Faysal Aziz

Cybersecurity in Action

Building and Breaking Real Systems : From Remote Lab Setup to Penetration Testing Mastery—All in Two Days

FA-0150 · Two Days

DevOps, Cloud & Infrastructure · Cybersecurity

Introduction

Cyber threats change daily, and if you're working in cybersecurity, you need to think like both the good guys and the bad guys. You can't just know the theory—you need to get your hands dirty with real systems.

This two-day intensive course throws you straight into the deep end with actual remote Linux servers, not just virtual machines running on your laptop. Why? Because when you're dealing with real infrastructure that mirrors what you'll encounter in your job, the skills you develop actually stick and transfer to the real world.

We've built this program around the same comprehensive approach you'd find in "The Complete Ethical Hacking Course" on Udemy, but we've focused everything on remote server environments. You'll set up secure testing labs, run penetration tests, and work through scenarios that cybersecurity professionals face every day. Your instructor brings three decades of hands-on experience to guide you through it all.

This isn't about memorizing which buttons to click in different tools. It's about developing the strategic thinking that lets you anticipate threats, find weaknesses before the bad actors do, and build stronger defenses. By the end, you'll understand how attackers think and how defenders can stay one step ahead.

Learning outcomes

By the end of this course, participants will be able to:

- **Establish Secure Remote Labs:** Configure and manage remote Linux servers to create isolated and secure environments for testing and analysis.
- **Conduct Vulnerability Assessments:** Utilize industry-standard tools to identify and assess vulnerabilities within systems and applications.
- **Perform Penetration Testing:** Execute structured penetration tests to exploit identified vulnerabilities and understand potential impacts.
- **Implement Security Measures:** Apply best practices to harden systems against common threats and mitigate identified risks.
- **Analyze and Report Findings:** Document testing procedures and results, providing actionable recommendations for remediation.

Prerequisites

Participants should have:

- **Basic Linux Proficiency:** Familiarity with command-line operations and system navigation.
- **Networking Fundamentals:** Understanding of TCP/IP, DNS, and common network protocols.
- **Access to Remote Servers:** Ability to connect to and manage remote Linux servers via SSH.
- **Security Mindset:** An interest in cybersecurity principles and ethical hacking practices.

Training outline

1. 1. Remote Lab Setup and Configuration

1.1. Server Provisioning

- Selecting appropriate cloud service providers (e.g., AWS, DigitalOcean).
- Deploying Linux distributions (e.g., Ubuntu, CentOS) on remote servers.

1.2. Secure Access Implementation

- Configuring SSH keys for secure authentication.
- Setting up firewalls and security groups to control access.

1.3. Environment Isolation

- Creating isolated environments using containers or chroot jails.

- Implementing network segmentation to simulate different security zones.

2. 2. Fundamentals of Vulnerability Assessment

2.1. Introduction to Vulnerabilities

- Understanding common vulnerabilities (e.g., CVEs, OWASP Top 10).
- Exploring the vulnerability lifecycle and disclosure processes.

2.2. Scanning Tools and Techniques

- Utilizing tools like Nmap for network discovery.
- Employing vulnerability scanners such as OpenVAS and Nessus.

2.3. Interpreting Scan Results

- Analyzing scanner outputs to identify critical vulnerabilities.
- Prioritizing vulnerabilities based on risk and exploitability.

3. 3. Penetration Testing Methodologies

3.1. Reconnaissance and Information Gathering

- Conducting passive and active reconnaissance.
- Leveraging tools like WHOIS, DNS enumeration, and Shodan.

3.2. Exploitation Techniques

- Exploiting common vulnerabilities (e.g., SQL injection, buffer overflows).
- Using frameworks like Metasploit for automated exploitation.

3.3. Post-Exploitation Strategies

- Maintaining access through backdoors and persistence mechanisms.
- Escalating privileges and lateral movement within networks.

4. 4. System Hardening and Defense Mechanisms

4.1. Security Best Practices

- Applying patches and updates to mitigate known vulnerabilities.
- Configuring services securely and minimizing attack surfaces.

4.2. Monitoring and Logging

- Setting up logging mechanisms to detect and respond to incidents.
- Implementing intrusion detection systems (e.g., Snort, OSSEC).

4.3. Incident Response Planning

- Developing response plans for potential security breaches.
- Conducting tabletop exercises to test readiness.

5. 5. Reporting and Documentation

5.1. Crafting Effective Reports

- Documenting findings in a clear and structured manner.
- Providing actionable recommendations for remediation.

5.2. Communicating with Stakeholders

- Presenting technical information to non-technical audiences.
- Advising on risk management and security investments.

This course offers a comprehensive, hands-on approach to cybersecurity, ensuring that participants not only learn theoretical concepts but also apply them in practical scenarios. With the guidance of an experienced instructor and the use of real remote servers, attendees will be well-equipped to tackle real-world security challenges.

© 2026 Faysal Aziz · Kuala Lumpur