ANALISA CARA KERJA DAN DAMPAK DARI SERANGAN VIRUS SPYWARE

RUDI HERMAWAN
Program Studi Teknik Informatika, Universitas Indraprasta PGRI
Email: Wowor99@gmail.com

Abstrak

Dunia internet merupakan jaringan global yang dipublikasikan kepada umum. Didalam internet ditemukan berbagai macam tindakan positif dan negative. Kalau berbicara dalam jaringan pada internet, lalu lintas informasi sudah sangat cepat. Jaringan internet masa sekarang sudah semakin mutakhir, Maka perlu keamanan untuk mengantisipasi perbuatan negative di internet. Salah satunya dengan berhati-hati dan bijak dalam mengambil aplikasi dari internet dan selalu menjaga kerahasiaan, serta menggunakan Anti Virus untuk membentengi sistem komputer untuk mencegah terjadi sesuatu yang tidak di inginkan pada saat sedang melakukan aktifitas yang terkoneksi dengan internet, seperti menyusupnya virus-virus seperti *adware*, *spyware*, *malware*, dan lainnya kedalam komputer kita dan mengawasi aktifitas surfing kita di dunia Internet. Virus *spyware* merupakan program yang dibuat untuk memata-matai komputer korbannya. Bila sudah terinfeksi virus *spyware* sudah tidak ada rahasia lagi dalam komputer korban. Dalam percobaan spyware menggunakan aplikasi Vmware akan membuat dua komputer virtual. komputer pertama sebagai penyerang dan satu lagi menjadi target serangan *spyware*. Dua komputer virtual diciptakan menggunakan aplikasi vmware. Penyerang menggunakan sistem operasi backtrack untuk menyerang target, sedangkan target korban menggunakan sistem operasi windows. Aktifitas dari komputer target yang terkena virus *spyware* terlihat segala aktifitasnya bisa dipantau, dikontrol bahkan bisa juga di ambil alih kewenangan sistemnya.

Kata kunci :*virus spyware, vmware, komputer virtual, backtrack, windows.*

Pendahuluan

Kemajuan teknologi internet membawa banyak keuntungan, khususnya untuk masyarakat secara luas dimana kini teknologi dapat dinikmati oleh hampir seluruh elemen masyarakat tanpa adanya batasan wilayah, waktu dan juga penggunanya. Jauh berbeda dengan dulu dimana teknologi hanya bisa dinikmati oleh mereka yang memiliki "dompet tebal". Bayangkan awal tahun 2000 pengguna internet di Indonesia masih sedikit dan bisa dihitung jari, dengan harga nya yang cukup mahal dibandingkan dengan sekarang.Tentu ini membawa sebuah perbedaan dengan kondisi sampai sekarang. Perkembangan teknologi internet baik aplikasi perangkat *device* untuk penggunanya ikut berkembang sangat pesat di negeri ini. Namun perkembangan ini belum dilengkapi dengan kesadaran dan kemampuan yang baik dari pengguna dalam melakukan aktifitasnya didunia *cyber.* Hal tersebut menjadi celah bagi para pelaku yang iseng maupun yang jahat untuk melakukan aksi mata-matai dari aktifitas komputer yang menjadi targetnya.

Fenomena *video clip* gadis mabuk di facebook pernah mewabah dan menjangkiti banyak user. Banyak dampak buruk yang terjadi dari video seronok tersebut. Pengguna facebook yang terkena *tag* pun menjadi risih dan malu di akun facebooknya berisi video seronok. Dampak lebih buruk akan terjadi bila pengguna mengklik video seronok tersebut. Bersiaplah komputer akan dimata-matai oleh penyusup karena *file* video itu berisi script program virus *spyware* yang akan aktif bila dihit oleh calon korban.

