Open Information Systems Security Group

Cutting Edge Hacking and Defense

"One of the best Hacking and Defense demonstrations on earth"

Why Attend This?

REGISTER NOW

- Taught by framework author(s) and subject matter experts directly
- OISSG developed US$20,000 worth of tools for free
- Continual online support
- A platform for continuous learning via Local Chapter
- Opportunity to speak to instructors after the course
- 100% satisfaction by attendees, contact us for referals

OISSG

A Non-Profit Organisation
www.oissg.org

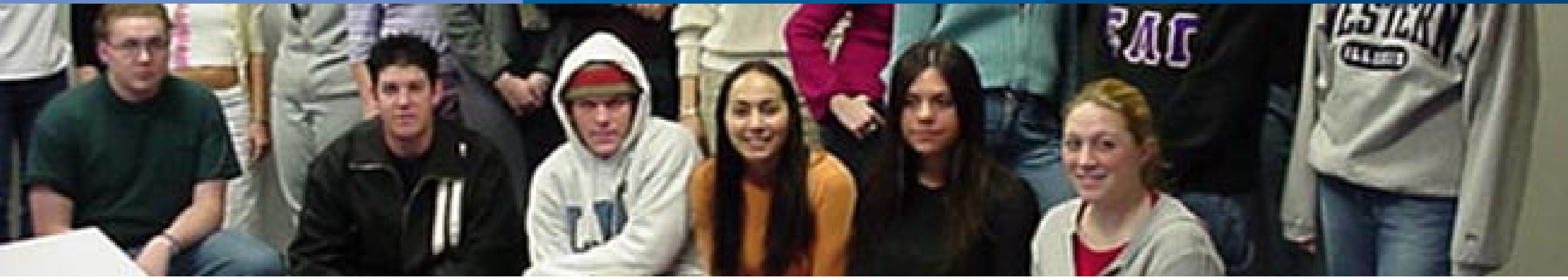
Workshop	Exam
25th - 27th November, 2007	27th November, 2007

- 35% Discounted fees
- Register for 3 at once, get the 4th free!
- Certification Exam Free with Workshop

Cost: US$ 1,500/-Per Person Only

Venue: The Fairmont Dubai
Contact: +971 50 9498556, Email: gulshan@oissg.org

Student comments



"One of the best and most in-depth technical courses I have undertaken. The vulnerabilities will scare you!"

"You will go home wondering how your network has survived thus far. It is a rude awakening for most IT professionals. It is Eye opening and shocking. Thanks to OISSG and its dynamic team, now we will be able to better defend our Networks."

"The ROI of this course is very high. This class will immediately influence our processes and procedures. It has definitely been worth the time and effort."

"Kudos to OISSG for a fine delivery! Courses should be like this, practically relevant, lucidly presented and informative. I feel empowered against hackers now."

"OISSG definitely provides you with clear details on how to use the tools and methodology behind hacking. This know how will make my job secure."

"The skill and presentation of the instructors is laudable. It was arguably, the most applicable and useful course to our everyday workload that I have attended."

"I thought the labs were good. They were real enough so that all the facets of the lab exercises made sense, and it was not as if all "evidence" was made up and did not work together. It was a great class for Computer Crime Investigators."

"I was impressed with instructor knowledge and experience - it came across very well in the presentations and labs."

"Being a member of law enforcement, I appreciated the fact that my perspective was kept in mind during the class."

"It was an excellent class! Well organized and planned. This is the first time the labs in such a class are actually worthwhile and the team teaching technique is what made it work well."

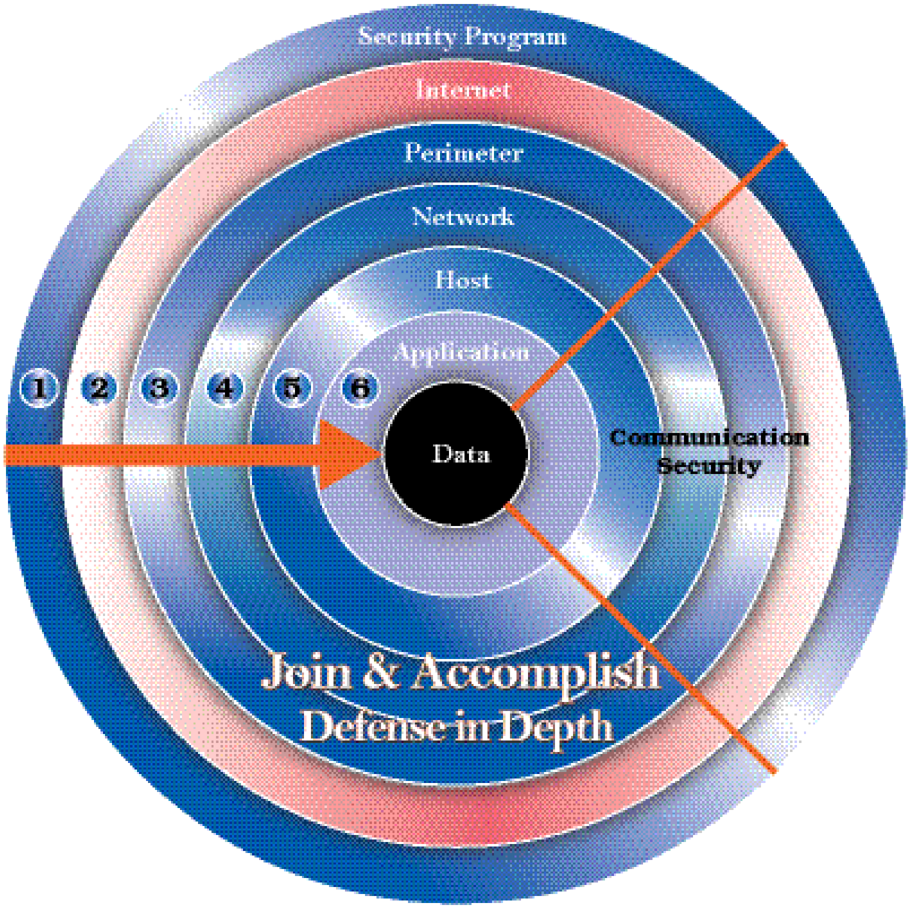
"The instructors are very knowledgeable, and they presented the topics in an easy to understand manner. They are a great team who represent OISSG well."

"I honestly believe this is the best course I've been on and got every pennies worth."

I thought the labs were very good - they definitely brought everything together into a "real world" type of scenario. Overall I was very satisfied.

Overview

This fast paced three days course discusses latest attack techniques and tools developed in the last two year. In order to give completeness to hacker techniques, course integrates old school ways of hacking which still works with cutting edge technologies. It also covers the latest hacking techniques used in underworld.



NOTE: While all modules together prepare you for an ISSAF Penetration Testing - Qualified (I-PTQ) certification, a participant may only take one or more course modules or any day depending on explicit requirement.

The course instructors are acclaimed professionals and security practitioners with deep practical knowledge and experience in Information Security.

Duration, Business Benefits, Target Audience

DURATION

This course is of 24 hours and will be covered in three days. Each day 8 hrs from 08:00 to 16:00

BUSINESS BENEFITS

- Learn latest hacking techniques developed in last two years
- Learn hacking techniques which are not available publicly
- Learn to manage vulnerabilities intelligently
- Learn how to avoid the cost of network downtime due to latest attacks
- Safeguard corporate image and customer trust by protection against latest attacks
- Justify security investments by effective security evaluation of existing security controls
- Get required tools, templates and resources and save significant consulting and product cost

TARGET AUDIENCE

Managers and Professionals who know the basics of information security and are looking to update their understanding and skills, which includes:

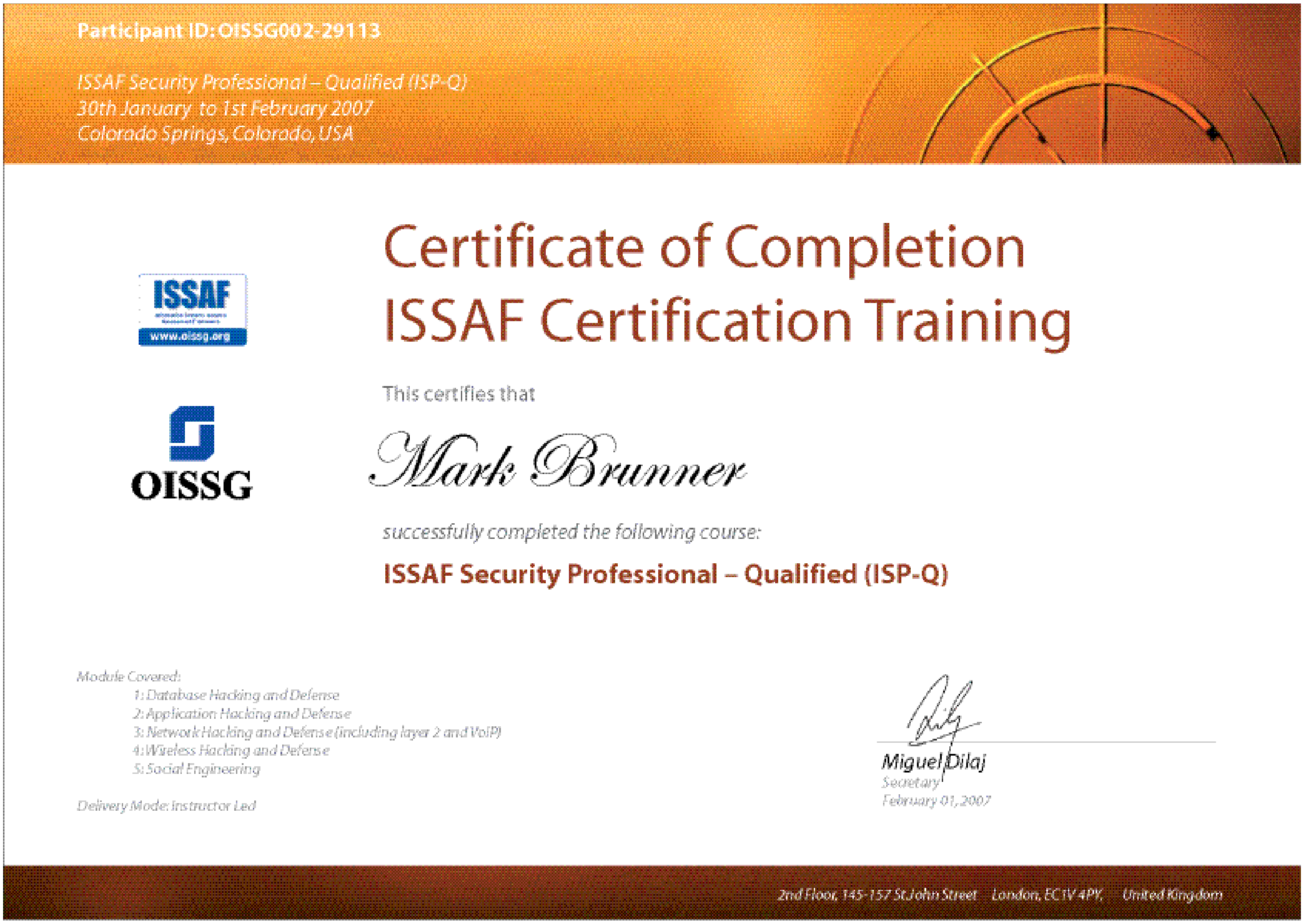
- IT Managers, IT Auditors and Computer Auditors
- IT Security Officers, Security Consultants, Analysts and Architects
- Penetration Testers
- Security Administrator(s), System and Network Administrator(s)
- Information Security Professionals
- Risk Analysts

