>> Windows Server

Hackproofing Windows Domains

EGOS! the education company

Zur Erfüllung der Vorgaben geltender Sicherheitsframeworks, Richtlinien und Gesetzen ist es notwendig Windows Domains und Netzwerke regelmäßig zu prüfen und Hardening-Maßnahmen zu ergreifen.

Ihr Nutzen

Im Seminar erforschen Sie die Sicherheit in Windows-Netzwerken aus der Sicht eines Angreifers und lernen wie die erfolgten Angriffe durch gezielte Hardening-Maßnahmen abgewehrt werden können. Sie werden in einer geschützten Laborumgebung Angriffe selbst vorbereiten, durchführen, Härtungsmaßnahmen ausrollen und im Anschluss über erneute Angriffe deren Effektivität prüfen.

Preis pro Teilnehmer

EUR 2750,- exklusive der gesetzlichen MwSt.

Seminardauer

5 Tag(e)/Day(s)

Voraussetzungen

Grundlegende Windows Administrationskenntnisse

Hinweise

Version: 2025

Seminarinhalte

1. Tag: Unauthenticated Network Access
* Einführung in das Metasploit Framework und das Lab

* Übersicht über Angriffe auf Netzwerkebene

* Discovery: Netzwerkscanning

* Angriff: NTLM-Relaying und Hintergrundwissen zu NTLMv2

* Angriff: Poisoning und Spoofing
- LLMNR, NBT-NS, mDNS Poisoning
- ARP-Spoofing
- DNS-Poisoning

2. Tag: Credential Harvesting
* Angriff: NTLM Relaying über SMB und HTTP

* Hardening von LLMNR, NBT-NS, mDNS, NTLM, SMB

* Angriff und Hardening: Credential Brute Forcing

* Recon
- Finden von Kennwörtern
- anderen interessanten Informationen (Credentials in Files)

* Hardening: Credentials in Files

3. Tag: Active Directory: Certificate Services
* Recon und Angriff: Active Directory Zertifikatsdienste (ADCS)

* Hardening: ADCS

* Grundlagen von Kerberos

4. Tag: Active Directory: Kerberos und Endpoints
* Angriff und Hardening: AS-REP Roasting

* Angriff und Hardening: Kerberoasting

* Angriff: Credentials aus LSA auslesen

5. Tag: Active Directory: Endpoint
* Angriff
- Pass-the-Hash
- Overpass-the-Hash
- Pass the Ticket
- DCSync

* Hardening: LSA

* Grundlagen Kerberos Delegations

* Angriff
- Kerberos Unconstrained Delegations
- Kerberos Resource Based Constrained Delegations

* Hardening: Kerberos Delegations

* Auditing von Active Directory mittels BloodHound