Conference Kit

Version 2.0

*** Over 30 Network Security Specialists and Researchers**
*** 7-tracks of Hands on Technical Training Sessions**
*** Network Assessment and Latest Attack Methods**
*** Fundamental Defense Methodologies**
*** Close Look At the Latest Computer and Network Security Technologies**
*** Advanced Computer and Network Security Topics**
*** 2-Days of Deep Knowledge Papers and Presentations**
*** Live Hacking Competition (CTF)**

Organised by:

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

Email: cbelinda@hackinthebox.org **or** dhillon@hackinthebox.org

Overview

The main aim of the HITBSecConf conference series is to enable the dissemination, discussion and sharing of deep knowledge network security information. Featuring presentations by respected members of both the mainstream network security arena as well as the underground or black hat community, HITBSecConf2006 - Malaysia will see over 30 of the world's leading network security specialists down to present their research and findings.

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.

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 Detail

Date: **18th – 19th September 2006**
Item: 7-Tracks Hands-On Technical Training Sessions
Time: 9am to 6pm

Date: **20th – 21st September 2006**
Item: 2-Tracks Security Conference and Exhibition
Time: 9am to 6pm

Date: **20th – 21st September 2006**
Item: Capture The Flag and Open-Hack Competition
Time: 9am to 5pm

Venue: The Westin Kuala Lumpur
199 Jalan Bukit Bintang
55100 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

Bruce Schneier - Chief Technical Officer, Counterpane Internet Security, Inc.
http://www.counterpane.com/crypto-gram.html

Presentation Title: Schneier on Security
Presentation Details:

Always interesting and entertaining, Bruce Schneier will talk about current topics in security, economics, and society.

About Bruce Schneier:

Internationally-renowned security technologist and author Bruce Schneier is both a Founder and the Chief Technical Officer of Counterpane Internet Security, Inc. the world's leading protector of networked information - the inventor of outsourced security monitoring and the foremost authority on effective mitigation of emerging IT threats.

Bruce is responsible for maintaining Counterpane's technical lead in world-class information security technology and its practical and effective implementation. Bruce's security experience makes him uniquely qualified to shape the direction of the company's research endeavors, as well as to act as a spokesperson to the business community on security issues and solutions.

Bruce is the author of eight books, including his current best seller, Beyond Fear: Thinking Sensibly about Security in an Uncertain World, which tackles the problems of security from the small to the large: personal safety, crime, corporate security, national security. Secrets & Lies: Digital Security in a Networked World, which was published in October 2000, has sold 150,000 copies. One of his earlier books, Applied Cryptography, now in its second edition, is the seminal work in its field and has sold over 200,000 copies and has been translated into five languages. He writes the free email newsletter Crypto-Gram, which has over 120,000 readers. He has presented papers at many international conferences, and he is a frequent writer, contributing editor, and lecturer on the topics of cryptography, computer security, and privacy.

Bruce designed the popular Blowfish and Twofish encryption algorithms, the latter a finalist for the new Federal Advanced Encryption Standard (AES). Bruce served on the board of directors of the International Association for Cryptologic Research, and is an Advisory Board member for the Electronic Privacy Information Center. Bruce holds an MS degree in computer science from American University and a BS degree in physics from the University of Rochester.

Mark Curphey - Vice President of Consulting, Foundstone

Presentation Title: What application security tools vendors don't want you to know and holes they will never find!

Presentation Abstract:

Software and application security is a hard nut to crack. Traditional network and operating system assessment and protection tools can be taught to look for repeatable conditions with reasonable results. However (and despite heavy marketing suggesting other wise) application protection and assessment tools suffer from a significant different order of problem. In this talk John Viega and Mark Curphey will systematically discuss and demonstrate the limitations of automated protection and assessment tools using live working examples. The talk will focus on code review tools, web application scanners and web application firewalls.

About Mark Curphey:

Mark Curphey is the Vice President of Consulting at Foundstone and responsible for the global services team. Recognized for his work in the software security field, Mark was the Director of Information Security at Charles Schwab (a large US based financial services company) where he was responsible for creating and managing the global application security program when software security wasn't yet on most companies radars. Mark founded OWASP, the Open Web Application Security Project that has become a well thought of reference site for developers and system architects and recommended reading by the US Federal Trade Committee. He has a Masters Degree in Information Security from the renowned Royal Holloway, University of London where he specialized in advanced cryptography. Mark is a Microsoft MVP for developer security.

In his words "I am passionate about software security; and I am passionate about preventing this industry spinning out of control with marketing and hype. This will definitely not be your average presentation with bullet pointed slides and the same old message regurgitated! Come prepared".

John Viega – Chief Security Architect, McAfee Inc.

Presentation Title: What application security tools vendors don't want you to know and holes they will never find!

About John Viega:

John is the co-author of three books on application security, Building Secure Software (Addison Wesley, 2001), Network Security with OpenSSL (O'Reilly, 2002) and the Secure Programming Cookbook (O'Reilly, 2003). He also built the CLASP application security process, which is available on-line. John's research areas have included application security, cryptography, programming languages and usability. He co-developed GCM, a mode of operation for block ciphers such as AES that has been incorporated into IPSec and the 802.1AE draft document, and is currently being standardized by NIST. Despite being cautious about embracing the open source security theory, John has been involved in many open source projects. He was the original author of the Mailman mailing list manager, and has been author or co-author of many other free projects, including RATS, SafeStr, XXL and ITS4.

