BAB 2

KAJIAN PERPUSTAKAAN : KESELAMATAN RANGKAIAN DAN KOMPUTER

2.0 PENGENALAN

Keselamatan rangkaian dan komputer merujuk kepada perkara yang merangkumi kawalan, pencegahan dan pemulihan sistem dan rangkaian komputer. Proses ini merupakan proses yang memerlukan pakar dan juga pengendali yang berpengalaman dalam menyelesaikan masalah dalam dunia rangkaian. Setiap rangkaian mempunyai berbagai-bagai jenis bentuk topologi keselamatan berdasarkan kepada topologi rangkaian masing-masing. Kepentingan dalam urusan kawalan keselamatan ini memerlukan satu kaedah keselamatan yang benar-benar padu dan jitu.

Ramai penyelidik menganggap topik keselamatan merupakan topik yang sukar dan sering berubah. Profesional IT juga menganggap bahawa persekitaran keselamatan rangkaian merupakan satu elemen yang mempunyai masalah kritikal dengan mana pelbagai masalah dihadapi setiap hari dalam menangani isu keselamatan (Wang, G.W, 1994). Setiap manusia dan organisasi mentafsirkan keselamatan dengan cara yang berbeza-beza. Ada yang menganggap kawalan keselamatan merupakan perkara remeh dan ada juga organisasi menganggap perkara ini amat berat dan perlu dibincangkan dengan lebih terperinci. Menurut Anderson (1985), setiap isu keselamatan rangkaian sebenarnya menggunakan konsep yang sama telah digunakan oleh sistem komputer itu sendiri. Tiga

elemen penting dalam dunia keselamatan rangkaian adalah penyulitan, protokol rangkaian dan juga protokol komputer itu sendiri (Walker, S.T , 1989).

Anggapan kawalan keselamatan merupakan satu perkara yang remeh merupakan tanggapan kuno kerana tanpa kawalan keselamatan yang baik, penceroboh mudah menceroboh sistem dan akhirnya sistem dan rangkaian komputer akan lumpuh dan mengakibatkan kerugian yang besar.

Pelbagai bentuk kawalan keselamatan diperkenalkan saban tahun, dan tak kurang juga banyak bentuk serangan terhadap kawalan keselamatan dilakukan. Pada tahun 1996 dilaporkan dalam anggaran 680 serangan setiap hari dilakukan terhadap sistem di Jabatan Pertahanan Amerika Syarikat (AIMD, 1996). Statistik dan laporan yang dibuat oleh Computer Emergency Response Team (CERT) pada laporan tahun 2001 menunjukkan 118,907 email melaporkan perkara yang berkaitan dengan keselamatan komputer. CERT juga menerima 2437 laporan dan mengendalikan hampir 52,628 berkaitan dengan keselamatan dalam tempoh Januari hinggan Disember 2001 (CERT, 2001). Peningkatan sebanyak purata hampir 300% laporan email diterima sejak 1994 hingga 2001 (CERT, 1994). Juga serangan yang dilakukan di laporkan di Malaysia juga menunjukkan peningkatan yang mana peningkatan hampir 400% sejak 1998 hingga Oktober 2002 (*NICER* , 2002).

Peningkatan yang dilaporkan jelas menunjukkan kawalan keselamatan merupakan perkara yang amat penting dan tidak boleh diambil ringan oleh setiap organisasi mahupun individu.

Namun yang jelas kawalan keselamatan diperlukan untuk memberikan keyakinan kepada pengendali rangkaian agar rangkaian dan sistem bebas dari pencerobohan. Tidak dapat dinafikan pencerobohan masih boleh berlaku dengan adanya kawalan keselamatan yang kuat, namun apa yang ditakrifkan di sini adalah pencerboh boleh mencuba untuk menggagalkan kawalan dengan teknik dan bentuk yang berbeza-beza untuk melepasi kawalan tersebut.

Oleh yang demikian pelbagai kaedah dibuat untuk meminimumkan pencerobohan dari terus berlaku. Rekabentuk rangkaian banyak memainkan peranan dalam menghindari pencerobohan daripada berlaku. Rekabentuk rangkaian yang rumit akan menyukarkan penceroboh dari menceroboh. Dengan implementasi berbagai-bagai bentuk kawalan keselamatan termasuklah *firewall* dan juga penggunaan Rangkaian Maya Persendirian (*Virtual Private Network*) pencerobohan menjadi semakin sukar.

Namun sejauh mana kita cuba untuk menghalang penceroboh dari menceroboh sistem, malah penceroboh dan penggodam akan cuba untuk menceroboh sistem. Pentadbir rangkaian perlu lebih peka kepada persekitaran dan sentiasa mengemaskini diri dengan teknik dan bentuk kawalan keselamatan kerana masa akan berubah dan kaedah pencerobohan turut menjadi lebih mudah.

2.1 KAWALAN KESELAMATAN DALAM & LUARAN

Kawalan keselamatan dalaman merujuk kepada kawalan keselamatan yang menumpukan kawalan dalaman. Selalunya pencerobohan berlaku dari luar, tetapi kawalan keselamatan dalaman merujuk kepada kawalan yang dilakukan kepada pengguna dalaman atau pengguna yang berada dalam lindungan *firewall*.

Dilaporkan banyak pencerobohan berlaku dan berpunca daripada rangkaian dalaman sendiri. Ini adalah ianya lebih mudah berbanding dengan pencerobohan yang dilakukan dari luar. Disebabkan rangkaian sering menjadi serangan dari luar maka *firewall* selalunya berupaya untuk menghalang dari serangan dari luar rangkaian dan bukan dari dalam rangkaian.

Termasuk dalam kawalan dalaman juga adalah kawalan terhadap bentuk fizikal sesuatu unit atau perkakasan rangkaian. Ini juga merujuk kepada lokasi pelayan dan juga lokasi *hub* dan *switch* serta *router*. Pendedahan peralatan ini kepada penceroboh akan memudahkan berlakunya penyalahgunaan dan pencerobohan dalaman.

Kawalan keselamatan luaran lebih sukar berbanding dengan kawalan dalaman. Kesukaran di sini bermakna penceroboh boleh berada di mana-mana dan menggunakan berbagai-bagai teknik. Tiada penyelesaian yang konkrit yang dapat mengelakkan pencerobohan rangkaian sepenuhnya. Pencerobohan masih berlaku. Perkara yang sering menjadi ukuran keselamatan dan langkah keselamatan kepada penceroboh luaran adalah

dengan menggunakan *firewall*. Namun penggunaan *firewall* semata-mata tidak mencukupi.

Jadual 2.1 : Perbezaan antara Kawalan dalaman dan luaran

	Kawalan Keselamatan Dalaman	Kawalan Keselamatan Luaran
1. Penggunaan *Firewall*	Mudah melepasi kerana berada dalam rangkaian	Sukar dilepasi kerana berada di luar rangkaian
2. Fizikal	Mudah kerana boleh mencapai bentuk fizikal.	Sukar kerana jauh dan serangan dibuat secara kawalan
3. Lokasi	Lebih mudah dikesan kerana berada dalam kawasan rangkaian.	Sukar dikesan dan perlu bantuan daripada pentadbir luar.
4. Pengetahuan	Mungkin merupakan pengguna dalaman yang mempunyai capaian tetapi terhad.	Di luar kawalan dan tidak mempunyai capaian langsung pada sistem.
5. Kebarangkalian berlaku.	Tinggi	Rendah.

Daripada perbezaan di atas jelas bahawa kawalan dalaman lebih penting berbanding kawalan pencerobohan luaran.

Kawalan dalaman dianggap penting kerana penceroboh yang cuba menceroboh sistem selalunya berada di dalam lingkungan *firewall*. Walaupun rangkaian dalaman telah dilengkapi dengan kawalan keselamatan *firewall* yang berupaya menghalang pengguna luar dari menceroboh sistem, kaedah pencerobohan masa kini yang terlalu maju membolehkan pengguna luar bertindak melepasi *firewall* rangkaian dan menjadi pengguna dalaman yang tidak sah (Hwang, K. & Gangadharan, M, 2001). Ini membolehkan ianya bertindak menceroboh sistem secara dalaman. Selalunya banyak sistem rangkaian (*server*, *gateway*, *firewall*, dll) membenarkan capaian terus dari

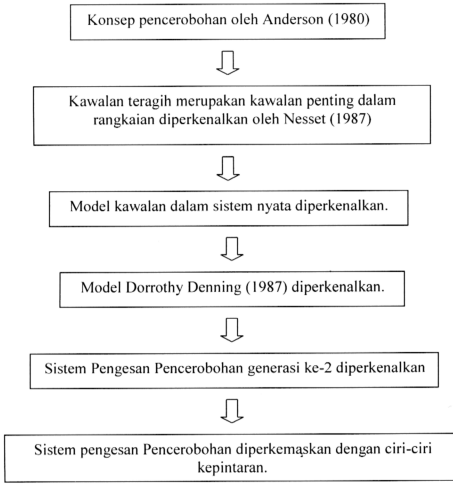
pengguna dalaman dan menghalang pengguna luar. Jika pengguna luar menjadi pengguna dalaman maka ia lebih mudah menceroboh kerana tiada halangan terus dari kawalan dalaman. Ini adalah kerana capaian dari dalam selalunya dianggap sah oleh pentadbir. Penyamaran pengguna luar sebagai pengguna dalaman membolehkan capaian secara terus kepada sistem-sistem tersebut dengan mudah. Serangan dari pengguna dalam dianggarkan mencapai sehingga 70% dari serangan-serangan yang berlaku (Hai Jin, et al., 2002).

