BAB 6

IMPLIKASI KESELAMATAN RANGKAIAN & KEPUTUSAN KE ATAS KAJIAN

6.0 IMPLIKASI KESELAMATAN RANGKAIAN

Keselamatan rangkaian merupakan elemen yang amat penting bagi melindungi persekitaran rangkaian daripada dicerobohi. Implikasi terhadap penyempurnaan isu keselamatan dalam rangkaian memberi kebebasan kepada pengguna menggunakan rangkaian. Rangkaian yang berada dalam keadaan yang selamat memberi satu transmisi yang sempurna kerana pengguna tidak perlu risau dengan data dan juga maklumat yang disimpan ataupun yang dihantar dalam rangkaian.

Keselamatan dalam rangkaian bukan sahaja penting, malahan merupakan elemen yang utama bagi memastikan keutuhan sesuatu rangkaian. Tanpa kawalan keselamatan yang baik keselamatan data dalam simpanan dan rangkaian akan tergugat.

Implementasi sistem RedAlert adalah satu pendekatan yang boleh digunakan dalam memberi satu mekanisme baru dalam memelihara keselamatan rangkaian. Sistem ini berupaya untuk menghalang penceroboh dari terus menceroboh sistem. Penceroboh berupaya untuk menceroboh untuk kali pertama tidak dapat meneruskan niat pencerobohan dalam beberapa saat selepas dikesan. Ini adalah hasil dari mekanisme yang digunakan bagi menghalang penceroboh terus menceroboh dalam rangkaian.

Penceroboh dari luar rangkaian mungkin boleh dihalang terus dari penceroboh, tetapi bagaimana pula penceroboh dari dalam rangkaian. Pengguna dalaman lebih mudah menjalankan aktiviti tidak sihat kerana tidak perlu untuk melepasi *firewall*. Kesan mungkin lebih bahaya jika berlaku serangan tidak diduga dari dalam rangkaian.

Implikasi dalam mengutamakan keselamatan rangkaian sebagai elemen penting bukan sahaja memberi perlindungan kepada pengguna malahan memberi masa yang lebih kepada pentadbir untuk menjalankan aktiviti lain selain daripada membaiki dan menyelenggarakan komputer yang diceroboh.

6.1 IMPLEMENTASI DALAM RANGKAIAN SEBENAR

Sistem RedAlert merupakan sistem sebenar yang dibangunkan untuk mengawal rangkaian dalam masa nyata. Sistem dibangunkan bertujuan memberi mekanisme tambahan kepada kawalan keselamatan yang ada selain daripada penggunaan *firewall* yang statik.

Percubaan dilakukan dalam rangkaian yang meliputi dua rangkaian dalam Universiti Malaya dengan penglibatan FSKTM dan Kolej Kediaman Ke-10 (KKTAZ). Kedua-dua kawasan ini merupakan tempat yang menempatkan 2 topologi rangkaian yang besar.

i. Fakulti Sains Komputer & Teknologi Maklumat

   Fakulti menempatkan ratusan komputer yang disambungkan kepada rangkaian berkelajuan 10/100 Mbps. Melibatkan beberapa lokasi makmal penyelidikan dan

juga beberapa switch yang berupaya untuk mengesan penceroboh dengan menggunakan SPAN pada switch. 2 Makmal yang digunakan dalam percubaan ini iaitu Makmal Penyelidikan Multimedia dan Makmal Penyelidikan Sistem & Rangkaian Komputer. Hos yang digunakan cuma melibatkan 6 buah komputer.

a. Makmal Penyelidikan Multimedia.

   Menempatkan tiga buah komputer yang mana masing-masing bertindak sebagai hos, IDS dan agen unicast.

b. Makmal Penyelidikan Sistem & Rangkaian Komputer.

   Menempatkan tiga buah komputer yang mana masing-masing bertindak sebagai hos, IDS dan agen unicast.

ii. Kolej Kediaman Tun Ahmad Zaidi (10)

Kolej ini juga menempatkan beberapa ratus komputer yang disambung terus ke rangkaian Universiti Malaya. Menggunakan persekitaran rangkaian 10/100 Mbps. Tidak menggunakan SPAN kerana tidak terdapat switch yang berupaya melakukannya. Percubaan melibatkan 3 komputer yang mana masing masing-masing bertindak sebagai hos, IDS dan agen unicast.

