Masterclass: Hacking and Securing Windows Infrastructure

Duration: 5 Days **Course Code: HSW** **Delivery Method: Virtual Classroom**

Overview:

This course combines two intensive courses that are focused on the security of a windows infrastructure, Part one covers the Hacking of a Windows Infrastructure and part 2 the Securing of a Windows Infrastructure. During the first two days 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. Exploits are not the only way to get to systems! We will go through the operating systems 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. After that everything is clear we will have the tools to our disposal. This course covers all aspects of Windows infrastructure security from the hacker's mind perspective!
The final three days teaches you how to implement securing technologies one at a time. This part of the course covers all aspects of Windows infrastructure security that everybody talks about, but 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. We really want you to leave the
class with the practical, ready-use knowledge and skills to secure your Windows infrastructure.

Target Audience:

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing a secure network and Windows Infrastructure.

Objectives:

- **After completing this course you should be able to:**
- Hack and Secure your windows platform
- Understand the tools of the attackers
- Recognize and investigate moder malware
- Manage and Secure Physical Access
- Interceping and securing communication
- Deploy and configure PKI
- Secure the web server
- Mitigate common password attacks
- Automate windows Security.

Prerequisites:

Attendees should meet the following prerequisites:

- Good hands-on experience in administering Windows infrastructure. At least 8 years in the field is recommended.

Testing and Certification

Recommended as preparation for the following exams:

- This course does not align to any particular exam.

Content:

Module 1: Hacking Windows Platform

- Detecting unnecessary services
- Misusing service accounts
- Implementing rights, permissions and privileges
- Direct Kernel Object Modification

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

- Practical walkthrough through tools
- Using tools against scenarios

Module 3: Modern Malware

- Techniques used by modern malware
- Advanced Persistent Threats
- Fooling common protection mechanisms

Module 4: Physical Access

- Misusing USB and other ports
- Offline Access techniques
- BitLocker unlocking

Module 5: Intercepting Communication

- Communicating through firewalls
- Misusing Remote Access
- DNS based attacks

Module 6: Hacking Web Server

- Detecting unsafe servers
- Hacking HTTPS
- Distributed Denial of Service attacks

Module 7: Data in-Security

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

Module 8: Password attacks

- Pass- the - Hash attacks
- Stealing the LSA Secrets
- Other

Module 9: Hacking automation

- Misusing administrative scripts
- Script based scanning

Module 10: Designing Secure Windows Infrastructure

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

Module 11: Securing Windows Platform

- Defining and disabling unnecessary services
- Implementing secure service accounts
- Implementing rights, permissions and privileges
- Driver signing

Module 12: Malware Protection

- Techniques used by modern malware
- Malware investigation techniques
- Analyzing cases of real malware
- Implementing protection mechanisms

Module 13: Managing Physical Security

- Managing port security: USB, FireWire and other
- Mitigating Offline Access
- mplementing and managing BitLocker

Module 14: Deploying and configuring Public Key Infrastructure

- Role and capabilities of the PKI in the infrastructure
- Designing PKI architecture
- PKI Deployment – Best practices

Module 15: Configuring Secure Communication

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

Module 16: Securing Web Server

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

Module 17: Providing Data Security and Availability

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

Module 18: Mitigating the common password attacks

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

Module 19: Automating Windows Security

- Implementing Advanced GPO Features
- Deploying Software Restriction: Applocker
- Advanced Powershell for administration

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia