Formatech
INTEGRATED LEARNING CENTERS
Learn from the Experts

Course Outline

Master Class: 360° Penetration Testing Course

Duration: 3 days (21 hours)

Introduction

You will enjoy it! The course teaches infrastructure security concepts, including the techniques on how to attack and how to respond with an appropriate countermeasure implementation. Our course has been developed around professional penetration testing and security awareness in the business and IT fields. To make sure that all participants gain the necessary infrastructure security knowledge, our classes have an intensive hands-on format.
All labs are always up to date and have 3 levels of difficulty. They can be easily adjustable to the overall level of the group. Every exercise is supported with lab instructions and multiple tools, both traditional and specialized. Our Trainers recommend students have some knowledge of security concepts, such as operating system services and architecture. However, all required concepts will be covered throughout the course.

Paula Januszkiewicz is a word-renowned Security Expert. Paula loves to perform Penetration Tests, IT Security Audits, and after all she says: 'harden'em all'! Enterprise Security MVP and trainer (MCT) and Microsoft Security Trusted Advisor.
Paula says: Penetration Test combines a lot of components that make a test to be a bit more professional. Starting with report templates, attitude, being legal and first steps, ending up with great tools and techniques. This course is fun but with a value!

Target audience

Network administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security, Chief Security Officers.

Topics Covered:

- Module 1: Evolution of Hacking
  - Evolution of vulnerabilities
  - Persistent Threats
  - Malware evolution
- Module 2: Operating System Services Security Overview
  - Services Security
  - Active Directory Security
- Module 3: Operating System Internal Security
  - Permissions and Privileges
  - Password Security
  - Offline Attacks
  - Pass-The-Hash Attacks with custom CQURE Tools

- Pass-The-Ticket Attacks
- DPAPI Attacks with custom CQURE Tools
- Cached Logons Attacks with custom CQURE Tools
- Exploiting a lack of access controls

- Module 4: Databases Security
  - SQL Server Service
  - Authentication Modes
  - Stored Procedures
- Module 5: Reconnaissance and Target Profiling
  - Network Scanning
  - Man-in-the-middle Attacks
- Module 6: Tampering with Communication (Wired and Wireless)
  - Wireless Protocols Security
  - NetBIOS Spoofing
  - SMB Security
- Module 7: Malicious Files Execution
  - Anti-antimalware techniques
  - Non-exe Malware
- Module 8: Google Hacking
  - Open Source Intelligence
  - Possible Targets
  - Building Advanced Queries
- Module 9: HTTP Request Building
  - Cross Site Scripting
  - Injection Attacks
  - Information Leakage and Error Handling
- Module 10: Legal Issues
  - Paperwork
  - Reporting
  - Responsibility