BAB II
LANDASAN TEORI

2.1. Profil Dan Tempat Penelitian

2.1.1 Profil Dinas Komunikasi Dan Informatika Bandung

Dinas Komunikasi Dan Informatika Kota Bandung dibentuk berdasarkan Peraturan Kota Bandung No.13 Tahun 2009 tentang perubahan atas peraturan daerah Kota Bandung Nomor 13 tahun 2007 tentan pembentukan dan susunan organisasi dinas daerah kota bandung mempunyai tugas dan kewajiban membantu Walikota dalam Bidang Komunikasi dan Informasi[7]. Dalam menyelenggarakan tugas dan kewajiban tersebut Dinas Komunikasi dan Informatika mempunyai fungsi:

1. Merumuskan kebijakan teknis dibidang komunikasi dan informasi.
2. Melaksanakan tugas operasional bidang komunikasi dan informatika yang meliputi: Bidang Pos dan Telekomunikasi, Bidang Telematika, Bidang Diseminasi Informasi, dan Bidang Hubungan Masyarakat.
3. Melaksanakan Pelayanan teknis administrasi meliputi: administrasi umum dan kepegawaian, administrasi perencanaan, dan evauasi pelaporan serta administrasi keuangan dinas.

Dalam melaksanakan tugas dan kewajiban dinas komunikasi dan informatika dipimpin oleh kepala dinas yang dalam pelaksanaan tugasnya dibantu oleh:

1. Sekretaris, membawahi:
    a. Sub Bagian Umum Dan Kepegawaian
    b. Sub Bagian Keuangan dan Program
2. Bidang Pos dan Telekomunikasi, membawahi:
    a. Seksi Pengendalian Pos dan Telemonikasi
    b. Seksi Pemberdayaan Pos dan Telekomunikasi
3. Bidang telematika, membawahi:
    a. Seksi Sarana dan PrasaranaTelematika

   b. Seksi e-Government dan Pemberdayaan Telematika
4. Bidang Diseminasi Informasi, membawahi:
   a. Seksi Pengelolaan Data dan Informasi
   b. Seksi Komunikasi dan Informatika
5. Bidang Hubungan Masyarakat, membawahi:
   a. Seksi Peliputan dan Dokumentasi
   b. Seksi Kemitraan Media dan Publikasi
6. Unit Pelaksana Teknik Dina
7. Kelompok Jabatan Fungsional

2.1.2 Visi dan Misi

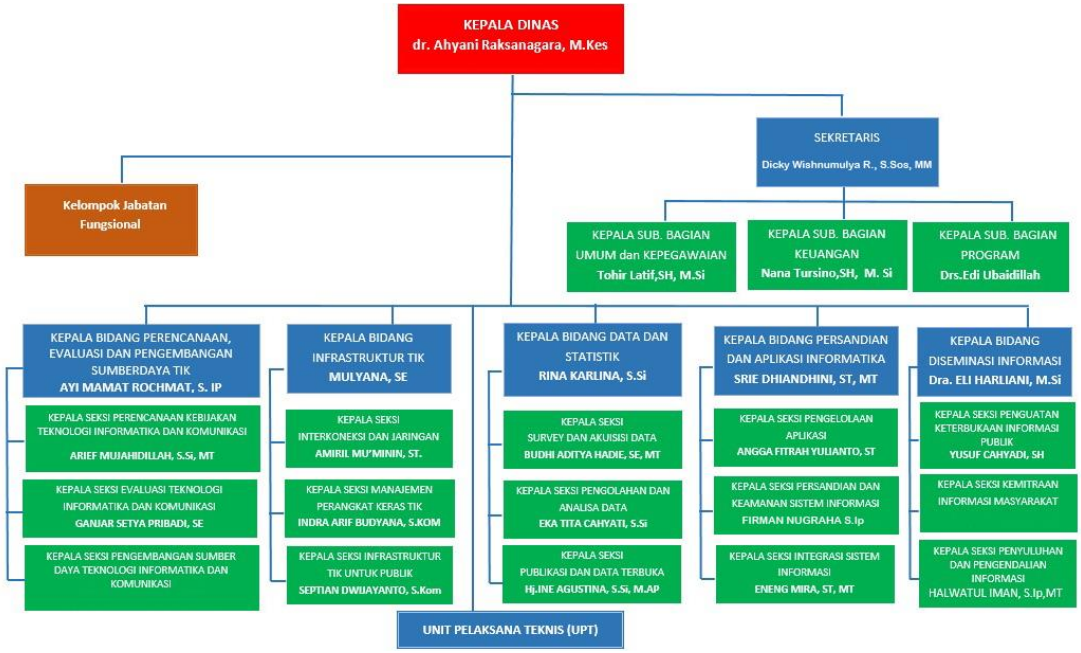
Visi dari Dinas Komunikasi Dan informatika Kota Bandung adalah "Terwujudnya efektifitas dan Efisiensi komunikasi dan informatika dalam penyelenggaraan pemerintah daerah untuk mendukung kota Bandung yang unggul, nyaman, dan sejahtera".

Penjelasan Visi Dinas Komunikasi dan Informatika sebagai berikut:

1. Terwujudnya efektivitas dan efisiensi Komunikasi dan Informatika, adalah terciptanya pusat pelayanan informasi bagi warga Kota Bandung, terutama dalam mengakses data yang memerlukan informasi baik menyangkut kebijakan umum pemerintah kota maupun perijinan-perijinan. Dengan pemahaman ini akhirnya diharapkan akan terwujud masyarakat yang mengerti dan memahami informasi daam berbagai kebijakan pemerintah yang dapat diaplikasikan dalam kehidupan sehari-hari baik bermasyarakat, berbangsa dan bernegara.
2. Bandung Kota Unggul adalah kota yang memiliki kelebihan dari daerah-daerah lain terutama dalam bidang komunikasi dan informatika.
3. Bandung sebagai Kota Nyaman adalah memberikan kebebasan, privasi, dan keleluasaan kepada masyarakat untuk mengakses setiap informasi program pembangunan yang disajikan oleh Pemerintah Kota Bandung.

Sedangkan Misi dari Dinas Komunikasi Dan Informatika Kota bandung adalah "Meningkatkan dan mengembangkan layanan public serta pemberdayaan dan pendayagunaan sarana dan prasarana komunikasi dan informatika dalam rangka mewujudkan budaya masyarakat berbasis teknologi dan informasi dan layanan yang lebih merata"[8].

2.1.3 Struktur Organisasi



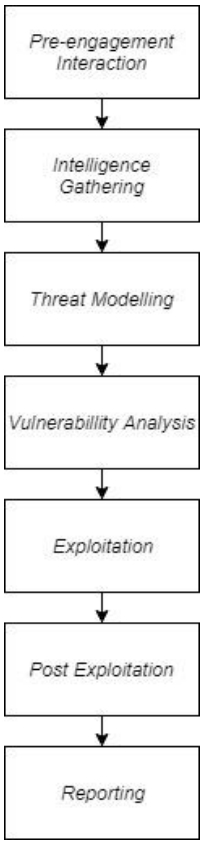
Gambar 2. 1 Struktur Organisasi di Dinas Komunikasi dan Infromatika Kota Bandung

2.2 Landasan Teori

2.2.1 Penetrating Testing Execution Standard (PTES)

Penetration Testing Execution Standard (PTES) merupakan sebuah standar baru yang di desain bisnis dan penyedia servis keamanan dengan menggunakan Bahasa yang umum dengan cakupan dalam melakukan penetration testing. PTES dimulai pada awal tahun 2009 dan berawal dari pertemuan antara anggota pendiri disaat membicarakan tentang kepentingan atau kelemahan dalam penetration

testing yang ada sekarang [9].Fase PTES didesain untuk menjelaskan sebuah *Penetration Testing* dan memastika *client* bahwa sebuah usaha level standarisasi akan diperluas pada *Penetration Testing* oleh semua orang yang melakukan tipe *assestment* ini[10]. 7 langkah dalam melakukan *Penetration Testing* execution:



Gambar 2. 2 Tahap-Tahap PTES (*Penetration Testing Execution Standard*)

2.2.1.1 Pre-Engagement Interaction

Pada tahap ini akan dilakukan pertukaran informasi, rencana dan persiapan untuk pengujian. Sebelum pengujian berlangsung akan dilakukan pertemuan antara penulis dan pihak yang akan *Penetration Testing*. Melakukan pertemuan untuk meminta konfirmasi ruang lingkup (*scope*).

2.2.1.2 Intelligence Gathering

Merupakan sebuah langkah untuk mendapatkan informasi sebanyak-banyaknya yang dapat dimanfaatkan dalam vulnerability assessment dan fase

eksploitasi. Semakin banyak informasi yang didapat dalam fase ini, semakin banyak serangan yang bias digunakan di masa yang akan datang**.** *Intelligance Gathering* dapat dipisah menjadi 3 level yaitu :

a. Level 1 *Information Gathering*

Pada level 1 *Information Gathering,* informasi sebagian besar didapatkan melalui *Tool* otomatis.

b. Level 2 *Information Gathering*

Pada level ini *Intelligence Gathering* menggunakan *Tool* otomatis pada level 1 dan analisis manual

c. Level 3 *Information Gathering*

Level 3 *Information Gathering,* merupakan yang paling canggih, menggunakan semua info dari Level 1 dan Level 2 dan banyak analisis manual.

2.2.1.3 Threat Modelling

Merupakan sebuah prosedur untuk mengoptimalisasi keamanan network dengan mengidentifikasi tujuan-tujuan dan kelemahan-kelemahan, dan menentukan tindakan balasan untuk mencegah, dan mengurangi efek-efek yang berbahaya untuk system. Di dalam konteks ini serangan-serangan yang berpotensi berbahaya seperti Denial of Service (DOS) atau tak sengaja seperti storage device failure.

2.2.1.4 Vulnerabillity Testing

Merupakan sebuah proses untuk mendapatkan sebuah kelemahan yang ada di system dan aplikasi yang dapat digunakan oleh penyerang. Kelemahan-kelemahan ini bias berada pada host dan kesalahan konfigurasi ataupun desain aplikasi yang tidak aman. Walaupun proses yang digunakan untuk melihat kelemahan tersebut bervariasi dan sangat bergantung pada komponen-komponen yang yang dicoba. Beberapa prinsip utama masih berlaku untuk proses tersebut.

a. Active Testing

Active Testing melibatkan interaksi secara langsung dengan komponen yang sedang di tes kerentanan keamanannya.

b. Passive Testing

Passive Testing melibatkan interaksi dengan data yang menggambarkan sebuah data, seperti contoh dokumen dari *Microsoft Office*, memungkinkan adanya daftar nama dari pembuat dokumen, perusahaan, kapan dokumen tersebut terakhir kali disimpan, kapan dokumen tersebut dibuat, dan lain-lain. Beberapa dokumen bahkan dapat menyimpan metadata yang unik, yang sangat berpotensi menyimpan alamat internal untuk ke server, alamat internal IP, dan informasi lain yang dapat digunakan *Penetration Tester* untuk mendapatkan akses ataupun informasi.

2.2.1.5 Exploitation

Merupakan sebuah proses dalam *Penetration Testing* yang berfokus dalam menetapkan akses kedalam sebuah sistem dengan melawati pembatasan keamanan. Jika vulnerability analysis dilakukan dengan benar, fase ini akan terencana dengan baik dan dengan serangan yang tepat.

