academy

Pentesting with Kali Linux (PWK) - OSCP

Partner Training

Training code	TSTOCP-CE
Gesproken taal	Engels
Taal materiaal	Engels
Dagdelen	10
Kosten	€5.495,00 excl. BTW Geen extra kosten.

Wat is OSCP - Pentesting with Kali Linux (PWK)

Penetration Testing with Kali Linux (PWK) is een geavanceerde penetratietest training, ontwikkeld voor pentesters, netwerkbeheerders en security professionals die een serieuze stap willen zetten in de wereld van professioneel pentesten.
In deze unieke training maak je in uitdagende, virtuele pentesting labs gebruik van de meest actuele ethical hacking tools en technieken waarmee een volledige penetratietest van begin tot eind wordt nagebootst. Je krijgt hiertoe de beschikking over een targetrijke, diverse en kwetsbare netwerkomgeving.
Een OSCP is in staat om bestaande kwetsbaarheden te identificeren en daarop georganiseerde aanvallen uit te voeren op gecontroleerde en gefocuste wijze, eenvoudige Bash of Python scripts te schrijven, bestaande exploit code in zijn voordeel aan te passen, netwerk pivoting en data exfiltratie uit te voeren.

Voor wie is OSCP - Pentesting with Kali Linux (PWK)

Deze training is interessant voor cursisten met diverse achtergronden en persoonlijke doelen:

- Security Professionals,
- Penetratietesters,
- Ethical Hackers,
- Netwerkbeheerders

en iedere ervaren IT specialist die out-of-the box naar de beveiliging van een IT omgeving wil leren kijken.

Voorvereisten

In verband met het niveau van de training is kennis of ervaring op CEH niveau een absolute pré. Minimaal zijn een goed begrip van TCP/IP, netwerken en een redelijke vaardigheid met Linux vereist. Niet verplicht maar prettig om te hebben zijn bekendheid met Bash scripting en basis Perl of Python kennis

academy

Doelstellingen

Doelstellingen zijn:

- Gebruik meerdere technieken voor het verzamelen van informatie om doelen te identificeren en op te sommen met verschillende besturingssystemen en services
- Schrijf basisscripts en hulpmiddelen om te helpen bij het penetratietestproces.
- Analyseren, corrigeren, wijzigen, cross-compileren en overdragen van publieke exploitcode.
- Succesvolle aanvallen zowel op afstand als op de client uitvoeren.
- Identificeer en exploiteer kwetsbaarheden in XSS, SQL-injectie en bestandsinclusie in webapplicaties.
- Implementeer tunnelingstechnieken om firewalls te omzeilen.
- Aantonen van creatieve probleemoplossing en lateraal denken

Indien een copyright van derden van toepassing is op deze training, vind je het copyright op https://academy.capgemini.nl/trademarks

Op de producten en diensten die genoemd zijn in dit document zijn de Algemene Voorwaarden van Capgemini Academy van toepassing. Kijk voor de laatste versie op https://academy.capgemini.com/. De prijzen van genoemde producten en diensten zijn aan verandering onderhevig. Controleer ook voor de meest recente prijzen, onze website.

Over Academy

De professionals van Capgemini Academy bieden IT'ers wat ze nodig hebben. Onze mensen hebben een scherp oog voor drijfveren, aandacht voor talent en besef van specifieke omstandigheden. Ze bewegen tot beweging. Programma's die hun oorsprong vinden in het dagelijks werk van onze zowel didactisch als inhoudelijk onderlegde trainers wakkeren het vuur aan. Praktijkverhalen die vertellen hoe je problemen met IT en de mensen eromheen nou écht oplost doen de rest.

Een instituut als het onze helpt mensen en organisaties iedere dag weer het beste uit zichzelf en elkaar te halen. Bereidt hen voor op het zelfbewust aangaan van de uitdagingen van morgen. Stimuleert leer- en nieuwsgierigheid. Opdat IT'ers en hun werkgever beter, langer en intensiever met elkaar vooruit kunnen. Tot wederzijds genoegen.

Capgemini Academy. We transform IT professionals
academy.capgemini.nl

IN/3A-018.18