

Course Outline: ESCA/LPT: EC-Council Certified Security Analyst

Learning Method: Instructor-led Classroom Learning

Duration: 5.00 Day(s)/ 40 hrs

Overview: ECSA is a security class like no other! Providing real world hands on experience, it is the only in-depth Advanced Hacking and Penetration Testing class available that covers testing in all modern infrastructures, operating systems and application environments.

EC-Council's Certified Security Analyst program is a highly interactive 5-day security class designed to teach Security Professionals the advanced uses of the available methodologies, tools and techniques required to perform comprehensive information security tests.

Who Should Attend:

- * System and Network Administrators
- * Security and Firewall Administrators
- * Security Engineers and Architects
- * MIS Directors
- * Professional Security Testers
- * Chief Security Officers
- * Professional Security Analysts
- * Chief Intelligence Officers
- * IT Auditors
- * Security Analyst
- * Risk Assessment Professionals
- * Vulnerability Auditors

At Course Completion:

Students will learn how to design, secure and test networks to protect your organization from the threats hackers and crackers pose. By teaching the tools and ground breaking techniques for security and penetration testing, this class will help you perform the intensive assessments required to effectively identify and mitigate risks to the security of your infrastructure. As students learn to identify security problems, they also learn how to avoid and eliminate them, with the class providing complete coverage of hacking and network security-testing topics

Outline:

Module 1 - Penetration Testing

Methodologies

- Understand how to structure and organize security tests

Phone: +357 70002770
www.computrain.com.cy



Understand the five stages of a common penetration test attack methodology

Analyze the tactical application of each phase

The Open Source Security Testing Methodology Manual (OSSTMM)

- Get an overview of The Security Map and sections of the OSSTMM
- Learn about an OSSTMM certified security test
- Understand what is a complete and valid OSSTMM security test
- See how the OSSTMM addresses privacy law compliance
- Learn how the OSSTMM addresses "Best Practices" compliance
- The NIST Methodology
 - See an overview of the NIST Four-Stage Penetration Testing methodology
 - See escalation of privileges according to the NIST methodology
 - Learn about the course methodology
- Learn about the methodology followed in this course
 - Learn about malicious hackers methodologies
 - Review a common malicious hacker attack methodology
 - Examine methodological variants

Module 2 - Test Planning and Scheduling

- Estimation of Resources for the Test
- Estimating time and cost of a test
 - Defining the test scope
- Determination of Test Objectives
 - Technical Preparation
- Attack network
- Attack workstation
- Gathering tools and exploits
- How to manage confidential data
 - Rules of Engagement
 - Non disclosure agreement
 - Liability limitations
 - Emergency phone number
 - Know the rules of engagement as they pertain to client target networks/systems
 - Defined Roles of the Involved Personnel
 - Review rules of engagement
 - Define test conditions
 - What should be included in rules of engagement
 - Reporting
 - Deliverables
 - Knowing what results are expected at the end of the test

Phone: +357 70002770
www.computrain.com.cy



- Presentation of results

Module 3 – Information Gathering

- Demonstrate understanding of the field of Competitive Intelligence
- Develop skills involved in competitive intelligence gathering
- Demonstrate understanding of Informational Vulnerabilities in depth
- Engage in Passive network discovery techniques
- Use advanced web resource skills to research identified targets in depth
- Formulate a picture of network boundaries, using IP and DNS information
- Analyze documents for potential Information Vulnerabilities

Information vulnerability and source of information

- Business intelligence
- Sales data
- R&D data
- Job advertising
- Web site
- Mailing list
- Other sources of great interest

Information gathering types

- Passive
- Active

- How and where to passively gather information

Information gathering applications

- Dig
- Host
- Nslookup
- Sam Spade
- Registrars
- DNSTracer
- kartOO
- Advanced web tricks
- And other tools and website
- Controls to protect information

Module 4 – Advanced Vulnerability Analysis Penetration Testing and Security Analysis

- Understand the three most common present vulnerability types
- Identify the potential impact of Information Vulnerabilities
- Identify the risks of Network Vulnerabilities
- Understanding the different types of System Vulnerabilities and their impact

TCP overview

- TCP protocol suite
- ICMP, UDP, ICMP, TCP
- Handshake

Phone: +357 70002770
www.computrain.com.cy



- Tear Down
- Port and Services
- Flags
- Traceroute and TCPTraceroute
- LFT
- Tools to probe protocols
- Paketto Kieretsu
- ScanRand
- Minewt
- Linkcat
- Paratrace
 - Identifying targets through sweeping
- Type of sweeps
 - Evaluating services through scanning
- Type of scans
- Stealth Scanning
- Bounce Attacks
- Reverse Ident Scanning
 - Nmap
- How to use Nmap
 - Nessus
- How to use Nessus
- How to avoid problems using Nessus
- Limitations of Nessus
 - Other scanners and tools overview
- Retina
- Saint
- Hping2
- Firewalk
- Nikto
- Languard
- ISS
- IpEye
- Nmap Tools
- SuperScan
- Friendly Pinger
- Cheops
- SATAN
 - Advanced OS fingerprinting techniques
- Proxy Servers
- Sniffing
- Tcpcat
- Windump
- Snort
- Ethereal
- Ettercap
- Dsniff
 - Windows Tools
- Dumpsec
- Winfo
- NAT
- Netbios Enumeration Techniques
- Userinfo
- Getacct
- Dumpreg
- WinFingerprint
- AD Enumeration
- SNMP
- Weaknesses
- Snmpwalk
- Snmpget

Phone: +357 70002770
www.computrain.com.cy



- Snmpgetnext
- SolarWinds
- SNScan
 - Phone Phreakers
- PBX testing
- Modem Testing
- War Dialing
- Fax Security
- Phone Sweep
- Toneloc
- THCSan
 - Countermeasures

Module 5 – Advanced Denial of Service (DoS) Penetration Testing and Security Analysis

- Attack Vectors
- The Battlefield
- DoS, DDoS, DRDoS
 - Identify the harm caused to the target system
 - Analyze the potential vulnerabilities in a system that could be exploited by a DoS attack
 - Outline the necessary steps to test a system's strength against a DoS attack
 - Gathering and documenting the results

Module 6 – Advanced Password Cracking Penetration Testing and Security Analysis

- Demonstrate understanding how passwords work in common operating systems
- Demonstrate knowledge of the Windows password schemes (PWL, LANMAN, NTLM, Active Directory)
- Demonstrate knowledge of Linux/Unix authentication mechanisms
- Demonstrate knowledge of alternate authentication mechanisms (SASL, LDAP, PAM, etc)
- Demonstrate knowledge of how distributed password cracking works
- Demonstrate knowledge of advanced password cracking attacks, such as Rainbow Tables
- Demonstrate ability to test strength of authentication mechanisms using password cracking
- Use common tools to crack Windows Passwords
- Use several free tools to crack Linux and common Unix passwords
- Use advanced approaches to password cracking by combining techniques and resources to compromise the target credentials

Module 7 – Advanced Social Engineering Penetration Testing and Security Analysis

- Describe what Social Engineering is
- Principles of social engineering

Phone: +357 70002770
www.computrain.com.cy



- Social Engineering Tips
- Type of social engineering attacks
- Define the techniques used to execute Social Engineering
- Social Engineering Goals
- Social Engineering Rules of engagement
- Recognize the threat of Social Engineering
- Outline the methods by which Social Engineering is performed
- Trusted positions enumeration
- Trusted person testing
- Request Testing
- Guided Suggestions
- Phishing
- Security Policies
- Gather and document the test results
- Define impact and points of consideration of Viruses on security testing and analysis
- Understand how common viruses work
- Learn how to safely test containment measures
- Evaluate target networks for proper containment measures
- Explain how vulnerabilities are discovered
- Demonstrate knowledge of tools and techniques for enumerating specific hosts and services
- Employ advanced tools to fingerprint specific operating systems
- Implement advanced port scanning techniques to further refine targeting information
- Employ tools like Netcat to verify service information, and eliminate false positives
- Learn operating system specific tools and techniques
- Use commonly available Microsoft Resource Kits for advanced Windows enumeration
- Use Null-Sessions for advanced Windows enumeration
- Use various common tools in Linux for Linux and Unix enumeration

