HITBSECCONF2009 – DUBAI
CONFERENCE KIT

Event Overview

Venue:
Sheraton Dubai Creek
Baniyas / Creek Road,
Dubai, UAE

20th & 21st April 2009

- TT1 - Web Application Security - Threats & Countermeasures
- TT2 - 802.11 Ninjitsu
- TT3 - The Exploit Laboratory 3.0

22nd & 23rd April 2009

- Dual Track Security Conference featuring 2 keynote speakers and 20 leading network security specialists
- Capture The Flag Competition Technology Exhibition

The largest network security conference in Asia and the only deep knowledge event in the Middle East!

The main aim of the HITBSecConf conference series is to create a truly technical and deep knowledge event in order to allow you to learn first hand on the security threats you face in todays super connected world. The HITBSecConf platform is used to enable the dissemination, discussion and sharing of critical network security information.

Presented by respected members of both the mainstream network security arena as well as the underground or black hat community, our events routinely highlight new and ground-breaking attack and defense methods that have not been seen or discussed in public before.

HITBSecConf2009 - Dubai will be our 3rd conference in the UAE and is expected to attract over 200 delegates from the GCC, Europe, North America and the Asia Pacific region. Come and learn from some of the leading experts in the network security arena.

HITBSecConf2009 - Dubai will also see our highly popular attack-only Capture The Flag competition being organized once again. This years contest will also include an additional binary reversing challenge as well!

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

Keynote Speakers

KEYNOTE 1 - Philippe Langlois
(Founder, Qualys / Intrinsec / TSTF)

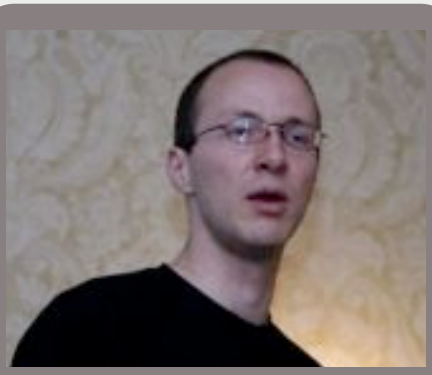
Philippe is an entrepreneur and security researcher. He is currently advisor to Netvibes and Global partner at Telecom Security Task Force. In 1999, he founded Qualys, world-leading vulnerability-assessment service delivered as an application service provider. He founded computer and network security company Intrinsec in 1995. He was also lead designer for Payline, the first French e-commerce payment gateway.

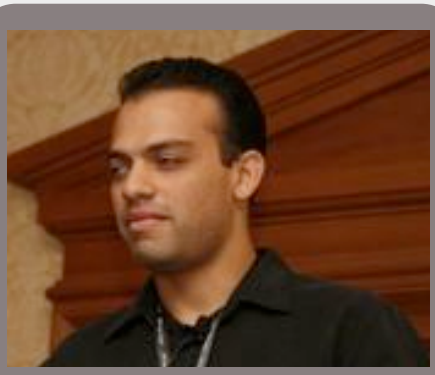
KEYNOTE 2 - Mark Curphey
(Director, Connected Information Security Group, Microsoft Corp)

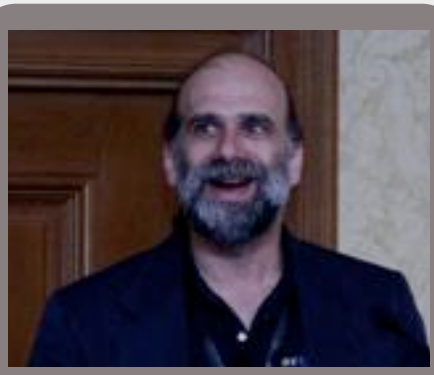
Mark is the founder of OWASP, the Open Web Application Security Project that has become a well thought of reference site for developers and system architects and recommended reading by the US Federal Trade Committee. He has a Masters Degree in Information Security from the renowned Royal Holloway, University of London where he specialized in advanced cryptography.

