Tugas Teori Keamanan Data – Rangkuman Essestial Terminology – Security Challenges

Modul 1 : CEHv7 – Introduction to Ethical Hacking

Dimas Rizky H.P. – 2110141011

3 D4 IT A

**Istilah-Istilah Mendasar Pada Keamanan Data**

Tentunya dalam bidang keamanan data terdapat beberapa istilah/terminologi yang umum digunakan pada saat mengaplikasikan ilmu ini, antara lain

* Hack Value

Istilah ini merupakana gagasan yang digunakan untuk mengukur seberapa layak sesuatu untuk dilakukan dalam kalangan hacker. Tidak jarang dinilai karena kelayakan materil saja namun juga kelayakan dalam pandangan *entertainment*.

* Target of Evaluation

Istilah ini merujuk ke sistem komputer, produk atau komponen IT yang memerlukan evaluasi tentang keamanan dari sistem tersebut.

* Attack

Attack merupakan istilah untuk merepresentasikan suatu kegiatan yang melanggar sistem keamanan. Hal ini berarti adanya serangan yang ditujukan ke suatu sistem oleh hacker ataupun tim khusus yang memang dibuat untuk melakukan serangan ke suatu sistem keamanan dari suatu sistem.

* Exploit

Merupakan salah satu metude/cara untuk menerobos suatu sistem keamanan dari suatu sistem IT dengan memanfaatkan celah yang ada.

* A Zero Day

Zero day merupakan ancaman komputer yang mencoba untuk melakukan exploit pada celah keamanan suatu aplikasi pada saat umur aplikasi tersebut terbilang sangat muda <1 hari. Celah yang diterobos biasanya belum banyak diketahui oleh orang lain ataupun celah yang coba untuk disembunyikan oleh developer aplikasinya

* Security

Merupakan keadaan dimana informasi dan infrasktruktur memiliki kemungkinan lebih kecil untuk mengalami pencurian, sabotase maupun gangguan

* Threat

Merupakan suatu aksi atau kejadian yang mungkin dapat mengancam keamanan sistem. Threat merupakan awal dari banyak pelanggaran terhadap keamanan yang ada

* Vulnerability

Istilah vulnerability merupakan istilah untuk mendifinisikan adanya celah, kelemahan, kesalahan desain atau implementasi yang dapat mengarahkan suatu sistem ke kejadian yang tidak terduga dan tidak diinginkan terkait dengan sistem keamanan dari suatu sistem itu sendiri.

* Daisy Chaining

Daisy chaining adalah sebutan untuk hacker yang berhasil kabur setelah melakukan aksinya, yaitu melakukan peretasan database dan mencuri data yang ada, lalu menghapus semua jejak yang telah ia tinggalkan dengan menghapus log dan jejak yang lainnya

**3 Elemen Penting dalam Keamanan Informasi/Data**

* Confidentiality (Kerahasiaan)

Confidentiality merupakan jaminan yang menjamin bahwa suatu data/informasi yang ada hanyalah dapat diakses oleh seorangan yang berwenang dan memiliki hak untuk mengaksesnya. Kejadian penerobosan celah keamanan di bagian ini banyak disebabkan karena adanya data handling yang buruk atau memang ada upaya peretasan dari hacker

* Integrity (Integritas)

Integirty merupakan tingkat seberapa data tersebut dapat dipercaya dalam kaitannya dengan kemungkinan adanya kesalahan data yang dapat mengakibatkan adanya perubahan wewenang yang buruk, misalnya data otorisasai admin dapat diganti dengan mudah oleh pegawai, dan lain lain.

Integrity merupakan jaminan dimana sebuah data atau informasi dapat diandalkan agar tepat dan akurat sesuai dengan tujuan adanya data tersebut

* Availability (ketersediaan)

Ketersediaan atau availability merupakan jaminan dimana sistem bertanggung jawab dalam menyimpan, memproses dan mengirimkan data dan informasi yang diperlukan oleh user yang berwenang.

**Authenticity (Keaslian) dan Non-Repudiation (Tidak dapata disangkal)**

* Authenticity
  + Authenticity merujuk ke karakteristik komunikasi, dokumen atau data apapun yang dapat memastikan sesuatu itu asli atau murni dan benar benar original ataupun tidak.
  + Peran utama dari adanya autentifikasi sendiri adalah untuk mengkonfirmasi, benar atau tidaknya **user yang mengklaim bahwa dirinya adalah ‘dirinya’** maksudnya apakah user tersebut merupakan user yang memang diharapkan atau hanya penyusup yang sedang melakukan exploit. Selain itu, juga memastikan **setiap pesan yang diterima adalah asli** ataukah sudah dimodifikasi dari bentuk aslinya.
  + **Teknologi Biometric, Smart Card ataupun Digital Certificates** dapat digunakan untuk memastikan keaslian suatu data, transaksi, komunikasi atau dokumen.
* Non repudiation
  + Hal ini merujuk ke kemampuan untuk memastikan suatu komunikasi yang terjalin benar benar tidak bisa disangkal authenticitynya.
  + No
  + Non repudiation merupakan salah satu cara untuk dapat menjamin bahwa pengirim pesan tersebut dapat menyangkal bahwa dirinya “adalah yang mengirimkan pesan itu” dan penerima pun juga tidak dapat menyangkal bahwa fakta “si pengirim telah menerima pesan tersebut”.
  + **Digital signature** dan **enkripsi** adalah beberapa cara yang digunakan untuk membangun authenticity dan non-repudiation dari sebuah dokumen atau pesan.

**Segitiga Keamanan, Fungsionalitas dan Usabilitas**

Terdapat beberapa paradoks dalam kemanan data yang ada, yaitu ada pada gambar di bawah ini :

Maksud dari diagram tersebut adalah :

* Bintang merupakan representasi kecendurungan sifat suatu sistem, apakah lebih fokus ke keamanannya, fungsionalitasnya atau usabilitasnya.
* Melakukan fokus ke poin keamanan, berarti semakin tinggi tingkat keamanannya, namun akan semakin rendah tingkat fungsionalitas dan usabilitasnya.
* Begitupun seterusnya, jika fokus ke fungsionalitas, keamanan dan usabilitas akan berkurang

**Security Challenges**

Ada beberapa tantangan dalam sistem keamanan yang ada saat ini, yaitu :

* Adanya perbedaan atau kontradiksi yang disebabkan oleh hukum dan regulasi yang berlaku dari pemerintah, hal ini seringkali menjadi hambatan atau ancaman tersendiri dalam keamanan suatu informasi. Seringkali metode keamanan suatu data kontradiksi dengan apa yang dituliskan pada hukum dan regulasi pemerintah. Hal ini dapat menghambat atau mengurangi faktor sekuritas data yang ada
* Teknologi lebih fokus berevolusi ke arah kemudahan penggunaan. Seperti yang sudah dipelajari, diagram segitiga mengatakan bahwa jika pengembangan suatu sistem lebih cenderung ke usabilitasnya, maka faktor sekuritas dan fungsionalitasnya akan turun. Hal ini juga yang menjadi tantangan dalam sistem keamanan saat ini.
* Semakin berkembangnya dan bertambahnya jumlah aplikasi berbasis jaringan, hal ini menjadi tantangan karena semakin luas aplikasi tersebut terhubung dengan jaringan, semakin terekspos juga data yang keluar masuk sebuah sistem melalui jaringan. Jaringan yang dimaksud tidak lain adalah Internet yang memiliki sifat openess.
* Semakin meningkatnya kompleksitas dari infrastruktur administrasi dan managemen sebuah komputer. Yang berarti peluang untuk ditemukan celah pada saat melakukan pengembangan akan semakin besar, melihat komplesitasnya yang tinggi cenderung membuat para pengembang melakukan kesalahan saat masa develop.
* Kesulitan dalam memusatkan sistem keamanan dalam lingkungan komputer terdistribusi. Teknologi cloud yang marak beredar akan menjadi tantangan tersendiri dalam sistem keamanan. Semakin luasnya jangkauan komputer terdistribusi memaksa keadaan untuk menemukan cara baru untuk melindungi keamanan datanya
* Dampak yang ditimbulkan atas adanya penerobosan atau serangan yang ditujukan pada asset suatu perusahaan akan sangat besar jika perusahaan tersebut tidak bersiap diri dalam hal sistem keamannya. Tentunya hal ini membuat para pemilik perusahaan untuk melakukan request atau permintaan adanya serangan/exploit terkontrol untuk mengetahui seberapa baik sistem keamanan suatu perusahaan tersebut. Hal ini menjadi sebuah tantangan karena semakin banyak suatu sistem dibobol akan semakin kuat sistem keamannya namun juga akan semakin banyak metode metode penerobosan baru yang ditemukan.