skillsoft
global knowledge™

AENOR
GESTIÓN
DE LA CALIDAD
ISO 9001

Masterclass: Windows Security and Infrastructure Management

Duración: 4 Días   Código del Curso: WSI

Temario:

This is an international Live Virtual Class, which means you will share the learning experience in a group of IT pros from around the world! The class is taught in English by Cybersecurity Experts! Remember that this course is limited to 12 participants total to ensure the highest quality and unique learning experience.

During this course you will have an opportunity to interact with the instructor and get their help with any problems you might encounter, just as if it was a regular class. About the course 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 systems are attacked, and how to protect the infrastructure from successful attacks which are sometimes caused by configuration mistakes.

Understanding internal OS protection mechanisms and services/roles completely provides a huge impact on the whole infrastructure security level. Unfortunately, the problem is… rarely anyone 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 walk in hackers' shoes and evaluate your infrastructure from their point of view.

Dirigido a:

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

Exámenes y certificación

What is wonderful about our certification is that it is lifetime valid with no renewal fees – the technology changes, but fundamentals and attitude remain mostly the same. Our Virtual Certificates, which entitle you to collect CPE Points, are issued via Accredible.

Contenido:

Module 1: Windows Internals ; System Architecture

a) Introduction to the Windows 10 and Windows Server 2019 security concepts

b) Architecture overview and terms

c) Key System Components i. Processes, Threads and Jobs ii. Services, Functions and Routines iii. Sessions iv. Objects and Handles v. Registry

d) Advanced Local Procedure Call

e) Information gathering techniques i. Windows Debugging ii. Performance Monitor iii. Windows Driver Kit iv. Other useful tools

Module 2: Process and Thread Management

a) Process and thread internals

b) Protected processes

c) Process priority management

d) Examining Thread Activity

e) Process and thread monitoring and troubleshooting techniques (advanced usage of Process Explorer, Process Monitor, and other tools)

Module 3: System Security Mechanisms

a) Integrity Levels

b) Session Zero

c) Privileges, permissions and rights

d) Passwords security (techniques for getting and cracking passwords)

e) Registry Internals

e) Kernel-mode debugging

f) User-mode debugging

g) Setting up kernel debugging with a virtual machine as the target

h) Debugging the boot process

i) Crash dump analysis

j) Direct Kernel Object Manipulation

k) Finding hidden processes

l) Rootkit Detection

Module 5: Memory Analysis

a) Memory acquisition techniques

b) Finding data and activities in memory

c) Step-by-step memory analysis techniques

d) Tools and techniques to perform memory forensic

Module 6: Storage Management

a) Securing and monitoring Files and Folders

b) Protecting Shared Files and Folders by Using Shadow Copies

c) Implementing Storage Spaces

d) Implementing iSCSI

e) Implementing FSRM, managing Quotas, File Screens, and Storage Reports

f) Implementing Classification and File Management Tasks, Dynamic Access Control

a) Windows Server Core Improvements in Windows Server 2019

b) AppLocker implementation scenarios

c) Advanced BitLocker implementation techniques (provisioning, Standard User Rights and Network Unlock?

d) Advanced Security Configuration Wizard

e) IPSec

f) Advanced GPO Management

g) Practicing Diagnostic and Recovery Toolkit

h) Tools

Module 9: Layered Network Services

a) Network sniffing techniques

b) Fingerprinting techniques

c) Enumeration techniques

d) Networking Services Security (DNS, DHCP, SNMP, SMTP and other)

e) Direct Access

f) High Availability features: cluster improvements and SMB ?Scale – Out File Server)

g) Network Load Balancing

Module 10: Monitoring and Event Tracing

a) Windows Diagnostic Infrastructure

b) Building auditing

		c) Expression-based audit policies
f) Monitoring Registry Activity	g) Configuring and troubleshooting Distributed File System	d) Logging Activity for Accounts and processes
g) Driver signing (Windows Driver Foundation)	Module 7: Startup and Shutdown	e) Auditing tools, techniques and improvements
h) User Account Control Virtualization	a) Boot Process overview	
i) System Accounts and their functions	b) BIOS Boot Sector and Bootmgr vs. the UEFI Boot Process	f) Auditing removable storage devices
j) Boot configuration		Module 11: Points of Entry Analysis
k) Services architecture	c) Booting from iSCSI	a) Offline access
l) Access tokens	d) Smss, Csrss, and Wininit	b) Kali Linux /other tools vs. Windows Security
m) Biometric framework for user authentication	e) Last Known Good configuration	c) Unpatched Windows and assigned attacks
Module 4: Debugging ; Auditing	f) Safe Mode capabilities	d) Domain Controller attacks
a) Available debuggers	g) Windows Recovery Environment (WinRE)	e) Man-in-the Middle attacks
b) Working with symbols	h) Troubleshooting Boot and Startup Problems	f) Services security
c) Windows Global Flags	Module 8: Infrastructure Security Solutions	
d) Process debugging		

Información Adicional:

Loads of Knowledge
The course is an intense workshop! During these 4 days we recommend a good cup of coffee – this course is really intense and in order not to miss a thing you MUST stay awake! Exercises All exercises are based on Windows Server 2016 and 2019, Windows 10 and Kali Linux. 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! Remember that the hybrid identity lab environment will stay online for an extra three weeks so you may practice even more after the training is completed!

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid