Mengenal Teknik Pencurian Identitas Online Sebagai Upaya Pengamanan Data Pribadi Studi kasus Penanggulangan Terhadap *Web Spoofing*

Listiarini Edy Sudiati
Fakultas Ilmu Komputer Universitas AKI

Abstract

There are many leakings of company's secret documents and personal documents as a result of online identity theft. There are several techniques of online identity theft used by hackers. Social engineering technique is the most common technique that is frequently used. Besides, there are still many other techniques which are recently used by keylogger, password cracking, and web spoofing. By knowing the techniques, it will minimize the occurrence of online identity theft. This paper will discuss the efforts to prevent the theft using web-spoofing techniques.

***Key words** : Theft technique, online identity, spoofing web.*

Pendahuluan

Perkembangan teknologi memungkinkan kita berkomunikasi dan bertransaksi dengan lebih cepat dan lebih mudah. Pembayaran rekening listrik, telpon ataupun transfer uang tidak harus antre panjang di loket-loket, cukup menggunakan "kartu sakti". Sehingga uang tunai di dompet tidak harus banyak, karena pembayaran bisa dilakukan secara digital. Penggunaan pembayaran digital ini menciptakan fenomena cashless society. Salah satu keuntungan dengan penggunaan pembayaran digital adalah akan menurunkan resiko kejahatan tradisional (seperti perampokan dan pencurian), dan juga akan mempermudah proses pembayaran itu sendiri seperti menghilangkan resiko antre seperti di atas.(Emir Pohan, 2001)

Perkembangan lainnya yang menarik adalah kebiasaan orang yang melakukan transaksi secara elektronik melalui media internet. Orang bisa membeli produk tanpa perlu tahu di mana sebenarnya letak toko penjualnya secara fisik. Beberapa jenis produk yang ditransaksikan seperti buku, pakaian dan barang lainnya yang lumrah, tetapi beberapa lainnya mentransaksikan produk yang bisa tergolong sebagai barang 'unik, aneh dan ataupun sangat privat' yang jika

dibeli secara fisik membuat yang bersangkutan merasa malu. Semua serba mudah, cepat dan dengan biaya transaksi yang lebih murah dibanding transaksi fisik. Berdasarkan data dari lembaga riset International Data Corp (IDC), pada tahun 2000 nilai transaksi melalui internet (e-commerce) mencapai US$350,38 miliar dan hingga 2004 naik mencapai US$ 3,14 triliun. (I Wayan Nuka Lantara, 2000)

Bahaya transaksi lewat internet. Di balik kemudahan transaksi melalui internet sebenarnya tersembunyi celah bahaya yang bisa mengancam pemanfaat teknologi itu sendiri, misalnya pencurian identitas. Dan pencurian identitas itu akan menimbulkan resiko-resiko kelanjutannya antara lain kerugian finansial dan pemanfaatan identitas hasil curian itu untuk tujuan yang menguntungkan si pencuri identitas. Di balik kemudahan transaksi melalui internet sebenarnya tersembunyi celah bahaya yang bisa mengancam pemanfaat teknologi itu sendiri, misalnya pencurian identitas. Dan pencurian identitas itu akan menimbulkan resiko-resiko kelanjutannya antara lain kerugian finansial dan pemanfaatan identitas hasil curian itu untuk tujuan yang menguntungkan si pencuri identitas.

Pengertian Pencurian Identitas

Pencuriaan identitas diartikan sebagai tindakan yang dilakukan untuk mengetahui identitas atau menggunakan identitas seseorang secara tidak sah. Identitas ini 31ias berupa nama, alamat rumah, institusi atau e-mail, bias juga berupa nomor PIN, nomor kartu kredit, password ataupun informasi pribadi lainnya.

Berdasarkan obyeknya, pencurian identitas 31ias digolongkan menjadi dua, yaitu:

a. Pencurian identitas pada level korporat/perusahaan, dan
b. Pencurian identitas pada level individual. Pencurian identitas pada level korporat umumnya dilakukan pada database informasi pelanggan yang dimiliki perusahaan. Hal ini 31ias dilakukan melalui pencurian lewat penggunaan teknologi untuk mengakses database konsumen/supplier perusahaan, melalui orang dalam perusahaan (insider) yang secara tidak sengaja maupun sengaja lengah terhadap keamanan penggunaan informasi pelanggan, maupun dari pihak insider yang mau ‘dibayar’ untuk membocorkan informasi pelanggan.

Salah satu contoh kasus di Indonesia yang pernah terekspos adalah pembuatan alamat situs palsu Bank BCA

oleh seorang mahasiswa salah satu perguruan tinggi di Jawa Barat yang dalam sehari 32ias mendapatkan ribuan nomer PIN beserta password nasabah pengguna internet banking BCA. Waktu itu, alamat website yang mestinya www.klikbca.com dikloning menjadi puluhan alamat website dengan variasi nama serupa tapi berbeda (missal: www.klikbac.com atau www.clickbca.com dan lainnya) untuk menjaring nasabah yang mungkin salah ketik lalu mengira sudah masuk dan menginput data PIN dan passwordnya yang langsung direkam secara otomatis oleh website yang dibuat pelaku. Jenis kejahatan ini juga sering diistilahkan sebagai phishing dan juga termasuk dalam jenis cyber fraud.

Teknik Pencurian Identitas Online

Pencurian password, pengambil alihan account, merupakan hal yang sering terjadi di dunia cyber. Bukan hal yang sulit untuk melakukannya.Tapi banyak yang bertanya-tanya bagaimana cara Hecker dengan gampang mendapatkan Password User.

Ada banyak teknik untuk mendapatkan password. Beberapa diantaranya tidak membutuhkan keahlian khusus. Berikut adalah teknik-teknik yang paling umum dan paling sering digunakan:

1. Social engineering
2. Keylogger
3. Web spoofing
4. Password cracking

Teknik Social Engineering

Beberapa pengertian mengenai Social Engineering :

a. *social engineering* mendefinisikan *social enginnering* sebagai "seni dan ilmu pengetahuan untuk membuat orang lain mengikuti kehendak kita" (Bernz, 2001).
b. "pemanfaatan trik-trik psikologis oleh *hacker* luar terhadap *user* berwenang dari sebuah sistem komputeran dalam rangka memperoleh informasi yang ia butuhkan untuk memperoleh akses ke sistem" (Palumbo, 2000).
c. "memperoleh informasi yang dibutuhkan (contoh, sebuah kata sandi) dari seseorang daripada mencoba menembus suatu sistem" (Berg, 1995),
d. *"security attack* dimana seseorang memanipulasi orang lain agar membuka informasi yang dapat digunakan untuk mencuri data, mengakses suatu system, akses ke ponsel, keuangan hingga identitas pribadi" (Guenther, 2001).

Secara umum *social engineering* adalah manipulasi cerdas seorang *hacker* memanfaatkan sifat alami manusia yang

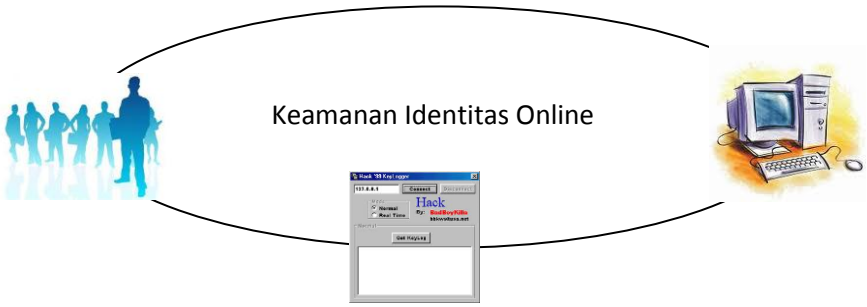
cenderung mudah untuk percaya. Tujuan sang *hacker* adalah untuk memperoleh informasi yang memungkinkannya untuk mendapatkan akses tidak sah ke suatu sistem berikut pula informasi yang ada pada sistem tersebut.

Tujuan & Sasaran Social Engineering

Tujuan utama dari *social engineering* adalah untuk memperoleh akses yang tidak sah ke sistem atau informasi dalam rangka melakukan *fraud* (penipuan atau kecurangan), penyusupan ke dalam jaringan, aktivitas mata-mata perindustrian, pencurian identitas, atau hanya untuk menghadirkan gangguan pada sistem atau jaringan. Sasaran-sasaran yang khas adalah perusahaan telephone, perusahaan dengan nama besar, institusi keuangan, agen pemerintah, instansi militer, dan rumah sakit.

Alasan Menggunakan Social Engineering

Mata rantai keamanan Identitas online bisa kita lihat pada gambar berikut ini.



Gambar 1. Mata Rantai Keamanan Identitas Online

Ada tiga elemen penting dalam sistem keamanan identitas online, yaitu faktor manusia atau pengguna, hardware dan software. Untuk elemen hardware, bisa disiasati dengan berbagai teknik pengamanan data. Demikian juga dengan software, ada beberapa software untuk membobol tingkat keamanan identitas online, tetapi juga terdapat software-software penangkalnya. Dari mata rantai keamanan identitas online, faktor manusia merupakan mata rantai terlemah. Keteledoran ataupun ketidaktahuan pengguna mengenai teknik pencurian identitas online menjadi salah satu penyebab terjadinya pencurian identitas online.

Karena faktor manusia atau pengguna merupakan elemen atau mata rantai terlemah dalam sistem keamanan data online, maka teknik Social

Engineering merupakn pilihan tepat untuk menghack.

Teknik Keylogger

Keylogger merupakan software/hardware yang bekerja dengan cara merekam setiap tombol yang kita tekan pada keyboard. Dengan kata lain, semua aktivitas dalam proses input data pada computer/laptop akan terekam pada software ini.

Fungsi Keylogger

Keylogger berfungsi sebagai perekam segala aktivitas pada PC atau laptop, sehingga apabila kita lupa suatu catatan atau mungkin password dalam browsing di internet, maka kita dapat membuka keylogger dan semua akan terlihat jelas apa yang telah kita lakukan.

Namun bahaya yang harus diwaspadai adalah orang-orang tertentu yang memanfaatkan keylogger ini untuk mencuri data-data atau password, tanpa diketahui.

Macam – cacam software keylogger antara lain :

a. ARDAMAX KEYLOGGER
b. GOLDEN KEYLOGGER
c. PERFECT KEYLOGGER
d. DIGITAL KEYLOGGER
e. REAL SPY KEYLOGGER
f. STEATH KEYLOGGER
g. CHILDSAFE KEYLOGGER

Ada cara aman untuk menghindari keyloger:

1. Gunakan password dengan karakter special seperti !@#$%^&*(){}[]. Kebanyakan
   keyloger akan mengabaikan karakter ini sehingga sang pelaku (pemasang keyloger) tidak akan mendapatkan password anda yang sebenarnya.
2. Persiapkan password dari rumah, simpan dalam bentuk teks. Saat ingin memasukkan password, tingal copy-paste ajah. Keyloger akan membaca password
   anda berdasarkan ketukan keyboard. Namun cara ini agak beresiko. Mengapa?
   karena saat anda melakukan copy, data anda akan tersimpan di clipboard. Saat ini banyak dijumpai software-software gratis yang bisa menampilkan data dalam
   clipboard.

Teknik *Password Cracking*

Password cracking adalah sebuah aplikasi yang menangkap paket data, yang dapat digunakan untuk mencuri password dan data lain dalam transit melalui beberapa jaringan.

"Hacking while sleeping" adalah istilah yang biasa dipakai oleh orang-orang yang melakukan password cracking. Karena pada umumnya dibuthkan waktu yang lama untuk melakukan pasword cracking. Bisa berjam-jam, bahkan berhari -hari! Semua itu tergantung dari target, apakah sang target menggunakan password yang umum, password memiliki panjang karakter yang tidak biasa, atau password memiliki kombinasi dengan karakter-karakter special. Salah satu software yang biasa digunakan untuk melakukan hal ini ialah dengan mengunakan Brutus, salah satu jenis software remote password cracker yang cukup terkenal. Brutus bekerja dengan teknik dictionary attack atau bruce-force attack terhadap port-port http, POP3,ftp, telnet, dan NetBIOS.

Dictionary Attack bekerja dengan mencobakan kata-kata yang ada dalam kamus password. Sedangkan brute – force attack bekerja dengan mencobakan semua kombinasi huruf, angka, atau karakter. Brute Force Atack bekerja sangat lambat dan membutuhkan waktu yang lamatergantung dari jenis spesifikasi komputernya dan panjang karakter passwordnya. Saat ini telah banyak situs yang menutup akses terhadap akses terhadap usaha login yang secara terus-menerus tidak berhasil. (Irlanda, 2010)

Teknik *Web Spoofing*

Hampir seluruh aspek dalam kehidupan kita seperti pendidikan, sosial, pemerintahan mengalami perubahan dan bergerak menuju era berbasis elektronik. *World Wide Web* (WWW atau Web) merupakan media standar untuk beberapa pekerjaan atau layanan ini. Dengan semakin banyaknya orang yang terus menggunakan Web untuk mendapatkan atau tukar-menukar informasi serta melakukan fungsi-fungsi yang begitu banyak, *Web spoofing* telah menjadi metode penyerangan yang menarik bagi *hackers* untuk mengumpulkan informasi yang berharga. *Web spoofing* memungkinkan penyerang untuk menciptakan "shadow copy" dari seluruh WWW. Web yang palsu tersebut kelihatan sama seperti yang aslinya : mempunyai halaman dan semua *link* yang sama (Edward W. felten, Dirk Balfanz, Drew Dean, Dan S. Wallach, 1997), Akan tetapi penyerang mengendalikan Web yang palsu tersebut sehingga aliran data pada jaringan antara *browser* pengguna dan Web akan melalui mesin penyerang. Akses ke Web bayangan diarahkan ke mesin penyerang yang memungkinkan penyerang untuk memonitor seluruh aktivitas pengguna termasuk mendapatkan dan mengubah informasi yang ditransfer melalui Web tersebut. Serangan yang demikian

memberikan metode bagi penyerang untuk mendapatkan informasi yang bersifat pribadi seperti : *password*, nomor rekening, alamat, nomor telepon dan lain-lain. Sebagai tambahan, serangan ini dapat digunakan untuk memberikan informasi palsu yang menyesatkan pengguna sehingga menyebabkan salah satu tipe dari "Denial of Service" attack dengan meniadakan akses pengguna ke informasi situs web yang diinginkan.

Penanggulangan Pencurian Identitas Online Studi Kasus Terhadap *Web Spoofing*

Salah satu contoh kasus web spoofing adalah kasus yang terjadi pada seorang nasabah bank BCA Kuta pada tanggal 16-17 Januari 2010 lalu (http://id.news.yahoo.com/dtik/20100120). Nasabah BCA tersebut kehilangan uang sejumlah 145 juta rupiah. Detailnya, pada tanggal 16 Januari 2010 terdapat 1 transaksi 5 juta rupiah, 6 transaksi masing-masing 10 juta rupiah dan 5 transaksi masing-masing 2 juta rupiah, total 75 juta rupiah. Kemudian tanggal 17 Januari 2010, uang sejumlah 70 juta rupiah kembali raib.

Hal yang harus digarisbawahi adalah nasabah tersebut tidak pernah memakai ATM dan selalu menggunakan layanan mobile-banking. Lalu bagaimana uang tersebut dapat berpindah tanpa sepengetahuannya?

Web spoofing memungkinkan penyerang untuk menciptakan "shadow copy" dari seluruh WWW. Web yang palsu tersebut kelihatan sama seperti yang aslinya : mempunyai halaman dan semua *link* yang sama. Akan tetapi penyerang mengendalikan Web yang palsu tersebut sehingga aliran data pada jaringan antara *browser* pengguna dan Web akan melalui mesin penyerang. Akses ke Web bayangan diarahkan ke mesin penyerang yang memungkinkan penyerang untuk memonitor seluruh aktivitas pengguna termasuk mendapatkan dan mengubah informasi yang ditransfer melalui Web tersebut. Serangan yang demikian memberikan metode bagi penyerang untuk mendapatkan informasi yang bersifat pribadi seperti : *password*, nomor rekening, alamat, nomor telepon dan lain-lain. Sebagai tambahan, serangan ini dapat digunakan untuk memberikan informasi palsu yang menyesatkan pengguna sehingga menyebabkan salah satu tipe dari "Denial of Service" attack dengan meniadakan akses pengguna ke informasi situs web yang diinginkan.

1. Cara Kerja Web Spoofing

Untuk menanggulangi terjadinya wb spoofing, maka perlu tahu cara kerja dari

wb spoofing itu sendiri. *Web Spoofing* melibatkan sebuah server web yang dimiliki penyerang yang diletakkan pada internet antara pengguna dengan WWW, sehingga akses ke web yang dituju pengguna akan melalui server penyerang.

a. Akses ke situs web diarahkan melalui sebuah *proxy server* : ini disebut (HTTP) *application proxy*. Hal ini memberikan pengelolaan jaringan yang lebih baik untuk akses ke server. Ini merupakan teknik yang cukup baik yang digunakan pada banyak situs-situs di internet, akan tetapi teknik ini tidak mencegah *Web Spoofing*.
b. Seseorang menaruh link yang palsu (yang sudah di-*hack*) pada halaman web yang populer. Salah satu contoh, adalah situs BCA yang dipalsukan. Situs asli beralamat di www.klikbca.com, sedangkan yang palsu http://www.bcaclick.com.
c. Kita menggunakan *search engine* (mesin pencari, seperti Yahoo, Alta Vista, Goggle) untuk mendapatkan link dari topik yang ingin dicari. Tanpa kita ketahui, beberapa dari link ini telah diletakkan oleh *hacker* yang berpura-pura menjadi orang lain. Seperti, pencarian untuk situs bank memberikan salah satu hasil http://www.chasebank..com, sayangnya kita mungkin tidak mengetahui bahwa URL sebenarnya dari Bank Chase Manhattan adalah http://www.chase.com.

Pada saat kita menggunakan *browser* untuk mengakses sebuah Web, semua yang ada pada NET (baik Internet maupun Intranet) direferensikan dengan *Universal Resource Locator* (URL). Pertama-tama penyerang harus menulis-ulang URL dari halaman web yang dituju sehingga mereka mengacu ke server yang dimiliki penyerang daripada ke server web yang sebenarnya. Misalnya, server penyerang terletak di www.attacker.com, maka penyerang akan menulis-ulang URL dengan menambahkan http://www.attacker.com didepan URL yang asli.

Contoh :

http://www.comicscorner.com akan menjadi

http://www.attacker.com/http://www.comicscorner.com

Hampir semua *browser* menggunakan HTML. Ada banyak perintah HTML, tetapi hanya ada beberapa yang terdapat baris URL. Karena itu penyerang harus mencari semua perintah khusus ini dan menggantinya pada halaman yang disalin untuk pengguna.

Dibawah ini adalah perintah khusus yang dicari (ini bukan merupakan dari sintaks HTML yang sebenarnya) (Brad C.

