





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.

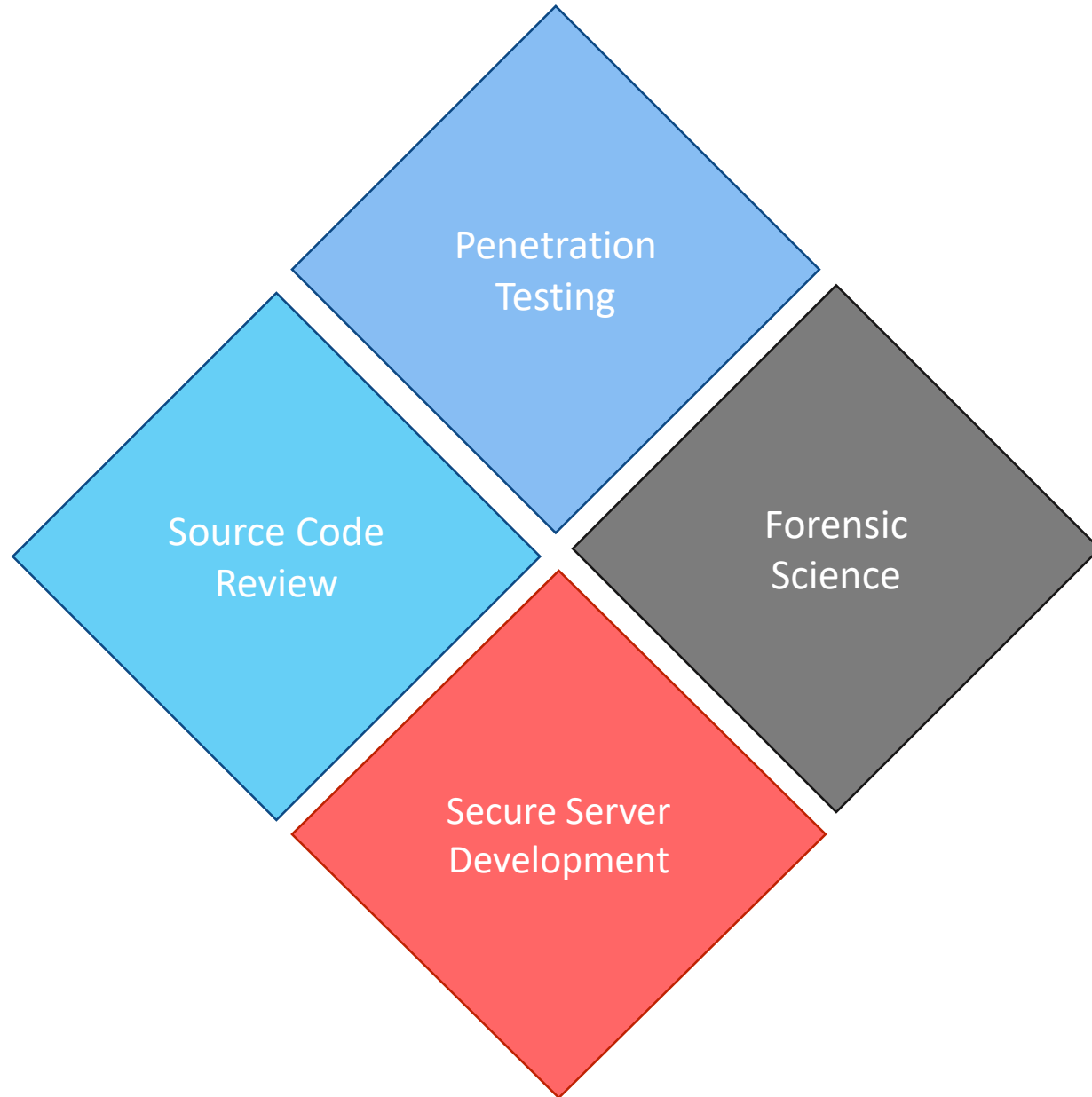
An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.

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.

