Publicatiedatum : 01/02/2024

Opleiding : Hacken en beveiliging, niveau 1

Praktijkcursus - 5d - 35u00 - Ref. HAC
Prijs : 3180 € V.B.

4,3 / 5

BEST

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 "Systeem- en netwerkbeveiliging, niveau 1" (ref. FRW).

Opleidingsprogramma

1 Hacken en beveiliging

- Aanvalsvormen, modus operandi, actoren, problemen.
- Audits en penetratietests, hun plaats in een ISMS.

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 Sniffing, interceptie, analyse, netwerkinjectie

- Anatomie van een pakket, tcpdump, Wireshark, tshark.
- Hijacken en onderscheppen 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.

Praktisch werk

Luisteren naar het netwerk met sniffers. Een mini packet interceptor bouwen in C. Scapy gebruiken (command line, python script): injecties, onderscheppen, pcap lezen, scannen, DoS, MitM.

3 Herkennen, scannen en tellen

- 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.

Praktisch werk

Het gereedschap nmap gebruiken, een NSE-script in LUA schrijven. Detectie van filtering.

4 Webaanvallen

- OWASP: organisatie, hoofdstukken, Top10, handleidingen, hulpmiddelen.
- Ontdek de infrastructuur en bijbehorende technologieën, sterke en zwakke punten.
- 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.

Praktisch werk

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

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 tijdens en na de operatie

- Aanval op Microsoft-authenticaties, PassTheHash.
- Van C naar assembler naar machinecode. Shellcodes.
- Shellcode codering, verwijderen van NULL bytes.
- Rootkits. Proces-exploits: Buffer Overflow, ROP, Dangling Pointers.
- Bescherming en omzeilen: Flag GS, ASLR, PIE, RELRO, Safe SEH, DEP. Shellcodes met hardgecodeerde/LSD-adressen.
- Metasploit: architectuur, functies, interfaces, workspaces, exploit schrijven, shellcode genereren.

Praktisch werk

Metasploit: werking, gebruik van de database. Msfvenom: genereren van shellcode, file trapping. Bufferoverloop onder Windows of Linux, werking met Meterpreter shellcode.

Data en plaats

KLAS OP AFSTAND
2026 : 20 apr., 20 apr., 22 juni, 22 juni, 24 aug., 14 sep., 21 sep., 21 sep., 5 okt., 30 nov., 30 nov.

PARIS LA DÉFENSE
2026 : 20 apr., 22 juni, 24 aug., 21 sep., 30 nov.

LILLE
2026 : 22 juni, 30 nov.