

Key data

Course Number: M2SA-FT
Version 2.0

Duration: 256 Contact Hours

Language:

1. English

Format:

1. Instructor-led Course (lecture and labs)
2. 60% Hands-On, 40% Lectures

Student Materials:

1. Student Workbooks
2. Student Reference Manuals
3. Software/Tools DVDs & CDs

Certification Exams:

1. Mile2 CNS™
2. Mile2 CPTS™
3. Mile2 CDFE™
4. Mile2 CISSO™
5. Mile2 CISAP™

Prerequisites:

- Strong Drive to Excel Professionally
- B.Tech / MCA / B.Sc. / M.Sc
- English language fluency
- Pass the Mile2 Security Academy™ Entrance Exam
- Pass the Mile2 Security Academy™ Admission Interview.

© 2008/9 Mile2

FBI: Computer Crime Costs \$67 Billion

Mile2

Mile2 is an Information Security Training and Consulting Organization based in the United States of America whilst operating in the Americas, Australia, Asia Pacific, Europe and the Middle East through its elite partner network. Mile2's focus is on the design, development and delivery of Information Security programs that meet military, government security agency, private sector and institutional specifications.

Mile2 Culture

Vision

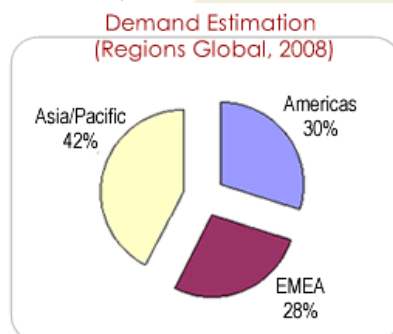
Being a relationship-focused company, our vision is to partner with our clients, consultants and instructors to predict, develop and deliver effective consulting and instruction services for emerging and mainstream technologies through diligent observation, research and implementation.

Goal

Mile2's enduring goal is to establish and contribute to a universal benchmark standard for adoption by Government, Military and Corporate Organizations whose intellectual property, secrets and infrastructure assets are significant strategic targets for compromise by elements with malicious and criminal intent.

Philosophy

In pursuing this enduring goal, Mile2 subscribes to a philosophy that endeavours to interface manpower, material and cutting edge technology to consistently yield optimum solutions to counter threats, while faithfully discharging our contractual and social obligations to our clients, consultants, instructors, students and the community.



Source: IDC, 2003

1. Information Security (IS) is one of the fastest growing segments of the Information Technology (IT) market.
2. Worldwide demand for IS services is expected to grow to USD\$23.6 Billion this year.
3. Global demand is much greater than supply as shown below:
 - Current worldwide demand for IS specialists: >60,000.
 - Projected worldwide demand for IS specialists by 2008: >188,000.
 - Expected shortfall is 100,000 IS professionals.
 - There are other roles in the IT industry which require professionals with high level of IS knowledge. The most significant of these are:
 - System and Network administrators - representing professionals involved in day-to-day administration of thousands of corporate systems and networks.
 - Systems and Software Development - representing professionals involved in design and development of computer systems and software.
 - Worldwide demand for professionals with IS skills expected to grow to 600,000 by 2008.

Mile2 Standards & Quality

Mile2 professional training standards cover pertinent industry standards while remaining largely "Vendor Independent" wherever possible. Mile2's distinguishing training hallmark is that our instructors immerse themselves deeply into their specialty. As such, they are able to bring about exciting laboratory exercises and real life examples into the classroom resulting in a fulfilling learning experience for our students. Mile2's instructor capabilities are derived not merely from their expected academic qualifications, but more importantly from impressive hands-on real world experience derived from related consultancy undertakings.

Mile2 Clients

Mile2 has served over 6000 private sector organizations and individuals in the finance, banking, insurance, oil and gas, telecommunications, outsourcing and education industries that place a high premium on Information Security. Mile2 has provided training services to most US military and intelligence agencies, as well as similar and related agencies for some of the USA's closest allies. These same services are available to the corporate and institutional world with student participation coming from a wide spectrum; it ranges from charities, banking, insurance, health, communications, transport, law enforcement and education to almost any sector imaginable.

Mile2 Clients Speak....

