

# Rediscover Security.



Illuminate your mind. Gain knowledge. Learn the threats of tomorrow, today.  
Be challenged by the experts who are doing innovative work. Meet and network with thousands of your peers from all corners of the world at the Black Hat Briefings USA 2004—the only technical security event to offer you the best of all worlds.



## Black Hat®

**Briefings & Training USA 2004**

July 24-29, 2004 • Caesars Palace Las Vegas

Training: 4 days, 22 topics • Briefings: 2 days, 9 tracks, 60 speakers

[www.blackhat.com](http://www.blackhat.com)

for updates and to register or call +1.916.944.4112



## Black Hat®

Briefings & Training USA 2004

Black Hat, Inc. • 2606 Second Avenue, #406 • Seattle, WA 98121 • [www.blackhat.com](http://www.blackhat.com)

### The World's Premier Technical Event for IT and Network Security Experts

- Held at the world renowned Caesars Palace Hotel from July 24-29, 2004
- **Early Bird Discount** closes July 1 – register early to receive the best rates. Use the discount code **PV04** to receive an additional discount.
- **Gain insights** from 60 speakers, including underground security specialists
- **Networking opportunities** with 2,000 of your peers from over 30 nations

[www.blackhat.com](http://www.blackhat.com)

## diamond sponsor



**BindView** is a leading provider of proactive business policy, IT security and directory management software worldwide. Our solutions enable customers to centralize and automate policy compliance, vulnerability assessment, directory administration and migration across the entire organization. Customers benefit from reduced risk and improved operational efficiencies with a verifiable return on investment. The BindView advantage? From a single console, administrators can audit, secure and manage operating systems, applications and directories. The software suite also provides in-depth auditing and reporting, as well as closed-loop problem identification and remediation, automating many tasks and allowing administrators to efficiently and securely manage the IT environment. [www.bindview.com](http://www.bindview.com)

## platinum sponsors

**Qualys** is the market-leading Web Service Provider offering on-demand Network Security Audits and Vulnerability Management. Qualys enables large and small organizations to manage security from an attacker's perspective and fix real-world weaknesses before they are exploited.

Qualys' Web services are used simultaneously by executives and technicians to measure security effectiveness, enforce security policy, and comply with regulations. Thousands of customers rely on Qualys, including Hershey Foods, Hewlett Packard, and The Thomson Corporation. Qualys is headquartered in Redwood Shores, California, with global offices in France, Germany and the U.K. [www.qualys.com](http://www.qualys.com)



**NetIQ** is a leading provider of Systems & Security Management and Web Analytics solutions.

NetIQ's Security Management and Content Security solutions help customers assure the rapid and efficient identification of, reduction of and response to risks, vulnerabilities and threats across their enterprise. Unique to the industry, NetIQ provides closed-loop security management by bringing together event detection and management, vulnerability and patch management and content security solutions that deliver unmatched breadth and depth of automated security and protection. [www.netiq.com](http://www.netiq.com)



## gold sponsors

**Cisco Systems** is the worldwide leader in networking for the Internet. Cisco hardware, software and service offerings are used to create Internet solutions so that individuals, companies, and countries have seamless access to information regardless of differences in time and place. News and information are available at [www.cisco.com](http://www.cisco.com)



**Configuresoft** provides the world's leading companies with software for maintaining granular, end-to-end control over system configurations on Windows-based servers, desktops, and mobile systems. Eight of the 25 largest companies in the world use Configuresoft software to address configuration management challenges and enforce compliance with their security and IT standards. Configuresoft is privately held and headquartered in Colorado Springs, CO. [www.configuresoft.com](http://www.configuresoft.com)



**Sana Security** develops and markets host-based intrusion prevention software (HIPS) that provides the most accurate, automated and effective detection and prevention of attacks for standard, complex and custom server applications on major platforms. Developed to commercialize breakthrough Sana Adaptive Profiling Technology (SanAPT) developed by founder Dr. Steven Hofmeyr, Sana Security's first product, Primary Response, protects the broadest range of platforms and applications, and requires fewer resources to manage, deploy and scale by eliminating the need for constant updating and management by security experts. [www.sanasecurity.com](http://www.sanasecurity.com)



## silver sponsors



Black Hat returns to the fabulous Caesars Palace Hotel in action-packed Las Vegas. Leave your business attire at home. Dress is casual, promoting a great learning environment for all delegates.

What we are offering this year:

- Wireless 802.11b access during the Briefings
- One-on-one access to our sponsors' senior technical executives, the top security products and consultancies in the world. Get tailored security solutions on the spot.
- A copy of *Security Assessment Case Studies for Implementing the NSA IAM* by Russ Rogers, Greg Miles, Ed Fuller, and Ted Dykstra.
- Breakpoint Books, our official bookseller, will be on hand and stocked with the latest books in security.
- An additional 2 tracks to make this the largest Black Hat event ever.
- Free admission to DEFCON for paid Black Hat delegates.

## Venue

### Caesars Palace Las Vegas

Address: 3570 Las Vegas Blvd South, Las Vegas, NV 89109  
Telephone: +1 702 731 7110 or toll free +1 800 634 6661 • Facsimile: +1 702 866 1700  
Reservations: +1 800 634 6661 Don't forget to mention **BLACKHAT** to get the group rate  
Deluxe: \$135 single/double per night • Palace Tower: \$169 king per night (these rooms are closest to the Conference Area)

## about Black Hat

### Black Hat Briefings

These sessions are intense, informative and cutting-edge, with no vendor sales pitches! Utilizing a proven track format, you'll be propelled to the front lines of security, where exploits and solutions are discussed, reviewed and even discovered onsite. Many speakers will profile never-before-shown tools and techniques.

### Black Hat Training

Black Hat Training has been offering world-class training around the world. Black Hat Training can explain even the most complicated security issues to any member in your organization in an effective, professional manner. Whether it is the network administrator or the CEO, the knowledge exchange can be tailored to your environment. When performing risk assessments, a most critical factor is to understand the threats so that a proper defense can be created.

### Black Hat Consulting

Black Hat Consulting was founded in 2000 to offer the best-of-breed services direct to you from the industry leaders who have developed them. Our Training and Consulting divisions address the global challenge of assuring that information in any form stays safe while providing access to it for business-critical needs. Escalating privacy issues are another major concern for many organizations; network security is a critical function in most businesses today. In every case, proper awareness is the key to maintaining a proper security posture. Chance favors the well prepared mind.

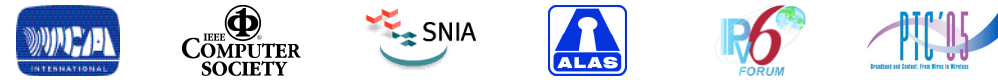
Black Hat Consulting brings world-class experts together to offer the final word in information security. Black Hat Services have been designed by thought leaders to protect and defend your infrastructure and to insure that your information stays safe. If an incident has already occurred, we can advise and assist. Black Hat Consulting also has unprecedented access to industry leaders who work with us on custom projects. Our staff is handpicked and extremely dynamic. Black Hat is synonymous with excellence in the security industry.

For more information, please visit our website at [www.blackhat.com](http://www.blackhat.com) or contact us via email at [info@blackhat.com](mailto:info@blackhat.com).

# A World Of Support

Black Hat's support within the security industry is unmatched by any other event. We gratefully acknowledge the participation of these organizations. You can pick up sample copies and information about them onsite at our Media Center!

## supporting organizations



## book sponsor SYNGRESS®

## lead print media partner CYBERDEFENSE

## e-newsletters & portals



## print publications



"Within seconds of getting to Black Hat I remember that this is not a normal security conference"

—Bruce Schneier, CTO, Counterpane Internet Security

## registration information

FEES:	on or before July 1	after July 1
<b>briefings</b>		
● Black Hat Briefings	\$1,295	\$1,495

Register with the discount code **PV04** and receive \$100 off the Briefings rate

## training

● Analyzing Software for Security Vulnerabilities	\$1,800	\$2,000
● Aspects of Offensive Root-kit Technology	\$1,800	\$2,000
● Designing A Secure Web Application	\$1,800	\$2,000
● Discover the Hidden: Steganography Investigator Training	\$2,000	\$2,200
● Enterprise Security: A Practical Approach to Developing an Information Security Program	\$1,800	\$2,000
● Hacking by Numbers: Bootcamp	\$2,200	\$2,400
● Hacking by Numbers: Chief of Staff	\$2,200	\$2,400
● Hacking by Numbers: Combat	\$2,200	\$2,400
● Hacking into a Cisco Network	\$2,000	\$2,200
● Intermediate Digital Forensics: Civil Litigation Matters	\$1,800	\$2,000
● Internal Security Threats: Identification and Prevention	\$2,000	\$2,200
● Microsoft Ninjitsu	\$2,000	\$2,200
● Network Application Design	\$1,800	\$2,000
● NSA InfoSec Assessment (IAM) - Level 1	\$1,600	\$1,800
● NSA InfoSec Evaluation (IEM) - Level 2	\$2,000	\$2,200
● OSSTMM Professional Security Analyst	\$1,900	\$2,100
● Securing Solaris & Locking Down Linux	\$2,000	\$2,200
● Ultimate Hacking: Black Hat Edition	\$2,000	\$2,200
● Ultimate Hacking: Expert	\$2,000	\$2,200
● Voice Over IP	\$2,000	\$2,200
● Web Applications: Attacks & Defense- Advanced Edition	\$2,000	\$2,200
● Windows Web Application Hacking	\$1,700	\$1,900

