EC-Council

CAST

CENTER FOR ADVANCED SECURITY TRAINING

CAST 614

Advanced Network Defense

Make The Difference

About EC-Council Center of Advanced Security Training (CAST)

The rapidly evolving information security landscape now requires professionals to stay up to date on the latest security technologies, threats and remediation strategies. CAST was created to address the need for quality advanced technical training for information security professionals who aspire to acquire the skill sets required for their job functions. CAST courses are advanced and highly technical training programs co-developed by EC-Council and well-respected industry practitioners or subject matter experts. CAST aims to provide specialized training programs that will cover key information security domains, at an advanced level.

Advanced Network Defense

Course Description

With this course you can be among the few who transcend the old idea of the hacker having all the fun, take pride being the defender, form an offensive mindset to skillfully orchestrate robust and solid defenses and reinvent popular belief by beating the hacker at his own game.

You will be evaluating advanced "hacks" and methods of defense fortification bringing you closer to establishing perfect security by reviewing best practices and methodologies you can apply to secure environments, provide segmentation and isolation to reduce the effectiveness of the Advanced Persistent Threat.

The course will cover fundamental areas of fortifying your defenses; you will discover methods of developing a secure baseline and how to "harden" your enterprise architectures from the most advanced attacks. Once a strategy for a fortified perimeter is defined the course moves on to defending against the sophisticated malware that is on the rise today and the importance of "live" memory analysis and real time monitoring.

Key features of CAST On-site:

01 Each of the courses selected from the CAST Advanced Training Suite will be specifically designed to meet the needs of each individual, based according to their current skills and pace of learning to meet your organisation's unique objectives and goals

02 CAST On-site expert/trainers will be flown down to your premise of choice at a date most suitable to you

03 CAST On-site allows students to receive training in more manageable sessions arranged over a spread of a few days that allowing for greater absorption of knowledge with an opportunity to practice and verify the new skills after each session prior to commencing the next one

04 With CAST On-site Advanced Security courses students will be able to take advantage of directly conversing with the chosen expert in matters unique to the student and your organisation

05 You can be rest assured that all challenges and objectives pertaining to your organisation's goals can be discussed in an environment that ensures complete confidentiality

06 Each individual client receives the required high level of training that is benchmarked to international best practise and standards

07 Each student receives a CAST Advanced Security Training Courseware that allows them to follow and revise the material that has been taught to them

08 Upon completion of the course, each student will receive a CAST On-Site Advanced Security Training certificate of attendance

CAST

EC-Council

How will this course benefit you?

01 Executing a set of techniques that are critical to the protection of your entire enterprise against some of today's most advanced threats

02 Reviewing methods of system deployments in as secure a state as possible while supporting your daily business requirements

03 Applying necessary techniques required for malware identification throughout the enterprise even in the case of the malware not being detectable by any of your security controls

04 Staging Advanced Attacks to appreciate methods of correctly eliminating or mitigating risk to an acceptable level

Who Should Attend

Firewall administrators, system architects, system administrators, windows admin or those responsible for or interested in:

- Identifying security weaknesses in computer systems or networks
- Exposing weaknesses for system's owners to fix breaches before being targets of compromise
- Applying hacking and pen testing constructively to defend against various possible attacks
- Analysing best practices in developing secure system and network configurations
- Establishing a secure baseline in deploying machines in a protected state
- Appreciating popular attack methods applied by hackers in order to fortify their systems

From practically any organization that handles important data would find this course beneficial, examples are:

- Government agencies
- Universities
- Hospitality
- Retail
- Banking and Financial institutions
- Brokerage and Trading firms
- Insurance
- Scientific institutions & research agencies
- Telecommunication
- Computer design firms
- Consulting firms
- Science and Engineering firms
- Those involved with online related businesses & transactions
- Card related businesses

CAST

EC-Council

Course Outline

01. Firewalls

- Firewalls
- Firewall Types: Stateless Packet Filters
- Improving Device Remote-Access Security
- Locking Down the Console Port
- Protecting Terminal Lines
- Establishing Encrypted Communications
- Configuring HTTPS
- Configuring SSH

LAB: Securing the Perimeter

02. Advanced Filtering

- Advanced Filtering Techniques
- Ingress Filtering
- Egress Filtering
- Source Address Verification (SAV)
- uRPF
- Additional Filtering Considerations
- Time-Based ACLs
- Reflexive ACLs
- Reflexive ACL vs. Static ACL
- Context-Based Access Control (CBAC)
- Essential Steps to Harden Routers

LAB: Advanced Filtering

03. Firewall Configuration

- Advanced Filtering Techniques
- Firewall Types: Stateful Packet Filters
- Application Proxies
- Application Proxies vs. Stateful Packet filters
- Web Application Firewalls
- Web Application Firewall Types
- Web Application Firewall Products
- Firewall Architecture
- Screened Subnet Firewall
- The Classic Firewall Architecture
- Belt and Braces Firewall
- Separate Services Subnet
- Fortress Mentality
- De-parameterization
- Perimeter Configuration

