



ISACA Hawaii Presents “StrawHat 2006”

THE HAWAII ISACA CHAPTER IS OFFERING A TWO-DAY SEMINAR COVERING SOME OF TODAY'S HOT IT SECURITY TOPICS. THIS UNIQUE TWO-DAY EVENT WILL LEAD PARTICIPANTS THROUGH A DETAILED OVERVIEW OF THE INFORMATION SECURITY AUDIT PROCESS AND WILL PROVIDE PARTICIPANTS WITH THE OPPORTUNITY TO APPLY NEWLY ACQUIRED SKILLS IN A HANDS-ON ENVIRONMENT.

Topics Covered:

July 20th:

Users Guide to Effectively Managing a Penetration Test.

July 21st:

Understanding the Techniques Employed by Today's Security Professionals

By:



Registration Deadline: Friday July 12, 2006

Please make checks payable to the Information System Audit and Control Association – Hawaii Chapter. ▶▶▶

Who Should Attend:

- IT auditors
- Internal Audit Directors
- CIO & CISOs
- System administrators
- Security personnel
- Ethical hackers/penetration testers who want to understand the concepts underlying their testing regimen

Fees: Members: \$ 150 per day.

Non-Members: \$ 160 per day.

Send Reply and Payment by check to: Kate Patterson C/O Bank of Hawaii – 130 Merchant St. cc309, Honolulu, HI 96846 by July 12, 2006. Cancellations received before July 17th, 2006 will be charged a \$25 cancellation fee. No refunds for cancellations occurring after July 17th; a substitute may attend in the place of a pre-registered attendee. If you have any questions, please email Kate:

kpatterson@boh.com



CPE Credits: 12



Event-@-a-Glance

Time	Tuesday July 20	Topics	Wednesday July 21	Topics
8:30-9 AM.	Users Guide to Effectively Managing a Penetration Test	Registration	Understanding the Techniques Employed by Today's Security Professionals	
9-9:15		Introduction		Introduction
9:15-10:15		Policy/Procedure		Reconnaissance
10:15-10:30		Break		Break
10:30-11:45		RFP/Selection		Scanning
11:45-1 PM.		Lunch		Lunch
1-2		Scoping		General Attacks
2-2:15		Break		Break
2:15-3:15		Project Management		Network Attacks
3:15-3:30		Break		Break
3:30-4:30		Reporting		Web App Attacks
4:30-5:00		RFP Lab		Hands On Analysis

Day One

Day one will address the business aspects related to the successful organization and management of a penetration test and will provide participants with the opportunity to walk through portions of the Request for Proposal (RFP) process.

- ∞ Developing a specific, customized RFP for a 3rd party assessment
- ∞ Project Risk Management
- ∞ Vendor evaluation and selection (skills, tools, methodologies, etc.)
- ∞ Managing the assessment (and the vendor) and communication
- ∞ Reviewing, agreeing on, and finalizing findings (content and format)
- ∞ Correlating findings to business risk and root cause
- ∞ Packaging and presenting findings for executive management

Recommended

As a best practice, there should never be sensitive data stored on a system used for audit/testing. ISACA, all other sponsors, and the trainers and facilitators cannot accept any responsibility for any data housed on the systems used for training.

Venue:

The Plaza Club

900 Fort Street, Pioneer Plaza,
Suite 2000
Honolulu, HI 96813
Phone: (808) 521-8905

Continental Breakfast and Lunch
Buffet included

Thursday July 20, 2006 and Friday
July 21, 2006

Registration 7:30 A.M.

Session 8:00 A.M. to 4:30 P.M.

Laptop Requirements:

BRING YOUR OWN LAPTOP WITH
WINDOWS AND LINUX

Or, a Windows Laptop and,
Burn a bootable image
of Backtrack found @

http://www.remote-exploit.org/index.php/BackTrack_Downloads





Event-@-a-Glance

Time	Tuesday July 20	Topics	Wednesday July 21	Topics
8:30-9 AM.	Users Guide to Effectively Managing a Penetration Test	Registration	Understanding the Techniques Employed by Today's Security Professionals	
9-9:15		Introduction		Introduction
9:15-10:15		Policy/Procedure		Reconnaissance
10:15-10:30		Break		Break
10:30-11:45		RFP/Selection		Scanning
11:45-1 PM.		Lunch		Lunch
1-2		Scoping		General Attacks
2-2:15		Break		Break
2:15-3:15		Project Management		Network Attacks
3:15-3:30		Break		Break
3:30-4:30		Reporting		Web App Attacks
4:30-5:00		RFP Lab		Hands On Analysis

Day Two

Day two will focus on the technical aspects of an actual assessment including an overview of today's top vulnerabilities and a demonstration on how to leverage tools that can be used to evaluate your level of risk. Participants will be able to apply this knowledge in a lab environment at the end of the session.

1. Reconnaissance

Reconnaissance enables attackers to create a complete profile of an organization's security posture. By using a combination of readily available tools and technique, attackers can reduce an unknown quantity of the organization's external connections to a specific range of domain names, network block, and individual IP addresses. This is achieved using tools such as Whois Lookups, ARIN, RIPE and APNIC, Google Hacking, Data Gathering from Job Postings, Web Sites and Government Data bases

2. Scanning

The Art of War Driving to Locate Unsecure Wireless LANs
 War Dialing for Renegade Modems
 Port Scanning: Traditional, Stealth and Blind Scanning
 Active and Passive Operating System Fingerprinting
 Firewalking to Determine Firewall Filtering Rules
 Vulnerability Scanning Using Nessus and Other Tools
 CGI Scanning with Whisker

3. Network-Level Attacks

Some of the most common network attacks include:
 Session Hijacking, Person-in-the-Middle Attacks
 Passive Sniffing

4. General Exploits

Some of the most common exploits include:
 IP Spoofing, Session Hijacking, Buffer Overflows
 Password Cracking using John the Ripper Password Cracker & L0pht Crack, File and Directory Hiding on Windows and Linux

5. Web Application Attacks

Some of the most common Web App attacks include:
 Account Harvesting, SQL Injection: Manipulating Back-end Databases, Session Cloning: Grabbing Other Users' Web Sessions