Faysal Aziz

Ethical Hacking and Cybersecurity

FA-0198 · 5-day

DevOps, Cloud & Infrastructure · Cybersecurity

Introduction

Welcome to our 5-day course on Ethical Hacking and Cybersecurity. This intensive training program is designed to provide you with hands-on experience in the field of cyber security and ethical hacking, equipping you with the skills to protect networks and systems from digital attacks. The course will take you through the fundamentals of cyber security and terminology, giving you a robust understanding of the structure and architecture involved. We will delve into Linux basics and network fundamentals, various hacking attacks and defense mechanisms, and the application of tools such as Nmaps, SQL injections, and much more. The course also includes practical lab sessions using remote servers and virtual machines with Kali Linux.

Learning outcomes

By the end of the course, you will be able to:

- Understand the foundations of cyber security, terminologies, structure and architecture.
- Utilize Linux for various cyber security tasks.
- Understand network basics and how to secure them.
- Conduct pre-connection and post-connection attacks.
- Perform WEP and WPA/WPA2 Cracking.
- Execute man in the middle attacks (MITM) and devise ways to prevent them.
- Gain full control over devices on the same network.
- Conduct SQL Injections and Brute force attacks.
- Use Nmaps, SSL Strips for ethical hacking purposes.
- Understand and perform Denial of Service (DoS) attacks and mitigation.
- Understand ARP Poisoning Detection & Security.

Prerequisites

1. Basic knowledge of computers and networking.
2. A computer with internet access for lab setup and exercises.
3. Basic understanding of command-line interface.

Training outline

1. Day 1 - Introduction and Lab Setup

- Foundations of Cyber Security: Understanding the basics
- Introduction to Cyber Security Terminologies
- Overview of the Cyber Security Structure and Architecture
- Setting up the lab with VMware, Virtual Box, and Kali Linux

2. Day 2 - Linux and Network Basics

- Introduction to Linux Basics
- Network Basics: Protocols, Models and Strategies
- Introduction to Pre-Connection Attacks
- Lab: Linux and Network Exercises

3. Day 3 - Advanced Attacks and Security

- Gaining Access and Post Connection Attacks
- WEP/WPA/WPA2 Cracking: Techniques and Strategies
- Man In The Middle Attacks (MITM): Understanding and Execution
- Gaining Full Control Over Devices On The Same Network
- Lab: Cracking and MITM Attacks

4. Day 4 - Cyber Threats and Defensive Measures

- Introduction to SQL Injections
- Brute Force Attacks: Understanding and Mitigation
- Denial of Service (DoS) Attacks: Tactics and Prevention
- ARP Poisoning Detection & Security: Techniques and Practices
- Lab: SQL Injections and Brute Force Attacks

5. Day 5 - Cyber Security Tools and Best Practices

- Introduction to Nmaps and SSL Strips
- Hacking old-school windows password
- Security & Mitigation: Best Practices and Guidelines
- Ethical Hacking: Laws and Ethics
- Lab: Implementing Security Measures and Using Cyber Security Tools

By the end of this course, you will have gained a strong foundation in ethical hacking and cyber security, making you capable of protecting a network and understanding the vulnerabilities that hackers might exploit. You'll be ready to delve deeper into the field of cyber security and play a crucial role in the digital world.

© 2026 Faysal Aziz · Kuala Lumpur