Note: John will be presenting this keynote with Mark Curphey (Vice President, Foundstone Professional Services - A division of McAfee Inc.)

Our distinguished panel of speakers

1.) **Anthony Zboralski** (Founder, HERT & PT. Bellua Asia Pacific)
2.) **Arnaud Ebalard** (Security Research Engineer, EADS Corporate Research Center)
3.) **Carlos Sarraute** (Senior Researcher, Core Security Technologies)
4.) **Dave Tamasi** (Lead Program Manager, Secure Windows Initiative Group, Microsoft Corporation)
5.) **Douglas MacIver** (Penetration Engineer, Microsoft Penetration Team, Microsoft Corporation)
6.) **Fabio Ghioni** (Independent Advisor to various MNCs and Government organizations)
7.) **Fabrice Marie** (Manager, FMA-RMS Singapore/Malaysia)
8.) **Fyodor Yarochkin** (Co-Author, XProbe)
9.) **Javier Burroni** (Senior Developer of Core Impact, Core Security Technologies)
10.) **Jim Geovedi** (Member of HERT & Security Consultant, PT Bellua Asia Pacific)
11.) **Joanna Rutkowska** (Senior Security Researcher, COSEINC)
12.) **Lisa Thalheim** (Independent Network Security Consultant)
13.) **Marc Schönefeld** (Independent Network Security Consultant)
14.) **Meder Kydyraliev** (Co-Author, XProbe)
15.) **Michael Davis** (Member, The Honeynet Project.)
16.) **Nguyen Anh Quynh** (PhD student of Keio university, Japan)
17.) **Nish Bhalla** (VP Consulting Solutions, Security Compass)
18.) **Paul Boehm** (Founding member of TESO Security, Security Consultant, SEC Consult)
19.) **Philippe Biondi** (Research Engineer at EADS Corporate Research Center)
20.) **Raditya Iryandi** (Information Security Consultant, Bellua Asia Pacific)
21.) **Raoul Chiesa** (Board of Directors Member@ Mediaservice.net ISECOM Group & TSTF)
22.) **Roberto Preatoni** (Founder, Zone-H Defacement Mirror)
23.) **Rohyt Belani** (Director, Mandiant)
24.) **Saumil Shah** (Director, Net-Square)
25.) **Shreeraj Shah** (Director, Net-Square)
26.) **Dr. Stefania Ducci** (Criminologic Researcher, United Nations Interregional Crime and Justice Research Institute, UNCRI)
27.) **Thorsten Holz** (HoneyNet Project Germany, Independent Network Security Researcher)
28.) **The Grugq** (Independent Network Security Researcher)
29.) **Van Hauser** (Founder, THC.org)
30.) **Wes Brown** (Founder, Ephemeral Security)
31.) **Yen Ming Chen** (Senior Managing Consultant, Foundstone - A Division of McAfee Inc.)

Training Sessions

HANDS ON TECHNICAL TRAINING SESSIONS
18TH AND 19TH SEPTEMBER 2006

TECHNICAL TRAINING TRACK 1:
ADVANCE WEB APPLICATION & SERVICES HACKING

Trainer: Shreeraj Shah, *Director* Net-Square Solutions

Outline:

A growing concern has been Web application security – Web and application servers are the target of regular attacks by attackers that exploit security loopholes or vulnerabilities in code or design. Adding to this concern are next generation applications; applications that are on the fast track and more appealing to the user, utilizing dynamic AJAX scripts, Web services and newer Web technologies to create intuitive and easy interfaces. The only constant in this space is change. In this dynamically changing scenario it is important to understand new threats that emerge in order to build constructive strategies to protect corporate assets.

This two–day workshop will expose students to both aspects of security: attacks and defense. To think of newer Web applications without Web services is a big mistake. Sooner or later existing applications will be forced to migrate to the new framework. This workshop includes several cases, demonstrations and hands-on exercises with newer tools to give you a headstart over others in the field.

The following topics will be covered in-depth during these sessions:

- Web Security Fundamentals and Principles, Trends and Opportunities
- Methods, Components and Protocols (HTTP, HTTPS and SOAP)
- Web application assessment methods – Blackbox and Whitebox approaches
- Web application Deployment and Security Deployment issues
- Web application Footprinting, Discovery and Profiling
- Search engines and their role in Web Application hacking (Google & MSN)
- Web application attack vectors and assets-to-attacks-mapping
- XML-based attacks
- SQL, LDAP, XPATH injection techniques
- XSS, Cross-site cookie spoiling and AJAX-hacking
- Web services frameworks
- Web services footprinting, discovery and profiling
- Web services attacks
- Web application firewall – Build and Deploy
- Web security controls and best practices
- Secure coding and reverse engineering methods
- Tools and Techniques
- Hands-on challenges and labs

TECHNICAL TRAINING TRACK 2:
ATTACKING & DEFENDING NETWORKS (ADVANCED LINUX EDITION)

Trainer: Nish Bhalla, *VP Consulting Solutions,* Security Compass

Outline:

The purpose of this course is to provide advanced tech leads, testers, administrators, network administrators and all other participants detailed security techniques and knowledge as applied to Network security and Host Security.

It is focused towards helping users understand how to find and write basic stack based exploits. Participants will also learn how to take advantages of vulnerabilities that might exists in an environment and use backchannels to connect back into a network.

Hands-on lab exercises reinforce the course material in a real world environment.

TECHNICAL TRAINING TRACK 3:
THE EXPLOIT LABORATORY

Trainer: Saumil Shah, Director Net-Square & SK Chong (Scan Associates Malaysia)

Outline:

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 intesive. The hands-on lab provides real-life examples of programs containing vulnerabilities, and participants are required to analyse and exploit these vulnerabilities.

TECHNICAL TRAINING TRACK 4:
TACTICAL VOIP: APPLIED VOIPHREAKING

Trainer: The Grugq, Independent Network Security Consultant

Outline:

This course addresses exploiting VoIP — from end user devices through carrier grade servers — including protocol level attacks, application bugs and common dangerous deployment mistakes. The course provides deep coverage of a broad spectrum of VoIP relevant security threats:

* Hijacking
* Sniffing
* Injecting
* Interdicting
* SPITing

Starting with a bits and bytes analysis of VoIP on the wire and progessing to exploit development, you will constantly be increasing your VoIP security skills. In addition to a thorough theoretical understanding of VoIP security issues, you will directly apply your knowlege in practical VoIP workshops. Each workshop addresses an aspect of VoIP security, further deepening your understanding and completing your skill set.

You will leave with a solid grounding in VoIP security assessment, including methodology, techniques and an advanced toolset to facilitate security auditing. You will also have comprehensive knowlege of the major VoIP protocolsuites, covering signalling, media and PSTN integration. Additionally, you will have exposure to, and training with, the most powerful and flexible VoIP security assessment tool suite available.

The VoIPhreaking tool suite, based on the VoIPy library, provides a flexible framework for VoIP security analysis. Coded by the grugq, this tool suite is specifically developed for VoIP hacking. After learning how to utilize the suite, you will also be able to extend the core suite to develop new and unique exploits and tests specific to your environment or engagement.

TECHNICAL TRAINING TRACK 5:
WAR DRIVING .GOV

Trainers: Anthony Zboralski, Founder of HERT & PT. Bellua Asia Pacific
Jim Geovedi, Security Consultant PT Bellua Asia Pacific & Member of HERT.

Outline:

The adoption and proliferation of wireless networks have reached emerging markets and Asia is not an exception. As part of their economic expansion, Asian countries have invested heavily in ICT and embraced wireless technology, both as a force-multiplier and to address cost constraints, in delivering "last-mile" solutions to business users and to provide the ever-growing number of mobile users with convenient access to internet. However, this growth in the use of wireless networks should ideally be accompanied by a suitable understanding of how such networks must be implemented to ensure security issues are addressed appropriately. Widely documented vulnerabilities in earlier versions of wireless security frameworks have rendered many of the implementation unusable and many efforts to upgrade the security environment were ineffective due to resource constraints and general ignorance on the part of the end-users.

By default, most wireless networks are insecure and present a number of threats:

- Loss of Confidentiality (atm transactions, emails, confidential documents, etc.)
- Denial of Service, business interruption
- Theft of Service
- Internal networks may be exposed to outsiders and hackers may propagate via wireless to your network, partners and clients
- Corporate networks could also be used to launch stealth attacks against other targets or to transit spam and other malicious data

If new converts and adopters of wireless technology are putting their faith blindly in product sales pitch, they are at risk from the exploitation of the many possible vulnerabilities and in turn, put the long-term continuity of their entire commercial endeavour at the hands of the would-be attackers.

The purpose of this course is to give a full understanding of what wireless networks are, how they work, how they are found and exploited, and how they can be secured.

This will not be your ordinary run-of-the-mill classroom type training class but will instead see attendees being taken on a war driving session in a fully airconditioned coach around the government areas of Putrajaya and Cyberjaya.

The students will learn how to attack wireless networks and how to secure them from both management and technical perspectives. There will be a discussion and case studies on actual wireless security penetration test.

THIS TRAINING IS FOR MALAYSIAN LAW ENFORCEMENT AND GOVERNMENT OFFICIALS ONLY

TECHNICAL TRAINING TRACK 6:
STRUCTURED NETWORK THREAT ANALYSIS AND FORENSICS

Trainers: Meling Mudin (spoonfork) & Lee Chin Sheng (geekool)
Outline:

The weary analyst battles the Internet: portscans 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 targetted 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

— Prerequisites

* Intermediate to advanced knowledge of TCP/IP
* Knowledge of Unix and Windows system

TECHNICAL TRAINING TRACK 7:
YIN AND YANG OF JAVA SECURITY PROGRAMMING

Trainer: Marc Schönefeld
Outline:

Opposed to the legends most white papers tell software written in Java is not secure by default. This course will provide the participants with the awareness to threats for java based software. It focuses on the current java (1.4.x , Tiger and Mustang releases) code based security features which are used to protect typical java application patterns (J2EE, Desktop Java, Applet, Servlets).

Secure Java Coding always starts from Sun's secure programming guidelines which are presented by associating attack types and possibilities for refactoring to harden the system. Executed java classes are based on bytecode, therefore knowledge of Java bytecode is essential to understand and extend java static code analysis tools like BCEL and findbugs.

Other important terms in java code-based security are "protection domains" and "permission collections". To reverse engineer protection domains an approach to extend the Java securitymanager is presented. A framework is presented that allows defining custom and complete permission sets when deploying java applications.

After hardening the JDK itself the java security engineer is concerned with raising the protection level of open source java middlweware components like Web servers (Jetty, Tomcat) or databases (cloudscape, pointbase).

Prerequisites:
A laptop capable of compiling java code (preinstalled Sun JDK 1.4.2_x and IBM Eclipse IDE 3.0.x).

