Publicatiedatum : 07/01/2025

Opleiding : Hacking en beveiliging, niveau 2, deskundigheid

Praktijkcursus - 3d - 21u00 - Ref. HKE
Prijs : 2100 € V.B.

4,6 / 5

BEST

In deze cursus leer je geavanceerde hacktechnieken. Je zult shellcodes en payloads maken om kwetsbaarheden in toepassingen op besturingssystemen te misbruiken, zodat je een beter inzicht krijgt in kwetsbaarheden en het beveiligingsniveau van je systeem kunt verhogen om ze te verhelpen.

Pedagogische doelstellingen

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

- Recente aanvallen en systeemexploits begrijpen
- Moderne technieken begrijpen om applicatiebeveiliging te omzeilen
- Het misbruiken van een kwetsbaarheid in toepassingen op Linux- en Windows-systemen
- Shellcodes en payloads maken (Linux en Windows)

Doelgroep

Managers, beveiligingsarchitecten, systeem- en netwerkbeheerders. Pentesters.

Voorafgaande vereisten

Goede kennis van IS-beveiliging, C, Python en assembler is vereist.

Opleidingsprogramma

1 Stand van de techniek in aanval en verdediging

- Een beetje actueel nieuws: 5G, blockchain, slimme contracten, IoT's (verbonden objecten), AI, IPv4, IPv6.
- De nieuwste aanvalstechnieken.
- De nieuwste verdedigingsstrategieën.

DEELNEMERS

Managers, beveiligingsarchitecten, systeem- en netwerkbeheerders. Pentesters.

VOORAFGAANDE VEREISTEN

Goede kennis van IS-beveiliging, C, Python en assembler is vereist.

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 Van C naar assembler naar machinecode

- Wat is assembler en machinecode. Compileren.
- Hoe een processor werkt.
- De basis van assembler en de basis van de C-taal.
- Coderingsconcepten (adresseermodi, registers, instructies, bewerkingen, etc.).

3 Aanvallen van toepassingen

- De concepten van kwaadaardige software en malware (virussen, rootkits, enz.).
- Stand van zaken met betrekking tot backdoors op Windows en Unix/Linux.
- Het opzetten van backdoors en trojans.
- Shellcodes, TCP reverse shell, TCP bind shell.
- Shellcode codering, verwijderen van NULL bytes.
- Procesuitbuiting: buffer overflow, ROP, Dangling Pointers.
- Beveiliging en omzeilen: GS vlag, ASLR, PIE, RELRO, Safe SEH, DEP. Shellcodes met hardgecodeerde adressen, LSD.
- Advanced Metasploit: architectuur, functies, interfaces, workspaces, exploit schrijven, shellcode genereren.

Praktisch werk

Shellcode-exploitatie: bufferoverloop (Windows of Linux). Beveiligingen omzeilen. Een root-shell verkrijgen met verschillende soorten bufferoverloop. Metasploit gebruiken en shellcode genereren.

4 Analysetechnieken

- Statische analyse van binaire bestanden.
- Hulpmiddelen voor dynamische analyse.
- Veiligheid in de zandbak.
- Reverse engineering en debugging.
- Moderne verpakkers en cryptografen.

Praktisch werk

Analyse van malware met behulp van verschillende analysetechnieken.

5 Cryptoanalyse

- Cryptoanalyse concepten (processen, encryptie, etc.).
- Identificatie van algoritmen.
- Aanvallen op stream encryptie, ECB en CBC modi.
- Aanvallen via zijkanalen.
- Aanvallen op blockchain.

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 : 16 maa., 22 juni, 7 okt., 16 nov.

PARIS LA DÉFENSE
2026 : 16 maa., 22 juni, 7 okt., 16 nov.