HITBSECCONF2007 - DUBAI
2ND - 5TH APRIL 2007 - SHERATON CREEK HOTEL
DEEP KNOWLEDGE SECURITY CONFERENCE

Hands on Technical Training
Dual Track Security Conference
Capture The Flag 'Live Hacking' Competition

HITBSecConf2007 - Dubai
CONFERENCE KIT 2.0

*** 20 Network Security Specialists and Researchers**
*** 4-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)
Suite 26-3, Level 26, Menara IMC
No 8. Jalan Sultan Ismail,
50250 Kuala Lumpur, Malaysia.
Phone: ++603-20394724
Fax: ++603-20318359

Overview

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

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

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

Event Detail

Date:	**2nd – 3rd April 2007**
Item:	4-Tracks Hands-On Technical Training Sessions
Time:	9am to 5pm
Date:	**4th – 5th April 2007**
Item:	Security Conference and Exhibition
Time:	9am to 4pm
Date:	**4th – 5th April 2007**
Item:	Capture The Flag 'Live Hacking' Competition
Time:	9am to 5pm
Venue:	Sheraton by The Creek Dubai, U.A.E.

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.

Training Sessions

HANDS ON TECHNICAL TRAINING SESSIONS
2ND AND 3RD APRIL 2007

TECHNICAL TRAINING TRACK 1: ADVANCE WEB APPLICATION & SERVICES HACKING

Trainer: Shreeraj Shah (Director, Net-Square)
Capacity: 24 pax
Duration: 2 days
Cost: (per pax) USD1299 (early bird) / USD1499 (non early-bird)
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.

TECHNICAL TRAINING TRACK 2: TACTICAL VOIP: APPLIED VOIPHREAKING

Trainer: The Grugq, Independent Network Security Consultant
Capacity: 24 pax
Duration: 2 days
Cost: (per pax) USD1299 (early bird) / USD1499 (non early-bird)
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

TECHNICAL TRAINING TRACK 3:
STRUCTURED NETWORK THREAT ANALYSIS AND FORENSICS

Trainers: Meling Mudin (spoonfork) & Lee Chin Sheng (geekool)
Capacity: 24 pax
Duration: 2 days
Cost: (per pax) USD1299 (early bird) / USD1499 (non early-bird)
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.

TECHNICAL TRAINING TRACK 4:
PACKET MASTERING THE MONKEY WAY

Trainer: Dr. Jose Nazario (Senior Software Engineer, Arbor Networks)
Capacity: 24 pax
Duration: 2 days
Cost: (per pax) USD1299 (early bird) / USD1499 (non early-bird)
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.

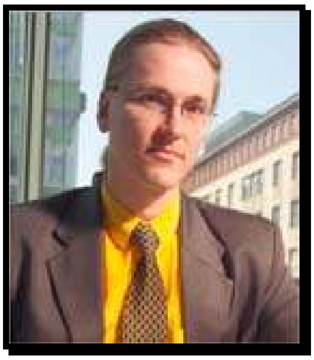
Day 1

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.

The Keynote Speakers



Mikko Hypponen – Chief Research Officer, F-Secure Corp

http://www.f-secure.com

Presentation Title: Online Crime and Crime Online
Presentation Details:

Who's really behind the network attacks? Who's launching the phishing scams? Who runs the botnets? How do they hide their malware? Where are they reselling the stolen bank accounts and credit card numbers? How do they move their money around? How do they recruit their money mules? What do these guys look like and how does all this really work? Is this the perfect crime?

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.

Lance Spitzner– Founder and President, Honeynet Project

http://www.honeynet.org

Presentation Title: Honeypots: Today and Tomorrow.
Presentation Details:

Honeypots are a powerful and widely used but misunderstood technology. Almost everyone has benefited from honeypot use, but few may realize it. We will address this by explaining what honeypots are, their value, and a brief history. We will then focus on the state of honeypot technology today, who is using them, and how they are being used. We will provide numerous examples of different honeypot technologies either released or currently under development. In addition, we will give examples of how many different organizations are using these technologies, and the value they are providing. Finally, by looking at the evolution and use of honeypots over the past 10 years, we will cover the future of honeypots, new technologies, and how they will most likely be used.

