HITB

Hack In The Box
Security Conference 2004

Conference Kit

* Network Assessment and Latest Attack Methods
* Fundamental Defense Methodologies
* Close look at the latest security technology
* Advanced Computer and Network Security topics
* Deep Knowledge Presentations

Organised by:

hack in the box
Keeping Knowledge Free

Hack In The Box (M) Sdn. Bhd. (622124-V)
Level 26, Menara IMC
No 8. Jalan Sultan Ismail,
50250 Kuala Lumpur, Malaysia.
Phone: ++603-20394724
Fax: ++603-20318359

Overview

The main aim of our conferences is to enable the dissemination, discussion and sharing of network security information. Presented by respected members of both the mainstream network security arena as well as the underground or black hat community, this years conference promises to deliver a look at several new attack methods that have not been seen or discussed in public before.

Along with that, we are also organizing a hacking competition known overseas as Capture The Flag. A contest first developed and presented at Defcon in Las Vegas, the idea behind a CTF competition is to allow for individuals (either solo or in teams) to hack into prepared servers running on an internal network in order to retrieve marked files or flags on these target machines. Participants are also allowed to attack each other if it requires them to do so. The winner or winners, who obtain the most number of flags in the shortest period of time – wins. The Intrusion Detection System log files and findings will be presented at the end of the conference.

We believe that this conference would be an ideal opportunity for vendors from within the industry to meet with not only the experts but to share their own expertise and technology with the public.

Event Details

Date: October 4th & 5th 2004
Item: 2-Track Training Sessions
Time: 9am to 6pm
Venue: The Westin, Kuala Lumpur

Date: October 6th & 7th 2004
Item: 3-Track Security Conference
Time: 9am to 6pm
Venue: The Westin, Kuala Lumpur

Date: October 6th & 7th 2004
Item: Capture The Flag and Open-Hack
Time: 9am to 6pm
Venue: The Westin, Kuala Lumpur

Who should attend: Anyone who is responsible for the security and privacy of information should attend including: CEO, CIOs, CTOs, VPs of Technology and Network Systems, Directors of IT, Directors of Technology, Systems Architects, Network Administrators, Network Security Officers, ISOs, Financial Managers, System Developers, Network Security Specialists, Security Consultants, Risk Managers, and System Administrators.

The Keynote Speakers

John Draper aka Captain Crunch – CTO/Co-founder ShopIP
(http://www.shopip.com)

Presentation Title: TBA
Presentation Details: TBA

About John:
An original member of the now famous "Homebrew Computer Club", Mr. Draper (AKA Captain Crunch), has over 30 years of programming and security expertise.

Widely known as the first security pioneer, Mr. Draper became interested while learning how to penetrate phone networks. He now uses his penetration skills to test the vulnerabilities in computer networks. While serving in the USAF, he worked on long range radar and radio equipment used for encryption. After a stint with American Astrionics, designing high speed Operation Amplifiers for precision missile guidance, he worked as an Engineering Technician at National Semiconductor.

He has been an innovator, writing high-speed analog encryption programs, specialized chebychev and butterworth filter circuit programs, and some of the first CAD programs. He then wrote the first cross-assemblers used in writing Assembly Language for the 8080, 6502, 1802, and 6800 chips.

At the Homebrew Computer Club, Mr. Draper designed his own computers and helped create the "Blue Box" tone generator. Introducing, among others, Steve Wozniak and Steve Jobs to the computing world, and a generation of hackers to the glorious concept of "phone phreaking", spawning the worldwide "2600" clubs. His work with Jobs and Wozniak led him to become the 13th employee of Apple computers, designing telephone interface boards, and developing both hardware and software for the Apple II.

Mr. Draper implemented the first FORTH language on the Apple II, utilizing it to write a word processor. After modifying it for commercial sale, Easy Writer, the world's first word processor was born. It took him only 20 minutes to port FORTH to the PC, and 48 hours later, Easy Writer was delivered to IBM, beating out Bill Gates and the early Microsoft team on the project. While working for IBM, Mr. Draper created the "Virtual Machine Interface", a screen and keyboard driver.

He is now a sought after Security consultant and Conference speaker, and has been touring the security conference circuit for years. His security expertise has led him to appearances on Nightline, Good Morning America and various radio shows nationwide, most recently on CNET radio in San Francisco, and The Learning Channel (The secret life of hackers).

Draper has appeared on A&E, and recently did a documentary for Channel Four in England. You can find him on the Discovery Channel Hall of Fame, further entrenching him as one of the true innovators of the industry. A co-founder of ShopIP, Mr. Draper performs security audits and is an architect of the CrunchBox firewall/IPS system. He also does database, Python, and secure GUI programming for SpamCruncher and CrunchBox.

Theo De Raadt – Project Leader, OpenBSD & OpenSSH
(http://www.openbsd.org)

Presentation Title: Exploit Mitigation Techniques
Presentation Details: OpenBSD has been auditing software for nearly 10 years, and while we have had significant success, it is clearly not enough. In the last 3 years a new view on preventing attacks has surfaced in the mindset of our group. A software exploit author starts by finding an interesting bug. Writing an exploit is easy because he can rely on a variety of system behaviours which are very deterministic. Many of these behaviours are not required for proper operation. Recently we have developed many new techiques which combine to thwart the attacker, without affecting regular software. We make the Unix process environment difficult to attack much like filling a house full of a variety of burglar traps.

About Theo:

Theo de Raadt has been involved with free Unix operating systems since 1990 (Minix!) and then became one of the founders and prime developers of NetBSD. In 1995 Theo created the OpenBSD project, creating a free Unix that focuses primarily on security technologies. A few years later he also started the OpenSSH project (the most deployed Open Source software). Theo works full time on advancing OpenBSD, OpenSSH, and any technology which enhances free Unix security.

This year's speakers

(Listed in alphabetical order)

Adam Gowdiak - Poznan Supercomputing and Networking Center

(http://www.man.poznan.pl)

Presentation Title: TBA
Presentation Details: TBA

About Adam:

Adam Gowdiak is a graduate of the Poznan University of Technology. Since 1996 he has been working as security engineer and systems analyst at Poznan Supercomputing and Networking Center. He is the finder of many security vulnerabilities in IRIX, AIX, Windows and Java Virtual Machine. He has been the speaker at many international computer and network security related events. His security research interests include reliable vulnerabilities exploitation techniques, new attack methodologies, mobile code security, intrusion detection/prevention systems and advanced reverse engineering techniques.

Emmanuel Gadaix – Co-Founder, Globe Relay

(http://www.relaygroup.com)

Presentation Title: Phreaking in the 21st Century
Presentation Details: Icons like Captain Crunch remind us that there was a time when phreakers were all the rage and abusing CCITT#5 phone switches was open to anybody with a blue box. As most Telco.s upgraded their equipment to support the new, out-of-band, digital SS7 signaling protocol, blue boxing was slowly but surely phased out. Phreakers went legit or quiet. The Internet and its lot of script kiddies became the center of interest.

Is phreaking dead? We beg to differ!

This presentation will focus on advanced phreaking techniques for the 21st century warrior. After a short presentation of current digital telecommunications network (with a focus on GSM/GPRS/EDGE and CDMA/3G) we will study how each element can be compromised for fun and profit. Nothing will be left untouched:

. Core Switching
. Radio Networks
. GPRS infrastructure
. 3G data
. Messaging (SMS, MMS, voicemail, USSD)
. Roaming, subscriber management platforms
. Fraud management
. Customer care systems
. Billing systems
. Mediation systems
. WAP servers
. Intelligent Network services (e.g. prepaid, VPN, conditional forwarding and screening etc.)
. Legal interception gateway
. Signaling devices
. Content aggregators
. Network Management Systems

We will also partially unveil the phreakers holy grail: Abusing out-of-band signaling by compromising SS7 nodes.

About Emmanuel:

Emmanuel started his career in GSM telecommunications in 1994, specializing in Network Management Systems and Intelligent Networks, participating in the launch of several cellular networks across Asia and Europe, with a focus on Value-Added Services. In 1997 he co-founded Globe Relay, a consulting firm based in Thailand with the purpose of focusing on the highly specialized security services for the GSM / 3G operator. Globe Relay has the combined strength of security knowledge in, both, the IP and GSM environments, including technologies such as GPRS, EDGE, CAMEL, etc.

Jose Nazario – Senior Software Engineer, Arbor Networks.

(http://www.arbornetworks.com)

Presentation Title: Packet Mastering
Presentation Details: The packet manipulation libraries "libdnet", "libpcap", and "libnids" are seen by many as difficult to use. however, they can be easy to use when you start working with them. this talk introduces these three libraries, the core of many interesting network applications. also, this talk will show how to tie them together with event based programming. once you learn these libraries and techniques, interesting network tools are within your grasp. the development language will be in C.

About Jose:

Dr. Jose Nazario is a worm researcher and senior software engineer at Arbor Networks. Dr. Nazario's research interests include large-scale Internet trends such as reachability and topology measurement, Internet events such as DDoS attacks and worms, source code analysis methods and datamining. He routinely writes and speaks on Internet security in forums that include NANOG, USENIX Security, BlackHat Briefings, CanSecWest and SANS. Dr. Nazario holds a Ph.D. in biochemistry from Case Western Reserve University.

Dr. Nazario is also the author of the ground-breaking book entitled "Defense and Detection Strategies against Internet Worms" which offers insight into worm trends and behavior, while providing practical protection techniques. Dr. Nazario was also co-author on the book "Secure Architectures with OpenBSD".

Kamal Hilmi Othman – Systems Engineer, NISER

(http://www.niser.org.my)

Presentation Title: TBA
Presentation Details: TBA

About Kamal:

Kamal Hilmi Othman is currently a systems engineer at NISER, focusing in the areas of perimeter defense, detection and intrusion analysis. He was previously a lecturer at a local Malaysian college; however, he now prefers to sit in as guest speaker for 'information security' classes at local Universities instead.

Kamal has recently presented papers at CanSecWest04 in Canada and USENIX04 in Boston Massachusetts. He is also an active member of the HITB Conference Organizing Committee.

Nitesh Dhanjani - Senior Consultant, Ernst & Young
(http://www.ey.com)

Presentation Title: TBA
Presentation Details: TBA

About Nitesh:

Nitesh Dhanjani is a senior consultant at Ernst & Young's Advanced Security Center. He has performed network, application, web-application, wireless, source-code, host security reviews and security architecture design services for clients in the Fortune 500.

Nitesh is the author of "HackNotes: Unix and Linux Security" (Osborne McGraw-Hill). He is also a contributing author for the best-selling security book "Hacking Exposed 4" and "HackNotes: Network Security".

Prior to joining Ernst & Young, Nitesh worked as consultant for Foundstone Inc. where he performed attack and penetration reviews for many significant companies in the IT arena. While at Foundstone, Nitesh both contributed to and taught parts of Foundstone's "Ultimate Hacking: Expert" and "Ultimate Hacking" security courses.

Nitesh has been involved in various educational and open-source projects and continues to be active in the area of system and Linux kernel development. He has published technical articles for various publications such as the Linux Journal.

Nitesh graduated from Purdue University with both a Bachelors and Masters degree in Computer Science. While at Purdue, he was involved in numerous research projects with the CERIAS (Center for Education and Research Information Assurance and Security) team. During his research at Purdue, Nitesh was responsible for creating content for and teaching C and C++ programming courses to be delivered remotely as part of a project sponsored by IBM, AT&T, and Intel.

Ollie Whitehouse – Director of Security Architecture, Atstake Limited UK
(http://www.atstake.com)

Presentation Title: Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks
Presentation Details: This presentation will cover and in addition carry on from the paper published in March 2004 of the same name by @Stake Security: .2.5G and 3.0G cellular technologies are here to stay.. This whitepaper assesses the issues still facing the industry since the GPRS Wireless Security: Not Ready for Primetime paper was published in June 2002. GTP (GPRS Tunneling Protocol) is now widely deployed in a majority of 2.5G and 3.0G cellular networks, and this paper reviews some of the potential attacks against the GTP protocol and the possible effects this will have on cellular providers. It also reviews some of the architectural alternatives that providers can consider. This paper will discuss several new as yet unpublished and undisclosed vulnerabilities in 3G equipment.

About Ollie:

As Director of Security Architecture at @stake, Ollie has several years of information technology experience. His professional experience includes systems integration, security consultancy, and project management. He has published a wide number of advisories in products from Microsoft Outlook through to SAP DB. In addition Ollie has also published a number of whitepapers covering the security of cellular and bluetooth technologies. At @stake, he forms part of the London based professional services organization, providing clients with Attack & Penetration services as well as system and application architecture reviews. Ollie also heads @stake's wCOE researching technologies that include PDA's, Bluetooth, WiFi, Cellular and other RF technologies and the applications that use or run over these technologies.

Saumil Shah – Founder & Director, Net-Square Solutions

(http://www.net-square.com)

Presentation Title: TBA
Presentation Details: TBA

About Saumil:

Saumil continues to lead the efforts in e-commerce security research at Net-Square. His focus is on researching vulnerabilities with various e-commerce and web based application systems. Saumil also provides information security consulting services to Net-Square clients, specializing in ethical hacking and security architecture. He holds a designation of Certified Information Systems Security Professional. Saumil has had more than nine years experience with system administration, network architecture, integrating heterogeneous platforms and information security and has performed numerous ethical hacking exercises for many significant companies in the IT area. Saumil is a regular speaker at security conferences such as BlackHat, RSA, etc.

Previously, Saumil was the Director of Indian operations for Foundstone Inc, where he was instrumental in developing their web application security assessment methodology, the web assessment component of FoundScan - Foundstone's Managed Security Services software and was instrumental in pioneering Foundstone's Ultimate Web Hacking training class.

Prior to joining Foundstone, Saumil was a senior consultant with Ernst & Young, where he was responsible for the company's ethical hacking and security architecture solutions. Saumil has also worked at the Indian Institute of Management, Ahmedabad, as a research assistant and is currently a visiting faculty member there.

Saumil graduated from Purdue University with a master's degree in computer science and a strong research background in operating systems, networking, information security, and cryptography. At Purdue, he was a research assistant in the COAST (Computer Operations, Audit and Security Technology) laboratory. He got his undergraduate degree in computer engineering from Gujarat University, India. Saumil is a co-author of "Web Hacking: Attacks and Defense" (Addison Wesley, 2002) and is the author of "The Anti-Virus Book" (Tata McGraw-Hill, 1996)

Shreeraj Shah - Director, Net-Square Solutions

(http://www.net-square.com)

Presentation Title: TBA
Presentation Details: TBA

About Shreeraj:

Shreeraj founded Net-Square in January 2000, to establish the company as a strong security research and security software development company. Net-Square has been instrumental in developing and exporting web security components companies such as Foundstone and NT OBJECTives. He leads research and development arm of Net Square. He has over 5 years of experience with system security architecture, system administration, network architecture, web application development, security consulting and has performed network penetration testing and application evaluation exercises for many significant companies in the IT arena. In the past Shreeraj worked with Chase Bank and IBM in area of web security.

Shreeraj graduated from Marist College with a Masters in Computer Science, and has a strong research background in computer networking, application development, and object-oriented programming. He received his graduate degree in Computer Engineering from Gujarat University, and an MBA from Nirma Institute of Management, India. Shreeraj has also authored a book titled "Web Hacking: Attacks and Defense" published by Addison Wesley.

S.K. Chong – Co-Founder & Security Consultant, Scan Associates Sdn. Bhd.

(http://www.scan-associates.net)

Presentation Title: TBA
Presentation Details: TBA

About SK:

S.K. Chong is Co-Founder and Security Consultant for SCAN Associates; a Malaysian based consulting and security Services Company. SCAN Associates is also two-time winner of the Capture the Flag hacking competition held last year in Malaysia. SK Chong is also the author of several white papers including "SQL Injection Walkthrough" and "Win32 Buffer Overflow Walkthrough". The paper detailed findings previously unknown exploit in Microsoft's SQL Server. Over the last 2 years, he has conducted more than 20 professional penetration tests on various local government and military agencies, financial and ISP companies as well as profession binary audit for company in Fortune 500. His primary interests include binary and code audits, exploit research and penetration testing.

The grugq

(http://grugq.tripod.com/reap/)

Presentation Title: The Art of Defiling: Defeating Forensic Analysis on Unix File Systems
Presentation Details: The rise in prominence of incident response and digital forensic analysis has prompted a reaction from the underground community. Increasingly, attacks against forensic tools and methodologies are being used in the wild to hamper investigations. This talk will: familiarize the audience with Unix file system structures; examine the forensic tools commonly used, and explore the theories behind file system anti-forensic attacks. In addition, several implementations of new anti-forensic techniques will be released during the talk. Anti-forensics has cost the speaker one job. This material has never been presented in the North American continent because anti-forensics scares the feds. Find out why.

About The Grugq:

The grugq has been researching anti-forensics for almost 5 years. Grugq has worked to secure the networks and hosts of global corporations, and hes also worked for security consultanting companies. His work as a security consultant was cut short by the publication of an article on anti-forensics. Currently, he slaves for a start-up, designing and writing IPS software. Grugq has presented to the UK's largest forensic practioner group where he scared the police. In his spare time, grugq likes to drink and rant.

Wong Chun Meng - Senior Consultant, Spectrum Edge Sdn. Bhd.

(http://www.spectrum-edge.com/)

Presentation Title: TBA
Presentation Details: TBA

About CM Wong:

Chun Meng has more than 5 years experience in the IT security field and is responsible for providing consulting services and security training for Spectrum Edge's customers. Areas of expertise include designing security management infrastructures, systems security, system forensics and ethical hacking focusing on Unix and Windows platforms. Chun Meng has provided his expertise to various financial institutions, government bodies, and multinationals primarily in Singapore and Malaysia. Prior to joining Spectrum Edge, Chun Meng worked as a consultant for Infinitum Security in Singapore, performing mainly ethical hacking and security systems audit work. In addition, he has contributed articles to CNET Asia as well as being an avid speaker at major security conferences in his own free time. Chun Meng graduated from Monash University with a Bachelors Degree in Electrical Engineering and is a Certified Information Systems Security Professional (CISSP).

Deep Knowledge Technical Training & Biz-Tech Training Overview

TECHNICAL TRAINING TRACK 1 SPAM ATTACKS AND HOW TO DEAL WITH THEM

BY: John T. Draper (aka Captain Crunch)

- **Date:** 4th & 5th October 2004
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax

This course will examine and discover the methods deployed by spammers, hackers, and other insurgents in their never ending quest to fill as many mailboxes with spam and smut as possible. Participants will get hands on experience in how to interpret spam mail headers, identify mail sending points, extract domain ownership information on who really owns these spam promoted web sites, and how to track them.

The course is based on analysis of the tools spammers use to control large amounts of infected machines for their deeds, whatever they are. This includes the use of Honey pots for the purpose of deliberately infecting a machine, then "sniffing" the network for anomalous behavior.

These sniffed logs are then examined to determine their protocol, examine payload, and identify unique "patterns" which are used to construct Snort IDS rules for the detection of any communication protocol the virus or Trojan may be using.

During the course, the participants will be introduced to the following methods, code, and tools for the identification of these viruses, as well as the following disciplines.

