training // July 30-August 2

Advanced Malware Analysis
//MANDIANT

Many malware authors take deliberate steps to thwart the reverse engineering of their tools. Students will learn to combat sophisticated malware head-on by studying its anti-analysis techniques. This course focuses on advanced topic areas related to combating malware defense mechanisms, and as such, a practiced and robust malware analysis skill set is required. Before learning specific malware anti-analysis techniques, students will arm themselves with critical skills by learning to script IDA Pro and various debuggers to overcome challenging or repetitive tasks. Students will learn detailed information about defeating packed and armored executable and be challenged to defeat several difficult specimens throughout the course. Malware stealth techniques such as process injection and rootkit technology will be introduced, and tools and methodologies will be presented to aid analysis of such techniques. Hands on exercises, labs, and instruction are all incorporated into the course.

Advanced Malware Deobfuscation
//Jason Geffner & Scott Lambert

Security researchers are facing a growing problem in the complexity of malicious executables. With an ever-increasing number of tools that malware authors use to compress and obfuscate executables, and the pressing urgency that analysts often face, it is vital for analysts to know the best methods to remove protections that they have never seen before.

Unpacking is the process of removing the compression and obfuscation applied by a "packer" (or "protector") to a compiled and linked binary. This class will focus on teaching attendees the steps required to effectively deal with both known and previously unknown packing techniques.

This is a hands-on course. Attendees will work on real-world malware through a series of lab exercises designed to build their expertise in thwarting anti-debugging and anti-disassembling techniques.

Advanced Memory Forensics in Incident Response
//Jamie Butler & Peter Silberman

Though many people in the security industry do forensics, very few do memory forensics. As an industry, we have overlooked some of the most important data in an investigation. Attackers know this. Forensic analysts can no longer rely on getting all of the information they need from the hard drive. Since there are many examples of malware that never touch the disk, drive analysis may lead to one conclusion, while memory analysis can lead to quite another. Drive analysis also takes significantly more time than memory analysis.

In performing Windows memory analysis, this class will focus on the use of freeware and open source tools to perform advanced memory analysis. Students will also be taught the concepts necessary to extend these tools or build new ones where the existing toolset does not meet all the needs of a particular incident.

Advanced Vulnerability Scanning Techniques Using Nessus
//Paul Asadoorian, Tenable Network Security

This course teaches advanced scanning techniques by using a real-world scenario to demonstrate how these techniques help to solve problems in an example work environment.

In this course you (or you and your team) will take on the role of a brand new security engineer for a financial company. You will be tasked with configuring and auditing a system to be used within your network environment. The system, and associated applications, makes up the environment used to manage the business. Currently, the old systems are in place and an upgrade is planned. The current vulnerability scanning process takes over a week to complete and there is duplication of effort and a known false positive rate. Additionally, breaches have occurred on the network and your company is in jeopardy of being fined due to compliance violations. The vulnerability management process is missing vulnerabilities that were exploited by attackers. A sample system has been provided for you, that exactly mirrors what will be used in production, right down to the passwords and configuration.

Advanced Windows Exploitation Techniques
//Offensive Security

An in depth, hardcore drilldown into advanced Windows Vulnerability Exploitation techniques from Offensive Security.

The course covers topics such as Egghunters, NX bypassing Techniques, Function Pointer Overwrites, Heap Spraying, Venetian Shellcode Encoding, Windows Kernel Exploitation and custom shellcode creation.

This course is extremely hands-on and includes a lab environment, which is geared to challenge and bring the most out of you. The case studies covered include vulnerabilities discovered by our research team, or exploits written by us.

Application Security: For Hackers and Developers
//Jared DeMott

There are four technical skills required by security researchers, software quality assurance engineers, or developers concerned about security: Source code auditing, fuzzing, reverse engineering, and exploitation. All these skills and more are covered. C/C++ code has been plagued by security errors resulting from memory corruption for a long time. Problematic code is discussed and searched for in lectures and labs. Web auditing is covered using WebGoat. Fuzzing is a topic book author DeMott knows about well. Mutation file fuzzing and framework definition construction (Sulley and Peach) are just some of the lecture and lab topics. When it comes to reversing C/C++ (Java and others are briefly discussed) IDA pro is the tool of choice. Deep usage of this tool is covered in lecture and lab. Exploitation discussions and labs are the exciting final component. You'll enjoy exploiting BSD local programs to Vista browsers using the latest techniques in Reverse Engineering, Source Code Auditing, Fuzzing and Exploitation

Students will walk out of this class knowing how to find and exploit bugs in software. This is useful to both developers and hackers. The exploit component will teach each common bug type including: stack overflows, function pointer overwrites, heap overflows, off-by-ones, FSEs, return to libc, integer errors, uninitialized variable attacks, heap spraying, and more. Shellcode creation/pitfalls and other tips and tricks will all be rolled into the exciting, final component.

Assessing and Exploiting Web Applications with Samurai-WTF
//Justin Searle & Kevin Johnson

Come take the official Samurai-WTF training course given by the two founders and lead developers of the project! You will learn the latest Samurai-WTF open source tools and as well as the latest techniques to perform web application penetration tests. After a quick overview of pen testing methodology, the instructors will lead you through the penetration and exploitation of various web applications, including client side attacks using flaws within the application. Different sets of open source tools will be used on each web application, allowing you to learn first hand the pros and cons of each tool. After you have gained experience with the Samurai-WTF tools, you will be challenged with a capture the flag event. This final challenge will give you time to practice your new skills at your own pace and experiment with your favorite new tools. This experience will help you gain the confidence and knowledge necessary to perform web application assessments and expose you to the wealth of freely available, open source tools.

Building a Better Mousetrap: Effective Techniques in Vulnerability Analysis and Intrusion Detection and Prevention
//Rohit Dhamankar & Rob King

It's a fact that hackers are getting smarter faster than network security hardware is getting better. To effectively defend your organization from attacks, you have to know more than just how to configure your IPS or IDS - you need to understand the art behind the science.

This course provides an in-depth look at vulnerability analysis, detection, and prevention from a network-based IPS/IDS standpoint. It starts with how vulnerabilities become vulnerabilities, how hackers attack them, how they look on the wire, and ends with how to write effective signatures and filters for attacks. More esoteric topics covered in this course (and very rarely in others) include how to avoid the dreaded False Positive, how to estimate performance, how to prevent data leakage, and - perhaps most importantly - the techniques hackers use to evade detection by IPS/IDSes, and how you can evade the evasions.

Building, Attacking and Defending SCADA Systems in the Age of Stuxnet
//Tom Parker & Jonathan Pollet

Supervisory control and data acquisition (SCADA) systems are some of the most poorly understood, yet most critical systems in use in the world today, and while they generally remain unseen are responsible for the smooth running of our daily routines—from the moment we turn on a tap in the morning, to turning off the lights at night. This two-day course will provide a primer, into the world of securing industrial control, and automation systems as they relate to the numerous industries where they are most prolific.

CISSP® Boot Camp
//Shon Harris, Logical Security

This Logical Security course trains students in all areas of the security Common Body of Knowledge (CBK). They will learn about security policy development, secure software development procedures, network vulnerabilities, attack types and corresponding countermeasures, cryptography concepts and their uses, disaster recovery plans and procedures, risk analysis, crucial laws and regulations, forensics basics, computer crime investigation procedures, physical security, and much, much more. They will explore the contents and concepts that make up the diverse domains and learn how they work together to provide true "in-depth" defense.

The CISSP exam is rigorous, covering ten security domains essential for the protection of information systems, corporations and national infrastructures. Understanding that security is an enterprise wide problem, these domains provide the candidate with a broad understanding of the technical, managerial and human factors that must coordinate effectively to keep information and systems secure.

