

Advancing Windows Security

Opis szkolenia

Na szkoleniu omawiane jest bezpieczeństwo systemów Windows w oparciu o Windows 7, Windows 8 i Windows Server 2008 R2, a także porównanie do starszych systemów operacyjnych Microsoft.

Podczas zajęć można nauczyć się, jak:

1. Konfigurować zabezpieczenia systemu Windows (poziom zaawansowany)
2. Rozwiązywać problemy (w stopniu zaawansowanym)
3. Monitorować zachowanie systemu operacyjnego
4. Zaprojektować zabezpieczenia systemu operacyjnego

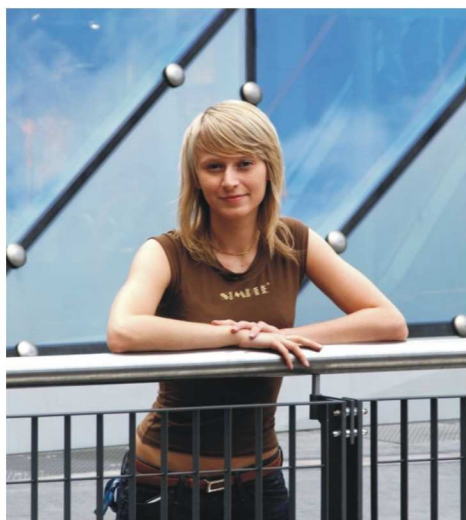
Forma szkolenia

Szkolenie jest połączeniem teorii oraz praktycznych przykładów i ćwiczeń, w oparciu o najlepsze praktyki i doświadczenia osobiste prowadzącego. Uczestnicy otrzymują podręczniki i użyteczne narzędzia do późniejszego wykorzystania w codziennej pracy oraz certyfikat ukończenia szkolenia podpisany przez trenera.

Grupa docelowa

Każdy doświadczony administrator sieci, architekt infrastruktury i programista, który chciałby zapoznać się z wewnętrznymi systemami zabezpieczeń Windows oraz związaną z systemem infrastrukturą.

Biografia



Paula Januskiewicz jest audytorem bezpieczeństwa systemów IT, wykonującym na co dzień testy penetracyjne oraz weryfikującym zabezpieczenia zarówno wewnętrzne, jak i styku z Internetem. Posiada tytuł Enterprise Security MVP, jest certyfikowanym trenerem (Microsoft Certified Trainer) oraz, jako jedna z dwóch osób w Polsce, posiada tytuł Microsoft Security Trusted Advisor. Paula była również nagradzana jako najlepszy mówca na wielu międzynarodowych konferencjach (prelegowała na TechEd North America, TechEd Middle East i TechEd Europe, i innych gdzie zajmowała pierwsze miejsca i uzyskiwała tytuły „prelegenta roku” np. Niemcy: ICE, Rumunia: IT-Camp itd.). Jest autorką artykułów na temat zabezpieczeń systemu Windows. Zwykle prowadzi autorskie szkolenia z zakresu bezpieczeństwa, tematów związanych z systemem Windows oraz wirtualizacji.

Pasją Pauli jest dzielenie się swoją wiedzą i doświadczeniem z innymi. Prowadzi własną firmę CQURE. Jest liderem grupy Women in Technology w Polsce. Prywatnie lubi zgłębiać nowe technologie i opisywać je na blogu: <http://blogs.technet.com/plwit>. Jest również współautorem uznanej angielskojęzycznej książki o Microsoft Forefront Threat Microsoft Management Gateway. W listopadzie 2011 r. będzie prelegentem na konferencji RSA China 2011!

Paula o kursie:

„Doskonale wiem, co ciekawi uczestników kursów o bezpieczeństwie: ataki na systemy Windows! Aby nadać odpowiedni ton szkoleniu zaczynamy właśnie od tej tematyki. Bardziej tradycyjne tematy kursu są omawiane w dniach drugim i trzecim. Dzień pierwszy pokazuje wszystkie sytuacje, jakie mogą wystąpić przy atakach na system operacyjny, reszta kursu uczy, że istnieją sposoby zwalczania i monitorowania tego, co uczestnicy kursu zobaczą na początku. Serdecznie polecam!”

Szczegóły kursu

Dzień 1: Wnętrze systemu Windows (wbudowane w system zabezpieczenia, wybrane słabości/podatności, zaawansowane prawa dostępu, mechanizmy ochrony haseł, rozwiązania kryptograficzne)

Dzień 2: Sieć Windows (monitoring i ochrona), zarządzanie zabezpieczeniami przy wykorzystaniu PowerShell

Dzień 3: Zaawansowane rozwiązywanie problemów i monitoring (kontrola złośliwego oprogramowania, monitorowanie poszczególnych zdarzeń w systemie operacyjnym, wprowadzenie do debugowania)

Advancing Windows Security

Module 1: Windows Internals

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

Module 2: Infrastructure Security Solutions

1. AppLocker & implementation techniques
2. BitLocker & implementation techniques
3. Advancing Security Configuration Wizard
4. Advancing IPsec
5. Advancing GPO
6. Practicing Diagnostic and Recovery Toolkit
7. Networking Services Security (DNS, DHCP, SNMP, SMTP and other)
8. Volume Shadow Copy Service from the security perspective

Module 4: Points of Entry Analysis

1. Offline Access
2. Linux BackTrack /other tools vs. Windows
3. Security: „Lets have fun!”
4. Unpatched Windows and assigned attacks
5. Advanced Network Sniffing
6. Fingerprinting Techniques
7. Enumeration Techniques
8. Domain Controller Attacks
9. Services Security

Module 3: Debugging & auditing

1. Available Debuggers
2. Working with Symbols
3. Process Debugging
4. Kernel-Mode Debugging
5. User-Mode Debugging
6. Setting up kernel debugging with a virtual machine as the target
7. Debugging the booting process
8. Crash Dump Analysis
9. Auditing tools and techniques
10. Monitoring Registry Activity

Module 5: Wireless Hacking

1. Wireless technology recognition
2. Wireless fingerprinting
3. Wireless hacking ideas and demos
4. Optimizing wireless hacking

BizTech Consulting SA

01-018 Warszawa

ul. Wolność 3A

tel. 22 100 10 10

e-mail: szkolenia@biztech.pl, www.biztech.pl

BIZTECH
E D U K A C J A