

Introduction

Teknologi Informasi yang berkembang cukup pesat dan terintegrasi ke dalam sistem bisnis yang dijalankan membutuhkan perhatian yang khusus dan tidak bisa dipandang sebelah mata.

Proses kontrol harus selalu dilakukan untuk mengetahui bahwa sistem yang digunakan sudah sesuai dan mencukupi kebutuhan proses bisnis yang dijalankan. Tingkat keamanan dari sistem yang dimiliki setidaknya harus sesuai dan berimbang dengan tingkat kerahasiaan informasi yang ada.

Lantas, bagaimana kita dapat mengetahui bahwa sistem yang kita miliki sudah cukup aman? Bagaimana melakukan self assessment terhadap sistem yang digunakan? Langkah-langkah apa saja yang harus ditempuh untuk melakukan pengamanan pada sistem tersebut? Kendali (security control) apa dan bagaimana yang harus diterapkan?

Begitu banyak jawaban terhadap pertanyaan-pertanyaan di atas, namun salah satu jawaban yang pasti adalah ketersediaan Sumber Daya Manusia (SDM) yang paham dan tanggap terhadap masalah keamanan. Masalah keamanan sistem IT hendaknya dipahami oleh semua pihak yang terkait dengan sistem informasi dan IT, mulai dari pengguna biasa (user), system administrator, pengelola jaringan, pengembang aplikasi, sampai ke pucuk pimpinan (top level management).

Network Security Training Schedule

Date : 21-23 April 2009
Place : Cyber Building Jakarta

Date	Materials
Day 1 21 April 2009	Introduction in to Network Security
	Introduction in to Linux/UNIX
	10 domains
	Cryptography
Day 2 22 April 2009	Penetration Testing
Day 3 23 April 2009	Firewall, IDS & IPS Theory
	Firewall, IDS & IPS Practise
	Log Monitoring and Management

Pelatihan ini akan disampaikan dalam bahasa Indonesia. Biaya pelatihan ini Rp. 5.250.000,-/orang. Fasilitas yang diberikan adalah training kit dan sertifikat.

Contact Persons:

Nursidah, Fikri Abdullah, Rois Solihin

Telp : 021 – 5208049

Fax : 021 – 5208005

Email : nur@indocisc.com, fikri@indocisc.com, rois@indocisc.com

Syllabus

Introduction to Network Security
<ul style="list-style-type: none">• beberapa statistik tentang computer/information security• klasifikasi keamanan• aspek/servis keamanan: confidentiality, integrity, authentication, non-repudiation & availability• jenis-jenis serangan (attack)
Evaluasi Keamanan Sistem dan Jaringan Komputer
<ul style="list-style-type: none">• Sesi ini berisi beberapa informasi mengenai pentingnya melakukan evaluasi dan pengamanan secara berkala. Akan dijelaskan juga hal-hal berikut ini:<ul style="list-style-type: none">➢ sumber lubang keamanan, vulnerability mapping➢ cara melakukan evaluasi: manual dan otomatis➢ etika➢ penggunaan network monitoring
Pengantar sistem UNIX/Linux
<ul style="list-style-type: none">• Beberapa tools yang akan digunakan menggunakan platform UNIX/Linux. Untuk itu perlu diberikan sedikit gambaran cara menggunakan sistem UNIX/Linux. Materi untuk topik ini tidak terlalu dalam akan tetapi ditargetkan agar peserta dapat menggunakan tools di sistem UNIX
Network monitoring/management
<ul style="list-style-type: none">• Network (jaringan) merupakan salah satu basis untuk melakukan serangan (attack). Untuk itu pengamanan terhadap jaringan merupakan salah satu cara untuk mengantisipasi dan mendeteksi adanya serangan. Pada bagian lain nantinya akan dijelaskan cara melakukan serangan. Untuk itu pada sesi ini akan disiapkan metoda pemantauannya. Beberapa tools yang berbasis Linux dan Microsoft Windows akan diperagakan dan dicoba

Keamanan server dan servis Internet: email dan web
<ul style="list-style-type: none">• Pada sesi ini kita akan meninjau servis-servis yang ada di Internet. Dua servis yang penting dan umum diberikan adalah servis web dan mail. Pada sesi ini akan disampaikan teori yang terkait dengan kedua servis tersebut beserta serangan terhadap web server dan mail server seperti antara lain web-defacing, mail bomb, mail palsu beserta cara melihat jejaknya (tracing)
Teknik penyerangan : Penetration Testing
<ul style="list-style-type: none">• Pencarian informasi atas target sampai melakukan probing pasif dan aktif terhadap sistem yang dituju.• Percobaan masuk ke sistem target, baik melalui jarak jauh maupun akses secara fisik di depan console. Cara memproteksi terhadap serangan ini akan disampaikan.• Percobaan melakukan serangan. Serangan dapat dilakukan dari Internet atau dari dalam (misalnya dari sebuah host yang sudah diambil alih / compromised). Serangan Denial of Service (DoS) attack akan dilakukan terhadap jaringan untuk meniadakan servis, network hijack untuk membajak sesi.
Teknik pengamanan: Firewall & Intrusion Detection System (IDS)
<ul style="list-style-type: none">• Teori dan teknik dasar pengimplementasian Firewall• Hubungan kebijakan keamanan yang diberlakukan• Perbedaan mendasar antara firewall dan IDS. Bagaimana cara kerja IDS, yang berdasarkan modes dan rules.• Mempraktekkan penggunaan dan pengelolaan firewall & IDS yang dikembangkan sendiri oleh INDO CISC, dimana sumbernya (berupa software) diambil dari produk open source