Oleh yang demikian kawalan dalaman perlu dikawal dengan lebih ketat lagi memandangkan pengguna luar boleh bertindak sebagai pengguna dalaman dengan menggunakan *gateway firewall* yang memisahkan rangkaian dalaman dan luaran. Perlu dinyatakan bahawa penggunaan *gateway firewall* cuma menghalang pengguna luaran dari mencapai sistem sebaliknya membenarkan capaian dari dalam. Pengabaian kawalan dari dalam akan membolehkan ianya diceroboh dengan mudah.

2.2 SISTEM PENGESANAN PENCEROBOHAN

Konsep pengesanan pencerobohan mula diperkenalkan pada 1980 oleh Anderson (1980) yang mana mencadangkan sistem pengawasan keselamatan yang melibatkan sistem audit log . Kemudiannya pada pertengahan tahun 80-an banyak perubahan berlaku terutamanya penggunaan komputer dalam kawasan yang teragih mengakibatkan perubahan yang besar dalam isu rangka kerja pengawasan. Anggapan Anderson (1980) mengenai rekabentuk kawalan rangkaian sama seperti kawalan satu komputer disangkal oleh Nesset (1987) yang menyatakan bahawa kawalan sistem teragih lebih penting dalam isu keselamatan

dan tidak berkaitan dengan sistem komputer peribadi. Banyak isu tambahan diperlukan dalam menangani isu keselamatan rangkaian teragih dengan mengembangkan lagi konsep sedia ada ke dalam keselamatan rangkaian (Nesset, Dan M., 1987).



Rajah 2.1 : Perkembangan Sistem Pengesan Pencerobohan

Pendapat mengenai isu keselamatan dalam rangkaian diperkukuh dengan mekanisme yang digunakan oleh satu komputer dan ianya boleh digunakan dalam mengutuhkan pengawasan mekanisme dalam rangkaian (Lu, Wen-Pai, & Malur K. Sundareshan, 1990). Seterusnya perdebatan mengenai kawalan keselamatan dan rangkaian dan komputer

diperkuatkan dengan adanya sistem pengesanan pencerobohan secara masa nyata. Menurut model yang diperkenalkan oleh Dorrothy Denning (1987), yang juga berdasarkan model yang diperkenalkan oleh Anderson (1980), berpendapat bahawa membina satu sistem pengawasan yang benar-benar selamat adalah terlalu susah, tetapi tidak mustahil dan juga sistem yang terlalu selamat juga kadang kala menjadi tidak selamat disebabkan penyalahgunaan oleh pentadbir sendiri (Denning, Dorothy, 1987).

Dorrothy Denning (1987) memperkenalkan model pengesanan yang boleh mengesan dengan mengawasi audit log berdasarkan bentuk dan kod penggunaan sistem yang tidak normal. Bentuk pengawasan seperti ini merupakan model yang dianggap sebagai satu permulaan bagi pengesan pencerobohan generasi ke-2 yang mana ianya lebih kompleks dan mampu menangani masalah sistem teragih dan juga pada masa yang sama memberi amaran dalam masa nyata.

Bertitik tolak daripada itu, generasi kedua untuk pengesan pencerobohan telah diperkenalkan. Generasi kedua membahagikan cara pengesanan kepada dua pendekatan iaitu pengesanan keganjilan (*anomaly detection*) (Teresa F. Lunt, 1990) dan pengesanan penyalahgunaan (*misuse detection*) (Mukherjee, B. et al., 1997). Pengesanan keganjilan merujuk kepada pengesanan perubahan dalam kod penggunaan atau perlakuan dalam sistem. Sebagai contoh, pada masa biasa sistem menjalankan aktiviti biasa dengan menggunakan 10% penggunaan CPU, tetapi pada satu masa yang tertentu dan tidak munasabah, contohnya pada jam 2 pagi penggunaan bertambah sebanyak 80% penggunaan CPU dan pada masa itu tiada pengguna yang menggunakan CPU tersebut.

Ini jelas menunjukkan bahawa ada perkara yang sedang berlaku dan mungkin penceroboh sedang menggunakan sistem tersebut. Manakala pengesanan penyalahgunaan dilakukan dengan melihat kepada kelemahan satu sistem yang mana boleh digambarkan oleh kod yang tertentu atau turutan sesuatu kejadian atau data.

Sebagai contoh, sistem akan menghantar paket atau kod tertentu dalam rangkaian apabila komunikasi dilakukan. Seorang penceroboh cuba untuk memasuki sistem dengan menggunakan protokol Telnet serta kata laluan yang salah, maka sistem akan menghantar semula kepada penceroboh dengan nilai atau kod "*Login incorrect*" yang menunjukkan kata laluan salah. Kod ini digunakan untuk mengesan kewujudan penceroboh yang cuba untuk memasuki sistem. Berikut adalah contoh kod seperti dalam contoh.

Jadual 2.2 : Kod dalam bentuk hexadesimal

```
00b0d0076f1900b0d0076f9c080045100042bd48400040060c8dcab
96daecab96daf00170428b01d1f145599cb74501816d0d16900004c
6f67696e20696e636f72726563740d0a0d0a6c6f67696e3a20
```

Jadual 2.3 : Kod dalam ASCII

```
.°D.o..°D.oœ..E..B½H@.@..▯ Ê¹m®Ê¹m¯...(°...U™ÉtP².ÐÑi..Login incorrect.
.
login: =
```

Penggunaan sebegini memerlukan kod yang banyak dan perlu disimpan dalam pangkalan data yang besar.

Sistem Pengesanan Pencerobohan (IDS) di kategori kepada *host-based* dan *network-based. Host-based* selalunya bertindak ke atas satu komputer sahaja manakala *network-*

based bertindak ke atas rangkaian dan selalunya mengawasi laluan rangkaian yang mana menggabungkan *host* dan rangkaian. Kedua-dua kaedah ini menjadi hampir sama apabila banyak teknik dan produk diperkenalkan dalam sistem pengesanan pencerobohan (Cannady, J. & J. Harrel., 1996).

Elemen tambahan dalam menjadikan IDS satu elemen yang penting dalam isu keselamatan komputer adalah dengan menambahkan ciri-ciri kepintaran dalam aplikasinya (Geib, C.W. & Goldman, R.P., 2001). Kebolehan mengesan penceroboh adalah satu fungsi utama, tetapi jika boleh ianya berperanan dalam menghalang dan memberi tindakan awal terhadap penceroboh adalah ciri tambahan yang amat baik. Bermakna IDS bukan sahaja terhad kepada proses pengesanan malahan berperanan besar dalam menghalang penceroboh dari terus menceroboh.

2.3 PRINSIP SISTEM PENGESANAN PENCEROBOHAN (IDS)

Prinsip IDS telah mula diperbincangkan sejak dahulu lagi dan semakin di kemas kini dari dahulu sehingga sekarang. Banyak IDS telah dicipta dan telah dibangunkan oleh pakar dan kebanyakan mekanisme yang digunakan oleh mereka adalah sama. Merujuk kepada *Next-generation Intrusion Detection System (NIDES)* (Anderson, D. et al., 1995), IDS kini bukan sahaja mengesan penceroboh dengan kaedah keganjilan dan penyalahgunaan, malahan ianya menggunakan kedua-dua kaedah yang sedia ada.

Prinsip asas yang mesti ada pada semua IDS adalah pengesan yang mampu mengesan penceroboh dalam apa jua keadaan. Rekabentuk dalam Sistem Pengesanan Pencerobohan

dipecahkan kepada 5 bahagian iaitu pengesan (*sensor*), agen, pengumpul, pengurus dan juga penganalisis.

i. Agen selalunya diletakkan dalam komputer dan merupakan proses yang kecil dan selalunya diletakkan dengan tujuan yang kecil. Agen selalunya berinteraksi dengan pengurus dalam menjalankan sesuatu arahan daripada pengurus.

ii. Pengesan merupakan aplikasi yang berupaya mengesan pencerobohan jika penceroboh cuba melakukan aktiviti. Pengesan selalunya berkebolehan seperti *sniffer* yang boleh mendapatkan maklumat daripada pengguna atas talian.

iii. Pengumpul berfungsi lebih kurang sama dengan agen cuma ianya berfungsi untuk mengumpul data yang didapati oleh pengesan dan disimpan dalam pangkalan data untuk tindakan analisis.

iv. Pengurus bertindak dalam menguruskan agen yang berada dalam talian. Semua tindakan agen bergantung kepada pengurus.

v. Penganalisis berupaya untuk menganalisis paket yang dikumpul oleh pengesan.

