APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

## Mata Ajar

***MANAJEMEN KEAMANAN INFORMASI DAN INTERNET***

## Topik Bahasan

***STRATEGI DAN CARA HACKER DALAM MENYERANG KEAMANAN INTERNET***

## Versi

***2013/1.0***

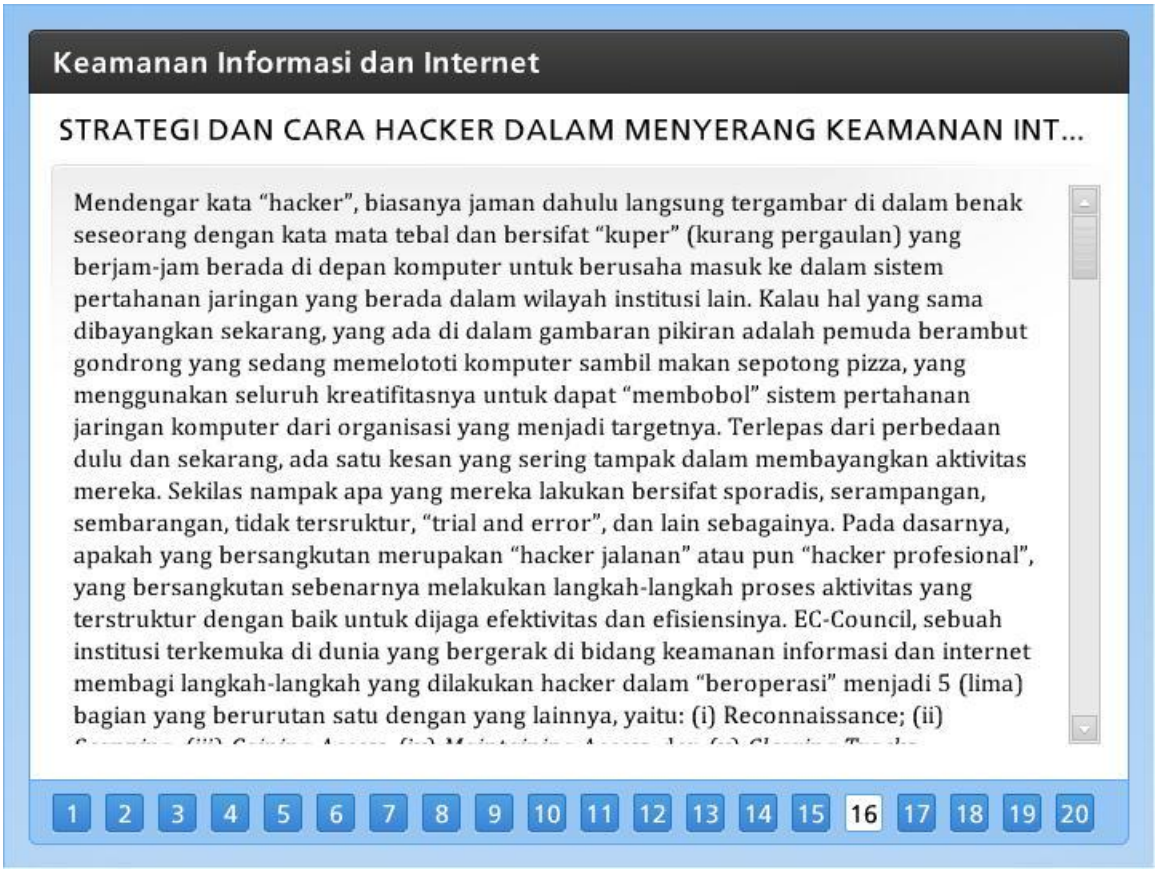
## Nama File

***MKIDI-3A-StrategiDan.pdf***

## Referensi Pembelajaran

***3-A***

# STRATEGI DAN CARA HACKER DALAM MENYERANG KEAMANAN INTERNET




Mendengar kata "hacker", biasanya jaman dahulu langsung tergambar di dalam benak seseorang dengan kata mata tebal dan bersifat "kuper" (kurang pergaulan) yang berjam-jam berada di depan komputer untuk berusaha masuk ke dalam sistem pertahanan jaringan yang berada dalam wilayah institusi lain. Kalau hal yang sama dibayangkan sekarang, yang ada di dalam gambaran pikiran adalah pemuda berambut gondrong yang sedang memelototi komputer sambil makan sepotong pizza, yang menggunakan seluruh kreatifitasnya untuk dapat "membobol" sistem pertahanan jaringan komputer dari organisasi yang menjadi targetnya. Terlepas dari perbedaan dulu dan sekarang, ada satu kesan yang sering tampak dalam membayangkan aktivitas mereka. Sekilas nampak apa yang mereka lakukan bersifat sporadis, serampangan, sembarangan, tidak tersruktur, "trial and error", dan lain sebagainya. Pada dasarnya, apakah yang bersangkutan merupakan "hacker jalanan" atau pun "hacker profesional", yang bersangkutan sebenarnya melakukan langkah-langkah proses aktivitas yang terstruktur dengan baik untuk dijaga efektivitas dan efisiensinya. EC-Council, sebuah institusi terkemuka di dunia yang bergerak di bidang keamanan informasi dan internet membagi langkah-langkah yang dilakukan hacker dalam "beroperasi" menjadi 5 (lima) bagian yang berurutan satu

