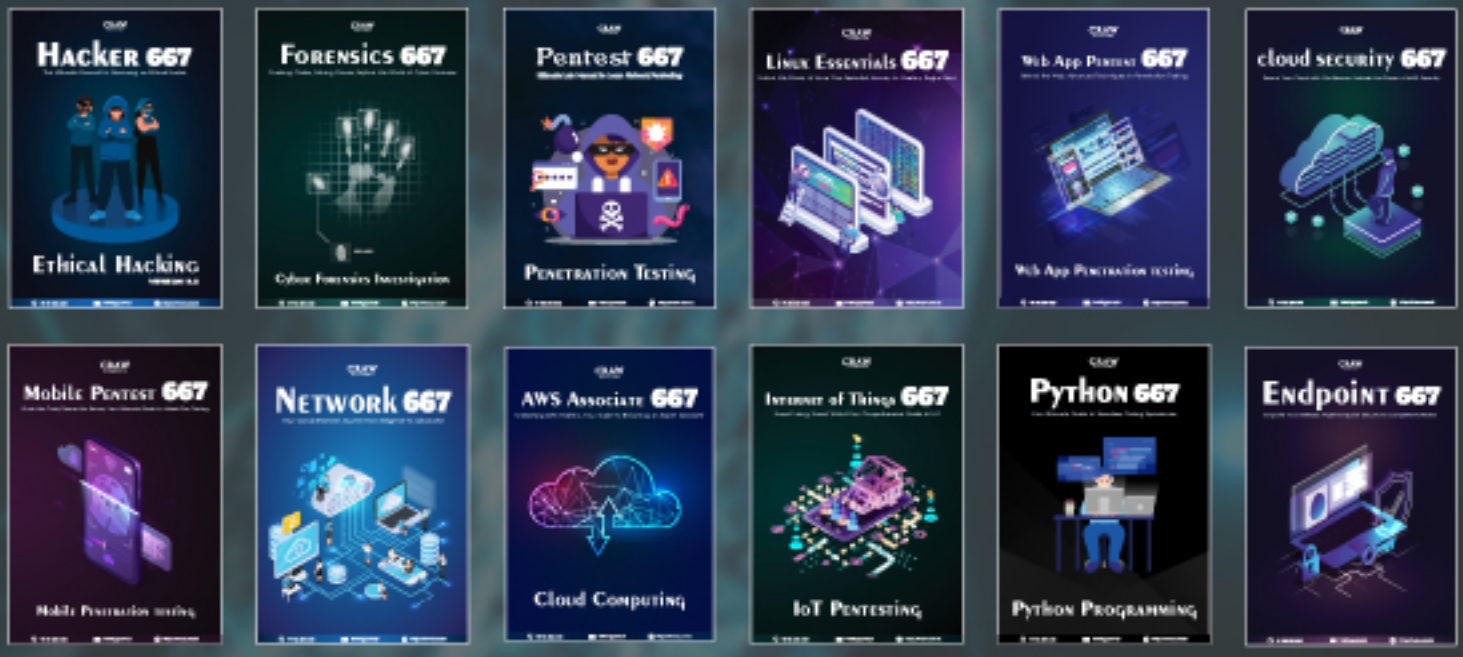
CRAW
ACADEMY

Learn | Research | Innovate

ONE YEAR INDUSTRY ORIENTED
CYBER SECURITY
DIPLOMA COURSE

version 2.0



TRAINING PARTNERS

OFFENSIVE SECURITY · RedHat · EC-Council · CISCO · PECB · CompTIA · python

Detailed One Year Diploma Course Curriculum

Level 1: Basic Networking

Table of Content

Program Overview

The Basic Networking Course offered by Craw Security, the premier Networking Training Institute in India, is designed to equip learners with the foundational skills and knowledge required to navigate the complex world of networking. This course lays the groundwork for understanding network infrastructure, network troubleshooting, protocols, and security principles essential for any aspiring IT professional.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Industry-leading cybersecurity experts with years of experience in penetration testing.
- ✓ Hands-on labs to learn with real-time problem-solving exercises.
- ✓ Cutting-edge curriculum to stay at the forefront of cybersecurity.
- ✓ Flexible Learning Options to choose from.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Basic Networking Course

Basic understanding of computer systems and the internet. In addition to this, no prior experience in networking is required, making this course ideal for beginners.

Target Audience

- ✓ Students and recent graduates aiming to build a career in IT and network administration.
- ✓ Professionals from other fields seeking to transition into IT and networking roles.
- ✓ Anyone with a curiosity about how network systems work and how to manage them effectively.
- ✓ Anyone who is concerned about the integrity of their network infrastructure.

Key Learning Outcomes

This Basic Networking Course will help you:

- ✓ **Understand Networking Fundamentals:** Gain a comprehensive understanding of basic networking concepts, including the OSI and TCP/IP models, networking topologies, and the role of each layer in data communication.
- ✓ **Identify and Utilize Networking Devices:** Learn about different networking hardware such as routers, switches, hubs, and bridges, and understand their specific functions within a network.
- ✓ **Implement Network Protocols and Standards:** Understand and apply key network protocols (e.g., HTTP, FTP, SMTP) and standards essential for the creation and maintenance of functional networks.
- ✓ **Configure Networks:** Acquire the skills to set up small to medium-sized networks, including configuring network devices, setting up WLANs (Wireless Local Area Networks), and managing IP addressing schemes.

- ✓ **Troubleshoot Network Issues:** Develop the ability to diagnose and resolve common network problems, enhancing network reliability and performance.
- ✓ **Ensure Network Security:** Understand basic network security principles and practices, including the use of firewalls, network security protocols, and the importance of secure network design.
- ✓ **IP Addressing and Sub netting:** Master IP addressing, including IPv4 and IPv6, and learn sub netting techniques to efficiently manage and segment networks and many more.

Certification Alignment

Our Basic Networking Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Certification Details -

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply basic networking techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  1. Documentation

2. Offer Letter
3. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India.

Course Curriculum

Module 01: Introduction to Networking

- ✓ Lesson 01: What is a Network?
- ✓ Lesson 02: Local Area Network (LAN) Explained
- ✓ Lesson 03: Wide Area Network (WAN) Explained
- ✓ Lesson 04: Type of Mode
- ✓ Lesson 05: Type of Communication

Module 02: Open Systems Interconnection (OSI) Model

- ✓ Lesson 01: What is Open Systems Interconnection (OSI)
- ✓ Lesson 02: Why we Need Open Systems Interconnection (OSI)
- ✓ Lesson 03: Open Systems Interconnection (OSI) Layers
- ✓ Lesson 04: Transmission Control Protocol (TCP) / User Datagram Protocol (UDP)
- ✓ Lesson 05: 3 Way Hand Shake

Module 03: Transmission Control Protocol (TCP) / Internet Protocol (IP) Model

- ✓ Lesson 01: What is Transmission Control Protocol (TCP) / Internet Protocol (IP)
- ✓ Lesson 02: Why we Need Transmission Control Protocol (TCP) / Internet Protocol (IP) Model
- ✓ Lesson 03: Transmission Control Protocol (TCP) / Internet Protocol (IP) Layer

Module 04: Sub Netting / Summarisation

- ✓ Lesson 01: Sub netting Explained
- ✓ Lesson 02: Classless Inter-Domain Routing (CIDR)
- ✓ Lesson 03: Create Subnets
- ✓ Lesson 04: Understanding Variable Length Subnet Masks (VLSM)
- ✓ Lesson 05: Private Internet Protocol (IP) Addresses Explained

Module 05: Packet Flow in Same & Different Network

- ✓ Lesson 01: What is Domain Name System (DNS) and How Does it Work?
- ✓ Lesson 02: Map Hostnames to Internet Protocol (IP) Addresses
- ✓ Lesson 03: Configure Cisco Device as Domain Name System (DNS) Client
- ✓ Lesson 04: How to Configure a Cisco Router as a DNS Server?
- ✓ Lesson 05: no Internet Protocol (IP) domain-lookup Command
- ✓ Lesson 06: Address Resolution Protocol (ARP) Explained
- ✓ Lesson 07: Address Resolution Protocol (ARP) Table on a Cisco Router

Module 06: Information about Networking Device

- ✓ Lesson 01: Network Devices
- ✓ Lesson 02: Network Hubs Explained

- ✓ Lesson 03: Network Switch Explained

- ✓ Lesson 04: Carrier Sense Multiple Access with Collision Detection (CSMA CD)
- ✓ Lesson 05: Collision & Broadcast Domain
- ✓ Lesson 06: How Switches Work
- ✓ Lesson 07: Layer 2 Switching
- ✓ Lesson 08: Network Router Explained
- ✓ Lesson 09: What Is Layer 3 Switch and how it Works in Our Network?

Module 07: Internet Protocol (IP) / Internet Control Message Protocol (ICMP)

- ✓ Lesson 01: Internet Control Message Protocol (ICMP)
- ✓ Lesson 02: Ping Explained
- ✓ Lesson 03: Extended Ping Command
- ✓ Lesson 04: Traceroute Explained
- ✓ Lesson 05: Traceroute Command
- ✓ Lesson 06: Show processes Command

Module 08: Automatic Private IP Addressing (APIPA)

- ✓ Lesson 01: What is Automatic Private IP Addressing (APIPA)
- ✓ Lesson 02: Why we Need Automatic Private IP Addressing (APIPA)
- ✓ Lesson 03: Automatic Private IP Addressing (APIPA)

Module 09: Address Resolution Protocol (ARP)

- ✓ Lesson 01: What is Address Resolution Protocol (ARP)
- ✓ Lesson 02: Why we Need Address Resolution Protocol (ARP)
- ✓ Lesson 03: Type of Address Resolution Protocol (ARP)

Module 10: Routing Protocols (Static & Dynamic)

- ✓ Lesson 01: Routing Protocols
- ✓ Lesson 02: Comparing Internal Routing Protocols (IGPs)
- ✓ Lesson 03: Administrative Distance & Metric
- ✓ Lesson 04: Equal Cost Multi-Path (ECMP) Explanation & Configuration
- ✓ Lesson 05: Understanding Loopback Interfaces and Loopback Addresses
- ✓ Lesson 06: Passive-interface Command

Module 11: Static - Next Hop / Exit Interface

- ✓ Lesson 01: What is IP Routing?
- ✓ Lesson 02: Local Routes and How they Appear in the Routing Table
- ✓ Lesson 03: Connected, Static, & Dynamic Routes
- ✓ Lesson 04: Floating Static Route - Explanation and Configuration
- ✓ Lesson 05: Default Static Route
- ✓ Lesson 06: Create a Static Host Route

Module 12: Dynamic - RIP / EIGRP / OSPF & BGP

- ✓ Lesson 01: OSPF Overview
- ✓ Lesson 02: Differences Between OSPF and EIGRP
- ✓ Lesson 03: Cisco Bandwidth Command vs Clock Rate and Speed Commands
- ✓ Lesson 04: OSPF Cost - OSPF Routing Protocol Metric Explained
- ✓ Lesson 05: OSPF Configuration

- ✓ Lesson 06: Designated & Backup Designated Router

Module 13: WAN Technologies

- ✓ Lesson 01: Wide Area Network
- ✓ Lesson 02: Cisco VPN - What is VPN (Virtual Private Network)?
- ✓ Lesson 03: WAN Connection Types - Explanation and Examples
- ✓ Lesson 04: Leased Line Definition, Explanation, and Example
- ✓ Lesson 05: Multiprotocol Label Switching (MPLS) Explained & Configured

Module 14: What is Network Address Translation (NAT)

- ✓ Lesson 01: Static Network Address Translation (NAT)
- ✓ Lesson 02: Dynamic Static Network Address Translation (NAT)
- ✓ Lesson 03: Port Address Translation (PAT) Configuration

Module 15: Access Control List (ACL)

- ✓ Lesson 01: What are Access Control List (ACL)?
- ✓ Lesson 02: Types of Access Control List (ACL)
- ✓ Lesson 03: Configuring Standard Access Control List (ACL)
- ✓ Lesson 04: Configuring Extended Access Control List (ACL)
- ✓ Lesson 05: Configuring Named Access Control List (ACL)