The student should have an understanding of most of the following concepts and technologies:

* Knowledge of basic Java programming tools (java, javac, javah).
* Basic to advanced Java and java bytecode programming knowledge as well as the core Java API is beneficial for understanding the key concepts
* Knowledge of basic security concepts like least privilege and security models
* Knowledge of common C based software threats is helpful for the JNI part

Conference Agenda

DAY 1
20TH SEPTEMBER 2006

07.30	**Registration**
08.50	**Welcome Address:** **Datuk Dr. Halim bin Shafie** (Chairman, Malaysian Communications & Multimedia Commission, MCMC)
09.00	**Keynote Address: Schneier on Security** **Bruce Schneier** (Chief Technology Officer, Counterpane Internet Security)
10.00	**Dave Tamasi** Security Engineering in Windows Vista
11:00	**Refreshment Break**

	TRACK I	**TRACK II**
11:30	**Thorsten Holz** Playing with Botnets for Fun and Profit	**Paul Boehm** Taming Bugs: The Art and Science of Writing Secure Code
12:30	**Networking Luncheon**	
13:15	**Van Hauser** Attacking the IPv6 Protocol Suite	**Fabrice Marie** Application Intrusion Prevention Systems: A new approach to protecting your data
14:15	**Saumil Shah** Writing Metasploit Plugins - From Vulnerability to Exploit	**RESERVED**
15:15	**The Grugq** VoIPhreaking: SIPhallis Unveiled	**Michael Davis** Client Honeypots - Its not only the network
16:15	**Refreshment Break**	
16:30	**Shreeraj Shah** WEB 2.0 Hacking – Attack & Defense	**Yen Ming Chen** Triple Play; Triple Threats? IPTV Security
17:30	**Marc Schonefeld** Pentesting Java/J2EE, discovering remote holes	**Lisa Thalheim** Visualization of Source Code for Auditing
18:30	**End of Day One**	

DAY 2
21ST SEPTEMBER 2006

08.00	**Registration**
09.00	**Keynote Address: What application security tools vendors don't want you to know and holes they will never find!** **Mark Curphey** (VP, Foundstone Professional Services - a division of McAfee Inc.) with **John Viega** (Chief Security Architect, McAfee Inc.)
10:00	**Refreshment Break**

	TRACK I	TRACK II
10:30	**Philippe Biondi & Arnaud Ebalard** Scapy and IPv6 networking	**Nish Bhalla** Finding Secrets in ISAPI
11:30	**Joanna Rutkowska** Subverting Vista Kernel for Fun and Profit	**Raoul Chiesa & Dr. Stefania Ducci** A new approach to Cybercrime: The Hacker's Criminal Profiling Project (HCPP)
12:30	**Networking Luncheon**	
13:15	**Douglas MacIver** Pen Testing Windows Vista BitLocker Drive Encryption from the Inside	**Roberto Preatoni & Fabio Ghioni** The Biggest Brother
14:15	**Nguyen Anh Quynh** Towards an Invisible Honeypot Monitoring Tool	**Jim Geovedi & Raditya Iryandi** Hacking a Bird in The Sky: Hijacking VSAT Connections
15:15	**Rohyt Belani** Smashing the stack for profit - period	**Carlos Sarraute & Javier Burroni** Using Neural Networks and Statistical Machinery to Improve Remote OS Detection
16:15	**Refreshment Break**	
16:30	**Wes Brown** MOSREF: Using Cryptography and Injectable Virtual Machines in Security	**RESERVED**
17:30	**Anthony Zboralski** TBA	**Fyodor Yarochkin & Meder Kydyraliev** Yet Another Web Application Testing Toolkit (YAWATT)
18:30	**End of Day Two**	
20:30 onwards	**HITBSECCONF2006 POST CONFERENCE PARTY SPONSORED BY MICROSOFT CORP.**	

The Speakers Profiles

1.) **Anthony Zboralski** (Founder, HERT & PT. Bellua Asia Pacific)

Anthony is the founder and CTO of Bellua Asia Pacific and the co-founder of the Hacker Emergency Response Team (HERT). He has more than ten years of progressive information security experience that include performing penetration testing, assessments, audit, computer forensics and other related services for some of the largest Asian banks and a dozen European-based Fortune 500 companies. Anthony was an invited speaker at HITB 2005, Cisco Security Summit 2005/2003, Apconex 2005, Syscan'05/04, Pakcon 2004, Info War Con Bruxelles 1996, Sicoval 1997, Infonord 1998… He's a certified ISO27001/BS7799 ISMS Auditor.

2.) **Arnaud Ebalard** (Security Research Engineer, EADS Corporate Research Center)

Arnaud EBALARD is a young security research engineer in EADS Corporate Research Center. He works on network security related topics. His current research fields cover IPv6 and Mobility (MIPv6, Mesh Networks, etc) and also PKI and VPN. After some work on Sebek *BSD port, he now takes part in Scapy IPv6 extensions development (http://namabiiru.hongo.wide.ad.jp/scapy6/).

3.) **Carlos Sarraute** (Senior Researcher, Core Security Technologies)

Carlos Sarraute has studied Mathematics at the University of Buenos Aires. He has been working since 2000 in CoreLabs, the research laboratory of Core Security Technologies. His areas of research are security vulnerabilities, attack planning and modeling, security events visualization, secure triggers, protocol design flaws (MySQL authentication, SSH timing analysis) and cryptoanalysis. He has given talks and courses about information security and cryptography in several universities in Argentina.

4.) **Dave Tamasi** (Lead Security Program Manager, Secure Windows Initiative Group, Microsoft Corporation)

Dave Tamasi, lead security program manager in the Secure Windows Initiative (SWI) group, has been with Microsoft Corporation since 1997. In that capacity, he works to secure operating system releases by driving security design and engineering best practices into the Windows organization. Most recently, he managed the Windows Vista penetration test, arguably one of the largest engagements of its kind in history.

5.) **Douglas MacIver** (Penetration Engineer, Microsoft Penetration Team, Microsoft Corporation)

Douglas MacIver joined Microsoft in 2004 as a penetration engineer, hell-bent on helping to build data privacy tools for the citizens of world. He has worked on security projects at Intel, PassEdge, InterTrust, and Microsoft.

6.) **Fabio Ghioni** (Independent Advisor to various MNCs and Government organizations)

Fabio Ghioni is advisor to several Multinational Corporations as well as Governments. He is the leading expert in the field of information security, competitive intelligence and intrusion management in an asymmetric environment. As consultant to several different Government institutions he has been the key to the solution of several terrorism cases in the past. He has serviced leading international corporations involved in the military, telecommunications, banking and technology industries. His key fields of research range from mobile and wireless competitive

security to the classification of information and forensics technologies applied to identity management and ambient intelligence.

7.) **Fabrice Marie** (Manager, FMA-RMS Singapore/Malaysia)

Fabrice is the manager of FMA-RMS, a small dedicated security consulting firm based in Singapore. Developer by trade for many years, he has been involved in the information security field for over 7 years. His interests are in secure programming, cryptography, open source and firewalling techniques. For the last few years he has been breaking mostly bank and telecom web applications in the Asia Pacific region, as well as performing penetration tests for them. Originally from France, Fabrice has been staying in Singapore for the last 6 years.

8.) **Fyodor Yarochkin** (Co-Author, XProbe)

Fyodor Yarochkin is a security hobbyist and happy programmer with a few years spent in business objectives and the “security” service delivery field. These years, however, weren’t completely wasted - Fyodor has been contributing his spare time to a few open and closed source projects, that attracted limited use among non-business oriented computer society. He has a background of system administration and programming and holds Engineering degree in Software Engineering.

Note: Fyodor is not ‘nmap Fyodor’. (http://www.snort.org/docs/faq.html#1.2)

9.) **Javier Burroni** (Senior Developer of Core Impact, Core Security Technologies)

Javier Burroni has been working in Core Security Technologies' CORE IMPACT development team for the last 5 years, where he developed exploits, information gathering modules, and other parts of IMPACT's kernel. He was also the principal author of the ImPacket packet construction library and is an active member of the python community. He is working on statistics applied to financial markets as part of his current studies in actuarial science at Buenos Aires University.

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

Jim is an information security consultant at Bellua Asia Pacific where his work in penetration testing allows him to focus on attack as well as defense. He has performed extensive research on network and host mapping, intrusion detection and prevention system, wireless hotspot security and operating system hardening. Jim was an active contributor in the development of FreeBSD and OpenBSD operating systems. He loves exploring computer system in unusual ways.

Jim has been an invited speaker on several conferences worldwide such as Bellua Cyber Security Asia, Hack In The Box, Cisco Security Summit and IT Underground as well as university and government symposiums. He has been quoted in numerous national publications including Jakarta Post, Kompas, and Detik-I-Net.

11.) **Joanna Rutkowska** (Senior Security Researcher, COSEINC)

Joanna Rutkowska has been involved in computer security research for several years. She has been fascinated by the internals of operating systems since she was in primary school and started learning x86 assembler on MS-DOS. Soon after she switched to Linux world, got involved with some system and kernel programming, focusing on exploit development for both Linux and Windows x86 systems.

A couple of years ago she has gotten very interested in stealth technology as used by malware and attackers to hide their malicious actions after a successful break-in. This includes various types of rootkits, network backdoors and covert channels. She now focuses on both detecting this kind of activity and on developing and testing new offensive techniques. She currently works as a security researcher for COSEINC, a Singapore based IT security company.

12.) **Lisa Thalheim** (Independent Network Security Consultant)

Lisa has spent a good part of the last seven years making and breaking software. She has worked in the field of wireless network security, biometrics, and bug finding in source and binaries. After four years of professional experience in software engineering and coding, she started working as a freelance computer security consultant two years ago, auditing software for security issues in both source and binary form. In the remaining time, she has worked on her duties as a student and is about to complete her diploma degree of Computer Science at the Humboldt University of Berlin, working on the issue of Security in Grid Computing.

13.) **Marc Schönefeld** (Independent Network Security Consultant)

Marc Schonefeld is an external PhD student at the University of Bamberg in Germany. His research covers the analysis of interdependencies between programming flaws (antipatterns) and vulnerabilities in software. By developing a framework for flaw detection he found a range of serious bugs in current java runtime environments (JDK) and other java based applications and middleware systems(like Jboss, Cloudscape database, …). Some of his findings led to the publication of a number of advisories by Sun Microsystems. In 2004 he presented at DIMVA and D-A-CH conferences and was speaker at Blackhat and RSA in 2003. Also in 2004 he was finalist for the European Information Security Award for his work on java based security antipatterns.

