Formatech
INTEGRATED LEARNING CENTERS
Learn from the Experts

Course Outline

Securing Windows Infrastructure

Duration: 3 days (18 hours)

Introduction

For so many years we have been asked to create a course like this! This course is just a great workshop that teaches how to implement securing technologies one at a time. The course covers all aspects of Windows infrastructure security that everybody talks about, but during the course you will learn how to implement them! Our goal is to teach you how to design and implement secure infrastructures based on the reasonable balance between security and comfort with great knowledge of attacker's possibilities. We really want you to go out from the class with the practical, ready-to- use and holistic approach and skills to secure your infrastructure.

This is a deep dive course on infrastructure services security. It is a must-go for enterprise administrators, security officers and architects. Delivered by one of the best people in the market in the security field – with practical knowledge from tons of successful projects, many years of real-world experience, great teaching skills and no mercy for misconfigurations or insecure solutions.

Paula Januszkiewicz is the world-known Security Expert. 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: Securing Windows services is a crucial process that makes hackers to pick someone else. This is one of my favorite trainings as there is an enormous amount of labs and discussion cases and when combined with the Hacking Windows Infrastructure course it creates a complete experience about what infrastructure security is all about.

Target Audience:

- Enterprise administrators
- Infrastructure architects
- Security professionals
- Systems engineers
- Network administrators,
- IT Professionals
- Security consultants and other people responsible for implementing network and perimeter security.

Pre-requisites

To attend this training you should have a good hands-on experience in administering Windows infrastructure. At least 8 years in the field is recommended. All exercises are based on Windows Server 2012 R2 and Windows 8.1. Some examples are also shown on Windows Server 2012 to accommodate the difference.

Topics Covered:

- Module 1: Designing Secure Windows Infrastructure

  On the market there are thousands solutions available to enrich security in our infrastructure. Idea of this module is to provide the complete knowledge and to gain the holistic approach for the areas that can be secured and for the measures that can be implemented.

- Module 2: Securing Windows Platform
  - Defining and disabling unnecessary services
  - Implementing secure service accounts
  - Implementing rights, permissions and privileges
  - Driver signing
- Module 3: Malware Protection
  - Techniques used by modern malware
  - Malware investigation techniques
  - Analyzing cases of real malware
  - Implementing protection mechanisms
- Module 4: Managing Physical Security
  - Managing port security: USB, FireWire and other
  - Mitigating Offline Access
  - Implementing and managing BitLocker
- Module 5: Deploying and configuring Public Key Infrastructure
  - Role and capabilities of the PKI in the infrastructure
  - Designing PKI architecture
  - PKI Deployment – Best practices
- Module 6: Configuring Secure Communication
  - Deploying and managing Windows Firewall –advanced and useful features
  - Deploying and configuring IPsec
  - Deploying secure Remote Access ((VPN, Direct Access, Workplace Join, RDS Gateway))
  - Deploying DNS and DNSSEC
- Module 7: Securing Web Server
  - Configuring IIS features for security
  - Deploying Server Name Indication and Centralized SSL Certificate Support
  - Monitoring Web Server resources and performance
  - Deploying Distributed Denial of Service attack prevention
  - Deploying Network Load Balancing and Web Farms
- Module 8: Providing Data Security and Availability
  - Designing data protection for Microsoft Office, PDF and other file types
  - Deploying Active Directory Rights Management Services
  - Deploying File Classification Infrastructure and Dynamic Access Control
  - Configuring a secure File Server
  - Hardening basics for Microsoft SQL Server
  - Clustering selected Windows services
- Module 9: Mitigating the common password attacks
  - Performing Pass the Hash attack and implementing prevention
  - Performing the LSA Secrets dump and implementing prevention
- Module 10: Automating Windows Security
  - Implementing Advanced GPO Features
  - Deploying Software Restriction: Applocker
  - Advanced PowerShell for administration