Laptop Needed

Course Fees

COURSE FEES

- Our course fee is significantly reduced due to the not-for-profit nature of our organization enabling us to give a 35% discount on it.The total fee for this course is USD 1500 per participant.
- While all modules together prepare you for an ISSAF Penetration Testing – Qualified certification, a participant may only take one or more course modules depending on explicit requirement. An individual module (per day) costs US$500
- Group Discounts: 3 or more from the same organization registering at the same time, 4th participant is free.
- ISSAF Certification (FREE) Certification is free following the participation in training which saves you US$ 150
- Detailed information on certification is given in certification section of this brochure.
- 100% fee expected prior to course participation.



Participant ID: OISSG002-29113

ISSAF Security Professional – Qualified (ISP-Q)
30th January to 1st February 2007
Colorado Springs, Colorado, USA

ISSAF
www.oissg.org

OISSG

Certificate of Completion
ISSAF Certification Training

This certifies that

Mark Brunner

successfully completed the following course:

ISSAF Security Professional – Qualified (ISP-Q)

Module Covered:
1: Database Hacking and Defense
2: Application Hacking and Defense
3: Network Hacking and Defense (including layer 2 and VoIP)
4: Wireless Hacking and Defense
5: Social Engineering

Delivery Mode: Instructor Led

Miguel Dilaj
Secretary
February 01, 2007

2nd Floor, 145-157 St John Street London, EC1V 4PY, United Kingdom

DELIVERABLES

In addition to all the presentation material, following tools and material would be provided to support participants' ability to perform penetration testing in their organizations:

1. SECURITY POSTURE EVALUATION FRAMEWORK (SPEF)

A dipstick current state assessment is essential for a sound implementation of information security management system. Further, how do you know your ISMS is effective and healthy? To assure this, the internal controls need to be assessed and tested for adequacy and effective operation. Tool provides a two-stage assessment of security implementation:

1. Firstly a dipstick assessment is based on ISO 27001 and provides a quick start to creating or strengthening existing ISMS.
2. At the next level, the drills down further to test efficacy and efficiency of individual controls based on well-researched domain specific assessment questionnaires.
3. You can also use SPEF to find out where your organization stands today to achieve ISO 27001 and ISSAF certification.

2. SECURITY PROJECTS DECISIONING FRAMEWORK (SPDF)

Internal selling of a security investment can be a nightmare that could even end with no results. Security proposals need to present a complete picture of goals realized and risks addressed vis-à-vis the implementation costs.

In this path-breaking decisioning framework, investment into a security project is scientifically measured against risks mitigated and strategic objectives achieved. This provides for a muchneeded model for presenting effectual business cases for security projects.

DELIVERABLES...

3. RETURN ON SECURITY INVESTMENT (ROSI) CALCULATOR

Utilizing an empirical database, this tool provides a focused quantitative assessment of business value against the investment of resources for security.

1. It performs threat & risk assessment and analyzes assessment results with exact cost benefits.
2. Provides exact figure how much you save by investment on information security
3. Revenue opportunities from enabling new business processes. What new things will a security investment allows you to do?
4. It also provides followings:
5. The annual cost of security incidents, untreated;
6. The residual annual cost of security incidents, after treatment;
7. The gross annual savings attributable to security treatments;
8. Amortized countermeasure upfront cost;
9. The annual cost of countermeasures, comprising recurring costs and amortized set-up cost;
10. The net annual savings.

4. TOOLS CD

Compiled through fieldwork of several professionals, this unique collection of security tools, on three CD volumes, provides a set of effective, current and tested tools in one place. This makes the most required tool in a given situation readily available, thus saving time and energy resulting into improved security on reduced cost.

To assure integrity of tools obtained from Internet, our team has performed extensive Malware testing to make these tools more trustworthy and reliable for use in business environments, addressing the following questions:

1. Which tool to use?
2. Which tool works?
3. Which tool to trust?
4. How to find a tool that is no longer available for download?

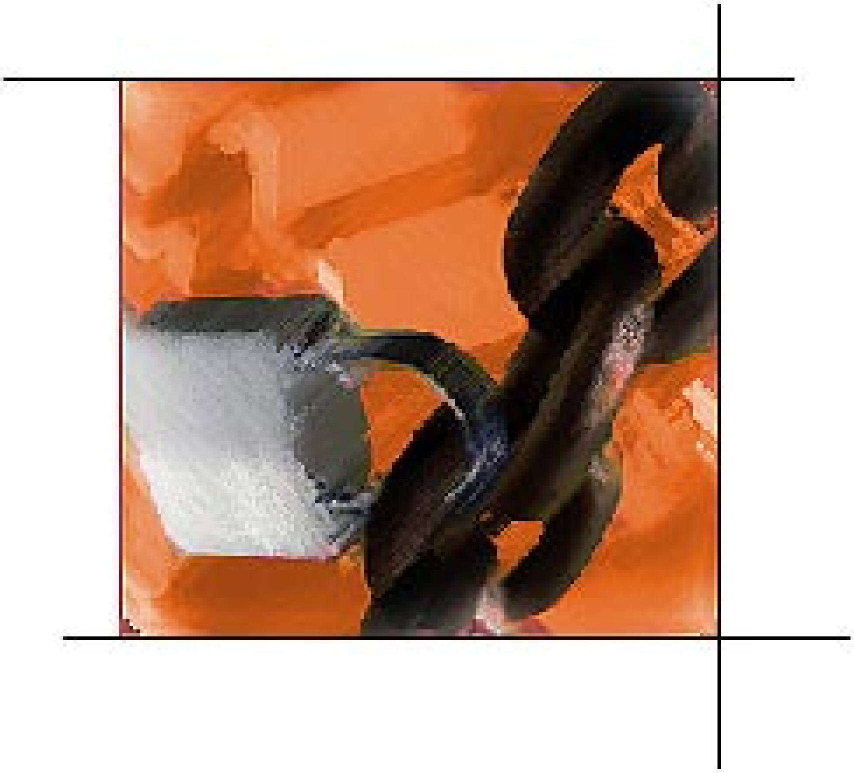
With the use of pre-compiled tools CD, you no longer have to be an expert to perform general or even specialized security tasks such as penetration testing. It works like hacking in the movies!

LIST OF OISSG PROPRIETARY TOOLS	Price (US$)
Information Risk Management Framework (IRMF)	4,000
Security Posture Evaluation Framework (SPEF) – Where your organization stands today to achieve ISO27001 certification?	4,000
Security Projects Decisioning Framework (SPDF)	3,000
Security Policy Framework (SPF)	2,000
Information Security Metrics Framework (ISMF)	3,000
Enterprise Change Management Framework	3,000
Return On Security Investment (RoSI) Calculator	2,000
Tested Tools DVD	1,000
Enterprise Security Policy Templates	None
Other Templates	None

