Masterclass: 360 pentesting course

Duration: 5 Days **Course Code: 360PTC** **Delivery Method: Virtual Learning**

Overview:

You will enjoy it! This all-round course teaches strategy and advanced techniques for performing internal infrastructure as well as web application penetration testing in highly secure environment.
This penetration testing course has been developed around professional penetration testing and security awareness in the business and IT fields.
During this course you will learn how to pick the right methodology for your project and later on you will learn how to perform a detailed reconnaissance on your target utilizing a vast range of tools and techniques, including OSINT, SOCMINT, Google dorking and public services enumeration.
The course will also teach you the most demanded Windows infrastructure and web applications penetration testing skills. Together we will prepare malicious payloads and reverse shells. We will also learn how to create successful phishing campaigns and create payloads utilizing office suite macros.
After we gain access to the target infrastructure, we will learn how to perform further exploitation and privilege escalation to reach our goal. In the latter part of the course we will focus on the web application penetration testing aspects.
Together we will review the key security issues related to web applications security and exploit them in practice in CQURE's custom-built training environment.
During this intense 5-day class we will also learn advanced features of industry-standard tools such as the Kali Linux, Burp Suite, Bloodhound, Metasploit and the Wireshark. To make sure that all participants gain the necessary infrastructure 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 all around the world by CQURE's world-renowned Experts. The training will allow you to prepare for penetration testing projects or red team exercises.. Every exercise is supported with lab instructions and multiple tools, both traditional and specialized.

Target Audience:

Pen-testers, red teamers, Windows network administrators, security professionals, systems engineers, IT professionals, security consultants and other people responsible for implementing infrastructure security.

Objectives:

- **After completing this course you should be able to:**
- Identify security profile of the target
- Perform the testing activities
- Figure out protection oportunities
- Optimize security controls to reduce risks

Prerequisites:

You should have at 3-5 years of experience in cybersecurity to attend this training or have successfully completed one of the following CQURE Academy courses: • Introduction to Pentesting Course • 30 Days to Web Application Pentesting Course You should have a good understanding of Windows infrastructure security concepts and features. Before attending this course, you should also be familiar with basic hacking tools and Kali Linux.

Content:

Module 1: Introduction to Penetration Testing • What is Penetration Testing • Cyber Kill Chain • MITRE ATT;CK Matrix • Testing methodologies • Reporting

Module 2: Reconnaissance • Open-Source Intelligence (OSINT) • Social Media Intelligence (SOCMINT) • Google hacking and alternative search engines • Subdomains and DNS enumeration • Public services enumeration • Discovering hidden secrets

Module 3: Infrastructure penetration testing • Modern company, systems and solutions • Determining attack scope • Discovering services • Attacking services • Vulnerable default configurations

Module 4: Weaponization and delivery • Generating malicious payloads • Office Suite macros • Reverse shells • Evasion techniques • Command and Control • Securing C2 environment • Building and executing phishing campaigns • Physical toolkit

Module 5: Exploitation and Installation • Types of vulnerabilities • Exploit development • Bypassing system guards • Living Off the Land Binaries • Stealth communication channels

Module 6: Privilege escalation • Token and privileges • Attacking services • Attacking file system • Accessing system secrets

Module 7: Lateral movement • Responder • Pass-The-Hash family attacks • Bloodhound • Critical Active Directory misconfigurations • Lateral movement within AD

Module 8: Introduction to Web Application testing • Modern Web standards and protocols • Modern Web languages and libraries • OWASP TOP 10 • Role of web-proxy • Work automatization • Business and logic issues • Supply chain attacks and vulnerable components • Chaining security issues • SSL/TLS issues • Information disclosures

Module 9: Browser's security mechanisms • Same Origin Policy • CORS and other exceptions • Security headers • Cookies' and local storage security • Differences across implementations

Module 10: Cross Site Scripting • Reflected and Stored Cross Site Scripting • Attacking Document Object Model • DOM clobbering • Bypassing weak CSP • Dangling markups

Module 11: Injections • Blacklisting vs whitelisting • SQL injections • Command injections • Header splitting and injection • Other injection attacks

Module 12: Authentication and Authorization • Attacks on authentication and authorization • Attacks on sessions • Insecure Direct Object Reference (IDOR) attacks • Default credentials • JSON Web Tokens • SAML • OAuth

Module 13: Insecure file handling • Path traversal • Content manipulation • Insecure file extensions

Module 14: Insecure inclusions • Local File Inclusion • Remote File Inclusion

Module 15: Testing API • OWASP Top 10 for API • Bypassing API access controls • Mass assignment attacks

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/