Jadual 6.1 : Konfigurasi komputer untuk ujian fasa 1-3

	Lokasi	IP	Gateway	Subnet mask
L1H1	M1 FSKTM	202.185.109.171	202.185.109.190	255.255.255.224
L1H2	M1 FSKTM	202.185.109.174	202.185.109.190	255.255.255.224
L1H3	M1 FSKTM	202.185.109.175	202.185.109.190	255.255.255.224
L2H1	M2 FSKTM	202.185.109.48	202.185.109.124	255.255.255.126
L2H2	M2 FSKTM	202.185.109.49	202.185.109.124	255.255.255.126
L2H3	M2 FSKTM	202.185.109.50	202.185.109.124	255.255.255.126
L3H1	KKTAZ	202.185.68.221	202.185.68.254	255.255.255.0
L3H2	KKTAZ	202.185.68.240	202.185.68.254	255.255.255.0
L3H3	KKTAZ	202.185.68.241	202.185.68.254	255.255.255.0

Setiap hos yang digunakan menggunakan sistem operasi pada platform Unix/Linux atau Windows, kecuali agen multicast mesti dalam pada platform yang menggunakan aplikasi iptables.

Jadual 6.2 : Konfigurasi hos dan OS serta aplikasi yang digunakan dalam ujian

Hos	Sistem Operasi	Aplikasi
L1H1	Red Hat Linux 8.0 (Psyche)	RedAlertMulti dan Iptables
L1H2	Red Hat Linux 8.0 (Psyche)	RedAlertMulti , Snort dan Iptables
L1H3	Windows 2000 Professional	RedAlertUni sahaja.
L2H1	Red Hat Linux 8.0 (Psyche)	RedAlertMulti , Snort dan Iptables
L2H2	Red Hat Linux 8.0 (Psyche)	RedAlertMulti dan Iptables
L2H3	Windows 98SE	RedAlertUni sahaja.
L3H1	Red Hat Linux 8.0 (Psyche)	RedAlertMulti , Snort dan Iptables
L3H2	Red Hat Linux 8.0 (Psyche)	RedAlertMulti dan Iptables
L3H3	Red Hat Linux 8.0 (Psyche)	RedAlertUni, RedAlertMulti dan Iptables

Penggunaan tiga rangkaian yang berbeza memberi pelbagai bentuk percubaan dengan topologi dan kawalan yang berbeza. 2 lokasi yang berjauhan memberi satu bentuk ujian dalam WAN. Ini bermakna ada 3 topologi rangkaian yang berbeza dengan beberapa siri ujian dapat dilakukan.

i. Subnet yang sama.

ii. Subnet berbeza dalam rangkaian yang sama.

iii. Subnet dan rangkaian yang berbeza.

Topologi rangkaian ini dilakukan dengan siri ujian menggunakan 3 kaedah serangan. Bentuk serangan yang dicipta adalah bentuk serangan tahap sederhana. Serangan dilakukan menggunakan peralatan serangan sedia ada yang dibangunkan oleh penggodam dan pengaturcara mahir. Bentuk serangan yang akan digunakan bagi tujuan percubaan termasuklah :

i. LANGuard Network Scanner.

ii. FTP Brute Force Attack

iii. TELNET Brute Force Attack

Bagi kelima-lima serangan yang dilakukan beberapa perlakuan kawalan keselamatan akan dipertimbangkan termasuklah

i. Penggunaan IDS.

ii. Penggunaan *Firewall.*

iii. Penggunaan agen Multicast dan Unicast.

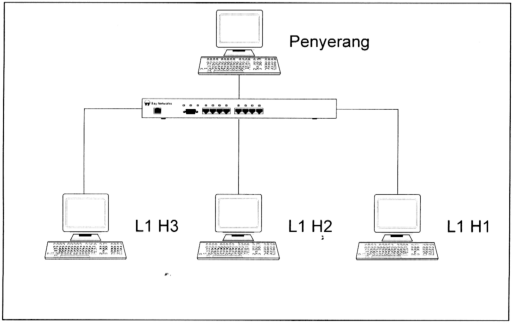
Keberkesanan serangan akan dinilai dari keupayaan sistem diceroboh dan tindakan yang dilakukan oleh sistem bagi menghalang pencerobohan dari terus menceroboh. Teknik pencerobohan dilakukan dalam masa yang berlainan dan berkala.

