Cybersecurity Workshop Series

Fundamentals of Software Assurance (3 Days)

The Sage Group's three-day workshop provides participants with a high-level overview of various aspects of Software Assurance in the context of a modern and Internet-connected environment. Through lecture, hands-on exercises, and group discussion, participants will gain a foundational perspective on the challenges of security software design and procurement, implementing secure software and other factors needed for a comprehensive software assurance solution. Upon completion of this workshop, each participant will be able to define software assurance terminology, compliance requirements, review software assurance principles, and gain an understanding of the impact of current threat trends on security software implementation.

Secure assurance refers to the ability to ensure security personnel, software implementers, purchasers, and users with a level of confidence that software will consistently operate in accordance with its intended goals. It includes software security, the process by which the software can operate effectively and securely even when it comes under attack. Ideally, assured software will not contain faults or weaknesses that can be exploited either by human attackers or by the insertion (intentional or unintentional) of malicious or poor code.

Section 1: Introduction to Software Assurance
Section 2: Why is Software at Risk
Section 3: Requirements for Secure Software
Section 4: SwA Initiatives, Activities, and Organizations
Section 5: Final Practical Exam/CAPSTONE Exercise

Cyber Tools and Analysis (4 Days)

Do you want to better understand how to use cyber tools in securing networks? Would you like to be better prepared to answer fairly technical security questions about Microsoft Active Directory, UNIX, Linux, databases, firewall, intrusion detection systems and major network services like the Domain Name Service? Would you like a combination of professional instruction and well-structured hands-on experiences securing these operating systems, applications and infrastructure?

The Sage Group's Cyber Tools and Analysis Hands-on Workshop concentrates on cyber security tools, operating systems, applications, network architectures and best practices in government and industry network security. The workshop uses a fifty percent hands-on approach (25 lab experiences) to focus not only on tool deployment and operation system configuration, but on cyber security network defense and analysis techniques. Participants will configure multiple operating systems, practice network defense techniques, and understand attack prevention methods in a state of the art security lab. No experience is required; however an understanding of technical security controls or some previous experience with system administration will enhance learning.

THE SAGE GROUP

Phone 877-697-2434
fax 877-697-2434
www.thesagegrp.com

Cybersecurity Workshop Series

IPv6 Practical Application & Implementation (3 Days)

The Sage Group's IPv6 Fundamentals and Implementation three-day hands-on training boot camp provides the latest skills and knowledge regarding IPv6 technology. The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared to 32 bits in IPv4, to enhance VoIP, QoS and security within your organization. This workshop will deep dive into such areas as Access Control Lists, IP Security and DNS implementation within an IPv6 network.

All participants will gain real world experience with IPv6 during their hand-on lab exercises as they create a plan that covers IPv6 implementation for DNS, mobility, multicasting, security, transition mechanisms, routing, and other IPv6 routing protocols. The IPv6 Fundamentals and Implementation training boot camp is concluded by a major technical hands-on lab where the class is divided into teams and gets to design and implement IPv6 according to 5 scenarios (the last scenario simulates merging of 2 organizations).

Topics Covered

- Fundamentals of IPv6
- The difference between IPv4 and IPv6
- IPv6 Internals (functionality of the various sub-protocols of IPv6)
- Implementing IPv6
- Planning IPv6 Implementation

Windows 8 and Server 2012 Security (3 Days)

The Sage Group's three-day hands-on Windows 8 and Server 2012 Security training and certification boot camp in Washington, DC or Live Online will show you how to secure Windows by hacking it! The class focuses on securing Windows 8 and Server 2012 by teaching you hands-on methods by which malicious attackers attack these platforms.

All attendees will be given remote access to the lab network via a web browser. The environment is completely virtual and completely yours and yours alone. You won't have to worry about sharing computers, or other participants attacking the same machines that you are.

Day 1: Attacking Windows 8

- Finding and exploiting vulnerabilities
- Bypassing Anti-virus
- New hacking tips and tricks with PowerShell

Day 2: Attacking Windows Webservers

- SQL Injection
- Cross site scripting
- File handling vulnerabilities
- .NET vulnerabilities

Day 3: Attacking Active Directory

- Credential harvesting
- Attacking the infrastructure with PowerShell
- Enumerating Active Directory
- Gaining Domain administrator level access

Advanced Systems and Applications Attack & Defense (5 Days)

The Sage Group's five-day Advanced Systems & Applications Attack & Defense boot camp was created for Network/Web Application Penetration testers that are looking for the little tips and tricks that will help them better attack high security environments. Participants that are Network/System Administrators with three or more years' experience working in environments such as financial institutions, DoD networks, or similar high security environments will benefit greatly from this workshop.