Using this course, students prepare for the exam, while at the same time obtaining essential security knowledge that can be immediately used to improve organizational security. This knowledge enhances services and products, secures business functions and infrastructures, provides better implementation processes, and can be used to restructure critical programs and procedures to help keep companies up-to-date on today's business and security strategies, technologies, and best practices.

CNSS-4012 Senior System Manager/CNSS-4015 System Certifier Combination Course
//Information Assurance Associates (IA2)

The IA2 CNSS-4012 Senior System Manager (SSM) and CNSS-4015 System Certifier double certificate course is specifically designed to consolidate all SSM and System Certifier knowledge requirements into a single, comprehensive curriculum. This course provides four days of intense, highly concentrated, non-technical professional training necessary to achieve the in-depth knowledge, skills, and abilities needed to enforce Information Assurance (IA) requirements, apply Information System Security (INFOSEC) methodologies and facilitate certification and accreditation (C&A) activities. Additionally, this course addresses professional and functional requirements necessary for System Managers and System Certifiers to identify specific assurance levels and evaluate risk impact thresholds in meeting applicable security policies, standards and requirements to ensure that accrediting authorities have the information necessary to make an objective accreditation determination based on an acceptable level of risk.

This course focuses on analyzing, evaluating, and assessing, information system security policies, processes and procedures necessary to ensure a comprehensive multi-disciplined assessment of technical and non-technical security features and associated safeguards. Special emphasis is placed on certification requirements for federal interest information system as well as identifying, implementing and integrating management and administrative solutions for securing critical information infrastructures and establishing standards necessary to help protect the confidentiality, maintain the integrity and ensure the availability of sensitive data and critical organizational computing resources.

CNSS-4016 Risk Analyst
//Information Assurance Associates (IA2)

This is a fully certified Committee on National System Security (CNSS)-4016 Risk Analyst course that provides four days of intense, highly concentrated, non-technical professional training necessary to achieve the fundamental knowledge, skills and abilities needed to analyze, assess, control, determine, mitigate and manage risk within a federal management and acquisition framework or within federal interest computer systems that store, process, display or transmit classified or sensitive information (e.g. Personally Identifiable Information (PII), Electronically Protected Health Information (ePHI)/Individually Identifiable Health Information (IIHI) , etc). This course addresses specific knowledge factors and functional requirements established for Entry and Intermediate Level Risk Analysts. Specific focus is directed on identifying, implementing and integrating management, acquisition and administrative risk methodologies for securing critical and sensitive information infrastructures and establishing standards necessary to help protect the confidentiality, maintain the integrity and ensure the availability of critical organizational computing resources.

Cyber Network Defense Bootcamp
//Adam Meyers

Cyber Network Defense is a critical and evolving requirement for organizations large and small in the 21st century. There are a number of component courses available for various disciplines in the realm of CND; however, there are very few options for a CND crash-course bootcamp that covers topics relevant to the overarching mission of defending the home network. Many courses teach the fundamentals of incident response utilities, malware analysis, and reverse engineering. In practice, we find many "detection" tools have limited success rates and can be quite misleading—from basic antivirus to highly specialized memory and hooking analysis tools.

This course will cover the holistic approach to CND, beginning with intelligence ingestion and easing into network anomaly detection and advanced network forensics. Following the understanding of the network layer, the course will introduce key concepts of incident analysis by providing an in-depth introduction into incident response device forensics using freely available and commercially licensed tools of the trade. With incident analysis and network forensics under their belts, students will then immerse themselves in nearly a full day of static and dynamic reverse engineering to include topics like manual unpacking and deobfuscation of command and control protocols. To round out the training, students will be given a short training in incident reporting and will learn how to present technical findings to managerial and executive level personnel in a clear and concise manner.

Designing Secure Protocols and Intercepting Secure Communications
//Moxie Marlinspike

This is a new and special training that covers both designing and attacking secure protocols. Attendees will learn the fundamentals of how to design a secure protocol, and be armed with the knowledge of how to evaluate the security of and discover weaknesses in existing protocols.

Attendees will walk away with everything they need to intercept several types of secure communication. Attendees will learn the fundamentals of how to design a secure protocol, and be armed with the knowledge of how to evaluate the security of and discover weaknesses in existing protocols.

This training will also cover tricks for attacking implementation vulnerabilities and holes in the glue between different protocols, which can allow for the interception of different types of secure traffic.

Detecting and Mitigating Attacks Using Your Network Infrastructure
//Cisco

Security engineering teams often focus on the security of networked workstations, servers, and applications, neglecting the network itself . Many networks also receive only rudimentary security controls that are often deployed inconsistently. These scenarios not only fail to completely protect the network from today's threats, but they also fail to fully utilize innate network capabilities and existing security controls to detect and mitigate attacks against the computing infrastructure of an organization.

During this course, students will learn leading network security practices from experts who developed these techniques and put them to practical use. The techniques covered in this course are not limited to those that are typically considered "security features"; this course will detail how to leverage network functionality (for example, routing protocols and Cisco IOS NetFlow) and security controls to provide a full range of attack identification and mitigation capabilities. This course is organized around a proven six-phase approach to incident response, which transitions from preparation through post mortem and includes extensive hands-on lab work.

Digital Intelligence Gathering Using Maltego
//Paterva

The IT security and intelligence community love Maltego—whether it be mapping a target's infrastructure or profiling a person's sphere of influence.

During this course we will help you unlock the true potential and raw power of Maltego – from helping you to understand the underlying technologies to extending Maltego with your own code. Join us and we'll show you how to navigate and map the Internet's darkest rivers… This course will also include practical sessions where learners will need to engage targets and participate in challenges.

Effective Fuzzing: Using the Peach Fuzzing Platform
//Michael Eddington, Deja Vu Security

The entirety of the course is student centric, hands on, and lab intensive. On day one, students will be instructed on the use of the Peach Fuzzing Platform, from a practitioner's perspective, learning the ways in which Peach can be used to fuzz a variety of targets including network protocol parsers, ActiveX/COM interfaces, file parsers, APIs, and web services. Students will also be introduced to new methods by which fuzzing can be utilized to locate security flaws not typically considered detectable by fuzzing, including N-tier applications.

On the second day, students will be exposed to the internals of Peach for a developer's perspective. The Peach architecture and module interfaces will be explained in great detail as to equip students with the skills necessary to extend and adapt Peach to their custom needs. Students will then develop their own Peach extensions in a lab environment.

Enterprise Security from Day 1 to Completion: A Practical Approach to Developing an Information Security Program
//Chris Conacher

It is day 1. You are charged with securing your company. You have limited resources, management that wants to see progress and a very complex problem to solve. Just where do you begin? Whether you are starting from scratch, working within an existing framework, or investigating what an Information Security program could mean for your company, creating a comprehensive Information Security program can be a daunting task.

- How do you breazk down an organization into meaningful, and manageable, pieces?
- Where do you concentrate your efforts and limited resources?
- How do you drill down into the detail without leaving gaps elsewhere?
- How do you develop audits that are relevant and provide meaningful information?
- Which of the thousands of policies, guidelines, procedures, standards and controls do you actually need and how do you get the employees to accept and follow them?
- How do you decide which countermeasures are actually relevant to your needs and how do you ensure that they mesh together?
- How do you manage everything once it is implemented?
- And, perhaps most importantly, how do you get the business to support all of your efforts and keep that support for ongoing and future initiatives?

This course aims to answer these questions and many more by providing a practical, step-by-step approach to securing an entire organization.

The Exploit Laboratory: Analyzing Vulnerabilities and Writing Exploits
//Saumil Udayan Shah & S.K. Chong

Have you ever found yourself staring at a vulnerability advisory with some proof-of-concept snippets and wished the author had rather attached a working exploit with it? Have you wished you could analyze vulnerabilities and write your own exploits for them? Have you wanted to debug and exploit custom built applications and binaries? The "Exploit Laboratory", now in its fifth year, is an intense hands-on class for those wishing to dive into vulnerability analysis and exploit writing. The "Exploit Laboratory" starts off with a basic insight into system architecture, process execution, operating systems and error conditions. The class then quickly accelerates to analyzing vulnerabilities with debuggers, reproducing reliable error conditions and writing working exploits for the same.

The "Exploit Laboratory" features popular third party applications and products as candidates for vulnerability analysis and exploitation, rather than building up on carefully simulated lab exercises. Most of the class time is spent working on lab exercises and examples. Lab examples and exercises used in this class cover both the Unix (Linux) and Microsoft Windows platforms, illustrating various error conditions such as stack overflows, heap overflows and memory overwrites. The latter part of the class focuses on topics such as browser exploitation, PDF exploitation and Mac OS X exploitation. All this is delivered in a down-to-earth, learn-by-example methodology, by trainers who have been teaching advanced topics in computer security for over 10 years.

This class is updated from the 2009 edition, featuring revised content on heap overflows, abusing exception handlers and more hands-on examples based on recent vulnerabilities. This class does NOT require knowledge of assembly language. A few concepts and a sharp mind is all you need.

The Exploit Laboratory: Black Belt Edition
//Saumil Udayan Shah & S.K. Chong

The "Exploit Laboratory: Black Belt" is a new and advanced class continuing from where The "Exploit Laboratory" left off. This class is for those curious to dig deeper into the art and craft of software exploitation. The "Black Belt" class begins with a quick overview of concepts covered in The "Exploit Laboratory", namely stack overflows, abusing exception handlers, heap overflows, memory overwrites, and other core concepts. The class then moves to deeper vulnerabilities such as integer overflows and format string bugs. We shall then focus on topics which involve breaking exploit prevention techniques like non executable stack, DEP, ASLR, etc. The "Black Belt" class also features an introduction to kernel exploitation, post exploitation techniques like return to libc, advanced heap spraying, an introduction to return oriented programming and an introduction to unusual shellcode.

"The Exploit Laboratory: Black Belt" requires a lot of hands on work. Lab examples used in this class cover Unix (Linux and Mac OS X) and Microsoft Windows platforms, featuring popular third party applications and products instead of simulated lab exercises.

As with the popular "Exploit Laboratory", all topics are delivered in a down-to-earth, learn-by-example methodology. The same trainers who brought you "The Exploit Laboratory" for over four years have been working hard in putting together advanced material based on past feedback.

The "Exploit Laboratory: Black Belt" is not recommended for those who have no prior experience with writing exploits, however, you may choose to combine this class with The Exploit Laboratory in succession over the course of 4 days.

Hacking by Numbers: Cadet Edition
//SensePost

Cadet Edition is an introductory course for technical people with no previous experience in the world of hacking. The course will present you with background information, technical skills and basic concepts required to get you going. This includes some coding and scripting, networking and Internet technologies, basic methodologies, essential thinking skills, tools and current hacking techniques. The course has been updated to accommodate the latest technologies and trends.

Cadet Edition is the ideal training ground to prepare you for the HBN Bootcamp, further self-study or other hacking courses.

Hacking by Numbers: Bootcamp Edition
//SensePost

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 the tools and technologies, but especially the thinking, strategies and the methodologies for every step along the way. "Hacking By Numbers—Bootcamp Edition" will give you a complete and practical window into the methods and thinking of hackers.

Hacking by Numbers: BlackOps Edition
//SensePost

Hacking By Numbers "BlackOps Edition" is your final course in the HBN series before being deployed into "Combat". Here, you'll sharpen your skills in real scenarios before being shipped off to battle. Where Bootcamp focuses on methodology and Combat focuses on thinking, BlackOps covers tools and techniques to brush up your skills on data exfiltration, privilege escalation, pivoting, client-side attacks and even a little exploit writing. You'll also focus on practical elements of attacking commonly found systems. The course is instructor-lead, with slides and structured labs that guide students through numerous scenarios. This is hands-on hacking made fun.

Hacking by Numbers: Combat Training
//SensePost

Combat Edition is our premier hacker training course. From the first hour, to the final minutes students are placed in different offensive scenarios as they race the clock to breach systems. Using experienced gained from thousands of assessments over the years, we have created dozens of real-life lab exercises who's solutions lie much more in the technique and an out-of-box thought process than in the use of scripts or tools. Each exercise is designed to teach a specific lesson and will be discussed in detail after they are completed; however there are no lab sheets or lectures as this course is non-stop hacking. In this way you learn from talented SensePost instructors, your colleagues and your own successes and failures.

Hacking by Numbers: Unplugged Edition
//SensePost

Hacking By Numbers "Unplugged Edition" is the ultimate Wi-Fi hacking course. With a strong focus on results the course outlines 3 broad offensive scenarios for Wi-Fi hacking and then presents participants with the background knowledge, methodologies, tools and thinking skills required to successfully breach security in each of those scenarios.

Hacking by Numbers: W^3
//SensePost

Hacking by Numbers—W^3 Edition is an intermediate web application hacking course for people with some experience in penetration testing.

The course will provide a refresher of HTTP and associated technologies before commencing with some more advanced level attacks ranging from assessment techniques of traditional web applications to newer technologies—such as AJAX, rich client media and HTML 5.

As with all courses in the Hacking by Numbers range, the W^3 course is a hands-on, highly practical course which intends to enable students to understand the trade and not the trick.

Hacking and Securing Oracle
//Alexander Kornbrust & Sumit Siddharth

The two-day hands-on course will teach the audience the security problems related to Oracle database. The training covers a variety of security problems arising from flaws such as insecure design, insecure features/packages, insecure PL/SQL code, patch management, weak passwords etc. The second day will focus on securing and hardening databases using built-in oracle features along with a number of externally available scripts and tools. Implementing auditing solutions will also be a part of the training. The audience will have access to an infrastructure with a number of Oracle components deployed, and they will be encouraged to identify/exploit/patch security vulnerabilities as they learn them. The training will provide software developers understanding of writing secure PL/SQL code, DBAs the understanding of thorough auditing of the database and penetration testers the understanding of how to break the unbreakable Oracle.

Hands-on Hardware Hacking and Reverse Engineering Techniques
//Joe Grand

This course is the first of its kind and focuses on hardware hacking and reverse engineering techniques commonly used against hardware products. It is a combination of lecture and hands-on exercises, culminating with students attempting to defeat the security of a custom-designed circuit board. We'll guide you through the hardware hacking process, explore basic electronics, experiment with test equipment, discuss embedded security, and dive into tips and techniques required for successful circuit modifications and hardware hacking. A more detailed course outline can be found on Grand Idea Studio's website.

Reverse Engineering with IDA Pro
//Christopher S. Eagle

The need for reverse engineering binary software components arises in more and more contexts every day. Common cases include analysis of malicious software such as viruses, worms, Trojans and rootkits, analyzing binary drivers in order to develop open source drivers for alternate platforms, analyzing closed source software for security flaws, and source code recovery in legacy systems. The first step in such an analysis is generally the acquisition of a high quality disassembly of the binary component. IDA Pro is touted as the premier disassembler available today. IDA Pro is capable of disassembling machine languages for a large number of microprocessors and microcontrollers and is particularly strong when used on Windows and Linux executables. This course will cover essential background material for effective reverse engineering before diving into the features of IDA Pro that set it apart from other disassemblers.

Incident Response Black Hat Edition
//MANDIANT

As the sophistication and threats caused by malicious attacks continue to increase, MANDIANT has raised the bar of effective detection, response, and remediation by introducing their Incident Response (IR) class. This two-day Special Edition class has been specifically designed for information security professionals and analysts who respond to computer security incidents. It is designed as an operational course, using case studies and hands-on lab exercises to ensure attendees are gaining experience in each topic area. Hands on exercises and labs in Windows Intrusion.