Prinsip IDS dinyatakan diguna pakai oleh kebanyakan sistem yang wujud. Jika di lihat kepada perkembangan kawalan keselamatan komputer dan rangkaian, implementasi sistem pengesanan pencerobohan lebih kepada kawalan dan tindakan. Ini berkait rapat dengan bentuk tindakan kawalan dalam implementasi IDS seperti penyataan SANS

Institute (2002) yang menyatakan bahawa elemen penting IDS adalah kawalan dan tindakan, pengendalian kejadian, analisis dan juga laporan terhadap apa juga kejadian berkaitan.

2.4 *SNIFFER* ATAU SISTEM PENGESAN PENCEROBOHAN

Sniffer merupakan alatan yang digunakan untuk melihat setiap perlakuan dan aktiviti yang berlaku dalam rangkaian. Ianya beroperasi dengan mendapatkan data dalam laluan rangkaian dan membolehkan pengguna melihat apa yang dilakukan oleh pengguna lain dalam rangkaian. Namun apa yang dapat diperhati oleh *sniffer* adalah dalam bentuk data binari. Ini bermakna setiap data yang dilihat akan dianalisis dan ditukar kembali dalam bentuk asal supaya pengguna dapat memahami kandungan data yang didapati. Terdapat dua bentuk *sniffer*, satu untuk tujuan komersial yang digunakan dalam mengawal rangkaian dan satu lagi digunakan untuk tujuan pencerobohan.

Bermula dengan cara mendapatkan aktiviti data dalam rangkaian, penggunaan *sniffer* dan penggunaan Sistem Pengesan Pencerobohan adalah dua kaedah yang hampir sama cuma yang membezakan antara kedua alatan ini adalah boleh mengenal pasti masalah pencerobohan atau tidak.

Jika rangkaian bertujuan mendapatkan maklumat operasi rangkaian, maka penggunaan sniffer adalah lebih baik. *Sniffer* berupaya mendapatkan maklumat tentang apa yang berlaku dalam rangkaian. Cuma masalah timbul apabila pentadbir mendapati ada masalah berlaku dalam rangkaian dan tertulis dalam log *sniffer*, mungkin pada masa itu sudah

terlambat pentadbir mengelak dan menghalang penceroboh dan mungkin rangkaian telah diceroboh.

Penggunaan *sniffer* dilanjutkan dengan penambahan sistem pengesan penceroboh di mana *sniffer* sedia ada digunakan dalam pengoperasian IDS. Kewujudan penggunaan *sniffer* tidak dapat dielakkan dalam IDS. Dari sistem operasi Windows sehingga kepada Linux dan UNIX, penggunaan *sniffer* diperlukan untuk mendapat dan mengumpul data dan dibandingkan dalam pangkalan data IDS untuk melengkapkan IDS. Jelas penemuan IDS adalah bermula daripada penyelidik yang menggunakan *sniffer*, cuma mereka mahu *sniffer* yang lebih baik seperti mana IDS sekarang yang mampu mengesan jejak penceroboh. Dari situ pula terfikir bahawa pengguna IDS dapat memberi manfaat jika dapat bertindak secara automatik tanpa kawalan pentadbir untuk mengawal penceroboh dengan menggunakan sistem *firewall*.

Penggunaan IDS dalam pendekatan isu keselamatan bersama *firewall* dapat di implementasi dengan adanya gabungan mantap antara kedua-dua sistem ini. Polisi dinamik dapat dibentuk jika ianya di adaptasi antara satu sama lain menggunakan teknologi agen.

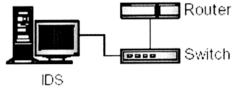
2.5 IMPLEMENTASI SISTEM PENGESAN PENCEROBOHAN

Sistem Pengesan Pencerobohan yang digunakan dalam kajian ini adalah Snort. Ianya merupakan salah satu Sistem Pengesan Pencerobohan yang baik dan menggunakan sistem terbuka. Rujuk jadual 2.5 untuk mengetahui kelebihan Snort berbanding IDS yang lain.

Untuk mengimplementasi penggunaan Snort dan IDS dalam rangkaian beberapa faktor perlu dilihat untuk menghasilkan konfigurasi yang betul dan tepat. Peletakan IDS perlu diteliti supaya ianya memberi lebih keberkesanan kepada pentadbir dalam mengawal rangkaian. Antara teknik kawalan yang digunakan dalam implementasi IDS adalah seperti berikut :

i. Penggunaan Switch Port Analyzer (SPAN)

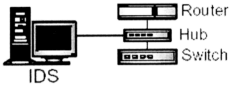
Penggunaan SPAN (Cisco, 2002) merujuk kepada penggunaan switch dalam rangkaian. Port ini merupakan port yang bertindak untuk menyalin semula kandungan paket dalam switch kepada satu switch yang ditetapkan bagi tujuan pemantauan.



Rajah 2.2 : Penggunaan Switch Port Analyzer (SPAN)

ii. Penggunaan Hub

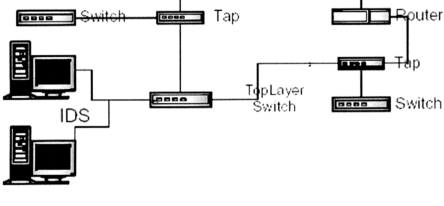
Hub yang digunakan untuk memantau pergerakan trafik adalah lebih mudah, tetapi ianya kurang praktikal. Ianya diletakkan antara router dan juga switch dengan mana IDS disambung melalui hub.



Rajah 2.3 : Penggunaan Hub

iii. Penggunaan Pili (*Tap*)

Penggunaan pili sama kepada penggunaan hub yang kurang praktikal. Peletakannya sama seperti peletakan hub. Rajah penggunaan pili boleh di lihat dimuka sebelah.



Rajah 2.4 : Penggunaan Pili (*Tap*)

2.6 SISTEM PENGESAN PENCEROBOHAN (IDS) - BENTUK & JENIS

Sistem pengesan pencerobohan mempunyai pelbagai bentuk dan jenis yang merujuk kepada tahap penggunaan masing-masing. Penghasilan IDS pula ada menggunakan sistem terbuka dan diedarkan secara percuma dan ada juga sistem yang dibuat secara komersial. Terdapat empat jenis IDS yang memainkan peranan yang penting dalam operasi IDS. Antaranya ialah :

i. Host Based IDS

IDS bentuk ini merupakan IDS yang mengawal log yang dikeluarkan dari beberapa sumber. Ianya sesuai diletakkan di dalam hos dan memantau aktiviti-aktiviti yang berlaku dalam hos itu sendiri. Ianya lebih kepada teknik penggunaan isu keselamatan sebagai kegunaan sendirian. Digunakan sebagai pengesan penceroboh berdasarkan tandatangan teknik pencerobohan.

ii. Network Based IDS

Mengawal semua laluan trafik yang melalui segmen IDS di mana agen diletakkan. Ia sering bertindak dalam dua bentuk keadaan iaitu *anomaly* dan tandatangan. Secara asasnya ianya bertindak seperti penghidu paket dalam rangkaian dan mempunyai mekanisme tambahan untuk mengesan penceroboh. Bergantung kepada kelajuan rangkaian, kekuatan komputer perlu di samakan bagi memastikan kecekapan IDS.

iii. Network Node IDS

Persekitaran rangkaian yang mempunyai kelajuan yang tinggi atau switch akan memberi masalah kepada banyak rangkaian IDS. Persekitaran ini sering kali gagal. Peratusan kejayaan adalah rendah kerana banyak paket hilang dalam rangkaian. Persekitaran sebegini sering kali menghalang perlakuan IDS. Dengan menggunakan Network Node, beberapa IDS dipecahkan kepada beberapa hos untuk mengawal rangkaian tertentu.

iv. Hybrid

Merupakan satu kaedah yang menggabungkan dua atau lebih IDS. Gabungan Network Node dengan hos IDS akan memberikan satu cara pengawalan yang baik. Ia selalu digunakan untuk tujuan yang kritikal. Sebagai contoh Sistem Pengesan Pencerobohan Prelude (2003).

Jadual 2.4 di bawah menunjukkan jenis-jenis IDS yang terdapat dalam pasaran. Kepelbagaian IDS dalam pasaran membuktikan kajian ke atas IDS telah lama dilakukan. Namun persoalannya kebanyakan IDS yang dicipta tidak memberi tindakan proaktif kepada sistem supaya sistem dapat menghalang penceroboh dari terus menceroboh sistem. Kebanyakan sistem yang dibina adalah merupakan sistem yang lebih ke arah komersial dan perniagaan serta tidak memenuhi keperluan rangkaian yang bertujuan menghalang pencerobohan dari berlaku. Walaupun begitu masih terdapat sistem dan diedarkan secara percuma untuk kegunaan persendirian yang mana memberi sedikit

keperluan kepada rangkaian untuk mengesan penceroboh. Jadual 2.4 menunjukkan sebahagian dari IDS yang wujud.

Jadual 2.4 : Contoh IDS yang wujud.

Jenis	Komersial	Freeware
Host Based	Intruder Alert Kane Secure Enterprise hp praesidium ids/9000 PréCis RealSecure OS Sensor KSM (Kane Security Monitor) Enterprise Guard eTrust Audit Appshield AuditGUARD Centrax (formerly eNTrax) Dragon Squire EMERALD eXpert-BSM Entercept 2.0 Entercept 2.0 Web Server Edition Tripwire	Swatch Abacus Project NOCOL Logsurfer
Network Based	CaptIO Prelude Shoki SHADOW Snort Tamandua Sentrus Sessionwall3 NID Netprowler E-Trust IDS CyberTracé BlackIce Sentry StealthWatch SecureNet Pro OpenSnort Netranger Manhunt Dragon Cisco Secure IDS BlackICE Guard RealSecure nPatrol	Prelude Shoki SHADOW Snort Tamandua

	Defense Worx IDS Network Flight Recorder Hogwash	
Network Node	BlackIce Agent RealSecure Server Sensor Tiny CMDS CentraxICE Snort (freeware) Cybercop Monitor SSE	-
Hybrid	Cybercop Monitor CentraxICE Real Secure Server sensor	-

2.7 SISTEM PENGESAN PENCEROBOHAN YANG WUJUD

Sistem pengesan pencerobohan banyak dibangunkan. Kebanyakan sistem dibangunkan adalah bertujuan untuk penggunaan sendiri. Terdapat pelbagai jenis sistem yang wujud termasuklah secara komersial atau sistem terbuka. Aspek-aspek yang dibandingkan merupakan aspek yang penting sahaja.

Perbandingan aspek yang dinyatakan adalah seperti:

i. Jenis IDS dan bentuk kawalan.

Bergantung kepada bentuk kawalan dan jenis IDS yang digunakan sama ada berasaskan rangkaian, hos atau *hybrid*.

ii. Kelajuan rangkaian yang dikawal.

Kelajuan rangkaian yang boleh digunakan oleh IDS yang dinyatakan. Merujuk kepada kebolehan IDS membuat kawalan terhadap rangkaian

tertentu sahaja. Ukuran yang dinyatakan adalah kelajuan rangkaian yang maksimum.

iii. Bentuk pengesanan.

Bentuk pengesanan yang digunakan dalam IDS adalah terbahagi kepada 2 iaitu *anamoly* dan berdasarkan tandatangan (*misuse*).

iv. Keserasian Platform.

Keserasian platform merujuk kepada platform yang boleh menjalankan IDS termasuklah penggunaan Linux, Unix dan Windows.

v. Operasi Masa Nyata

Kebolehan IDS beroperasi dalam masa nyata. Bermakna ianya menjalankan proses mengumpul data sambil menganalisis maklumat yang dikumpul.

vi. Kebal dari serangan.

Boleh melindungi diri sendiri daripada serangan luar. Bermakna ianya mempunyai mekanisme sendiri untuk menghalang dari serangan penceroboh.

vii. Masa Pengesanan

Bermaksud masa di antara masa mengesan pencerobohan dengan masa pencerobohan berlaku.

viii. Defragmentasi IP

Kebolehan memecahkan paket IP untuk mendapatkan tandatangan dan data berkaitan dalam paket.

ix. Bentuk Operasi

Kebolehan sistem beroperasi sama ada secara pemusatan atau teragih.

x. Sistem Terbuka

Sistem yang dibangunkan adalah terbuka atau sebaliknya. Sistem dibina bertujuan komersial ataupun tidak.

xi. Ciri –ciri IDS

Kebolehan yang boleh dilakukan oleh IDS. Ia juga merujuk kepada ciri tambahan yang boleh dilakukan oleh sistem.

2.8 PERBANDINGAN SISTEM PENGESAN PENCEROBOHAN

Jadual 2.5 : Perbandingan Sistem Pengesan Pencerobohan

Jenis IDS	Snort (2003)	Shadow (2003)	NFR NID (2003)	EMARALD (2003)	CyberCop (2003)
Bentuk Kawalan	Rangkaian	Rangkaian	Rangkaian	Host dan Rangkaian	Hybrid
Kelajuan Rangkaian	Rangkaian sederhana.	Rangkaian sederhana.	Rangkaian tinggi	Rangkaian tinggi.	Rangkaian Laju
Bentuk Pengesanan	Tandatangan	Tandatangan	Tandatangan/ Anomaly	Tandatangan/ Anomaly	Tandatangan
Keserasian Platform	Kebanyakan sistem yang ada.	Kebanyakan sistem yang ada	Memerlukan sistem teragih.	Solaris	WIN NT
Operasi Masa Nyata	Boleh	Tidak	Boleh	Ya	Ya
Kebal Serangan	Tidak	Tidak	Boleh	Tidak	Tidak
Masa Pengesanan	Sederhana	Tidak Nyata	Laju	Tidak Nyata	Tidak Nyata
Defragmentasi IP	Tidak	Tidak	Boleh	Tidak Nyata	-
Bentuk Operasi	Pemusatan	Pemusatan	Pemusatan	Pemusatan dan Teragih	Pemusatan
Sistem terbuka	Ya dan *Freeware*	Ya dan *Freeware*	Tidak dan bertujuan Komersial	Tidak dan bertujuan Komersial	Tidak dan bertujuan Komersial
Ciri IDS	Trafik Dns, dos, Serangan Finger, icmp, ms-sql, rpc, telnet, Web-attacks, web-cgi, web-frontpage, Web-iis, web-misc	Boleh mencipta sebarang tandatangan untuk tujuan pengesanan. Tidak terhad.	Menganalisis trafik SMTP, Denial of Services dan mengesan beberapa bentuk pencerobohan yang ditetapkan.	Integriti Fail, Serangan DOS, akses Salah, FTP dan kesalahan dalam katalaluan.	Menghalang lebih daripada 400 jenis pencerobohan.

2.9 SISTEM TERBUKA SNORT – KAJIAN TERHADAP IDS

Snort merupakan satu aplikasi yang dibangunkan secara terbuka yang memberi peluang kepada pengaturcara untuk memperbaiki dan mengemaskannya. Ia merupakan alatan automatik yang berupaya mengesan penceroboh. Snort berupaya mengesan secara setempat dan juga secara besar dalam rangkaian. Snort boleh bertindak sebagai pengawal dalam rangkaian dan kandungan dalam rangkaian boleh di lihat dan dianalisis melalui Snort. Tetapi Snort bukanlah merupakan sistem yang berupaya menghalang penceroboh apabila ianya mengesan penceroboh melalui pemantauan rangkaian yang di buat. Snort cuma berupaya untuk melakukan pemantauan seterusnya terpulang kepada pentadbir rangkaian.

Penghasilan teknologi IDS telah banyak menghasilkan pelbagai jenis IDS seterusnya merancakkan lagi dunia keselamatan rangkaian. Ini termasuklah sistem yang dicipta untuk tujuan komersial dan ada dihasilkan dengan percuma seperti sistem terbuka. Antaranya ialah Cisco Secure IDS (2003), NetSpecter (2003), RealSecure (2003), dan bagi sistem terbuka pula termasuklah Snort (2003), SHADOW(2003), dan TRIPWIRE (2003).

Snort merupakan IDS yang bersifat 'lightweight' dan berasaskan kepada IDS rangkaian. Penggunaan Snort adalah percuma tertakluk kepada cara penggunaan yang telah ditetapkan oleh Snort sendiri. Snort bersifat ramah pengguna kerana ianya dicipta secara sistem terbuka dan dapat digunakan oleh pelbagai platform termasuklah UNIX, Linux,

AIX dan juga Windows. Snort IDS amat mudah untuk di konfigurasi dan sesuai digunakan sama ada dalam rangkaian atau komputer peribadi.

Snort juga boleh bertindak sebagai *sniffer* yang mana boleh mengesan dan melihat perjalanan paket yang melalui rangkaian. Ianya bertindak sebagai IDS yang aktif yang boleh memberi amaran kepada pentadbir jika berlaku sebarang cubaan untuk menceroboh. Snort mesti diletakkan dalam rangkaian yang mempunyai laluan trafik yang tidak terlalu berat kerana kepantasan Snort bertindak adalah bergantung kepada kelajuan komputer yang menjalankan Snort.

Pengesan pencerobohan yang digunakan oleh Snort adalah berasaskan tandatangan (*signature*) bagi setiap jenis pencerobohan. Snort akan menghidu rangkaian dan membandingkan setiap paket dengan pangkalan data *signature*. Jika *signature* yang dibandingkan dengan paket adalah sama, maka ianya dianggap sebagai cubaan untuk menceroboh. Kemudian terpulang kepada pentadbir untuk mentafsir sama ada ianya pencerobohan atau tidak. Contoh tandatangan yang digunakan untuk mengesan penceroboh adalah seperti berikut:

Jadual 2.7 : Tandatangan dalam Snort IDS

```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (msg:"TELNET login
incorrect"; content:"Login incorrect"; flow:from_server,established;
reference:arachnids,127; classtype:bad-unknown; sid:718; rev:6;)
```

Tandatangan yang dinyatakan menunjukkan paket yang dihantar daripada *server* melalui port 23 dengan kandungan paket "Login incorrect" adalah satu bentuk cubaan pencerobohan. Daripada *signature* ini IDS dapat mengesan sumber dan destinasi paket dan seterusnya memberi amaran kepada pentadbir. Setiap tandatangan atau *signature* yang digunakan adalah berasaskan kepada beberapa faktor dan mesti mempunyai syarat berikut :

i. Jenis Flags, amaran atau log.

ii. Protokol digunakan sama ada TCP, UDP atau ICMP.

iii. Destinasi dan sumber port yang digunakan.

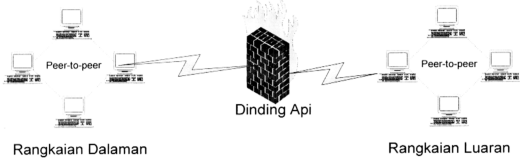
iv. Maklumat kandungan dalam paket yang dipantau.

Penggunaan Snort IDS bukan sahaja memberi peluang kepada pengaturcara untuk menambah dan memperbaiki sistem itu sendiri. Ianya memberi kelebihan kepada pengguna untuk menambah *signature* sendiri dan mempelbagaikan penggunaan Snort itu sendiri.

2.10 KAWALAN *FIREWALL*

Kawalan tambahan dengan penggunaan *firewall* merujuk kepada penggunaan kawalan keselamatan yang lama dan popular. *Firewall* merupakan teknologi yang popular dan pendekatannya amat memberi kesan dalam mengawal keselamatan rangkaian (Smith, R.N. & Bhattacharya, S, 1997). Ianya dicipta bertujuan untuk menghalang daripada penyalahgunaan rangkaian dalaman dari pengguna luaran. Ianya membahagikan dan membezakan rangkaian kepada dua iaitu rangkaian dari luar (*external*) dan rangkaian dalaman (*internal*). Selalunya *firewall* dicipta untuk menapis trafik di antara rangkaian

dikawal (internal) dengan mana-mana rangkaian luaran yang tidak dikawal. Ianya bertujuan untuk memastikan sumber-sumber yang tidak dipercayai dari luar rangkaian daripada memasuki rangkaian dengan mudah.



Rajah 2.5 : *Firewall*

Firewall konvensional berfungsi untuk mengawal laluan rangkaian. Dengan erti kata lain *firewall* membezakan pengguna dengan mengawal laluan pengguna luar dari masuk ke dalam rangkaian dengan bebas. Menurut Steven M. Bellovin (1999) walaupun ramai penyelidik berpendapat penggunaan *firewall* tidak begitu baik, namun penggunaan *firewall* masih merupakan mekanisme kawalan yang paling baik. *Firewall* yang sering digunakan untuk mengawal laluan trafik data ialah proxy *firewall* (Zalenski, R, 2002), penapisan paket dan penyamaran IP. Ketiga-tiga jenis *firewall* ini bertindak dengan cara yang berbeza. Cuma penyelidikan banyak dibuat dalam menggabungkan ketiga-tiga jenis ini menjadi satu bentuk *firewall* yang dinamik dan efisien. Namun sejak dulu penyelidikan lebih tertumpu kepada penyelidikan gateway (Smith, R.N. & Bhattacharya, S, 1997) *firewall* atau penapisan paket yang dianggap kurang efisien pada masa kini.

Untuk menjamin keupayaan *firewall* dalam rangkaian, beberapa perkara asas perlu di lihat pada *firewall* itu sendiri. Setiap *firewall* mesti mempunyai empat perkara asas yang berikut:

i. Polisi rangkaian yang merujuk kepada rekabentuk, proses, pemasangan dan juga penggunaan *firewall* itu. Ianya mentakrifkan bagaimana *firewall* hendak digunakan dalam sesuatu rangkaian. Ia juga merujuk kepada peraturan yang dikenakan dalam rangkaian yang membezakan rangkaian dalaman dan rangkaian luaran.

ii. Mekanisme Pengenalan merupakan mekanisme yang digunakan dalam proxy *firewall* untuk mengenal pasti pengguna yang boleh melepasi *firewall*.

iii. Penapisan paket berfungsi untuk menapis paket-paket yang melalui *firewall*. Selalunya penapisan paket berdasarkan syarat-syarat yang ditentukan dalam polisi *firewall* dengan melihat alamat sumber dan destinasi IP, port sumber dan destinasi serta protokol yang digunakan sama ada TCP,UDP atau ICMP.

iv. Aplikasi *gateway* biasa digunakan untuk menapis perkhidmatan yang tidak benarkan dalam polisi rangkaian. Ia selalu digabungkan dengan router penapis paket untuk menghasilkan keselamatan dan penapisan yang lebih baik.

Rekabentuk *firewall* sering kali berubah dan banyak rekabentuk telah diperkenalkan dari dahulu sehingga sekarang. Namun antara rekabentuk *firewall* yang wujud ialah personal *firewall*, router *firewall*, host *firewall* dan berbagai jenis *firewall* yang lain mengikut kesesuaian rangkaian. Generasi *firewall* konvensional masih ada digunakan tetapi *firewall* generasi baru yang memperkenalkan *firewall* teragih telah banyak menyelesaikan masalah terutamanya dalam polisi keselamatan dan juga laluan data. *Firewall* konvensional dahulu sering menjadi serangan penggodam kerana teknologi penggodam sekarang ini makin maju dan mudah (Gangadhram, M. & Hwang, K., 2001).

Terdapat dua rekabentuk asas *firewall* iaitu *host firewall* dan *gateway firewall*. Kedua-dua bentuk ini sering kali menjadi perbandingan dan juga digunakan dalam mengimplementasikan *firewall* pada masa kini. Bertitik tolak daripada itu juga wujud satu jenis *firewall* yang mana dinamakan *Distributed Micro-firewall* (Hwang, K. & Gangadharan, M., 2001). Ianya bertindak dalam mengawal rangkaian yang kecil tetapi diletak pada komputer dalam subnet-subnet yang berbeza mengikut kesesuaian pengguna dan pentadbir rangkaian. Micro-*firewall* bertindak lebih aktif berbanding dengan gateway *firewall* yang mana dapat dibezakan dengan beberapa perspektif. Penggunaan micro-*firewall* adalah menjadi lebih efisien jika penggunaannya digabungkan dengan penggunaan gateway *firewall* yang sedia ada. Ini bermakna gateway *firewall* tidak ditinggalkan sebaliknya penyelidikan dibuat dengan menumpukan sepenuh perhatian kepada penggabungan gateway dan micro-*firewall* itu sendiri. Tambahan dengan penggunaan sistem pengesanan pencerobohan secara tidak langsung akan memberi impak kepada polisi yang hendak dilaksanakan pada *firewall* tersebut.

Berikut adalah perbezaan antara gateway *firewall* dan juga Micro-*firewall* dari beberapa perspektif.

Jadual 2.8 : Perbezaan Micro-*firewall* dan Gateway *Firewall*

Perspektif	Gateway *Firewall*	Micro-*Firewall*
Polisi Kawalan	Mengawal keseluruhan data dalam rangkaian	Mengawal satu host sahaja.
Kesan Kepada Rangkaian	Menyebabkan rangkaian menjadi lembab (bottlenet).	Kesan yang sedikit akan dirasai oleh sistem terbabit sahaja
Keberkesanan	Berkesan kepada pengguna dari luar sahaja bukan dari dalam rangkaian.	Berkesan kepada kedua-dua rangkaian. Dalam dan luar.
Keupayaan	Terhad dan memerlukan tambahan keupayaan jika rangkaian bertambah.	Tidak perlu menambah keupayaan jika host ditambah.
Kegagalan	Tinggi. Jika *firewall* mengalami masalah, seluruh rangkaian akan mengalami.	Rendah. Jika *firewall* mengalami masalah, cuma sistem itu sahaja akan terlibat
Konfigurasi	Sukar kerana rangkaian yang besar memerlukan konfigurasi yang lebih komplek.	Mudah kerana ianya terhad kepada satu sistem sahaja.

