TWEEDAAGSE TRAINING
'INFRASTRUCTURE HARDENING'

Wat is netwerk hardening? Wat maakt een infrastructuur veilig of onveilig? Wat is een DMZ en waar dient hij voor? Hoe maak ik optimaal gebruik van mijn Firewall? Welke maatregelen moet ik nemen om effectieve system hardening uit te voeren? Wat voorkom je met system hardening?

Deze en tal van andere vragen komen aan bod tijdens de tweedaagse training 'Infrastructure Hardening' van Secured by Design.

Dag 1 Theorie en praktijk

Op de eerste dag staat het concept en de noodzaak van infrastructure hardening centraal. Je krijgt inzicht in de attack vectors en de werkwijze van een hacker. Hoe komen hackers binnen en hoe worden systemen/infrastructuren gebruikt om het doel te bereiken? Je gaat zelf hiermee aan de slag in de labomgeving.

Dag 2: Praktijk

Op dag twee is het ontwerp en implementatie van een veilige omgeving de focus. Op basis van de labomgeving zal er een casus worden uitgewerkt. Deze casus zal erin resulteren dat de deelnemer een veilig ontwerp zal opstellen en deze implementeren in de labomgeving. Hierbij komen ook onderwerpen als server hardening aan bod. Gedurende deze training zul je hardening

Tijdens de workshop worden een aantal scenario's besproken over hackers en hoe deze gebruik maken van een 'klassieke' infrastructuur om hun doel te bereiken. Vervolgens zal het 'Security by Design' concept duidelijk maken welke principes gehanteerd dienen te worden in het ontwerp om deze weerbaarheid te vergroten.

Investering

De investering is €900,- per deelnemer.
Dit is inclusief:
- twee dagen training op locatie
- de workshop reader en het lesmateriaal

Voor wie?

- IT infrastructuur specialisten met persoonlijke of zakelijke interesse voor security.
- Netwerkbeheerders /-architect
- Systeembeheerders

SECURED BY DESIGN
UNITED BY KNOWLEDGE

TWEEDAAGSE TRAINING

'INFRASTRUCTURE HARDENING'

Onderwerpen

Attack vectors van hackers
Stepping stones voor hackers
Beperkingen en mogelijkheden van huidige infrastructuren
- *Protocollen (zoals HTTP, FTP, SSH)*
- *Services (zoals mail, web, DNS services)*

Virtualisatie en hardening

System Hardening
- *Windows*
- *Linux*

Netwerksegmentatie en het nut hiervan
- *Netwerk hardening*
- *De rol van een Firewall*

Voorkennis

De volgende voorkennis is van belang voor het volgen van de training:

Basics van netwerken; IP adressen, subnetten, MAC adres, Gateway
Basics van Operating Systems; Linux, Windows, Services

Na deze workshop kun je:

Zelfstandig een systeemhardening uitvoeren op zowel Windows als Linux
Zelfstandig een netwerkontwerp opstellen dat gebruik maakt van netwerksegmentatie
Zelfstandig effectieve Firewall regels opstellen
Een robuuste en weerbare infrastructuur ontwerpen

Contact info

A. Apollo Arena Gebouw (7e etage)
Herikerbergweg 31
1101 CN Amsterdam

E. security@securedbydesign.nl
T. 06 15 17 55 34

Aanmelden?

Direct inschrijven of meer informatie ontvangen over deze of andere trainingen? Dat kan!
Mail naar: security@securedbydesign.nl

SECURED BY DESIGN
UNITED BY KNOWLEDGE