuraikan teori-teori yang mendukung untuk penelitian ini. Berisi materi mengenai jaringan wireless, aspek-aspek kelemahan dan ancaman serta metode keamanan yang digunakan dalam teknologi wireless.

BAB III METODOLOGI PENELITIAN

Dalam bab ini memaparkan secara rinci mengenai metode yang digunakan dalam pengumpulan data maupun metode untuk pengembangan sistem yang dilakukan pada penelitian ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini berisi analisa dan perbandingan dari sistem keamanan wireless yang menggunakan WPA2-PSK dengan yang menggunakan Captive Portal, termasuk kelebihan maupun kekurangan dari sistem tersebut.

BAB V PENUTUP

Pada bab ini berisi kesimpulan dan saran yang dapat peneliti rangkum selama

proses penelitian berlangsung.

DAFTAR PUSTAKA

Daftar pustaka memuat keterangan buku-buku dan literatur yang menjadi acuan dalam penulisan laporan skripsi ini.