"Saya akui bahawa saya telah membaca karya ini pada pandangan saya karya ini adalah memadai dari skop dan kualiti untuk tujuan penganugerahan Ijazah Sarjana Muda Kejuruteraan Elektronik (Elektronik Industri)"

Tandatangan : 

Nama Penyelia : En. Redzuan Bin Abdul Manap

Tarikh : 1/4/2005

KAJIAN KES MENGENAI PENCEROBOHAN SISTEM RANGKAIAN KOMPUTER DAN CARA MENGATASINYA

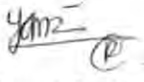
MARZIAN HAIRANI BINTI MAT ISHAK

Laporan Ini Dikemukakan Sebagai Memenuhi Sebahagian Daripada Syarat Penganugerahan Ijazah Sarjana Muda Kejuruteraan Elektronik (Elektronik Industri)

Fakulti Kejuruteraan Elektronik dan Kejuruteraan Komputer
Kolej Universiti Teknikal Kebangsaan Malaysia

Mac 2005

"Saya akui laporan ini adalah hasil kerja saya sendiri kecuali ringkasan dan petikan yang tiap-tiap satunya telah saya jelaskan sumbernya."

Tandatangan : 

Nama Penulis : Marzian Hairani Binti Mat Ishak

Tarikh : 26 Mac 2005

Buat ayahanda dan bonda tercinta, terima kasih di atas segala jasa dan pengorbanan selama ini. Buat teman-teman seperjuangan, terima kasih di atas segala bantuan dan tunjuk ajar daripada kalian.

PENGHARGAAN

Alhamdulillah...syukur kehadrat Illahi, kerana dengan limpah kurnia-Nya dapat saya menyiapkan laporan Projek Sarjana Muda dalam tempoh yang ditetapkan.

Setinggi penghargaan ditujukan buat penyelia projek iaitu En. Redzuan bin Abdul Manap dan En. Badrul Hisham bin Ahmad di atas dorongan dan tunjuk ajar mereka dalam menyiapkan projek ini. Terima kasih juga buat pegawai sistem maklumat KUTKM, En. Razif Bin Abdul Hamid yang banyak menyalurkan maklumat dan sudi meluangkan masa memberi tunjuk ajar kepada saya. Segala maklumat yang diberikan amatlah saya hargai.

Sekalung penghargaan dan jutaan terima kasih ditujukan istimewa buat ayahanda dan bonda yang banyak memberi nasihat dan dorongan kepada saya dalam menyiapkan projek ini. Penghargaan ini juga diberikan buat insan tersayang, Mohamad Naim bin Mohd Yasir kerana sentiasa memberi sokongan tanpa jemu kepada saya. Segala pengorbanan kalian amat bermakna buat saya dan akan saya hargai buat selamanya

Ucapan terima kasih juga buat teman-teman seperjuangan di atas segala bantuan dan kerjasama yang telah diberikan. Segala masalah yang berkaitan dengan projek sering dibincangkan dan diselesaikan bersama. Akhir kata, sekali lagi ucapan terima kasih buat semua yang terlibat samada secara langsung atau secara tidak langsung.

Sekian terima kasih...

ABSTRAK

Projek ini tertumpu kepada kajian mengenai kes pencerobohan sistem rangkaian komputer dan cara mengatasinya. Konsep keselamatan adalah penting dalam memastikan maklumat-maklumat tidak dicuri oleh golongan penceroboh. Faktor utama yang menyebabkan berlakunya pencerobohan sistem rangkaian komputer di sesebuah organisasi ialah sikap pentadbir atau pengurus sistem yang tidak mengambil berat dan tidak mengendahkan keselamatan rangkaian di dalam sesebuah organisasi. Kebanyakan penceroboh menjalankan aktiviti pencerobohan sistem rangkaian komputer cuba meniru atau mengubah data-data penting dalam organisasi untuk tujuan tertentu seperti sabotaj, sikap dengki antara satu sama lain, mementingkan diri sendiri, faktor kewangan, cabaran daripada rakan sebaya dan sebagainya. Data-data mengenai kes pencerobohan yang berlaku di Malaysia selama lima tahun dibuat kajian dan analisis secara terperinci. Sesebuah organisasi perlulah mewujudkan kaedah perlindungan dan mengadakan suatu persekitaran keselamatan yang meliputi semua aspek seperti kawalan persekitaran rangkaian, perisian, perkakasan dan undang-undang. Semua aspek ini mestilah diaplikasikan bagi memastikan persekitaran keselamatan sistem rangkaian komputer adalah terjamin

ABSTRACT

This project focused on a case study about the intrusion of computer network systems and how to deter these problems. The security concepts are important to ascertain the private information or fact of the organizations so that the intruder cannot steal it. The main factors that cause the problem happened is that the administrator do not taking care about the data security in the organizations. The intruders' tries to copy, damage or change the important data. So, this study case tries to explore the types of the intrusion in the computer network and how they are solved. The protection in the network computer systems is needed to solve the problems from happens.

