# *BAB 7*

## PENUTUP DAN CADANGAN MASA HADAPAN

Pada umumnya sistem yang dibangunkan mencapai objektif dan matlamat asal dalam menghasilkan satu mekanisme baru bagi tujuan menghalang penceroboh dari menceroboh sistem. Mekanisme kawalan keselamatan ini merupakan satu bentuk kawalan yang boleh diimplementasi dalam masa nyata dan memberi kesan yang positif kepada pengguna dan rangkaian.

Walaupun wujud beberapa kelemahan dalam sistem, namun ianya bukan satu titik penamat dalam menghalang pencerobohan dari terus berlaku. Sekurang-kurangnya ia dapat memberi satu peluang untuk pentadbir dalam melindungi rangkaian masing-masing dengan penuh keyakinan. Tambahan, mekanisme ini memberi satu lagi masalah kepada penceroboh yang selama ini mudah dan senang menceroboh rangkaian tanpa halangan. Walaupun halangan wujud, penceroboh masih boleh memecahkan halangan tersebut dan menceroboh rangkaian.

Setiap ciptaan dan penemuan ada kelebihan dan kekurangan. Segala teori dan pandangan serta implementasi tidak akan menemui jalan akhir. Segala kesukaran ada penyelesaiannya. Segala ciptaan ada kelebihan dan ada kelemahan yang mana memberi peluang kepada penyelidik lain berfikir kaedah dan mekanisme baru dalam menghasilkan satu kawalan keselamatan yang lebih baik dan lebih efisien.

## 7.1 KEPUTUSAN BERDASARKAN TEORI DAN PRAKTIKAL

Berdasarkan keputusan yang diterima dalam fasa implementasi dan ujian, ternyata keputusan teori dan keputusan secara praktikal adalah sama. Ini adalah disebabkan oleh implementasi sistem adalah nyata dan tepat dalam fasa penyelidikan.

Secara teori, apabila berlaku serangan ke atas rangkaian, RedAlert akan bertindak membuat polisi baru dan polisi baru dihantar ke rangkaian yang ditetapkan serta mengemaskini polisi dengan kadar segera.

Berdasarkan ujian yang telah dilakukan, polisi keselamatan rangkaian akan berubah dan dinamik mengikut kesesuaian apabila serangan berlaku. Pendekatan ini bukan sahaja memberi peluang kepada pentadbir untuk menjalankan tugas lain kerana tugas mengawal keselamatan telah diambil alih oleh sistem, malahan ianya memberi satu kesan jejak tambahan penceroboh.

Kesan jejak tambahan kepada penceroboh bermakna, RedAlert berperanan mengemaskini polisi keselamatan, dan IDS berperanan mengesan pencerobohan. Ini bermakna jika pada mula polisi keselamatan tidak ketat dan penceroboh cuba menceroboh rangkaian, pencerobohan berjaya namun ianya gagal apabila polisi baru dilaksanakan. Jejak penceroboh disimpan dalam IDS yang mana penceroboh boleh dikesan secara nyata selepas ia memasuki rangkaian tanpa kebenaran.

Walaupun implementasi sistem RedAlert masih lagi dalam percubaan dan ujian dengan menggunakan sistem terbuka, tidak mustahil ianya dapat diimplementasi dengan apa jua platform yang wujud termasuk penggunaan platform Windows.

Secara teori dan praktikal, sistem RedAlert amat berkesan dalam menghalang penceroboh terus menceroboh sistem dengan menghasilkan polisi keselamatan *firewall* menggunakan bentuk serangan dari penceroboh itu sendiri. Pendekatan dinamik dan automatik memberi kesan positif dalam mengawal keselamatan rangkaian yang semakin sukar sekarang ini.

