Faysal Aziz

Penetration Testing and Red Teaming Essentials

A 1-day course outline for the cybersecurity team

FA-0346 · 1-day

Cybersecurity

Introduction

In today's digital age, where cybersecurity threats are ever-evolving and becoming more sophisticated, the importance of a proactive security posture cannot be overstated. Penetration testing and red teaming are critical disciplines within cybersecurity, designed to simulate real-world attacks on systems, networks, and infrastructure to identify vulnerabilities before they are exploited by malicious actors. As organizations increasingly rely on digital infrastructure, the demand for skilled professionals who can effectively test and secure these systems is growing rapidly.

This course offers a deep dive into the world of ethical hacking, where you will learn not just to think like a hacker but to act like one, under controlled and ethical parameters. We aim to equip you with the knowledge, skills, and techniques necessary to assess and improve the security posture of an organization, ensuring you are ready to tackle current and emerging security challenges. By understanding the mindset and methods of potential attackers, you can help build more resilient systems that can withstand sophisticated cyberattacks.

Learning outcomes

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

- Understand the methodology and tools used for penetration testing and red teaming.
- Identify and exploit vulnerabilities in systems and networks.
- Develop strategies for securing systems against cyberattacks.
- Conduct comprehensive red team exercises to simulate real-world attack scenarios.

- Analyze the outcomes of penetration tests and red team exercises to recommend security improvements.

Prerequisites

- Basic understanding of networking concepts and protocols.
- Familiarity with common operating systems, especially Windows and Linux.
- Knowledge of scripting or programming languages (Python, Bash).
- Previous experience in IT or cybersecurity is advantageous but not mandatory.

Training outline

1. Introduction to Ethical Hacking

1. Definition and scope of penetration testing and red teaming
2. Ethical and legal considerations in hacking
3. Differences between penetration testing, vulnerability assessments, and red teaming

2. Planning and Scoping

1. Understanding the objectives and scope of engagement
2. Rules of engagement and legal implications
3. Gathering intelligence and identifying targets

3. Reconnaissance and Footprinting

1. Techniques for gathering information on target systems
2. Tools and resources for passive and active reconnaissance
3. Analyzing information to identify potential vulnerabilities

4. Scanning and Enumeration

1. Network scanning techniques and tools
2. Enumerating services, ports, and live hosts
3. Vulnerability scanning and analysis

5. Gaining Access and Exploitation

1. Techniques for exploiting system vulnerabilities
2. Social engineering tactics
3. Client-side and server-side attacks
4. Bypassing security mechanisms

6. Post-Exploitation

1. Maintaining access with backdoors and rootkits
2. Escalating privileges
3. Harvesting sensitive information
4. Covering tracks and clearing logs

7. Real-world Attack Simulations (Red Team Exercises)

1. Planning and executing a red team operation
2. Role-playing attacker scenarios
3. Using advanced persistent threat (APT) tactics

8. Analysis and Reporting

1. Analyzing data from penetration tests
2. Documenting findings and recommendations
3. Developing effective remediation strategies

9. Best Practices and Mitigation Strategies

1. Secure coding practices
2. Security policies and compliance
3. Regular updates and patches

10. Wrap-Up and Future Trends

1. Summary of key takeaways
2. Discussion on emerging trends in cybersecurity
3. Q&A session

This comprehensive outline covers the full spectrum of penetration testing and red teaming, providing participants with a robust foundation in both the theoretical and practical aspects of this critical field in cybersecurity.

© 2026 Faysal Aziz · Kuala Lumpur