EC-Council Certified Security Analyst (ECSA)

http://www.eccouncil.org

EC-Council

ECSA™

EC-Council Certified Security Analyst

Introduction

EC-Council Certified Security Analyst (ECSA) complements the Certified Ethical Hacker (CEH) certification by exploring the analytical phase of ethical hacking. While CEH exposes the learner to hacking tools and technologies, ECSA takes it a step further by exploring how to analyze the outcome from these tools and technologies. Through groundbreaking penetration testing methods and techniques, ECSA class helps students perform the intensive assessments required to effectively identify and mitigate risks to the security of the infrastructure.

This makes ECSA a relevant milestone towards achieving EC-Council's Licensed penetration Tester, which also ingrains the learner in the business aspect of penetration testing. The Licensed Penetration Tester standardizes the knowledge base for penetration testing professionals by incorporating the best practices followed by experienced experts in the field.

The objective of EC-Council Certified Security Analyst is to add value to experienced security professionals by helping them analyze the outcomes of their tests. ECSA leads the learner into the advanced stages of ethical hacking.

Advanced Penetration Testing and Security Analysis

The ECSA/LPT training 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. Students will learn how to design, secure and test networks to protect your organization from the threats hackers and crackers pose. By teaching the LPT methodology 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 analysis and network security-testing topics.

Requirements

Pass exam 412-79 to achieve EC-Council Certified Security Analyst (ECSA) certification. Benefits ECSA is for experienced hands in the industry and is backed by a curriculum designed by the best in the field. Greater industry acceptance as seasoned security professional. Learn to analyze the outcomes from using security tools and security testing techniques. Requirement for the LPT certification.Certification

Exam

Students will be prepared for EC-Council's ECSA exam 412-79 on the last day of the class.
This certification is also pre-requisite to EC-Council's Licensed Penetration Tester Program.

Frequently Asked Questions

1. How does ECSA deliver value to a security professional like me?
ECSA teaches you to interpret and analyze outcomes you come across during routine and exceptional security testing. It helps you analyze the symptoms and pin point the causes of those symptoms which reflect the security posture of the network.

2. Why should I take ECSA when I am already certified as a security professional?
Most security certifications highlight the management aspects or the technical aspects alone. ECSA helps you bridge the gap to a certain extent by helping you detect the causes of security lapses and what implications it might carry for the management. This leads you to a step closer to becoming a licensed penetration tester, where you become a complete penetration testing professional.

3. How does ECSA deliver value to the enterprise's security team?
Having an ECSA on your enterprise security team will enhance value to the team as you would have a professional aboard who is exposed to advanced security testing and proficient to make studied analysis of the situation.

4. How is ECSA different from CEH?
CEH exposes the learner to various hacking tools and techniques, while ECSA exposes the learner to the analysis and interpretation of results obtained from using those tools and techniques.

5. I have over three years experience in the industry. Should I opt for ECSA instead of CEH?
ECSA is not a replacement for CEH. CEH provides the learner with the foundation ground over which you can fortify your skills using knowledge gained from ECSA

6. How long is the training?

The ECSA and LPT training are combined into a single ECSA/LPT Certification Boot camp class. The duration of this boot camp is 5 days. You will be prepared for ECSA and LPT certification at the end of this class.

7. What is the cost of the exam?

The ECSA exam costs USD 300.00

Course Description

ECSA/LPT 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/LPT program is a highly interactive 5-day security class designed to teach Security Professionals the advanced uses of the LPT methodologies, tools and techniques required to perform comprehensive information security tests. 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 analysis and network security-testing topics.

Who Should Attend

Network server administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals.

Duration:

5 days (9:00 – 5:00) Certification

ECSA/LPT Certification Bootcamp

Module 1: The Need for Security Analysis

What Are We Concerned About?
So What Are You Trying To Protect?
Why Are Intrusions So Often Successful?
What Are The Greatest Challenges?
Environmental Complexity
New Technologies
New Threats, New Exploits
Limited Focus
Limited Expertise
Authentication
Authorization
Confidentiality
Integrity
Availability
Nonrepudiation
We Must Be Diligento:p>
Threat Agents
Assessment Questions
How Much Security is Enough?
Risk
Simplifying Risk
Risk Analysis
Risk Assessment Answers Seven Questions
Steps of Risk Assessment
Risk Assessment Values
Information Security Awareness
Security policies
Types of Policies
Promiscuous Policy
Permissive Policy

