Introduction to Pentesting Course (IPC)

Cursusduur: 3 Dagen **Cursuscode: IPC**

Beschrijving:

CQURE Academy focuses on professional knowledge sharing in different areas and for various audiences – CxOs, IT Pros and the end-users as well.
We provide exceptional trainings for IT Security Professionals worldwide, having over 40 deep-dive courses and workshops in our portfolio to choose from. CQURE Academy is also known for its customized and bespoke Masterclasses, that are tailored to client's needs and infrastructure. We have experience in delivery of customized cybersecurity training to professionals from various organizations, including the governmental organizations, law enforcement, military and other critical infrastructure sectors.
For those who would like to expand their skills at their own pace, CQURE Academy offers a variety of on-demand courses on different levels of difficulty and specialization.
Each of CQURE courses complements the idea to become somebody that we call a "Security Expert2.0" – a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in systems, how do they work, how to investigate them, establish monitoring and make all the skills useful while working within the organization. Security Expert 2.0 can also work with the IT and business experts at the same time. Currently, on the market there are many certifications and trainings available, but quite often they offer advanced technological knowledge but omit its fundamentals. How can you be security experts without knowing why attacks happen? Security Expert 2.0 knows. In details!
Each class delivers a dose of practical experience as it contains cases and examples from the real-life projects. We know that well-grounded knowledge is a key to success, so we have introduced the approach described below to assure the best quality in education: We cover fundamentals on Windows Security and Management, so that when vulnerability occurs or something unexpected happens, you will be able to understand the background of an issue and can fix it. Our fundamentals are not that basic though!We include deep-dive monitoring techniques so that when a problem with availability, confidentiality or performance pops up – who are they going to call? You!We bring the specialization within hacking and securing infrastructure. Hacking is to understand what the weakest points are and how to use them – good engineers think "how things can be made to work" and good security experts think "how things can be made to fail!". Securing brings a great value, as it teaches you how to become hacker-resistant and what interesting settings and solutions you can bring into practice!We bring in the specialization within certain subjects, as we value knowledge about security related topics and widely used technologies.

Examens en certificering

After the completion of our all of our Masterclasses, Workshops and selected On-Demand courses we provide our students with an **online certification**.

What is wonderful about our certificate is that it is lifetime valid - technology changes, but fundamentals and attitude remain mostly the same. Our Virtual Certificates, which **entitle you to collect CPE Points**, are issued via **Accredible** – an online platform equipped with some superb features like: easy online access to the Certificate and the Badge, and the "Add to LinkedIn" button in case you would like to share the certificate with your colleagues.

To be sure you stay secure, Accredible uses a **Blockchain** verification and bank-level encryption in order to control and manage all the certification processes. This platform provides our alumni with an easy access to their certificates, protects their data and provides an easy method of sharing the information about their acquired competences.

Cursusinhoud:

You will enjoy it! This course serves as an introductory course for performing internal and web application penetration testing. Our course has been developed around professional penetration testing and security awareness in the business and IT fields.

During the course you will learn how to pick the right methodology for your project and acquire the skills on how to successfully perform target reconnaissance and get valuable data on the objective. Later on, we will go through various aspects of Web Application Pentesting and review the key concepts of web app security.

We will also familiarize ourselves with Web Application pentester’s best friend: the Burp Suite. Afterwards we will go through the OWASP Top 10 for 2021 to get a better understanding of top vulnerabilities to look for during our work. During the final stage of the training, we will guide you through various methods of infrastructure penetration testing. We will learn how to determine the attacks scope, discover vulnerable services and configurations.

After we have successfully prepared for the pen-test, the next steps will be to weaponize and in this chapter we will undergo the preparation of malicious payloads and reverse shells. As soon as we have gained the access to the target system, we will try various methods of privilege escalation and lateral movement.

To make sure that all participants gain the necessary security concepts and knowledge, our classes have an intensive hands-on labs format and we have prepared tons of exercises that you will be able to perform even after the course concludes, as we will grant you an extra 3-weeks of lab access. The knowledge used to prepare the unique content of this amazing course has been gathered during tons of penetration testing projects done all around the world by CQURE Experts.

The training will allow you to understand the penetration tester’s perspective on security, and learn crucial tools and concepts needed for everyone considering developing their career in penetration testing or cybersecurity in general. Every exercise is supported by lab instructions and multiple tools, both traditional and specialized. CQURE trainers recommend students have some knowledge of security concepts, such as operating system services

- Discovering hidden secrets

Module 4: Web Applications

- Introduction to HTTP
- Modern web applications, frameworks and web programming languages
- Client and server-side security
- The hidden gems of web browsers
- The role of web-proxy

Module 5: Introduction to Burp Suite

- Tool overview
- Community and Pro features
- Basic web attacks using Burp Suite
- Work automatization
- Useful extensions

Module 6: Introduction to Web Attacks

- OWASP TOP 10 project
- OWASP TOP 10 for 2021
- Discovering Access Control issues
- Injections attacks
- SQL Injection attacks
- Insecure file inclusions
- Web attacks and Remote Code Execution

Module 8: Using and creating offensive security tools

- Programing languages for offensive tasks
- Types of shells
- Generating reverse shell
- Generating web shell
- Bypassing firewalls
- Finding exploits
- Reviewing and fixing public exploits

Module 9: Security solutions

- Security solutions on modern systems
- Yara rules
- Bypassing Anti-Virus and EDRs
- Alternative file types
- Living Off the Land Binaries

Module 10: Privilege escalation

- How Windows access control works?
- Attacking services
- Attacking file system
- Accessing system secrets
- Mimikatz

and architecture. However, all required concepts will be covered throughout the course.

Module 1: Introduction to Penetration Testing

- Functional issue or security issue?

- What is Penetration Testing?

- What skills should Pentester have?

- The best operating system, web browser and other tools

- Cyber Kill Chain

Module 2: Performing security testing

- Testing methodologies

- Measuring severity of an issue

- Risk matrix and CVSS score

- Vulnerabilities and Risks

- The role of automatization

- What defines a test scope?

- How to create good report?

- Useful reporting tools

Module 3: Reconnaissance

- Why is recon needed?

- Open-Source Intelligence (OSINT)

- Google hacking and alternative search engines

- DNS and WHOIS databases

Module 7: Infrastructure penetration testing

- Infrastructure as entry point

- Modern architecture

- Introduction to TCP and UDP

- Nmap – powerful port scanner

- Nmap scripts

- Ncat – netcat for 21st century

- Vulnerable default configurations

Module 11: Lateral movement

- Sniffing

- Gathering network information

- Bloodhound

- Pass-The-Hash family attacks

- Critical Active Directory issue

- Subdomain enumeration
- Social Media Intelligence (SOCMINT)
- Public services enumeration

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein