BAB 1

PENGENALAN

1.1 Pengenalan

Kini, serangan siber menjadi semakin rumit. Laporan tahunan daripada Computer Emergency Response Team (CERT) menerangkan pertambahan bilangan insiden keselamatan komputer setiap tahun (CERT, 2002). Sistem Pengesanan Pencerobohan (IDS) disenaraikan sebagai salah satu daripada teknologi untuk menghalang serangan terhadap rangkaian selain daripada dinding api (*firewall*) dan Identifikasi sumber pencerobohan (*intrusion source identification*) (Furguson *et al.,* 1998). IDS boleh ditakrifkan sebagai sistem yang mencuba untuk mengidentifikasikan penggunaan yang tidak dibenarkan, keganjilan dan penyalahgunaan sistem komputer (Puketza *et al.*, 1996). Sistem Penindakbalasan Pencerobohan (IRS) pula menyediakan mekanisme penindakbalasan kepada IDS. Namun demikian, kebanyakan IRS bertindak balas terhadap serangan dengan hanya melalui penjanaan laporan atau amaran (Carver, 2001). Penyelidikan oleh (Cohen, 1999) mendapati bahawa kejayaan satu-satu serangan itu adalah bergantung kepada jurang masa (*time gap*) di antara pengesanan dan penindakbalasan. Secara ringkasnya, sekiranya penceroboh diberi masa tiga puluh jam, penceroboh telah berjaya sepenuhnya menceroboh.

Masalah jurang masa wujud di antara IDS dan IRS. Ini bermakna masalah jurang masa boleh diselesaikan sama ada menerusi IDS dan IRS. Untuk menyelesaikan masalah jurang masa ini, penyelidikan yang telah dilaksanakan oleh (Carver, 2000) yang memfokuskan kepada adaptasi (*adaptive*) IDS telah menumpukan ke arah usaha untuk menghasilkan IDS yang boleh diadaptasikan.

Melalui penyelidikan ini, sekiranya IDS berada di dalam keadaan sentiasa terkemas kini dan dapat pengesanan segala jenis pencerobohan, ini seterusnya akan dapat memastikan pengesanan dapat dilakukan dengan cepat. Sekiranya pengesanan dapat dilakukan dengan cepat, maka masalah jurang masa dapat diselesaikan. Walau bagaimanapun, pengesanan semata-mata tanpa tindak balas sewajarnya adalah tidak berfaedah. Apa yang diperlukan di sini adalah unsur tindak balas yang diakui oleh (Carver, 2001) adalah lebih penting dari IDS. Oleh yang demikian, untuk penyelidikan ini, pengurangan jurang masa menerusi IRS atau penindakbalasan dilaksanakan. Selain daripada IRS dilihat lebih penting daripada IDS, pengurangan jurang masa ke atas IRS dilihat akan memperlengkapkan lagi keseluruhan penyelidikan pengurangan jurang masa yang melibatkan IDS dan IRS.

Dengan ini, dapatlah diringkaskan bahawa penyelidikan ini akan menumpukan usaha untuk mengurangkan jurang masa di antara pengesanan dan penindakbalasan dengan memfokuskan penyelidikan ke arah penindakbalasan atau IRS.

Bagi memastikan usaha ke arah pengurangan jurang masa menerusi penindakbalasan berjaya dilaksanakan, salah satu teknik penindakbalasan telah dipilih. Ini adalah berdasarkan kepada kebaikan yang ada kepada teknik penjejakan berbanding dengan teknik-teknik penindakbalasan yang telah di senaraikan oleh (Carver, 2001). Secara umumnya, kaedah penindakbalasan penjejakan menawarkan penindakbalasan seterusnya setelah punca pencerobohan diketahui. Penjejakan pencerobohan diperlukan sebagai keperluan untuk membangunkan penindakbalasan segera (Dong-li, 2002).

Teknologi penjejakan boleh dibahagikan kepada dua kategori utama, Penjejakan IP dan Penjejakan Sambungan (Buchholz, 2002). Fokus akan diberikan ke arah Penjejakan Sambungan berikutan oleh penjejakan IP memerlukan penglibatan komponen perkakasan (selalunya penghala) (Tatsuya dan Shigeyuki, 2002) sebagai komponen utama dan ini adalah tidak bersesuaian dengan persekitaran penyelidikan yang akan dilakukan dan merupakan salah satu kekangan terhadap penyelidikan ini.

Daripada tinjauan ke atas teknik-teknik penjejakan sambungan (Snap, 1991), (Staniford-Chen dan Heberlein, 1995), (Zhang dan Paxon, 2000), (Yoda dan Etoh, 2000) dan (Schnackenberg dan Djahandari, 2000), teknik penjejakan berasaskan-rangkaian (*network-based tracing*) merupakan teknik yang menjadi pilihan penyelidikan berbanding dengan teknik penjejakan berasaskan-hos (*host-based*) dan penjejakan pasif lebih digunakan berbanding dengan pendekatan aktif (Wang *et al.*, 2001). Sehingga ke saat ini, penyelidikan penjejakan sambungan seperti (Yung, 2002) dan (Dohono *et al.*, 2002) masih tertumpu kepada teknik penjejakan sambungan berasaskan-rangkaian.

Keseluruhan teknik penjejakan sambungan berasaskan-rangkaian cuba untuk menyelesaikan masalah yang dikenali sebagai pengesanan batu loncatan. Batu loncatan merupakan kaedah yang digunakan oleh penceroboh untuk melindungi jejak pencerobohannya dengan cara mempergunakan hos atau perantara sebelum melakukan pencerobohan yang sebenar (Zhang dan Paxon, 2000). Ini dapat dilihat menerusi penyelidikan yang telah dilakukan oleh penyelidik-penyelidik seperti (Snap, 1991), (Staniford-Chen dan Heberlein, 1995), (Zhang dan Paxon, 2000), (Yoda dan Etoh, 2000) dan (Schnackenberg dan Djahandari, 2000). Di sebabkan oleh penyelidik-penyelidikan menunjukkan kepentingan kajian terhadap pengesanan batu loncatan, algoritma pengesanan batu loncatan ini diselidiki dengan mendalam. Hasil daripada penyelidikan terhadap algoritma ini kemudiannya dioptimumkan ke arah untuk menghasilkan algoritma pengesanan batu loncatan yang dapat mengesan batu loncatan dengan lebih pantas.

Oleh yang demikian, keseluruhan penyelidikan ini akan bertumpu kepada pengurangan jurang masa penindakbalasan dengan mengoptimumkan algoritma pengesanan batu loncatan.

1.2 Latar Belakang

Penyelidikan yang dilakukan oleh (Cohen, 1999) mendapati bahawa kejayaan sesuatu serangan itu bergantung kepada jurang masa di antara pengesanan dan penindakbalasan.

Daripada tinjauan yang telah dilakukan oleh (Carver, 2001) menerangkan IDS semasa mempunyai mekanisme yang terhad berbanding dengan ancaman semasa. Penindakbalasan masih lagi menggunakan proses manual dan ini dibuktikan akan menghasilkan jurang masa yang besar di antara pengesanan dan penindakbalasan (Cohen, 1999).

Walaupun penyelesaian terhadap permasalahan ini telah pun diselidiki oleh (Carver, 2001) melalui pendekatan pengesanannya, namun demikian penyelidikan yang dilakukan di dalam tesis memilih untuk menyelesaikan masalah ini menerusi pendekatan penindakbalasan. Ini adalah disebabkan oleh pendekatan penindakbalasan dilihat lebih baik daripada penyelesaian sebelumnya (pendekatan pengesanan). Penyelidikan difokuskan ke arah teknik penjejakan pencerobohan yang disenaraikan oleh (Carver, 2002) sebagai salah satu teknik penindakbalasan yang perlu diambil perhatian.