Infrastructure Attacktecs™ & Defentecs™: Hacking Cisco Networks
//Steve Dugan

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 in 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 2600 series routers, and 2950T switches for their labs. The lab core will consist of 3750s, 2800s, and servers of various flavors. Students will be required to bring their own laptops to attach to the labs (with appropriate caution). Students must have a working serial port and terminal emulator. This class will focus on internal infrastructure vulnerabilities and will not be covering firewalls, VPN concentrators, or IPS tools.

Introduction to Malware Analysis
//Jason Geffner & Scott Lambert

Security researchers are facing a growing problem in the complexity of malicious executables. While dynamic black-box automation tools exist to discover what malware will do on a given execution, it is often important for an analyst to know the full capabilities of a given malware sample. What port does it listen on? What password does it expect for backdoor access? What files will it write to? What will it do tomorrow that it didn't do today?

This class will focus on teaching attendees the steps required to understand the functionality of given malware samples. This is a hands-on course. Attendees will work on real-world malware through a series of lab exercises designed to build their expertise in understanding the analysis process.

Macsploitation
//Vincenzo Iozzo & Dino Dai Zovi

This two-day course will take students through the complete process of finding and exploiting vulnerabilities in and on Mac OS X, highlighting the unique aspects of the operating system that vulnerability researchers must be aware of. Each unit of the course includes lecture and lab sessions designed to give students the background they need and then the opportunity to get hands-on experience applying those techniques.

Malware Analysis: Black Hat Edition
//MANDIANT

Almost every computer incident involves some trojan, backdoor, virus, or rootkit. Incident responders must be able to perform rapid analysis on the malware encountered in an effort to determine the purpose of unknown code. This course provides a rapid introduction to the tools and methodologies used to perform malware analysis on executables found on Windows systems. Students will learn to infer the functionality of a program by analyzing disassembly and by watching how it changes a system as it runs in a debugger. They will learn how to extract investigative leads from host and network-based indicators associated with a malicious program and how to identify specific coding constructs in disassembly. They will be taught about dynamic analysis and the Windows APIs most often used by malware authors. Each section is filled with in class demonstrations, exercises where the students follow along with the instructor, and labs with real malware where the students practice what they have learned on their own.

Mobile Hacking
//HOTWAN

The course is intended to provide a better understanding of the emerging trends and threats in the mobile space. Students will be introduced to multiple smartphone technologies and development environments. They will have opportunity to inspect/audit mobile apps, circumvent operating systems, leverage mobile forensics and conduct/witness network based attacks.

NBISE BQST (Basic Qualified Security Tester) Pen-Testing Exam: Review Course
//Veris Group

So what exactly IS a penetration test and how do you define a qualified penetration tester? These questions have loomed over the security community for many years without concrete answers, leading to often sub-standard engagements and an inability to differentiate service offerings in the penetration-testing field. The National Board of Security Examiners (NBISE), partnering with the UK- based Council for Registered Ethical Security Testers (CREST), is offering rigorous and technically difficult examinations and certifications for the penetration-testing workforce. The goal of these certifications is to provide a measure of assurance that certified individuals are operationally capable of thorough and repeatable penetration tests. The NBISE Board Qualified Security Tester (BQST) certification is targeted at intermediate-level penetration testers. Even given its intermediate status, the exam is unlike any certification non-U.K. penetration testers have experienced previously, leading to very low pass rates for non-U.K. applicants. Candidates who have taken the exam have testified that the process is challenging and sets a high standard for those who attempt it.

The purpose of this course is to prepare participants for both the breadth of knowledge required and the uniquely heavy hands-on focus NBISE utilizes for the BQST exam. A wide range of topics will be reviewed, from soft skills to exploitation techniques for network devices, Windows and Unix systems with a large number of associated practical, lab-based scenarios. The course will challenge participants with a "firehose" of information and scenarios conducted under time pressure. As such, this course is not designed for participants without experience and previous training in the topic areas. It is expected that the student have a fundamental understanding of the material presented in the syllabus. This course will primarily serve to review foundation knowledge and provide greater understanding of each subject. Fifty to sixty percent of the time spent in this course will be in hands-on labs and practice tests, which have been designed to emulate conditions a penetration tester will experience throughout examination and the entire penetration test engagement lifecycle.

This course has been endorsed by NBISE and meets its standards of training for the BQST examination. Successful completion of the course will allow participants to enter the examination with confidence and a strong foundation for success. More importantly, students will have thorough and practical baseline knowledge on the successful execution of network and web application penetration tests.

Offensive Countermeasures: Defensive Tactics that Actually Work
//PaulDotCom

One of the big questions we get is why Offensive Countermeasures are so important. Well, to be honest, you will need it someday. The current threat landscape is shifting. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. Some of the things we talk about you may implement immediately, others may take you a while to implement. Either way, consider what we discuss as a collection of tools at your disposal when you need them to annoy attackers, attribute who is attacking you and, finally, attack the attackers.

More to the point, the old strategies of security have failed us and will continue to fail us unless we start becoming more offensive in our defensive tactics.

Pentesting with BackTrack
//Offensive Security

This is an intensive, hands-on Security class by the creators of Backtrack especially designed for delivery in BlackHat Trainings. "Pentesting with BackTrack" is designed for network administrators and security professionals who need to get acquainted with the world of Offensive Security. The course introduces the latest hacking tools and techniques using the world renowned BackTrack 5.

A experienced and seasoned team of Security Professionals will help you take your skills a few steps further. "Common" hacking techniques are revisited from a professional and practical approach for a better and more efficient pentest. The course is heavily laced with the "do it yourself" approach, and will expose you to the raw underlying mechanisms of the various attack vectors.

We keep our classes small to maximize each students learning potential. This also gives the instructors the ability to spend more time with each student.

Are you up the challenge? Are you ready to Try Harder?

Pentesting with Perl
//Joshua Abraham

The object of the course is to cover many of the tasks that need to be performed during a penetration assessment as well as to improve existing tools and build new tools as needed.

This course will help to streamline much of the tedious aspects of pentesting. We will use Perl to get the job done quickly and effectively. The goal of the course is to help everyone to automate many of the tasks they are performing manually, so that they can focus on more complex issues. The ability to automate tasks is critical to being a successful penetration tester. We need to be spending time on the most complex issues that cannot be tested through the use of automated tools!

Physical Penetration Testing: Introduction
//The CORE Group

Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door. Those who attend this session will leave with a full awareness of how to best protect buildings and grounds from unauthorized access, as well as how to compromise most existing physical security in order to gain access themselves. Attendees will not only learn how to distinguish good locks and access control from poor ones, but will also become well-versed in picking and bypassing many of the most common locks used in North America in order to assess their own company's security posture or to augment their career as a penetration tester.

Physical Penetration Testing: Advanced
//The CORE Group

This course is geared specifically towards individuals who already have a solid foundation of knowledge in the field of physical penetration. Those with an established understanding of the mechanics of locks and the basic ways in which they can be compromised (lockpicking, shimming, bypassing, decoding, bumping, etc) can learn highly advanced and specialized techniques in this course. Topics that cannot be covered in a simple introduction will be demonstrated and perfected over two full days of in-depth instruction. Impressioning fully-functioning keys for unknown locks, manipulating the dials of safes, and advanced lockpicking and lock bumping techniques will be covered in great detail.

NOTE: due to the sensitive nature of the material in this program (most particularly safe-cracking) entry into this course is restricted to Law Enforcement Officers, Government Personnel, and Properly-Credentialed Established Security Professionals only. If taking this course, you must register utilizing a domain name that can verify your place of employment.

Real World Security: Attack, Defend, Repel
//Peak Security

Finally! This is the course on Information Security you've been searching for! "Real World Security: Attack, Defend, & Repel" is a complete 2 day simulation that will not only test your existing skills, but provide you with a real life scenario where you can learn valuable new skills. Whether you work in incident response, active detection and defense, security evaluations, or penetration testing; this course will give you that incredibly rare opportunity to put it all to the test, and learn BOTH sides of the house. Team Fortress 2 meets hacker training.