About Lance:

Mr. Spitzner is considered to be a leader in the field of honeypot research. He invented and developed the concept of honeynets, is the author of the book "Honeypots: Tracking Hackers", co-author of "Know Your Enemy: 2nd Edition", and has published over fifty security whitepapers and articles.
He is founder of the Honeynet Project; a global, non-profit security research organization that captures, analyzes, and shares information on cyber threats at no cost to the public.

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.

He has spoken and worked with numerous organizations around the world, including NSA, FIRST, the Pentagon, the FBI Academy, the President's Advisory Board, West Point, the Navy War College, the Department of Justice, and Monetary Authority of Singapore. His work has been documented in the media such as CNN, BBC, NPR, and Wall Street Journal. Before information security, Mr. Spitzner served seven years in the Army, four as an officer in the Army's Rapid Deployment Force. Mr. Spitzner earned a B.A. History from the University of Illinois-Champaign and an MBA from the University of Illinois-Chicago.

Our distinguished panel of speakers

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

Emmanuel is a founder of Telecom Security Task Force (TSTF) which specializes in providing security services to mobile carriers. His passion for telecommunications security started in the early 90's while exploring worldwide X.25 networks. In 1994 he joined Nokia Telecommunications and participated in the launch of several GSM networks across Asia. In 1997 he founded The Relay Group in Thailand, a company seen as a pioneer of the Penetration Testing business in the region. Emmanuel is also involved in the development of alternative energy projects.

2.) Enno Rey (ERNW GmbH)

Enno Rey loves playing with network protocols and devices since he first heard about the internet protocol family. Prior to founding a specialized team of security researchers in 2001 he's been working as a sysadmin and network operator. He has vast experience in designing, operating, troubleshooting and securing large networks. Furthermore he is one of the authors of the first and only German book on penetration-testing, has written several articles and white papers and is a frequent speaker on conferences. Enno’s twelve years of information security experience include a wide variety of topics, amongst them cryptography, pentesting/auditing, secure network design and technology risk evaluation. Throughout the years he has acquired the usual security certifications (CISSP, CISA, BS 7799 Lead Auditor) and has provided security consultancy services to many Fortune 500 enterprises and governmental agencies.

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

Fabrice Marie is a senior security consultant working for FMA-RMS, a small dedicated security firm based in Singapore with offices in Kuala Lumpur. Developer by trade for many years, he has been involved in the information security fields for over 7 years. His interests are in cryptography, trusted operating systems, secure programming, open source and firewalling techniques. For the last three years he has been breaking mostly bank and telco web applications in the region, as well as performing penetration tests for them.

4.) Hendrik Scholz (Lead VoIP Developer, Freenet Cityline GmbH)

Hendrik Scholz is a lead VoIP developer and systems engineer at Freenet Cityline GmbH in Kiel, Germany. While studying and working in Kiel (Germany), Melbourne (Australia), Atlanta (Ga, USA) and Orlando (Fl, USA) he contributed to FreeBSD and specialized on networking security issues. Nowadays the average work day consists of a healthy mix of design, development and debugging. Having access to all sorts of VoIP devices hacking on those became a spare time passion. Publications include various presentations as well as additions to the SIP Express Router (SER, available at iptel.org). Some publications are available at http://www.wormulon.net/publications/

5.) Marc Webber Tobias (Investigative Attorney and Security Specialist)

Marc Weber Tobias is an investigative attorney and security specialist living in Sioux Falls, South Dakota. He represents and consults with lock manufacturers, government agencies and corporations in the U.S. and overseas regarding the design and bypass of locks and security systems. He has authored five police textbooks, including Locks, Safes, and Security, which is recognized as the primary reference for law enforcement and security professionals worldwide. The second edition, a 1400 page two-volume work, is utilized by criminal investigators, crime labs, locksmiths and those responsible for physical security. A ten-volume multimedia edition of his book is also available online. His website is security.org, Marc is a member of a number of professional security organizations, including the American Society of Industrial Security (ASIS), Association of Firearms and Tool Marks Examiners (AFTE), American Polygraph Association (APA) and American Association of Police Polygraphists (AAPP).

