Duration: 5 days

Masterclass:

Hacking and Securing Microsoft SQL Server 2019

Author:
Mike Jankowski-Lorek

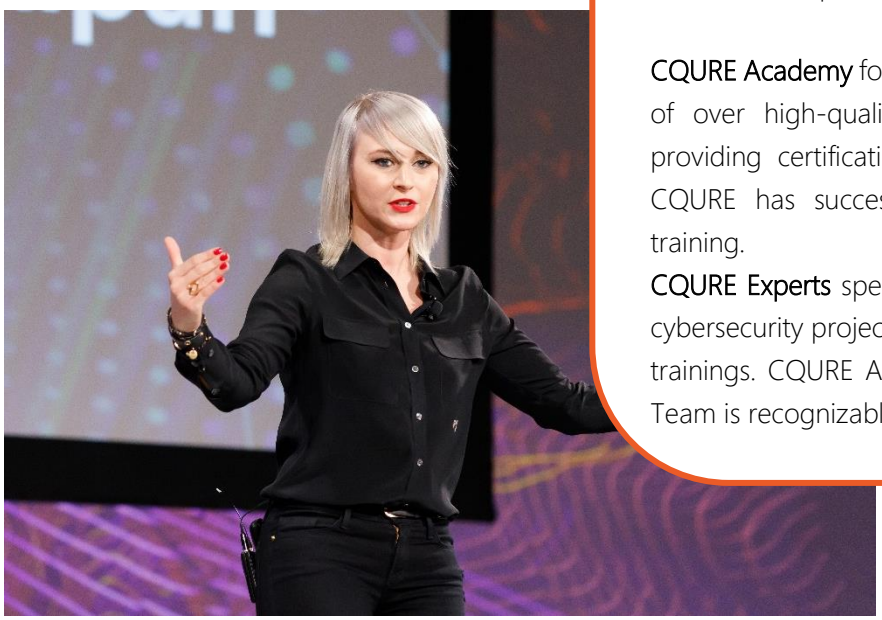
CQURE

Warsaw New York Dubai Zug

info@cqure.pl

www.cqure.pl
www.cqureacademy.com

Mike Jankowski-Lorek is a solution architect, developer, data scientist and security expert with more than 12-years' experience in the field. He designs and implements solutions for Databases, Network & Management area, mainly for Microsoft platform for medium to enterprise level organizations. Mike holds multiple certifications, especially security, database and software development related. He is one of core Experts at CQURE and holds a **PhD in Computer Science.**



CQURE Academy focuses on cybersecurity training program consisting of over high-quality 20 technical workshops and seminars and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based training.

CQURE Experts speak at international events and engage in multiple cybersecurity projects – they bring their knowledge and experience to trainings. CQURE Academy also involves R&D – that is why CQURE Team is recognizable in the cybersecurity field.

In this workshop you will analyze, learn and practice critical tasks for implementing highly secure SQL Server infrastructure. We'll start with identifying security needs regarding database servers and look at the most common attack types and use them on 'out of the box' installation. In simple words we will hack our systems!

Then we will discuss impact of system and network security on databases server. Next, we will go through every layer of protection offered by SQL Server with lots of real-life examples and hands on labs. At the end we will look at the monitoring and auditing our infrastructure to detect threats and react to them. Additionally, we'll play with security of other SQL Services and Azure SQL Databases. Our goal is to show and teach you how to protect your precious data in SQL Server environment and how database security mechanisms work. After the course you will be able to test and secure your SQL Server infrastructure. And to get more practice we offer three extra weeks of labs online!

We want you to leave the class with scripts, checklists and practical, ready-to-use knowledge of how to hack, test and secure your SQL Server infrastructure!

This course is a must-go for database administrators, IT professionals and security officers dealing with database servers. Delivered by hilly skilled SQL and database enthusiast with practical knowledge, multiple successful projects, many years of real-world experience and great teaching skills. The course has a form of intense workshop where we make a deep dive inside the SQL Server. All exercises are based on SQL Server 2019 and Windows Server 2019.

Target audience

Database administrators, infrastructure architects, security professionals, system engineers, advanced database developer, IT professionals, security consultants and other people responsible for implementing databases security.

Prerequisites

To attend this training you should have good hands-on experience in administering Microsoft SQL Server infrastructure. At least 2 years in the field is recommended.

Materials

Author's unique tools and scripts, over 100 pages of exercises, presentations slides with notes.

Agenda

Module 1 Hacking SQL Server Infrastructure

a) Discovering SQL Server instances
b) SQL injection using men in the middle
c) Capturing SQL credentials using men in the middle
d) Decrypting SQL Logins passwords
e) Gaining access to SQL Server on compromised Windows Server

Module 2: SQL Server security baseline concepts

a) Defining security objectives
b) Configuring service accounts
c) Auditing database permissions
d) Implementing physical protection
e) Configuring firewall
f) Securing client-server communication

Module 3: SQL Server Instance security

a) Limiting permissions
b) Securing CLR
c) Implementing protection for extended procedures
d) Protecting linked servers (OPENROWSET)
e) Securing by using policies
f) Hiding instance metadata

Module 4: Managing Logins and Passwords

a) Authentication options
b) Implementing password policies
c) Securing connection strings

Customizing login / user authorization

Module 5: Encryption in SQL Server

a) Key management
b) Code and data encryption
c) Managing certificates
d) Transparent database encryption
e) Encryption in HA and Disaster Recovery

Module 6: Protecting database backups

a) Securing backup files

b) Setting backup file passwords and encryption

c) Handling keys and certificate backups

d) Security considerations while restoring to another SQL Server instance

Module 7: Monitoring and auditing

a) Login auditing options

b) Data access auditing

c) Data Manipulation Language custom auditing

d) Policy-based management

e) Forensics case study

Module 8: Securing other SQL Server services

a) SQL Server Agent

b) SQL Server Analysis Services

c) SQL Server Reporting Services

d) Azure SQL Database