
# Conference Kit

*** 30 Network Security Specialists and Researchers**
*** 6-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)**
*** Zone-H Hacking Challenge**

**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 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 Detail

**Date:** **26th – 27th September 2005**
**Item:** 7-Tracks Training Sessions
**Time:** 9am to 6pm

**Date:** **28th – 29th September 2005**
**Item:** 2-Tracks Security Conference and Exhibition
**Time:** 9am to 6pm

**Date:** **28th – 29th September 2005**
**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.

# Dual-Track Security Conference
# 28th & 29th September 2005

## The Keynote Speakers

**Tony Chor – Group Program Manager, Microsoft Internet Explorer, Microsoft Corporation**
http://www.microsoft.com

**Presentation Title:** Internet Explorer Security: Past, Present, and Future
**Presentation Details:**

Microsoft's Internet Explorer team is on the frontline of the battle to protect users from malware and social attacks. Tony Chor will outline threats to secure browsing, discuss Microsoft's response with Internet Explorer for Windows XP SP2, and detail the implementation of safety features in the upcoming Internet Explorer 7.0, such as the Phishing Filter and Protected Mode.

**About Tony:**

Tony Chor is the Group Program Manager of the Microsoft's Internet Explorer team. He is responsible for leading the IE team's security response as well as for driving the design, development, and release of new versions of IE including IE 6 in XP SP2 and IE 7 for XP and Windows Vista.

Tony is a fifteen year veteran of Microsoft and has worked on a variety of projects including digital imaging in Windows Vista, MSN Explorer, Works, Encarta Online, Bookshelf, Picture It!, and Golf. He holds a B.S. in Computer Science from Stanford University.

**Mikko Hypponen – Chief Research Officer, F-Secure Corp**
http://www.f-secure.com

**Presentation Title:** Mobile Malware
**Presentation Details:**

The first real viruses infecting mobile phones were found during late 2004. Since then, dozens of different viruses and Trojans - including cases like Commwarrior, Lasco and Skulls - have been found. Mobile phone viruses use totally new spreading vectors such as Multimedia messages and Bluetooth.

How exactly do these mobile viruses work? We'll have a look at their code and discuss what factors affect their spreading speeds. Virus writers have always been trying to attack new platforms. What draws them now towards the mobile phone? Are phones as a platform simply widespread enough, or is the possibility of making easy money via phone billing systems driving this development? Where are we now and what can we expect to see in the Mobile Malware of the future?

**About Mikko:**

Mr. Mikko Hypponen is the Chief Research Officer at F-Secure Corp. He has been analysing viruses since 1991. He has consulted several high-profile organizations on computer security issues, including IBM, Microsoft, FBI, US Secret Service, Interpol and the Scotland Yard. Mr. Hypponen (35) led the team that infiltrated the Slapper worm attack network in 2002, took down the world-wide network used by the Sobig.F worm in 2003 and was the first to warn the world about the Sasser outbreak in 2004.

Mr. Hypponen and his team has been profiled by Wall Street Journal, Vanity Fair, New York Times and Newsweek. He has been an invited member of CARO (the Computer Anti-Virus Researchers Organization) since 1995.

Apart from computer security issues, Mr. Hypponen enjoys collecting and restoring classic arcade video games and pinball machines from past decades. He lives with his family, and a small moose community, on an island near Helsinki.

# Conference Speakers

(Listed in alphabetical order)

1. Aaron Higbee, Principal Consultant, Foundstone, a division of McAfee,Inc.
2. Anthony Zboralski (Gaius), Founder, Hackers Emergency Response Team (HERT)
3. Christoff Breytenbach, Senior IT Security Consultant, Sensepost
4. Dave Aitel , CEO, Immunity Inc.
5. Dave Mckay, Independent Security Consultant
6. Emmanuel Gadaix, Founder, Telecom Security Task Force (TSTF)
7. Fabio Ghioni
8. Fabrice Marie, Manager, FMA-RMS
9. Fyodor Yarochkin, Co-Author, X-Probe
10. Jim Geovedi, Information Security Consultant, PT Bellua Asia Pacific
11. Joanna Rutkowska Founder, Invisiblethings.org
12. Jose Nazario, Senior Software Engineer, Arbor Networks
13. Nish Bhalla, VP Consulting Solutions, Security Compass
14. Marc Shoenefeld,Freelance Network Security Consultant
15. Marius Eriksen, Google
16. Meder Kydyraliev, Co-Author, X-Probe
17. Roberto Preatoni, Founder, Zone-H Defacement Mirror
18. Rohyt Belani, Director, Red Cliff Consulting
19. San, Member, X-Focus China
20. Shreeraj Shah, Director, Net-Square Solutions
21. Swaraj, Suresec UK
22. The grugq, Independent Anti-forensics Researcher
23. Tim Pritlove, Chaos Computer Club
24. Zubair Khan, Freelance Network Security Consultant

# Event At A Glance

**HANDS ON TECHNICAL TRAINING SESSIONS**
**26TH AND 27TH SEPTEMBER 2005**

**TECHNICAL TRAINING TRACK 1:**
**WEB APPLICATION SECURITY – ATTACK AND DEFENCE**

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

**Outline:** 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. 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.

**TECHNICAL TRAINING TRACK 2:**
**EXPLOITING AND DEFENDING NETWORKS**

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

**Outline:** The purpose of this course is to provide tech leads, testers, administrators, network administrators, help desk support and all other participants detailed security techniques and knowledge as applied to UNIX, Windows and Network security. It goes from the very basic concepts of understanding of Operating Systems (UNIX & Windows), learning the concepts of attacking and protecting Operating Systems, Networks & Network Devices. Participants would also learn how to take advantages of vulnerabilities that might exists in an environment. The training will not only show the latest techniques for exploiting the environment, but also how to defend the organization infrastructure against those weaknesses. Hands-on lab exercises reinforce the course material in a real world environment.

**TECHNICAL TRAINING TRACK 3:**
**WAR DRIVING KUALA LUMPUR**

**Trainers:** Anthony Zboralski (Gaius), *Founder* Hackers Emergency Response Team (HERT) and Jim Geovedi, *Information Security Consultant* PT Bellua Asia Pacific.

**Outline:** This class will involve a war drive around Kuala Lumpur on the first day and as such is limited to **8 participants only.**

This two day hands-on workshop will cover wireless/mobile environments intrusion detection, secure wireless protocols, denial of service, privacy and anonymity, prevention of traffic analysis, wireless networking, monitoring and surveillance...

**HANDS ON TECHNICAL TRAINING SESSIONS**
**26TH AND 27TH SEPTEMBER 2005**

## TECHNICAL TRAINING TRACK 4: PACKET MASTERING THE MONKEY WAY

**Trainers**: Dr. Jose Nazario, *Senior Software Engineer* Arbor Networks and Marius Eriksen *Software Engineer*, Google.com

**Outline:**

In this course you will learn how to code in C using libpcap, libdnet, libnids, and drive it all with libevent. The main language will be C, but we will also cover python bindings to these techniques.