From US Marine Office: *"The CPTS course was taught to the Marine Corps Information Assurance Assessment Team and it was found to be a value-added skill set needed to accomplish our mission. The Marine Corps' current schools for Information Assurance Technician MOS 0689 does not offer any training like the CPTS course, so this would reinforce the need for this certification to be added to the DoDD 8570.1- M as Technical Level II and the CPTE as Technical Level III. We are already seeing the effects of commands using the 8570 as a tool to ensure properly trained personnel are assessing their networks. But we are also seeing contracting agencies and government agencies only training to what is written in the 8570.1-M and nothing else. This is going to hurt the IT sections that have specialized traits such as Information Assurances that do penetration testing and threat analysts work.*



"The Mile2 CPTS and CPTE surpasses the level of training provided by other certifications similar to it such as Foundstone and CEH (CNDA which they call it now), due to extensive hands on training that you receive. The CPTS / CPTE also teach the methodology of how to perform an assessment from a penetration tester's standpoint. The CEH is out to training only to teach how to pass a test and how to use dangerous tools. I have taken both courses and have found this (CPTS) to be one of the most professional certification courses I have been to, comparable only to CISSP.

"Being a former Marine Corps Data Chief and now a part of the Marine Corps Information Assurance Assessment Team I think that these two certifications would take vital role in training of our IA workforce. As Sun Tzu stated "Know your enemy".

Thank you for your time on this matter and I hope this information helps you in your studies of the 8570."

(Name Withheld for Security Reasons)

Technical Lead

US Marine Corps Information Assurance Assessment Team (MCIAAT)

From a Professional IT Security Professional: *"I must say that I am quite impressed with the entire training experience. I have a little over 15 years in security and assessment related work experience specific to IT. Even with that experience, I was impressed with the level of knowledge and expertise of the three instructors who taught the class and the information covered. What impressed me most was that almost no topic was discussed that was not fully supported with a hands-on lab designed to actually teach me to perform the task on my own. This is a very different approach to many of the 'Theory only' based classes that I have attended.*

As a result of this experience, I will be sending all of our current and future penetration and security assessment staff members to the CPTS and CPTE as soon as humanly possible."

Jared R. Greene, CISSP-ISSAP, ISSMP, CCNP, CCDP, CIPT, CTT, MCSE

Division President, Lead Assessor
InfoSight Assessment Services

From a Professional IT Security Analyst: *"It is very hard to choose the right training and with budgets tight for training money, you really hate to choose poorly. I've had a lot of experience with training in the security field. I retired from the Air Force about three years ago after a 20 year career, 10 of which I spent as a Technical Instructor. I now manage a team of security folks who specialize in Network Security assessments and penetration tests. As the leader of this group, it is my responsibility to identify appropriate training for them. We have set up a training path and try to keep it current.*

I chose the CPTS course for the following reasons. I really liked the course outline. The course was recommended by several users on the Security Focus Pen Test mailing list.

My experience with the course was very positive. The course content was right on, the instructor was very knowledgeable and obviously very experienced. They teach useful skills (not exam prep). The course material was up to date and plentiful. They also provided a wealth of resources to continue learning beyond your course. I really like that. I also liked the fact that the instructor was down to earth, did not try to convince us that he knew everything, and built upon the experiences of everyone in the course. My favourite day of the course is where we stayed late and played capture the flag, exercising the skills we had either just learned or sharpened."

Kelly Sparks, CISSP GSNA GGSC
Principal Computer Analyst, Dynetics, Inc.

From US Federal Aviation Administration Security Analyst: *"Having attended both the CPTS and CPE security training classes presented by Mile2, I will definitely recommend this training for IS security analysts within the FAA (Federal Aviation Administration).*



As you may know, our certification and authorization packages performed on various critical infrastructure assets are directed by FISMA guidelines, as well as other Federal directives and orders. FISMA guidelines state that 'periodic testing and evaluation of the effectiveness of information security policies, procedures and practices, to be performed with a frequency depending on risk,...which shall include testing of management, operational, and technical controls of every information system identified in the inventory...

The only way for an organization to know the effectiveness of the security controls already in place is to think like an attacker, and be knowledgeable about, and skilled with, the cyber attack tools that are readily available to anyone. This is not different than securing a house or other structure. You must know all of the entry points in order to make sure those are secure. This is where the value of the Mile2 CPTS/E classes lie. Mile2 instructors do not just teach theory of information system attacks. They have real world penetration testing experience that they professionally convey in a hands-on environment. I have attended a similar course offered through SANS which taught volumes about tools and theory, but with 300 other individuals in the class, and no hands-on until the last day of class, the learning experience was disappointing, to say the least. All Mile2 classes I have attended have had no more than 15 students, which allow substantial one-on-one time with the instructor.

