Virtuelt kursus
4 dage **DKK 19.999**
Nr. 87795 A ekskl. moms

Dato **Sted**

Masterclass: Windows Security and Infrastructure Management with Windows Internals [WSI]

Lær at se på din infrastruktur med en hackers øjne. Du lærer at konfigurere passwordmekanismer hensigtsmæssigt, bruge PowerShell i sikkerhedssammenhænge, DNS-konfiguration og meget mere, der kan sikre din virksomhed mod angreb. Undervisningen foregår på engelsk.

Dette er et dybdegående kursus i konfiguration af infrastrukturservices og optimering af deres sikkerhedsniveau og interne Windowsfunktioner. Kurset er et must for virksomhedsadministratorer, sikkerhedsmedarbejdere og -arkitekter. Kurset leveres af nogle af markedets mest kyndige folk inden for sikkerhed, som har praktisk viden fra et utal af succesrige projekter, mange års erfaring fra den virkelige verden og fantastiske undervisningsevner.

En sikker infrastrukturkonfiguration bør være den vigtigste forsvarslinje i enhver organisation. Desværre er medarbejderne, som er den vigtigste ressource, ikke altid opmærksomme på sikkerhedsniveauet i deres virksomheder, mulige indgangspunkter, hvordan operativsystemer angribes, og hvordan de skal beskytte infrastrukturen mod succesfulde angreb der fx kan skyldes konfigurationsfejl. Når man som medarbejder forstår de interne mekanismer og services/roller, der er forbundet med beskyttelsen af et operativsystem, har det en uvurderlig indvirkning på hele infrastrukturens sikkerhedsniveau.

Deltagerprofil

Kurset er relevant for virksomhedsadministratorer, infrastrukturarkitekter, sikkerhedsprofessionelle, systemingeniører,

netværksadministratorer, IT-professionelle, sikkerhedskonsulenter og andre med ansvar for at implementere netværks- og perimetersikkerhed.

Udbytte

- Få dybdegående viden om den interne struktur og arkitektur i Windows
- Lær om forskellige sikkerhedsmekanismer i Windows
- Lær om avancerede metoder og værktøjer til fejlfinding og debugging af Windowssystemer
- Få viden om forskellige aspekter af netværkssikkerhed og lær at håndtere sikkerhedstrusler

Det får du på arrangementet

- Øvelser og inddragelse
- Kursusbevis
- Erfaren underviser
- Maks. 12 deltagere
- Casearbejde
- Materiale på engelsk
- Undervisning på engelsk

Indhold

Module 1: Windows Internals & System Architecture

- Introduction to the Windows 10 and Windows Server 2019 security concepts
- Architecture overview and terms
- Key System Components
  a) Services, Functions and Routines
  b) Sessions
  c) Objects and Handles
  d) Registry
- Advanced Local Procedure Call
- Information gathering techniques
  a) Windows Debugging
  b) Performance Monitor
  c) Windows Driver Kit
  d) 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 2019
- 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

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

Anmeldelser af Masterclass: Windows Security and Infrastructure Management with Windows Internals [WSI]

Ekstremt dygtig lærer, man bliver virkeligt godt klædt på. Altid flotte omgivelser og en virkelig, virkelig god kantine.
— Mikkel Rønne Hansen Region Hovedstaden.

Materiale

Øvelser, præsentationslides med noter og alle laboratorieøvelser vil være tilgængelige for deltagerne i yderligere tre uger efter kursets afslutning.

CPE-point (Continuing professional education)

Du har mulighed for at optjene efteruddannelsespoint ved at gennemføre dette kursus.

Form

Kurset er virtuelt med live underviser. Før du deltager i det virtuelle kursus, vil vi altid forsøge at arrangere en testsession på 15 - 20 minutter en uges tid før, for at sikre, at du er i stand til at deltage i masterclassen. Herunder finder du kravene til at oprette forbindelse til det virtuelle kursus:

- En computer med en stabil internetforbindelse (skal helst køre Windows eller Mac OS).
- Tilladelser til udgående RDP-forbindelser til eksterne servere (til vores laboratoriemiljø) – port 3389
- Et headset (hovedtelefoner og mikrofon)
- Webcam (indbygget eller tilsluttet)
- En ekstra skærm er nyttig, men ikke påkrævet

UNDERVISER

Paula Januszkiewicz

Paula er verdenskendt som sikkerhedsekspert. Paula elsker at lave penetrationstests, IT-sikkerhedsevalueringer, og hendes motto er: "harden em all"! Enterprise Security MVP og -underviser (MCT) og Microsoft Security Trusted Advisor.

UNDERVISER

Kamil

Kamil er en infrastruktur- og sikkerhedsekspert, Office 365 mest værdifulde professionelle, træner (Microsoft Certified Trainer) og Certified Technology Specialist (CTS). Han er medlem af Microsoft Windows Server System (WSS.PL), en af de bedste talere i Warsaw Windows Users & Specialists Group (WGUiSW). Han er medlem af International Association of Microsoft Certified Trainers (IAMCT) og Polish Infrastructure Group (PiNG).

Har du faglige spørgsmål så kontakt

Malene Kjærsgaard
+45 72202523
mch@teknologisk.dk