KONSEP PENERAPAN KEAMANAN JARINGAN PUBLIK DI LINGKUNGAN KAMPUS STMIK BINA PATRIA

Sugeng Wahyudiono[1)], **Deni Lestiono**[2)]
[1)] *"Manajemen Informatika" STMIK BINA PATRIA*
[2)] *"Manajemen Informatika" STMIK BINA PATRIA*
Email : farosgisaka@gmail.com[1)], *denilestiono@gmail.com*[2)],

ABSTRACT

Internet or public-based information system security of a campus is an issue that requires more attention on security holes may exist within the operating system and computer network that may cause weaknesses and open holes for the hackers and crackers can use them to infiltrate into the computer or server network. Security aspects or computer or server in the internet/public are Privacy/Confidentiality, Integrity, Availability, and Authenticity. The method of using username/password is available in the internet network or server computer systems.

Keywords*: Security, Network, Server, Hacker, Data Theft, Username and Password Method*

ABSTRAK

Keamanan sistem informasi kampus berbasis Internet atau Publik adalah suatu keharusan untuk lebih diperhatikan. adanya lubang-lubang keamanan pada system operasi maupun Jaringan Komputer yang dapat menyebabkan kelemahan dan terbukanya lubang sehingga dapat digunakan para hacker, cracker untuk menyusup ke dalam jaringan computer maupun server tersebut. Aspek keamanan komputer atau server dalam Internet/ Publik adalah Privacy / Confidentiality, Integrity, Availability dan Authenticity. Metode dari Penggunaan Username/ password terdapat pada Jaringan internet maupun pada system komputer server

Kata Kunci : *Keamanan, Jaringan, Server, Hacker, Pencurian Data, Metode Username, Password*

1. Pendahuluan

Pada era serba Digital seperti sekarang ini, 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 yang lain di dalam Internet, data itu akan melewati sejumlah komputer yang lain yang berarti akan memberi kesempatan pada user tersebut untuk mengambil alih satu atau beberapa komputer. Kecuali suatu komputer terkunci di dalam suatu ruangan yang mempunyai akses terbatas dan komputer tersebut tidak terhubung ke luar dari ruangan itu, maka komputer tersebut akan aman. Pembobolan sistem keamanan di Internet terjadi hampir tiap hari di seluruh dunia.

Kejahatan cyber atau lebih dikenal dengan *cyber crime* adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengekploitasi komputer lain yang terhubung juga pada internet. Adanya lubang-lubang keamanan pada system operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para hacker, cracker dan script kiddies untuk menyusup ke dalam computer tersebut. Kejahatan yang terjadi dapat berupa:

a. Pencurian terhadap data
b. Akses terhadap jaringan internal
c. Perubahan terhadap data-data penting
d. Pencurian informasi dan berujung pada penjualan informasi

2. Literatur

2.1. Penelitian Sebelumnya

Beberapa penelitian sebelumnya yang berkaitan dengan keamanan jaringan adalah pengeleloaan jaringan pada laboratorium berbasis client server. Salah satunya adalah penelitian dengan judul Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali (I Gusti Komang, 2015).Selain itu penelitian yang terkait dengan konsep kemanan jaringan publik. Salah satunya adalah penelitian dengan judul Implementasi Keamanan Jaringan Komputer Pada Virtual Private Network (VPN) Menggungakan Ipsec (Rudol, 2017).

2.2. Landasan Teori

a. Aplikasi

Aplikasi adalah komponen yang berguna melakukan pengolahan data maupun kegiatan- kegiatan seperti pembuatan dokumen atau pengolahan data. Aplikasi adalah PC yang berinteraksi langsung dengan user. Aplikasi berjalan di atas sistem operasi, sehingga agar aplikasi bisa di aktifkan, kita perlu melakukan instalasi sistem operasi dahulu (Wahana, 2013).

