APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

EMPAT DOMAIN KERAWANAN SISTEM II

Versi

2013/1.0

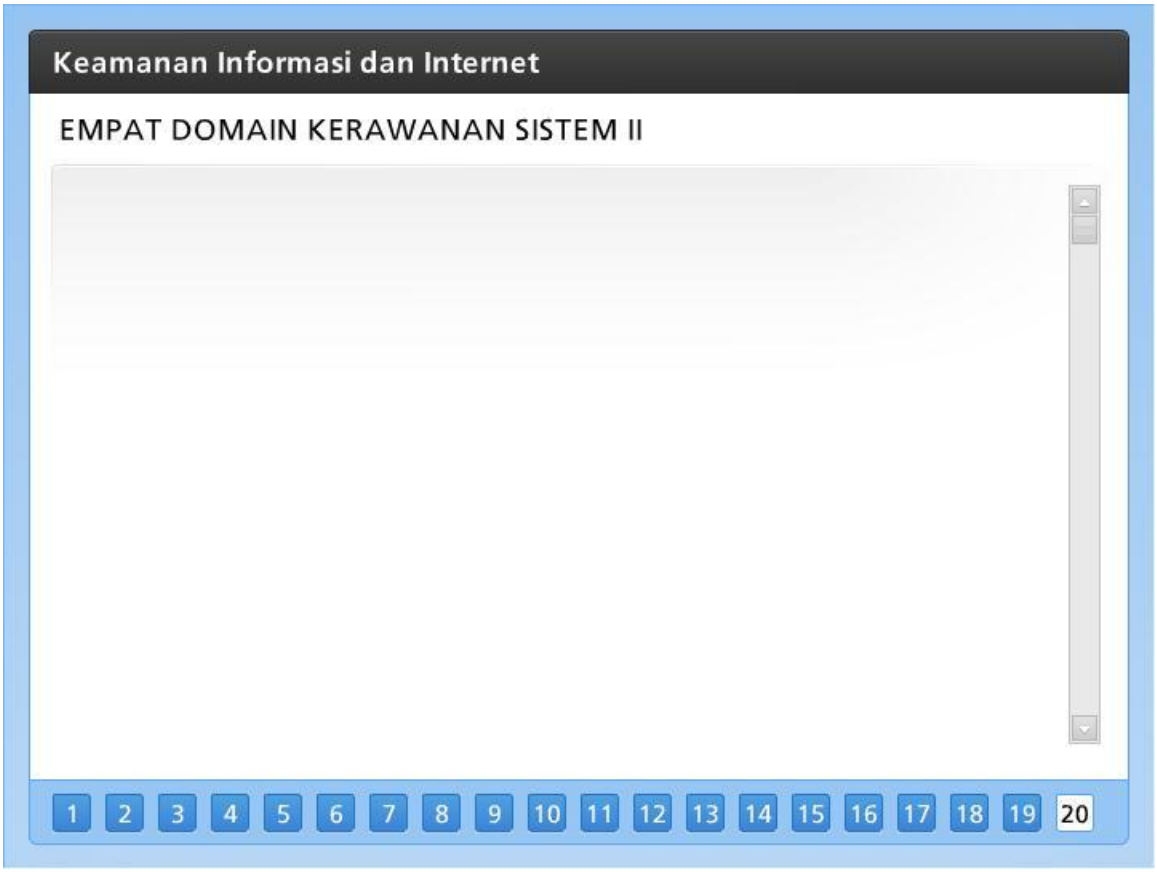
Nama File

MKIDI-5A-EmpatDomain2.pdf

Referensi Pembelajaran

5-A

EMPAT DOMAIN KERAWANAN SISTEM II



Dewasa ini terdapat banyak sekali tipe dan jenis serangan yang terjadi di dunia maya. Sesuai dengan sifat dan karakteristiknya, semakin lama model serangan yang ada semakin kompleks dan sulit dideteksi maupun dicegah. Berikut adalah berbagai jenis model serangan yang kerap terjadi menerpa dunia maya, terutama yang dikenal luas di tanah air.

Malicious Software

Malware merupakan program yang dirancang untuk disusupkan ke dalam sebuah sistem (baca: target penyerangan) dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemilikinya. Merugikan dalam arti kata dampak negatif yang ditimbulkan dapat berkisar mulai dari sekedar memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem dimaksud. Ada tiga jenis malware klasik yang paling banyak ditemui, yaitu: Virus, Worm, dan Trojan Horse.