2.2.1.6 Post Exploitation

Tujuan dari fase post exploitation ialah untuk menentukan harga dari system dan untuk mempertahankan kontrol dari sistem agar dapat digunakan untuk nanti. Harga dari sebuah system dapat ditentukan dengan melihat sensitifitas data yang disimpan disana dan kegunaan mesin dalam system yang akan digunakan nanti. Adanya sebuah perjanjian pada fase ini agar sistem klien tidak mendapatkan resiko-resiko yang disebabkan oleh *Penetration Tester.*

a. *Protect The Client*

1. Kecuali jika sudah disetujui, akan tidak ada perubahan dalam *Service* yang dianggap penting oleh klien pada infrastruktur mereka.
2. Semua perubahan, termasuk perubahan konfigurasi, harus didokumentasikan
3. Daftar semua aksi yang dilakukan kepada sistem harus disimpan
4. *Password* agar as opposed to the file data itselfidak dimasukkan didalam *Report*

5. Semua metode ataupun alat, yang digunakan dalam untuk menjaga akses dan dapat berefek kepada sistem tidak akan dimasukkan tanpa sepengetahuan klien
6. Semua data yang didapatkan akan dihapus setelah klien mendapatkan laporan terakhir, metode yang digunakan dan bukti dpenghapusan akan diberikan kepada klien

b. *Protect Yourself*

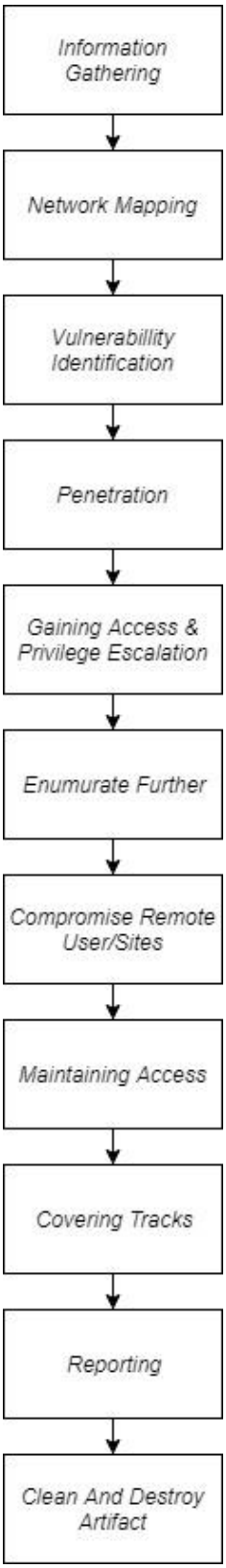
1. Pastikan semua kontak atau pernyataan ditandatangani oleh klien dan *Pentester*
2. Gunakan Enkripsi kepada sistem dan media yang akan mendapatkan dan menyimpan data klien

2.2.1.7 Reporting

Merupakan sebuah langkah untuk menuliskan laporan yang mendeskripsikan hasil lengkap pengujian dan presentasi yang sudah dipersiapkan dengan rekomendasi dan penyelesaiannya.

2.2.2 Information Systems Security Assessment Framework (ISSAF)

ISSAF adalah suatu kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi kedalam berbagai domain dan rincian evaluasi yang spesifik atau kriteria pengujian untuk setiap domainnya [11]. Hal ini bertujuan untuk menyediakan masukan terhadap penilaian keamanan berdasarkan skenario sebenarnya. Kecukupan penggunaan ISSAF untuk memenuhi syarat penilaian keamanan pada sebuah Organisasi dan bisa digunakan sebagai referensi untuk memenuhi keamanan informasi lainnya. ISSAF mencakup aspek penting dalam memproses keamanan, penilaian, dan membantu untuk mendapatkan gambaran lengkap tentang kerentanan yang mungkin ada. Berikut tahapan – tahapan pada ISSAF (*Information System Security Assesment Framework*):



Gambar 2. 3 Tahap-Tahap ISSAF

2.2.2.1 Information Gathering

Dalam tahap ini peneliti menggunakan Internet untuk mendapatkan informasi sebanyak-banyaknya dari target (Perusahaan atau Orang) dengan menggunakan metode teknikal (DNS/WHOIS) dan non-teknikal (Search Engine, list E-mail, dan lain-lain). Information Gathering tidak membutuhkan peneliti untuk menetapkan hubungan dengan sistem target. Informasi bisa didapatkan melalui sumber-sumber publik seperti internet, dan organisasi-organisasi yang mempunyai informasi public, seperti perpustakaan dan lain-lai**n**

2.2.2.2 Network Mapping

Setelah informasi berhasil didapatkan, pendekatan teknikal yang dapat dilakukan ialah meletakkan "Footprint" ke sistem ataupun jaringan yang diinginkan. Untuk lebih efektif, Network Mapping sebaiknya dilakukan dengan sesuai dengan rencana. Rencana ini mencakup kemungkinan titik terlemah atau hal-hal yang paling penting dari perusahaan yang akan di nilai**.**

2.2.2.3 Vulnerability Identification

Disaat Vulnerability Identification, penguji akan melakukan beberapa aktifitas untuk mendapatkan kerentanan yang ada pada sistem.

2.2.2.4 Penetration

Penguji akan mencoba untuk mendapatkan akses secara illegal dengan cara mengakali seistem keamanan dan mencoba untuk mencapai akses level seluas-luasnya.

2.2.2.5 Gaining Access & Privilege Escalation

Di beberapa situasi, sebuah sistem dapat dinilai lebih jauh, dalam fase ini mengizinkan penguji untuk memastikan dan mendokumentasikan kemungkinan gangguan, dan penyebaran serangan otomatis. Hal ini memungkinkan hasil dari pengujian yang lebih baik kepada target secara menyeluruh.

2.2.2.6 Enumerate Further

Dalam tahap ini, memungkinkan penguji untuk mendapatkan informasi tambahan berdasarkan proses pada sistem.

2.2.2.7 Compromise Remote User/Sites

Sebuah kerentanan sudah cukup untuk membuka seluruh network, sebagaimanapun amannya sebuah jaringan. Penguji dapat mencoba untuk menggunakan *remote user*. Hal ini dapat memudahkan untuk mendapatkan hak akses untuk ke jaringan yang lebih dalam

2.2.2.8 Maintaining Access

Dengan menggunakan sesuatu seperti *Backdoor*, penguji dapat kembali ke dalam sebuah sistem, bahkan jika sistem yang diuji sudah tidak lagi ada. *Backdoor* dapat dibuat dengan beberapa cara, baik dengan menggunakan *root-kit*, dengan mengizinkan sistem target terkoneksi dengan server penguji dan lain-lain.

2.2.2.9 Covering the Track

Pada tahapan ini, penguji akan menghapus jejak-jejak yang ada dengan cara menyembunyikan file, dan juga menghapus log files

2.2.2.10 Reporting

Pada tahap ini, penguji akan melakukan penulisan laporan yang mendeskripsikan hasil pengujian dengan rekomendasi dan penyelesaiannya.

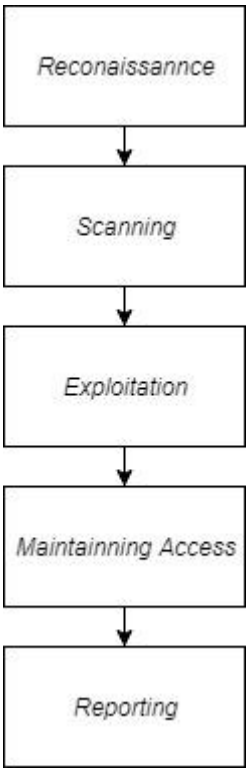
2.2.2.11 Clean And Destroy Artifacts

Semua informasi yang telah dibuat atau diletakkan di sistem sudah harus dihapus pada tahap ini. Jika tidak dapat dilakukan, dengan *remote system*, hal ini harus diberitahukan kepada pihak yang diuji agar para staff IT pada pihak tersebut dapat menghapus informasi ini setelah laporan diterima

