Introduction

Behind the information systems that electronically govern almost every aspect of our lives, there are applications and databases that process and keep our data. If the application and the database –parts of system that we all implicitly trust to process and hold our critical or sensitive data– are not secure, the potential impact on our lives, and even on our broader society, could be devastating.

In many cases, deploying network security countermeasures can defend our system against malicious attacks. But in other cases, the original vulnerability lies with the software. A software can be correct without being secure. The software can meet every requirement and perform every specified action flawlessly, yet still be exploited by a malicious user. Even after putting so much time, money, and effort on network security, the potential problems will still be there as long as the application's and database's security vulnerabilities get no serious attention.

Some of the vulnerabilities –perhaps– are already discovered over the years as we deploy the application and the database. The rest of the software vulnerabilities remain undiscovered, but they're there. They all have the potential to be discovered and be exploited. What matters is: by whom.

Why then do we think it's necessary to share the methods for attacking and securing application and databases with you? Because we want to put this information into the hands of database administrators, security professionals, and network auditors so that these people understand more fully how others may attack their systems and how to defend.

In this hands-on course, you will gain experience in the core application and database security vulnerability discovery, exploitation, and remediation methods.

INDOCISC Network Security
Application and Database Security
Hands on Training

Application and Database Security Training Schedule

Date : 17, 18, 19 Februari 2009
Place : Menara Bidakara Jakarta

Date	Materials
Day 1 **17 Februari 2009**	Introduction to Application & Database Security
	Common Application Threats and Vulnerabilities
	Application Security Exploits
	Securing Application
Day 2 **18 Februari 2009**	Common Database Threats and Vulnerabilities
	Database Security Exploits Theory
	Database Security Exploits Hands On
Day 3 **19 Februari 2009**	Securing Database Theory
	Securing Database Hands On
	Checklist & Discussion

This course will be delivered in Bahasa Indonesia. All courseware & materials (course materials, security tools in a live CD, computer facility for each), coffee break, lunch, certificate are included with IDR 5.250.000,-/person.

Contact Persons:
Nursidah, Fikri Abdullah, Rois Solihin
Telp : 021 – 5208049, 021-70148058
Fax : 021 – 5208049
Email : nur@indocisc.com, fikri@indocisc.com, rois@indocisc.com

Syllabus

Introduction to Application & Database Security
• The Roles of Software/Application in Critical Aspects of Our Lives • Security Problems in Software/Application and the Root Causes • Solving the Problems: Three Common Secure Software Development Methodologies ➢ Microsoft's SDL, Cigital's Touchpoints, OWASP's CLASP
Common Application Security Threats and Vulnerabilities
• Review of Web Application Basics • Review of Security Frames for Web Application • Common Web Application Threats • Common Web Application Vulnerabilities
Hands On: Application Security Exploits
• Setup & Demo • Class Practices in Indentifying Application Vulnerabilities • Class Practices in Exploiting Sample Web Application
Securing Application
• Common Web Application Countermeasures • Applied Knowledge for Software/Application Security

INDUCISC Network Security
Application and Database Security
Hands on Training

Common Database Security Threats and Vulnerabilities
• Review of Database Basics • Review of Security Frames for Database • Common Database Threats • Common Database Vulnerabilities
Hands On: Database Security Exploits
• Class Practices in Indentifying Database Vulnerabilities • Class Practices in Exploiting Sample Database
Securing Database
• Common Web Application Countermeasures • Applied Knowledge for Software/Application Security
Software Security Checklist & Discussion
Security Threats and Vulnerability Checklists for your Software/Application Security Threats and Vulnerability Checklists for your Database

Target audience for this course is a hands-on web application developer/ designer/architect/analyst, who is already familiar with software development lifecycle, and is seeking for an fundamental understanding of today's best practices in secure software development.

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).

INDOCISC Network Security
Network Security
Hands on Training

Network Security Training Schedule

Date : 17, 18, 19 Februari 2009
Place : Menara Bidakara Jakarta

Date	Materials
Day 1 **17 Februari 2009**	Introduction in to Network Security
	Introduction in to Linux/UNIX
	Network Monitoring Management
	Cryptography
Day 2 **18 Februari 2009**	Server dan Internet Services Security
	Initial Access
	Casing the joint
	Penetration Testing
Day 3 **19 Februari 2009**	Firewall, IDS & IPS Theory
	Firewall, IDS & IPS Practise

This course will be delivered in Bahasa Indonesia. All courseware & materials (course materials, security tools in a live CD, computer facility for each), coffee break, lunch, certificate are included with IDR 5.250.000,-/person.

Contact Persons:
Nursidah, Fikri Abdullah, Rois Solihin
Telp : 021 – 5208049, 021-70148058
Fax : 021 – 5208049
Email : nur@indocisc.com, fikri@indocisc.com, rois@indocisc.com

Syllabus

Introduction to Network Security
• beberapa statistik tentang computer/information security • klasifikasi keamanan • aspek/servis keamanan: confidentiality, integrity, authenctication, non-repudiation & availability • jenis-jenis serangan (attack)
Evaluasi Keamanan Sistem dan Jaringan Komputer
• Sesi ini berisi beberapa informasi mengenai pentingnya melakukan evaluasi dan pengamanan secara berkala. Akan dijelakan juga hal-hal berikut ini: ➢ sumber lubang keamanan, vulnerability mapping ➢ cara melakukan evaluasi: manual dan otomatis ➢ etika ➢ penggunaan network monitoring
Pengantar sistem UNIX/Linux
• 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
• 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

INDOCISC Network Security
Network Security
Hands on Training

Keamanan server dan servis Internet: email dan web
• 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: casing the joint, initial access, attack, exploit
• 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 utuk membajak sesi.
Teknik pengamanan: Firewall & Intrusion Detection System (IDS)
• 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