Learn from the Experts

Masterclass:Hacking and Hardening Hybrid Environment

Security Tips from Expert who has access to a Source Code of Windows!

Duration: 3 days

Michael Jankowski-Lorek is a Solutions architect

He designs and implements solutions for Databases, Network & Management area, mainly for Microsoft platform.

He also designs and administers IT Infrastructure based on Microsoft systems and network solution from CISCO.

He is currently finishing PhD thesis in which he is combining academic knowledge, professional experience and strong technical skills.

Everyone has heard about hackers. It is commonly known that their jobs differ from system administrator jobs. However, things they do in their darkened rooms are definitely interesting and worth knowing. Many of the techniques they use are very useful in everyday administration tasks. Is it that easy to get into systems? What about Windows and hybrid environments – are all of these security features preventing all of the attacks possible before? Well no! And we need to know how to implement features properly in order to be on a safe side! Windows solutions and Azure are designed to protect against known and emerging security threats across the spectrum of attack vectors but this can be achieved only when configuring these settings properly! A Hackers' knowledge is considered to be valuable, both by system creators and common users. Administrators do not have to be taught how to be a hacker; it is often enough to show them one simple, but very interesting tool or technique, to change the point of view on their own IT environment. Topics covered in this seminar help you to walk in hacker's shoes and evaluate your network from their point of view. Be careful – this workshop is designed for IT and Security professionals who want to take their skills and knowledge to the next level. After this workshop, you will be familiar with hacker techniques, which can be useful to protect yourself against. This is a two days training with demos and reasonable and smart explanations.

Audience

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

Materials

Author's unique tools, presentations slides with notes, workshop instructions.

Certification

At the end participants will receive the online Certificate of attendance signed by the CQURE Speaker.

Formatech
INTEGRATED LEARNING CENTERS
Learn from the Experts

Agenda

Module 1: On premise security: Windows 10 / Windows Server 2016 solutions

This module introduces security solutions built-in the operating system.

1. Detecting unnecessary services
2. Misusing service accounts
3. Services architecture
4. Implementing rights, permissions and privileges
5. Integrity Levels
6. Usage of privileged accounts
7. Browser security
8. Access tokens
9. Information gathering tools
10. PowerShell v5 as a hacking tool
11. Security management automation
12. Security in hybrid environments
13. Containers
14. Nano Server for Windows Server 2016

Module 2: Malicious activities: attacks on Identity and malware

This module involves various attacks on identity, mitigations and risk assessment factors. You will learn techniques used by modern malware. Especially for ransomware the launch process itself has changed over years to reach its final form – it is important to know how to prevent it.

1. Extracting hashes from SAM and NTDS.dit databases
2. Meaning of SYSTEM and SECURITY registry hives
3. Kerberos and NTLMv2 issues
4. Performing the Pass-The-Hash attack
5. Cached logons (credentials)
6. Data Protection API (DPAPI) case for cached logons
7. Credential Guard (Virtual Secure Mode)
8. Application Whitelisting (AppLocker, Device Guard)
9. Code signing techniques
10. Cloud-based malware protection
11. Performing the LSA Secrets dump and implementing prevention
12. Implementing account scoping
13. Good practices for implementing Local Admin Password Solution
14. Windows Defender Advanced Threat Protection
15. Cloud based monitoring
16. Authentication Mechanism Assurance
17. Using virtual smart cards
18. Multi-factor Authentication

Module 3: In cloud and hybrid security: managing hybrid environments

In this module you will become familiar with important aspects of cloud security including easy to use solutions, integration with the current environment and monitoring tools.

1. Shielded VMs
2. Storage Encryption
3. Just Enough Administration
4. Desired State Configuration
5. Azure Information Protection
6. Microsoft Operations Management Suite
7. Active Directory and Azure AD security
8. Multi Factor Authentication with Azure

Module 4: Attacking and Securing Windows Network Solutions

Starting from simple network sniffing, ending up with advanced network monitoring to the size of the buffers written. Several techniques used during the training.

1. Monitoring network usage by processes
2. Port scanning techniques
3. Vulnerability scanning
4. Network Protocols
5. Name Resolution Attacks
6. SMB Relay attack and enabling SMB signatures
7. Implementing IPSec and DNSSec
8. Detecting attacks with Machine Learning
9. Internet Information Server Security
10. Advanced Threat Analytics

Module 5: Windows Security Summary

Module covers discussion about solutions and implementations with top priorities.