Johnson, “How Web Spoofing Works”, System Expert Corporation)

<A HREF=”URL”>

membuat *link* ke sesuatu

<APPLET CODE BASE=”URL”>

menentukan lokasi *Java applet*

<AREA HREF=”URL”>

menentukan area dari sebuah bagian

<BODY BACKGROUND=”URL”> membuat gambar latar belakang

<EMBED SRC=”URL”>

memasukkan sebuah objek ke sebuah halaman

<FORM ACTION=”URL”>

membuat sebuah form

<FRAME SRC=”URL”>

membuat source untuk sebuah frame

<IMG SRC=”URL”>

menampilkan sebuah gambar

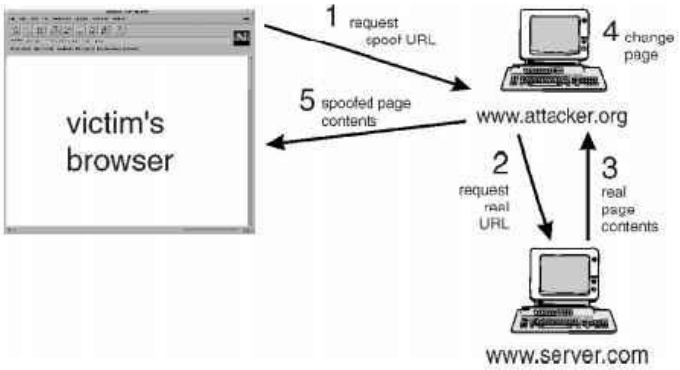
<INPUT “URL”>

membuat source untuk sebuah input

Setelah menulis-ulang URL langkah-langkah berikut terjadi pada waktu serangan *Web spoofing* (Edward W. felten, Dirk Balfanz, Drew Dean, Dan S. Wallach, 1997)

Pengguna me-request sebuah halaman melalui URL situs Web tersebut dari browser web.

1. Server penyerang mendapatkan halaman yang diinginkan dari server web yang sebenarnya.
2. Server Web yang sebenarnya menyediakan halaman tersebut ke server yang dimiliki oleh penyerang.
3. Server penyerang menulis-ulang halaman yang dimaksud.
4. Server penyerang memberikan versi halaman yang sudah ditulis-ulang kepada pengguna.



Gambar 2. Me-request halaman dari URL yang ditulis-ulang

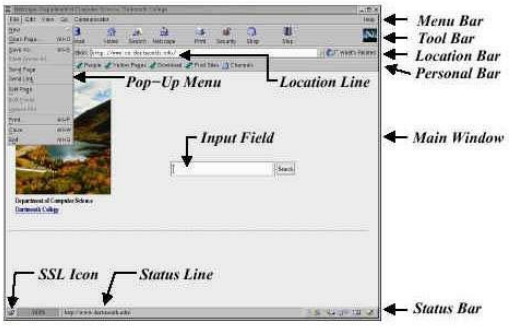
Karena seluruh URL pada halaman web yang ditulis-ulang telah mengacu kepada server penyerang, maka jika pengguna mengikuti *link* pada halaman yang baru, halaman tersebut juga akan diperoleh dari server penyerang. Pengguna akan tetap terperangkap dalam web palsu yang dibuat oleh penyerang, dan dapat terus mengikuti *link* tanpa dapat meninggalkannya.

Metode yang digunakan penyerang untuk mengarahkan korban ke server web penyerang dipermudah dengan adanya kelemahan dalam design pada *location bar* dari hampir semua browser Internet. Karena kelamahan dalam design tersebut, jika sebuah URL tidak cukup pada kotak lokasi, maka *browser* dapat menampilkan bagian akhir dari URL, misalnya :

http://www.attackers.com/http://www.comicscorner.com,

Maka baris alamat URL hanya akan menampilkan http://www.comicscorner.com…, yang akan membantu penyerang dalam usaha menipu korban agar mengira mereka mengunjungi situs yang benar. Tetapi kelemahan design ini diatasi dengan hanya menarik dan menempatkan *address bar* ke sisi kanan dari *button bar* yang standar (Paul O`Brian, "Web Spoofing-What are you looking at?", April 2001) Sifat yang menyulitkan dari serangan ini adalah ia dapat bekerja meskipun ketika korban me-*request* sebuah halaman melalui "*secure connection*". Jika korban melakukan akses halaman Web yang "aman" (akses Web menggunakan *Secure Socket Layer*) pada sebuah situs Web palsu, semua akan berlangsung kelihatan berlangsung normal, halaman web akan ditampilkan dan penunjuk "secure connection" (biasanya berupa gambar sebuah gembok atau kunci) akan menyala.

Meskipun serangan *Web Spoofing* hampir efektif, masih ada beberapa yang memungkinkan korban dapat mengetahui bahwa serangan *spoofing* sedang berlangsung. Akan tetapi penyerang dapat menghilangkan petunjuk akan adanya serangan dan membuat penyerang dapat menghapus jejaknya.