Tujuan Penelitian

Memberikan pemahaman dan informasi mengenai virus *Spyware* yang merupakan program jahat dirancang untuk mengintip maupun mencuri data-data pribadi milik korbannya. Virus *Spyware* ini menjadi lebih berbahaya kalau dibuat dengan tujuan mencari uang. Kecerobohan dalam menggunakan aplikasi-aplikasi ataupun berselancar di dunia maya mempunyai tingkat resiko yang tinggi terkena *spyware.*

Manfaat Penelitian

Dengan mengenal dan mengetahui cara kerja virus *spyware* diharapakan menjadi lebih bijak dan berhati-hati dalam mencari aplikasi di internet untuk di download dan harus perhatikan baik-baik setiap *pop up* yang muncul karena *pop up* tersebut bisa menjadi *kamuflase* bagian dari virus *spyware*. Dengan sikap hati-hati ini dapat meminimalkan resiko terkena serangan virus spyware.

Tinjauan Pustaka

Keamanan komputer merupakan hal yang sangat penting untuk diperhatikan dalam pesatnya perkembangan dunia internet. Dunia Internet merupakan jaringan global yang dipublikasikan kepada umum. Didalam internet dapat ditemukan berbagai macam tindakan positif dan negative. (S'To, 2004). Dalam jaringan internet lalu lintas informasi sudah sangat cepat. Jaringan internet pada masa sekarang sudah semakin mutakhir, maka perlu keamanan untuk mengantisipasi perbuatan negative yang ada pada jaringan internet (Amperiyanto Tri 2009). Dengan selalu berhati-hati dan bijak dalam menyerap dan mengambil sesuatu dari internet dan selalu untuk menjaga kerahasiaan, serta selalu menggunakan Anti Virus untuk membentengi sistem komputer kita dan teknik-teknik lainnya untuk mencegah terjadi sesuatu yang tidak di inginkan pada saat sedang melakukan aktifitas yang terkoneksi dengan internet, seperti menyusupnya virus-virus seperti adware, *spyware*, *malware*, dan lainnya kedalam komputer kita dan mengawasi aktifitas surfing kita di dunia Internet.

Definisi

Virus adalah suatu aplikasi yang dapat mereplikasi diri dalam suatu jaringan komputer, bersifat merusak dan memiliki kemampuan untuk menginfeksi file lain menjadi memiliki sifat-sifat yang sama seperti dirinya. Virus akan mengubah ukuran program yang terinfeksi tanpa mengubah tanggal modifikasi suatu aplikasi. Sudah sering kita mendengar mengeluhkan kinerja komputernya karena kinerja komputernya yang "lambat". Sering pula kita dengar protes atau sekadar omelan kekesalan pengguna komputer karena menumpuknya iklan *pop-up* yang tiba-tiba saja muncul saat sedang *Surfing* di internet. *Pop-up* yang muncul tanpa disadari oleh pengguna komputer disebabkan oleh program yang berhasil di-*install* dengan tujuan untuk mengamati aktivitas komputer secara rahasia. Lebih terkenal dengan sebutan *spyware*. Hasilnya seperti yang sudah banyak diketahui dan sangat mengganggu.

Virus *spyware* merupakan *script* program komputer yang dibuat untuk memata-matai komputer korbannya. Awalnya virus *spyware* ini digunakan untuk memata-matai profil pengguna komputer dan penggunaannya dalam menampilkan iklan yang sesuai dengan minat pengguna komputer tersebut. Bila korban sudah terinfeksi virus *spyware* ini sudah tidak ada rahasia lagi dalam komputernya karena penyusup berhasil memantau segala aktifitas dari korban.

VMware merupakan software virtualisasi yang bisa digunakan untuk membuat *virtual machine.* Dengan Aplikasi Vmware ini bisa melakukan percobaan dengan menggunakan sistem OS apapun mulai dari windows, mac, linux, *install mikrotik di vmware* dan lain sebagainya. VMware dapat menjalankan banyak sistem operasi atau OS dalam satu PC atau laptop. Keuntungan melakukan percobaan dengan aplikasi Vmware yang lainnya adalah bisa bereksperimen tanpa harus takut kerusakan atau kehilangan pada OS utama.