Lab: Selecting a Firewall Architecture

04. Hardening: Establishing a Secure Baseline

- Windows NT/2000/2003 and XP
- Windows 2000/2003/XP
- Windows 2003
- Windows Vista
- Server 2003 Architecture
- Broken Kernel
- Modes of the OS
- UNIX/Linux
- Secure Server Guidelines
- Hardening Systems
- Security Compliance Manager
- Device Security
- Essential Steps to Harden Switches

LAB: Hardening

Windows Server 2008 Security (Part I)

- Server 2008 Components
- Enterprise Protection
- AD RMS
- AD RMS Components
- EFS
- EFS Enhancements in Server 2008
- EFS Best Practices

LAB: Server 2008 Lab

Windows Server 2008 Security (Part II)

- IPsec Rules
- Firewall Scripting
- netsh
- Isolating a Server
- Group Policy Object
- Server Isolation Steps
- Domain Isolation
- Domain Isolation Issues
- Best Practices
- Trusted Platform Module
- Wave Systems
- TPM Architecture
- Crypto API
- Example
- Embassy Server Software
- Embassy Client Software
- Self-Encrypting Drives

LAB: TPM

05. Intrusion Detection and Prevention Why Intrusion Detection?

- Windows NT/2000/2003 and XP
- Fortress Mentality
- Intrusion Detection 101
- What is Intrusion Detection?
- False positives!
- Topology concerns
- Recommended in most circles
- Realistic
- Intrusion Prevention
- Types of IPS
- Host-Based Intrusion Prevention Systems
- Host-Based Intrusion Prevention Systems

LAB: Intrusion Detection

06. Protecting Web Applications

- Windows NT/2000/2003 and XP
- Top 10 www.owasp.org
- Injection Flaws
- Cross Site Scripting
- Broken Authentication
- Insecure Cryptographic Storage
- Reverse Engineering Web Apps
- Tools
- Hackbar
- Tamper Data
- The Two Main Attacks for Web
- XSS
- SQL Injection
- xp_cmdshell
- There is More
- More Tools
- SQL Inject Me
- XSS ME
- Choose The Right Database
- Practice, Practice, Practice
- Tutorials
- Mutillidae
- Web Application Firewalls
- Components of Web Application Firewall

LAB: Protecting Web Apps

07. Memory Analysis

- Data Types Revisited
- Volatile
- System date and time
- Current network connections and Open ports
- Processes that opened ports
- Cached NetBIOS Names
- Users Currently Logged On
- Internal routing
- Running Processes
- Pslist
- Trivia
- Pslist –t
- Tasklist
- Tlist
- Running Services
- Open Files
- Process Memory Dumps

LAB: Memory Analysis

08. Endpoint protection

- Introduction to NAC
- NAC Defined
- NAC General Architecture
- NAC General Architecture Illustrated
- NAC Concepts
- Inline NAC
- Out-of-Band
- Identifying NAC Requirements
- Implementing User-Based Identity Access Control
- Network Access Protection (NAP)
- NAP Components
- NAP Enforcement
- NAP Best Practices
- 802.1x
- EAP Explained

LAB 1: Network Access Protection with DHCP

LAB 2: Network Access Protection with IPsec

LAB 3: Endpoint Protection

09. Securing Wireless

- ireless Tools
- Wireless Vulnerabilities Summary
- MAC Filtering
- Hiding Access Points
- Hijacking
- Jamming
- Identifying Targets
- Wardriving
- Sniffing on Wireless
- Attacking Encrypted Networks
- Wep Data
- The other case
- Reality
- WPA Tools
- WPA
- LEAP
- Asleap
- Comparison

TRAINERS PROFILE:

Kevin Cardwell

Kevin Cardwell served as the leader of a 5 person Red Team that achieved a 100% success rate at compromising systems and networks for six straight years. He has conducted over 500 security assessments across the globe. His expertise is in finding weaknesses and determining ways clients can mitigate or limit the impact of these weaknesses.

He currently works as a free-lance consultant and provides consulting services for companies throughout the world, and as an advisor to numerous government entities within the US, Middle East, Africa, Asia and the UK . He is an Instructor, Technical Editor and Author for Computer Forensics, and Hacking courses. He is the author of the Center for Advanced Security and Training (CAST) Advanced Network Defense course. He is technical editor of the Learning Tree Course Penetration Testing Techniques and Computer Forensics. He has presented at the Blackhat USA, Hacker Halted, ISSA and TakeDownCon conferences. He has chaired the Cybercrime and Cyberdefense Summit in Oman. He is author of Bactrack: Testing Wireless Network Security. He holds a BS in Computer Science from National University in California and a MS in Software Engineering from the Southern Methodist University (SMU) in Texas. He developed the Strategy and Training Development Plan for the first Government CERT in the country of Oman that recently was rated as the top CERT for the Middle East. he serves as a professional training consultant to the Oman Information Technology Authority, and developed the team to man the first Commercial Security Operations Center in the country of Oman. He has worked extensively with banks and financial institutions throughout the Middle East, Europe and the UK in the planning of a robust and secure architecture and implementing requirements to meet compliance. He currently provides consultancy to Commercial companies, governments, major banks and financial institutions in the Gulf region to include the Muscat Securities Market (MSM) and the Central Bank of Oman. Additionally, he provides training and consultancy to the Oman CERT and the SOC team in the monitoring and incident identification of intrusions and incidents within the Gulf region.

EC-Council