6.2 TOPOLOGI RANGKAIAN

6.2.1 Topologi Rangkaian Fasa 1

Rangkaian yang digunakan dalam percubaan pertama menggunakan tiga buah PC yang diletakkan dalam subnet yang sama dan mempunyai IP global. Tiga buah PC ini dihubungkan disambungkan kepada switch yang sama. Penyerang berada dalam rangkaian yang sama juga.

Penyerang akan menyerang salah satu dari hos yang ada dalam rangkaian samaada L1H1 atau L1H2.



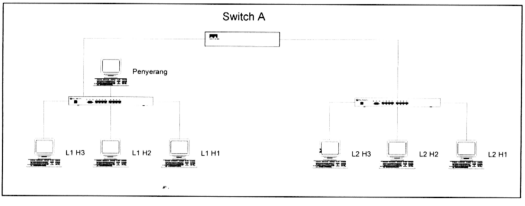
Rajah 6.1 : Topologi ujian fasa1

6.2.2 Topologi Rangkaian Fasa 2

Percubaan yang kedua melibatkan rangkaian yang lebih besar daripada percubaan fasa pertama. Dalam percubaan ini, ia melibatkan 2 rangkaian subnet yang berbeza yang terpisah.

Setiap subnet mempunyai 3 buah PC yang masing-masing mempunyai IP global. Penyerang masih lagi berada dalam subnet pertama dengan mana menggunakan PC dan juga teknik serangan yang sama.

Serangan akan dilakukan kepada 4 buah PC yang berbeza, 2 hos berada dalam subnet pertama dan 2 hos lagi diletakkan dalam subnet kedua.

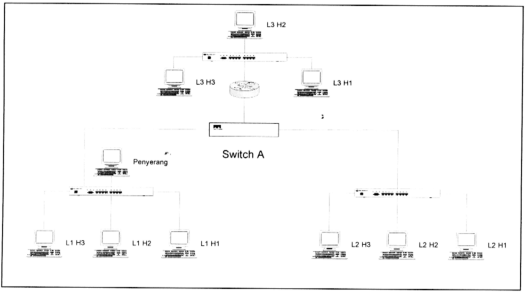


Rajah 6.2 : Topologi ujian fasa 2

6.2.3 *Topologi Rangkaian Fasa 3*

Percubaan dalam fasa ketiga melibatkan topologi rangkaian yang lebih besar daripada fasa 1 dan fasa 2. Fasa ketiga melibatkan lebih banyak PC yang diletakkan pada 3 lokasi yang berbeza. Lokasi dalam fasa 2 dibesarkan kepada topologi WAN yang mana memberi satu bentuk cubaan di luar rangkaian dan subnet.

Sebagaimana percubaan dalam fasa 1 dan fasa 2, setiap subnet diletakkan 3 PC yang masing-masing mempunyai IP global. Penyerang masih lagi berada pada kedudukan lama seperti dalam fasa 1 dan 2. Serangan akan dilakukan kepada 6 PC. Serangan dalam fasa 1 dan 2 diulangi dengan menambah serangan baru kepada subnet yang ditambah iaitu subnet di luar rangkaian.



Rajah 6.3 : Topologi ujian fasa 3

6.3 BENTUK SERANGAN

Pengujian yang dilakukan untuk mengetahui keberkesanan aplikasi RedAlertIDS memerlukan beberapa bentuk serangan yang berbeza. Setiap serangan yang dilakukan sebanyak beberapa kali dalam rangkaian dan topologi yang berbeza. Tempat tapak serangan adalah dari dua sudut iaitu dalaman dan luaran.

Serangan yang dilakukan adalah menggunakan komputer yang mempunyai konfigurasi seperti berikut:

Jadual 6.3 : Konfigurasi Komputer Penyerang

Sistem Operasi	Microsoft Windows 2000 Professional
Versi	5.0.2195 Service Pack 3 Build 2195
Syarikat Pembuat	Dell Computer Corporation
Model	OptiPlex GX400
Pemproses	x86 Family 15 Model 1 Stepping 2 GenuineIntel ~1779 Mhz
Bios	Phoenix ROM BIOS PLUS Version 1.10 A05
Ingatan Rawak	256 MB

6.3.1 LANGuard Network Scanner

Percubaan serangan yang dilakukan adalah dengan menggunakan *LANGuard Network Scanner*. Versi yang digunakan ialah 2.0. Ianya merupakan peralatan yang digunakan untuk mengimbas port yang dibuka oleh satu hos atau pelayan. Selalunya penceroboh akan mengenalpasti port yang dibuka oleh hos sebelum membolehkan penceroboh menyerang hos.

Pengimbas ini bertindak mengimbas port dan juga servis yang dibuka oleh hos dalam rangkaian. Pengimbas boleh bertindak mengimbas rangkaian dalam satu julat tertentu atau hanya satu hos sahaja.

Serangan dari pengimbas port ini perlu ditangani dengan hanya menutup port yang tertentu atau menghalang terus IP berkenaan dari terus membuat pengimbasan. Tindakan yang akan diambil oleh sistem RedAlert ialah dengan menghalang terus port yang di imbas dan menghalang IP berkenaan dari terus menjalankan pengimbasan.

6.3.2 *FTP Brute Force Attack*

Serangan seterusnya dilakukan dengan menggunakan teknik serangan *brute force* ke atas FTP. Serangan ini dilakukan dengan menggunakan satu himpunan fail yang terdiri daripada katalaluan yang akan digunakan untuk meneka katalaluan yang sebenar.

Serangan dilakukan kepada satu hos sahaja pada satu-satu masa. Kebarangkalian mendapatkan katalaluan adalah tinggi jika sistem dibiarkan meneka dalam jangka masa yang lama.

Oleh yang demikian RedAlert perlu mengambil tindakan proaktif dengan menghalang port 21 dari terus diserang. Halangan ini akan menyebabkan tindakan penekaan katalaluan tidak dilakukan dengan efisien. Tambahan pula halangan

dapat dilakukan dengan menghalang IP yang berkenaan dari menjalankan proses penekaan katalaluan.

6.3.3 Telnet Brute Force Attack

Serangan sama seperti serangan sebelum ini cuma serangan ini lebih ditumpukan kepada aplikasi Telnet.

Tindakan yang diambil berbeza sedikit dengan hanya menutup port 23 yang merupakan port bagi aplikasi Telnet.

6.4 KEPUTUSAN HASIL SERANGAN

Setiap serangan dilakukan dengan menggunakan pendekatan kawalan keselamatan yang sama dengan mana pendekatan kawalan adalah seperti berikut:

i. Kehadiran IDS atau tidak.

ii. Wujud *firewall* atau tidak.

iii. Menggunakan multicast atau tidak.

iv. Menggunakan Unicast atau tidak.

Jadual 6.4 : Konfigurasi pendekatan kawalan keselamatan bagi setiap ujian serangan.

	Pendekatan Kawalan Keselamatan			
Konfigurasi	IDS	*Firewall*	Multicast	Unicast
1	Tiada	Tiada	Tiada	Tiada
2	Tiada	Tiada	Tiada	**Ada**
3	Tiada	Tiada	**Ada**	Tiada
4	Tiada	Tiada	**Ada**	**Ada**
5	Tiada	**Ada**	Tiada	Tiada
6	Tiada	**Ada**	Tiada	**Ada**
7	Tiada	**Ada**	**Ada**	Tiada
8	Tiada	**Ada**	**Ada**	**Ada**
9	**Ada**	Tiada	Tiada	Tiada
10	**Ada**	Tiada	Tiada	**Ada**
11	**Ada**	Tiada	**Ada**	Tiada
12	**Ada**	Tiada	**Ada**	**Ada**
13	**Ada**	**Ada**	Tiada	Tiada
14	**Ada**	**Ada**	Tiada	**Ada**
15	**Ada**	**Ada**	**Ada**	Tiada
16	**Ada**	**Ada**	**Ada**	**Ada**

Setiap konfigurasi dikenakan kepada setiap hos, dan setiap hos dalam rangkaian mempunyai konfigurasi yang sama pada satu-satu masa.