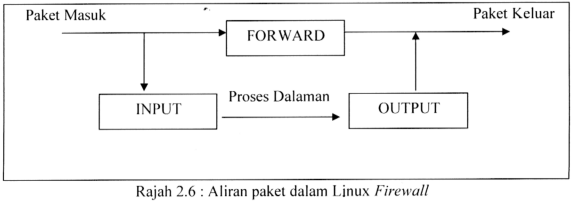
2.11 LINUX MICRO *FIREWALL*

Keselamatan dan penggunaan *firewall* dalam Sistem Operasi Linux lebih dikenali dengan micro-*firewall*, yang mana ianya dibangunkan dan direkabentuk untuk menjadi aplikasi *firewall* oleh kebanyakan pengguna sistem operasi Linux. Penggunaan *firewall* dalam Linux lebih kepada pengguna dalaman Linux sendiri. Kernel dalam Linux menyokong aplikasi *firewall* seperti penapisan paket (*packet filtering*). Ianya merupakan *firewall* yang terbina dalam Linux Kernel sejak Linux versi 2.0 dibangunkan. *Packet filtering* berfungsi pada aras network, yang mana data hanya boleh melepasi sistem berdasarkan polisi yang ditetapkan. Rujukan dilakukan pada paket bagi setiap jenis paket, sumber dan destinasi alamat serta maklumat port yang digunakan.

Linux *firewall* berfungsi adalah untuk menyokong kawalan keselamatan yang sedia ada dalam rangkaian. Ianya berfungsi untuk memberi sokongan tambahan seperti kawalan *microfirewall*. Linux *firewall* yang menggunakan penapisan paket berfungsi dalam berbagai kaedah dan bentuk aplikasi termasuklah penggunaan sebagai *Network Address Translation* (NAT) dan *masquerading router*. Linux *firewall* juga digunakan untuk servis *redirect* dan kawalan rangkaian. Pada masa sekarang Linux *firewall* lebih maju dan menumpukan aplikasi kawalan perhubungan antara dalaman dengan luaran.

Sejak dari dahulu, Kernel Linux menyokong aplikasi *micro-firewall*. Bermula dengan penggunaan Kernel 2.0 yang menggunakan *ipfwadm* seterusnya pengenalan *ipchains* pada Linux Kernel 2.2. Linux *firewall* yang terbaru menggunakan aplikasi *iptables* dan *Netfilter* yang dibentuk pada Kernel 2.4 selepas penggunaan *ipchains*. Dalam penggunaan *microfirewall* dalam linux terdapat operasi asas yang digunakan oleh ketiga-tiga bentuk kawalan ini. Rantaian kawalan diselaraskan kepada bentuk OUTPUT, INPUT dan FORWARD pada setiap polisi.

Penggunaan rantaian *firewall* di gambarkan seperti berikut:



Rajah 2.6 : Aliran paket dalam Linux *Firewall*

Tiga kitaran yang mewakili proses dalam Linux *firewall*. Setiap paket yang melalui kitaran di atas akan diperiksa dan dibandingkan dengan polisi *firewall*. Jika dalam polisi menyatakan DROP, maka paket akan digugurkan tetapi jika polisi paket menyatakan ACCEPT, maka paket akan diterima dan dimasukkan ke kitar seterusnya atau dikeluarkan terus untuk proses selanjutnya.

Setiap rantaian mempunyai polisi yang tertentu. Setiap satu polisi mempunyai tindakan untuk paket. Setiap paket akan dibandingkan dengan polisi-polisi tertentu, dan jika polisi itu dipenuhi maka paket akan terus dibandingkan dengan polisi seterusnya sehingga tamat atau tiada polisi lagi. Mekanisme dalam tindakan paket data yang melalui proses digambarkan seperti aturan berikut:

i. Apabila paket sampai ke sistem melalui rangkaian (bentuk fizikal Kad ethernet), Kernel akan melihat destinasi paket tersebut.

ii. Jika destinasi adalah untuk sistem dan rangkaian tersebut, paket seterusnya dilalukan ke dalam rantaian INPUT. Jika tiada masalah dalam rantaian tersebut, paket dilalukan ke rantaian seterusnya.

iii. Jika paket bukan untuk sistem dalam rangkaian maka paket akan dilalukan terus ke rantaian FORWARD. Jika rantaian FORWARD tidak di set maka paket akan digugurkan. Jika rantaian FORWARD diset, paket akan

memasuki rantaian tersebut. Jika polisi diterima dengan betul, paket di hantar keluar.

iv. Akhirnya, jika program dalam sistem hendak keluar dari sistem, paket ini mesti melalui rantaian OUTPUT. Jika polisi ditepati, baru paket dapat di keluarkan ke destinasi yang dikehendaki.

2.12 LINUX *FIREWALL* VERSI IPTABLES KERNEL 2.4.x

Iptables atau *Netfilter* (Netfilter, 2003) adalah versi terbaru dalam Linux *firewall* yang menggunakan Linux Kernel 2.4 dan ke atas. Versi iptables dalam Linux *firewall* ini merupakan hasil dari pembaikan ipfwadm dan ipchains dalam versi sebelumnya. Iptables masih mengekalkan ciri-ciri dalam Linux *firewall* asal dan menambahkan beberapa ciri-ciri baru yang lebih baik dan terkini. Ianya diperkemaskan dengan mengemaskini aplikasi NAT dalam ipchains sebelum ini dan memperkenalkan teknik baru dengan menggunakan teknik *packet mangling*. Teknik ini digunakan dalam Linux Kernel 2.4 sebagai tambahan kepada router dan *firewall* sedia ada.

Iptables dan Netfilter mempunyai beberapa ciri-ciri tambahan yang mana berfungsi dalam memberi keputusan dan kawalan yang lebih baik pada *firewall*. Antara ciri-ciri tambahan pada iptables berbanding ipchains dan ipfwadm :

i. Pengawalan yang lebih baik. Ia membuat pemeriksaan setiap paket yang ada dengan melihat setiap paket. Jelas memberi kelebihan kepada iptables

yang berupaya untuk menganalisis paket samaada paket itu dalam protokol icmp, udp atau tcp. Sebagai tambahan kepada ipchains, iptables berupaya membuat penapisan kepada icmp dengan melihat dan membenarkan cuma icmp echo-reply bila echo-request dilakukan. Ipchains tidak boleh berbuat demikian. Jelas kebanyakan pentadbir menghalang echo-request tetapi tanpa disedari menerima echo-reply dari teknik pencerobohan seperti Smurf (CERT, 1998), Trible Flood Network (CERT, 1999) dan juga Loki 2 back-door (Loki, 2002).

ii. Interaksi antara rantaian INPUT,OUTPUT dan FORWARD yang lebih berkesan berbanding sistem lama di mana perjalanan paket dari multi host-home berlaku dalam ketiga-tiga rantaian. *Iptables* membenarkan perjalanan berlaku dalam rantaian FORWARD sahaja.

iii. Pemisahan yang dilakukan antara penapisan paket dan juga *network address translation (NAT)* . Ianya dilakukan dalam rantaian NAT yang berbeza dalam rantaian *firewall* sebelum ini. Ipchains melakukan NAT, DNAT dalam rantaian yang sama, iptables memisahkan antara NAT dan rantaian *firewall* sendiri.

iv. Boleh melakukan penapisan mengikut tcp dan juga mengikut alamat MAC yang sebelum ini tidak dapat dilakukan oleh ipchains.

v. Berupaya untuk menghadkan sambungan rangkaian. Iptables berupaya untuk menghadkan sambungan dalam rangkaian seperti serangan SYN-flooding Denial of Service (SYN, 2003).

Perlu dijelaskan bahawa sistem yang akan dibangunkan dalam kajian ini akan menggunakan Linux *Firewall* kerana ianya memberikan kelebihan dan kemudahan dalam pengkajian. Linux *firewall* digunakan dan digabungkan dengan Sistem Pengesan Pencerobohan yang juga merupakan Sistem Terbuka iaitu Snort. Iptables digunakan dalam proses polisi *firewall* rangkaian.

2.13 IMPLEMENTASI GABUNGAN IDS DAN MICRO *FIREWALL*

Dalam menyatakan implementasi gabungan antara IDS dan juga *firewall*, beberapa faktor dan bentuk implementasi harus dinyatakan. Penggabungan ini melibatkan beberapa teknik yang mana menggunakan micro-*firewall* sebagai asas *firewall*. Micro-*firewall* merupakan sejenis *firewall* yang bertindak secara kecil dan beroperasi dalam satu hos dalam rangkaian LAN yang kecil.

