

ITSY 1075 Certified Security Analyst

ACC Fall Term 2008

Instructor: Larry Detar, IT Training Solutions

Contact Information matt@ittrainingsolutions.net, Phone: **801-649-4030**

Course Description:

ECSA/LPT is a security class that provides real world hands on experience. It is an in-depth Advanced Hacking and Penetration Testing class 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.

Prerequisites:

Experienced IT professionals with networking and server experience.

Course Learning Objectives:

Students will learn how to

- Design, secure and test networks to protect their organization from the threats hackers and crackers pose.
- Perform the intensive assessments required to effectively identify and mitigate risks to the security of your infrastructure.
- Identify, avoid and eliminate security problems using the analysis and network security-testing topics.

Rationale:

At the end of this course, students will understand the main issues and skills to be a security professional. This course will prepare students for the ECSA certification examination.

Intended Audience:

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

Resources Required:

Lab.

Texts for the Course: *None*

Length of Course: 40-hours

Evaluation:

Those who participate in class discussions and miss no more than three class meetings will be awarded 4.0 continuing education units. The ECSA certification exam will be conducted on the last day of training. Students need to pass the online Prometric exam 412-79 to receive the ECSA certification. The Student also will be prepared for the LPT certification. The ECSA certification exam purchase and registration will be the responsibility of the student. The exam may be scheduled and taken anytime following the course at any PearsonVue or Prometric testing centers.

Course Content:

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 Diligent: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 3: 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
- Scenario 2: SYN Immediate Response RST
- Scenario 3: SYN SYN+ACK ACK
 - Using Wireshark for Security Administration
- Detecting Internet Relay Chat Activity
- Wireshark as a Detector for Proprietary Information Transmission
- Sniffer Detection
- Wireless Sniffing with Wireshark
- AirPcap
- Using Channel Hopping
- Interference and Collisions
- Recommendations for Sniffing Wireless
- Analyzing Wireless Traffic
- IEEE 802.11 Header
- IEEE 802.11 Header Fields
- Filters
- Filtering on Source MAC Address and BSSID
- Filtering on BSSID
- Filter on SSID
- Wireless Frame Types Filters
- Unencrypted Data Traffic
- Identifying Hidden SSIDs
- Revealed SSID
- Identifying EAP Authentication Failures
- Identifying the EAP Type

- Identifying Key Negotiation Properties
- EAP Identity Disclosure
- Identifying WEP
- Identifying TKIP and CCMP
- Identifying IPSec/VPN
- Decrypting Traffic
- Scanning
- TCP Connect Scan
- SYN Scan
- XMAS Scan
- Null Scan
- Remote Access Trojans
- NetBus Analysis
- 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)
- Wireless Networks Testing
- Wireless Communications Testing
- Report Recommendations
- Wireless Attack Countermeasures
- Wireless Penetration Testing with Windows
- Attacks And Tools
- War Driving
- The Jargon – WarChalking
- WarPumpkin
- Wireless: Tools of the Trade
- Mapping with Kismet
- WarDriving with NetStumbler
- How NetStumbler Works?
- “Active” versus “Passive” WLAN Detection
- Disabling the Beacon

- Running NetStumbler
- Captured Data Using NetStumbler
- Filtering by Channels
- Airsnort
- WEPCrack
- Monkey-Jack
- How Monkey-Jack Works
- Before Monkey-Jack
- After Monkey-Jack
- AirCrack-ng
- How Does It Work?
- FMS and Korek Attacks
- Crack WEP
- Available Options
- Usage Examples
- Cracking WPA/WPA2 Passphrases
- Notes
- Determining Network Topology: Network View
- WarDriving and Wireless Penetration Testing with OS X
- What is the Difference between "Active" and "Passive" Sniffing?
- Using a GPS
- Attacking WEP Encryption with KisMAC
- Deauthenticating Clients
- Attacking WPA with KisMAC
- Brute-force Attacks Against 40-bit WEP
- Wordlist Attacks
- Mapping WarDrives with StumbVerter
- MITM Attack basics
- MITM Attack Design
- MITM Attack Variables
- Hardware for the Attack Antennas, Amps, WiFi Cards
- Wireless Network Cards
- Choosing the Right Antenna
- Amplifying the Wireless Signal
- Identify and Compromise the Target Access Point
- Compromising the Target
- Crack the WEP key
- Aircrack-ng Cracked the WEP Key
- The MITM Attack Laptop Configuration
- IP Forwarding and NAT Using Iptables
- Installing Iptables and IP Forwarding
- Establishing the NAT Rules
- Dnsmasq
- Configuring Dnsmasq
- Apache Web Servers
- Virtual Directories
- Clone the Target Access Point and Begin the Attack
- Start the Wireless Interface
- Deauthenticate Clients Connected to the Target Access Point
- Wait for the Client to Associate to Your Access Point
- Spoof the Application
- Modify the Page

- Example Page
- Login/php page
- Redirect Web Traffic Using Dnsmasq

Module 7: Designing a DMZ

- Introduction
- DMZ Concepts
- 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
- Analyzing 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