Thought Leadership...
Valiant
Technologies

Val-Ed™

Valiant Technologies Education & Training Services

5-day Hands-on Workshop on Ethical Hacking

Welcome to Valiant Technologies. We are a specialty consulting and training organization that focuses on information security at the strategic and operational levels. With significant strength also in information security assurance services, Valiant CISSTech, as we were formerly known, has been serving clients across many countries - Bahrain, Hong Kong, India, Kuwait, Malaysia, Maldives, Saudi Arabia, Sri Lanka, South Africa, Sultanate of Oman, Thailand, United Arab Emirates, and Zambia.

Val-Ed™, our educational services division offers a variety of ready-packaged and tailor-made educational and training programs in the area of information security. This catalogue provides detailed information on one of the educational and training offering to clients in the area of information security technology, management and assurance.

We have a full range of services that we offer covering the full spectrum of information security and our services catalogue provides details of the following services that we provide to clients. Please ask for a services catalogue for more details on these services:

- Testing and hardening of information system defenses:
    - Vulnerability assessment
    - Penetration testing
    - Application security testing
    - Hardening of servers and network components
    - Periodic evaluation of network security
- Information Security Management Services
    - Security Policies, Procedures and Guidelines
    - Security Awareness Program
    - Risk Assessment and Analysis
    - Executive Management briefings on Security
    - Vendor selection for security products
    - Computer Forensics Investigation\
    - ISO-27001 preparatory services
    - Fill-in Security Manager program
- Control and Assurance Services
    - Gap analysis against ISO-27001, COBIT, ISSAF
    - Information security controls review
    - Information Systems Security Audit
    - Control assessment for SOX compliance
- Business Continuity and Disaster Recovery Management

We look forward to being of service to you and look forward to hearing your interest.

- Valiant Team

List of regular programs offered by Valiant Technologies

	Course Name	Duration (days)
1	Workshop for CISSP certification aspirants	4
2	Workshop for CISA certification aspirants	5
3	Workshop for CISM certification aspirant	4
4	Workshop for CBCP certification aspirants	5
5	Workshop for Security+ certification aspirants	6
6	Workshop on BCP and DRP	2
7	Workshop on Change Management	1
8	Workshop on Information Security Policies	3
9	Information Security for Senior Management	½
10	Security Awareness for IT user management	2
11	Ethical Hacking and securing your networks	6
12	Sarbanes Oxley Act – Structure and Implementation	2
13	Digital Evidence for IT / IS Auditors	1
14	IS Audit: Principles and Practices	3
15	ISO 27001: Process and Implementation	5
16	Auditing Information Technology	3
17	Management for Technology Professionals	3

CV of principal instructor, Dr. Rama K Subramaniam is found on the last page

Workshop Description

A penetration tester is not a hacker! Managements mandate penetration testers to carry out various activities that evaluate, assess, certify and accredit the security of an information system that contains critical information assets. Since this process involves assessment of the security, there is a strong need for tester to bring in the best practices in penetration testing and adherence to the highest standards of professional ethics.

The objective of the course is to provide the in depth knowledge of the Information Security and Ethical Hacking. An attempt has been made to include all new techniques to the course so that you can be well aware of all Internet security concepts practiced in the industry.

Valiant Technologies has designed and offered many workshops for professionals interested in understanding penetration testing during the past many years in different parts of the world including India (Chennai & Bangalore – multiple times), UAE (Dubai and Abu Dhabi – multiple times), Bahrain (multiple times), Oman (multiple times), Saudi Arabia (Al-Khobar and Riyadh – multiple times), Kuwait and Sri Lanka (multiple times).

This course goes beyond what other courses generally teach – use of a plethora of tools and the ability to 'hack.' This course teaches you to look at security from multiple perspectives. Graduates of this course would have skill sets to talk to senior management and advice them on how to protect their networks.

The course uses the skills and tools a hacker uses but makes it positive – helps the candidate to know how to use these tools and methods to perform professional grade penetration testing. The intense hands-on content of this program distinguishes it from other tools oriented course

This workshop is for you...

Studies by a number of organizations across the world have consistently predicted that the next biggest investment in the IT industry would be in security. This training and certification would be useful for:

- Information System and technology professionals wanting to get into the thick of information security testing and certification of networks
- IT and IS Auditors, Networking professionals and security officers
- Security consultants and professionals needing an up-to-date knowledge of the methodology, techniques and globally recognized best practices in conducting penetration testing for various environments
- Security professionals who have acquired vendor-certifications wanting to move into a perspective level of security practice
- Professionals who have generic security and assurance certifications like CISSP, SSCP, SCNP, CISA, CISM, Security+ who would like to move into a more hands-on discipline like penetration testing
- Professionals who have passed ethical hacking and related certifications would like to graduate to penetration testing

At the end of the program, participants would take an on-line examination and successful candidates will be eligible to receive the coveted MASE certificate from Appinlabs, USA, in association with Manipal University.

