Virtuelt kursus
3 dage **DKK 14.999**
Nr. 91034 A ekskl. moms

Dato **Sted**

Masterclass: Advanced Active Directory Attacks [AADA]

Lær, hvordan du implementerer sikker Microsoft Active Directory-infrastruktur. På kurset kommer vi igennem alle de moderne angreb mod centrale Windows-identitetsløsninger, så du kan lære, hvordan du forhindrer dem! Vores mål er at vise dig, hvordan du gør dine AD-infrastrukturer sikre baseret på angriberes muligheder. Undervisningen foregår på engelsk med live underviser.

Deltagerprofil

Kurset er for dig, der fx er enterprise-administrator, infrastrukturarkitekt, sikkerhedsmedarbejder, systemtekniker, netværksadministrator, IT-fagperson, sikkerhedskonsulent eller dig, der har ansvar for at implementere netværks- og perimetersikkerhed.

Forudsætninger

Du skal have god praktisk erfaring med administration af Windows-infrastruktur for at deltage på kurset. Vi anbefaler, at du har mindst 8 års praktisk erfaring.

Udbytte

- Få den nødvendige viden til at beskytte dine Windows-indentitetsløsninger mod angreb
- Lær, hvordan du kan gøre dine AD-infrastrukturer sikre

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- Få penetrationstesterens viden og værktøjer

Det får du på arrangementet

- Øvelser og inddragelse
- Kursusbevis
- Erfaren underviser
- Maks. 12 deltagere
- Casearbejde
- Materiale på engelsk
- Undervisning på engelsk

Indhold

Module 1: Authentication protocols

- NTLM
- Kerberos
- Claim based authentication

Module 2: Identity attacks

- Pass-the-Hash attacks
- Stealing the LSA Secrets
- Modern identity attacks techniques
- Password guessing, spraying a brute-forcing
- MITM attacks, NBNS/LLMNR spoofing, NTLM Relay, Kerberoasting
- Offline attacks, decrypting DPAPI a DPAPI-NG
- Attacks against smart card authentication

Module 3: Active Directory attacker persistency

- Achieving persistence, Skeleton Key, Golden Ticket attack
- Windows Hello for Business Security, NGC keys
- DCSync and DCShadow
- AdminSDholder

Module 4: Mitigating the identity attacks

- Pass-the-Hash attack prevention
- LSA protection
- Credential Guard

Module 5: Azure AD security

- Stealing Azure AD tokens
- Azure MFA and FIDO2 auditing
- Azure AD application security

Form

Kurset er virtuelt med live underviser.

Før du deltager i det virtuelle kursus, vil vi altid forsøge at arrangere en testsession på 15 - 20 minutter en uges tid før, for at sikre, at du er i stand til at deltage i masterclassen. Herunder finder du kravene til at oprette forbindelse til det virtuelle kursus:

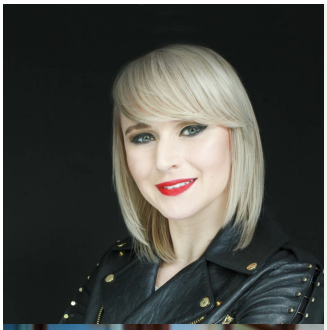
- En computer med en stabil internetforbindelse (skal helst køre Windows eller Mac OS).

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- Tilladelser til udgående RDP-forbindelser til eksterne servere (til vores laboratoriemiljø) – port 3389
- Et headset (hovedtelefoner og mikrofon)
- Webcam (indbygget eller tilsluttet)
- En ekstra skærm er nyttig, men ikke påkrævet

Materiale

Du får adgang til unikke værktøjer og præsentationsslides i løbet af kurset. Alle labs forbliver online i yderligere 3 uger, så du kan øve endnu mere, efter kurset er afsluttet. Alle øvelser er baseret på Windows Server 2016 og 2019, Windows 10 og Kali Linux.



UNDERVISER

Paula Januszkiewicz

Paula er verdenskendt som sikkerhedsekspert. Paula elsker at lave penetrationstests, IT-sikkerhedsevalueringer, og hendes motto er: "Harden em all!". Hun er Enterprise Security MVP og -underviser (MCT), og så er hun Microsoft Security Trusted Advisor.

UNDERVISER

Michael Grafnetter

Michael er ekspert i Windows Security, Microsoft Azure og PowerShell. Han har en kandidatgrad i softwareudvikling, og i begyndelsen af 2021 blev han tildelt Titlen Microsoft Azure Most Valuable Professional. Hans unikke DSInternals Framework afslører mange udokumenterede Active Directory-sikkerhedsfunktioner, og det er allerede blevet integreret i flere tredjepartsløsninger til identitetsstyring og Active Directory-genoprettelse efter nedbrud.

Har du faglige spørgsmål så kontakt

Malene Kjærsgaard
+45 72202523
mch@teknologisk.dk