ISI KANDUNGAN

SENARAI JADUAL

SENARAI RAJAH

SENARAI GAMBAR

SENARAI SINGKATAN

ACL	-	Access Control Logic
ATM	-	Auto Teller Machine
IDS	-	Intrusion Detection System
IP	-	Internet Protocol
IPsec	-	Internet Protocol Security
LAN	-	Local Area Network
OS	-	Operation Systems

SENARAI LAMPIRAN

BAB I

PENGENALAN

1.1 PENGENALAN PROJEK

Dalam era teknologi maklumat, penggunaan komputer dan telekomunikasi amat meluas. Saban hari media cetak dan elektronik melaporkan tentang perkembangan yang terbaru. Hingga kini, semakin banyak organisasi menggunakan sistem pengkomputeran bagi menawarkan perkhidmatan atau produk mereka dengan cara yang lebih pantas, cekap dan berkesan. Dengan menggunakan komputer, segala maklumat dihantar secara elektronik melalui talian komunikasi dari suatu tempat ke suatu tempat yang lain.

Walau bagaimanapun, ada sesetengah pihak atau golongan yang berniat jahat seperti penceroboh boleh memperoleh maklumat rahsia atau mengubah maklumat tersebut dengan cara pintas pada talian komunikasi atau menggunakan cara yang lain. Dalam kes tertentu, jika sistem perkomputeran tidak berfungsi, maka segala kerja dan urusan tidak dapat dilaksanakan. Misalnya, pengguna tidak dapat mengeluarkan wang dari *Automatic Teller Machine (ATM).*

Oleh demikian, sistem keselamatan komputer memainkan peranan penting bagi memastikan segala kepincangan dapat diatasi dengan cara yang betul dan berkesan. Lantaran daripada itu, satu kajian mengenai pencerobohan sistem rangkaian komputer telah dilakukan dan kaedah perlindungan sistem rangkaian komputer turut dihuraikan di dalam tesis ini.

1.2 OBJEKTIF PROJEK

Projek yang berasaskan kajian kes ini mempunyai banyak kepentingan terutamanya kepada pengguna komputer. Salah satu objektif kajian ini dijalankan adalah untuk mengkaji dan memahami tentang jenis-jenis ancaman dan pencerobohan sistem rangkaian komputer yang seringkali berlaku di dalam arus teknologi maklumat. Projek ini juga bertujuan untuk mengetahui konsep-konsep keselamatan rangkaian komputer bagi memastikan masalah pencerobohan dapat diatasi.dengan sebaik mungkin. Antara tujuan lain kajian ini dijalankan adalah untuk mendedahkan prosedur sesuatu pencerobohan sistem rangkaian komputer dilakukan.

Di samping itu, kes-kes yang terlibat dalam pencerobohan sistem rangkaian komputer juga turut dikaji dan dikenalpasti. Masalah pencerobohan sistem rangkaian komputer yang kian menular di seluruh negara perlu diatasi supaya keselamatan data dan maklumat penting adalah terjamin. Selain itu, kajian ini juga adalah untuk mengenalpasti sistem-sistem perlindungan yang digunakan untuk melindungi rangkaian komputer daripada dicerobohi.

1.3 SKOP PROJEK

Skop projek ini dibahagikan kepada tiga bahagian utama. Antaranya ialah kajian tentang pencerobohan terhadap sistem rangkaian komputer dan analisa kes-kes pencerobohan sistem rangkaian komputer yang berlaku. Selain itu juga, kaedah perlindungan dan cara mengatasi masalah pencerobohan sistem rangkaian komputer juga dibuat kajian.

1.4 PERNYATAAN MASALAH

Era globalisasi yang melanda dunia tidak lengkap tanpa kewujudan perkembangan teknologi maklumat. Biarpun teknologi maklumat mendatangkan banyak manfaat kepada orang ramai, namun ianya tidak akan terlepas daripada ancaman-ancaman yang boleh mendatangkan impak buruk kepada semua pihak. Antara ancaman yang dihadapi oleh pengguna teknologi maklumat ialah fenomena pencerobohan komputer. Penceroboh sistem rangkaian komputer merupakan individu yang boleh mendatangkan ancaman dan menyebarkan virus kepada komputer dan sistem rangkaian. Mereka akan cuba menyalahgunakan kemudahan ini untuk kepentingan mereka.