Broad Content Areas

Module 1

1 Introduction to Information Security & Ethical Hacking
2 Desktop and Server Security
3 Viruses, Worms, Spywares
4 LAN Security
5 Firewalls & Security
6 Internet Security

Module 2

1 Information Gathering
2 Attacking the System-1

Module 3

1 Attacking the System-2
2 Data Backup
3 Art of Googling

Module 4

1 Penetration Testing
2 Catching Criminals
3 Cryptography and Forensics
4 Security Auditing
5 Linux and Unix

Detailed contents are provided on the following pages

Dr Rama K Subramaniam will personally deliver this workshop and he would be supported by lab-assistants who will work with the participants during their hands-on exercises and assist them in acquiring sufficient hands-on exposure.

Module-1

1. Introduction to Information Security & Ethical Hacking

- Introduction
- Cyber Threats
- Hacker Vs Cracker
- Ethical Hacking
- Challenges for a Hacker
- Don’t Get Caught
- Introductory Tutorial on Networks

2. Windows Security

- Windows Security
- Hacking into Windows XP, NT
- SAM (Security Accounts Manager)
- Deleted Files Restoration
- Registries
- Vulnerability
- Exploit
    - Definition
    - Digital Rights Management
    - Internet Explorer, Remote Desktop Protocol
    - Universal Plug and Play
    - Wi-Fi
    - Windows Meta File
- How to Look for Vulnerabilities?
- Securing Windows
    - Security Centre
    - Updating
    - System Configuration Utility
    - Windows Task Manager
- Windows Password Breaking

3. Viruses, Worms, Spywares

- Spywares
- Viruses and Worms Introduction
- Modes of Spreading
- Countermeasures

4. LAN Security

- Setting up a Local Area Network Connection
- Threats to LAN
- Network and File Sharing
- Firewalls
- Anti Virus
- Anti Spywares

- Network Scanners
- Hacking MAC Address
- Wifi Network Security
    - Discovery of Rogue Access Points & Vulnerabilities
    - Lock Down all Access Points
    - Encryption, Authentication and VPN
    - Wireless LAN Policies
    - Intrusion Detection and Protection

5. Firewalls & Security

- Introduction to Firewalls
- Working of a Firewall
- Types of Firewalls
- Packet Filters
- Proxy Gateways
- Network Address Translation
- Intrusion Detection
- Logging

6. Internet Security

- IP Addresses
- Finding an IP Address
- Through Instant Messaging Software
- Through Internet Relay Chat
- Through Website
- Through Email Headers
- Through Message Board Postings
- Anonymous Surfing
- Proxies Servers
- Transparent Proxies
- Anonymous Proxies
- Distorting Proxies
- Elite Proxies
- Free Proxy Servers
- Analysis of Email Headers
- Yahoo Email
- Google Email
- Email Tracking
- IP Tracing using Email
- Microsoft Outlook Security
- IP Addresses: Dangers & Concerns
- SSL (Secure Sockets Layer)
- SSH Dynamic Port Forwarding
- IP Spoofing

Module-2

1. Information Gathering

- Information Gathering for a Remote System
- Port Scanning
- Sockets
- Detection of TCP Port Scan
- TCP SYN Scanning
- Detection of SYN Scans
- SYN/ACK Scanning
- Detection of SYN/ACK Port Scan
- TCP FIN Scanning
- TCP XMAS tree scanning
- ACK Scanning
- UDP Ports
- Utility
- Daemon Banner Grabbing
- ICMP Messages
- Fingerprinting
- OS Fingerprinting
- Remote OS Fingerprinting

2. Attacking the System-1

- Introduction
- Non-technical Attacks
- Network Infrastructure Attacks
- Operating System Attacks
- Application & Other Specialized Attacks
- Technical Attacks
    - Denial of Services Attacks (DoS Attacks)
    - Distributed DoS Attacks (dDoS)
    - Key Logging
    - Trojan Attacks
    - Cross Site Scripting (XSS)
    - Input Validation
    - SQL Injection
    - Buffer Overflows
    - Email Forging

- Security Measures for Software Programmers

Module-3

1. Attacking the System-2

- Phishing
- Password Cracking
    - Password Guessing
    - Dictionary Based Attacks
    - Brute-Force Attacks
    - Default Passwords
- Attacks on LOG Files
- Sniffer Attacks
- Detection of Sniffers Running
- Stopping Sniffing Attacks
- Proxy Servers
- Spy Ware Software
- Remote Administration Tools (RATs)
- Viruses & Worms
- Anti-virus Software
- Some Protection Tools

2. Data Backup

- Reasons for Data Backup
- Strategies for Data Backup
    - Online
    - Softwares
    - Tape; CD
    - Email
    - Storage Area Network (SAN)
    - Network Attached Storage
- Action Plan for Data Recovery

3. Art of Googling

- Basic Search Techniques
    - Phrase Search
    - + Operator Search
    - - Operator Search
    - . Operator Search
    - * Operator Search
    - ~ Operator Search
    - Range Search
  - Advanced Search Techniques
    - Site
    - Intitle, Allintitle
    - Inurl, Allinurl
    - Link
    - Phonebook: Rphonebook, Bphonebook
  - Daterange
  - Cache
  - Filetype
- Google as a Proxy Server
- Robots.txt

Module-4

1. Penetration Testing

- Definition
- Methodology
- Basic Approaches
- External and Internal Views
-

2. Catching Criminals

Cyber Terrorism

- Overview
- Forms of Cyber Terrorism
- Factors & Reasons
- Countermeasures
- Challenges
- Case Study of China-Eagle Union Hacker Group

Honey Pots

- Definition
- Research Honey Pots
- Production Honey Pots
- Low Involved Honey Pots
- High Involved Honey Pots
- Pros & Cons
- Famous Honey Pots
- Honeynets

Cyber Laws

- Relevance of Cyber Laws
- Scope of Cyber Laws
- Relevant Acts- Domain Name Disputes
- Cyber crimes and Penalties

3. Cryptography and Forensics

Encryption & Cryptography

- Introduction to Cryptography
- Private Key Encryption
- Public Key Encryption
- DES Algorithm
- RSA Algorithm
- Hash Functions
- MD5 HASH algorithm
- Digital Signatures
- Encyptor setup

Computer Forensics

- Introduction to Forensics
- Digital Evidence
- Requirements for Forensics

- Steps taken in Forensics investigation
    - Acquisition
    - Identification
    - Evaluation
    - Presentation

- Forensic Toolkit

Steganography & Data Hiding

- Introduction
- Digital Watermarking
- Steganography v/s Cryptography
- Types of Steganography
    - In band Data Insertion
    - Data Algorithmic
    - Overt Based Grammar
    - Out-band Data Insertion
    - Overwriting Data Insertion
    - Overt Based Object Generation
- Steganography Tools & Applications

4. Security Auditing

- Audit Objectives
- Risk Analysis
- Auditing Steps
    - Previous Check
    - Planning & Organization
    - Network Control - Policies / Stds
    - Network Control - Hardware / Software
    - Network Data Standards and Data Access
    - Hardware and Software Backup and Recovery
    - Software Communications
    - Access to Network Operating Systems Software and Facilities
    - Data Encryption and Filtering
    - Internet Applications
    - Password Protection

- Security Trends

5. Linux and Unix

- Overview
- Root User
- Accessing Root

Dr. Rama K Subramaniam

MBA(UK), PHD, FCA, CISA, CISM, CISSP, CEH, CHFI, CSQP, MCSE, Security+

He is Director of Valiant Technologies Pvt Ltd and Tejas Brainware Systems Pvt Ltd. He has been an information security consultant, trainer and educator for over a decade. He has trained experts in many information security domains across Gulf nations, India, Far East and Africa. He is a consultant to a number of organizations in the commercial, government, armed forces, judiciary and law enforcement segments in these countries.

He serves as India's country representative at International Federation of Information Processing (IFIP), serving on their Technical Committee TC-11 dealing with information security. He is current Chairman of ISCCRF, a not-for-profit trust carrying out research in cyber crime management

He is a certified and experienced professional in the areas of creating and implementing secure information security architecture; internal controls systems and processes; conceptualization, creation, testing and maintenance of business continuity and disaster recovery plans; security audits and certification of network infrastructure; conceptualization and implementation of multi-factor authentication processes (including PKI and X.509 compliant certification infrastructure); creation, assessment and certification of SOX, COSO, CoBIT, ISO-27001, ISO-17799 and ISO-15408 compliant information security management systems.

He served earlier as Global Chair of the Education and Awareness Principles Expert Group of Globally Accepted Information Security Principles (GAISP), based in the United States and is former Global Chair of the Accreditation Process committee of Open Information Systems Security Group (OISSG), based in the UK where he estblished their certification and accreditation processes. He is the charter President of the first chapter of ISSA (Information Systems Security Association) in Asia and served on the boards of Dubai and Chennai chapters of ISACA.

He was formerly Managing Director of Thewo Corporate Services based in Lusaka, Zambia; Group Operations Director or Benetone Group of Companies based in Bangkok, Thailand and Commercial Director of Dynaspede Integrated Systems Ltd, based in Mumbai.