Teknik penjejakan yang di dalamnya terkandung pelbagai teknik diselidiki yang hasil daripada penyelidikan yang dilakukan mendapati bahawa teknik penjejakan berasaskan rangkaian adalah lebih sesuai untuk dikaji selanjutnya. Ini adalah berdasarkan penyelidikan seperti (Staniford-Chen dan Heberlein, 1995) (Zhang dan Paxon, 2000) dan (Yoda dan Etoh, 2000) serta beberapa penyelidikan terbaru seperti (Dohono *et al.,* 2002) dan (Wang *et al*, 2002) yang masih menumpukan usaha ke arah menyediakan teknik penjejakan yang lebih berkesan.

Keseluruhan teknik penjejakan berasaskan rangkaian ini memfokuskan kepada masalah untuk menyelesaikan masalah yang dikenali sebagai pengesanan batu loncatan. Algoritma untuk menyelesaikan masalah batu loncatan ini dikaji dan penyelidikan untuk mengoptimumkannya ke arah untuk menghasilkan satu algoritma yang lebih baik dijalankan.

1.3 Pernyataan Masalah

"Adakah dengan mengoptimumkan algoritma pengesanan batu loncatan dapat mengurangkan jurang masa di antara pengesanan dan penindakbalasan"

Masalah pengesanan batu loncatan difokuskan dan dinyatakan seperti berikut

Sambungan c_i adalah sambungan tunggal daripada hos komputer H_i (sumber) kepada H_{i+1} (destinasi). Pengguna mungkin log melalui jujukan hos-hos komputer H_1, H_2, H_3,..., H_{n+1} melalui Rantaian Sambungan c_1, c_2, c_3, ..., c_{n-1} di mana sambungan c_i adalah login jauh (*remote login*) daripada hos H_i hingga ke hos H_{i+1}.

Sekiranya diberi sambungan c_n,

"Bagaimanakah kaedah untuk menawan, mengenal pasti dan membandingkan sambungan-sambungan lain c_1, c_2, c_3, ..., c_{n-1} di dalam rantaian, dan sambungan manakah yang terlibat"

"Bagaimanakah pengoptimuman dapat dilakukan untuk menjadikan algoritma pendekatan pengesanan batu loncatan dapat dilakukan dengan lebih pantas"

"Bagaimanakah menentu-ukur masa yang digunakan untuk penjejakan pencerobohan sama ada masa sebelum pengoptimuman dan selepas pengoptimuman"

1.4 Tujuan

Tujuan utama penyelidikan ini adalah untuk pengoptimuman keseluruhan penindakbalasan (IRS) dengan cara mengoptimumkan algoritma pengesanan batu loncatan bagi mengurangkan jurang masa di antara pengesanan dan penindakbalasan (IDS).

1.5 Objektif

Berikut disenaraikan objektif untuk penyelidikan ini.

i. Untuk menyelidik pendekatan mengurangkan jurang masa penindakbalasan (IRS) dengan memfokuskan kepada pendekatan pengesanan batu loncatan.
ii. Untuk mengoptimumkan algoritma pengesanan batu loncatan.
iii. Untuk membandingkan algoritma pengesanan batu loncatan sedia ada dan algoritma yang telah dioptimumkan.

1.6 Skop

Berikut disenaraikan pula skop untuk penyelidikan ini.

i. Penyelidikan ini hanya terhad kepada pengoptimuman pendekatan penindakbalasan (atau lebih tepat lagi algoritma pengesanan batu loncatan) untuk menghasilkan satu pendekatan yang lebih optimum.
ii. Pengoptimuman algoritma pengesanan batu loncatan hanya melibatkan pengesanan di dalam satu-satu segmen Kawasan Rangkaian Setempat (LAN) yang memungkinkan pencerapan paket rangkaian dilakukan hanya melalui satu titik segmen itu sahaja.
iii. Data yang digunakan di dalam algoritma pengesanan batu loncatan hanyalah tertumpu pada paket TCP (atau lebih tepat lagi paket TELNET).
iv. Data yang digunakan adalah hasil daripada penjanaan skrip TELNET (Telnet Scripting Tools v1.0) menggunakan prasarana rangkaian sebenar. Ini adalah bagi memastikan data adalah sama dengan data sebenar rangkaian dan tetap untuk setiap pengujian yang dilakukan.
v. Pencerapan data masa dalam menentu-ukur algoritma sama ada optimum atau tidak bergantung kepada fungsi (*System.milisecond()*) dalaman bahasa pengaturcaraan java versi 1.4.1_04 (Java versi 2).

1.7 Andaian

Berikut adalah andaian yang telah diberikan untuk penyelidikan ini

i. Pengesanan batu loncatan terhad untuk mengenal pasti hos yang merupakan sumber kepada serangan. Pengenalpastian dan penentusahan pengguna sebenar hos adalah di luar bidang pengesanan. Pengesanan batu loncatan adalah terhad kepada penjejakan hos yang digunakan sahaja.

ii. Persekitaran LAN yang digunakan membolehkan pencerapan maklumat keseluruhan paket rangkaian dilakukan hanya pada satu titik di dalam rangkaian tersebut.

1.8 Kepentingan Kajian

Penyelidikan pengoptimuman algoritma pengesanan batu loncatan di dalam pendekatan penindakbalasan dilakukan bagi mengurangkan masa jurang masa penindakbalasan (IRS). Kejayaan mengurangkan jurang masa penindakbalasan bukan sahaja berjaya menyelesaikan sebahagian masalah jurang masa, namun berjaya juga melengkapkan pasangan penyelidikan sebelum ini yang mengurangkan jurang masa melalui pengesanan (IDS). Kejayaan mengurangkan jurang masa ini dilihat berfaedah dari segi untuk mengurangkan kadar peratusan pencerobohan selepas pengesanan oleh IDS. Penyelidikan ini dilihat berpotensi untuk diterapkan di dalam IDS sedia ada yang hanya berkeupayaan untuk mengesan pencerobohan sahaja. Pihak yang bertanggungjawab seperti Pentadbir Sistem atau Rangkaian kini boleh memastikan pencerobohan rangkaian tidak hanya dikesan tetapi diketahui sumbernya dan diberi penindakbalasan dengan lebih cepat dan efisien.

1.9 Hasil Jangkaan

Hasil jangkaan penyelidikan ini adalah berupa algoritma pengesanan batu loncatan yang lebih optimum berbanding dengan algoritma-algoritma pengesanan batu loncatan sedia ada. Melalui pengoptimuman algoritma ini, apabila diguna-pakai sebagai komponen di dalam penindakbalasan (IRS), akan mewujudkan penindakbalasan yang lebih baik dan ini seterusnya akan mencapai matlamat mengurangkan jurang masa di antara pengesanan dan penindakbalasan secara umumnya dan mengurangkan jurang masa penindakbalasan secara khususnya.

1.11 Organisasi Tesis

Penyelidikan ini membincangkan pengurangan jurang masa penindakbalasan melalui pengoptimuman algoritma pengesanan batu loncatan. Bab 1 memberikan pengenalan, latar belakang, pernyataan masalah, tujuan, objektif, kepentingan kajian, skop, andaian dan hasil jangkaan keseluruhan penyelidikan ini. Bab 2 pula menghuraikan kajian latar belakang yang telah dilakukan sepanjang tempoh penyelidikan dilakukan. Bab 3 menerangkan kerangka kerja Penyelidikan. Bab 4 membincangkan rekabentuk yang dilakukan di dalam penyelidikan ini. Bab 5 pula menerangkan implementasi yang dilakukan. Bab 6 membincangkan pengujian yang dilakukan di dalam penyelidikan ini. Bab 7 memberikan hasil, analisa dan keputusan yang diperlolehi daripada sesi pengujian yang dijalankan. Bab 8 menutup penyelidikan ini dengan membincangkan perihal sejauh mana penyelidikan ini mencapai objektifnya, sumbangan penyelidikan, kekurangan dan diakhiri dengan cadangan masa hadapan yang boleh dilakukan.