2.2.3 Open Web Application Security Project (OWASP)

Open Web Application Security Project (OWASP) adalah sebuah komunitas yang bebas dan terbuka yang berdedikasi untuk memungkinkan organisasi untuk mengembangkan, membeli, dan menjaga aplikasi yang dapat dipercaya, semua *tools*, dokumen, forum yang digunakan OWASP bersifat gratis dan terbuka untuk siapa saja yang tertarik untuk memperbaiki keamanan aplikasi

[12]. Berikut merupakan tahapan dari *Framework OWASP (Open Web Application Security Project) :*



Gambar 2. 4 Tahap – Tahap Owasp

2.2.10.1 Reconaissannce

Reconnaissance atau tahap *Information Gathering* adalah tahap awal yang bertujuan untuk mengumpulkan data informasi mengenai target, dimana pada tahap ini, *tester* akan mencoba mengumpulkan semua data informasi sebanyak-banyaknya mengenai target, seperti hobi, jenis komputer, nama anak, alamat, yang semuanya bisa berguna untuk tahap selanjutnya.

2.2.10.2 Scanning

Scaning atau sering dikenal dengan tahap *vulnerability assessment* merupakan proses dimana *tester* mengumpulkan berbagai informasi mengenai *vulnerability* (kerentanan) yang terdapat pada sebuah *Website* seperti pada *engine, plugins, themes* dan *username* yang terdapat pada *Website* target. Dalam tahap ini *tester* akan mencari berbagai kemungkinan mengenai adanya *vulnerability* yang bisa digunakan oleh *attacker* untuk merusak dan memanipulasi data yang ada pada *Website*

2.2.10.3 Exploitation

Exploitation atau tahap *gainning access* merupakan kegiatan lanjutan untuk masuk kedalam sistem keamanan komputer setelah diketahui adanya *bugs* (cela) dan *vulnerability* (kerentanan) yang didapatkan dalam proses *Scanning*.

2.2.10.4 Maintaining Access

Proses *maintaining acces* dilakukan untuk mengamankan jalur yang sudah digunakan untuk masuk kedalam sistem keamanan komputer agar bisa dipergunakan kembali tanpa harus mengulang dari langkah pertama. Biasanya seorang *attacker* atau *pentester* dan menanamkan aplikasi berupa *malware* berupa *rootkit, trojan, keyloger, virus, bootnet* dan *backdoor* agar *attacker* dapat kembali masuk kedalam sistem komputer lagi tanpa harus melakukan proses dari awal.

2.2.10.5 Reporting

Pada tahap ini, seluruh data yang ditemukan berupa *vulnerability* (kerentanan) yang diperoleh dari hasil evaluasi, data bisa berupa *screenshoot, tools* yang digunakan, data *traffic* yang terekam semuanya bisa dijadikan bahan untuk dokumentasi dan presentasi, yang akan dibuatkan laporan secara terstruktur dari kegiatan penetrasi dari tahap awal sampai akhir sebagai solusi penanganan sistem keamanan pada aplikasi *web* agar lebih baik lagi.

2.2.4 Accunetix

Pada bulan Juli 2005, Acunetix Web Vulnerability Scanner dirilis: alat heuristik yang dirancang untuk meniru metodologi hacker untuk menemukan kerentanan berbahaya seperti SQL *Injection* dan cross site scripting. Satu dekade kemudian Acunetix Vulnerability Scanner telah menjadi alat pilihan bagi banyak pelanggan di Pemerintah, Militer, Pendidikan, Telekomunikasi, Perbankan, Keuangan, dan E-Commerce sektor, termasuk banyak perusahaan Fortune 500. Acunetix Vulnerability Scanner tersedia baik sebagai online dan di solusi premis. Acunetix Vulnerability Scanner mendeteksi dan melaporkan berbagai macam kerentanan dalam aplikasi yang dibangun pada arsitektur seperti WordPress, PHP, ASP.NET, Java *Framework* s, Ruby on Rails dan banyak lainnya. Acunetix Vulnerability Scanner membawa fitur-set yang luas dari kedua alat pengujian

penetrasi otomatis dan manual, memungkinkan analis keamanan untuk melakukan penilaian kerentanan yang lengkap, dan perbaikan terdeteksi ancaman, dengan hanya satu produk. [13]

2.2.5 Risk Rating Methodology

Metode penelitian yang dilakukan menggunakan OWASP Risk Rating Methodology. Dengan pendekatan OWASP ini akan membantu dalam menentukan standar keamanan aplikasi. Standar menentukan resiko menurut OWASP Risk Rating Methodology yaitu:

Risk = *Likelihood* * Impact

Dimana langkah – langkah yang akan dilakukan dalam menentukan resiko dari nilai *likelihood* dan *impac* yang didapat adalah sebagai berikut:

1. *Identifying a Risk*

   Langkah pertama ialah mengidentifikasi resiko keamanan yang perlu dinilai. Penguji perlu mengumpulkan informasi tentang ancaman yang terlibat, serangan yang akan digunakan, kelemahan yang terlibat, dan dampak yang terjadi jika proses sukses mengeksploitasi sistem. Serangan mungkin dilakukan oleh beberapa kelompok penyerang, bahkan terdapat pula beberapa dampak bisnis yang berbeda. Secara umum, kesalahan terbesar pengaturan sistem adalah menentukan langkah dengan menggunakan opsi terburuk, yang akan dijadikan risiko tertinggi secara keseluruhan.

2. *Factor of estimating likelihood*

   Setelah mengidentifikasi potensi risiko, langkah kedua adalah memperkirakan "*likelihood*". Ada sejumlah faktor yang dapat membantu menentukan "*likelihood*". Tujuannya adalah untuk memperkirakan kemungkinan serangan sukses dari sekelompok penyerang. Ada beberapa agen ancaman yang dapat mengeksploitasi kerentanan tertentu, sehingga biasanya itu adalah langkah terbaik untuk menggunakan skenario terburuk

Adapun angka-angka yang akan digunakan untuk memperkirakan "*likelihood*" secara keseluruhan.

2.1.Threat Agent Factors

Faktor pertama yang berhubungan dengan agen ancaman yang terlibat. Tujuannya adalah untuk memperkirakan kemungkinan serangan sukses oleh kelompok ini agen ancaman.

2.2.Vulnerability Factors

Faktor berikutnya yang berhubungan dengan kerentanan yang terlibat. Tujuannya adalah untuk memperkirakan kemungkinan kerentanan yang terlibat dan dapat dieksploitasi berdasar agen ancaman di atas.

3. *Factor of estimating likelihood*

Ada dua macam dampak setelah menentukan "*likelihood*". Yang pertama adalah "*Technical Impact* " pada aplikasi, penggunaan data, dan penyediaan fungsi. Yang kedua adalah "*Business Impact* " pada bisnis dan perusahaan yang beroperasi aplikasi. Setiap faktor memiliki rating dampak dari 0 sampai 9 untuk memperkirakan dampak keseluruhan.

4. *Determining Severity of Risk*

Dalam langkah ini, diidentifikasikan tingkat *likelihood* dan Impact . Skala dibagi menjadi tiga bagian, yaitu:

Tabel 2. 1 Likelihood and Impact Level

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Informal Method

Dalam beberapa kasus, tidak ada yang salah dalam menentukan faktor dan menentukan jawaban. Penguji sistem tetap menentukan faktor-faktor dan mengidentifikasi faktor-faktor kunci "*drive*" yang menentukan hasilnya. Penguji sistem bisa menemukan penentuan awal yang salah dengan mempertimbangkan aspek resiko yang tidak jelas.