b. Jaringan

Jaringan komputer adalah himpuan "interkoneksi" antara 2 komputer autonomous atau lebih yang terhubung dengan media tranmisi kabel atau tanpa kabel (wireless). Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown, atau melakukan control lainya, maka komputer-komputer tersebut bukan autonomous (tidak melakukan control terhadap komputer lain dengan akses penuh). Dua komputer dikatakan terkoneksi apabila keduanya bias saling bertukar data/informasi, berbagai resourse yang dimiliki, seperti file, printer, media penyimpanan (hardisk, floppy disk, cd-room, flash disk, dll). Data yang berupa teks, audio maupun video bergerak melalui media kabel atau tanpa kabel sehingga memungkinkan pengguna komuter dalam jaringan komputer dapat saling bertukar file atau data, mencetak pada printer yang sama dan menggunakan hardware atau software yg terhubung dalam jaringan secara bersama-sama.

c. Jaringan Publik

Sebuah jaringan publik dijalankan sebagai sebuah layanan yang tersedia untuk pelanggan. Setiap individu atau perusahaan yang membayar biaya berlangganan dapat menggunakan jaringan. Sebuah perusahaan yang menawarkan layanan komunikasi dikenal sebagai penyedia layanan. Konsep penyedia layanan ini cukup luas, dan melampaui Internet Service Provider (ISP). Bahkan, terminologi berasal dari perusahaan yang menawarkan layanan suara telepon analog.

3. Metode

3.1 Metode Ancaman Dalam Jaringan Publik

Pada dasarnya ancaman datang dari seseorang yang mempuyai keinginan memperoleh hak akses ilegal ke dalam suatu jaringan komputer. Oleh karena itu, harus ditentukan siapa saja yang diperbolehkan mempunyai akses legal ke dalam system yang berisi aplikasi maupun data penting, dan ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan sangat berguna apabila dapat membedakan tujuan-tujuan tersebut pada saat merencanakan sistem **Keamanan jaringan** komputer .

Beberapa tujuan para penyusup adalah:

a. Ingin tahu sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut The Curius.

b. Membuat sistem jaringan menjadi down, atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai The Malicious.
c. Berusaha untuk mengambil atau memanipulasi sumber daya di dalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup seperti ini sering disebut sebagai The Profile Intruder.
d. Ingin tahu data apa saja yang ada di dalam jaringan komputer untuk selanjutnya dimanfaatkan untuk mendapat uang. Penyusup seperti ini sering disebut sebagai The Competition.

1) Pengguna Internet

Pengguna terhubung ke Internet melalui layanan Internet Service Provider (ISP), baik dengan menggunakan modem, DSL, cable modem, wireless, maupun dengan menggunakan leased line. ISP ini kemudian terhubung ke Internet melalui network provider (atau upstream). Di sisi Web Server, terjadi hal yang serupa. Server Internet terhubung ke Internet melalui ISP atau network provider lainnya. Gambar tersebut juga menunjukkan beberapa potensi lubang keamanan (security hole).

Di sisi pengguna, komputer milik pengguna dapat disusupi virus dan trojan horse sehingga data-data yang berada di komputer pengguna (seperti nomor PIN, nomor kartu kredit, dan kunci rahasia lainnya) dapat disadap, diubah, dihapus, dan dipalsukan. Jalur antara pengguna dan ISP dapat juga di sadap. Sebagai contoh, seorang pengguna yang menggunakan komputer di lingkungan umum (public facilities) seperti di Warung Internet (warnet) dapat disadap informasinya oleh sesame pengguna warnet tersebut (atau pemilik warnet yang tidak bertanggung jawab) ketika dia mengetikkan data-data rahasia melalui web.

Di sisi ISP, informasi dapat juga disadap dan dipalsukan. Sebagai contoh bila sistem keamanan dari sang ISP ternyata rentan, dan dia kebobolan, maka mungkin saja seorang cracker memasang program penyadap (sniffer) yang menyadap atau mengambil informasi tentang pelanggan ISP tersebut.