All of the modules include hands-on labs that allow the student to gain an understanding of the attack tools, which is paramount in mitigating attacks.

All in all, Mile2 training far surpasses that of SANS for the following reasons:

- 1) *Small class size ensures that all questions from students are discussed and answered, either as a group, or one-on-one with the instructor. This is not possible in a large class setting typical of SANS training.*
- 2) *Hands-on experience with attack tools on a daily basis.*
- 3) *Lower cost than SANS training, usually by at least \$500.00.*

Thank you for presenting the penetration testing material in such a way that was very conducive to really absorbing the knowledge needed to better help me protect the critical information infrastructure of our nation."

(Name Withheld for Security Reasons) M.S. IA, CISSP
Senior Information Systems Security Analyst
Federal Aviation Administration / MMAC

From United Nations Security Officer:

"The CPTS course was excellent!"

Ernst H.,
United Nations Office on Drugs and Crime



From US ARMY IT Security Officer: *"The current table of certifications which meet DoD IA requirements per 8570.1-M is lacking in training focused on meeting threats to the DoD computer network operations environment.*

The CPTS course as taught is relevant to DoD Computer Network Defense efforts at Technical Level II and should be considered for inclusion in the matrix. The CPTS provides excellent awareness of the hacker threat to DoD AIS and the Tactics, Techniques and Procedures used by the hacker community.

In light of the recent cancellation of the military Computer Network Defense level III course at Fort Gordon due to interpretation of DoD Dir 8570, I would support adding the CPTS to the matrix to fill this void."



Name Withheld for Security Reasons)

LTC, AV, xxxxxxxx
CISSP, MCSA, MCSE, IANM
xxxxxx-DCSIM Information Assurance / Network Operations

From US Air Force Security Analyst: *"...it is clear that CPTS should be added into the certification matrix as either a Level II or Level III certification. Traditionally, IA personnel are gleaned from experienced System Administrators and/or Network Engineers/Operators that already have the underlying expertise of a system or set of systems in order to perform effective penetration tests in addition to feedback on understanding the vulnerability and the risk mitigation.*



I attended the CPTS course in XXXXXX without any expectations assuming that the instructor, XXXXX, would have been someone that had memorized the tool-set and briefed off of the slides. To my surprise, XXXXX was extremely knowledgeable with demonstrated real-world experience in the Penetration Testing arena. The course started off with an introduction to the Open Source Security Testing Methodology, and Rules of Engagement for a professional penetration tester, followed by the theory behind an attack, performing an actual attack, and ending with mitigations for the attack...this structure went on throughout all of the 15-or-so course modules. The modules ranged anywhere from "Google hacking" by using advanced operators, to constructing an actual exploit and running the exploit on a vulnerable machine. The CPTS certification should be considered for either Level II or Level III certification based on the idea that CISSP is used as a high-level understanding of security across many different areas, and CPTS is applying the understanding of security by performing the actual task that the CISSP course theorizes about."

Name Withheld for Security Reasons)

XXXXXXXX, SSgt, USAF
XXXXXXXXXXXXXXXXXXXX

The Mile2 Security Academy™ Programme

Governments and private corporations have been and are changing their traditional business models to e-business models. Financial institutions offer on-line banking solutions; multinationals manage their complex fusion of business processes through integrated enterprise applications, many of which store confidential data; retailers offer a bewildering array of products globally through on-line channels; stocks, bonds and futures are traded through on-line accounts.

E-Business models are highly dependent on electronic information and so are vulnerable to threats from sources such as hackers, viruses and denial of service attacks. It is vitally important that stakeholders are confident that business conducted via e-business models is secure and that associated risks are minimized through good management.

This confidence is delivered via **information security assurance**, which is *“the global approach to business involving authentication and verification of the on-going confidentiality, integrity and availability of an organization’s critical business information, so as to firstly promote the confidence of clients, business partners, the community and employees; secondly, to preserve the business position; and thirdly, to ensure business continuity.”*

The objective of information security assurance is to reduce an organization’s risk of business damage from a security incident to an acceptable level, whilst retaining the ability to carry out business. Demand for qualified and competent information security assurance professionals will far outstrip supply in the next few years. This is due to the obvious fact that every responsible organization, globally, will seek to manage their risks from security incidents. And security incidents are on the rise, every day.

