BAB III

PENYADAPAN DATA PRIBADI PENGGUNA INTERNET YANG DILAKUKAN MELALUI MONITORING AKTIVTAS KOMPUTER

A. Pihak-Pihak yang Terkait Dalam Penyadapan Data Pribadi Pengguna Internet

Pemanfaatan teknologi komputer pada saat ini telah mendorong pertumbuhan bisnis yang sangat pesat, karena berbagai informasi dapat disajikan dengan canggih dan sangat mudah diperoleh. Melalui hubungan jarak jauh dengan memanfaatkan teknologi maka dapat digunakan untuk melakukan suatu transaksi bisnis. Pihak-pihak yang terkait dalam transaksi bisnis tidak harus bertatap muka, cukup melalui peralatan komputer dan telekomunikasi, maka transaksi bisnis akan berlangsung sama seperti transaksi bisnis biasa yang dilakukan secara bertatap muka. Kondisi yang demikian merupakan pertanda dimulainya era siber dalam bisnis.

Dampak positif tersebut tidak selalu berlangsung demikian, di sisi lain timbul pihak-pihak lain yang dengan itikad tidak baik mencari keuntungan dengan melawan hukum, yang berarti melakukan pelanggaran dan kejahatan[15].

[15]*Heru Soepratmo, Kejahatan Komputer dan Siber Serta Antisipasi Pengaturan Pencegahannya di Indonesia, http://solusihukum.com, Diakses pada tanggal 05 Juli 2010 pukul 14:29 WIB*

Penyalahgunaan komputer dalam perkembangannya menimbulkan permasalahan yang sangat rumit, diantaranya proses pembuktian atas suatu tindak pidana (faktor yuridis). Terlebih lagi penggunaan komputer untuk tindak pidana ini memiliki karakter tersendiri atau berbeda dengan tindak pidana yang dilakukan tanpa menggunakan komputer (konvensional). Perbuatan atau tindakan, pelaku dan alat bukti dalam tindak pidana biasa dapat dengan mudah diidentifikasi, tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer[16].

Semakin banyaknya penyedia jasa internet dan semakin terjangkaunya biaya untuk mengakses internet, membuat semakin banyak orang mulai mengenal internet dan menggunakannya[17]*. internet atau disebut juga dengan cyberspace, pada saat ini dapat dikatakan sebagai suatu sarana yang dibutuhkan oleh banyak orang, baik digunakan untuk berkomunikasi, sekedar mencari informasi, hingga digunakan untuk melakukan transaksi bisnis. Karena tingginya kebutuhan manusia akan internet maka semakin banyak juga orang yang menyalahgunakan sarana tersebut. Hingga saat ini kasus-kasus kejahatan internet atau disebut juga dengan cybercrime semakin banyak bermunculan, dengan jenis-jenis kejahatan baru yang sulit untuk diidentifikasi.*

Penyadapan yang dilakukan oleh seseorang yang tidak bertanggung jawab untuk mencuri data dari pengguna internet merupakan salah satu bentuk cybercrime karena seseorang yang tidak bertanggung jawab tersebut telah melewati batas-batas haknya dengan memasuki wilayah pribadi orang

---

[16]*Puspita Dewi, Tindak Pidana Penipuan Untuk Memperoleh Informasi Personal (Phising) Melalui Pengiriman E-Mail, Unikom, 2008*

[17]*Ibid, Hlm 41*

lain. Penyadapan biasanya dilakukan dengan menggunakan program-program atau software yang diaplikasikan pada komputer. Banyak software yang di buat secara khusus untuk melakukan penyadapan dalam jaringan komputer. Salah satu program yang sering digunakan untuk melakukan penyadapan itu dinamakan dengan istilah sniffing tools atau jika diterjemahkan dalam bahasa Indonesia berarti alat pemantau jaringan, dimana software yang telah diaplikasikan pada sebuah komputer yang terhubung dengan suatu jaringan, maka komputer dengan aplikasi tersebut dapat memantau komputer-komputer yang terhubung dalam suatu jaringan.

