WWW.BLACKHAT.COM
digital self defense

Black Hat Asia Briefings & Training 2003

Black Hat Briefings 18 & 19 December 2003

Speakers & Topics

Black Hat Training 16 & 17 December 2003

1. Analyzing Software for Security Vulnerabilities
2. Web Hacking: Countdown to Lockdown
3. Discover the Hidden: Steganography Investigator Training
4. Microsoft Ninjitsu:Securely Deploying MS Technologies
5. Windows Buffer Overflow Developments
6. Hacking by Numbers: Bootcamp
7. Infrastructure Attacktecs™ & Defentecs™: “Hacking Cisco Networks”
8. Ultimate Hacking: Expert

First Ever Capture the Flag (CtF) Competition

Black Hat Asia 2003 Exhibition

Briefings and Training Registration Form on Page 19

Speakers and Topics at Black Hat Briefings Asia 2003

MOSDEF Tool Release
David Aitel, Immunity, Inc.

Cisco Security
Stephen Dugan, CCSI

Automated Binary Reverse Engineering
Halvar Flake, Reverse Engineer, Black Hat

International DMCA Laws
Jennifer Stisa Granick, Lecturer in Law and Executive Director of the Center for Internet and Society (CIS) at Stanford University

All New Zero Day
David Litchfield, Founder, Next Generation Security Software

Addressing Complete Security to Save Money
Russ Rogers, Chief Technical Officer, Security Horizon, Inc

Honeypots Against Worms 101
Laurent Oudot, Computer Security Engineer, Rstack team

Putting The Tea Back Into CyberTerrorism
SensePost

HTTP Fingerprinting and Advanced Assessment Techniques
Saumil Udayan Shah, Director, Net-Square Solutions

Win32 One-Way Shellcode
S.K. Chong, Co-Founder & Security Consultant, SCAN Associates.

TBA
Tim Mullen, CIO and Chief Software Architect, AnchorIS.Com

Shiva
Shaun Clowes

Networking Security
Jeremy Rauch

The Art of Defiling: Defeating Forensic Analysis on Unix File Systems
The grugq

TBA
Harry SK Tan, Director, Centre for Asia Pacific Technology Law & Policy (CAPTEL)

Black Hat Training Class 1	
Analyzing Software for Security Vulnerabilities	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD2980 or USD1700	SGD3330 or USD1900

Certification: A Certificate of Completion will be offered.

The C programming language gives the programmer a lot of rope to hang himself with - and C++ just adds to the feature list. Both languages have an impressive number of subtle pitfalls, and many of these can be leveraged by a skilled attacker to execute code on a computer on which these vulnerable programs run. But while almost everybody seems to understand then significance of these programming mistakes, few actually sit down and analyze code from the security analysis perspective. This workshop focuses on teaching security-specific code-analysis, both in source and in binary form.

Day One: Open-Source Day
The first day ("Open-Source day") will attempt to thoroughly review most common (and not so common) security-critical bugs in C (if that is possible) and to teach guidelines & methodologies for code review. Problems specific to C++ code will be covered, and various tools that are supposed to assist in source code review will be discussed. After the theoretical/demonstration part is finished, the remainder of the day will be used to practice hands-on auditing on some open-source server software.

Although we are dealing with open-source-software during the first day, IDA Pro will be used to generate Function Flowgraphs etc. to aid in understanding, and to verify the existence of certain bugs. IDA's built-in scripting language will help us in eliminating some of the more boring parts of the analysis process.

Day Two: Closed-Source Day
The second day ("Closed-Source day") will transfer the principles of source-code analysis to the closed-source world: By using IDA Pro and a few home-brewn plugins the students will be introduced into the specific problems when dealing with the analysis of commercial closed-source software. Specific focus will be put on both the automation of some of the more annoying tasks and on repairing & understanding some of the things that modern C++ compilers generate in the binary. Again, after the theoretical part of the day is finished, the students will be given a lot of opportunity to collect hands-on experience in the process of auditing binaries.

What to bring:
Students must bring their own Laptop with a full version of IDA Pro 4.5 installed.
Failure to do so will make participation impossible. Black Hat offers discount pricing for this software to registered students. Please contact store<a>blackhat.com

A general knowledge of x86-assembly language is required to follow the course, as is a good knowledge of C/C++. Several other tools will be provided on the CD (IDA Plugins, C Compiler, Source Analysis Helpers, IDC Scripts).

Trainer:
Halvar Flake is Black Hat's resident reverse engineer. Originating in the fields of copy protection and digital rights management, he gravitated more and more towards network securityover time as he realized that constructive copy protection is more or less fighting windmills. After writing his first few exploits he was hooked and realized that reverse engineering experience is a very handy asset when dealing with COTS software. With extensive experience in reverse engineering, network security, penetration testing and exploit development he recently joined BlackHat as their main reverse engineer.

Black Hat Training Class 2	
Web Hacking: Countdown to Lockdown	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD2810 or USD1600	SGD3160 or USD1800

Certification: A Certificate of Completion will be offered.

Overview:

"It is 9 p.m. Your company's web store application is broken, and incidentally, tomorrow is the launch date of the company's web store. The media is waiting, and so is your board of directors. You need to fix it by 5 a.m. to make the 7 a.m. launch deadline. FIND OUT WHAT IS WRONG, AND FIX IT."

The course gives the students an overview of web application security, by first having them find the security holes with a web application modeled on a real life example, and then take the necessary steps to secure it, from various aspects.

Key Learning Objectives:

- Problems that occur when developing a web application.
- Security issues when deploying a web application.
- Web application security testing
- Securely configuring web servers
- Spotting basic errors in web application code
- Basic error handling techniques
- Securing the back end database connection

General Learning Objectives:

- Developing procedures to test and maintain the security of a web application.
- Secure coding techniques
- Proficiency with security testing tools and procedures.

Who Should Attend:

a. Developers: Learn what can go wrong with badly written application code, and how to prevent such errors.

b. Web site administrators: Learn how to securely configure a web server and an application server, without compromising on functionality.

c. Project managers / IT managers: Learn how to be effective in maintaining a secure web application, going ahead.

d. Security consultants: who primarily work on penetration testing of web applications and providing remediation procedures and recommendations.

What to bring:

Participants are requested to bring their own laptops. The course is OS friendly – Participants using Windows 2000, Linux, Mac OS X are all welcome. The course is Internet independent.

Trainers:

Saumil Udayan Shah

Founder and Director, Net-Square Solutions Pvt. Ltd.

Saumil continues to lead the efforts in e-commerce security research at Net-Square. His focus is on researching vulnerabilities with various e-commerce and web based application systems. Saumil also provides information security consulting services to Net-Square clients, specializing in ethical hacking and security architecture. He holds a designation of Certified Information Systems Security Professional. Saumil has had more than nine years experience with system administration, network architecture, integrating heterogenous platforms, and information security and has perfomed numerous ethical hacking exercises for many significant companies in the IT area. Saumil is a regular speaker at security conferences such as BlackHat, RSA, etc.

Previously, Saumil was the Director of Indian operations for Foundstone Inc, where he was instrumental in developing their web application security assessment methodology, the web assessment component of FoundScan - Foundstone's Managed Security Services software and was instrumental in pioneering Foundstone's Ultimate Web Hacking training class.

Prior to joining Foundstone, Saumil was a senior consultant with Ernst & Young, where he was responsible for the company's ethical hacking and security architecture solutions. Saumil has also worked at the Indian Institute of Management, Ahmedabad, as a research assistant and is currently a visiting faculty member there.

Saumil graduated from Purdue University with a master's degree in computer science and a strong research background in operating systems, networking, infomation security, and cryptography. At Purdue, he was a research assistant in the COAST (Computer Operations, Audit and Security Technology) laboratory. He got his undergraduate degree in computer engineering from Gujarat University, India. Saumil is a co-author of "Web Hacking: Attacks and Defense" (Addison Wesley, 2002) and is the author of "The Anti-Virus Book" (Tata McGraw-Hill, 1996)

Nitesh Dhanjani
Nitesh Dhanjani is a senior consultant for Ernst & Young's Advanced Security Center. He has performed network, application, web-application, wireless, source-code, host security reviews and security architecture design services for clients in the Fortune 500.

Nitesh is the author of "HackNotes: Unix and Linux Security" (Osborne McGraw-Hill). He is also a contributing author for the best-selling security book "Hacking Exposed 4" and "HackNotes: Network Security".

Prior to joining Ernst & Young, Nitesh worked as consultant for Foundstone Inc. where he performed attack and penetration reviews for many significant companies in the IT arena. While at Foundstone, Nitesh both contributed to and taught parts of Foundstone s "Utimate Hacking: Expert" and "Ultimate Hacking" security courses.

Nitesh has been involved in various educational and open-source projects and continues to be active in the area of system and Linux kernel development. He has published technical articles for various publications such as the Linux Journal.

Nitesh gratuated from Purdue University with both a Bachelors and Masters degree in Computer Science. While at Purdue, he was involed in numerous research projects with the CERIAS (Center for Education and Research Information Assurance and Security) team. During his research at Purdue, Nitesh was responsible for creating content for and teaching C and C++ programming courses to be delievred remotely as part of a project sponsored by IBM, AT&T, and Intel.

Black Hat Training Class 3	
Discover the Hidden: Steganography Investigator Training	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD2810 or USD1600	SGD3160 or USD1800

A Black Hat Certificate of Completion will be offered.

WetStone Technologies, Inc., Security Horizon and Black Hat are proud to announce the availability of their Steganography Investigator Training Course. This two-day course provides detailed information and hands-on practice for individuals responsible for investigating the suspected use of digital steganography. Upon completion of the course, students can expect to have detailed background information about the latest steganography tools, the knowledge necessary to conduct a thorough investigation and the ability to present their findings in a court of law.

Students will first be given an overview of steganography to include how it is used by criminals and terrorists. They will learn about best-of-breed technologies and how they embed information in both digital image and audio carriers. Unique to this course is that students will have the opportunity to work with a number of these tools, allowing them to become familiar with what is available and how they may be used in the unauthorized transmission of information. Once the foundation is established, the course goes on to teach investigative strategies, techniques and tools that will assist in the discovery and preservation of evidence. Both forensic and web-based investigative methods will be covered. The course ends with an exercise in which students will be required to report their findings in a courtroom presentation.

This course is hands-on and allows students to use tools and techniques employed by criminals to hide information as well as the methods and strategies necessary to discover and present this as evidence. All hardware and software will be provided and students will receive a copy of course materials and steganography tools. Students will also have the option to purchase WetStone Technologies' steganography detection products at a special Black Hat conference price. A certificate of completion will be awarded at the end of the course.

Pre-requisites
Students will be required to have basic computer skills and knowledge of the Windows environment. They will be subject to a background verification prior to final acceptance into the course. Students are not required to provide any materials.

Who should attend?
Law enforcement, Intelligence, Security Consultants, Corporate Investigators, Forensic Accountants, Other IT Investigators

What to bring:
Just yourself! All tools and materials will be provided to you.

Trainer:
Chet Hosmer is a co-founder, and the President and CEO of WetStone Technologies, Inc. He has over 25 years of experience in developing high technology software and hardware products, and during the last 15 years, has focused on research and development of information security technologies. His specialty areas include: secure time, intrusion detection and response, and cyber forensics.

Chet is a co-chair of the Technology Working Group, one of the seven working groups of the National Institute of Justice's Electronic Crime and Terrorism Partnership Initiative. He is also the Director of the Computer Forensics Research and Development Center of Utica College. Chet is a member of the IEEE and the ACM, and holds a B.S. Degree in Computer Science from Syracuse University.

Black Hat Training Class 4	
Microsoft Ninjitsu: Securely Deploying MS Technologies	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD3160 or USD1800	SGD3510 or USD2000

A Black Hat Certificate of Completion will be offered.

New and Improved! This training session now includes elements of Windows 2003 Server security and configuration, and a first look at “Titanium,” the Exchange Server 2003 beta.

The key to securing a Microsoft infrastructure is to build security into the foundation. When properly configured, the Microsoft suite of technologies can be deployed to provide highly available, reliable, and secure network services.

This intensive two-day course will take you on a journey through the full deployment cycle of the most common Microsoft products, stopping along the way to sniff the packets and secure the route less traveled. If you make it to the end of Day Two in one piece, you will be prepared to snatch the pebble from the Master's palm.

Day One: Infrastructure

- Win2k / Win2k3 Domain Controllers
    - Active Directory Domains and Forests
    - Server Role Wizards (Win2k3)
    - New RRAS Options and Basic Firewall (Win2k3)
    - Sites and Services
    - Group Policy and Organizational Units
    - Certificate Services
    - Terminal Services
- Client Configuration
    - Leveraging XP Pro Clients
    - Security Policies
    - System Restrictions
    - Software Restrictions
    - Encryption and IPSec
- Exchange 2000 / Titanium
    - Setup and Configuration
    - Default protocols: HTTP, SMTP, POP3, IMAP
    - Multiple sites
    - OWA (HTTPS/HTTP)
    - OWA 2003/Front and Backend Servers
- SQL Server 2000
    - Setup and Configuration
    - Authentication Modes
    - SQL Server/Agent Service Security Contexts
    - Client/Process data access and best practices
    - Auditing Tools
- IIS 5 / IIS 6
    - Setup and Configuration
    - ISAPI extensions and application mapping
    - HTTPS Configuration and Certificates
    - IIS Lockdown / URL Scan
    - Secure ASP Development and Auditing Tools
    - IIS 6.0 Security Overview and Default Configurations

Day Two: Deploying Internet Services

- ISA Server
    - Setup and Configuration
    - Packet Filters and Protocol Rules
    - Policy Elements (Address Sets, Authentication, Schedules)
    - Application Filters
    - Web, Firewall and Secure NAT Clients
- Publishing Services
    - Web Publishing
    - Publishing Exchange Services (SMTP, POP3, etc)
    - 3rd Party SMTP Gateway Solutions and Filtering
    - Publishing Multiple OWA Sites Securely
    - Feature Pack 1 enhancements
    - Publishing Terminal Services, Alternate Port Configuration, and TS Web
- Remote Access
    - RAS and Routing Service Configuration
    - Client VPN Setup
    - Point-to-point ISA VPN Servers

Note that aspects of Day Two, “Deploying Internet Services” may be integrated into Day One’s “Infrastructure” material as required where relevant.

What to bring:
Students should bring their own network ready laptops (with CD) preferably running Windows XP and an open mind. A CD will be provided with reference material, sample code, and utilities. Where possible, students should pre-install VMWare images of Win2k and associated software applications should they wish to participate in and experiment with “live” configuration changes.

This course covers a substantial amount of material for many different Microsoft applications and technologies in relatively short period of time. Students should expect a wide range of topics and a quick pace.

Trainer:
Timothy Mullen is CIO and Chief Software architect for AnchorIS.Com, a developer of secure enterprise-based accounting solutions. Mullen is also a columnist for Security Focus' Microsoft Focus section, and a regular contributor of InFocus technical articles. A.k.a. Thor, he is the founder of the "Hammer of God" security co-op group.

Black Hat Training Class 5	
Windows Buffer Overflow Developments	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD2810 or USD1600	SGD3160 or USD1800

A Black Hat Certificate of Completion will be offered.

This class will bring to you the magic of being able to write your own buffer overflows against the Windows platform.

What You Will Learn:

- The basics of Windows SEH handling
- How to take advantage of Ollydbg's many exploit-development features
- How to write reliable, robust, Windows exploits
- Techniques for analyzing different problems that occur when
- writing Windows exploits
- Several techniques for exploiting heap overflows (advanced students)
- A general understanding of exploit development covering:
    - How exploit-ability is determined
    - Several different methodologies for exploit development
    - Design of a reliable exploit

No other class has taught exploit development at this level

Who Should Attend:

This course is ideal for someone who has read Aleph1's paper and wants to take the next step. It will also help people who have just started writing their own overflows, and want to get better at it, or want to learn new techniques for writing overflows on the Windows platform. If you are an experienced buffer overflow writer for Linux or Solaris, then this class will help you port your knowledge to the Windows platform.

- Technical personnel who want to go beyond the CISSP level of knowledge, and already have some experience with programming.
- Information Security Professionals
- Anyone with an interest in understanding exploit development

What will be provided:

You will be provided with a temporary license to Immunity CANVAS (http://www.immunitysec.com/CANVAS/) in order to keep you from having to learn how to write shellcode and how to exploit overflows all in one class.

All target VMWare images will be provided.

Prerequisites:

Students should have experience with 'C' programming and basic computer architecture. The better you are with assembly language, the more you will get out of this class, but you should at the very least know what a register is, and know what the instructions "mov" "call" and "jmp" do and how they work. You don't have to be a assembly language programmer to take this class, but you should have no problems understanding Aleph1's smashing the stack paper

Basic knowledge of Ollydbg is a welcome bonus. Ollydbg is freely available at:
http://home.t-online.de/home/Ollydbg/

Basic knowledge of Python is also required. This requirement is easy to pick up (should take you one hour or less) if you have basic knowledge in C. We recommend any of the tutorials placed online (www.python.org).

You should know what "LoadLibraryA()" does. (I.E. You need a basic familiarity with the Win32 API. This is less important if you are a strong C programmer.)

You must bring a hacker's mentality with you.

What to bring:
One laptop with RedHat 9 installed, and VMWare 4 for Linux installed.The RedHat installation must have pyGTK installed.

The disk on your laptop needs to have at least 2 gigs free disk space for VMWare images and software.

Trainer:
Dave Aitel is the founder of Immunity, Inc. and the primary developer of CANVAS and the SPIKE Application Assessment Suite. His previous experience, both within the US Government and the private sector has given him a broad background in exploit development, training, and speaking. He has discovered numerous new vulnerabilities in products such as Microsoft IIS, SQL Server 2000, and RealServer.

Immunity, Inc. is a New York City based consulting and security software products firm. CANVAS, Immunity's flagship product, is a sophisticated exploit development and demonstration framework.

