HITBSECCONF2008 – MALAYSIA

CONFERENCE KIT 2.0

Hack In The Box (M) Sdn. Bhd. (622124-v)
Suite 26.3, Level 26, Menara IMC,
No. 8 Jalan Sultan Ismail,
502050 Kuala Lumpur,
Malaysia

Tel: +603-20394724
Fax: +603-20318359
Site: http://conference.hackinthebox.org/hitbsecconf2008kl/

27th & 28th October

- TT1 - Structured Network Threat Analysis & Forensics
- TT2 - Bluetooth, RFID and Wireless Hacking
- TT3 - Web Application Security - Advanced Attack & Defense
- TT4 - The Exploit Laboratory

29th & 30th October

- Triple Track Security Conference featuring 4 keynote speakers and over 35 international experts
- Capture The Flag 'Live Hacking' Competition
- Lock Picking Village
- Bluetooth, RFID and WiFi Village

The largest network security conference in Asia and the Middle East!

The main aim of our conference is to enable the dissemination, discussion and sharing of deep knowledge network security information. Presented by respected members of both the mainstream network security arena as well as the underground or black hat community, our events routinely highlight new and ground-breaking attack and defense methods that have not been seen or discussed in public before.

HITBSecConf2008 - Malaysia will be our 6th conference in Malaysia and is expected to attract over 1000 attendees from around the Asia Pacific region and from around the world. This year's event will also see the introduction of a third track to our conference program called the 'HITB Labs'. These new hands-on sessions are designed to give attendees a closer and deeper understanding of various security issues from physical security bypass methods to the security of RFID and other wireless based technologies.

HITBSecConf2008 - Malaysia will also see our highly popular team-based hacking competition known as Capture The Flag. First developed and presented at Defcon in the US, the idea behind a CTF competition is to allow for teams of three to hack into prepared servers running in order to retrieve marked files or flags on these target machines. Participants will also be required to defend their systems from attack. Teams will be judged on both their defensive as well as the offensive game play.

We believe HITBSecConf is an ideal platform for leading network security vendors to not only meet with some of the leading network security specialists but to also showcase their own technology and solutions with the public as well.

Keynote Speakers

KEYNOTE 1 - Jeremiah Grossman
(Founder and CTO of Whitehat Security)

Jeremiah Grossman, founder and chief technology officer of WhiteHat Security, is a world-renowned expert in web application security and a founding member of the Web Application Security Consortium (WASC). Prior to WhiteHat, Mr. Grossman was an information security officer at Yahoo!

KEYNOTE 2 - Marcus Ranum
(Chief Security Officer, Tenable Network Security)

Marcus J. Ranum is a world-renowned expert on security system design and implementation. He is recognized as the inventor of the proxy firewall. He has designed a number of groundbreaking security products including the DEC SEAL, the TIS firewall toolkit, the Gauntlet firewall, and NFR's Network Flight Recorder intrusion detection system. In 2001, he was awarded the TISC "Clue" award for service to the security community, and the ISSA Lifetime Achievement Award.

KEYNOTE 3 - Dr. Anton Chuvakin
(Chief Logging Evangelist, LogLogic)

Dr Anton Chuvakin, GCIH, GCFA is a recognized security expert and author of the book "Security Warrior" and a contributor to "Know Your Enemy II", "Information Security Management Handbook", "Critical Threads 2006", "Hacker's Challenge 3", and "PCI Compliance".

KEYNOTE 4 - THE FOUNDERS OF THE PIRATE BAY
(Peter Sunde [brokeop] with Fredrik Niej [TiAMO])

brokep, is a Norwegian-Finnish computer expert and one of the co-founders of the World's Largest Bit Torrent site - The Pirate Bay. TiAMO is also a co-founder of TPB and the owner of 'the most lawyer unfriendly hosting provider' - PRQ.