dengan yang lainnya, yaitu: (i) Reconnaissance; (ii) *Scanning*; (iii) *Gaining Access*; (iv) *Maintaining Access*; dan (v) *Clearing Tracks*.

Mendengar kata "hacker", biasanya jaman dahulu langsung tergambar di dalam benak seseorang dengan kata mata tebal dan bersifat "kuper" (kurang pergaulan) yang berjam-jam berada di depan komputer untuk berusaha masuk ke dalam sistem pertahanan jaringan yang berada dalam wilayah institusi lain. Kalau hal yang sama dibayangkan sekarang, yang ada di dalam gambaran pikiran adalah pemuda berambut gondrong yang sedang memelototi komputer sambil makan sepotong pizza, yang menggunakan seluruh kreatifitasnya untuk dapat "membobol" sistem pertahanan jaringan komputer dari organisasi yang menjadi targetnya. Terlepas dari perbedaan dulu dan sekarang, ada satu kesan yang sering tampak dalam membayangkan aktivitas mereka. Sekilas nampak apa yang mereka lakukan bersifat sporadis, serampangan, sembarangan, tidak tersruktur, "trial and error", dan lain sebagainya. Pada dasarnya, apakah yang bersangkutan merupakan "hacker jalanan" atau pun "hacker profesional", yang bersangkutan sebenarnya melakukan langkah-langkah proses aktivitas yang terstruktur dengan baik untuk dijaga efektivitas dan efisiensinya. EC-Council, sebuah institusi terkemuka di dunia yang bergerak di bidang keamanan informasi dan internet membagi langkah-langkah yang dilakukan hacker dalam "beroperasi" menjadi 5 (lima) bagian yang berurutan satu dengan yang lainnya, yaitu: (i) Reconnaissance; (ii) *Scanning*; (iii) *Gaining Access*; (iv) *Maintaining Access*; dan (v) *Clearing Tracks*.

