Masterclass: Advanced Active Directory Attacks

Duración: 3 Días   Código del Curso: AADA   Version: 1.2

Temario:

This is a deep dive workshop on Active Directory services security, a must-go for 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.
This workshop will present you the critical tasks performed by skilled attacker or pentester against Active Directory and its key components. The course focuses on attacks and security of Windows identity solutions.
Exploits are not the only way to get to the systems! We will go through the operating systems' builtin 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 workshop covers all aspects of Active Directory identity 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 organization. You will gain penetration tester's knowledge and tools.
The course is an intense workshop! During these 3 days you will not need your caffeine candies – this workshop is really intense and it will keep you awake all the time!

Dirigido a:

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

Prerequisitos:

- To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5 years in the field is recommended.

Exámenes y certificación

Contenido:

Module 1: Authentication protocols

a) NTLM

b) Kerberos

c) Claim based authentication

Module 2: Identity attacks

a) Pass-the-Hash attacks

b) Stealing the LSA Secrets

c) Modern identity attacks techniques

d) Password guessing, spraying a bruteforcing

e) MITM attacks, NBNS/LLMNR spoofing, NTLM Relay, Kerberoasting

f) Offline attacks, decrypting DPAPI a DPAPI-NG

g) Attacks against smart card authentication

Module 3: Active Directory attacker persistency

a) Archieving persistence, Skeleton Key, Golden Ticket attack

b) Windows Hello for Business Security, NGC keys

c) DCSync and DCShadow

d) AdminSDholder

Module 4: Mitigating the identity attacks

a) Pass-the-Hash attack prevention

b) LSA protection

c) Credential Guard

Module 5: Azure AD security

a) Stealing Azure AD tokens

b) Azure MFA and FIDO2 auditing

c) Azure AD application security

Información Adicional:

Unique exercises:
All exercises are based on Windows Server 2016 and 2019, Windows 10, Kali Linux and Azure Cloud. This workshop is based on practical knowledge from tons of successful projects, many years of real-world experience and no mercy for misconfigurations or insecure solutions!
Materials:
Author’s unique tools, presentations slides.
Platform and Technical Requirements:
To participate in the course you need a Stable internet connection. For the best learning experience we also need you to have a webcam, headphones and a microphone. Open RDP port 3391 for the connection to the Lab environment is needed as well. We will setup a secure Zoom classroom for every day of the course – we will send you a safe link to join the conference by e-mail.

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid