MAKALAH

ETHICA HACKER

(dibuat untuk memenuhi tugas mata kuliah Ethical Hacking)

Oleh
Geir Cesar Mamahit
NIM 18208044

UNIVERSITAS NEGERI MANADO
FAKULTAS TEKNIK
PENDIDIKAN TEKNOLOGI INFORMASI & KOMUNIKASI
2021

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa. Bahwa saya telah menyelesaikan tugas mata kuliah Ethical Hacking. Dengan segenap kemampuan yang saya miliki, dalam penyusunan tugas atau makalah ini, tidak sedikit hambatan yang telah saya hadapi. Ada beberapa materi yang akan saya bahas dan jelaskan walau pengertian ini belum bisa dikatakan sempurna tetapi semoga materi ini dapat bermanfaat dan menjadi sumbangan pemikiran bagi pihak yang membutuhkan, khususnya bagi penulis sehingga tujuan yang diharapkan dapat tercapai, Amin.

Tondano, Juni 2021

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Pada mulanya, internet sempat diperkirakan akan mengalami kehancuran oleh beberapa pengamat komputer di era 1980-an karena kemampuannya yang pada saat itu hanya bertukar informasi satu arah saja. Namun semakin ke depan, ternyata perkiraan tersebut meleset, dan bahkan sekarang menjadi suatu kebutuhan akan informasi yang tiada henti-hentinya dipergunakan. Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini, misalnya kita dapat melakukan transaksi perbankan kapan saja dengan e-banking, e-commerce juga membuat kita mudah melakukan pembelian maupun penjualan suatu barang tanpa mengenal tempat. Mencari referensi atau informasi mengenai ilmu pengetahuan juga bukan hal yang sulit dengan adanya e-library dan banyak lagi kemudahan yang didapatkan dengan perkembangan Internet. Tentunya, tidak dapat dipungkiri bahwa teknologi Internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada.

Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer secara online dengan risiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun Negara disamping menimbulkan kejahatan-kejahatan baru. Sehingga keamanan sistem informasi berbasis internet menjadi suatu keharusan untuk lebih diperhatikan karena jaringan internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu komputer ke komputer lain di dalam internet, data itu akan melewati sejumlah komputer yang lain yang berarti akan memberikan kesempatan pada user tersebut untuk mengambil alih satu atau beberapa komputer. Seringkali sebuah sistem jaringan berbasis internet memiliki kelemahan atau sering disebut juga lubang keamanan (*hole*). Akibat masih banyaknya lubang kelemahan sistem di internet ini dapat dimanfaatkan oleh para peretas untuk tujuan tidak baik, seperti pencurian data nasabah bank, *phising*, dan lain sebagainya. Namun demikian masih ada tujuan baiknya yakni memberitahukan kelemahan suatu sistem informasi tertentu sehingga dapat segera diperbaiki. Apabila lubang tersebut tidak ditutup, pencuri bisa masuk dari lubang itu. Pencurian data dan sistem dari internet saat ini sudah sering terjadi. Kejahatan di internet ini populer dengan nama *cyber crime.*

1.2 Rumusan Masalah

a) apa yang dimaksud dengan *cybercrime* dan keterkaitannnya dengan kegiatan *hacking?*

b) Apa itu *hacker atau cracker* dan bagaimana perbedaaannya?
c) Seperti apa dan bagaimana bentuk kegiatan hacking tersebut dalam dunia internet?

1.3 Maksud dan Tujuan

1.3.1 Maksud

Memberikan informasi bagi pembaca mengetahui lebih jauh tentang kejahatan computer yang disebut *cybercrime* lebih detil tentang *hacker* dan *cracker*, dan kegiatan *hacking* itu sendiri serta meluruskan salah kaprah tentang pengertian hacker yang benar dan janganlah menjadi cracker yang berbahaya dan tidak ada gunanya. Di masyarakat umum, istilah *hacker* ini banyak tersalahgunakan atau rancu dengan istilah Cracker. Dimana sering para pecinta teknologi yang merasa dirugikan langsung mengasumsikan bahwa si *hacker* inilah biang keroknya.

1.3.2. Tujuan

Makalah di susun dengan tujuan, antara lain:

a) Memenuhi salah satu tugas mata kuliah Komputer Audit
b) Mengetahui pengertian *Cyber Crime*, *Hacker* dan *Cracker*, kegiatan *hacking?*
c) Bagaimana pengaruhnya yang akan timbul dan bagaimana cara kita menyingkapinya?