## *Reconnaissance*

Yang dimaksud dengan "reconnaissance" adalah suatu tahap persiapan dimana hacker atau pihak yang akan melakukan "serangan" berusaha mencari informasi sebanyak-banyaknya mengenai target atau sasaran sistem yang ingin diserang sebelum rangkaian proses penyerangan dilaksanakan. Ada dua jenis model *reconnaissance* yang dikenal, yaitu yang bersifat pasif dan aktif. Usaha terkait dikatakan aktif apabila tidak ada interaksi langsung antara pihak penyerang dengan target atau sasaran yang ingin diserang. Katakanlah seorang hacker yang ingin menyerang sebuah bank, maka yang bersangkutan akan melakukan studi pustaka atau mempelajari lewat *browsing* internet mengenai seluk beluk sistem yang ingin diserang. Dengan mendapatkan referensi dari berbagai sumber seperti artikel, majalah, koran, *vendor release*, dan lain sebagainya - tidak jarang yang bersangkutan dapat mengetahui jenis sistem komputer yang dipergunakan oleh bank terkait, lengkap dengan tipe sistem operasi dan topologi jaringannya. Sementara proses terkait dikatakan aktif, jika dilakukan aktivitas interaksi secara langsung dengan sistem atau pemangku kepentingan pada bank terkait. Misalnya sang hacker berpura-pura ingin membuka rekening bank sehingga dapat mempelajari sistem komputer yang dioperasikan oleh *customer service*, atau menelepon ke *help*

*desk* bank yang bersangkutan untuk melihat mekanisme dan prosedur yang dipergunakan dalam menjawab kebutuhan pelanggan, atau dengan cara mengunjungi situs *internet bank* terkait untuk melihat dan menduga-duga teknologi yang berada di belakang aplikasi tersebut, dan lain sebagainya.

## Scanning

Setelah mengetahui seluk beluk sekilas mengenai lingkungan dan karakteristik dari target sistem yang ingin diserang, barulah tahap berikutnya adalah melakukan "scanning". Sesuai dengan definisi dan konteksnya, "scan" merupakan sebuah proses dimana hacker dengan menggunakan berbagai alat dan *tools* berusaha mencari celah masuk atau lokasi tempat serangan akan diluncurkan. Seperti halnya seorang pencuri yang dapat masuk ke dalam rumah melalui pintu, jendela, atap rumah, atau gorong-gorong bawah tanah, seorang hacker melalui aktivitas ini berusaha mencari lubang-lubang kerawanan tempat serangan masuk. Biasanya, yang akan di-*scan* pertama kali adalah *port* dalam sistem komputer *(port scanning)*, atau melalui pemetaan jaringan *(network mapping)*, atau melalui pencarian kerawanan/kerapuhan *(vulnerability scanning)*, dan lain sebagainya. Hal yang perlu baik-baik diperhatikan adalah bahwa perbuatan "scanning" terhadap sistem jaringan komputer milik orang lain pada dasarnya merupakan aktivitas yang melanggar undang-undang, kecuali seijin pihak yang berkepentingan. Dan jika tidak hati-hati, maka pihak terkait akan dengan mudah mengetahui kegiatan ini, terlebih-lebih jika yang bersangkutan memiliki perangkat IDS*(Intrusion Detection System)* yang dapat mendeteksi seandainya terjadi penyusupan atau *intrusion* dari pihak luar ke dalam sistem yang dilindungi. Hasil dari tahap *scanning* adalah diketemukannya cara bagi hacker untuk masuk ke dalam sistem.

## Gaining Access

Jika dua tahap sebelumnya yaitu *reconnaissance*dan *scanning* masih bersifat "pasif", dalam arti kata bahwa aktivitas yang dilakukan masih sekedar meraba-raba kehandalan sistem yang ingin diserang, pada tahap *gaining access* ini usaha penetrasi aktif mulai dilaksanakan. Pada dasarnya yang dilakukan oleh hacker adalah melakukan eksploitasi terhadap kelemahan, kerawanan, dan/atau kerapuhan (baca: *vulberability*) yang ada pada sistem. Cara mendapatkan akses yang dimaksud sangatlah beraneka-ragam, tergantung karakteristik dan hasil dari proses *scanning* sebelumnya. Misalnya adalah dengan melakukan *password cracking* alias mencoba menebak hingga "memaksakan" kata kunci rahasia yang memungkinkan hacker memperoleh hak akses untuk masuk ke dalam sistem. Jenis lainnya adalah mekakukan aktivitas yang menyebabkan terjadinya fenomena *buffer overflows* sehingga data rahasia yang seharusnya tersimpan aman dapat diakses dan diambil oleh yang tidak memiliki otoritas. Pendekatan *gaining access* lainnya adalah dengan melakukan apa

