BAB 2
TINJAUAN PUSTAKA

2.1 Profil Dan Tempat Penelitian

2.1.1 Profil Dinas Komunikasi Dan Informatika Kabupaten Tangerang

Dinas Komunikasi dan Informatika adalah unsur pelaksana otonomi Daerah yang menyelenggarakan pelayanan di bidang Komunikasi dan Informatika, yang dipimpin oleh seorang Kepala Dinas yang berkedudukan di bawah dan bertanggung jawab kepada Bupati melalu Sekretaris Daerah. Dinas Komunikasi dan Informatika mempunyai tugas pokok melaksanakan urusan pemerintahan daerah berdasarkan asas otonomi dan tugas pembantuan di bidang Komunikasi dan Informatika sesuai dengan kewenangan dan kebijakan Pemerintah Daerah. Susunan organisasi Dinas Komunikasi dan Informatika, terdiri dari Kepala dinas, Sekretariat (Sub Bagian Perencanaan dan Keuangan, Sub Bagian Umum dan Kepegawaian), Bidang Komunikasi dan Informasi (Seksi Pos dan Telekomunikasi, Seksi Informasi Publik), Bidang Telematika (Seksi Pengembangan Telematika, Seksi Pengolahan Data Elektronik), Bidang Layanan Pengadaan Secara Elektronik (Seksi Pengembangan System, Seksi Pengembangan Layanan), Unit Pelaksana Teknis, Kelompok Jabatan Fungsional.

2.1.2 Visi dan Misi

Visi adalah pandangan jauh tentang suatu perusahaan ataupun lembaga, visi juga dapat di artikan sebagai tujuan perusahaan atau lembaga dan apa yang harus dilakukan untuk mencapai tujuannya tersebut pada masa yang akan datang atau masa depan. Visi tidak dapat dituliskan secara lebih jelas karena menerangkan mengenai detail gambaran sistem yang di tujunya, ini disebabkan perubahan ilmu serta situasi yang sulit diprediksi selama masa yang panjang.

Berikut ini adalah visi dan misi Dinas Komunikasi dan Informatika Kabupaten Tangerang yang menjadi pondasi utama guna untuk memajukan kualitas pemerintah daerah.

Visi : “Mewujudkan masyarakat Kabupaten Tangerang yang maju, inovatif dan berwawasan teknologi informatika menuju Tangerang Gemilang”.

Misi :

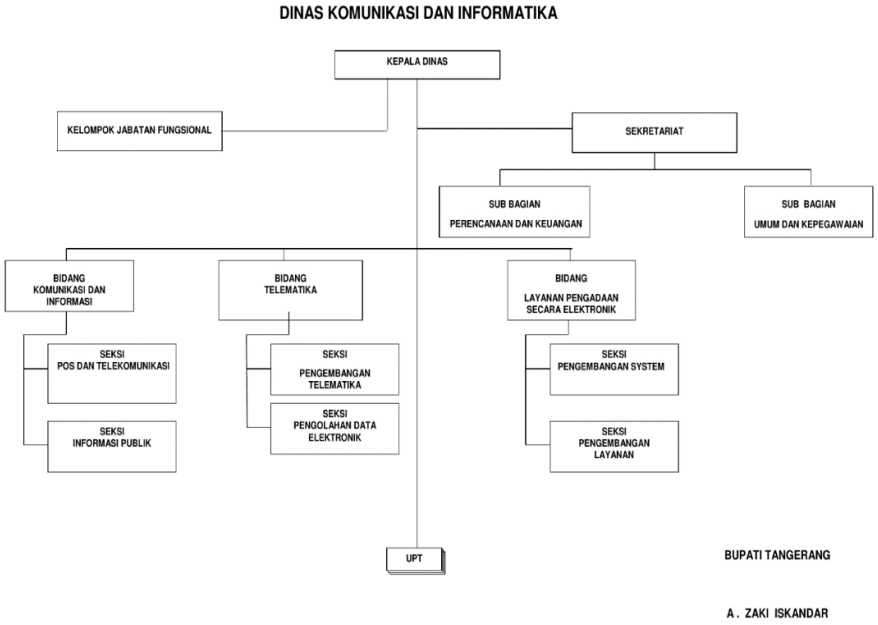
1. Meningkatkan transparansi aparatur Pemerintah Kabupaten Tangerang melalui teknologi informasi
2. Meningkatkan sumber daya aparatur dalam rangka profesionalisme aparatur yang berdasarkan teknologi informatika
3. Meningkatkan partisipasi dan pemahaman masyarakat terhadap kebutuhan teknologi informatika
4. Meningkatkan dan mengembangkan teknologi informatika untuk melayani masyarakat KabupatenTangerang
5. Meningkatkan kualitas sumber daya aparatur, memenuhi kebutuhan operasional dinas, meningkatkan kualitas laporan keuangan dan perencanaan dinas

Adapun tugas dan kewajiban yang harus dilakukan pihak Dinas Komunikasi dan Informatika adalah sebagai berikut.

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

2.1.3 Struktur Organisasi

Berikut ini adalah gambar dari struktur organisasi yang menunjukan hubungan setiap bagian di Dinas Komunikasi dan Informatika Kabupaten Tangerang.