Di sisi penyedia jasa, dalam hal Web Server yang menyediakan layanan Internet.ada juga potensi lubang keamanan. Berbagai kasus tentang keamanan dan institusi finansial sudah dilaporkan. Misalnya, ada kasus di Amerika serikat dimana seorang cracker berhasil masuk ke sebuah institusi finansial dan mengambil data-data nasabah dari berbagai bank yang berada dalam naungan institusi finansial tersebut. Di Indonesia sendiri ada "kasus" domain "plesetan" klikbca.com yang sempat membuat heboh.

2) Pelaku Kejahatan Internet

Tipe – tipe dari para pelaku kejahatan di dunia maya umumnya tipe mereka diambil dari cara kerja dan tujuan mereka dalam melakukan tindakan perilaku yang menyimpang. Namun dalam perkembangannya, pengertian hacker ini menjurus ke arah yang lebih negatif. Karenanya , istilah pun bertambah untuk membedakan yang satu dengan yang lainyakni ada cracker , phreaker , dan carder.

a) Cracker
   Merupakan seseorang yang masuk secara illegal ke dalam system komputer. Istilahnya cracker ini merupakan para hacker yang menggambarkan kegiatan yang merusak dan bukan hacker pada pengertian sesungguhnya. Hacker dan Cracker mempunyai proses yang sama tapimotivasi dan tujuan yang berbeda. Cracker adalah hacker yang merusak , oleh sebab itu istilah hacker menjadi buruk di masyarakat bahkan sekarang ada dinamakan white hacker dan blackhacker.
b) Phreaker
   Ditinjau dari tujuannya, phreaker merupakan seseorang yang

melakukantindakan kejahatan terhadap jaringantelepon misalnya menyadap jaringan telepon seseorang atau badan pemerintahan dan menelpon interlokalgratis. Pada tahun 1971, seorang veteran perang Vietnam bernama JohnDraper menemukan cara menelponjarak jauh , tanpa mengeluarkan biaya. Triknya adalah dengan menggunakan sebuah peluit, yang menghasilkan suara kurang lebih 2600 mhz saat menelpon. Dari sinilah istilah phreaker mulai dikenal.

c) Carder
Merupakan kelompok orang yang melakukan tindakan kejahatan dengan melakukan manipulasi nomor kartu kredit orang lain dan menggunakannya untuk kepentingan pribadi. Sejarah yang paling fenomenal adalah seorang carder yang bernama Kevin Mitnick melakukan manipulasi kartu kredit sebanyak 2000 nomor kartu kredit. Berbagai virus dan tindakan para carder untuk menyerang semakin ganas. Tidak kurang situs – situs besar yang mempunyai tingkat keamanan yang tinggi berhasil dijebol seperti situs berita internasional CNN.com, Yahoo.com, Astaga.com, bahkan situs pemerintahan Amerika seperti situs gedung putih , FBI, dan Microsoft pun terkena serangan pula.

3.2 Sekuriti Internet

1) Alasan Ketidakamanan Internet

Dari uraian di paragraf-paragraf sebelumnya, kita tahu bahwa sebenarnya internet belumlah benar-benar aman. Beberapa alasan utama ketidakamanan internet adalah sebagai berikut:

a) Internet adalah wilayah bebas tak bertuan, tak ada pemerintahan dan hukum yang mengaturnya. Manajemen dan perlindungan keamanan masing-masing jaringan diserahkan sepenuhnya kepada penanggungjawab jaringan (administrator jaringan internet). Dan pada kenyataannya, tidak semua administrator jaringan, mengerti dengan baik tentang keamanan internet.
b) Masih banyaknya 'hole' (lubang) di sistem komputer dan jaringan yang dapat dimanfaatkan oleh cracker demi keuntungan/kepuasan nafsu pribadinya.
c) Akses user dari kamar (tempat terpencil) dan lemahnya pengawasan dari orang lain, sehingga nafsu pribadilah yang akan menguasai si user;
d) Kurangnya kesadaran adanya 'hole' kejahatan di internet oleh kebanyakan user.
e) Belum adanya standar keamanan manajemen jaringan internet.

