



H@cker Halted TM **Asia Pacific**
2011
- Malaysia -

InterContinental Kuala Lumpur
15 - 17 November 2011

STOP the Data Leaks.
SECURE the Code.



H@cker Halted™

Asia Pacific
2011
- Malaysia -

EC-Council Asia Pacific

Level 3-10, Block F,
Phileo Damansara 1,
Jalan 16/11,
Off Jalan Damansara,
46350 Petaling Jaya,
Selangor D.E.
MALAYSIA.
T: (60)3.7665.0911
F: (60)3.7665.2022
enquiry@eccouncilapac.org
www.eccouncilapac.org

About Hacker Halted Asia Pacific 2011

Presented by EC-Council, the objective of the global series of Hacker Halted conferences is to raise international awareness towards increased education and ethics in Information Security.

This conference series has grown to become a significant event for the information security community as it covers a variety of critical domains within information security, and addresses current critical threats and development.

Hacker Halted aspires to be a complete and comprehensive Information Security conference and Information Security workshop that will educate and equip its participants with the in-depth knowledge of understanding the threats and countermeasures to needed overcome information security vulnerabilities present today.

The Hacker Halted conference series is aimed at providing the opportunity to CEOs, COOs, CIOs, CFOs, Senior IT Professionals and all other decision makers to assess the best practices in acquiring, implementing, managing and measuring information security.

The event covers in-depth topics into various security issues plaguing the world. In addition to highlighting current digital security threat, renowned speakers and industry experts will also discuss the various means of protection and countermeasures in dealing with the digital threats.

Since 2004, Hacker Halted has been organized in many cities around the world, including Miami, Mytle Beach, Kuala Lumpur, Singapore, Dubai, Mexico City, Cairo, Taipei, Guangzhou and Tokyo.

STOP the Data
Leaks.

SECURE the
Code.





Delegate Mix

The topics within Hacker Halted conference are targeted to specific key personnel within an organization and also between different industries. The security measures of the banking industry differ from the security needs of small-medium enterprises. This is to ensure all industries meet their specific needs and expectations for maximum consumption of relevant knowledge and skills. Therefore, we will have a good mix of delegates.

Key Executives - CEO, CIO, CTO, CISO **40%**

Technical Specialist, Researchers, Engineers **30%**

IT Managers, IT Directors **20%**

Others, Academics **10%**



Who should attend?

Executive Management

The management of most organizations is looked upon for guidance and directions. Having said that, as security is the main concern of all organizations, it is highly important that key management members are aware of the risks to their organizations whilst implementing appropriate measures and directives. And to be able to implement all of that within a certain range to ensure maximum return of investment.

CEOs, CIOs, CSOs, CTOs, Head of Departments, Auditors, Technologist

Technical Specialist

This category includes IT network and system managers, application information administrators, developers, security auditors, "power users" (end-users who develop and share spreadsheet and database applications etc.) and various others.

Key IT Networking staff, IT Managers, IT Directors

The Top 10 reasons why you should attend Hacker Halted Asia Pacific 2011

- Participate and be part of one of the most recognized information security events.
- Gain perspective through keynote addresses on the current state of information security as well as emerging trends and threats.
- It has a comprehensive agenda. Choose from the various workshop covering critical domains of information security.
- Match your information and learning needs, and learn how to address everyday challenges.
- Expand and empower your own information security knowledge.
- Gain valuable insights from networking by sharing information.
- Be among the first to learn about the latest products, meet with potential clients and generate new business with valuable leads.
- Discover and evaluate new technology, products and services that are being showcased.
- Share the platform with some of the best and brightest of your profession.
- Networking opportunity with the best subject matter experts in person and exchange your experiences.

Hacker Halted Conference

Day-1 : 15 Nov 2011

NIGHT HACK LIVE

Meet the top hackers and experience the coolest ethical hacking demonstration in town!
7 - 10pm

Exclusively FREE for Hacker Halted Asia Pacific 2011 participants only!

Hacker Halted Workshop

Day-2 : 16 Nov 2011

Day-3 : 17 Nov 2011



INTERCONTINENTAL KUALA LUMPUR 15 - 17 NOVEMBER 2011

For more information, please contact
Nicholas @ (603) 7665 0911 or
e-mail to enquiry@eccouncilapac.org

HACKER HALTED ASIA PACIFIC

Level 3-10, Block F,
Phileo Damansara 1,
Jalan 16/11, Off Jalan Damansara,
46350 Petaling Jaya,
Selangor D.E.

Registration. Let's Get Started!



Largest Hacker Halted Crowd We Had in Asia Pacific with Over 500 Participants!



Lively and Interactive Conference



Live Hacking Demonstration in Night Hack Live



Highly Technical Hands-on Workshop



World Class Ethical Hackers On Board



The reunion of Certified Ethical Hackers



AGENDA

Conference

Time	Topic
09.00am	Opening
09.15am	Welcome and Opening Keynote: Defending the Frontier 3.0 <i>Presenter: Jay Bavisi</i>
10.00am	Morning Refreshment
10.30am	I built what? - Why The Bad Guys Do It Better <i>Presenter: Sean Bodmer</i>
11.15am	Advanced Forensics Analysis - Why Reverse Engineer? <i>Presenter: Wayne Burke</i>
12.00pm	And you will know us by the trail of our logs Malware research and analysis using logs <i>Presenter: Zachary Wolff</i>
12.45pm	Lunch Break
01.45pm	Web Shellz: SQL Injection, and Cross-Site Scripting is Boring - Gimme a command prompt <i>Presenter: Joe McCray</i>
02.30pm	Transparent Botnet Command And Control for Smartphones Over Sms <i>Presenter: Georgia Weidman</i>
03.15pm	Taking On Advanced Persistent Threats <i>Presenter: Kevin Cardwell</i>
04.00pm	Afternoon Refreshment
04.30pm	Panel Discussion
05.15pm	Secrets to Hacking: The Challenges, Risks and Rewards <i>Presenter: Haja Mohideen</i>
06.00pm	Closing Keynote: 9/11: Ten Years Later (How Crisis Intervention and Planning Affect Secure Infrastructures) <i>Presenter: Drew Williams</i>
06.30pm	Break (Dinner is not included)
07.30pm	Night Hack Live
10.00pm	End

Note:

Topics and times in the agenda are tentative and subject to change.

STOP the Data Leaks. SECURE the Code.

Workshop

- Workshop 1:
Crash Course in Penetration Testing
- Workshop 2:
Network Defense
- Workshop 3:
Crimeware Attribution
- Workshop 4:
Web Application Security

Day 1

Time	Topic
08.30am	Registration
09.00am	Session 1
10.30am	Morning Break (30 mins)
11.00am	Session 2
12.30pm	Lunch (60 mins)
01.30pm	Session 3
03.30pm	Afternoon Break (30 mins)
04.00pm	Session 4
05.30pm	End

Day 2

Time	Topic
09.00am	Session 5
10.30am	Morning Break (30 mins)
11.00am	Session 6
12.30pm	Lunch (60 mins)
01.30pm	Session 7
03.30pm	Afternoon Break (30 mins)
04.00pm	Session 8
05.30pm	End

Workshop 1: Crash Course in Penetration Testing

Date: 16 - 17 November 2011

This course will cover some of the newer aspects of penetration testing such as Open Source Intelligence Gathering with Maltego and other Open Source tools.

Advanced Scanning, Enumeration, Exploitation (remote and client-side), and Post-Exploitation relying heavily on the features included in the Metasploit Framework will also be covered.

Emphasis throughout the entire workshop will be placed on being as stealthy as possible, and dealing with popular defensive technologies such as:

- Network Intrusion Detection/Prevention Systems
- Host-Based Intrusion Detection/Prevention Systems
- Web Application Firewalls
- Anti-Virus
- Content-Filtering Proxies

Web Application penetration testing will be covered as well with focus on practical exploitation of cross-site scripting (XSS), cross-site request forgery (CSRF), local/remote file includes, and SQL Injection.



Trainer: Joseph McCray

DAY ONE

Penetration Testing Fundamentals

Scope of Modern Pentests

The Down & Dirty

Open Source Intelligence (OSINT)
Scanning
Enumeration
Vulnerability Testing

Owning Boxes for Fun and Profit

Exploitation
Post-Exploitation (Old School)
Metasploit (MSF)

DAY TWO

Transitioning from Network to Web App Penetration Testing

What Makes up a Web Application Assessment

Injection Vulnerabilities

Abuse of Trust Vulnerabilities

File Handling/Redirection Vulnerabilities

Filter/IDS/Web Application Firewall Evasion

* Topics are tentative and are subject to change

For further information,
please e-mail to
enquiry@eccouncilapac.org
or contact
Ven Ping at
(603) 7665 0911

Workshop 2: Network Defense

Date: 16 - 17 November 2011

In this course, you learn how to analyze risks and deploy the appropriate countermeasures to reduce your exposure to network threats. The course consists of hands-on labs to learn the concept of basic network filtering and "sanity" checking at the perimeter. The course will consist of learning the main components of the security model, and then how to mitigate and reduce the risk of each attack method. In the course the student will learn how to deploy cryptography to assist in the securing of the network. The course will cover the essential steps you need to apply at the host machine. Additionally, the course will focus on the top mitigation techniques and strategies to implement and reduce the chance of a compromise. It is estimated that 85% of the publicized attacks in 2010 would have not been successful if these top mitigation techniques were deployed.

The students will learn the components and requirements of a robust Vulnerability Management program, and practice these components in hands-on labs. Vulnerability ratings are generic as the tool creator does not know your network, so the severity rating might be either higher or lower depending on each organizations security architecture; therefore, the course will cover the process of calculating vulnerability severity and tailoring a publicized vulnerability score to a score more realistic based on the network environment.



Trainer: Kevin Cardwell

DAY ONE

Introduction to Network Defense

LAB: Security Model
LAB: Allowing a Service

TCP/IP 101

LAB: TCP/IP

Introduction to Hacking

LAB: Hacking

Vulnerability Management

LAB: Vulnerability Assessment
LAB: Vulnerability Severity

DAY TWO

Basic concepts of Filtering and Best Practices

LAB Basic Filtering

Cryptography as a Defense

LAB Algorithms
LAB Hashing
LAB Remote Access

Deploying Countermeasures

LAB Deploying Countermeasures
LAB Application Whitelisting

Host Based Protection

Introduction to Concepts of Advanced Defense

* Topics are tentative and are subject to change

For further information,
please e-mail to
enquiry@eccouncilapac.org
or contact
Ven Ping at
(603) 7665 0911

Workshop 3: Crimeware Attribution

Date: 16 - 17 November 2011

It is more important to understand the 'who' and 'why' behind any intrusion within your enterprise. Tracking down and pursuing threats in a manner as to better understand and characterize their level of threat. In this course you will walk through numerous criminal groups and their various skill levels, capabilities, motivation, and resources. You will walk away with not only additional knowledge of criminal groups, but their capabilities, crimeware families, criminal tools, and how to trace back the threat to determine their level of capabilities. This course will also cover some tools and tactics any security professional or intelligence analyst can use to engage specific threats that are targeted in nature. These skills are right from the team who co-authored the content in the upcoming book "Tradecraft: Countering Cyber Espionage and Advanced Cyber Threats" published by McGraw-Hill Professional Press.



