BAB 1

PENGENALAN KEPADA PENGKAJIAN

1.0 PENGENALAN

Komunikasi data dalam rangkaian komputer melibatkan dua atau lebih komputer. Komunikasi komputer ini dilihat dengan lebih jauh lagi dengan mana dua rangkaian komputer setempat (LAN) di gabungkan menjadi satu rangkaian yang lebih besar iaitu rangkaian luas (WAN).

Komunikasi data dalam rangkaian komputer menggunakan protokol-protokol tertentu yang membolehkan komputer berkomunikasi dengan baik dan memahami satu sama lain. Dua komputer dapat berinteraksi satu sama lain seperti mana manusia berkomunikasi dengan bahasa yang sama. Dua atau lebih komputer yang disambung dengan menggunakan satu talian rangkaian menjadikannya satu perhubungan komunikasi komputer. Juga dinamakan dua rangkaian ialah perhubungan di antara komputer dan juga pelayan.

Beberapa model yang boleh digunakan dalam menjadikan satu rangkaian komputer termasuklah *Hybrid* dan juga STAR. Hubungan komputer disambung antara satu sama lain membolehkan ianya berkomunikasi antara satu sama lain. Komunikasi boleh terjadi dengan adanya penghantaran dan juga penerimaan serta maklum balas dalam rangkaian. Komunikasi rangkaian lebih jelas dengan penghantaran paket-paket maklumat dari

sumber kepada penerima dan penerima membalas kembali paket tersebut dalam tempoh masa tertentu.

Dalam menjalankan komunikasi tersebut, protokol perlu digunakan bagi membolehkan ianya berkomunikasi satu sama lain. Protokol utama dalam dunia rangkaian ialah Sistem terbuka antara hubungan (*Open Sistem Interconnection*). Dalam protokol ini terdapat 7 lapisan yang digunakan untuk membolehkan rangkaian komputer dijalankan. Ini termasuk aras aplikasi, persembahan, sesi, kaedah pengangkutan, rangkaian, pautan data dan juga lapisan fizikal. Satu mesej dihantar mesti melalui kesemua aras dan lapisan yang dinyatakan di atas. Penghantaran komunikasi komputer yang baik merupakan komunikasi komputer yang tiada kegagalan dalam penghantaran paket.

Komunikasi data dapat dilakukan bermula dengan pengumpulan paket data. Paket-paket dikumpul sebelum dihantar dan dipecahkan kembali setelah diterima oleh penerima dan selalunya berlaku dalam lapisan pengangkutan. Manakala lapisan rangkaian mempunyai paket-paket yang mengandungi kepala dan juga data itu sendiri. Ianya dilakukan dengan melalui port yang tertentu dalam komunikasi rangkaian komputer. Port merupakan tempat di mana dua komputer dihubungkan dan destinasi utama dalam satu perhubungan. Port membolehkan satu proses dilaksanakan dan juga membolehkan komunikasi dilaksanakan.

Paket-paket dalam komunikasi komputer mempunyai *pattern* tertentu dan mempunyai corak yang seimbang dan boleh dikenal pasti. Pengenalpastian paket yang ganjil membolehkan sistem mengetahui aktiviti pencerobohan sedang berlaku.

Dalam pengendalian rangkaian dan juga komunikasi antara dua komputer, seperkara yang tidak boleh dielakkan ialah pengganggu yang mengganggu sistem dan juga rangkaian. Apa yang dinyatakan dan diistilahkan di sini ialah pengganggu sistem atau penggodam. Jelas menunjukkan penggodam merupakan individu yang menyalahgunakan rangkaian sistem komputer dan juga mencuri data rahsia. Pengganggu sistem juga boleh dirujuk sebagai satu individu yang mencerobohi sistem dan juga menyebabkan sistem tergendala dan rosak. Penceroboh dibahagikan kepada beberapa kategori utama iaitu penceroboh dalaman dan penceroboh luaran. Penceroboh luaran bermakna penceroboh yang berada di luar kawasan rangkaian. Penceroboh ini selalunya menggunakan teknik pencerobohan pelayan dan pencerobohan *firewall*. Mereka terdiri daripada pengguna yang tidak dikenali dan sukar dikesan. Penceroboh luaran sering menggunakan talian seperti Internet, talian panggilan (*dail-up*) dan juga rangkaian luaran yang lain seperti WAN.

Manakala pencerobohan dalaman merujuk kepada pencerobohan yang dilakukan dari dalam. Selalunya penceroboh sebegini memberi kepada kesan yang besar kepada rangkaian kerana penceroboh dalaman lebih mengetahui selok-belok rangkaian mereka, dan ini akan memudahkan pencerobohan dilakukan.

Terdapat tiga kaedah utama dalam pencerobohan rangkaian komputer yang dapat melumpuhkan rangkaian dan komunikasi data. Tiga cara tersebut ialah secara fizikal, sistem dan kawalan jauh. Secara ringkasnya pencerobohan secara fizikal merujuk kepada gangguan terus kepada fizikal seperti wayar, komputer dan juga pelayan. Manakala pencerobohan sistem merujuk kepada penceroboh yang mempunyai capaian kepada sistem (walaupun pengguna biasa) dan mencari lubang yang boleh digunakan untuk mendapatkan maklumat rahsia. Selalunya penceroboh sebegini sukar dikesan dan dijejaki. Pencerobohan kawalan jauh pula merujuk kepada pencerobohan peringkat tinggi dan penceroboh perlu mempunyai teknik tersendiri.

Oleh yang demikian dalam menangani masalah sebegini, rangkaian mestilah mempunyai satu mekanisme untuk mengesan dan juga menjaga keselamatan dari penceroboh dan juga pengganggu sebegini. Dalam pada itu terdapat pelbagai kaedah yang digunakan untuk menghalang penceroboh dengan menggunakan peralatan seperti *firewall*. Namun apa yang dibimbangi ialah penceroboh dikenal pasti sebanyak hampir 80% adalah dari penceroboh dalaman. Yang mana lebih teruk lagi penceroboh berada dalam *firewall* tersebut.

Dengan ini masih terdapat masalah dalam penggunaan *firewall*. Penggunaan *firewall* tidak dapat menyelesaikan masalah tersebut dan ini akan memberi peluang kepada penceroboh dalaman menceroboh sistem.

Bertitik tolak daripada itu juga, kawalan keselamatan terhadap rangkaian mestilah dititik beratkan. Kawalan keselamatan ini termasuklah mengenali siapa dan dari mana penceroboh melakukan pencerobohan. Penceroboh yang menceroboh dikenal pasti dengan mengesan penceroboh melalui beberapa kaedah. Selepas dikesan penceroboh akan diambil tindakan selanjutnya seperti tindakan undang-undang selepas bukti mencukupi.

Dua kaedah dikenal pasti dalam mengesan pencerobohan berlaku dalam sistem ialah pengesan keganjilan (*Anomaly* Detection) dan pengenalpastian tandatangan (*Signature Recognition*). Kedua-dua kaedah di atas dikenal pasti dari beberapa sudut. Pengesanan keganjilan merujuk kepada kaedah yang biasa digunakan dalam pengesanan penceroboh. Pendekatan sebegini selalunya membezakan dua situasi yang mana situasi yang selalu atau sering berlaku dan kemudian dibandingkan dengan situasi yang jarang berlaku. Apabila situasi jarang ini berlaku, sistem pengesan akan mengesan dan memberitahu aktiviti yang berkemungkinan bermasalah. Selalunya satu ukuran asas akan ditentukan dan aktiviti ganjil akan dibandingkan dengan ukuran asas tadi. Seterusnya pengenalpastian tandatangan merujuk kepada teknik yang sering digunakan oleh syarikat komersial. Selalunya syarikat akan mengenal pasti bentuk transmisi isyarat setiap data. Dengan adanya tandatangan ini, pengguna akan dikenal pasti bahawa transmisi yang dibuat adalah sah. Apabila satu transmisi atau penghantaran paket berlainan maka sistem akan memberi isyarat langsung menyatakan satu aktiviti ganjil sedang berlaku. Kod transmisi dibanding antara satu sama lain dan kod mestilah sama seperti dalam tandatangan asal.

Selalunya tindakan susulan akan diambil setelah sistem mengenal pasti penceroboh atau sistem menjalankan aktiviti ganjil. Pelbagai langkah perlu diambil apabila sistem sedang atau telah diceroboh. Antara tanda yang sering digunakan oleh pengendali rangkaian ialah mengemaskinikan *firewall*, mengeluarkan bunyi amaran, menyimpan log fail dalam sistem, menghantar e-mel kepada pengendali sistem, menyimpan maklumat seperti IP dan masa berlaku, menjalankan program tambahan untuk menghalang pencerobohan atau memutuskan talian terhadap penceroboh.

Senario pencerobohan dan pengenalpastian serta tindakan digambarkan seperti berikut: Terdapat lima langkah utama yang boleh dilihat sebagai langkah untuk menceroboh satu sistem atau rangkaian.

Langkah 1: Pengenalpastian Luaran

Penceroboh akan mengenal pasti sistem atau rangkaian yang hendak diserobohi dan mendapatkan seberapa maklumat yang dikehendaki. Maklumat penting seperti IP, Nama komputer, lokasi, nama syarikat dan nama pengendali sistem. Penceroboh akan mendapatkan seberapa banyak maklumat mengenai sistem dan rangkaian yang hendak diceroboh.

Langkah 2: Pengenalpastian dalaman.

Penceroboh akan lebih mendekati sistem dengan mendapatkan sentuhan luaran sistem dan menjalankan proses pengimbasan. Melihat sistem secara lebih dekat namun tiada tindakan yang diambil lagi. Menjalankan pengimbasan seperti

pengimbasan TCP/UDP serta mendapatkan maklumat mengenai komposisi rangkaian serta peralatan keselamatan yang digunakan oleh rangkaian atau sistem. Pada peringkat ini penceroboh sudah menjalankan aktiviti biasa yang dijalankan oleh pengguna biasa. Peringkat ini sistem yang hendak diceroboh sudah berupaya memberitahu pengendali mengenai proses pengimbasan sedang berlaku. Tetapi tiada tindakan dilakukan. Ibarat penceroboh sudah mendapatkan pintu tetapi belum cuba untuk membukanya.

Langkah 3 : Penggunaan.

Peringkat di mana penceroboh cuba untuk menggunakan pintu yang diimbas untuk masuk ke dalam sistem atau rangkaian. Penceroboh akan menggunakan kaedah laluan seperti pengguna normal dan selalunya sistem sukar mengesan ketika ini melainkan penceroboh menggunakan kaedah lain dan dianggap ganjil oleh sistem atau rangkaian. Penceroboh akan cuba memasuki sistem dan cuba berada dalam sistem seperti pengguna biasa.

Langkah 4: Penaklukan.

Penceroboh ketika ini cuba untuk memasuki dan mengawal sistem secara total. Ketika ini penceroboh cuba untuk menghilangkan jejak dan memasuki sistem sedalam yang boleh tanpa dikesan. Selalunya penceroboh akan memasukkan kekuda supaya membolehkan mereka memasuki sistem untuk kali kedua dan sebagainya.

Langkah 5 : Keuntungan

Pada peringkat ini penceroboh mula mendapatkan sebanyak mungkin maklumat yang boleh digunakan untuk kepentingan sendiri. Penceroboh yang jahat akan cuba untuk melumpuhkan sistem.

Dalam senario di atas dicadang supaya sistem kawalan keselamatan mestilah bermula daripada langkah 3 sehingga langkah 5. Pendekatan mesti dilihat untuk mengelakkan sistem diceroboh dan mengelakkan maklumat dari dicuri. Didapati jika penceroboh masih berada pada peringkat 3 dan 4, pengendali sistem masih boleh mengelakkan daripada penceroboh terus menjalankan langkah 5. Ini akan menyelamatkan sistem dan maklumat rahsia.

Namun walau bagaimana sistem dikawal dan dikemas kini, masalah pencerobohan sistem tidak dapat diatasi 100%. Sebagai pengawal sistem, pengemaskinian sistem mesti dilakukan dari masa ke semasa. Sebagai langkah terbaik, membendung masalah lebih baik daripada mengubati.

1.1 OBJEKTIF PROJEK

Secara keseluruhannya projek ini meliputi objektif seperti berikut:

i. Memahami konsep pemantauan pemberitahuan masalah yang dapat mengurangkan masalah pencerobohan daripada berlaku.

ii. Mendapatkan model dalam proses pemantauan dan juga pemberitahuan dalam sistem pengesanan pencerobohan serta penggunaan *firewall*.

iii. Integrasi sistem sedia ada, *firewall* dan IDS untuk proses pengawalan yang lebih efisien supaya dapat menghasilkan sistem yang boleh menjana pemberitahuan yang cekap, efektif dan berkesan pada sistem.

iv. Mengkaji & menetapkan proses penghantaran maklumat yang efisien dalam proses mengemaskini polisi keselamatan *firewall* yang baru.

1.2 MASALAH YANG AKAN DISELESAIKAN.

Terdapat masalah ditimbulkan berikut penggunaan sistem pengesanan pencerobohan dan *firewall*:

i. Pentadbir sistem kurang mahir dengan teknologi ini. Sistem pengesanan pencerobohan bukan sahaja sukar difahami malahan tindakan atau pemberitahuan mengenai pencerobohan juga sukar ditafsir kerana terdapat banyak pencerobohan tidak sahih berlaku.

ii. Masalah mengenai teknik pemberitahuan masalah tidak cekap pada sistem sedia ada. Pangkalan data perlu disedia untuk menganalisis maklumat dan juga jenis pencerobohan dan tindakan perlu disediakan untuk memudahkan tindakan lanjut diambil.

iii. Tindakan yang lambat diambil oleh pentadbir bila berlakunya serangan ke atas rangkaian. Tiada tindakan automatik dan dinamik diambil walaupun serangan boleh dikatakan tahap tinggi.

iv. Tiada mekanisme terkini yang efisien dalam proses pemberitahuan masalah serangan kepada pentadbir yang berkenaan.

1.3 SKOP PROJEK

Skop projek sistem ini akan melingkupi kajian kes di Fakulti Sains Komputer & Teknologi Maklumat. Kajian kes ini melibatkan dengan meletakkan beberapa sistem di beberapa tempat yang strategik di dalam fakulti untuk mendapatkan data pencerobohan serta menghasilkan mekanisme tindakan dengan perubahan polisi pada *firewall*.

Skop dibahagikan kepada beberapa pengujian sistem dari satu subnet sehingga kepada subnet di luar rangkaian dengan melibatkan rangkaian berada jauh dari subnet. Pengujian skop melibatkan skop di Kolej Kediaman Tun Ahmad Zaidi dengan menggunakan rangkaian sedia ada yang dibekalkan oleh Universiti Malaya.

Tiga subnet digunakan dalam 3 fasa percubaan melibatkan beberapa kaedah serangan dan tindakan atas serangan dikaji sama ada serangan berjaya atau tidak dengan tambahan menggunakan sistem yang dibangunkan bersama sistem sedia ada.

Penglibatan sistem sedia ada dengan menggunakan iptables sebagai *firewall* dan juga Snort IDS sebagai IDS pemerhati.

1.4 ORGANISASI TESIS

Penulisan dibahagikan kepada 7 bahagian utama. Bahagian pertama merupakan bahagian yang menerangkan secara ringkas senario yang berlaku dalam keselamatan rangkaian dan tindakan yang diambil sekiranya berlaku serangan atau tindakan balas lain dari dalam

rangkaian. Juga dinyatakan objektif, skop dan juga masalah yang cuba diselesaikan dalam proses pengkajian.

Bahagian 2 menceritakan tentang skop yang lebih besar mengenai pengkajian terhadap Sistem Pengesan Pencerobohan (IDS) , *firewall* dan transmisi protokol multicast dan unicast. Secara terperinci dijelaskan bentuk, kegunaan dan perkaitan antara satu sama lain. Juga dijelaskan secara terperinci mengenai konsep asas IDS, *firewall*, multicast dan juga penggunaan unicast. Bab ini juga menumpukan perbandingan dan juga kegunaan beberapa jenis IDS dan juga *firewall*. Secara dasar kepentingan elemen *firewall* dan IDS dalam kawalan keselamatan juga dijelaskan.

Bahagian 3 pula menjelaskan mengenai penggunaan polisi dalam isu keselamatan. Ianya menekankan aspek keperluan polisi keselamatan dalam menangani masalah keselamatan dalaman dan luaran. Penjelasan mengenai perkaitan polisi keselamatan dengan penggunaan protokol multicast, Sistem Pengesan Pencerobohan dan juga *firewall* dalam isu keselamatan turut dibincangkan.

Bahagian 4 menjelaskan tentang rangka kerja sistem yang dibangunkan. Konsep mengenai sistem yang akan dibangunkan dibincang secara terperinci. Konsep sistem RedAlert dan fungsi yang berkaitan dalam sistem dibincangkan. Penggunaan dan tahap kepentingan fungsi dalam sistem diperkatakan. Bentuk dan mekanisme yang digunakan oleh sistem untuk mengelak pencerobohan dari terus berlaku diterangkan dengan beberapa contoh nyata.

Bahagian 5 pula menceritakan mengenai rekabentuk dan algoritma setiap fungsi dan perkaitan antara satu fungsi dengan fungsi lain. Ada diterangkan beberapa bentuk algoritma lain yang berkaitan secara tidak langsung dengan sistem.

Bahagian 6 menerangkan proses implementasi dan juga ujian yang dilakukan ke atas sistem. Juga penjelasan mengenai serangan yang digunakan dalam fasa ujian. Jenis serangan yang digunakan serta alatan yang menjana serangan dijelaskan. Juga keputusan mengenai serangan dan hasil daripada tindakan sistem yang dibangunkan.

Bahagian 7 merupakan bahagian terakhir yang membincangkan topik berkaitan dengan hasil yang diperolehi serta kebaikan dan juga kelemahan sistem. Kemampuan mekanisme yang dihasilkan dalam menghalang dan mengelak daripada terus berlaku dibincangkan. Juga dijelaskan cadangan sistem pada masa depan hasil dari kajian yang dijalankan.