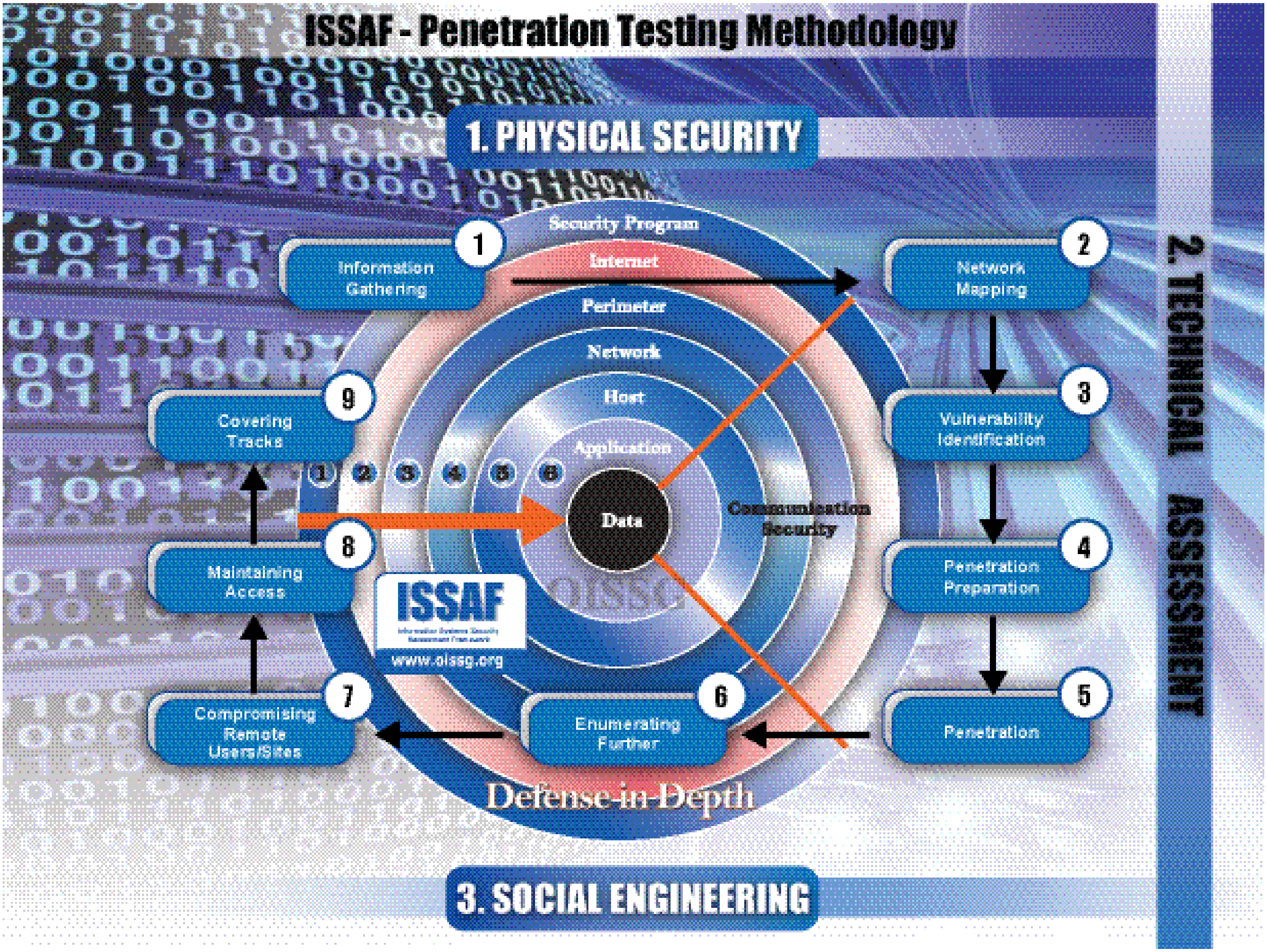
Deliverables

Security Policy Awareness Tool (SPAT)

This tool focuses on effective and auditable distribution of relevant policies to different user groups. It works interactively as a gate-keeper during log-on process to caution a user on key policy aspects, prior to system use. The system keeps a trail of users' interactions for records.



Course Contents



Course Contents

Overview of Cutting Edge Hacking Methodology

Step 1 – Information Gathering

Step 1.1 – Passive Information Gathering (without touching the target)

Achieving followings by exploiting Google, MSN, Yahoo:

- Obtaining your username and passwords
- Compromising mission critical servers
- Finding your personal emails and your messenger's buddy list
- How paid books, serial numbers and products are obtained
- Obtaining highly sensitive data e.g. enterprise security assessment reports
- How we hacked Microsoft?
- How we hacked US military?
- Stealing billion$ budget information
- How attacker finds millions of credit cards?
- Does Google knows what you doing in your bedroom?
- Can Google lead to a terrorist attack?
- Finding proprietary source code
- Using Google to exploit source code
- Compromising your laptop/PC by exploiting Google desktop

Automating all which is mentioned above against your organization

And more…

Step 1.2 – Active Information Gathering

- Email Systems – User Account Enumeration
- SMTP Headers Analysis – Email Received from Target
- SMTP Headers Analysis – Bounced E-mail
- SMTP Headers Analysis – Read Receipt
- Perform BGP (Border Gateway Protocol) Query
- DNS Interrogation - Perform Zone Transfer on Primary, Secondary and ISP name server
- DNS Interrogation - Perform Zone Transfer by dictionary attack
- DNS INTEROGATION - Finding IPv6 IP blocks in use though DNS queries
- Mirror Target Web Site

Step 2 – Advanced Network Mapping

- Find live hosts
- Port and service scanning
- Perimeter network mapping (router, firewalls)
- Identifying critical services
- Operating System fingerprinting
- Identifying routes using Management Information Base (MIB)
- Service fingerprinting
- War-Dialing Attacks

Course Contents

Overview of Cutting Edge Hacking Methodology

Step 1 – Information Gathering

Step 1.1 – Passive Information Gathering (without touching the target)

Achieving followings by exploiting Google, MSN, Yahoo:

- Obtaining your username and passwords
- Compromising mission critical servers
- Finding your personal emails and your messenger's buddy list
- How paid books, serial numbers and products are obtained
- Obtaining highly sensitive data e.g. enterprise security assessment reports
- How we hacked Microsoft?
- How we hacked US military?
- Stealing billion$ budget information
- How attacker finds millions of credit cards?
- Does Google knows what you doing in your bedroom?
- Can Google lead to a terrorist attack?
- Finding proprietary source code
- Using Google to exploit source code
- Compromising your laptop/PC by exploiting Google desktop

Automating all which is mentioned above against your organization

And more…

Step 1.2 – Active Information Gathering

- Email Systems – User Account Enumeration
- SMTP Headers Analysis – Email Received from Target
- SMTP Headers Analysis – Bounced E-mail
- SMTP Headers Analysis – Read Receipt
- Perform BGP (Border Gateway Protocol) Query
- DNS Interrogation - Perform Zone Transfer on Primary, Secondary and ISP name server
- DNS Interrogation - Perform Zone Transfer by dictionary attack
- DNS INTEROGATION - Finding IPv6 IP blocks in use though DNS queries
- Mirror Target Web Site

Step 2 – Advanced Network Mapping

- Find live hosts
- Port and service scanning
- Perimeter network mapping (router, firewalls)
- Identifying critical services
- Operating System fingerprinting
- Identifying routes using Management Information Base (MIB)
- Service fingerprinting
- War-Dialing Attacks

Step 3 – Vulnerability Identification

- Identify vulnerabilities
- Perform false positive and false negative verification
- Enumerate discovered vulnerabilities
- Estimate probable impact (classify vulnerabilities found)
- Identify attack paths and scenarios for exploitation

Step 4 - Penetration Preparation

- Penetration preparation tips
- Introduction to automated pen-test frameworks
- Using Metasploit

Step 5 – Penetration

- Gaining control over windows 2003
- Defacing a website
- Adding a user
- Adding a user into administrator group
- Connecting server through terminal service
- Downloading and implementing a root-kit
- Hiding Attacker's Presence

Step 6 – Enumerating Further

- Sniffing traffic
- Gathering cookies
- Collecting email addresses
- Identifying routes and networks
- Performing password attacks
- Mapping internal networks

Repeating step 1-5 as appropriately

Step 7 – Compromise Remote Users/Sites

- XSS attack – Gaining access to internal network.
- XSS attack - Stealing enterprise data

Step 8 – Maintaining Access

- Placing Application & Kernel Level Rootkits which are not detected by Anti-Viruses
- How an Attacker Hides Files And Clears Logs

Step 9 – Clearing Logs

- Clear Logs – Windows Systems
- Clear Logs - Unix Systems

Game Over!

Course Contents

STRUCTURED PASSWORD CRACKING

- Hash Gathering
- Password Cracking
- Password Cracking in cluster environment

APPLICATION HACKING

- Phishing Attack
- In-Depth SQL Injection Attacks

DATABASE HACKING

- MS SQL
- Oracle

ANTI-VIRUS SYSTEMS HACKING

- Shutting down anti-virus systems
- Bypassing anti-virus systems

INTRUSION PREVENTION SYSTEM (IPS) HACKING

- Evading IPS (Network Level)
- Evading IPS (Application Level)

STEGANOGRAPHY - WHAT AL-QAEDA USES FOR SECURE COMMUNICATION?

- Introduction & Applications of Information Hiding
- Step-By-Step Uses of Steganography

HONEYPOTS - TRACKING HACKERS

- The Business Value of Honeypots
- Step-By-Step Implementation of Your Honeypots
- Maintain Your Honeypots

COMBATING SPAM - DEVELOPING ENTERPRISE ANTI-SPAM POLICY

- What is Spam and Why People Spam (Analysis of few famous spam)
- Step-By-Step Demonstration of Email Spoofing and Spamming
- Developing Enterprise Anti-Spam Policy

SUDDENLY MY NETWORK IS DOWN, WHAT TO DO? - REAL WORLD INTRUSION ANALYSIS

- Understanding Protocol Basics
- Traffic Analysis
- You've been Hacked – Performing Real World Intrusion Analysis

COMPROMISING ENTIRE NETWORK: MAN-IN-THE-MIDDLE ATTACK USING ADVANCE ARP CACHE POISONING:

- Capturing Plain Text Password
- Breaking SSL Tunnel
- Manipulating Email/WEB Traffic

SWITCH AND SWITCHING PROTOCOL ATTACKS

- Spanning Tree Attacks - How Gigabit Bandwidth Is Converted to Megabits?
- Converting Switch Functionality to a Hub – CAM Table Attack
- Isolating VLAN Security – VLAN spoofing and Double Encapsulation Attacks
- Bypassign Private VLAN Security
- Compromising Entire LAN by DHCP "Starvation" Attacks
- Denial of Service by Cisco Discovery Protocol (CDP) Attacks
- VLAN Trunking Protocol (VTP) Attacks
- DHCP Hacking
- Denial of Service by Multicast Brute Force Failover Analysis
- Denial of Service by Random Frame Stress Attack

ROUTER AND ROUTING PROTOCOLS HACKING

- Routing Issues (VTY/TTY Connections, SNMP, TFTP, FINGER, Console Port, Loose and Strict Source
- Routing, IP Spoofing etc…)
- Routing Protocol Issues (Autonomous System, RIP, OSPF, BGP, IRDP, IGRP, EIGRP)

VOIP HACKING

- VoIP Network Eavesdropping
- VoIP Interception and Modification
- VoIP Session and Application Hacking
- VoIP Network Infrastructure Denial of Service (DoS)

WIRELESS HACKING

- Scanning and detecting wireless networks
- Bypassing MAC filtering
- Hacking protected (WEP,WPA) wireless networks