Gambar 2.1 Struktur Organisasi Diskominfo Kabupaten Tangerang

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
    c. Sub Bagian Perencanaan
2. Kepala Bidang Telekomunikasi, membawahi:
    a. Kepala Seksi Layanan Telekomunikasi dan Persandian
    b. Kepala Seksi Pengawasan dan Pengendalian Telekomunikasi
3. Kepala Bidang Layanan Pengadaan Secara Elekronik (LPSE) :
    a. Kepala Seksi Pengembangan Layanan LPSE
    b. Kepala Seksi Pengembangan Sistem LPSE
4. Kepala Bidang Informasi dan Komunikasi :
    a. Kepala Seksi Informasi Publik
    b. Kepala Seksi Pemberitaan dan Informasi Media
    c. Kepala Seksi Publikasi dan Dokumentasi

5. Bidang Hubungan Masyarakat, membawahi:
    a. Seksi Peliputan dan Dokumentasi
    b. Seksi Kemitraan Media dan Publikasi
6. Kepala Bidang Telematika
    a. Kepala Seksi Pengembangan Infrastruktur Telematika
    b. Kepala Seksi Pengolahan Data Elektronik dan Statistik
    c. Kepala Seksi Perencanaan Teknologi Informasi dan Komunikasi
7. Kepala Subbagian Tata Usaha UPT Radio Daerah
8. Kepala UPT Radio Daerah
9. Kelompok Jabatan Fungsional

2.2 Landasan Teori

2.2.1 Keamanan Informasi

Keamanan informasi adalah perlindungan informasi dan karakteristiknya (kerahasiaan, integritas, dan ketersediaan) meliputi sistem dan perangkat keras yang digunakan, menyimpan, mengirim informasi, melalui penerapan program kebijakan, pelatihan kesadaran, dan teknologi [2].

Ada dua masalah utama keamanan informasi, diantaranya: *Threats* (Ancaman), dan *Vulnerability* (Kerentanan).

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman yang mungkin timbul dari kegiatan pengolahan informasi berasal dari 3 hal utama, yaitu: alam, manusia, dan lingkungan. Ancaman terhadap keamanan informasi berasal dari individu, organisasi, mekanisme, atau kejadian yang memiliki potensi untuk menyebabkan kerusakan pada sumber-sumber informasi perusahaan. Pada kenyataannya, ancaman dapat bersifat internal, yaitu berasal dari dalam perusahaan, maupun eksternal atau berasal dari luar perusahaan. Ancaman dapat juga terjadi secara sengaja atau tidak sengaja. Sedangkan kerentanan adalah kerentanan atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang

mencoba menyusup terhadap sistem tersebut. Tiga tujuan utama keamanan informasi, yaitu:

1. Kerahasiaan (Confidentiality)

   Melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif, sumber daya manusia, dan sistem pengolahan transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan

2. Integritas (Integrity)

   Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

3. Ketersediaan (Avalability)

   Data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya.

2.2.2 Internet

Pengertian internet (interconnection networking) sendiri adalah jaringan komunikasi global yang terbuka dan menghubungkan jutaan bahkan milyaran jaringan komputer dengan berbagai tipe dan jenis, dengan menggunakan tipe komunikasi seperti telepon, satelit dan lain sebagainya. Awalnya internet merupakan jaringan komputer yang dibentuk oleh Departemen Pertahanan Amerika Serikat pada tahun 1969 melalui sebuah proyek yang disebut dengan ARPANET. Misi awal dari proyek ini awalnya hanya untuk keperluan militer saja, tetapi lambat laun terus berkembang dan bisa dinikmati oleh semua kalangan [3]. Fasilitas yang dimiliki oleh internet diantaranya :

1. WWW

   World Wide Web atau yang sering disingkat dengan WWW merupakan sebuah sistem yang terdapat pada internet dan bertugas melakukan pencarian sekaligus pemberian informasi yang cepat dengan menggunakan teknologi hypertext.Untuk membuat hypertext, diciptakanlah sebuah bahasa pemrograman yang disebut *Hyper Text Markup Language* (HTML). HTML berfungsi mengikat alamat WWW atau file dalam sebuah dokumen

yang biasanya ber-extention *.htm atau *.html. Untuk mengirimkan file tersebut, diperlukan peran dari protokol pengiriman data yang spesifik yaitu *Hyper Text Transfer Protocol* (HTTP). Selain itu, untuk menemukan setiap hubungan hypertext diperlukanlah *Uniform Resource Locator* (URL).

2. Email

   Email merupakan surat atau pesan elektronik yang dikirimkan dan diterima antar pengguna komputer. Email memungkinkan seorang individu mengirimkan pesan ke individu lainnya dengan waktu yang cepat, bahkan dalam hitungan detik. Saat ini perkembangan email sangatlah pesat, email tidak hanya berisi teks saja. Kita bisa melampirkan file multimedia seperti gambar, foto, video bahkan animasi.

3. *Mailing-List*

   Mailing-List atau yang sering disebut dengan milis merupakan salah satu discussion group yang terdapat pada internet. Untuk menjadi anggota sebuah milis, kita terlebih dahulu mengirimkan email ke subsription address dan menunggu persetujuan dari moderator milis tersebut. Biasanya, anggota dari milis saling bertukar informasi, pendapat, dan lain sebagainya.

4. BBS

   Bulletin Board System atau yang biasa disingkat BBS merupakan suatu pusat layanan informasi yang menyediakan berbagai macam informasi dari berbagai bidang tertentu seperti bidang pendidikan, bisnis, sosial, teknologi dan lain-lain. Dengan menggunakan fasilitas ini, pengguna dapat bertukar pikiran dengan pengguna lainnya pada topik tertentu. Biasanya, pengguna yang mengakses BBS dapat mengunggah maupun mengunduh berita dari pengguna lain dengan mudah.

5. *Chatting*

   Chatting merupakan percakapan antara dua atau lebih pengguna komputer secara realtime dengan memanfaatkan jaringan internet. Bagi pengguna komputer yang telah melengkapi perangkat komputernya dengan webcam, maka mereka dapat chatting dengan melihat wajah pengguna lain yang di ajak chatting tersebut.

