
 577, Gold Plaza, Punjab Jewelers, M.G. Road,
Opp. Treasure Island Mall,
Indore, Madhya Pradesh 452001, INDIA

 +91-99777-47-168

 info@armourinfosec.com



WE ARE A LEARNING PLATFORM

About Us

Armour Infosec is a piece of knowledge and technical security solutions providing Company. We are a part of the Genext Group. We are delivering technology services and training to students and professionals. We are specialized in IT Security, Ethical Hacking, Cyber Security, Network Security, Website Security, Wireless Security, Web Designing And Development, Search Engine Optimization, Android Application Development, Network Support And Annual Maintenance Contract, Hardware & Networking and more. We give students the best of our knowledge which helps them for their bright future.

Ethical hackers use their knowledge to secure and improve the technology of organizations. They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach.

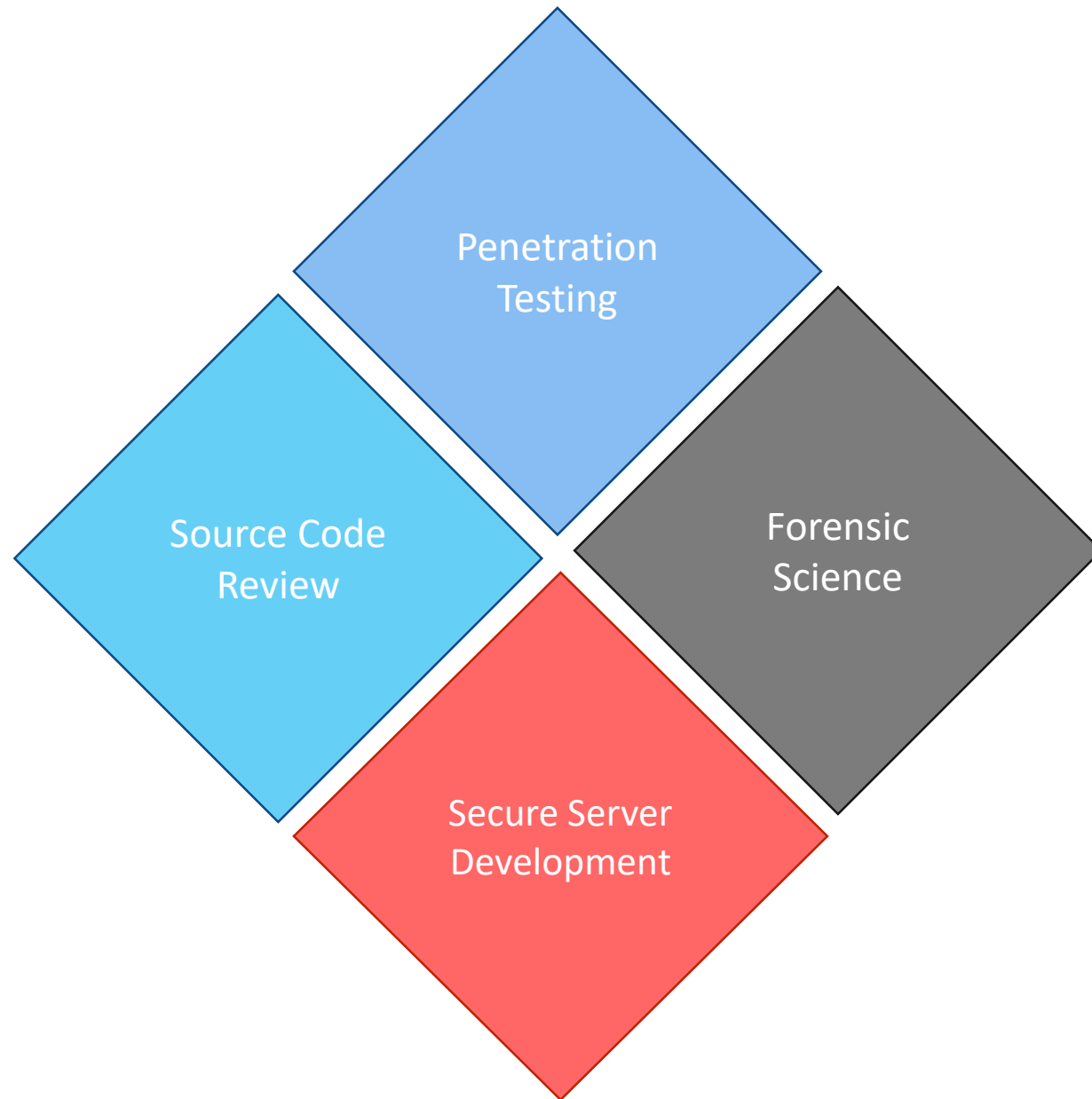
An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.

We believe in quality, client and student's satisfaction more than anything else. Education is very necessary for all and we are providing it in a manner that our trainees get the best in the industry.

WHY CHOOSE US



- **Our Quality Training and Professional Services.**
- **Necessary Theory and Maximum Practical.**
- **We teach Manual Methods Instead of Automate tools.**
- **Evening, Morning and Weekend batches available.**
- **Network administration and Development in Core.**
- **Amazing Ambience with skillful Trainees.**
- **We Provide Study Material with Necessary Tools and Practical Sessions.**
- **We held Workshops and Seminars on the Current topics of system Hacks.**



OUR COURSES



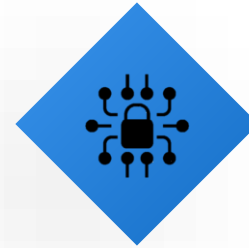
**Certified Information
Security Expert**



**Armour Infosec Certified
Ethical Hacking Penetration
Testing Expert**



**Armour Infosec Certified
Computer Hacking &
Forensic Expert**



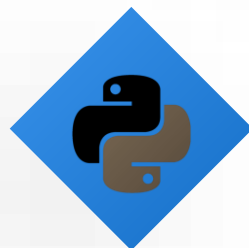
**Certified Network Security
Expert**



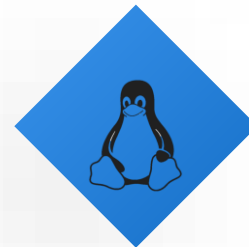
**Certified Web Security
Expert**



**Certified Wireless Security
Expert**



Python for Hackers



**Certified Linux Server
Administrator**



**Certified Windows Server
Administrator**

TITLE HERE

Certified Information Security Expert



What are the Objectives of the course?

