

(R)

Mekanisme Pengemaskinian Polisi Keselamatan *Firewall* dengan Pendekatan Sistem Pengesan Pencerobohan dan Protokol Multicast

Tesis ini dihantar kepada

Fakulti Sains Komputer & Teknologi Maklumat

Universiti Malaya

Dalam memenuhi keperluan pengijazahan

Sarjana Sains Komputer

oleh

NOR BADRUL ANUAR JUMA'AT

(WGAZ01006)

Julai, 2003

Penyelia : Prof. Dato' Ir. Dr. Mashkuri Hj. Yaacob



ABSTRAK

Sistem pengesan pencerobohan merupakan sistem yang bertindak dalam mengesan pencerobohan yang berlaku dalam masa nyata. Walaupun begitu masih terdapat kelemahan dalam penggunaan sistem ini kerana tiada mekanisme yang menghalang terus penceroboh dari terus menceroboh.

Bertitik tolak daripada itu, tesis ini menghuraikan keperluan penyelidikan dan proses dalam menghasilkan satu mekanisme tindakan proaktif bagi menghalang penceroboh dari terus menceroboh. Mekanisme yang dibangunkan merupakan agen yang bertindak sebagai pemantau, pemberitahu dan penggerak bagi mengubah polisi *firewall* dalam rangkaian. Perubahan polisi adalah berdasarkan kepada bentuk dan sumber serangan. Perubahan polisi ini dapat dilakukan dengan mudah, cepat, masa nyata dan boleh berlaku tanpa pengetahuan pentadbir. Ini seterusnya mengelak dari penceroboh dari terus menceroboh.

Seterusnya tesis ini membuktikan bahawa, tindakan proaktif Sistem Pengesan Pencerobohan boleh digunakan dalam mengemaskini polisi keselamatan *firewall*. Tambahan penggunaan protokol multicast dapat mempercepatkan proses pengemaskinian polisi tersebut.

PENGHARGAAN

Di kesempatan ini saya ingin mengucapkan jutaan terima kasih kepada penyelia saya, Prof. Dato' Ir. Dr. Mashkuri Hj. Yaacob kerana telah memberi banyak sokongan, bantuan dan juga nasihat sepanjang pengajian dan penyelidikan saya.

Saya juga ingin mengucapkan ribuan terima kasih kepada Prof. Madya. Dr. Zainab Awang Ngah, En. Ling Teck Chaw dan En. Phang Keat Keong kerana telah banyak membantu, memberi nasihat serta pandangan dalam menyempurnakan penyelidikan ini. Terima kasih kerana memberi peluang menggunakan peralatan rangkaian yang mungkin tidak dapat diperolehi di tempat lain.

Terima kasih kepada Prof. Madya Dr. Wan Mohd Azhar dan Prof. Dr. Mohd Razali Agus, pengetua dan bekas pengetua Kolej Kediaman Tun Ahmad Zaidi kerana sudi memberi peluang menggunakan peralatan rangkaian di kolej.

Terima kasih tidak terhingga kepada En. Ang Tan Fong, Puan Miss Laiha Mat Kiah , En. Jeffrey Chua Sers Loong, En. Jimmy Tan Kai Hong, En. Auzani Fikry, En. Amiruddin Kamsin, pensyarah-pensyarah dan pengajar-pengajar FSKTM atas bantuan, sokongan dan tujuan ajar dalam masa membuat penyelidikan di Makmal FSKTM.

Akhir sekali, terima kasih diucapkan kepada staf FSKTM, staf dan pelajar Kolej 10 atas sokongan moral dan bantuan lain dalam proses menyiapkan penyelidikan ini.

KANDUNGAN

ABSTRAK	i
PENGHARGAAN	ii
KANDUNGAN	iii
SENARAI RAJAH	vii
SENARAI JADUAL	viii
ABBRIBRASI	x
BAB 1	1
PENGENALAN KEPADA PENGKAJIAN.....	1
1.0 PENGENALAN.....	1
1.1 OBJEKTIF PROJEK	8
1.2 MASALAH YANG AKAN DISELESAIKAN.....	9
1.3 SKOP PROJEK	10
1.4 ORGANISASI TESIS.....	10
BAB 2	13
KAJIAN PERPUSTAKAAN : KESELAMATAN RANGKAIAN DAN KOMPUTER	13
2.0 PENGENALAN.....	13
2.1 KAWALAN KESELAMATAN DALAM & LUARAN.....	16
2.2 SISTEM PENGESANAN PENCEROBOHAN	18
2.3 PRINSIP SISTEM PENGESANAN PENCEROBOHAN (IDS).....	22
2.4 SNIFFER ATAU SISTEM PENGESAN PENCEROBOHAN.....	24
2.5 IMPLEMENTASI SISTEM PENGESAN PENCEROBOHAN.....	26
2.6 SISTEM PENGESAN PENCEROBOHAN (IDS) - BENTUK & JENIS	28
2.7 SISTEM PENGESAN PENCEROBOHAN YANG WUJUD	31
2.8 PERBANDINGAN SISTEM PENGESAN PENCEROBOHAN	34
2.9 SISTEM TERBUKA SNORT – KAJIAN TERHADAP IDS.....	35
2.10 KAWALAN FIREWALL.....	37

2.11	LINUX MICRO FIREWALL	41
2.12	LINUX FIREWALL VERSI IPTABLES KERNEL 2.4.x.....	44
2.13	IMPLEMENTASI GABUNGAN IDS DAN MICRO FIREWALL	46
2.14	PERSEKITARAN MULTICAST.....	48
2.15	KESELAMATAN MULTICAST.....	53
2.16	STRUKTUR IP MULTICAST SKOP UNTUK IP VERSI 4	56
BAB 3		58
POLISI DALAM ISU KESELAMATAN		58
3.0	PRINSIP KEMASKINI POLISI.....	58
3.1	KONSEP POLISI FIREWALL.....	59
3.1.1	Polisi Persekutaran Berisiko Rendah.....	60
3.1.2	Polisi Persekutaran Berisiko Sederhana.....	61
3.1.3	Polisi Persekutaran Berisiko Tinggi	62
3.2	POLISI BERKESAN RANGKAIAN	63
3.2.1	Ancaman.....	64
3.2.2	Perkara Dinalai.....	65
3.3	PRINSIP PENGEMASKINIAN POLISI FIREWALL.....	69
3.4	PROAKTIF PENGESAN PENCEROBOHAN	70
3.5	KOMUNIKASI MULTICAST & PENGEMASKINIAN POLISI	73
3.6	MULTICAST DAN BROADCAST	78
3.7	KEBARANGKALIAN DALAM MENANGANI ISU KESELAMATAN	79
BAB 4		83
RANGKA KERJA SISTEM REDALERT		83
4.0	PENGOPERASIAN SISTEM REDALERT	83
4.1	PENDEKATAN DINAMIK SISTEM REDALERT	87
4.2	SNORT DAN SISTEM REDALERT	89
4.3	POLISI FIREWALL SISTEM REDALERT	90
4.4	TRANSMISI DATA SISTEM REDALERT	94

4.5 RANGKA KERJA SISTEM <i>REDALERT</i> SECARA KESELURUHAN	96
BAB 5	102
REKABENTUK DAN PENDEKATAN SISTEM REDALERT.....	102
5.0 REKABENTUK SISTEM <i>REDALERT</i>	102
5.1 HIERARKI ALGORITMA APLIKASI <i>REDALERTIDS</i>	104
5.2 FUNGSIAN APLIKASI <i>REDALERTIDS</i>	106
5.3 REKABENTUK INTEGRASI PANGKALAN DATA.....	110
5.4 ALGORITMA POLISI <i>FIREWALL</i>	113
5.5 FUNGSIAN TRANSMISI DATA SISTEM <i>REDALERT</i>	117
5.6 PENDEKATAN SISTEM REDALERT DALAM RANGKAIAN	120
BAB 6	123
IMPLIKASI KESELAMATAN RANGKAIAN & KEPUTUSAN KE ATAS KAJIAN	123
6.0 IMPLIKASI KESELAMATAN RANGKAIAN	123
6.1 IMPLEMENTASI DALAM RANGKAIAN SEBENAR	124
6.2 TOPOLOGI RANGKAIAN	128
6.2.1 Topologi Rangkaian Fasa 1	128
6.2.2 Topologi Rangkaian Fasa 2	129
6.2.3 Topologi Rangkaian Fasa 3	130
6.3 BENTUK SERANGAN.....	131
6.3.1 LANGuard Network Scanner.....	131
6.3.2 FTP Brute Force Attack	132
6.3.3 Telnet Brute Force Attack	133
6.4 KEPUTUSAN HASIL SERANGAN	134
6.4.1 Fasa 1	135
6.4.2 Fasa 2	136
6.4.3 Fasa 3	137
6.5 KESIMPULAN.....	140

BAB 7	141
PENUTUP DAN CADANGAN MASA HADAPAN	141
7.1 KEPUTUSAN BERDASARKAN TEORI DAN PRAKTIKAL	142
7.2 RUMUSAN	143
7.3 KELEBIHAN SISTEM	145
7.4 KELEMAHAN SISTEM	148
7.5 CADANGAN MASA DEPAN	149
7.6 SUMBANGAN PENYELIDIKAN	151
RUJUKAN.....	154
BIBLOGRAFI.....	158
LAMPIRAN I - IP MULTICAST	160