6. *Newsgroup*

   Sama halnya dengan milis, newsgroup juga merupakan salah satu discussion group yang ada di internet. Untuk mengakses suatu newsgrup, diperlukan jaringan komputer khusus yang biasa disebut UseNet. Setiap newsgroup di atur berdasarkan satu topik umum yang kemudian dibagi menjadi beberapa sub topik dibawahnya.

7. FTP

   FTP atau *File Transfer Protocol* merupakan layanan internet untuk melakukan transfer file antara pengguna komputer dengan suatu server di internet. Jadi, kita bisa melakukan pengiriman (upload) atau menyalin (download) sebuah file antara komputer kita dengan komputer lain yang terhubung pada jaringan internet. FTP umumnya dimanfaatkan sebagai wahana pendukung yang sangat diperlukan untuk pertukaran maupun penyebarluasan sebuah file melalui jaringan internet.

8. Gopher

   Gopher merupakan protokol layer aplikasi TCP/ IP yang dirancang khusus untuk keperluan distribusi, pencarian, maupun pengambilan dokumen melalui jaringan internet.

2.2.3 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer adalah:

1. Membagi sumber daya: contohnya berbagi
2. pemakaian printer, CPU, memori, harddisk
3. Komunikasi: Email, IM, Chatting
4. Akses informasi: contohnya *web browsing*

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta layanan disebut klien (*client*) dan yang memberikan layanan disebut pelayan

(*server*). Arsitektur ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer. Klasifikasi Berdasarkan skala:

1. *Local Area Network* (LAN)
2. *Metropolitant Area Network* (MAN)
3. *Wide Area Network* (WAN)

Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai client dan juga server. Tetapi ada jaringan yang memiliki komputer yang khusus didedikasikan sebagai server sedangkan yang lain sebagai client. Ada juga yang tidak memiliki komputer yang khusus berfungsi sebagai server saja [4]. Karena itu berdasarkan fungsinya maka ada dua jenis jaringan komputer:

1. *Client-server*

Yaitu jaringan komputer dengan komputer yang didedikasikan khusus sebagai server. Sebuah service/layanan bisa diberikan oleh sebuah komputer atau lebih. Contohnya adalah sebuah domain seperti http://www.detik.com yang dilayani oleh banyak komputer web server. Atau bisa juga banyak service/layanan yang diberikan oleh satu komputer. Contohnya adalah server jtk.polban.ac.id yang merupakan satu komputer dengan multi service yaitu mail server, web server, file server, database server dan lainnya.

2. *Peer-to-peer*

Yaitu jaringan komputer dimana setiap host dapat menjadi server dan juga menjadi client secara bersamaan. Contohnya dalam file sharing antar komputer di Jaringan Windows Network Neighbourhood ada 5 komputer (kita beri nama A,B,C,D dan E) yang memberi hak akses terhadap file yang dimilikinya. Pada satu saat A mengakses file share dari B bernama data_nilai.xls dan juga memberi akses file soal_uas.doc kepada C. Saat A mengakses file dari B maka A berfungsi sebagai client dan saat A memberi akses file kepada C maka A berfungsi sebagai server. Kedua fungsi itu dilakukan oleh A secara bersamaan maka jaringan seperti ini dinamakan peer to peer.

Berdasarkan topologi jaringan: Berdasarkan topologi jaringan, jaringan komputer dapat dibedakan atas:

1. Topologi bus

2. Topologi bintang
3. Topologi cincin
4. Topologi Mesh (Acak)
5. Topologi Pohon (Hirarkis)
6. Topologi Linier

Adapun manfaat yang didapat dari menggunakan jaringan adalah sebagai berikut:

1. Jaringan memungkinkan manajemen sumber daya lebih efisien. Misalnya, banyak pengguna dapat saling berbagi printer tunggal dengan kualitas tinggi, dibandingkan memakai printer kualitas rendah di masing-masing meja kerja. Selain itu, lisensi perangkat lunak jaringan dapat lebih murah dibandingkan lisensi stand-alone terpisah untuk jumlah pengguna sama. Jaringan membantu mempertahankan informasi agar tetap andal dan up-to-date.
2. Sistem penyimpanan data terpusat yang dikelola dengan baik memungkinkan banyak pengguna mengaskses data dari berbagai lokasi yang berbeda, dan membatasi akses ke data sewaktu sedang diproses.
3. Jaringan membantu mempercepat proses berbagi data (data sharing). Transfer data pada jaringan selalu lebih cepat dibandingkan sarana berbagi data lainnya yang bukan jaringan.
4. Jaringan memungkinkan kelompok kerja berkomunikasi dengan lebih efisien. Surat dan penyampaian pesan elektronik merupakan substansi sebagian besar sistem jaringan, disamping sistem penjadwalan, pemantauan proyek, konferensi online dan groupware, dimana semuanya membantu team bekerja lebih produktif.
5. Jaringan membantu usaha dalam melayani klien mereka secara lebih efektif. Akses jarak-jauh ke data terpusat memungkinkan karyawan dapat melayani klien di lapangan dan klien dapat langsung berkomunikasi dengan pemasok.

Terdapat tiga tipe jaringan yang umum digunakan diantaranya adalah :

1. Jaringan *Workgroup*

Jaringan ini terdiri dari beberapa unit komputer yang dihubungkan dengan menggunakan Network Interface Card atau yang biasa disebut dengan Local Area Network Card, serta dengan menggunakan kabel BNC maupun UTP. Semua unit komputer yang terhubung dapat mengakses data dari unit komputer lainnya dan juga dapat melakukan print document pada printer yang terhubung dengan unit komputer lainnya.

2. Jaringan LAN

LAN (*Local Area Network*) adalah suatu kumpulan komputer, dimana terdapat beberapa unit komputer (client) dan 1 unit komputer untuk bank data (server). Antara masing-masing client maupun antara client dan server dapat saling bertukar file maupun saling menggunakan printer yang terhubung pada unit-unit komputer yang terhubung pada jaringan LAN. Berdasarkan kabel yang digunakan ,ada dua cara membuat jaringan LAN, yaitu dengan kabel BNC dan kabel UTP.

