Masterclass: Securing Windows Infrastructure

Duration: 3 days

(if combined with Hacking Windows Infrastructure: 5 days)

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.

Top-speaker at world known conferences, including being No 1 speaker at Microsoft Ignite!

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.

The course is an intense workshop! During these 3 days we provide caffeine candies – this course is really intense and in order not to miss a thing you MUST stay awake!

We really want you to leave from the class with practical, ready-to-use knowledge of how to get into the infrastructure.

This is a deep dive course. 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! The course has a form of intense workshop and you MUST stay awake just not to miss a thing!**

All exercises are based on Windows Server 2012 R2, Windows 8.1 and Windows Server 2016, Windows 10. This course is based on practical knowledge from tons of successful projects, many years of real-world experience and no mercy for misconfigurations or insecure solutions!

Prerequisites:

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.

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.

Materials

Author's unique tools, over 200 pages of exercises, presentations slides with notes.

Agenda

Module 1: Designing Secure Windows Infrastructure

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

Module 2: Securing Windows Platform

a) Defining and disabling unnecessary services
b) Implementing secure service accounts
c) Implementing rights, permissions and privileges
d) Driver signing

Module 3: Malware Protection

a) Techniques used by modern malware
b) Malware investigation techniques
c) Analyzing cases of real malware
d) Implementing protection mechanisms

Module 4: Managing Physical Security

a) Managing port security: USB, FireWire and other
b) Mitigating Offline Access
c) Implementing and managing BitLocker

Module 5: Deploying and configuring Public Key Infrastructure

a) Role and capabilities of the PKI in the infrastructure
b) Designing PKI architecture
c) PKI Deployment – Best practices

Module 6: Configuring Secure Communication

a) Deploying and managing Windows Firewall – advanced and useful features
b) Deploying and configuring IPsec
c) Deploying secure Remote Access (VPN, Direct Access, Workplace Join, RDS Gateway)
d) Deploying DNS and DNSSEC

Module 7: Securing Web Server

a) Configuring IIS features for security
b) Deploying Server Name Indication and Centralized SSL Certificate Support
c) Monitoring Web Server resources and performance
d) Deploying Distributed Denial of Service attack prevention
e) Deploying Network Load Balancing and Web Farms

Module 8: Providing Data Security and Availability

a) Designing data protection for Microsoft Office, PDF and other file types
b) Deploying Active Directory Rights Management Services
c) Deploying File Classification Infrastructure and Dynamic Access Control
d) Configuring a secure File Server
e) Hardening basics for Microsoft SQL Server
f) Clustering selected Windows services

Module 9: Mitigating the common password attacks

a) Performing Pass-the-Hash attack and implementing prevention
b) Performing the LSA Secrets dump and implementing prevention

Module 10: Automating Windows Security

a) Implementing Advanced GPO Features
b) Deploying Software Restriction: Applocker
c) Advanced Powershell for administration