Our Distinguished Panel of Speakers

1. AR (Independent Network Security Researcher, Securebits)

2. Adrian 'pagvac' Pastor (ProCheckUp Ltd. / GNUCITIZEN)

3. Akshay Agrawal (Practice Manager, Microsoft Information Security ACE Team)

4. Andrew 'Q' Righter (HacDC)

5. Alexander Tereshkin (Principal Researcher, Invisible Things Lab)

6. Charlie Miller (Principal Analyst, Independent Security Evaluators)

7. Ching Tim Meng (Security Consultant, Cable & Wireless)

8. Dino Covotsos (Managing Director, Telspace Systems)

9. Dino Dai Zovi (Security Researcher)

10. Ero Carrera (Reverse Engineering Automation Researcher, zynamics GmbH)

11. Haroon Meer (Technical Director, Sensepost Information Security)

12. Hernan Ococha (Senior Security Consultant, Core Security Technologies)

13. Ilfak Guilfanov (Founder/CEO of Hex-Rays SA and creator of IDA Pro)

14. Jamie Butler (Coauthor of Rootkits: Subverting the Windows Kernel)

15. Jim Geovedi (Member of HERT & Security Consultant, PT. Bellua Asia Pacific)

16. Julian Ho (Chief Operating Officer, THINKSecure Pte. Ltd.)

17. King Tuna (Independent Network Security Researcher)

18. Kris Kaspersky (Independent Network Security Researcher / Author for Xakep Magazine)

19. Lee Chin Sheng [geekool] (Independent Network Security Researcher)

20. Matthew Geiger (Forensics Specialist, CERT)

21. Meling Mudin [spoonfork] (Independent Network Security Researcher)

22. Marc Weber Tobias (Investigative Attorney and Security Specialist)

23. Nitesh Dhanjani (Senior Manager, Ernst & Young)

24. Paul Craig (Principal Security Consultant, Security-Assessment.com)

25. Pedram Amini (Manager, Security Research, TippingPoint)

26. Petko D. Petkov [pdp] (GNUCITIZEN)

27. Shreeraj Shah (Director, BlueInfy)

28. Saumil Shah (Founder, Net-Square)

29. Teo Sze Siong (Senior Web Security Researcher, F-Secure Corporation)

30. The Grugq (Independent Network Security Researcher)

TT1 - Structured Network Threat Analysis & Forensics

The weary analyst battles the Internet: port scans are coming at you left and right, worms are spreading like wildfire, servers are compromised and confidential data are lost and stolen. This is a familiar scene, one that could be detected, prevented and and if it has already happened, contained.

This a hands-on class that will teach you on how to detect, analyze, and perform incident response and handling. We will throw at you tons of packet capture files, and we will show you how to analyze them using Open Source tools. When we say analyze, we mean: looking for signs of attacks, determining the source and attack destination, and detecting targeted vulnerabilities. We will also show you how to build, deploy and manage NSM (Network Security Monitoring) architecture.

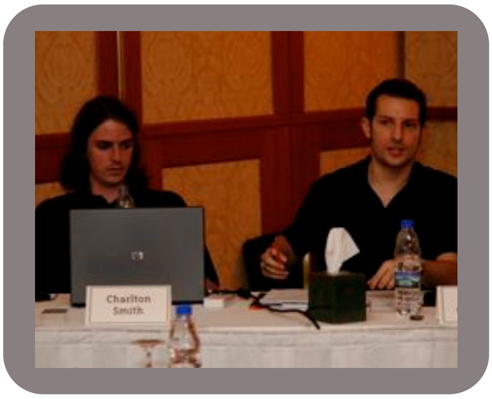
At the end of the two-day session, you should be able to

* Perform structured network traffic and threat analysis
* Build, deploy, and manage NSM architecture
* Collect evidence and perform network and server forensic
* Use Open Source tools for SNT/TA effectively
* Build a defensible network using NSM
* Know WHAT to do when given packet capture files

Whom this training is for

* Security analysts
* System administrators
* Anyone who is interested in building defensible networks
* Anyone who is interested in building NSM architecture

TT2 - Bluetooth, RFID & Wireless Hacking



Wireless networks are continually growing in our modern world and society. This 2 day course aims to demystify wireless network security and inform attendees on how to improve wireless LAN security and Bluetooth security. This will be achieved via theory and practical. Attendees will first obtain detailed theoretical analysis of different wireless security schemas (i.e. Theory), thereafter have hands on experience in how the attacks are performed (i.e. Practical).