Teknik umum yang biasa dilakukan oleh seseorang untuk menyadap data pribadi pengguna internet dengan menggunakan progaram sniffing tools yaitu dengan cara memantau suatu jaringan komputer dimana dalam satu jaringan komputer tersebut terhubung dengan banyak komputer, korban biasanya tidak sadar bahwa aktivitasnya di dalam internet sedang disadap oleh orang lain. Pada dasarnya pelaku memanfaatkan ketidak hati-hatian dari pengguna internet, dengan tujuan untuk mencuri informasi pribadi dari pengguna internet seperti informasi pribadi yang dikirim melalui email, dan data pribadi seperti username dan password dari sebuah website yang dimiliki oleh pengguna internet.

Pihak-pihak yang terkait dalam penyadapan data pribadi pengguna internet diantaranya yaitu :

1. *Sniffer adalah pelaku penyadapan. Sniffer menggunakan program sniffing tools yang beragam jenis karakternya dan sangat mudah didapatkan dengan cara mengunduhnya melalui internet. Sniffing*

tools yang terkenal dan biasanya digunakan oleh sniffer antara lain yaitu etheral, tcpdump, ettercap, dsniff, etherpeak, airopeak dan lain-lain[18].

2. *Netter adalah pengguna internet. Dalam hal ini adalah korban penyadapan yaitu pengguna internet.*

Pada kenyataannya, masih sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas penyadapan ini. Yang lebih menakutkan lagi, biasanya pelaku penyadapan melakukan sniffing di tempat-tempat rawan, misalnya yaitu seorang karyawan yang melakukan sniffing di perusahaan tempat dia bekerja, atau seorang pengunjung warung internet melakukan sniffing untuk mencuri password email, bahkan mencuri data transaksi bank melalui kartu kredit.

Pada awalnya program sniffing seperti etheral, tcpdump, ettercap, dsniff, etherpeak, airopeak dan lain sebagainya digunakan dengan tujuan yang positif, yaitu untuk mempertahankan jaringan dan sistem agar dapat bekerja secara normal. Biasanya sniffing tools digunakan sebagai asisten manajemen jaringan untuk memonitor dan sebagai fitur analisis yang dapat membantu memecahkan masalah jaringan, mendeteksi intrusi, control atau pengawasan jaringan konten[19].

---

[18]*Neonmap, Op.Cit Active Sniffing Detector (ARP Spoofing) with Artificial Neural Network Method, http://www.jasakom.com.*

[19]*Vega Valentine, Anne Yuliyanti, Bertalya, Adopsi Enkripsi Jefferson Wheel pada Protokol One-Time Password Authentication untuk Pencegahan Sniffing pada Password E-mail, Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010) Yogyakarta, 19 Juni 2010.*

Namun seiring perkembangan teknologi, perangkat lunak seperti ini mulai dikembangkan untuk kegunaan yang negatif, yaitu untuk mengambil data dan informasi rahasia pengguna internet yang tidak terenkripsi selama data dan informasi user tersebut melintasi suatu jaringan komputer. Selain itu, penggunaan negatif sniffing tools yang merugikan untuk keamanan jaringan antara lain[20]:

a. *Penangkapan sandi, yang merupakan alasan utama untuk sebagian besar penggunaan sniffing tools secara illegal.*
b. *Menangkap informasi, transakasi khusus dan bersifat pribadi seperti username, kartu kredit, rekening dan password.*
c. *Merekam email atau pesan instan dan melanjutkannya.*
d. *Beberapa sniffing tools bahkan dapat mengubah informasi target sistem komputer dan menyebabkan kerusakan.*
e. *Merusak keamanan jaringan untuk mendapatkan otoritas akses yang lebih tinggi.*

Target sniffers adalah kecerobohan dan ketidaktelitian para pengguna jasa situs-situs yang tersedia di internet seperti situs jual-beli online, internet banking, online shopping, game online dan yang paling sering menjadi korban dari sniffers pada saat ini yaitu situs jejaring sosial yang pada saat ini sangat digemari oleh banyak pengguna internet[21].

