Masterclass: Hacking Windows Infrastructure

Duration: 2 days

Paula Januszkiewicz is a word-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!

In this workshop you will investigate the critical tasks for a high-quality penetration test. We'll look at the most efficient ways to map a network and discover target systems and services. Once it has been done, we will search for vulnerabilities and reduce false positives with manual vulnerability verification. At the end we will look at exploitation techniques, including the use of authored and commercial tools. In the attack summary we will always go through the securing techniques.

Exploits are not the only way to get to systems! We will go through the operating systems' build in problems and how they can be beneficial for hackers! One of the most important things to conduct a successful attack is to understand how the targets work. *To the bones*! After that everything is clear and the tool is just a matter of our need.

The course that covers all aspects of Windows infrastructure security from the hacker's mind perspective! Our goal is to show and teach you what kind of mechanisms are allowing to get inside the infrastructure and how to get into operating systems. **After the course you will gain penetration tester's knowledge and tools. And to get more practice we offer one extra week of labs online!**

We really want you to leave from the class with practical, ready-to-use knowledge of how to get into the infrastructure.

This is a deep dive course. It is a must-go for enterprise administrators, security officers and architects. Delivered by one of the best people in the market in the security field – with practical knowledge from tons of successful projects, many years of real-world experience, great teaching skills and **no mercy for misconfigurations or insecure solutions! The course has a form of intense workshop and you MUST stay awake just not to miss a thing!**

All exercises are based on Windows Server 2012 R2, Windows 8.1 and Windows Server 2016, Windows 10.

Target audience

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

Prerequisites

To attend this training you should have good hands-on experience in administering Windows infrastructure. At least 8 years in the field is recommended.

Materials

Author's unique tools, over 150 pages of exercises, presentations slides with notes.

Agenda

Module 1: Hacking Windows Platform

a) Detecting unnecessary services
b) Misusing service accounts
c) Implementing rights, permissions and privileges
d) Direct Kernel Object Modification

Module 2: Top 50 tools: the attacker's best friends

a) Practical walkthrough through tools
b) Using tools against scenarios

Module 3: Modern Malware

a) Techniques used by modern malware
b) Advanced Persistent Threats
c) Fooling common protection mechanisms

Module 4: Physical Access

a) Misusing USB and other ports
b) Offline Access techniques
c) BitLocker unlocking

Module 5: Intercepting Communication

a) Communicating through firewalls
b) Misusing Remote Access
c) DNS based attacks

Module 6: Hacking Web Server

a) Detecting unsafe servers
b) Hacking HTTPS
c) Distributed Denial of Service attacks

Module 7: Data in-Security

a) File format attacks for Microsoft Office, PDF and other file types
b) Using incorrect file servers' configuration
c) Basic SQL Server attacks

Module 8: Password attacks

a) Pass-the-Hash attacks
b) Stealing the LSA Secrets
c) Other

Module 9: Hacking automation

a) Misusing administrative scripts
b) Script based scanning