Masterclass: Windows Security and Infrastructure Management

Duration: 5 Days **Course Code: WSI** **Delivery Method: Virtual Learning**

Overview:

This is a deep dive course on infrastructure services configuration. Secure infrastructure configuration should be the first and most important line of defense in any organisation. Unfortunately employees are not always cyber security aware 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 and Windows 8.1. Some examples are also shown on Windows Server 2012 to accommodate the difference.

Target Audience:

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:

Attendees should meet the following prerequisites:

- Good hands-on experience in administering Windows infrastructure. At least 8 years in the field is recommended.

Testing and Certification

Recommended as preparation for the following exams:

- There is currently no exam linked to this course.

Content:

Module 1: Windows Internals ; System Architecture

- Introduction to the Windows 10 and Windows Server 2016 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
- 3 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 2016
- AppLocker implementation scenarios
- Advanced BitLocker implementation techniques (provisioning, Standard User R? ights 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/