Gambar 3. Contoh sebuah Browser Window

Status line dari *browser* merupakan kemungkinan pertama yang dapat memberi petunjuk kepada korban bahwa mereka sedang menghadapi serangan *spoofing*. *Status line* merupakan sebaris teks di bagian bawah *window browser* yang menampilkan bermacam-macam pesan, khususnya tentang status pada saat menunggu transfer halaman web ke *browser*. Ketika *mouse* diarahkan ke sebuah *hyperlink* halaman Web, maka *status line* akan menampilkan URL dari *link* yang ditunjuk. Sehingga korban dapat memperhatikan bahwa URL yang ditampilkan pada *status line* sudah ditulis-ulang. Kedua, ketika sebuah halaman web sedang diambil, *status line* secara singkat akan menampilkan nama dari server yang sedang berhubungan dengan *browser*. Karena itu korban dapat melihat bahwa www.attacker.com akan ditampilkan dan bukan merupakan alamat dari halaman web yang diinginkan. Penyerang dapat menutupi petunjuk ini dengan menambahkan sebuah program *JavaScript* untuk setiap halaman web yang ditulis-ulang. Karena program *JavaScript* dapat menulis ke dalam *status line*, dan memungkinkan untuk menggabungkan aksi *JavaScript* dengan kejadian-kejadian yang berhubungan, maka penyerang dapat memastikan bahwa *status line* selalu memperlihatkan apa yang seharusnya ditampilkan pada halaman web yang sebenarnya.

Location line dari *browser* memperlihatkan URL dari halaman yang sedang ditampilkan pada *browser*. *Location line* yang sebenarnya mempunyai dua sifat interaktif yang umum : menerima input dari keyboard dan menampilkan menu *history*. Serangan ini akan menyebabkan URL yang ditulis-ulang muncul pada *location line* yang dapat memberi tanda kepada korban bahwa halaman web tersebut telah di *spoofing*. Petunjuk ini dapat disembunyikan dengan menggunakan *JavaScript*. Sebuah program *JavaScript* dapat menyembunyikan *location line* yang sebenarnya dan menggantinya dengan *location line* yang palsu. *Location line* dapat dibuat agar menunjukkan URL yang diharapkan oleh korban dan juga dapat menerima input dari keyboard yang memungkinkan korban untuk menulis URL secara manual. Program *JavaScript* dapat menulis-ulang URL yang diketik sebelum halaman web tersebut diakses. Untuk menerima input pada bar yang palsu, digunakan label input standar pada HTML. Akan tetapi teknik ini menimbulkan masalah yaitu bagaimana membatasi *location line* palsu yang dapat diedit pada tempat yang sesuai di *location bar*. Label input mempunyai ukuran dalam jumlah karakter, tapi ukuran dari karakter

tergantung pada font yang dipilih oleh pengguna. Penyerang dapat menggunakan *atribut style* untuk menentukan font dan ukurannya supaya tempat untuk menerima input akan mempunyai ukuran yang benar. Tetapi jika pengguna memilih font yang berbeda, maka *browser* akan mengabaikan spesifikasi yang sudah dibuat penyerang dan menggunakan font yang dipilih oleh pengguna. Penyerang dapat mengatasi masalah ini dengan menghapus *location line* dari location bar pada gambar latar belakang (jika bar palsu yang dibuat lebih kecil dari yang sebenarnya), atau dengan menentukan font dan ukuran yang pantas dan berharap bahwa pengguna yang ingin menggunakan font yang dipilih mereka sendiri tidak terlalu kecil atau terlalu besar.

Saat ini didapati bahwa penyerang tidak dapat memanipulasi *location bar* pada jendela *browser* yang sedang aktif (salah satu fitur yang ditambahkan karena adanya serangan *web spoofing*). Penyerang dapat membuka sebuah *window* baru dengan *location bar* yang dimatikan, tapi ini akan menimbulkan masalah baru. (Yougu Yuan, Eileen Zishuang Ye, Sean Smith, "Web Spoofing 2001")

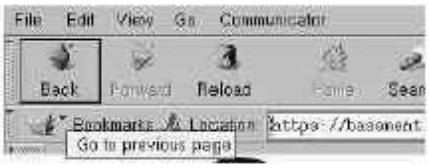
a. Pada beberapa konfigurasi Netscape Navigator, mematikan satu bar akan mengaktifkan alarm keamanan.
b. Pada Internet Explorer, kita dapat mematikan bar tanpa memicu alarm. Tapi kita tidak dapat secara meyakinkan menyisipkan *location bar* yang palsu, karena terdapat spasi yang tampak memisahkan *browser bar* (dimana *location bar* seharusnya berada) dan isi yang disediakan oleh server (dimana bar yang palsu berada).

Membiarkan semua bar menyala pada *window* yang baru membuat *spoofing* tidak mungkin dilakukan sedangkan mematikan sebagian akan menimbulkan masalah. Akan tetapi, masalah ini tidak akan terjadi jika kita mematikan semua bar pada *window* yang baru. Selanjutnya, ketika melakukan hal ini, penyerang dapat mengganti semua bar tersebut dengan bar palsu yang dibuat dan semua bar tersebut akan kelihatan dengan ukuran dan jarak yang tepat karena penyerang tersebut yang mengaturnya.