14.) **Meder Kydyraliev** (Co-Author, XProbe)

Meder Kydyraliev is a security researcher interested in network security and applications of AI techniques in ethical hacking. Lately, together with Fyodor, he has been researching to find an intelligent way to automate security assessment processes to free up some time for creative stuff. Meder has obtained his B.S. in software engineering from AUCA/Kyrgyzstan and is currenlty working as an associate for KPMG Singapore doing infosec assessments.

15.) **Michael Davis** (Member, The Honeynet Project)

He is an active developer and deployer of intrusion detection systems, with contributions to the Snort Intrusion Detection System. Michael is also a member of the Honeynet project where he is working to develop data and network control mechanisms for windows based honeynets.

Michael also works with McAfee, Inc. a leader in anti-virus protection and vulnerability management, as a Special Projects Research Scientist where he performs confidential and cutting edge security research. Michael has also worked for companies such as 3com and managed two Internet Service Providers.

Lastly, Michael is an active developer in the Open Source community and has ported many popular network security applications to the Windows platform including snort and honeyd. Currently, Michael is a contributing author to Hacking Exposed, the number one book on hacker methodology.

16.) **Nguyen Anh Quynh** (PhD student of Keio university, Japan)

Nguyen Anh Quynh is a PhD student of Keio university, Japan. His research interests include computer security, networking, forensic, virtualization, robust system and Operating System. He is one of the key contributors of Xen Virtual Machine, and he also contributes to various other open source projects. Currently he is working on security problems of virtual machines, specifically focus on Xen.

17.) **Nish Bhalla** (VP Consulting Solutions, Security Compass)

Nishchal Bhalla is a specialist in product testing, code reviews, web application testing, host and network reviews.

He has coauthored “Buffer Overflow Attacks: Detect, Exploit & Prevent”and is a contributing author for “Windows XP Professional Security” and “HackNotes: Network Security”. Nish has also been involved in the open source projects such as OWASP and YASSP. He has also written articles for securityfocus.com and also spoken at web seminars for Global Knowledge and University of Florida.

Prior to joining Security Compass, Nish was a Principal Consultant at Foundstone, where he performed numerous security reviews for major software companies, online banking and trading web sites, and e-commerce sites. He also helped develop and teach the “Secure Coding” class, the Ultimate Hacking, Ultimate Web Hacking and Ultimate Hacking Expert classes. Prior to working at Foundstone, Nish provided engineering and security consulting services as an independent consultant to a variety of organizations including Sun Microsystems, Lucent Technologies, TD Waterhouse & The Axa Group.

Nish holds his Masters in Parallel Processing from Sheffield University, is a post graduate in Finance from Strathclyde University and a Bachelor in Commerce from Bangalore University.

18.) **Paul Boehm** (Founding member of TESO Security, Security Consultant, SEC Consult)

Paul Böhm was a founding member of TESO Security in 1998, and has spent a lot of time breaking code. In 2003 he has worked on quantum cryptography at the University of Vienna where he has developed and implemented an improved efficiency qc protocol. His current interest is in Vulnerabilty Defense and Secure Software. He works as a Security Consultant for SEC Consult.

19.) **Philippe Biondi** (Research Engineer at EADS Corporate Research Center)

Philippe BIONDI works as a research engineer at EADS Corporate Research Center in the system information security lab. He gave many talks in security or open source conferences. He is the author of open source projects like Scapy, Shellforge, and was co-author of LIDS.

20.) **Raditya Iryandi** (Information Security Consultant, Bellua Asia Pacific)

Raditya Iryandi has been a technology junkie since he was a teenager. He loves dealing with telecommunication systems such as satellite, Wi-Fi and modern phreaking. Recently he joined Bellua Asia Pacific as an information security consultant. Prior to joining Bellua, he was Technical Director at C2PRO Consulting.

21.) **Raoul Chiesa** (Board of Directors Member@ Mediaservice.net ISECOM Group & TSTF)

Raoul Chiesa was born in Turin on 3rd July 1973: he has been one of the first hackers in Italy.

His first "wanderings" on the international computer networks of the biggest Eighties' and Nineties' companies date back to 1986, when he was 13, under the nickname of "Nobody". After a series of sensational interferences, such as telcos and other military, governmental, and financial institutions, he was officially recognised as one of the main members of the European and North American hacker scene by international authorities in 1995.

As founder and C.T.O. of @ Mediaservice.net, an italian vendor-independent, security consulting firm, Raoul Chiesa has been active in the field of computer security research at a high level since 1997, together with a team of experts and technicians who gave their contribution to national and international Security R&D projects.

In 2000, Prof. Danilo Bruschi, President of CLUSIT, asked him to be a founder member of the Italian Association for Computer Security; since the first year of activity of the association, Raoul Chiesa has been a member of its Board of Directors, participating in the work of the Study Commission about the "Certifications in Computer Security" and acting as a coordinator of the "Open Source and Security" Commission.

In 2002, two security researchers and Raoul founded the italian-based association "Blackhats.it", a group of security experts and hackers, some of whom working in the field of ICT, who decided to collaborate as a single entity. It is a handful of computer security professionals, strongly linked to "underground" world and genuine hacker philosophy, men and women who devoted themselves to technological innovations and to the improvement of security standards on the Internet.

Since 2003, Raoul Chiesa is the Southern Europe Referent for TSTF (Telecom Security Task Force), an international panel of consultants with high level skills on telcos present in four continents; in the same year Raoul Chiesa was elected in the ISECOM's International Executive Board, following his role of Director of Communications for the Institute (2004).

