Publicatiedatum : 09/01/2024

Opleiding : Inbraakdetectie en SOC

Praktijkcursus - 4d - 28u00 - Ref. TRU
Prijs : 2520 € V.B.

3,8 / 5

Deze zeer praktische cursus presenteert de meest geavanceerde aanvalstechnieken tot nu toe en laat zien hoe je ze kunt detecteren. Aan de hand van aanvallen op geïdentificeerde doelwitten (webservers, clients, netwerken, firewalls, databases, etc.) leert u hoe u de meest geschikte reactie kunt lanceren. Je leert ook over het SOC-concept en alle tools die je nodig hebt als SOC-analist.

Pedagogische doelstellingen

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

- Analyse- en detectietechnieken identificeren en begrijpen
- De kennis verwerven die nodig is om verschillende tools voor inbraakdetectie in te zetten
- Oplossingen voor inbraakpreventie en -detectie implementeren
- De concepten en omgeving van een SOC begrijpen
- Weten hoe je analysetools moet gebruiken

Doelgroep

Systeem- en netwerktechnici en -beheerders.

Voorafgaande vereisten

Goede kennis van netwerken en beveiliging. Bekend zijn met de ANSSI-beveiligingshygiënegids. De introductiecursus cyberbeveiliging hebben afgerond.

Opleidingsprogramma

DEELNEMERS

Systeem- en netwerktechnici en -beheerders.

VOORAFGAANDE VEREISTEN

Goede kennis van netwerken en beveiliging. Bekend zijn met de ANSSI-beveiligingshygiënegids. De introductiecursus cyberbeveiliging hebben afgerond.

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 Netwerkprotocollen begrijpen

- Andere aspecten van de protocollen IP, TCP en UDP.
- Focus op ARP en ICMP.
- Geforceerde routering van IP-pakketten (bronroutering).
- IP-fragmentatie en regels voor hermontage.
- De noodzaak van serieus filteren.
- Uw servers beveiligen: een must.
- Technologische tegenmaatregelen: van filterende routers tot stateful inspection firewalls; van proxies tot reverse proxies.
- Een snel overzicht van oplossingen en producten.

Praktisch werk

Klassiek verkeer bekijken en analyseren. Verschillende sniffers gebruiken.

2 Aanvallen op TCP/IP

- Hoe hackers [[Spoofing]" IP.
- Denial of service-aanvallen uitvoeren.
- De TCP-techniek om het volgnummer te voorspellen.
- TCP-sessiediefstal: Hijacking (Hunt, Juggernaut).
- Begrijpen hoe hackers erin slagen om aanvallen op SNMP uit te voeren.
- TCP Spoofing aanval (Mitnick): demystificatie.

Praktisch werk

Injectie van pakketten die op het netwerk worden gemaakt. Deelnemers kunnen kiezen voor grafische tools, Perl, C of speciale scripts.

3 Inlichtingen verzamelen

- Zoeken naar sporen: Whois-databases, DNS-servers, zoekmachines raadplegen.
- Leer de technieken voor het instellen van serveridentificatie.
- De context begrijpen: resultaten analyseren, filterregels bepalen, specifieke gevallen.

Praktisch werk

Niet-intrusieve technieken gebruiken om informatie te zoeken over een potentieel doelwit (gekozen door de deelnemers). Gebruik van tools voor het scannen van netwerken.

4 Trojaanse paarden en backdoors detecteren

- Stand van zaken met betrekking tot backdoors op Windows en Unix. Wat is een backdoor?
- Hoe je backdoors en trojans instelt.
- Scripts naar clients downloaden, browserfouten uitbuiten.
- Covert Channels": client-server toepassing die ICMP gebruikt.
- Voorbeeld van communicatie met gedistribueerde Denial of Service-agenten.

Praktisch werk

Analyse van Loki, een client-server die ICMP gebruikt. Toegang tot privégegevens met je browser.

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 en uitbuiten van kwetsbaarheden

- De controle over een server overnemen: kwetsbaarheden vinden en misbruiken.
- Voorbeelden van het opzetten van "achterdeuren" en het verwijderen van sporen.
- Hoe omzeil ik een firewall (netcat en bounces)?
- Onderzoekstechnieken voor dienstweigering.
- Wat is DDoS (Distributed Denial of Service)? Hoe organiseren hackers zich om zo'n aanval uit te voeren?
- Buffer overflow aanvallen.
- Kwetsbaarheden in de broncode misbruiken. Vergelijkbare technieken: "Format String", "Heap Overflow".
- Wat zijn de kwetsbaarheden in webapplicaties? Hoe kunnen ze worden gedetecteerd en beschermd?
- Hoe kwaadwillenden erin slagen om informatie uit een database te stelen.
- Wat zijn RootKits?

Praktisch werk

Exploitatie van de bug gebruikt door de "Code Red" worm. Het verkrijgen van een root-shell met behulp van verschillende soorten bufferoverloop. Testen van een denial of service (Jolt2, Ssping). Netcat gebruiken om een firewall te omzeilen. SQL-injectietechnieken gebruiken om de webauthenticatie te omzeilen.

6 Het SOC (Beveiligingscentrum)

- Wat is een SOC?
- Waar wordt het voor gebruikt? Waarom gebruiken steeds meer bedrijven het?
- SOC-functies: logging, monitoring, audit en beveiligingsrapportage, analyse na een incident.
- De voordelen van een SOC.
- Oplossingen voor een SOC.
- SIM (Security Information Management).
- SIEM (Security Information and Event Management).
- SEM (Security Event Management).
- Voorbeeld van een monitoringstrategie.

7 De taak van de SOC-analist

- Wat doet een SOC-analist?
- Welke vaardigheden heeft het?
- Waarschuwingen en gebeurtenissen bewaken en sorteren.
- Prioriteit geven aan waarschuwingen.

8 Hoe ga je om met een incident?

- De tekenen van een succesvolle IS-inbraak.
- Wat hebben de hackers bereikt? Hoe ver zijn ze gekomen?
- Hoe reageer je op een succesvolle inbraak?
- Welke servers worden beïnvloed?
- Zoek het ingangspunt en vul het.
- De Unix/Windows gereedschapskist voor het vinden van bewijs.
- Opschonen en terugbrengen naar productie van gecompromitteerde servers.

Data en plaats

KLAS OP AFSTAND
2026 : 9 juni, 15 sep., 17 nov.

PARIS LA DÉFENSE
2026 : 9 juni, 15 sep., 17 nov.