Penyerang bisa mendapatkan bar yang palsu dengan gambar yang didapatkan dari *browser* yang sebenarnya melalui xv. Karena *browser* memberikan namanya ke server, maka penyerang dapat mengetahui apakah akan menyediakan gambar Netscape atau Internet Explorer. Pertama penyerang akan mencoba meletakkan gambar pada *window* yang palsu yang menghasilkan bar yang kelihatan seperti asli. Contohnya, Netscape 4.75 akan meninggalkan spasi pada sisi

kanan untuk *scroll bar*. Tetapi dengan membuat sebuah frame dan dan mengisinya dengan sebuah gambar latar belakang akan dapat menghindari masalah ini. Gambar latar belakang akan terlihat berulang-ulang. Masalah ini dapat diatasi dengan mengatur frame ke ukuran yang tepat.

Untuk membuat bar yang palsu kelihatan meyakinkan, harus dibuat se-interaktif mungkin sesuai dengan aslinya. Hal ini dapat dilakukan dengan memberikan *event handler* untuk *onmouseover, onmouseout, dan onclick*. Ini merupakan teknik yang sama yang biasanya digunakan untuk membuat tombol dinamik pada halaman web yang umum. Ketika pengguna menggerakkan mouse ke sebuah tombol pada bar yang palsu, tombol tersebut akan berubah ke rupa yang baru (akan menjadi lebih fokus) dan menampilkan pesan yang sesuai pada status bar. Teknik yang serupa juga dapat dipergunakan pada menu bar yang palsu dan lain-lainnya.



Gambar 4. Contoh pop-up tool bar palsu pada Netscape

Jika pengguna meng-klik menu bar palsu, ia akan mengharapkan sebuah menu yang muncul seperti pada browser yang asli. Untuk Internet Explorer, menu pop-up palsu dapat dibuat dengan menggunakan *popup object* dengan gambar sebuah menu pop-up yang asli. Untuk Netscape digunakan fitur *layer*, juga dengan sebuah gambar menu pop-up yang asli. Menu pop-up yang sebenarnya mempunyai kemampuan interaktif ketika pengguna meng-klik pilihan yang bermacam-macam; Untuk interaksi yang demikian dapat digunakan *image maps*.

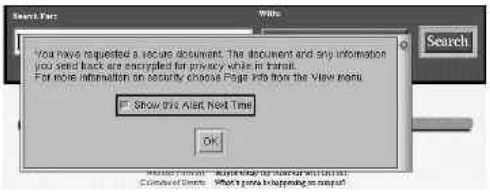
Gambar 5. Contoh pop-up tool bar asli pada Netscape

Warning Window SSL

Pada sebuah *browser* biasanya muncul *warning window* (tampilan peringatan) ketika pengguna membangun dan mengakhiri sebuah koneksi SSL. Untuk menjaga perilaku ini, penyerang

perlu melakukan *spoof* pada tampilan peringatan tersebut. Walaupun *JavaScript* dapat memunculkan *alert window* yang kelihatan sama dengan *warning window* dari SSL, *warning window* SSL mempunyai simbol yang berbeda untuk mencegah *Web Spoofing*. Untuk hal ini harus dilakukan (Yougu Yuan, Eileen Zishuang Ye, Sean Smith, "Web Spoofing 2001") :

a. Untuk Netscape Navigator, dapat digunakan fitur *layer*. Halaman yang sudah di-*spoof* berisi layer tersembunyi awal yang terdapat *warning window*. Penyerang menampilkan layer tersebut pada saat tampilan peringatan tersebut seharusnya muncul. Awalnya, dapat dilihat bahwa warning *window* palsu ini tidak ditampilkan sebagaimana mestinya, karena ia menutupi *input field* yang sebenarnya. Hal ini dapat diatasi dengan mengganti *input field* dengan sebuah gambar yang sama dengannya pada warning *window* yang sudah di-*spoof*.
b. Untuk Internet Explorer, dapat digunakan *Model Dialog* dengan HTML yang menampilkan isi yang sama dengan *warning windows*.



Gambar 6. Warning Window SSL palsu pada Netscape

Gambar 7. Warning Window SSL asli pada Netscape

Untuk memeriksa keaslian dari situs web tersebut. Jika keasliannya sudah dipastikan, maka pengguna dapat mengakses situs tersebut (Paul O`Brian, "Web Spoofing-What are you looking at?", April 2001)

2. Langkah Pencegahan

Untuk jangka pendek, pertahanan paling baik adalah dengan menjalankan strategi dibawah ini : (Edward W. felten, Dirk Balfanz, Drew Dean, Dan S. Wallach, 1997)

1. Tidak mengaktifkan *Javascript* pada *browser* sehingga penyerang tidak dapat menyembunyikan petunjuk atau bukti dari adanya penyerangan.
2. Memastikan bahwa location line dari browser selalu tampak.
3. Memperhatikan URL yang ditampilkan pada *location line* dari *browser* untuk memastikan URL tersebut mengacu pada server dari situs sebenarnya yang dikunjungi.