22.) **Roberto Preatoni** (Founder, Zone-H Defacement Mirror)

Roberto Preatoni (aka Sys64738): 37, is the founder of the defacement/cybercrime archive Zone-H (http://www.zone-h.org). He's also CEO of an International ITsec company (Domina Security) which is active in European and former soviet countries. He has been globetrotting, lecturing in several ITsec security conferences, including Defcon in the US. He has been interviewed by several print and online newspapers where he shares his experiences relating to cyberwar and cybercrimes.

23.) **Rohyt Belani** (Director, Mandiant)

Rohyt Belani is a Director with Mandiant. His expertise encompasses the areas of wireless security, application security and incident response. Rohyt is also an experienced and talented instructor of technical security education courses.

Prior to joining Mandiant, Mr. Belani was a Principal Consultant at Foundstone. Earlier in his career, he was a Research Group Member for the Networked Systems Survivability Group at the Computer Emergency Response Team (CERT).

Mr. Belani is a frequent author of articles for SecurityFocus, a reputed information security portal and SC magazine. He is also a contributing author for the Osborne publication, Hack Notes – Network Security and the Addison-Wesley publication, Extrusion Detection: Security Monitoring for Internal Intrusions. Rohyt is a regular speaker at various industry conferences and forums like OWASP, HTCIA, FBI-Cyber Security Summit, New York State Cyber Security Conference and HITBSecConf2005 - Malaysia. Additionally, he has presented at several Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM) - sponsored conferences.

Mr. Belani holds a Bachelor of Engineering in Computer Engineering from Bombay University and a Master of Science in Information Networking from Carnegie Mellon University. He is a Certified Information Systems Security Professional (CISSP).

24.) **Saumil Shah** (Director, Net-Square)

Saumil continues to lead the efforts in e-commerce security research and product development at Net-Square. His focus is on researching vulnerabilities with various e-commerce and web based application systems, system architecture for Net-Square's tools and products, and developing short term training programmes. 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 heterogenous platforms, and information security and has perfomed numerous ethical hacking exercises for many significant companies in the IT area. Saumil is a regular speaker and trainer 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, infomation 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)

25.) **Shreeraj Shah** (Director, Net-Square)

Shreeraj Shah is founder and director of Net-Square. He has five years of experience in the field of security with a strong academic background. He has experience in 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. 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 Bachelor's degree in Engineering, Instrumentation and Control from Gujarat University, and an MBA from Nirma Institute of Management, India. Shreeraj is the co-author of "Web Hacking: Attacks and Defense" published by Addison Wesley. He has published several advisories, tools, and white papers as researcher, and has presented at conferences including HackInTheBox, RSA, Blackhat, Bellua, CII, NASSCOM etc. You can find his blog at http://shreeraj.blogspot.com/.

26.) **Dr. Stefania Ducci** (Criminologic Researcher, United Nations Interregional Crime and Justice Research Institute, UNCRI)

Ms. Ducci has a University degree in Law (University of Bologna), and a Master degree in Criminology (University of Turin), both obtained with full marks cum laude. She has focused her course of study in Law on Criminal Law, Criminology and Forensic Medicine, themes that has been studied thoroughly during the Master in Criminology.

Since September 2003 she has been working for UNICRI (United Nations Interregional Crime And Justice Research Institute), a United Nations agency dealing with crime prevention and control, as well as criminal justice. Back in 2004, she began collaborating with Raoul Chiesa on personal basis. The studies carried out in team formed the basis of the H.C.P. Project.

For the Hacker Criminal Profiling Project, Stefania has used an independent research approach, providing her support and cooperation during her spare time, fascinated by the huge research possibilities and professional evolution offered by the Project. Her principal interest consists in reading books about hacker and hacking cases, as well as those dealing with criminal profiling.

27.) **The Grugq** (Independent Network Security Researcher)

The Grugq is a domain expert consultant on VoIP security, digital forensic analysis and reverse engineering. The Grugq has spent 7 years working with all aspects of information security, from penetration testing to solutions and product development. The Grugq's career has seen him working for financials, security consulting companies, start-ups and, most recently, founding his own information security company.

The Grugq's information security expertise ranges from penetration testing and source code auditting, through to rootkit technologies and advanced digital forensic analysis and investigation. Since 2001 the Grugq has been involved in active Voice over IP security research, recently completing successful audits for major European and Asian telcos.

The Grugq's domain expertise in VoIP security has seen him present at conferences, release advisories and complete assessments for national European and major Asian telcos. Additionally, he has developed strategic whitepapers for enterprise VoIP deployments. Based on his experiences with numerous audits, the Grugq has developed a VoIP security assessment tool suite to facilitate more accurate, effective and rapid VoIP centric penetration testing.

28.) **Thorsten Holz** (HoneyNet Project Germany, Independent Network Security Researcher)

Thorsten Holz is a Ph.D. student at the Laboratory for Dependable Distributed Systems in Mannheim, Germany. There he teaches besides "system administration" also more interesting courses like the "hacking lab", a half year long CTF-style course. In addition, he is a member of 0ld Eur0pe, a team of students that regularly competes in CTF contests -finally they won the UCSB CTF in December 2005.

Thorsten is one of the founders of the German Honeynet Project. His work there concentrates currently on bots and botnets. He is one of the authors of the "Know Your Enemy: Tracking Botnets" paper and has also published some other papers in this area, e.g., at SecurityFocus and various academic conferences / magazines. Besides this, he is also interested in other areas of IT security, e.g., phishing, web application (in-)securities, or exploitation techniques.

He gave talks and trainings at various conferences. CanSecWest / EuSec / PacSec, Black Hat, CCC, and various other (academic) conferences are examples. Moreover, he is the editor-in-chief of the German IT security magazine MISC. You can find his blog at http://honeyblog.org

29.) **Van Hauser** (Founder, THC.org)

In 1995, van Hauser founded the longest living hacking group which is still highly active today: The Hacker's Choice (www.thc.org). In his long history of greyhat activities, Van Hauser has created some well loved tools like THC-Scan, hydra & amap (also part of Nessus), secure_delete, parasite and many more; He has also written numerous research papers including "Placing Backdoors through Firewalls", "How to cover your tracks" and "Anonymizing Unix Systems". He has presented at various international network security conferences.

30.) **Wes Brown** (Founder, Ephemeral Security)

Wes Brown is a long-time network security practitioner who specializes in code reviews, web application assessments, penetration testing, and tools development.

Prior to joining Accuvant as a senior security consultant, Wes worked for Internet Security System's X-Force Consulting team. He conducted hundreds of penetration tests and web application assessments for ISS clients ranging from the smallest to Fortune 500 companies. He was also responsible for many of the in-house tools that helped the external assessment consulting practice succeed. He also can be frequently seen at industry conferences, having spoken at Defcon in the past.

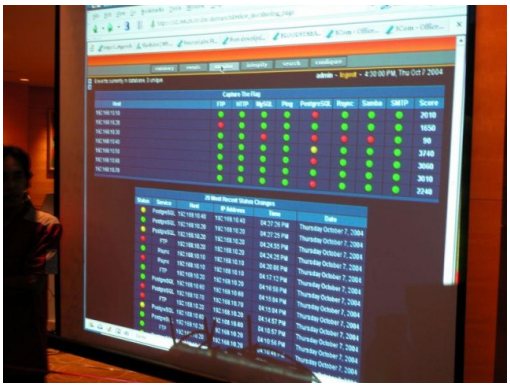
In founding Ephemeral Security, Wes hopes to advance the state of the art in network security by doing innovative and original research work. When not conducting consulting work, he has spent the last year and half on the Mosquito Environment along with other members of his company.

Currently, he is hard at work as one of Accuvant's lead consultants which gives him an opportunity to test the tools and environments that is developed as part of Ephemeral Security's research efforts. He does the majority of the automation and tools that streamlines the assessment practice's engagements, increasing quality while reducing turnaround time. Of course, Wes also does conventional consulting with a keen focus on code reviews and application assessments.

31.) **Yen Ming Chen** (Senior Managing Consultant, Foundstone - A Division of McAfee Inc.)

Yen-Ming leads Foundstone consultants to provide strategic security consulting services to Global 2000 clients. With almost a decade of experience in business development, IT and security, Yen-Ming brings extensive knowledge in both business and technology to his clients. Yen-Ming established the Asian Pacific branch in Singapore for Foundstone and has been instrumental in growing business for Foundstone in APAC. He has performed security assessments for security technologies (ISA server, firewall, and other security products), business applications (financial applications, CRM, and Tax software) and other technologies (multi-functional office equipments and IPTV). He contributed to Four books and numerous articles published on SecurityFocus and other magazines. He's frequent speaker for conferences like CSI, MISTI and others. He served as a Lead Instructor for Foundstone's Ultimate Hacking series classes. Before joining Foundstone, Yen-Ming worked at Carnegie Mellon University and he created the first intrusion detection system appliance prototype using PicoBSD and Snort. He also wrote the first intrusion detection log correlation and analysis program, snort-stat, for Snort. Yen-Ming held a MS in Information Networking from Carnegie Mellon University and a BS in Mathematics from National Central University.

Capture The Flag (CTF)



Overview

This Capture the Flag will be the sixth CtF game to be held in Malaysia, after the hugely successful games held during HITB Security Conference in 2002, 2003, 2004, 2005 and INFOSEC 2003. This year, we're continuing the highly successful format we deployed 3 years ago - whereby each participating team will be given a server to defend, and at the same time launch penetrative attacks against the other teams. As such, participants must know how to attack and plant Flags on opponent's servers in order to score points, and at the same time, know how to defend their own box from being compromised and losing points.

While all this is happening, the CtF Score Server will be keeping track of Services and Flags running on each team's chosen server, so teams can't totally close all Services on the box either. If the Score Server does not detect a Service/Flag on the chosen server, it will deduct points for the team concerned. Teams will not know which Services/Flags the Score Server is looking for, and will have to infer this from the game play. This setup duplicates a common computing infrastructure environment in the enterprise.

Online registration for HITBSecConf2006 – Malaysia is now open!

Important dates:

- 14th April - Registration Opens
- 1st June - Early Bird Registration Closes
- 14th September - Training Registration Closes

To register, point your browsers to:

http://conference.hackinthebox.org/hitbsecconf2006kl/register.php

OR

https://conference.hitb.org/hitbsecconf2006kl/register.php

Event Organizer

Hack In The Box (M) Sdn. Bhd.

Supported & Endorsed By

Malaysian Communications and Multimedia Commission (MCMC)

Malaysian Administrative Modernisation & Management Planning Unit

Main Sponsors

Foundstone - A division of McAfee Inc.

Microsoft Corporation

Official Airline Partner
Malaysia Airlines
Official Hotel
Westin Kuala Lumpur

MEDIA PARTNERS

SUPPORTING ORGANIZATIONS