Namun, terdapat juga golongan penceroboh yang hanya menjalankan aktiviti yang tidak berfaedah ini sebagai satu keseronokan dan hobi semata-mata tanpa memikirkan kesan buruk yang akan dihadapi kelak. Kebanyakan daripada penceroboh ini menceroboh sistem maklumat di syarikat-syarikat swasta dan jabatan kerajaan untuk mencuri maklumat dan data-data sulit. Selain itu, ada juga sesetengah daripada golongan ini menceroboh sistem rangkaian komputer di institusi pengajian tinggi dan mencuri atau mengubah data-data penting pada sistem maklumat peribadi

pelajar dan kakitangan, sistem maklumat fakulti, keputusan peperiksaan pelajar, penyata gaji dan sebagainya.

Masalah pencerobohan dan kecurian maklumat akan bertambah menular di dalam arus teknologi maklumat sekiranya ia tidak dibendung oleh sesebuah organisasi dan pihak yang bertanggungjawab. Oleh demikian, langkah penyelesaian perlulah diambil oleh setiap pihak dalam sesebuah organisasi bagi memastikan maklumat sentiasa berada dalam keadaan terjamin dan selamat.

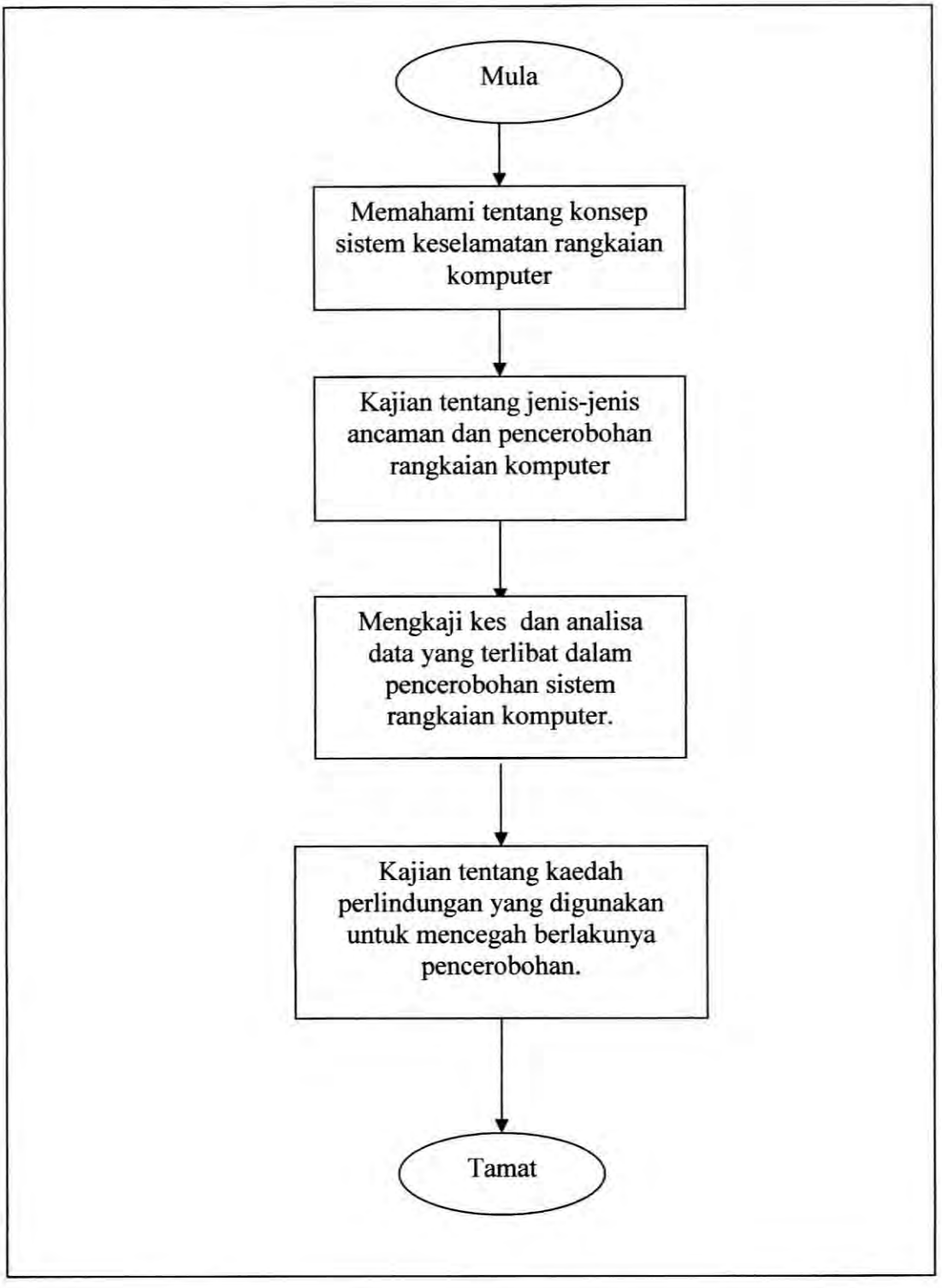
1.5 METODOLOGI PROJEK

Metodologi projek adalah penting bagi memastikan projek dapat dijalankan dengan lebih lancar dan teratur. Dalam menjalankan kajian ini, terdapat beberapa kaedah pendekatan yang telah diaplikasikan. Kaedah pendekatan projek yang pertama ialah memahami konsep-konsep sistem keselamatan rangkaian komputer. Pemahaman konsep-konsep keselamatan rangkaian komputer adalah penting dan merupakan asas utama dalam menjalankan projek. Pencarian maklumat ini dilakukan dengan merujuk pada bahan-bahan bacaan yang berkaitan tentang konsep sistem keselamatan rangkaian komputer.

Selain itu, kajian mengenai ancaman-ancaman dan pencerobohan rangkaian komputer juga dilakukan dengan menggunakan bahan-bahan rujukan seperti buku, majalah-majalah, suratkhabar dan melayari internet. Untuk kajian kes-kes pencerobohan dan analisa data-data tentang kes pencerobohan yang berlaku, maklumat data-data tersebut diperoleh daripada sumber internet dan seterusnya analisa dibuat dengan menggunakan carta-carta dan graf-graf supaya ianya lebih mudah untuk difahami. Maklumat-maklumat tentang kaedah perlindungan bagi

masalah pencerobohan rangkaian komputer juga dikaji berdasarkan sumber daripada bahan-bahan rujukan dan artikal.