Repeatable Method

Untuk mempertahankan nilai/hasil, maka perlu dilakukan proses yang lebih formal dan menghitung hasilnya kembali. Ada banyak ketidakpastian dalam perkiraan ini dan faktor-faktor dimaksudkan untuk membantu penguji sistem untuk mendapatkan hasil yang masuk akal. Proses ini dapat didukung oleh alat otomatis untuk membuat perhitungan lebih mudah.

Langkah pertama adalah untuk memilih salah satu pilihan yang terkait dengan setiap faktor dan memasukkan nomor yang terkait dalam tabel. Kemudian mengambil rata-rata skor untuk menghitung *likelihood* keseluruhan. Sebagai contoh:

Tabel 2. 2 Likelihood Factor

Threat agent Factors					***Vulnerability Factors***			
Skill level	*Motive*	*Opportunity*	*Size*		*Ease of discovery*	*Ease of exploit*	*Awareness*	*Intrusion detection*
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								

Selanjutnya, penguji sistem perlu mengetahui dampak keseluruhan. Proses ini hampir sama dengan perhitungan *likelihood* pada tabel 2.2 Masukan nilai setiap faktor yang terkait ke dalam tabel. Kemudian mengambil rata-rata skor untuk menghitung Impact secara keseluruhan. Sebagai contoh:

Tabel 2. 3 **Asumsi Impact**

Technical Impact					Business Impact		
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical Impact =7.25 (HIGH)				Overall business Impact =2.25 (LOW)			

Determining Severity

Selanjutnya penguji sistem dapat menggabungkan dengan cara mengkalikan hasil rata-rata *likelihood* dengan Impact untuk mendapatkan nilai keparahan akhir untuk suatu resiko.

Tabel 2. 4 **Overal Risk Severity**

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Dari contoh diatas, rating *likelihood* rating menunjukkan bahwa Medium sedangkan technical Impact menunjukkan High, maka dalam perspektif teknikal, overal risk security menunjukkan level high.

5. *Deciding what to fix*

Setelah risiko aplikasi telah diklasifikasikan, langkah berikutnya adalah memprioritaskan daftar mana yang terlebih dahulu harus diperbaiki. Sebagai aturan umum, resiko yang paling parah harus diperbaiki terlebih dahulu.

6. *Costumizing the Risk Rating Model*

   Proses menentukan penilaian disesuaikan dengan faktor apa saja yang dapat mempengaruhi resiko yang serius. Ada beberapa cara untuk menyesuaikan faktor diantaranya:

   a. *Adding Factor*

      Penguji sistem dapat memilih berbagai faktor apa saja yang penting bagi organisasi tertentu. Sebagai contoh, aplikasi militer bisa menambahkan faktor dampak terkait dengan hilangnya nyawa manusia atau informasi rahasia. Penguji sistem mungkin juga menambahkan faktor *likelihood*, seperti kesempatan bagi penyerang atau enkripsi kekuatan algoritma.

   b. Costumizing Options

      Ada beberapa pilihan sampel yang terkait dengan masing-masing faktor. Penguji sistem juga dapat mengubah rentang penilaian dengan pilihan yang telah ditetapkan sebelumnya. Cara terbaik untuk mengidentifikasi nilai yang tepat adalah dengan membandingkan peringkat yang dihasilkan dengan penilaian yang dihasilkan oleh tim ahli.

   c. *Weighting Factor*s

      Metode ini mengasumsikan bahwa semua faktor sama pentingnya. Penguji sistem dapat mengukur faktor dengan menekan secara lebih signifikan untuk bisnis yang lebih spesifik. Tapi jika semuanya sama, dapat dilakukan dengan mencocokan penilaian resiko bisnis yang akurat.