Marc was Chief of the Organized Crime Unit, Office of Attorney General in the State of South Dakota, and as such directed many criminal investigations. He also worked special investigations for the Office of Governor, State of South Dakota for sixteen years, and was responsible for conducting internal inquiries for the executive branch of government and for the state prison system.

Marc has lectured extensively in the United States and Europe on physical security and certain aspects of criminal investigations and interrogation technique. He holds several patents involving the bypass of locks and security systems. Marc contributes a column to engadget.com and has been featured in many publications as well as radio and television stories around the world.

6.) Nitin Kumar (Independent Security Engineer / Researcher)

Mr. Nitin Kumar is an independent Security Engineer & researcher from the India's Himalayan Region. He has been involved in Network Security Analysis and Penetration Techniques. He likes reverse engineering, researching OS & Network Security. He is a recent graduate in Bachelor of Technology, Computer Science & holds RHCE certification. His clients include some of most reputed organizations of India. His latest work involves the development of boot kit (a technique to subvert Windows 2000/XP/2003 System using custom boot sector).

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

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 theCertifications in Computer Security and acting as a coordinator of the Open Source and Security’s 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 â€œundergroundâ€ 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).

8.) Rodrigo Rubira Branco (Software Engineer, IBM)

Rodrigo Rubira Branco (BSDaemon) is a Software Engineer at IBM, member of the Advanced Linux Response Team (ALRT), part of the IBM Linux Technology Center (IBM/LTC) Brazil also working in the IBM Toolchain (Debugging) Team for PowerPC Architecture.

He is the maintainer of the StMichael/StJude projects (www.sf.net/projects/stjude), the developer of the SCMorphism (www.kernelhacking.com/rodrigo) and has talks at the most important security-related events in Brazil (H2HC, SSI, CNASI). Rodrigo is also a member of the Rise Research (www.risesecurity.org).

9.) 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 Bachelors 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/.

10.) Tareq Saade (Program Manager, MSRR, Microsoft Corporation)

Tareq Saade, a former Dubai resident, is a program manager on the Microsoft Security Research & Response team. MSRR is responsible for creating technology around the collection and consumption of telemetry from a wide variety of Microsoft security technologies including SpyNet which Tareq helped build.

11.) 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.

12.) Vipin Kumar (Independent Network Security Consultant/Analyst)

Mr. Vipin Kumar is an independent security consultant and analyst. He has experience in system and network security as well as programming and project design. He likes to develop specialized software and/or stuffs related to windows kernel. He holds MCSE and Bachelors in Technology in Computer Science. His latest work involves the development of boot kit (a technique to subvert Windows 2000/XP/2003 System using custom boot sector). He is currently analyzing windows vista kernel architecture.

13.) Window Snyder (Chief Security Something-or-Other, Mozilla Foundation)

Window Snyder is Chief Security Something-or-Other at Mozilla Corporation.

Prior to joining Mozilla, Ms. Snyder was a principal, founder, and core team member at Matasano, a security services and product company based in New York City and a senior security strategist at Microsoft in the Security Engineering and Communications organization. At Microsoft she managed the relationships between security consulting companies and the Microsoft product teams and the outreach strategy for security vendors and security researchers. Previously she was responsible for security sign-off for Windows XP SP2 and Windows Server 2003.

Ms. Snyder was Director of Security Architecture at @stake. She developed application security analysis methodologies and led the Application Security Center of Excellence. She was a software engineer for 5 years focused primarily on security applications, most recently at Axent Technologies, now Symantec.

Ms. Snyder is co-author of Threat Modeling, a manual for security architecture analysis in software.

