Publicatiedatum : 16/02/2024

Opleiding : Hacken en pentesting: ingebedde architecturen

Praktijkcursus - 4d - 28u00 - Ref. HAE
Prijs : 2460 € V.B.

Meestal bestaat de basisarchitectuur uit een centrale verwerkingseenheid (CPU), een besturingssysteem (of specifieke software) en de bijbehorende connectiviteit: dit zijn allemaal onderdelen die kwetsbaar zijn voor aanvallen en die moeten worden beoordeeld en beschermd, zonder de tegenmaatregelen te vergeten die moeten worden ingezet.

Pedagogische doelstellingen

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

- De impact en omvang van een kwetsbaarheid bepalen
- De technieken begrijpen die hackers gebruiken en in staat zijn om hun aanvallen af te slaan
- Het beveiligingsniveau van een ingebedde architectuur meten
- Een penetratietest uitvoeren

Doelgroep

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

Voorafgaande vereisten

Goede kennis van IB-beveiliging, netwerken, systemen (met name Linux) en programmeren. Of kennis die gelijkwaardig is aan die van de cursus "Systeem- en netwerkbeveiliging, niveau 1" (ref. FRW).

Opleidingsprogramma

1 Een herinnering aan ingebedde architecturen

- Gewone en boordcomputersystemen.
- De verschillende soorten ingebedde architectuur.
- De verschillende beperkingen in verband met de oplossing aan boord.

DEELNEMERS

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

VOORAFGAANDE VEREISTEN

Goede kennis van IB-beveiliging, netwerken, systemen (met name Linux) en programmeren. Of kennis die gelijkwaardig is aan die van de cursus "Systeem- en netwerkbeveiliging, niveau 1" (ref. FRW).

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 Hacken en beveiliging

- Aanvalsvormen, modus operandi, actoren, problemen.
- Audits en penetratietests.

3 De geïntegreerde omgeving

- Netwerk: 4G, LTE, LoRA, WiFi, MQTT, 802.11.15.4, ZigBee, Z-Wave, 6LoWPAN en BLE (Bluetooth LE).
- Firmware, het besturingssysteem van het apparaat: Windows, Linux x86/x64 bits of Raspbian.
- Encryptie: beschermt communicatie en gegevens die op het apparaat zijn opgeslagen.
- Hardware: chip, chipset, opslag, JTAG, UART-poorten, sensoren, camera, enz.
- Architectuur: ARM, MIPS, SuperH, PowerPC.
- Systeemstructuur, onderdelen, bescherming en updates.

4 Kwetsbaarheden in ingebedde architecturen

- De zoektocht naar kwetsbaarheden.
- Authenticatiemechanismen.
- Koppelingen tussen een ingebed systeem en zijn omgeving (connectiviteit): netwerk, sensor en randapparatuur.
- De toepassingen en programma's op een ingebed systeem identificeren en gebruiken.
- Methodologie voor inbraaktesten.
- Tools: analysers, debuggers, disassemblers en decompilers.

Praktisch werk

Het veiligheidsniveau van een ingebedde architectuur meten.

5 Aanvallen

- Fysieke aanvallen.
- Uitrusting: toegang tot de verschillende onderdelen.
- Draadloze connectiviteit, communicatieprotocol. Emissieanalyse.
- Software: structuur van bestandssystemen, kwetsbaarheden in gehoste applicaties, toegang tot diensten via applicaties.
- Uitzonderingsafhandeling testen met behulp van een programma, uitputtingsaanvallen.
- Systeem herprogrammeren.
- Introductie van vervalste informatie.

Praktisch werk

Toegang krijgen tot een ingebed systeem via verschillende aanvallen. Een penetratietest uitvoeren.

6 Het auditrapport

- De inhoud.
- Secties die je niet over het hoofd mag zien.

Praktisch werk

Vul een vooraf ingevuld rapport in.

Data en plaats

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.

PARIS LA DÉFENSE
2026 : 9 juni, 20 okt.