Official Conference Website:
http://conference.hitb.org/hitbsecconf2009dubai/

Our Distinguished Panel of Speakers







1.) Anthony Zboralski (Founder, Bellua Asia Pacific / HERT)

2.) Billy Rios (Security Engineer, Microsoft Corp)

3.) Chris Evans (Security Lead, Google Corp)

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

5.) Lance Spitzner (Founder, HoneyTech)

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

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

8.) Nitin Kumar (Founder, nvLabs)

9.) Roberto Preatoni (Founder, WSLabi - The Exploit Marketplace)

10.) Rodrigo Rubira Branco (Security Expert, Check Point Software Technologies)

11.) Saumil Shah (Founder, Net-Square)

12.) Sebastian Porst (Security Consultant, zynamics GmbH)

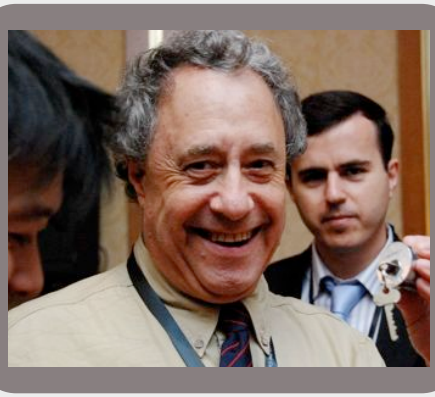
13.) Shreeraj Shah (Founder, BlueInfy)

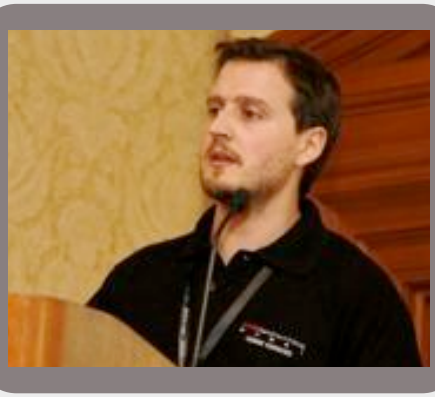
14.) Steve Anson (Director, Forward Discovery)

15.) The Grugq (Independent Network Security Researcher)

16.) Vipin Kumar (Founder, nvLabs)

17.) Wes Brown (Senior Security Consultant, Matasano Security)





TT1 – Web Application Security – Threats & Countermeasures

Trainers: Shreeraj Shah (Founder, BlueInfy) and Vimal Patel (Co-Founder, BlueInfy)
Capacity: 25 Students

Outline:

Introduction and adaptation of new technologies like Ajax, Rich Internet Applications and Web Services has changed the dimension of Application Hacking. We are witnessing new ways of hacking web based applications and it needs better understanding of technologies to secure applications. The only constant in this space is change. In this dynamically changing scenario in the era of Web 2.0 it is important to understand new threats that emerge in order to build constructive strategies to protect corporate application assets. Application layers are evolving and lot of client side attack vectors are on the rise like Ajax based XSS, CSRF, Widget injections, RSS exploits, Mashup manipulations and client side logic exploitations. At the same time various new attack vectors are evolving around SOA by attacking SOAP, XML-RPC and REST. It is time to understand these advanced attack vectors and defense strategies.

The course is designed by the author of "Web Hacking: Attacks and Defense", “Hacking Web Services” and “Web 2.0 Security – Defending Ajax, RIA and SOA” bringing his experience in application security and research as part of curriculum to address new challenges. Application Security is hands-on class. The class features real life cases, hands one exercises, new scanning tools and defense mechanisms. Participants would be methodically exposed to various different attack vectors and exploits. In the class instructor will explain new tools like wsScanner, scanweb2.0, AppMap, AppCodeScan etc. for better pen-testing and application audits.