SENARAI RAJAH

Rajah 2.1 : Perkembangan Sistem Pengesan Pencerobohan	19
Rajah 2.2 : Penggunaan Switch Port Analyzer (SPAN).....	26
Rajah 2.3 : Penggunaan Hub	27
Rajah 2.4 : Penggunaan Pili (<i>Tap</i>).....	27
Rajah 2.5 : <i>Firewall</i>	38
Rajah 2.6 : Aliran paket dalam Linux <i>Firewall</i>	42
Rajah 3.1 : Komunikasi multicast.....	75
Rajah 4.1 : Konfigurasi ringkas rekabentuk rangkaian sistem RedAlert	86
Rajah 4.2 : Saling bertindak Snort dan RedAlert menggunakan MySQL	89
Rajah 4.3 : Tindakan Lanjutan pada <i>Firewall</i> selepas RedAlert.....	91
Rajah 4.4 : Komunikasi multicast menggunakan unicast.....	94
Rajah 4.5 : Sistem RedAlert secara keseluruhan	97
Rajah 6.1 : Topologi ujian fasa1	128
Rajah 6.2 : Topologi ujian fasa 2	129
Rajah 6.3 : Topologi ujian fasa 3	130

SENARAI JADUAL

Jadual 2.1 : Perbezaan antara Kawalan dalaman dan luaran	17
Jadual 2.2 : Kod dalam bentuk hexadesimal	21
Jadual 2.3 : Kod dalam ASCII.....	21
Jadual 2.4 : Contoh IDS yang wujud.....	30
Jadual 2.5 : Perbandingan Sistem Pengesan Pencerobohan	34
Jadual 2.7 : Tandatangan dalam Snort IDS	36
Jadual 2.8 : Perbezaan Micro- <i>firewall</i> dan Gateway <i>Firewall</i>	41
Jadual 2.9 : Skop TTL Multicast	57
Jadual 3.1 : Perbezaan antara multicast dan Unicast.....	74
Jadual 3.2 : IP untuk transmisi Broadcast.....	79
Jadual 4.1 : Konfigurasi teknikal bagi setiap rangkaian	98
Jadual 4.2 : Perbezaan transmisi multicast dan unicast	100
Jadual 5.1 : Deskripsi dalam pangkalan data.....	110
Jadual 5.2 : Kegunaan pangkalan data dalam sistem RedAlert.....	111
Jadual 5.3 : Struktur pangkalan data RedAlert.....	112
Jadual 5.4 : Struktur pangkalan data Redaction.....	112
Jadual 5.5 : Pengiraan masa menggunakan timered()	116
Jadual 5.6 : Perbezaan fungsi Uni RedAlert dan Multi RedAlert	121
Jadual 6.1 : Konfigurasi komputer untuk ujian fasa 1-3	125
Jadual 6.2 : Konfigurasi hōs dan OS serta aplikasi yang digunakan dalam ujian	126
Jadual 6.3 : Konfigurasi Komputer Penyerang	131
Jadual 6.4 : Konfigurasi pendekatan kawalan keselamatan bagi setiap ujian serangan	134
Jadual 6.5 : Keputusan ujian Fasa 1.....	135
Jadual 6.6 : Keputusan ujian Fasa 2.....	136
Jadual 6.7 : Keputusan ujian Fasa 3.....	138
Jadual 6.8 : Keputusan ujian Fasa 3.....	138

ABBRIBRASI

ASCII	American Standard Code for Information Interchange
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
ATM LSR	Asynchronous Transfer Mode Label Switching Router
CPU	Center Processing Unit
DVMRP	Distance Vector Multicast Routing Protocol
DOS	Disk Operating System
DNAT	Dynamic Network Address Translation
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMPv2	Internet Group Management Protocol Version 2
IGMPv3	Internet Group Management Protocol Version 3
IMAP	Internet Message Access Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol Version 6
IPv4	Internet Protocol Version 4
IPX	Internetwork Packet Exchange

ICMPv4	Internet Control Message Protocol Version 4
ICMPv6	Internet Control Message Protocol Version 6
IGRP	Interior Gateway Routing Protocol
LAN	Local Area Network
MAC	Media Access Control
MIKE	Multicast Internet Key Exchange
NAT	Network Address Translator
OSPF	Open Shortest Path First
OSI	Open System Interconnection
PDU	Protocol Data Unit
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast – Sparse Mode
PIM-DM	Protocol Independent Multicast – Dense Mode
POP3	Post Office Protocol
RCP	Remote Copy Protocol
RIP2	Routing Information Protocol version 2
Rlogin	Remote Login
RSVP	Resource Reservation Protocol.
SPAN	Switched Port Analyzer
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TOS	Type of Service
TTL	Time-to-live
URL	Uniform Resource Locator, Universal Resource Locator

UDP	User Datagram Protocol
VBR	Variable Bit Rate
VRRP	Virtual Router Redundancy Protocol
VLAN	Virtual Local Area Network
VMTP	Versatile Message Transaction Protocol
WAN	Wide Area Network
WWW	World Wide Web