Masterclass: Hacking and Hardening Windows Infrastructure Workshop

Including Windows 10 and its new security features! Can Windows 10 be hacked?!

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

Duration: 1 day

Paula Januszkiewicz is a world-renowned Security Expert. Paula loves to perform Penetration Tests, IT Security Audits, and after all she says: 'harden'em all'! Enterprise Security MVP and trainer (MCT) and Microsoft Security Trusted Advisor.

Top-speaker at world known conferences, including being No 1 speaker at Microsoft Ignite!

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 10 – 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 10 is 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 one day training with demos and reasonable and smart explanations.

Paula says: *Pure coolness with a value! This training shows how to overuse mistakes that are made nowadays in the infrastructures. It is great to learn from other people's mistakes, right?*

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

All rights reserved. All content (texts, trademarks, illustrations, photos, graphics, files, designs, arrangements etc.) of CQURE agendas is protected by copyright and other protective laws. Copying, duplicating and diffusing the content without CQURE's permission is formally forbidden and may result in financial penalty.

Agenda

Module 1: Windows 10 / Windows Server 2016 - Platform Security and Internals

This module will prepare you for the training! It also contains very useful tips about auditing your environment and understanding security mechanisms used by Windows.

a. Detecting unnecessary services
b. Misusing service accounts
c. Services architecture
d. Implementing rights, permissions and privileges
e. Integrity Levels
f. Usage of privileged accounts
g. Browser security
h. Registry internals
i. Monitoring registry activity
j. Boot configuration
k. Access tokens
l. Information gathering tools
m. PowerShell as a hacking tool
n. Security management automation

Module 2: Attacks on Credentials and Prevention Solutions

This module involves usage of the custom tools built by the CQURE Team. Some of the tools were first on the market, so you are learning from the best!

a. Extracting hashes from SAM and NTDS.dit databases
b. Meaning of SYSTEM and SECURITY registry hives
c. Kerberos and NTLMv2 issues
d. Performing the Pass-The-Hash attack
e. Performing the Pass-The-Ticket attack
f. Cached logons (credentials)
g. Data Protection API (DPAPI) case for cached logons
h. Credential Guard (Virtual Secure Mode)
i. Performing the LSA Secrets dump and implementing prevention
j. Implementing account scoping
k. Good practices for implementing Local Admin Password Solution
l. Authentication Mechanism Assurance
m. Using virtual smart cards

Module 3: Attacking and Securing Windows Network

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

a. Monitoring network usage by processes
b. Monitoring network stack (stackwalk)
c. Building a network visibility map
d. Host identification
e. Port scanning techniques
f. Vulnerability scanning
g. Sniffing techniques
h. Active sniffing: ARP cache poisoning and DNS spoofing
i. IP address spoofing
j. NETBIOS issues
k. SMB Relay attack
l. Enabling SMB signatures
m. Implementing IPSec and DNSSec

Module 4: Handling Ransomware and Other Malicious Software

In this module you will become familiar with the 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.

a. Analysis of Malware Samples
b. Virus, Worms, Trojans and Spywares
c. Detection of Malicious Code
d. Implementation of Ransomware prevention
e. Application Whitelisting (AppLocker, Device Guard) and EMET
f. Code signing techniques

Module 5: Offline Access – Threats and Prevention

Offline access is immediately rewarding the attacker: you do not have to try hard to get the highest privileges and possibility to change anything you want on a drive. In this module you will learn the impact of offline access and how according to best practices we can prevent it.

a. Misusing USB and other ports
b. Offline Access techniques
c. Implementation of the BitLocker in the enterprise scale

Module 6: Windows Security Summary

Module covers discussion about solutions and implementations with top priorities.

All rights reserved. All content (texts, trademarks, illustrations, photos, graphics, files, designs, arrangements etc.) of CQURE agendas is protected by copyright and other protective laws. Copying, duplicating and diffusing the content without CQURE's permission is formally forbidden and may result in financial penalty.