WARNING:

Computer and network vulnerabilities will be revealed.

Black Hat, Europe's premier technical ICT security event, returns in 2005 to provide solutions to your security challenges.

- Share information with hundreds of expert colleagues from 20 nations about new tools, techniques and defenses
- Gain insights from 30 expert speakers with no vendor sales pitches
- Obtain in-depth knowledge at hands-on Training classes preceding the Briefings

Black Hat®

Briefings & Training Europe 2005

29 March-1 April • Amsterdam, the Netherlands

www.blackhat.com
for updates and to submit Call for Papers

sponsors

diamond

BIND VIEW Insight at Work

gold

Configuresoft

ARBOR NETWORKS

supporting associations

CLUSIF

WACA INTERNATIONAL

GOVCIB Genootschap van

IPv6 FORUM

eema www.eema.org

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.

diamond sponsor

BindView BindView solutions and expertise strengthen, streamline and automate controls across all levels of IT security, operations and compliance.

Deployed in some of the world's largest organizations, our scalable solutions for Compliance Monitoring, Vulnerability Management, Identity Administration and Configuration Management share a flexible framework to secure today's most popular operating systems, databases and applications.

Award-winning BindView solutions help you:

- Deploy and enforce IT security controls to match standards and best practices
- Access and secure multi-platform environments
- Provision and manage user identities and access controls
- Standardize and maintain secure system configurations
- Meet IT compliance and reporting deadlines
- Pass required audits
- Demonstrate due care for regulations
- Operationalize security best practices

With an integrated approach to IT Security Compliance, BindView helps you implement strong operational controls and processes to create a closed-loop risk management lifecycle. With BindView's solutions, organizations reduce IT risk exposure and deliver improved business results. **www.bindview.com**

gold sponsors

Configuresoft Configuresoft is the recognized leader in highly scalable enterprise policy compliance, configuration management, and security patch management technology, serving eight of the "Global 25" corporations.

Based in Colorado Springs, Colorado, the company's products offer large-scale computing environments the ability to collect and analyze the most detailed information available about system application settings, events and operational trends, to a centralized point of management and control. Configuresoft provides the tools to keep mission-critical systems properly configured, while ensuring compliance

with stringent regulatory mandates, such as Sarbanes-Oxley, HIPAA, GLBA and FISMA, operational standards and evolving process methodologies.

www.configuresoft.com

Arbor Networks Arbor Networks' Peakflow solutions ensure the security and operational integrity of the world's most critical networks. Today's sophisticated threats require organizations to have network-wide solutions to successfully prevent costly downtime, network cleanup, and loss of customer confidence.

Arbor's solutions are built on the proven Peakflow platform, an architecture for network-wide data collection, analysis, and anomaly detection. Peakflow provides a real-time view of network activity enabling organizations to:

- instantly protect against worms, DDoS attacks, insider misuse, and traffic
- and routing instability; segment and harden the network from future threats,
- and maintain business continuity.

www.arbornetworks.com

supporting organisations

media partners

Black Hat®
Briefings & Training Europe

29 March - 1 April 2005 • Grand Hotel Krasnapolsky, Amsterdam

for updates, complete schedule listing, session descriptions, pricing and to register, go to

www.blackhat.com

training

29-30 March
All classes consist of two days of training.

Analyzing Software for Security Vulnerabilities
Halvar Flake, Black Hat

Digital Investigations: Practical Digital Forensic Analysis
the Grugq

Hackers on Honeypots
Laurent Oudot

Hacking by Numbers: Bootcamp
SensePost

Hacking by Numbers: Combat
SensePost

Infrastructure Attacktecs™ & Defentecs™: Cisco Voice Over IP
Steve Dugan & Rodney Thayer

Infrastructure Attacktecs™ & Defentecs™: Hacking Cisco Networks
Steve Dugan, 101labs

Web Applications: Attacks & Defense-Advanced Edition
Saumil Udayan Shah

Under the Hood: Hands-On Hardware Hacking and Defense Techniques
Joe Grand, Grand Idea Studio

Register with the code BREU and receive 100 EUR off the Briefings rate

Partial Briefings agenda shown.
Go to **www.blackhat.com** for complete schedule, session descriptions and to register.

briefings

31 March-1 April
Two days, 4 tracks, 23 topics

Keynote
Simon Davies, Privacy International

Yersinia, A Framework For Layer 2 Attacks
David Barroso Berrueta, S21SEC Company & Alfredo Andres, S21SEC Company

Hacking PGP
Jon Callas, PGP Corporation

Hacking Windows Internals
Cesar Cerrudo, Application Security

Advancements in Malware Profiling and Rootkit Detection
Matt Conover, Symantec

Symbian Security
Job de Haas

A New Password Capture on Cisco System Devices
Steve Dugan, 101Labs

Building Zero-Day Self-Defending Web Applications
Arian Evans, FishNet Security

Network Flows and Security
Nicolas Fischbach, COLT Telecom & Sécurité.Org

Comparing, Navigating, Auditing: Using Specialized Graphs for Reverse Engineering
Halvar Flake, Black Hat & Rolf Rolles

Can You Really Trust Hardware? Exploring Security Problems in Hardware Devices
Joe Grand, Grand Idea Studio

Digital Forensics
the Grugq

Mac OS X Kernel Insecurity
Christian Klein & Ilja van Sprundel

Database Rootkits
Alexander Kornbrust, Red-Database-Security

Bluetooth Hacking - Full Disclosure
Adam Laurie, trifinity.org; Martin Herfurt, trifinity.org and Marcel Holtmann, trifinity.org

All New Zero Day
David Litchfield, NGS Software

Google Hacking for Penetration Testers
Johnny Long

WLAN and Stealth Issues
Laurent Oudot, RSTACK Team

Revolutions in Web Server/Application Assessments
Sensepost

Defeating Automated Web Assessment Tools
Saumil Shah, Net-Square Solutions

Owning Anti-Virus: Weaknesses in a Critical Security Component
Alex Wheeler, ISS X-Force & Neel Mehta, ISS X-Force

Automatically Detecting Web Application Vulnerabilities by Variable Flow Reconstruction
Stefano Zanero, Politecnico di Milano University

Black Hat®

Briefings & Training Europe

registration

Register with the code **BREU** and receive 100 EUR off the Briefings rate

Black Hat Briefings - 31 March & 1 April 2005

○	I am attending the Black Hat Briefings	1199 EUR

Black Hat Training 2-Day Courses – 29 & 30 March 2005

○	Analyzing Software for Security Vulnerabilities	1550 EUR
○	Digital Investigations: Practical Digital Forensic Analysis	1550 EUR
○	Hackers and Honeypots	1550 EUR
○	Hacking by Number: Bootcamp	1850 EUR
○	Hacking by Number: Combat	1850 EUR
○	Infrastructure Attacktecs™ & Defentecs™: Hacking Cisco Networks	1700 EUR
○	Infrastructure Attacktecs™ & Defentecs™: Voice Over IP	1700 EUR
○	Under the Hood: Hands-On Hardware Hacking and Defense Techniques	1550 EUR
○	Web Applications: Attacks & Defense – Advanced Edition	1600 EUR

register online at www.blackhat.com

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.