Topics Covered

- Attacking From the Outside
- Bypassing Anti-Virus & HIPS
- DLL Injection & Process Injection
- Advanced Post-Exploitation
- Capture the Flag Team Hacking

Cybersecurity Workshop Series

Mobile Application Security/Mobile Hacking (5 Days)

The Sage Group's five-day workshop focuses on hands-on mobile security. You'll start off with setting up your environment (emulator/sdk/hardware/etc.). Once done the workshop quickly moves into using your device as an attack platform. From there the workshop goes into the basics of forensics, reverse engineering mobile applications, exploiting mobile applications on each respective platform, and finally on to attacking web services from each platform.

Day 1 and 2: Android

- Building the Android environment
- Using Android as a Pentest Platform
- Reverse engineering Android apps
- Exploiting Android apps
- Attacking web services via Android apps
- Android forensics

Day 2-5: iPod/ iPhone/iPad

- Building the iPod/iPhone/iPad testing environment
- Using iPod/iPhone/iPad as a Pentest Platform
- Jail Breaking iDevices
- iDevice forensics
- Reverse engineering iPod/iPhone/iPad apps
- Exploiting iPod/iPhone/iPad apps

Exploit Development (5 Days)

The Sage Group's five-day workshop takes participants from relatively little exposure to the subject of exploit development to covering some very advanced concepts in the span of just five days. We begin the class with lower level, easy to grasp topics and then expand on those rapidly throughout the week.

For participants with a limited programming background and experience, worry not! Templates are provided for each exploit with the intent to cut down on the raw programming time in class, instead focusing more on the methodology and mindset that goes into writing these different exploits.

Here are some of the topics to look forward to:

- Stack Overflows (in both Linux and Windows)
- Abusing structured exception handlers on Windows
- Shellcoding Tricks (Negative jumps, egghunters, fragmented shellcode)
- Browser, PDF, and ROP exploits

Advanced Malware Analysis (5 Days)

The Sage Group's five-day immersion workshop is focused on hands-on malicious code analysis. You'll learn how to perform both dynamic and static analysis on all major file types (PE files, Office Documents, PDF documents, etc.). You'll learn how to do volatile memory analysis (carving malicious executables of RAM), and you'll also learn how to de-obfuscate malicious JavaScript.

Day 1: Dead Box Forensics

- Recovering deleted files
- Dealing with steganography
- Dealing with encryption

Day 2: Dynamic Analysis

- Building an analysis environment
- Identifying malicious activity

Day 3: Static Analysis

- Building a malware database archive
- Identifying malicious capability

Day 4: Network Traffic Analysis & Network IDS Signature Development

- PCAP analysis
- IDS signature development

Day 5: Browser Forensics & Memory Analysis

- Mass injection analysis
- Charting malware redirection
- Carving executables out of RAM

Cybersecurity Workshop Series

Python Immersion (5 Days)

The Sage Group's five-day Python Immersion workshop is for security professionals that have very little programming experience.

If you've ever struggled in a programming class because you wanted the instructor to put programming concepts in plain and simple English – this class is for you.

If you've ever tried learning programming from a book that spent too much time on math, and writing absolutely programs like a CD collection database – this class is for you.

If you've ever wanted a programming workshop to be about stuff you could actually use at work – this class is for you.

This is a functional programming workshop focused on programming concepts that can be used to accomplish common security tasks such as log parsing, password cracking, port scanning, vulnerability testing, web application security testing, malware analysis, and exploit development. There won't be a bunch of math, no CD collection databases, and no useless programming mumbo jumbo.

Each day the participants will learn a few basic programming concepts, and then use some sample code (skeleton scripts) to perform security tasks. The participants will keep the skeleton

scripts so that when they get back to work they'll have something that they can use a crib sheet to do other security tasks.

Day 1: Programming Concepts, Parsing Files, Logs, and PCAPs

- Python basics
- Text file parsing
- Log parsing
- PCAP parsing

Day 2: System Administration and Password Cracking

- Windows and *nix administration
- Password cracking
- Netcat-like functionality
- Port-scanning

Day 3: Network and Web Application Vulnerability Testing

- Vulnerable Service Identification
- SQL injection
- XSS
- RFI/LFI

Day 4: Forensics and Malware Analysis

- Memory analysis
- Identifying/classifying malware
- HexEditing/disabling malware

Day 5: Reverse Engineering, Fuzzing and Exploit-Dev

- Debugging
- Protocol fuzzing
- File format fuzzing
- Exploiting software

THE SAGE GROUP

Phone 877-697-2434
fax 877-697-2434
www.thesagegrp.com