## 7.2 RUMUSAN

Secara keseluruhannya projek ini telah berjaya dalam menyelesaikan beberapa aspek penting dalam isu keselamatan terutamanya dalam menangani isu pencerobohan. :

i. Berjaya mewujudkan mekanisme terkini yang efisien dalam proses pemberitahuan masalah serangan kepada pentadbir yang berkenaan.

ii. Berjaya menghasilkan tindakan automatik dan dinamik dilakukan oleh mekanisme dalam menghalang penceroboh.

iii. Pentadbir sistem tidak perlu mahir dalam menguasai bentuk serangan. Mekanisme yang senang dikonfigurasi untuk keperluan rangkaian sedia ada.

Berdasarkan daripada penyelidikan yang dilakukan beberapa objektif telah dicapai dengan mana memenuhi beberapa keperluan:

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

ii. Sudah mengenal pasti pemberitahuan sahih pada sistem mengenai pencerobohan.

iii. Berjaya menghasilkan sistem yang boleh menjana pemberitahuan yang cekap, efektif dan berkesan pada sistem.

iv. Berjaya mendapatkan model dalam proses pemantauan dan juga pemberitahuan dalam sistem pengesanan pencerobohan serta penggunaan *firewall*.

v. Mengintegrasikan sistem sedia ada, *firewall* dan IDS untuk proses pengawalan yang lebih efisien.

vi. Berjaya mengkaji & menetapkan proses penghantaran maklumat yang efisien dalam proses mengemaskini polisi keselamatan *firewall* yang baru.

## 7.3 KELEBIHAN SISTEM

i. Tindakan halangan automatik

Sistem berupaya untuk menjalankan polisi *firewall* baru secara automatik tanpa pengendalian pentadbir. Jika serangan berlaku pada waktu malam dan waktu pentadbir tiada, pencerobohan masih boleh dielakkan dengan sistem ini.

ii. Berupaya melumpuhkan serangan.

Serangan boleh dilumpuhkan apabila penceroboh cuba untuk menceroboh sistem. Ini bermakna pencerobohan tidak dapat menceroboh beberapa rangkaian berdekatan apabila gagal dalam rangkaian pertama. Ini seterusnya melumpuhkan penceroboh dari terus menceroboh.

iii. Mengurangkan kawalan pentadbir.

Pentadbir tidak perlu lagi berkawal seperti dahulu. Tindakan boleh diambil oleh sistem secara sistematik. Pentadbir perlu memastikan IDS dan sistem berjalan dengan baik serta mengemaskini tandatangan serangan dan juga konfigurasi sistem secara berkala.

iv. Kawalan menyeluruh dalam rangkaian.

Bermakna kawalan yang dijalankan oleh sistem menyeluruh dan tidak terhad kepada beberapa rangkaian sahaja. Ini dapat dipastikan dengan

meletakkan agen berkaitan dalam sistem. Kawalan menyeluruh ini memberi satu pendekatan kawalan keselamatan yang ketat.

v. Kawalan melangkau luar rangkaian LAN.

Kawalan bagi sistem tidak terhad kepada LAN sahaja. Sistem juga boleh beroperasi dengan LAN yang lain di luar subnet. Aplikasi membenarkan komunikasi melalui unicast yang membenarkan komunikasi terus dengan agen unicast. Agen unicast bertindak sebagai jambatan perhubungan dengan agen multicast yang lain.

vi. Masa tindakan yang cepat dan pantas.

Disebabkan serangan yang dilakukan mungkin pantas dan cepat, masa tindakan perlu lebih cepat dan pantas bagi memberi amaran kepada rangkaian yang lain tentang pencerobohan yang berlaku. Dengan masa tindakan dalam masa nyata, penceroboh dapat dihalang dari terus menceroboh.

vii. Tindakan "false positive"

Tindakan "false positive" dapat dikurangkan dengan mana sistem *RedAlert* bertindak cuma berdasarkan tempoh masa. Walaupun pengguna yang sah dihalang dari masuk ke dalam sistem buat masa tertentu. Sistem *RedAlert* sebenarnya akan membenarkan pengguna masuk semula setelah tindakan pengemaskinian *firewall* dilakukan semula. Ini bermakna tindakan "false positive" berlaku seketika sahaja dan mengurangkan

kegagalan sistem. Walaupun berlaku tindakan "false positive" ke atas sistem, ianya bukan menghalang terus sebaliknya membenarkan kemasukan semula dalam tempoh masa tertentu.

viii. Mudah diselenggara dan ditadbir.

Sistem dan aplikasi yang melibatkan RedAlert mudah untuk dikonfigurasi, pentadbir cuma perlu tahu serangan yang perlu dihalang dan membuat polisi jika serangan berlaku. Tambahan, pentadbir perlu tahu di mana lokasi setiap unicast bagi melaksanakan komunikasi unicast sebagai laluan komunikasi multicast.

ix. Penggunaan CPU dan RAM yang rendah.

Peratusan penggunaan CPU dan RAM yang rendah memberikan masa bertindak yang pantas dan cepat. Penggunaan CPU yang hampir 0.1% dapat memberikan masa larian sistem lebih lama dan mampu bertahan 24x7. Tambahan pula, penggunaan RAM yang rendah juga mengurangkan kegagalan sistem jika berlaku kekurangan ingatan. Aturcara dibangunkan dalam bentuk aplikasi *daemon* yang bertindak dalam sistem secara sendiri tanpa kawalan pentadbir.

## 7.4 KELEMAHAN SISTEM

i. Tidak mesra pengguna.

Sistem dicipta tidak begitu mesra pengguna. Walaupun terdapat aplikasi untuk tujuan konfigurasi, sistem masih tidak terdapat antaramuka yang menarik. Ini adalah kerana aplikasi dibangunkan menggunakan aturcara C yang menghasilkan antaramuka 8 bit sahaja.

ii. Pergantungan aplikasi luaran.

Ini merupakan kelemahan yang ketara. Pergantungan aplikasi luaran seperti Snort dan juga iptables memberi satu kekangan kepada sistem. Pembangunan IDS dan juga *firewall* sendiri boleh memberi satu elemen kekuatan kepada sistem.

iii. Tindakan sistem operasi terhad.

Tindakan sistem hanya terhad kepada OS Linux sahaja. Walaupun begitu agen unicast IDS boleh terdiri daripada OS Windows. Cuma *firewall* sahaja memerlukan OS Linux. Ini memberi kekangan kepada sistem untuk bertindak secara lebih efisien.

iv. Kaedah penyulitan.

Kaedah penyulitan yang digunakan dalam semua aplikasi yang melibatkan komunikasi menggunakan kaedah penyulitan simetri. Penggunaan satu kunci sahaja dengan algoritma *XOR blok* merupakan kaedah penyulitan

yang lemah. Walaupun begitu ianya masih boleh menyahsulit data berkaitan. Ini juga adalah disebabkan penyulitan XOR walaupun nampak mudah ianya tidak memberi kesan atau impak yang besar kepada sistem, jika algoritma lain seperti DES atau SSL hendak digunakan, maka subprogram penyulitan perlu dimasukkan ke dalam subprogram aturcara sahaja. Ini tidak mengganggu secara langsung Sistem *RedAlert* yang dibangunkan.

## 7.5 CADANGAN MASA DEPAN

i. Perluasan sistem operasi.

Aplikasi yang dibangunkan boleh diperkembangkan kepada sistem *firewall* dalam persekitaran yang pelbagai seperti Windows. Pembangunan dalam Windows cuma memerlukan satu aplikasi micro-*firewall*. Aplikasi unicast dan multicast boleh beroperasi dalam OS Windows.

ii. Pembangunan aplikasi IDS dan *firewall*.

Aplikasi IDS dan *firewall* yang digunakan bergantung kepada aplikasi sedia ada. Penyelidikan dalam menghasilkan IDS dan *firewall* kegunaan sendiri akan memberikan satu pendekatan baru tanpa pergantungan kepada sistem terbuka lain.

iii. Pendaftaran agen unicast

Penyelidikan seterusnya boleh diteruskan dengan membuat satu proses pendaftaran unicast. Pentadbir tidak perlu lagi tahu lokasi unicast sebaliknya sebaik sahaja ianya dijalankan, satu agen pendaftar akan mendaftar lokasi baru pada agen unicast.

iv. Menyokong aplikasi IPv6.