Conference Agenda

DAY 1
4TH APRIL 2007

07.30	**Registration**	
08.50	**Welcome Address by TRA / CEO of DU**	
09.00	**Keynote Address 1: Online Crime and Crime Online** Mikko Hypponen, Chief Research Officer, F-Secure Corp.	
10:00	**BREAK**	
	TRACK I	**TRACK II**
10:30	**HEWLETT PACKARD MIDDLE EAST**	**Digging into SNMP 2007 - An Exercise on Breaking Networks** Enno Rey, ERNW Gmbh
11:30	**NGN Security – Next Generation Nightmare** Emmanuel Gadaix, Founder, Telecom Security Task Force, TSTF	**Open Source Open Security** Window Snyder, Chief Security Something or Other, Mozilla Corporation
12:30	**LUNCH**	
13:30	**Vboot Kit: Compromising Windows Vista Security** Vipin Kumar & Nitin Kumar, Independent Network Security Consultants/Researchers	**DU**
14:30	**BREAK**	
15:00	**Ravage Unleashed: The Tactical VoIP Toolkit** The Grugq, Independent Network Security Consultant	**Opened in Ten Seconds: The Insecurity of Mechanical Locks** Marc Webber Tobias, Investigative Attorney and Security Specialist
16:00	**END**	
17:00	**MICROSOFT COCKTAIL / RECEPTION PARTY IN SHERATON DUBAI CREEK FOR CONFERENCE SPEAKERS AND ALL DELEGATES**	

DAY 2
5TH APRIL 2007

08.30	**Registration**	
09.00	**Keynote Address 2: Honeypots: Today and Tomorrow** Lance Spitzner, Founder Honeynet Project	
10:00	**BREAK**	
	TRACK I	**TRACK II**
10:30	**ETISALAT / SYMANTEC MIDDLE EAST**	**Spam goes VOIP – Number Harvesting for Fun and Profit** Hendrik Scholz, Lead VoIP Developer, Freenet Cityline Gmbh
11:30	**Robbing Banks: Easier Done Than Said** Fabrice Marie, Founder, FMA-RMS Singapore & Malaysia	**A Middle Eastern Perspective of the Malware Landscape** Tareq Saade, Program Manager, Microsoft Security Research & Response (MSRR), Microsoft Corporation
12:30	**LUNCH**	
13:30	**Kernel Hacking: If I really know I can hack** Rodrigo Rubira Branco, Software Engineer, IBM and member of the Advanced Linux Response Team (ALRT)	**SCANIT**
14:30	**BREAK**	
15:00	**X.25 Networks in the Arab World** Raoul Chiesa, Board of Directors member @Mediaservice.net ISECOM Group & Telecom Security Task Force (TSTF)	**TBA** Shreeraj Shah , Director, Net-Square
16:00	**END**	

Capture The Flag (CTF)

Overview

This Capture the Flag will be the second CtF game to be held in the Middle East region after the attack-only game which was run in Bahrain in April of 2005. The attack-only CTF is different from the game that has been held in HITB Security Conference in 2002, 2003, 2004, 2005 and INFOSEC 2003.

Instead of each participant having to attack and defend, participants in the game will be expected to launch penetrative attacks against **single or multiple target servers**. Each machine is configured with various services (some of which may be vulnerable while others might not be). Participants are required to retrieve pre-configured files or 'flags' from the target machine in order to score points. Attendees are not bared from attacking each other however any participant found using denial of service attacks will be removed from the game immediately. First place teams will get USD3,000, USD2,000 for 2nd place and USD1,000 for 3rd place. The CTF competition and all prizes are sponsored by Scan Associates Sdn. Bhd.

HITBSECCONF2007 - DUBAI
2ND - 5TH APRIL 2007 - SHERATON CREEK HOTEL
DEEP KNOWLEDGE SECURITY CONFERENCE

Hands on Technical Training
Dual Track Security Conference
Capture The Flag 'Live Hacking' Competition

We have space for ONLY 200 ATTENDEES!

Make sure you book your seats early!

Important dates:

- 1st January 2007 - Registration Opens
- 1st February 2007 - Early Bird Reg. Closes
- 30th March 2007 - Training Reg. Closes

To register, point your browsers to:

http://conference.hackinthebox.org/hitbsecconf2007dubai/register.php

OR

http://conference.hitb.org/hitbsecconf2007dubai/register.php