ARMOURINFOSEC

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.

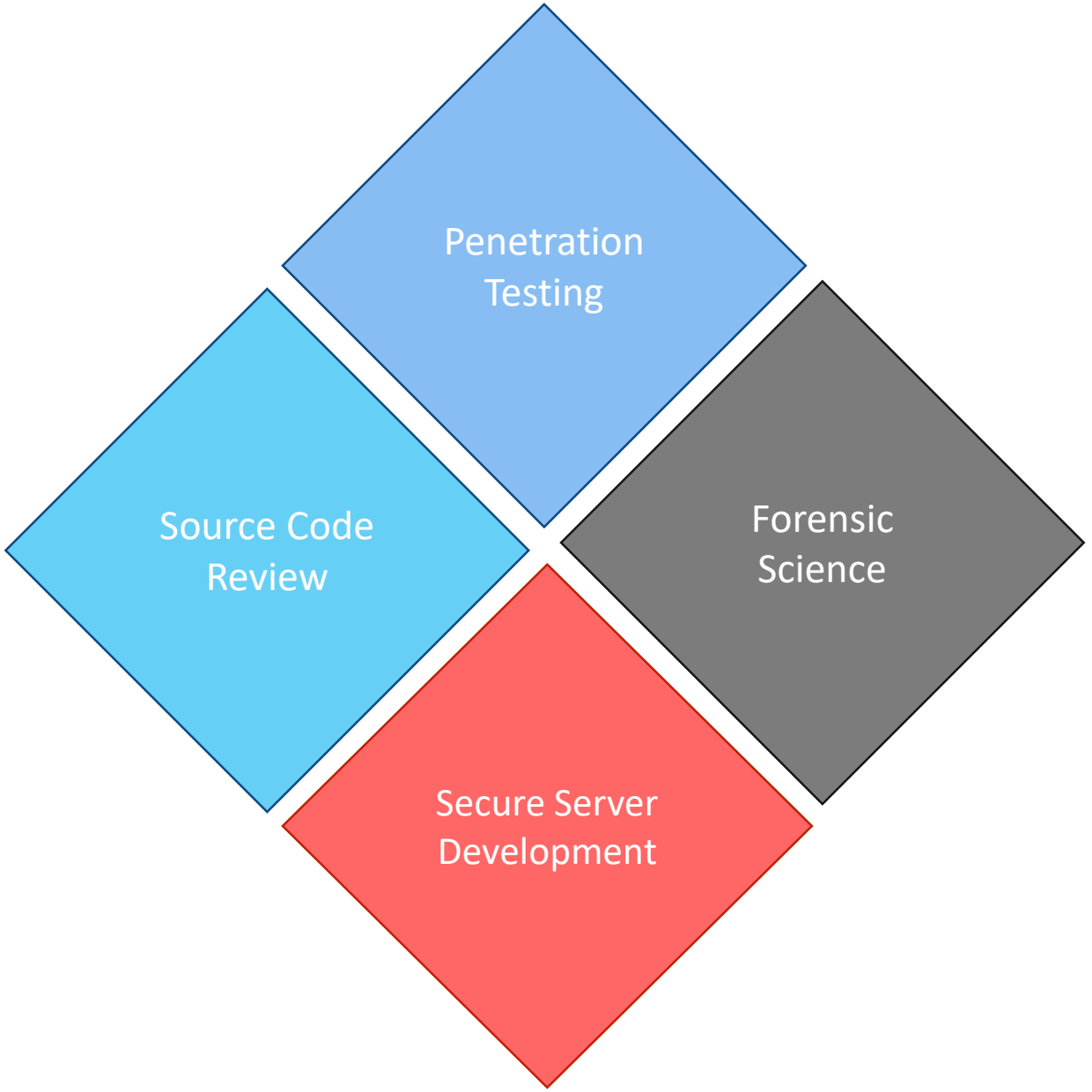
An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.

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.

ARMOURINFOSEC

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.**



ARMOURINFOSEC

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

ARMOURINFOSEC

OUR COURSE

Certified Web Security Expert

Web Security Testing (WST) is the Security testing techniques for vulnerabilities or security holes in corporate websites and web applications. These vulnerabilities leave websites open to exploitation.

Companies now a days are moving their most applications and critical business process on web. Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited Web sites altered by attackers.

It is sad but true that many of the advantages that make online applications so convenient, also make them incredibly insecure. As a result, hackers are able to use web applications to penetrate enterprises' network and access private customer databases. The resulting identity and data theft has become a major concern for corporations and consumers alike

DURATION

2 hours/ day X 75 days

ENROLL NOW

ARMOURINFOSEC

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

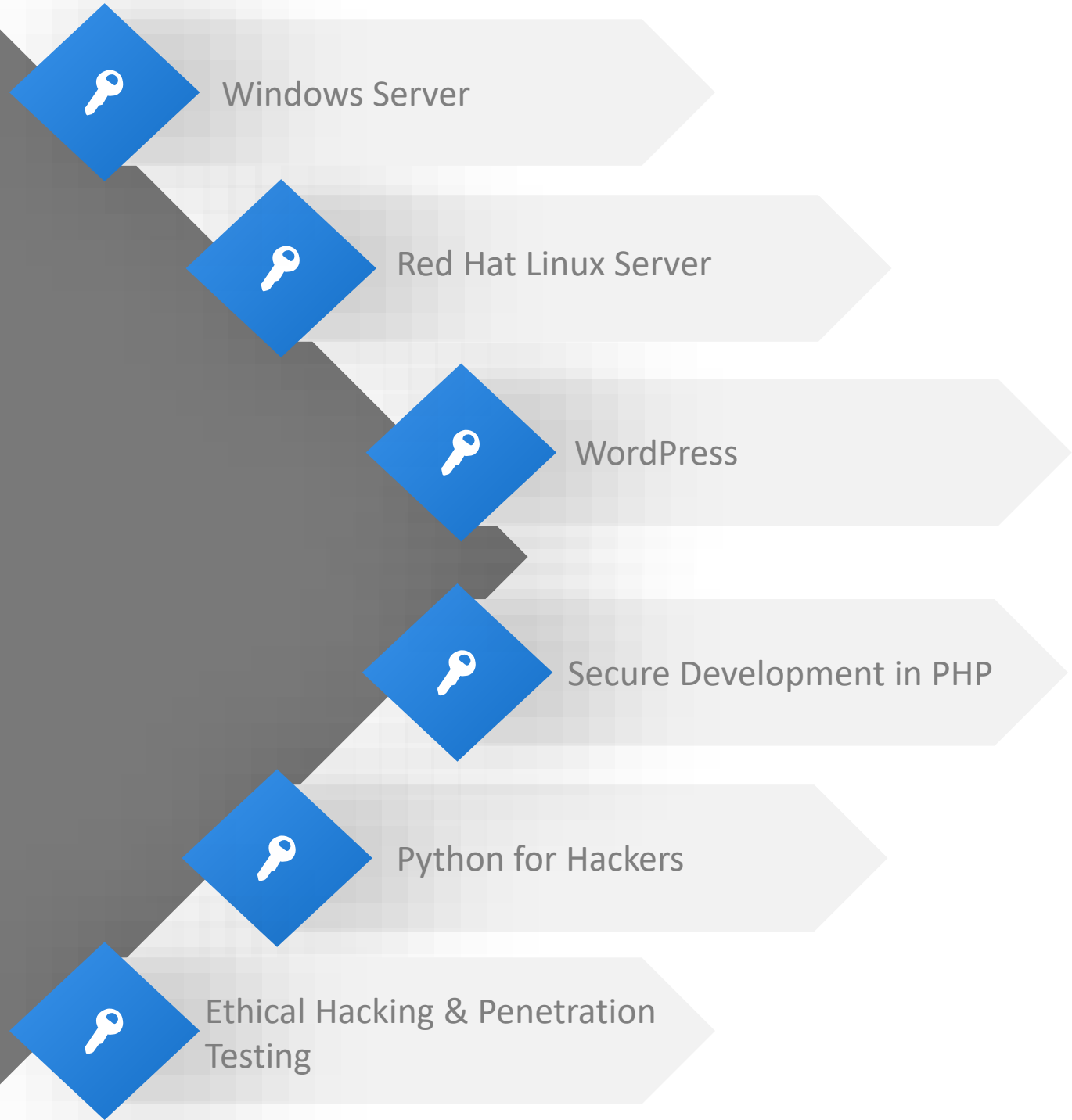
What are the Required Skillsets?

- 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.

Units Covered



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

Web Security

This module will enable learners to gain knowledge and skills in a series of advanced and current concepts in cyber security, and related to enterprise and infrastructure security. After the completion of this module learners will have a comprehensive understanding of the framework, security controls, networking concepts, traffic analysis, packet analyzers, sniffers, firewalls, SIEM, VLAN, VPN, identity and access management, and much more. The Application and Web Application Security course will enable learners to gain knowledge and skills in OWASP tools and methodologies, insecure deserialization, clickjacking, black box, white box, fuzzing, symmetric/asymmetric cryptography, hashing, digital signatures, API security, patch management, and much more.

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

ARMOURINFOSEC

Web Security

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

Web Security

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

Web Security

MODULE 05: 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 06: 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

Web Security

MODULE 07: 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

Web Security

MODULE 08: 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

Web Security

MODULE 09: 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 Metsploit
- 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

Web Security

MODULE 10: 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

Web Security

MODULE 11: 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
- Directory Traversal
- Banner Grabbing with Wget
- Discovering Framework Risks
- Identifying Vulnerable Targets with Shodan
- Tampering of Untrusted Data
- OWASP and the Top 10 Web Application Security Risks
- Hidden Field Tampering
- Mass Assignment Attacks
- Cookie Poisoning
- Insecure Direct Object References
- Defending Against Tampering
- Basic techniques
- Deep data hiding
- Brute-force and dictionary attacks
- Account lockout attack
- Path and information disclosure
- Forced browsing
- Path traversal
- Unicode encoding
- Parameter delimiter
- Incjection attacks
- PHP injection
- Direct static code injection
- Attacks Involving the Client
- Reflected Cross Site Scripting (XSS)
- Persistent Cross Site Scripting (XSS)
- Defending Against XSS Attacks
- Identifying XSS Risks and Evading Filters
- Client Only Validation
- Insufficient Transport Layer Security
- Cross Site Request Forgery (CSRF)
- Cross Site Tracing attack (XST)
- Cross Site Request Forgery attack (XSRF)
- Attacks against Identity Management and Access Controls
- Understanding Weaknesses in Identity Management
- Identity Enumeration
- Weaknesses in the 'Remember Me' Feature
- Resources Missing Access Controls
- Insufficient Access Controls
- Privilege Elevation
- Denial of Service Attacks
- Understanding DoS
- Exploiting Password Resets
- Exploiting Account Lockouts
- Distributed Denial of Service (DDoS)
- Automating DDoS Attacks with LOIC
- DDoS as a Service
- Features at Risk of a DDoS Attack
- Other DDoS Attacks and Mitigations
- More advanced techniques
- Spying on data with a browser
- Session hijacking
- Insecure Cryptographic Storage
- Unvalidated Redirects and Forwards
- Exposed Exceptions Logs with ELMAH
- Vulnerabilities in Web Services