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 Sera 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

SENARAI RAJAH

SENARAI JADUAL

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