---

[20] *Loc. Cit*

[21] *Neonmap, Op.Cit Active Sniffing Detector (ARP Spoofing) with Artificial Neural Network Method, http://www.jasakom.com.*

Contoh kasus penyadapan yang sering dialami oleh pengguna internet pada saat ini adalah penyadapan terhadap akun dari pengguna internet dalam situs jejaring sosial. Situs jejaring sosial pada saat ini menjadi suatu trend baru yang digunakan oleh masyarakat untuk berkomunikasi dengan orang lain baik yang sudah kenal seperti saudara, teman atau rekan bisnis, bahkan orang yang baru dikenal dalam situs jejaring sosial itu sendiri.

Layanan yang diberikan oleh situs jejaring sosial pada saat ini sangat membantu seseorang dalam melakukan aktifitasnya mulai dari berkomunikasi, mencari hiburan seperti memainkan aplikasi permainan yang disediakan oleh situs jejaring sosial itu sendiri, melakukan promosi suatu produk hingga transaksi bisnis pun dilakukan dalam situs jejaring sosial tersebut. Kemudahan inilah yang membuat masyarakat menjadi sangat tertarik untuk memiliki akun dalam situs jejaring sosial tersebut.

Metode yang dilakukan oleh sniffers untuk menyadap pengguna situs jejaring sosial yaitu dengan cara memantau data-data pemilik akun dalam situs jejaring sosial yang melewati suatu jaringan, kemudian data tersebut diterjemahkan kembali oleh sniffers dengan suatu software khusus sehingga data-data pemilik akun jejaring sosial tersebut dapat terbaca oleh sniffers.

Pentingnya akun situs jejaring sosial yang dimiliki pengguna internet membuat akun situs tersebut menjadi sangat berharga dan mempunyai nilai ekonomis contohnya yaitu, Zynga Texas Holdem Poker yang merupakan salah satu aplikasi permainan dalam suatu situs jejaring sosial yang dimainkan dengan mempertaruhkan chips atau disebut juga dengan uang virtual yang sudah disediakan oleh aplikasi permainan tersebut sangat

dibutuhkan oleh pengguna aplikasi tersebut agar dapat memainkan aplikasi permainan tersebut, sehingga banyak dari pengguna aplikasi permainan tersebut mencari cara cepat untuk mendapatkan chips yaitu dengan membelinya pada sesama pengguna aplikasi permainan tersebut dengan harga yang telah ditentukan. Hal ini membuat akun seseorang menjadi sangat berharga dan mempunyai nilai ekonomis bagi pemiliknya. Pengguna internet yang demikianlah yang menjadi salah satu sasaran dari penyadapan yang dilakukan oleh sniffers untuk mencuri seluruh data dan akun jejaring sosialnya tersebut untuk mengambil chips atau disebut juga uang virtual yang mempunyai nilai ekonomis.

Berdasarkan fakta yang ada pada saat ini, dalam satu hari terjadi beberapa pencurian terhadap akun situs jejaring sosial. Korban umumnya tidak terlalu paham mengenai dunia internet[22]*. Berdasarkan keterangan dari seorang pengguna internet yang sering memainkan aplikasi permainan dalam situs jejaring sosial, penyadapan dengan program sniffing tools yang terjadi khususnya di kota Makassar semakin meningkat dengan drastis. Dengan metode pengamanan jaringan standar yang diaplikasikan pada notebook kemudian menginstal aplikasi anti sniffing dari Microsoft yang bernama Promqry 1.0, kemudian memantau ke beberapa host yang mencurigakan maka terlihat dalam alamat IP (internet protocol address) dalam notebook sudah banyak dijejali dengan serangan Sniffer*[23]*. Hal tersebut membuktikan tingginya kasus penyadapan yang terjadi yang dilakukan oleh pihak yang tidak berkepentingan untuk mencuri data dari*

[22]*Ibid, Hlm 44*

[23]*Neonmap, Op. Cit, Active Sniffing Detector (ARP Spoofing) with Artificial Neural Network Method.*

pengguna internet. Semakin meningkatnya kasus kejahatan internet pada saat ini sudah sangat meresahkan pengguna internet.