- Implement technical strategies, tools, and techniques to secure data and information for your organization.
- Adhere to ethical security behavior for risk analysis and mitigation
- Understand security in cloud computing architecture in depth
- Comprehend legal requirements, privacy issues and audit process methodologies within the cloud environment
- Focus on IT compliance and the integrity of enterprise systems to establish a more secure enterprise IT framework

What are the Required Skillsets?

- Information security analysts must have strong analytical skills. They have to be able to study computer systems, assess any potential risks, and consider possible solutions.
- Creativity is critical for information security analysts. They must be able to anticipate cyber-attacks, always thinking one step ahead of a cyber threat. This kind of forward-thinking takes creativity.
- Threats to cybersecurity are always changing, as are solutions. Information security analysts have to constantly update their knowledge on the latest data-protection news, cyber-security legislation, and practices and techniques.

What are the career benefits of this training?

- Cybersecurity is vital for career roles such as penetration tester, cybersecurity analyst, network analyst, cybersecurity auditor, cybersecurity architect, forensics investigator, and many more.
- There are 2000+ cybersecurity jobs in India and 40,000+ in the US (Indeed.com). Cybersecurity job roles are expected to rise to six million worldwide by 2019.
- Expertise your skills in the management side of information security, including topics like governance, program development, and program, incident, and risk management.

OUR COURSE

Armour Infosec Certified Ethical Hacking & Penetration Testing Expert

Introducing Armour Infosec Certified Ethical Hacking and Penetration Testing Expert Certification module which is designed in a way that every topic will be covered with practical as well as theoretical Knowledge to the Students by the Professionals. Our aim is to make a Student, An IT Security Professional. Security threats are not only harmful, but sometimes undetectable too. If a person is enough oriented with Security countermeasures, he/she can prevent himself/herself from any attack before it happened. We are providing knowledge, the best in the industry. We have well designed labs with Network equipment's for live demonstration of Hacking Operations and for the prevention, we have a team of Professionals. For the Best experience in the world of Cyber Security, This module is well designed with all the principles of cyber security. We are working to spread the information security awareness campaigns to all the peoples, who are somehow connected to the internet and are using social networking sites to connect with the world. The strategies to maintain all the prevention countermeasures applied on a network are must to live forever. Our module contains Networking Fundamentals, Kali Linux Fundamentals, Introduction to Penetration Testing & Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks & Detecting Live System, Proxies, VPNs and Tor, Enumeration, System Hacking, Trojans and Backdoors, Viruses and Worms, Sniffers, Social Engineering, Denial of Service, Session Hijacking, Hacking Web servers, Advanced Exploitation Techniques, Hacking Web Applications, SQL Injection, Hacking Wireless Networks, Mobile Hacking, Evading IDS, Firewalls, and Honeypots, Buffer Overflow, Cryptography

DURATION



2 hours/ day X 150 days

ENROLL NOW



Units Covered



Windows Server



Red Hat Linux Server



WordPress



Secure Development in PHP



Python for Hackers



Ethical Hacking & Penetration
Testing

Secure Development in PHP



This module, PHP Web Application Security, helps developers to understand security risks, how vulnerabilities can be exploited, and how to avoid those attacks. First, you'll learn about how to defend against cross-site scripting, including new approaches such as content security policy. Next, you'll learn about how cross-site request forgery works, why it works so well, and how you can implement protection using PHP. Finally, the module will wrap up by teaching you how to protect against SQL injection attacks, covering not only MySQL but also other relevant databases PHP supports.

MODULE 01: INTRODUCTION

- Introduction to PHP

MODULE 02: PHP OVERVIEW

- What is PHP
- The history of PHP
- Why choose PHP
- Installation overview

MODULE 03: FIRST STEPS

- Embedding PHP code on a page
- Outputting dynamic text
- The operational trail
- Inserting code comments

MODULE 04: EXPLORING DATA TYPES

- Variables
- Strings
- String functions
- Numbers part one Integers
- Numbers part two
- Floating points
- Arrays
- Associative arrays
- Array functions
- Booleans
- NULL and empty
- Type juggling and casting
- Constants

Secure Development in PHP



MODULE 05: CONTROL STRUCTURES

Logical Expressions

- If statements
- Else and elseif statements
- Logical operators
- Switch statements

Loops

- While loops
- For loops
- Foreach loops
- Continue
- Break

- Understanding array pointers

MODULE 06: USER-DEFINED FUNCTIONS

- Defining functions
- Function arguments

- Returning values from a function
- Multiple return values

- Scope and global variables
- Setting default argument values

MODULE 07: DEBUGGING

- Common problems

- Warnings and errors

- Debugging and troubleshooting

MODULE 08: BUILDING WEB PAGES WITH PHP

- Links and URLs
- Using GET values
- Encoding GET values

- Encoding for HTML
- Including and requiring files
- Modifying headers

- Page redirection
- Output buffering

Secure Development in PHP




MODULE 09: WORKING WITH FORMS AND FORM DATA

- Building forms
- Detecting form submissions
- Single-page form processing
- Validating form values
- Problems with validation logic
- Displaying validation errors
- Custom validation functions
- Single-page form with validations




MODULE 10: WORKING WITH COOKIES AND SESSIONS

- Working with cookies
- Setting cookie values
- Reading cookie values
- Unsetting cookie values
- Working with sessions



MODULE 11: MYSQL BASICS

- MySQL introduction
- Creating a database
- Creating a database table
- CRUD in MySQL
- Populating a MySQL database
- Relational database tables
- Populating the relational table



MODULE 12: USING PHP TO ACCESS MYSQL

- Database APIs in PHP
- Connecting to MySQL with PHP
- Retrieving data from MySQL
- Working with retrieved data
- Creating records with PHP
- Updating and deleting records with PHP
- SQL injection
- Escaping strings for MySQL
- Introducing prepared statements

Secure Development in PHP



MODULE 13: APPLICATION CRUD

- Finding a subject in the database
- Refactoring the page selection
- Creating a new subject form
- Processing form values and adding subjects
- Passing data in the session
- Validating form values
- Creating an edit subject form
- Using single-page submission
- Deleting a subject
- Cleaning up
- Assignment Pages CRUD
- Assignment results Pages CRUD

MODULE 14: WORKING WITH FILES AND DIRECTORIES

- File system basics
- Understanding file permissions
- Setting file permissions
- PHP permissions
- Accessing files
- Writing to files
- Deleting files
- Moving the file pointer
- Reading files
- Examining file details
- Working with directories
- Viewing directory content