Black Hat Training Class 6	
Hacking by Numbers: Bootcamp	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD3680 or USD2100	SGD4030 or USD2300

A Certificate of Completion will be offered.

Last year SensePost compromised over 200 networks worldwide. This course is a behind the scenes look at how it is done, with hands on instruction and real world case studies.

Overview:
Reality, Theory and Practice.
This course is the "How did they do that?" of modern hacking attacks. From start to finish we will lead you through the full compromise of a company's IT systems, explaining not only the tools and technologies, but especially the thinking, strategies and the methodologies for every step along the way. Based on SensePost's acclaimed "Applied Hacking Techniques" course, "Hacking By Numbers" will give you a complete and practical window into the methods and thinking of hackers.

1. Our course is focused on tuning the mind. How does one *think* when attempting to compromise a network from the Internet. Our reasoning is as follows
    - Work according to a methodology
    - Determine your strategy
    - Select your tools (this should flow naturally from [b])
    - Execute your attack
    - From this you can see that the emphasis is not on the tools and how to use them. But on the *thinking* behind the tools.
2. Our course is strongly method based. We perform all of our assessments according to a strict methodology that we believe ensures the best chances of a successful penetration. The course is delivered exactly according to this strict methodology, thereby giving you a systematic approach to attack and penetration.
3. Our course is strongly case-study based. We base each lesson on a real life scenario and use the case to describe and demonstrate our thinking and techniques. We then give each student the opportunity to apply those techniques in the lab and on the 'net.
4. Our course is *less* tools based. Although the course is extremely practical and technical in nature, it probably focuses less on the use of specific tools and utilities then other courses. Our thinking is that tools come and go and that anyone with a browser and a basic understanding of English can find and use the right tool for a specific job. Sometimes the 'right' tool doesn't exist and it needs to be built. In either case, our focus is on teaching the student how to decide what tool to use at various points of an attack, and how those tools should be applied to complete the job at hand.
5. Our course is 100% real-world. Each trainer spends all the time that he's not giving training, actually performing assessments and penetration tests. i.e. the other 25 days of the month. Therefore, our course is not about how *hackers* break into networks, its about how *we* break into networks. Our trainers are all highly skilled and experienced security practitioners that are globally recognized in the field.

Course Structure:
"Hacking by Numbers" runs for two days during which the SensePost trainers will walk you, step-by-step, through real-life hacking attacks. We'll start by identifying the target systems, teach you how to breach the target perimeter, and demonstrate how to extend these attacks in order to completely compromise the internal networks.

What You Will Learn:

This course will teach you by means of real examples, solid theory and hands-on exercises how a hacker would go about breaking into your network. Armed with this knowledge you can test and ensure that your systems are secure against these kinds of threats and attacks. Delegates will perform all hands on exercises using pre-configured laptops and will gain practical experience with the tools and utilities that are used everyday by industry analysts and underground specialists in the field.

How it Will Work:

Each student will be provided with a state-of-the-art laptop for the duration of the course. The machines are loaded with a Unix™ and a Microsoft™ operating system and are pre-configured with the vast range of tools, documents, software and other utilities required for the practical components of the course. Our dedicated lab environment and a direct connection to the open Internet ensure a real and authentic experience. At each step of the way we explain what was actually done to circumvent system security (that's the reality part), why it was done like that (the theory part) and how you can try it yourself (where you get to practice what we preach).

At the end of the course each student will receive a CD-ROM containing, not only the tools and utilities covered in the course, but also a huge collection of additional software and resources.

Who Should Attend:

Information security officers, system and network administrators, security consultants, government agencies and other nice people will all benefit from the valuable insights provided by this class. Remember that this course is practical and of an extremely technical nature, so a basic understanding of networking, security, Unix™ and NT™ is a course prerequisite.

What to bring:

Just Yourself. All necessary equipment will be provided, including pre-configured laptops, tools and utilities.

Trainers:

Roelof Temmingh is the technical director of SensePost where his primary function is that of external penetration specialist. Roelof is internationally recognized for his skills in the assessment of web servers. He has written various pieces of PERL code as proof of concept for known vulnerabilities, and coded the world-first anti-IDS web proxy "Pudding". He has spoken at many International Conferences and in the past year alone has been a keynote speaker at SummerCon (Holland) and a speaker at The BlackHat Briefings (New Orleans). Roelof drinks tea and smokes Camels.

Haroon Meer is one of SensePost's senior technical specialists. He specializes in the research and development of new tools and techniques for network penetration and has released several tools, utilities and white-papers to the security community. He has been a guest speaker at many Security forums including BlackHat Briefings (New Orleans). Haroon doesn’t drink tea or smoke camels.