TT2 – 802.11 Ninjitsu

Trainers: Anthony Zboralski (Founder, HERT & Bellua Asia Pacific)
Jim Geovedi (Member, HERT & Security Consultant, Bellua Asia Pacific)

Capacity: 25 Students

Outline:

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

Course Agenda

Wireless and its technology usage
Wireless networking breakdown
Security of wireless and progression
What is wardriving?
Attacking wireless brief
Wireless Protocols and Architecture
Analysis of various wireless protocols
Wireless architecture and design
802.11 Protocol Analysis
Network Mapping and Methodology for securing wireless networks
Antenna variations
Monitoring the wireless network, including packet analysis
Various toolsets including Netstumbler, Kismet, the Aero suites and so fourth
Traffic injection tools
Spoofing
Flooding
Aircrack and Aero suite of tools
Airsnort
WEP hacking cracking
WPA, WPA2 hacking techniques
Frame generation

TT3 – The Exploit Laboratory 3.0

Trainers: Saumil Shah (Founder, Net-Square) & SK Chong (Security Consultant, Scan Associates Berhad).
Capacity: 25 Students

Outline:

Have you ever found yourself staring at a vulnerability advisory with some proof-of-concept snippets and wished the author had rather attached a working exploit with it? Have you wished you could analyze vulnerabilities and write your own exploits for them? Have you wanted to debug and exploit custom built applications and binaries? The Exploit Laboratory is an intense hands-on class for those wishing to dive into vulnerability analysis and exploit writing. The Exploit Laboratory starts off with a basic insight into system architecture, process execution, operating systems and error conditions. The class then quickly accelerates to analysing vulnerabilities with debuggers, reproducing reliable error conditions and writing working exploits for the same.

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

All this - delivered in a down-to-earth, learn-by-example methodology, by trainers who have been teaching advanced topics in computer security for over 8 years. This class is updated from the 2007 edition, featuring new content on heap overflows, abusing exception handlers and more hands-on examples based on recent vulnerabilities. The class features Mac OS X exploitation, for the first time. This class does NOT require knowledge of assembly language. A few concepts and a sharp mind is all you need.

Learning Objectives

- Understanding Error Conditions
- Types of error conditions: Stack Overflows, Heap Overflows, Format String bugs, etc.
- Process execution and memory map under Linux and Windows
- Debugging applications and sharpening debugging skills, using GDB and WinDBG
- Putting together an exploit
- Shellcode - various types of shellcode and functionality
- Crafting the attack vector and payload
- Making the exploit work reliably
- Stack overflows on Linux and Windows
- Return to stack vs. Return through registers
- Abusing Structured Exception Handlers
- Heap overflows in Linux
- Overwriting the Global Offset Table
- Heap overflows in Windows
- Format string bugs
- Browser exploitation [new]
- Using and extending the Metasploit framework [new]
- Exploits on Mac OS X [new]
- Vista exploits and defeating ASLR [new]

CONFERENCE DAY 1 - 22ND APRIL 2009

7:30 AM	**REGISTRATION**
8:50 AM	TBC - Welcome Address: H.E. Mohammed Nasser Al-Ghanim Director General of the UAE Telecommunications Regulatory Authority (TRA)
9:00 AM	**From Hacking, Startups to HackLabs: Global Perspective and New Fields** Philippe Langlois (Founder of Qualys, Intrinsec & Telecom Security Task Force (TSTF)
10:00 AM	**COFFEE BREAK**

	TRACK 1	TRACK 2
10:30 AM	**PLATINUM SPONSOR**	**Biting the Hand that Feeds You (Reloaded)** Billy Rios (Security Engineer, Microsoft Corporation)
11:30 AM	**Modern Threats and Cyberwar - Lessons Learned? Maybe Not.** Roberto Preatoni (Founder, WSLabi - The Exploit Marketplace)	**Application Defense Tactics & Strategies - WAF at the Gateway** Shreeraj Shah (Founder, BlueInfy)
12:30 PM	**LUNCH BREAK**	
1:30 PM	**Using a Dynamic (FORTHy!) Language for Shellcode** Wes Brown (Senior Security Consultant, Matasano Security)	**GOLD SPONSOR**
2:30 PM	**Honeypots and the Insider Threat** Lance Spitzner (Founder, HoneyTech)	**Psychotronica: Exposure, Control, and Deceit** Nitesh Dhanjani (Senior Manager, Ernst & Young)
3:30 PM	**NKill - The Internet Killboard** Anthony Zboralski (Founder, Bellua Asia Pacific / HERT)	**Protecting Airports and Other High Security Facilities: Security Considerations** Marc Weber Tobias (Investigative Attorney and Physical Security Specialist)
4:30 PM	**END**	

