



Cyber Forensics Analysis and Investigation Program



CYBERYAAN

TRAINING & CONSULTANCY

Module 1 : Networking Essentials

1.1 : Introduction to Computer Network

1.2 : Network Topologies and Type

1.3 : IP Addressing

1.4 : Subnet Mask, Subnetting and CIDR

1.5 : VLSM, Wild Card, Summarization

1.6 : Networking Models

1.7 : OSI Model

1.8 : Networking Device, Cabling, Network Simulator Tools



CYBERYAAN

TRAINING & CONSULTANCY

Module 1 : Networking Essentials

1.9 : ARP and ICMP

1.10 : Packet Flow

1.11 : Routing – Static and Dynamic

1.12 : Static Routing – Next HOP IP and Exit Interface

1.13 : Dynamic Routing - RIP, EIGRP and OSPF

1.14 : Remote Service Configuration

1.15 : DHCP Configuration

1.16 : ACLs



CYBERYAAN

TRAINING & CONSULTANCY

Module 1 : Networking Essentials

1.17 : Switching

1.18 : L2 Protocols - CDP, VLN, STP, DTP, VTP

1.19 : Ether Channel

1.20 : Port Security



CYBERYAAN

TRAINING & CONSULTANCY

Module 2 : Kali - Linux

2.1 : Introduction to linux

2.2 : Setting Up Lab

2.3 : Exploring Kali

2.4 : Sudo Overview

2.5 : Navigating the file system

2.6 : Basic Commands

2.7 : Creating, Viewing and Editing text Files

2.8 : Managing users and Group



CYBERYAAN

TRAINING & CONSULTANCY

Module 2 : Kali - Linux

2.9 : File Privileges and Permissions

2.10 : Linux Networking

2.11 : Process Management

2.12 : Services and Demos

2.13 : Log Analysis

2.14 : Archiving Files

2.15 : Debain Package Management

2.16 : Road Ahead – Towards Penetration Testing



CYBERYAAN

TRAINING & CONSULTANCY

Module 3 : Python Programming

3.1 : Introduction

3.2 : Set Up

3.3 : Variables and data types

3.4 : Numbers

3.5 : String formatting

3.6 : Booleans and Operators

3.7 : Tuples

3.8 : Lists



CYBERYAAN

TRAINING & CONSULTANCY

Module 3 : Python Programming

3.9 : Dictionaries

3.10 : Sets

3.11 : Conditionals

3.12 : Loops

3.13 : Reading and Writing

3.14 : User Input

3.15 : Exception and Error Handling

3.16 : Comprehensions



CYBERYAAN

TRAINING & CONSULTANCY

Module 3 : Python Programming

3.17 : Functions and Code Resuse

3.18 : Lambdas

3.19 : The Python Package Manner

3.20 : Python Virtual Environment

3.21 : Introduction to Sys

3.22 : Introduction to request

3.23 : Introduction to pwntools

3.24 : Projects



CYBERYAAN

TRAINING & CONSULTANCY

Module 4 : Ethical Hacking

4.1 : Networking Refresher

4.2 : Linux Refresher

4.3 : Introduction to Information Security

4.4 : Introduction to Ethical Hacking

4.5 : Foot Printing / Information Gathering

4.6 : Scanning

4.7 : Enumeration

4.8 : Vulnerabilities Analysis



CYBERYAAN

TRAINING & CONSULTANCY

Module 4 : Ethical Hacking

4.9 : System Hacking

4.10 : Malware and Threats

4.11 : Sniffing

4.12 : Social Engineering

4.13 : Denial of Service

4.14 : Session Hijacking

4.15 : IDS, IPS and Firewalls

4.16 : Hacking Web Servers



CYBERYAAN

TRAINING & CONSULTANCY

Module 4 : Ethical Hacking

4.17 : Hacking Web Applications

4.18 : SQL Injection

4.19 : Hacking Wireless Network

4.20 : Hacking Mobile Platforms

4.21 : Introduction to IOT

4.22 : Introduction to cloud computing

4.23 : Cryptography and Steganography



CYBERYAAN

TRAINING & CONSULTANCY

Module 5 : Digital Forensics

- 5.1 : Introduction to computer Forensics
- 5.2 : Digital Investigation and analysis
- 5.3 : Concepts of Hard disk and File System
- 5.4 : Evidence Duplication and Extraction
- 5.5 : Counter Anti forensics Strategies
- 5.6 : Windows forensics Analysis
- 5.7 : Linux Forensics Analysis
- 5.8 : Mac Forensics Analysis



CYBERYAAN

TRAINING & CONSULTANCY

Module 5 : Digital Forensics

5.9 : Network Forensics Analysis

5.10 : Web Breach Forensics

5.11 : Dark Web forensics Analysis

5.12 : Data repository forensics

5.13 : Cloud Forensics and Analysis

5.14 : Email forensics and Investigation

5.15 : Malware Analysis

5.16 : Mobile Forensics and Analysis

5.17 : IOT Forensics and Analysis



CYBERYAAN

TRAINING & CONSULTANCY

Module 6 : Threat Hunting

6.1 : Introduction to Threat Hunting

6.2 : Introduction to Malware

6.3 : Mitre

6.4 : Cyber Threats

6.5 : Cyber Kill Chain Methodology

6.6 : Event IDS, Logging and Siem

6.7 : Requirements, Planning, direction and review

6.8 : Data Collection and Processing



CYBERYAAN

TRAINING & CONSULTANCY

Module 6 : Threat Hunting

6.9 : Data Analysis

6.10 : Intelligence Reporting



CYBERYAAN

TRAINING & CONSULTANCY

Module 7 : Incident Handler and Reporting

- 6.1 : Introduction and Process to Incident Handling and Response
- 6.2 : Proactive digital investigation preparedness and First Response
- 6.3 : Cyber Threat Handling and Mitigation
- 6.4 : Email Security Management
- 6.5 : Network Security Incident Response and Countermeasure
- 6.6 : Web App threat Response and Remediation
- 6.7 : Cloud Security Incident Management
- 6.8 : Insider risk management and responses



CYBERYAAN

TRAINING & CONSULTANCY

Training Duration : 200 to 220 Hrs

Training Mode : Online and Offline

Important Notes :

1. Laptop is Mandatory
2. Fees is 60000 + 18% Gst (CEH Practical / CHFI Exam Voucher Included)
Choose Any One
3. Instalment Date is before of 10th of Every Month.
4. Late Fees is applicable – 1000



CYBERYAAN

TRAINING & CONSULTANCY

Contact Us

1/4, Single Storey, 3rd Floor, Near Vishal Mega Mart, Tilak Nagar, New Delhi –
110018

Follows

Instagram : @_cyberyaan_

LinkedIn : Cyberyaan Training and Consultancy