3. Jaringan WAN

WAN (*Wide Area Network*) adalah kumpulan dari LAN dan/atau Workgroup yang dihubungkan dengan menggunakan alat komunikasi modem dan jaringan Internet, dari/ke kantor pusat dan kantor cabang, maupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat serta dengan biaya yang relatif murah. Sistem jaringan ini dapat menggunakan jaringan Internet yang sudah ada, untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan PC Stand Alone/Notebook yang berada di lain kota ataupun negara.

2.2.4 Black Box Testing

Black box testing adalah pengujian yang dilakukan hanya mengamati hasil eksekusi melalui data uji dan memeriksa fungsional dari perangkat lunak. Pada pengujian ini, penguji hanya melihat interfacenya dan fungsionalitasnya saja, tanpa perlu mengetahui proses apa saja yang terjadi pada proses detilnya. Pada proses ini penguji hanya diberitahukan alamat website atau alamat IP nya saja,

dan mencoba untuk memecahkan website tersebut seolah-olah menjadi hacker. Black box testing adalah metode pentest dimana diasumsikan penguji sistem tidak mengetahui sama sekali infrastruktur dari target pentest. Dengan demikian pada pengujian black box ini penguji sistem harus mencoba untuk menggali dari awal semua informasi yang diperlukan kemudian melakukan analisis serta menentukan jenis attack yang akan dilakukan.

2.2.5 *Proof of Concept Exploit*

Proof of Concept Exploit atau sering disebut dengan (PoC) adalah sebuah jenis serangan terhadap sistem komputer atau jaringan. Hal ini dilakukan hanya untuk membuktikan bahwa semua itu bisa dilakukan, dan ini umumnya tidak menimbulkan kerugian, namun menunjukkan bagaimana seorang hacker dapat memanfaatkan kerentanan dalam perangkat lunak atau mungkin perangkat kerasnya[5].

2.2.6 *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. 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[6].

Informasi yang dihasilkan *ISSAF* di organisasikan menjadi evaluasi kriteria, evaluasi tersebut di tinjau berdasarkan domainnya masing – masing. Kriteria evaluasi yang di maksud adalah :

1. Deskripsi kriteria evaluasi
2. Tujuan dan objektif
3. Pra-syarat melakukan evaluasi

4. Proses evaluasi
5. Menampilkan hasil yang di inginkan
6. Rekomendasi pencegahan
7. Referensi dokumen external

2.2.6.1 Tujuan Metode ISSAF

Tujuan dari metode *Information Systems Security Assessment Framework* (ISSAF) adalah untuk menyediakan titik tunggal referensi berupa penilaian keamanan. Ini adalah referensi yang sangat sesuai dengan masalah penilaian keamanan dan merupakan proposisi nilai untuk bisnis. Dalam memenuhi tujuan ini, ISSAF memiliki memiliki agenda tingkat tinggi yang diantaranya adalah :

1. Evaluasi kebijakan dan proses keamanan informasi organisasi dan pastikan mereka memenuhi persyaratan industri dan tidak melanggar undang-undang dan peraturan yang berlaku
2. Identifikasi infrastruktur sistem informasi penting yang diperlukan untuk proses bisnis organisasi dan evaluasi keamanan mereka
3. Lakukan penilaian kerentanan & tes penetrasi untuk menyoroti kerentanan sistem dan dengan demikian mengidentifikasi kelemahan dalam sistem, jaringan dan aplikasi
4. Mengevaluasi kontrol yang diterapkan ke berbagai domain keamanan dengan :
    a. Menemukan kesalahan konfigurasi dan meluruskannya
    b. Mengidentifikasi risiko terkait dengan teknologi yang digunakan dan mengatasinya
    c. Mengidentifikasi risiko dalam orang atau proses bisnis dan mengatasinya
    d. Memperkuat proses dan teknologi yang ada
5. Memprioritaskan kegiatan penilaian sesuai dengan tingkat kritis sistem, biaya pengujian, dan potensi keuntungan.
6. Mengajarkan orang tentang melakukan penilaian keamanan
7. Mengajarkan orang tentang keamanan sistem, jaringan dan aplikasi
8. Menyediakan informasi tentang :

a. Mengulas pengembangan, monitoring & proses audit
b. Membangun dan mengulasan Rencana Pemulihan suatu kejadian
c. Tinjauan terhadap masalah keamanan

9. Kepatuhan terhadap standar hukum & peraturan
10. Kesadaran keamanan
11. Manajemen yang efektif untuk proyek penilaian keamanan
12. Terlindung dari eksploitasi *social enginering.*
13. Tinjauan kontrol keamanan fisik

Pendekatan ini didasarkan pada penggunaan jalur terpendek yang dibutuhkan untuk mencapai tujuan seseorang dengan menemukan kekurangan yang dapat dimanfaatkan secara efisien, dengan sedikit usaha. Tujuan dari kerangka kerja ini adalah untuk memberikan kelengkapan dan akurasi, efisiensi terhadap penilaian keamanan.

2.2.7 Penilaian Keamanan Web Aplikasi (*ISSAF*)

Keamanan suatu web aplikasi merupakan keamanan semua kompone – komponen yang digunakan oleh web aplikasi, web server yang menjalankan web aplikasi dan modul – modul pada web server. Semua trafik yang di arahkan ke web server yaitu dengan melalui protokol http/https, yang mana trafik tersebut ada yang bisa dipercaya dan ada pula yang tidak di blok oleh *firewall.* Web server sering menjadi sasaran untuk dijadikan target penyerangan[7].

