Publicatiedatum : 01/08/2024

Opleiding : Wireshark - Controle en prestaties

Praktijkcursus - 3d - 21u00 - Ref. RUE
Prijs : 2020 € V.B.

4,1 / 5

Wireshark maakt regelmatige, diepgaande analyse van netwerken mogelijk om potentiële problemen op te sporen. In deze cursus leer je hoe je Wireshark kunt gebruiken om protocollen te controleren. Zodra de informatie is vastgelegd, kan deze worden bekeken op de grafische interface van het programma of via de ATS tshark-modus.

Pedagogische doelstellingen

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

- Inzicht in analyse van netwerkstromen
- Weten hoe je netwerkactiviteit kunt filteren en analyseren
- Rapporten maken
- Hoe Wireshark gebruiken om netwerkprestatieproblemen te diagnosticeren

Doelgroep

Systeembeheerders, netwerkbeheerders en ontwikkelaars.

Voorafgaande vereisten

Basiskennis van TCP/IP.

Praktische modaliteiten

Leer methodes

Training die theorie en praktijk afwisselt. Tijdens de hele cursus wordt veel praktisch werk gedaan.

Opleidingsprogramma

DEELNEMERS

Systeembeheerders, netwerkbeheerders en ontwikkelaars.

VOORAFGAANDE VEREISTEN

Basiskennis van TCP/IP.

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 Een herinnering aan de basis

- Communicatiemethoden (unicast, multicast, broadcast).
- Topologieën en toegangscontrole. OSI-model.
- Format d'une trame Ethernet. Taille et signification (Runt, Giant…) et le protocole ARP.
- Laag 2 protocol (802.3, 802.1p, 802.1q, 802.1ad). Laag 2 multicast.
- IP pakketformaat.
- Adresses particulières (loopback). Adresses de multicast (adresses connues), méthode de diffusion.
- ICMP-protocol (rol en analyse van antwoorden).

2 Het Wireshark-scherm

- Werkbalk.
- Filterzone.
- Weergavegebied verpakking.
- Veld dat de inhoud van het geselecteerde pakket in hexadecimaal weergeeft.
- Statusbalk (toegang tot expertmodus, annotaties, toont aantal vastgelegde pakketten en huidig profiel).

3 Analysetaken met Wireshark

- Netwerkcommunicatie vastleggen in "duidelijke tekst" (bijv. Telnet, HTTP).
- Controleer welke applicaties door bepaalde hosts worden gebruikt.
- Definieer een referentiepunt voor netwerkcommunicatie.
- Controleer of bepaalde netwerkservices goed werken.
- Identificeer wie verbinding wil maken met het draadloze netwerk.
- Onverwacht verkeer vastleggen. Host- of netwerkverkeer vastleggen en analyseren.
- Bestanden die via FTP of HTTP zijn overgedragen bekijken en opnieuw samenvoegen. VoIP-communicatie bekijken en beluisteren.

4 Problemen oplossen met Wireshark

- Identificeer abnormale vertragingen.
- TCP-problemen identificeren.
- HTTP-problemen detecteren.
- Toepassingsfouten detecteren.
- Genereer grafieken.
- Identificeer verzadigde bufferproblemen.
- Problemen met dubbele IP-adressen detecteren.
- Problemen met het DHCP-protocol of de DHCP-relay identificeren.

5 Taken voor beveiligingsanalyse

- Toepassingen detecteren die niet-standaard poorten gebruiken.
- Identificeer verkeer dat afkomstig is van of gaat naar een verdachte host.
- Machines identificeren die een IP-adres proberen te krijgen.
- Identificeer een herkenningsproces op het netwerk.
- Externe adressen op een kaart vinden en plaatsen.
- Bestudeer een TCP- of UDP-conversatie tussen een client en een server.
- Zoek bekende handtekeningen van aanvallen op je netwerk.

Data en plaats

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.

KLAS OP AFSTAND
2026 : 4 mei, 29 juni, 9 sep., 16 nov.

PARIS LA DÉFENSE
2026 : 4 mei, 29 juni, 9 sep., 16 nov.