yang dinamakan sebagai *session hijacking* alias melakukan pembajakan hak akses seseorang oleh hacker sehingga yang bersangkutan dapat masuk ke dalam sistem yang bukan merupakan teritorinya. Proses memperoleh hak akses ini dapat berlangsung dalam waktu yang cukup singkat hingga memakan waktu yang relatif panjang, tergantung dari sejumlah faktor, seperti: arsitektur dan konfigurasi jaringan, jenis sistem operasi yang dipergunakan, keahlian hacker yang bersangkutan, jenis *tool* atau alat bantu yang dipergunakan, dan lain sebagainya. Jika hacker telah berhasil masuk ke tahap ini, maka ekspose resiko yang dihadapi organisasi atau institusi yang memiliki sistem terkait sudah sedemikian tingginya. Gagal mendeteksi percobaan ini akan mendatangkan malapetaka yang cukup besar bagi yang bersangkutan.

## Maintaining Access

Tahap ini adalah sebuah periode dimana setelah hacker berhasil masuk ke dalam sistem, yang bersangkutan berusaha untuk tetap bertahan memperoleh hak akses tersebut. Pada saat inilah sering diistilahkan bahwa sistem yang ada telah berhasil diambil alih oleh pihak yang tidak berhak (baca: *compromised*). Ketika periode ini berlangsung, kendali sepenuhnya berada di tangan hacker. Yang bersangkutan dapat melakukan apa saja yang diinginkannya, seperti melakukan hal-hal yang tidak berbahaya - seperti menuliskan pesan peringatan kepada pemilik sistem - hingga melakukan tindakan yang destruktif, seperti mencuri data, merubah konten, menanam aplikasi mata-mata, mengacaukan konfigurasi, memanipulasi informasi, merusak isi *hard disk*, dan lain sebagainya. Tidak banyak yang dapat dilakukan oleh pemilik sistem jika hacker telah memasuki tahap ini, kecuali berusaha melakukan *counter measures* agar dampak atau akibat negatif yang ditimbulkan hacker dapat ditekan seminimal mungkin.

### *Covering Tracks*

Akhirnya tahap akhir yang dipandang sulit dan sering dilupakan oleh hacker - karena alasan buru-buru, ceroboh, atau kurang keahlian - adalah aktivitas penghapusan jejak. Dikatakan sulit karena selain banyak hal yang harus dilakukan oleh hacker dan cukup memakan waktu, penegak hukum selalu saja memiliki cara untuk mencari tahu jejak keteledoran pelaku kejahatan seperti hacker ini. Untuk dapat melakukan penghapusan jejak secara nyaris “sempurna”, selain membutuhkan sumber daya yang tidak sedikit, diperlukan pula pengetahuan dan keahlian yang prima dari hacker yang bersangkutan. Rekam jejak memperlihatkan bahwa dari berbagai jenis kejahatan hacking di dunia, jarang sekali yang jarang terungkap pelaku dan modus operandinya. Berbagai jenis pengapusan jejak banyak dikenal di kalangan hacker, misalnya teknik *steganography, tunneling, log files altering,* dan lain sebagainya.

Dengan mengetahui tahapan-tahapan hacker beroperasi ini maka diharapkan para praktisi pengaman jaringan komputer dan internet paham betul kompleksitas proses dan ekspose resiko yang dihadapi sehari-hari. Semakin dalam seorang hacker masuk ke dalam rangkaian proses terkait, semakin tinggi ancaman resiko yang dihadapi oleh calon korban yang bersangkutan.