Module 16: Dynamic Host Configuration Protocol

- ✓ Lesson 01: Dynamic Host Configuration Protocol (DHCP) & Domain Name System (DNS)
- ✓ Lesson 02: Configure Cisco Router as Dynamic Host Configuration Protocol (DHCP) Server
- ✓ Lesson 03: Dynamic Host Configuration Protocol (DHCP) Relay Agent
- ✓ Lesson 04: Configure Cisco Router as a Dynamic Host Configuration Protocol (DHCP) Client
- ✓ Lesson 05: Automatic Private IP Addressing (APIPA)

Module 17: Telnet & Secure SHell (SSH)

- ✓ Lesson 01: What is Telnet & Secure Shell (SSH)
- ✓ Lesson 02: Why we Need Telnet & Secure Shell (SSH)
- ✓ Lesson 03: Telnet & Secure Shell (SSH)
- ✓ Lesson 04: Setting Up Telnet
- ✓ Lesson 05: Setting Up Secure Shell (SSH)

Module 18: Load Balancing Protocol

- ✓ Lesson 01: What is Network Redundancy and What are its Benefits?
- ✓ Lesson 02: Cisco First Hop Redundancy Protocol (FHRP) Explained
- ✓ Lesson 03: Cisco Hot Standby Router Protocol (HSRP) Explained
- ✓ Lesson 04: Cisco Hot Standby Router Protocol (HSRP) Configuration
- ✓ Lesson 05: Cisco Hot Standby Router Protocol (HSRP) Preempt Command

Module 19: Layers 2 Protocols

- ✓ Lesson 01: What is Layer 2
- ✓ Lesson 02: Why we Need Layer 2 Protocol
- ✓ Lesson 03: Cisco Discovery Protocol (CDP)
- ✓ Lesson 04: Link Layer Discovery Protocol (LLDP)

Module 20: Virtual Local Area Network (VLAN)

- ✓ Lesson 01: What is a Virtual Local Area Network (VLAN)?
- ✓ Lesson 02: Configuring Access & Trunk Ports
- ✓ Lesson 03: Configuring Voice Virtual Local Area Network (VLAN)
- ✓ Lesson 04: Configuring Allowed Virtual Local Area Network (VLAN)
- ✓ Lesson 05: Cisco Dynamic Trunking Protocol (DTP) Explained
- ✓ Lesson 06: What is Virtual Trunking Protocol (VTP)?
- ✓ Lesson 07: Virtual Trunking Protocol (VTP) Modes
- ✓ Lesson 08: Virtual Trunking Protocol (VTP) Configuration

Module 21: Different Types of Spanning Tree Priority (STP)

- ✓ Lesson 01: Network Bridge Explained
- ✓ Lesson 02: How Spanning Tree Priority (STP) Works
- ✓ Lesson 03: Electing the Root Switch in Spanning Tree Priority (STP)
- ✓ Lesson 04: Spanning Tree Priority: Root Primary and Root Secondary
- ✓ Lesson 05: Selecting Spanning Tree Priority (STP) Root Port
- ✓ Lesson 06: Selecting Spanning Tree Priority (STP) Designated Port (DP)

Module 22: Ether-Channel (L2)

- ✓ Lesson 01: What is Ether Channel and Why Do We Need It?
- ✓ Lesson 02: Ether Channel Port Aggregation Protocol (PAgP)
- ✓ Lesson 03: Ether Channel Link Aggregation Control Protocol (LACP)
- ✓ Lesson 04: Multi chassis Ether Channel (MEC) and its Options
- ✓ Lesson 05: Cisco Layer 3 Ether Channel - Explanation and Configuration

Module 23: Port Security

- ✓ Lesson 01: Cisco Console Port Security
- ✓ Lesson 02: Exec-timeout Command
- ✓ Lesson 03: Encrypt Local Usernames and Passwords

For more information, please visit our course page website
https://www.craw.in/basic-networking-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401

Connect on WhatsApp: +91 8448897124
Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 2: Linux Essentials

Table of Content

Program Overview

The Linux Essentials Training Course, offered by Craw Security, the Best Linux Training Institute in India, is designed to provide foundational knowledge and skills in Linux. This program covers a broad range of topics, from basic Linux operations to advanced system administration and security. Our course is structured to ensure that participants gain practical experience and theoretical understanding of Linux, making them proficient in navigating and managing Linux environments.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in Linux and as a system administrator.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Cutting-edge curriculum to stay at the forefront of the system administration domain.
- ✓ Receive detailed study guides and resources designed to enhance your learning experience.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.
- ✓ Benefit from our continuous support even after completing the course, ensuring your long-term success.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Linux Essentials Course

This course is suitable for beginners. However, a basic understanding of computer systems and networks is beneficial to fully grasp the concepts taught.

Target Audience

- ✓ Aspiring IT professionals,
- ✓ System administrators,
- ✓ Network engineers,
- ✓ Cybersecurity enthusiasts,
- ✓ Anyone looking to enhance their Linux skills to make an outshining career in this domain.

Key Learning Outcomes

This Linux Essentials Course will help you:

- ✓ **Understanding of Linux Basics:** Gain a solid understanding of Linux, including its history, benefits, and how it compares to other operating systems.
- ✓ **Command Line Proficiency:** Develop proficiency in using the Linux command line interface (CLI), including navigating the file system, managing files and directories, and executing basic commands and utilities.

- ✓ **File System Navigation and Management:** Learn to navigate and manage Linux file systems, and understand file types, directories, and the hierarchical structure.

- ✓ **User and Group Management:** Acquire the skills to manage users and groups within a Linux environment, setting permissions and ensuring security.
- ✓ **File Permissions and Security:** Understand file permissions and how to modify them to secure access to files and directories, ensuring system security and user privacy.
- ✓ **Networking Fundamentals:** Gain insights into basic networking concepts on Linux, including configuring network interfaces, managing network services, and troubleshooting connectivity issues.
- ✓ **Introduction to Shell Scripting:** Learn the basics of shell scripting to automate repetitive tasks, enhance productivity, and perform complex administrative tasks with ease.
- ✓ **System Administration Basics:** Acquire foundational knowledge in Linux system administration, including system monitoring, managing processes, and installing software.
- ✓ **Linux Security Basics:** Understand the fundamental security concepts and practices in Linux, including firewall management, security updates, and best practices to protect the system.
- ✓ **Real-World Applications:** Apply the learned concepts in real-world scenarios, preparing for practical applications in professional environments.

Certification Alignment

Our Linux Essentials Training Course is widely recognized by Craw Security. Moreover, you can even give a versatile touch to this course by adding a value-added certification from the House of Red Hat to add charms to your resume. Craw Security is even a proud partner of Red Hat Incorporation to derive its courses and certifications training at the facilities to Craw Security at very affordable and discounted prices.

Certification Details & Criteria

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply Linux Essentials techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.

- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.

- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
    4. Documentation
    5. Offer Letter
    6. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India.

Course Curriculum

Module 01: Getting Started with Red Hat Enterprise Linux

- ✓ Lesson 01: What Is Linux?

Module 02: Accessing the Command Line

- ✓ Lesson 01: Access the Command Line
- ✓ Lesson 02: Access the Command Line with the Desktop
- ✓ Lesson 03: Execute Commands with the Bash Shell
- ✓ Lesson 04: Lab: Access the Command Line

Module 03: Managing Files from the Command Line

- ✓ Lesson 01: Describe Linux file system Hierarchy Concepts
- ✓ Lesson 02: Specify Files by Name
- ✓ Lesson 03: Manage Files with Command-line Tools
- ✓ Lesson 04: Make Links Between Files
- ✓ Lesson 05: Match File Names with Shell Expansions
- ✓ Lesson 06: Lab: Manage Files from the Command Line

Module 04: Getting Help in Red Hat Enterprise Linux

- ✓ Lesson 01: Lab: Get Help in Red Hat Enterprise Linux

Module 05: Creating, Viewing & Editing Test Files

- ✓ Lesson 01: Redirect Output to a File or Program
- ✓ Lesson 02: Edit Text Files from the Shell Prompt
- ✓ Lesson 03: Change the Shell Environment
- ✓ Lesson 04: Lab: Create, View, and Edit Text Files

Module 06: Managing Local Users and Groups

- ✓ Lesson 01: Describe User and Group Concepts
- ✓ Lesson 02: Gain Superuser Access

- ✓ Lesson 03: Manage Local User Accounts
- ✓ Lesson 04: Manage Local Group Accounts

- ✓ Lesson 05: Manage User Passwords
- ✓ Lesson 06: Lab: Manage Local Users and Groups

Module 07: Controlling Access to Files

- ✓ Lesson 01: Interpret Linux File System Permissions
- ✓ Lesson 02: Manage File System Permissions from the Command Line
- ✓ Lesson 03: Manage Default Permissions and File Access
- ✓ Lesson 04: Lab: Control Access to Files

Module 08: Monitoring and Managing Linux Process

- ✓ Lesson 01: Process States and Lifecycle
- ✓ Lesson 02: Control Jobs
- ✓ Lesson 03: Kill Processes
- ✓ Lesson 04: Monitor Process Activity
- ✓ Lesson 05: Lab: Monitor and Manage Linux Processes

Module 09: Controlling Services and Daemons

- ✓ Lesson 01: Identify Automatically Started System Processes
- ✓ Lesson 02: Control System Services
- ✓ Lesson 03: Lab: Control Services and Daemons

Module 10: Configuring and Securing SSH

- ✓ Lesson 01: Access the Remote Command Line with Secure Shell (SSH)
- ✓ Lesson 02: Configure Secure Shell (SSH) Key-based Authentication
- ✓ Lesson 03: Customize Open Secure Shell (SSH) Service Configuration
- ✓ Lesson 04: Lab: Configure and Secure Shell (SSH)

Module 11: Analyzing and Storing Logs

- ✓ Lesson 01: Describe System Log Architecture
- ✓ Lesson 02: Review Syslog Files
- ✓ Lesson 03: Review System Journal Entries
- ✓ Lesson 04: Preserve the System Journal
- ✓ Lesson 05: Maintain Accurate Time
- ✓ Lesson 06: Lab: Analyze and Store Logs

Module 12: Managing Networking

- ✓ Lesson 01: Describe Networking Concepts
- ✓ Lesson 02: Validate Network Configuration
- ✓ Lesson 03: Configure Networking from the Command Line
- ✓ Lesson 04: Edit Network Configuration Files
- ✓ Lesson 05: Configure Hostnames and Name Resolution
- ✓ Lesson 06: Lab: Manage Networking

Module 13: Archiving and Transferring Files

- ✓ Lesson 01: Manage Compressed tar Archives
- ✓ Lesson 02: Transfer Files Between Systems Securely

- ✓ Lesson 03: Synchronize Files Between Systems Securely
- ✓ Lesson 04: Lab: Archive and Transfer Files

Module 14: Installing and Updating Software Packages

- ✓ Lesson 01: Install and Update Software Packages
- ✓ Lesson 02: Register Systems for Red Hat Support
- ✓ Lesson 03: Explain and Investigate RPM Software Packages
- ✓ Lesson 04: Install and Update Software Packages with Differential Network Flow (DNF)
- ✓ Lesson 05: Enable Differential Network Flow (DNF) Software Repositories
- ✓ Lesson 06: Lab: Install and Update Software Packages

Module 15: Accessing Linux File System

- ✓ Lesson 01: Identify File Systems and Devices
- ✓ Lesson 02: Mount and Unmount File Systems
- ✓ Lesson 03: Locate Files on the System
- ✓ Lesson 04: Lab: Access Linux File Systems

Module 16: Analyzing Servers and Getting Support

- ✓ Lesson 01: Analyze and Manage Remote Servers
- ✓ Lesson 02: Get Help From Red Hat Customer Portal
- ✓ Lesson 03: Detect and Resolve Issues with Red Hat Insights

For more information, please visit our course page website:
https://www.craw.in/linux-essential-training-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 3: Python Programming

Table of Content

Program Overview

The Python Programming Training Course offered by Craw Security, renowned as the Best Python Training Institute in India, is designed to equip students with a profound understanding of Python programming, from the basics to advanced concepts. Our course caters to the needs of individuals aiming to excel in the fields of software development, data analysis, cybersecurity, and various other domains that rely on Python as a core programming tool.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Python tech gurus with highly credible experience in Python programming.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Cutting-edge curriculum to stay at the frontiers of the Python domain.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Python Programming

A basic understanding of computer operations and programming concepts is beneficial but not mandatory. Eagerness to learn and apply new programming skills.

