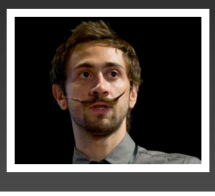
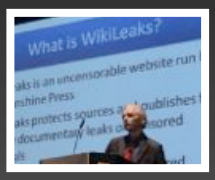
HITBSECCONF2010 MALAYSIA

OCTOBER 11TH - 14TH 2010
CROWNE PLAZA MUTIARA
KUALA LUMPUR

The 8th Edition of Asia's Premier Deep Knowledge Network Security Conference




OCTOBER 4TH - 5TH

HITB TRAINING 1 - Exploit Lab 5.0

OCTOBER 6TH - 7TH

HITB TRAINING 2 - Exploit Lab: Black Belt

OCTOBER 11TH - 12TH

TECH TRAINING 1 - Web 2.0 Hacking - Advanced Attack & Defense

TECH TRAINING 2 - SAP Security In-Depth

TECH TRAINING 3 - Hunting Web Attackers

TECH TRAINING 4 - Malcode & Threat Analysis

OCTOBER 13TH - 14TH

- **Quad Track Security Conference**
- **HITB Labs**
- **HITB SIGINT**
- **Capture The Flag 'Weapons of Mass Destruction' 2.0**
- **Hard Hack Village (Arduino)**
- **Lock Picking Village (now with safe cracking!)**

REGISTER ONLINE
(ONLY MYR899)

HTTP://CONFERENCE.HACKINTHEBOX.ORG/HITBSECCONF2010KUL/

Keynote Speakers - 13th October

Chris 'Weld Pond' Wysopal (Founder / CTO, Veracode)

Chris Wysopal (aka Weld Pond), Veracode's CTO and Co-Founder, is responsible for the company's software security analysis capabilities. In 2008 he was named one of InfoWorld's Top 25 CTO's and one of the 100 most influential people in IT by eWeek. Chris was one of the first vulnerability researchers for web applications and Windows, publishing advisories in Lotus Domino, Cold Fusion, and Windows back in the mid 1990's. He was one of the original members of L0pht Heavy Industries, and co-author of L0phtCrack.

Paul Vixie (President, Internet Systems Consortium)

Paul Vixie holds the record for "most CERT advisories due to a single author" which came primarily from his years hacking on BIND4 and BIND8. Later on he cut off the oxygen supply to his brain by wearing a necktie for AboveNet, MFN, and PAIX. At the moment he is President at ISC where his primary duty is to sign paychecks for the people who bring you BIND9 and F.ROOT-SERVERS.NET. He is the current Chairman of ARIN, and is also an occasional critic of just about everything.

Special Keynote Panel - 14th October

"The Future of Mobile Malware & Cloud Computing Security"

Mikko Hypponen (Chief Research Officer, F-Secure)

MODERATOR

Paul Ducklin (Head of Technology, Sophos Asia Pacific)

Denis Maslennikov (Head, Mobile Research Group, Kaspersky Labs)

Dr. Jose Nazario (Senior Manager, Security Research, Arbor Networks)

Dr. Dinesh Nair

Listen and interact with leading experts in the field of mobile malware and cloud computing as they discuss the current and future threats facing cloud computing deployments and how malware is already evolving to not only make use of the cloud but also harness the power of your mobile devices!

HITB TRAINING 1 - EXPLOIT LAB 5.0

The Exploit Laboratory features popular third party applications and products as candidates for vulnerability analysis and exploitation, rather than building up on carefully simulated lab exercises. Most of the class time is spent working on lab exercises and examples. Lab examples and exercises used in this class cover both the Unix (Linux) and Microsoft Windows platforms, illustrating various error conditions such as stack overflows, heap overflows and format string bugs. The latter part of the class focuses on topics such as advanced "one-way" shellcode, multi-stage payloads, integrating your own exploits into frameworks such as Metasploit, bypassing protection mechanisms, etc.

All this – delivered in a down-to-earth, learn-by-example methodology, by trainers who have been teaching advanced topics in computer security for over 9 years. This class is updated from the 2009 edition, featuring new content on heap overflows, abusing exception handlers and more! The class also features Mac OS X exploitation techniques and does NOT require knowledge of assembly language. A few concepts and a sharp mind is all you need.

HITB TRAINING 2 - EXPLOIT LAB: BLACK BELT

The Exploit Laboratory Black Belt is a new and advanced class continuing from where The Exploit Laboratory left off. This class is for those curious to dig deeper into the art and craft of software exploitation. The Black Belt class begins with a quick overview of concepts covered in The Exploit Laboratory, namely stack overflows, abusing exception handlers, heap overflows, memory overwrites, and other core concepts. The class then moves to deeper vulnerabilities such as integer overflows and format string bugs. We shall then focus on topics which involve breaking exploit prevention techniques like non executable stack, DEP, ASLR, etc. The Black Belt class also features an introduction to kernel exploitation, post exploitation techniques like return to libc, advanced heap spraying, return oriented programming and JIT spraying.

HITB TRAINING 1 - WEB 2.0 HACKING - ADVANCED ATTACK AND DEFENSE

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.

HITB TRAINING 2 - SAP SECURITY IN-DEPTH

This training will help you understand the involved threats and risks facing SAP implementations and how to mitigate them. You will review the whole picture, from the security of the Environment and the SAP application-level gateways (SAProuter, Webdispatcher), through the assessment and hardening of the Operating Systems and Databases and their interaction with the SAP systems up to the security of the SAP Application Layer: Authentication, User security, Password Policies, Authorization subsystem, Interface Security, Component Security, Auditing, Monitoring and more!

HITB TRAINING 3 - HUNTING WEB ATTACKERS

The goal of this innovative training is to help white-hats improve their skills in the on-going cyber war against web attackers. Attendees will learn how to detect web intruders, and then how to strike-back so that they can better identify the assailants or neutralize their actions. This technical hunt will be based on hands-on exercises launched with the help of the instructor on a dedicated LAN. Students will have the opportunity to apply those special techniques in a real world environment.

HITB TRAINING 4 - MALCODE & THREAT ANALYSIS

This course is designed for information security professionals who are tasked with protecting networks and businesses from a broad range of threats. Students will learn how to identify new threats to their own networks and the internet at large, and how to protect against them. Rather than focusing on reverse engineering and malcode dissection, we will instead focus on a simple approach that many people can use to quickly gather specific, usable information about threats. This course is not designed to be tool specific but rather it discusses a broad approach and multiple techniques that can be used quickly to assess new threats and determine how to respond to them.

ALL TRAININGS ARE HRDF CLAIMABLE UNDER SBL KHAS

Hack In The Box (M) Sdn. Bhd.
Suite 26.3, Level 26, Menara IMC,
No. 8 Jalan Sultan Ismail, 50250 Kuala Lumpur

Tel: +603-20394724 **Fax:** +603-20318359
Email: conferenceinfo@hackinthebox.org

HITBSECCONF2010 MALAYSIA

The 8th Edition of Asia's Premier Deep Knowledge Network Security Conference