Masterclass: Hacking and Securing Windows Infrastructure

Duration: 5 days

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!

For so many years we have been asked to create a course like this! This course is just a great workshop that teaches how to implement securing technologies one at a time. The course covers all aspects of Windows infrastructure security that everybody talks about and during the course you will learn how to implement them! Our goal is to teach you how to design and implement secure infrastructures based on the reasonable balance between security and comfort with great knowledge of attacker's possibilities.

This is a deep dive course on infrastructure services security, a must-go for enterprise administrators, security officers and architects. It is 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. In this workshop you will investigate the critical tasks for a high-quality penetration test. We will 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.

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

Exploits are not the only way to get to systems! We will go through the operating systems' build in problems and explore 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*! Afterwards everything is clear and the tool is just a matter of our need.

The course 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. To get more practice we offer one extra week of labs online!

The course is an intense workshop! During these 5 days we provide caffeine candies – this course is really intense and in order not to miss a thing you MUST stay awake!

All exercises are based on Windows Server 2012 R2, Windows 8.1 and Windows Server 2016, Windows 10. This course is based on practical knowledge from tons of successful projects, many years of real-world experience and no mercy for misconfigurations or insecure solutions!

Prerequisites:

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

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.

Materials

Author's unique tools, over 200 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

Module 10: Designing Secure Windows Infrastructure

On the market there are thousands of solutions available to enrich security in our infrastructure. Idea of this module is to provide the complete knowledge and to gain the holistic approach to the areas that can be secured and the measures that can be implemented.

Module 11: Securing Windows Platform

a) Defining and disabling unnecessary services
b) Implementing secure service accounts
c) Implementing rights, permissions and privileges
d) Driver signing

Module 12: Malware Protection

a) Techniques used by modern malware
b) Malware investigation techniques
c) Analyzing cases of real malware
d) Implementing protection mechanisms

Module 13: Managing Physical Security

a) Managing port security: USB, FireWire and other
b) Mitigating Offline Access
c) Implementing and managing BitLocker

Module 14: Deploying and configuring Public Key Infrastructure

a) Role and capabilities of the PKI in the infrastructure
b) Designing PKI architecture
c) PKI Deployment – Best practices

Module 15: Configuring Secure Communication

a) Deploying and managing Windows Firewall – advanced and useful features
b) Deploying and configuring IPsec
c) Deploying secure Remote Access (VPN, Direct Access, Workplace Join, RDS Gateway)
d) Deploying DNS and DNSSEC

Module 16: Securing Web Server

a) Configuring IIS features for security
b) Deploying Server Name Indication and Centralized SSL Certificate Support
c) Monitoring Web Server resources and performance
d) Deploying Distributed Denial of Service attack prevention
e) Deploying Network Load Balancing and Web Farms

Module 17: Providing Data Security and Availability

a) Designing data protection for Microsoft Office, PDF and other file types
b) Deploying Active Directory Rights Management Services
c) Deploying File Classification Infrastructure and Dynamic Access Control
d) Configuring a secure File Server
e) Hardening basics for Microsoft SQL Server
f) Clustering selected Windows services

Module 18: Mitigating the common password attacks

a) Performing Pass-the-Hash attack and implementing prevention
b) Performing the LSA Secrets dump and implementing prevention

Module 19: Automating Windows Security

a) Implementing Advanced GPO Features
b) Deploying Software Restriction: Applocker
c) Advanced Powershell for administration