2) Aspek Keamanan Komputer dalam Internet

Saat kita menggunakan komputer dengan koneksi internet untuk keperluan penting yang membutuhkan privasi dan integritas tinggi, baik yang bersangkutan dengan transaksi maupun tukar menukar data yang sifatnya privat, maka harus diperhatikan beberapa syarat keamanan Internet di bawah ini.

a) Privacy / Confidentiality
Sistem harus memastikan bahwa informasi dikomunikasikan dan disimpan secara aman dan hanya dapat diakses oleh mereka yang berhak saja. Data-data pribadi yang bersifat pribadi harus dapat terjaga dan dapat di pastikan terproteksi dengan baik. Contoh kasus seperti usaha penyadapan (dengan program sniffer). Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi .

b) Integrity
Sistem harus memastikan bahwa informasi dikirimkan secara menyeluruh, lengkap dan dalam keadaan tidak berubah. Informasi yang dikirim tidak bisa diubah tanpa seijin pemiliknya.Contoh serangan adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, "man in the middle attack" dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

c) Availability
Sistem yang bertugas mengirimkan, menyimpan dan memproses informasi dapat digunakan ketika dibutuhkan oleh mereka yang membutuhkannya. Contoh hambatan "denial of service attack" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.

d) Authenticity
Sistem harus memastikan bahwa pihak, obyek, dan informasi yang berkomunikasi adalah riil dan bukan palsu. Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga"intellectual property", yaitu dengan meni dokumen atau hasil karya dengan "tangan" pembuat) dan digital signature.
Metode authenticity yang paling umum digunakan adalah penggunaan username beserta password-nya. Metode username/password ini ada berbagai macam
jenisnya, berikut ini adalah macam-macam metode username/password:

1. Tidak ada username/password
2. Pada sistem ini tidak diperlukan username atau password untuk mengakses suatu jaringan. Pilihan ini merupakan pilihan yang palin tidak aman.
3. Statis username/password
4. Pada metode ini username/password tidak berubah sampai diganti oleh administrator atau user. Rawan terkena playbacks attacka, eavesdropping, theft, dan password cracking program.
5. Expired username/password
6. Pada metode ini username/password akan tidak berlaku sampai batas waktu tertentu (30-60 hari) setelah itu harus direset, biasanya oleh user. Rawan terkena playback attacks, eavesdropping, theft, dan password cracking program tetapi dengan tingkat kerawanan yang lebih rendah dibanding dengan statis username/password.
7. One-Time Password (OTP)
8. Metode ini merupakan metoda yang teraman dari semua metode username/password. Kebanyakan sistem OTP berdasarkan pada "secret passphrase", yang digunakan untuk membuat daftar password. OTP memaksa user jaringan untuk memasukkan password yang berbeda setiap kali melakukan login. Sebuah password hanya digunakan satu kali.

e) Access Control
Sistem harus dapat melakukan kontrol akses. Merupakan cara pengaturan akses kepada informasi. berhubungan dengan masalah authentication dan juga privacy menggunakan kombinasi userid/password atau dengan

f) NonRepudiation
Sistem harus memastikan bahwa pihak yang melakukan transaksi tidak dapat menolak, menyangkal transaksi yang telah dilakukannya.

3) Security Attack Models

Menurut W. Stallings [William Stallings, "Network and Internetwork Security," Prentice Hall, 1995.] serangan (attack) terdiri dari :

a) Interruption
Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Contoh serangan adalah "denial of service attack".

b) Interception
Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan (wiretapping).

c) Modification
Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.

d) Fabrication
Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

4) Sumber lubang keamanan

Lubang keamanan (security hole) dapat terjadi karena beberapa hal; salah disain (design flaw), salah implementasi, salah konfigurasi, dan salah penggunaan.

a) Salah Disain
Lubang keamanan yang ditimbulkan oleh salah disain umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, maka biarpun diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.