Day 1

- Introduction to Wireless Hacking
- Wireless Protocols and Architecture
- Network Mapping and Methodology for securing wireless networks
- Discovery of wireless networks
- Antenna variations
- Wireless hacking tools and attacks
- Defending against wireless hacking

Day 2

- Introduction to Bluetooth hacking techniques
- Bluetooth vulnerabilities overview
- Bluetooth hacking tools and techniques
- Defending against Bluetooth attacks

Full Course Outline available online

TT3 – Web Application Security – Advanced Attack & Defense

Introduction and adaptation of new technologies like Ajax, Rich Internet Applications and Web Services has changed the dimension of Application Hacking. We are witnessing new ways of hacking web based applications and it needs better understanding of technologies to secure applications.

The only constant in this space is change. In this dynamically changing scenario in the era of Web 2.0 it is important to understand new threats that emerge in order to build constructive strategies to protect corporate application assets.

Application layers are evolving and lot of client side attack vectors are on the rise like Ajax based XSS, CSRF, Widget injections, RSS exploits, Mashup manipulations and client side logic exploitations. At the same time various new attack vectors are evolving around SOA by attacking SOAP, XML-RPC and REST. It is time to understand these advanced attack vectors and defense strategies.

The course is designed by the author of "Web Hacking: Attacks and Defense", "Hacking Web Services" and "Web 2.0 Security – Defending Ajax, RIA and SOA" bringing his experience in application security and research as part of curriculum to address new challenges. Application Hacking 2.0 is hands-on class.

The class features real life cases, hands one exercises, new scanning tools and defense mechanisms. Participants would be methodically exposed to various different attack vectors and exploits. In the class instructor will explain new tools like wsScanner, scanweb2.0, AppMap, AppCodeScan etc. for better pen-testing and application audits.

TT4 – The Exploit Laboratory

This workshop shall introduce how buffer overflow vulnerabilities arise in programs and how they get exploited. The workshop will take you deep inside how programs are loaded and execute within memory, how to spot buffer overflow conditions and how exploits get constructed for these overflow conditions. By exposing the inner mechanisms of such exploits, we will understand how to prevent such vulnerabilities from arising.

The workshop will cover analysis of stack overflows, heap overflows and format string vulnerabilities. Examples of vulnerabilities shall be provided on both the Windows as well as the Unix platform. The class is highly hands-on and very lab intensive. The hands-on lab provides real-life examples of programs containing vulnerabilities, and participants are required to analyze and exploit these vulnerabilities.

Who should attend?

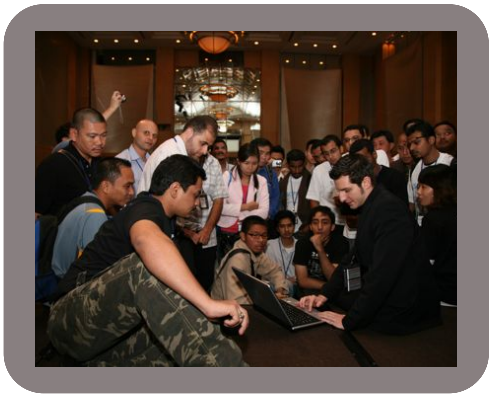
Pen-testers, developers, just about anyone who wants to understand how exploits work.