Module 8 – Advanced Internal Penetration Testing and Security Analysis

- Review the most common platforms
- Appraise a typical network environment
- Outline the steps of the assessment
- Describe the tools used for internal testing
- Viruses and Containment Testing
- Categorize and Identify range and function of present Viruses
- Identify threat levels and countermeasures of various viruses

Phone: +357 70002770
www.computrain.com.cy



- Employ Automated Vulnerability Scanners
- understand the strengths and weaknesses of Automated Scanners
- Using Nessus to refine target information
- Analyzing the results given by Nessus and other Automated Scanners
- Overview of common vulnerability scanners
- Cerberus Internet Scanner

- Somarsoft Hyena
- Languard
- Nessus
- Saint
- SATAN
- Employing Exploitation for verification of Vulnerabilities: Owning the Box
- Understand the specifics of common classes of System Vulnerabilities
- Understand Stack based overflows
- Understand Format String vulnerabilities
- Understand Heap based overflows
- Develop and execute proof of concept Stack based overflows
- Develop and execute proof of concept Understand Format String vulnerabilities

- Develop and execute proof of concept Understand Heap based overflows
- Demonstrate understanding of aspects of an exploit, in terms of threat agents and methods of countering such threats
- Demonstrate ability to employ Shellcode within exploits
- Gather and document the test results

Module 9 - Advanced External Penetration Testing and Security Analysis

- Describe the goals of external testing Network Categories
- Understand the challenges facing a tester in an external penetration test
- Evaluate the potential attacks from outside of a security perimeter Web Security Challenges
- Current situation
- Attack Trends
- What creates those vulnerabilities
- Understand the impact of web applications on Perimeter Security
- Test and Analyze higher-layer applications for Network Vulnerabilities
- Demonstrate Knowledge of common types of web application System Vulnerabilities
- Employ attack proxies to audit web applications

Phone: +357 70002770
www.computrain.com.cy



- Employ application scanners to audit web applications
- Anatomy of a remote exploit
- Common Attacks
- Network packet sniffers
- IP spoofing
- Password attacks
- Distribution of sensitive internal information to external sources
- Man-in-the-middle attacks
- Phishing
- Examine the methodology of external penetration testing
- Demonstrate the tools used for external penetration testing
- Website Crawler
- Idle Scanning
- Form Scalpel
- Java Decompiler
- Brutus AET2
- Achilles
- Web Proxies
- Gather and document the results
- Demonstrate knowledge of vulnerabilities in Router
- Understanding many Informational Vulnerabilities, as well as network vulnerabilities present in many routers
- Analyzing Cisco packet captures for information disclosure and cracking Cisco passwords
- Demonstrate knowledge of vulnerabilities in various network devices
- Explore the role of Network Appliances such as printers and PBX's in potential security violations
- Using Man in the Middle Attacks to intercept secured and encrypted traffic
- The potential for router exploitation
- Router Attacks
- DDoS Attacks
- Routing Table Attacks
- Arp Poisoning
- SNMP Attacks
- Brute Force Attacks
- BGP attacks
- Analysis of router vulnerabilities and attacks
- CVE
- US-CERT

Module 10 - Advanced Router Penetration Testing and Security Analysis

- Overview of routing technologies
- Router Security
- Routing Protocols

Phone: +357 70002770
www.computrain.com.cy



- Packet Storm
- Neohapsis
- Bugtraq
- SecurityFocus
- Tools used for testing
- Gathering and documenting the results

