Laporan Pendahuluan Praktikum Keamanan Data

Web Hacking

Dimas Rizky H.P. – 2110141011

World Wide Web ( www ) merupakan bagian dari Internet yang paling populer, sehingga serangan paling banyak terjadi lewat port 80 atau yang dikenal sebagai web hacking, berupa deface situs, SQL injection, serta memanfaatkan kelemahan scripting maupun HTML form. Port 80, Web Server Port ini biasanya digunakan untuk web server.

* Apa itu Web Hacking?

Adapun hacking didefinisikan menjadi Tindakan di luar otoritas atau tindakan mematahkan/membobol mekanisme keamanan sebuah sistem informasi atau sistem jaringan (Http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html). Jadi, singkatnya web hacking dapat diartikan Tindakan menerobos mekanisme keamanan dari suatu sistem yang direpresentasikan dalam world wide web.

* Siapa yang Melakukan Web Hacking?

Menerobos mekanisme keamanan suatu jaringan, bukanlah tindakan yang gampang untuk dilakukan. Jadi, siapakah pelaku web hacking tersebut? Seiring perkembangan internet yang benar-benar pesat dan diiringi perkembangan security dan underground, membuat siapa saja dapat menjadi pelaku. Tidak ada keharusan bahwa pelaku web hacking adalah orang yang pintar komputer dan internet, atau lain sebagainya.

* Mengapa Melakukan Web Hacking?

Ada banyak alasan orang melakukan web hacking, diantaranya adalah:

* + Wanna Be A Hacker ( ingin menjadi seorang hacker ).
  + Mendapatkan popularitas.
  + Ingin mendapat pujian.
* Bagaimana seseorang melakukan web hacking?

Internet sudah hampir menjangkau segala sisi kehidupan yang ada di dunia ini. Informasi mengenai web hacking dapat anda temukan dengan berselancar ke Google. Google, search engine yang terkenal menjawab pertanyaan Bagaimana. Dengan memasukkan kata (keyword) pada baris isian pencarian maka anda akan dibawa ke tempat-tempat yang berhubungan dengan web hacking.

* Jenis serangan yang mungkin terjadi pada web:

1. Pembajakan Password FTP Di pertengahan 2009, maraknya satu bentuk pembajakan password FTP yang disebut juga serangan “gumblar” atau “martuz” , mempatenkan model pencurian ini menjadi salah satu cara yang paling sering digunakan untuk melakukan hacking. Cara kerja gumblar atau martuz adalah memodifikasi hasil pencarian Google sehingga setiap klik pada link yang tampil di hasil pencarian akan diredirectkan ke situs penyedia badware. Serangan ini mengambil keuntungan dari sebuah fakta bahwa ada banyak PC yang miskin perlindungan di dunia. Dan personal komputer tersebut nahasnya adalah milik webmaster yang informasi login websitenya disimpan di personal komputer mereka. Karena itulah, lengkapi personal komputer anda dengan perlindungan antivirus yang memadai untuk pencegahan infeksi gumblar atau martuz di situs anda. Dan jangan sekali-kali membookmark informasi login anda.
2. Serangan Remote File Inclusion (RFI) Sebelum kemunculan gumblar atau martuz, serangan RFI adalah satu bentuk ancaman terbesar. Prinsip kerja serangan RFI adalah menipu sebuah website yang telah berjalan untuk mengcopy kode dari website eksternal. Kode yang dicopy menyusup ke dalam script yang dieksekusi, dan menjadi bagian di dalamnya. Sehingga, setiap script tersebut dieksekusi kembali, sebaris kode tersebut juga ikut dieksekusi. Sebaris kode tersebut fungsinya adalah untuk mendownload badware ke komputer pengakses.
3. Serangan Local File Inclusion (LFI) Serangan LFI hampir sama seperti RFI, bedanya mereka mencoba untuk menipu sebuah halaman web agar menampilkan konten dari file sistem server yang penting, yang seharusnya restricted dan tidak boleh diakses. Indikasi serangan LFI adalah di akses log website anda akan tampil koding seperti ini: Cara menanggulangi serangan LFI adalah dengan melatih kemampuan koding kita dan memperdalam pengetahuan tentang pembatasan .htaccess
4. Serangan Injeksi SQL Pada dasarnya serangan ini sama dengan RFI dan LFI, bedanya obyek yang diserang adalah halaman web yang menggunakan Structured Query Language (SQL) untuk melakukan query dan memanipulasi database, semisal MySQL. Cara kerjanya adalah dengan menanamkan komando SQL di sebaris koding untuk menipu sistem agar membocorkan informasi rahasia. Berikut salah satu contoh dari serangan injeksi SQL yang nantinya akan muncul pada akses log website anda
5. Password Attack Di samping gumblar, ada cara lain bagi penyerang untuk mencuri password situs anda. Yaitu dengan berulang-ulang mencoba untuk login dengan kombinasi user ID dan password yang berbeda, berharap untuk menebak manakah yang benar.