EC-Council

CENTER FOR ADVANCED SECURITY TRAINING

CAST 612

Advanced Mobile Hacking & Forensics

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 Mobile Hacking & Forensics

Course Description

Digital Mobile Forensics is fast becoming a lucrative and constantly evolving field, this is no surprise as the mobile phone industry has been witnessing some unimaginable growth, some experts say it may even replace the Computer for those only wishing to send and receive emails. As this area of digital forensics grow in scope and size due to the prevalence and proliferation of mobile devices and as the use of these devices grows, more evidence and information important to investigations will be found on them. To ignore examining these devices would be negligent and result in incomplete investigations. This growth has now presented new and growing career opportunities for interested practitioners in corporate, enforcement, and military settings. Mobile forensics is certainly here to stay as every mobile device is different and different results will occur based on that device requiring unique expertise. This course was put together focusing on what today's Mobile Forensics practitioner requires, some of the advanced areas this course will be covering are the intricacies of manual Acquisition (physical vs. logical) & advanced analysis using reverse engineering , understanding how the popular Mobile OSs are hardened to defend against common attacks and exploits.

CAST

EC-Council

How will this course benefit you?

01	Staying updated and abreast of the latest technologies that are being developed and used by the best in the field
02	Protect your organization by retrieving stolen data and incriminating evidence from communications devices used by rogue employees
03	Influence results of civil, private litigation and criminal cases by providing crucial evidence such as the suspects involved, their locations at the time of question and the role they played by extracting this information from mobile devices
04	Refine current mobile forensic processes by addressing its unique problems of preserving crucial data and producing valid results
05	Protecting your organization by conducting proper & regular IT Audit investigations on mobile devices to ensure no misuse of company information

Who Should Attend

Information security professional

- Risk Assessment Professionals
- Digital Forensics Investigators
- Information Security Professionals
- Mobile Developers
- Penetration Testers - CEH Professionals
- Law Enforcement Officers and Government Agencies
- Attorneys, Paralegals and First Responders
- Accountants and Financial Personnel
- Anyone who deals with implementation, testing, security hardening of mobile devices

CAST

EC-Council

Pre-requisites

- Students should have an understanding of Fundamental principles and process for digital forensics
- Knowledge includes evidence acquisitions, examination analysis and final reporting
- A minimum of 6 months Digital Forensics experience is recommended

Recommended Certifications

Before attending this course, it's recommended that students have:

- CHFI certification or equivalent knowledge.
- A+ certification or equivalent knowledge.
- Network+ certification or equivalent knowledge.

Course Outline

01. Mobile Hacking and Digital Forensic Challenges

This module will cover a broad refresher of the fundamental principles and methodologies used for legal forensics investigations

- History of Digital Forensics
- Global Legal System - Challenges
- Technical Aspects of Mobile Forensics (What are the challenges)
- Trace, Seize and investigate – Cyber Crime Case Scenarios
- Criminal / Civil Incidents
- Cyber Fraud
- Insider / Unknown Threats
- Recommended reading

Lab 1: Scenario Case Investigation

Lab 2: Evidence Analysis

After completing this module, students will be familiar with:

- Creating a new case using FTK and import case evidence
- Standard Evidence storage acquisition of a hard disk
- Using FTK and Caine Live CD for case evidence analysis and evidence priority
- Exploring the difference of Physical vs. Logical Evidence Acquisition

02. Mobile Hardware Design for iPhone, BlackBerry, Android and other devices

This module will focus on the hardware design specifications of the popular mobile devices

- Forensics Methodology
- Why we need in-depth knowledge of the designs
- iDevice teardown schematics (Ipad, Iphone and Ipad)
- Android teardown schematics (HTC and Samsung)
- Blackberry Bold teardown
- Standard designs of other mobile devices
- Mobile Hardware Tool Kits

Lab: Under the hood of an iPhone

After completing this module, students will be familiar with:

- Diving deep into the hardware aspects of mobile devices
- Appreciating the different methods, techniques and tools involved

03. Mobile Software design and the common boot process for Smart Devices

This module explains how mobiles boot, and use architectural design components. It also describes how data is stored and accessed for the IOS system

- Fundamental Open Source Software
- Why specialize? And Latest News
- Mobile OSX Architecture
- Core Definitions
- UI Framework IOS
- OSX Boot Overview
- iPhone DFU – Recovery Modes
- Android Boot Process
- IOS Kernel Design
- Jail-breaking / Rooting, REALLY? why, what and how

Lab: Jail-breaking and Rooting

After completing this module, students will be familiar with:

- Understanding Apple and Android Architecture
- Appreciating UI Frameworks and IOS Kernel Design
- Jail-breaking and rooting IOS and Android

04. Mobile Device Storage and Evidence Acquisition Techniques

This module explains how user data is stored and how to deal with deleted user evidence. It also describes the array of techniques that offer the greatest success for evidence acquisition

- Analysis Open Source Tool and SDK Software kits for Apple and Android
- Evidence Acquisition
- Smart Phone Characteristics
- Slack Space – Hidden Data
- MBR – EFI Basic Storage Designs
- Partitions and device specifics
- Passcode Protection – Encrypted Backups

Lab 1: Binary Reality

Lab 2: Accessing Evidence

After completing this module, students will be familiar with:

- Using manual open-source evidence acquisition methods
- Bypassing passcode protection
- The importance of HEX editors
- Primary unix commands and techniques used

05. Advanced Mobile Attack Analysis

This module explains the genre and advanced Mobile Attacks

- How Mobile Devices get Hacked
- Debuggers and Decompiles
- Reverse Engineering
- IPA and APK Packages
- iPhone App Store Specifics

Lab 1: Hacking Tools and Analysis

Lab 2: Building our Environment

After completing this module, students will be familiar with:

- Analyzing Real Threats
- Using open source tools and techniques

06. Mobile Device Hacking Techniques and Tools

This module explains how to analyze evidence and produce detailed evidence reports. It also describes how technical savvy people can obscure evidence to negate or destroy the evidence

- Hacking can kill you
- Threat Predictions 2011 / 2012
- Mobile Hacking Techniques
- IOS Platform Weaknesses
- Android Platform Weaknesses
- Blackberry Platform Weaknesses

Lab 1: Popular Software for Analysis

After completing this module, students will be familiar with:

- Understanding Hacking Techniques and Tools.
- Launching Spear Phishing Attacks.
- Planting Hidden Payloads

07. Penetration Testing and Exploitation Vectors

This module explains the Penetration Testing training Life Cycle. It also describes the tools and techniques we can use for exploitation Vectors

- Information Gathering
- Manual Exploitation
- Exploit Frameworks
- Cracking Passwords

Lab 1: Pen Test 101
Lab 2: Pen Test Model - BlueTooth Hacking

Note: This module is designed to be 100% hands-on covering the penetration testing methodology by utilizing BackTrack v5r1

08. Mobile Forensic Hardware and Software Field Kits

This module explains Forensics Hardware Options. It also describes how we can build our portable Forensics field kits

- DIY Toolkit Options and costs
- Commercial Comparisons
- Pros and cons of open source
- Field Kit Review and best practices

Lab 1: Tag and Bag

Lab 2: Building our Forensic Station and Toolkit

After completing this module, students will be familiar with:

- Using open source tools and techniques
- Using commercial packages
- Critical aspects related to Chain of Custody, documentation
- and protection of evidence techniques

09. Forensic Software, Evidence Analysis and Reporting

This module explains how to wrap-up the case by compiling the report and focuses on presenting the technical results in Laymen terms

- Disclaimer/ Legal
- Introduction to software packages
- Forensics Reports
- Best Evidence Rule
- Evidence Report Documentation

Lab 1: Creating the Report

After completing this module, students will be familiar with:

- Categorizing Evidence
- Evidence Tampering
- The various software used

TRAINERS PROFILE:

Wayne Burke

Wayne Burke has had considerable hands-on IT Security experience consulting or lecturing, whether it was for Government Agencies, Healthcare Institutions, Financial and international companies.

His experience in the public / defense sectors is equally complemented by assignments undertaken for heavyweight world renowned corporations including Yahoo, Xerox, AT&T and Texas Instruments to name but a few. He is imminently qualified in his field in that he holds a string of professional qualifications in Networking to name a few (MCT, MCSE, Cisco, Network+) and IT Security (CIW-SA, Security+, CEH, ECSA, LPT, CHFI) besides a bachelor's degree in science.

Wayne is currently the CSO for Sequrit CSI, responsible for the technical realm and security management, which includes consulting teams. He is a captain of a global operating group of penetration testers and security experts. Wayne and his group have delivered security assessments, Penetration Test assignments and customized training for International Corporations and many Government Agencies such as: EPA, FAA, DOJ, DOE, DOD + 8570: Air force, Army, Navy, Marines, FBI and Statewide Law Enforcement Offices in the USA.

In Europe: NATO, Europol, MOD (Military of Defense UK) various EU Law Enforcement, Dutch Ministry of Defense, Ministry of Justice, local European Law Enforcement: UK, Ireland, Switzerland, Belgium, Holland, Denmark.

ASIA: Singapore Gov, Philippines' Presidential Office, the Undersecretary, and Cyber Crime Police Specialist Unit. Jakarta, Tax Investigations Office. Various Malaysian Gov agencies. Plus Corporate and government bodies from Africa, and numerous Gulf locations to name a few. His office has become his next long haul international flight.

Wayne's consulting and training undertakings cover specializing in Penetration Testing, Forensics, Security Expert Advisor and secure infrastructure design. His expertise include DMZ firewalls, Secure VPNs, EAP/TLS, PEAP, SSL, PKI, Smart Cards, Biometrics, IPSEC, IDS, Vulnerability Scanners, AV, Honey Pots, Audits, filtering policies, multi-layer encrypted file systems, patch management and deployments. He additionally develops customized and blended security curriculum.

Wayne is constantly engaged in helping businesses optimize their systems security vision He is acknowledged as an expert consultant and trainer serving large organizations with cutting edge IT security. His wide range of all product experience has helped to develop his overall systems security knowledge. Wayne has a passion for tracing malicious hackers in pursuit of which he has had to grapple with issues, which are inextricably entwined in meeting the everyday challenges of information systems security.

EC-Council