Publicatiedatum : 23/08/2024

Opleiding : Hacken en pentesting: IoT

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

4,4 / 5

Het Internet of Things (IoT) ontwikkelt zich snel en maakt nu deel uit van ons dagelijks leven. Daarom is het een van de grootste uitdagingen voor IT-beveiliging. Daarom is het een van de grootste uitdagingen voor IT-beveiliging. We moeten op de hoogte zijn van hun kwetsbaarheden, zodat we de juiste respons kunnen geven en het beveiligingsniveau kunnen verhogen.

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 aangesloten object 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 IoT's (Connected Objects)

- De verschillende soorten IoT (Connected Objects).
- Draadloze protocollen (WiFi, enz.) en hun bereik (werkafstand). Koppelingen met M2M.
- Architecturen: ARM, MIPS, SuperH, PowerPC.

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 IoT-omgeving

- Netwerk: 4G, LTE, LoRA, WiFi, MQTT, 802.11.15.4, ZigBee, Z-Wave, 6LoWPAN en BLE (Bluetooth LE).
- Toepassing: webapp, mobiele app, web, mobiel of API (SOAP, REST).
- 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.

Praktisch werk
Verzamel de informatie (hardware, chip, etc.) waaruit het verbonden object bestaat.

4 Kwetsbaarheden

- De zoektocht naar kwetsbaarheden.
- Links tussen het verbonden object en een netwerk.
- Authenticatiemechanismen.
- Installatie zoeken en standaardwachtwoord.
- Methodologie voor inbraaktests voor IoT's (Connected Objects).
- Gereedschappen: logische analysers, debuggers, disassemblers en decompilers.

Praktisch werk
Het beveiligingsniveau van een IoT (Connected Object) meten.

5 Aanvallen

- Software (XSS, SQLi, command injection, slecht afgehandelde uitzonderingen en RCE of DoS geheugencorruptie aanvallen).
- Hardware (JTAG, SWD, UART, SPI, I2C-bus, enz.).
- Draadloze connectiviteit, communicatieprotocol. Emissieanalyse.

Praktisch werk
Toegang krijgen tot een verbonden object 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.

KLAS OP AFSTAND
2026 : 15 juni, 14 dec.

PARIS LA DÉFENSE
2026 : 15 juni, 14 dec.