Publicatiedatum : 13/06/2024

Opleiding : Python voor Pentest

Praktijkcursus - 4d - 28u00 - Ref. PYH
Prijs : 2100 € V.B.

3,8 / 5

Deze cursus is bedoeld voor mensen die al een basiskennis hebben van de taal Python en behandelt de verschillende modules en toepassingen van Python bij inbraaktesten.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Het gemakkelijker maken om exploits te ontwikkelen in Python
- Taakverwerking en bewerkingen automatiseren
- Beveiligingsoplossingen omzeilen
- Verschillende talen koppelen met Python

Doelgroep

CISO's, beveiligingsconsultants, ingenieurs en technici, systeem- en netwerkbeheerders.

Voorafgaande vereisten

Kennis van Python.

Praktische modaliteiten

Leer methodes

Tijdens de sessie wordt het geleerde beoordeeld aan de hand van een reeks oefeningen (50-70% van de tijd).

Opleidingsprogramma

1 Python voor HTTP, verzoeken

- Ontwikkeling van een uitputtend zoeksysteem.
- Captcha omzeilen.

DEELNEMERS

CISO's, beveiligingsconsultants, ingenieurs en technici, systeem- en netwerkbeheerders.

VOORAFGAANDE VEREISTEN

Kennis van Python.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

2 Ontwikkeling van een BurpSuite Python-module

- Inleiding tot BurpSuite.
- Ontwikkeling van een passieve detectiemodule voor Web Application Firewalls.

3 Een blinde SQL-injectie exploiteren

- Bit-voor-bit extractie en gedragsanalyse.

4 Inleiding tot gedistribueerde taken

- Inleiding tot de Slowloris aanval.
- Ontwikkeling van een gedistribueerde Slowloris-exploit.

5 Python en HTTP-knoeien

- Inleiding tot MITMProxy.
- Ontwikkeling van een "SSL Striping" module.

6 Python en forensisch onderzoek

- Volatiliteit.
- Vleesmolen.
- Netwerk forensisch onderzoek met Scapy.

7 C en Python, Cython

- ctypes.
- Ontwikkeling van een Cython antivirus- en backdoormodule.

8 Antivirus en backdoors

- Shell-codes.
- Creatie van een geavanceerde achterdeur.

9 Bedrijfsketen

- Uitbuiting van meerdere kwetsbaarheden.
- Creatie van een complete exploit (POC).

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

Data en plaats

KLAS OP AFSTAND
2026 : 23 juni, 22 sep.

PARIS LA DÉFENSE
2026 : 23 juni, 22 sep.