Konfigurasi ini dilakukan dengan mana kehadiran elemen-elemen keselamatan yang digunakan dalam kajian.

6.4.1 Fasa 1

Jadual 6.5 : Keputusan ujian Fasa 1

Konfigurasi			**Mangsa**	**Serangan**								
				LanGuard			**FTP**			**Telnet**		
H1	**H2**	**H3**		**H1**	**H2**	**H3**	**H1**	**H2**	**H3**	**H1**	**H2**	**H3**
1-15	1-15	X	L1H1	0	0	X	0	0	X	0	0	X
1-15	1-15	X	L1H2	0	0	X	0	0	X	0	0	X
1-15	16	X	L1H1	0	0	X	0	0	X	0	0	X
1-15	16	X	L1H2	0	**1**	X	0	**1**	X	0	**1**	X
16	1-15	X	L1H1	**1**	0	X	**1**	0	X	**1**	0	X
16	1-15	X	L1H2	0	0	X	0	0	X	0	0	X
16	16	X	L1H1	**1**	**1**	X	**1**	**1**	X	**1**	**1**	X
16	16	X	L1H2	**1**	**1**	X	**1**	**1**	X	**1**	**1**	X

Keputusan dalam ujian fasa pertama ini memberi makna seperti berikut:

i. Keputusan di atas merujuk kepada konfigurasi rangkaian seperti dalam fasa 1. Rujuk rajah 6.1.

ii. Nilai 0 merujuk kepada kebarangkalian sistem mengalami kegagalan dan serangan yang dilakukan telah berjaya.

iii. Nilai 1 merujuk kepada kebarangkalian sistem akan selamatan dan serangan akan gagal hasil tindakan proaktif sistem *RedAlert*.

iv. Nilai X pula merujuk kepada sistem yang tidak berkaitan dan tidak termasuk dalam kajian. H3 tidak berkaitan kerana tiada konfigurasi dikenakan ke atas sistem.

v. Hasil dari keputusan di atas membuktikan bahawa setiap serangan ke atas sistem akan gagal jika wujud konfigurasi ke-16 seperti dalam jadual 6.4.

vi. Serangan ke atas sistem akan berjaya jika menggunakan konfigurasi 1-15 seperti dalam jadual 6.4.

vii. L1H1 merujuk kepada hos pertama dalam rangkaian 1, label ini digunakan untuk semua hos dalam rangkaian.

6.4.2 Fasa 2

Jadual 6.6 : Keputusan ujian Fasa 2

Konfigurasi		**Mangsa**	**Serangan**					
L1	**L2**		**LanGuard**		**FTP**		**Telnet**	
			L1	**L2**	**L1**	**L2**	**L1**	**L2**
1 – 15	1 – 15	L1 H2	0	0	0	0	0	0
1 – 15	1 – 15	L2 H2	0	0	0	0	0	0
1 – 15	16	L1 H2	0	0	0	0	0	0
1 – 15	16	L2 H2	0	**1**	0	**1**	0	**1**
16	1 – 15	L1 H2	**1**	0	**1**	0	**1**	0
16	1 – 15	L2 H2	0	0	0	0	0	0
16	16	L1 H2	**1**	**1**	**1**	**1**	**1**	**1**
16	16	L2 H2	**1**	**1**	**1**	**1**	**1**	**1**

Keputusan dalam ujian fasa kedua ini memberi makna seperti berikut:

i. Keputusan di atas merujuk kepada konfigurasi rangkaian seperti dalam fasa 2. Rujuk rajah 6.2.

ii. L1 merujuk kepada subnet 1 dan L2 merujuk kepada subnet 2.

iii. Konfigurasi pada L1 dan L2 masing-masing sama bagi setiap hos. Oleh yang demikian hos 2 diambil sebagai keputusan bagi setiap rangkaian. Maka keputusan akan merujuk kepada L1H2 dan L2H2 masing-masing merujuk kepada hos ke-2 dalam subnet 1 dan 2.

iv. Nilai 0 merujuk kepada kebarangkalian sistem mengalami kegagalan dan serangan yang dilakukan telah berjaya.

v. Nilai 1 merujuk kepada kebarangkalian sistem akan selamatan dan serangan akan gagal hasil tindakan proaktif sistem RedAlert.

vi. Hasil dari keputusan di atas membuktikan bahawa setiap serangan ke atas sistem akan gagal jika wujud konfigurasi ke-16 seperti dalam jadual 6.4.

vii. Serangan ke atas sistem akan berjaya jika menggunakan konfigurasi 1-15 seperti dalam jadual 6.4.

viii. Keputusan masih lagi sama dengan keputusan fasa 1 yang mana konfigurasi 16 seperti dalam jadual 6.4 dapat menggagalkan serangan.