Virus

Sejak kemunculannya pertama kali pada pertengahan tahun 1980-an, virus komputer telah mengundang berbagai kontroversi akibat aksinya yang beraneka ragam. Seiring dengan

perkembangan teknologi komputer, virus menemukan berbagai cara-cara baru untuk menyebarkan dirinya melalui berbagai modus operandi. Pada dasarnya, virus merupakan program komputer yang bersifat "malicious" (memiliki tujuan merugikan maupun bersifat mengganggu pengguna sistem) yang dapat menginfeksi satu atau lebih sistem komputer melalui berbagai cara penularan yang dipicu oleh otorasisasi atau keterlibatan "user" sebagai pengguna komputer. Fenomena yang mulai ditemukan pada awal tahun 1980-an ini memiliki beribu-ribu macam atau jenis sejalan dengan perkembangan teknologi komputer dewasa ini - terutama setelah dikembangkannya teknologi jaringan dan internet. Jenis kerusakan yang ditimbulkan virus pun menjadi bermacam-macam. Mulai dari yang sekedar mengganggu seperti menampilkan gambar-gambar yang tidak sepantasnya, hingga sampai yang bersifat mendatangkan kerugian ekonomis seperti memformat hard disk atau bahkan merusak file-file sistem operasi sehingga mengganggu komputer yang bersangkutan. Ditinjau dari cara kerjanya, virus dapat dikelompokkan menjadi:

a. *Overwriting Virus* - merupakan penggalan program yang dibuat sedemikian rupa untuk menggantikan program utama (baca: host) dari sebuah program besar sehingga menjalankan perintah yang tidak semestinya;

b. *Prepending Virus* - merupakan tambahan program yang disisipkan pada bagian awal dari program utama atau "host" sehingga pada saat dieksekusi, program virus akan dijalankan terlebih (bereplikasi) dahulu sebelum program yang sebenarnya;

c. *Appending Virus* - merupakan program tambahan yang disisipkan pada bagian akhir dari program host sehingga akan dijalankan setelah program sebenarnya tereksekusi;

d. *File Infector Virus* - merupakan penggalan program yang mampu memiliki kemampuan untuk melekatkan diri (baca: attached) pada sebuah file lain, yang biasanya merupakan file "executable", sehingga sistem yang menjalankan file tersebut akan langsung terinfeksi;

e. *Boot Sector Virus* - merupakan program yang bekerja memodifikasi program yang berada di dalam boot sector pada cakram penyimpan (baca: disc) atau disket yang telah diformat. Pada umumnya, sebuah boot sector virus akan terlebih dahulu mengeksekusi dirinya sendiri sebelum proses "boot-up" pada komputer terjadi, sehingga seluruh "floppy disk" yang digunakan pada komputer tersebut akan terjangkiti pula (perhatikan bahwa dewasa ini, modus operandi sejenis terjadi dengan memanfaatkan media penyimpan USB);

f. *Multipartite Virus* - merupakan kombinasi dari Infector Virus dan Boot Sector Virus dalam arti kata ketika sebuah file yang terinfeksi oleh virus jenis ini dieksekusi, maka virus akan

menjangkiti boot sector dari hard disk atau partition sector dari komputer tersebut, dan sebaliknya; dan

g. *Macro Virus* - menjangkiti program "macro" dari sebuah file data atau dokumen (yang biasanya digunakan untuk "global setting" seperti pada template Microsoft Word) sehingga dokumen berikutnya yang diedit oleh program aplikasi tersebut akan terinfeksi pula oleh penggalan program macro yang telah terinfeksi sebelumnya.

Perlu diperhatikan bahwa virus hanya akan aktif menjangkiti atau menginfeksi sistem komputer lain apabila ada campur tangan manusia atau "user" sebagai pengguna. Campur tangan yang dimaksud misalnya dilakukan melalui: penekanan tombol pada keyboard, penekanan tombol pada mouse, "pemasukan" USB pada komputer, pengiriman file via email, dan lain sebagainya.

Worms

Istilah "worms" yang tepatnya diperkenalkan kurang lebih setahun setelah "virus" merupakan program malicious yang dirancang terutama untuk menginfeksi komputer-komputer yang berada dalam sebuah sistem jaringan. Walaupun sama-sama sebagai sebuah penggalan program, perbedaan prinsip yang membedakan worms dengan pendahulunya virus yaitu yang bersangkutan tidak memerlukan campur tangan manusia atau pengguna dalam melakukan penularan atau penyebarannya. Worms merupakan program yang dibangun dengan algoritma tertentu sehingga yang bersangkutan mampu untuk mereplikasikan dirinya sendiri pada sebuah jaringan komputer tanpa melalui intervensi atau bantuan maupun keterlibatan pengguna. Pada mulanya worms diciptakan dengan tujuan tunggal yaitu untuk mematikan sebuah sistem atau jaringan komputer. Namun belakangan ini telah tercipta worms yang mampu menimbulkan kerusakan luar biasa pada sebuah sistem maupun jaringan komputer, seperti merusak file-file penting dalam sistem operasi, menghapus data pada hard disk, memacetkan aktivitas komputer (baca: hang), dan hal-hal destruktif lainnya.

Karena karakteristiknya yang tidak melibatkan manusia, maka jika sudah menyebar sangat sulit untuk mengontrol atau mengendalikannya. Usaha penanganan yang salah justru akan membuat pergerakan worms menjadi semakin liar tak terkendali dan "mewabah". Untuk itulah dipergunakan penanganan khusus dalam menghadapinya.

Trojan Horse

Istilah "Trojan Horse" atau Kuda Troya diambil dari sebuah taktik perang yang digunakan untuk merebut kota Troy yang dikelilingi benteng nan kuat. Pihak penyerang membuat sebuah patung kuda raksasa yang di dalamnya memuat beberapa prajurit yang nantinya ketika sudah berada di dalam wilayah benteng akan keluar untuk melakukan penyerangan dari dalam. Adapun bentuk kuda dipilih sebagaimana layaknya sebuah hasil karya seni bagi sang Raja agar dapat dengan leluasa masuk ke dalam benteng yang dimaksud.

Ide ini mengilhami sejumlah hacker dan cracker dalam membuat virus atau worms yang cara kerjanya mirip dengan fenomena taktik perang ini, mengingat pada waktu itu bermuncukan Anti Virus Software yang dapat mendeteksi virus maupun worms dengan mudah untuk kemudian dilenyapkan. Dengan menggunakan prinsip ini, maka penggalan program malicious yang ada dimasukkan ke dalam sistem melalui sebuah program atau aktivitas yang legal - seperti: melalui proses instalasi perangkat lunak aplikasi, melalui proses "upgrading" versi software yang baru, melalui proses "download" program-program freeware, melalui file-file multimedia (seperti gambar, lagu, dan video), dan lain sebagainya.

Berdasarkan teknik dan metode yang digunakan, terdapat beberapa jenis Trojan Horse, antara lain:

- *Remote Access Trojan* - kerugian yang ditimbulkan adalah komputerkorban serangan dapat diakses secara remote;
- *Password Sending Trojan* - kerugian yang ditimbulkan adalah password yang diketik oleh komputer korban akan dikirimkan melalui email tanpa sepengetahuan dari korban serangan;
- *Keylogger* - kerugian yang ditimbulkan adalah ketikan atau input melalui keyboard akan dicatat dan dikirimkan via email kepada hacker yang memasang keylogger;
- *Destructive Trojan* - kerugian yang ditimbulkan adalah file-file yang terhapus atau hard disk yang terformat;
- *FTP Trojan* - kerugian yang terjadi adalah dibukanya port 21 dalam sistem komputer tempat dilakukannya download dan upload file;
- *Software Detection Killer* - kerugiannya dapat program-program keamanan seperti zone alarm, anti-virus, dan aplikasi keamanan lainnya; dan

- *Proxy Trojan* - kerugian yang ditimbulkan adalah di-"settingnya" komputer korban menjadi "proxy server" agar digunakan untuk melakukan "anonymous telnet", sehingga dimungkinkan dilakukan aktivitas belanja online dengan kartu kredit curian dimana yang terlacak nantinya adalah komputer korban, bukan komputer pelaku kejahatan.

Web Defacement

Serangan dengan tujuan utama merubah tampilah sebuah website - baik halaman utama maupun halaman lain terkait dengannya - diistilahkan sebagai "Web Defacement". Hal ini biasa dilakukan oleh para "attacker" atau penyerang karena merasa tidak puas atau tidak suka kepada individu, kelompok, atau entitas tertentu sehingga website yang terkait dengannya menjadi sasaran utama. Pada dasarnya deface dapat dibagi menjadi dua jenis berdasarkan dampak pada halaman situs yang terkena serangan terkait.

Jenis pertama adalah suatu serangan dimana penyerang merubah (baca: men-deface) satu halaman penuh tampilan depan alias file index atau file lainnya yang akan diubah secara utuh.Artinya untuk melakukan hal tersebut biasanya seorang 'defacer' harus berhubungan secara 'langsung' dengan mesin komputer terkait. Hal ini hanya dapat dilakukan apabila yang bersangkutan sanggup mendapatkan hak akses penuh (baca: priviledge) terhadap mesin, baik itu "root account"atau sebagainya yang memungkinkan defacer dapat secara interaktif mengendalikan seluruh direktori terkait. Hal ini umumnya dimungkinkan terjadi dengan memanfaatkan kelemahan pada sejumlah "services" yang berjalan di sistem komputer.

Jenis kedua adalah suatu serangan dimana penyerang hanya merubah sebagian atau hanya menambahi halaman yang di-deface.Artinyayang bersangkutan men-deface suatu situs tidak secara penuh, bisa hanya dengan menampilkan beberapa kata, gambar atau penambahan "script" yang mengganggu.Dampaknya biasanya adalah menghasilkan tampilan yang kacau atau mengganggu.Hal ini dapat dilakukan melaluipenemuan celah kerawanan padamodel scripting yang digunakan, misalnya dengan *XSS injection*, *SQL* atau *database injection,*atau memanfaatkan sistem aplikasi manajemen website yang lemah (baca: CMS = Content Management System).

Denial of Services (DoS)

Serangan yang dikenal dengan istilah DoS dan DDoS (Distributed Denial of Services) ini pada dasarnya merupakan suatu aktivitas dengan tujuan utama menghentikan atau meniadakan layanan

(baca: services) sistem atau jaringan komputer - sehingga sang pengguna tidak dapat menikmati fungsionalitas dari layanan tersebut - dengan cara mengganggu ketersediaan komponen sumber daya yang terkait dengannya. Contohnya adalah dengan cara memutus koneksi antar dua sistem, membanjiri kanal akses dengan jutaan paket, menghabiskan memori dengan cara melakukan aktivitas yang tidak perlu, dan lain sebagainya.

Dengan kata lain, DOS dan/atau DDoS merupakan serangan untuk melumpuhkan sebuah layanan dengan cara menghabiskan sumber daya yang diperlukan sistem komputer untuk melakukan kegiatan normalnya. Adapun sumber daya yang biasa diserang misalnya: kanal komunikasi (baca: bandwidth), kernel tables, swap space, RAM, cache memories, dan lain sebagainya. Berikut adalah sejumlah contoh tipe serangan DoS/DDoS:

1. *SYN-Flooding*: merupakan serangan yang memanfaatkan lubang kerawanan pada saat koneksi TCP/IP terbentuk.
2. *Pentium 'FOOF' Bug*: merupakan serangan terhadap prosessor yang menyebabkan sistem senantiasa melakukan “re-booting”. Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan.
3. *Ping Flooding*: merupakan aktivitas “brute force” sederhana, dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, sehingga mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (network). Hal ini terjadi karena mesin korban dibanjiri (baca: flood) oleh peket-paket ICMP.

Yang membedakan antara DDoS dengan DoS adalah pada DDoS serangan dilakukan serempak oleh beberapa komputer sekaligus, sehingga hal ini sangat ampuh dalam membuat sistem atau jaringan komputer tertentu lumpuh dalam waktu cepat.

Botnet

Salah satu jenis serangan yang paling banyak dibicarakan belakangan ini dan menjadi trend di negara-negara maju adalah “botnet” yang merupakan singkatan dari “Robot Network”. Pada dasarnya aktivitas botnet dipicu dari disusupkannya program-program kecil - bersifat seperti virus, worms, maupun trojan horse - ke dalam berbagai sistem komputer server yang ada dalam jejaring internet tanpa sepengatahuan pemiliknya. Program malicious yang disusupkan dan ditanamkan pada server ini pada mulanya bersifat pasif, alias tidak melakukan kegiatan apa-apa yang mengganggu.