**Day 1**

a) TCP/IP and ethernet networking overview
b) Packet capture with libpcap
c) Packet construction with libdnet
d) Libnids and stream reconstruction techniques

**Day 2**

a) Recap and questions from day 1
b) Event driven programming (signals, read, write, timers), libevent
c) Common tool classes: scanners, snifers, and tracers
d) Bringing it all together:
e) A simple stream sniffer (illustrating the use of libnids and libevent)
f) A simple port scanner (illustrating libpcap, libevent, libdnet)
g) Questions and other things you can do.

## TECHNICAL TRAINING TRACK 5: DIGITAL INVESTIGATIONS: PRACTICAL DIGITAL FORENSIC ANALYSIS

**Trainer:** The grugq, *Independent Anti-forensics Researcher*
**Outline:** As the number of IT security incidents increases month upon month, the need for effective digital investigation techniques grows. This course teaches students how to conduct a successful digital forensic investigation, and builds a solid base of knowledge for further learning. Using a task-oriented approach, students will learn digital forensic analysis techniques and methodologies which can be applied immediately. During the course, strong emphasis is placed on technical understanding and skills.

The core curriculum of the course revolves around multiple File System Intensive sessions, focusing on file systems used on both Windows and UNIX/Linux platforms such as NTFS and Ext2FS. These File System Intensives use a combination of lectures and task-oriented hands-on lab exercises to instruct and reinforce the deep, low-level, file system knowledge crucial for effective digital forensic analysis and investigations. The lab exercises will teach core skills, such as how to:

* seize and preserve digital media
* recover deleted files (both manually and with tools)
* uncover evidence of tampering
* build a time-line

**TECHNICAL TRAINING TRACK 6:**
**HACKING BY NUMBERS – GUERILLA EDITION**

**Trainers:** Christoff Breytenbach
**Outline:**

Reality, Theory and Practice! This course is the "How did they do that?" of modern hacking attacks. From start to finish we will lead you through the full compromise of a company's IT systems, explaining the tools and technologies, but especially the thinking, strategies and the methodologies for every step along the way. "Hacking By Numbers - Guerilla Edition" will give you a complete and practical window into the methods and thinking of hackers.

'Guerilla' is SensePost's 'community-oriented' course, designed to address the needs the the community - students, hobbyists & researchers. Like all our courses, it is strongly method based and emphasizes structure, approach and thinking over tools and tricks. The course is popular with beginners, who gain their first view into the world of hacking, and experts, who appreciate the sound, structured
approach.

**TECHNICAL TRAINING TRACK 7:**
**THE EXPLOIT LABORATORY - BUFFER OVERFLOW BLACK ARTS**

**Trainers:** Saumil Udayan Shah & SK Chong
**Outline:**

This class shall introduce how buffer overflow vulnerabilities arise in programs and how they get exploited. The class 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 class 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.

***DEEP KNOWLEDGE SECURITY CONFERENCE***
***DAY 1 - 28TH SEPTEMBER 2005***

| | |
|---|---|
| **08.00** | Registration |
| **09.00** | Keynote Address: Internet Explorer Security: Past, Present, and Future<br>**Tony Chor *Group Program Manager, Microsoft Internet Explorer,* Microsoft Corporation** |
| **10:30** | Refreshment Break |

| | **TECHNICAL TRACK** | **BUSINESS-TECH TRACK** |
|---|---|---|
| **11:00** | Nematodes - Beneficial Worms<br>**Dave Aitel (Immunity Inc)** | |
| **12:00** | Networking Luncheon | |
| **13:00** | STIF-ware Evolution<br>**Meder Kydyraliev and**<br>Fyodor Yarochkin, *Co-Authors,* X-Probe) | Project Blinkenlights / Arcade<br>**Tim Pritlove (Chaos Computer Club)** |
| **14:00** | **VoIPhreaking: How to make free phone calls and influence people**<br>The grugg, *Independent Anti-Forensics Specialist* | Cyber Skirmishes<br>**Zubair Khan, *Independent Security Consultant*** |
| **15:00** | Web Hacking Kung-Fu and Art of Defense<br>**Shreeraj Shah, *Director***<br>**Net-Square Solutions** | Corp vs Corp: Profiling Modern Espionage<br>**Roberto Preatoni, *Founder* Zone-H Defacement Mirror and Fabio Ghioni** |
| **16:00** | Refreshment Break | |
| **16:30** | Hacking Windows CE<br>**San, X-Focus China** | Social Engineering Fundamentals<br>**Anthony Zboralski (Gaius), *Founder* Hackers Emergency Response Team (HERT) & Dave Mckay, *Independent Security Consultant*** |
| **17:30** | Hide-And-Seek: Defining the Roadmap for Malware Detection on Windows<br>**Joanna Rutkowska, *Founder,* Invisiblethings.org** | Trends in Real World Attacks: A Compilation of Case Studies<br>**Rohyt Belani *Director*, Red Cliff Consulting** |
| **18:30** | End of Day One | |

***DEEP KNOWLEDGE SECURITY CONFERENCE***
***DAY 2 - 29TH SEPTEMBER 2005***

| | |
|---|---|
| **08.00** | Registration |
| **09.00** | Keynote Address: Mobile Malware<br>**Mikko Hypponen, *Director of Anti Virus Research*, F-Secure Corp.** |
| **10:30** | Refreshment Break |

| | **TECHNICAL TRACK** | **BUSINESS-TECH TRACK** |
|---|---|---|
| **11:00** | Assessing Server Security - State of the Art<br>**Christoff Breytenbach, *Senior IT Security Consultant*, Sensepost** | |
| **12:00** | Networking Luncheon | |
| **13:00** | **Analyzing all that data: Techniques for sifting haystacks and finding needles.**<br>Dr. Jose Nazario, *Senior Software Engineer* Arbor Networks | *- TBA -*<br>**Marius Eriksen *Software Engineer,* Google.com** |
| **14:00** | Wi-Fi Hotspot Security<br>**Jim Geovedi *Information Security Consultant* PT Bellua Asia Pacific.** | **Phishing Attacks: A Guide to Self Assessment**<br>**Aaron Higbee, *Principal Consultant*, Foundstone, a division of McAfee,Inc.** |
| **15:00** | Exploiting Microsoft Services For Unix<br>**Swaraj, Suresec UK** | Hacking Internet Banking Applications<br>**Fabrice Marie, *Manager,* FMA-RMS** |
| **16:00** | Refreshment Break | |
| **16:30** | Analyzing Code for Security Defects<br>**Nish Bhalla, *VP Consulting Solutions*, Security Compass** | *- TBA -*<br>**Emmanuel Gadaix, *Founder*, Telecom Security Task Force (TSTF)** |
| **17:30** | Java & Secure Programming<br>**Marc Shoenefeld, *Freelance Network Security Consultant*** | |
| **18:30** | End of Day Two | |

# The Speakers Profiles

**1. Aaron Higbee**

**Presentation Title:** Phishing Attacks: A guide to self assessment
**Presentation Details:**

This is not another presentation about identifying phishing attacks and other scams. Phishing Attacks, a guide to self assessment aims to answer all the political and technical questions in planning and executing a phishing exercise for your own organization.