BAB II

PEMBAHASAN

2.1 Pengertian *Cyber Crime*, *Hacker* dan *Cracker*

Cybercrime adalah kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber*. Banyak diantaramya adalah pegawai sebuah perusahaan yang loyal dan dipercaya oleh perusahaannya, dan dia tidak perlu melakukan kejahatan komputer. Mereka adalah orang-orang yang tergoda pada lubang-lubang yang terdapat pada sistem computer. Sehingga kesempatan merupakan penyebab utama orang-orang tersebut menjadi 'penjahat cyber'. Cyber crime ini dapat dikategorikan menjadi *Cyberpiracy*, *Cybertrespass*, *Cybervandalism*.

Hacking adalah kegiatan menerobos program komputer milik orang/pihak lain. Hacker memiliki konotasi negatif karena kesalahpahaman masyarakat akan perbedaan istilah hacker dan cracker. Banyak orang memahami bahwa hacker lah yang mengakibatkan kerugian pihak tertentu seperti mengubah tampilan suatu situs web (defacing). Menyisipkan kode-kode virus dan lain sebagainya. Padahal mereka adalah cracker, yang menggunakan celah keamanan yang belum diperbaiki oleh pembuat perangkat lunak (bug) untuk menyusup dan merusak sistem. Atas alasan ini biasanya para hacker dipahami menjadi 2 golongan White Hat Hackers, yakni hacker yang sebenarnya dan cracker yang sering disebut dengan istilah Black Hat Hackers.

White hat hacker adala istilah teknologi informasi dalam bahasa inggris yang mengacu kepada peretas yang secara etis menunjukan suatu kelemahan dalam sebuah sistem komputer. White hat secara umum lebih memfokuskan aksinya kepada bagaimana melindungi sistem, diaman bertentangan dengan black hat yang lebih memfokuskan aksinya kepada bagaimana menerobos sistem tersebut.

Blach hat hacker adalah istilah teknologi informasi yang mengacu kepada peretas yaitu mereka yang menerobos keamanan sistem komputer tanpa ijin, umumnya dengan maksud untuk mengakses komputer-komputer yang terkoneksi ke jaringan tersebut. Istilah cracker diajukan oleh Richard Stallman untuk mengacu kepada peretas dalam arti ini.

2.2 Perbedaan Hacker dan Cracker

Hacker

Mempunyai kemampuan menganalisa kelemahan suatu sistem atau situs. Sebagai contoh : jika seorang hacker mencoba menguji situs Yahoo! dipastikan isi situs tersebut tak akan berantakan dan mengganggu yang lain. Biasanya hacker melaporkan kejadian ini untuk diperbaiki menjadi sempurna. Hacker mempunyai etika serta kreatif dalam merancang suatu program yang berguna bagi siapa saja. Seorang Hacker tidak pelit membagi ilmunya kepada orang-orang yang serius atas nama ilmu pengetahuan dan kebaikan.

Cracker

Mampu membuat suatu program bagi kepentingan dirinya sendiri dan bersifat destruktif atau merusak dan menjadikannya suatu keuntungan.

Sebagian contoh : Virus, Pencurian Kartu Kredit, Kode ***, Pembobolan Rekening Bank, Pencurian Password E-mail/Web Server. Kasus yang paling sering ialah Carding yaitu Pencurian Kartu Kredit, kemudian pembobolan situs dan mengubah segala isinya menjadi berantakan. Sebagai contoh : Yahoo! pernah mengalami kejadian seperti ini sehingga tidak bisa diakses dalam waktu yang lama, kasus click BCA.com yang paling hangat dibicarakan tahun 2001 lalu.

2.3 Kegiatan *Hacking*

Sejarah

Terminologi hacker muncul pada awal tahun 1960-an diantara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka berkutat dengan sejumlah komputer mainframe. Kata hacker pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik ketimbang yang telah dirancang bersama.

Kemudian pada tahun 1983, istilah hacker berubah menjadi negatif. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer The 414s yang berbasis di Milwaukee AS. 414 merupakan kode area lokal mereka. Kelompok yang kemudian disebut hacker tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Satu dari pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Kemudian pada perkembangan selanjutnya muncul kelompok lain yang menyebut-nyebut diri hacker, padahal bukan. Mereka ini (terutama para pria dewasa) yang mendapat kepuasan lewat membobol komputer dan mengakali telepon (phreaking). Hacker sejati menyebut orang-orang ini 'cracker' dan tidak suka bergaul dengan mereka. Hacker sejati memandang cracker sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. Hacker sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi hacker. Para hacker mengadakan pertemuan setiap setahun sekali yaitu diadakan setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan hacker terbesar di dunia tersebut dinamakan Def Con. Acara Def Con tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas hacking.