Prudent Policy
Paranoid Policy
Acceptable-Use Policy
User-Account Policy
Remote-Access Policy
Information-Protection Policy
Firewall-Management Policy
Special-Access Policy
Network-Connection Policy
Business-Partner Policy
Other Important Policies
Policy Statements
Basic Document Set of Information Security Policies
ISO 17799
Domains of ISO 17799
No Simple Solutions
U.S. Legislation
California SB 1386
Sarbanes-Oxley 2002
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
USA Patriot Act 2001
U.K. Legislation
How Does This Law Affect a Security Officer?
The Data Protection Act 1998
The Human Rights Act 1998
Interception of Communications
The Freedom of Information Act 2000
The Audit Investigation and Community Enterprise Act 2005

Module 2: Advanced Googling
Site Operator
intitle:index.of
error | warning
login | logon
username | userid | employee.ID | "your username is"
password | passcode | "your password is"

admin | administrator
admin login
–ext:html –ext:htm –ext:shtml –ext:asp –ext:php
inurl:temp | inurl:tmp | inurl:backup | inurl:bak
intranet | help.desk
Locating Public Exploit Sites
Locating Exploits Via Common Code Strings
Searching for Exploit Code with Nonstandard Extensions
Locating Source Code with Common Strings
Locating Vulnerable Targets
Locating Targets Via Demonstration Pages
"Powered by" Tags Are Common Query Fodder for Finding Web Applications
Locating Targets Via Source Code
Vulnerable Web Application Examples
Locating Targets Via CGI Scanning
A Single CGI Scan-Style Query
Directory Listings
Finding IIS 5.0 Servers
Web Server Software Error Messages
IIS HTTP/1.1 Error Page Titles
"Object Not Found" Error Message Used to Find IIS 5.0
Apache Web Server
Apache 2.0 Error Pages
Application Software Error Messages
ASP Dumps Provide Dangerous Details
Many Errors Reveal Pathnames and Filenames
CGI Environment Listings Reveal Lots of Information
Default Pages
A Typical Apache Default Web Page
Locating Default Installations of IIS 4.0 on Windows NT 4.0/OP
Default Pages Query for Web Server
Outlook Web Access Default Portal
Searching for Passwords
Windows Registry Entries Can Reveal Passwords
Usernames, Cleartext Passwords, and Hostnames!

Module III: TCP/IP Packet Analysis

TCP/IP Model
Application Layer
Transport Layer
Internet Layer
Network Access Layer
Comparing OSI and TCP/IP
Addressing
IPv4 Addresses
IP Classes of Addresses
Reserved IP Addresses
Private Addresses
Subnetting
IPv4 and IPv6
Transport Layer
Flow Control
Three-Way Handshake
TCP/IP Protocols
TCP Header
IP Header
IP Header: Protocol Field
UDP
TCP and UDP Port Numbers
Port Numbers
TCP Operation
Synchronization or 3-way Handshake
Denial of Service (DoS) Attacks
DoS Syn Flooding Attack
Windowing
Acknowledgement
Windowing and Window Sizes
Simple Windowing
Sliding Windows
Sequencing Numbers
Positive Acknowledgment and Retransmission (PAR)
UDP Operation
Port Numbers Positioning between Transport and Application Layer (TCP and UDP)

Port Numbers
http://www.iana.org/assignments/port-numbers
What Makes Each Connection Unique?
Internet Control Message Protocol (ICMP)
Error Reporting and Error Correction
ICMP Message Delivery
Format of an ICMP Message
Unreachable Networks
Destination Unreachable Message
ICMP Echo (Request) and Echo Reply
Detecting Excessively Long Routes
IP Parameter Problem
ICMP Control Messages
ICMP Redirects
Clock Synchronization and Transit Time Estimation
Information Requests and Reply Message Formats
Address Masks
Router Solicitation and Advertisement

Module 4: Advanced Sniffing Techniques
What is Wireshark?
Wireshark: Filters
IP Display Filters
Example
Wireshark: Tshark
Wireshark: Editcap
Wireshark: Mergecap
Wireshark: Text2pcap
Using Wireshark for Network Troubleshooting
Network Troubleshooting Methodology
Using Wireshark for System Administration
ARP Problems
ICMP Echo Request/Reply Header Layout
TCP Flags
TCP SYN Packet Flags Bit Field
Capture Filter Examples
Scenario 1: SYN no SYN+ACK