b) Implementasi kurang baik
Lubang keamanan yang disebabkan oleh kesalahan implementasi sering terjadi. Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean. Akibatnya cek atau testing yang harus dilakukan menjadi tidak dilakukan. Lubang keamanan yang terjadi karena masalah ini sudah sangat banyak, dan yang mengherankan terus.terjadi, seolah-olah para programmer tidak belajar dari pengalaman.

c) Salah konfigurasi
Meskipun program sudah diimplementasikan dengan baik, masih dapat terjadi lubang keamanan karena salah konfigurasi. Contoh masalah yang disebabkan oleh salah konfigurasi adalah berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi "writeable". Apabila berkas tersebut merupakan berkas yang penting, seperti berkas yang digunakan untuk menyimpan password, maka efeknya menjadi lubang keamanan.

d) Salah menggunakan program atau system
Salah penggunaan program dapat juga mengakibatkan terjadinya lubang keamanan. Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal. Sering terjadi cerita horor dari sistem administrator baru yang teledor dalam menjalankan perintah "rm -rf" di sistem UNIX (yang menghapus berkas atau direktori beserta sub direktori di dalamnya). Akibatnya seluruh berkas di system menjadi hilang

mengakibatkan Denial of Service (DoS). Apabila system yang digunakan ini digunakan bersama-sama, maka akibatnya dapat lebih fatal lagi. Untuk itu perlu berhati-hati dalam menjalan program, terutama apabila dilakukan dengan menggunakan account administrator seperti root tersebut.

4. Hasil dan Pembahasan

Contoh-contoh Kejahatan di Internet dan Cara Penanggulangannya

1. Bom Mail

Pengiriman bom mail ke sebuah e-mail address, biasanya dimulai oleh sentimen pribadi si pemilik e-mail address (target) dengan cracker. Cracker mengirimkan e-mail sebanyak-banyaknya ke komputer target, sehingga sistem di komputer target down (hang-up) karena kepenuhan e-mail.Cara penanggulangannya:

1) Konsultasi dengan ISP (Internet Service Provider)
2) Protes ke pengirim & ISP pengirim
3) Menaruh filtering software di mail server, untuk mencegah pengiriman e-mail oleh cracker yang sudah teridentifikasi.

2. Batu Loncatan Penyerangan

Sistem komputer dengan pengamanan lemah, tak jarang digunakan oleh cracker sebagai batu loncatan untuk menyerang target (komputer) lain, dengan maksud untuk lebih mengaburkan jejak si cracker .Untuk itu, setiap penanggung jawab sistim komputer, sebenarnya tidak hanya bertanggung jawab terhadap sistimnya sendiri, tapi juga bertanggung jawab terhadap jaringan lain, baik yang terdekat maupun jaringan yang relatif jauh dari jaringan Internet wilayahnya. Sebagai langkah preventif, penerapan sistim deteksi penerobosan merupakan suatu hal yang sangat disarankan.

3. Pemalsuan ID

Seorang cracker hampir dapat dipastikan tidak akan pernah memakai ID (identifitas) asli yang dimilikinya. Cracker akan berusaha menggunakan ID milik orang lain, atau membuat ID palsu dalam setiap gerakannya. Untuk mendapatkan ID orang lain, cracker dapat mencari lewat penye-"trap"-an data-data yang lewat jaringan, dan menganalisanya. Penanggulangannya adalah dengan penggunaan server yang didukung oleh costumer service dari pembuat program adalah suatu hal yang mutlak diperlukan oleh situs internet, terutama yang mempunyai tingkat kepopuleran yang tinggi. Sehingga setiap kelemahan yang ditemukan dari suatu sistim bisa segera didapatkan penanggulangannya. Selain itu, perlu juga dipertimbangkan pemilihan server dari pembuat program yang lebih mengutamakan kestabilan sistem daripada kelebihan fungsi-fungsi di level aplikasi. Penggunaan sistim otentikasi yang baik seperti otentikasi dengan menggunakan kartu pintar (smart card), sidik jari dan lain-lain, merupakan salah satu jalan keluar dari masalah ini.