1. *Purpose*

   Untuk membuat web aplikasi dan web server seaman mungkin dari serangan dan menutup beberapa informasi yang tidak di perlukan, yang akan mempersulit *attacker* untuk bisa mendapatkan informasi.

2. *Objective*

   Untuk mendapatkan akses terhadap *remote-machine* dengan melewati *firewall* dan menguasai jaringa. Mengumpulkan informasi apa saja dari jaringan dan server.

3. *Expected Result*

Pada umumnya setiap perusahaan ataupun organisasi menempatkan *firewall* untuk keamanan biasanya pada port 80 untuk webserver.

4. *Pre-requisite*

   Basik pengetahuan dari HTTP Protocol.

2.2.7.1 *Identifying web server vendor and version*

Langkah pertama ketika melakukan penilaian web aplikasi adalah mengidentifikasikan web server pada aplikasi apa yang berjalan. Untuk mendeteksi webser, hal – hal yang perlu dilakukan yaitu :

1. Banner grabbing
2. Menggunakan alat otomatis untuk mendeteksi web server
3. Default file detection
4. Mengecek ekstensi file pada server

2.2.8 Penilaian Keamanan Web Aplikasi Lanjutan(*ISSAF*) SQLi

Penilaian keamanan web aplikasi lanjutan akan memfokuskan penjelasan terhadap serangan *sql-injection.* Dengan teknik ini pihak ketiga(*attacker)* bisa membuat atapun menambahkan peritah sql dengan menggunakan *special-symbol* untuk mendapatkan suatu akses. Setelah mendapatkan kendali terhadap server dapat dipastikan bahwa server sql lainnya dapat dipetakan. *Sql-injection* ini terjadi karena lemahnya validasi input pada suatu web aplikasi, pada saat itu pula *attacker* memanipulasi perintah sql (*SQL Query*) dengan kumpulan statement sql kedalam web aplikasi. Aplikasi yang tidak memvalidasi hasil masukan dari pengguna (*user*) inilah yang menyebabkan potensi kerentanan terhadap *sql-injection,* ada beberapa cara untuk mengeksploitasi kerentanan tipe ini diantaranya adalah :

1. Changing SQL values
2. Concatenating SQL Values
3. Adding Function calls & stored Procedures to a statement
4. Typecast and concatenate retrieved data
5. Adding system functions & procedure to find out critical information about the server

Dalam pengujian ruang lingkup, *ISSAF* mengujinya dengan menggunakan Microsoft SQL server 2000 sebagai *Database Management System,*web server dan autentikasi website. Pada pengujian ini juga disediakan dua halaman berupa asp (*Active Server Pages*) yang pertama digunakan untuk menampung hasil masukan dari pengguna dan kedua untuk mengecek masukan dari pengguna terhadap data didalam database yang menggunakan perintah SQL. Untuk menguji kerentanan *sql-injection* terdapat beberapa cara yang bisa dilakukan, yaitu dengan cara memasukan spesial karakter kedalam masukan(*Input*). Contoh spesial karakter dapat dilihat pada tabel berikut.

Tabel 2.1 Spesial Karakter

SQL Injection Special Character						
‘	;	,	“	%	-	*

Bypass user authentication merupakan pengujian yang didasarkan pada halaman utama seorang user/admin, dimana pada pengujian ini *attacker* berusaha untuk menguji validasi masukan dari halaman login dengan cara memasukan suatu nilai yang memungkinkan *attacker* untuk bisa mendapatkan hak akses istimewa (*privileges access*) tanpa masuk sebagai user/admin, adapun masukan (*payload*) yang dimaksud adalah sebagai berikut[8].

1. ' Or 1=1); --
2. 'OR"='
3. ' any_bad_value
4. ‘ “
5. ‘ “or”
6. ‘admin’—
7. “any_bad_value” ‘ etc

Berdasarkan ketujuh spesial karakter (*payload*) diatas peneliti akan mengambil contoh penggunaan pada *payload* ‘OR”=’. Penggunaan karakter ini akan menjadi bahan yang sangat kuat ketika seorang *attacker* memasukan nilai kedalam suatu *form* yang terdapat pada website yang akan diuji, karena karakter tersebut sudah terbukti penggunaanya mampu mengacaukan hubungan antara suatu website yang terkait dengan sistem database yang dikelola oleh target.

2.2.9 Dnsdumpster

Dnsdumpster adalah alat yang digunakan untuk meneliti suatu domain, alat ini mampu menemukan kumpulan *host* yang terhubung dengan *host* tersebut. Terlebih dari pada hanya mencari dengan *DNS Lookup* alat ini mampu menemukan *sub-domain* dan *web-hosts*, alat ini juga bisa digunakan untuk pengumpulan data seperti mencari *http-header,banner for netblock*. Hasil keluaran dari penggunaan aplikasi ini berupa pemetaan (*mapping*) suatu domain dan subdomainnya.

2.2.10 NSE (*Nmap Scripting Engine*)

NSE merupakan salah satu fitur nmap yang fleksibel. Memungkinkan programmer untuk menulis (dan mengembangkan) *script* ini untuk melakukan automate scanning pada jangkauan jaringan yang luas. Script ini kemudian di eksekusi secara paralel dengan kecepatan dan efisiensi watu yang telah di tentukan Nmap itu sendiri[9]. Fungsi yang digunakan pada NSE ini berdasarkan hal-hal berikut ini :

1. *Network Discovery*

   Network Discovery merupakan tahap *look-up,whois* berdasarkan data dari domain target, menggunakan perintah query dari ARIN,RIPE, atau APNIC untuk menentukan hak milik dari target IP.

2. *More sophisticated version detection*

   Deteksi versi sistem berfungsi untuk mencari kumpulan *service* melalui alat ini dan basis pencocokan sistem dari regula ekspresi.

