Publicatiedatum : 05/04/2024

Opleiding : Hacken en beveiliging met CyberRange

Praktijkcursus - 5d - 35u00 - Ref. HCR
Prijs : 3120 € V.B.

In deze geavanceerde training leert u de essentiële technieken om het beveiligingsniveau van uw informatiesysteem te meten. Naar aanleiding van deze aanvallen leert u hoe u de juiste reactie kunt geven en het beveiligingsniveau van uw netwerk kunt verhogen.

Pedagogische doelstellingen

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

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

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 "Beveiliging van systemen en netwerken" (ref. SCR).

Praktische modaliteiten

Praktisch werk

De CyberRange van Airbus CyberSecurity wordt gebruikt om realistische scenario's met echte cyberaanvallen te maken en uit te spelen.

Opleidingsprogramma

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 "Beveiliging van systemen en netwerken" (ref. SCR).

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.

1 Hacken en beveiliging

- Aanvalsvormen.
- Bedieningsprocedures.
- Spelers en problemen.

2 Sniffing, interceptie, analyse, netwerkinjectie

- Anatomie van een pakket, tcpdump, Wireshark, tshark.
- Kaping en onderschepping van communicatie (man-in-the-middle, VLAN-aanvallen, honeypots).
- Pakketten: sniffen, lezen/analyse van een pcap, extractie van bruikbare gegevens, grafische weergaven.
- Scapy: architectuur, mogelijkheden, gebruik.
- De scenario's en tools die beschikbaar zijn op CyberRange.

Praktisch werk

Meeluisteren op het netwerk met sniffers. Scapy gebruiken (commandoregel, pythonscript): injecties, onderschepping, pcap lezen, scannen, DoS, man-in-the-middle (MITM).

3 Herkennen, scannen en opsommen

- Inlichtingen verzamelen, hot reading, darknet-exploitatie en social engineering.
- Herkenning van diensten, systemen, topologie en architectuur.
- Soorten scans, detectie van filters, firewalking, fuzzing.
- Camouflage door spoofing en bouncing, padidentificatie met traceroute, bronroutering.
- IDS- en IPS-ontwijking: fragmentatie, geheime kanalen.
- Nmap: scan en exporteer resultaten, opties.
- Andere scanners: Nessus, OpenVAS.
- De scenario's en tools die beschikbaar zijn op CyberRange.

Praktisch werk

Gebruik van het hulpprogramma nmap en detectie van filtering op het CyberRange-platform.

4 Webaanvallen

- OWASP: organisatie, hoofdstukken, Top10, handleidingen, hulpmiddelen.
- Ontdek de infrastructuur en bijbehorende technologieën, sterke en zwakke punten.
- Aan de clientzijde: clickjacking, CSRF, cookiediefstal, XSS, componenten (Flash, Java). Nieuwe vectoren.
- Serverzijde: authenticatie, sessiediefstal, injecties (SQL, LDAP, bestanden, commando's).
- Opname van lokale en externe bestanden, aanvallen en cryptografische vectoren.
- Omzeilen en omzeilen van bescherming: voorbeeld van WAF-omzeilingstechnieken.
- Burp Suite, ZAP, SQLmap, BeEF tools.
- Scenario's beschikbaar op CyberRange.

Praktisch werk

Implementatie van verschillende webaanvallen onder echte omstandigheden aan de server- en clientzijde met CyberRange.

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.

5 Aanvallen van toepassingen

- Metasploit: architectuur, functies, interfaces, workspaces.
- Exploit schrijven, shellcode genereren.

Data en plaats

KLAS OP AFSTAND
2026 : 20 apr., 27 juli, 2 nov.

PARIS LA DÉFENSE
2026 : 13 apr., 20 juli, 26 okt.