Trainer: Sean Bodmer

DAY ONE

- Introduction & State of the APT
- History of Deception
- Cyber Counterintelligence
- History of Criminal Profiling
- Legal & Ethical Aspects on Deception
- Attack Tradecraft- Hackers use to enter your network
- Operational Deception, Misinformation & Disinformation

DAY TWO

- Tools, Tactics, and Procedures
- Attack Attribution
- Attribution
- Understanding Advanced Persistent Threats (APT)
- "When" and "When, not to act"
- Implementation & Validation

* Topics are tentative and are subject to change

For further information,
please e-mail to
enquiry@eccouncilapac.org
or contact
Ven Ping at
(603) 7665 0911

Workshop 4: Web Application Security

Date: 16 - 17 November 2011

This is a revolutionary web application hacking workshop with complete hands-on experience, covering the entire process of hacking web applications inside out.

The workshop aims to provide developers and programmers the best understanding on web application security, with in depth experimentation on the important aspects in web application such as application mapping authentication, access control, injection flaws and advanced exploitation.

Participants learn the essential knowledge on web application security testing and all the advanced techniques for finding and countermeasures security threats in applications.

Scope of Training Includes:

- Anatomy of cross-site scripting attack
- SQL Injection vs Oracle, MySQL and MSSQL
- Authenticating the non-authenticable
- Interpreting the injections (LDAP, XPath, SOAP and other injection)
- And more...



Trainer: Wayne Burke

DAY ONE

Web Application Intro

HTTP Protocol Basics
Cookies
Sessions

Information Gathering

Gathering Information on target
Infrastructure
Fingerprinting Framework and
Applications

Vulnerability Assessment

Nessus
Nikto

DAY TWO

XSS

Cross Site Scripting
Anatomy of a XSS exploitation
The Three Types of XSS
Finding XSS

SQL Injection

Introduction to SQL injection

* Topics are tentative and are subject to change

For further information,
please e-mail to
enquiry@eccouncilapac.org
or contact
Ven Ping at
(603) 7665 0911

Hacker Halted Asia Pacific 2011 Speakers



Zachary Wolff

Zachary Wolff currently spends his days deploying and tuning SIEM solutions for LogRhythm, Inc. When he's not busy with that you will find him sifting through an ever-growing log collection in search of new and interesting attack patterns. Prior to LogRhythm, Zachary spent three years on the Threat Research team at Webroot Software, researching malware and special projects.



Wayne Burke

The CSO for Securit CSI, holds responsibility for the technical realm and security management, which includes consulting teams. He is a captain of a global operating group of penetration testers and security experts. Wayne and his group have delivered security assessments, Penetration Test assignments and customized training for International Corporations and many Government Agencies such as: EPA, FAA, DOJ, DOE, DOD + 8570: Air force, Army, Navy, Marines, FBI and Statewide Law Enforcement Offices in the USA.

Wayne's consulting and training undertakings cover specializing in Penetration Testing, Forensics, Security Expert Advisor and secure infrastructure design. His expertise include DMZ firewalls, Secure VPNs, EAP/TLS, PEAP, SSL, PKI, Smart Cards, Biometrics, IPSEC, IDS, Vulnerability Scanners, AV, Honey Pots, Audits, filtering policies, multi-layer encrypted file systems, patch management and deployments.

His experience in the public / defense sectors is equally complemented by assignments undertaken for heavyweight world renowned corporations including Yahoo, Xerox, AT&T and Texas Instruments to name but a few. He is imminently qualified in his field in that he holds a string of professional qualifications in Networking to name a few (MCT, MCSE, Cisco, Network+) and IT Security (CIW-SA, Security+, CEH, ECSA, LPT, CHF) besides a bachelor's degree in science.



Sean M. Bodmer

Sean is an active Threat Intelligence Analyst at Damballa specializing in the analysis and attribution of signatures and behaviors used by cyber criminal operators and malware purveyors. Sean focuses his time learning the tools, techniques, and procedures behind attacks and intrusions related to various advanced and persistent threats. Sean has worked in several Information Systems Security and cyber counter-intelligence roles for various firms and customers over the past fourteen years across United States. Most notably he has spent several years performing intrusion, and intruder analysis/attribution for Fortune 100, Defense Department, and 'other' Federal Agencies and has shared numerous accounts of his findings at various Industry conferences relating to the inner-workings of advanced and persistent

threats. Sean has lectured at several Industry conferences over the years such as Defcon, PhreakNIC, DC3, NW3C, Bluehat, Hacker Halted, ISSA, MAAWG, and CERT/CC discussing his interest in analyzing, understanding, and manipulating the minds and morale of persistent threats without their knowledge.