Kasus lainnya yaitu tertangkapnya seorang cracker yang berasal dari Indonesia yang bernama Wenas Agusetiawan yang berumur 15 tahun di Singapura. Kasus ini terjadi pada tahun 2000. Wenas yang menggunakan inisaial nama Hantu Crew (HC) di dalam dunia maya didakwa telah melakukan aktivitas ilegal pada perusahaan Data Storage Institute (DSI) Singapura. Wenas ditangkap setelah melakukan penyusupan pada server DSI dengan cara mencari celah kosong sebagai jalan masuk pada jaringan server dengan menggunakan program aplikasi komputer (software) yang dibuat khusus untuk mendeteksi kelemahan keamanan komputer yang terhubung dengan jaringan tersebut. Tindakan yang dilakukan oleh Wenas Agusetiawan tersebut mengakibatkan kerugian terhadap perusahaan DSI tersebut diantaranya yaitu bocornya rahasia perusahaan, kerusakan pada server perusahaan tersebut, dan tercurinya data-data pribadi milik perusahaan tersebut, disamping dampak-dampak lainnya yang mengakibatkan kerugian pada perusahaan[24]*.*

Berikut petikan berita yang ditulis oleh Donny BU yang meliput langsung persidangan Wenas tersebut. Saat hadir di persidangan Pengadilan Rendah Singapura divisi Juvenile Court, terdakwa Wenas didampingi oleh kedua orang tuanya. Bahkan pihak Kedutaan Besar Republik Indonesia (KBRI) menugaskan Thony Saut P. Situmorang (second secretary) dan A.Guntur Setyawan (third secretary) dari bidang konsuler untuk hadir di

[24]*Detikcom, Hacker Indonesia di Singapura, http //groups.yahoo.com/group /berita-it/message/5517, Diakses pada 06 Desember 2010 pukul 05:30 WIB*

persidangan. Persidangan dilaksanakan pada hari Kamis tanggal 20 juni 2000 pukul 10.15 waktu Singapura, dalam bahasa Inggris. Dalam persidangan tersebut, bertindak selaku hakim adalah hakim Mark Tay dan sebagai penuntut umum adalah jaksa Chew. Sedangkan pengacara yang mendampingi terdakwa adalah Mimi Oh. Hadir pula dalam persidangan tersebut Mark Koh, Investigation Officer Computer Crime Branch CID (Criminal Investigation Department) Singapura sebagai investigator dan yang menyusun statement of Facts (SOF) yang berisi kronologis lengkap tindakan terdakwa, mulai dari laporan korban, penahanan, hasil investigasi, fakta kasus hingga kerugian korban. Statements of Facts atau SOF yang bernomor D/000603/001/D tersebut merupakan bahan rujukan bagi jaksa Chew dalam mengajukan tuntutannya.

Akibat tindakan Wenas yang masih berumur 15 tahun yang telah melakukan aktivitas ilegal terhadap dua server perusahaan Singapura, berdasarkan SOF yang disusun oleh Mark Koh, terdapat 16 buah tuntutan yang merupakan tuntutan untuk setiap aktivitas yang dilakukan oleh terdakwa secara ilegal pada dua buah server perusahaan Singapura tersebut, baik yang dilakukannya sewaktu masih di Australia maupun setelah mendarat di Singapura. Hingga persidangan selesai, belum dapat diambil keputusan mengenai kasus tersebut. Baik hakim, penuntut umum maupun pengacara terdakwa sama-sama membutuhkan waktu tambahan untuk mempelajari kasus tersebut. Karena Pengadilan Rendah Singapura baru pertama kali menghadapi kasus cybercrime yang melibatkan warga negara asing. Akhirnya pada sidang akhir ditetapkan bahwa terdakwa dikenai hukuman

denda senilai Rp 150 juta. Tidak dijelaskan secara rinci mengenai pasal-pasal yang dilanggar[25].

Kasus penyadapan untuk memperoleh informasi dan data finansial pun terjadi di Israel. Polisi Israel berhasil menangkap Yeron Bolondi, 32 tahun seorang pelaku perampokan bank Sumitomo. Yeron Bolondi berhasil mencuri dana sekitar 13.9 juta poundsterling pada bank Sumitomo secara online. Pelaku tertangkap tangan saat sedang mengoperasikan software keylogger untuk memperoleh informasi dan data finansial lebih banyak lagi. Yeron Bolondi, 32 tahun, dijatuhi dakwaan telah melakukan tindak pidana pencucian uang dan penipuan. Simon Perry, tokoh dari Computer Associates mengatakan bahwa penggunaan software-software keylogger dalam kasus-kasus kejahatan internet sangat tinggi sehingga penggunaan software anti spyware sangat dianjurkan sekali bagi perusahaan-perusahaan dalam melindungi jaringan data perusahaan dari ancaman kejahatan internet. Computer Associates juga menyatakan bahwa di Inggris sebagian besar kasus kejahatan pencurian data finansial secara online sering dilakukan dengan menggunakan bantuan berbagai software keylogger[26].

B. Modus Penyadapan Data Pribadi Pengguna Internet

Cyberspace sebagai wahana komunikasi yang berbasis komputer (computer mediated communication), banyak menawarkan realitas baru dalam berinteraksi di dunia maya. Adanya interaksi antar pengguna cyberspace telah banyak bergeser ke arah terjadinya penyalahgunaan

---

[25] *Kasus-Kasus CyberCrime Dunia, http://www.hacking-tutorial.co.cc, diakses pada tanggal 24 Oktober 2010 pukul 22:45 WIB*

[26] *Loc. Cit*

hubungan sosial berupa kejahatan yang khas yang memiliki karakteristik berbeda dengan tindak pidana konvensional yang selama ini telah dikenal. Namun ada juga yang berpandangan bahwa kejahatan melalui internet (cybercrime) memiliki kesamaan bentuk dengan kejahatan yang ada di dunia nyata[27]*.*

Munculnya beberapa kasus cybercrime di Indonesia, seperti pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya e-mail, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program komputer, sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya Cybercrime telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet. Selama ini didalam ruang lingkup kejahatan konvensional, dikenal dengan dua jenis kejahatan sebagai berikut :

1. *Kejahatan kerah biru (blue collar crime)*

   Kejahatan ini merupakan jenis kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti misalnya perampokkan, pencurian, pembunuhan dan lain-lain.
2. *Kejahatan kerah putih (white collar crime)*

---

[27]*Tubagus Ronny Rahman Nitibaskara, Ketika Kejahatan Berdaulat, Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi, Peradaban, Jakarta, 2001, hlm. 53*

> *Kejahatan jenis ini terbagi dalam empat kelompok kejahatan, yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.*

Berbeda dengan kejahatan konvensional, kejahatan dunia maya (cybercrime) muncul sebagai akibat dari adanya komunitas dunia maya dalam internet, kejahatan dunia maya (cybercrime) mempunyai ciri khas dan karakteristik tersendiri berbeda dengan dua jenis kejahatan di atas yang merupakan kejahatan konvensional. Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal berikut:

1. *Ruang lingkup kejahatan;*
2. *Sifat kejahatan;*
3. *Pelaku kejahatan;*
4. *Modus kejahatan;*
5. *Jenis kerugian yang ditimbulkan.*