MODULE 15: SENDING EMAILS

- Configuring PHP for email
- Sending email with mail()
- Using headers
- Reviewing SMTP
- Using PHPMailer

Ethical Hacking & Penetration Testing

You will learn how to patch these networks as well as web applications with input validation using regular expressions. You will learn a security design pattern to avoid introducing injection vulnerabilities by input validation and replacing generic system calls with specific function calls. You will learn how to hack web apps with SQL injection vulnerabilities and retrieve user profile information and passwords. You will learn how to patch them with input validation and SQL parameter binding. Understand the better view of network application pentesting, Web Application Pentesting followed by reverse engineering and buffer-overflow. You will learn the hacking methodology, Nessus tool for scanning vulnerabilities, Kali Linux for penetration testing, and Metasploit Framework for gaining access to vulnerable Windows Systems, deploying keylogger, and performing Remote VNC server injection. You will learn security in memory systems and virtual memory layout, and understand buffer overflow attacks and their defenses.

MODULE 01: KALI LINUX FUNDAMENTALS

- Kali Linux history and introduction
- Kali Linux GUI desktops
- Kali Linux Commands
- Tar and zips
- Compiling programs
- Identifying software packages
- Installing and removing software
- User account management
- Changing a user account password
- Passwd & Shadow file formats
- File permissions
- Directory permissions
- Octal representation
- Changing permissions
- Setting default permissions
- Internet addressing
- Network services
- Commonly available services
- Fundamental network configuration files
- Network control scripts

MODULE 02: INTRODUCTION TO PENETRATION TESTING & ETHICAL HACKING

Hacking Concepts

- Introduction to Hacking
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who is a Hacker?
- Hacker Classes
- Hacktivism
- Hacking Phases
- Defense in Depth

Vulnerability Assessment & Penetration Testing

- Vulnerabilities
- Vulnerability Research
- Vulnerability Research Websites
- What is Penetration Testing?
- Why Penetration Testing
- Penetration Testing Methodology
- Security Policies
- Types of Security Policies

- Steps to Create and Implement Security Policies

Disaster Recovery & Risk Management

- Defining Risk Management
- Strategies for Managing Risk
- How to Analyze Risk
- Disaster Recovery Strategies
- Plan Testing and Execution

Ethical Hacking & Penetration Testing

MODULE 03: FOOTPRINTING AND RECONNAISSANCE

Footprinting Concepts and Methodology

- Footprinting Terminology
- What is Footprinting?
- Why Footprinting?
- Objectives of Footprinting
- Footprinting Threats

Footprinting using Search Engines

- Finding Company's External and Internal URLs
- Public and Restricted Websites
- Collect Location Information
- People Search
- People Search Online Services
- People Search on Social Networking Services
- Gather Information from Financial Services
- Footprinting through Job Sites
- Monitoring Target Using Alerts

Website Footprinting

- Mirroring Entire Website
- Website Mirroring Tools
- Extract Website Information from <http://www.archive.org>
- Monitoring Web Updates Using Website Watcher

Email Footprinting

- Tracking Email Communications

- Collecting Information from Email Header
- Email Tracking Tools

Footprinting using Google

- 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 Tools

WHOIS Footprinting

- WHOIS Lookup
- WHOIS Lookup Result Analysis
- WHOIS Lookup Tools
- WHOIS Lookup Online Tools

DNS Footprinting

- Extracting DNS Information
- DNS Interrogation Tools
- Using Nslookup
- Dig for Unix / Linux

Network Footprinting

- Locate the Network Range
- Determine the Operating System
- Traceroute
- Traceroute Analysis

- Traceroute Tools

Footprinting using Social Engineering

- Footprinting through Social Engineering
- Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
- Collect Information through Social Engineering on Social Networking Sites

Footprinting using Social Networking Sites

- Collecting Facebook Information
- Collecting Twitter Information
- Collecting LinkedIn Information
- Collecting Youtube Information
- Tracking Users on Social Networking Sites

Footprinting Tools

- Maltego
- Domain Name Analyzer Pro
- Web Data Extractor
- Additional Footprinting Tools

Ethical Hacking & Penetration Testing

MODULE 04: SCANNING NETWORKS

Scanning Networks Concepts and Methodology

- Network Scanning
- Scanning Methodology

Check for Live Systems

- ICMP Scanning
- Ping Sweep
- Ping Sweep Tools

Banner Grabbing

- Banner Grabbing Tools
- Banner Grabbing Countermeasures: Disabling or Changing Banner
- Hiding File Extensions from Web Pages

Check for Open Ports

- Three-Way Handshake
- TCP Communication Flags
- Create Custom Packet Using TCP Flags

- Scanning IPv6 Network
- Scanning Tool
- Hping2 / Hping3
- Hping Commands
- Scanning Techniques
- Nmap
- TCP Connect / Full Open Scan
- Stealth Scan (Half-open Scan)
- Xmas Scan
- FIN Scan
- NULL Scan
- IDLE Scan
- ICMP Echo Scanning/List Scan
- UDP Scanning
- Inverse TCP Flag Scanning
- ACK Flag Scanning

Scanning Beyond IDS

- IDS Evasion Techniques
- SYN/FIN Scanning Using IP Fragments

Scan for Vulnerability

- Security Alerts
- Vulnerability Scanning
- Vulnerability Scanning Tool
- IBM Appscan
- GFI Languard
- Network Vulnerability Scanners
- Analyzing the Scan Results
- Generating Reports
- Remediation
- Patch Management

MODULE 05: PROXIES, VPNS AND TOR

- Proxy Servers
- Why Attackers Use Proxy Servers?
- Use of Proxies for Attack
- Proxy Chaining
- Proxy Tools

- Free Proxy Servers
- HTTP Tunneling Techniques
- Why do I Need HTTP Tunneling
- HTTP Tunneling Tool
- SSH Tunneling

- SSH Tunneling Tools
- Spoofing IP Address
- IP Spoofing Detection Techniques
- Tor: anonymous internet access
- How tor works

Ethical Hacking & Penetration Testing

MODULE 06: ENUMERATION

Enumeration Concepts

- What is Enumeration?
- Techniques for Enumeration
- Services and Ports to Enumerate

NetBIOS Enumeration

- NetBIOS Enumeration Tools
- Enumerating User Accounts
- Enumerate Systems Using Default Passwords

FTP Enumeration

- Banner Grabbing
- TFTP Enumeration
- Metasploit Modules

SSH Enumeration

- Version Scanning
- Banner Grabbing
- Scripts to enumerate
- Bruteforce

MSSql Enumeration

- Information Gathering
- SQL Users Enumeration
- Bruteforcing mssql
- Interactive database shell

VNC Enumeration

- Cracking Password
- Connecting to VNC

SNMP Enumeration

- SNMP (Simple Network Management Protocol) Enumeration
- Working of SNMP
- Management Information Base (MIB)
- SNMP Enumeration Tools

UNIX/Linux Enumeration

- UNIX/Linux Enumeration Commands
- Linux Enumeration Tools

LDAP Enumeration

- LDAP Enumeration Tools

Telnet Enumeration

- Scripts Scanning
- Banner Grabbing
- Brute forcing

Web Enumeration

- HTTP Method Enumeration
- HTTP Basic Authentication
- Checking Running Service Version

MySQL Enumeration

- Basic Commands

- MySQL BruteForcing

NTP Enumeration

- NTP Enumeration Commands

SMTP Enumeration

- SMTP Enumeration Tools

DNS Enumeration

- DNS Zone Transfer Enumeration Using NSLookup
- DNS Enumeration Tools

SMB Enumeration

- SMB Enumeration Tools
- Null sessions
- Syntax for a null session
- Viewing shares

NFS Enumeration

- Script Scan
- Enumerate NFS share
- Escalate the Privileges by NFS

Remote Desktop Enumeration

- Login with known credentials
- Nmap Scripts
- Brute-force
- Adding User to RDP group

Ethical Hacking & Penetration Testing

MODULE 07: SYSTEM HACKING

Windows Hacking & Security

- Introducing Operating System
- Introduction of Windows Hacking
- Bootloader
- File system
- Windows command & Powershell
- Special or shell folder in windows
- Windows Registry
- Group Policies
- Batch Programming & Windows Scripting

Cracking Passwords

- Password Cracking
- Password Complexity
- Password Cracking Techniques
- Types of Password Attacks
- Passive Online Attack
- Active Online Attack
- Distributed Network Attack
- Elcomsoft Distributed Password Recovery
- Non-Electronic Attacks
- Default Passwords
- Manual Password Cracking (Guessing)
- Stealing Passwords Using USB Drive
- Stealing Passwords Using Keyloggers
- Microsoft Authentication
- How Hash Passwords Are Stored in Windows SAM?

- What Is LAN Manager Hash?
- LM "Hash" Generation
- LM, NTLMv1, and NTLMv2
- NTLM Authentication Process
- Kerberos Authentication
- Salting
- PWdump7 and Fgdump
- L0phtCrack
- Ophcrack
- Cain & Abel
- Winrtgen and rtgen
- RainbowCrack
- Password Cracking Tools
- LM Hash Backward Compatibility
- How to Disable LM HASH
- How to Defend against Password Cracking
- Implement and Enforce Strong Security Policy

Executing Applications

- Executing Applications: RemoteExec
- Executing Applications: PDQ Deploy
- Executing Applications: DameWare NT Utilities

Spyware

- What Does the Spyware Do?
- Types of Spywares
- Desktop Spyware
- Email and Internet Spyware

- Child Monitoring Spyware
- Screen Capturing Spyware
- USB Spyware
- Audio Spyware
- Video Spyware
- Print Spyware
- Telephone/Cellphone Spyware
- GPS Spyware
- How to Defend Against Spyware
- Anti-Spywares

Keylogger

- Types of Keystroke Loggers
- Methodology of Attacker in Using Remote Keylogger
- How to Defend Against Keyloggers
- Anti-Keylogger

Hiding Files

- Rootkits
- Types of Rootkits
- How Rootkit Works
- Detecting Rootkits
- Steps for Detecting Rootkits
- How to Defend against Rootkits
- Anti-Rootkit

Ethical Hacking & Penetration Testing

MODULE 07: SYSTEM HACKING

NTFS Data Stream

- How to Create NTFS Streams
- NTFS Stream Manipulation
- How to Defend against NTFS Streams
- NTFS Stream Detectors

What is Steganography?

- Application of Steganography
- Classification of Steganography
- Technical Steganography
- Linguistic Steganography
- Steganography Techniques
- How Steganography Works
- Types of Steganography

- Whitespace Steganography Tool
- Image Steganography
- Least Significant Bit Insertion
- Masking and Filtering
- Algorithms and Transformation
- Image Steganography Tools
- Document Steganography Tools
- Video Steganography Tools
- Audio Steganography Tools
- Folder Steganography Tools
- Spam/Email Steganography
- Natural Text Steganography
- Issues in Information Hiding

- Steganalysis
- Steganalysis Methods/Attacks on Steganography
- Detecting Text and Image Steganography
- Detecting Audio and Video Steganography
- Steganography Detection Tools

Covering Tracks

- Why Cover Tracks?
- Covering Tracks
- Ways to Clear Online Tracks
- Disabling Auditing
- Covering Tracks Tool
- Track Covering Tools

MODULE 08: PRIVILEGE ESCALATION

Escalating Privileges

- Privilege Escalation
- Privilege Escalation Tools
- How to Defend Against Privilege Escalation
- How to Do Privilege Escalation in Linux and Windows
- Tools that can help identify potential privilege escalation vulnerabilities on a system.
- How to create users

Linux Privilege Escalation

- Manual Enumeration
- User Details
- Operating System & Kernel Details
- Network Details
- Applications & Services Details
- User home directory enumeration
- Automated Enumeration
- Kernel Exploits
- Service Exploits

- Password Mining
- Linux File Permissions
- PATH Variable (Path abusing)
- Sudo (Shell Escape Sequences and Abusing Intended Functionality)
- Capabilities
- Cron Jobs & Systemd Timers
- NFS Root Squashing

Ethical Hacking & Penetration Testing

MODULE 08: PRIVILEGE ESCALATION

Windows Privilege Escalation

- Manual Enumeration
- User Details
- Operating System & Kernel Details
- Network Details
- Applications & Services Details
- User home directory enumeration
- Automated Enumeration
- Kernel Exploits
- Service Exploits
- Registry Exploits
- Password Mining
- Scheduled Tasks
- mimikatz
- Impersonation and Potato Attacks
- Startup Apps

MODULE 09: MALWARE THREATS

Trojan Concepts

- What is a Trojan?
- Purpose of Trojans
- What Do Trojan Creators Look For
- Indications of a Trojan Attack
- Common Ports used by Trojans