BLUETOOTH HACKING

- Identifying Bluetooth Network
- Hacking Bluetooth

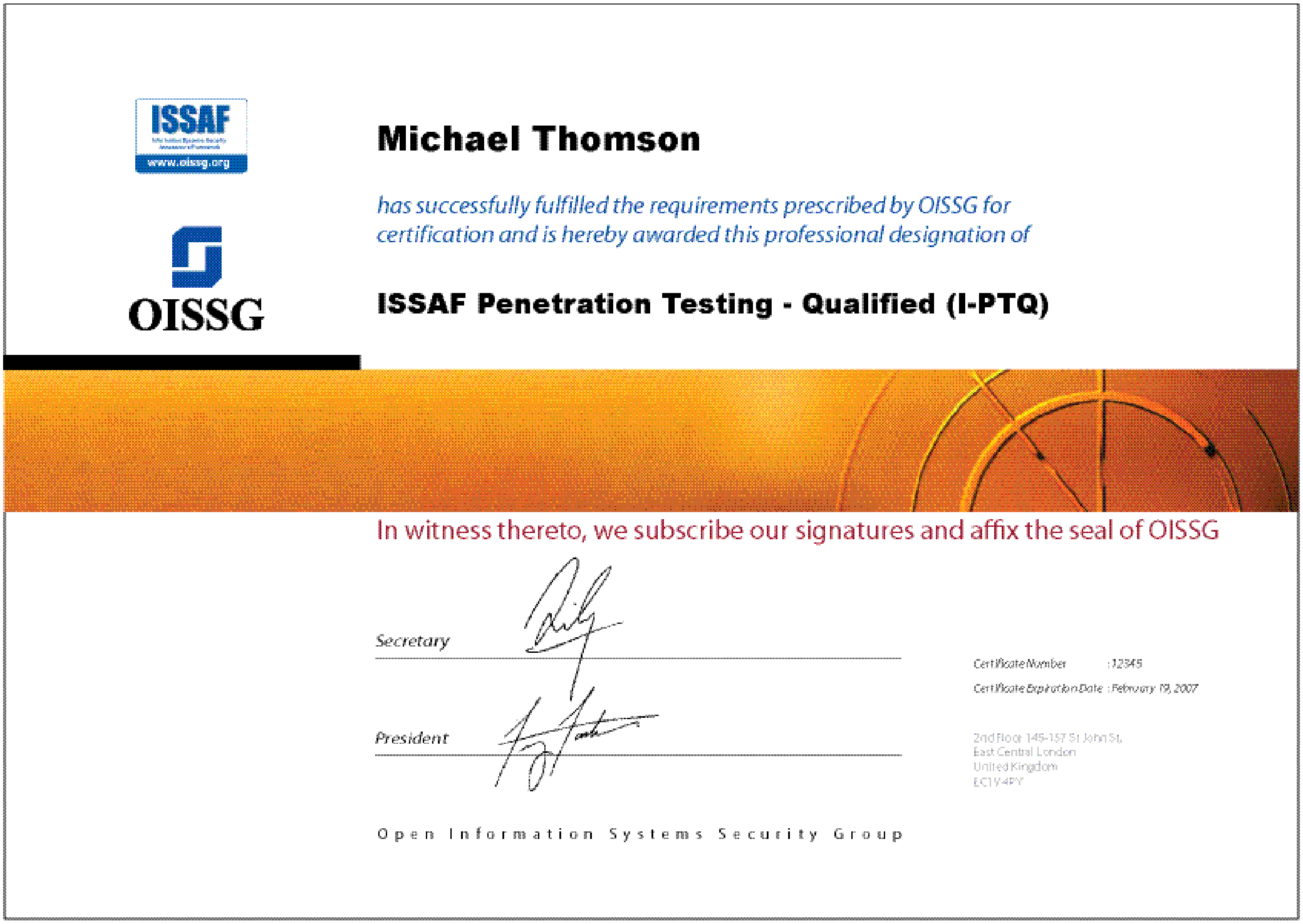
IDENTIFYING AND ANALYZING ADWARE/SPYWARE

ISSAF Penetration Testing Qualified (I-PTQ) Examination

This certification focuses on penetration testing of networks and technical assessment of the security architecture of an organization’s security process. This certification tests the ability of the candidate to apply ISSAF methodologies in carrying out penetration testing and in assessing and certifying security architecture in organizations. While the focus will be on assessment and certification of the security architecture in place, candidates will be expected to demonstrate good understanding of the penetration testing process itself as discussed in the sections on technical assessment in the ISSAF document. While a year of experience in penetration testing would be beneficial while taking the examination, it is not a pre-requisite. Candidates can attain this credential by passing a two-hour examination containing 150 MCQs and attaining 70% grade.

Those who want to be certified to teach this course at ATPs and at OISSG organized training events must pass this examination with 85% grade.

If you want to participate in ISP-Q, do write us at certifications@oissg.org



ISSAF
www.oissg.org

OISSG

Michael Thomson

has successfully fulfilled the requirements prescribed by OISSG for certification and is hereby awarded this professional designation of

ISSAF Penetration Testing - Qualified (I-PTQ)

In witness thereto, we subscribe our signatures and affix the seal of OISSG

Secretary ______________________

President ______________________

Certificate Number : 12345
Certificate Expiration Date : *February 19, 2007*

2nd Floor 145-157 St John St,
East Central London
United Kingdom
EC1V 4PY

Open Information Systems Security Group

Principal Instructor

Not yet 30, **Balwant Rathore** is a visionary entrepreneur and an avid information security professional. This time he is into the invention of Information Systems Security Assessment Framework (ISSAF) along with team OISSG after his outstanding and award winning performance in an acclaimed Police organization. He is founder member of OISSG and currently acting as Vice President. Under his leadership OISSG has emerged from a group of people to a professionally managed organization.

He is a technologist and frequent speaker to security briefings across the globe. He also writes for magazines like InformIT, Voice&Data, Network Magazines etc.

Balwant has provided security assessment, business continuity and computer crime investigation services to a wide variety of banking, financial institutions, including several "Top 10" banks, telecom and many more enterprises in Europe, North America, and Asia.

In his spare time, he develops new methodologies, security tools, and contributes to open-source security projects.

"An early member of the Open Information Systems Security Group, **Frank Sadowski** has engaged in facilitating and promoting future releases of the ISSAF, a comprehensive security assessment framework, co-authored by security specialists from many parts around the globe. He currently works as OISSG's Director of Security Awareness for the Middle East. Prior to joining the Middle East division of OISSG, he was a consultant in Europe, where he helped automotive clients deploy secure payment processes across their worldwide dealer networks. His passion for innovation, expert multilingual skill, and efficiency working with cross disciplinary teams have previously led him through a number of exciting roles in cutting edge technology companies in Germany, France, Spain, and the USA. Mr. Sadowski holds a B.S. in International Business from Bordeaux Business School (France) and from Muenster University of Applied Sciences (Germany)."