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



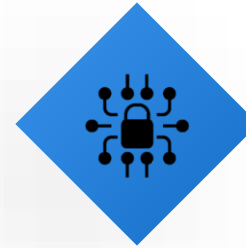
Certified Information Security Expert



Armour Infosec Certified Ethical Hacking Penetration Testing Expert



Armour Infosec Certified Computer Hacking & Forensic Expert



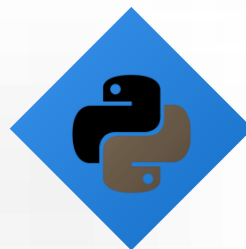
Certified Network Security Expert



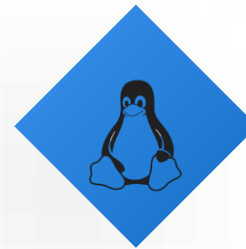
Certified Web Security Expert



Certified Wireless Security Expert



Python for Hackers



Certified Linux Server Administrator



Certified Windows Server Administrator

OUR COURSE

Armour Infosec Certified Computer Hacking & Forensic Expert



Armour Infosec Certified Computer hacking and forensic Expert is the collection, preservation, analysis, identification and presentation of computer-related evidence that can be useful in criminal cases for the purpose of facilitation or furthering the reconstruction of events found to be criminal.

You will learn how to search valuable information on typical Linux systems 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 defences.

Computer hacking and forensic expert is one of the largest growing professional certifications. The main goals of computer forensics are the preservation, identification, extraction, documentation and interpretation of recovered computer data



DURATION



2 hours/ day X 45 days



ENROLL NOW



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



Perform incident response and forensics, evidence collections, digital forensic acquisitions, bit-stream Imaging/acquiring of the digital media seized during the process of investigation. Examine and analyze text, graphics, multimedia, and digital images. Crack (or attempt to crack) password protected files, Conduct thorough examinations of computer hard disk drives, and other electronic data storage media

Recover information and electronic data from computer hard drives and other data storage devices, Follow strict data and evidence handling procedures, Maintain audit trail (i.e., chain of custody) and evidence integrity, Work on technical examination, analysis and reporting of computer-based evidence, Prepare and maintain case files, Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files, Recover deleted files and partitions in Windows, Mac OS X, and Linux

Investigate events for evidence of insider threats or attacks, Support the generation of incident reports and other collateral

Investigate and analyze all response activities related to cyber incidents, Plan, coordinate and direct recovery activities and incident analysis tasks, Examine all available information and supporting evidence or artefacts related to an incident or event

MODULE 01: INTRODUCTION TO FORENSICS

- What is forensics?
- Professions needing forensics

MODULE 02: INVESTIGATIONS

- Differences with legal investigations
- Reasons for corporate investigations
- Preparing for an investigation
- Forensic workstation
- Encase
- Ftk
- Coroners toolkit
- Prodiscover basic
- Audit policies
- Reporting
- Unix tools
- Sleuth kit
- Deft linux

Course Details



MODULE 03: OPERATING SYSTEMS

- Windows family
- Mac os x
- Linux
- Other types of operating systems
- Boot processes
- File systems: windows-based
- File systems: linux
- File systems: mac os
- File systems: cd
- Raid
- Autostarting
- Executable types and structure: windows
- Executable types and structure: unix-based
- Disk partitions

MODULE 04: IMAGE ACQUISITION

- Image formats
- Image acquisitions under linux
- Image acquisitions under windows
- Volatile information
- Data recovery
- Hard drives

MODULE 05: NETWORK ACQUISITIONS

- Osi reference model
- Tcp/ip
- Network attacks
- Reasons for network acquisitions
- Man in the middle attacks
- Capturing traffic
- Network miner
- Other network tools
- Wireless networking
- Wireless tools
- Firewalls and their uses
- Intrusion detection systems

MODULE 06: DATA SPACES

- Alternate data streams
- Deleted files
- Hidden partitions
- Slack space and swap file
- Registry
- Virtual memory
- System recovery checkpoints: windows
- Audit logs and settings

Course Details



MODULE 07: DATA RECOVERY

- Graphics files
- E-mail
- Internet: cache, cookies, etc.
- Metadata
- Log files
- Steganography
- Steganography techniques: images and video
- Steganography techniques: audio and documents
- Steganalysis
- Compression

MODULE 08: VIRTUAL MACHINES

- Virtual machines
- Checkpoints
- Data formats
- Hypervisors

MODULE 09: MOBILE FORENSICS

- IOS
- Android
- Symbian OS
- Tools
- Memory considerations
- Sim cards

MODULE 10: MALWARE FORENSICS

- Malware forensics
- Static malware analysis
- Dynamic malware analysis