

## **Ethical Hacking and Countermeasures Course Outline**

### **COURSE CODE: ECCEHV6**

This class will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus creation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking.

This course prepares you for EC-Council Certified Ethical Hacker exam 312-50

### **Who Should Attend**

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

### **Duration:**

5 days (9:00 – 5:00)

### **Certification**

The Certified Ethical Hacker certification exam 312-50 will be conducted on the last day of training. Students need to pass the online Prometric exam to receive CEH certification.

### **Legal Agreement**

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

## **Module 1: Ethics and Legality**

- What is an Exploit?
- The security functionality triangle
- The attacker's process
- Passive reconnaissance
- Active reconnaissance
- Types of attacks
- Categories of exploits
- Goals attackers try to achieve
- Ethical hackers and crackers - who are they
- Self proclaimed ethical hacking
- Hacking for a cause (Hacktivism)
- Skills required for ethical hacking
- Categories of Ethical Hackers
- What do Ethical Hackers do?
- Security evaluation plan
- Types of Ethical Hacks
- Testing Types
- Ethical Hacking Report
- Cyber Security Enhancement Act of 2002
- Computer Crimes
- Overview of US Federal Laws
- Section 1029
- Section 1030
- Hacking Punishment

## **Module 2: Footprinting**

- What is Footprinting
- Steps for gathering information
- Whois
- <http://tu cows.com>
- Hacking Tool: Sam Spade
- Analyzing Whois output
- NSLookup
- Finding the address range of the network
- ARIN
- Traceroute
- Hacking Tool: NeoTrace
- Visual Route
- Visual Lookout
- Hacking Tool: Smart Whois
- Hacking Tool: eMailTracking Pro
- Hacking Tool: MailTracking.com

### **AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

## Module 3: Scanning

- Determining if the system is alive?
- Active stack fingerprinting
- Passive stack fingerprinting
- Hacking Tool: Pinger
- Hacking Tool: WS\_Ping\_Pro
- Hacking Tool: Netscan Tools Pro 2000
- Hacking Tool: Hping2
- Hacking Tool: icmpenum
- Detecting Ping sweeps
- ICMP Queries
- Hacking Tool: netcraft.com
- Port Scanning
- TCPs 3-way handshake
- TCP Scan types
- Hacking Tool: IPEye
- Hacking Tool: IPSECSCAN
- Hacking Tool: nmap
- Port Scan countermeasures
- Hacking Tool: HTTrack Web Copier
- Network Management Tools
- SolarWinds Toolset
- NeoWatch
- War Dialing
- Hacking Tool: THC-Scan
- Hacking Tool: PhoneSweep War Dialer
- Hacking Tool: Queso
- Hacking Tool: Cheops
- Proxy Servers
- Hacking Tool: SocksChain
- Surf the web anonymously
- TCP/IP through HTTP Tunneling
- Hacking Tool: HTTPort

## Module 4: Enumeration

- What is Enumeration
- NetBios Null Sessions
- Null Session Countermeasures
- NetBIOS Enumeration
- Hacking Tool: DumpSec
- Hacking Tool: NAT
- SNMP Enumeration
- SNMUtil
- Hacking Tool: IP Network Browser
- SNMP Enumeration Countermeasures
- Windows 2000 DNS Zone transfer
- Identifying Win2000 Accounts
- Hacking Tool: User2SID
- Hacking Tool: SID2User
- Hacking Tool: Enum
- Hacking Tool: UserInfo
- Hacking Tool: GetAcct
- Active Directory Enumeration

### AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

## Module 5: System Hacking

- Administrator Password Guessing
- Performing Automated Password Guessing
- Legion
- NTInfoScan
- Defending Against Password Guessing
- Monitoring Event Viewer Logs
- VisualLast
- Eavesdroppin on Network Password Exchange
- Hacking Tool: LophtCrack
- Hacking Tool: KerbCrack
- Privilege Escalation
- Hacking Tool: GetAdmin
- Hacking Tool: hk
- Manual Password Cracking Algorithm
- Automatic Password Cracking Algorithm
- Password Types
- Types of Password Attacks
- Dictionary Attack
- Brute Force Attack
- Distributed Brute Force Attack
- Password Change Interval
- Hybrid Attack
- Cracking Windows 2000 Passwords
- Retrieving the SAM file
- Redirecting SMB Logon to the Attacker
- SMB Redirection
- Hacking Tool: SMBRelay
- Hacking Tool: SMBRelay2
- SMBRelay Man-in-the-Middle (MITM)
- SMBRelay MITM Countermeasures
- Hacking Tool: SMBGrinder
- Hacking Tool: SMBDie
- Hacking Tool: NBTDeputy
- NetBIOS DoS Attack
- Hacking Tool: nbname
- Hacking Tool: John the Ripper
- LanManager Hash
- Password Cracking Countermeasures
- Keystroke Logger
- Hacking Tool: Spector
- AntiSpector
- Hacking Tool: eBlaster
- Hacking Tool: SpyAnywhere
- Hacking Tool: IKS Software Logger
- Hardware Tool: Hardware Key Logger
- Hacking Tool: Rootkit
- Planting Rootkit on Windows 2000 Machine
- \_rootkit\_ embedded TCP/IP Stack
- Rootkit Countermeasures
- MD5 Checksum utility
- Tripwire

### AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

- Covering Tracks
- Disabling Auditing
- Auditpol
- Clearing the Event Log
- Hacking Tool: Elslave
- Hacking Tool: Winzapper
- Hacking Tool: Evidence Eliminator
- Hidding Files
- NTFS File Streaming
- Hacking Tool: makestrm
- NTFS Streams Countermeasures
- LNS
- Steganography
- Hacking Tool: ImageHide
- Hacking Tool: MP3Stego
- Hacking Tool: Snow
- Hacking Tool: Camera/Shy
- Steganography Detection
- StegDetect
- Encrypted File System
- Hacking Tool: dskprobe
- Hacking Tool: EFSView
- Buffer Overflows
- Creating Buffer Overflow Exploit
- Outlook Buffer Overflow
- Hacking Tool: Outoutlook

## **Module 6: Trojans and Backdoors**

- What is a Trojan Horse?
- Overt and Covert
- Hacking Tool: QAZ
- Hacking Tool: Tini
- Hacking Tool: Netcat
- Hacking Tool: Donald Dick
- Hacking Tool: SubSeven
- Hacking Tool: BackOrifice 2000
- Back Oriffice Plug-ins
- Hacking Tool: NetBus
- Wrappers
- Hacking Tool: Graffiti
- Hacking Tool: Silk Rope 2000
- Hacking Tool: EliteWrap
- Hacking Tool: IconPlus
- Packaging Tool: Microsoft WordPad
- Hacking Tool: Whack a Mole
- Trojan Construction Kit
- BoSniffer
- Hacking Tool: FireKiller 2000
- Covert Channels
- ICMP Tunneling

### **AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

- Hacking Tool: Loki
- Reverse WWW Shell
- Backdoor Countermeasures
- BO Startup and Registry Entries
- NetBus Startup and Registry Keys
- Port Monitoring Tools
- fPort
- TCPView
- Process Viewer
- Inzider - Tracks Processes and Ports
- Trojan Maker
- Hacking Tool: Hard Disk Killer
- Man-in-the-Middle Attack
- Hacking Tool: dsniff
- System File Verification
- TripWire

## **Module 7: Sniffers**

- What is a Sniffer?
- Hacking Tool: Ethereal
- Hacking Tool: Snort
- Hacking Tool: WinDump
- Hacking Tool: EtherPeek
- Passive Sniffing
- Active Sniffing
- Hacking Tool: EtherFlood
- How ARP Works?
- Hacking Tool: DSniff
- Hacking Tool: Macof
- Hacking Tool: mailsnarf
- Hacking Tool: URLsnarf
- Hacking Tool: Webspay
- Hacking Tool: Ettercap
- Hacking Tool: SMAC
- MAC Changer
- ARP Spoofing Countermeasures
- Hacking Tool: WinDNSSpoof
- Hacking Tool: WinSniffer
- Network Tool: IRIS
- Network Tool: NetInterceptor
- SniffDet
- Hacking Tool: WinTCPKill

### **AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

## **Module 8: Denial of Service**

- What is Denial of Service Attack?
- Types of DoS Attacks
- How DoS Work?
- What is DDoS?
- Hacking Tool: Ping of Death
- Hacking Tool: SSPing
- Hacking Tool: Land
- Hacking Tool: Smurf
- Hacking Tool: SYN Flood
- Hacking Tool: CPU Hog
- Hacking Tool: Win Nuke
- Hacking Tool: RPC Locator
- Hacking Tool: Jolt2
- Hacking Tool: Bubonic
- Hacking Tool: Targa
- Tools for Running DDoS Attacks
- Hacking Tool: Trinoo
- Hacking Tool: WinTrinoo
- Hacking Tool: TFN
- Hacking Tool: TFN2K
- Hacking Tool: Stacheldraht
- Hacking Tool: Shaft
- Hacking Tool: mstream
- DDoS Attack Sequence
- Preventing DoS Attack
- DoS Scanning Tools
- Find\_ddos
- SARA
- DDoSPing
- RID
- Zombie Zapper

## **Module 9: Social Engineering**

- What is Social Engineering?
- Art of Manipulation
- Human Weakness
- Common Types of Social Engineering
- Human Based Impersonation
- Important User
- Tech Support
- Third Party Authorization
- In Person
- Dumpster Diving
- Shoulder Surfing
- Computer Impersonation
- Mail Attachments
- Popup Windows
- Website Faking
- Reverse Social Engineering
- Policies and Procedures
- Social Engineering Security Policies
- The Importance of Employee Education

### **AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

## **Module 10: Session Hijacking**

- What is Session Hijacking?
- Session Hijacking Steps
- Spoofing Vs Hijacking
- Active Session Hijacking
- Passive Session Hijacking
- TCP Concepts - 3 way Handshake
- Sequence Numbers
- Sequence Number Example
- Guessing the Sequence Numbers
- Hacking Tool: Juggernaut
- Hacking Tool: Hunt
- Hacking Tool: TTYWatcher
- Hacking Tool: IP Watcher
- Hacking Tool: T-Sight
- Remote TCP Session Reset Utility
- Dangers Posed by Session Hijacking
- Protection against Session Hijacking

## **Module 11: Hacking Web Servers**

- Apache Vulnerability
- Attacks against IIS
- IIS Components
- ISAPI DLL Buffer Overflows
- IPP Printer Overflow
- msw3prt.dll
- Oversized Print Requests
- Hacking Tool: Jill32
- Hacking Tool: IIS5-Koei
- Hacking Tool: IIS5Hack
- IPP Buffer Overflow Countermeasures
- ISAPI DLL Source Disclosure
- ISAPI.DLL Exploit
- Defacing Web Pages
- IIS Directory Traversal
- Unicode
- Directory Listing
- Clearing IIS Logs
- Network Tool: LogAnalyzer
- Attack Signature
- Creating Internet Explorer (IE) Trojan
- Hacking Tool: IISExploit
- Hacking Tool: UnicodeUploader.pl
- Hacking Tool: cmdasp.asp
- Escalating Privileges on IIS
- Hacking Tool: IISCrack.dll
- Hacking Tool: ispc.exe
- Unspecified Executable Path Vulnerability
- Hacking Tool: CleanIISLog

- File System Traversal Countermeasures
- Microsoft HotFix Problems
- UpdateExpert
- Cacls utility
- Network Tool: Whisker
- N-Stealth Scanner
- Hacking Tool: WebInspect
- Network Tool: Shadow Security Scanner

## **Module 12: Web Application Vulnerabilities**

- Documenting the Application Structure
- Manually Inspecting Applications
- Using Google to Inspect Applications
- Directory Structure
- Hacking Tool: Instant Source
- Java Classes and Applets
- Hacking Tool: Jad
- HTML Comments and Contents
- Hacking Tool: Lynx
- Hacking Tool: Wget
- Hacking Tool: Black Widow
- Hacking Tool: WebSleuth
- Cross Side Scripting
- Session Hijacking using XSS
- Cookie Stealing
- Hacking Tool: IEEN

## **Module 13: Web Based Password Cracking Techniques**

- Basic Authentication
- Message Digest Authentication
- NTLM Authentication
- Certificate based Authentication
- Digital Certificates
- Microsoft Passport Authentication
- Forms based Authentication
- Creating Fake Certificates
- Hacking Tool: WinSSLMiM
- Password Guessing
- Hacking Tool: WebCracker
- Hacking Tool: Brutus
- Hacking Tool: ObiWan
- Hacking Tool: Munga Bunga
- Password dictionary Files
- Attack Time
- Hacking Tool: Variet
- Hacking Tool: PassList
- Query Strings
- Post data
- Hacking Tool: cURL
- Stealing Cookies
- Hacking Tool: CookieSpy
- Hacking Tool: ReadCookies
- Hacking Tool: SnadBoy

### **AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

## Module 14: SQL Injection

- What is SQL Injection Vulnerability?
- SQL Insertion Discovery
- Blank sa Password
- Simple Input Validation
- SQL Injection
- OLE DB Errors
- 1=1
- blah' or 1=1
- Stealing Credit Card Information
- Preventing SQL Injection
- Database Specific SQL Injection
- Hacking Tool: SQLDiet
- Hacking Tool: SQLExec
- Hacking Tool: SQLbf
- Hacking Tool: SQLSmack
- Hacking Tool: SQL2.exe
- Hacking Tool: Oracle Password Buster