The audience will learn how to organize a phishing attack and leverage it into an exercise that will test user awareness and IT's procedures to phishing incident response. Technical topics will include:

1.) How to word a compelling, believable phishing email scenario
2.) How to build the phishing web server
3.) How to mass mail the phishing scam to bypass potential mail filters
4.) How to safely collect the data of those who fall for the scam

The presentation will also cover the non-technical considerations that need to be thought of before and after the attack. If the phishing attack was planned right, the email and firewall team will be better prepared to respond to this threat, and more importantly, the recipient will gain valuable security awareness training that will help them at work and at home. With proper planning and execution, the victims actually thank you when it's over.

**About Aaron:**

Aaron Higbee is a principal consultant for Foundstone, a division of McAfee. Prior to Foundstone, Aaron was a network abuse investigator for Earthlink Network and Roadrunner and has witnessed every type of Internet abuse since its inception. Aaron draws on his consulting experience building phishing exercises for Foundstone's clients.

**2. Anthony Zboralski (Gaius)**
*Founder*, Hackers Emergency Response Team (HERT)

**Presentation Title:** Social Engineering Fundamentals
**Presentation Details:**

You might say there are two specialties within the job classification of con artist. Somebody who swindles and cheats people out of their money belongs to one sub-specialty, the grifter. Somebody who uses deception, influence, and persuasion against businesses, usually targeting their information, belongs to the other sub-specialty, the social engineer." -Kevin Mitnik

In today's world confidence scams present quite possibly the highest threat to security with in the business world. Control of information, withholding and leaking, can lead to massive failures and losses depending on how skilled the attacker may be. In combination with disinformation and propaganda, social engineering can as fatal as or even lead to loss of customer and shareholder confidence.

**About Anthony:**

Anthony Zboralski leads Bellua Asia Pacific, an Information Security consulting company based In Jakarta, Indonesia. He has more than 9 years of experience performing penetration tests, assessments, forensics and related services for some of the largest banks in Asia and a dozen Fortune 500 companies including Aerospatiale, Air France, Allianz, AXA, Electricite de France, Lagardere-Matra…

He is also known as Gaius, one of HERT cofounders and wrote some articles for phrack and hert.org (tunnelx, ciscogdb, procx, etc.). Anthony has been involved into hacking and security community since 1989 (started on x25 with otosync and bayernpower [Matthias]). He is 29 now, living in Indonesia with wife and two kids.

**3. Christoff Breytenbach**
*Senior IT Security Consultant*, Sensepost

**Presentation Title:** Assessing Server Security - State of the Art
**Presentation Details:**

Over 70% of all the open ports on the Internet are web servers. In order to effectively evaluate an organization's Internet security posture we must be able to effectively assess web server security. This talk takes a comprehensive look at the question of assessing web server security over the Internet. During the talk we consider the progress that has been made in web server security over the last few years, and the progress that has been made in attacking web servers over the same time. We visit the new vulnerabilities introduced by web applications and discuss the thinking applied to discover such vulnerabilities.

Finally, we describe the state of the art of web server scanning technology.

This talk should be split over two sessions and will cover the following topics:

**Web Security - Yesterday & Today:**

Web server security has improved dramatically since the dark days of IIS4 and the possibly even darker days of IIS5. In this section we discuss the new protection mechanisms built into Windows 2003 Server and IIS6 in particular. To demonstrate the improvements web servers have made common attack vectors will be discussed and demonstrated against IIS5.x & IIS6 servers.

**The Hunt - Finding servers to attack:**

Web servers can run on any port on any server. And a single web server may serve numerous different sites. Finding these servers and sites is the first challenge for the attacker. In this section we discuss and demonstrate current 'footprinting' methodology and tools, with special focus on the automation of footprinting technologies.

**State of the Art - Current Tools & Techniques:**

In October 2004 SensePost introduced 'Wikto" a Windows tool that took CGI scanning to a new level. The integration of search engine technology, combined with the ability to cascade results and the use of fuzzy logic to detect false positives built on the work done in tools like Nikto to

produce arguably the best CGI scanner available today. In this section we demonstrate and discuss the thinking behind Wikto and examine the challenges of introducing Wikto technology into the renowned Nessus open source security scanner.

**Opening Windows - Analyzing Web Applications:**

Insecure web applications are the single biggest threat to web server security today. However, the variety of development approaches and the custom nature of these applications makes the automated discovery of vulnerabilities on such systems near to impossible. Current web application security scanners only reveal the tip of the iceberg and security analysts have access to very simply copy-cat analysis tools. In this section we discuss an alternative approach to black-box web application security assessment and demonstrate new technology designed to enable detailed and intelligent analysis.

Each section will include detailed technical demonstration and an open forum for questions and comments.

**About Christoff:**

Christoff Breytenbach studied B.Com Informatics at the University of Pretoria, South Africa. During 1999, while still studying, he was employed part time at the University's Bureau of Institutional Research and Planning as a Natural/Adabas programmer. He started fulltime employment at the end of 1999 doing Visual Basic development work on company secretarial systems. His career moved towards information security in 2000 when he joined NetXactics (formerly eSafe Technologies) where one of his areas of expertise was application integration and technical support of cryptographic tokens.

Christoff joined AST Security Management in 2001 as an information security architect, specialising in network security consulting, architecture design and implementations. Just one of the various projects he was involved in, included Microsoft Certificate Services architecture design as a partner consultant to Microsoft Consulting Services South Africa. In August of 2002, Christoff joined SensePost as a senior IT security consultant involved in the various assessment services SensePost provides, including internal-, external-, architecture-, web application- / services- and database security assessments. Christoff has presented various talks (Internet Solutions' Internetix conference, MSUG, ISSA, TechEd, etc.), papers (editorial for ITP Asia etc.), and presented various Black Hat- and SensePost training sessions, both locally and internationally. Christoff holds various certifications, including CISSP and MCSE in Security.

**4. Dave Aitel**
*CEO,* Immunity Inc.

**Presentation Title:** Nematodes - Beneficial Worms
**Presentation Details:**

This presentation presents concepts for taking expoitation frameworks into the next evolution: solving complex security problems by generating robustly controllable beneficial worms. The Why, How, and What of Nematode creation are discussed, along with some concepts in Mesh routing.

Problems discussed include legal issues, controlling your worm, writing an intermediate language, the Nematode Intermediate Language (NIL) for writing robust worms, reliability problems, commications protocols, and future work.

