Adversary Ops Infrastructure Edition Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

This hands-on course focuses on advanced infrastructure security testing techniques, using real-world scenarios and offensive research. Delegates will learn to identify, exploit, and remediate vulnerabilities across on-premises and cloud environments. The course is designed to keep skills up to date with the latest threat landscape, providing practical experience through extensive lab exercises led by experienced penetration testers.

Target Audience

- Intermediate knowledge of infrastructure application security (at least 2 years' experience)
- Competency with common command line syntax
- Experience using virtual labs for penetration testing and/or offensive research

Target audience

- Penetration testers and red teamers
- Security consultants and architects
- Network administrators with security experience
- CSIRT/SOC teams and blue teamers
- Security and IT managers and team leads
- In-house security teams from intermediate to pro-level
- Other security and IT practitioners and managers seeking to understand the current threat landscape

What You Will Learn

Delegates will learn how to:

- Think and behave like an advanced, real-world threat actor
- Identify and exploit commonly used vulnerabilities that have recently caused damage and disruption
- Deploy the latest and most common network infrastructure and cloud hacking techniques, including novel methods undetectable by scanners
- Analyse vulnerabilities within their own organisation and customise hacking techniques in response
- Apply a wide range of hacks for Windows, Linux, Microsoft Azure, AWS, Google Cloud Platform, and software development systems
- Remediate as well as attack weaknesses in infrastructure
- Use lab-based exercises to reinforce practical skills