Cybersecurity Attack and Defense Fundamentals

TG148

Course Overview:

This course equips IT and cybersecurity professionals with essential knowledge and skills to identify, prevent, and respond to modern cyber threats. As organizations increasingly depend on complex digital infrastructures, this training provides a vital foundation in ethical hacking, network defense, and digital forensics. Participants will explore common vulnerabilities and attack methods while developing the ability to implement effective countermeasures and forensic investigations.

Course Objective:

-Understand key cybersecurity concepts, threats, and vulnerabilities

-Identify and respond to network-level and application-level attacks

-Apply network and digital forensics techniques for incident analysis

-Implement secure authentication, authorization, and cryptographic methods

-Evaluate and strengthen wireless network security

Course Outline:

Module 1: Introduction to Cybersecurity and Ethical Hacking

-Ethical hacking essentials

-Information security principles

-Common threats and vulnerabilities

Module 2: Network-Level Attacks

-Sniffing and eavesdropping techniques

-Denial-of-Service (DoS) attacks

-Session hijacking fundamentals

Module 3: Application-Level Attacks

-OWASP Top 10 overview

-SQL injection and webserver exploitation

-Application vulnerability management

Module 4: Wireless Network Security

-Fundamentals of wireless networking

-Wireless encryption types

-Securing wireless communications

Module 5: Identification and Authentication

-Authentication and authorization concepts

-Secure identification techniques

-Overview of access control systems

Module 6: Cryptographic Techniques

-Symmetric vs. asymmetric encryption

-Cryptographic algorithms and applications

-Public Key Infrastructure (PKI)

Module 7: Network Forensics

-Fundamentals of network forensics

-Event correlation and traffic analysis

-Tools for forensic investigation

Module 8: Digital Forensics Essentials

-Digital evidence and data acquisition

Training Language:

English

Training Methodology:

The course combines various teaching methods, including instructor-led presentations, group discussions, case study analyses, and assessments through quizzes and a final exam to engage participants and ensure they understand and retain the material.

Venue | Date | Fees

Riyadh | 12-10-2025 | 17,250 SAR

-Forensics investigation phases

-Reporting and legal considerations

Module 9: Case Studies in Cyber Defense

-Real-world attack scenarios

-Incident response simulations

-Lessons learned from breaches

Module 10: Final Assessment and Review

-Knowledge quiz and final exam

-Group discussion on key takeaways

-Feedback and course wrap-up

Who Should Attend:

-Cybersecurity Analysts

-Information Security Officers

-IT Administrators

-Network Engineers