Target Audience

- ✓ Aspiring programmers seeking to learn Python from scratch.
- ✓ Professionals aiming to enhance their programming skills for career advancement.
- ✓ Individuals who are genuinely interested in data analysis, machine learning, web development, or cybersecurity.
- ✓ Anyone who is willing to make an outstanding career in the Python domain.

Key Learning Outcomes

This Python programming Training Course will help you:

- ✓ **Master Python Syntax and Core Programming Concepts:** Understand and apply the fundamental principles of Python programming, including variables, data types, operators, and control structures.
- ✓ **Solve Real-world Problems:** Utilize Python to develop solutions for a variety of challenges in software development, data analysis, automation, and more, enhancing problem-solving abilities.
- ✓ **Develop and Debug Python Applications:** Gain the ability to create functional Python applications, utilizing best practices in coding and debugging to ensure efficiency and reliability.

- ✓ **Implement Object-Oriented Programming (OOP):** Apply OOP principles in Python to design and implement reusable and modular code, enhancing software architecture and design.
- ✓ **Work with Data Structures and Algorithms:** Employ Python's built-in data structures (lists, tuples, sets, dictionaries) effectively, and understand how to approach and solve problems using algorithms.
- ✓ **Utilize Python Libraries and Frameworks:** Explore and implement solutions using powerful Python libraries and frameworks for web development, data analysis, machine learning, and more.

Certification Alignment

Our Python Programming Training Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply Python Programming Training techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 35 to 40 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations & claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  7. Documentation
  8. Offer Letter

9. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the **1 Year Cybersecurity Diploma Course** after the completion of this course, which is basically a 12-course bundle of cybersecurity by Craw Security whose maximum courses are accredited to the **FutureSkills Prime, a MeitY — NASSCOM,** Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Introduction

- ✓ Lesson 01: Programming language introduction
- ✓ Lesson 02: Translators (Compiler, Interpreter and assembler)
- ✓ Lesson 03: Uses of computer programs
- ✓ Lesson 04: Algorithm
- ✓ Lesson 05: Flow chart

Module 02: Python Introduction

- ✓ Lesson 01: History
- ✓ Lesson 02: Why python created
- ✓ Lesson 03: Fields of use
- ✓ Lesson 04: Use of Python in Cyber security
- ✓ Lesson 05: Reasons for using python
- ✓ Lesson 06: Syntax
- ✓ Lesson 07: Installation of Integrated Development Environment (IDE) Pycharm / Visual studio
- ✓ Lesson 08: Running a hello world program

Module 03: Comparison of Python with other Programming Language

- ✓ Lesson 01: Python vs Java
- ✓ Lesson 02: Python vs C++

Module 04: Data Type

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Discuss all data types
- ✓ Lesson 03: Use type() to show dynamically typed language

Module 05: Variables

- ✓ Lesson 01: What is variable
- ✓ Lesson 02: Declaration rules
- ✓ Lesson 03: Multiple variable declaration
- ✓ Lesson 04: Valid and invalid variables
- ✓ Lesson 05: Type casting

Module 06: String

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Declaration

- ✓ Lesson 03: All Functions with examples

Module 07: Operators

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Arithmetic operators
- ✓ Lesson 03: Assignment operators
- ✓ Lesson 04: Comparison operators
- ✓ Lesson 05: Logical operators
- ✓ Lesson 06: Identity operator
- ✓ Lesson 07: Bitwise operator
- ✓ Lesson 08: Membership operator

Module 08: List

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Declaration
- ✓ Lesson 03: All Functions with examples

Module 09: Tuple

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Declaration
- ✓ Lesson 03: All Functions with examples

Module 10: Dictionary

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Declaration
- ✓ Lesson 03: All Functions with examples

Module 11: Set

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Declaration
- ✓ Lesson 03: All Functions with examples

Module 12: Conditional Statement

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: If introduction with examples
- ✓ Lesson 03: If statement practice questions
- ✓ Lesson 04: If- else introduction with examples
- ✓ Lesson 05: If - else statement practice questions
- ✓ Lesson 06: elif introduction with examples
- ✓ Lesson 07: elif statement practice questions
- ✓ Lesson 08: Nested if
- ✓ Lesson 09: Short hand if- else

Module 13: Looping

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: While loop

- ✓ Lesson 03: Introduce modules (pyautogui)
- ✓ Lesson 04: While loop practice questions
- ✓ Lesson 05: For loop introduction with examples
- ✓ Lesson 06: For loop practice questions
- ✓ Lesson 07: Nested loop

Module 14: Function

- ✓ Lesson 01: Introduction function
- ✓ Lesson 02: Declaration, calling of function
- ✓ Lesson 03: Lambda function
- ✓ Lesson 04: Filter
- ✓ Lesson 05: Reduce function
- ✓ Lesson 06: Map function

Module 15: File Handling

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Text file handling
- ✓ Lesson 03: Binary file handling

Module 16: Python Array

- ✓ Lesson 01: Array Introduction
- ✓ Lesson 02: Array basic operations
- ✓ Lesson 03: Array Function

Module 17: Object Oriented Programming (OOPs)

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Difference b/w procedural programming and Object Oriented Programming (OOPs)
- ✓ Lesson 03: Class
- ✓ Lesson 04: Object
- ✓ Lesson 05: Encapsulation
- ✓ Lesson 06: Inheritance
- ✓ Lesson 07: Abstraction
- ✓ Lesson 08: Polymorphism

Module 18: Date and Time

- ✓ Lesson 01: Date and time function off date time module

Module 19: Web Scrapping

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Introduce basic html tags
- ✓ Lesson 03: Introduction to requests library
- ✓ Lesson 04: Introduction to bs4
- ✓ Lesson 05: Scrapping through Beautiful Soup

Module 20: Network Interaction

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Client
- ✓ Lesson 03: Server
- ✓ Lesson 04: Port number
- ✓ Lesson 05: IP
- ✓ Lesson 06: Client - server connection with python code

Module 21: Tkinter

- ✓ Lesson 01: Introduction to Graphical User Interface (GUI) programming
- ✓ Lesson 02: Widgets introduction and code
- ✓ Lesson 03: Create Login form project
- ✓ Lesson 04: Task Text to speech

Module 22: Database Connection

- ✓ Lesson 01: Introduction to database
- ✓ Lesson 02: Install My Structured Query Language (MySql)
- ✓ Lesson 03: Explain basic query of sql
- ✓ Lesson 04: Connection with python
- ✓ Lesson 05: Execute some queries by python

Module 23: Multithreading

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Real life examples
- ✓ Lesson 03: Perform operations over threads

Module 24: Mail Sending Program

- ✓ Lesson 01: Python project to send email
- ✓ Lesson 02: App password generating
- ✓ Lesson 03: Sending email

Module 25: Python for Image Processing

- ✓ Lesson 01: Using opencv library
- ✓ Lesson 02: Accessing image
- ✓ Lesson 03: Red Green Blue (Rgb) to Grayscale
- ✓ Lesson 04: Resizing
- ✓ Lesson 05: Filters
- ✓ Lesson 06: Saving image

Module 26: Introduction to Machine Learning

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Steps to create Machine Learning (ML) Application
- ✓ Lesson 03: Real examples of Machine Learning

Module 27: Introduction to Data Science

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Terminology used in Data Science

Module 28: Introduction to Artificial Intelligence

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Artificial Intelligence (AI) Websites as example

For more information, please visit our course page website:
https://www.craw.in/learn-python-training-in-delhi-python-course/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel

Level 4: Ethical Hacking

Table of Content

Program Overview

Our Ethical Hacking Course is designed to offer an immersive experience in the world of cybersecurity and ethical hacking. This program covers the fundamental skills and knowledge needed to protect organizations against cyber threats and vulnerabilities. Through a hands-on approach, participants will learn to think like hackers to defend against future attacks. This course is ideal for aspiring cybersecurity professionals seeking to enhance their skills in network security, system penetration testing, and ethical hacking.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in ethical hacking fundamentals and security.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Cutting-edge curriculum to stay at the forefront of the ethical hacking sector.
- ✓ Join a community of cybersecurity enthusiasts and professionals for networking and support.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Ethical Hacking

- ✓ Basic understanding of networking concepts.
- ✓ Familiarity with operating systems, especially Windows and Linux.
- ✓ A keen interest in cybersecurity and ethical hacking.

Target Audience

- ✓ IT professionals who are seeking to transition into cybersecurity roles.
- ✓ Network administrators and engineers.
- ✓ Security officers and practitioners.
- ✓ College students and recent graduates looking to enter the cybersecurity field, and
- ✓ Anyone who is willing to know more about the ethical hacking course.

Key Learning Outcomes

This Ethical Hacking Course will help you:

- ✓ **Understanding of Ethical Hacking Fundamentals:** Gain a comprehensive understanding of what ethical hacking is, including the ethics and legality surrounding the practice. Learn about the role of an ethical hacker in strengthening the cybersecurity posture of organizations.

- ✓ **Proficiency in Identifying Vulnerabilities:** Develop the ability to perform thorough vulnerability assessments to identify potential security weaknesses in computer systems, networks, and applications.
- ✓ **Skills in Exploiting Vulnerabilities:** Learn how to exploit identified vulnerabilities in a controlled and safe environment. This includes gaining unauthorized access to systems in a manner that mimics the approach of malicious hackers, with the intent of finding and fixing the vulnerabilities.
- ✓ **Expertise in Penetration Testing:** Acquire the skills to conduct comprehensive penetration tests, simulating cyberattacks on an organization's network to evaluate the security of the system.
- ✓ **Knowledge of Countermeasures and Preventive Measures:** Understand and be able to implement countermeasures to protect against hacking attacks. Learn about various security practices and technologies that can be employed to secure systems and networks.
- ✓ **Familiarity with Various Hacking Tools and Techniques:** Gain hands-on experience with the latest hacking tools and techniques used in real-world cybersecurity assessments, including those for network scanning, password cracking, and encryption/decryption.
- ✓ **Insight into Emerging Cybersecurity Trends:** Stay abreast of the latest cybersecurity threats and trends, including those related to cloud computing, mobile platforms, and IoT devices. Learn how to adapt and apply ethical hacking techniques to new technologies.
- ✓ **Preparation for Industry-Recognized Certifications:** Prepare for various industry-recognized certifications such as Certified Ethical Hacker (CEH), CompTIA Security+, and Offensive Security Certified Professional (OSCP), enhancing career prospects and professional credibility.
- ✓ **Critical Thinking and Problem-Solving Skills:** Develop critical thinking and problem-solving skills essential for identifying and mitigating complex cybersecurity challenges.
- ✓ **Ethical Decision-Making and Professionalism:** Emphasize the importance of ethics and professionalism in the cybersecurity field. Understand the legal implications of hacking and ensure all activities are conducted within legal and ethical boundaries.

Certification Alignment

Our Ethical Hacking Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Certification Details -

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply ethical hacking best practices and techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Provider:** FutureSkills Prime
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  10. Documentation
  11. Offer Letter
  12. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India.