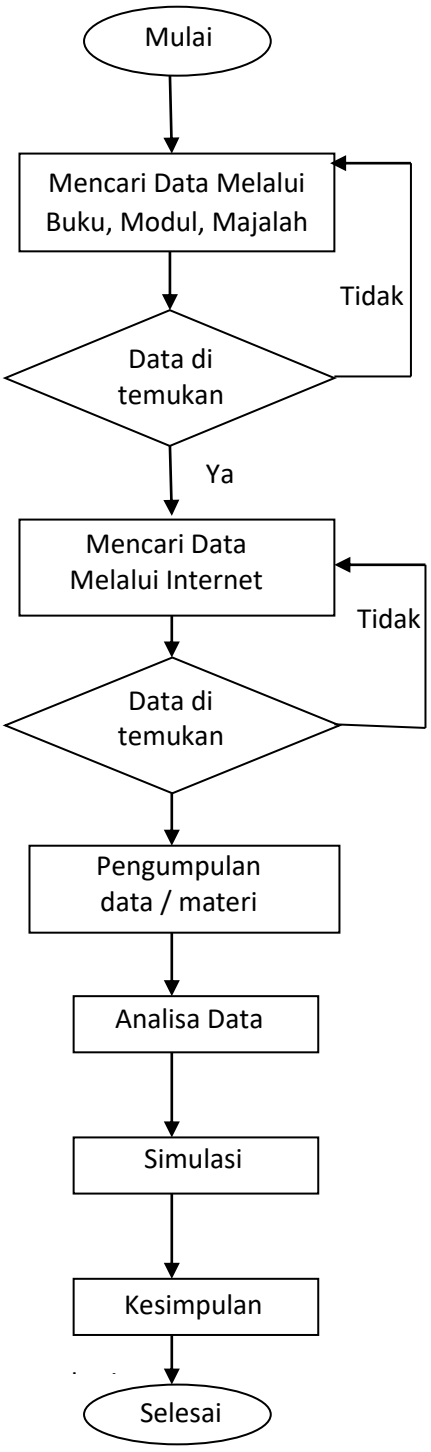
Backtrack merupakan salah satu Sistem Operasi Linux yang didasari dari *resourcedebian*, namun kini backtrack telah di modifikasi menjadi alat perang di dunia maya, baik itu aksi *hacking*, *cracking* dan kejahatan kriminal dunia maya lainnya, linux backtrack sangat populer dari awal *release* dia buat, kini backtrack banyak dipakai di kalangan para linuxer, untuk melatih kemampuan mereka, dengan mengandalkan *tools* pentes yang telah di sediakan oleh linux backtrack itu sendiri, apa yang terbaru release backtrack 5 R3 ini, penambahaan 60 *tools* pentes, kemudian perbaikan *bug* yang terdapat di versi *release* sebelumnya di backtrack 5 R3. Backtrack, penemunya adalah Mati Aharoni dan Max Mosser. Mati Aharoni adalah seorang konsultan sekuriti,

Window 7 merupakan salah satu sistem operasi yang dibuat oleh perusahaan Microsoft windows yang mana untuk menggantikan windows sebelumnya, yaitu Windows vista, dan windows 7 itupun sendiri dirilis untuk Perusahaan Microsoft pada tanggal 22 juli tahun 2009. Yang mana Windows 7 itu dirilis kurang dari 3 tahun setelah Windows vista. Windows 7 di *install* pada salah satu komputer virtual yang diposisikan sebagai target korban dari penetrasi mengunakan serangan *spyware*.

Metodologi Penelitian

Penelitian ini bersifat kajian pustaka atau *library research*. Data yang diperoleh paparkan secara deskriptif yang disertai dengan analisis sehingga menunjukkan suatu kajian ilmiah yang dapat dikembangkan dan diterapkan lebih lanjut.Materi Penelitian ini juga bersumber dari website, buku dan berdasarkan pengalaman yang secara langsung berurusan dengan *Spyware*, beserta sample pembuatan *Spyware* yang akan di cantumkan di akhir bab sebagai daftar pustaka.

Kerangka Pemikiran



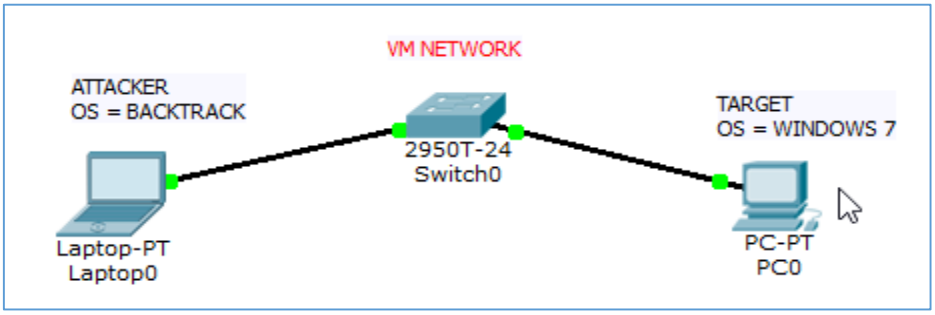
Gambar 1. Kerangka Berfikir Penelitian Virus *Spyware*

Hasil dan Pembahasan

Untuk mengetahui secara rinci cara kerja dan dampak dari serangan virus *spyware* ini aktifitas percobaan dilakukan dengan menciptakan dua komputer virtual yang satu komputer virtual bertindak sebagai penyerang dan satu lagi komputer virtual diciptakan target dari serangan *spyware*. Dua komputer virtual tersebut diciptakan menggunakan aplikasi vmware versi 10. Komputer virtual penyerang menggunakan sistem operasi backtrack 5 R3 untuk menyerang target, sedangkan komputer virtual sebagai target korban menggunakan sistem operasi windows 7.

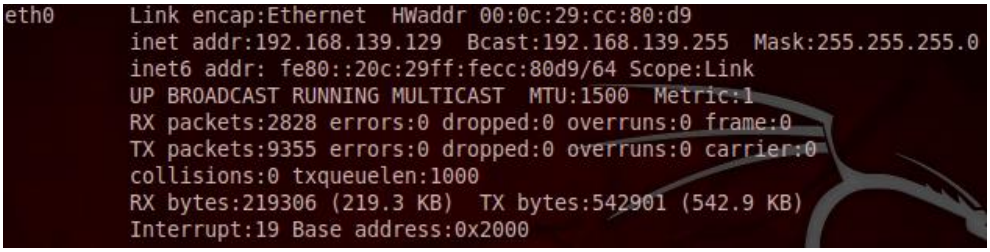
Simulasi

Dalam melakukan aksi peneterasi dalam simulasi ini komputer penyusup mengumpulkan informasi sebanyak-banyaknya dari komputer korban dengan teknik footprint baru sesuaikan menggunakan jalan masuk yang mana dan menggunakan teknik yang tepat untuk melumpuhkan targetnya. Dalam percobaan *spyware* ini Vmware akan membuat dua komputer virtual seperti terlampir pada gambar dibawah ini.



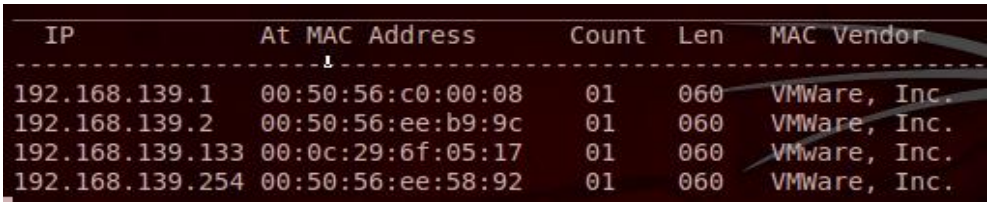
Gambar 2. Rancangan Komputer Penyerang dan Komputer Target Korban

Langkah awal sebelum melakukan peneterasi ke target adalah dengan footprint mencuri untuk mendapatkan informasi dari target komputer target yang terhubung dalam satu jaringan dengan.



Gambar 3. Informasi IP Address dari Penyerang

Untuk mendapatkan informasi yang lebih detil tentang ip *address* yang terkoneksi aktif dalam satu jaringan dengan target perlu dilakukan *scanning network*, hasilnya seperti dibawah ini



Gambar 4. Hasil dari Network Mapping

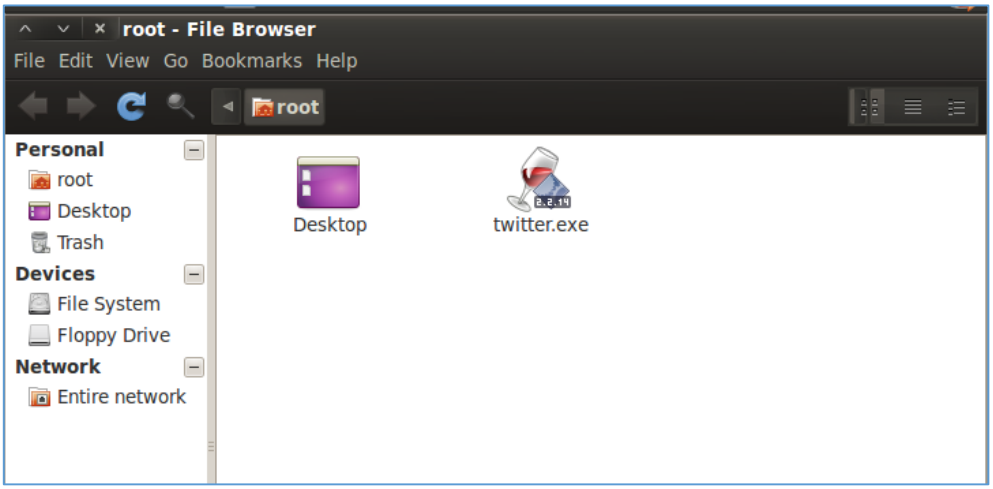
Informasi dari target sudah didapat saatnya aktifitas penetrasi mulai dilakukan oleh penyerang dengan menggunakan teknik *exploit multi handler*, teknik ini digunakan untuk menghasilkan target serangan yang semua informasi pentingnya nanti tetap dapat dimonitoring dan di kendalikan oleh penyerang.

Gambar 5. Teknik *Exploit Multi Handler*

Saatnya pembuatan satu file virus *spyware* memanfaatkan keuggulan dan kemudahan dari tool msfpayload, msfencode, msfvenom yang dimiliki oleh konsol backtrack5 R3. Dengan *tools* tersebut file yang dihasilkan menjadi satu buah ancaman baru bagi korban selain berfungsi sebagai virus *spyware*, file tersebut bisa menjadi jalan masuk pintu belakang (backdoor) bagi para penyerang untuk melumpuhkan target korban. Untuk mengelabuhi korban agar korban tidak mengetahui file yang dikirim adalah virus, maka dibuat penamaan file yang tersamarkan *kamuflase name.*

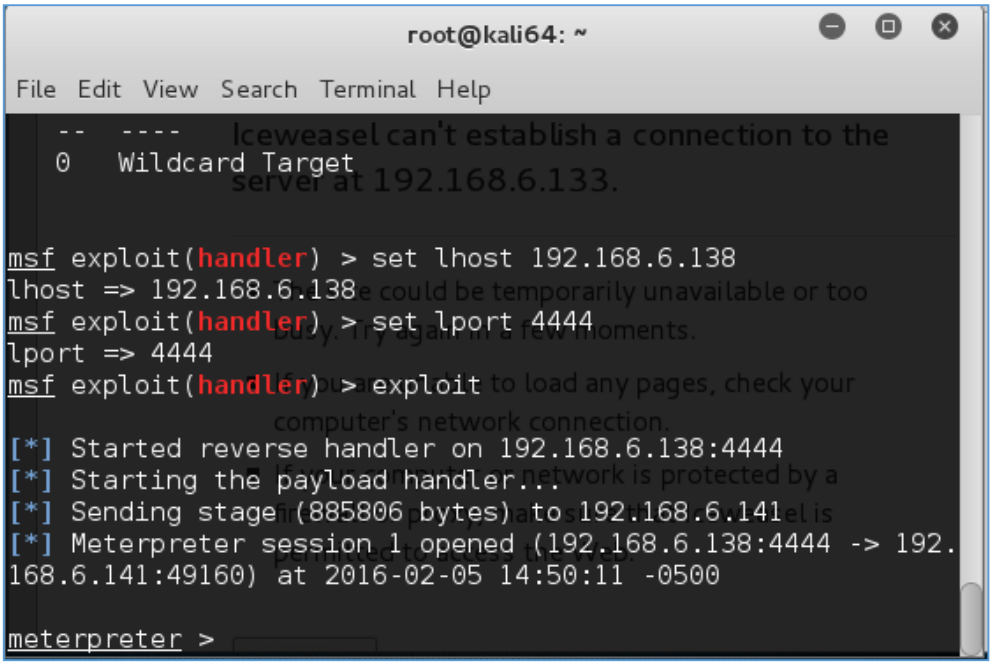
Gambar 6. Proses Pembuatan File *Spyware*