3. Vulnerability detection

   Ketika tipe baru dari kerentanan di temukan, biasanya hal yang dilakukan adalah melakukan *scanning* pada suatu jaringan untuk mengidentifikasikan kerentanan sistem sebelum ada pihak ketiga yang melakukannya.

4. *Backdoor detection*

   Banyaknya pihak ketiga (*attacker*) dan beberapa *automate-worms* yang meninggalakan jejak *backdoor* untuk jalur masuk yang di gunakan *attacker* tersebut.

5. *Vulnerability exploitation*

   NSE juga bisa di gunakan untuk untuk memanfaatkan kerentanan dari pada hanya menemukan kerentanan tersebut. Pencapaian untuk menambahkan *custom exploit* bisa sangat membantu untuk sebagian user (dalah hal ini adalah *pentester*).

2.2.11 Jenis Kerentanan

Beberapa serangan berdampak pada suatu web aplikasi yang dapat merugikan pemilik dari website tersebut. Jenis serangan itu meliputi :

2.2.11.1 *SQL Injection*

SQL *Injection* adalah teknik untuk mengeksploitasi sebuah halaman *web* yang memakai basis data (*database*) seperti *My*SQL dengan memberikan kode kedalam *query* SQL. Terdapat 3 jenis metode serangan menggunakan SQL *Injection* diantaranya :

1. ***Error Based* SQL *Injection***

   Error Based SQL *Injection* dalam melakukan exploitasi kedalam halaman *web* yang menggunakan *database* hanya menampilkan pesan *error* jika exploitasi berhasil dilakukan, pesan *error* tersebut memberikan beragam informasi seperti versi *database* yang digunakan, yang dapat dimanfaatkan oleh *attacker*.

2. ***Union Based* SQL *Injection***

   Union Based SQL *Injection* adalah metode SQL *Injection* dengan memanfaatkan perintah *query* UNION dan menggabungkannya dengen beberapa perintah *query* lain seperti SELECT untuk menghasilkan informasi yang diinginkan oleh *attacker*.

3. ***Blind* SQL *Injection***

   Blind SQL *Injection*, metode serangan menggunakan jenis ini tidak akan menampilkan pesan *error* pada halaman *web* atau tidak juga menampilkan data atau informasi yang diinginkan, karena serangan dengan menggunakan metode *Blind* SQL *Injection* hanya menghasilkan kondisi *True* atau *False* dari *query* SQL yang dimasukan pada sebuah halaman *web* yang menjadi target.

Berdasarkan jenis kerentanan SQL *Injection* masing – masing memiliki dampak yang berbeda – beda, namun pada akhirnya selalu memiliki hasil yang sama pada jenis kerentanan SQL *Injection*. Karena dengan adanya kerentanan ini rahasia tentang struktur database ataupun data yang ada didalamnya bisa terancam, karena seorang *attacker* bisa dengan mudah menggunakan celah ini untuk bisa mendapatkan informasi mengenai database.

2.2.11.2 *XSS (Cross Site Scripting)*

XSS adalah salah satu jenis serangan *web* yang dilakukan dengan memanfaatkan kelemahan dan kesalahan yang terletak pada penulisan *scripting* pada suatu aplikasi *web* sehingga memungkinkan seseorang untuk menginjeksikan suatu *tag* HTML ataupun *Client Side Script* pada aplikasi *web* tersebut dikarenakan adanya variabel yang tidak disanitasi dengan baik. Dari serangan XSS ini seorang *attacker* akan mencoba mendapatkan suatu hak akses berupa *session cookies* dengan adanya interaksi langsung dengan pihak korban (*victim*) dengan berbagai macam pendekatan seperti *social engineering*. Karena tanpa adanya interaksi dengan korban, mustahil bagi seorang *attacker* untuk bisa mendapatkan suatu hak akses yang akan digunakan untuk menyusup kedalam sistem.

2.2.11.3 *DOS (Denial of service)*

DOS *(Denial of service)* adalah metode untuk mencegah pengguna untuk mendapatkan layanan yang diberikan oleh *server*, dengan harapan metode ini dapat mematikan dan menyibukan *server* dengan membanjiri layanan pada *server*.

2.2.12 WAMP (*Windows-Apache-MySQL-PHP*)

WAMP adalah sebuah program penginstal ciptaan Romain Bourdon. Program ini mengemas MySQL, PHP, dan *Apache* sehingga memudahkan para pengembang sistem yang hendak menggunakan ketiga perangkat lunak tersebut untuk membuat aplikasi berbasis web. WAMP tergolong sebagai perangkat lunak gratis (*opensource software)*, suatu jenis *software* yang bisa dipakai dan didistribusikan secara bebas kepada siapa saja. Siapapun bisa memperolehnya

dengan mengunduh pada situs http://www.wampserver.com/en/download.php. Selain ketiga software yang telah disebut sebelumnya, WAMP menyediakan WampServer yang bertindak sebagai manajer bagi program-program yang terkemas dalam WAMP. Selain itu, software ini juga memiliki tool bernama phpmyadmin yang berbasis aplikasi web. Aplikasi ini memudahkan pengguna berinteraksi dengan database server MySQL dalam mengakses data dalam database[10].

2.2.13 Acunetix

Pada bulan Juli 2005, *Acunetix Web Vulnerability Scanner* dirilis: *heuristic tools* 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 Frameworks, 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[11].

