Corrientes 861 Piso 5 - S2000CTH -Rosario
Tel: +54 (341) 426 4844 - info@fullsolutions.com
www.fullsolutions.com

Curso: Ethical Hacking and Countermeasures

Module 1: Introduction to Ethical Hacking

- Who is a Hacker?
- Essential Terminologies
- Effects of Hacking
- Effects of Hacking on Business
- Elements of Information Security
- Authenticity and Non-Repudiation
- The Security, Functionality, and Usability Triangle
- What Does a Hacker Do?
- Phase 1 – Reconnaissance
    - Reconnaissance Types
- Phase 2 – Scanning
- Phase 3 – Gaining Access
- Phase 4 – Maintaining Access
- Phase 5 – Covering Tracks
- Types of Attacks on a System
    - Operating System Attacks
    - Application-Level Attacks
    - Shrink Wrap Code Attacks
    - Misconfiguration Attacks
- Why Ethical Hacking is Necessary?
- Defense in Depth
- Scope and Limitations of Ethical Hacking
- What Do Ethical Hackers Do?
- Skills of an Ethical Hacker
- Vulnerability Research
- Vulnerability Research Websites
- What is Penetration Testing?
- Why Penetration Testing?
- Penetration Testing Methodology

Module 2: Footprinting and Reconnaissance

- Footprinting Terminologies
- What is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Finding a Company's URL
- Locate Internal URLs
- Public and Restricted Websites
- Search for Company's Information
    - Tools to Extract Company's Data
- Footprinting Through Search Engines
- Collect Location Information
- People Search
    - People Search Using http://pipl.com
    - People Search Online Services
    - People Search on Social Networking Services
- Gather Information from Financial Services
- Footprinting Through Job Sites
- Monitoring Target Using Alerts

Microsoft Partner

- Competitive Intelligence Gathering
- WHOIS Lookup
- Extracting DNS Information
- DNS Interrogation Tools
- DNS Interrogation Online Tools
- Locate the Network Range
- Traceroute
- Mirroring Entire Website
- Extract Website Information from http://www.archive.org
- Tracking Email Communications
- Footprint Using Google Hacking Techniques
- What a Hacker Can Do With Google Hacking?
- Google Advance Search Operators
- Finding Resources using Google Advance Operator
- Google Hacking Tool: Google Hacking Database (GHDB)
- Google Hacking Tools
- Additional Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing

Module 3: Scanning Networks

- Network Scanning
- Types of Scanning
- Checking for Live Systems – ICMP Scanning
- Ping Sweep
- Three-Way Handshake
- TCP Communication Flags
- Hping Commands
- Scanning Techniques
- Scanning Tools
- Scanning Countermeasures
- OS Fingerprinting
- Banner Grabbing Tools
- Hiding File Extensions
- Vulnerability Scanning
- Network Vulnerability Scanners
- Network Mappers
- Proxy Servers
- Why Attackers Use Proxy Servers?
- Use of Proxies for Attack
- Free Proxy Servers
- TOR (The Onion Routing)
- TOR Proxy Chaining Software
- HTTP Tunneling Techniques
- Why do I Need HTTP Tunneling?
- Additional HTTP Tunneling Tools
- SSH Tunneling
- Proxy Tools
- Types of Anonymizers
- Anonymizer Tools
- Spoofing IP Address
- IP Spoofing Countermeasures
- Scanning Pen Testing

Microsoft Partner

Module 4: Enumeration

- What is Enumeration?
- Techniques for Enumeration
- Netbios Enumeration
- Enumerating User Accounts
- Enumerate Systems Using Default Passwords
- SNMP (Simple Network Management Protocol) Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- SMTP Enumeration
- DNS Zone Transfer Enumeration Using nslookup
- Enumeration Countermeasures
- Enumeration Pen Testing

Module 5: System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- Password Cracking
    - Password Complexity
    - Password Cracking Techniques
    - Types of Password Attacks
        - Passive Online Attacks: Wire Sniffing
        - Password Sniffing
        - Passive Online Attack: Man-in-the-Middle and Replay Attack
        - Active Online Attack: Password Guessing
            - Active Online Attack: Trojan/Spyware/Keylogger
            - Active Online Attack: Hash Injection Attack
    - Rainbow Attacks: Pre-Computed Hash
    - Distributed Network Attack
    - Non-Electronic Attacks
    - Manual Password Cracking (Guessing)
    - Automatic Password Cracking Algorithm
    - Stealing Passwords Using USB Drive
- Microsoft Authentication
- How Hash Passwords are Stored in Windows SAM?
- What is LAN Manager Hash?
- Kerberos Authentication
- Salting
- Password Cracking Tools
- How to Defend against Password Cracking?
- Privilege Escalation
- Privilege Escalation Tools
- How to Defend against Privilege Escalation?
- Executing Applications
- Keylogger
- Types of Keystroke Loggers
- Keyloggers
- Spyware
    - What Does the Spyware Do?
    - Types of Spywares
- How to Defend against Keyloggers?
    - Anti-Keylogger
    - Anti-Keyloggers