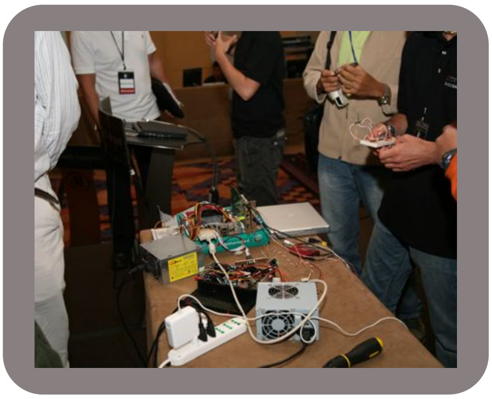
Key learning objectives

Understanding error conditions.
Categories of error conditions - stack overflow, heap overflow, off-by-one, format string bugs, integer overflows (this class will deal only with stack, heap and format string)
Unix process memory map
Win32 process memory map
Writing shellcode
Real life exploit construction
Secure coding practices
Kernel level protection mechanisms

Full Course Outline available online

HITB Labs





These new lab sessions have been added to cater to attendees who would like to gain a deeper understanding through hands on tutorial sessions.

Each session caters for a total of 50 participants with laptops and runs for a total of 120 minutes. The HITB Lab will run over the 2-day conference period (29th and 30th October) with 3 sessions held on each day.

Some of the HITB Labs topics that we have lined up include:

Bluetooth, RFID and Wireless

A hardcore intensive session conducted by members of TOOOL USA and researchers from Telspace Systems, this lab will take attendees through all they need to do to attack some of the popular wireless technologies penetrating our every day lives. Topics covered include breaking 802.11 b/g/n networks, cracking WEP/WPA/WPA2, attacking RFID tags, RFID passports and attacking Bluetooth devices for fun, fame and mayhem.

Advanced Lock Picking and Physical Security Bypass Methods

Conducted by members of TOOOL USA and Marc Weber Tobias, lawyer and physical security specialist for over 10 years. This lab expands on the topics covered within the Lock Picking village. Attendees who have mastered the basic lock picking skills but who hunger for more can learn how to bump and pick their way through some of the higher security locks. Learn also about other physical security bypass methods and how attackers are breaking the locks of today.

Lab Schedule

29th October 2008	30th October 2008
2:15pm - 4:15pm ADVANCED NETWORK FORENSICS LAB	2:15pm - 4:15pm ADVANCED WIRELESS LAB
4:30pm - 6:30pm ADVANCED LOCK PICKING LAB	4:30pm - 6:30pm DETECTING AND REMOVING MALWARE WITH A/V SOFTWARE

CONFERENCE DAY 1 - 29TH OCT 2008

7:30 AM	REGISTRATION
9:00 AM	The Art of Click-Jacking Keynote Address 1: Jeremiah Grossman (Founder, Chief Technology Officer of WhiteHat Security)
10:00 AM	Cyberwar is Bullshit Keynote Address 2: Marcus Ranum (Chief Security Officer, Tenable Network Security)
11:00 AM	COFFEE BREAK

	TRACK 1	TRACK 2	TRACK 3 (HITB LAB)
11:30 AM	PLATINUM SPONSOR	Bluepilling the Xen Hypervisor Alexander Tereshkin (Senior Researcher, Invisible Things Lab)	
12:30 PM	LUNCH BREAK		
1:15 PM	Pass the Hash Toolkit for Windows Hernan Ochoa (Senior Security Consultant, Core Security Technology)	An Effective Methodology to Enable Security Evaluation at RTL Level and Automate Vulnerability Detection in Future Hardware Mary Yeoh (Security Evaluation Lead, Intel Security Center of Excellence [SeCoE])	
2:15 PM	Internet Explorer 8.0 - Trustworthy Engineering & Browsing Vishal Kumar (Senior Lead Security Manager, Microsoft Corporation)	Hacking Internet Kiosks Paul Craig (Principal Security Consultant, Security-Assessment.com	ADVANCED NETWORK FORENSICS LAB Meling Mudin (spoonfork) and Lee Chin Shing (geekool)
3:15 PM	TBA Ero Carrera (Reverse Engineering Automation Engineer, zynamics GmbH)	Full Process Reconstitution from Memory Peter Silberman (Engineer, Mandiant Inc.)	
4:15 PM	COFFEE BREAK		
4:30 PM	MoocherHunting: Real-Time Geo-Location of Moochers, Hackers and Unauthorized WiFi Users Julian Ho (Chief Operating Officer, THINKSecure Pte. Ltd.)	Browser Exploits - A New Model for Browser Security Saumil Shah (Founder/CEO Net-Square Solution)	ADVANCED LOCK PICKING LAB Q (HacDC), Deviant Olam (TOOOL USA) and Eric Michaud (TOOOL USA)
5:30 PM	Mac OS Xploitation Dino Dai Zovi (Independent Network Security Researcher)	Time for a Free Hardware Foundation? Roberto Preatoni (Founder, Zone-H Defacement Mirror and WSLabi)	
6:30 PM	Hacking A Bird In The Sky 2.0 Jim Geovedi and Raditya Iryandi (Security Consultants, Bellua Asia Pacific / HERT)	How the Leopard Hides His Spots - OS X Anti-Forensics Techniques The Grugq (Independent Network Security Researcher)	
7:30 PM	END		

