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.

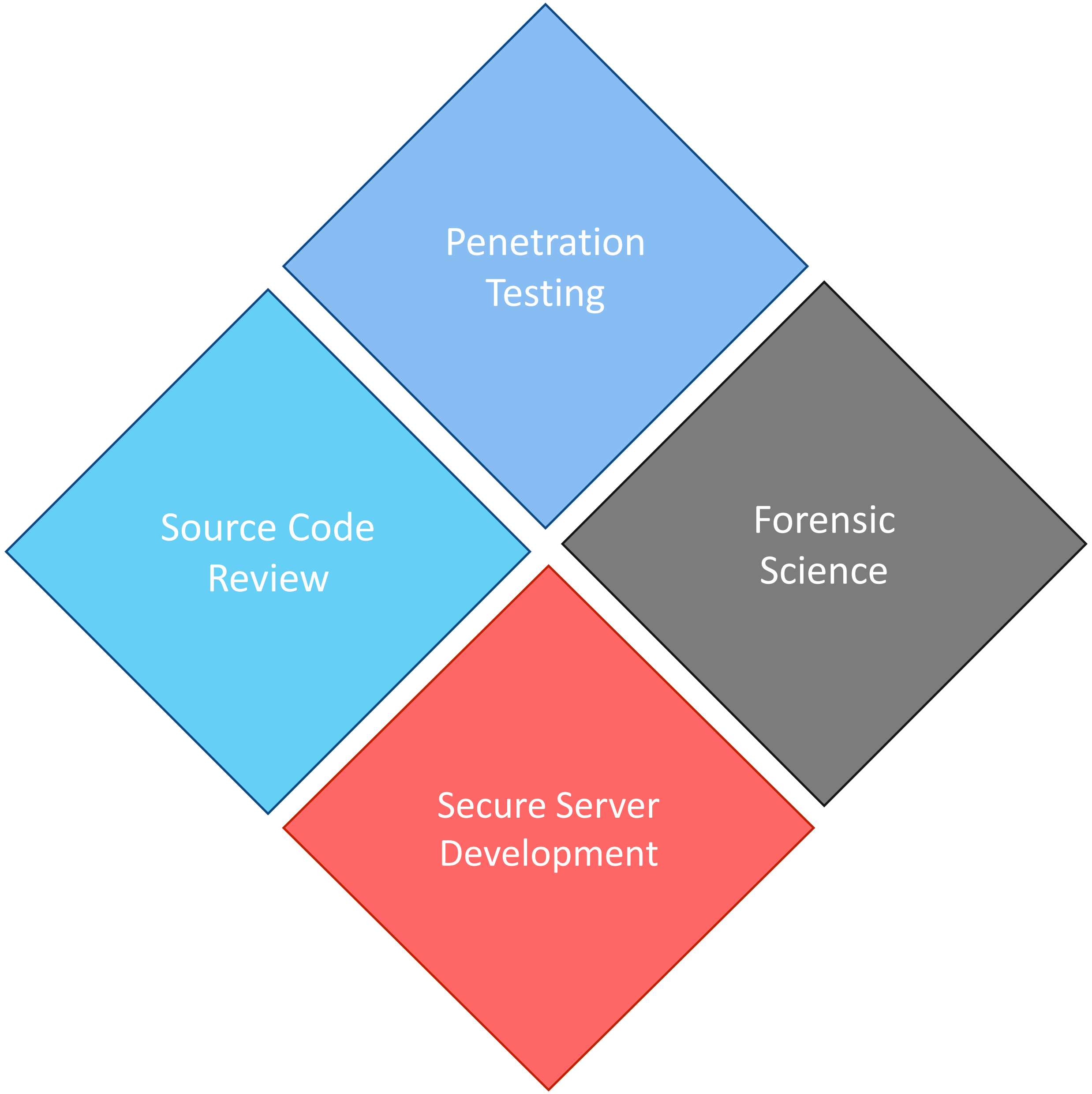
An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization’s consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.

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.**



Penetration Testing

Source Code Review

Forensic Science

Secure Server Development

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

OUR COURSE

Certified Wireless Security Expert

Wireless networks are popping up everywhere. It will be the most commonly used technology among computer networks in the near future. They provide a lot of freedom but not without cost: Too many home and corporate wireless networks are left wide open for attack .This course takes an in-depth look at the security challenges of many different wireless technologies, exposing you to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, you'll navigate your way through the techniques which are used by the attackers to exploit WiFi networks, including attacks against WEP, WPA/WPA2, PEAP, TTLS, and other systems.
Using assessment and analysis techniques, this course will show you how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems

DURATION

2 hours/ day X 30 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

- Windows Server
- Red Hat Linux Server
- WordPress
- Secure Development in PHP
- Python for Hackers
- Ethical Hacking & Penetration Testing

Course Details

You will learn how to search for valuable information on a typical Linux system with LAMP services, and deposit and hide Trojans for future exploitation. You will learn how to patch these web apps 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. 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

Introduction to wireless networks

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

Wireless network attacks independent of used encryption

- Introduction
- DoS: RF jamming
- DoS: CSMA/CA jamming
- The use of deauthentication attack for jamming network

- 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

WPA attacks

- 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

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

ARMOURINFOSEC

Course Details

MODULE 03: 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: Tcpdump/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