**About Dave:**

Dave Aitel is the CEO of Immunity, Inc, and is still responsible for research and development for their flagship CANVAS product. In addition, he created and distributes under the Gnu Public license the fuzzing tool, SPIKE, the web application analysis tool SPIKE Proxy, and the remote access tool Hydrogen. His original stint was as a computer scientist at the National Security Agency, after which he spent a few years at @stake, a private security consulting firm, and finally started Immunity, Inc. Immunity's product CANVAS is used by penetration testing firms, government agencies, large financial firms, and other companies who wish to simulate information attacks against their infrastructure.

5. **Dave Mckay**

**Presentation Title:** Social Engineering Fundamentals
**Presentation Details:** ** Presenting with Anthony Zboralski

**About Dave:**

Dave McKay is an independent security consultant. McKay has been involved in the information security field for going on 9 years. McKay's prior employment includes an impressive list of companies where he served in a security capacity including, Hotmail, Google, Microsoft, US Department of Defense and @stake (now Symantec). McKay is now in Rome writing a book.

6. **Emmanuel Gadaix**
*Founder,* Telecom Security Task Force (TSTF)

**Presentation Title:** TBA
**Presentation Details:** TBA

**About Emmanuel:**

Emmanuel has been involved in the information security and telecommunications fields for over 12 years. Originally from Western Europe, Emmanuel has been living in Southeast-Asia since 1993. After few years spent at Nokia commissioning mobile networks' NMS and IN systems, he started his own security consulting company in 1997, which eventually got acquired by Trusecure in 2001.

Emmanuel focuses on the emerging threats facing the telecommunications industry today. He founded the Telecom security Task Force (TSTF) to provide clients with specialized security services for their GSM/GPRS/UMTS/SS7/VoIP/IMS networks.

He is a CISSP, a Certified ISO-8583 Financial Transaction Protocol Engineer and a Certified Oracle DBA

**7. Fabio Ghioni**

**Presentation Title:** TBA
**Presentation Details:** ** Presenting with Roberto Preatoni

**About Fabio:**

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.

**8. Fabrice Marie**
*Manager,* FMA-RMS

**Presentation Title:** Hacking Internet Banking Applications
**Presentation Details:**

The general public sentiment is that the banks, having always been the guardians of our money, are expert at safeguarding it. Unfortunately, internet corporate banking and personal banking applications are usually ridden with bugs. Internet Banking Applications development is nowadays out-sourced to third party software vendors that have poor understanding of security, and incomplete quality management processes. Most of the time the applications are extremely insecure before they get audited by security professional third-parties.

This presentation will demonstrate the various attacks that almost always work (and those that do not), on your “bank-next-door” internet banking application, illustrated with real life statistics. We will outline the regular technical attacks and will focus on a hit parade of business logic attacks. We will steal money from other customers, buy shares for free, and spy on other customers bank records among many other frauds.

This demonstration will highlight the solutions to some of the challenges the banks will face online to ensure that their data handling practices are compliant with their country’s privacy regulations and banking regulations among others.

**About Fabrice:**

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 6 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 5 years.

**9. Fyodor Yarochkin**
*Co-Author*, X-Probe

**Presentation Title:** TBA
**Presentation Details:** TBA

**About Fyodor:**

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 Yarochkin is not 'nmap Fyodor'. (http://www.snort.org/docs/faq.html#1.2)

**10. Jim Geovedi**
*Information Security Consultant* PT Bellua Asia Pacific.

**Presentation Title:** Wi-Fi Hotspot Security
**Presentation Details:**

It's cool to live in a wireless world. Wireless is the latest thing. It's the excitement of the year. It's the expectation for the decade. Bandwidth for the masses is the hopeful war cry of the tech evangelist. The elusive *last mile* solution.

Hotels, airports, coffee shops, pubs, and many places provide Wi-Fi hotspots for yuppies, executives campaign for mobile workplaces, PDAs and smartphones are the latest determiner for the hip.

This presentation will cover the basic approach behind Wi-Fi hotspot security design and architecture. During the presentation, vulnerabilities and methods for exploiting Wi-Fi hotspot will be showed.

**About Jim:**

Jim Geovedi is HERT's new evil thinker. While most of his time goes towards providing information security advisory and training services to private enterprises and government in Indonesia through Bellua Asia Pacific, in his spare time Jim amuses himself by working on open-source security software and operating system development projects.

**11. Joanna Rutkowska**
*Founder*, Invisiblethings.org

**Presentation Title:** Hide & Seek
**Presentation Details:** TBA

**About Joanna:**

Joanna Rutkowska is an independent security researcher. Her main interest is in stealth technology, that is, in the methods used by attackers to hide their malicious actions after a successful break-in. This includes various types of rootkits, network backdoors and covert channels. She is interested in both detecting this kind of activity and in developing and testing new offensive techniques.

She develops assessment and detection tools mainly for pen-testing companies. She has previously presented at the 21st Chaos Communication Congress, IT Underground 2004 and HiverCon2003. She lives in Warsaw, Poland.

**12. Dr. Jose Nazario**
*Senior Software Engineer*, Arbor Networks.

**Presentation Title:** Analyzing all that data: Techniques for sifting haystacks and finding needles.
**Presentation Details:**

Previously, gathering data was a difficult task, and so simple data analysis techniques worked well. now with access to information increasing, and the need to get an even broader coverage of events, making sense of mountains of data has never been more pressing. The great risk in this scenario is missing an indicator or losing data.

This presentation will introduce you to a number of techniques for making sense of large collections of data, including sorting and clustering techniques, fuzzy matching, and trend analysis. These techniques have applicability in numerous applications, such as mail filtering and network event analysis.

**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".

**13. Nish Bhalla**

*VP Consulting Services,* Security Compass

**Presentation Title:** Analyzing Code for Security Defects
**Presentation Details:**

The objective of the talk is understanding how to review large code bases for security defect. It can be used as methodology to identify security problems when reviewing code. The overall focus will be on the finding security vulnerabilities and the implementation of countermeasures however, the same techniques can also be implemented to help develop secure development practices.

Reviewing code to find vulnerabilities is becoming more and more common. Reviewing code is not only useful from a developers point of view but also from an attacker's point of view. The talk will cover basics of threat analysis, how to assess threats and what are some of the vulnerabilities that could exists in code when performing code reviews for large code bases.

**About Nish:**

Nishchal Bhalla is a specialist in product testing, code reviews, web application testing, host and network reviews and IDS architecture design and deployments. He is the VP of Consulting Services at Security Compass providing consulting services for major software companies & Fortune 500 companies.

He is writing the section on writing exploits for an upcoming title "Buffer Overflow Attacks: Detect, Exploit & Prevent" and is a contributing author for "Windows XP Professional Security" and "HackNotes: Network Security", he was also the tech editor for "Exploiting Software: How to Break Code".

Nish has also been involved in the open source projects such as OWASP and YASSP. He has also written for security focus.

Prior to joining Security Compass, Nish was a Principal Consultant at Foundstone, where he not only helped develop the "Secure Coding" class but also taught the Ulimate Hacking, Ultimate Web Hacking and Ultimate Hacking Expert classes. Apart from working for Foundstone, some of the other companies Nish has worked for include TD Waterhouse, The Axa Group and Lucent.

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.

**14. Marc Shoenefeld**

**Presentation Title:** Java & Secure Programming
**Presentation Details:** Java is not secure by default, you as a programmer can use its built-in features to make your software more secure, but on the other your errors and the flaws in the software stack below (like the JDK) can add a wide range of vulnerabilities to your java software. The talk is about the causes for errors and the techniques to detect them.

**About Marc:**

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.

**15. Marius Eriksen**
*Software Engineer,* Google.com

**Presentation Title**: TBA
**Presentation Details:** TBA

**About Marius:**

Marius Eriksen is a software engineer at Google, Inc. and is an OpenBSD developer. He has developed and maintained many open source projects and has failed to release many more. Marius has mostly been involved with systems security, distributed filesystems, networking middleware and security and general operating systems kernel development. Marius' recent open source work include work on transparent end-to-end networking portability and contextual user interfaces.

**16. Meder Kydyraliev**
*Co-Author*, X-Probe

**Presentation Title:** TBA
**Presentation Details:** ** Presenting with Fyodor Yarochkin

**About Meder:**

Meder Kydyraliev is a freelance security researcher, has obtained his bachelor of science degree in software engineering from AUK/Kyrgyzstan and is at early stage of getting to know what real security industry(sic) is. For past 2 years he has been involved in research and development of Xporbe2 active OS fingerprinting tool. Some of his personal interests include: network reconnaissance, information gathering techniques and applications of distributed computing in information security tools. His senior project was titled "Multi-threaded, distributed platform for information security tools".

**17. Roberto Preatoni**
*Founder*, Zone-H Defacement Mirror

**Presentation Title:** TBA
**Presentation Details:** TBA

**About Roberto:**

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.

**18. Rohyt Belani**
*Director,* Red Cliff Consulting

**Presentation Title:** Trends in Real World Attacks: A Compilation of Case Studies
**Presentation Details:**

The number of reported security incidents has always been proportional to the number of vendor-issued vulnerabilities. However, recently this trend seems to have broken. This can be attributed to an increase in attacks against custom applications, attacks targeting end-users, zero-day exploits, and self-propagating worms. This presentation will discuss such trend-breaking real world attacks ranging from the installation of keystroke-logging Trojans on end-user machines through an IE buffer overflow to attacks against wireless clients. Each case study will discuss the motivation of the attack, an overview of the underlying technical details and its impact on business.

**About Rohyt:**

Rohyt Belani is a Director with Red Cliff Consulting. 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 Red Cliff, 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. He is also a contributing author for the Osborne publication, Hack Notes – Network Security. Rohyt is a regular speaker at various industry conferences and forums like OWASP, HTCIA, FBI-Cyber Security Summit, HP World, New York State Cyber Security Conference and HackInTheBox-Malaysia. Additionally, he has presented at several Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM) -sponsored conferences on the topics of fault-tolerant distributed systems, wireless networks, and advanced network simulation.

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).

**19. San**
X-Focus, China

**Presentation Title:** Hacking Windows CE
**Presentation Details:**

The network features of PDAs and mobiles are becoming more and more powerful, so their related security problems are attracting much more attention. This paper will show a buffer overflow exploitation example in Windows CE. It will cover knowledge about the ARM architecture, memory management and the features of processes and threads of Windows CE. It will also shows how to write a shellcode in Windows CE including knowledge about decoding shellcode of Windows CE.

1 - Windows CE Overview
2 - ARM Architecture
3 - Windows CE Memory Management
4 - Windows CE Processes and Threads
5 - Windows CE API Address Search Technology
6 - The Shellcode for Windows CE
7 - System Call
8 - Windows CE Buffer Overflow Exploitation
9 - About Decoding Shellcode
10 - Conclusion

**About San:**

San is a security researcher, who has been working in the Research Department of NSFocus Information Technology (Beijing) Co., Ltd for more than three years. He's also the key member of XFocus Team. His focus is on researching and analysing application security, and he's also the main author of "Network Penetration Technology" (Chinese version book).

**20. Shreeraj Shah**
*Director*, Net-Square Solutions

**Presentation Title:** Web Hacking Kung-Fu and Art of Defense
**Presentation Details:**

Web attacks are on the rise and new methods of hacking are evolving. This presentation will cover new methodologies for web application footprinting, discovery and information gathering with a new range of tools.

Web applications are getting exploited using various new injection techniques like advanced SQL injection, LDAP query, XPATH goofing etc. All these new exploit methods will be discussed. The HTTP stack is changing in application frameworks like .NET. The stack can be utilized for defense using HTTP interfaces. Defense methodology for web applications are required to combat new threats emerging in the field.

This will be a deep-knowledge presentation that will be full of **live demos, examples and new tools**!

**About Shreeraj:**

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.

**21. Swaraj**
Suresec UK

**Presentation Title:** Exploiting Microsoft Services For Unix
**Presentation Details:**

Microsoft Services for Unix is a new component in the Windows suite which lets you run UNIX based applications on a win32 platform with very little effort. Microsoft has ported a number of utilities and packages to make the transition an easy task and to eliminate the need to have a dedicated UNIX platform. This presentation will cover the weakness in such a deployment and further cover all security issues including design flaws of the subsystem internals and will focus on different exploitation techniques.

**About Swaraj:**

Swaraj works for suresec as a senior security researcher, he enjoys code auditing and writing exploits for fun, he also works for debian linux distribution as a member of the security audit group which proactively fixes security vulnerabilities.He goes by an alias called jaguar ,in the past has found a number of vulnerabilities and has contributed to the debian project.

**22. The grugq**
*Anti Forensics Specialist*

**Presentation Title:** VoIPhreaking: How to make free phone calls and influence people
**Presentation Details:**

The recent explosion in internet telephony has led to the exposure of the (previously) closed Public Service Telephone Network (PSTN) to the wilds of the internet. Voice over IP (VoIP) technology presents new and interesting security challenges, many of which are completely ignored until after deployment. These security issues, such as new avenues for fraud, present serious risks to tradition telephony companies. This talk explores the technologies behind VoIP infrastructures, focusing on their weaknesses and faults. **LIVE DEMOS** will help illustrate that attacks which violate VoIP system security are not only practical, but are already here. The era of VoIPhreaking has begun.

**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.

**23. Tim Pritlove**
*Chaos Computer Club*

**Presentation Title:** Project Blinkenlights
**Presentation Details:**

In 2001, Project Blinkenlights developed the “Blinkenlights light installation in Berlin, Germany turning the “Haus des Lehrers building at Alexanderplatz into a huge computer screen, worlds most interactive light installation achieving a broad range of public participation. The “screen consisted of 18 windows in 8 floors therefore providing a matrix of 144 monochrome “pixels that could be individually turned on and off. Blinkenlights combined the charme of a low tec installation with high-profile computer programming and managed to deliver a high level of participation for the public. People could send in their own animations to be played back on the screen. They could also play the classic computer game Pong in real time just using their mobile phone.

Encouraged by the great success of the installation, the group got invited to join the Nuit Blanche art exhibition in 2002 in Paris to create the successor project named “Arcade. Targetting the Biblioth que nationale de France, the group managed to build worlds big gest interactive light installation so far. The installation made use of greyscaling redefining the appearance and flexibility compared to the original installation. The screen used 26 windows on 20 floors resulting in 520 “pixels. Each pixel allowed displaying 8 dierent brightnesses. The installation covered 3370 square meters making it visible from many kilometers away.

**About Tim:**

Tim Pritlove is a long time computer hacker, events organizer and member of the Chaos Computer Club. Working as a programmer, teacher and consultant he played around with a variety of computer systems and computer networks since the early eighties. He is the organizer of the annual Chaos Communicaton Congress and the quadren nial Chaos Communication Camp. Tim is the coordinator and project leader of Project Blinkenlights that became famous for interactive light installations in public buildings. In another life, he is an assistant professor and system administrator at the University of Arts in Berlin.

**24. Zubair Khan**

*Independent Security Consultant*

**Presentation Title:** Cyber Skirmishes
**Presentation Details:**

High-tech information warfare is fast becoming a reality. The term information warfare covers a wide range of activity, including corporate and military espionage and intelligence collection, psychological operations and perception management, attacks on communication systems, consumer fraud, and information piracy. In addition, the concept covers specifically computer-related issues: viruses, Trojan horses, and deliberate and targeted hacking efforts such as computer break-ins and denial-of-service attacks (where hackers flood an Internet server with traffic to overload and disable it). Cyber warfare is politically-motivated computer hacking that inflicts severe societal harm, and may also effect nation's economy and defense. Cyber Warfare is so rapid that it may not give an opponent enough time to "surrender" before permanent and devastating damage is done. It has recently become of increasing importance to the military, the intelligence community, and the business world. Military planners are now imagining soldiers at computer terminals silently invading foreign networks to shut down radars disable electrical facilities and disrupt phone services.

**# Introducing Cyber warfare**
**# Globalization of Cyber Warfare**
**# Outsourcing Warfare**
**# Cyber Targets**
**# Psychology of Modern Warfare**
**# Cyber Weapons**
**# Retaliation and Defense Tools**

**# Cyber battleground of Palestine and Israel**

- Political and social effects caused by hacking incidents ( Real Examples)
- Targets
- Searching More Targets
- Famous Hacker Groups
- Volunteer Hackers
- Formation of Groups and their strategies
- Globalizing the war
- Tactics

**# Cyber battleground of Iran and USA**

- Political and social effects caused by hacking incidents ( Real Examples)
- Targets
- Searching More Targets
- Famous Hacker Groups
- Volunteer Hackers
- Formation of Groups and their strategies
- Globalizing the war
- Tactics

**# Cyber battleground of China and USA**

- Political and social effects caused by hacking incidents ( Real Examples)
- Targets
- Searching More Targets

- Famous Hacker Groups
- Volunteer Hackers
- Formation of Groups and their strategies
- Globalizing the war
- Tactics

**# Cyber battleground of India and Pakistan**

- Political and social effects caused by hacking incidents ( Real Examples)
- Targets
- Searching More Targets
- Famous Hacker Groups
- Volunteer Hackers
- Formation of Groups and their strategies
- Globalizing the war
- Tactics

**# Capabilities of Al Qaeda**
**# Al Qaeda's Interest In Cyber Warfare**
**# Al Qaeda's Cryptography as Communication**
**# Cyber attacks during war of Terrorism**
**# Cyber attack on Al Qaeda by US**
**# Cyber Defense Strategies**
**# How hacking affect military operations?**
**# Influencing Foreign Policy**
**# How cyber attacks can spark a Real War?**
**# Cyber Propaganda and Terrorism**
**# ECHELON**
**# Revolution in Military affairs and C4I**
**# International Law**
**# Future of Cyber Warfare**

## About Zubair:

Zubair Khan is a freelance network security consultant. He has been researching mainly on DDoS Attacks and also on various other facets of network security for the past six years. He has given network security consultancy to top organizations of Pakistan. Recently he worked as a network security consultant for C4i of Pakistan. C4i is one of the directorates of Pakistan Army providing secure mode of communication for peacetime and war.

Zubair is founder of hacker's conferences in Pakistan. His two major events Islamabad Hackers Training Camp 2004 and Islamabad Hackers Convention 2005 turned out to be a huge success. These events created a platform for security professionals in Pakistan. He has also conducted security trainings at various forums which includes government organizations. His research and work is recognized by Chairman of Pakistan Engineering Development Board and Chairman of Pakistan Engineering Council. His work and efforts to create network security awareness are greatly appreciated by high officials of country and also by media agencies.

# Deep Knowledge Hands-On Technical Training Sessions

## TECHNICAL TRAINING TRACK 1
## WEB APPLICATION SECURITY – ATTACK AND DEFENCE

**BY:** Shreeraj Shah (Net-Square Consulting)

- **Date:** 26th & 27th September 2005
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax
- **Cost:** RM1800 (early bird) RM2200 (non-early bird)

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.

## TECHNICAL TRAINING TRACK 2
## EXPLOITING & DEFENDING NETWORKS

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

- **Date:** 26th & 27th September 2005
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax
- **Cost:** RM1800 (early bird) RM2200 (non-early bird)

**Details:**

The purpose of this course is to provide tech leads, testers, administrators, network administrators, help desk support and all other participants detailed security techniques and knowledge as applied to UNIX, Windows and Network security. It goes from the very basic concepts of understanding of Operating Systems (UNIX & Windows), learning the concepts of attacking and protecting Operating Systems, Networks & Network Devices. Participants would also learn how to take advantages of vulnerabilities that might exists in an environment. The training will not only show the latest techniques for exploiting the environment, but also how to defend the organization infrastructure against those weaknesses. Hands-on lab exercises reinforce the course material in a real world environment.

Understanding TCP/IP, Windows, and Unix

- TCP/IP
  - Understanding the 3-way handshake
  - Understanding UDP
  - Understanding ICMP

- Windows
  - Understanding Domains and Workgroups
  - Domain Trust relationships
  - Enumeration
  - Understanding SIDs and RIDs
  - Registry and sam files
  - Common Services (Netbios, Web servers, IIS)
- UNIX
  - DIG / nslookup
  - Users and Groups (Understanding Unix file Permissions, User, Group)
  - Common services (FTP, Telnet, SSH, TFTP, RPC, NFS)

Introduction Attack & Penetration

- A&P Methodology
  - Foot-printing
  - Scanning
  - Enumeration
  - Exploiting Vulnerabilities
  - Installing Rootkits and Backdoors
  - Cleaning up

- Foot-printing
  - whois
  - Search engines
  - Google hacking
  - News-groups
  - Corporate Websites
  - EDGAR

- Scanning

- Finding Live Hosts
- Port scanning (Connect, SYN, FIN)
- Passive network monitoring

- Enumeration
  - OS Fingerprinting
  - Detailing network service information (Banner Grabbing, DNS information)
  - Obtaining list of valid users and resources
  - Passive network monitoring
  - OS Specific Enumeration

  - Unix
    - User enumeration via Apache
    - User enumeration via Finger
    - User enumeration via r-services
    - Obtaining user info using NIS

  - Windows
    - Enumerating windows users and shares (net, nete, enum, local, global, nltest, dumpsec, getmac, epdump, ldp)

- Source sifting web portals
  - Mirroring web sites (wget, Black Widow, Offline explorer)

- Brute forcing authentication
  - Brutus
  - Hydra
  - Extending Hydra to Brute Force Custom Protocols
  - MS-SQL Brute forcing (sqldict, shell script)
  - Mysql / Oracle
  - TS-Grind

- Mis-configurations
  - TFTP
  - NFS (nfsshell)
  - X Vulnerabilities (xscan)

- Buffer Overflows (metasploit)

- Obtaining and Cracking password files
  - Windows (sam, pwdump3, LSA Secrets)
  - Unix ( /etc/shadow,  NIS (ypcat))
  - Cracking passwords ( l0phtcrack,  john)

Exploiting Network Specific Vulnerabilities

- Sniffing (Promiscous mode)
- ARP Spoofing
- Hijacking TCP connections
- 802.11
  - Quick Overview
  - Kismet
  - Aircrack

- Owning Network Devices
  - Cisco router password cracking
  - Attacking services (Telnet, SNMP, HTTP, Obtaining config files)

- Firewalls
  - Fingerprinting Firewalls.

Auditing

- Windows cleanup
  - disabling audit logs (Evenviewer)
  - Web Server Logs

- UNIX Cleanup
  - Xinet revisited & /etc/syslog.conf
  - utmp and wtmp
  - xferlog
  - maillog
  - lastlog
  - shell histories

Installing Backdoors and Rootkits

- Port redirection techniques

- Windows backdoors and rootkits
  - Fake Gina
  - Winvnc
  - Hiding files in windows
  - Keyloggers

- Back-dooring Unix
  - Installing a Remote Shell Service using xinted
  - Setting SETUID and SETGID on executable files
  - .rhosts
  - Loki2
  - Trojanized commonly used commands

- Linux Rootkits
  - LKM based
- Covert Channels
  - Reverse shell
  - Msn-shell
  - XML-shell

## TECHNICAL TRAINING TRACK 3
## WAR DRIVING KUALA LUMPUR

**BY**: Anthony Zboralski (Gaius), *Founder* Hackers Emergency Response Team (HERT) and Jim Geovedi, *Information Security Consultant* PT Bellua Asia Pacific

- **Date:** 26th & 27th September 2005
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 8 pax
- **Cost:** RM2000 per pax (early bird) / RM2400 (non-early bird)

**Note:** Participants are required to bring their own laptops. Wireless enabled laptops aren't required as students will connect to the Kismet Server using a network hub in the training room as well as in the bus.

This class will involve a war drive around Kuala Lumpur on the first day and as such is limited to **8 participants only.**

This two day hands-on workshop will cover wireless/mobile environments intrusion detection, secure wireless protocols, denial of service, privacy and anonymity, prevention of traffic analysis, wireless networking, monitoring and surveillance...

Wireless Technology is ubiquitous: hand phones, cordless phones, Wi-Fi LANs Bluetooth are everywhere. While wireless technology may be desirable to corporations because of the mobility and cost-saving it offers, wireless security has been elusive.

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 network could be used to launch stealth attacks against other targets or to transit spam

The 2-day course will cover:

- Introduction to Bluetooth and WiFi Security
- War Driving in Kuala Lumpur
- Analysing and mapping wireless networks.
- Attacking Wireless Networks and Bluetooth Devices
- Defending Wireless Networks
- Intrusion Detection and Monitoring

## TECHNICAL TRAINING TRACK 4
## PACKET MASTERING THE MONKEY WAY

**BY:** Dr. Jose Nazario, *Senior Software Engineer* Arbor Networks and Marius Eriksen *Software Engineer*, Google.com

- **Date:** 26th & 27th September 2005
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax
- **Cost:** RM1800 (early bird) RM2200 (non-early bird)

In this course you will learn how to code in C using libpcap, libdnet, libnids, and drive it all with libevent. The main language will be C, but we will also cover python bindings to these techniques.

**Day 1**

a) TCP/IP and ethernet networking overview
b) Packet capture with libpcap
c) Packet construction with libdnet
d) Libnids and stream reconstruction techniques

**Day 2**

a) Recap and questions from day 1
b) Event driven programming (signals, read, write, timers), libevent
c) Common tool classes: scanners, snifers, and tracers
d) Bringing it all together:
e) A simple stream sniffer (illustrating the use of libnids and libevent)
f) A simple port scanner (illustrating libpcap, libevent, libdnet)
g) Questions and other things you can do.

## TECHNICAL TRAINING TRACK 5
## DIGITAL INVESTIGATIONS: PRACTICAL DIGITAL FORENSIC ANALYSIS

**BY:** The Grugq

- **Date:** 26th & 27th September 2005
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax
- **Cost:** RM1800 (early bird) RM2200 (non-early bird)

As the number of IT security incidents increases month upon month, the need for effective digital investigation techniques grows. This course teaches students how to conduct a successful digital forensic investigation, and builds a solid base of knowledge for further learning. Using a task-oriented approach, students will learn digital forensic analysis techniques and methodologies which can be applied immediately. During the course, strong emphasis is placed on technical understanding and skills.

The core curriculum of the course revolves around multiple File System Intensive sessions, focusing on file systems used on both Windows and UNIX/Linux platforms such as NTFS and Ext2FS. These File System Intensives use a combination of lectures and task-oriented hands-on lab exercises to

instruct and reinforce the deep, low-level, file system knowledge crucial for effective digital forensic analysis and investigations. The lab exercises will teach core skills, such as how to:

* seize and preserve digital media
* recover deleted files (both manually and with tools)
* uncover evidence of tampering
* build a time-line

Each File System Intensive concludes with a sample investigation, reinforcing the skills developed within the course and building an understanding of how to successfully conduct a real investigation. During the File System Intensive sessions, students will learn about the forensic analysis process, as well as the techniques and methodologies necessary for successful digital forensic investigations.

**Prerequisites:** Students should be comfortable using Linux as an operating environment. Students will be assigned machines (desktops) in pairs. Each machine will include a Linux installation, including X windows. Development tools (e.g. gcc, make, etc.) will be installed, however no development experience is required. All tools will be provided on CD-ROM.

## TECHNICAL TRAINING TRACK 6
## HACKING BY NUMBERS – GUERILLA EDITION

**BY:** Christoff Breytenbach - Sensepost

- **Date:** 26th & 27th September 2005
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax
- **Cost:** RM2000 (early bird) / RM2400 (non early-bird)

### OVERVIEW

Reality, Theory and Practice! This course is the “How did they do that?” of modern hacking attacks. From start to finish we will lead you through the full compromise of a company’s IT systems, explaining the tools and technologies, but especially the thinking, strategies and the methodologies for every step along the way. “Hacking By Numbers - Guerilla Edition” will give you a complete and practical window into the methods and thinking of hackers.

‘Guerilla’ is SensePost’s ‘community-oriented’ course, designed to address the needs the the community - students, hobbyists & researchers. Like all our courses, it is strongly method based and emphasizes structure, approach and thinking over tools and tricks. The course is popular with beginners, who gain their first view into the world of hacking, and experts, who appreciate the sound, structured
approach.

### WHO SHOULD ATTEND

Information security officers, system and network administrators, security consultants, government agencies and other nice people will all benefit from the valuable insights provided by this class. Remember that this course is practical and of an extremely technical nature, so a basic understanding of networking, security, Unix™ and NT™ is a course prerequisite

## TECHNICAL TRAINING TRACK 7
## THE EXPLOIT LABORATORY - BUFFER OVERFLOW BLACK ARTS

**BY:** Saumil Udayan Shah & SK Chong

- **Date:** 26th & 27th September 2005
- **Venue:** The Westin, Kuala Lumpur
- **Duration:** 2-days
- **Capacity:** 30 pax
- **Cost:** RM2000

### OVERVIEW

This class shall introduce how buffer overflow vulnerabilities arise in programs and how they get exploited. The class 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 class 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.

### 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

### Notes

Students will be required to:

Have a working knowledge of operating systems, Win32 and Unix
Compile programs using GCC
Use vi/pico/joe editors

** Understanding of C programming would be a bonus.

**About the trainers**

**SAUMIL UDAYAN SHAH,**
**Founder and CEO, Net-Square Solutions Pvt. Ltd.**

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 ten 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.

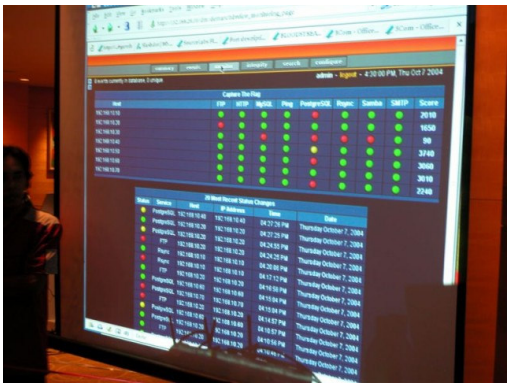
Prior to joining Foundstone, Saumil was a senior consultant with Ernst & Young, where he was responsible for the company's ethical hacking and security architecture solutions. Saumil has also worked at the Indian Institute of Management, Ahmedabad, as a research assistant and is currently a visiting 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). He has served as a technical editor for "Hacking Exposed 2nd Ed", and has contributed to "Know your Enemy - the Honeynet Project" book.

**SK CHONG**
**Security Consultant, SCAN Associates**

S.K. (CISSP) is a security consultant from SCAN Associates. His job allows him to play with all kinds of hacking tools in his penentration testing. Most often, he needs to modify and/or enhance these tools before it can be used for legal penetration testing against banks, ISP and goverment agencies. These experiences help him wrote a few security whitepapers on SQL Injection, Buffer Overflow, Shellcode and Windows Kernel stuff, including one of which published in Phrack E-zine #62. His researches was presented in Blackhat (Singapore) 2003, HITBSecConf2003 - Malaysia, RuxC0n2004 (Australia), XCon2004 (China) and many other security conferences.

# Capture The Flag (CTF)



**Overview**

This Capture the Flag will be the fifth CtF game to be held in Malaysia, after the hugely successful games held during HITB Security Conference in 2002, 2003, 2004 INFOSEC 2003 and BCS2005 in Indonesia. This year, we're continuing the highly successful format we deployed 2 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.

# Zone-H Hacking Challenge


Zone-H in colaboration with the Hack in The Box crew will organize a web-based hackgame at HITBSecConf2005 in which participants will be challenged to try to beat the hackgame in the shortest possible time. The hackgame rules are fairly simple. There is a central server offering an online hackgame which is developed along three different levels. The three levels are of increasing difficulty, all of them can be beaten just using a simple web browser so there will be no need to bring your own exploits or your own laptop. Each participant has a limited amount of time to beat all three levels; upon completion of each level a separate scoring mechanism will assign to the participant some points based on a time-mission scheme.


All the participants will be rewarded with some gifts. Beating the first level will grant the participant a Zone-H keystrap, beating the second level will win you an exclusive Zone-H Exploit Repository CD, beating the third level will grant you the beautilful Zone-H t-shirt. Finally, the best three hackers (fastest time) will win a free Hands on Hacking seminar seat (to be held in Kuala Lumpur in cooperation with Hack in The Box in 2006). Are you ready for the challenge?


**REGISTRATION NOW OPEN !!!**
**REGISTER ONLINE**

**http://conference.hackinthebox.org/hitbsecconf2005kl/register.php**

Suruhanjaya Komunikasi dan Multimedia Malaysia
*Malaysian Communications and Multimedia Commission*

Malaysian Communications and Multimedia Commission (MCMC)

MAMPU

Malaysian Administrative Modernisation & Management Planning Unit

**Main Sponsor**

Microsoft®

Microsoft Corporation

**Official Airline Partner**

malaysia AIRLINES

Malaysia Airlines

**Media Partners:**


The Virus Bulletin Conference takes place at The Burlington, Dublin, Ireland, 5 to 7 October 2005. Register here.

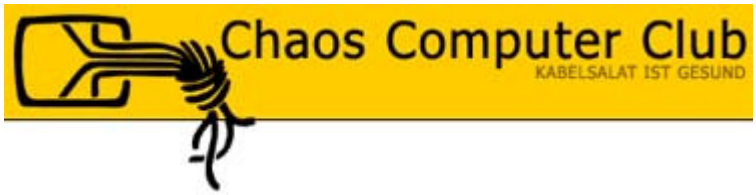
**Our Speakers Are Supported By:**


Bellua Asia Pacific


F-Secure Corporation

**Supporting Organizations**


HERT




Chaos Computer Club (Germany)


X-Focus China


Zone-H Defacement Mirror


Xatrix Security


SyScan05


Special Interest Group in Security & Information InteGrity Singapore