Course Curriculum

Module 01: Introduction to Basics of Ethical Hacking

- ✓ Lesson 01: Intro To Ethical Hacking
- ✓ Lesson 02: Types of Attacks
- ✓ Lesson 03: Hacking Methodology
- ✓ Lesson 04: Cyber Kill Chain
- ✓ Lesson 05: Types of Attackers
- ✓ Lesson 06: Confidentiality, Integrity, and Availability (CIA) Traid
- ✓ Lesson 07: Risk Management
- ✓ Lesson 08: Cyber Laws

Module 02: Foot-printing Active (Tool-Based Practical)

- ✓ Lesson 01: What is Active Footprinting
- ✓ Lesson 02: Different kinds of information gathered in Footprinting
- ✓ Lesson 03: Tools for Active Footprinting = nmap, hping, Masscan

Module 03: Foot-printing Passive (Passive Approach)

- ✓ Lesson 01: What is passive footprinting
- ✓ Lesson 02: Footprinting Through Whois
- ✓ Lesson 03: Footprinting Through Website / Web services

- ✓ Lesson 04: Footprinting Through search engine
- ✓ Lesson 05: Footprinting Through DNS
- ✓ Lesson 06: Footprinting Through Email
- ✓ Lesson 07: Footprinting Through Network
- ✓ Lesson 08: Footprinting Through Social Media
- ✓ Lesson 09: Tools for Passive Footprinting – Google dorks, shodan, netcraft

Module 04: In-depth Network Scanning

- ✓ Lesson 01: Overview of Network Scanning
- ✓ Lesson 02: Scanning Methodology
- ✓ Lesson 03: Host Discovery
- ✓ Lesson 04: Port Scanning Techniques
- ✓ Lesson 05: Scanning tools – nmap, netdiscover, arp-scan -1

Module 05: Enumeration User Identification

- ✓ Lesson 01: Enumeration Concepts
- ✓ Lesson 02: Network Basic Input Output System (NetBIOS) Enumeration
- ✓ Lesson 03: Simple Network Management Protocol (SNMP) Enumeration
- ✓ Lesson 04: Lightweight Directory Access Protocol (LDAP) Enumeration
- ✓ Lesson 05: Simple Mail Transport Protocol (SMTP) Enumeration
- ✓ Lesson 06: Domain Name System (DNS) Enumeration

Module 06: System Hacking Password Cracking & Bypassing

- ✓ Lesson 01: Authentication
- ✓ Lesson 02: Gaining Access
- ✓ Lesson 03: Password cracking
- ✓ Lesson 04: Password Cracking Techniques
- ✓ Lesson 05: Steganography

Module 07: Viruses and Worms

- ✓ Lesson 01: Introduction to Malware
- ✓ Lesson 02: Types of Viruses
- ✓ Lesson 03: Types of Worms

Module 08: Trojan and Back door

- ✓ Lesson 01: Types of Trojans
- ✓ Lesson 02: Components Of a Trojan

Module 09: Bots and Botnets

- ✓ Lesson 01: Introduction to Botnets
- ✓ Lesson 02: Characteristics of Botnets

Module 10: Sniffers MITM with Kali

- ✓ Lesson 01: Introduction to Ettercap and Bettercap
- ✓ Lesson 02: Practical on Ettercap
- ✓ Lesson 03: Practical on Bettercap

Module 11: Sniffers MITM with Windows

- ✓ Lesson 01: Introduction to Wireshark
- ✓ Lesson 02: Practical on Wireshark

Module 12: Social Engineering Techniques Theoretical Approach

- ✓ Lesson 01: Types of Social Engineering Attacks
- ✓ Lesson 02: Human Based Social Engineering Attacks
- ✓ Lesson 03: Computer Based Social Engineering Attacks
- ✓ Lesson 04: Mobile Based Social Engineering Attacks

Module 13: Social Engineering Toolkit Practical Based Approach

- ✓ Lesson 01: Practical on zphisher
- ✓ Lesson 02: Practical on Social Engineering Toolkit (SET)

Module 14: Denial of Service (DOS) & Distributed Denial-of-Service (DDOS) Attacks

- ✓ Lesson 01: Denial of Service (DOS) / Distributed Denial-of-Service (DDOS) Concepts
- ✓ Lesson 02: Denial of Service (DOS) / Distributed Denial-of-Service (DDOS) Attack Techniques
- ✓ Lesson 03: Denial of Service (DOS) / Distributed Denial-of-Service (DDOS) Tools
- ✓ Lesson 04: Denial of Service (DOS) / Distributed Denial-of-Service (DDOS) Protection Tools and Techniques

Module 15: Web Session Hijacking

- ✓ Lesson 01: Session Hijacking Concepts
- ✓ Lesson 02: Session Hijacking Techniques
- ✓ Lesson 03: Session Hijacking Tools

Module 16: SQL Injection Manual Testing

- ✓ Lesson 01: SQL Injection Concept
- ✓ Lesson 02: Types of SQL Injection
- ✓ Lesson 03: Working Of SQL Injection
- ✓ Lesson 04: SQL Injection Methodology

Module 17: SQL Injection Automated Tool-Based Testing

- ✓ Lesson 01: Practical on sqlmap
- ✓ Lesson 02: Practical on Ghauri

Module 18: Basics of Web App Security

- ✓ Lesson 01: Fundamentals of Web Application Security
- ✓ Lesson 02: Common Vulnerabilities in Web Applications
- ✓ Lesson 03: Best Practices for Web App Security

Module 19: Hacking Web servers

- ✓ Lesson 01: Web Server Hacking Techniques
- ✓ Lesson 02: Server Rooting Methods
- ✓ Lesson 03: Securing Web servers

Module 20: Hacking Wireless Networks Manual CLI Based

- ✓ Lesson 01: Wireless Network Basics
- ✓ Lesson 02: Manual Hacking Techniques for Wi-Fi Networks
- ✓ Lesson 03: Command Line Tools for Wireless Hacking

Module 21: Hacking Wireless Network

- ✓ Lesson 01: Automated Wireless Hacking Tools
- ✓ Lesson 02: Wireless Network Exploitation Methods
- ✓ Lesson 03: Wireless Security Best Practices

Module 22: Evading IDS, Firewall

- ✓ Lesson 01: Intrusion Detection System (IDS) Evasion Techniques
- ✓ Lesson 02: Firewall Evasion Methods
- ✓ Lesson 03: Stealth and Evasion Tools

Module 23: Honey pots

- ✓ Lesson 01: Introduction on Honeypots
- ✓ Lesson 02: Types Of Honeypots
- ✓ Lesson 03: Install Of Honeypot (KF Sensor)

Module 24: Buffer Overflow

- ✓ Lesson 01: Introduction to Buffer Overflow

Module 25: Cryptography

- ✓ Lesson 01: What is cryptography, encryption, decryption
- ✓ Lesson 02: Types of cipher – substitution (Caesar) and Transposition (rail fence) techniques
- ✓ Lesson 03: Keys in cryptography – asymmetric and symmetric
- ✓ Lesson 04: What is encoding
- ✓ Lesson 05: Example of encoding
- ✓ Lesson 06: What is hashing
- ✓ Lesson 07: Example of hashes of a string

Module 26: Penetration Testing: Basics

- ✓ Lesson 01: Penetration Testing Overview
- ✓ Lesson 02: Phases of Penetration Testing
- ✓ Lesson 03: Reporting and Remediation

Module 27: Mobile Hacking

- ✓ Lesson 01: Mobile Security Threats
- ✓ Lesson 02: Exploiting Mobile Platforms
- ✓ Lesson 03: Theory of mobile and mobile attacks
- ✓ Lesson 04: Practical of Androrat

Module 28: Internet of Things (IoT) Hacking

- ✓ Lesson 01: Internet of Things (IoT) Concepts
- ✓ Lesson 02: Internet of Things (IoT) Hacking Methodology
- ✓ Lesson 03: Internet of Things (IoT) Hacking Tools
- ✓ Lesson 04: Internet of Things (IoT) Security Tools

Module 29: Cloud Security and many more

- ✓ Lesson 01: Cloud Computing Concepts
- ✓ Lesson 02: Cloud Computing Threats
- ✓ Lesson 03: Cloud Computing Attacks
- ✓ Lesson 04: Cloud Security Tools

For more information, please visit our course page website:
https://www.craw.in/ethical-hacking-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 5: Advanced Penetration Testing

Table of Content

Program Overview

The Advanced Penetration Testing course offered by Craw Security, the foremost and international-standard cybersecurity training institute in India, is designed to provide participants with the skills and knowledge required to perform comprehensive security assessments of IT systems. This intensive program goes beyond the basics, delving into the advanced techniques and tools used by cybersecurity professionals to identify, evaluate, and mitigate vulnerabilities in a variety of environments.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Industry-leading cybersecurity experts with years of experience in penetration testing.
- ✓ Hands-on labs to learn with real-time problem-solving exercises.
- ✓ Cutting-edge curriculum to stay at the forefront of cybersecurity.
- ✓ Flexible Learning Options to choose from.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Penetration Testing

Participants should have a foundational understanding of information security concepts and basic penetration testing skills. Familiarity with Linux and Windows operating systems, networking, and web technologies is recommended.

Target Audience

- ✓ Security Officers
- ✓ Auditors
- ✓ Security Professionals
- ✓ Site Administrators
- ✓ Cybersecurity Professional
- ✓ IT Professional
- ✓ Information Security manager
- ✓ Network Administrator
- ✓ System Administrator
- ✓ Security Analyst
- ✓ Ethical Hackers
- ✓ IT Consultants

Key Learning Outcomes

This Penetration Testing Course will help you:

- ✓ **Penetration Testing:** Perform complex penetration tests in order to assess the security of IT systems.
- ✓ **Vulnerability Assessment:** Determine vulnerabilities in web applications, networks, and systems to compromise and exploit.
- ✓ **Learn Methods To Prevent Data Breach: Formulate all-encompassing methods to safeguard systems from potential breaches.**

- ✓ **Report Making:** Produce and deliver comprehensive reports to stakeholders detailing findings and recommendations.
- ✓ **Ethical and Legal Considerations:** Comprehend the ethical and legal implications of performing penetration tests in accordance with industry regulations and standards.
- ✓ **Defensive Strategies:** Gain knowledge of defensive strategies and tactics in order to mitigate and fix discovered vulnerabilities, thereby fortifying cybersecurity postures as a whole.

Certification Alignment

Our Advanced Penetration Testing is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply advanced penetration testing techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 35 to 40 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations & claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  13. Documentation
  14. Offer Letter
  15. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the **1 Year Cybersecurity Diploma Course** after the completion of this course, which is basically a 12-course bundle of cybersecurity by Craw Security whose maximum courses are accredited to the **FutureSkills Prime, a MeitY — NASSCOM,** Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Introduction to Penetration Testing

- ✓ Lesson 01: What is Advanced Penetration Testing (APT)
- ✓ Lesson 02: Types of Penetration Testing & Areas
- ✓ Lesson 03: Demo Report Understanding

Module 02: In-Depth Scanning

- ✓ Lesson 01 : Scan All Top 20 Ports

Module 03: Exploitation

- ✓ Lesson 01: Basics of Exploitations

Module 04: Command Line Fun

- ✓ Lesson 01: Basic of Linux Commands
- ✓ Lesson 02: Permission Commands

Module 05: Getting Comfortable with Kali Linux

- ✓ Lesson 01: Introduction to Kali Linux

Module 06: Bash Scripting

- ✓ Lesson 01: Introduction to Bash Scripting
- ✓ Lesson 02: Bash Scripting Fundamentals
- ✓ Lesson 03: Tool Creation - Password Generator
- ✓ Lesson 04: Functions

Module 07: Practical Tools

- ✓ Lesson 01: Essential Tools

Module 08: Active Information Gathering

- ✓ Lesson 01: Domain Name System (DNS) Enumerations
- ✓ Lesson 02: Automating Lookups
- ✓ Lesson 03: Domain Name System (DNS) Zone Transfers
- ✓ Lesson 04: NMAP and Masscan
- ✓ Lesson 05: Port Enumeration

Module 09: Passive Information Gathering

- ✓ Lesson 01: Website Recon
- ✓ Lesson 02: Netcraft, Shodan, Email Harvesting
- ✓ Lesson 03: Open Source Intelligence (OSINT) Framework

Module 10: Introduction to Buffer Overflows

- ✓ Lesson 01: Introduction of Buffer Over Flow (BOF)
- ✓ Lesson 02: Basic Data Structure Understanding
- ✓ Lesson 03: Types of Buffer Over Flow BOF

Module 11: Buffer Overflows

- ✓ Lesson 01: Capture the Flag (CTF) on Buffer Over Flow (BOF)

Module 12: Fixing Exploits

- ✓ Lesson 01: Capture the Flag (CTF) on Fixing Exploits

Module 13: Locating Public Exploits

- ✓ Lesson 01: Find Exploits on Google Hacking Database
- ✓ Lesson 02: Find Exploits on GitHub

Module 14: Antivirus Evasion

- ✓ Lesson 01: Introduction to Antivirus Evasion
- ✓ Lesson 02: Working of Antivirus Evasion
- ✓ Lesson 03: Obfuscation Techniques

Module 15: File Transfers

- ✓ Lesson 01: File Transfers Using FTP, Telnet, SSH, PHP, Python

Module 16: Windows Privilege Escalation

- ✓ Lesson 01: Service Exploits - Insecure Service Permissions
- ✓ Lesson 02: Service Exploits - Unquoted Service Path
- ✓ Lesson 03: Service Exploits - Weak Registry Permissions
- ✓ Lesson 04: Service Exploits - Insecure Service Executables
- ✓ Lesson 05: Registry – Auto Runs, etc.

