COURSE TABLE OF CONTENTS

Capture The Flag (CTF) Challenges Workshop

OEM: Koenig Original • Duration: 2 Days (15 hrs)

COURSE MODULES & TOPICS

Module 1: CTF Competitions and Platforms

- Purpose and educational value of CTF competitions
- Jeopardy-style and Attack-Defense formats
- Competition structure, scoring, flags, and hints
- Challenge lifecycle and participant experience
- Overview of CTF platforms and infrastructure

Module 2: CTF Categories and Challenge Concepts

- Digital Forensics and Incident Response (DFIR)
- Web security and application vulnerabilities
- Network security and packet analysis
- Cryptography and reverse engineering
- Binary exploitation, OSINT, and cloud security
- Selecting categories based on audience and outcomes

Module 3: Challenge Design and Development

- Generating challenge ideas and defining objectives
- Building realistic scenarios and narratives
- Writing clear descriptions, hints, and rules
- Setting difficulty levels and solve paths
- Creating challenge files and supporting artifacts
- Flag formats, generation, storage, and validation
- Avoiding unintended solutions and design flaws
- Practical challenge-development exercises

Module 4: Deployment and Infrastructure with Docker

- Docker fundamentals for CTF challenge deployment
- Building and configuring challenge containers
- Container networking and service exposure
- Isolation, permissions, and environment security
- Resource allocation and basic scalability
- Deployment workflow and troubleshooting

Module 5: Testing, Validation, and Quality Assurance

- Testing from a participant's perspective
- Verifying intended and unintended solution paths
- Flag validation and submission testing
- Troubleshooting challenge behavior and dependencies
- Reviewing stability, fairness, and difficulty
- Writing solution guides and deployment documentation

© Koenig Solutions

Module 6: Hands-on Challenge Build and Presentation

- Developing a complete practical CTF challenge
- Preparing challenge assets and deployment configuration
- Deploying and testing the challenge environment
- Validating the flag and documenting the solution
- Peer review and final challenge presentation