6.4.3 Fasa 3

Dalam ujian fasa 3 ini terdapat 3 konfigurasi rangkaian berbeza yang mana merujuk kepada subnet yang digunakan dan subnet yang tidak digunakan. Tiga ujian yang dilakukan dirujuk sebagai:

a. Subnet 1 dan 3 dikonfigurasi, dan subnet 2 diabaikan. Keputusan ditunjukkan dalam jadual 6.7.

b. Subnet 2 dan 3 digunakan serta subnet 1 diabaikan. Keputusan terdapat ujian dijadualkan dalam jadual 6.8.

c. Ketiga-tiga subnet digunakan dengan konfigurasi seperti dalam jadual 6.4. Keputusan ujian dijadualkan dalam jadual 6.9.

d. Keputusan yang dijadualkan merujuk kepada hos 2 yang mana akan sama dengan hos yang lain dalam subnet masing-masing.

Jadual 6.7 : Keputusan ujian Fasa 3

Konfigurasi		**Mangsa**	**Serangan**								
L1	**L3**		**LanGuard**			**FTP**			**Telnet**		
			L1	**L2**	**L3**	**L1**	**L2**	**L3**	**L1**	**L2**	**L3**
1 – 15	**1 – 15**	L1 H2	0	X	0	0	X	0	0	X	0
1 – 15	**1 – 15**	**L2 H2**	X	X	X	X	X	X	X	X	X
1 – 15	**1 – 15**	**L3 H2**	0	X	0	0	X	0	0	X	0
1 – 15	**16**	L1 H2	0	X	0	0	X	0	0	X	0
1 – 15	**16**	**L2 H2**	X	X	X	X	X	X	X	X	X
1 – 15	**16**	**L3 H2**	0	X	**1**	0	X	**1**	0	X	**1**
16	**1 – 15**	L1 H2	**1**	X	0	**1**	X	0	**1**	X	0
16	**1 – 15**	**L2 H2**	X	X	X	X	X	X	X	X	X
16	**1 – 15**	**L3 H2**	0	X	0	0	X	0	0	X	0
16	**16**	L1 H2	**1**	X	**1**	**1**	X	**1**	**1**	X	**1**
16	**16**	**L2 H2**	X	X	X	X	X	X	X	X	X
16	**16**	**L3 H2**	**1**	X	**1**	**1**	X	**1**	**1**	X	**1**

Jadual 6.8 : Keputusan ujian Fasa 3

Konfigurasi		**Mangsa**	**Serangan**								
L2	**L3**		**LanGuard**			**FTP**			**Telnet**		
			L1	**L2**	**L3**	**L1**	**L2**	**L3**	**L1**	**L2**	**L3**
1 – 15	**1 – 15**	L1 H2	X	X	X	X	X	X	X	X	X
1 – 15	**1 – 15**	**L2 H2**	X	0	0	X	0	0	X	0	0
1 – 15	**1 – 15**	**L3 H2**	X	0	0	X	0	0	X	0	0
1 – 15	**16**	L1 H2	X	X	X	X	X	X	X	X	X
1 – 15	**16**	**L2 H2**	X	**0**	0	X	**0**	0	X	**0**	0
1 – 15	**16**	**L3 H2**	X	0	**1**	X	0	**1**	X	0	**1**
16	**1 – 15**	L1 H2	X	X	X	X	X	X	X	X	X
16	**1 – 15**	**L2 H2**	X	**1**	0	X	**1**	0	X	**1**	0
16	**1 – 15**	**L3 H2**	X	0	0	X	0	0	X	0	0
16	**16**	L1 H2	X	X	X	X	X	X	X	X	X
16	**16**	**L2 H2**	X	**1**	**1**	X	**1**	**1**	X	**1**	**1**
16	**16**	**L3 H2**	X	**1**	**1**	X	**1**	**1**	X	**1**	**1**