CONFERENCE DAY 2 - 23RD APRIL 2009

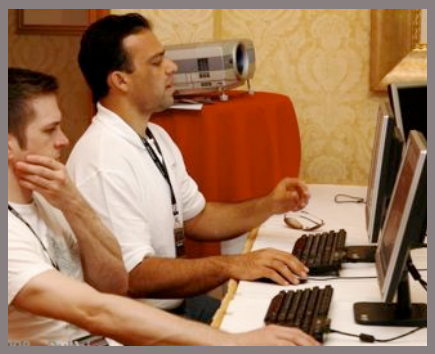
7:30 AM	**REGISTRATION**
9:00 AM	**Security Cogs and Levers** Mark Curphey (Director, Connected Information Security Group, Microsoft Corporation)
10:00 AM	**COFFEE BREAK**

	TRACK 1	TRACK 2
10:30 AM	**The Reverse Engineering Intermediate Language REIL and its Applications** Sebastian Porst (Security Consultant, zynamics GmbH)	**PLATINUM SPONSOR**
11:30 AM	**Pickpocketing mWallets: A Guide to Looting Mobile Financial Services** The Grugq (Independent Network Security Researcher)	**VBootKit 2.0 - Attacking Windows 7 via Boot Sectors** Vipin Kumar (Founder, nvLabs.in) & Nitin Kumar (Founder, nvLabs.in)
12:30 PM	**LUNCH BREAK**	
1:30 PM	**GOLD SPONSOR**	**Cross Domain Leakiness: Divulging Sensitive Information and Attacking SSL Sessions** Chris Evans (Security Lead, Google Corp) & Billy Rios (Security Engineer, Microsoft Corporation)
2:30 PM	**Telecom Infrastructure Security: the SS7 protocols** Emmanuel Gadaix (Founder, TSTF) & Philippe Langlois (Founder, Intrinsec / Qualys / TSTF)	**Advanced Payload Strategies: What's New, What Works and What Doesn't** Rodrigo Rubira Branco (Security Expert, Check Point Software Technologies)
3:30 PM	**Filesystem Forensics: Are You Pwned?** Steve Anson (Director, Forward Discovery)	**TBA** Saumil Shah (Founder, Net-Square)
4:30 PM	**END**	

Capture The Flag (CTF)

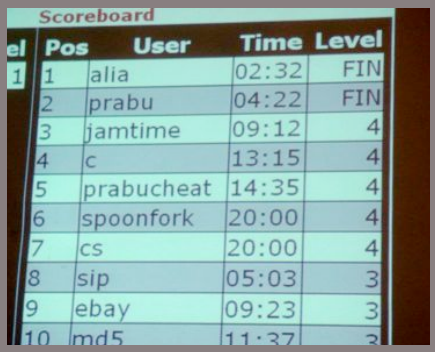
The objectives of the game is for individuals or teams of 2 participants to by pass 4 randomized web based challenges and 4 binary reversing challenges within a stipulated time frame. The top two (2) participant(s) with the fastest time in solving the 4 randomized challenges as well as the 4 binary reversing questions wins a Macbook Air sponsored by iSIGHT Partners!!!

All participants are required to BRING YOUR OWN LAPTOPS in order to play. Attack targets in the form of a centralized web server and file server will be available on-site. The servers will be made available over a Wired connection and over a 802.11 g Wireless network.



Participants should be well versed in the following areas:

- Reverse engineering
- Binary analysis
- Debugging
- SQL injection (blind / error based)
- CSS
- File Inclusion
- Cookie Hijacking


Scoreboard

Pos	User	Time	Level
1	alia	02:32	FIN
2	prabu	04:22	FIN
3	jamtime	09:12	4
4	c	13:15	4
5	prabucheat	14:35	4
6	spoonfork	20:00	4
7	cs	20:00	4
8	sip	05:03	3
9	ebay	09:23	3
10	md5	11:37	3

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

1.) Your Name + Team Mates Name

2.) Your Email Address

3.) Any questions you might have regarding the game / gameplay