The Mile2 Security Academy™ is built upon proven hands-on, tried and tested, information assurance methodologies utilized by our international group of specialized consultants. It maps to the Information Assurance technical and management skill requirements of the U. S. Department of Defense as outlined in the U.S Department of Defense 8570.01-M Information Assurance Workforce Improvement Programme. The Academy also enhances business skills needed to identify protection opportunities, justify testing activities and optimize security controls appropriate to business needs in order to reduce business risk. We go far beyond simply teaching you to “Hack” -- the norm with the classes that have been available until now. The Mile2 Security Academy™ is developed on the same principles and uses the same methods as those of a hacker, but its focus is on professional penetration testing and securing information assets. Students will enjoy an in-depth programme that is continuously updated to maintain and incorporate the ever changing security environment. The Mile2 Security Academy™ offers up-to-date proprietary, practical laboratories that have been researched and developed by leading information security professionals from around the world.

Mile2 will select applicants who meet stringent prerequisites, pass the entrance exam and interview successfully with Mile2 executives. Students will be exposed to the no-hype, serious business of information security assurance from Day One. 60% of instructor-student contact will be in practical labs designed by Mile2, and students will be expected to work in groups to complete challenging assignments. Performance will be assessed via multiple assignments and group projects, four knowledge-based exams, and one performance-based practical exam.

Programme Faculty

Mile2 Instructors keep abreast of their expertise by undertaking consulting assignments, as we believe that an equal emphasis on theoretical and real world experience is essential for effective knowledge transfer to you, the student. The Academy will feature multiple instructors from various Mile2 Country Offices.

Upon Completion

Mile2 Security Academy™ graduates will obtain real world security knowledge that will enable them to design information security management systems, recognize vulnerabilities, expose system weaknesses and help safeguard against threats. Graduates will have mastered the information security skills in high-demand by leading organizations globally. Upon successful completion of assignments, group projects, knowledge-based exams and the final performance-based practical exam, Mile2 Security Academy™ graduates would be certified as a Certified Netsec Specialist™, a Certified Penetration Testing Specialist™, a Certified Forensics Digital Examiner™, Certified Information Systems Security Officer™, and a Certified Information Security Assurance Professional™.

Programme Modules

The Heart of Information Assurance: Information Security Management Systems

- Module 1** Security Management Practices
- Module 2** Access Control Systems & Methodology
- Module 3** Cryptography
- Module 4** Physical Security
- Module 5** Enterprise Security Architecture
- Module 6** Law, Investigation, & Ethics

The IEEE (Implementing, Establishing, Evaluating & Enforcing) of Network Security

Module 7 Network Fundamentals

- Network Types (LANs, WANs)
- Network Topologies
- Ethernet, Token Ring
- ATM, ISDN, X.25
- Wireless
- Wiring
- Network Devices
- VLANs

- IP Concepts
- Packets and Addresses
- IP Service Ports
- IP Protocols
- TCP
- UDP
- CMP
- DNS

- IOS and Router Filters
- Routing Basics
- Understanding Cisco IOS
- Working of Routing Protocols
- Role/ Implementation of Access Control Lists

- Hands on Lab

Module 8 Telecommunications & Network Security

- TCP/IP Suite
- LAN, MAN, and WAN Topologies and Technologies
- Cable Types and Issues
- Broadband versus Baseband Technologies
- Ethernet and Token Ring
- Network Devices
- Firewall Types and Architectures
- Dial-up and VPN Protocols
- DNS and NAT Network Services
- FDDI and SONET
- X.25, Frame Relay, and ATM
- Wireless LANs and Security Issues

- Cell Phone Fraud
- VoIP
- Types of Attacks

Module 9 Designing & Configuring Secure VPNs

- VPN scenarios
 - Connecting remote users
 - Business partners
 - Branch offices
 - Hub and spoke architecture
 - Fully meshed topology
 - Comparing trusted and secure VPNs

- VPN technologies
 - VPNs at layers 2 and 3
 - Tunneling
 - Switching
 - MPLS
 - IPSec

- Security requirements
 - Privacy
 - Data confidentiality
 - Data integrity
 - Authentication
 - Maintaining availability
 - Role of cryptography

- Comparing tunneling types
 - Compulsory
 - Voluntary
 - Layer 2
 - Layer 3

- Implementing site-to-site tunnels
 - Generic Routing Encapsulation (GRE)
 - Defining MTU, routing and security issues
 - Allowing Internet access

- Creating tunnels for Access VPNs
 - L2F
 - PPTP
 - Layer 2 Tunneling Protocol (L2TP)
 - Implementing PPP authentication
 - Selecting PAP, CHAP or EAP
 - RADIUS servers
 - TACACS+