Types of Trojans

- Command Shell Trojans
- GUI Trojans
- Document Trojans
- E-mail Trojans
- Defacement Trojans
- Botnet Trojans
- Proxy Server Trojans
- FTP Trojans
- VNC Trojans

- HTTP/HTTPS Trojans
- ICMP Tunneling
- Remote Access Trojans
- Covert Channel Trojan
- E-banking Trojans
- Banking Trojan Analysis
- Destructive Trojans
- Notification Trojans
- Credit Card Trojans
- Data Hiding Trojans (Encrypted Trojans)
- Trojan Analysis: Flame
- Flame C&C Server Analysis
- Trojan Analysis

Trojan Detection

- How to Detect Trojans
- Scanning for Suspicious Ports

- Port Monitoring Tools
- Process Monitoring Tools
- Scanning for Suspicious Registry Entries
- Registry Entry Monitoring Tools
- Scanning for Suspicious Device Drivers
- Device Drivers Monitoring Tools
- Scanning for Suspicious Windows Services
- Windows Services Monitoring Tools
- Scanning for Suspicious Startup Programs
- Windows Startup Registry Entries
- Startup Programs Monitoring Tools
- Scanning for Suspicious Files and Folders
- Files and Folder Integrity Checker
- Scanning for Suspicious Network Activities
- Detecting Trojans and Worms with Capsa Network Analyzer

Ethical Hacking & Penetration Testing

MODULE 09: MALWARE THREATS

Trojan Infection

- How to Infect Systems Using a Trojan
- Wrappers
- Wrapper Covert Programs
- Different Ways a Trojan can Get into a System
- How to Deploy a Trojan
- Evading Anti-Virus Techniques

Anti-Trojan Software

- Anti-Trojan Software's

Virus and Worms Concepts

- Introduction to Viruses
- Virus and Worm Statistics
- Stages of Virus Life
- Working of Viruses: Infection Phase
- Working of Viruses: Attack Phase
- Why Do People Create Computer Viruses
- Indications of Virus Attack
- How does a Computer Get Infected by Viruses
- Common Techniques Used to Distribute Malware on the

Web

- Virus Hoaxes and Fake Antiviruses
- Virus Analysis

Types of Viruses

- System or Boot Sector Viruses
- File and Multipartite Viruses
- Macro Viruses
- Cluster Viruses
- Stealth/Tunneling Viruses
- Encryption Viruses
- Polymorphic Code
- Metamorphic Viruses
- File Overwriting or Cavity Viruses
- Sparse Infector Viruses
- Companion/Camouflage Viruses
- Shell Viruses
- File Extension Viruses
- Add-on and Intrusive Viruses
- Writing a Simple Virus Program

- Terabit Virus Maker
- JPS Virus Maker and DELmE's Batch Virus Maker

Worms

- How is a Worm Different from a Virus?
- Worm Analysis: Stuxnet
- Worm Maker: Internet Worm Maker Thing

Malware Analysis

- What is Sheep Dip Computer?
- Anti-Virus Sensors Systems
- Malware Analysis Procedure: Preparing Testbed
- Malware Analysis Procedure
- Virus Analysis Tool: IDA Pro
- Online Malware Testing: VirusTotal
- Online Malware Analysis Services

Detection Methods

- Virus and Worms
- Companion Antivirus
- Anti-virus Tools

Ethical Hacking & Penetration Testing

MODULE 10: SNIFFERS

Sniffing Concepts

- Wiretapping
- Packet Sniffing
- Sniffing Threats
- How a Sniffer Works
- Types of Sniffing Attacks
- Passive Sniffing
- Active Sniffing
- Protocols Vulnerable to Sniffing
- SPAN Port

MAC Attacks

- MAC Flooding
- MAC Address/CAM Table
- How CAM Works
- What Happens When CAM Table is Full?
- Mac Flooding Switches with macof
- MAC Flooding Tools
- How to Defend against MAC Attacks

DHCP Attacks

- How DHCP Works
- DHCP Request/Reply Messages
- IPv4 DHCP Packet Format
- DHCP Starvation Attack

- Rogue DHCP Server Attack
- How to Defend Against DHCP Starvation and Rogue Server Attack

ARP Poisoning

- What is Address Resolution Protocol (ARP)?
- ARP Spoofing Techniques
- ARP Spoofing Attack
- How Does ARP Spoofing Work
- Threats of ARP Poisoning
- ARP Poisoning Tools
- How to Defend Against ARP Poisoning
- ARP Spoofing Detection: XArp

Spoofing Attack

- Spoofing Attack Threats
- MAC Spoofing/Duplicating
- MAC Spoofing Technique: Windows
- MAC Spoofing Tool: SMAC
- IRDP Spoofing
- How to Defend Against MAC Spoofing

DNS Poisoning

- DNS Poisoning Techniques
- Intranet DNS Spoofing
- Proxy Server DNS Poisoning

- DNS Cache Poisoning
- How to Defend Against DNS Spoofing

Sniffing Tools

- Sniffing Tool: Wireshark
- Follow TCP Stream in Wireshark
- Display Filters in Wireshark
- Additional Wireshark Filters
- Sniffing Tool: Tcpcdump/Windump
- Packet Sniffing Tool: Capsa Network Analyzer
- Network Packet Analyzer: OmniPeek Network Analyzer
- Network Packet Analyzer: Observer
- Network Packet Analyzer: Sniff-O-Matic
- Network Packet Analyzer: JitBit Network Sniffer
- Chat Message Sniffer: MSN Sniffer 2
- TCP/IP Packet Crafter: Colasoft Packet Builder
- How an Attacker Hacks the Network Using Sniffers

Sniffer Detection Technique

- How to Defend Against Sniffing
- How to Detect Sniffing
- Sniffer Detection Technique: Ping Method
- Sniffer Detection Technique: ARP Method
- Sniffer Detection Technique: DNS Method
- Promiscuous Detection Tool: PromqryUI

Ethical Hacking & Penetration Testing

MODULE 11: SOCIAL ENGINEERING

Social Engineering Concepts

- What is Social Engineering?
- Behaviors Vulnerable to Attacks
- Factors that Make Companies Vulnerable to Attacks
- Why Is Social Engineering Effective?
- Warning Signs of an Attack
- Phases in a Social Engineering Attack
- Impact on the Organization
- "Rebecca" and "Jessica"
- Common Targets of Social Engineering

