Wireshark - Audit et performance

Cours Pratique de 3 jours - 21h
Réf : RUE - Prix 2024 : 2 290CHF HT

Wireshark permet une analyse régulière et approfondie des réseaux pour identifier d'éventuels problèmes. Ce cours vous permettra de prendre en main Wireshark pour vérifier des protocoles. Après la capture des informations, ces dernières sont consultables sur l'interface graphique du programme ou via le mode ATS tshark.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre l'analyse des flux réseau

Savoir filtrer et analyser l'activité du réseau

Savoir produire des rapports

Savoir utiliser Wireshark pour diagnostiquer des problèmes de performance du réseau

MÉTHODES PÉDAGOGIQUES

Formation alternant théorie et pratique. De nombreux travaux pratiques sont réalisés tout au long de la formation.

LE PROGRAMME

dernière mise à jour : 10/2020

1) Rappels des fondamentaux

- Méthodes de communications (unicast, multicast, broadcast).
- Les topologies et le contrôle d'accès. Modèle de l'OSI.
- Format d'une trame Ethernet. Taille et signification (Runt, Giant…) et le protocole ARP.
- Protocole de couche 2 (802.3, 802.1p, 802.1q, 802.1ad). Multicast de couche 2.
- Format d'un paquet IP.
- Adresses particulières (loopback). Adresses de multicast (adresses connues), méthode de diffusion.
- Protocole ICMP (rôle et analyse des réponses).

2) L'écran de Wireshark

- Barre d'outils.
- Zone de filtrage.
- Zone d'affichage des paquets.
- Zone d'affichage du contenu du paquet sélectionné en hexadécimal.
- Barre d'état (accès au mode expert, aux annotations, affiche le nombre de paquets capturés et le profil en cours).

3) Les tâches d'analyse avec Wireshark

- Capture des communications réseaux en "clear text" (exemple Telnet, HTTP).
- Vérifier quelles sont les applications utilisées par certains hôtes.
- Définir un point de référence pour la communication réseau.
- Vérifier le bon fonctionnement de certains services du réseau.
- Identifier qui veut se connecter au réseau sans-fil.
- Capturer du trafic inattendu. Capturer et analyser le trafic d'un hôte ou d'un réseau.
- Visualiser et réassembler des fichiers transférés par FTP ou HTTP. Visualiser et écouter des communications en VoIP.

PARTICIPANTS

Administrateurs système, administrateurs réseau et développeurs.

PRÉREQUIS

Connaissances de base de TCP/IP.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

4) Les tâches de dépannage avec Wireshark

- Identifier des délais anormaux.
- Identifier des problèmes TCP.
- Détecter des problèmes HTTP.
- Détecter des erreurs applicatives.
- Générer des graphiques.
- Identifier des problèmes de buffer saturés.
- Détecter des problèmes d'adresses IP dupliquées.
- Identifier des problèmes liés au protocole DHCP ou au relais DHCP.

5) Les tâches d'analyse de sécurité

- Détecter des applications utilisant des ports non-standard.
- Identifier du trafic en provenance ou à destination d'un hôte suspect.
- Identifier les machines essayant d'obtenir une adresse IP.
- Identifier un processus de reconnaissance sur le réseau.
- Localiser et placer sur une carte des adresses externes.
- Examiner une conversation TCP ou UDP entre un client et un serveur.
- Localiser des signatures connues d'attaques sur votre réseau.

LES DATES

CLASSE À DISTANCE
2024 : 03 juin, 16 sept., 25 nov.