- Implementing IP Security
 - Introduction
 - IPSec tunnel and transport modes
 - IPSec and NAT

- VPN Security
 - VPNs and Firewalls
 - Authentication

- Hands On Lab

Module 10: Designing and Configuring Firewalls

- Introduction
 - What is a firewall
 - Firewall Usage
 - How do firewalls work
- Firewall Components
 - Basic Design
 - Limitations of Firewalls
- Firewall Policy
 - Where to start
 - Firewall policy requirements
 - Sample firewall policy
- Selection Criteria
 - Build or buy dilemma
 - Factors
 - Types of firewalls
 - Firewall Architectures
- Installing and Configuring Firewalls
 - Selecting the OS
 - Scanning for Vulnerabilities
 - Hardening the Bastion Host
 - Services
- Installing and Configuring CheckPoint Firewall – 1 NG
- Monitoring Firewall – 1 NG
- Installing and Configuring ISA Server
- Monitoring ISA Server
- IPTables Concepts and Implementation
 - Packet processing
 - The flow of IPTables
 - Configuration Options
 - Case study and practice
- Hands on Lab

Module 11: Designing and Configuring IDS

- IDS goals and roles
 - Definitions
 - Matrix
 - IDS Components , Roles and Goals
- IDS Technologies and Techniques
 - Detection process
 - Behavioral patterns
 - Collection and analysis of Information
- IDS Designs
 - Host based designs
 - Network based designs
- Identifying IDS Signatures
 - When and how to analyze
 - Recognizing exploits with anomaly detection, pattern matching and stateful analysis
 - Interval Analysis, real-time analysis, statistical analysis and signature analysis.
 - Improving quality of signatures
 - Writing a signature for a new exploit
- IDS Deployment
 - Detecting external threats

- Detecting internal threats
- Monitoring for attacks
- Determining attack methods
- Detecting scans
- Surveillance monitoring

- IDS Limitations
- Configuring IDS
- Snort Foundations
- Installing and configuring Snort
- IDScenter
- Installing, configuring and scanning with eTrust IDS
- Installing, configuring and running ISS Scanners
- Hands On Lab

Module 12 Securing Windows 2000/2003

- Windows 2000 Security Goals
 - Exposing the inherent weaknesses of the default Windows 2000 configuration
 - Enhancing and defining your security document for the Windows 2000 infrastructure
 - Achieving your security goals through the use of the latest technologies: PKI, Kerberos, SSL, NTFS, EFS, IPsec
- Implementing the latest technologies
 - Authentication components: SATs, SIDs, ACEs, WinLogin, DNS, LSA, MSGINA, SAM
 - Enhancing authentication through Group Policy
- Extending authentication security
 - Smart cards
 - Biometric devices
 - Integrating certificate-based authentication
 - Configuring and verifying Kerberos authentication parameters in the Active Directory (AD) using Group policies
 - Evaluating the concerns of down-level authentication with NT LAN Manager (NTLM)
- Securing resources with NTFS permissions
 - Setting NTFS Discretionary Access Control Lists (DACLs)
 - Configuring inheritance using industry best practices
 - Designing an enterprise-wide audit strategy
- Deploying the Encrypting File System (EFS)
 - Enabling EFS with digital certificates
 - Setting up recovery agents
 - Creating a file recovery policy using smart cards
- Exposing native NTFS vulnerabilities
 - Penetrating a Windows 2000/XP system using real-world hacker utilities
 - Reconfiguring native security
 - Running third-party tools to test and harden your system

