Masterclass:

Hacking and Securing Windows Infrastructure

Duration: 5 days

CQURE

Warsaw New York Dubai Zug

info@cqure.pl

www.cqure.pl
www.cqureacademy.com

CQURE has been providing cybersecurity services and trainings since it was set up in Warsaw in 2008. Throughout the years, our services have reached a wide range of clients around the world, which allowed us to open new offices in New York (2013), Dubai (2014), and Zug (2016).

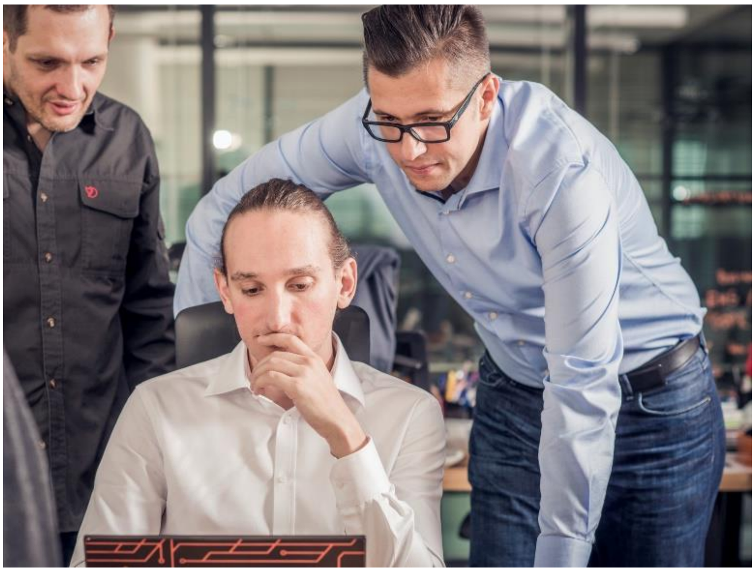
CQURE Academy focuses on cybersecurity training program consisting of over 40 high-quality technical workshops and seminars and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based training.

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.

Hacking and Securing Windows Infrastructure

For so many years we have been asked to create a course like this! This course is just a great workshop that teaches how to implement securing technologies one at a time. The course covers all aspects of Windows infrastructure security that everybody talks about and during the course you will learn how to implement them! Our goal is to teach you how to design and implement secure infrastructures based on the reasonable balance between security and comfort with great knowledge of attacker's possibilities.

About the course



This is a deep dive course on infrastructure services security, a must-go for enterprise administrators, security officers and architects. It is 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. In this workshop you will investigate the critical tasks for a high-quality penetration test. We will look at the most efficient ways to map a network and discover target systems and services. Once it has been done, we will search for vulnerabilities and reduce false positives with manual vulnerability verification. At the end we will look at exploitation techniques, including the use of authored and commercial tools. In the attack summary we will always go through the securing techniques.

Duration: 5 days (35 hours)
Running hours: 9AM - 4PM (CET)

Loads of Knowledge

The course is an intense workshop! During these 5 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

This workshop is based on practical knowledge from tons of successful projects, many years of real-world experience, and no mercy for misconfigurations or insecure solutions! 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

Certification

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.

Target Audience

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

Agenda

Module 1: Understanding Windows Platform

1. Introduction to the Windows 10/11 and Windows Server security concepts
2. Architecture overview
3. Key System Components
    a. Processes, Threads and Jobs
    b. Services, Functions and Routines
    c. Sessions
    d. Objects and Handles
    e. Registry
4. Rights, permissions and privileges
5. Access Tokens
6. Win32 API

Module 2: Modern Attack Techniques

1. Discussion: Top attack techniques
2. Advanced Persistent Threats
3. Initial access vectors
    a. Phishing – rev shell mail phishing bob
    b. Valid Credentials– password spray exc.
    c. Spoofing – DSN Twist
    d. Vulnerable components (drive by download)
    e. Weak defaults
    f. Other vectors

Module 3: Local Privilege Escalation Techniques

1. Escalation through Windows Services
    a. Unquoted service path
    b. Image and DLL manipulation
2. Schedule Tasks
3. Access Token Manipulation
    a. SeImpersonate
    b. SeTcb
    c. Create User Token
4. Process Injection
5. DLL Injection and Reflective DLL Injection
6. CreateRemoteThread
7. Process memory (powerpick / psinject)
8. Memory Injection
9. Other techniques

Module 4: Securing Offline Access

1. Offline Access techniques
2. TPM Architecture
3. Implementing BitLocker
4. Discussing BitLocker

Module 5: Windows Authentication

1. Architecture & Cryptography
    a. Windows Logon
    b. Windows Logon Types
    c. LSASS Architecture
    d. NTLM
    e. Kerberos
    f. Token Based Authentication - PRT
2. SAM Database
3. NTDS.dit
4. LSA Secrets & gMSA accounts
5. Secrets, credentials and Logon Data
6. SSP Providers
7. Data Protection API

Module 6: Attacks On Identity Infrastructure

1. Pass-the-Hash, OverPTH attacks
    a. Pass the ticket
    b. Golden and silver ticket
    c. Pass the PRT
    d. Shadow Credentials / NGC

2. NBNS/LLMNR spoofing, NTLM Relay, Kerberoasting

3. DCSync and DCShadow

4. AdminSDholder
5. Other identity attack techniques

Module 7: Protecting Identity in the Modern Infrastructure

1. Credential Guard
2. LAPS
3. LSA Protection
4. SMB Signing and Encryption
5. Managing Krbtgt
6. Detection of the identity attacks
7. Monitoring AD Infrastructure
8. Analyzing complex AD infrastructure (Bloodhound, Pingcastle etc.)

Module 8: Hybrid Deployment

1. Hybrid Identity
2. Account synchronization using Azure AD Connect
3. Password Hash Synchronization
4. Pass-through Authentication
5. Seamless SSO
6. Federation with Active Directory Federation Services

Module 9: Attack and protection of MSSQL

1. Offline access
2. TDS Injection
3. Weak Authentication Schema
4. Securing MSSQL server instance
5. TDE Encryption
6. Extracting credentials

Module 10: Secure Active Directory Certificate Services (PKI)

1. Reviewing misconfigurations
2. Misusing certificates
3. Implementing best practices
4. Kill-Chain with certificates

Module 11. Windows Infrastructure Services

1. Securing and monitoring DNS Service
2. Securing and monitoring Internet Information Services
3. Securing the File Server

Module 12: Securing Windows Platform

1. Malware protection approach
2. Implementing Application Whitelisting
3. Configuring Exploit Guard
4. Attack Surface Reduction Rules
5. Controlled Folder Access
6. Reviewing security benchmarks

Summary: Top 50 tools: the attacker's and defender’s best friends

1. Practical walkthrough through tools
2. Tools for Red Team / Pentesters
3. Tools for Blue Team