Aplikasi boleh dibangunkan dengan menyokong IPv6. Sistem sekarang ini dibangunkan dengan menggunakan protokol komunikasi IPv4.

v. Kaedah penyulitan.

Kaedah penyulitan boleh diintegrasikan dengan aplikasi RedAlert yang dibangunkan. Penggunaan PKI (*Public Key Infrastructure*) boleh digunakan dalam aplikasi. Walaupun mudah ianya memerlukan sedikit kemahiran dalam menggabungkan semua aplikasi yang terlibat dengan komunikasi.

## 7.6 SUMBANGAN PENYELIDIKAN

Penyelidikan yang telah dijalankan selama 2 tahun ini telah memberi banyak pengalaman dan pengajaran dalam ilmu yang berkaitan rangkaian. Penyelidikan yang dilakukan juga banyak menggunakan sumber terbuka yang mana memberi peluang kepada penyelidik untuk membaca dan memahami algoritma yang digunakan oleh sesuatu aplikasi sistem terbuka tersebut. Banyak aspek telah disentuh dalam menyempurnakan penyelidikan ini termasuklah aspek yang penting seperti:

i. Sistem Pengesanan Pencerobohan.

   Penggunaan IDS yang memainkan peranan penting dalam aplikasi RedAlert. Snort dikaji dari segi keberkesanan, keserasian, kebolehan dan keutuhan operasi dan menjejak penceroboh.

ii. Sistem *Firewall* Linux.

   Iptables merupakan *firewall* baru dalam Linux Kernel 2.4.x menggantikan Ipchains yang sudah ketinggalan zaman. Kajian dalam keberkesanan, kebolehan dan keserasian integrasi dengan aplikasi RedAlert.

iii. Komunikasi Multicast & Unicast.

   Penyelidikan dilakukan terhadap kebolehan dan keberkesanan penggunaan protokol multicast dalam proses kemaskini polisi *firewall*.

iv. Persekitaran Linux Red Hat.

Penyelidikan banyak dilakukan dalam persekitaran Linux Red Hat. Banyak aplikasi terlibat dalam proses memahami kegunaan dan perkaitan antara satu aplikasi dengan aplikasi yang lain.

Walaupun begitu sumbangan utama dalam penyelidikan ini adalah memberi satu pendekatan baru dalam proses pengemaskinian polisi *firewall*. Proses kemaskini yang sebelum ini dilakukan secara manual telah dilakukan secara automatik. Tambahan pula polisi yang diubah mengikut persekitaran dengan menimbang keadaan semasa. Bermakna jika tiada pencerobohan berlaku maka polisi kawalan tidak ketat dan sebaliknya jika pencerobohan berlaku polisi akan diketatkan.

Polisi *firewall* yang dinamik dengan penggunaan micro-*firewall* ini memberi lebih kawalan keselamatan kepada rangkaian. Penggunaan IDS membantu memberi kawalan lebih efisien dan tepat dalam membuat polisi baru dalam menghalang pencerobohan.

Mekanisme baru ini dikuatkan lagi dengan mekanisme transmisi multicast dan jambatan unicast untuk mempercepatkan proses penghantaran polisi baru. Pendekatan ini bukan sahaja memendekkan masa malahan tidak menjalankan proses kerja yang banyak semata-mata menghantar maklumat polisi.

Jambatan unicast sebagai penghubung 2 atau lebih rangkaian yang menggunakan transmisi multicast. Jambatan unicast ini hanyalah sebagai tambahan jika sistem digunakan dalam kawasan yang lebih besar dari 1 subnet.

Dari penyelidikan yang dilakukan, masa pengemaskinian polisi keselamatan, peralatan keselamatan dan sumber manusia yang digunakan serta wang dapat dijimatkan.