Karmil Asgarally has more than 8 years experience as both a financial auditor and an IT auditor. After working for Andersen Worldwide and KPMG, he obtained exposures in Mauritius, the African continent and the Middle East region from both a business and security perspective. He is currently working with Zakum Development Company (ZADCO), an Abu Dhabi based Oil Company in the United Arab Emirates. He holds ACCA, CISA and CISSP qualifications.

1	Abbott Laboratories
2	Abu Dhabi Commercial Bank (ADCB)
3	Abu Dhabi Company for Onshore Oil Operations (ADCO)
4	Abu Dhabi Investment Authority (ADIA)
5	Abu Dhabi Marine Operating Company (ADMA-OPCO)
6	Abu Dhabi Police
7	Al Futtaim Group
8	Al Jazeera
9	Algosaibi Information Systems
10	Aljomaih Holding
11	Alzabie & Co.
12	American University in Dubai (AUD)
13	Aub Dhabi National Insurance Company (ADNIC)
14	College of the North Atlantic (CNA)
15	Commercial Bank International (CBI)
16	Commercial Bank, Qatar (CBQ)
17	Computer Arabia
18	Dar Alwatan Journalism Printing, Kuwait
19	Dolphin Energy
20	Dubai Courts
21	Dubai eGovernment
22	Dubai Financial Market
23	Dubai Financial Services Authority (DFSA)
24	Dubai Islamic Bank
25	Dubai Ports, Customs and Free Zone Corporation (PCFC)
26	Emaar Financial Services
27	Emirates Identity Authority
28	Emirates Post
29	ESAB Middle East FZE
30	Etisalat Academy
31	Geco Mechanical & Electrical
32	General Head Quarter - Armed Forces Abu Dhabi
33	General Postal Corporation, Qatar
34	Goltens Company
35	Gulf International Bank (GIB)
36	INFOBAHN Systems
37	Islam Online
38	Kuwait Clearing Company
39	Kuwait University
40	Libano Suisse Insurance Co.
41	Majestic Hotels
42	Methanol Chemicals Company
43	Micromedia Qatar
44	Ministry of Education (MoE), Qatar
45	Ministry of Foreign Affairs (MFA), Qatar
46	Ministry of Interior (MoI), Qatar
47	Ministry of Interior (MoI), Qatar
48	Mittal Steel Company
49	Mövenpick Hotels & Resorts
50	National Bank of Dubai
51	National Gas Shipping Company Limited (NGSCO)
52	National Marine Dredging Company (NMDC)
53	National Petroleum Construction Company (NPCC)
54	Oman Insurance Company (PSC)
55	Oryx GTL
56	PRO TECHnology
57	Public Works Authority, ASHGHAL
58	Qatar Financial Centre Regulatory Authority
59	Qatar Fuel Additives Company Limited (QAFAC)
60	Qatar Information & Marketing (QIM)
61	Qatar Vinyl Company LTD.
62	Saudi Hollandi Bank-Riyadh, KSA
63	Saudi Telecom
64	Sharjah Airport International Free Zone (SAIF-Zone)
65	Sharjah Islamic Bank (SIB)
66	SHUAA Capital P.S.C.
67	Teyseer Group of Companies
68	The Centre for GIS - State of Qatar
69	The King Fahd University of Petroleum & Minerals (KFUPM)
70	Urban Planning & Development Authority (UPDA), Qatar

About OISSG

Open Information Systems Security Group (OISSG) is a not-for-profit organization head quartered in London. Our vision is to spread information security awareness by hosting an environment where security enthusiasts from all over the globe share and build knowledge. It was established with the objective of evolving a set of open standards, guidelines and good practices in the area of information security. As a first step in this direction, a comprehensive framework for the assessment of information systems security has been released. The Framework is known as ISSAF, which can be downloaded from www.oissg.org/issaf.

1920 Ambleside dr.
Colorado Springs
Colorado, USA 80915

Phone:	+1 719 573 4949
Email:	info@oissg.org
Web:	www.oissg.org

2nd Floor, 145-157 St. John Street,
London, EC1V 4PY,
United Kingdom.

Phone:	+44 (0) 207 871 4033
Fax:	+44 (0) 207 160 5209
Email:	info@oissg.org
Web:	www.oissg.org

Registration Form

Event: Cutting Edge Hacking and Defense

	Name	Department	Job Title	Email
1st Delegate				
2nd Delegate				
3rd Delegate				
4th Delegate				
5th Delegate				
To assist us with future correspondence, please supply the following details:				
Head of Department				
Training Manager				
Booking Contact				

Register Now

Contact Marketing at OISSG

Tel: +971 50 9498556

Fax: +971 4 3197775

Email: gulshan@oissg.org

OISSG

A Non-Profit Organisation

www.oissg.org

Workshop
25th - 27th November, 2007

Exam
27th November, 2007

- **35% Discounted fees**
- **Register for 3 at once, get the 4th free!**
- **Certification Exam Free with Workshop**

Cost: US$ 1,500/-Per Person Only

Venue: The Fairmont Dubai

Contact: +971 50 9498556, Fax: +971 4 3197775, Email: gulshan@oissg.org