## Module 15: Hacking Wireless Networks

- 802.11 Standards
- What is WEP?
- Finding WLANs
- Cracking WEP keys
- Sniffing Traffic
- Wireless DoS Attacks
- WLAN Scanners
- WLAN Sniffers
- MAC Sniffing
- Access Point Spoofing
- Securing Wireless Networks
- Hacking Tool: NetTumbler
- Hacking Tool: AirSnort
- Hacking Tool: AiroPeek
- Hacking Tool: WEP Cracker
- Hacking Tool: Kismet
- WIDZ- Wireless IDS

## Module 16: Virus and Worms

- Cherobyl
- ExploreZip
- I Love You
- Melissa
- Pretty Park
- Code Red Worm
- W32/Klez
- BugBear
- W32/Opaserv Worm
- Nimda
- Code Red
- SQL Slammer
- How to write your own Virus?
- Worm Construction Kit

### AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

## **Module 17: Novell Hacking**

- Common accounts and passwords
- Accessing password files
- Password crackers
- Netware Hacking Tools
- Chknull
- NOVELBFH
- NWPCRAK
- Bindery
- BinCrack
- SETPWD.NLM
- Kock
- userdump
- Burglar
- Getit
- SpooFlog
- Gobbler
- Novelffs
- Pandora

## **Module 18: Linux Hacking**

- Why Linux ?
- Linux Basics
- Compiling Programs in Linux
- Scanning Networks
- Mapping Networks
- Password Cracking in Linux
- Linux Vulnerabilities
- SARA
- TARA
- Sniffing
- A Pinger in Disguise
- Session Hijacking
- Linux Rootkits
- Linux Security Countermeasures
- IPChains and IPTables

## **Module 19: IDS, Firewalls and Honeypots**

- Intrusion Detection System
- System Integrity Verifiers
- How are Intrusions Detected?
- Anomaly Detection
- Signature Recognition
- How does IDS match Signatures with Incoming Traffic?
- Protocol Stack Verification
- Application Protocol Verification
- What Happens after an IDS Detects an Attack?
- IDS Software Vendors
- SNORT

### **AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

- Evading IDS (Techniques)
- Complex IDS Evasion
- Hacking Tool: fragrouter
- Hacking Tool: TCPReplay
- Hacking Tool: SideStep
- Hacking Tool: NIDSbench
- Hacking Tool: ADMutate
- IDS Detection
- Tools to Detect Packet Sniffers
- Tools to inject strangely formatted packets onto the wire
- Hacking Through Firewalls
- Placing Backdoors through Firewalls
- Hiding behind Covert Channels
- What is a Honeygot?
- Honeygot Evasion
- Honeygot vendors

## **Module 20: Buffer Overflows**

- What is a Buffer Overflow?
- Exploitation
- Assembly Language Basics
- How to Detect Buffer Overflows in a Program?
- Skills Required
- CPU/OS Dependency
- Understanding Stacks
- Stack Based Buffer Overflows
- Buffer Overflow Technical Implementation
- Writing your own Buffer Overflow Exploit in C
- Defense against Buffer Overflows
- Type Checking Tools for Compiling Programs
- StackGuard
- Immunix

## **Module 21: Cryptography**

- What is PKI?
- Digital Certificates
- RSA
- MD-5
- RC-5
- SHA
- SSL
- PGP
- SSH
- Encryption Cracking Techniques

### **AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

- **Module 22 : Penetration Testing**
- Need for a Methodology
- Penetration Test vs. Vulnerability Test
- Reliance on Checklists and Templates
- Phases of Penetration Testing
- Passive Reconnaissance
- Best Practices
- Results that can be expected
- Indicative passive reconnaissance steps include (but are not limited to)
- Introduction to Penetration Testing
- Type of Penetration Testing Methodologies
- Open Source Vs Proprietary Methodologies
- Security Assessment Vs Security Auditing
- Risk Analysis
- Types of Penetration Testing
- Types Ethical Hacking
- Vulnerability Assessment Vs Penetration Testing
- Do-it Yourself Testing
- Firms Offering Penetration Testing Services
- Penetration Testing Insurance
- Explication of Terms of Engagement
- Pen-Test Service Level Agreements
- Offer of Compensation
- Starting Point and Ending Points of Testing
- Penetration Testing Locations
- Black Box Testing
- White Box Testing
- Grey Box Testing
- Manual Penetration Testing
- Automated Penetration Testing
- Selecting the Right Tools
- Pen Test Using Appscan
- HackerShield
- Pen-Test Using Cerberus Internet Scanner
- Pen-Test Using CyberCop Scanner
- Pen-Test Using Foundscan
- Pen-Test Using Nessus
- Pen-Test Using NetRecon
- Pen-Test Using Retina
- Pen-Test Using SAINT
- Pen-Test Using SecureNET
- Pen-Test Using SecureScan
- Pen-Test Using SATAN, SARA and Security Analyzer
- Pen-Test Using STAT Analyzer
- Pen-Test Using Twwsan
- VigilEnt
- WebInspect
- Evaluating Different Types of Pen-Test Tools
- Platform on Which Tools Will be Used

**AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

- Asset Audit
- Fault Tree and Attack Trees
- GAP Analysis
- Device Inventory
- Perimeter Firewall Inventory
- Web Server Inventory
- Load Balancer Inventory
- Local Area Network Inventory
- Demilitarized Zone Firewall
- Internal Switch Network Sniffer
- Application Server Inventory
- Database Server Inventory
- Name Controller and Domain Name Server
- Physical Security
- ISP Routers
- Legitimate Network Traffic Threat
- Unauthorized Network Traffic Threat
- Unauthorized Running Process Threat
- Loss of Confidential Information
- Business Impact of Threat
- Pre-testing Dependencies
- Post-testing Dependencies
- Failure Management
- Test Documentation Processes
- Penetration Testing Tools
- Defect Tracking Tools
- Configuration Management Tools
- Disk Replication Tools
- Pen-Test Project Scheduling Tools
- Network Auditing Tools
- DNS Zone Transfer Testing Tools
- Trace Route Tools and Services
- Network Sniffing Tools
- Denial of Service Emulation Tools
- Traditional Load Testing Tools
- System Software Assessment Tools
- Operating System Protection Tools
- Fingerprinting Tools
- Port Scanning Tools
- Directory and File Access Control Tools
- File Share Scanning Tools
- Password Directories
- Password Guessing Tools
- Link Checking Tools
- Web site Crawlers
- Web-Testing based Scripting Tools
- Buffer Overflow Protection Tools
- Buffer Overflow Generation Tools
- Input Data Validation Tools
- File encryption Tools
- Database Assessment Tools
- Keyboard Logging and Screen Reordering Tools

**AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)

- System Event Logging and Reviewing Tools
- Tripwire and Checksum Tools
- Mobile-Code Scanning Tools
- Centralized Security Monitoring Tools
- Web Log Analysis Tools
- Forensic Data and Collection Tools
- Security Assessment Tools
- Multiple OS Management Tools
- SANS Institute TOP 20 Security Vulnerabilities
- All Operating System Platforms
- Default installs of operating systems and applications
- Accounts with no passwords or weak passwords
- Nonexistent or incomplete backups
- Large number of open ports
- Not filtering packets for correct incoming and outgoing addresses
- Nonexistent or incomplete logging
- Vulnerable Common Gateway Interface (CGI) programs
- Windows-specific
- Unicode vulnerability-Web server folder traversal
- Internet server application programming interface (ISAPI) extension buffer overflows
- IIS Remote Data Services (RDS) exploit
- Network Basic Input Output System (NetBIOS), unprotected Windows networking shares
- Information leakage via null session connections
- Weak hashing in SAM (Security Accounts Manager)-LanManager hash
- UNIX-specific
- Buffer overflows in Remote Procedure Call (RPC) services
- Sendmail vulnerabilities
- Bind weaknesses
- Remote system command (such as rcp, rlogin, and rsh) vulnerabilities
- Line Printer Daemons (LPD) vulnerabilities
- Sadmin and mountd exploits
- Default Simple Network Management Protocol (SNMP) strings
- Penetration Testing Deliverable Templates
- Test Status Report Identifier
- Test Variances
- Test Comprehensive Assessment
- Summary of Results (Incidents)
- Test Evaluation
- Names of Persons (Approval)
- Template Test Incident Report
- Template Test Log
- Active Reconnaissance
- Attack Phase
- Activity: Perimeter Testing
- Activity: Web Application Testing – I
- Activity: Web Application Testing – II
- Activity: Wireless Testing
- Activity: Acquiring Target
- Activity: Escalating Privileges
- Activity: Execute, Implant & Retract
- Post Attack Phase & Activities
- Automated Penetration Testing

**AVANTUS TRAINING PTE LTD**

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: [enquiries@AvantusTraining.com](mailto:enquiries@AvantusTraining.com)

[www.AvantusTraining.com](http://www.AvantusTraining.com)