NEW MODULES UPDATES 2024

1 Year Diploma in Cyber Security & Ethical Hacking

1 year Diploma is a Ethical Hacking & Cyber Security training course/training provided by FORENSIC ACADEMY in Punjab, Mohali, Chandigarh, Haryana – (with International Online Classes). This Cyber Security/ Ethical Hacking Course is provided by the professionals of Forensic Academy. It is framed by the expert professionals of FORENSIC ACADEMY having hands-on experience in Cyber Security & Ethical hacking.

- About 1 YEAR Cyber Security & Ethical Hacking Certification Training/Course
  - → 1 Year Diploma Fees: Rs 80,000/- ~~(95,000)~~
  - → Full-fledged course designed by Forensic Academy covering all domains of hacking.
  - → Framed in a manner such that it covers all aspects of Ethical Hacking & Cyber Security.
  - → Complete Ethical Hacking / Cyber Security toolkit will be provided.
  - → Along with the toolkit complete study material and guidance will be provided.
  - → Live Hacking demonstrations will be provided.
  - → Complete Industry exposure with hands-on experience on Cyber Security/Ethical Hacking projects.
  - → Tests will be scheduled at regular intervals.

Why Forensic Academy?

Forensic Academy is an emerging Information Security Company providing Information Security Solutions to clients. Key factors which play role that why Forensic Academy is best for Cyber Security & Ethical Hacking training are: Quality, affordability, regular exams, professional environment, guidance by experts, worth time utilization.

Training/Course Modules:

→ Introduction

- ○ Introduction to Cyber Security and Ethical Hacking
- ○ Introduction to all Underground Ethical Hacking Community
- ○ Types

→ Basics of Operating System and Architecture

- ○ Introduction to OS Architecture
- ○ Windows, Linux, Unix
- ○ Kernel System
- ○ Bootloader/ BIOS System

→ Linux

- ○ Introduction to Linux
- ○ Linux Architecture
- ○ Installation VM or virtual Box
- ○ Linux Installation – Kali OS, Parrot, ubuntu
- ○ Linux File System and Commands

- What is Shell and Bash Scripting
- Basic Scripting
- All Linux Commands and Tools

→ Networking

- Introduction to Network
- Internet / Network
- Lab Setup for Networking
- IPv4 / IPv6
- Mac Address
- Protocol like UDP, ICMP, TCP etc
- CISCO packet tracer tools

→ Network Security

- Information Gathering and Foot printing
- Network Vulnerability Assessment
- Network Penetration Testing
- Security Testing
- Port Scanning
- Nmap and Zenmap
- Metasploit Framework
- Scapy and Hping3
- Wireshark
- DoS and DDoS attack
- MITM attack – bettercap tool
- VPN and Proxy Server
- Networking Testing Report
- Sparta Tool
- WLAN Security
- WiFi Penetration Testing / hacking
- Router Configuration
- Network Router System
- Network Server Hacking
- Exploit DB – Hacking

→ Web Security and Hacking

- Introduction to web
- Frontend and backend
- Hacking and Security
- Advance Burp suite and ZAP proxy tool – penetration testing
- OWASP TOP 10
- XSS / JS Injection
- SQL Injection
- LFI or RFI
- CSRF / SSRF
- Sensitive Data exposure
- XML Injection
- Broken access control
- Security misconfiguration
- OTP bypass
- OS Command injection
- Google Dorking
- Admin page bypassing
- Database Create / Security Assessment
- Database hacking and security
- Payment gateway bypassing – hacking
- VAPT
- Apache2 or NGINX Hacking
- Phishing
- Website Testing
- Report Designing
- Manual Security Testing
- Automation Security Testing
- Bug Hunting – Tool and Techniques
- Bug Reporting – Hacker one, bugcroud
- Web & Network CTF / Hacking Machines

→ Android Penetration Testing

- Android Architecture
- JDK & JAVA using Android
- Android Application Development Overview Process
- Development Technologies
- Application Security Testing
- Firebase DB
- Google / SAMSUNG in Android
- Gene motion Lab Setup
- Rooted Phone – Investigation
- Android Testing using burp suite
- OWASP TOP 10 – Android PT
- Automation Application Testing
- Manual Application Testing
- Tool Based Analysis
- Android Security Reporting
- Android APK Penetration Testing

→ OS and Server Hardening

- OS Architecture works
- OS Security
- Window and Linux Server Hardening
- Secure Services
- Mod Security
- Log and Events Handling
- IDS and IPS / Firewall Security
- Data Protection
- Data Encryption
- Physical Server
- Server Lab Setup
- Ubuntu Server – Setup
- Redhat Server – Setup
- CentOS Server – Setup
- Server Development
- Window Server Setup
- Manual Configuration
- IIS Web Server Configuration
- FTP , SMTP, SAMBA, SSH all service configration

- File encryption
- Root password configuration
- Grub Security
- USB Port Security
- Apache2 Mod Security
- NGINX Mod Security
- Enable Firewall
- System Hardening
- Window Server 2008, 12
- Linux – Server Ubuntu, RHEL , CentOS

→ Cloud Penetration Testing & Hacking

- Fundamental of Cloud Computing
- Cloud Penetration Testing Concepts
- Introduction to Cloud Security
- Learning Objectives
- Architectural Concepts of Cloud
- Model of Cloud Computing
- Cloud Deployment Models
- Important Terminologies
- Cloud Security Concepts
- Cloud Data Lifecycle
- Security Issues in Cloud & its solution
- RISK Concerning
- Security Through Access Management
- Using Cloud Environment
- AWS Cloud, Azure Cloud, Alibaba Cloud Services
- Google Cloud
- Cloud Server Deployment
- Cloudflare – Security
- Cloud buckets – Penetration testing
- Azure bucket testing

→ IoT / OT Penetration Testing & Hardware Security & Hacking

- Fundamental of IoT
- Introduction to IoT Penetration Testing
- Real World IoT Application
- OWASP Top 10 IoT Threats
- Practical Labs & Tool
- IoT Model Security
- Manual & Automation IoT VAPT
- Amazon Alexa IoT Security Testing
- IoT based Camera IoT Security Testing
- Router IoT Security
- Wireshark for IoT
- Nmap for IoT Testing
- Burpsuite for IoT Hacking
- Fundamental of OT
- Introduction to ICS Architecture
- OT Hacking
- OT Hacking Methodology
- ICS/SCADA Testing
- SCADA Penetration Testing
- SCADA using nmap
- SCADA using nessus
- Hacking using Hardware Tools
- NodeMCU Hacking
- WiFi Jamming Hardware Practical
- Rubber Ducky
- PiCCoo Ducky Scripting
- USB Hacking Hardware
- Firmware Analysis
- Firmware Testing & Extraction
- JTAG Analysis
- Modbus Concepts
- SCADA – Data Station Working Model
- Automation like: Powerplant, Water Dam, Nuclear Plant SCADA Based Data Canter working

→ Forensic Investigation

- Corporate Forensic | Criminal forensics
- Computer forensic, Mobile , Server, cloud , social media forensic
- Introduction
- Chain of custody & 6A's of forensics
- Legal study of evidence acquisition
- Disk based forensics
- Network forensics
- Data packet analysis
- USB Forensics
- Memory Analysis
- Window forensic
- Deleted Data recovery Forensic
- Drone Forensics
- Wifi Router forensic
- CCTV & Video forensic
- IoT Forensic
- Android forensic
- IOS forensic
- Tool based on forensic study
- Deleted android recovery
- Image forensic
- Evidence recovery
- Evidence recovery
- Protocol standard
- WLAN security
- Dead vs Live forensic
- HDD Investigation
- Social media forensic – WhatsApp, Instagram , snapchat forensic
- Cloud based forensic
- Contact number forensic
- SIM card forensic
- CDR , IPDR Analysis
- Cyber Cell investigation
- Gallery image investigation
- Transaction forensic
- VPN forensics

- Forensic with CDAC Department tool: FTK, Autopsy, Mobiledit, Stellar data recovery, Mobile check, SIM Analysis, ADVIK CDR Analysis and many more……

→ COMPLIANCE

- Basic principles of assessment & auditing
- Types of Auditing
- IT Laws and Acts
- ISO 200:200:203basics
- PCIDSS
- BFSI Sector – for Security Industry
- Risk Assessment
- BCM
- Network Security
- Banking Auditing working
- Physical Security and Compliance
- GRC
- Type or Auditee
- PDCA
- Auditing Documentation
- Auditor Exams & Files
- Auditing Responsibility
- Internal Auditor

→ Certified Malware Analysis

- Malware Fundamentals
- Malware Costing
- Types
- Virus and Trojan
- Antivirus Working
- Live malware samples
- Tool kit providing
- Malware encryption
- Packing analysis
- Malicious Code & Pattern Analysis
- Complete malware analysis
- Static Malware analysis
- Dynamic Analysis

- In depth study of Self-defending malware
- Maneuvering Techniques
- Persistence Techniques
- Self-Destructive
- Self-avoidance
- Security degradation
- Malicious Documents
- Memory forensic
- Registry settings
- System services & settings
- Keylogger spyware software
- Trojan and backdoors Analysis
- Rootkits Analysis
- Opensource malware analysis
- Live malware testing
- Sandbox Analysis
- Malware toolkit
- Yara rules
- Build own yara rules
- YaraGen auto rules builder
- Automation Analysis
- Working with C & Python – concepts
- Hardware damage-based malware
- Android based Malware Analysis
- Reverse Engineering – RE
- Fundamental of Reverse Engineering
- Software reverse engineering
- Lab Setup
- Lab solve
- How to patch programs
- Cracking
- Tool RE Analysis
- Working with NSA GHIDRA, Assembly, IDApro, x64DBG

→ Incident Response & Team Leading for Corporate

- Fundamental of Incident
- What is incident
- Incident Types
- Incident Categories
- What is Incident Handling
- Incident Handlers are responsible
- Incident Handling Life-Cycle
- Incident Preparation
- Security Controls
- Goal of preparation
- Preparation key points
- Prepare system-built checklist
- Conduct war games
- Source of signs
- Detect signs
- Long-Term containment
- Follow up – Incident Handling
- Security POLICY
- CIA Policy
- Events and Incident
- IR Teams
- Live response
- Goals of IR
- What is IOC
- IOC formats & Tools
- Digester management

Hands on Practical Tool Live Working

www.forensicacademy.in

About Forensic Academy Certification & Training

- Egyptian Accreditation Council | Forensic Academy is Accreditation Body by: EGAC.
- 9001:2015 Certified Company | Forensic Academy follows the guidelines of the ISO 9001 standard. Fulfills its own requirements.
- Ministry of Micro, Small and Medium Enterprises | Forensic Academy Registered by Indian Govt. MSME.
- With IAF member

FORENSIC ACADEMY 2024 MODULES UPDATE ©

FORENSIC ACADEMY • SINCE 2022
Approved By MSME