Hierarki Hacker

Ternyata Hacker juga mempunyai tingkatan-tingkatan, tiap tingkatan di bedakan dengan kemampuan dan ilmu yang dimiliki sang hacker :

a) Elite

Ciri-ciri : mengerti sistem operasi luar dalam, sanggup mengkonfigurasi & menyambungkan jaringan secara global, melakukan pemrogramman setiap harinya, effisien & trampil, menggunakan pengetahuannya dengan tepat, tidak menghancurkan data-data, dan selalu mengikuti peraturan yang ada. Tingkat Elite ini sering disebut sebagai ‘suhu’.

b) Semi Elite

Ciri-ciri : lebih muda dari golongan elite, mempunyai kemampuan & pengetahuan luas tentang komputer, mengerti tentang sistem operasi (termasuk lubangnya), kemampuan programnya cukup untuk mengubah program eksploit.

c) Developed Kiddie

Ciri-ciri : umurnya masih muda (ABG) & masih sekolah, mereka membaca tentang metoda hacking & caranya di berbagai kesempatan, mencoba berbagai sistem sampai akhirnya berhasil & memproklamirkan kemenangan ke lainnya, umumnya masih menggunakan Grafik User Interface (GUI) & baru belajar basic dari UNIX tanpa mampu menemukan lubang kelemahan baru di sistem operasi.

d) Script Kiddie

Ciri-ciri : seperti developed kiddie dan juga seperti Lamers, mereka hanya mempunyai pengetahuan teknis networking yang sangat minimal, tidak lepas dari GUI, hacking dilakukan menggunakan trojan untuk menakuti & menyusahkan hidup sebagian pengguna Internet.

e) Lammer

Ciri-ciri : tidak mempunyai pengalaman & pengetahuan tapi ingin menjadi hacker sehingga lamer sering disebut sebagai ‘wanna-be’ hacker, penggunaan komputer mereka terutama untuk main game, IRC, tukar menukar software prirate, mencuri kartu kredit, melakukan hacking dengan menggunakan software trojan, nuke & DoS, suka menyombongkan diri melalui IRC channel, dan sebagainya. Karena banyak kekurangannya untuk mencapai elite, dalam perkembangannya mereka hanya akan sampai level developed kiddie atau script kiddie saja.

Jenis Kegiatan Hacking

a) Social Hacking,

yang perlu diketahui : informasi tentang system apa yang dipergunakan oleh server, siapa pemilik server, siapa Admin yang mengelola server, koneksi yang dipergunakan jenis apa lalu bagaimana server itu tersambung internet, mempergunakan koneksi siapa lalu informasi apa saja yang disediakan oleh server tersebut, apakah server tersebut juga tersambung dengan LAN di sebuah organisasi dan informasi lainnya

b) Technical Hacking,

merupakan tindakan teknis untuk melakukan penyusupan ke dalam system, baik dengan alat bantu (tool) atau dengan mempergunakan fasilitas system itu sendiri yang dipergunakan untuk

menyerang kelemahan (lubang keamanan) yang terdapat dalam system atau service. Inti dari kegiatan ini adalah mendapatkan akses penuh kedalam system dengan cara apapun dan bagaimana pun.

Kemampuan Dasar Hacking

a) Pelajari Bahasa Pemrograman

Menguasai hanya satu bahasa pemrograman saja tidak akan mencapai tingkat kemampuan hacker atau bahkan seorang programer, perlu belajar cara pemrograman secara umum, tidak bergantung pada satu bahasa mana pun. Anda perlu mencapai tahap dimana dapat mempelajari bahasa baru dalam beberapa hari, dengan menghubungkan apa yang ada di manual dengan apa yang telah Anda ketahui. Perlu memplajari beberapa bahasa yang jauh berbeda dengan satu dengan yang lainya. Bahasa-bahasa terpenting dalam hacking adalah Pyton, C, Perl, dan LISP tapi paling baik sebetulnya mempelajari semuanya karena masing-masing mewakili cara pendekatan pemrograman yang berbeda dan tiap bahasa akan memberi pelajaran-pelajaran berharga.

b) Kuasai Sistem Operasi

Tentu saja seorang hacker harus menguasai sistem operasi contohnya windows, linux dll. Karena inti dari komputer tersebut adalah system operasi.

c) Pelajari Worl Wide Web

Maksudnya lebih dari sekedar menggunakan browser, tetapi mempelajari cara menulis HTML, bahasa markup Web.

d) Pelajari Jaringan Komputer

Jaringan komputer yang menghubungkan kita dengan orang lain di internet, sehingga perlu memplejari Jaringan komputer.

Semakin banyak dari hal-hal diatas yang sudah Anda kerjakan, semakin besar kemungkinan Anda adalah calon hacker berbakat, karna ilmu tentang komputer anda akan semakin terasah.

Metodologi Hacking

a) Reconaissance

Reconnaissance atau dikenal juga dengan footprinting merupakan langkah pertama metodologi hacking yang bertujuan untuk mendapatkan informasi awal, seperti alamat ip, dns server, domain, table routing, sistem operasi dan lain sebagainya. Namun, seluruh informasi tersebut tidak selalu diambil secara diam - diam dan tidak jarang perusahaan - perusahaan menyebarkan dokumentasi jaringannya sendiri yang dipublikasikan di internet. Terdapat cukup banyak tools yang digunakan oleh hacker dalam reconnaissance, misalnya melihat informasi register domain pada situs-situs tertentu seperti, whois.net, arin.net dan lain-lain. Intinya adalah untuk mendapatkan informasi sebanyak - banyaknya sebagai persiapan untuk melakukan langkah berikutnya. Untuk pencegahannya, batasi untuk tidak menyebarkan informasi penting anda tersebut jika anda sering browsing di internet.

b) Scanning

Jika seorang hacker telah mengenali sistem secara keseluruhan pada langkah pertama metodologi hacking maka pada langkah kedua metodologi hacking, seorang hacker mulai mencari jalur penyusupan

yang lebih spesifik. Jalur penyusupan tersebut dapat berupa port yang umum digunakan oleh sistem, misal : port 80 untuk http, port 21 untuk ftp, port 3389 untuk terminal service dan port 1433 untuk microsoft sql server. Langkah kedua metodologi hacking tersebut dikenal sebagai langkah metodologi scanning dan tools yang sering digunakan antara lain, solarwinds, war ping, sam spade, nmap, dan superscan. Untuk pencegahannya anda bisa melakukan minimalisasi penggunaan port dan service yang tidak diperlukan lagi. Serta jangan lupa untuk selalu menggunakan firewall dan memonitoring jaringan secara berkala.

c) Enumeration

Jika seorang hacker telah berhasil pada langkah kedua metodologi hacking di atas yang juga disebut scanning maka pada langkah ketiga metodologi hacking di sini merupakan langkah lanjutan untuk mengambil informasi yang lebih detail dari target hacker. Informasi tersebut dapat berupa user-user, sharing folder, dan service yang sedang berjalan termasuk dengan versinya dan mulai dari sinilah serangan mulai dilakukan dengan berbagai cara, seperti sniffing paket maupun man in the minddle.

d) Penetration

Pada langkah ke-empat di sini, seorang hacker mulai mengambil alih sistem setelah ia memperoleh informasi yang dibutuhkan dan bisa dikatakan jika seorang hacker mampu masuk kedalam langkah metodologi hacking ke-empat ini berarti ia telah melewati pintu terpenting petahanan suatu sistem. Namun, sayangnya terkadang jebolnya pintu pertahanan disebabkan oleh kelalaian sistem tersebut sendiri seperti, penggunaan password yang lemah dan mudah ditebak. Bisa jadi hacker pun masuk tidak dengan hak administrator, namun seorang hacker mampu menyerang resource sehingga akhirnya mendapatkan hak akses administrator.

e) Elevation

Setelah seorang hacker mampu mengakses suatu sistem pada langkah metodologi hacking ke-empat di atas maka pada langkah ke-lima disini seorang hacker mulai mengubah status privilege-nya setara dengan user yang memiliki hak penuh terhadap sistem tersebut.

f) Pilfer

Setelah seorang hacker mampu melewati langkah ke-lima metodologi hacking di atas maka dengan memperoleh kontrol penuh terhadap sistem, seorang hacker sangat leluasa untuk melakukan apa yang diinginkannya seperti mengambil data confidential baik dalam bentuk teks, database, dokumen dan e-mail.

g) Expansion

Pada langkah ke-tujuh metodologi hacking, seorang hacker mulai melakukan lagi proses reconnaissance, sccaning dan enumeration dengan target sistem lainnya. Tidak hanya dengan menyusup pada satu sistem saja, namun seorang hacker mampu memperluas penyusupannya dengan memasuki sistem dan jaringan yang lain. Langkah metodologi disini disebut dengan expansion.

h) Housekeeping

Dengan melakukan proses yang sering dikenal dengan sebutan convering track, hacker berusaha menghapus jejaknya dengan bersih. Langkah metodologi hacking kedelapan inilah yang disebut housekeeping. Hacker yang cerdik akan meninggalkan korban tanpa meninggalkan pesan dan pada umumnya sistem mencatat event-event penting yang terjadi dalam log file yang dapat mendeteksi keberadaan hacker. Sekalipun seorang hacker tidak meninggalkan pesan, namun mungkin saja seorang hacker tersebut pergi dengan meninggalkan kesan kepada sang korban. Kesan tersebut biasanya berupa backdoor atau jalan belakang untuk masuk ke dalam sistem lagi dan backdoor dibuat agar seorang hacker tersebut masih dapat menyusup masuk ke dalam sistem walaupun jalur sebelumnya telah tertutup. Backdoor tersebut dapat diciptakan dengan membuat user yang memiliki kontrol penuh terhadap sistem, seperti misalnya menginstall rootkit, menyebar trojan maupun meletakkan shell yang dapat dieksekusi secara remote.

2.4 Kode Etik Hacking

a) Mampu mengakses komputer tak terbatas dan totalitas.
b) Semua informasi haruslah FREE.
c) Tidak percaya pada otoritas, artinya memperluas desentralisasi.
d) Tidak memakai identitas palsu, seperti nama samaran yang konyol, umur, posisi, dll.
e) Mampu membuat seni keindahan dalam komputer.
f) Komputer dapat mengubah hidup menjadi lebih baik.
g) Pekerjaan yang di lakukan semata-mata demi kebenaran informasi yang harus disebar luaskan.
h) Memegang teguh komitmen tidak membela dominasi ekonomi industri software tertentu.
i) Hacking adalah senjata mayoritas dalam perang melawan pelanggaran batas teknologi komputer.
j) Baik Hacking maupun Phreaking adalah satu-satunya jalan lain untuk menyebarkan informasi pada massa agar tak gagap dalam komputer.

Cracker tidak memiliki kode etik apapun.

BAB III

PENUTUP

3.1 Kesimpulan

Dunia maya tidak berbeda jauh dengan dunia nyata. Mudah-mudahan para penikmat teknologi dapat mengubah mindsetnya bahwa hacker itu tidak selalu jahat. Menjadi hacker adalah sebuah kebaikan tetapi menjadi seorang cracker adalah sebuah kejahatan. Segalanya tergantung individu masing-masing. Para hacker menggunakan keahliannya dalam hal komputer untuk melihat, menemukan dan memperbaiki kelemahan sistem keamanan dalam sebuah sistem komputer ataupun dalam sebuah software. Oleh karena itu, berkat para hacker-lah Internet ada dan dapat kita nikmati seperti sekarang ini, bahkan terus di perbaiki untuk menjadi sistem yang lebih baik lagi. Maka hacker dapat disebut sebagai pahlawan jaringan sedang cracker dapat disebut sebagai penjahat jaringan karena melakukan melakukan penyusupan dengan maksud menguntungkan dirinya secara personallity dengan maksud merugikan orang lain.

3.2 Saran

Banyak penjahat di dunia internet ini, dan mereka selalu berusaha mencari kelengahan kita sewaktu sedang surfing di internet, apalagi pada saat ini bisnis di dunia internet sangat menjanjikan. Oleh karena itu ke hati-hatian sangat diutamakan jangan sampai para penyusup masuk ke system dan mengobrak-abriknya.

Berikut ini ada beberapa tips agar terhindar dari tangan tangan jahil di dunia maya, antara lain:

a) Gunakan Antivirus, Anti Spyware dan Anti Adware
b) Gunakan Firewall
c) Gunakan Internet Browser yang lebih baik
d) Ganti password sesering mungkin dan buat password yang sukar ditebak
e) Jangan terkecoh e-mail palsu

DAFTAR PUSTAKA

http://hackerklp01.blogspot.co.id/2013/11/makalah-hacking_8365.html

http://tentanghackerdancracker.blogspot.co.id/

http://bsi4p3.blogspot.co.id/2014/04/makalah-hacker.html

https://www.academia.edu/27922261/BAB_I_PENDAHULUAN_1_1_Latar_Belakang_Masalah