Di samping itu, rujukan daripada jurnal-jurnal berkaitan turut dilakukan untuk memahami dengan lebih mendalam lagi tentang pencerobohan rangkaian komputer. Kaedah pendekatan lain adalah melalui temubual dengan pegawai-pegawai yang mahir dalam sistem keselamatan rangkaian komputer. Kaedah ini lebih berkesan kerana pelajar mendapat pendedahan dan penerangan yang lebih tepat daripada mereka. Rajah 1.1 menunjukkan carta alir projek.yang dijalankan.



Rajah 1.1 : Carta alir projek

BAB II

KAJIAN LATAR BELAKANG

2.1 KONSEP KESELAMATAN

Keselamatan rangkaian komputer merupakan satu ciri yang penting dalam sistem pengoperasian kerana maklumat yang disimpan dalam sistem komputer adalah berharga kepada sesebuah organisasi. Kewujudan rangkaian komputer yang meluas akan menyukarkan peranan sistem pengoperasian untuk mengawal pencapaian data oleh pengguna yang sah serta menghalang aktiviti-aktiviti pencerobohan.

Oleh demikian, konsep-konsep keselamatan adalah penting diketahui untuk memastikan maklumat-maklumat tidak dicuri oleh golongan penceroboh. Konsep keselamatan boleh dikaji dalam beberapa bidang iaitu sumber tempatan dan sumber rangkaian, dasar dan mekanisme, pengesahan dalaman dan luaran serta pembuktian.

2.1.1 Sumber Tempatan dan Sumber Rangkaian

Pencapaian sumber tempatan dapat dikawal dengan menghadkan kegunaan sumber tertentu seperti komputer peribadi kepada pengguna yang sah sahaja. Sumber tersebut boleh disimpan dalam bilik terkunci yang hanya boleh dicapai oleh sesiapa yang mempunyai kunci bilik tersebut. Namun begitu, kewujudan rangkaian komputer telah menyenangkan pencapaian sumber tersebut dari mana-mana komputer lain yang dapat menghantar data ke sumber rangkaian. Lantaran daripada itu, keselamatan sumber rangkaian mestilah dilaksanakan melalui pengesahan dan penyulitan [1].

2.1.2 Dasar dan Mekanisme

Dasar keselamatan merupakan peraturan yang ditetapkan oleh sesebuah organisasi mengenai pencapaian sumber maklumat. Contohnya, hanya bendahari sahaja diberi kebenaran untuk mencapai data kewangan, manakala hanya pentadbir yang dapat mencapai maklumat sesuatu produk. Kesemua dasar yang ditetapkan oleh organisasi tersebut dilaksanakan melalui pelbagai mekanisme keselamatan. Mekanisme merupakan alatan yang digunakan untuk mencapai objektif dasar keselamatan tesebut. Contohnya, dasar yang diberi itu boleh dicapai melalui berbagai mekanisme seperti kegunaan kata laluan untuk mencapai akaun yang mengandungi maklumat kewangan atau maklumat-maklumat penting itu akan disulitkan (pengengkripan) supaya tidak boleh dicapai oleh pengguna yang tidak mempunyai kekunci penyahsulitan [1].