BAB III
METODOLOGI PENELITIAN

3.1 Subjek dan Objek Penelitian

Pada penelitian ini subjek penelitiannya adalah *penetration testing*. Objek penelitian yang akan dilakukan merupakan *penetration testing* pada jaringan *wireless* di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal. Objek penelitiannya adalah pengujian keamanan jaringan *wireless* menggunakan metode PTES.

3.2 Alat dan Bahan Penelitian

Alat adalah segala sesuatu yang dibutuhkan dalam penelitian ini yang menguji jaringan *wireless* menggunakan metode PTES, dalam hal ini alat yang digunakan terdiri dari 2 bagian yaitu :

3.2.1 *Hardware* Laptop

1. Processor Intel Core i3-6006U @ 2.0 GHz
2. RAM 8 GB
3. SSD 240 GB dan Harddisk 1 TB
4. TP-Link USB Wifi Adapater WN722N

3.2.2 *Software*

1. Virtualbox Sistem Operasi Kali Linux
2. *Tools* Aircrack-Ng
3. *Tools* MDK3

Bahan penelitian adalah segala informasi yang dibutuhkan untuk menunjang proses keberhasilan pengujian dalam penelitian ini berupa referensi penelitian sebelumnya, teori pendukung dan data yang diperoleh dilokasi pengujian.

3.3 Proses Penelitian

Tahapan proses yang dilakukan dalam penelitian ini digambarkan dalam diagram alir pada gambar 3.1 sebagai berikut :

Gambar 3. 1 Diagram alir penelitian

3.3.1 Tahap Observasi

Pada tahap ini dilakukan survei dan pengamatan langsung untuk menemukan permasalahan terhadap studi kasus yang diambil yaitu pada Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal. Ditemukan permasalahannya adalah sistem konfigurasi

jaringan *wireless* yang diterapkan masih *default* bawaan *vendor* dan hanya melakukan perubahan pada enkripsi *password*.

3.3.2 Tahap Identifikasi

Setelah melakukan observasi atau survei dari hasil pengamatan maka dilakukan identifikasi masalah tentang apa yang akan diteliti dengan menentukan topik, masalah dan metode yang akan digunakan untuk dapat menyelesaikan permasalahan yang ada.

3.3.3 Studi Literatur

Dalam pengujian dan pembuatan laporan tentu saja penulis memerlukan informasi-informasi yang akurat dengan mencari dan membaca penelitan sebelumnya dan teori dalam mendukung penelitian ini dengan studi literatur yang dilakukan memperoleh informasi mengenai solusi untuk memecahkan permasalahan yang ada.

3.3.4 Pengumpulan Data

Dalam penelitian ini perlu dilakukan pengumpulan data berupa observasi, wawancara, dan eksperimen. Adapun teknik pengumpulan data yang dilakukan dalam penelitian ini adalah sebagai berikut :

1. Metode Wawancara

   Penulis bertatap muka langsung dengan narasumber di Kantor Balai Desa Kalisapu yaitu Dodi Trianto sebagai administrator jaringan *wireless* untuk mengajukan pertanyaan-pertanyaan secara langsung terkait dengan proses penggunaan jaringan *wireless* (*wifi*) di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal, dalam hal ini penulis mengajukan beberapa pertanyaan meliputi :

   1. Berapa banyak pegawai yang ada di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal?

2. Jenis *provider* apa yang digunakan di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal?
3. Bagaimana dengan keamanan yang digunakan pada perangkat *wireless* yang diterapkan?
4. Apakah jaringan *wireless* (*wifi*) yang digunakan stabil dan tidak ada gangguan?
5. Apakah jaringan *wireless* (*wifi*) yang diterapkan dapat diakes oleh orang luar?
6. Apakah ada yang pernah mencoba melakukan serangan melalui jaringan *wireless* (*wifi*) di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal?

Hasil dari wawancara ini dapat dilihat pada tabel 3.1 berikut :

Tabel 3. 1 Hasil Wawancara

Pertanyaan	Hasil
1	10 orang
2	Indihome
3	Belum pernah dilakukan perubahan selain *password* yang digunakan
4	Sering mengalami gangguan, tidak stabil, terkadang koneksinya lambat
5	Dapat diakses siapa saja yang mengetahui *password* yang diterapkan
6	Belum mengetahui

2. Metode Eksperimen

Melakukan percobaan dengan aplikasi yang akan digunakan dalam penelitan untuk memperoleh data-data yang diperlukan dalam tahap analisis penelitian.

3.3.5 Analisis

Adapun kegiatan yang dilakukan dalam tahapan ini adalah sebagai berikut :

Metode yang digunakan dalam *penetration Test* ini yaitu *PTES* (*Penetration Testing Execution Standard*) yang terdiri dari 7 Tahapan yaitu :

1. *Pre-Engagement* (Pra-Interaksi)

   Menjelaskan tentang apa yang akan dilakukan dalam proses uji penetrasi, melakukan perjanjian dengan pemilik sistem jaringan *wireless* yaitu kantor balai desa kalisapu dan menjelaskan dampak yang diperoleh serta gangguan pelayanan ketika proses uji penetrasi sedang berlangsung.

2. *Intelligence Gathering* (Pengumpulan Informasi)

   Mengumpulkan informasi yang didapat setelah melakukan observasi dan eksperimen mengenai penggunaan jaringan *wireless* di Kantor Balai Desa Kalisapu, Adapun hasilnya sebagai berikut :

   1. Terdapat 1 *router* yang tersedia di kantor balai desa kalisapu.
   2. Konfigurasi masih bawaan *vendor*.
   3. Enkripsi *password* menggunakan *WPA2-PSK*.
   4. Jaringan *wireless* dapat digunakan oleh siapa saja yang mengetahui *password* yang diterapkan.
   5. Jaringan *wireless* digunakan untuk menangani proses administrasi, penyimpanan *database* lokal, layanan akses internet.

3. *Threat Modelling* (Pemodelan Ancaman)

   Pada tahap ini peneliti menentukan ancaman yang mungkin bisa terjadi berdasarkan hasil dari tahap sebelumnya, untuk mempermudah proses uji coba serangan yang akan dilakukan. Terdapat celah keamanan sebagai berikut :

1. Enkripsi menggunakan *WPA2-PSK*, yang kemungkinan masih bisa di *crack* atau bobol[9].
2. Tidak menerapkan pembatasan *mac address*.
3. Siapa saja dapat terhubung jika mengetahui *password* jaringan tersebut.
4. Semua komputer dan perangkat lainnya terhubung dalam satu *router* dan satu *ssid*.
5. Tidak adanya pembatasan *user*.

4. *Vulnerability Analysis* (Analisis Kerentanan)

Pada tahap ini peneliti mencari dan mengidentifikasi kerentanan yang terdapat pada jaringan *wireless* tersebut, penulis telah menganalisis kerentanan sebagai berikut :

1. Enkripsi *WPA2-PSK* memiliki celah keamanan yang dapat diserang menggunakan teknik *cracking the encryption*.
2. Sistem konfigurasi masih *default* dapat dimanfaatkan untuk menyerang infrastruktur jaringan yang digunakan dengan diuji *cut* koneksi jaringan yang dapat coba melalui serangan *Router attack*.

5. *Exploitation* (Eksploitasi)

Pada tahap ini peneliti melakukan uji coba serangan ke jaringan *wireless LAN* yang berada di Kantor Balai Desa Kalisapu dimana jenis pengujian dapat dilihat pada tabel 3.2.

Tabel 3. 2 Jenis Pengujian

Jenis Pengujian	**Batasan Serangan**	***Software***
Cracking The Encryption	Serangan pada jaringan *wireless* di Kantor Balai Desa Kalisapu dengan mengeksploitasi	*Aircrack-ng*

Jenis Pengujian	Batasan Serangan	*Software*
	menguji kekuatan *password wifi* tersebut.	
Router Attack	Serangan memutus jalur koneksi (*offline*) pada pengguna yang aktif.	*MDK3*

Serangan dilakukan masing-masing sebanyak 5 kali serangan pada jaringan *wireless* agar hasil semakin akurat dan kemudian dilakukan evaluasi serta memberikan rekomendasi keamanan jaringan dengan mengacu 5 parameter keamanan jaringan yaitu *Confidentiality*, *Integrity*, *Availability*, *Authentication*, *Non-repudiation*.

6. *Post-Exploitation* (Pasca-Eksploitasi)

   Melakukan analisis bagian yang paling rentan dan menjelaksan bagian yang terkena resiko serta dampaknya dan memastikan prosedur yang disepakati sebelumnya dapat digunakan selama tahap pasca eksploitasi.

7. *Report* (Pelaporan)

   Menyajikan laporan lengkap hasil setelah dilakukan uji penetrasi dengan melaporkan status penyerangan, resiko yang ditemukan dan bagaimana rekomendasi penanggulangan resiko pada celah yang ditemukan.

3.3.6 Laporan Hasil

Pada tahap ini penulis melakukan pelaporan dari hasil metode *PTES* yang digunakan dengan melakukan pengujian evaluasi keamanan jaringan dan membuat rekomendasi sistem keamanan jaringan yang baik untuk diterapkan di Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal dalam bentuk laporan tugas akhir.