Social Engineering Techniques

- Introduction of Social Engineering

- Types of Social Engineering
- Human-based Social Engineering
- Technical Support
- Authority Support
- Human base
- Human base: Eavesdropping and Shoulder Surfing
- Human base: Dumpster Diving
- Computer based Attacks
- Computer based Attacks: Pop-Ups
- Computer based Attacks: Phishing
- Computer based Attacks: Spear Phishing
- Computer based Attacks: Using Social Media

Mobile based

- Mobile based: Publishing Malicious Apps
- Mobile based: Repackaging Legitimate Apps
- Mobile based: Fake Security Applications
- Mobile based: Using SMS
- Insider Attack
- Disgruntled Employee
- Preventing Insider Threats
- How to Detect Phishing Emails
- Anti-Phishing Toolbar: Netcraft
- Anti-Phishing Toolbar: PhishTank
- Identity Theft

MODULE 12: DENIAL OF SERVICE

DoS/DDoS Concepts

- What is a Denial of Service Attack?
- What are Distributed Denial of Service Attacks?
- How Distributed Denial of Service Attacks Work
- Symptoms of a DoS Attack
- Cyber Criminals
- Organized Cyber Crime: Organizational Chart

DoS Attack Techniques

- Bandwidth Attacks
- Service Request Floods
- SYN Attack

- SYN Flooding
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Permanent Denial-of-Service Attack
- Application Level Flood Attacks

Botnet

- Botnet Propagation Technique
- Botnet Ecosystem
- Botnet Trojan: Shark
- Poison Ivy: Botnet Command Control Center
- Botnet Trojan: PlugBot

- Botnet Trojans: Illusion Bot and NetBot Attacker

Denial of Service Attack Detection Techniques

- Activity Profiling
- Wavelet Analysis
- Sequential Change-Point Detection
- Post-Attack Forensics
- Techniques to Defend against Botnets
- DoS/DDoS Protection at ISP Level
- Enabling TCP Intercept on Cisco IOS Software
- Advanced DDoS Protection Appliances

Ethical Hacking & Penetration Testing

MODULE 13: SESSION HIJACKING

Session Hijacking Concepts

- What is Session Hijacking?
- Why Session Hijacking is Successful?
- Key Session Hijacking Techniques
- Brute Forcing Attack
- Spoofing vs. Hijacking
- Session Hijacking Process
- Types of Session Hijacking
- Attack Vectors
- The Impact of Session Hijacking
- Session Hijacking and the OWASP Top 10

Session Hijacking in Web Applications

- The Stateless Nature of HTTP
- Persisting State Over HTTP
- Session Persistence in Cookies
- Session Persistence in the URL
- Session Persistence in Hidden Form Fields
- Hijacking Sessions in Web Applications

- Hijacking Cookies with Cross Site Scripting
- Exposed Cookie Based Session IDs in Logs
- Exposed URL Based Session IDs in Logs
- Leaking URL Persisted Sessions in the Referrer
- Session Sniffing
- Session Fixation
- Brute Forcing Session IDs
- Session Donation

Session Hijacking in Network and Client Level

- Understanding TCP
- Reviewing the Three-way Handshake in Wireshark
- Generation and Predictability of TCP Sequence Numbers
- Blind Hijacking
- Man in the Middle Session Sniffing
- IP Spoofing
- UDP Hijacking
- Man in the Browser Attacks
- Network Level Session Hijacking in the Wild

Mitigating the Risk of Session Hijacking

- Use Strong Session IDs
- Keep Session IDs Out of the URL
- Don't Reuse Session ID for Auth
- Always Flag Session ID Cookies as HTTP Only
- Use Transport Layer Security
- Always Flag Session ID Cookies as Secure
- Session Expiration and Using Session Cookies
- Consider Disabling Sliding Sessions
- Encourage Users to Log Out
- Re-authenticate Before Key Actions

Automating Session Hijack Attacks

- Manipulating Session IDs with OWASP ZAP
- Testing Session Token Strength with Burp Suite
- Dynamic Analysis Testing with NetSparker
- Other Tools

Ethical Hacking & Penetration Testing

MODULE 14: HACKING WEB SERVERS

Introduction & fundamentals of Metasploit

- Terminologies and Requirement of Metasploit
- Metasploit Architecture
- Mixins and Plugins
- Msfconsole
- Exploits in Metasploit
- Important commands for Exploits usage
- Payload Basics
- Generating Different Payloads
- Database in Metasploit
- Meterpreter in Metasploit
- Meterpreter usage in Metasploit

Information Gathering & Vulnerability scanning via Metasploit

- Port scanning with Metasploit
- Target mssql
- Service information via Metasploit

- SNMP sniffing
- Psnuffel script in Metasploit
- Custom scanner by user
- SMB Login Check Scanner
- Open VNC server scanning
- WMAP web scanner in Metasploit
- NeXpose scanner via Metasploit
- Nessus usage and Metasploit

Exploit-payload Creation

- Design Goals for an Exploit
- mixins in exploit writing
- Msfvenom
- AN Shellcode

Client side Attacks

- Binary Payloads
- Trojans for linux via Metasploit
- Malicious PDF file via Metasploit

- After exploitation stuff
- Privilege Escalation
- Pass the hash attack
- Session stealing attacks
- Registry and backdoors in Metasploit
- Packet sniffing with Metasploit
- Bypassing the forensic investigation
- Monitoring and searching the victim

Scripts, Meterpreter and Ruby extension

- Automation of Meterpreter via rc scripts
- Irb shell programming in Meterpreter
- Backdooring the remote system
- Keylogging the remote system
- Metsvc exploitation
- Persistence exploitation services

Ethical Hacking & Penetration Testing

MODULE 15: ADVANCED EXPLOITATION TECHNIQUES

Web server Concepts

- Web server Market Shares
- Open Source Web server Architecture
- IIS Web server Architecture
- Understanding How Web Servers Are Hacked
- The Impact of Hacking
- Web Servers versus Web Applications
- The Role of Cloud

Discovering Risks & Misconfiguration in Web Servers

- Crawling, Enumeration, and Directory Traversal
- Mirroring Websites
- Reconnaissance and Footprinting
- HTTP Fingerprinting
- Social Engineering
- Internal Leakage
- Debug Settings
- Excessive Access Rights
- Misconfigured SSL
- Weaknesses in Default Configurations
- Other Attacks against Web Servers

Website Defacement

- HTTP Response Splitting
- Web Cache Poisoning
- Brute Forcing Authentication Schemes
- Streamline Testing with Automation
- Hacking Web Applications

Web server Security Tools

- Syhunt Dynamic
- N-Stalker Web Application Security Scanner
- Wikto
- Acunetix Web Vulnerability Scanner
- HackAlert
- QualysGuard Malware Detection
- Managing and Hardening Web Servers

What is Patch Management?

- Identifying Appropriate Sources for Updates and Patches
- Installation of a Patch
- Implementation and Verification of a Security Patch or Upgrade
- Patch Management Tools
- Designing for Network Segmentation
- Sandboxing

Web server Concepts

- Web server Market Shares
- Open Source Web server Architecture
- IIS Web server Architecture
- Understanding How Web Servers Are Hacked
- The Impact of Hacking
- Web Servers versus Web Applications
- The Role of Cloud

Discovering Risks & Misconfiguration in Web Servers

- Crawling, Enumeration, and Directory Traversal
- HTTP Fingerprinting
- Social Engineering

- Internal Leakage
- Debug Settings
- Excessive Access Rights
- Misconfigured SSL
- Weaknesses in Default Configurations
- Other Attacks against Web Servers

Website Defacement

- HTTP Response Splitting
- Web Cache Poisoning
- Brute Forcing Authentication Schemes
- Streamline Testing with Automation
- Hacking Web Applications

Injection

- HTML Injection
- OS Command Injection
- OS Command Injection – Blind
- PHP Code Injection
- Server-Side Includes (SSI) Injection
- SQL Injection – Double Query
- Based
- XML/XPath Injection

Ethical Hacking & Penetration Testing

MODULE 15: ADVANCED EXPLOITATION TECHNIQUES

Web server Security Tools

- Syhunt Dynamic
- N-Stalker Web Application Security Scanner
- Wikto
- Acunetix Web Vulnerability Scanner
- HackAlert

- QualysGuard Malware Detection
- Managing and Hardening Web Servers

What is Patch Management?

- Identifying Appropriate Sources for Updates and Patches
- Installation of a Patch
- Implementation and Verification of a Security Patch or

Upgrade

- Patch Management Tools
- Support and End of Life
- Locking Down Services
- Designing for Network Segmentation
- Sandboxing

MODULE 16: HACKING WEB APPLICATIONS

Web App Concepts

- Introduction to Web Applications
- Web Application Components
- How Web Applications Work?
- Web Application Architecture
- Web 2.0 Applications
- Vulnerability Stack
- Web Attack Vectors

Understanding Security in Web Applications

- The State of Web Application Security
- Understanding Web Application Security
- Query Strings, Routing, and HTTP Verbs
- The Discoverability of Client Security Constructs
- Protections Offered by Browsers
- What the Browser Can't Defend Against

Reconnaissance and Footprinting

- Spidering with NetSparker
- Forced Browsing with Burp Suite

- Banner Grabbing with Wget
- Server Fingerprinting with Nmap
- Discovery of Development Artefacts with Acunetix
- Discovery of Services via Generated Documentation
- Discovering Framework Risks
- Identifying Vulnerable Targets with Shodan

Tampering of Untrusted Data

- Understanding Untrusted Data
- Parameter Tampering
- Hidden Field Tampering
- Mass Assignment Attacks
- Cookie Poisoning
- Insecure Direct Object References
- Defending Against Tampering
- Brute-force and dictionary attacks
- Account lockout attack
- Path and information disclosure
- Forced browsing

- Path traversal
- Unicode encoding
- Parameter delimiter

Broken Authentication & Session Management

- Broken Authentication – CAPTCHA Bypassing
- Broken Authentication – Forgotten Function
- Broken Authentication – Insecure Login Forms
- Broken Authentication – Logout Management
- Broken Authentication – Password Attacks
- Broken Authentication – Weak Passwords
- Session Management – Cookies (HTTPOnly)
- Session Management – Cookies (Secure)
- Session Management – Session ID in URL
- Session Management – Strong Sessions

Ethical Hacking & Penetration Testing

MODULE 16: HACKING WEB APPLICATIONS

Cross-Site Scripting (XSS)

- Cross-Site Scripting (XSS) – Reflected
- Cross-Site Scripting (XSS) – Stored
- Cross-Site Scripting (XSS) – DOM

Security Misconfiguration

- Cross-Domain Policy File (Flash)
- Cross-Origin Resource Sharing (AJAX)
- Cross-Site Tracing (XST)
- Denial-of-Service (XML Bomb)
- Insecure WebDAV Configuration

Sensitive Data Exposure

- Base64 Encode Sensitive Data

- HTML5 Web Storage

- Host Header Attack

Missing Functional Level Access Control

- Directory Traversal – Directories
- Directory Traversal – Files
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Server Side Request Forgery (SSRF)
- XML External Entity Attacks (XXE)

Advanced Web Exploitation Techniques

- Insecure Direct Object References (IDOR)
- Insecure Deserialization
- Session Hijacking
- Session Fixation

- Automated Security Testing

- Improper Error Handling

- Understanding Salted Hashes

- Insecure Cryptographic Storage

- Unvalidated Redirects and Forwards

- Exposed Exceptions Logs with ELMAH

- Vulnerabilities in Web Services

Other Web Exploitation Techniques

- ClickJacking

- HTTP Verb Tampering

- HTTP Response Splitting

- Unrestricted File Upload

- Cross-Site Request Forgery (CSRF/XSRF)

Ethical Hacking & Penetration Testing

MODULE 17: SQL INJECTION

Why SQL Injection Matters

- The Significance of SQL Injection
- Executing a SQL Injection Attack
- The Impact of a Successful Attack
- SQL Injection in the Wild

Understanding SQL Queries

- Understanding Structured Query Language
- Statement Termination
- Using the SQL Comment Syntax
- SQL Queries versus Data
- The Value of Internal Exceptions

The Mechanics of SQL Injection Attacks

- Types of SQL Injection
- The Single Character Injection Test
- Modifying the Query Structure
- Circumventing Website Logins
- Modifying Data and Database Objects
- Identifying the Risk in Code
- Understanding and Detecting Input Sanitization

Discovering Schema and Extracting Data

- Understanding the Union Operator
- Executing Union Injection
- Manual Database Structure Discovery with Error-based Injection

- Querying System Objects for Schema Discovery
- Extracting Schema Details with Union Injection
- Enumerating Result Sets with Sub-queries
- Extracting Schema Details with Error-based Injection