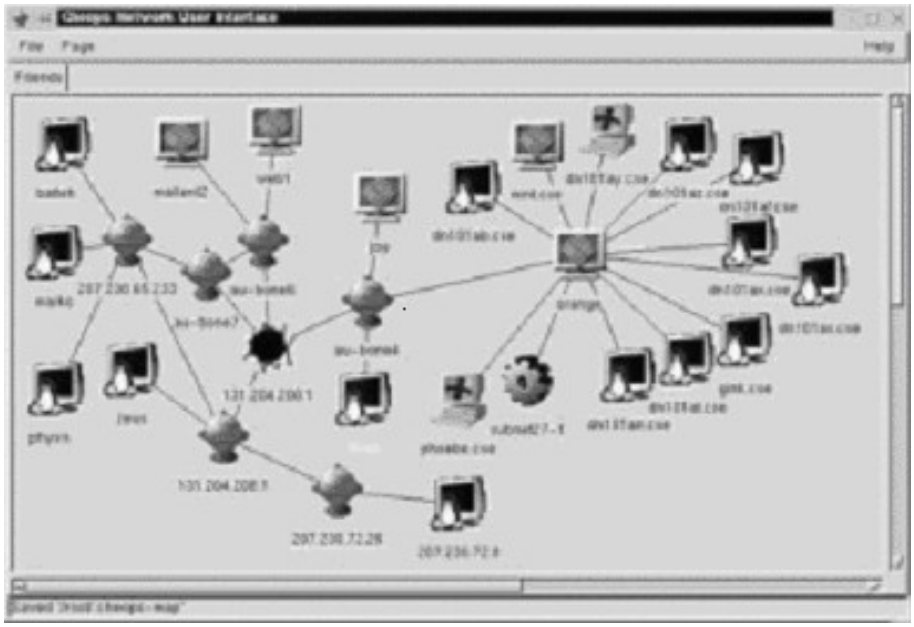
Banyak metode yang sering digunakan oleh cracker untuk dapat mengetahui username dan password dari sebuah akun (account). Akun yang dimaksud di sini dapat berupa akun apa saja, seperti akun email, akun jejaring sosial, akun messenger, dan lain sebagainya. Namun, akun yang sering dijadikan sasaran para hacker adalah akun email. Adanya pemikiran bahwa akun email menjadi dasar atau acuan untuk memiliki akun lain seperti messenger juga jejaring sosial membuat hacker selalu mengincar username serta password dari akun email. Salah satu cara yang digunakan hacker untuk mengetahui informasi akun seseorang adalah sniffing. Sniffing atau dalam konteks pencurian password sering disebut password sniffing adalah

suatu teknik pencurian password dengan bantuan perangkat lunak untuk mengambil informasi remote login seperti username dan password. Teknik sniffing relatif sulit diketahui user karena penyerangan dilakukan terhadap protokol dan langsung menyadap informasi akun dari server[28].

Untuk menembus sistem jaringan, cracker melakukan beberapa tahapan-tahapan standar yang dilalui dan hal ini dikenal dengan istilah anatomy of a hack, tahapan-tahapan tersebut adalah:

1. *Footprinting, sebagai tahap awal yang dilakukan oleh cracker yaitu mengumpulkan informasi tentang jaringan yang dijadikan target, nama, alamat, dan lain-lain.*
2. *Scanning, yaitu melakukan identifikasi terhadap pengguna internet yang aktif, peta jaringan, jalur akses, layanan-layanan yang sedang dijalankan, sistem operasi pengguna internet dan scanning terhadap kelemahan-kelemahan yang mungkin ada pada layanan yang digunakan. Contoh tool untuk memetakan jaringan, scanning dan lain sebagainya dapat menggunakan Cheops seperti gambar dibawah ini:*

[28]*Vega Valentine, Anne Yuliyanti, Bertalya, Op.Cit, Adopsi Enkripsi Jefferson Wheel pada Protokol One-Time Password Authentication untuk Pencegahan Sniffing pada Password E-mail, Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010) Yogyakarta, 19 Juni 2010.*

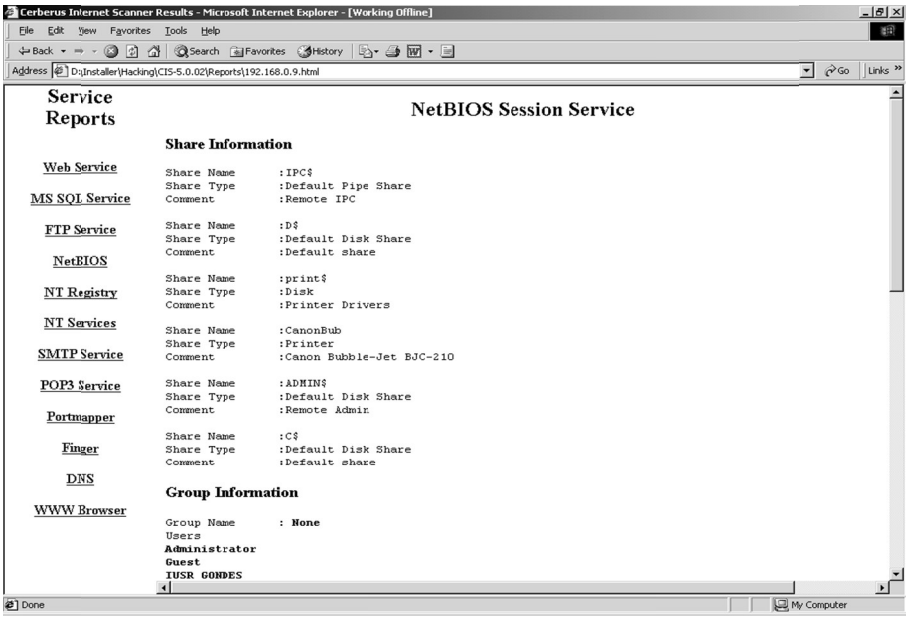


Gambar 1.

Gambar diatas menejelaskan, tampak software yang telah diaplikasikan pada sebuah komputer yang terhubung pada suatu jaringan maka komputer tersebut mampu mendeteksi pengguna internet yang aktif pada jaringan yang sama meliputi peta jaringan, jalur akses, layanan yang sedang digunakan, sistem operasi komputer yang digunakan, dan kelemahan yang ada pada layanan.

3. *Enumeration, yaitu cara seorang cracker untuk memperoleh daftar pengguna internet, mencari jaringan pengguna internet dengan level keamanan rendah, dan identifikasi aplikasi yang dijalankan setelah melakukan scanning pada komputer target. Contoh tool untuk enumeration adalah CIS (Cerberus Internet Scanner) yang*

digunakan untuk mendeteksi komputer yang menggunakan sistem operasi MicrosoftWindows.



Gambar 2.

Pada gambar dua di atas menjelaskan bahwa dengan menggunakan software khusus yang dinamakan CIS (Cerberus Internet Scanner), maka pengguna internet yang menggunakan sistem oprasi Microsoft Windows yang terhubung dalam satu jaringan dapat teridentifikasi aplikasi yang dijalankannya seluruh laporan mengenai sistem oprasi dan kelemahan komputer yang digunakan oleh pengguna internet dapat terpantau.

4. *Gaining Access, yang merupakan tahap selanjutnya bertujuan untuk mendapatkan akses masuk ke dalam computer target. Cara yang digunakan bermacam-macam salah satunya yaitu dengan*

memanfaatkan bug yang ada pada sistem untuk mendapatkan akses dan lain sebagainya.

5. *Escalating Privileges, yaitu bertujuan untuk memperoleh kontrol penuh atas sistem target. Cara yang ditempuh bisa dengan menggunakan metode pembuka kode (Crack Password).*
6. *Pilfering, yaitu metode selanjutnya yang digunakan oleh cracker untuk mengidentifikasi mekanisme yang dapat digunakan untuk mendapatkan akses terhadap komputer yang memiliki sistem kepercayaan (trust).*
7. *Covering Tracks, adalah tahap selanjutnya yang dilakukan oleh cracker sebagai upaya menghilangkan kecurigaan dari administrator asli, setelah akses penuh atas sistem diperoleh dengan cara menghapus log.*
8. *Creating Backdoors, yaitu memasang Beberapa backdoor untuk menjamin hak akses akan diperoleh kembali dengan mudah.*
9. *Denial of Service, merupakan tahap terakhir yang apabila gagal memperoleh hak akses, cracker dapat menggunakan kode-kode yang sudah tersedia untuk mematikan target*[29]*.*

Penyadapan yang biasa dilakukan oleh cracker yang mempunyai keahlian tinggi dalam bidang internet menimbulkan kerugian bagi pengguna internet baik kerugian material maupun kerugian immaterial. Walaupun tindakan cracker menimbulkan kerugian bagi pengguna internet tetapi tidak semua pelaku melakukan serangan dalam suatu sistem jaringan untuk kejahatan. Pada dasarnya penyadapan terjadi karena kurangnya

[29]*Puji Hartono, Serangan-Serangan pada Sistem, puji@perpustakan-islam.com, Diakses pada tanggal 28 Sepetember 2010, pukul 23.30 WIB*

pengetahuan pengguna akan dunia internet. Kecerobohan dalam mengakses data menjadi penyebab utama terjadinya kejahatan dalam dunia maya.