### FOUR EASY WAYS TO REGISTER:

<b>ONLINE:</b>	www.blackhat.com
<b>MAIL:</b>	Convention & Meeting Services P. O. Box 740 Fair Oaks, CA 95628-0740
<b>PHONE:</b>	+1.916.944.4112
<b>FAX:</b>	+1.916.944.3126

To register via fax or mail, please print and complete the online registration form at [www.blackhat.com](http://www.blackhat.com)

[WWW.BLACKHAT.COM](http://WWW.BLACKHAT.COM)

# briefings

Partial schedule shown. Go to [www.blackhat.com](http://www.blackhat.com) for complete schedule, session descriptions and to register.

At the Black Hat USA 2004 Briefings you will be placed right on the front lines. Spanning two days with nine separate tracks, our speakers will be releasing current "never before seen" tactics and tools. The sessions are intense, informative and cutting edge.

DEEP KNOWLEDGE	PRIVACY & ANONYMITY	COMPUTER FORENSICS & LOG ANALYSIS
<b>Automated Binary Reverse Engineering</b> Halvar Flake, Black Hat <b>Trust No-one, Not Even Yourself OR The Weak Link Might Be Your Build Tools</b> David Maynor, ISS X-force <b>Attacking Obfuscated Code with IDA Pro</b> Chris Eagle, Computer Science Department Naval Postgraduate School <b>Practical Win32 and UNICODE Exploitations</b> FX, Phenôelit	<b>Privacy, Economics and Immediate Gratification</b> Dr. Alessandro Acquisti, Carnegie Mellon University & Institute for the Study of Labor (IZA) <b>Tracking Prey in the Cyberforest</b> Bruce Potter, The Shmoo Group <b>You got that with GOOGLE?</b> Johnny Long <b>Information Hiding in Executable Binaries</b> Rakan El-Khalil	<b>Evasion and Detection of Web Application Attacks</b> K.K. Mookhey, Network Intelligence India. Pvt. <b>Steganography, Steganalysis &amp; Cryptanalysis</b> Michael T. Raggo, VeriSign <b>The Evolution of Incident Response</b> Kevin Mandia, Red Cliff Consulting <b>Detecting 0-days Attacks With Learning Intrusion Detection Systems</b> Stefano Zanero, Politecnico di Milano University, Milano, Italy
POLICY, MANAGEMENT & THE LAW	TURBO TALKS	APPLICATION SECURITY
<b>The First International Cyber War</b> Peter Feaver, Duke University <b>Managing Hackers: The Top 8 Rules for Creating Productive Security Operations</b> Navy NCIS <b>When the Tables Turn</b> Sensepost <b>Hacker Court '04: Pirates of the Potomac</b> Chief Judge Philip M. Pro, Chief United States District Court Judge for the District of Nevada <b>RFID Tags and the Question of Personal Privacy</b> Dan Bailey, RFID Solutions Architect <b>Privacy: Do As I Say... Not as I Do</b> Sarah Gordon, Symantec Corporation <b>Google Attacks</b> Patrick Chambet, EdWeb - ON-X Group <b>Managing MSIE Security in Corporate Networks by Creating Custom Internet Zones</b> Patrick Chambet, EdWeb - ON-X Group <b>Insecure IP Storage Networks: Problems with Network Attached Storage (NAS)</b> Himanshu Dwivedi, @stake	<b>WorldWide WarDrive 4</b> Chris Hurley aka Roamer <b>Managing Hackers: The Top 8 Rules for Creating Productive Security</b> James C. Foster, CSC <b>Debunking Events Per Second (EPS) Numbers</b> Robert Angelino, High Tower Software <b>RFID Tags and the Question of Personal Privacy</b> Dan Bailey, RFID Solutions Architect <b>Privacy: Do As I Say... Not as I Do</b> Sarah Gordon, Symantec Corporation <b>Google Attacks</b> Patrick Chambet, EdWeb - ON-X Group <b>Managing MSIE Security in Corporate Networks by Creating Custom Internet Zones</b> Patrick Chambet, EdWeb - ON-X Group <b>Insecure IP Storage Networks: Problems with Network Attached Storage (NAS)</b> Himanshu Dwivedi, @stake	<b>Antivirus Security Software Tests</b> Sarah Gordon, Symantec Corporation <b>Integer Overflows In-Depth</b> David LeBlanc, Microsoft <b>Pocket PC Abuse</b> Seth Fogie, Aircscanner <b>Hacking Without Re-inventing the Wheel</b> Nitesh Dhanjani, Ernst & Young's Rudolph W. Giuliani Advanced Security Center in New York <b>Shoot the Messenger</b> Brett Moore, security-assessment.com <b>Blind SQL Injection Automation Techniques</b> Cameron Hotchkies, aka nummish, 0x90.org
LAYER 0	ZERO DAY DEFENSE	ZERO DAY ATTACK
<b>Introduction to Embedded Security</b> Joe Grand, Grand Idea Studio <b>"They'll Never See It coming!"</b> Stephen Dugan, 101Labs <b>A Historical Look at Hardware Token Compromises</b> Joe Grand, Grand Idea Studio	<b>Acting in Milliseconds- Why Defense Processes Need to Change</b> Dominique Brezinski, Pyrogen <b>A Comparison Buffer Overflow Prevention Implementations &amp; Weaknesses</b> Peter Silberman, iDEFENSE <b>Defeating Automated Web Assessment Tools</b> Saumil Shah, NetSquare Solutions	<b>All New 0-Day</b> David Litchfield, Next Generation Security Software <b>NoSEBrEaK- Defeating Honeynets</b> Thorsten Holz, RWTH-Aachen University <b>Maximilian Domseif, RWTH-Aachen University</b> Christian Klein, University of Bonn

