

Geraardsbergsesteenweg 117A
9860 Oosterzele
Belgium

+32 478 288375
pieter.gheysens@sparkles.be
www.sparkles.be



Windows Security Master Class
with Paula Januszkiewicz

March 19 – March 21, 2012
Belgium (TBD)



Overview

The deep dive Windows Security Master Class teaches advanced Windows operating system security, based on Windows 7, Windows 8 and Windows Server 2008 R2, with comparison to older Microsoft operating systems.

During Advancing Windows Security Master Classes you will learn how to:

- Configure Windows Internals security (advanced)
- Perform advanced troubleshooting
- Configure efficient monitoring and what are the monitoring points
- Establish an operating system protection
- Get access to Windows in unauthorized way



Format

The training is a mix of theory and practical implementation, based on best practices and personal experiences of the teacher. Attendees get the workbook and useful tools to use later on everyday tasks.

Target Audience

Any experienced network administrator and infrastructure architect will benefit from the training. Some exposure to the basics of operating system security concepts is helpful. It is recommended students have some knowledge of security concepts, such as operating system services and architecture. However, all required concepts will be covered throughout the course.

Date & Location

March 19 – March 21, 2012 (3 days)

Belgium (TBD)



Teacher



Paula Januszkiewicz is the IT Security Auditor and Penetration Tester, Enterprise Security MVP, trainer (MCT) and Microsoft Security Trusted Advisor. She is also a top speaker at many international conferences (incl. TechEd North America, TechEd Middle East and TechEd Europe and other) and writes articles on Windows Security. The trainings she conducts usually cover Security, Windows operating system topics and Virtualization. Paula is passionate about sharing her knowledge with others. She conducted many IT security audits and penetration tests – these are her everyday tasks. She drives her own company CQURE. Paula is the leader of the Women in Technology group in Poland. In private, she enjoys researching new technologies and describes them on her blog <http://blogs.technet.com/plwit>. She is also a co-author of the Microsoft Forefront Threat Management Gateway 2010 book. She will be speaking on RSA China 2011 conference!

Latest public sessions @ TechEd North America 2011

- [Rethinking Cyber Threats: Experts Panel](#)
- [Network Layers \(in\) Security](#)
- [Unmasking Administrator's Evil](#)



Price

The cost for this intensive 3 day Master Class is **1500,- euro** (taxes not included). This price includes your participation to the Master Class, coffee/tea, lunch and the printed materials presented during the Master Class.

Early bird price of 1300,- euro until January 1, 2012.

Payment in advance is required to book your seat for the Master Class. Limited places available: first come, first served. Registration is only complete and will be confirmed after payment. Transfer the total amount of your fees by bank transfer to the account of Sparkles: 733-0567754-43 (use your full name in the message) or use the IBAN code for international payment: IBAN BE 66 7330 5677 5443 (BIC code: KREDBEBB).

Cancellation is possible up to 3 weeks before the seminar - if received in writing. In this case, 25% of the total amount is charged for administration. Otherwise, the full registration fee is due, regardless of the reason of cancellation. Replacement is possible at no extra charge.



Outline Windows Security Master Class

Windows Internals

- Introduction to the Windows 7/ Windows „8“/ Windows Server security concepts
- Operating system files security
- Passwords security (techniques of getting passwords and techniques of cracking)
- Process Monitoring (Advancing Process Explorer, Process Monitor and other tools)
- Integrity Levels
- Session Zero
- Priorities in operating system (influencing the operating system continuity)
- Kernel Mode vs. User-Mode Execution
- Driver Signing (Windows Driver Foundation)
- Advanced privileges for operating system objects and rights
- User Account Control Virtualization
- Registry Internals
- Auditing privileges with PowerShell
- PowerShell for Security (deep-dive into Windows Internals) + Windows „8“ update
- WMI for Security

Infrastructure Security Solutions

- AppLocker & implementation techniques
- BitLocker & implementation techniques
- Advancing Security Configuration Wizard
- Advancing IPsec
- Advancing GPO
- Practicing Diagnosing and Recovery Toolkit
- Networking Services Security (DNS, DHCP, SNMP, SMTP and other)
- Volume Shadow Copy Service from the security perspective
- Tools

Debugging & Auditing

- Available Debuggers
- Working with Symbols
- Process Debugging
- Kernel-Mode Debugging
- User-Mode Debugging
- Setting up kernel debugging with a virtual machine as the target
- Debugging the booting process
- Crash Dump Analysis
- Auditing tools and techniques
- Monitoring Registry Activity
- Rootkit Detection



Points of Entry Analysis

- Offline Access
- Linux BackTrack /other tools vs. Windows Security: „Lets have fun!“
- Unpatched Windows and assigned attacks
- Advanced Network Sniffing
- Fingerprinting Techniques
- Enumeration Techniques
- Domain Controller Attacks
- Services Security
- Man-in-The Middle Attacks

Bonus Module: Wireless Hacking



Registration Windows Security Master Class

Send registration form to pieter.gheysens@sparkles.be or fax to +32 56 324372

Course Details

Date: March 19-21, 2012 (3 days)

Location: Belgium (TBD)

Teacher: Paula Januszkiewicz (CQURE)

Price: 1500,- euro (taxes not included) – early bird until January 1, 2012: 1300,- euro

Registration Details

Name:

Function:

Company:

Address:

ZipCode + City + Country:

Phone:

Fax:

Email:

Invoice for the attn. of:

Invoice address:

VAT number:

Date, Name and signature:

Invoice will be sent after registration. Payment details: KBC 733-0567754-43 or IBAN BE 66 7330 5677 5443 (BIC code: KREDBEBB). Cancellation is possible up to 3 weeks before the seminar - if received in writing. In this case, 25% of the total amount is charged. Otherwise, the full registration fee is due, regardless of the reason of cancellation. Replacement is possible at no extra charge.