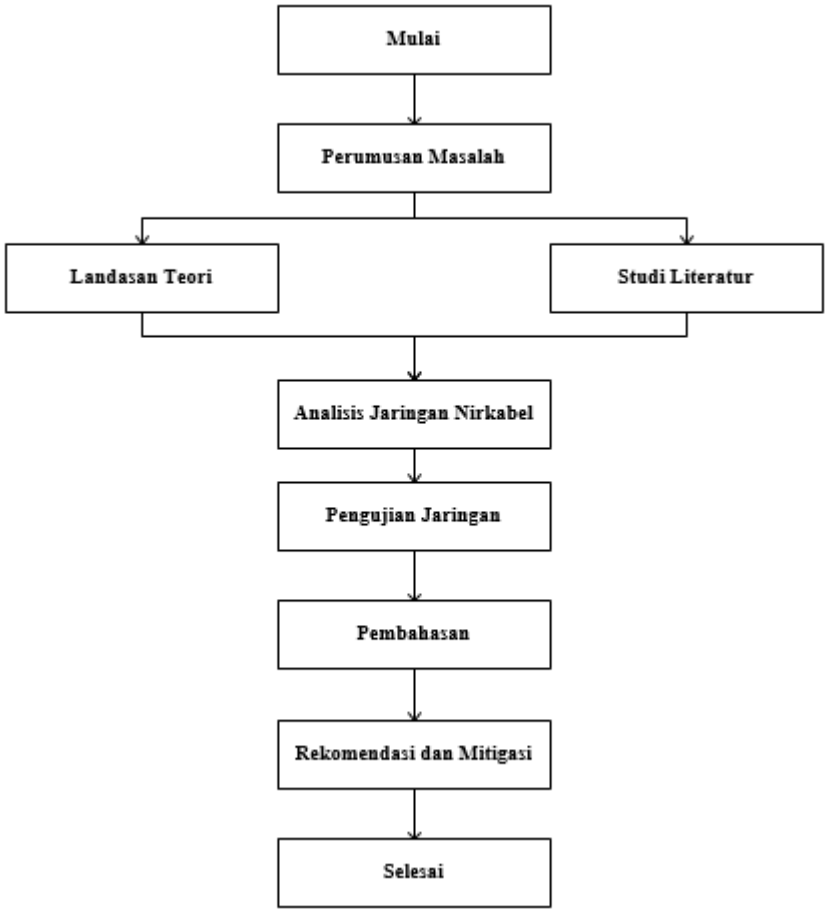
BAB III

METODE PENELITIAN

3.1. Desain Penelitian



Gambar 3.1 Desain Penelitian

(Sumber : Data Olahan Penulis)

Penelitian ini dimulai dengan merumuskan masalah penelitian yang akan dikaji. Penulis kemudian mengumpulkan landasan teori dan literature-literatur penelitian yang berhubungan dengan apa yang sebelumnya telah dirumuskan dalam rumusan masalah penelitian untuk digunakan sebagai bahan kajian dan memperkuat landasan teori yang akan dikemukakan oleh penulis dan melakukan perbandingan penelitian-penelitian yang telah ada sebelumnya dengan penelitian yang saat ini sedang penulis lakukan. Kedua tahap ini juga berperan penting bagi penulis dalam menentukan cara yang baik dan efisien pada tahap selanjutnya yaitu tahap analisis jaringan nirkabel. Selain itu juga berguna sebagai bahan landasan dasar penulis dalam melakukan penelitian ini.

Tahapan selanjutnya adalah penulis melakukan analisis terhadap jaringan nirkabel yang sedang berjalan pada mall-mall besar dikota Batam. Mall yang menjadi tempat penelitian adalah Nagoya Hill Shopping Mall, Mega Mall Batam Centre, dan Kepri Mall Batam. Setelah penulis selesai menganalisis jaringan yang sedang berjalan, maka dilanjutkan dengan tahap pengujian jaringan. Pada tahap ini, penulis akan melakukan penetrasi jaringan yang sedang berjalan dengan menggunakan metode *Evil Twin Attack.*

Setelah pengujian selesai dilakukan, akan dilanjutkan dengan tahapan pembahasan. Pada tahap ini penulis menjabarkan hasil serta pembahasan dari pengujian yang dilakukan. Kemudian tahapan terakhir adalah Rekomendasi dan Mitigasi. Rekomendasi disini adalah berupa tips dan trik yang dapat digunakan oleh pihak cafe untuk meningkatkan keamanan jaringan nirkabelnya. Tidak selesai

dengan rekomendasi, penulis juga memberikan sebuah mitigasi yang dapat dilakukan apabila terjadi penyerangan terhadap jaringan nirkabel.

3.2. Standar dan Indikator Pengujian Keamanan

PTES (*Penetration Testing Execution Standard*) membuat sebuah dokumentasi standar-stadar yang umumnya digunakan untuk melakukan sebuah penetrasi testing pengujian keamanan. Standar tersebut adalah sebagai berikut :

Gambar 3.2 Logo PTES

(Sumber : Team, 2017)

3.2.1. *Pre-engagement Interations*

Mendefinisikan ruang lingkup merupakan salah satu komponen terpenting dari pengujian keamanan, namun ini juga merupakan salah satu hal yang paling banyak diabaikan. Walaupun sudah banyak artikel yang telah ditulis tentang berbagai alat dan teknik yang bisa dimanfaatkan untuk mendapatkan akses ke jaringan, sangat sedikit artikel yang menuliskan tentang tujuan dari melakukan pengujian, persiapan, mengabaikan untuk benar-benar menyelesaikan perjanjian sebelumnya yang mana memiliki potensial memberikan penetrasi tester hal-hal yang tidak termasuk dalam ruang lingkup pengujian, ketidak puasan pelanggan, dan bahkan masalah hukum. Ruang lingkup sebuah proyek secara khusus

mendefinisikan apa yang akan diuji. Bagaimana masing-masing aspek test yang akan dilakukan harus dibahas dalam aturan perjanjian atau disebut juga kontrak. Tujuan utama dari tahapan ini adalah untuk mendiskusikan apa yang akan diuji, ruang lingkup, serta biaya yang menjadi kesepakatan dalam menjalankan pengujian.

3.2.2. *Intelligence Gathering*

Bagian ini mendefinisikan aktivitas pengumpulan informasi dari sebuah pengujian keamanan. Tujuan dari dokumentasi ini adalah untuk menyediakan standar yang dirancang khusus untuk pentester melakukan pengintaian terhadap target. Dokumentasi tersebut merinci proses pemikiran dan tujuan dari pengintaian, dan bila digunakan dengan benar, membantu pembaca untuk menhasilkan rencana yang sangat strategis untuk menyerang target.

Level atau tingkatan adalah konsep penting yang dijalankan oleh PTES secara keseluruhan. Mendefinisikan tingkatan memungkinkan kita menklarifikasi hasil dan kegiatan yang dibayangkan, seperti usaha, akses terhadap informasi, dan lainnya. Tingkatan *Intelligence Gathering* dibagi atas tiga kategori. Yaitu *Information Gathering Compliance Driven, Best Practice* dan *State Sponsored.*

3.2.3. *Threat Modeling*

Bagian ini mendefinisikan pendekatan pemodelan ancaman yang diperlukan untuk pelaksanaan pengujian penetrasi yang benar. Standar tidak menggunakan model tertentu, namum mengharuskan model yang digunakan konsisten dalam hal representasinya ancaman, kemampuan mereka, kualifikasi mereka sesuai dengan

organisasi yang sedang diuji, dan kemampuan untuk berulang kali diaplikasikan pada tes masa depan dengan hasil yang sama.

Standar tersebut berfokus pada dua elemen kunci dari permodelan *Threat Modeling* tradisional dan Penyerang (*threat community/agent*). Masing-masing dipecah menjadi aset bisnis dan proses bisnis dan komunitas ancaman dan komunitasnya. Minimal, keempat elemen tersebut harus diidentifikasi dan didokumentasikan dengan jelas dalam setiap penetrasi testing. *High level threat modeling process* terdiri dari empat bagian, yaitu

1. Mengumpulkan informasi yang relevan
2. Mengumpulkan dan mengkategorikan aset primer dan sekunder
3. Identifikasi dan ketegorisasi ancaman dan komunitas ancamannya
4. Memetakan komunitas ancaman terhadap aset primer dan sekunder

3.2.4. *Vulnerability Analysis*

Uji kerentanan adalah proses menemukan kekurangan dalam sistem dan aplikasi yang dapat dimanfaatkan oleh penyerang. Kelemahan ini bisa berada diantara *host* dan *service misconfiguration*, atau desain aplikasi yang tidak aman. Meskipun proses yang digunakan untuk mencari kekurangan bervariasi dan sangat bergantung pada komponen tertentu yang diuji, beberapa principal utama berlaku untuk prosesnya.

Ketika melakukan analisis kerentanan terhadap jenis *tester* mana saja, benar-benar harus menguji pengujian kedalaman yang berlaku dan luasnya untuk memenuhi tujuan dan/ atau persyaratan hasil yang diinginkan. Nilai kedalaman

dapat mencakup hal-hal seperti lokasi alat penilaian, *authentication requirements*, dan lain-lain. Apapun ruang lingkupnya, pengujian harus disesuaikan untuk memenuhi persyaratan mendalam untuk mencapai tujuan. Kedalaman pengujian harus selalu divalidasi untuk memastikan hasil penilaian memenuhi harapan. Selain kedalaman, luasnya juga harus diperhatikan saat melakukan pengujian kerentanan. Nilai keluasan dapat mencakup hal-hal seperti jaringan target, segmen, host, aplikasi, inventaris, dan lain-lain.

3.2.5. *Exploitation*

Tahapan eksploitasi dari sebuah uji penetrasi hanya berfokus pada penetapan akses kesistem atau sumber daya dengan cara melewati pembatasan keamanan. Jika tahap sebelumnya, analisis kerentanan dilakukan dengan benar, tahapan ini harus berjalan dengan baik seperti yang direncanakan. Tujuan utamanya adalah mengidenfikasi titik masuk utama ke dalam organisasi dan untuk mengindetifikasi aset target yang bernilai tinggi.

Jika tahap analisis kerentanan selesai dengan benar, daftar target yang bernilai tinggi seharusnya sudah sesuai. Akhirnya vector serangan harus mempertimbangkan probabilitas keberhasilan dan dampak tertinggi pada organisasi.

3.2.6. *Post Exploitation*

Tujuan dari tahap *Post-Exploitation* adalah untuk mengetahui nilai mesin yang dikompromikan dan untuk dipelihara control mesin untuk digunakan nantinya. Nilai mesin ditentukan oleh sensitivitas data yang tersimpan itu dan

digunakan mesin dalam mengorbankan jaringan lebih lanjut. Metode yang dijelaskan dalam tahapan ini dimaksudkan untuk membantu penguji mengidentifikasi dan mendokumentasikan data sensitive, mengidentifikasi pengaturan konfigurasi, saluran komunikasi dan hubungan dengan perangkat jaringan lain yang bisa digunakan utnuk mendapatkan akses lebih jauh kejaringan, dan mensediakan satu atau lebih metode untuk mengakses mesin lain waktu. Jika kasus di mana metode ini berbeda dari Aturan yang telah disepakati, maka aturan kontrak /aturan perjanjian harus diikuti.

3.2.7. *Reporting*

Tahapan ini dimaksudkan untuk menentukan kriteria dasar untuk pelaporan pengujian pentetrasi. Meskipun sangat dianjurkan untuk menggunakan format yang disesuaikan, berikut ini harus memberikan pemahaman tingkat tinggi tentang hal yang diperlukan dalam laporan serta struktur laporan serta struktur laporan untuk meberikan nilai bagi pembaca.

3.3. Metode dan Skenario Pengujian

Penulis menentukan secara acak café yang akan dijadikan tempat penelitian. Setiap cafe yang akan diteliti, peneliti menggunakan waktu sekitar 5 sampai dengan 10 menit untuk menangkap jaringan yang ada disekitaran cafe. Berikut adalah daftar cafe yang dijadikan sebagai tempat penelitian.

Tabel 3.3 Cafe Tempat Penelitian

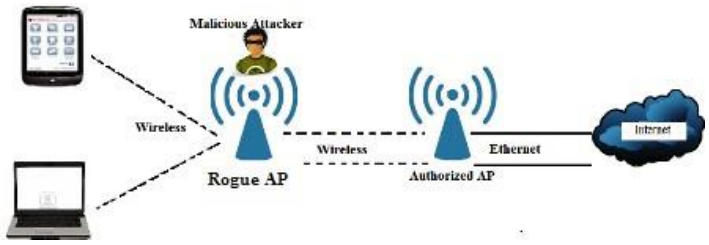
Nama Mall	**Nama Cafe**
Nagoya Hill Shopping Mall	Malaya Cafe
Mega Mall Batam Centre	Byza Cafe
Kepri Mall	Coffe Town

3.3.1. Metode Pengujian

Metode pengujian jaringan nirkabel yang digunakan dalam penelitian ini adalah *Evil Twin Attack*. Untuk menggunakan metode ini, ada beberapa *tool* yang perlu disiapkan seperti Airodump-ng dan Airbase-ng pada Kali linux. Selain itu, paket-paketnya yang diperlukan juga harus diinstall seperti dhcp server, mdk3, php dan lainnya sesuai apa yang telah dijelaskan pada bab sebelumnya.

Metode *Evil Twin Attack* atau kadang juga disebut dengan *Rogue Access Point* adalah sebuah metode dimana penyerang memanfaatkan alamat MAC yang terdapat disetiap perangkat jaringan untuk membuat kembarannya dengan alamat MAC yang sama. Akan tetapi, seluruh koneksi jaringan pada AP yang asli, akan diputuskan secara paksa dengan tujuan agar pengguna melakukan koneksi ke jaringan AP palsu yang telah kita siapkan. Apabila pengguna telah berhasil melakukan koneksi, mereka tidak akan mendapatkan kenyamanan jaringan yang sama dengan sebelumnya, karena ini adalah sebuah AP palsu yang kita siapkan dengan tujunan untuk mengambil data yang kita perlukan. Pada penelitian ini, penulis hanya membuat sebuah halaman web login dimana meminta pengguna untuk mengisi kata sandi AP dengan benar.

Setelah pengguna telah memasukkan kata sandi yang benar sesuai *HandShake* yang telah kita terima, maka secara otomatis mereka akan terputus dari koneksi AP palsu ini, dan AP asli sudah dapat digunakan kembali dengan normal. Gambaran bagaimana cara metode ini bekerja dapat dilihat pada Gambar 3.3.1 berikut ini.



Gambar 3.3.1 Illustrasi Metode *Evil Twin Attack*
(Sumber : Olahan Penulis)

3.3.2. Skenario Pengujian

Adapun skenario dalam pengujian dimulai dengan memili secara acak cafe yang menurut peneliti cukup ramai pengunjungnya. Setelah tempat telah ditentukan, hal selanjutnya yang dilakukan adalah meminta izin terhadap pihak manager bahwa penulis akan melakukan penelitian pada tempat tersebut. Apabila izin diberikan, makan langkah selanjutnya adalah memulai menganalisis jaringan nirkabel yang digunakan serta jaringan nirkabel yang ada di area jangkauan. Dari hasil analisis atau *scanning* yang telah dilakukan, langkah selanjutnya adalah memanfaatkan data yang telah diperoleh untuk melakukan penyerangan terhadap jaringan tersebut.

Pada tahap ini berbagai jenis persiapan dan penyerangan akan diluncurkan terhadap jarinan nirkabel, berupa pemanfaatan alamat MAC yang ada untuk

membuat sebuah AP palsu beserta web pancingannya. Saat AP palsu telah berhasil dibuat, semua pengguna AP asli akan diputuskan secara paksa yang mana gunanya untuk memancing mereka untuk melakukan koneksi terhadap AP yang telah penulis buat.

Hal terakhir yang perlu dilakukan adalah menunggu pengguna melakukan koneksi, dan memasukkan data yang kita perluka (*password)*. Setelah pengguna telah memasukkan kata sandi dengan benar, AP asli dapat digunakan kembali secara normal.

3.4. Lokasi dan Jadwal Penelitian

3.4.1. Lokasi Penelitian

Penelitian dilakukan pada jaringan nirkabel café di wilayah Nagoya Hill Shopping Mall, Kepri Mall Batam, dan Mega Mall Batam Centre di Kota Batam.

3.4.2. Jadwal Penelitian

Penelitian dilakukan terhitung sejak September2017 hingga Januari 2018 dimana analisis dan pengujian jaringan nirkabel dilakukan pada hari sabtu dan minggu kisaran jam 12.00-21.00 WIB.

Tabel 3.4 Lokasi dan Jadwal Penelitian

Kegiatan Penelitian	**September 2017**				**Oktober 2017**				**November 2017**				**Desember 2017**				**Januari 2018**			
	Minggu Ke																			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Pengajuan Judul																				
Pencarian Referensi																				
Pengumpulan Data																				
Pengolahan Data																				
Pembuatan Laporan																				