- Examining spam mail to identify it's source
- Using network tools to identify the organization the spam came from
- Setting up an IDS and network analysis system
- Sniffing and identification of virus or Trojan communication protocols.
- Examining methods of acting on IDS events in real time.
- Network tracing to identify upstream providers
- Examining how viruses and worms are spread.

Participants would have access to UNIX and Windows OS machines, with access to Python programming language, used to write specialized programs and tools.

Key Learning Objectives:

- How to manage and deal with the large volume of spam
- How to protect your network from hostile attacks from inside or outside threats
- How to write Snort rules in almost "real time" to detect new threats as they come in
- Identification of 'Phishing' schemes, and Email tracking.
- Tracking down spammers
- Spam reporting techniques.
- Basic Python programming

General Learning Objectives:

- How to protect you and your network from outside threats
- How to develop a spam managed Email system
- How to report spam, and what ISP's want in their reports.

Who should Attend:

- Network and System administrators
- CTO's and technical management
- John Q Public
- Students
- Law Enforcement
- Attorneys
- Lawmakers
- Anyone interested in a spam free internet experience.

TECHNICAL TRAINING TRACK 2
WEB APPLICATION SECURITY – ATTACK AND DEFENCE

BY: Saumil Shah & Shreeraj Shah [Net-Square Consulting and MIMOS Consulting Group (MCG)]

- **Date:** 4 & 5th October 2004
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax

Beginning with an introduction to Web applications, the participants will be offered an insight into web hacks and their resulting effects, followed by thorough assessment methodologies and defense strategies for varying environments.

Who Should Attend

This course is designed for:

a) Developers: Learn what can go wrong with badly written application code, and how to prevent such errors.
b) Web site administrators: Learn how to securely configure a web server and an application server, without compromising on functionality.
c) Project managers / IT managers: Learn how to be effective in maintaining a secure web application, going ahead.

Skills Required

- Operational comfort with Windows 2000 or Linux
- Basic Windows 2000 or Linux administration skills
- Basic scripting skills - Perl, PHP, ASP. Participants should be able to review example code and spot errors, without knowing the correct syntax, and should be intuitively able to fix it.
- Basic SQL skills or knowledge.

Introduction to web applications

- Components of a web application
- Basics of web technologies and protocol information
- Evolution of technologies and impact on security
- Understanding other basic web security-related concepts
- Learning tools like netcat, achilles etc. to understand its usage and application. (Hands on for the group)

Web Hacking – Areas of attack

Various attacks will be covered in detail with demonstration followed by hands on exercises. Following is a brief list of attacks.

- Cross-site scripting attacks
- SQL Query Injection
- Session Hijacking
- Buffer Overflows
- Java Decompilation
- HTTP brute forcing
- Trojan Horses and Malware products
- Form Manipulation, Query Poisoning
- Input Validation,Parameter Tampering
- Authentication
- Information leakage
- File operations
- Client-side manipulations
- Cryptography
- Error/Exception handling

Attack and Defense strategies

- Impact of attacks
- Risk analysis
- Countermeasures
- Defense strategies and methods

Assessment Methodology and Defending Applications

- Reconnaissance – Profiling a web application
- Black-box and White-box testing
- Exploiting vulnerabilities
- Defending applications
- Secure coding strategies

Hands-on :

The training programme will end with an “assessment challenge” – a live Web Application. Working with time constraints, participants are expected to analyze the application, identify and exploit loopholes and apply all defense strategies learnt, to secure the application.

BIZ-TECH TRAINING
HACKERS INSIGHT FOR CIOS

BY: Jorge Sebastiao [E-Security Gulf Group (ESGulf)]

- **Date:** 5th October 2004
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 1-day
- **Capacity:** 15 pax

Information security is critically important to today's organizations. You business may depend on the future of an e-Banking. Esgulf has developed a comprehensive practical course that introduces you to information security and protection from the Hackers perspective. This one-day intensive course prepares you to understand your organization information protection needs in the new age of the Internet.

We will cover practical topics of information security. We expose the participants to the nature of vulnerabilities and how they are being exploited by hackers today. We will highlight the state-of-the-art technologies to defend and manage the risk against these threats. We will build real awareness about today's dangers in information security. We provide a practical view of the real dangers your organization faces from Hackers and understand the requirements to develop effective protection standard, policies and monitoring systems for their own business. This course is based 100% on practical and real world examples.

Key Learning Objectives:

Web Security Basics

- Security in the News, Attacks and their nature
- Threats, Vulnerabilities, Methodology for Security

Hacker's Viewpoint

- Information gathering techniques
- Penetration, Exploiting weaknesses and vulnerabilities
- Gaining access, Pilfering
- Covering tracks, Creating back doors, Denial of Service
- Google as a search tool
- Downloading and Installing
- Scanning, Penetrating

Wireless Security

- Basics
- Bluetooth
- Wifi

Social Engineering

- Weakest Link, Human Element
- Security Awareness, Beyond traditional Info Security
- Protection, Detection, Response

Key elements of Info Security

- Policy
- 2x7x365
- Security Awareness, Training, Education
- Incidence Response
- BCP/DRP

Hacking Workshops

- Using Google
- Hacking Passwords
- Stealing Emails
- Hacking WWW sites

Who Should Attend:

- Upper Management and key decision makers.
- Technical managers

ITINERARY

Date	Item	Duration	Trainer / Speaker
October 4th & October 5th	**Technical Training Track 1**	2 Days	John T. Draper
October 4th & October 5th	**Technical Training Track 2**	2 Days	Saumil Shah & Shreeraj Shah
October 5th	**Biz-Tech Training**	1 Day	Jorge Sebastiao
Date	**Item**	**Duration**	
October 6th & October 7th	**Triple Track Security Conference**	2 Days	
October 6th & October 7th	**Capture The Flag**	2 Days	
October 6th & October 7th	**Open-Hack**	2 Days	

PRICING

Training & Conference:

Item	Cost
Technical Training Track 1 + Conference	**RM1,860.00**
Technical Training Track 2 + Conference	**RM1,860.00**
Business Training + Conference	**RM1,860.00**

Training Only

Item	Cost
Technical Training Track 1	**RM1,500**
Technical Training Track 2	**RM1,500**
Business Training	**RM1,500**

Conference Only

Item	Cost
2-Day Triple Track Security Conference	**RM360** (before August 1st 2004) **RM450** (there after)

HOW TO MAKE PAYMENT

Please ensure cheques are made payable to:

HACK IN THE BOX (M) SDN. BHD.
Maybank Account No: 514178-207038

Write your FULL NAME and Conference Registration ID on the back of the cheque, and mail it to us. Alternatively, you can deposit the cheque to us at any Maybank Cheque Deposit Machine and **fax the deposit slip** to our office or **scan it and e-mail it** to conferenceinfo -at-hackinthebox.org.

If you are a Maybank account holder, you may make a direct deposit into our account at any Maybank ATM. Your deposit slip should once again be **faxed to us** or **scanned and e-mailed** as above.

DO NOTE! Your conference seat is not considered secured till payment and proof of payment has been received by us.

CONTACT INFORMATION

For Event Registration, please register online at:

http://conference.hackinthebox.org/register.php

For information regarding sponsorship, please contact:

- Dhillon Andrew, Dhillon@hackinthebox.org
- Dinesh Nair, dinesh@hackinthebox.org

For information regarding Capture the Flag competition (CtF) and Open-Hack, please contact:

- Meling Mudin (spoonfork), mel@hackinthebox.org

For general enquiries, please contact:

- The Organizing Committee, conferenceinfo@hackinthebox.org

MAILING ADDRESS

Hack In The Box (M) Sdn. Bhd. (622124-V)
Level 26 Menara IMC,
No 8, Jalan Sultan Ismail
50250 Kuala Lumpur, Malaysia.
Phone: ++603-20394724
Fax: ++603-20318359