Overview

—

The Advanced Diploma in Information Security (ADIS) offers a comprehensive curriculum that spans a wide range of cybersecurity domains. Throughout the course of one year, you will gain practical knowledge and hands-on experience in the following areas:

- Information Security vs Cybersecurity
- Fundamentals of Linux
- Networking Principles
- Microsoft Server Essentials
- Offensive Security Tactics
- Network Pentesting
- Web Application Pentesting
- Wireless Pentesting

- Active Directory Pentesting
- Android Pentesting
- Security Operation Center Operations
- Python Programming
- ISO 9001 and Cybersecurity
- Capture The Flag Challenges
- Global Certification Preparation
- Internship and Introduction to Bug Bounty

Our program focuses on delivering a holistic approach to cybersecurity education, ensuring that you are well-equipped to address the challenges and opportunities presented by the rapidly evolving digital landscape. Whether you are beginning your journey in cybersecurity or seeking to advance your existing skills, the Advanced Diploma in Information Security will empower you to emerge as a proficient cybersecurity professional, ready to tackle the complex security issues of today and tomorrow.

Embark on Your Cybersecurity Journey Today and Shape a Secure Tomorrow.

OVERVIEW

Modules

01

EXPLORING CYBERSECURITY

- Information Security vs Cybersecurity

- Cybersecurity Basic Terminologies

- CIA Triad

- Cyberkill Chain

- Phases of Hacking

- Phases of Penetration Testing

- Ethics & Legal Considerations in Cybersecurity

- Security Policies,Standards & Best Practices

Modules

02

DISCOVERING LINUX

- Windows vs Linux
- History & Evolution of Linux
- Linux Distributions
- Linux Installation & Configuration
- File System Hierarchy & Directory Structure
- File & Directory Permissions
- Linux Basic Commands
- File System Maintenance & Troubleshooting
- Linux Shell Scripting
- Virtualization & Containers

03

NETWORKING UNVEILED

- Types of Computer Networks
- Networking Devices
- Networking Topologies
- Transmission Media Standards & OSI Reference Model
- Networking Protocols
- Routing & Switching
- Troubleshooting

Modules

MICROSOFT FUNDAMENTALS

04

- Configuring Windows Server
- Active Directory Domain Services
- ADDS Account Creation & Management
- GPO Management & DHCP
- Windows Server Security & Encryption
- RAID Levels
- Kerberos

SECURITY OFFENSIVE TACTICS

05

- Understanding the Role of Offensive Security in Information Security
- Common Attack Vectors & Methodologies
- Basic Tools & Techniques
- Reconnaissance & Footprinting
- Scanning & Enumeration
- Gaining Access
- Maintaining Access
- Clearing Tracks
- Social Engineering
- Phishing Attacks

Modules

NETWORK PENTESTING

06

- Reconnaissance & Enumeration Techniques
- Osint & Social Engineering
- Target Discovery
- Enumeration Techniques
- Vulnerability Identification
- Service & System Exploitation
- Protocol Attacks
- Evasion Techniques
- Wireshark
- Spoofing

WEB APPLICATION PENTESTING

07

- Introduction to Web Application
- Fundamentals of HTTP
- Configuring Web Application
- Importance of Web Application Security
- Web Application Security Frameworks
- Methodology
- Planning Phase
- Attack/Execution Phase
- Post-Execution Phase
- Web Application Vulnerabilities
- Burp Suite for Pentesters
- Vulnerability Scanning

Modules

- Password Attacks

- SQL Injection

- XSS

- JWT Attacks

- CSRF

- SSRF

- OS Command Injection

- Directory Traversal

- Authentication Vulnerabilities

- Business Logic Vulnerabilities

- File Upload Vulnerabilities

- Information Disclosure Vulnerabilities

- Fuzzing & Directory Enumeration

- Multiple Ways to Banner Grabbing

- Web Shells & Reverse Shells

WIRELESS PENTESTING

- Wireless Reconnaissance

- Identify Wireless Network

- Vulnerability Research

- Exploitation

- Remediation & Security Controls

- Making Wireless Hacking Device

- Detecting Hidden SSID

- Aircrack-ng

- Wifi Pumpkin3

08

Modules

ACTIVE DIRECTORY PENTESTING

09

- Overview of Active Directory
- Importance of Active Directory Security
- Types of Attacks Against Active Directory
- Reconnaissance & Information Gathering
- Attacking the Active Directory
- Kerberoasting
- Asreproasting Attacks Using Impacket
- Pass-the-hash Attacks
- Maintaining Access

ANDROID PENTESTING

10

- Android Intro and Security Architectures
- Android Lab Setup
- Android Static Analysis
- Android Dynamic Analysis
- Decompiling Android Apks Using Jadx and Mobsf
- Exploiting Input Validation Flaws
- Testing for Insecure Data Storage
- Testing for Authentication & Authorization Flaws
- Testing Android Apks using Drozer
- Frida Tools
- Objection

Modules

SECURITY OPERATION CENTER

11

- What is Security Operation Center
- Security Information & Event Management
- Architecture & Components
- Logging Process
- SIEM Sizing
- SIEM Solutions
- Managed SIEM
- Splunk
- Log Creating using Use Cases
- Incident Response Team
- Cyber Threat Intelligence
- Indicators of Compromise

PYTHON PROGRAMMING 101

12

- Introduction to Python
- Variables & Data Structures
- Control Flow & Loops
- Function & Modules
- File Handling
- Error Handling & Exception Handling
- Object Oriented Programming

Modules

- Introduction to Libraries and Modules

- Working With APIs

- Introduction to Databases

ISO 9001

13

- Introduction to ISO 9001 & Cybersecurity

- Cybersecurity Frameworks & Standards

- Risk Management & Cybersecurity

- Information Security Management System(ISMS)

- Cybersecurity Controls & Measures

- Incident Response & Business Continuity Planning

- Employee Awareness & Training

- Supply Chain Management & Cybersecurity

CAPTURE THE FLAG

14

- Introduction to Capture the Flag

- Web Exploitation

- Reverse Engineering

- Cryptography & Steganography

- Forensics & Digital Investigations

- OSINT

- CTF Tools & Resources

GLOBAL CERTIFICATION

INTERNSHIP & INTRODUCTION TO BUG BOUNTY

Career Opportunities !!

In today's digitally evolving world, the demand for cybersecurity expertise has reached unprecedented heights. The Advanced Diploma in Information Security not only meets this demand but propels you into a realm of unparalleled opportunities that extend far beyond the horizon. With meticulous precision and guidance from industry pioneers, this immersive one-year journey transcends conventional education, setting you on a trajectory where your skills are not just sought after but indispensable.

Enroll in the Advanced Diploma in Information Security and empower yourself for a future where opportunities are yours to seize. Embrace the realm of cybersecurity and emerge as a proficient professional, primed to secure the digital world.

Why this Course?

In an ever-evolving landscape marked by emerging threats and advancing technology, the realm of cybersecurity undergoes perpetual transformation. For those aspiring to venture into offensive or defensive security domains, this course serves as an essential stepping stone. It furnishes a comprehensive insight into the latest techniques and tools embraced by the industry. Equipping you with vital knowledge and hands-on proficiency, this course acts as a springboard for success, catering to newcomers and individuals seeking to enhance their existing skill set.

NAVIGATING DIGITAL EVOLUTION

In a landscape shaped by constant digital evolution, cybersecurity expertise is no longer a luxury—it's a necessity.

GATEWAY TO OPPORTUNITIES

Open doors to limitless opportunities through the Advanced Diploma in Information Security, where your potential knows no bounds.

CRAFTED BY INDUSTRIAL EXPERTS

Curated and crafted by industry pioneers, our program provides you with insights and knowledge that are cutting-edge and relevant.

BEYOND CONVENTIONAL LEARNING

This one-year journey transcends the ordinary, propelling you into a future where your skills are in high demand and your capabilities are boundless. Empower Your Future with Expertise

WHY THIS COURSE?

Why choose Offenso

Join Offenso Hackers Academy for an unparalleled Cybersecurity learning experience. Benefit from our experienced trainers who bring real-world expertise to the classroom. Engage in interactive sessions with industry experts, gaining valuable insights from their practical knowledge. Our cutting-edge curriculum covers the latest trends and tools in Cybersecurity. Enhance hands-on practical exercises to apply your skills in simulated scenarios. Network with professionals, creating connections that support your career growth. Receive career guidance and placement support, leveraging our industry connections. Enjoy state-of-the-art facilities, providing an optimal learning environment. Start your journey to become a skilled Cybersecurity professional with Offenso Hackers Academy.

WHY CHOOSE OFFENSO

FAQs

Q. **What is the course format?**

A. The course is a combination of lecture-style lessons and hands-on labs and exercises.

Q. **Who would benefit from enrolling in this course?**

A. The course is ideal for anyone looking to start a career in Cybersecurity or for IT professionals looking to enhance their knowledge and skills in the field of Cybersecurity

Q. **Is prior knowledge of cybersecurity required?**

A. No prior knowledge of Cybersecurity is essential. The course is designed to provide comprehensive coverage of the subject, starting with the fundamentals and building up to more advanced topics.

Q. **What is the estimated time commitment for the course?**

A. The course is designed to be completed in 1 year. Participants have to spend a minimum of 10 hours in a week on coursework including lessons labs and exercises.

offenso™
Hackers Academy