Micro-*firewall* ditempatkan di dalam hos dan akan membentuk sempadan masing-masing dengan mengawal hos yang terbabit sahaja. Ini bermakna setiap rangkaian LAN mempunyai sekurang-kurangnya beberapa micro-*firewall* dan satu pengurus polisi. Setiap hos diletakkan satu micro-*firewall* yang bertindak sebagai *firewall* persendirian.

Fungsi bagi setiap implementasi micro-*firewall* bagi mengawal, mengelak, mengesan dan memberi amaran terdiri daripada 3 elemen asas iaitu pengurus polisi dan juga micro-*firewall* sendiri pada hos dan gateway *firewall*. Setiap hos mempunyai sempadan masing-masing dan setiap subnet LAN akan dibezakan dengan sempadan polisi yang dikawal oleh pengurus polisi. Bersamaan dengan implementasi itu, penggunaan IDS di letakkan sebagai pengawal dan pengesan pencerobohan.

Dalam sebuah organisasi yang mempunyai beberapa LAN akan membentuk beberapa pengurus polisi dan satu pengurus polisi akan membentuk sempadan polisi yang di dalamnya mempunyai beberapa hos yang menjalankan micro-*firewall*. IDS diletakkan di setiap hos untuk memberi lebih tinggi peratusan pengesanan. Analisis mengenai pencerobohan akan dilakukan di hos sendiri.

Implementasi micro-*firewall* dan IDS melibatkan beberapa langkah utama termasuklah:

i. IDS pada hos micro-*firewall* mengesan pencerobohan berlaku.

ii. IDS memberi tindakan dengan memberitahu pengurus polisi, dan seterusnya membuat polisi baru.

iii. Polisi baru dihantar kepada setiap pengurus polisi yang lain untuk mengemaskini polisi.

iv. Polisi rangkaian telah berubah, *firewall* menghalang penceroboh dari terus menceroboh.

Hasil gabungan dan tindakan dari ketiga-tiga elemen asas yang dinyatakan, jelas menunjukkan bahawa proses untuk menghalang, mengesan, mengawal dan membuat tindakan dalam masa nyata dapat dilaksanakan dengan baik. Secara kolektif, dalam menghasilkan proses tindakan masa nyata ini pengemaskinian polisi pada *firewall* perlu dilaksanakan secara dinamik bagi menghalang sebarang cubaan menceroboh sama ada dari dalam atau luar (Smith, R.N. & Bhattacharya, S, 1997). Perlu dinyatakan juga bahawa setiap tindakan yang dilaksanakan perlu memberi peluang kepada setiap pengurus polisi untuk berkomunikasi antara satu sama lain supaya ianya lebih baik dan cepat serta tepat. Implementasi IDS dan micro-*firewall* secara teragih memberi kelebihan kepada pentadbir untuk mengawal rangkaian agar menjadi lebih baik.

Polisi sebegini dengan mana memberi peluang kepada micro-*firewall* mengemaskini *firewall* masing-masing akan memberi kelebihan dalam mengelak serangan dari dalam. Penggunaan gateway *firewall* selalunya memberi kawalan dan halangan serangan pengguna dari luar. Perlu juga diingatkan bahawa pengguna dalam juga terlibat dalam polisi keselamatan rangkaian.

2.14 PERSEKITARAN MULTICAST

Dalam persekitaran rangkaian, perhubungan antara satu sistem dengan satu sistem yang lain memerlukan protokol dan teknik tertentu. Kebanyakan transmisi dalam TCP atau UDP, servis unicast digunakan yang berkemampuan menghantar mesej satu nod pada satu masa. Semua transmisi unicast adalah titik ke titik (*point to point*). Jika satu transmisi hendak dihantar kepada beberapa destinasi dengan menggunakan unicast

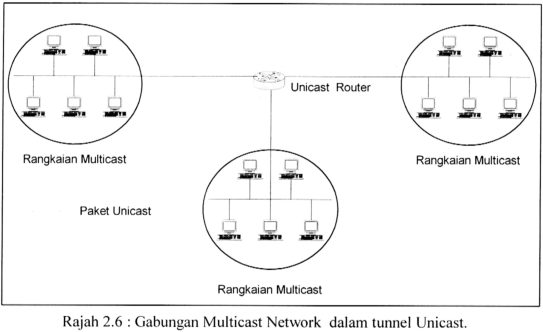
transport servis, nod unicast akan digandakan kepada beberapa nilai supaya dapat menghantar kepada semua penerima. Ini bermakna proses *replicated unicast* berlaku untuk membolehkan transmisi berjaya.

Dengan demikian untuk memudahkan transmisi kepada beberapa destinasi dengan mudah, penggunaan multicast transport servis digunakan. Dengan menggunakan kemudahan multicast ini, satu transmisi tidak perlu menggandakan nod untuk tujuan penghantaran seperti unicast. Ianya cuma menggunakan kemudahan multicast yang mana membolehkan data dikirim ke beberapa destinasi dengan menggunakan satu nod sahaja.

Dalam menjalankan operasi/aplikasi yang menggunakan pengiriman data yang banyak kepada beberapa penerima yang berbeza, multicast adalah cara yang terbaik. Aplikasi yang menggunakan *unicast* sesuai ditukarkan kepada bentuk multicast seperti transmisi radio dan juga video dalam rangkaian. Pada masa dahulu dan sehingga sekarang satu kajian menyeluruh berkenaan dengan multicast backbone (Mbone) (Erikson, H., 1994) telah dan masih dijalankan oleh penyelidik.

Mbone telah memperkenalkan penggunaan IP multicast dengan menggunakan protokol *Distance Vector Multicast Routing Protocol* (DVMRP). Dari mula sehingga sekarang, DVMRP yang stabil digunakan pada platform UNIX dengan aplikasi mrouted. Pada mulanya Mbone diperkenalkan pada peranti UNIX dengan menggunakan tunnel DVMRP. Mekanisme tunnel mendefinisikan bahawa dua peranti UNIX berhubung dengan menggunakan aplikasi mrouted. Ianya mengimplementasikan penghantaran IP

multicast dengan menggunakan Unicast. Mekanisme ini membenarkan *encapsulate* IP multicast dimasukkan dalam unicast paket dan cuma multicast router sahaja menghantar multicast di setiap penghujung paket. Secara kasar ianya merujuk kepada perhubungan antara dua atau lebih gabungan rangkaian multicast dengan menggunakan transmisi unicast. Bermakna paket Multicast ke rangkaian multicast lain melalui transmisi unicast.



Rajah 2.6 : Gabungan Multicast Network dalam tunnel Unicast.

Komunikasi multicast merujuk kepada komunikasi satu kepada banyak dan banyak kepada banyak dalam menyampaikan data. Penyelidikan mengenai multicast masih lagi berjalan dengan rancak dan masih lagi tiada penghujung mengenai titik akhir bagi multicast. IP multicast mula diperkenalkan dan dikaji secara menyeluruh semasa pengkajian mengenai "audiocast" pada 1992 (Casner, S. & Deering, S., 1992). Dalam memperkenalkan model berkaitan dengan IP multicast, Deering (1991) membuat satu standard berkaitan dengan multicast. Model ini menggambarkan bagaimana multicast beroperasi dalam rangkaian sama ada proses penghantaran atau penerimaan. Model

berkaitan (Deering, Stephen E. & Cheriton, David R., 1990) dengan multicast adalah seperti berikut:

i. Semantic IP, merujuk kepada sumber yang boleh menghantar multicast paket pada bila-bila masa tanpa mengetahui sama ada ia berada dalam kumpulan atau tidak. IP multicast adalah berasaskan kepada UDP dan bukan TCP.

ii. Kumpulan terbuka. Sumber cuma perlu tahu alamat multicast tanpa perlu mengetahui kumpulan multicast. Sumber tidak perlu dan tidak semestinya menjadi ahli kumpulan. Setiap kumpulan boleh mempunyai sumber yang berbeza.

iii. Kumpulan Dinamik. Kumpulan Multicast boleh menyertai dan meninggalkan kumpulan pada bila-bila masa tanpa perlu memaklumkan kepada sesiapa.

Model yang diperkenalkan oleh Stephen E. Deering (1990) ini tidak meliputi perbincangan mengenai keperluan dalam rangkaian bagaimana ianya hendak dihala. Model ini juga tidak menerangkan secara terperinci mengenai mekanisme untuk memberi kualiti pada servis, keselamatan dan juga peletakan alamat.

