Masterclass: Windows Security and Infrastructure Management

Duration: 5 Days Course Code: WSI

Overview:

Nederlands:
Deze cursus verdiept zich in de configuratie van infrastructurele services, het verbeteren van het beveiligingsniveau en interne processen in Windows. Het is een must voor bedrijfsadministrators, security officers en architecten. De cursus wordt gegeven door een van de beste docenten op het gebied van beveiliging, met praktische kennis uit tientallen succesvolle projecten, vele jaren ervaring in de 'echte wereld', uitstekende onderwijsvaardigheden en geen enkele genade voor verkeerde configuraties of onveilige oplossingen.
Een veilige configuratie van de infrastructuur zou de belangrijkste verdedigingslinie moeten zijn in elke organisatie. Helaas zijn mensen, het meest waardevolle bedrijfsmiddel, zich niet altijd bewust van het beveiligingsniveau in hun bedrijf, van mogelijke punten van binnenkomst, van de manier waarop besturingssystemen worden aangevallen en van de mogelijkheden om infrastructuur te beveiligen tegen aanvallen, die soms al het gevolg kunnen zijn van een foutje in de configuratie. Wie perfecte kennis heeft van interne beveiligingsmechanismen, services en serverrollen van besturingssystemen kan enorm veel invloed hebben op het beveiligingsniveau van de infrastructuur als geheel. Maar het probleem is ... dat er nauwelijks iemand is die die invloed heeft!
Deze cursus gaat in op geavanceerde toegangsrechten, wachtwoordmechanismen, interne Windows-processen, het gebruik van de PowerShell voor beveiligingsdoeleinden, het krijgen van ongeautoriseerde toegang, geavanceerde DNS-configuraties en veelvoorkomende configuratiefouten, Active Directory-beveiliging, IIS-beveiliging, debugging, geavanceerde monitoring, probleemoplossing en nog veel meer!
Met behulp van deze training kunt u zich inleven in de rol van hacker en uw infrastructuur bekijken vanuit diens optiek.
Alle oefeningen zijn gebaseerd op Windows Server 2012 R2, Windows 8.1 en Windows Server 2016, Windows 10.
==========
English:
This is a deep dive course on infrastructure services configuration, increasing their level of security and windows internals. 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 secure infrastructure configuration should be the most important line of defense in every organization. Unfortunately people, the most valuable resource, are not always aware of the level of security in their companies, possible points of entry, how operating system are attacked and how to protect infrastructure from successful attacks, sometimes caused by configuration mistakes. Understanding perfectly internal operating system protection mechanisms and knowing how operating systems services or server roles work allows having huge impact on the security level of the whole infrastructure. But the problem is that… rarely anybody has this impact!

Advanced access rights, password mechanisms, windows internals, PowerShell usage for security purposes, gaining unauthorized access, advanced DNS configuration and common configuration mistakes, Active Directory security, IIS Security, debugging, advanced monitoring and troubleshooting and much more! Topics covered during this training will help you to feel for the hackers' role and evaluate your infrastructure from their point of view.

All exercises are based on Windows Server 2012 R2, Windows 8.1 and Windows Server 2016, Windows 10.

Target Audience:

Nederlands:
Bedrijfsadministrators, infrastructuurarchitecten, beveiligingsprofessionals, systeemengineers, netwerkbeheerders, IT-professionals, beveiligingsconsultants en andere personen die verantwoordelijk zijn voor het implementeren van netwerk- en perimeterbeveiliging.
==========
English:
Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network a perimeter security.

Objectives:

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.

Content:

Module 1: Windows Internals ; System Architecture

- Introduction to the Windows 7/8.1 and Windows Server 2008/2012 R2 security concepts
- Architecture overview and terms:
- Key System Components
- Processes, Threads and Jobs
- Services, Functions and Routines
- Sessions
- Objects and Handles
- Registry
- Advanced Local Procedure Call
- Information gathering techniques:
- Windows Debugging
- Performance Monitor
- Windows Driver Kit
- Other useful tools

Module 2: Process and Thread Management

- Process and thread internals
- Protected processes
- Process priority management
- Examining Thread Activity
- Process and thread monitoring and troubleshooting techniques (advanced usage of Process Explorer, Process Monitor, and other tools)

Module 3: System Security Mechanisms

- Integrity Levels
- Session Zero
- Privileges, permissions and rights
- Passwords security (techniques for getting and cracking passwords)
- Registry Internals
- Monitoring Registry Activity
- Driver signing (Windows Driver Foundation)
- User Account Control Virtualization
- System Accounts and their functions
- Boot configuration
- Services architecture
- Access tokens
- Biometric framework for user authentication

Module 4: Debugging ; Auditing

- Available debuggers
- Working with symbols
- Windows Global Flags
- Process debugging
- Kernel--mode debugging
- User--mode debugging
- Setting up kernel debugging with a virtual machine as the target
- Debugging the boot process
- Crash dump analysis
- Direct Kernel Object Manipulation
- Finding hidden processes
- Rootkit Detection

Module 5: Memory Analysis

- Memory acquisition techniques
- Finding data and activities in memory
- Step--by--step memory analysis techniques
- Tools and techniques to perform memory forensic

Module 6: Storage Management

- Securing and monitoring Files and Folders
- Protecting Shared Files and Folders by Using Shadow Copies
- Implementing Storage Spaces
- Implementing iSCSI
- Implementing FSRM, managing Quotas, File Screens, and Storage Reports
- Implementing Classification and File Management Tasks, Dynamic Access Control
- Configuring and troubleshooting Distributed File System

Module 7: Startup and Shutdown

- Boot Process overview
- BIOS Boot Sector and Bootmgr vs. the UEFI Boot Process
- Booting from iSCSI
- Smss, Csrss, and Wininit
- Last Known Good configuration
- Safe Mode capabilities
- Windows Recovery Environment (WinRE)
- Troubleshooting Boot and Startup Problems

Module 8: Infrastructure Security Solutions

- Windows Server Core Improvements in Windows Server 2012 R2
- AppLocker implementation scenarios
- Advanced BitLocker implementation techniques(provisioning, Standard User Rights and Network Unlock)
- Advanced Security Configuration Wizard
- IPSec
- Advanced GPO Management
- Practicing Diagnostic and Recovery Toolkit
- Tools

Module 9: Layered Network Services

- Network sniffing techniques
- Fingerprinting techniques
- Enumeration techniques
- Networking Services Security (DNS, DHCP, SNMP, SMTP and other)
- Direct Access
- High Availability features: cluster improvements and SMB (Scale – Out File Server)
- Network Load Balancing

Remote Access

- Network Location Awareness
- Wireless technology recognition
- Wireless fingerprinting
- Wireless hacking ideas and demos
- Optimizing wireless hacking
- Protecting wireless networks

Module 10: Monitoring and Event Tracing

- Windows Diagnostic Infrastructure
- Building auditing
- Expression--based audit policies
- Logging Activity for Accounts and processes
- Auditing tools, techniques and improvements
- Auditing removable storage devices

Module 11: Points of Entry Analysis

- Offline access
- Linux BackTrack /other tools vs. Windows Security
- Unpatched Windows and assigned attacks
- Domain Controller attacks
- Man--in--the Middle attacks
- Services security

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/