Microsoft Partner

- How to Defend against Spyware?
- Rootkits
- Types of Rootkits
- How Rootkit Works?
- Detecting Rootkits
    - Steps for Detecting Rootkits
- How to Defend against Rootkits?
- What is Steganography?
- Types of Steganography
- Image Steganography
- Steganography Detection Tools
- System Hacking Penetration Testing

Module 6: Trojans & Backdoors

- What is a Trojan?
- Purpose of Trojans
- Indications of a Trojan Attack
- Common Ports used by Trojans
- How to Infect Systems Using a Trojan?
- Wrappers
- Different Ways a Trojan can Get into a System
- How to Deploy a Trojan?
- Evading Anti-Virus Techniques
- Types of Trojans
- Destructive Trojans
- Notification Trojans
- Credit Card Trojans
- Data Hiding Trojans (Encrypted Trojans)
- How to Detect Trojans?
- Process Monitoring Tool: What's Running
    - Process Monitoring Tools
- Scanning for Suspicious Windows Services
- Scanning for Suspicious Startup Programs
- Scanning for Suspicious Files and Folders
- Scanning for Suspicious Network Activities
- Trojan Countermeasures
- Backdoor Countermeasures
- Pen Testing for Trojans and Backdoors

Module 7: Viruses & Worms

- Introduction to Viruses
- Stages of Virus Life
- Working of Viruses: Infection Phase
- Working of Viruses: Attack Phase
- Indications of Virus Attack
- Virus Hoaxes
- Virus Analysis:
- Types of Viruses
- Transient and Terminate and Stay Resident Viruses
- Writing a Simple Virus Program
- Computer Worms
- How is a Worm Different from a Virus?

Microsoft Partner

- Example of Worm Infection: Conficker Worm
- Worm Analysis:
- Malware Analysis Procedure
- Online Malware Testing:
- VirusTotal
- Online Malware Analysis Services
- Virus Detection Methods
- Virus and Worms Countermeasures
- Anti-virus Tools
- Penetration Testing for Virus

Module 8: Sniffers

- Sniffing Threats
- How a Sniffer Works?
- Hacker Attacking a Switch
- Types of Sniffing
- Protocols Vulnerable to Sniffing
- Hardware Protocol Analyzers
- SPAN Port
- MAC Flooding
- MAC Spoofing/Duplicating
- DNS Poisoning Techniques
- Sniffing Tools
- Discovery Tools
- Additional Sniffing Tools
- How an Attacker Hacks the Network Using Sniffers?
- How to Defend Against Sniffing?

Module 9: Denial of Service

- What is a Denial of Service Attack?
- What is Distributed Denial of Service Attacks?
- Symptoms of a DoS Attack
- Cyber Criminals
- DoS Attack Techniques
- Botnet
- DoS Attack Tools
- Detection Techniques
- DoS/DDoS Countermeasure Strategies
- Post-attack Forensics
- Techniques to Defend against Botnets
- DoS/DDoS Countermeasures
- DoS/DDoS Protection at ISP Level
- DoS/DDoS Protection Tool
- Denial of Service (DoS) Attack Penetration Testing

Module 10: Session Hijacking

- What is Session Hijacking?
- Why Session Hijacking is Successful?
- Key Session Hijacking Techniques
- Brute Forcing
- Spoofing vs. Hijacking
- Session Hijacking Process

Microsoft Partner

- Packet Analysis of a Local Session Hijack
- Types of Session Hijacking
- Predictable Session Token
- Man-in-the-Middle Attack
- Client-side Attacks
- Cross-site Script Attack
- Session Fixation
- Network Level Session Hijacking
- The 3-Way Handshake
- TCP/IP Hijacking
- Man-in-the-Middle Attack using Packet Sniffer
- Session Hijacking Tools
    - Paros
    - Burp Suite
    - Firesheep
- Countermeasures
- Protecting against Session Hijacking
- Session Hijacking Remediation
- Session Hijacking Pen Testing

Module 11: Hijacking Webservers

- Website Defacement
- Why Web Servers are Compromised?
- Impact of Webserver Attacks
- Webserver Misconfiguration
- Directory Traversal Attacks
- HTTP Response Splitting Attack
- Web Cache Poisoning Attack
- HTTP Response Hijacking
- SSH Bruteforce Attack
- Man-in-the-Middle Attack
- Webserver Password Cracking
- Web Application Attacks
- Webserver Attack Methodology
    - Information Gathering
    - Webserver Footprinting
        - Webserver Footprinting Tools
    - Mirroring a Website
    - Vulnerability Scanning
    - Session Hijacking
    - Hacking Web Passwords
- Webserver Attack Tools
- Web Password Cracking Tool
- Countermeasures
- How to Defend Against Web Server Attacks?
- Patches and Hotfixes
- What is Patch Management?
- Webserver Security Tools
- Web Server Penetration Testing

Microsoft Partner

Module 12: Hijacking Web Applications

- How Web Applications Work?
- Web 2.0 Applications
- Vulnerability Stack
- Web Attack Vectors
- Web Application Threats
- Unvalidated Input
- Parameter/Form Tampering
- Directory Traversal
- Security Misconfiguration
- Injection Flaws
    - SQL Injection Attacks
    - Command Injection Attacks
    - Command Injection Example
    - File Injection Attack
- Cross-Site Scripting (XSS) Attacks
    - How XSS Attacks Work?
    - Cross-Site Scripting Attack Scenario: Attack via Email
    - XSS Example: Attack via Email
    - XSS Example: Stealing Users' Cookies
    - XSS Example: Sending an Unauthorized Request
    - XSS Attack in Blog Posting
    - XSS Attack in Comment Field
    - XSS Cheat Sheet
    - Cross-Site Request Forgery (CSRF) Attack
    - How CSRF Attacks Work?
- Buffer Overflow Attacks
- Cookie/Session Poisoning
- Session Fixation Attack
- Improper Error Handling
- Insecure Cryptographic Storage
- Broken Authentication and Session Management
- Unvalidated Redirects and Forwards
- Footprint Web Infrastructure
- Web Spidering Using Burp Suite
- Hacking Web Servers
- Analyze Web Applications
- Attack Authentication Mechanism
- Username Enumeration
- Password Attacks: Password Functionality Exploits
- Password Attacks: Password Guessing
- Password Attacks: Brute-forcing
- Session Attacks: Session ID Prediction/ Brute-forcing
- Cookie Exploitation: Cookie Poisoning
- Authorization Attack
- Session Management Attack
- Attack Web App Client
- Web Application Hacking Tools
- Web Application Countermeasures
- Web Application Pen Testing

Microsoft Partner

Module 13: SQL Injections

- What is SQL Injection?
- SQL Injection Attacks
- Server Side Technologies
- HTTP Post Request
- SQL Injection Detection
- SQL Injection Black Box Pen Testing
- Types of SQL Injection
- What is Blind SQL Injection?
- SQL Injection Methodology
- Transfer Database to Attacker's Machine
- Interacting with the Operating System
- Interacting with the FileSystem
- How to Defend Against SQL Injection Attacks?

Module 14: Hacking Wireless Networks

- Wireless Networks
- Types of Wireless Encryption
- WEP Encryption
- How WPA Works?
- Temporal Keys
- How WPA2 Works?
- WEP vs. WPA vs. WPA2
- WEP Issues
- Wireless Threats: Access Control Attacks
- Wireless Threats: Integrity Attacks
- Wireless Threats: Confidentiality Attacks
- Wireless Threats: Availability Attacks
- Wireless Threats: Authentication Attacks
- Rogue Access Point Attack
- Wireless Hacking Methodology
- Find Wi-Fi Networks to Attack
- Attackers Scanning for Wi-Fi Networks
- Footprint the Wireless Network
- Wireless Sniffers
- Aircrack-ng Suite
- Man-in-the-Middle Attack
- WEP Cracking Using Cain & Abel
- WPA Brute Forcing Using Cain & Abel
- Wireless Security Layers
- How to Defend Against Wireless Attacks?
- Wireless Intrusion Prevention Systems
- Wi-Fi Vulnerability Scanning Tools
- Wireless Penetration Testing

Microsoft Partner

Module 15: Buffer Overflow

- Buffer Overflows
- Why are Programs And Applications Vulnerable?
- Understanding Stacks
- Stack-Based Buffer Overflow
- Understanding Heap
    - Heap-Based Buffer Overflow
- Stack Operations
    - Shellcode
- Knowledge Required to Program Buffer Overflow Exploits
- Buffer Overflow Steps
- Simple Uncontrolled Overflow
- Simple Buffer Overflow in C
- Identifying Buffer Overflows
- How to Detect Buffer Overflows in a Program?
- Buffer Overflow Penetration Testing

Module 16: Penetration Testing

- Introduction to Penetration Testing
- Security Assessments
- Vulnerability Assessment
- Penetration Testing
- Why Penetration Testing?
- What Should be Tested?
- What Makes a Good Penetration Test?
- Types of Penetration Testing
    - External Penetration Testing
    - Internal Security Assessment
    - Black-box Penetration Testing
    - Grey-box Penetration Testing
    - White-box Penetration Testing
    - Announced / Unannounced Testing
    - Automated Testing
    - Manual Testing
- Common Penetration Testing Techniques
- Using DNS Domain Name and IP Address Information
- Enumerating Information about Hosts on Publicly-Available Networks
- Phases of Penetration Testing
- Penetration Testing Methodology
- Outsourcing Penetration Testing Services
- Evaluating Different Types of Pentest Tools
- Application Security Assessment Tools

Microsoft Partner