"Real World Security: Attack, Defend, & Repel" attempts to challenge and motivate information security professionals to hone the knowledge and skills they already have, and also to learn "the other side", as well. The class will be split into two halves, attackers and defenders. On the second day, those two teams will trade sides, allowing every student the opportunity to learn both sides and work with all instructors.

The scenarios and exercises are instructor chosen and lead, and will escalate in tiers of difficulty as the course progresses. What may begin as a simple defense will evolve into something more complicated, based on the scenario.

As is true in the real world, you'll be forced to do your "job" under the restrictions of your company "Boss". Your boss will assign you a specific goal that you need to achieve by the end of the 4th scenario. You'll gather more information about the target, and your own company, as you move through each scenario. In some cases, you may be lucky enough to find new tools to add to your arsenal as you work through each scenario.

The RSA Cryptosystem: Attacks and Implementation Dangers
//Andrew Lindell

Every security professional knows the basics of encryption, but do they really know how it works? The fact is that we often look at cryptographic primitives as mystical black boxes. This is sometimes advantageous but can also lead to misunderstandings and mistakes. For example, it is important to use only standardized schemes. Similarly, in order to properly determine what key lengths must be used for public-key encryption, digital signatures, and key exchange, we need to know what the best algorithms are for attacking these schemes and how they work. Furthermore, we need to look at the history and development of these attacks in order to make safe predictions for the coming decade. Finally, many cryptosystems are broken due to implementations that seem robust but actually leave the door wide open to attack. Without an understanding of these often surprising and elegant attacks, it is almost impossible to implement crypto properly.

In this one-day intensive course, we will focus on the RSA cryptosystem in great depth. Participants will gain a thorough understanding of how the RSA cryptosystem works and the main algorithmic issues that arise when implementing it. In addition, we will study attacks on RSA with a focus on the lessons learned from these attacks. We conclude with a session on choosing key-lengths for RSA-based cryptosystems, based on a comprehensive understanding of the issues involved.

In addition to frontal lectures, this one-day course includes interactive exercise sessions in order to ensure a good understanding of the material studied.

This course is essential to developers who need to understand cryptographic primitives in depth in order to properly use them and also to security professionals who need to make truly informed decisions about what products to use and why.

SAP Security In-Depth
//Mariano Nuñez Di Croce & Juan Pablo Perez Etchegoyen

Have you ever wondered whether your business-critical SAP implementation was secure? Do you know how to check it? Have you imagined which could be the impact of an attack to your core business platform? Do you know how to prevent it? This training is the answer to these questions.

For many years, SAP security has been a synonym of "segregation of duties" or "security roles and profiles". While this kind of security is mandatory and of absolute importance, there are many threats that have been so far overlooked and are even more dangerous, such as the possibility of taking remote control of the entire SAP landscape without having any user in any system.

This training will help you to fill this knowledge gap, allowing you to understand the risks involved and how to mitigate them. You will review the whole picture, from the security of the Environment and the SAP application-level gateways (SAProuter, Webdispatcher), through the assessment and hardening of the Operating Systems and Databases and their interaction with the SAP system up to the security of the SAP Application Layer: Authentication, User security, Password Policies, Authorization subsystem, Interface Security, Web applications Security, Backdoors, ABAP (in)security, Auditing, Monitoring and more!

The training is organized with many hands-on exercises, which will help you grasp practical knowledge quickly. You will learn how to assess the security of an SAP implementation and then secure the critical security gaps you discovered. You will be able to learn how to use different SAP security tools, as well as Bizploit, the first opensource ERP Penetration Testing framework, developed by the instructor.

The training also provides a quick introduction to basic SAP concepts, which allows non-SAP security professionals to follow the course smoothly.

The Shellcode Lab
//Ty Miller

So you have found a vulnerable target. You throw your exploit at it with its default shellcode. You sit there with high hopes of compromising the system, but you don't get a shell. So what happened? There is a good chance the victim machine failed to connect back to you with the pre-packaged shellcode. Wouldn't it be great if you could write your own shellcode to bypass security controls such as firewalls and authenticated proxies to increase your exploitation success rate!

Well now you can!

You will be provided with a "Virtual Shellcode Development Environment" that is designed to enable students to develop shellcode across multiple platforms. Students will learn how to write shellcode for Linux, Mac 64-bit OSX and Windows. The development of the shellcode is presented using easy to learn techniques. Starting off with an introduction to different shellcoding techniques on each platform, an introduction to basic memory management and assembly, followed by creating simple shellcode to write to stdout and call functions.

This gives students a base understanding and practical experience to develop simple shellcode. The complexity is then increased to more useful shellcode such as command execution, dynamic Windows shellcode, setting up backdoor listeners using sockets, shellcode networking to remotely gain a command shell, and egg hunter shellcode to search through memory for our payload. All of this is done whilst holding your hand so that you don't miss a beat. Students will also learn about staged-loading shellcode to bypass security controls such as firewalls and authenticated proxies, and kernel shellcode to perform privilege escalation.

Students are taught how to encode their shellcode using the Metasploit Exploit Framework (MSF), and insert it into exploits that will be used to show that their shellcode was successfully executed. They will learn how to use MSF to generate shellcode for a variety of platforms, as well as how to integrate their shellcode into MSF so that it is available to all Metasploit exploits.

Symmetric Cryptography: Constructions and Cryptanalysis
//Andrew Lindell

Every security professional knows the basics of encryption, but does everyone really understand what a block cipher for example is supposed to achieve? The fact is that we often look at cryptographic primitives as mystical black boxes. This is sometimes advantageous but can also lead to misunderstandings and mistakes. For example, a deep understanding of how block ciphers work is essential in order to understand why it is so important to only use standardized ciphers like 3DES and AES and why modes of encryption are so essential. Such an understanding also clarifies the ramifications of the choice of key-length and block size in a block cipher, and the output length of a hash function. Finally, many cryptosystems are broken due to implementations that seem robust but actually leave the door wide open to attack. Without an understanding of how these primitives really work, it is almost impossible to implement crypto properly.

In this course, participants will gain an in-depth understanding of how symmetric cryptographic primitives are constructed and broken, with a focus on block ciphers and cryptographic hash functions. We will study the main construction paradigms as well as basic cryptanalytic attacks on these primitives. The course also covers important advanced cryptanalytic attacks like differential and linear cryptanalysis, with a focus on how to apply them. Finally, we will study popular constructions like the DES and AES ciphers, and the SHA family of hash functions.

In addition to frontal lectures, the course includes multiple interactive and exercise sessions where participants will be challenged to apply the material learned to new problems.

This course is essential to developers who need to understand cryptographic primitives in depth to properly use them and also to security professionals who need to make truly informed decisions about what products to use and why.

Tactical Exploitation
//Val Smith

Penetration testing often focuses on individual vulnerabilities and services, but the quickest ways to exploit are often hands on and brute force. This two-day course introduces a tactical approach that does not rely on exploiting known vulnerabilities. Using a combination of new tools and lesser-known techniques, attendees will learn how hackers compromise systems without depending on standard exploits. The class alternates between lectures and hands-on testing, providing attendees with an opportunity to try the techniques discussed. A virtual target network will be provided, along with all of the software needed to participate in the labs.

In the first half of the course, attendees will investigate a wide variety of information gathering and footprinting techniques, many of which are critical to a successful penetration test. The Metasploit Framework will be used as a development platform for building custom discovery tools.

In the second half of the course, the focus will shift from information discovery to information exploitation. Attendees will learn how to compromise common operating systems, and once in, how to gain access to the rest of the network.

The course is well-suited to penetration testers of any skill level and all security professionals who have a basic grasp of networking and software exploits. This course differs from a typical ethical hacking program in that the focus is on techniques that are not affected by patch levels. A portion of the class will be dedicated to building new tools, on the fly, to solve the challenges posed by a difficult penetration test.

Tampering with Security Seals
//The CORE Group

Tamper-Resistant Tags and Security Seals are used widely around the world in applications involving inventory coverage and repair, public utility metering, and cargo shipment integrity. These devices are an integral part of our nation's Customs and Border Control enforcement and they are used in the protection and transportation of hazardous chemicals and even nuclear materials. Yet, for all their prevalence, most of these tags and seals are horribly weak and vulnerable to compromise. This training course will discuss in-depth the ways in which many such products function, and students will perform hands-on attacks against the bulk of tamper-resistant devices on the market today. Be prepared for two days of deep knowledge and rolled-up sleeves… as all student stations come equipped with heat guns, solvent chemicals, and a wide range of tools and trickery.

TCP/IP Weapons School 3.0: Black Hat Edition
//Richard Bejtlich, Taosecurity

Is your network safe from intruders? Do you know how to find out? Do you know what to do when you learn the truth? If you need answers to these questions, TCP/IP Weapons School 3.0 (TWS3) is the Black Hat course for you. This vendor-neutral, open source software-friendly, reality-driven two-day event will teach students the investigative mindset not found in classes that focus solely on tools. TWS3 is hands-on, lab-centric, and grounded in the latest strategies and tactics that work against adversaries like organized criminals, opportunistic intruders, and advanced persistent threats.

Ultimate Hacking: Black Hat Edition
//Foundstone

Foundstone created the ultimate in "Hands On" security training. Designed to arm security pros with the skills to keep hackers at bay, Ultimate Hacking: Black Hat Edition is an action-packed two-day intensive class covering the latest methodologies, tools, and techniques necessary to secure an organization. This special "Black Hat" edition is a derivative of the longer Ultimate Hacking class that is taught to the general public, the military, and many government agencies. Foundstone has taken the best content from Ultimate Hacking and created a shorter, accelerated version for Black Hat.

Ultimate Hacking Black Hat Edition begins from a "zero-knowledge" perspective. Start by profiling your target, then learn how to identify and exploit well-known and obscure vulnerabilities in the most popular operating systems including Windows and multiple Unix flavors.

But don't just listen to us—put your skills to use and learn by doing. Foundstone challenges you with countless hands-on exercises to demonstrate your expertise as you race other students to achieve the ultimate goal…getting root.

Ultimate Hacking: Wireless Edition
//Foundstone

Mission-critical data, secrets and other company information transmitted into the air cause hackers everywhere to rejoice!

Wireless networks bring unique challenges to those tasked with their defense. How confident are you that your wireless infrastructure can withstand the latest attacks by the world's cleverest hackers? Do vendors' claims tell the whole story? Where is your Achilles heel? Beyond the authorized wireless infrastructure you know exists in your organization, what about the wireless networks that aren't supposed to be there? Do you know when an onsite vendor or consulting company tucked away in a forgotten conference room plugs in their mobile access point?

What about that temporary access point in a QA lab that is still there months later? What about the wireless clients themselves? Laptops, smart phones, printers, VoIP phones, HVAC systems, and even the remote controls in your executive board rooms are all using wireless technologies. Organizations may have a secured wireless infrastructure but find themselves in trouble when these untamed devices are coaxed into connecting to a clever hackers fake access point. Untamed devices that are jacked into your companies ethernet seeking tools like "linksys" are creating a bridge for attackers to get onto your internal network.

Foundstone's internationally renowned, "Ultimate Hacking: Hands On" series goes wireless to help you see your wireless networks the way hackers see them. Learn the tools, techniques and methods attackers use against you in order to develop an effective defense against their increasingly sophisticated onslaught. Knowledge is power and you do not want the hackers to know more about your wireless networks than you do…

Virtualization for Incident Responders: Principles and Techniques for Recovering Evidence from Virtualized Systems and Cloud Environments
//Eric M. Fiterman, Methodvue

The cost and efficiency benefits to virtualization and cloud computing have driven many organizations to dramatically consolidate physical infrastructure, greatly reducing the complexity of provisioning IT resources and inventory in a heterogeneous IT environment. As more infrastructure and storage are virtualized, first responders will be increasingly tasked with recovering, restoring, and analyzing evidence that may not be found using traditional means. This course is intended for information security personnel who are responsible for handling incidents involving virtual infrastructure, cloud service providers, or desktop virtualization platforms.

The Web Application Hacker's Handbook, 2nd Edition: Live!
//Dafydd Stuttard & Marcus Pinto

Our "Web Application Hacker's Handbook" is still the most deep and comprehensive general purpose guide to hacking web applications that is currently available. But not for long, because the 2nd Edition is just around the corner.

So if you're a fan of the original or want to try your hand exploiting everything in it, you've come to the right place. But this year you're in luck with the 2nd Edition nearing publication, we're putting out a one-off preview class and you will get the chance to learn from the authors (and hack) what we've put in, before it hits the printers!

Did we mention Burp Suite? If you want to learn from the author of Burp, you're in luck again… We have run courses for over 5 years at Black Hat, and we know what you want. This structured course is balanced at 120 slides with numerous opportunities to watch instructor-led demos, whilst hacking your way through over 150 lab exercises, spanning .Net, J2EE, PHP and finishing with a "Capture the Flag" contest.

In our labs, no question is left unanswered (or unsolved)!

Web Application (In)Security
//John Heasman & Daniel Martin

Finally, the long awaited successor to NGS's hugely popular Web Application (In)Security Course is coming to BlackHat Vegas this year! The course has been completely updated with new challenging labs, demos and material which cover both the fundamentals of web application assessment and as well as key web technologies such as Ruby on Rails, Flex Remoting, Silverlight WCF, Java Server Faces, HTML5 and NoSQL.

This is a cutting-edge, hands-on course aimed at hackers who want to exploit web applications, and developers who want to know how to defend them. The course covers the entire process of hacking a web application, from initial mapping and information gathering, through to advanced exploitation techniques.

This year, the course contains more than 300 brand new lab examples, containing virtually every vulnerability that has ever been found in web applications. Even the most capable hackers will be challenged and find plenty to take away. We will also demonstrate the very latest hacking techniques developed over the past year.

The course concludes with a catch-the-flag contest, where participants try out their skills against a series of challenging scenarios, with prizes for winners. Attendees are expected to be familiar with core web technologies like HTTP and JavaScript.

A terrific resource for this course is the book "The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto. The book is available for purchase from Amazon.com and provides pertinent and relevant information directly related to the course.

Web Security
//Elie Bursztein

The Web Security course gives a 360-degree overview of web application security, with in-depth treatment of several significant topics such as user authentication, browser security, business logic, data handling, and distributed threats. For every presented we cover motivating attacks, defense mechanisms, and security tools and techniques. Throughout the course, we balance cutting-edge research results with practical skill development.

The goal of the course is to teach modern web application security to IT professionals who have some prior understanding of web technologies (e.g. HTML, CSS, JavaScript), and to give IT decision-makers the tools necessary to evaluate and navigate this complex landscape.

Windows Physical Memory Acquisition and Analysis
//Matthieu Suiche

In this live incident response and forensics course, students will learn using software based acquisitions methods about different full memory dump file format (Microsoft Hibernation file, Microsoft crash dump, and raw dump). Using MoonSols Windows Memory Toolkit (win32dd, win64dd, hibr2bin, hibr2dmp, dmp2bin, bin2dmp, etc). Students will learn the difference between hardware and software acquisition method. Based on this, they will learn how to do advanced analysis of these dumps, such as the hibernation file, using the Microsoft Debugger WinDbg. The analysis part of the training will explain basis of processor memory management, Windows memory and process management internals, WinDbg SDK and scripting. At the end of the course, students will be able to analyze a Windows Hibernation File from Windows 7 x64 with WinDbg. The students will also be able to perform a "cloud memory analysis" for VMWare Workstation and Microsoft Hyper-V R2 products.