- Protecting Active Directory objects
 - Setting permissions on directory objects
 - Delegating control over directory Organizational Units (OUs)
 - Ensuring enterprise-wide Registry security
 - Building and deploying templates to secure your environment
 - Configuring user privileges
 - Setting AD, Registry & file system security
 - Gaining global control of system services
 - Checking for compliance using templates
 - Establishing security baselines
 - Ensuring the integrity and confidentiality of data transmission
 - Securing data exchange with IPsec
 - Configuring the public and private key infrastructure with X.509 certificates
 - Applying industry best practices in security policy documents
 - Encryption architectures
 - Symmetric vs. asymmetric
 - Implementing encryption standards
 - Managing Windows 2000 PKI components
 - Installing and configuring Windows 2000 Certificate Server
 - Establishing standalone, enterprise and intermediate Certificate Authorities (CAs)
 - Selecting algorithms using Cryptographic Service Providers (CSPs)
 - Installing, creating, revoking and deleting X.509 digital certificates
 - Hands On Lab
- Module 13 Securing UNIX & Linux**
- Achieving UNIX security
 - Defending against exploits
 - Detecting intrusions with audits and logs
 - Avoiding security loopholes by replacing weak components
 - Protecting data and systems with cryptography
 - Pretty Good Privacy (PGP)
 - Gnu Privacy Guard (GnuPG)
 - Authenticity and integrity through digital signatures and cryptographic hashes
 - Establishing secure account usage
 - The UNIX login process
 - Controlling account access with Pluggable Authentication Modules (PAM)
 - Enforcing password quality
 - Monitoring and disabling accounts
 - Tracking account usage
 - How and when to disable accounts
 - Managing user and group IDs
 - Logging in across the network
 - Risks of trusted hosts and networks
 - Providing strong authentication for login with S/Key, tokens and OPIE
 - Replacing TELNET and rlogin servers and clients with SSH
 - Controlling root access
 - Configuring secure terminals
 - Preventing insecure network access
 - Gaining root privileges with su
 - Using groups instead of root identity
 - Auditing superuser activity
 - Limiting access to privileged accounts
 - Detecting misuse and attacks with log files
 - Role-based access control (RBAC)
 - Risks of UNIX all-or-nothing access
 - RBAC in Solaris
 - RBAC in NSA Security-Enhanced Linux
 - Adding RBAC with sudo
 - Directory structure and partitioning for security
 - Files, directories, devices and links
 - Employing read-only partitions
 - Ownership and access permissions
 - Using Access Control Lists (ACLs)
 - Immutable and append-only files
 - Backup and integrity testing
 - Safeguarding backed-up data
 - Detecting intrusions with Tripwire
 - The Network File System
 - Identifying NFS vulnerabilities
 - Securing NFS via Secure RPC
 - Hardening UNIX systems
 - Increasing security with yassp, TITAN and Bastille
 - Defending against distributed denial-of-service attacks
 - Risks from unwanted program execution
 - Starting programs surreptitiously
 - Running programs as other users
 - Checking cron and at queuing
 - Issues with scripts
 - Avoiding startup script vulnerabilities
 - Deflecting Trojan horse & other attacks
 - TCP/IP and its security loopholes
 - Killer pings, syn floods and their fixes
 - The critical role of DNS
 - Hardening the TCP/IP suite
 - Securing internal network services
 - Enabling enhanced logging
 - Installing OpenSSH and OpenSSL
 - Using DES encryption for secure RPC
 - Network authentication using Kerberos
 - X Window System vulnerabilities/solutions
 - Safely connecting to external networks

- Controlling and logging server access with TCP wrappers and xinetd
- Minimizing the effects of buffer overflow exploits
- Reducing information leakage
- Securing FTP, e-mail and Web access

Application Security

Module 14 Applications & Systems Development

Operational Security

Module 15 Operations Security

Attacking to Defend - Penetration Testing

- Module 16** Business & Technical Logistics for Penetration Testing
- Module 17** Information Gathering
- Module 18** Linux Fundamentals
- Module 19** Detecting Live Systems
- Module 20** Getting Rich from Enumeration
- Module 21** Cryptography Decrypted
- Module 22** Vulnerability Assessment Tools
- Module 23** Hacking Windows
- Module 24** Advanced Vulnerability & Exploitation Techniques
- Module 25** Malware, Trojans, Viruses & Botnets - Sandboxes
- Module 26** Cracking Wireless Networks
- Module 27** Packet Sniffing - Session Hijacking
- Module 28** Attacking the Firewall & IDS
- Module 29** Attacking Databases
- Module 30** Attacking Web Technologies

Computer Forensics (Servers, Personal Computers, Notebooks & Laptops)

- Module 31** Introduction to Computer Crime
- Module 32** Disk Storage Concepts
- Module 33** Forensic Examination
- Module 34** Electronic Discovery & Digital Evidence
- Module 35** Specialized Examination Tools
- Module 36** Seizure Concepts
- Module 37** Forensic Examination
- Module 38** Advanced Artefact Recovery
- Module 39** Crypto & Password Recovery

- Module 40** Specialized Digital Media Analysis & Recovery
- Module 41** Cyber-terrorism & Internet Investigations
- Module 42** Electronic Discovery, Acquisition & Analysis Laboratory
- Module 43** Documenting & Reporting Digital Evidence
- Module 44** Presentation of Digital Evidence

Business Continuity & Disaster Recovery

Module 45 Business Continuity Planning