Security Analysis

- What is Intrusion Detection?
- The need for IDS
- Sensor Placement
- IDS overview
- IDS detection methods
- Detection Engines
- IDS analysis challenges
- Analysis Engines
- Host Based Challenges
- Network Based challenges
- Penetration testing techniques
- IDS Evasion Techniques
- IDS Insertion Attack
- IDS Fragmentation Attack
- Tools used for IDS testing and countermeasures
- PSAD
- Samhain
- Tripwire
- Stick
- Snot
- AdMutate
- Nikto
- Apsend
- Apsr
- Gathering and documenting test results

Module 11 - Advanced Firewall Penetration Testing and Security Analysis

- Introduction to firewalls
- What is a Firewall
- Commonly use Firewall
- Personal Firewall
- Type of Firewall
- Technical overview of firewall systems
- Different implementations
 - NAT
 - PAT
- Limitations
 - Vulnerability analysis of firewall
- Things a firewall cannot see
- Penetration testing steps
 - Tools used for testing firewalls
- Firewalk
- Ftester
 - Gathering and documenting the results

Module 12 - Advanced Intrusion Detection Systems (IDS) Penetration Testing and

Phone: +357 70002770
www.computrain.com.cy



Module 13 – Advanced Wireless Penetration Testing and Security Analysis

- Present an overview of Wireless Security
- Types of wireless Network
- Technology used in WLAN
- Access Point
- Chipsets
- Learn about Wireless Technologies
- Understand the problems with WLAN security
- Issues with WLAN Security
- WEP security issues
- Cisco LEAP
- EAP
- 802.1X
- WPA
- TKIP
- RADIUS
- Examine the tools used for Wireless Networks Testing
- Aircrack-ng
- WepCrack
- Monkey-Jack
- Kismet
- Examine Countermeasures

Module 14 – Advanced Application Penetration Testing and Security Analysis

- Identify types of common applications
- Common Applications used
- Outline the technology of the applications
- Mobile code
- OLE
- DCOM
- ActiveX
- JAVA
- CGI
- Detect the vulnerabilities in the applications
- Buffer Overflow
- Stack Overflow
- Format Strings
- Vulnerable functions
- Examine the techniques of penetration testing
- Reverse Engineering
- Spoofing Authentication
- Intercepting Data
- Modifying input
- CSS/XSS
- Describe the tools employed in testing the applications
- Modifying source of page
- Intercepting and modifying requests
- GDB

Phone: +357 70002770
www.computrain.com.cy



- Metasploit
- CANVAS
- CORE Impact
- NIKTO
- SQLDict
- SQLbf
- SQLexec
- SQLsmack
- Discover and analyze Web Application System Vulnerabilities
- Use SQL-Injection attacks against target servers to retrieve database information
- Test for Cross-Site Scripting vulnerabilities
- Use automated scanners, such as Nikto, for web application testing
- Document the results of the testing

- Perimeter compromise
- Stolen Equipment
- Bypassing system security mechanisms
- Social Engineering
- Analyze the potential attacks against the physical environment
 - Intrusion Detection systems
 - Types of locks and their features
 - Point out recommended safeguards to these attacks
- Access Control
- Equipment anti-theft devices
- Restricted zones
- Security Policies
- Guards
- Awareness, Training, and Education
- Document the test results

Module 16 - Reporting and Documentation

Module 15 - Advanced Physical Security Penetration Testing and Security Analysis

- Identify the goal of physical security
- The four security process
- Component of physical security
- Threats to physical security
 - Recognize the potential vulnerabilities of an organization with poor physical security
- Piggybacking

- Learn the basics of report writing
- Major Stages of report writing
- Understand the requirements of the report
- Report types
- Focus of the report
- Review different report writing options
- Online DB
- Spreadsheet
- Using Template
- Using a tree

Phone: +357 70002770
www.computrain.com.cy



- Free Flow document
Outline reporting tips
- Do a report workshop
- Questionable areas, how to address them
Describe the reporting consultation

Phone: +357 70002770
www.computrain.com.cy

