



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

Special Interest Group in Security and Information Integrity (SIG²)

Centre for Competency

OSSTMM PROFESSIONAL SECURITY TESTER (OPST)

delivered by Sensecurity Institute

12-15 November 2003

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



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

1. INTRODUCTION

The OSSTMM project (Open Source Security Testing Methodology Manual) by The Institute for Security and Open Methodologies (ISECOM) aims to ensure perfect quality with a reasonable cost effectiveness for security tests. The project was initiated by Pete Herzog, the Managing Director of ISECOM and since 2001 an international team of experts has been working on a standard methodology for security tests. The manual, which is now available in its second edition is internationally recognized by a constantly increasing number of authorities, universities and companies as standard methodology for security tests and more and more professional testers use it as guideline for performing security tests. OSSTMM website is available at <http://www.osstmm.org>

Brought into Singapore by Sensecurity Institute (SI for short), SIG² had the privilege to attend one of the first batch of course delivered by their most experienced trainer, Christopher.

2. COURSE CONTENT

In security pen-testing, comprehensiveness as far as possible is important for it takes just a single loophole for potential adversary to compromise a weak system. From there on, the domino effect starts to kick in from one system to another. A comprehensive (best effort) and methodological testing process is what OSSTMM was designed to address. It is not a course, which goes through a list of “so called” hacker tools. Definitely, it is not a course for security professionals or hacker wannabes, hoping to learn a trick or two in penetration testing.

OSSTMM suggested method of computing scheduling requirements is very useful for pen-testers to approximate or gauge the amount of time needed for basic scanning which is often a fixed and time consuming portion of security pen-testing.



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

3. COURSE CONDUCT

The course is conducted in a very conducive environment. M hotel is centrally located and offers excellent facilities. In addition, the training rooms are private and quiet. Though we did not lunch with the rest of the students, but based on personal experience, the lunch catered was of the highest quality.

We also understand that Christopher was trained and certified by ISECOM and the LaSalle University in Spain. So definitely, we are trained by a qualified person, that not only have the experience, but the proper training to deliver the course more effectively. It is not often that a course instructor is trained overseas by the course developer, and these little gritty are indicators that quality

4. COST EFFECTIVENESS

In particular, we like to highlight an interesting exercise that we found refreshing. The brain-teasing exercises presented at the start of each lesson is something interesting and useful to remind attendees that security pen-testing is not all about following a set of procedures and process and hoping to get the best out of it. Creativity and innovative ways of looking at problems is often the crux to discovering new weaknesses during penetration testing and vulnerability discovery, not to mentioned how one, as a ITSEC consultant can spot a security gap.

5. RECOMMENDATION

We see that the students are not able to relate the framework to their work. In addition, they may not have seen how they can integrate and reinforce planning and management skills learnt in OPST to their technical skills and experience. There is also a lack of challenging exercises that will make the students think more and engage more.



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

We also see that the course administration could be better. For instance, the course materials could be given in a CD so as to facilitate the students to make use the course materials to present their case to the management. And although the students are arranged to seat in pairs, we do not see much interaction between the students. It will be best if we can help these students to learn together by engaging them in some larger-scale projects mentioned above. This will also help them to network.

It would be our recommendation that proper steps are taken to address the above issues.

EVALUATED BY

Lim Boon Seng, CISSP, CCNA
Member, SIG²
hooha@security.org.sg

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

REVIEWED BY

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

APPROVED FOR DISSEMINATION BY

Aloysius Cheang, CISA, CISSP, GCIH
President, SIG²
aloysius@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: OSSTMM Professional Security Tester (OPST)					
Organizer: Sensecurity Institute (http://www.sensecurity.org)					
Instructor: Christopher Low (Chief Instructor, Sensecurity Institute)					
Time/Date: 12 – 15 November 2003					
Prerequisite: Basic computing knowledge					
Course Categories: Planning and Management					
Relevancy: IS Security Consultant					
Course Content	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Clarity of course objectives		x			
Agreement between course objectives and course content	x				
Relevancy of course content to real world issues		x			
Course Content Rating: 4 (<i>A useful and methodological way to perform pen-test and could served as good guidelines for security professionals and managers to audit their IT systems.</i>)					
Course Conduct	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Organisation and the manner of the conduct of the course			x		
Knowledge communication of the subject matter		x			

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



**Special Interest Group in
Security and Information Integrity
(SIG^2)**

<http://www.security.org.sg>

Making difficult concepts understandable		x			
Simulating interest in the subject area		x			
Demonstrating a positive attitude towards participation		x			
Course Conduct Rating: 4 (<i>More hands-on would allow attendees to better appreciate some of the concepts discussed in the OSSTMM 3.0 e.g. methods of testing NIDS, FW etc.</i>)					
Cost Effectiveness	Excellent (5)	Good (4)	Average (3)	Fair (2)	Inadequate (1)
Quality of the course content		x			
Quality of the course material		x			
Quality of the instructor		x			
Quality of the course facilities		x			
Cost Effectiveness Rating: 4					
Overall Rating: 4 (Good)					

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