4. Pencurian File Password atau data Customer

Salah satu cara untuk mendapatkan ID milik orang lain, tak jarang seorang cracker berusaha mencuri file password dari suatu sistem, kemudian menganalisanya. Lebih dari itu, cracker secara pribadi ataupun bersindikat, berusaha mencuri data rahasia suatu perusahaan untuk dijual ke perusahaan lawan.Untuk penanggulangan pencurian file password adalah dengan melakukan pencegahan penggunaan password yang mudah ditebak, sehingga biarpun file dicuri, tidak terlalu bermanfaat. Cara lainnya adalah dengan menggunakan sistim shadowing pada sistim password di sistim Unix, atau untuk sistim WindowNT, Microsoft menerapkan sistim enkripsi (penyandian). Biasanya, sistim server yang menangani jasa web ini tidak menggunakan pendekatan keamanan dalam pengoperasiannya. Padahal, walaupun suatu sistim dikatakan kuat oleh pembuatnya,kalau

tidak didukung dengan security policy (peraturan /kebijaksanaan internal keamanan) dan pengoperasian yang baik, tidak akan bisa menghasilkan sistim yang kuat. Selain itu, hubungan dengan pihak pembuat program merupakan salah satu hal yang diperlukan dalam membangun sistim yang tahan serangan. Untuk pengamanan data yang melewati jaringan terbuka seperti Internet, tidak ada jalan lain selain penggunaan enkripsi sehingga data yang lewat tidak bisa dimanfaatkan orang yang tidak berhak ataupun oleh cracker.

5. Penggantian isi Homepage (Deface)

Masalah ini pun sering kali menimpa beberapa site di Indonesia. Contohnya oleh cracker portugis (dalam masalah Timor Timur) dan Cina (tentang kerusuhan Mei 1998 yang banyak menewaskan orang-orang Cina di Indonesia). Bahkan, di Jepang pun HP Science Technology Agency di-crack lewat penggantian halaman depan HP. Di AS, seorang cracker pernah berhasil mendapatkan ratusan ribu data kartu kredit dari hasil analisa program yang ditanamkan di server ISP-nya.
Untuk menangani masalah ini biasanya seorang admin web harus bekerja keras untuk bisa mengembalikan halaman websitenya kembali seperti semula. Alangkah baiknya jika seorang admin web selalu mengikuti perkembangan berita-berita yang berkaitan dengan celah-celah keamanan aplikasi yang digunakan pada web tersebut. Dengan mengikuti berita tersebut maka seorang admin web dapat selalu mengupdate aplikasi yang di gunakan pada web nya sehingga terhindar dari deface. Selain itu admin web juga harus sering-sering mem back up data web sitenya terutama database, hal ini perlu dilakukan untuk langkah awal jika admin web tersebut sudah kecolongan maka dia dengan segera dapat mengembalikan websitenya kembali seperti semula.

6. Program Jebakan

Trojan Horse(kuda troya) sudah dikenal sebagai salah satu teknik cracker yang sangat ampuh dan sering digunakan dalam kejahatan-kejahatan di Internet. Cracker memberikan program gratis, yang feature-nya bagus (banyak fungsi-fungsi program yang bermanfaat) dan penggunaanya mudah dan enak (user friendly), tetapi di dalam program tersebut, sebenarnya si cracker 'menanamkan' program lain yang tidak terlihat oleh user. Misalnya program untuk pencurian ID dan password, pencurian file-file tertentu dan lain-lain.Cara penanggulangannya yang paling utama adalah dengan memasang Fire Wall dan Ativirus yang selalu di up date. Selain itu juga dengan mengupdate Sistem Operasi yang digunakan untuk menutup hole atau lubang keamanan pada Sistem Operasinya.

7. Shutdown Service

Seorang cracker terkadang berusaha meng-hang-up suatu sistem, dengan tujuan agar sistem target tidak dapat melayani service dari semua user. Kejadian ini pernah menimpa Microsoft, yang mana akses ke homepage-nya oleh semua user ditolak, karena komputer server dibuat 'sibuk' sendiri oleh si cracker.Biasanya penyebab masalah ini adalah terletak pada program server yang menangani suatu jasa/service tertentu. Yang paling sering terjadi adalah desain program server yang tidak memikirkan/ mempertimbangkan masalah Keamanan jaringan, sehingga penggunaan buffer (tempat penampungan sementara di memori/hard disk) tidak terkontrol dan mengakibatkan server tidak bisa menangani permintaan jasa dari pengguna yang sebenarnya. Untuk menanggulangi masalah ini, penanggung jawab sistim sebaiknya selalu melakukan pengecekan terhadap program yang dipakainya dengan melakukan pencocokan jejak (log) kriptografi dari programnya dengan jejak yang disediakan oleh pembuat program.

4. 1 Cara Aman Berselancar di Dunia Maya

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.

1. Gunakan Favorites atau Bookmarks

Pengguanaan Favorites atau Bookmarks ini dimaksudkan untuk menjamin website yang dimasuki adalah benar-benar website bisnis internet yang telah diikuti, sebab banyak upaya pencurian username dan password dengan cara membuat website palsu yang sama persis dengan aslinya, dengan URL yang mirip dengan aslinya. Jika dalam melakukan aktifitas menemukan kejanggalan yaitu tampilan halaman yang berubah dan koneksi terputus lalu muncul halaman yang meminta memasukkan username dan password,

2. Gunakan Antivirus

Pastikan pada komputer sudah terinstal Antivirus, gunakan Antirus profesional seperti Norton Antivirus, McAfee Antivirus, Kaspersky, F-Secure dan antivirus buatan vendor yang sudah berlisensi. Penggunaan antivirus akan sangat membantu untuk mengantisipasi masuknya virus ke PC. Update antivirus juga sangat bermanfaat untuk menangani jika terdapat virus baru yang beredar.

3. Gunakan anti Spyware dan anti Adware

Selain Virus ada yang harus diwaspadai yaitu Spyware dan Adware, Spyware adalah sebuah program kecil yang masuk ke komputer kita dengan tujuan memata-matai kegiatan berinternet kita dan mencuri semua data penting termasuk username dan password, Adware juga begitu tetapi lebih pada tujuan promosi yang akan memunculkan jendela/pop-up di komputer kita ketika sedang browsing, biasanya berupa iklan website porno.

4. Gunakan Firewall

Untuk lebih mengoptimalkan pertahanan komputer maka gunakanlah firewall, untuk Windows XP dan Vista bisa menggunakan firewall standar yang ada, saat ini ada beberapa firewall yang cukup mumpuni untuk mencegah para penyusup, seperti Comodo Firewal, Zone Alarm, ataupun mengaktifkan Fireall bawaan Windows.

5. Gunakan Internet Browser yang lebih baik

Daripada menggunakan Internet Explorer bawaan WIndows, lebih baik menggunakan Browser alternatif yang lebih aman dan mempunyai proteksi terhadap hacker yang lebih canggih.Saat ini beberapa penyedia browser yang selalu bersaing memberikan yang terbaik bagi user, seperti Mozila Firefox, Opera, Google Chrome dan lain-lain.

6. Hilangkan Jejak

Windows dan browser biasanya akan menyimpan file-file cookies, history atau catatan aktivitas user ketika berinternet, ini merupakan sumber informasi bagi para hacker untuk mengetahui kegiatan user dan juga mencuri username dan password yang telah digunakan dalam berinternet, selain itu hacker juga biasa mengikut sertakan file-file pencuri data mereka di folder-folder yang menyimpan cookies dan history ini di komputer .(Cookies = file yang masuk ke komputer ketika kita mengunjungi sebuah website.

History = Daftar kegiatan kita ketika berinternet yang disimpan oleh browser yang kita gunakan). Selalu hapus semua jejak berinternet agar para hacker tidak bisa menyusup ke komputer.

7. Ganti password sesering mungkin

Yang paling penting adalah mengganti password yang digunakan sesering mungkin, sebab secanggih apapun para hacker dapat mencuri username dan password tidak akan berguna. jika password sudah berubah ketika para hacker itu berusaha masuk ke website bisnis internet yang diikuti

8. Buat password yang sukar ditebak

Jangat buat password yang berisikan tanggal lahir, nama keluarga, nama biatang peliharaan , atau menggunakan kalimat pendek dan umum digunakan sehari-hari. Buatlah password sepanjang mungkin semaksimal mungkin yang diperbolehkan, buat kombinasi antara huruf besar dan huruf kecil dan gunakan karakter spesial seperti ? >) / & % $, dan yang paling penting jangan simpan catatan password di komputer dalam bentuk file, buatlah catatan pada selembar kertas dan taruh di tempat yang aman di sisi komputer , buatlah seolah-olah itu bukan catatan password, jangan simpan di dompet, jika dompet hilang maka akan kesulitan nantinya.

9. Jangan terkecoh e-mail palsu

Jika mendapatkankan email yang seakan-akan dari pengelola website bisnis internet atau e-gold yang ikuti dan meminta untuk mengirimkan username dan password , jangan hiraukan dan segera hapus email tersebut, jangan klik link apapun yang ada dan jangan buka attachment yang disertakan, pihak pengelola bisnis internet dan e-gold tidak pernah mengirim email semacam itu.

5. Kesimpulan

Penerapan dan persiapan yang matang dalam membangun suatu keamanan Jaringan komputer sangat dibutuhkan yang bertujuan untuk mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasikan kemungkinan perusakan tersebut. Membangun sebuah keamanan sistem harus merupakan langkah-langkah yang terintegrasi pada keseluruhan subsistemnya, dengan tujuan dapat mempersempit atau bahkan menutup adanya celah-celah unauthorized actions yang merugikan. Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya menuju ke tahap pengamanan fisik dan pengamanan data. Pengaman akan adanya penyerangan sistem melaui jaringan juga dapat dilakukan dengan melakukan pengamanan FTP, SMTP, Telnet dan pengamanan Web Server.

Daftar Pustaka

Ariyus. D. (2007). *Intrusion Detection System*, Andi Yogyakarta. Yogyakarta,.

Babys, Jemi Yohanis., Kusrini. and Sudarmawan., (2013). "ANALISIS ASPEK KEAMANAN INFORMASI JARINGAN KOMPUTER (Studi Kasus: STIMIK Kupang)". Seminar Nasional Informatika 2013 (semnasIF 2013) UPN "Veteran" Yogyakarta, ISSN: 1979-2328, E-7 – E14.

Dony . I., (2007)."Intrusion Detection System", ANDI, Yogyakarta.

Edhy. S. (2005). "*Komunikasi Data Dan Jaringan Komputer*", Graham Ilmu, Yogyakarta,

Junior, Dkk, (2009). Perancangan Intrusion Detection System pada Jaringan Nirkabel BINUS Universitas, Jakarta.

Lukas. T. (1995) ."*Jaringan Computer*".PT. Alex Media Komputindo, Jakarta.

Nugraha, M. Satria. (2010) "Implementasi Intrusion Detection System untuk Filtering Paket Data", *Skripsi Program S1 Teknik Informatika Universitas Islam Negeri*, Jakarta,.

Putri. L. (2011)."Implementasi Intrusion Detection System (IDS) menggunakan Snort pada jaringan Wireless", *Skripsi Program S1 Teknik Informatika Universitas Islam Negeri*, Jakarta.

Pawar, M.V. and Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, pp.503-506

Sopandi. D. (2008) *Instalasi dan Konfigurasi Jaringan Komputer*. Informatika Bandung, Bandung.

Sukamaaji, Anjik dan Riant, (2008). *Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan*, Andi Yogyakarta, Yogyakarta.