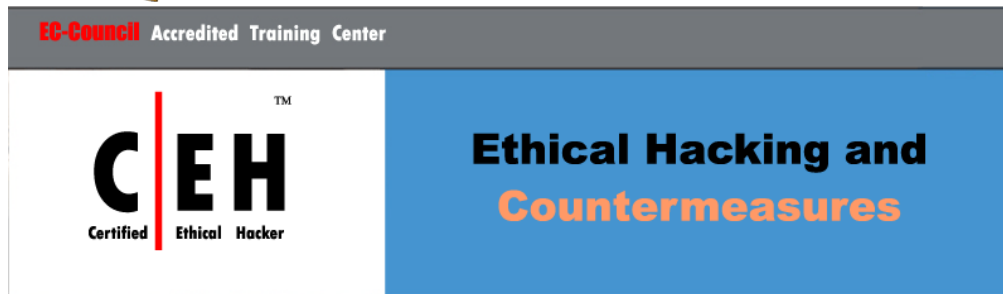




IT Security Certification Courses Outlines



Course Description

This class will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking.

This course prepares you for EC-Council Certified Ethical Hacker exam 312-50

Who Should Attend

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Duration:

5 days (9:00 – 5:00)

Certification

The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online Prometric exam to receive CEH certification.

Legal Agreement

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Pricing:

\$2995.00 per person. (Price includes books, handouts, and exam fees).
Group discounts available.



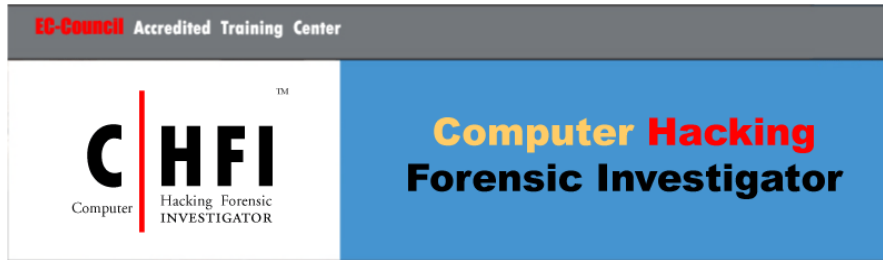
Course Outline Version 5

- Module 1: Introduction to Ethical Hacking
- Module 2: Footprinting
- Module 3: Scanning
- Module 4: Enumeration
- Module 5: System Hacking
- Module 6: Trojans and Backdoors
- Module 7: Sniffers
- Module 8: Denial of Service
- Module 9: Social Engineering
- Module 10: Session Hijacking
- Module 11: Hacking Web Servers
- Module 12: Web Application Vulnerabilities
- Module 13: Web-based Password Cracking Techniques
- Module 14: SQL Injection
- Module 15: Hacking Wireless Networks
- Module 16: Virus and Worms
- Module 17: Physical Security
- Module 18: Linux Hacking
- Module 19: Evading IDS, Firewalls, and Honeypots
- Module 20: Buffer Overflows
- Module 21: Cryptography
- Module 22: Penetration Testing

SELF-STUDY MODULES

- Covert Hacking
- Writing Virus Codes
- Assembly Language Tutorial
- Exploit Writing
- Smashing the Stack for Fun and Profit
- Windows Based Buffer Overflow Exploit Writing
- Reverse Engineering

For Full Course Details please visit the following URL –
<http://www.eccouncil.org/EC-Council%20Education/ceh-course-outline.htm>



Course Description

The CHFI course will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute. Many of today's top tools of the forensic trade will be taught during this course, including software, hardware and specialized techniques. The need for businesses to become more efficient and integrated with one another, as well as the home user, has given way to a new type of criminal, the "cyber-criminal." It is no longer a matter of "will your organization be comprised (hacked)?" but, rather, "when?" Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cyber-criminal, then this is the course for you.

Who Should Attend

Police and other law enforcement personnel, Defense and Military personnel, e-Business Security professionals, Systems administrators, Legal professionals, Banking, Insurance and other professionals, Government agencies, IT managers

Prerequisites

It is strongly recommended that you attend the CEH class before enrolling into CHFI program.

Duration:

5 days (9:00 – 5:00)

Certification

The CHFI 312-49 exam will be conducted on the last day of training. Students need to pass the online Prometric exam to receive the **CHFI** certification.

Pricing:

\$2995.00 per person. (Price includes books, handouts, and exam fees).
Group discounts available.



Course Outline v2

Module I: Computer Forensics in Today's World

Module II: Law And Computer Forensics

Module III: Computer Investigation Process

Module IV: Computer Security Incident Response Team

Module V: Computer Forensic Laboratory Requirements

Module VI: Understanding File systems and Hard disks

Module VII: Windows Forensics

Module VIII: Linux and Macintosh Boot processes

Module IX: Linux Forensics

Module X: Data Acquisition and Duplication

Module XI: Recovering Deleted Files

Module XII: Image Files Forensics

Module XIII: Steganography

Module XIV: Computer Forensic Tools

Module XV: Application password crackers

Module XVI: Investigating Logs

Module XVII: Investigating network traffic

Module XVIII: Router Forensics

Module XIX: Investigating Web Attacks

Module XX: Tracking E-mails and Investigating E-mail crimes

Module XXI: Mobile and PDA Forensics

Module XXII: Investigating Trademark and Copyright Infringement

Module XXIII: Investigative Reports

Module XXIV: Becoming an Expert Witness

Module XXV: Forensics in action

APPENDIX:

1. Investigating Wireless Attacks
2. Forensics Investigation Using EnCase
3. First Responder Procedures
4. Checklist for Choosing a Forensic Examiner
5. Investigation Checklist

Full Course Details: <http://www.eccouncil.org/EC-Council%20Education/Chfi-Course.htm>



The SCNS certification is the all new starting point with the SCP.

The Security Certified Network Specialist (SCNS) program focuses on the critical defensive technologies that are the foundation of securing network perimeters, such as firewalls, intrusion detection, and router security. The up-to-date security lessons and the hands-on labs in the SCNS courseware bring the security networking world to the candidates.

To prepare for the examination, candidates are recommended to attend training with an SCP Authorized Training Partner (ATP). The course to prepare for the exam is called, Tactical Perimeter Defense (TPD). Course details can be found here: <http://www.securitycertified.net/tpd.htm>.

The SCNS certification requires the passing of one exam (number SC0-451), details of the exam can be found here: http://www.securitycertified.net/tpd_domain_objectives.htm.

The exam is designed to validate the essential perimeter security skills, including: Network Defense Fundamentals, Hardening Routers and ACLs, Implementing IPsec and VPNs, Advanced TCP/IP, Securing Wireless Networks, Designing and Configuring Intrusion Detection Systems, and Designing and Configuring Firewall Systems.

As the security industry moves quickly, skills require consistent validation. The SCNS credential is valid for two years from the pass date. Recertification is required to maintain good standing.

Prerequisite for this certification is Security+ or equivalent experience.

Pricing: \$2495.00 per person. (The price includes handouts, books, and exam fees).

Group discounts available



The Security Certified Network Professional (SCNP) program focuses on the required elements of securing a network, such as securing Windows and Linux systems. The current lessons and detailed hands-on labs in the SCNP courseware bring a high level of security skills to the candidates.

To prepare for the examination, candidates are recommended to attend training with an SCP Authorized Training Partner (ATP). The course to prepare for the exam is called, Strategic Infrastructure Security (SIS). Course details can be found here:

<http://www.securitycertified.net/sis.htm>.