Jadual 6.9 : Keputusan ujian Fasa 3

Konfigurasi		**Mangsa**	**Serangan**								
L1, L2	**L3**		**LanGuard**			**FTP**			**Telnet**		
			L1	**L2**	**L3**	**L1**	**L2**	**L3**	**L1**	**L2**	**L3**
1 – 15	**1 – 15**	L1 H2	0	0	0	0	0	0	0	0	0
1 – 15	**1 – 15**	**L2 H2**	0	0	0	0	0	0	0	0	0
1 – 15	**1 – 15**	**L3 H2**	0	0	0	0	0	0	0	0	0
1 – 15	**16**	L1 H2	0	0	0	0	0	0	0	0	0
1 – 15	**16**	**L2 H2**	0	0	0	0	0	0	0	0	0
1 – 15	**16**	**L3 H2**	0	0	**1**	0	0	**1**	0	0	**1**
16	**1 – 15**	L1 H2	**1**	**1**	0	**1**	**1**	0	**1**	**1**	0
16	**1 – 15**	**L2 H2**	**1**	**1**	0	**1**	**1**	0	**1**	**1**	0
16	**1 – 15**	**L3 H2**	0	0	0	0	0	0	0	0	0
16	**16**	L1 H2	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
16	**16**	**L2 H2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
16	**16**	**L3 H2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Keputusan dalam ujian fasa ketiga ini memberi makna seperti berikut:

i. Keputusan di atas merujuk kepada konfigurasi rangkaian seperti dalam fasa 2. Rujuk rajah 6.3.

ii. Nilai 0 merujuk kepada kebarangkalian sistem mengalami kegagalan dan serangan yang dilakukan telah berjaya.

iii. Nilai 1 merujuk kepada kebarangkalian sistem akan selamatan dan serangan akan gagal hasil tindakan proaktif sistem RedAlert.

iv. Hasil dari keputusan di atas membuktikan bahawa setiap serangan ke atas sistem akan gagal jika wujud konfigurasi ke-16 seperti dalam jadual 6.4.

v. Serangan ke atas sistem akan berjaya jika menggunakan konfigurasi 1-15 seperti dalam jadual 6.4.

vi. L1 merujuk kepada subnet 1, L2 merujuk kepada subnet 2 dan L3 merujuk kepada subnet 3 dalam rangkaian.

vii. Konfigurasi pada L1, L2 dan L3 masing-masing sama bagi setiap hos. Oleh yang demikian hos 2 diambil sebagai keputusan bagi setiap rangkaian. Maka keputusan akan merujuk kepada L1H2, L2H2 dan L3H2 masing-masing merujuk kepada hos ke-2 dalam subnet 1,2 dan 3.

viii. Keputusan masih lagi sama dengan keputusan fasa 1 dan 2 yang mana konfigurasi 16 seperti dalam jadual 6.4 dapat menggagalkan serangan.

ix. Tiga ujian telah dilakukan ke atas fasa 3 ini dengan mana merujuk kepada konfigurasi dilakukan kepada L1 dan L3 (Jadual 6.7), L2 dan L3 (Jadual 6.8) dan L1 bersama L2 dan L3 (Jadual 6.9).

6.5 KESIMPULAN

Kesimpulannya setiap serangan yang dilakukan ke atas hos yang dijangka tidak akan berjaya sekiranya pendekatan kawalan keselamatan yang diambil mengikut spesifikasi berikut:

i. Setiap hos diletakkan IDS, *firewall* dan juga RedAlertMulti.

ii. Setiap subnet mesti wujud satu RedAlertUni sebagai jambatan transmisi multicast.

iii. Setiap rangkaian mesti menyokong transmisi multicast.

Setiap ujian yang dijalankan berlandaskan kepada pendekatan kawalan keselamatan dan elemen-elemen yang mesti wujud. Ujian yang dilakukan semuanya berjaya menghalang penceroboh dari terus menceroboh ke dalam rangkaian seterusnya ke dalam sistem.