Charl van der Walt is a founder member of SensePost. He studied Computer Science at UNISA, Mathematics at the University of Heidelberg in Germany and has a Diploma in Information Security from the Rand Afrikaans University. He is an accredited BS7799 Lead Auditor with the British Institute of Standards in London. Charl has a number of years experience in Information Security and has been involved in a number of prestigious security projects in Africa, Asia and Europe. He is a regular speaker at seminars and conferences nationwide and is regularly published on internationally recognized forums like SecurityFocus. Charl has a dog called Fish.

Black Hat Training Class 7	
Infrastructure Attacktecs™ & Defentecs™: **"Hacking Cisco Networks"**	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD3680 or USD2100	SGD4030 or USD2300

A Black Hat Certificate of Completion will be offered.

Attacktecs™ Attack Techniques used to exploit network infrastructure, servers, databases and other services with the intent of stealing or destroying intellectual property and/or to deny users and clients legitimate access.

Defentecs – Defense Techniques and implementation methods used to defend against the latest Attacktecs.

This class will cover a wide variety of the publicly available exploit tools and how they can be used specifically against a Cisco infrastructure. A majority of the class time will be spent doing practical labs. Therefore, a certain level of Cisco expertise will be expected. The training will also cover the possible defenses against these attacks.

Students will be using 2651 routers, and 1900 switches for their labs. The lab core will consist of 3600s, 2900s, 2500s and servers of various flavors. Students will be required to bring their own laptops to (with appropriate caution) attach to the labs. This class will focus on Cisco Router and Switch vulnerabilities and will not be covering PIX firewalls, VPN concentrators, or IDS tools.

Here is a list of some of the topics that will be covered:

- Ways of Password Nabbing
- Sniffing traffic on a switch
- VLAN Hopping and 802.1Q issues
- Root Bridge Takeovers
- Local and remote HSRP attacks
- Routing manipulation/injection with RIP, IGRP, EIGRP, OSPF
- BGP attacks
- SNMP Exploits
- Tunneling attacks
- DoS and DDoS issues and preventive methods

What to bring:
Your laptop with a 10BaseT Network card, web browser and telnet client.
You must provide your own laptop. No loaner laptops will be available.

Trainer:
Stephen Dugan is currently an independent contract instructor and network engineer.b He has been teaching Cisco networking for the last 3 years focusing on Router and Switch configuration, Voice/Data integration, and Network Security. His students come mostly from Fortune 500 companies and large service providers. He also teaches private internal classes to Cisco Employees. As a Sr. Network Engineer he has worked on the design and implementation of large enterprise, government contractor, and service provider networks. He is also working on a new series of security books entitled "Hacker Attacktecs." The first three planned books will cover Windows, Unix/Linux, and Cisco exploits and how to defend against them.

Black Hat Training Class 8	
Ultimate Hacking: Expert	
Course Length: 2 Days	CPEs: 16

Course Fee	
Before 1 Dec 2003	After 30 Nov 2003
SGD3680 or USD2100	SGD4030 or USD2300

A Foundstone Certificate of Completion will be offered.

Designed as the natural follow on course to Ultimate Hacking and other "Hacking" classes, Ultimate Hacking: Expert brings your expertise up-to-date with the latest techniques, exploits and threats. This is an in-depth and detailed Hands On course designed for the advanced security professional interested in discovering the inner workings of serious security vulnerabilities and techniques to counter them.

Class Overview
Day 1 starts with advanced network reconnaissance including techniques for stealth scans and identification of services running on non-standard ports. This is followed with an overview of monitoring switched networks using Arp spoofing and other techniques. The dangers and detection of covert channels are explored using ICMP, UDP, TCP and HTTP protocols. The day finishes with the introduction of a SQL hacking methodology that will take you through SQL enumeration to remote command execution.

Throughout the day, students participate in labs that reinforce the topics presented. These labs include sniffing in a switched environment, remote service identification using binary nudge strings, and creating covert channels to hide interactive network access.

Day 2 presents advanced UNIX configuration techniques, including chroot environments. Students compile and test malicious Linux Kernel Modules, the ultimate example of a Unix rootkit. Finish the day testing your skills against a hardened network with the Ultimate Lab.

Linux Kernel Module labs step through the process of installing the malicious modules, then modification of the modules to avoid detection by current Unix rootkit detection tools.

Who Should Take the Course?
System and network administrators, security personnel, auditors, and consultants with advanced Windows and UNIX skills.

What to bring:
Nothing to bring. All necessary equipment will be provided including preconfigured workstations, tools and utilities.