   Strategi ini akan mengurangi resiko dari penyerangan walaupun pengguna masih dapat menjadi korban jika tidak teliti dalam memperhatikan *location line*.

Saat ini JavaScript, ActiveX dan Java cenderung untuk memudahkan *spoofing* dan serangan yang berhubungan dengan keamanan lainnya, sehingga direkomendasikan untuk tidak mengaktifkannya. Dengan melakukan hal ini akan menyebabkan kehilangan fungsi-fungsi yang berguna pada browser, tetapi pengguna dapat menutup kehilangan ini dengan mengaktifkan fitur-fitur ini secara selektif ketika mengunjungi situs terpercaya yang membutuhkannya.

Untuk halaman yang diambil melalui "secure connection", indikator "secure connection yang lebih baik akan sangat membantu. Daripada hanya menunjukkan "secure connection", browser harus dapat secara jelas memberitahu siapa yang ada di ujung lain dari koneksi tersebut. Informasi ini harus ditampilkan dalam bahasa yang jelas yang mudah dimengerti oleh pengguna yang baru; Harus dapat menyebutkan sesuatu seperti "Microsoft.Inc" dari pada "www.microsoft.com."

Direkomendasikan juga bahwa jika seorang pengguna pernah mengunjungi suatu situs dan autentikasi serta keamanannya telah dibuktikan, maka pengguna tersebut menyimpan link yang tepat dalam sebuah repository (tempat penyimpanan). Repository ini akan digunakan kemudian sebagai titik masuk ke situs web yang diperlukan oleh pengguna.

Implementasi dari teknologi DNSSEC adalah langkah lain yang dapat diambil untuk membuat serangan Web Spoofing lebih sulit dilakukan oleh penyerang. DNSSEC memungkinkan situs web untuk membuktikan nama domain dan alamat IP yang sesuai dengannya menggunakan tanda tangan digital dan

enkripsi yang menggunakan kunci publik. Dengan DNSSEC, ketika pengguna mendapatkan jawaban dari DNS, pengguna dapat membuktikan bahwa DNS tersebut berasal seseorang yang disahkan untuk memberikan jawaban. Untuk DNSSEC dapat bekerja secara efektif, server DNS dari pengguna dan server DNS dari situs web mendukung teknologi DNSSEC, bersama-sama dengan Internet root dan server domain top-level. Jika semua ini sudah dipenuhi, server DNS situs web menggunakan enkripsi dengan kunci publik untuk mengirimkan tanda tangan digital ke server DNS lokal

Kesimpulan

Beberapa teknik yang umum digunakan oleh hacker untuk memperoleh identitas online secara illegal atau pencurian identitas online adalah social engineering, keylogger, password cracker dan web spoofing. Penulis mengangkat studi kasus pencurian identitas online menggunakan web spoofing. *Web Spoofing* adalah metode untuk mendapatkan informasi rahasia yang penting melalui sistem WWW. Serangan melibatkan sebuah server web penyerang yang diletakkan pada internet antara pengguna dengan WWW, sehingga akses ke web yang dituju pengguna akan melalui server penyerang. Penyerang kemudian akan menulis ulang URL dari situs yang dituju dan membuat tampilan pada *window browser* tampak seperti aslinya. Untuk itu pengguna harus teliti dan berhati-hati pada saat mengunjungi suatu situs dengan memperhatikan URL dari situs yang dikunjungi pada *location line* dari *browser* serta melakukan tindakan pencegahan lain yang diperlukan untuk menghindari serangan *Web Spoofing*.

Daftar Pustaka

Al Berg, "Al Berg Cracking a Social Engineer," LAN Times, 1995.
http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html

Brad C. Johnson, "How Web Spoofing Works", System Expert Corporation

Bernz, "The complete Social Engineering FAQ!"
http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt

Edward W. felten, Dirk Balfanz, Drew Dean, Dan S. Wallach, "Web spoofing: An Internet Con Game",
Technical Report 540-96 (revised Feb 1997), Department of Computer Science, Princeton University

Frank O`Dwyer, "Hyperlink Spoofing: An Attack on SSL Server Authentication", Rainbow Diamond Limited, January 1997. <http://www.brd.ie/papers/sslpaper/sslpaper.html>

Glen Bruce, Rob Dempsey, "Security in Distributed Computing", Prentice Hall, 1997.

Paul O`Brian, "Web Spoofing-What are you looking at?", April 2001.
<www.sans.org/infoseqFAQ/threats/web_spoof.htm>

Computer Security Institute. "Social engineering: examples and countermeasures from the real-world,"
http://www.gocsi.com/soceng.htm

Wendy Arthurs, "A Proactive Defence to Social Engineering," SANS Institute, 2001.
http://www.sans.org/infosecFAQ/social/defence.htm

Yougu Yuan, Eileen Zishuang Ye, Sean Smith, "Web Spoofing 2001", Technical Report TR2001-409,

Department of Computer Science/ Institute for Security Technology Studies Dartmouth College, July 2001.