Bertitik tolak daripada itu wujud satu topologi Multicast yang menumpukan kepada rangkaian setempat. Multicast Rangkaian setempat (*Local-Area Multicast*) merujuk kepada keupayaan multicast dalam menangani masalah dalam rangkaian setempat. Ianya bermula dengan penyelidik memikirkan bahawa menangani masalah unicast dalam rangkaian setempat adalah dengan cara menggunakan multicast jika maklumat yang hendak dihantar sama dan tidak perlu sebarang arahan atau tindakan. Ini bermakna penerima hanya menerima sahaja tanpa perlu mempersoalkan apa yang dihantar. Penggunaan unicast perlu memaksa penerima dan penghantar mengetahui maklumat antara satu sama lain.

Kewujudan *local-area* Multicast adalah disebabkan masalah protokol multicast dalam rangkaian yang besar. Masalah ini bukan bermakna multicast tidak boleh berkomunikasi dalam rangkaian yang besar tetapi ianya memerlukan penumpuan yang lebih kepada rangkaian yang bukan dalam struktur multicast. Penyelidikan dalam multicast memberi lebih menumpuan kepada penyelidikan multicast dalam rangkaian setempat. Jika ada rangkaian yang membenarkan komunikasi multicast dalam rangkaian besar, ianya tidak dapat memenuhi keperluan yang baik sebagaimana protokol lain seperti komunikasi unicast. Kajian dalam menstabilkan multicast dalam rangkaian setempat memberi kelebihan kepada penggunaan multicast dengan mengabungkan multicast dan unicast dalam komunikasi rangkaian yang lebih besar.

Secara teori, rangkaian multicast digambarkan sebagai satu rangkaian yang besar di mana setiap rangkaian disambung antara satu sama lain dengan membolehkan rangkaian

multicast berfungsi. Tetapi sebenarnya rangkaian multicast tidak seperti yang digambarkan. Ianya wujud secara berasingan antara rangkaian dengan rangkaian lain dan kebanyakan rangkaian tidak mahu disambungkan kepada talian yang menyokong multicast. Multicast sebenarnya boleh diwujudkan di mana-mana rangkaian sama ada ianya menyokong sambung keluar atau tidak. Tambahan pula boleh dikatakan semua rangkaian yang wujud membolehkan komunikasi multicast sama ada disedari atau tidak, cuma yang membezakan antara satu rangkaian dengan lain ialah sama ada multicast itu disambung ke MBone atau sebaliknya.

Secara tidak disedari multicast telah memberi kesan dan impak yang besar dalam komunikasi dalam rangkaian setempat serta memberi kaedah perolehan data yang lebih baik dan pantas. Namun persoalan mengenai multicast dalam rangkaian setempat masih dipersoalkan mengenai keselamatan dan juga keserasian dalam rangkaian.

2.15 KESELAMATAN MULTICAST

Isu keselamatan dalam komunikasi multicast merupakan topik yang tidak boleh dianggap mudah. Ianya bukan seperti penggunaan polisi keselamatan seperti unicast. Penggunaan isu keselamatan dalam komunikasi unicast mudah kerana ianya merujuk kepada sambungan satu ke satu yang mana penerima dan penghantar mudah dikenali. Berbeza dengan komunikasi multicast yang mana penerima tidak dapat ditentukan dengan jelas dan tepat kerana penerima hanya dikenal pasti dengan menggunakan satu alamat multicast sahaja.

Jika dilihat kepada penggunaan komunikasi multicast beberapa isu keselamatan boleh disentuh dengan melihat keperluan komunikasi multicast itu sendiri. Isu keselamatan di lihat lebih sukar dalam komunikasi multicast kerana beberapa faktor, antaranya:

i. Bukan komunikasi unicast.

   Komunikasi multicast tidak sama dengan komunikasi unicast di mana dalam komunikasi unicast, penerima dan penghantar boleh diketahui dengan mudah.

ii. Penerima tidak diketahui oleh penghantar.

   Penerima tidak dapat ditentukan dengan tepat. Bermakna setiap penerima hanya perlu menggunakan alamat kumpulan dalam komunikasi multicast untuk menerima maklumat dari penghantar.

iii. Penerima juga boleh bertindak sebagai penghantar.

   Penerima yang menerima maklumat daripada penghantar boleh bertindak sebagai penghantar semula kerana penerima mengetahui kumpulan multicast dan memudahkan penerima menjadi penghantar kedua dan bertindak sebagai pencerobohuntuk menggagalkan komunikasi.[1]

iv. Masalah skala dalam rangkaian.

   Sempadan multicast masih dalam penyelidikan, maka skala komunikasi multicast masih lagi besar. Rekabentuk multicast tidak terhad dan ini menyukarkan proses kawalan data dan keselamatan rangkaian.

Dengan wujudnya faktor yang dinyatakan, isu keselamatan dalam komunikasi multicast mestilah ditakrif dengan terperinci. Dalam mentakrif penggunaan polisi keselamatan dalam rangkaian menggunakan komunikasi multicast, beberapa keperluan kawalan diperlukan yang mana lain daripada keperluan asas dalam komunikasi unicast. Secara umumnya adalah seperti berikut:

i. **Kawalan ahli dalam kumpulan Multicast.**

Perkara utama yang perlu ditekankan di sini ialah penerima yang hendak menerima data dalam kumpulan multicast mestilah ditakrifkan secara tepat. Ini adalah bertujuan memastikan hanya kumpulan yang tertentu sahaja menerima paket yang hantar. Pengguna *public-key* boleh digunakan untuk menetapkan kumpulan penerima. Juga proses memasuki dan meninggalkan kumpulan multicast mestilah dilihat dengan lebih mendalam.

ii. **Data Kumpulan**

Semua maklumat yang dihantar dengan menggunakan komunikasi multicast mestilah menggunakan teknologi enkripsi yang baik. Ini bermakna setiap maklumat yang hendak dihantar mestilah menggunakan algoritma tertentu dalam teknologi kriptografi. Teknologi kriptografi seperti penggunaan *private key* boleh digunakan untuk memastikan cuma kumpulan penerima sahaja boleh mentafsir data.

iii. **Sumber Data**

Semua penerima data dari kumpulan multicast boleh memastikan cuma satu sumber sahaja boleh menghantar maklumat. Ini bermakna setiap penerima dalam komunikasi multicast sudah mengetahui sumber data. Ini bertujuan

mengelakkan daripada penerima menerima data yang lain daripada penghantar yang salah.

Penggunaan teknologi kriptografi banyak mempengaruhi keselamatan data dalam komunikasi multicast. Merujuk kepada penggunaan kriptografi dalam komunikasi multicast, penggunaan kunci dalam rekabentuk keselamatan komunikasi multicast digunakan. Modul MIKE (*Multicast Internet Key Exchange*) digunakan untuk menguruskan kunci. Modul MIKE ini berfungsi dalam menghasilkan Multicast Security Association (MSA) yang sama dengan standard *Security Association*. Penggunaan MSA bertanggungjawab dalam mengendalikan autentikasi dan kunci data sewaktu komunikasi. Multicast IKE tidak sama dengan Unicast IKE.

2.16 STRUKTUR IP MULTICAST SKOP UNTUK IP VERSI 4

Struktur skop IP multicast merupakan peletakan alamat IP yang lain dari skop IP biasa. Skop IP merujuk kepada 2 iaitu skop pentadbiran dan juga skop berdasarkan *Time to Live* (TTL). Secara umumnya IPv4 memperuntukkan IP untuk multicast dalam lingkungan IP 224.0.0.0 sehingga 239.255.255.255.

Skop IP multicast memperuntukkan skop setempat dan skop global berdasarkan lingkungan yang dinyatakan di atas. Beberapa kumpulan IP yang dikhaskan untuk simpanan iaitu bermula 224.0.0.0 sehingga 224.0.0.254. Kumpulan IP ini hanya digunakan dalam rangkaian setempat (LAN). Selalunya ia digunakan untuk penggunaan protokol halaan dan juga penyelenggaraan. Penggunaan kumpulan multicast ini adalah

bertujuan untuk menghalang *multicast router* menghala keluar datagram multicast ke luar dari rangkaian setempat.

Merujuk kepada skop TTL pula, kebanyakan IP Multicast menggunakannya sebagai tambahan kepada skop IP yang sedia ada. Penggunaan TTL berperanan dalam menghalang daripada data multicast keluar daripada rangkaian yang sepatutnya.

TTL yang tinggi akan memberi kesan kepada perjalanan paket multicast dalam rangkaian. Sama seperti paket dalam unicast, paket multicast akan mengalami kekurangan 1 TTL apabila melepasi router. Bermakna TTL yang sedikit akan menghadkan perjalanan paket multicast. Penggunaan TTL dalam menghadkan komunikasi adalah terhad.

Jadual 2.9 : Skop TTL Multicast

TTL	Skop
0	Terhad kepada host yang sama
1	Terhad kepada subnetwork yang sama
15	Terhad kepada site yang sama
63	Terhad kepada region yang sama
127	Seluruh Dunia
191	Seluruh dunia; talian terhad
255	Tidak Terhad