Virtual Training

Hacking by Numbers: Cadet Online Edition by SensePost // June 13-16

Make the most of your time! This course is an introduction to the art and science of computer hacking. If you take this course online, you will be prepared to take a more advanced Hacking by Numbers course at Black Hat USA 2011. Registrants who complete the Virtual Training will receive a $500 discount good towards another SensePost live training course at Black Hat USA 2011.

7.30.2011 - 8.4.2011 | LAS VEGAS, NEVADA

black hat
DIGITAL SELF DEFENSE
1932 1st Avenue #204
Seattle, WA 98101

black hat
BRIEFINGS & TRAINING

Six days. Fifty-six classes. Ninety presentations.

Black Hat Briefings & Training USA 2011
July 30-August 4 // Caesars Palace // Las Vegas

EMBEDDING SECURITY
WWW.BLACKHAT.COM

//welcome

Black Hat's flagship event returns for its fourteenth year to Caesars Palace Las Vegas. Black Hat is best known for its intense, informative, cutting edge, no vendor-pitch sessions that often showcase never before seen techniques and research.
Amongst the offerings this year:

- 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.
- Over 50 different training classes offered on weekend and weekday sessions to make this one of the comprehensive top level security training events in the industry.
- The Briefings will be comprised of in depth presentations consisting of seven Briefings tracks and two Workshop tracks running concurrently over two days for a total of over 90 sessions.
- Black Hat Arsenal returns for its second year. This enormously popular area will highlight open source and free tools.
- Executive Briefing for C-level delegates which will take place the day before the start of the Briefings.
- Networking opportunities with over 5000 of your peers from over 40 nations

Register with the code **B1H1UGSA** and receive 20% off your registration
*Discount is only good towards new registrations.

//about Black Hat

The Black Hat Briefings are a series of highly technical information security conferences that bring together thought leaders from all facets of the infosec world—from the corporate and government sectors to academic and even underground researchers. The environment is strictly vendor-neutral and focused on the sharing of practical insights and timely, actionable knowledge. Black Hat remains the best and biggest event of its kind, unique in its ability to define tomorrow's information security landscape.

In addition to the large number of short, topical presentations in the Briefings, Black Hat also provides hands-on, high-intensity, multi-day Trainings. The Training sessions are provided by some of the most respected experts in the world and many also provide formal certifications to qualifying attendees.

Black Hat's decade of leadership attracts the most prestigious names from the full spectrum of security thinkers, and ensures that the conference stays on the leading edge of new security trends as they emerge. Our commitment to delegate feedback also helps keep our presentations aligned to the needs and desires of our delegates.

From its inception in 1997, Black Hat has grown from a single annual conference in Las Vegas to a global conference series with annual events in Abu Dhabi, Barcelona, Las Vegas and Washington DC. It has also become a premiere venue for elite security researchers and the best security trainers to find their audience.

//briefings

Spanning two days with fourteen separate tracks, our speakers will be releasing current "never before seen" tactics, tools and research. A complete listing of speakers, session titles and topic descriptions can be found at www.blackhat.com

//presentations

Apple iOS Security Evaluation: Vulnerability Analysis and Data Encryption
Dino Dai Zovi

Covert Post-Exploitation Forensics With Metasploit
Robert McGrew, National Forensics Training Center and McGrewSecurity

Crypto for Pentesters
Thomas Ptacek, Matasano Security

Going to Lahore
Mikko Hypponen, F-Secure

Hacking .Net Applications: The Black Arts
Jon McCoy, .NET Software Engineer

Owning Your Phone at Every Layer: A Mobile Security Panel
Moderator: Tyler Shields, Veracode Research Lab

Reviving Smart Card Analysis
Karsten Nohl, Cryptographer & Security Researcher and Chris Tarnovsky, Flylogic

Server-Side JavaScript Injection: Attacking NoSQL and Node.js
Bryan Sullivan, Adobe

Sophail: A Critical Analysis of Sophos Antivirus
Tavis Ormandy, UNIX Security Researcher

//workshops

A Taste of the Latest Samurai-WTF DVD
Justin Searle, InGuardians

Investigating Live CDs using Volatility and Physical Memory Analysis
Andrew Case, Digital Forensics Solutions

Zero Day Malware Cleaning with the Sysinternals Tools
Mark Russinovich, Windows Azure Group at Microsoft

Infosec 2021 - A Career Odyssey
Lee Kushner, LJ Kushner and Associates

//special events

Black Hat Arsenal: Tool/Demo Area
//August 3-4
Back by popular demand, Black Hat is pleased to offer a Tool/Demo area for independent researchers and the open source community that will allow delegates to view and test tools firsthand and have direct access to the developers of the tools.

Black Hat Bookstore: BreakPoint Books
//July 31-August 4
Come by the official bookstore and browse and purchase the latest titles in security.

Black Hat Circuit
//August 3
When the annual Black Hat reception starts to wind down and you're looking for a place to go, don't fret, because the Black Hat Circuit will just be getting warmed up. The Black Hat Circuit will feature themed rooms from key exhibitors; offering conference delegates a venue to continue their technology conversations and networking activities. Participating Circuit sponsors have gone the extra mile in providing food and drinks.

Black Hat Embassy: Media Partners
//August 3-4
Come by the Embassy and learn more about venerable institutions such as DoD, FBI, Cloud Security Alliance, ISSA, EFF and more.

Black Hat Executive Briefing
//August 2
One hundred executives from Global 2000 corporations and federal agencies are invited to attend a full day of high-level discussions about topics unique to Black Hat.

The Executive Briefing will begin with an introduction from one of the highest-ranked US government officials, discussing the importance of cyber security to homeland security.

The morning sessions will preview the most important technical discussions planned for the main Black Hat Briefings. Lead by Jeff Moss, founder of Black Hat and DEF CON, these previews will enable executives to discuss the implications of the newest vulnerabilities and attacks with their peers and the actual researchers. Executives can then use this knowledge to prepare their teams ahead of time and direct their technical experts to the most important research being released. The afternoon sessions will include a number of strategic discussions around the latest threats to the public and private sectors and long-term countermeasures to be taken into consideration.

Black Hat Merchandise Store
//August 2-4
Get your Black Hat branded merchandise - t-shirts, jackets, mugs, barware, lab coats and more!
Please note: No cash will be accepted. Purchases can be made with any major credit or debit card.

Black Hat Exhibit Hall
//August 3-4
Here is your chance to meet with and explore the offerings that the top security companies have to offer.

Black Hat Workshops
//August 3-4
In our experience, Security professionals are always looking for the latest tools and resources to perform their jobs effectively and efficiently. This year we will be hosting two tracks of security workshops to provide delegates a deeper understanding with regards to a specific subject. These tracks will run concurrently with the Briefings presentations and are available to all persons holding a Briefings pass.

What we hope to achieve: Greater awareness and access to terrific work for the security world at large. These will be deep technical sessions that can give delegates a chance to delve deeply into tech and hopefully take away practical applications to the information presented.

DEF CON
Planning on attending DEF CON this year but don't want to head to the Rio and potentially miss out at Black Hat? As a registered Black Hat USA 2011 attendee you can now pre-purchase your DEF CON pass and save $50 off of the $150 DEC CON registration price.

Event Audio & Video: The Source of Knowledge
//August 3-4
Afraid you'll miss a session? The Source of Knowledge will be onsite to sell audio and video recordings of the Briefings sessions. Media, including iPad ready presentations may be purchased onsite at a substantial discount.

Hacker Court
//August 3
This is the tenth year anniversary of the venerable Hacker Court. Come by the session to see an engaging mock trial that demonstrates legal issues in cyberspace. All events are fictitious, but legally accurate.