Module 17: Linux Privilege Escalation

- ✓ Lesson 01: Service Exploits
- ✓ Lesson 02: Weak File Permissions - Readable /etc/shadow
- ✓ Lesson 03: Weak File Permissions - Writable /etc/shadow
- ✓ Lesson 04: Weak File Permissions - Writable /etc/passwd
- ✓ Lesson 05: Sudo - Shell Escape Sequences, etc.

Module 18: Password Attacks

- ✓ Lesson 01: Password Spraying and Dictionary Attack

Module 19: Port Redirection and Tunneling

- ✓ Lesson 01: Port Redirection and Tunneling Using Chisel

Module 20: Active Directory Attacks

- ✓ Lesson 01: Introduction of Active Directory (AD)
- ✓ Lesson 02: Basics of Active Directory (AD)
- ✓ Lesson 03: Enumeration of Active Directory (AD)

Module 21: Power Shell Empire

- ✓ Lesson 01: Introduction of Empire
- ✓ Lesson 02: Getting Shell Using Empire

Module 22: Trying Harder: The Labs

- ✓ Lesson 01: Introduction to Penetration Testing Labs
- ✓ Lesson 02: Hands-On Practice

Module 23: Penetration Test Breakdown

- ✓ Lesson 01: Understanding Penetration Test Reports
- ✓ Lesson 02: Debriefing and Recommendations

Module 24: Report Writing

- ✓ Lesson 01: Proof of Concept (POC)
- ✓ Lesson 02: Executive and Management Report
- ✓ Lesson 03: Technical Report For IT and security Department

For more information, please visit our course page website
https://www.craw.in/penetration-testing-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,

Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 6: Cyber Forensics Investigation

Table of Content

Program Overview

The Cyber Forensics Investigation Course offers an in-depth exploration of the techniques and tools required for conducting successful cyber investigations. Covering a wide range of topics from basic concepts to advanced analytical methods, this program combines theoretical knowledge with practical hands-on experience, ensuring students are well-prepared to tackle real-world challenges in the cyber forensics domain.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in cyber forensics and security.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Stay abreast with our latest cyber forensics curriculum under the prime guidance of world-class training professionals.
- ✓ Explore real-world scenarios to understand the complexities of cyber investigations in our Case Studies section.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Cyber Forensics Investigation

- ✓ Basic understanding of computer systems and networks.
- ✓ Familiarity with operating systems such as Windows and Linux.
- ✓ No prior experience in cyber forensics is required, making this course suitable for beginners.

Target Audience

- ✓ IT professionals looking to specialize in cyber forensics.
- ✓ Law enforcement personnel involved in digital investigations.
- ✓ Legal professionals seeking to understand cyber forensics.
- ✓ Students and recent graduates aspiring to build a career in cyber security and forensics, and
- ✓ Anyone who is willing to learn more about cyber forensics investigation.

Key Learning Outcomes

This Cyber Forensics Investigation Course will help you:

- ✓ **Fundamental Understanding of Cyber Forensics:** Gain a solid foundation in the principles of cyber forensics, including the importance of ethical practices, legal considerations, and the role of forensics in cybersecurity.
- ✓ **Digital Evidence Management:** Develop the ability to identify, collect, preserve, and document digital evidence while maintaining its integrity and the chain of custody, ensuring it remains admissible in legal proceedings.

- ✓ **Forensic Analysis Techniques:** Master a range of techniques for the forensic analysis of digital data. This includes the ability to work with various types of digital evidence, such as files, emails, and images, across different platforms and devices.
- ✓ **Use of Forensic Tools and Software:** Become proficient in using leading forensic tools and software to analyze and extract valuable information from digital devices, including computers, smartphones, and networks.
- ✓ **Network and Mobile Forensics:** Acquire specialized knowledge in network forensics, including the analysis of network traffic and logs, as well as mobile device forensics, focusing on the retrieval and analysis of data from smartphones and tablets.
- ✓ **Incident Response and Handling**: Learn to effectively respond to cybersecurity incidents with a forensics-focused approach. Understand how to conduct initial assessments, mitigate threats, and implement strategies to prevent future incidents.
- ✓ **Reporting and Presentation of Findings:** Develop the skills necessary to prepare comprehensive forensic reports and present findings in a clear, concise manner that is understandable to non-technical stakeholders, including legal teams and courtrooms.
- ✓ **Preparation for Certification:** Prepare for globally recognized certifications in cyber forensics, enhancing professional credibility and marketability in the cybersecurity field.

Certification Alignment

Our Cyber Forensics Investigation Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Certification Details -

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply digital forensics techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.

- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  16. Documentation
  17. Offer Letter
  18. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Computer Forensics in Today's World

- ✓ Lesson 01: Understanding the cyber crime
- ✓ Lesson 02: Understanding cyber law
- ✓ Lesson 03: Common attack
- ✓ Lesson 04: Digital evidence
- ✓ Lesson 05: Types Digital forensic
- ✓ Lesson 06: Challenge in cybercrime investigation

Module 02: Computer Forensics Investigation Process

- ✓ Lesson 01: Rules of Digital forensic investigation
- ✓ Lesson 02: Chain of custody, Standard Operating Procedure (SOP)
- ✓ Lesson 03: Lab work, Crime Scene Investigation (CSI), about Raids, Incident response
- ✓ Lesson 04: Checklist to prepare before the investigation.
- ✓ Lesson 05: Precaution during search and seizure
- ✓ Lesson 06: Equipment's and tools software/hardware based

Module 03: Understanding Hard Disks and File Systems

- ✓ Lesson 01: Hard disk design and architecture
- ✓ Lesson 02: Various File systems
- ✓ Lesson 03: Understanding booting process
- ✓ Lesson 04: Window & Linux File system

Module 04: Data Acquisition and Duplication

- ✓ Lesson 01: Understanding the concept of data acquisition
- ✓ Lesson 02: Rules of data acquisitions
- ✓ Lesson 03: Types of data acquisitions
- ✓ Lesson 04: Live & Dead acquisitions
- ✓ Lesson 05: Data acquisition Format
- ✓ Lesson 06: Live and dead acquisition on window & Linux

Module 05: Defeating Anti-Forensics Techniques

- ✓ Lesson 01: Insight of anti-forensic technique
- ✓ Lesson 02: Steganography pros & cons
- ✓ Lesson 03: Types of Steganography
- ✓ Lesson 04: Basic stenographic model
- ✓ Lesson 05: Data sanitization by hardware and software tools
- ✓ Lesson 06: Password cracking technique
- ✓ Lesson 07: Deleted data recovery
- ✓ Lesson 08: Encryption methods

Module 06: Windows Forensics

- ✓ Lesson 01: Methodology of window forensic
- ✓ Lesson 02: Collecting volatile data & non-volatile data
- ✓ Lesson 03: Window forensic analysis
- ✓ Lesson 04: Gathering information by tools
- ✓ Lesson 05: Examine whole file
- ✓ Lesson 06: Examine network information
- ✓ Lesson 07: Examine process information
- ✓ Lesson 08: Examine event logs
- ✓ Lesson 09: Understanding metadata

Module 07: Linux and Mac Forensics

- ✓ Lesson 01: Methodology of Linux forensics
- ✓ Lesson 02: Collecting file system information
- ✓ Lesson 03: Collecting volatile data & non-volatile data
- ✓ Lesson 04: Collecting login history and currently logged in user
- ✓ Lesson 05: Collecting hostname, data, time, uptime data
- ✓ Lesson 06: Gathering network information
- ✓ Lesson 07: Gathering open port information
- ✓ Lesson 08: Analyzing log files in Linux OS
- ✓ Lesson 09: Collecting suspicious information
- ✓ Lesson 10: Collection network information

Module 08: Network Forensics

- ✓ Lesson 01: Introduction of network forensics
- ✓ Lesson 02: Network forensics process
- ✓ Lesson 03: Analyzing different network logs
- ✓ Lesson 04: Log file analysis
- ✓ Lesson 05: Log management challenges
- ✓ Lesson 06: Analyzing network traffics
- ✓ Lesson 07: Gathering info through sniffing
- ✓ Lesson 08: Sniffing tools

Module 09: Investigating Web Forensics

- ✓ Lesson 01: Introduction to web application forensics
- ✓ Lesson 02: Indicators of a web attack
- ✓ Lesson 03: Web application threats
- ✓ Lesson 04: Web attack investigation methodology
- ✓ Lesson 05: Analyzing web logs client/admin

Module 10: Dark Web Forensics

- ✓ Lesson 01: Introduction to dark web forensics
- ✓ Lesson 02: Layers of internet
- ✓ Lesson 03: Tor browser architecture
- ✓ Lesson 04: Investigating tor

Module 11: Cloud Forensics

- ✓ Lesson 01: Cloud models
- ✓ Lesson 02: Cloud computing threats & attack
- ✓ Lesson 03: Cloud forensics
- ✓ Lesson 04: Cloud crimes

Module 12: Investigating Email Crimes

- ✓ Lesson 01: Email server architecture
- ✓ Lesson 02: Understanding email structure
- ✓ Lesson 03: Email crime investigation procedure
- ✓ Lesson 04: Analyzing email

Module 13: Malware Forensics

- ✓ Lesson 01: Introduction to malware forensics
- ✓ Lesson 02: What is malware & what can malware do
- ✓ Lesson 03: Type of malware
- ✓ Lesson 04: Different ways malware can get into a system
- ✓ Lesson 05: Components of malware
- ✓ Lesson 06: Types Malware analysis
- ✓ Lesson 07: Tools for malware analysis
- ✓ Lesson 08: Deep study on malware cases

Module 14: Mobile Forensics

- ✓ Lesson 01: Introduction of mobile forensics
- ✓ Lesson 02: Why do we need mobile forensics
- ✓ Lesson 03: Challenges in mobile forensics
- ✓ Lesson 04: Mobile devices and fundamental component
- ✓ Lesson 05: Mobile phone evidence extraction process
- ✓ Lesson 06: Removable and external data storage
- ✓ Lesson 07: Data Acquisition from iOS Devices & android
- ✓ Lesson 08: Data Acquisition and Analyzing SIM Cards
- ✓ Lesson 09: Examination and analysis
- ✓ Lesson 10: Mobile forensic tools

Module 15: IoT Forensics

- ✓ Lesson 01: Understanding the IoT forensics
- ✓ Lesson 02: Understanding IoT & IoT issues
- ✓ Lesson 03: IOT architecture
- ✓ Lesson 04: Learning objectives of IoT forensics
- ✓ Lesson 05: IoT security problems
- ✓ Lesson 06: IoT attack surface area

For more information, please visit our course page website:
https://www.craw.in/cyber-forensics-investigation-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 7: Web Application Security

Table of Content

Program Overview

The Web Application Security Course offers a wide range of topics related to web pentesting and security for IT Professionals who want to push their IT Skills to another level with the techniques and knowledge of Web Pentesting. This specially organized course is dedicated to clearing the topics on web security infrastructure, troubleshooting methods, security solutions, and laws related to web application security for IT Professionals.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in Linux and as a system administrator.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Cutting-edge curriculum to stay at the forefront of web application security.
- ✓ Receive detailed study guides and resources designed to enhance your learning experience.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.
- ✓ Benefit from our continuous support even after completing the course, ensuring your long-term success.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Web Application Security

A beginner can definitely join this course, however, a basic knowledge of web tech, computing languages, and usual IT concepts can give you a better flow.

Target Audience

- ✓ Developers
- ✓ Security Professionals
- ✓ System Administrators
- ✓ Quality Assurance/ Testers
- ✓ Project Managers
- ✓ IT Managers and Executives
- ✓ Students and Educators
- ✓ Freelancers and Consultants
- ✓ Entrepreneurs and Startups
- ✓ Anyone with an Interest in Cybersecurity

Key Learning Outcomes

A web application security course can greatly benefit IT professionals in several ways:

- ✓ **Understanding Common Threats:** One will get a better knowledge of usual risks & loopholes that affect web apps, such as SQL injection, XSS, CSRF, and IDOR.
- ✓ **Secure Development Practices:** To create web applications with built-in security features and lower the possibility of introducing vulnerabilities throughout the development process, they will master secure coding methods and methodologies.

- ✓ **Effective Testing Methods:** The course will cover a variety of testing approaches and tools, such as vulnerability scanning, penetration testing, and code review procedures that are used for measuring the security posture of online applications.
- ✓ **Incident Response Skills:** IT workers will learn the necessary skills for incident identification, analysis, containment, and recovery in the event of a security incident affecting web applications.
- ✓ **Compliance and Regulations:** They will be aware of the appropriate regulations and laws about online application security compliance, including the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and others.
- ✓ **Risk Management:** IT workers will be able to successfully identify, prioritize, and mitigate security threats by learning risk management principles that are relevant to web application security in this course.
- ✓ **Securing Infrastructure:** To defend web applications from outside threats, IT professionals will learn how to deploy and secure web servers, databases, and other infrastructure components.
- ✓ **Secure Deployment Practices:** To guarantee that web applications are deployed securely, they will learn about secure deployment methods, such as secure configuration management, patch management, and secure deployment pipelines.
- ✓ **Security Awareness Training:** To teach staff members about web application security and best practices for preserving security vigilance, the course may include modules on security awareness training.
- ✓ **Career Advancement:** Gaining expertise in web application security can boost an IT professional's credibility, increase their value to companies, and create prospects for career growth in cybersecurity areas.

Certification Alignment

Web Application Security is a specially customized training program to develop the technical skills and knowledge of IT Professionals who want to follow a career path including cybersecurity & web application security. Moreover, a certification offered by Craw Security will let you strengthen your value in the IT Sector. You can go for the training & certification program by contacting Craw Security.

Certification Details & Criteria

Certification Details -

After the completion of the Web Application Security course, one will be able to sit for the examination. This exam will testify to the skills and knowledge of professionals related to web application security. Moreover, after the examination, professionals will receive a certificate validating their performance for future demonstrations.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  19. Documentation
  20. Offer Letter
  21. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India.

Course Curriculum

Module 01: Introduction

- ✓ Lesson 01: Networking and protocol
- ✓ Lesson 02: Hypertext Transfer Protocol (HTTP) & Hypertext Transfer Protocol Secure (HTTPS)

Module 02: Owasp Top 10

- ✓ Lesson 01: Briefing about various frameworks
- ✓ Lesson 02: Explaining the OWASP top 10

Module 03: Recon for bug hunting

- ✓ Lesson 01: Subdomains enumeration
- ✓ Lesson 02: Domains filtration
- ✓ Lesson 03: Endpoints enumeration
- ✓ Lesson 04: Grepping responses

Module 04: Advanced SQL Injection

- ✓ Lesson 01: Union based SQLI
- ✓ Lesson 02: SQL Authentication Bypass
- ✓ Lesson 03: Error based SQLI
- ✓ Lesson 04: Time-based SQLI
- ✓ Lesson 05: In-band and out-of-band SQLI
- ✓ Lesson 06: Create our own script to automate the process of Blind SQLi

Module 05: Command injection

- ✓ Lesson 01: DVWA source code review
- ✓ Lesson 02: PHP command injection with various functions
- ✓ Lesson 03: Filter bypass

Module 06: Session Management and Broken Authentication Vulnerability

- ✓ Lesson 01: Cookie hijacking
- ✓ Lesson 02: HSTS policy bypass

Module 07: Cross-Site Request Forgery (CSRF)

- ✓ Lesson 01: protection bypass

Module 08: Server Site Request Forgery (SSRF)

- ✓ Lesson 01: Filter bypass
- ✓ Lesson 02: Server-side configuration check

Module 09: Cross-Site Scripting (XSS)

- ✓ Lesson 01: Explaining JavaScript
- ✓ Lesson 02: Reflected JavaScript
- ✓ Lesson 03: Stored JavaScript
- ✓ Lesson 04: DOM-based JavaScript

Module 10: Insecure Direct Object Reference (IDOR)

- ✓ Lesson 01: Universally Unique Identifier (UUID) protection

Module 11: Sensitive Data Exposure and Information Disclose

- ✓ Lesson 01: GIT source code disclosure
- ✓ Lesson 02: Client-side source code review

Module 12: Server Site Template Injection (SSTI)

- ✓ Lesson 01: Template engine Explaining
- ✓ Lesson 02: Various exploitation techniques with various Template engine

Module 13: Multi-Factor Authentication Bypass

- ✓ Lesson 01: Brute-force attacks
- ✓ Lesson 02: Creating wordlists
- ✓ Lesson 03: Logic errors bypass

Module 14: HTTP Request Smuggling

- ✓ Lesson 01: Explaining HTTP/1.1 and HTTP/2
- ✓ Lesson 02: CL-TE attack
- ✓ Lesson 03: TE-CL attack
- ✓ Lesson 04: TE-TE attack

Module 15: External Control of File Name or Path

- ✓ Lesson 01: Whitelisting and blacklisting
- ✓ Lesson 02: Bypassing blacklisting

- ✓ Lesson 03: Brief on regex

Module 16: Local File Inclusion (LFI) and Remote File Inclusion (RFI)

- ✓ Lesson 01: Traversal payload
- ✓ Lesson 02: Bypass WAF
- ✓ Lesson 03: Reading and inclusion difference

Module 17: Directory Path Traversal

- ✓ Lesson 01: Path traversal payload to read the file

Module 18: HTML Injection

- ✓ Lesson 01: Explaining HTML web page
- ✓ Lesson 02: Reflected HTML injection
- ✓ Lesson 03: Stored HTML injection

Module 19: Host Header Injection

- ✓ Lesson 01: Apache Config Brief
- ✓ Lesson 02: Host header Explaining

Module 20: File Upload Vulnerability

- ✓ Lesson 01: POST method explain
- ✓ Lesson 02: Encoded POST method
- ✓ Lesson 03: Various headers related to file upload

Module 21: JWT Token Attack

- ✓ Lesson 01: JWT tokens algorithms
- ✓ Lesson 02: Brute force on HS256 algo
- ✓ Lesson 03: Logic error bypass

Module 22: Flood Attack on Web

- ✓ Lesson 01: XXE vulnerability to cause DOS
- ✓ Lesson 02: Business logic to cause DOS

Module 23: Report Writing

- ✓ Lesson 01: POC (proof of concept)
- ✓ Lesson 02: Executive and Management Report
- ✓ Lesson 03: Technical Report For IT and security Department

For more information, please visit our course page website:
https://www.craw.in/learn-web-application-security-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel

Level 8: Mobile Application Security

Table of Content

Program Overview

The Mobile Application Security Course offered by Craw Security is designed to equip participants with the knowledge and skills required to secure mobile applications against cyber threats. The course covers a wide range of topics, including mobile application architecture, security best practices, and vulnerability assessment.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in network administration and security.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Real-world case studies and practical exercises.
- ✓ Interactive sessions and group discussions.
- ✓ Complete job placement assistance.
- ✓ Cutting-edge curriculum to stay at the forefront of the networking domain.
- ✓ Access Comprehensive course material, resources, and live sessions through both online and offline modes to suit your learning preferences.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Mobile Penetration Testing

Participants are required to have a basic understanding of cybersecurity concepts and mobile application development.

Target Audience

- ✓ IT professionals,
- ✓ Students and recent graduates aiming to build a career in IT and mobile app security domain.
- ✓ Professionals from other fields seeking to transition into IT and mobile application security roles.
- ✓ Mobile application developers with a curiosity about how mobile application systems work and how to manage
- ✓ Anyone who is interested in securing mobile applications.

Key Learning Outcomes

This Mobile Application Security Course will help you:

- ✓ **Understanding Mobile Application Security Concepts:** Participants will gain a comprehensive understanding of the key concepts and principles of mobile application security, including common threats and vulnerabilities.
- ✓ **Identifying and Mitigating Security Vulnerabilities:** Participants will learn how to identify and mitigate common security vulnerabilities in mobile applications, such as insecure data storage, insufficient authentication, and improper session handling.

- ✓ **Implementing Best Practices:** Participants will learn best practices for securing mobile applications, including secure coding practices, encryption techniques, and secure communication protocols.
- ✓ **Conducting Vulnerability Assessments and Penetration Testing:** Participants will learn how to conduct vulnerability assessments and penetration testing on mobile applications to identify and address security weaknesses.
- ✓ **Mobile Device Management (MDM):** Participants will learn about mobile device management (MDM) solutions and how they can be used to enhance the security of mobile applications and devices.
- ✓ **Security Compliance and Regulations:** Participants will gain an understanding of security compliance requirements and regulations relevant to mobile applications, such as GDPR and HIPAA.
- ✓ **Security Incident Response:** Participants will learn how to respond to security incidents involving mobile applications, including incident detection, analysis, and mitigation.
- ✓ **Secure Development Lifecycle:** Participants will learn about the secure development lifecycle (SDLC) for mobile applications and how to integrate security into every phase of the development process.
- ✓ **Mobile Application Security Best Practices:** Participants will learn and apply best practices for securing mobile applications, including secure coding, secure authentication, secure data transmission, and secure storage.
- ✓ **Secure Mobile Application Deployment:** Participants will learn about secure deployment strategies for mobile applications, including app signing, app distribution, and app monitoring.

Certification Alignment

Our Mobile Application Security Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply Mobile Application Security techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.

- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  22. Documentation
  23. Offer Letter
  24. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Introduction to Mobile Penetration Testing

- ✓ Lesson 01: Scope
- ✓ Lesson 02: Methodology
- ✓ Lesson 03: Tools

Module 02: Lab Setup

- ✓ Lesson 01: Kali lab setup
- ✓ Lesson 02: Burp suite setup
- ✓ Lesson 03: Mobile penetration testing lab setup

Module 03: Android Architecture

- ✓ Lesson 01: Layers of Android architecture
- ✓ Lesson 02: Key Components
- ✓ Lesson 03: Application lifecycle
- ✓ Lesson 04: Security Model

Module 04: Apl File structure

- ✓ Lesson 01: Core components
- ✓ Lesson 02: Common file structure patterns
- ✓ Lesson 03: File structure example

Module 05: Reversing App with Apktool

- ✓ Lesson 01: Overviews
- ✓ Lesson 02: Functionality
- ✓ Lesson 03: Installation
- ✓ Lesson 04: Usage
- ✓ Lesson 05: Common usage case

Module 06: Reversing App with MobSf

- ✓ Lesson 01: Overviews
- ✓ Lesson 02: Functionality
- ✓ Lesson 03: Installation and setup
- ✓ Lesson 04: Feature and Capabilities
- ✓ Lesson 05: Scan the app with mobsf

Module 07: Static Analysis

- ✓ Lesson 01: Types of static analysis
- ✓ Lesson 02: Tools and techniques
- ✓ Lesson 03: Benefits
- ✓ Lesson 04: How to perform static analysis

Module 08: Scanning Vulnerability with Drozer

- ✓ Lesson 01: Overviews
- ✓ Lesson 02: Dynamic analysis
- ✓ Lesson 03: Injection attacks
- ✓ Lesson 04: Exploitation

Module 09: Improper Platform Usage

- ✓ Lesson 01: Definition
- ✓ Lesson 02: attacks
- ✓ Lesson 03: Impact
- ✓ Lesson 04: Mitigation
- ✓ Lesson 05: Tools and resources

Module 10: Insecure Data Storage

- ✓ Lesson 01: Definition
- ✓ Lesson 02: Storing passwords in plain text
- ✓ Lesson 03: Unprotected databases
- ✓ Lesson 04: Impact
- ✓ Lesson 05: Mitigation
- ✓ Lesson 06: Tools and resources

Module 11: Insecure Communication

- ✓ Lesson 01: Definition
- ✓ Lesson 02: Unencrypted protocols
- ✓ Lesson 03: Missing or misconfigured SSL/TLS
- ✓ Lesson 04: Impact
- ✓ Lesson 05: Mitigation
- ✓ Lesson 06: Tools and resources

Module 12: Insecure Authentication

- ✓ Lesson 01: Definition
- ✓ Lesson 02: Weak password policies
- ✓ Lesson 03: Lack of multi-factor authentication
- ✓ Lesson 04: Impact
- ✓ Lesson 05: Mitigation
- ✓ Lesson 06: Tools and resources

Module 13: Insufficient Cryptography

- ✓ Lesson 01: Common vulnerability
- ✓ Lesson 02: Impact
- ✓ Lesson 03: Prevention and Mitigation
- ✓ Lesson 04: Continuous monitoring and updates

Module 14: Insecure Authorization

- ✓ Lesson 01: Common vulnerability
- ✓ Lesson 02: Impact
- ✓ Lesson 03: Prevention and Mitigation

Module 15: Client Code Quality

- ✓ Lesson 01: Important of client code quality
- ✓ Lesson 02: Code structure and Organization
- ✓ Lesson 03: Readability and Maintainability

Module 16: Code Tampering

- ✓ Lesson 01: Objective
- ✓ Lesson 02: Techniques
- ✓ Lesson 03: Detection and Prevention
- ✓ Lesson 04: Implications

Module 17: Reverse Engineering

- ✓ Lesson 01: Purpose
- ✓ Lesson 02: Techniques
- ✓ Lesson 03: Tools
- ✓ Lesson 04: Reversing Malware

Module 18: Extraneous Functionality

- ✓ Lesson 01: Security risks
- ✓ Lesson 02: User Experience (UX) issues
- ✓ Lesson 03: Code review and refactoring
- ✓ Lesson 04: Automated Analysis tools

Module 19: SSL Pinning

- ✓ Lesson 01: Public key Pinning
- ✓ Lesson 02: Certificate Pinning
- ✓ Lesson 03: Benefits of SSL pinning
- ✓ Lesson 04: Certificate Authority (CA)

Module 20: Intercepting the Network Traffic

- ✓ Lesson 01: Packet Capture
- ✓ Lesson 02: Network sniffing
- ✓ Lesson 03: Protocol Analysis
- ✓ Lesson 04: Traffic Decryption

Module 21: Dynamic Analysis

- ✓ Lesson 01: Introduction to Dynamic Analysis
- ✓ Lesson 02: How to perform dynamic analysis
- ✓ Lesson 03: Dynamic Debugging

- ✓ Lesson 04: Dynamic Decomplication

Module 22: Report Preparation

- ✓ Lesson 01: Consider the objective of the report
- ✓ Lesson 02: The test compiles a comprehensive report
- ✓ Lesson 03: Detailing their findings of vulnerability

Module 23: IOS Penetration: Basics

- ✓ Lesson 01: Introduction to IOS Penetration testing
- ✓ Lesson 02: IOS structure
- ✓ Lesson 03: How to secure you application

Module 24: Report Writing

- ✓ Lesson 01: Proof of Concept (POC)
- ✓ Lesson 02: Executive and Management Report
- ✓ Lesson 03: Technical Report For IT and security Department

For more information, please visit our course page website:
https://www.craw.in/mobile-application-security-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 9: IoT Pentesting

Table of Content

Program Overview

The IoT Pentesting Course at Craw Security is designed to equip cybersecurity enthusiasts with the necessary skills to identify and mitigate vulnerabilities in IoT devices and networks. This hands-on course covers the latest techniques and tools used in IoT penetration testing, preparing students to secure IoT systems against cyber threats effectively. Apart from that, this course lays the foundation for aspiring IT professionals by providing them with essential knowledge of security principles.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading and experienced instructors with extensive industry knowledge.
- ✓ Practical, hands-on training on real IoT devices and networks.
- ✓ Comprehensive coverage of IoT security concepts and methodologies.
- ✓ Access to cutting-edge tools and techniques used in IoT pentesting.
- ✓ Interactive sessions and group activities to enhance the learning experience.
- ✓ Career guidance and job placement assistance.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of Internet of Things Pentesting Course

Participants should have a basic understanding of networking and cybersecurity concepts. Familiarity with Linux operating systems and programming languages such as Python would be beneficial but not mandatory.

Target Audience

- ✓ Cybersecurity professionals
- ✓ Network administrators
- ✓ IT professionals
- ✓ Ethical hackers
- ✓ Security enthusiasts, and
- ✓ Anyone who is willing to enhance one's knowledge and seeking entry to this IoT domain in the cybersecurity trajectory.

Key Learning Outcomes

This IoT Pentesting Course will assist you in the following activities:

- ✓ **Understanding IoT Security Fundamentals:** Gain a deep understanding of the fundamental concepts and principles of IoT security, including the unique challenges and vulnerabilities associated with IoT devices and networks.

- ✓ **Identifying IoT Vulnerabilities**: Learn how to identify common vulnerabilities in IoT devices and networks, such as insecure communication protocols, weak authentication mechanisms, and lack of secure update mechanisms.
- ✓ **Conducting IoT Penetration Testing:** Develop the skills to conduct penetration tests on IoT systems, including discovering and exploiting vulnerabilities to assess the security posture of IoT devices and networks.
- ✓ **Implementing IoT Security Measures:** Learn how to implement security measures to protect IoT devices and networks, including secure configuration, data encryption, and access control mechanisms.
- ✓ **Analyzing IoT Security Data:** Learn how to analyze and interpret IoT security data, including logs, network traffic, and device behavior, to identify and mitigate security threats.

Certification Alignment

Our IoT Pentesting Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Certification Details -

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply IoT Pentesting techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.

- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  25. Documentation
  26. Offer Letter
  27. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Overview of IOT Why IOT is so important?

- ✓ Lesson 01: What is Internet of Things (IOT)?
- ✓ Lesson 02: Why is Internet of Things (IoT) important?

Module 02: Internet of Things (IoT) Pentesting

- ✓ Lesson 01: OWASP TOP 10
- ✓ Lesson 02: What is Internet of Things (IoT) Pentesting
- ✓ Lesson 03: What is Internet of Things (IoT) Security?
- ✓ Lesson 04: Previous Internet of Things (IoT) Security Hacks
- ✓ Lesson 05: Internet of Things (IoT) Vulnerabilities
- ✓ Lesson 06: Internet of Things (IoT) Pentesting Methodology

Module 03: Introduction of IoT

- ✓ Lesson 01: How does Internet of Things (IoT) work?
- ✓ Lesson 02: Advantages & Disadvantage's

Module 04: Introduction to Sensor Network

- ✓ Lesson 01: Explanation
- ✓ Lesson 02: Use of sensor with example

Module 05: Communication Models in Internet of Things (IoT)

- ✓ Lesson 01: Explanation

Module 06: Frequency

- ✓ Lesson 01: What is radio wave?
- ✓ Lesson 02: Radio Frequency Spectrum band
- ✓ Lesson 03: Explanation

Module 07: Wireless protocol

- ✓ Lesson 01: Difference type of protocols
- ✓ Lesson 03: Explanation

Module 08: Comparing web and IOT protocols

- ✓ Lesson 01: Explanation

Module 09: SPI, UART, I2C

- ✓ Lesson 01: Explanation

Module 10: Firewall

- ✓ Lesson 01: Explanation

Module 11: ARDUINO

- ✓ Lesson 01: Explanation with practical

Module 12: Raspberry

- ✓ Lesson 01: Explanation with practical

Module 13: Introduction to Mobile app platform

- ✓ Lesson 01: Explanation

Module 14: Flipper zero

- ✓ Lesson 01: Explanation with practical

Module 15: Firmware

- ✓ Lesson 01: Usage of firmware for penetester
- ✓ Lesson 02: What is it?
- ✓ Lesson 03: Extracting squashfs file system from file system
- ✓ Lesson 04: How to obtain firmware?
- ✓ Lesson 05: Explanation with practical

Module 16: Analysing IOT Hardware

- ✓ Lesson 01: Explanation

Module 17: SDR (software defined radio)

- ✓ Lesson 01: Explanation with practical

Module 18: Conceiving a new IOT product- Product Requirement document for IoT

- ✓ Lesson 01: Explanation

Module 19: Basic Intro Cloud Iaas Paas Saas-IoT data, platform and software as a service revenue

- ✓ Lesson 01: Explanation

Module 20: Basic Introduction of ICS

- ✓ Lesson 01: Explanation

For more information, please visit our course page website:
https://www.craw.in/learn-internet-of-things-iot-pentesting-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 10: Endpoint Security

Table of Content

Program Overview

The Endpoint Security Course at Craw Security provides comprehensive training on protecting endpoints such as desktops, laptops, and mobile devices from cyber threats. Participants will learn the latest techniques and best practices for securing endpoints in today's dynamic threat landscape. Moreover, learners will have the benefit of learning the best endpoint security practices in this international-standard training program offered under the promising guidance of several instructors having 10+ years of quality experience.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in network administration and security.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Cutting-edge curriculum to stay at the front of the cybersecurity domain.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of End Point Security

Participants should have a basic understanding of cybersecurity concepts and familiarity with operating systems like Windows and Linux.

Target Audience

- ✓ Cybersecurity professionals,
- ✓ IT professionals,
- ✓ Network administrators, and
- ✓ Anyone interested in enhancing their knowledge of endpoint security.

Key Learning Outcomes

This Endpoint Security Course will help you:

- ✓ **Un Understanding of Endpoint Security Fundamentals:** Gain a comprehensive understanding of the basic concepts and principles of endpoint security, including the types of threats and vulnerabilities faced by endpoints.
- ✓ **Endpoint Security Technologies and Tools:** Learn about the various technologies and tools used in endpoint security, such as antivirus software, firewalls, and intrusion detection systems, and how to effectively use them to protect endpoints.

- ✓ **Endpoint Vulnerability Assessment and Management:** Learn how to assess and manage vulnerabilities in endpoints, including identifying vulnerabilities, prioritizing them based on risk, and implementing mitigation measures.

- ✓ **Endpoint Security Best Practices:** Understand the best practices for securing endpoints, including security configurations, patch management, and data protection measures.
- ✓ **Endpoint Security Policy and Compliance**: Learn about endpoint security policies and compliance requirements, including how to develop and implement effective security policies and ensure compliance with relevant regulations.
- ✓ **Incident Response and Recovery:** Gain the skills to effectively respond to and recover from endpoint security incidents, including identifying and containing threats, mitigating the impact of incidents, and restoring affected endpoints to a secure state.
- ✓ **Hands-on Experience:** Get hands-on experience with real-world scenarios and practical lab sessions, allowing you to apply your knowledge and skills in a simulated environment.
- ✓ **Certification Preparation:** Prepare for industry-recognized certifications in endpoint security, enhancing your credibility and career prospects in the cybersecurity field.

Certification Alignment

Our Endpoint Security Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Certification Details -

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply endpoint security techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.

- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  28. Documentation
  29. Offer Letter
  30. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Implementing Internet Security Antivirus

- ✓ Lesson 01: Importance of Internet Security
- ✓ Lesson 02: Malware
- ✓ Lesson 03: Antivirus protection
- ✓ Lesson 04: Internet security tips to know

Module 02: Multi Factor Authentication (MFA)

- ✓ Lesson 01: Three Main Types of MFA Authentication Methods
- ✓ Lesson 02: How Multi-Factor Authentication Works
- ✓ Lesson 03: Multi Factor Authentication (MFA) Examples
- ✓ Lesson 04: Two-Factor Authentication (2FA)
- ✓ Lesson 05: Adaptive Authentication or Risk-based Authentication

Module 03: Mobile Device Management For Industry

- ✓ Lesson 01: What is mobile device management
- ✓ Lesson 02: How mobile device management works
- ✓ Lesson 03: Application security
- ✓ Lesson 04: Identity and access management (IAM)
- ✓ Lesson 05: Endpoint security
- ✓ Lesson 06: BYOD mobile device management

Module 04: Data Loss Prevention (DLP)

- ✓ Lesson 01: Data Loss Prevention (DLP) Basics
- ✓ Lesson 02: Who use Data Loss Prevention (DLP)
- ✓ Lesson 03: Why we need Data Loss Prevention (DLP)
- ✓ Lesson 04: How does Data Loss Prevention (DLP) works
- ✓ Lesson 05: Data Loss Prevention (DLP) solutions

Module 05: Security Information and Event Management

- ✓ Lesson 01: Introduction

- ✓ Lesson 02: Indexing
- ✓ Lesson 03: Analysis logs and Alerts
- ✓ Lesson 04: Dashboard creation
- ✓ Lesson 05: Event Type

Module 06: Advanced Persistent Threat (APT) Attack

- ✓ Lesson 01: What is Advanced Persistent Threat (APT) Attack
- ✓ Lesson 02: Advanced persistent threat (APT) progression
- ✓ Lesson 03: Advanced Persistent Threat (APT) security measures
- ✓ Lesson 04: Application and domain whitelisting
- ✓ Lesson 05: Access control

Module 07: Mitre Attack Framework

- ✓ Lesson 01: Introduction to Mitre
- ✓ Lesson 02: Matrix
- ✓ Lesson 03: Tactics
- ✓ Lesson 04: Techniques and Sub-Techniques
- ✓ Lesson 05: Mitigation

Module 08: Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)

- ✓ Lesson 01: Endpoint Detection and Response (EDR) / Extended Detection and Response (XDR) Introduction
- ✓ Lesson 02: Common Endpoint Detection and Response (EDR) / Extended Detection and Response (XDR) Products
- ✓ Lesson 03: Kill Processes
- ✓ Lesson 04: Managing Endpoints with EDR/XDR
- ✓ Lesson 05: Use Case with SIEM, EDR and XDR

Module 09: Unified Threat Management (UTM)

- ✓ Lesson 01: Introduction to Unified Threat Management (UTM)
- ✓ Lesson 02: Feature of Unified Threat Management (UTM)
- ✓ Lesson 03: Benefit of using Unified Threat Management (UTM) Solution

Module 10: Firewall

- ✓ Lesson 01: Introduction
- ✓ Lesson 02: Reason to have a firewall
- ✓ Lesson 03: Modern Firewall Design
- ✓ Lesson 04: Common Firewall Technologies
- ✓ Lesson 05: Next Generation Firewall

Module 11: ISO 27001

- ✓ Lesson 01: Introduction to ISO
- ✓ Lesson 02: Updation in ISO 27001
- ✓ Lesson 03: Clauses
- ✓ Lesson 04: Controls

For more information, please visit our course page website:
https://www.craw.in/learn-end-point-security-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 11: AWS Associate

Table of Content

Program Overview

The AWS Associate Course from the House of Amazon Web Services at Craw Security is structured to equip participants with the skills and knowledge required to become proficient in AWS cloud technologies. The course covers a wide range of topics, including cloud computing concepts, AWS services, security best practices, and more.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from the best experts in the field who have a lot of experience with security and cloud management.
- ✓ Real-life problem-solving situations are used in hands-on tasks to help you learn.
- ✓ Cutting-edge curriculum to maintain a position at the top of the cloud area.
- ✓ You can access course materials and live meetings in two different ways, depending on how you like to learn.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of AWS Associate

Participants are required to have a basic understanding of cloud computing concepts and some experience with AWS services. A fundamental knowledge of networking and security concepts is also beneficial.

Target Audience

- ✓ IT professionals,
- ✓ System administrators,
- ✓ Developers,
- ✓ The individuals preparing for the AWS Certified Solutions Architect – Associate exam, and
- ✓ Anyone looking to build a career in cloud computing.

Key Learning Outcomes

This AWS Associate Course will help you:

- ✓ **Understanding of Cloud Computing:** Develop a deep understanding of cloud computing concepts, including the benefits, architecture, and deployment models.
- ✓ **AWS Services Proficiency:** Gain practical experience with a wide range of AWS services, such as EC2, S3, RDS, and IAM, and learn how to leverage them to build scalable and secure solutions.
- ✓ **Architectural Design Skills:** Learn how to design resilient and scalable architectures on AWS, considering factors such as performance, reliability, and cost optimization.

- ✓ **Security Best Practices:** Understand best practices for securing AWS environments, including data encryption, access control, and compliance with regulatory requirements.

- ✓ **Application Deployment and Management:** Learn how to deploy and manage applications on AWS, including monitoring, troubleshooting, and optimizing performance.
- ✓ **Preparation for AWS Certification:** Prepare for the AWS Certified Solutions Architect – Associate exam, which validates expertise in designing and deploying scalable systems on AWS.
- ✓ **Hands-on Experience:** Gain practical, hands-on experience through labs and projects that simulate real-world scenarios, ensuring you are ready to apply your skills in a professional setting.
- ✓ **Career Advancement:** Enhance your career prospects in cloud computing and IT by acquiring in-demand skills and a globally recognized certification from AWS.

Certification Alignment

Our AWS Associate Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Certification Details -

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply basic cloud-related tactics in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.

- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.

- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  31. Documentation
  32. Offer Letter
  33. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Designing Highly Available, Cost-effective, scalable systems

- ✓ Lesson 01: Planning and Design
- ✓ Lesson 02: Monitoring and Logging
- ✓ Lesson 03: Hybrid IT Architectures
- ✓ Lesson 04: Elasticity and Scalability

Module 02: Implementation and Deployment

- ✓ Lesson 01: Amazon EC2
- ✓ Lesson 02: Amazon S3
- ✓ Lesson 03: Amazon Web Service Cloud Formation
- ✓ Lesson 04: Amazon Web Service VPS
- ✓ Lesson 05: Amazon Web Service IAM

Module 03: Data Security

- ✓ Lesson 01: AWS IAM(Identify and Access Management)
- ✓ Lesson 02: Amazon Web Service VPC
- ✓ Lesson 03: Encryption Solutions
- ✓ Lesson 04: Cloud watch logs
- ✓ Lesson 05: Disaster Recovery
- ✓ Lesson 06: Amazon Route 53
- ✓ Lesson 07: AWS Storage Gateway
- ✓ Lesson 08: Disaster Recovery
- ✓ Lesson 09: Amazon Web Service Import/Export

Module 04: Troubleshooting

- ✓ Lesson 01: Check AWS services Health
- ✓ Lesson 02: Monitor and Optimize resource usage

For more information, please visit our course page website
https://www.craw.in/aws-associate-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel

Level 12: AWS Cloud Security

Table of Content

Program Overview

The AWS Security Course from the House of Amazon Web Services at Craw Security is structured to provide participants with comprehensive knowledge and practical skills to secure AWS environments. The course covers various aspects of security including identity and access management, data protection, monitoring, and incident response in AWS. In this course, working cybersecurity individuals will get a chance to hone their current cloud computing technologies with a decent upgrade of various knowledge-boosting capabilities under the promising guidance of varied cloud professionals with many years of quality experience.

Program Features

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from the best experts in the field who have a lot of experience with security and cloud management.
- ✓ Real-life problem-solving situations in the shape of case studies are used in hands-on tasks to help you learn.
- ✓ Cutting-edge curriculum to maintain a position at the top of the cloud area.
- ✓ You can access learning resources and live meetings in two different ways, depending on how you like to learn.
- ✓ A good value in the preparation of certification content with a decent training module under prime supervision of valuable instructors cum cloud experts.

Delivery Mode

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of AWS Cloud Security

Participants should have a basic understanding of AWS services and cloud computing concepts. Knowledge of security fundamentals is recommended but not mandatory.

Target Audience

- ✓ IT professionals,
- ✓ Security analysts,
- ✓ Cloud architects,
- ✓ System administrators,
- ✓ The individuals preparing for the AWS Security Course exam, and
- ✓ Anyone looking to build and enhance one's knowledge parameters in cloud security.

Key Learning Outcomes

This AWS Security Course will assist you in obtaining some of the best practices related to the AWS Security Course::

- ✓ **Understanding AWS Security:** Gain a comprehensive understanding of security best practices for AWS environments.
- ✓ **Implementing Security Controls:** Learn how to implement and configure security controls to protect AWS resources.

- ✓ **Data Protection:** Learn how to secure data in transit and at rest using encryption and other security measures.
- ✓ **Monitoring and Auditing:** Learn how to monitor and audit AWS environments to detect and respond to security threats.
- ✓ **Incident Response:** Develop the skills to respond to security incidents in AWS, including identifying, containing, and mitigating threats.
- ✓ **Security Best Practices:** Learn and apply security best practices for AWS services and configurations.
- ✓ **Compliance:** Understand compliance requirements and learn how to ensure AWS environments meet these standards.
- ✓ **Hands-on Experience:** Gain practical, hands-on experience through labs and projects to reinforce learning and skills development.

Certification Alignment

Our AWS Security Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification Details & Criteria

Certification Details -

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply advanced techniques related to AWS Security in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the Exam

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security Certification Criteria

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with 1 Year Cyber Security Course

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.

- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  34. Documentation
  35. Offer Letter
  36. Joining Date/ Timeline of Joining

What to Choose After this Course

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course Curriculum

Module 01: Overview of Security in Amazon Web Service (AWS)

- ✓ Lesson 01: Amazon Web Service (AWS) shared security responsibility model
- ✓ Lesson 02: Amazon Web Service (AWS) account security features
- ✓ Lesson 03: Amazon Web Service (AWS) Security services

Module 02: AWS Identity and Access Management

- ✓ Lesson 01: IAM Authentication
- ✓ Lesson 02: IAM Authorization
- ✓ Lesson 03: Aws Organization
- ✓ Lesson 04: SSO (Single SignOn)

Module 03: AWS Virtual Private Cloud

- ✓ Lesson 01: Virtual Private Cloud (VPC) Peering Connection
- ✓ Lesson 02: Virtual Private Cloud (VPC) Flow Logs
- ✓ Lesson 03: Virtual Private Network (VPN) Connection

Module 04: Data Security in AWS

- ✓ Lesson 01: Encryption and decryption fundamental
- ✓ Lesson 02: Amazon Web Service (AWS) KMS
- ✓ Lesson 03: Amazon Macie

Module 05: Securing Servers in Amazon Web Service (AWS)

- ✓ Lesson 01: EC2 Security
- ✓ Lesson 02: Amazon Inspector
- ✓ Lesson 03: Amazon Web Service (AWS) Shield

Module 06: Edge Security in AWS

- ✓ Lesson 01: Amazon Web Service (AWS) Web Application Firewall (WAF)
- ✓ Lesson 02: Amazon Cognito
- ✓ Lesson 03: Amazon Web Service (AWS) Guard Duty
- ✓ Lesson 04: Security Hub

Module 07: Monitoring in AWS

- ✓ Lesson 01: Amazon Web Service (AWS) Cloud watch
- ✓ Lesson 02: Monitoring Amazon EC2

Module 08: Logging and Auditing in AWS

- ✓ Lesson 01: Amazon Web Service (AWS) Cloud Watch Logs
- ✓ Lesson 02: Amazon Web Service (AWS) Cloud Trail
- ✓ Lesson 03: Amazon Web Service (AWS) Artifact
- ✓ Lesson 04: Amazon Web Service (AWS) Config
- ✓ Lesson 05: Amazon Web Service (AWS) Trusted Advisor

For more information, please visit our course page website:
https://www.craw.in/aws-security-training-and-certification-course-in-delhi/

Note* If you want to take this Single Course then Training Price will be different from the Diploma Course Price

Contact us

Craw Cyber Security Private Limited, India (Head Office)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel