Faysal Aziz

Cybersecurity 2023:

Unlocking Cybersecurity Mastery with Industry Titans

FA-0148 · 5-Day

DevOps, Cloud & Infrastructure · Cybersecurity

Introduction

5-Day Training

In an era dominated by digital transactions, the importance of cybersecurity has never been more paramount. We're proud to bring you trainers who aren't just academicians; they hail from a hands-on industry background and were instrumental in developing the online transaction system of Union Pay, one of Asia's largest bank card services. With their insights and real-world experience, you're set to grasp not only the fundamentals but also the intricate nuances of cybersecurity.

Learning outcomes

By the end of this training, participants will:

- Understand the fundamental principles of cybersecurity.
- Familiarize with essential terminologies and concepts.
- Grasp the basics of network security and how vulnerabilities arise.
- Explore ethical hacking methodologies and specific techniques.
- Recognize and understand different security protocols including Kerberos.
- Develop the skills to detect and mitigate various cyber-attacks.

Prerequisites

- Basic understanding of computer systems and networks.
- Familiarity with basic IT terminology.

- An inquisitive mindset ready to delve deep into cybersecurity.

Training outline

1. Day 1: Introduction to Cybersecurity

Morning Session:

- Introduction and Overview
- Historical Context of Cybersecurity
- Importance of Cybersecurity in Today's World

Afternoon Session:

Key Terminologies and Concepts

- Malware, Phishing, Encryption, Firewalls, VPN, etc.

- Basic Principles of Cybersecurity
- Importance of a Multi-Layered Security Approach

2. Day 2: Delving Deeper - Cyber Threats and Basic Network Concepts

Morning Session:

- Types of Cyber Threats and Their Impacts

Introduction to Network Concepts

- OSI Model
- IP Addressing and Subnetting

Afternoon Session:

- Common Network Vulnerabilities
- Introduction to Firewalls, Proxies, and Intrusion Detection Systems
- Overview of Ethical Hacking and its Importance

3. Day 3: Network Security and Introduction to Ethical Hacking

Morning Session:

Deep Dive into Network Security

- VPNs, Encryption Standards, Secure Protocols

Basic Tools for Ethical Hacking

- Nmap, Metasploit, Wireshark, etc.

Afternoon Session:

Practical Ethical Hacking Exercises

- WEP and WPA/WPA2 Cracking

4. Day 4: Advanced Ethical Hacking Techniques

Morning Session:

- Bypassing Windows Security
- Man-in-the-Middle (MitM) Attack

Afternoon Session:

- Post Connection Attacks
- ARP Poisoning and Detection

5. Day 5: Security Systems and Protocols

Morning Session:

- Introduction to Kerberos
- Other Common Security Systems and Protocols

Afternoon Session:

- Practical Session on Implementing Security Systems
- Recap and Q&A Session

By leveraging this training framework, participants will gain a solid foundation in cybersecurity, enriched by the unique perspectives and experiences of trainers from the industry. The training program is designed to increase in intensity as it progresses to give the pupils time to adjust and adapt. There shall also be periodic assessments and gamified training to ensure maximum learning outcome.

© 2026 Faysal Aziz · Kuala Lumpur