



*Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>*

Special Interest Group for Security and Information Integrity (SIG²)

Centre for Competency

Secure Infrastructure (Lab Session)

Evaluation Report

**Delivered by E&Y Labs for Internet & Security, SG
30th - 31st October 2003**

**<Based on Information System Security
Course Evaluation Methodology DRAFT version
0.2 >**



*Special Interest Group in
Security and Information Integrity
(SIG^2)*
<http://www.security.org.sg>

TABLES OF CONTENT

1. INTRODUCTION	3
1.1 Course Objectives	3
1.2 Scope of Course	3
1.3 Course Evaluation Method.....	3
2. Evaluator's Comments.....	4
2.1 Relevancy Assessment.....	4
2.2 Courses Content Assessment	4
2.3 Courses Conduct Assessment.....	6
ANNEX A – Course Evaluation Form.....	8
Course Evaluation Form	8



*Special Interest Group in
Security and Information Integrity
(SIG^2)*
<http://www.security.org.sg>

1. INTRODUCTION

1.1 Course Objectives

The “Secure Infrastructure (Lab Session) course aims to equip participants with the necessary skills to implement and deploy organisation infrastructure services in a secure manner.

The course includes a Lab Session to test out and simulate real-world deployment configurations, such as secure configuration settings, patch management, as well as end-user restriction controls.

1.2 Scope of Course

- The course is designed only for organisations that use Microsoft Windows platform as the office automation tool. It covers Microsoft applications such as Domain Controllers, IIS Web Servers as well as SQL server.
- The practical Lab sessions focus on the new security features in a Microsoft Windows Server 2003 environment.

1.3 Course Evaluation Method

The Course Evaluation is done using the Information System Security Course Evaluation Methodology as a benchmark, which focuses primarily at 3 key areas:

- Relevancy of the Course,
- Course Content; and
- Course Conduct (which is how the course was conducted)



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

2. Evaluator's Comments

2.1 Relevancy Assessment

Relevancy is determined by the following matrix:

	General Awareness	Planning & Management Concepts	Domain Specific
Senior Management	Highly Relevant	Relevant	-
IS Security Program Manager	Relevant	Highly Relevant	Relevant
IS Security Consultant	Relevant	Highly Relevant	Highly Relevant
IS Administrator and Operator	Relevant	Relevant	Highly Relevant
End User	Highly Relevant	-	-

This course falls in into the category of Domain Specific, even though the scope of the course spanned across multiple Microsoft applications as well as a small percentage of Unix security. It can be considered as a very security domain specific type of courses, focusing only on the security elements.

Based on the above matrix, the course is highly relevant for an IS Security Consultant as well as for the folks involved in day-to-day security operations. As for an IS Security Manager type of role, it can be considered as a 2-day crash course mainly for awareness update.

2.2 Courses Content Assessment

The courses are evaluated according to the following criteria:

Course Content based on the Subject Outline

Infrastructure Deployment for AD, DNS, IIS, SQL and DC

- Different deployment strategies were analysed to identify the pros and cons of each method.



*Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>*

Concept of Active Directory (Domain Trees, Forests, Organisational Units) and Application of GPO (Group Policy Objects)

- Various security features of the new Windows Server 2003 were studied for different enforcement purposes such as the use of Kerberos, IPSec, EFS, as well as the auditing of events.
- The Lab provided a pair of DC and member server for practising the capabilities of GPs as well as implementing IPsec for secure communications.

Authorisation

- Some concepts of Access Control List (SACL and DACL) were briefly touched on. The interesting part is using Security Policy Template to enforce such rights on the domain, which enhances the overall manageability on the users.

New Security Features in Windows Server 2003 and IIS6

- Lots of new features were highlighted. However, some of the features could not be practised due to the limitation of the Lab setup. One such feature is a Forest Trust, which is not supported in the predecessor, which is the Server 2000 version. Nevertheless, most of the features were well explained.
- The IIS section was conceptual walk-thru as there was no hands-on the new features. IIS6 was interestingly trying to mimic typical web servers in the Unix space through stripped-down or harden configuration files which contains all essential settings. This is a plus for the command-line folks and hated GUI. A new worker process makes it even more resistant to buffer overflow attacks. However, IIS 6 only runs on Server 2003.

Securing IIS 5

- This is a lot more useful as organisations running IIS would most likely be still using version 5. Various methods of hardening were covered in the Lab sessions, such as individual settings via the GUI or using tools like URLScan or MS IIS Lockdown utility.

Securing Microsoft SQL

- Two concepts were briefly explained with regards to SQL Server Authentication and Authorisation. Authentication would prefer Windows Kerberos Authentication. Authorisation would be using built-in role based for granular permission controls to database objects.

Patch Management



*Special Interest Group in
Security and Information Integrity
(SIG^2)*
<http://www.security.org.sg>

- This concept of patch management is tackled using Microsoft SUS (Software Update Services) utility which different modes of obtaining updates. Though some unsuccessful attempts were encountered, main due to the wireless Lab setup with too many simultaneous downloads of large updates files.

Enhancing UNIX Security

- This was the only non-windows topic in the course. It is definitely good to cover the other major platform but trying out an eTrust Access Control from CA (Computer Associates) product might be mistaken as some form of marketing for them. Nevertheless, this section was well taken with some brief hands-on on the basic features of the eTrust product, accompanied with a demo on eTrust Audit for enterprise auditing requirements.

2.3 Courses Conduct Assessment

Course Conduct

- The course was presented in an organised manner, except for a few technical glitches due to the wireless setup for the lab.
- The instructor did a good job in communicating the essentials as well as highlighting the differences between the current and the predecessor versions of products. He has demonstrated his knowledge of the subject matter by making difficult concepts understandable.
- The instructor tried to simulate interest in the subject area, but somehow, the participants were probably too engross with fiddling the machines in front of them. He did a good job by facilitated through out the 2 days, even though interaction amongst the participants during the class was minimal.

Cost Effectiveness

- The course materials come in 2 binders (1 with the presentation slides, the other is a Lab Exercise Manual)
- Some quality checks should be done the course materials as there were some obvious mistakes, or typo-errors
- The Lab facility was rather small and is kind of cramp, with 2 sharing a pair of DCs. However, as the machines were mostly on wireless, it was not that messy but there was some minor traffic congestion encountered on the wireless LAN during the patch management exercise.



*Special Interest Group in
Security and Information Integrity
(SIG²)*
<http://www.security.org.sg>

- On the whole, the instructor has done a good job. Moreover, he encouraged the participants to network as much as possible and also to exchange name cards and contacts at the end of the course.

EVALUATED BY

Vincent Leong, GSEC
Director, CC (Course Evaluation) and Committee Member, SIG²
vincent@security.org.sg

Khoh Chih Jeun, CISA, CISSP
Director, CC (Product Evaluation) and Committee Member, SIG²
chihjeun@security.org.sg

REVIEWED BY

Aloysius Cheang, CISA, CISSP, GCIH
President, SIG²
alloysius@security.org.sg

APPROVED FOR DISSEMINATION BY

Aloysius Cheang, CISA, CISSP, GCIH
President, SIG²
alloysius@security.org.sg



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

ANNEX A – Course Evaluation Form

Course Evaluation Form					
Course Title: Secure Infrastructure					
Organizer: Ernst & Young Labs for Internet & Security					
Instructor:					
Time/Date: 9 am to 5 pm from 30th – 31st October 2003					
Prerequisite: Some basic hands-on knowledge is required					
Course Categories: Domain Specific					
Relevancy: Highly Relevant – IS Security Consultants and Operation folks, Relevant – IS Security Manager and above					
Course Content Rating	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Clarity of course objectives		✓			
Agreement between course objectives and course content		✓			
Relevancy of course content to real world issues		✓			
Detail Coverage of Subject Topic		✓			
Course Content Rating: GOOD (SCORE =16/20)					
Course Conduct Rating	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Organisation and the manner of the conduct of the course		✓			

“IT Security...the Gathering. By enthusiasts for enthusiasts”



Special Interest Group in
Security and Information Integrity
(SIG²)
<http://www.security.org.sg>

Knowledge communication of the subject matter		✓			
Making difficult concepts understandable		✓			
Simulating interest in the subject area			✓		
Demonstrating a positive attitude towards participation		✓			
Course Conduct Rating: GOOD (SCORE =20/25)					
<hr/>					
Cost Effectiveness Rating	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Course Duration			✓		
Quality of the course content		✓			
Quality of the course material		✓			
Quality or Subject Knowledge of the instructor		✓			
Quality of the course facilities			✓		
Cost Effectiveness Rating: GOOD (SCORE =18/25)					
<hr/>					
Overall Rating: GOOD (SCORE = 54/70 = 77.4%)					

“IT Security...the Gathering. By enthusiasts for enthusiasts”