Trojan Analysis Example NetBus Analysis

Module 5: Vulnerability Analysis with Nessus

Nessus
Features of Nessus
Nessus Assessment Process
Nessus: Scanning
Nessus: Enumeration
Nessus: Vulnerability Detection
Configuring Nessus
Updating Nessus Plug-Ins
Using the Nessus Client
Starting a Nessus Scan
Generating Reports
Data Gathering
Host Identification
Port Scan
SYN scan
Timing
Port Scanning Rules of Thumb
Plug-in Selection
Dangerous plugins
Scanning Rules of Thumb
Report Generation
Reports: Result
Identifying False Positives
Suspicious Signs
False Positives
Examples of False Positives
Writing Nessus Plugins
Writing a Plugin
Installing and Running the Plugin
Nessus Report with output from our plugin
Security Center http://www.tenablesecurity.com

Module 6: Advanced Wireless Testing

Wireless Concepts
Wireless Concepts
802.11 Types
Core Issues with 802.11
What's the Difference?
Other Types of Wireless
Spread Spectrum Background
Channels
Access Point
Service Set ID
Default SSIDs
Chipsets
Wi-Fi Equipment
Expedient Antennas
Vulnerabilities to 802.1x and RADIUS
Wired Equivalent Privacy
Security - WEP
Wired Equivalent Privacy
Exclusive OR
Encryption Process
Chipping Sequence
WEP Issues
WEP - Authentication Phase
WEP - Shared Key Authentication
WEP - Association Phase
WEP Flaws
WEP Attack
WEP: Solutions
WEP Solution – 802.11i
Wireless Security Technologies
WPA Interim 802.11 Security
WPA
802.1X Authentication and EAP
EAP Types
Cisco LEAP
TKIP (Temporal Key Integrity Protocol)

Multitiered Firewall With a DMZ Flow
DMZ Design Fundamentals
Advanced Design Strategies
Designing Windows DMZ
Designing Windows DMZ
Precautions for DMZ Setup
Security Analysis for the DMZ
Designing Sun Solaris DMZ
Placement of Servers
Advanced Implementation of a Solaris DMZ Server
Solaris DMZ Servers in a Conceptual Highly Available Configuration
Private and Public Network Firewall Ruleset
DMA Server Firewall Ruleset
Solaris DMZ System Design
Disk Layout and Considerations
Designing Wireless DMZ
Placement of Wireless Equipment
Access to DMZ and Authentication Considerations
Wireless DMZ Components
Wireless DMZ Using RADIUS to Authenticate Users
WLAN DMZ Security Best-Practices
DMZ Router Security Best-Practice
DMZ Switch Security Best-Practice
Six Ways to Stop Data Leaks
Reconnex

Module 8: Snort Analysis

Snort Overview
Modes of Operation
Features of Snort
Configuring Snort
Variables
Preprocessors
Output Plugins
Rules
Working of Snort
Initializing Snort

Signal Handlers
Parsing the Configuration File
Decoding
Possible Decoders
Preprocessing
Detection
Content Matching
Content-Matching Functions
The Stream4 Preprocessor
Inline Functionality
Writing Snort Rules
Snort Rule Header
Snort Rule Header: Actions
Snort Rule Header: Other Fields
IP Address Negation Rule
IP Address Filters
Port Numbers
Direction Operator
Rule Options
Activate/Dynamic Rules
Meta-Data Rule Options: msg
Reference Keyword
sid/rev Keyword
Classtype Keyword
Payload Detection Rule Options: content
Modifier Keywords
Offset/depth Keyword
Uricontent keyword
fragoffset keyword
ttl keyword
id keyword
flags keyword
itype keyword : icmp id
Writing Good Snort Rules
Sample Rule to Catch Metasploit Buffer Overflow Exploit
Tool for writing Snort rules: IDS Policy Manager
Subscribe to Snort Rules

Honeynet Security Console Tool
Key Features

Module 9: Log Analysis
Introduction to Logs
Types of Logs
Events that Need to be Logged
What to Look Out For in Logs
W3C Extended Log File Format
Automated Log Analysis Approaches
Log Shipping
Analyzing Syslog
Syslog
Setting up a Syslog
Syslog: Enabling Message Logging
Main Display Window
Configuring Kiwi Syslog to Log to a MS SQL Database
Configuring Ethereal to Capture Syslog Messages
Sending Log Files via email
Configuring Cisco Router for Syslog
Configuring DLink Router for Syslog
Configuring Cisco PIX for Syslog
Configuring an Intertex / Ingate/ PowerBit/ SurfinBird ADSL router
Configuring a LinkSys wireless VPN Router
Configuring a Netgear ADSL Firewall Router
Analyzing Web Server Logs
Apache Web Server Log
AWStats
Configuring AWStats for IIS
Log Processing in AWStats
Analyzing Router Logs
Router Logs
Analyzing Wireless Network Devices Logs
Wireless Traffic Log
Analyzing Windows Logs
Configuring Firewall Logs in Local Windows System
Viewing Local Windows Firewall Log

Viewing Windows Event Log
AAnalyzing Linux Logs
iptables
Log Prefixing with iptables
Firewall Log Analysis with grep
Analyzing SQL Server Logs
SQL Database Log
ApexSQL Log
Configuring ApexSQL Log
Analyzing VPN Server Logs
VPN Client Log
Analyzing Firewall Logs
Why Firewall Logs are Important
Firewall Log Sample
ManageEngine Firewall Analyzer
Installing Firewall Analyzer
Viewing Firewall Analyzer Reports
Firewall Analyzer Log Reports
Analyzing IDS Logs
SnortALog
IDS Log Sample
Analyzing DHCP Logs
DHCP Log
NTP Configuration
Time Synchronization and Logging
NTP Overview
NTP Client Configuration
Configuring an NTP client using the Client Manager
Configuring an NTP Server
NTP: Setting Local Date and Time
Log Analysis Tools
All-Seeing Eye Tool: Event Log Tracker
Network Sniffer Interface Test Tool
Syslog Manager 2.0.1
Sawmill
WALLWATCHER
Log Alert Tools

Network Eagle Monitor
Network Eagle Monitor: Features
SQL Server Database Log Navigator
What Log Navigator does?
How Does Log Navigator Work?
Snortsnarf
Types of Snort Alarms
ACID (Analysis Console for Intrusion Databases)

Module 10: Advanced Exploits and Tools
Common Vulnerabilities
Buffer Overflows Revisited
Smashing the Stack for Fun and Profit
Smashing the Heap for Fun and Profit
Format Strings for Chaos and Mayhem
The Anatomy of an Exploit
Vulnerable code
Shellcoding
Shellcode Examples
Delivery Code
Delivery Code: Example
Linux Exploits Versus Windows
Windows Versus Linux
Tools of the Trade: Debuggers
Tools of the Trade: GDB
Tools of the Trade: Metasploit
Metasploit Frame work
User-Interface Modes
Metasploit: Environment
Environment: Global Environment
Environment: Temporary Environment
Metasploit: Options
Metasploit: Commands
Metasploit: Launching the Exploit
MetaSploit: Advanced Features
Tools of the Trade: Canvas
Tools of the Trade: CORE Impact

IMPACT Industrializes Penetration Testing
Ways to Use CORE IMPACT
Other IMPACT Benefits
ANATOMY OF A REAL-WORLD ATTACK
CLIENT SIDE EXPLOITS
Impact Demo Lab

Module 11: Penetration Testing Methodologies

Module 12: Customers and Legal Agreements

Module 13: Rules of Engagement

Module 14: Penetration Testing Planning and Scheduling

Module 15: Pre Penetration Testing Checklist

Module 16: Information Gathering

Module 17: Vulnerability Analysis

Module 18: External Penetration Testing

Module 19: Internal Network Penetration Testing

Module 20: Routers and Switches Penetration Testing

Module 21: Firewall Penetration Testing

Module 22: IDS Penetration Testing

Module 23: Wireless Network Penetration Testing

Module 24: Denial of Service Penetration Testing

Module 25: Password Cracking Penetration Testing

Module 26: Social Engineering Penetration Testing

Module 27: Stolen Laptop, PDAs and Cell phones Penetration Testing

Module 28: Application Penetration Testing

Module 29: Physical Security Penetration Testing

Module 30: Database Penetration testing

Module 31: VoIP Penetration Testing

Module 32: VPN Penetration Testing

Module 33: War Dialing

Module 34: Virus and Trojan Detection

Module 35: Log Management Penetration Testing

Module 36: File Integrity Checking

Module 37: Blue Tooth and Hand held Device Penetration Testing

Module 38: Telecommunication and Broadband Communication Penetration Testing

Module 39: Email Security Penetration Testing

Module 40: Security Patches Penetration Testing

Module 41: Data Leakage Penetration Testing

Module 42: Penetration Testing Deliverables and Conclusion

Module 43: Penetration Testing Report and Documentation Writing

Module 44: Penetration Testing Report Analysis

Module 45: Post Testing Actions

Module 46: Ethics of a Licensed Penetration Tester

Module 47: Standards and Compliance

This document is for informational purposes only. EC-Council MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. EC-Council logo is registered trademarks or trademarks of EC-Council in the United States and/or other countries.