Blind SQL Injection

- Basic and Blind Attack Success Criteria
- Understanding a Blind Attack
- Applying Boolean Based Injection
- Constructing Yes and No Questions for Boolean Based Injection
- Enumerating via ASCII Values
- Where Time Based Injection Makes Sense
- Understanding the WAITFOR DELAY Command
- Constructing a Time Based Attack

Advanced SQL Injection Concepts

- Database Server Feature Comparison
- Establishing Account Identity and Rights
- Enumerating Other Databases on the System
- Creating Database Logins
- Extracting Passwords from SQL Server Hashes
- Replicating a Table Using OPENROWSET
- Executing Commands on the Operating System
- SQL Injection for Network Reconnaissance

Defending Against Attacks

- Implement Proper Error Handling
- Validating Untrusted Data
- Query Parameterization
- Stored Procedures
- Object Relational Mappers
- The Principle of Least Privilege
- Isolating the Database Network Segment
- Using an IDS or WAF
- Keeping Software Patched and Current

Evasion Techniques

- Understanding Signatures
- Basic Evasion Techniques
- Encoding for Evasion
- Splitting Strings
- White Space Diversity
- Inline Comments
- Variables
- String Manipulation

Automating Attacks

- Testing in the Browser with SQL Inject Me
- Fuzz Testing with Burp Suite
- Data Extraction with Havij
- Schema Mapping with sqlmap
- Dynamic Analysis Testing with NetSparker

Ethical Hacking & Penetration Testing

MODULE 18: HACKING WIRELESS NETWORKS

Introduction to wireless networks

- Wireless transmission standards
- 11 wireless network types
- Encryption and authentication standards
- Wireless network cards in Linux – overview
- Wireless network interface cards in Linux

Wireless security (half) measures

- MAC address filtering
- Changing the MAC address of the wireless network card
- Disabling ESSID broadcast
- Finding a hidden access point with disabled ESSID broadcast
- Limiting wireless coverage

Wireless network attacks independent of used encryption

- Introduction
- DoS: RF jamming

- DoS: CSMA/CA jamming
- The use of deauthentication attack for jamming network traffic
- DoS: Deauthentication attack
- Wireless MITM

WEP attacks

- WEP encryption
- Chopchop
- The overview and demonstration of the chop-chop attack
- Keystream reuse
- Generating packets without knowing the network key
- Interactive packet replay and ARP request replay
- The demonstration of the PTW and KoreK attacks
- Caffe Latte Attack
- Creating a fake access point – the Caffe Latte attack

- Introduction to wireless networks

WPA attacks

- WPA
- The dictionary attack on WPA
- WPA2
- Rainbow tables
- The dictionary attack on WPA – using hash tables
- Cowpatty attack
- DoS: Taking advantage of the MIC failure holdoff time

Advanced attacks against WPA

- WPA TKIP attack
- WPA TKIP broken
- Beck-Tews attack enhanced
- Michael Reset attack

MODULE 19: HACKING MOBILE PLATFORMS

Mobile Platform Attack Vectors

- Rise of Mobility
- Areas to Consider
- Device Security
- Android Security Features
- Look out

- Application Security
- GEO Tagging
- Mobile Applications
- SOPHOS
- Trend Micro Security
- Byod Concerns

- IScan
- Options
- App Permissions
- The Virtualization Option

Ethical Hacking & Penetration Testing

MODULE 19: HACKING MOBILE PLATFORMS

Hacking Android OS

- Android OS Architecture
- Android Device Administration API
- Android Vulnerabilities
- Android Rooting
- Rooting Android Phones using SuperOneClick
- Rooting Android Phones Using Superboot
- Android Rooting Tools
- Session Hijacking Using DroidSheep
- Android-based Sniffer: FaceNiff
- Android Trojans
- Securing Android Devices
- Google Apps Device Policy
- Remote Wipe Service: Remote Wipe
- Android Security Tool: DroidSheep Guard
- Android Vulnerability Scanner: X-Ray
- Android Device Tracking Tools

MODULE 20: EVADING IDS, FIREWALLS, AND HONEYPOTS

- Introduction of Working with Firewalls
- Understanding Firewalls
- Firewall Architectures
- Types of Firewalls
- Evading Firewalls
- Evading Firewalls using Tunneling
- Evading Firewalls using External Systems
- Evading Firewalls using MITM Attacks
- Firewalls Evation Tools
- Honeypots Defined
- Types of Honeypots
- Detecting Honeypots
- Honeypot using Atomic Software
- Introduction to IDS
- Intrusion Detection Systems
- Introduction to Evading IDS
- Encryption & Flooding
- Obfuscating
- Fragmentation Attacks
- Overlapping Fragments
- Points of Vulnerabilities in IDS
- How to avoid IDS Demo
- Insertion Attacks
- Evasion Attacks
- Denial of Service Attacks
- Application Layer- Attacks
- Time to Live Attacks
- False Positive Generation
- Urgency Flag
- Session Splicing
- Pre Connection SYN
- Post Connection SYN
- Snort
- More tools
- Ways to Detect
- ADMmutate
- Other Evading Tools
- Centralized Security Management
- IDS Penetration Testing

Ethical Hacking & Penetration Testing

MODULE 21: BUFFER OVERFLOW

- Buffer Overflow
- Stacks
- Stack overflow
- Heaps
- Heap Overflow
- Format Strings
- Format Strings Buffer Overflow
- Integer Overflow
- Vulnerabilities to Buffer Overflow
- Buffer Overflow
- Handling Buffer Overflow
- Identifying Buffer Overflow
- Defense Against Buffer Overflows
- Programming Countermeasures
- Buffer Overflow Security Tools

MODULE 22: CRYPTOGRAPHY

- Cryptography
- Types of Cryptography
- Government Access to Keys (GAK)
- Ciphers
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- RC4, RC5, RC6 Algorithms
- The DSA and Related Signature Schemes
- RSA (Rivest Shamir Adleman)
- Example of RSA Algorithm
- The RSA Signature Scheme
- Message Digest (One-way Hash) Functions
- Message Digest Function: MD5
- Secure Hashing Algorithm (SHA)
- What is SSH (Secure Shell)?
- MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Certification Authorities
- Digital Signature
- SSL (Secure Sockets Layer)
- Transport Layer Security (TLS)
- Disk Encryption Tools
- Code Breaking Methodologies
- Brute-Force Attack
- Meet-in-the-Middle Attack on Digital Signature Schemes