Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

360° Penetration Testing Course

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **3 Gün**

Overview

Bu eğitim, nasıl saldırıya geçileceği ve uygun bir karşı önlem uygulamasına nasıl cevap verileceği ile ilgili teknikleri içeren altyapı güvenliği kavramlarını öğretir. Eğitimimiz iş ve BT alanlarında profesyonel penetrasyon testi ve güvenlik bilinci etrafında geliştirilmiştir. Tüm katılımcıların gerekli altyapı güvenliği bilgisini edinmelerini sağlamak için, sınıflarımız yoğun bir uygulamalı formata sahiptir.

Prerequisites

Bu eğitime katılmak için herhangi bir ön koşul yoktur.

Who Should Attend

Bu eğitime ağ yöneticileri, altyapı mimarları, güvenlik uzmanları, sistem mühendisleri, ağ yöneticileri, BT uzmanları, güvenlik danışmanları, ağ ve çevre güvenliğini uygulamaktan sorumlu diğer kişiler, güvenlik şefleri katılabilir.

What You Will Learn

Bu eğitim esnasında nasıl saldırıya geçileceği ve uygun bir karşı önlem uygulamasına nasıl cevap verileceği ile ilgili teknikleri içeren altyapı güvenliği kavramlarını öğreneceksiniz. 360° Penetration Testing eğitimi iş ve BT alanlarında profesyonel penetrasyon testi ve güvenlik bilinci etrafında geliştirilmiştir. Tüm katılımcıların gerekli altyapı güvenliği bilgisini edinmelerini sağlamak için, sınıflarımız yoğun bir uygulamalı formata sahiptir.

Outline

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 tools
- Pass-The-Ticket Attacks
- DPAPI Attacks with custom tools
- Cached Logons Attacks with custom 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