PWNIE Awards
//August 3
In 2011 the Black Hat USA Briefings are once again providing the venue for the Pwnie Awards, the security industry's premier award show celebrating the achievements and failures of the security community over the past year. For more information about the awards or to submit a nomination, please visit the official Pwnie Awards website at http://pwnies.com

Uplink: Streaming Live from Black Hat USA
//August 3-4
This year thousands of security professionals from around the world are making plans to be a part of Black Hat USA 2011. But not all of those people will actually be in Las Vegas. With Black Hat Uplink, you can experience essential content that shapes the security industry for the coming year—for only $595.

Now you can get a taste of Black Hat USA from your desk–this year's live event will be streamed directly to your own machine with Black Hat Uplink:

- Access to the seven Briefings tracks on each day of the Briefings and the keynotes—a total of 70+ possible sessions to view.
- Post-conference access to Uplink content; go back and review the presentations that you missed or watch the presentations that interested you the most as many times as you want for up to 60 days after the event.
- Get show promotional pricing for the "Source of Knowledge" DVDs should you wish to purchase ALL of the recordings from Black Hat USA and/or DEF CON 19.

//sponsors

diamond

Qualys

platinum

Cisco
LogRhythm — Comply. Secure. Optimize.
Microsoft
nitrosecurity
rackspace Hosting
RSA
Symantec

gold

ArcSight — An HP Company
Core Security Technologies
IBM
IOActive — Comprehensive Computer Security Services
McAfee
NetWitness
Norman
Novell
Rapid7
red lambda
Solera Networks
Trustwave — Security begins with Trust

silver

Accuvant Labs
Adobe
Fluke networks
amazon.com
Blue Coat
BluePoint Security — Revolutionizing computer security
Cenzic
Damballa
Dell SecureWorks
eEye Digital Security
Fidelis Security Systems
Foreground Security
Fortify — An HP Company
GFI
Guidance Software
HBGary
Imperva
Integralis — An NTT Communications Group Company
loglogic
mocana
NCP Secure Communications
NetOptics
phishme.com
Pico — tiny mighty machines
Qualcomm
radware — Smart Network. Smart Business.
RedSeal
rune — Information Security Corporation Pte Ltd
SAINT
splunk>
SRA International, Inc. — Honesty and Service
StillSecure
Stonesoft
Tenable Network Security
TippingPoint
WhiteHat Security
Venafi

additional supporter

MITRE

//registration

Register early and receive substantial savings off the onsite cost of your registration.

//briefings:

Early:	$1495 // ends April 30
Regular:	$1695 // ends June 15
Late:	$2095 // ends July 29
Onsite:	$2495 // July 30–Aug 4
Training:	$1000–$5100 per course

//group registration:

Register with a group and Save: 10% off of Briefings for groups of six or more and 15% off of Briefings for groups of twelve or more. For more information on Group Registration, visit www.blackHat.com

//venue

//Caesars Palace Las Vegas

Black Hat returns to the fabulous Caesars Palace in action-packed Las Vegas. Leave your business attire at home. Dress is casual, promoting a great learning environment for all delegates. All Black Hat sessions and events will take place at Caesars Palace. Take advantage of the hotel's central location and have convenient access to the conference floor and to a plethora of other activities.

The Black Hat group rate closes on July 3. Take advantage of discounted room rates by reserving your room early.

Group discount code: SCBLA1
Reservations: +1 866 227-5944

//sustaining sponsors

Core Security Technologies
IBM
IOActive
Microsoft
NetWitness
Qualys
Trustwave

training matrix

CATEGORY

course name	auditing & assessment	application security & development	certification	cryptography	forensics	hardware	malware analysis	managerial/policy	network	physical security	reverse engineering	system administration	virtualization	vulnerability & exploit development
Advance Malware Analysis by MANDIANT							x							
Advance Malware Deobfuscation by Bixtor Technologies							x							
Advance Memory Forensics in Incident Response by Jamie Butler & Peter Silberman					x									x
Adv. Vulnerability Scanning Techniques Using Nessus by Paul Asadoorian, Tenable Network Security	x													
Advance Windows Exploitation Techniques by Offensive Security			x											x
Application Security: For Hackers and Developers by Jared De Mott, Crucial		x												x
Assessing and Exploiting Web Applications with Samurai-WTF by Justin Searle & Kevin Johnson	x													
Building, Attacking a Defending SCADA Systems in the Age of Stuxnet by Tom Parker	x					x			x					
Building A Better Mousetrap by Rohit Dhamankar & Rob King							x		x					
CISSP Boot Camp by Logical Security-Shon Harris			x											
CNSS-4012 Senior System Manager/CNSS-4015 System Certifier Combination Course by IA2			x											
CNSS-4016 Risk Analyst by IA2			x											
Cyber Network Defense Bootcamp by Adam Meyers							x	x	x					
Designing Secure Protocols and Intercepting Secure Communications by Moxie Marlinspike				x					x					
Detecting & Mitigating Attacks Using Network Infrastructure by Cisco									x					
Digital Intelligence Gathering Using Maltego by Paterva	x													
Effective Fuzzing: Using the Peach Fuzzing Platform by Michael Eddington	x	x												x
Enterprise Security from Day 1 to Completion by Chris Conacher	x						x							
Exploit Laboratory By Saumil Shah	x													x
Exploit Laboratory: Black Belt Edition by Saumil Shah	x													x
Hacking and Securing Oracle (Crash Course) by Alexander Kornbrust & Sumit Siddharth	x													
Hacking By Numbers: BlackOps Edition by Sensepost	x													
Hacking By Numbers: Bootcamp by Sensepost	x													
Hacking by Numbers: Cadet by Sensepost	x													
Hacking By Numbers: Combat by Sensepost	x													
Hacking by Numbers: Unplugged by Sensepost									x					
Hacking by Numbers: W^3 by Sensepost	x	x												
Hands-On Hardware Hacking & Reverse Engineering Techniques by Joe Grand						x					x			
IDA Pro Class: Reverse Engineering with IDA Pro by Chris Eagle											x			
Incident Response: Black Hat Edition by MANDIANT					x			x	x			x		
Infrastructure Attacktecs & Defentecs: Hacking Cisco Networks by Steve Dugan									x					
Introduction to Malware Analysis by Bixtor Technologies							x							
Macsploitation by Vincenzo Iozzo & Dino Dai Zovi	x	x												
Malware Analysis: Black Hat Edition by MANDIANT							x				x			
Mobile Hacking by HotWAN	x													
NBISE BQST (Basic Qualified Security Tester) Pen-Testing Exam Review Course by Veris Group	x													
Offensive Countermeasures: Defensive Tactics that Actually Work by PaulDotCom	x								x			x		
Pentesting with BackTrack by Offensive Security	x													
Pentesting with Perl by Joshua Abraham	x													
Physical Penetration Testing: Advanced by The CORE Group										x				
Physical Penetration Testing: Introduction by The CORE Group										x				
Real World Security: Attack, Defend, Repel by Peak Security	x								x			x		
RSA Cryptosystems by Andrew Lindell				x										
SAP Security In-Depth by Onapsis	x	x												
The Shellcode Lab by Ty Miller														x
Symmetric Cryptography by Andrew Lindell				x										
Tactical Exploitation by Val Smith	x								x					
Tampering with Security Seals by The CORE Group										x				
TCP/IP Weapons School 3.0 by Richard Bejtlich	x													
Ultimate Hacking: Black Hat Edition by Foundstone	x													
Ultimate Hacking: Wireless Edition by Foundstone									x					
Virtualization for Incident Responders by MethodVue					x								x	
Web App Hacker's Handbook by Dafydd Stuttard & Marcus Pinto	x	x												
Web Application (in)Security by John Heasman & Daniel Martin	x	x												
Web Security by Elie Burszstein	x	x												
Windows Physical Memory Acquisition & Analysis by Matthieu Suiche					x									