Proses pengambilan file dan proses pengiriman file *spyware* ke komputer target bisa memanfaatkan share dokumen bisa juga memanfaatkan email maupun aplikasi media sosial seperti facebook, twitter, path, dll.



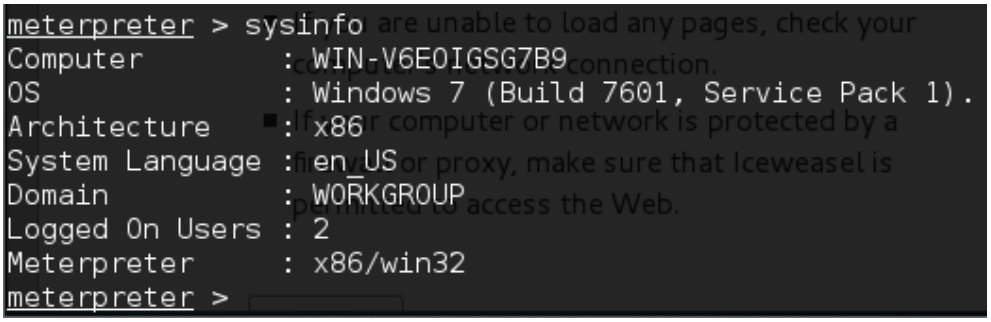
Gambar 7. Proses Pengiriman Virus *Spyware* ke Target

Setelah proses pengiriman berhasil penyerang mengaktif *handler* untuk menunggu respon dari file *spyware* pada saat ada penekan aktif dari user korban maka *handler* di komputer korban akan aktif layaknya sebuah detonator yang akan aktif menunggu *handler* pemicu dari file *spyware*



Gambar 8. Handler Aktif Konsol di Penyerang Berubah Menjadi Meterpreter

Konsol meterpreter merupakan konsol kesukaan dari banyak penyusup untuk mengambil session dari komputer yang menjadi targetnya. Dengan konsol ini penyusup sudah bisa masuk kedalam sistem windows 7 dari target korban dan dapat melakukan banyak aktifitas mata-mata dari komputer korban,



Gambar 9. Session Korban Sudah Dimasuki oleh Penyerang

Implikasi

Dampak dari komputer yang terserang virus *spyware* semua aktifitas dalam menggunakan komputer sudah dimonitor oleh pelaku penyerang karena penyerang punya banyak cara untuk mengendus aktifitas dari korban. Aktifitas yang dapat di monitor antara lain:

1. *Keylogger* atau Perekam ketikan merupakan sebuah *tools* yang digunakan untuk memantau penekanan tombol papan ketik. Sebuah perekam ketikan biasanya akan menyimpan hasil pemantauan penekanan tombol papan ketik tersebut ke dalam sebuah berkas cecatat (*log file*). Beberapa perekam ketikan tertentu bahkan dapat mengirimkan hasil rekamannya ke surel tertentu secara berkala. *Keylogger* dapat digunakan untuk kepentingan yang baik atau bahkan bisa digunakan untuk kepentingan yang jahat. Kepentingan yang baik antara lain untuk memantau produktivitas karyawan, untuk penegakan hukum dan pencarian bukti kejahatan. Kepentingan yang buruk antara lain pencurian data dan *password*.
2. *Snapshoot*, dengan *tools* ini penyusup dapat merekam dalam bentuk gambar segala aktifitas kegiatannya di depan komputer. Aktifitas tersebut seperti meng *capture* atau *screenshot* segala aktifitas komputer target.
3. Videocam, fitur yang dapat menampilkan aktifitas pengguna secara citra/gambar bergerak secara real time yang dikendalikan oleh penyusup. Disini penyusup dapat melihat aktifitas pengguna dari target korban secara live.
4. Remote login, fitur yang memungkinkan penyusup dapat mengakses (login) ke sebuah target host. dengan memanfaatkan remote login, penyusup dapat mengoperasikan sebuah komputer korban dari jarak jauh.

Solusi Penanggulangan

Untuk menanggulangi ancaman virus *spyware* dapat menggunakan perangkat anti-*spyware* untuk melindungi komputer dari jenis ancaman ini. *Spybot* adalah salah satu contohnya dan perangkat ini bekerja dengan sangat baik dalam mengidentifikasi dan menghapus tipe-tipe *malware* tertentu yang sering tidak dihiraukan oleh program anti-virus. Namun, seperti program anti-virus lainnya, sangat penting untuk selalu meng-update definisi *Spybot's* dan melakukan pemindaian rutin.

Simpulan dan Saran

Simpulan

Dari pembahasan di atas dapat di ambil kesimpulan bahwa *Spyware* adalah program jahat yang dirancang untuk mengintip maupun mencuri data-data pribadi milik korbannya. Data-data ini seperti nomor kartu kredit, password atau data-data penting kita yang nantinya akan mereka gunakan untuk keperluan yang tidak bertanggung jawab. *Spyware* menjadi lebih berbahaya karena biasanya dibuat dengan tujuan mencari uang.Kecerobohan dalam menggunakan aplikasi-aplikasi ataupun berselancar di dunia maya mempunyai tingkat resiko

yang tinggi terkena *spyware*. Bijak dan berhati-hati dalam mencari file untuk di download perhatikan baik-baik setiap *pop up* yang muncul bila tidak yakin dengan kondisi *pop up* tersebut yang terbaik mengklik tombol close. Dan waspada terutama situs-situs porno karena penyebaran virus yang terbanyak di area situs yang mengandung konten pornografi.

Saran

Untuk mencegah terjangkitnya virus *spyware* ini ada beberap tips yang disarankan kepada pengguna komputer ataupun perangkat mobile yang hobi berselancar di dunia maya beberapa saran ini antara lain :

1. Jangan pernah menerima dan menjalankan konten jenis apapun jika datang dari situs yang anda tidak ketahui dan tidak dipercaya.
2. Menginstall aplikasi anti *spyware* seperti spybot untuk meminimalisir terjadinya pengintaian pada komputer anda.
3. Tingkatkan keamanan browser dengan mencegahnya menjalankan program yang mungkin berbahaya secara otomatis, yang terkadang terdapat dalam laman web. Jika menggunakan Mozilla *Firefox*, anda dapat menginstal tambahan *NoScript*.

Daftar Pustaka

Amperiyanto Tri (2002). *Buku Suci Trojan The Client*. Jakarta: Elex Media Komputindo

Fringki Firmansyah (2014). *Sistem Operasi Linux Backtrack*. Diakses dari https://firmansah93.wordpress.com/2014/03/09/sistem-operasi-linux-backtrack/

Hermawan Rudi (2015). *Modul Network Security*. Jakarta: G-Inova.

Indonesia Cyber Army. (2002). *Tools Hacking*. Diakses dari http://indocyberarmy.blogspot.co.id/2012/12

Tactical Technology Collective and Front Line Defenders (2011). Cara *melindungi komputer dari Spyware* . Diakses dari https://securityinabox.org/id/chapter_1_2

S'to,(2004). *Seni Teknik Hacking Uncensored*. Jakarta: Jasakom.