Trainers:
Why **Foundstone**?
Method Based - Foundstone courses teach you the Hacker Methodology so that you thoroughly understand the threats that you face. Utilizing this methodology, unwanted intruders are adept at finding weaknesses across their targeted networks. By combining these weaknesses, they methodically escalate their privileges as they burrow through defenses to their ultimate goal – getting root.

Understanding the Hacker Methodology and the thought process that intruders employ is critical to protecting your network and will allow you to build effective defenses and limit your risk.

Hands On – Foundstone courses always use Hands On exercises and labs to reinforce key concepts. Our courses are never "slide shows". You're challenged with multiple exercises that require you to apply your new knowledge on our target networks so that you're ready to apply your new skills immediately.

Time Tested – Foundstone has taught thousands of security professionals how best to defend their networks. Ranging from the principles of good security practices and advanced techniques to web security, secure coding and incident response, Foundstone is the proven expert in security education.

Experts – Foundstone courses are taught by practicing security consultants who are hired by leading Fortune 100 companies, the military and government agencies to secure their networks. Foundstone brings real world experience from these engagements to the class room. Many of our instructors are authors of internationally best selling security titles. Learn from the one's who wrote the book on security – not the ones who read it.

Foundstone's management team and selected staff are uniquely qualified to present this material, having performed hundreds of security assessments for Fortune 500 companies. Instructors have managed or directed the security-assessment teams at three of the Big 5 accounting firms, as well as amassed real-world experience ranging from the United States Air Force to Wall Street. Members of the instructor team authored the best-selling Hacking Exposed: Network Security Secrets & Solutions and write a weekly column for InfoWorld magazine. They are also frequent speakers at industry conferences such as NetWorld+Interop, Usenix, and the Black Hat Briefings.

Black Hat Asia 2003 Briefings first ever Capture the Flag (CtF) Competition

This event is open only to paid registrants of the Black Hat Asia Briefings and Training.

Dates & Venue
16-17 December 2003, from 6pm to 8am, 14 hours of gaming at the Marina Mandarin Hotel.

Game Scenario
Qwerty Security Research is a newly established IT security company that provides network security consultancy services, distributes security products and publishes security advisories. The company has recently launched a web portal that allows Internet users to access to its advisories and to sign up for its premium security alerting service. The CEO of Qwerty Security Research has recently published a statement on the web portal claiming that the portal is designed from ground up with security in mind and is impossible to penetrate. Your mission is to prove otherwise.

After performing the necessary information gathering you conclude that Qwerty Security Research owns the IP range 192.168.50.0/24 and 192.168.60.0/24. The URL of the web portal is at http://192.168.50.5

To prove that the CEO is not entirely correct regarding the security of the site, you have to achieve the following objectives:

1. Obtain the /etc/passwd file of any compromised *NIX systems.
2. Obtain the /etc/shadow file of any compromised *NIX systems.
3. Steal ALL credit card numbers from the web portal.
4. Plant a file <yourname>.txt in C:\ of the web portal.

Participation

1. Contestants may participate individually or in pairs.
2. Each participating team-pair or person is allowed to bring in only one notebook and is allocated only one network and power point.
3. Participants are expected to bring their own tools and exploits, as there may be no Internet access provided for them to download their tools.
4. Upon registration, each participant will be assigned a single IP address. Participants are not allowed to change their IP addresses or to spoof the IP/MAC addresses of another person.
5. Participation is open to registrered delegates of the Black Hat Asia 2003 Briefings.

Scoring
Participants will be judged based on their total score and the time they take to capture/plant the flags. The start time will be recorded for each participant during registration. This allows participants who arrive late to take part in the competition as well. At any time, the participants can declare that they want to end their game. The end time for every participant will be recorded.

The participant who successfully obtained the highest score within the shortest time will be the winner of the competition. The second and third place will be calculated as follows:

- second place = 2nd_max(score) and min(endTime – startTime)
- third place = 3rd_max(score) and min(endTime – startTime)

The time factor applies only if there are several participants with the same score.

Rules
The following rules ensure proper functioning of the competition. Participants that violate any of the following rules will be disqualified.

1. During the competition, there will be both scheduled and unscheduled Pit Stops. During the Pit Stops, all participants are required to leave the room and are only allowed to return at the end of the Pit Stop period.
2. No Denial of Service (DoS) attacks of any kind are to be launched.
3. No flooding of the network (e.g. UDP flood, smurf attacks).
4. No attacking or exploiting of other participant's systems.
5. No shutting down, disabling or patching of vulnerable systems.
6. No defacement or changing of the /etc/passwd and /etc/shadow files on vulnerable systems.

7. No harassment of other participants.
8. No planting or launching of worm, virus, or other destruction code.
9. No physical attacks are allowed.
10. No attacking or exploiting of network infrastructure devices, such as switches, routers, etc. (e.g. ARP cache poisoning, switch MAC table flooding and traffic re-routing are NOT allowed).
11. No changing, spoofing of IP addresses allowed. Participants must use the IP addresses assigned to them.
12. No changing, spoofing of MAC addresses allowed.
13. No removal of flags planted by other participants.

Prizes

Chance to win one of the following prizes:

- Free admission to a future Black Hat Briefings.
- a Sony Ericsson T610 Mobile Phone compliments of MobileCiti.
- A Black Hat branded short sleeve button down shirt.

Registration

Participation is by pre-registration only.
Details will be available on blackhat.com from 1 December 2003.

Black Hat Asia 2003 Exhibition

The Most Advanced Security Related Products & Solutions Will Be Showcased In This Year's Black Hat Asia!

Dates: 18-19 December 2003
Venue: Marina Mandarin Hotel, Singapore
Function Rooms: Aquarius-Pisces & Gemini-Libra (Ground Level)

The first 500 to pre-register at blackhat.com for the exhibition will receive a special Black Hat Token!

All training and briefing attendees will be automatically registered for the exhibition upon confirmed registration.

REGISTRATION FORM

BlackHat
Briefings Asia

To register complete the form below and send it together with full payment to:

The York Group (Singapore) Pte Ltd
101, Upper Cross Street, #05-35
Singapore 058357

For enquiry, call:
Tel: (65) 6462 0773, Fax (65) 6535 6206
Email: Singapore@TheYorkGroup.com

Personal Particulars: □ Mr □ Ms □ Mrs □ Dr □ Mdm [Please print or type]

Name ______________________________ Title ______________________

Company ____

Address ____

______________________________ CISSP/SSCP______________________

Phone^ ______________________________ Fax ______________________

Email^ ______________________________ Special Diet: ______________________

Tick (✓) your selection in the space provided

	Black Hat Training 2-Day Courses	Dates	Fee before 1 Dec 2003	Fee after 30 Nov 2003	✓
1	Analyzing Software for Security Vulnerabilities	16 & 17 Dec 03	SGD2980 or USD1700	SGD3330 or USD1900	
2	Web Hacking: Countdown to Lockdown	16 & 17 Dec 03	SGD2810 or USD1600	SGD3160 or USD1800	
3	Discover the Hidden: Steganography Investigator Training	16 & 17 Dec 03	SGD2810 or USD1600	SGD3160 or USD1800	
4	Microsoft Ninjitsu: Securely Deploying MS Technologies	16 & 17 Dec 03	SGD3160 or USD1800	SGD3510 or USD2000	
5	Windows Buffer Overflow Developments	16 & 17 Dec 03	SGD2810 or USD1600	SGD3160 or USD1800	
6	Hacking by Numbers: Bootcamp	16 & 17 Dec 03	SGD3680 or USD2100	SGD4030 or USD2300	
7	Infrastructure Attacktecs™ & Defentecs™: "Hacking Cisco Networks"	16 & 17 Dec 03	SGD3680 or USD2100	SGD4030 or USD2300	
8	Ultimate Hacking: Expert	16 & 17 Dec 03	SGD3680 or USD2100	SGD4030 or USD2300	

	Black Hat Briefings				
A	I am attending the Black Hat Briefings	18 & 19 Dec 03	SGD1230 or USD700	SGD1450 or USD825	
	Total				

□ I enclose my bank draft / cheque* ______________________________, payable to The York Group (Singapore) Pte Ltd for the total amount stated above.

□ Please send me an invoice, for administrative purpose, contact Mr/Ms ______________________

of Department ____________________ Tel: ____________________ Fax: ____________________

- Credit Card payment is only available in US Dollars at www.blackhat.com.
- Registration forms submitted must be accompanied by full payment.
- You may cancel your registration before 16 Nov 2003 for a full refund. For cancellation thereafter till 15 Dec 2003, 15% will be forfeited. Refunds will be processed after the conference.
- Fees include training or speaking notes, meals and coffee breaks.
- Stay at Official Hotel Marina Mandarin Singapore; special rate of SGD140+++ for Black Hat attendees. Email us for details.

□ I want the Free Book, Syngress' "Hack Proofing Your Network, Second Edition"

* Delete where non applicable

^ Mandatory; for confirmation and updates

THE YORK GROUP
INTERNATIONAL TECHNOLOGY PARTNERS