

Opleiding : TLS/SSL, installatie, configuratie en implementatie

Praktijkcursus - 2d - 14u00 - Ref. LSL

Prijs : 1480 € V.B.

★★★★☆ 3,9 / 5

De TLS (Transport Layer Secure) standaard is het meest gebruikte protocol voor het beveiligen van applicatie-uitwisselingen. Deze cursus geeft je een goed begrip van de architectuur, het protocol en de beveiligingsdiensten van TLS. Je implementeert het aan de client- en serverzijde van beveiligde uitwisselingen.

Pedagogische doelstellingen

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

- ✓ Het TLS-protocol implementeren
- ✓ Sterke en veilige configuratie van TLS-clients en -servers
- ✓ TLS-verkeer analyseren
- ✓ Aanvallen op TLS begrijpen

Doelgroep

Systeem- en netwerktechnici en -beheerders, beveiligingsarchitecten en beveiligingsmanagers.

Voorafgaande vereisten

Basisvaardigheden op het gebied van computer en netwerk.

Opleidingsprogramma

1 Cryptografie en beveiligingsdiensten

- Terminologie en cryptografische principes.
- Belangrijkste cryptografische algoritmen en hun gebruik in TLS: AES, DHE, ECC, RSA, DSA.
- Hashfunctie (MD5, SHA1, SHA2, SHA3) met en zonder sleutel (Hmac).
- Cryptografische besturingsmethoden.
- Cryptanalyse en aanvallen op cryptografische functies.
- Beveiligingsdiensten: vertrouwelijkheid, authenticatie, integriteit.

Praktisch werk

Encryptie en decryptie met OpenSSL en cryptanalyse.

DEELNEMERS

Systeem- en netwerktechnici en -beheerders, beveiligingsarchitecten en beveiligingsmanagers.

VOORAFGAANDE VEREISTEN

Basisvaardigheden op het gebied van computer en netwerk.

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 Certificaten en digitale handtekeningen

- Digitale handtekening.
- Aanvallen op publieke sleutels.
- Certificaten en PKCS12 sleutelimplementatie.
- Certificaatprofielen voor TLS.

Praktisch werk

Certificaatontwerp (client- en serverkant) en PKCS12 aan de clientkant.

3 TLS-architectuur en -services

- Positionering van de verschillende versies: SSLv3, TLS1.0, TLS1.1, TLS1.2.
- Architectuur, beveiligingsprotocol en -diensten, TLS-uitwisselingen.
- Cijfersuites configureren.

Praktisch werk

Een TLS-client configureren en TLS-verkeer analyseren.

4 Het TLS-protocol configureren en implementeren

- Client- en server-side configuratie.
- Configuratie voor eenvoudige serverauthenticatie.
- Certificaten implementeren en versleutelingsalgoritmen configureren aan de serverkant.
- Serverauthenticatie, configuratie van certificatenwinkel.

Praktisch werk

TLS configureren en implementeren op de Apache webserver.

5 Geavanceerde TLS-protocoldiensten

- TLS-uitbreidingen en -functies.
- Verschillende verificatiemethoden: OpenPGP certificaat, PSK.
- Ticket en sessie heropenen.
- Benchmarking van sessies.
- De TLS-client configureren (PKCS12).

Praktisch werk

TLS clients en servers configureren voor sterke en wederzijdse authenticatie. Implementatie van uitbreidingen, prestatieanalyse.

6 Veiligheidsanalyse en vooruitzichten voor het TLS-protocol

- Aanvallen op het TLS-protocol.
- Beste praktijk, configuratiecontrole.
- Inleiding tot het DTLS-protocol.
- Presentatie van de toekomstige versie van TLS 1.3.

Praktisch werk

Het TLS protocol doorlichten. Aanvallen op TLS implementeren. DTLS configureren en implementeren.

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.

2026 : 26 maa., 18 juni, 28 sep., 3 dec.

2026 : 26 maa., 18 juni, 28 sep., 3 dec.