Register with the code **PV04** and receive \$100 off the Briefings rate

A complete schedule and listing of speakers, session titles and topic descriptions can be found at [www.blackhat.com](http://www.blackhat.com)

# training

Black Hat Training is designed to raise the professional's competence level on specific security topics. At the Black Hat USA 2004 Training, we will be offering twenty-two different courses:

development	information security	investigations	managerial	systems administration	technical
<b>Analyzing Software for Security Vulnerabilities</b> Black Hat: Halvar Flake <b>Aspects of Offensive Root-kit Technology</b> Greg Hoglund, Rootkit.com & Jamie Butler <b>Network Application Design &amp; Secure Implementation</b> Black Hat: Drew Miller	<b>NSA InfoSec Assessment Methodology (IAM) - Level 1</b> Security Horizon <b>NSA InfoSec Evaluation Methodology (IEM) - Level 2</b> Security Horizon	<b>Discover the Hidden: Steganography Investigator Training</b> WebStone Technologies	<b>Enterprise Security From Day 1 to Completion: Developing an Information Security Program</b> Black Hat: Chris Conacher	<b>Microsoft Ninjitsu: Securely Deploying MS Technologies</b> Timothy Mullen	<b>Designing A Secure Web Application Through Enlightenment and Understanding</b> Next Generation Security Software <b>Hacking by Numbers: Bootcamp</b> SensePost <b>Hacking by Numbers: Combat</b> SensePost <b>Infrastructure Attacktects™ &amp; Defentecs™: "Hacking into a Cisco Network"</b> Steve Dugan
<b>Windows Web Application Hacking: Recon to Root</b> Black Hat: Drew Miller & Joshua Betts <b>Web Applications: Attacks &amp; Defense- Advanced Edition</b> Saumil Udayan Shah	<b>OSSTMM Professional Security Analyst (OPSA)</b> DIAD Security	<b>Intermediate Digital Forensics: Civil Litigation Matters</b> eForensics	<b>Hacking by Numbers: Chief of Staff</b> SensePost	<b>Securing Solaris and Locking Down Linux</b> Jay Beale	<b>Infrastructure Attacktects™ &amp; Defentecs™: Voice Over IP</b> Steve Dugan & Rodney Thayer <b>Internal Security Threats: Identification and Prevention</b> Arbor Networks <b>Ultimate Hacking: Black Hat Edition</b> Foundstone <b>Ultimate Hacking: Expert</b> Foundstone



Register early to ensure a seat in the class of your choice. Go to [www.blackhat.com](http://www.blackhat.com) for complete class descriptions and to register.

www.blackhat.com