2.2.14 Vega

Vega adalah program aplikasi yang dibangun untuk pengujian keamanan aplikasi berbasis web, aplikasi ini berbasis *Graphic User Interface* (GUI) dan dapat beroperasi diberbagai macam sistem operasi pada komputer, karena aplikasi ini dibangun menggunakan bahasa pemrograman java, modul yang terdapat didalamnya sangat banyak dan dapat diperluas menggunakan javascript. Operasi yang dilakukan vega dapat dibagi menjadi dua bagian: beroperasi sebagai pemindaian otomatis (*automated scanner*) dan *intercepting proxy*. Pemindaian

secara otomatis (*automated scanner*) dilakukan dengan cara *crawling website*s, *extracting links*, *processing forms* dan menjalankan modul untuk menemukan kemungkinan injeksi pada website, modul – modul dapat melakukan hal- hal seperti mengotomatiskan permintaan pengajuan (*submit request*) dengan parameter yang di fuzz, misalnya pengujian seperti *cross-site-scripting* (*XSS*) atau *SQL injection*. Pemindaian sebagai proxy (*intercepting proxy*) dilakukan untuk analisis yang lebih spesifik dengan cara berhubungan langsung dengan web aplikasi menggunakan web-browser, ketika menggunakan mode ini, proxy yang aktifkan oleh vega akan berjalan pada lokalhost sebagai proxy server kemudian web-browser menggunakan proxy dari vega tersebut, hasil *request* dan *response* akan terlihat langsung pada aplikasi vega, mode ini juga bisa melakukan intersepsi kriteria (*interception criteria*) untuk permintaan keluar (*outgoing request*) dari web-browser atau respon masuk(*incoming response*) dari server. *Request* dan *response* ini disimpan dalam keadaan dimana keduanya bisa diedit sampai dapat dikirimkan kembali ke server.

2.2.15 Nikto

Nikto merupakan suatu alat gratis (*opensource*) yang di gunakan untuk pemindaian suatu web aplikasi dengan menggunakan CLI(*command line interfaces*) karna nikto dikembangkan menggunakan bahasa pemrograman perl. meskipun tidak adanya *user interface* pada nikto tetapi didalamnya terdapat 6700 potensi kerentanan file/program untuk pengujian. Dengan fitur *auto scanning* yang dilakukan nikto untuk mencari kerentanan secara automatis[].

2.2.16 Burpsuite

Burp Suite adalah alat yang sangat bagus sekali untuk pengujian keamanan aplikasi web. Alat ini sangat bagus untuk pentester dan peneliti keamanan. Ini berisi berbagai alat dengan antarmuka banyak di antara mereka yang dirancang untuk memudahkan dan mempercepat proses menyerang aplikasi website. Burp merupakan tools proxy yang berjalan pada port 8080 dengan protokol HTTP dimana request dan respon dapat diintercept dan dianalisa sebelum sampai kepada server atau klien, Fungsi Umum: *intercepting proxy*, *crawling* & *spider*, *web application scanner*, *attacker tools*, *repeater* dan *sequencer tools*[12]. Burpsuite

bekerja sebagai *intercepting tools* yang artinya, alat ini akan merekam semua *request* & *response* yang dilakukan melalui web browser yang digunakan untuk memodifikasi paket – paket yang akan diminta dan kemudian di kirimkan ke server target. Dengan kata lain semua trafik yang terdapat pada browser seorang *user* akan di proses oleh burpsuite guna untuk melakukan modifikasi terhadap paket – paket yang akan dikirmkan.

2.2.17 Kali Linux

Kali Linux adalah distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan digunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh Offensive Security. Kali linux dikembangkan oleh pengembang Backtrack sebelumnya yaitu Mati Aharoni bersama pengembang baru bernama Devon Kearns dari Offensive Security. Secara umum kali linux memiliki berbagai macam tools yang dapat dibagi ke dalam beberapa kasifikasi berdasarkan fungsi utamanya yaitu :

1. Information Gathering digunakan untuk mengumpulkan informasi dari suatu sistem
2. Reverse Enginerring digunakan untuk menganalisa suatu sistem melalui identifikasi komponen-komponennya dan keterkaitan antar komponen tersebut lalu membuat abstraksi dan informasi perancangan dari sistem yang dianalisa
3. Exploitation Tools digunakan untuk mengekspoitasi celah yang terdapat pada suatu sistem.
4. Vulnerability Assessement digunakan untuk melakukan pencarian, identifikasi, perhitungan terhadap celah keamanan suatu sistem
5. Privilege Escalation digunakan untuk melakukan serangan yang bertujuan untuk menaikkan tingkat akses didalam suatu sistem[13].

2.2.18 *Payload*

"Data aktual" yang terdapat didalam sebuah paket atau file dikurangi semua header yang terpasang untuk dikirimkan dan dikurangi semua meta data deskriptif. Dalam paket jaringan, header ditambahkan ke payload untuk transportasi dan kemudian dibuang di tempat tujuan. Dalam struktur nilai kunci-

kunci, kunci dan panjangnya adalah data deskriptif tentang nilai (payload). Dalam analisis perangkat lunak berbahaya (*malicious code*) seperti worm, virus dan Trojan, ini mengacu pada hasil perangkat lunak yang menghasilkan dampak negatif. Contoh dari tugas payload meliputi penghancuran data, pesan dengan teks yang menghina atau pesan e-mail palsu dikirim ke sejumlah besar orang[14].

Sebuah *payload* mengacu pada komponen virus komputer yang melakukan aktivitas berbahaya. Terlepas dari kecepatan penyebaran virus, tingkat ancaman virus dihitung akibat kerusakan yang diakibatkannya. Virus dengan muatan yang lebih kuat cenderung lebih berbahaya. Meski tidak semua virus membawa *payload*, akan tetapi tetap saja beberapa *payload* dianggap sangat berbahaya. *Payload* juga dikenal sebagai perusak. Contohnya adalah beberapa virus yang menyalin dirinya dari satu komputer ke komputer lainnya. Virus lain dapat mencuri data atau file, mengizinkan menguping atau akses tidak sah, menghancurkan data dan menimbulkan konsekuensi lainnya. Hal ini juga memungkinkan virus membawa beberapa *payload*. Saat ini malware lebih kecil kemungkinannya untuk memasukkan *payload* yang menyebabkan kerusakan pada file sistem; Sebagai gantinya, mereka mengaktifkan akses *backdoor* ke komputer pengguna dan pencurian informasi sensitif[15]. Beberapa cara untuk mengeksekusikan *payload* meliputi:

1. Dengan menggunakan komputer yang tidak terlindungi (komputer tanpa *anti-virus* terpasang) terhubung ke jaringan
2. Dengan booting komputer menggunakan media removable yang terinfeksi
3. Dengan membuka file yang terinfeksi
4. Dengan menjalankan program yang terinfeksi
5. Dengan mengaktifkan bom logika

2.2.19 *Common Weakness Enumeration (CWE)*

Common weakness enumeration ditargetkan untuk pengembang dan praktisi keamanan, merupakan daftar resmi jenis kelemahan perangkat lunak yang digunakan untuk :

1 Berfungsi sebagai bahasa yang umum untuk menggambarkan kelemahan keamanan perangkat lunak dalam hal arsitektur, Desain, atau kode.

2 Berfungsi sebagai standar yang menjadi tolak ukur alat-alat keamanan perangkat lunak penargetan kelemahan-kelemahan pada sistem.

3 Menyediakan satu standar dasar untuk identifikasi kelemahan, mitigasi dan pencegahan.

2.2.19.1 *Introduction*

Suatu organisasi ingin memastikan bahwa produk perangkat lunak yang mereka dapatkan dan kembangkan bebas dari kelemahan keamanan yang sudah umum. Saat ini, alat dan layanan berkualitas tinggi untuk menemukan kelemahan dalam kode dan pertanyaan baru adalah alat layanan yang tepat / baik untuk pekerjaan tertentu sulit untuk dijawab karena kurangnya struktur dan definisi dalam industri penilaian kode. CWE diciptakan khusus untuk mengatasi masalah ini. MITRE mulai mengerjakan masalah mengkategorikan kelemahan perangkat lunak pada awal tahun 1999, saat meluncurkan daftar CVE. Sebagai bagian dari pengembangan tim CVE MITRE, CVE mengembangkan Klasifikasi awal dan kategorisasi kerentanan, serangan, kesalahan, dan konsep lainnya untuk membantu mendefinisikan kelemahan perangkat lunak. Namun, walaupun cukup untuk CVE terlalu kasar untuk digunakan untuk mengidentifikasi dan mengkategorikan fungsionalitas yang ditawarkan dalam penawaran penilaian keamanan kode industri. Untuk mendukung penggunaan kesetiaan dan kecerdikan semacam itu diperlukan, seperti detail dan deskripsi tambahan untuk masing-masing node dan kelompok yang berbeda seperti efek, perilaku, dan rincian pelaksanaan, dan lain-lain. Untuk melakukan ini, MITER mengambil potongan pertama untuk merevisi Kategori CVE internal bekerja untuk digunakan dalam industri penilaian kode pada tahun 2005 sebagai bagian dari partisipasi MITER di perangkat yang disponsori oleh US Department of Homeland Security (DHS) Institut Nasional perangkat lunak (NIST) metrik jaminan proyek dan evaluasi alat (SAMATE). Kami mendokumentasikan, yang berjudul menghasilkan daftar contoh kerentanan awal untuk periset (PLOVER), adalah dokumen kerja yang berisi daftar lebih dari 1.500 beragam kerentanan dunia nyata yang diidentifikasi dengan nama CVE mereka. Kerentanan di PLOVER disusun dalam kerangka konseptual rinci yang saat ini menyebutkan 290 jenis kelemahan, kebiasaan,

kesalahan, dan kekurangan perangkat lunak, dengan sejumlah besar contoh kerentanan nyata untuk masing-masing. PLOVER mewakili usaha pertama yang benar-benar upaya bottom-up untuk mengambil kesalahan dan kekurangan yang diamati di dunia nyata yang ada dalam kode, abstrak mereka dan klasifikasi mereka menjadi kelas umum yang mewakili kerentanan potensial yang lebih umum yang dapat ada dalam kode tersebut, dan akhirnya mengatur mereka dalam struktur relatif yang sesuai sehingga membuatnya mudah diakses dan bermanfaat bagi beragam khalayak untuk beragam kebutuhan. Langkah selanjutnya setelah PLOVER adalah menetapkan definisi dan deskripsi yang dapat diterima tentang kelemahan umum masyarakat di bawah proyek SAMATE NIST, yang menyebabkan terciptanya daftar "enumerasi kelemahan umum" dan taksiran klasifikasi terkait. Daftar CWE sekarang berfungsi sebagai mekanisme untuk mendeskripsikan kemampuan penilaian kerentanan kode dalam kaitannya dengan cakupan CWE yang berbeda[16].

2.2.20 *Web crawler*

Suatu web aplikasi berisikan kumpulan – kumpulan informasi yang sangat besar dengan topik yang berbeda – beda, berbeda dengan koleksi tradisional seperti perpustakaan, Web tidak memiliki struktur konten terpusat. Data ini bias di unduh menggunakan *web crawler.* Jadi, *web crawler* adalah suatu perangkat lunak untuk mengunduh halaman per halaman yang terdapat pada web aplikasi secara automatis. Hal ini biasa juga disebut dengan istilah *web spider* atau *web robot. Web crawling* adalah metode yang penting untuk mengumpulkan dan menyimpan data yang berada di internet[17]. Hal – hal yang mampu dilakukang dengan *web crawler* diantaranya adalah :

1 Dengan mengecek setiap halaman yang dapat di unduh
2 Dengan mengecek apakah halaman yang akan diunduh diperbolehkan/ tidak dengan cara mengecek melalui file dari *robot-exclusion.*
3 Mengunduh seluruh halaman.