The SCNP certification requires that candidates hold an SCNS credential, in good standing, and the successful passing of one exam (number SC0-471). Details of the exam can be found here:

<http://www.securitycertified.net/sis.htm>

The exam is designed to validate the essential security skills for securing strategic elements of the network, including: Analyzing Packet Signatures, Creating Security Policies, Performing Risk Analysis, Ethical Hacking Techniques, Internet and WWW Security, Cryptography, Hardening Linux Computers, and Hardening Windows Server 2003.

Due to the speed at which the security industry changes, security skills require updating, and as such, the SCNP credential is valid for two years from the pass date. Recertification is required within two years to maintain good standing.

The prerequisite for this certification is the SCNS. Candidates must possess their SCNS, in good standing, prior to receiving their SCNP credential.

Pricing: \$2495.00 per person. (The price includes handouts, books, and exam fees)

Group discounts available



The SCNA program will focus on the advanced security skills and technologies of building trusted networks. The skills and knowledge of the SCNA program includes: Law and Legislation issues, Forensics, Wireless Security, Securing Email, Biometrics, Strong Authentication, Digital Certificates and Digital Signatures, PKI Policy and Architecture, and Cryptography. The timely information and hands-on labs allow candidates to experience the applications within a teaching environment.

As networks, and network security evolves, the move toward trusted networks is inevitable. Candidates who wish to remain on the cutting edge of their security career must have this knowledge, and these skills. These candidates are aware that the defense provided by the firewall and IDS alone, while required, are not enough.

The SCNA Exams

Prerequisite for this certification is the Security Certified Network Professional (SCNP) credential, with good standing.

The SCNA program is divided into two exams. To achieve the SCNA credential, candidates must achieve passing scores on both exams. The first exam is titled: Enterprise Security Implementation (ESI). The ESI exam is supported by the course material found in the two SCNA courses, with details found http://www.securitycertified.net/esi_domain_objectives.htm. The second exam, http://www.securitycertified.net/tse_domain_objectives.htm, covers all facets of the SCNP and SCNA courses. TSE is an exciting and challenging exam that is entirely scenario-based; many of the exam items may be several pages in length.

Once Exam SC0-501 and SC0-502 have been successfully written, SCNA status is achieved. The Security Certified Network Architect will have his or her name on the Certified Professionals page of the SCP website and receive a certification packet, sent via regular air mail within 4 weeks of pass date. Please allow time for the packet to be received.

The SCNA credential is then valid for two years from the pass date. Recertification is required at that time with a passing score on Exam SC0-502 only.

http://www.securitycertified.net/esi_domain_objectives.htm is designed to validate the technically advanced skills that a security architect requires. These skills include, but are not limited to: Law and Legislation issues, Forensics, Wireless Security, Securing Email, Biometrics, Strong Authentication, Digital Certificates and Digital Signatures, PKI Policy and Architecture, and Cryptography.



http://www.securitycertified.net/tse_domain_objectives.htm will cover all facets of technologies covered in all four of The SCP courses. To successfully complete The Solution Exam, candidates will require knowledge of the following, but limited to: Firewalls, Intrusion Detection, Operating System Security, Risk Analysis, Security Policies, Signature Analysis, Virtual Private Networks, Router Security, Law and Legislation issues, Forensics, Wireless Security, Securing Email, Biometrics, Strong Authentication, Digital Certificates and Digital Signatures, PKI Policy and Architecture, and Cryptography.

The SCNA Courses

There are two SCNA Courses, titled: Advanced Security Implementation (ASI), and Enterprise Security Solutions (ESS). These two courses are strongly recommended in preparation for the SCNA exams. [Full details on the ASI course can be found here - http://www.securitycertified.net/asi.htm](http://www.securitycertified.net/asi.htm)

[Full details on the ESS course can be found here. http://www.securitycertified.net/ess.htm](http://www.securitycertified.net/ess.htm)

Pricing: \$2495.00 per person. (The price includes handouts, books, and exam fees)

Group discounts available