CONFERENCE DAY 2 – 30TH OCT 2008

7:30 AM	REGISTRATION
9:00 AM	Welcome to the owned World Keynote Address 3: Dr. Anton Chuvakin (Chief Research Officer, Log Logic Inc)
10:00 AM	Dissolving an Industry as a Hobby Keynote Address 4: Peter Sunde [brokep] and Fredrik Neij [TiAMO] (Founders of The Pirate Bay - TPB)
11:00 AM	COFFEE BREAK

	TRACK 1	TRACK 2	TRACK 3 (HITB LAB)
11:30 AM	PLATINUM SPONSOR	TBA Petko D. Petkov (Founder, GNUCITIZEN and House of Hackers)	
12:30 PM	LUNCH BREAK		
1:15 PM	Remote Code Execution Through Intel CPU Bugs Kris Kaspersky (Independent Network Security Researcher and Author for XAKEP Magazine)	GOLD SPONSOR	
2:15 PM	iPwning the iPhone Charlie Miller (Principal Analyst, Independent Security Evaluators)	How to Build Your Own Password Cracker with a Disassembler and a Little VM Magic Matthew Geiger (Forensics Specialist, CERT US)	ADVANCED 802.11, RFID & BLUETOOTH LAB Q (HacDC) and King Tuna (Independent Network Security Consultant)
3:15 PM	Next Generation Reverse Shell AR (Independent Network Security Researcher, Securebits)	Pushing the Camel Through the Eye of a Needle Haroon Meer (Technical Director, Sensepost)	
4:15 PM	COFFEE BREAK		
4:30 PM	Decompilers and Beyond Ilfak Guilfanov (Founder/CEO Hex-Rays SA and Creator of IDA Pro)	Top 10 Web 2.0 Attacks Shreeraj Shah (Founder, BlueInfy)	DETECTING AND REMOVING MALWARE WITHOUT ANTI VIRUS SOFTWARE Tim Ching Meng (Security Consultant, Cable & Wireless)
5:30 PM	Cracking into Embedded Devices and Beyond! Adrian 'pagvac' Pastor (ProCheckUp Ltd. / GNUCITIZEN)	Suddenly Psychic - Knowing Everything about Everyone Nitesh Dhanjani (Senior Manager, Ernst & Young) with Akshay Agrawal (Practice Manager, Microsoft Information Security ACE Team)	
6:30 PM	CTF PRIZE GIVING + CHARITY AUCTION IN AID OF PR4A (CHILDREN WITH AUTISM)		
7:30 PM	END		

Capture The Flag (CTF)

The objectives of the game is for teams (maximum of 3 participants per team) to gain as many points as possible by defending their servers, and attacking other teams' servers. Teams will be given identical pre-configured vmware image of a Gentoo Linux installation. There will be custom services running on the server. This services contain vulnerabilities, such as buffer overflows, format string and so on. The teams' objective is to analyze the services, find vulnerabilities and write exploits. As such, the following skills are needed:

- Reverse engineering
- Debugging
- Binary analysis
- Exploit writing

The ability to write a working exploit will enable the team to attack other servers, retrieving the flag associated with each service running on the server and thus scoring an offensive point. The ability to keep the services running will enable the teams to score a defensive point.

HITBSecConf2007 - MALAYSIA
3rd - 6th September 2007 - Kuala Lumpur
Deep Knowledge Security Conference
Capture The Flag
"Live Hacking"
Competition
CTF & CTF Prize Sponsor

Scoring

Offensive Points: Gained by hacking into other team's server and retrieving their flags.
Defensive Points: Gained by keeping your server's services running.

In order to score an offensive point, all that a team needs to do is hack into other team's server, retrieve the flag, and submit it to the score server. In order to get defensive score, teams must keep their services running and accessible to the ScoreBot. The ScoreBot will periodically connect to the team's server and perform either two actions: set new flags on the services and/or retrieve flags from the services. Failure of the ScoreBot to complete either of these 2 actions when it connects will result in point deductions.

More points are given for offensive attacks as opposed to defensive score. Defensive scores are the same for all services, while offensive scores vary depending on the complexity level of the exploit needed to hack the service. During the course of the game, the score server will randomly set new flags on each teams' services. This means that a service can have as many as 10 unique flags throughout the game - so if a particular team has an exploit against this service, they can get 10 times the points multiplied by the number of teams.

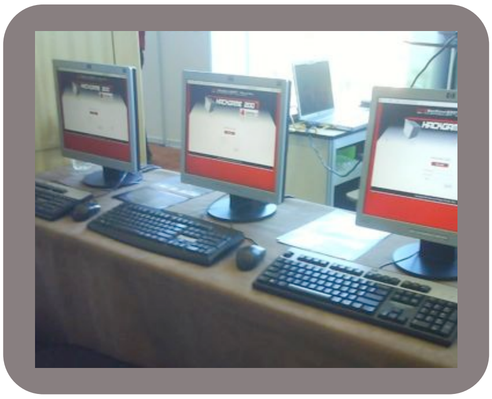
To register, please send an email with the following details to ctfinfo@hackinthebox.org

1.) Team Name

2.) Team Leaders Name + Email Address

3.) Team Members Names + Email Addresses

Open Hack



For the second time ever in a HITBSecConf we will be organizing an Open-Hack competition with a slight twist inspired by the Pwn-to-own contest run by the guys at CanSecWest.

The purpose of an Open Hack is to uncover new and previously unknown software vulnerabilities in operating systems and software. This year's Open Hack will involve a fully patched Macbook Air with a default install of Leopard with all patches applied and the firewall set to default settings (possibly running os X 10.5.5 [by the time October rolls around]).. Similar to the contest in CanSecWest, the machine will be accessible via Wifi and Wired Ethernet connections. Be the first to hack in and you walk away with a brand new machine and possibly USD5000 in prize money!

ANY VULNERABILITIES DISCOVERED MUST BE HANDLED USING <u>RESPONSIBLE DISCLOSURE</u> METHODS.

Lock Picking Village (LPV)

Set up and run by members from the The Open Organization of Lockpickers (TOOOL USA), attendees to this year's event will yet again get a chance to try their hands at bumping and other physical security bypass methods.

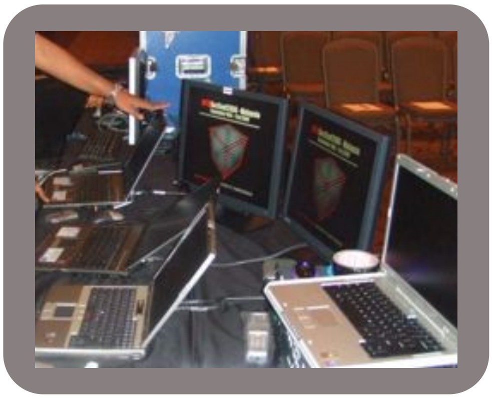
It has always been customary for TOOOL-sponsored physical security sessions to incorporate some degree of audience interaction and hands-on training. Sometimes this has taken the form of publicly-submitted locks being given on the spot security analysis, other times members of the general public with no lockpicking experience have been invited to attempt a bypass in order to demonstrate its ease. Overall, however, the most rewarding and educational form of audience participation has tended to be occasions when a wide array of hardware is put forth and individuals can attempt use of the very tools and techniques demonstrated in the security session they just witnessed.

When sample locks and picks are made available, the public inevitably finds most equipment astonishingly easy to compromise and comes away with a better understanding of how to protect themselves. It is in this spirit of educational fun that The Open Organization of Lockpickers has begun to organize "Lockpick Villages" at security events around the world. Attendees of technology conferences can learn about physical security in a training session, then can immediately attempt to apply what they have witnessed… often to great effect.

Picks, wrenches, and plenty of guidance and advice are made available to the public in the Lockpick Village. All who participate are guaranteed to have a good time and to come away with a healthier and more in-depth understanding of physical security hardware. Please feel free to bring a lock that you trust and see if it stands up to our battery of tests.

> Attendees who have already tried their hands at lock-picking at last year's HITBSecConf in Malaysia are encouraged to sit in for the Advanced Lock Picking and Physical Security Bypass Lab.

Wireless Village (Bluetooth, RFID, WiFi)



This new addition to the conference line up follows the similar principal of the Lock Picking Village in allowing attendees a better understanding of complex security issues through a hands on learning process.

This wireless village will be run by both members of Telspace Systems, one of South Africa's largest network security companies and the members of TOOOL USA who have also conducted similar Wireless Villages in DEFCON in the United States.

Attendees will get a chance to play around with Wireless 802.11 a/b/g/n scanners, RFID readers, Bluetooth sniper rifles and other nifty gadgets. If you think the security of your devices is assured because you're using WPA2 or that your Bluetooth is set to 'invisible', it's time to think again. Attendees will be exposed to the following topics:

<u>802.11 Hacking Tools and Techniques</u>

Aircrack and Aero suite of tools
Airsnort
WEP hacking cracking
WPA, WPA2 hacking techniques

<u>Bluetooth Hacking Tools and Techniques</u>

BTscan , Bluestumbler , Bluescan , BT Browser
Bluesnarf
Bluebug
Bloover II
Carwhisperer
Blueprinting (SDP tool)

Price List

27th & 28th October 2008

Item	Trainer	Duration	Price Early Bird / Normal & Credit Card
TECHNICAL TRAINING 1 Structured Network Threat Analysis & Forensics	Meling Mudin (spoonfork) and Lee Chin Shing (geekool)	2 Days	MYR 3299 / 3899 (USD 1049 / USD 1249)
TECHNICAL TRAINING 2 Bluetooth, RFID & Wireless Hacking	Dino Covotsos (Telspace Systems), Charlton Smith (Telspace Systems) & Q (TOOOL USA)	2 Days	MYR 3299 / 3899 (USD 1049 / USD 1249)
TECHNICAL TRAINING 3 Web Application Security - Advanced Attack and Defense	Shreeraj Shah (Blueinfy)	2 Days	MYR 3299 / 3899 (USD 1049 / USD 1249)
TECHNICAL TRAINING 4 The Exploit Laboratory	Saumil Shah (Net-Square) & SK Chong (Scan Associates)	2 Days	MYR 3299 / 3899 (USD 1049 / USD 1249)

29th & 30th October 2008

Item	Duration	Price
Triple Track Security Conference featuring new HITB Lab	2 Days	Early Bird: MYR 499 (USD 159) Normal Price: MYR 899 (USD 289) Walk-in: MYR 1099 (USD349) Students: MYR 250
Capture The Flag 'Live Hacking' Competition	2 Days	MYR 899 / USD 289 (per team of 3)
Open Hack Competition	2 Days	FREE FOR REGISTERED CONFERENCE DELEGATES
Lock Picking Village	2 Days	FREE AND OPEN TO PUBLIC
Wireless Village (Bluetooth, RFID, 802.11x)	2 Days	FREE AND OPEN TO PUBLIC
Industry Showcase & Exhibition	2 Days	FREE AND OPEN TO PUBLIC

REGISTER ONLINE NOW!

http://conference.hackinthebox.org/hitbsecconf2008kl/register/
http://conference.hitb.org/hitbsecconf2008kl/register/