Joe McCray

Joe McCray is an Air Force Veteran and has been in security for over 10 years. Joe has been involved in over 150 high level penetration testing engagements and has some major hacking accomplishments that he can share with his students and clients. His extensive experience and deep knowledge, mixed with his comedic style has lead Joe to be one of the most highly sought after speaking experts in the industry. Joe makes speaking appearances and gives seminars at major events in the security community such as Black Hat, DefCon, BruCon, Hacker Halted and more. Joe is the recipient of the 2009 EC-Council Instructor Circle of Excellence Award and the 2010 EC-Council Instructor of the Year Award.



Georgia Weidman

Georgia Weidman is a penetration tester and independent security researcher. She is the Director of Cyberwarfare at Reverse Space, a hacker space in the Washington, DC area. She holds a M.S. in Secure Software and Information Security, an Associate CISSP, and Offensive Security Certified Professional (OSCP) certification. She got her start in security as a team captain in the Collegiate Cyber Defense Competition, and now she serve as an attacker in the Mid-Atlantic region. She run GRM n00bs (<http://www.grmn00bs.com>) a website dedicated to videos, tutorials, and podcasts for information security beginners. Aside from security, she work in A/V particularly making security conference videos, and photography.



Kevin Cardwell

Kevin Cardwell spent 22 years in the U.S. Navy, during this time he tested and evaluated Surveillance and Weapon system software, some of this work was on projects like the Multi-Sensor Torpedo Alertment Processor (MSTRAP), Tactical Decision Support System (TDSS), Computer Aided Dead Reckoning Tracer (CADRT), Advanced Radar Periscope Discrimination and Detection (ARPDD), and the Remote Mine Hunting System (RMHS). He has worked as both software and systems engineer on a variety of Department of Defense projects and early on was chosen as a member of the project to bring Internet access to ships at sea. Following this highly successful project he was selected to head the team that built a Network Operations Center (NOC) that provided services to the commands ashore and ships at sea in the Norwegian Sea

and Atlantic Ocean. He served as the Leading Chief of Information Security at the NOC for six years prior to retiring from the U.S. Navy. During this time he was the leader of a 5 person Red Team that had a 100% success rate at compromising systems and networks.



Haja Mohideen

Haja is the Co-Founder and currently the Technical Director of EC-Council. He manages the certifications and training programs for EC-Council. Mr Mohideen is well-known as the creator of popular certification programs such as the CEH, CHFI, ECSA/LPT and ECSP. With more than 17 years of experience specializing in the development, support and project management of PC software and hardware in distributed computing environment, he has trained various Fortune 500 companies as well as US government agencies.

The Premier Information Security Conference of The Year in Asia Pacific

Hacker Halted Asia Pacific 2011 is a comprehensive hacker conference covering a broad topic area to provide IT professionals a platform to understand and discuss today's information security environment. Unlike any other hacker conferences, **Hacker Halted Asia Pacific 2011** covers real information security issues and discusses solutions that fit into global security attacks scenarios, and sheds light on how to deal with increasing threats, compliance as well as regulatory issues.

Hacker Halted Asia Pacific 2011 will be the 21st iteration of global successful series and 6th in Malaysia.

Throughout the series, **more than 400 international cyber security experts** presented in Hacker Halted and attracted **over 10,000 information security professionals** across the world.

Additional privileges:

NIGHT HACK LIVE

Hackers Are Here. Where Are You?

No one is immune to hacking.
Businesses and individuals alike.

Falling prey to an attack can involve
serious consequences.

Have you ever wondered what can be
hacked?

Now in Kuala Lumpur - See the top
hackers demonstrate hacking "live"
with the latest tools and
methodologies!

