

# HITB SECCONF 2011

MAY 17 - 20 @ NH GRAND KRASNAPOLSKY **AMSTERDAM**

The 2nd Annual HITB Deep Knowledge Security Conference in Europe

## MAY 17TH - 18TH

### TECH TRAINING 1

Hunting Web Attackers

### TECH TRAINING 2

The Exploit Lab: Black Belt

### TECH TRAINING 3

Windows Physical Memory  
Acquisition & Analysis

### TECH TRAINING 4

Web Hacking 2.0



## MAY 19TH - 20TH

- Quad Track Security Conference
- HITB Labs
- HITB SIGINT
- Capture The Flag World Domination
- Hacker Spaces Village & Technology Showcase
- Lock Picking Village by TOOOL.nl

## Keynote Speaker - 19th May

Joe Sullivan (Chief Security Officer, Facebook)



Joe Sullivan is the Chief Security Officer at Facebook, where he manages a small part of a company-wide effort to ensure a safe internet experience for Facebook users. He and the Facebook Security Team work internally to develop and promote high product security standards, partner externally to promote safe internet practices, and coordinate internal investigations with outside law enforcement agencies to help bring consequences to those responsible for spam, fraud and other abuse. Joe also oversees Facebook's physical security team and the company's commerce-related regulatory compliance program, and works on other regulatory and privacy-related legal issues.

## Keynote Panel Discussion - 20th May

The Economics of Vulnerabilities



Lucas Adamski  
(Director of Security Engineering, Mozilla Corp)



Chris Evans  
(Information Security Engineer, Google Corp)



Steve Adgebite  
(Senior Security Strategist, Adobe Inc.)



Aaron Portnoy  
(Manager, Security Research Team, TippingPoint / ZDI)



Dave Marcus  
(Director, McAfee / Avert Labs)



Katie Moussouris  
(Senior Security Strategist, Microsoft MSRC)

**Trading of 0-day computer exploits between hackers has been taking place for as long as exploits have existed. Projects like the Zero Day Initiative and more recently Mozilla and Google's reward programs for exploit disclosure has since created a legitimate source of income for security researchers. But what about the black market?**

## REGISTER ONLINE

<http://conference.hackinthebox.nl/hitbseconf2011ams/>

Students and members from participating hackerspaces pay EUR250. Contact your respective hackerspaces for the discount codes! Early bird registration closes on the **18th of February 2011**

# HANDS ON TECHNICAL TRAINING SESSIONS

17TH - 18TH MAY

## TECH TRAINING 1 - HUNTING WEB ATTACKERS



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

## TECH TRAINING 2 - THE EXPLOIT LABORATORY: BLACK BELT



The Exploit Laboratory Black Belt is a new and advanced class continuing from where The Exploit Laboratory left off. This class is for those curious to dig deeper into the art and craft of software exploitation and begins with a quick overview of concepts covered in The Exploit Laboratory, namely stack overflows, abusing exception handlers, heap overflows, memory overwrites, and other core concepts. We shall then focus on topics which involve breaking exploit prevention techniques like non executable stack, DEP, ASLR, etc.

## TECH TRAINING 3 - WINDOWS PHYSICAL MEMORY ACQUISITION & ANALYSIS



The aim this intensive two-day course is to convert computer science and forensics professionals into fully operational live memory analysts for the Corporate, Law enforcement and Government environments. In this technical course, attendees will learn how to use software-based acquisition methods (with MoonSols utilities such as win32dd and win64dd, and even Windows itself) and the clockwork of different full memory dump file format. The audience will also learn the difference between hardware and software acquisition methods and how to do advanced analysis on these dumps.

## TECH TRAINING 4 - WEB HACKING 2.0



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 for pen-testers, consultants, auditors and QA teams. Web Hacking 2.0 is extensively hands-on class with real life challenges and lab exercises. Participants would be methodically exposed to various different attack vectors and exploits. The learning sessions feature real life cases, hands one exercises, new scanning tools and exploits.

# OTHER CONFERENCE HIGHLIGHTS

19TH - 20TH MAY

## HITB LABS & HITB SIGINT

First introduced in 2008, the HITB Labs form the third track in our quad-track line up. Catering for only 60 attendees, these sessions are intensive, hands-on presentations that require audience interaction so please bring your own laptops if you intend to attend. Seats are given out on a first come first serve basis so be sure to be at the room at least 10 minutes before the session commences.

The HITB SIGINT (Signal Intelligence/Interrupt) sessions are designed to provide a quick 15 minute overview for material and research that's up and coming – stuff that isn't quite ready for the mainstream tracks of the conference but deserve a mention nonetheless. These session are not only for seasoned security professionals but is also open to all final year students based in The Netherlands or around Europe who want to present their projects to industry experts and the security community.

## LOCK PICKING VILLAGE BY TOOOOL.NL

Set up and run by members from the The Open Organization of Lockpickers (TOOOOL Netherlands), attendees to this year's event will get a chance to try their hand at picking, shimmying, bumping, safecracking, and other physical security attacks. It has always been customary for TOOOOL-sponsored physical security sessions to offer some degree of audience interaction and hands-on training. Sometimes this has taken the form of publicly-submitted locks being given on the spot security analysis, other times members of the general public with no lock-picking experience have been invited to attempt a bypass in order to demonstrate its ease.

## CAPTURE THE FLAG - WORLD DOMINATION

Capture The Flag – World Domination is an attack only competition set up and run for the very first time by the HITB.nl CTF Crew! The game mimics real world scenarios and events, bringing the technical attack fun of hacking into the competition. For the first time ever, the CTF introduces a new section, hardware hacking and lock picking! Whether it is to lock pick a simple lock to get a flag, to exploit a certain binary or a need to bypass the encryption on a embedded system, this game will make even the most elite "hackers" sweat. There are over 30+ flags to capture and flag points decrease after each submission. Fastest player to submit a flag gets more points compared to the next player. The winner is determined by who ever has the most points.

## HACKERSPACES VILLAGE & TECHNOLOGY SHOWCASE

Free and open to public, attendees to the Hackerspaces Village will get an inside look at hackerspaces, their community, projects and even get their hardware hack-on! In the village you will find representatives from the various .EU and Netherlands based hackerspaces who will be on site showcasing their projects. Each hackerspace will also present in the HITB SIGINT session highlighting the details of their current projects or developments. Alongside the hackerspaces, CTF and Lock Picking Village, there will also be a technology showcase of next generation network security technology, products and solutions.

