Publicatiedatum : 10/06/2024

Opleiding : Een Linux/Unix-systeem beveiligen

Praktijkcursus - 3d - 21u00 - Ref. SRX
Prijs : 1800 € V.B.

4,6 / 5

Deze zeer praktische cursus laat je zien hoe je een beveiligingsstrategie opstelt, Linux-servers beveiligt en een beveiligingsniveau handhaaft. De cursus behandelt onder andere het beveiligen van een geïsoleerd systeem, het beveiligen van het bedrijfsnetwerk en wat je moet weten om een beveiligingsaudit uit te voeren.

Pedagogische doelstellingen

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

- Het beveiligingsniveau van uw Linux/Unix-systeem meten
- Inzicht in systeembeveiligingsoplossingen
- Beveiliging implementeren voor een Linux/Unix-toepassing
- Netwerkbeveiliging instellen

Doelgroep

Systeem- en netwerktechnici en -beheerders.

Voorafgaande vereisten

Goede kennis van systemen en netwerkbeheer.

Praktische modaliteiten

Praktisch werk

De vele oefeningen worden uitgevoerd op een netwerk van Unix en Linux servers.

Opleidingsprogramma

DEELNEMERS

Systeem- en netwerktechnici en -beheerders.

VOORAFGAANDE VEREISTEN

Goede kennis van systemen en netwerkbeheer.

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 Inleiding

- Waarom een systeem beveiligen?
- Een veilige authenticatiestrategie definiëren.
- De verschillende versleutelingsalgoritmen. Een wachtwoord versleutelen. Wachtwoord verifiëren.
- Voorbeelden van woordenboekaanvallen.

2 Veiligheid en Open Source

- Correcties worden snel aangebracht en bugs worden openbaar gemaakt.
- De aanpak van de hacker: ken de mazen, weet hoe aan te vallen.
- Voorbeeld van een oplossing voor kwetsbaarheden en beveiliging. Welke oplossing?

3 Te volledige installatie: Linux-voorbeeld

- Debian, RedHat en andere distributies.
- Vermijd de valkuil van eenvoudige installatie.
- Lichtere kernel. Stuurprogramma's voor randapparatuur.

Praktisch werk

Faciliteiten optimaliseren met het oog op veiligheidsbeheer.

4 Lokale systeembeveiliging

- Voorbeelden van opzet en onoplettendheid.
- Standaard lage permissiviteit. Controle op bestandsrechten, effectieve scripts en commando's voor diagnostiek.
- Alleen-lezen FS: bestandskenmerken, beschikbaarheid en interesse. Tripwire-tools.
- Hoe lang bewaar je logboeken?
- Het hulpmiddel voor loganalyse: logwatch. Reageren in realtime: voorbeeldscript. RPM gebruiken als HIDS.
- PAM instellen in verschillende contexten.
- Inperking van procesuitvoering. Terminologie: DAC, MAC, RBAC, context, model, enz.

Praktisch werk

Werk aan rechten, logboeken en processen.

5 Netwerkbeveiliging

- Een firewall gebruiken? Wrappers gebruiken?
- Filters instellen voor toegang tot services.
- Een firewall veilig configureren.
- Diagnostische commando's. Een NetFilter firewall opzetten onder Linux.
- iptables filosofie en syntaxis.
- De xinetd super-server. Wrapper toegangsbeperkingen, traceerbestanden.
- Een audit van actieve diensten uitvoeren. Ssh.

Praktisch werk

Een firewall configureren. Functionele diensten auditen.

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.

6 Hulpprogramma's voor beveiligingsaudits

- Merkgebonden producten en gratis alternatieven.
- Crack, John the Ripper, Qcrack.
- HIDS- en NIDS-inbraakdetectiesystemen.
- Test de kwetsbaarheid met Nessus.
- Een veiligheidshulpmiddel implementeren.

Praktisch werk
Gebruik van een aantal tools.

Data en plaats

KLAS OP AFSTAND
2026 : 25 maa., 4 mei, 24 juni, 7 okt., 16 dec.

PARIS LA DÉFENSE
2026 : 24 juni, 7 okt., 16 dec.