Karena karakteristik inilah makanya sering dinamakan sebagai “zombies”. Yang menarik adalah bahwa pada saatnya nanti, si penyerang yang diistilahkan sebagai “Master Refer” secara “remote” akan mengendalikan keseluruhan zombies yang berada di bawah “kekuasannya” untuk melakukan penyerangan secara serentak dan simultan ke suatu target tertentu. Pada saat inilah maka seluruh zombies yang jumlahnya dapat mencapai puluhan ribu bahkan jutaan tersebut langsung bersifat aktif melakukan kegiatan sesuai yang diinginkan oleh “master”-nya.

Dengan melakukan aktivasi terhadap zombies ini maka serangan botnet dapat dilakukan secara serempak dengan beragam skenario yang memungkinkan, seperti: melakukan DDoS secara masif, mematikan sistem komputer secara simultan, menularkan virus dan worms secara serentak, menginfeksi puluhan ribu server dengan trojan horse dalam waktu singkat, dan lain sebagainya.

Tingkat kesulitan untuk menangani botnet dikenal sangat tinggi dan kompleks, karena karakteristiknya yang mendunia membuat koordinasi multi-lateral harus dilakukan secara intensif dan sesering mungkin. Disamping itu tidak mudah untuk mendeteksi adanya beraneka ragam jenis zombies yang dalam keadaan non aktif atau “tidur” tersebut; apalagi mencoba untuk mengalokasikan dimana posisi sang Master Refer sebagai dalang pengendali serangan botnet terkait.

Phishing

Phishing merupakan sebuah proses “pra-serangan” atau kerap dikatakan sebagai “soft attack” dimana sang penyerang berusaha mendapatkan informasi rahasia dari target dengan cara menyamar menjadi pihak yang dapat dipercaya - atau seolah-olah merupakan pihak yang sesungguhnya. Contohnya adalah sebuah email yang berisi suatu informasi yang mengatakan bahwa sang pengirim adalah dari Divisi Teknologi Informasi yang sedang melakukan “upgrading” sistem; dimana untuk memperlancar tugasnya, sang penerima email diminta untuk segera mengirimkan kata kunci “password” dari “user name” yang dimilikinya. Atau situs sebuah bank palsu yang memiliki tampilan sama persis dengan situs aslinya namun memiliki alamat URL yang mirip-mirip, sehingga diharapkan sang nasabah akan khilaf dan secara tidak sadar memasukkan kata kunci rahasianya untuk mengakses rekening yang dimaksud.

Serangan “phishing” ini kerap dikategorikan sebagai sebuah usaha “social engineering”, yaitu memanfaatkan pendekatan sosial dalam usahanya untuk mendapatkan informasi rahasia sebagai

alat untuk melakukan penyerangan di kemudian hari. Modus operandi yang paling banyak ditemui saat ini adalah usaha phishing melalui SMS pada telepon genggam, dimana sudah banyak korban yang harus kehilangan uangnya karena diminta untuk melakukan transfer ke rekening tertentu dengan berbagai alasan yang seolah-olah masuk akal sehingga berhasil menjebak sang korban.

SQL Injection

Pada dasarnya SQL Injection merupakan cara mengeksploitasi celah keamanan yang muncul pada level atau "layer" database dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat penyerang memasukkan nilai "string" dan karakter-karakter contoh lainnya yang ada dalam instruksi SQL; dimana perintah tersebut hanya diketahui oleh sejumlah kecil individu (baca: hacker maupun cracker) yang berusaha untuk mengeksploitasinya. Karena tipe data yang dimasukkan tidak sama dengan yang seharusnya (sesuai dengan kehendak program), maka terjadi sebuah aktivitas "liar" yang tidak terduga sebelumnya - dimana biasanya dapat mengakibatkan mereka yang tidak berhak masuk ke dalam sistem yang telah terproteksi menjadi memiliki hak akses dengan mudahnya. Dikatakan sebagai sebuah "injeksi" karena aktivitas penyerangan dilakukan dengan cara "memasukkan" string (kumpulan karakter) khusus untuk melewati filter logika hak akses pada website atau sistem komputer yang dimaksud.

Contoh-contoh celah kerawanan yang kerap menjadi korban SQL Injection adalah:

- Karakter-karakter kendali, kontrol, atau filter tidak didefinisikan dengan baik dan benar (baca: Incorrectly Filtered Escape Characters);
- Tipe pemilihan dan penanganan variabel maupun parameter program yang keliru (baca: Incorrect Type Handling);
- Celah keamanan berada dalam server basis datanya (baca: Vulnerabilities Inside the Database Server);
- Dilakukan mekanisme penyamaran SQL Injection (baca: Blind SQL Injection); dan lain sebagainya.

Cross-Site Scripting

Cross Site Scripting (CSS) adalah suatu serangan dengan menggunakan mekanisme "injection" pada aplikasi web dengan memanfaatkan metode HTTP GET atau HTTP POST. Cross Site Scripting biasa

digunakan oleh pihak-pihak yang berniat tidak baik dalam upaya mengacaukan konten website dengan memasukkan naskah program (biasanya java script) sebagai bagian dari teks masukan melalui formulir yang tersedia.

Apabila tidak diwaspadai, script ini dapat begitu saja dimasukkan sebagai bagian dari teks yang dikirim ke web setiap pengunjung, misalnya melalui teks masukan buku tamu atau forum diskusi yang tersedia bagi semua pengunjung website. Script yang menyisip di teks yang tampil ini dapat memberi efek dramatis pada tampilan website mulai dari menyisipkan gambar tidak senonoh sampai mengarahkan tampilan ke website lain.

CSS memanfaatkan lubang kelemahan keamanan yang terjadi pada penggunaan teknologi "dynamic page". Serangan jenis ini dapat diakibatkan oleh kelemahan yang terjadi akibat ketidakmampuan server dalam memvalidasi input yang diberikan oleh pengguna - misalnya algoritma yang digunakan untuk pembuatan halaman yang diinginkan tidak mampu melakukan penyaringan terhadap masukkan tersebut. Hal ini memungkinkan halaman yang dihasilkan menyertakan perintah yang sebenarnya tidak diperbolehkan.

Serangan CSS ini populer dilakukan oleh berbagai kalangan. Namun sayangnya, banyak penyedia layanan yang tidak mengakui kelemahan tersebut dan mau melakukan perubahan pada sistem yang mereka gunakan. Citra penyedia layanan merupakan harga yang dipertaruhkan ketika mereka mengakui kelemahan tersebut. Sayangnya dengan tindakan ini konsumen atau pengguna menjadi pihak yang dirugikan.

Dari sisi kerapuhan dan keamanan, CSS dapat bekerja bak penipu dengan kedok yang mampu mengelabui orang yang tidak waspada. Elemen penting dari keberhasilan CSS adalah "social engineering" yang efektif dari sisi penipu. CSS memampukan seseorang yang tidak bertanggungjawab melakukan penyalahgunaan informasi penting.

Sebelum sampai pada proses penyalahgunaan tersebut, penyerang biasanya mengambil langkah-langkah awal terlebih dahulu dengan mengikuti pola tertentu. Langkah pertama, penyerang melakukakan pengamatan untuk mencari web-web yang memiliki kelemahan yang dapat

dieksploitasi dengan CSS. Langkah kedua, sang penyerang mencari tahu apakah web tersebut menerbitkan informasi yang dapat digunakan untuk melakukan pencurian infomasi lebih lanjut. Informasi tersebut biasanya berupa "cookie". Langkah kedua ini tidak selalu dijalankan. Langkah ketiga, sang penyerang membujuk korban untuk mengikuti sebuah link yang mengandung kode, ditujukan untuk mendapatkan informasi yang telah disebutkan sebelumnya. Kemampuan melakukan "social engineering" dari sang penyerang diuji disini. Setelah mendapatkan informasi tersebut, sang penyerang melakukan langkah terakhir, pencurian maupun pengubahan informasi vital.

Pada kenyataannya, masih banyak sekali ditemukan jenis-jenis serangan seperti yang dikemukakan di atas, seperti: *Land Attack*, *Man-in-the-Middle Attack*, *Packet Spoofing*, *Password Cracking*, *Sessions Hijacking*, dan lain sebagainya. Pada intinya keseluruhan jenis serangan itu bervariasi berdasarkan tipe-tipe kerawanan atau "vulnerabilities" yang terdapat pada sistem terkait yang kurang dijaga keamanannya.